Network Camera
User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision Website (*https://www.hikvision.com/*).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

HDMI: The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMILogo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS." HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

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

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

Safety Instruction

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

Laws and Regulations

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

Transportation

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

Power Supply

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

System Security

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

Battery

- Improper use or replacement of the battery may result in explosion hazard.
- Replace with the same or equivalent type only. Dispose of used batteries in conformance with the local codes.

Maintenance

- If the product does not work properly, please contact your dealer or the nearest service center. We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.

- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.

Usage Environment

- Make sure the running environment meets the requirement of the device. The operating temperature shall be -30° to 60° C (-22° to 140° F), and the operating humidity shall be 95% or less, non-condensing.
- When any laser equipment is in use, make sure that the device lens is not exposed to the laser beam, or it may burn out.
- Do not expose the device to high electromagnetic radiation or dusty environments.
- For an indoor-only device, place it in a dry and well-ventilated environment.
- Do not aim the lens at the sun or any other bright light.

Emergency

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

Time Synchronization

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

Contents

Chapter 1 System Requirements

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

- **Operating System**: Microsoft Windows XP SP1 and above version
- **CPU**: 2.0 GHz or higher
- **RAM**: 1 GB or higher
- **Display**: 1024×768 resolution or higher
- **Web Browser**: Internet Explorer 8.0 and above version, Mozilla Firefox 30.0 to 51, or Google Chrome 31 to 51

Chapter 2 Device Activation and Accessing

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

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

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start
Access www.hikvision.com to download the SADP software to install.

Steps

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

STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

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

5. Click **OK**. **Device Status** changes to **Active**.
6. Optional: Change the network parameters of the device in **Modify Network Parameters**.

2.2 Activate the Device via Browser

You can access and activate the device via a Web browser.

Steps

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

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

set the IP address ofthe PC to 192.168.1.100.

3. Input 192.168.1.64 in the browser.

4. Set device activation password.

STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

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

5. Click **OK**.

6. Input the activation password to log in to the device.

7. Optional: Go to **Configuration** → **Network** → **Basic** → **TCP/IP** to change the IP address of the device to the same segment of your network.

2.3 Login

Log in to the device via a Web browser.

2.3.1 Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	• Internet Explorer 8+ • Google Chrome 57 and earlier version • Mozilla Firefox 52 and earlier version	Follow pop-up prompts to complete plug-in installation.
	• Google Chrome 57+ • Mozilla Firefox 52+	Click Download Plug-in to download and install plug-in.
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+	Plug-in installation is not required. Go to **Configuration** → **Network** → **Advanced Settings** → **Network Service** to enable WebSocket or Websockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

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

2.3.2 Admin Password Recovery

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

You can reset the password by setting the security question or e-mail.

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

Security Question

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

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

E-Mail

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

2.3.3 Illegal Login Lock

Improves the security when accessing the device via the Internet.

The admin user can set the login attempts with a wrong password. When your login attempts with a wrong password reaches the set times, the device locks.

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

Chapter 3 Live View

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

2.4 Live View Parameters

Supported functions vary by model.

2.4.1 Enable and Disable Live View

This function quickly enables or disables live view of all channels.

- Click to start live view of all channels.
- Click to stop live view of all channels.

2.4.2 Adjust Aspect Ratio

Steps

1. Click Live View.
2. Click to select the aspect ratio.
   - 4:3 refers to 4:3 window size.
   - 16:9 refers to 16:9 window size.
   - refers to original window size.
   - refers to self-adaptive window size.
   - refers to original ratio window size.

2.4.3 Live View Stream Type

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

2.4.4 Select the Third-Party Plug-in

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

Steps

1. Click Live View.
2. Click to select the plug-in.

NOTE: When you access the device via Internet Explorer, select Webcomponents or QuickTime. When you access the device via other browsers, select Webcomponents, QuickTime, VLC, or MJPEG.

2.4.5 Window Division

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

2.4.6 Light

Click to turn on or turn off the illuminator.

2.4.7 Count Pixel

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

Steps

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

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

2.4.8 Start Digital Zoom

Detailed information of any region in the image.

Steps

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

2.4.9 Auxiliary Focus

Used for motorized devices. It can improve the image if the device cannot focus clearly.

For devices that support ABF, adjust the lens angle, then focus and click the ABF button on the device. The device will then focus clearly.

Click to focus automatically.

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

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

2.4.10 Lens Initialization

Lens initialization is used on devices equipped with a motorized lens. This function can reset the lens when long time zoom or focus results in a blurred image. This function varies by model.

Manual Lens Initialization

Click to operate lens initialization.

Auto Lens Initialization

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

2.4.11 Quick Set Live View

Quick setup of PTZ, display settings, OSD, video/audio, and VCA resource settings on the live view page.

Steps

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

   NOTE: This function is supported only by certain models.

2.4.12 Lens Parameters Adjustment

Adjusts the lens focus, zoom, and iris.

- **Zoom**
  - Click , and the lens zooms in.
  - Click , and the lens zooms out.
- **Focus**
  - Click , then the lens focuses far, and distant objects are clear.
  - Click , then the lens focuses near, and nearby object are clear.

- **PTZ Speed**
  - Slide  to adjust the speed of the pan/tilt movement.
- **Iris**
  - When the image is too dark, click to enlarge the iris.
  - When the image is too bright, click to stop down the iris.

2.4.13 Conduct 3D Positioning

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

Steps

1. Click to enable the function.
2. Select a target area in live image.
   - Left click on a point on the 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 view: 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 view: 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.

2.5 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 a stable network environment.
- **UDP**
  UDP is suitable for an unstable network environment that does not demand high video fluency.
- **MULTICAST**
  MULTICAST is suitable for situations in which there are multiple clients. You should set the multicast

address for them before selection.

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

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

3. Click **OK**.

2.6 Set Smooth Streaming

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

Before You Start

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

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

Steps

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

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

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

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

4. Save the settings.

Chapter 4 Video and Audio

This chapter introduces configuring video and audio related parameters.

4.1 Video Settings

This section introduces setting video parameters such as stream type, video encoding, and resolution.

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

4.1.1 Stream Type

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

Main Stream
This stream is the best stream performance the device supports. It usually offers the best resolution and frame rate the device can achieve. But, high resolution and frame rate usually mean larger storage space and higher bandwidth requirements in transmission.

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

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

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

Steps

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

After restoring the device (not restored to default settings), the quantity of custom video streams and their names are kept, but the related parameters are restored.

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

   NOTE: Up to 32 letters and symbols (except &, <, >, ', or ") are allowed for the stream name.
3. Customize the stream parameters (i.e., resolution, frame rate, max. bitrate, video encoding).
4. Optional: Add stream description as needed.
5. Optional: If a custom stream is not needed, click × to delete it.
6. Click **Save**.

4.1.2 Video Type

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

Video
Only video content is contained in the stream.

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

4.1.3 Resolution

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

4.1.4 Bitrate Type and Max. Bitrate

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

Variable Bitrate
The device automatically adjusts the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate, but it guarantees the image quality of complex scenes.

4.1.5 Video Quality

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

4.1.6 Frame Rate

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

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

4.1.7 Video Encoding

The compression standard the device adopts for video encoding.

NOTE: Available compression standards vary by model.

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

- **H.264+**
  H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can

estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50 percent with the same maximum bitrate in most scenes.

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

NOTE: When H.264+ is enabled, **Video Quality**, **I Frame Interval**, **Profile,** and **SVC** are not configurable.

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

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

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

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

- **I-Frame Interval**
  Defines the number of frames between two I-frames.

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

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

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

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

- **MPEG4**
  MPEG4, referring to MPEG-4 Part 2, is a video compression format developed by the 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, the higher the quality of the image, and the requirement for network bandwidth is also higher.

4.1.8 Smoothing

The stream smoothness. The higher the smoothing value, the better the stream fluency, though the video quality may not be satisfactory. The lower the value of the smoothing, the higher the stream quality, though it may appear less fluent.

4.2 ROI

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

4.2.1 Set ROI

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

Before You Start
Check the video coding type. ROI is supported when the video coding type is H.264 or H.265.

Steps

1. Go to **Configuration** → **Video/Audio** → **ROI**.
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** in **Fixed Region** to draw the 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, the clearer the detected region image.

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

4.2.2 Set Face Tracking ROI

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

Steps

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

   NOTE: ROI level means the image quality enhancing level. The larger the value, the better the image quality.

4. Click **Save**.

4.2.3 Set Target Tracking ROI

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

Before You Start
Go to **Configuration** → **PTZ** → **Smart Tracking** to set the smart tracking settings.

Steps

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

4.2.4 Set License Plate Tracking ROI

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

Steps

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

NOTE: ROI level means the image quality enhancing level. The larger the value, the better the image quality.

4. Click **Save**.

4.3 Display Info. on Stream

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

Steps

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

4.4 Audio Settings

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

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

4.4.1 Audio Encoding

Select the audio encoding compression of the audio.

4.4.2 Audio Input

NOTE: Connect the audio input device as required.

The audio input display varies by model.

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

4.4.3 Audio Output

NOTE: Connect the audio output device as required.

This is a switch of the device audio output. You can adjust the output volume as required. When it is disabled, all device audio cannot output. The audio output display varies by model.

4.4.4 Environmental Noise Filter

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

4.5 Two-way Audio

Realizes 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 a built-in microphone and speaker, the two-way audio function can be enabled directly.

Steps

1. Click **Live View**.
2. Click on the toolbar to enable the two-way audio function of the camera.
3. Click and select , then move the slider to adjust the volume.
4. Click to disable the two-way audio function.

4.6 Display Settings

Parameter settings to adjust image features.

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

Click **Default** to restore the settings.

4.6.1 Scene Mode

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

- **Image Adjustment**
  Adjust the **Brightness**, **Saturation**, **Hue**, **Contrast**, and **Sharpness** to best display the image.
- **Exposure Settings**
  Exposure is controlled by the combination of iris, shutter, and photo sensibility. You can adjust the image effect by setting exposure parameters.

  In manual mode, you need to set **Exposure Time**, **Gain**, and **Slow Shutter**.
- **Focus**
  Adjusts the focus mode and the minimum focus distance.

4.6.2 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.

- **Min. Focus Distance**
  When the distance between the scene and lens is shorter than the Min. Focus Distance, the lens does not focus.

- **Day/Night Switch**
  The Day/Night Switch function can provide color images in the day mode and black/white images in the night mode. The switch mode is configurable.

- **Day**
  The image is always in color.

- **Night**
  The image is always in black/white.

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

- **Scheduled-Switch**
  Set the **Start Time** and the **End Time** to define the day mode duration.

- **Triggered by Alarm Input**
  Two trigger modes are available: **Day** and **Night**. For example, if the trigger mode is **Night**, the image turns black and white when the device receives an alarm input signal.

  NOTE: The Day/Night Switch function varies by model.

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

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

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

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

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

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

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

- **WDR**
  WDR (Wide Dynamic Range) provides clear images in environments with strong illumination differences.

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

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

- **HLC**
  When the bright area of the image is overexposed and the dark area is underexposed, enable HLC (High Light Compression) to weaken the bright area and brighten the dark area, to achieve light balance of the overall picture.

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

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

  - **Normal**

    Set the DNR level to control the noise reduction. A higher level means a stronger degree of reduction.

  - **Expert**

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

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

- **EIS (Electronic Image Stabilization)**
  Increase the stability of the video image by using jitter compensation technology.

- **Mirror**
  When the live view image is the reverse of the actual scene, this function reorients the display to

show the image normally. Select the mirror mode as needed.

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

4.6.3 Image Parameters Switch

The device automatically switches image parameters in set time periods.

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

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

Steps

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

   NOTE: For Linked Scene configuration, refer to *Scene Mode*.
3. Click **Save**.

4.6.4 Video Standard

Video standard is an ability of a video card or video display device to define the number of colors that are shown and the resolution. The two most common video 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.

4.6.5 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.

Set the output mode to ON/OFF to control the output.

4.7 OSD

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

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

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

- **Displayed Information**
  Set camera name, date, week, and their related display format.
- **Text Overlay**
  Set customized overlay text on image.
- **OSD Parameters**
  Set OSD parameters such as **Display Mode**, **OSD Size**, **Font Color**, and **Alignment**.

4.8 Set Privacy Mask

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

Steps

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

NOTE: Up to four areas are supported for setting.

4.9 Overlay Picture

Overlay a customized picture on live view.

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

Steps

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

NOTE: The picture with a red rectangle will appear in live view after a successful upload.

3. Check Enable Picture Overlay.
4. Drag the picture to adjust its position.

5. Click **Save**.

4.10 Set Target Cropping

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

Steps

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

   NOTE: After enabling target cropping, the third stream resolution cannot be configured.
3. Select a **Cropping Resolution**. A red frame appears in the live view.
4. Drag the frame to the target area.
5. Click **Save**.

   NOTE: Only certain models support target cropping, and the function varies by camera model.

   Some functions may be disabled after enabling target cropping.

Chapter 5 Video Recording and Picture Capture

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

5.1 Storage Settings

This section introduces configuring several common storage paths.

5.1.1 Set Memory Card

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

Before You Start

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

Steps

1. Go to the storage management setting page: **Configuration** → **Storage** → **Storage Management** → **HDD Management**.
2. Select the memory card, and click **Format** to start initializing the memory card.

   NOTE: The memory card **Status** turns to **Normal** from **Uninitialized**, which means the memory card can be used normally.
3. Optional: Define the memory card **Quota**. Input the quota percentage for different contents according to your need.
4. Click **Save**.

5.1.2 Detect Memory Card Status

Detects the status of a Hikvision memory card, and receive notifications when your memory card is detected to be abnormal.

Before You Start

Install a memory card in the device.

Steps

1. Go to the memory card detection setting page: Configuration → Storage → Storage Management → Memory Card Detection.
2. Click Status Detection to check the Remaining Lifespan and Health Status of your memory card.
   - **Remaining Lifespan**: The percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. Change the memory card if the remaining lifespan is not enough.

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

  NOTE: Change the memory card when the health status is not "good."

3. Click **R/W Lock** to set the reading and writing authority to the memory card.

   1) Add a Lock. Set the **Lock Switch** to ON.

   2) Enter the password.

   3) Click **Save**

5.1.3 Unlock

NOTE: If you use the memory card on the camera 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 camera, go to **HDD Management** interface to unlock the memory card manually. Select the memory card, click the **Unlock** button next to the **Format** button, then enter the correct password to unlock it.

1. Remove the Lock. Set the **Lock Switch** to OFF.
2. Enter the password in **Password Settings**.
3. Click **Save**.

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

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

If the camera, which adds a lock to a memory card, is restored to the factory settings, you can go to the **HDD Management** interface to unlock the memory card.

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

5.1.4 Set FTP

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

Before You Start
Get the FTP server address.

Steps

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

2. Configure FTP settings.

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

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

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

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

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

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

5.1.5 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.

Steps

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

   - **Server Address**: The IP address of the network disk.
   - **File Path**: The saving path of network disk files.
   - **Mounting Type**: Select file system protocol according to the operation system.

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

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

5. Click **Save**.

5.1.6 eMMC Protection

If you enable eMMC protection, the lifespan of the eMMC is displayed.

5.1.7 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 supported only by certain models.

Steps

> **CAUTION:** If cloud storage is enabled, the pictures are stored in the cloud storage server preferentially.

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 storage server.
Server IP	The IP address of the cloud storage server. It supports IPv4 address.
Serve Port	The port of the cloud storage server. 6001 is the default port and you are not recommended to edit it.
User Name and Password	The user name and password of the cloud storage server.
Picture Storage Pool ID	The ID of the picture storage region in the cloud storage server. Make sure storage pool ID and the storage region ID are the same.

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

5. Click **Save**.

5.2 Video Recording

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

5.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

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

Steps

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

   NOTE: The record type varies by model.

   - **Continuous**: The video will be recorded continuously according to the schedule.
   - **Motion**: When motion detection is enabled and trigger recording is selected as the linkage method, object movement is recorded.
   - **Alarm**: When alarm input is enabled and trigger recording is selected as the linkage method, the video is recorded after receiving an alarm signal from an external alarm input device.
   - **Motion | Alarm**: Video is recorded when motion is detected or an alarm signal is received from the external alarm input device.
   - **Motion & Alarm**: Video is recorded only when motion is detected and an alarm signal is received from an external alarm input device.
   - **Event**: The video is recorded when a configured event is detected.
4. Set schedule for the selected record type. Refer to *Set Arming Schedule* for the setting operation.
5. Click **Advanced** to set the advanced settings.
   - **Overwrite**: Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise, the camera cannot record new videos.
   - **Pre-record**: The time period set to record before the scheduled time.
   - **Post-record**: The time period set to stop recording after the scheduled time.
   - **Stream Type**: Select the stream type for recording.

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

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

5.2.2 Record Manually

Steps

1. Go to Configuration → Local.

2. Set the **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click to start recording. Click to stop recording.

5.2.3 Set Lite Storage

After 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, the larger the frame rate and bitrate, and the shorter the recommended storage time.
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 lite storage is enabled, an 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 this function.

5.2.4 Playback and Download Video

You can search, play back, 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 showe on the timing bar.

3. Click to play the video files.
   - Click to clip video files.
   - Click to play video files in full screen. Press **ESC** to exit full screen.

   NOTE: Go to **Configuration** → **Local**, click **Save clips to** to change the saving path of clipped video files.

4. Click on the playback interface to download files.

1) Set the search condition and click **Search**.

2) Select the video files and then click **Download**.

NOTE: Go to **Configuration** → **Local**, and click **Save downloaded files to** to change the saving path of downloaded video files.

5.3 Capture Configuration

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

5.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

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

Steps

1. Go to Configuration → Storage → Schedule Settings → Capture → Capture Parameters.
2. Set the capture type.
   - **Timing**: Capture a picture at the configured time interval.
   - **Event-Triggered**: Capture a picture when an event is triggered.
3. Set the Format, Resolution, Quality, Interval, and Capture Number.
4. Refer to *Set Arming Schedule* for configuring schedule time.
5. Click **Save**.

5.3.2 Capture Manually

Steps

1. Go to Configuration → Local.
2. Set the **Image Format** and saving path to for snapshots.
   - **JPEG**: The picture size of this format is comparatively small, which is better for network transmission.
   - **BMP**: The picture is compressed with good quality.
3. Click **Save**.
4. Click near the live view or play back window to capture a picture manually.

5.3.3 View and Download Picture

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

Steps

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

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

Chapter 6 Event and Alarm

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

6.1 Basic Event

6.1.1 Set Motion Detection

Detects moving objects in the detection region and triggers 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.
4. Check Enable Dynamic Analysis for Motion.
    1) Go to **Configuration** → **Local**.
    2) Set **Rules** to **Enable**.
5. Select **Configuration Mode**, and set rule region and rule parameters.
    - For information about normal mode, see *Normal Mode*.
    - For information about expert mode, see *Expert Mode*.
6. Set the arming schedule and linkage methods. For information about arming schedule settings, see *Set Arming Schedule*. For information about linkage methods, see *Linkage Method Settings*.
7. Click **Save**.

6.1.2 Expert Mode

You can configure the day/night switch motion detection parameters according to the actual needs.

Steps

1. Select expert mode in **Configuration**.
2. Set expert mode parameters.
    - **Day/Night Switch**
        - **OFF**: Day/night switch is disabled.
        - **Day/Night Auto-Switch**: The system switches day/night mode automatically according to the environment. It displays color images during the day and black and white images at night.

- **Day/Night Scheduled-Switch**: The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

- **Sensitivity**: The higher the sensitivity value, the more sensitive the motion detection. If the sensitivity is set to *0*, motion detection and dynamic analysis do not take effect.

- **Proportion**: The proportion that a moving object occupies in the drawn area. When the object size exceeds the set proportion, motion detection is triggered.

1) Select an **Area** and click **Draw Area**. Click and drag the mouse on the live video, then release the mouse to finish drawing one area.

Figure 1, Set Rules

- **Stop Drawing:** Finish drawing one area.

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

3. Optional: Repeat the above steps to set multiple areas.

6.1.3 Normal Mode

Set the motion detection parameters according to the device default parameters.

Steps

1. Select normal mode in **Configuration**.

2. Set the normal mode sensitivity. The higher the sensitivity value, the more sensitive the motion detection. If the sensitivity is set to 0, motion detection and dynamic analysis do not take effect.

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

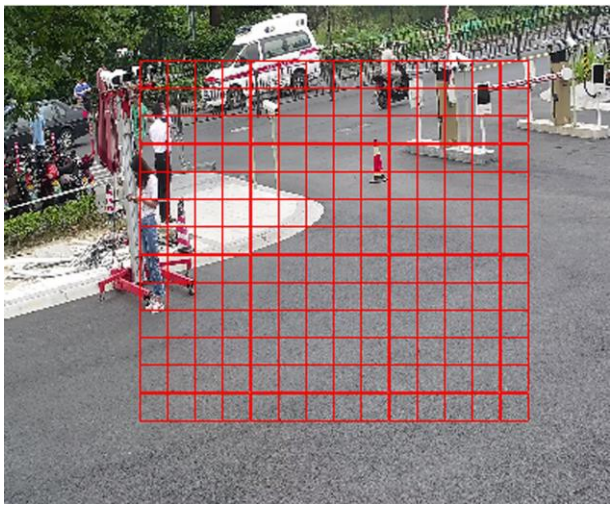


Figure 2, Set Rules

- **Stop Drawing:** Stop drawing one area.
- **Clear All:** Clear all the areas.

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

6.1.4 Set Video Tampering Alarm

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

Steps

1. Go to Configuration → Event → Basic Event → Video Tampering.
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value, the easier to detect the area covering.
4. Click **Draw Area** and drag the mouse in the live view to draw the area.
   - **Stop Drawing:** Finish drawing.
   - **Clear All:** Delete all the drawn areas.

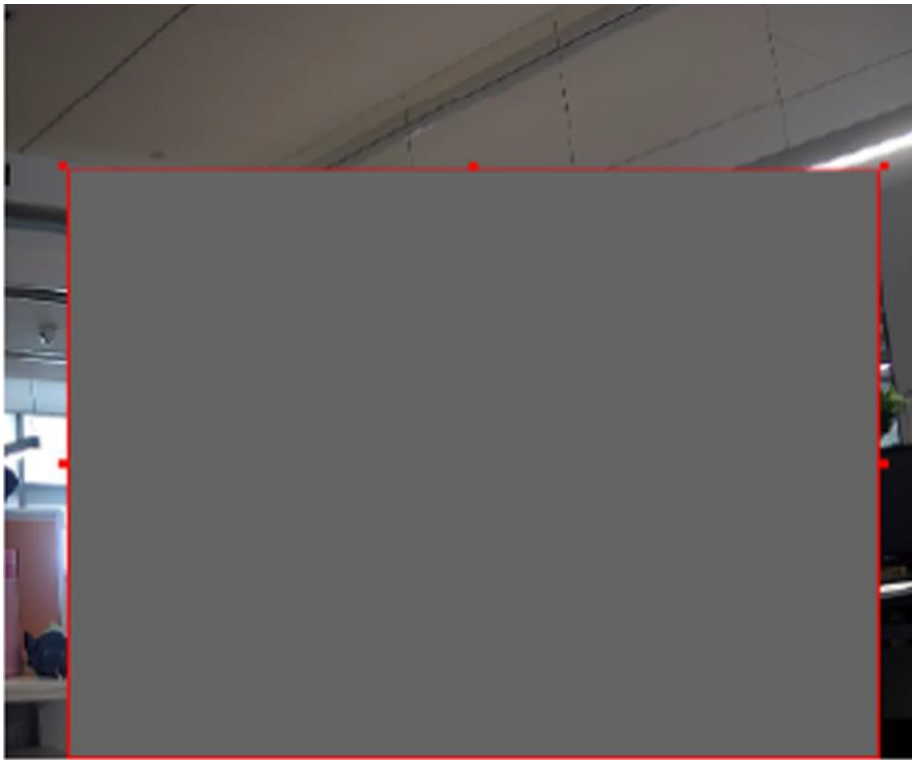


Figure 3, Set Video Tampering Area

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

6. Click **Save**.

6.1.5 Set PIR Alarm

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

Steps

NOTE: Only certain models support PIR alarm.

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

2. Check Enable PIR Alarm.

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

4. Click **Save**.

6.1.6 Set Exception Alarm

Exceptions 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 current device's IP address is the same as another device in the network.
   - **Illegal Login:** Incorrect user name or password entered.
3. Refer to *Linkage Method Settings* for setting linkage method.
4. Click **Save**.

6.1.7 Set Alarm Input

Alarm signal from an 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 cables connection.

Steps

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

6.1.8 Set Video Quality Diagnosis

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

Steps

1. Go to Configuration → Event → Basic Event → Video Quality Diagnosis.
2. Select Diagnosis Type.

3. Set the corresponding parameters.

Alarm Detection Interval
The time interval to detect the exception.

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

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

1. Check **Enable**, and the selected diagnosis type will be detected.
2. Set arming schedule. See *Set Arming Schedule*.
3. Set linkage method. See *Linkage Method Settings*.
4. Click **Save**.

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

6.1.9 Set Vibration Detection

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

Steps

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

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

6.2 Smart Event

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

The function varies by model.

6.2.1 Detect Audio Exception

Audio Exception Detection detects abnormal sound in the surveillance scene such as the sudden increase/decrease in sound intensity, and certain actions can be taken in response.

Steps

1. Go to Configuration → Event → Smart Event → Audio Exception Detection.
2. Select one or several audio exception detection types.
   - **Audio Loss Detection**: Detects sudden loss of audio track.
   - **Sudden Increase of Sound Intensity Detection**: Detects sudden increase in sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.

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

     The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set it as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
   - **Sudden Decrease of Sound Intensity Detection**: Detect sudden decrease of sound intensity. **Sensitivity** is configurable.
3. Refer to *Set Arming Schedule* for setting scheduled time. Refer to *Linkage Method Settings* for setting linkage methods.
4. Click **Save**.

   NOTE: The function varies according to different models.

6.2.2 Set Defocus Detection

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

Steps

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

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

6.2.3 Detect Scene Change

Scene Change Detection detects change in the surveillance scene. Certain actions can be taken when an alarm is triggered.

Steps

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

NOTE: The function varies by model.

6.2.4 Set Face Detection

Detects faces in the detection region. If a face is detected, the device triggers the linkage actions.

Steps

1. Go to Configuration → Event → Smart Event → Face Detection.
2. Check Enable Face Detection.
3. Optional: Highlight to display the face in the image.
4. Check Enable Dynamic Analysis For Face Detection.
   1) Go to **Configuration** → **Local**, set **Rules** to **Enable**.
5. Set **Sensitivity**. The lower the sensitivity, the face profile or an unclear face is more difficult to detect.
6. Set the arming schedule and linkage methods. For information about arming schedule settings, see *Set Arming Schedule*. For information about linkage methods, see *Linkage Method Settings*.
7. Click **Save**.

6.2.5 Set Video Loss

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

Steps

1. Go to Configuration → Event → Basic Event → Video Loss.
2. Check **Enable**.

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

4. Click **Save**.

6.2.6 Set Intrusion Detection

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

Steps

1. Go to Configuration → Event → Smart Event → Intrusion Detection.

2. Check **Enable**.

3. Select a **Region**. For the detection region settings, refer to *Draw Area*.

4. Set rules.

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

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

   - **Object:** Specify the object type to be detected and the device detects only the selected type of object.

Figure 4, Set Rule

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

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

7. Click **Save**.

6.2.7 Set Line Crossing Detection

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

Steps

1. Go to Configuration → Event → Smart Event → Line Crossing Detection.
2. Check **Enable**.
3. Select one **Line** and set the size filter. For the size filter settings, refer to *Set Size Filter*.
4. Click **Draw Area** and a line with an arrow appears in the live video. Drag the line to the location on the live video as desired.
5. Set rules.
   - **Direction:** The direction from which the object crosses the line.
     - **A<->B**: Objects crossing the line from either direction will be detected and alarms triggered.
     - **A->B**: Only objects crossing the configured line from the A side to the B side will be detected.
     - **B->A**: Only objects crossing the configured line from the B side to the A side will be detected.
   - **Sensitivity:** The percentage of the body part of an acceptable target that crosses the pre-defined line. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that crosses the pre-defined line. ST stands for the complete target body. The higher the sensitivity value, the more easily the alarm can be triggered.
   - **Object:** Specify the object type to be detected and the device will detect only that object type.

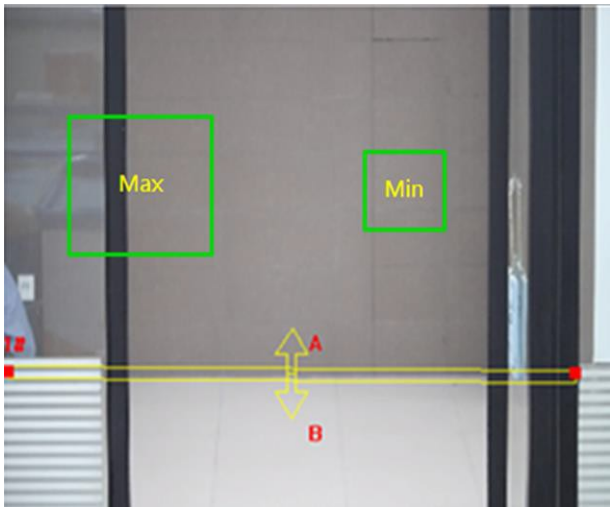


Figure 5, Set Rule

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

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

8. Click **Save**.

6.2.8 Set Region Entrance Detection

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

Steps

1. Go to Configuration → Event → Smart Event → Region Entrance Detection.

2. Check **Enable**.

3. Select one **Region**. For the region settings, refer to *Draw Area*.

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

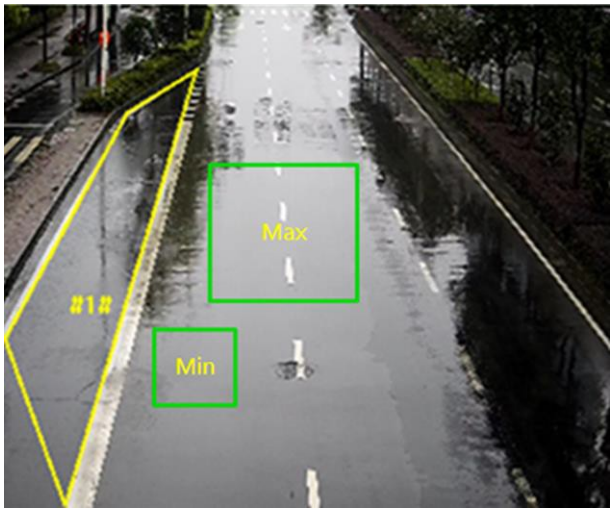


Figure 6, Set Rule

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

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

7. Click **Save**.

6.2.9 Set Region Exiting Detection

Detect objects exiting from a pre-defined virtual region. If it occurs, the device can take linkage actions.

Steps

1. Go to Configuration → Event → Smart Event → Region Exiting Detection.

2. Check **Enable**.

3. Select one **Region**. For the detection region settings, refer to *Draw Area*.

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

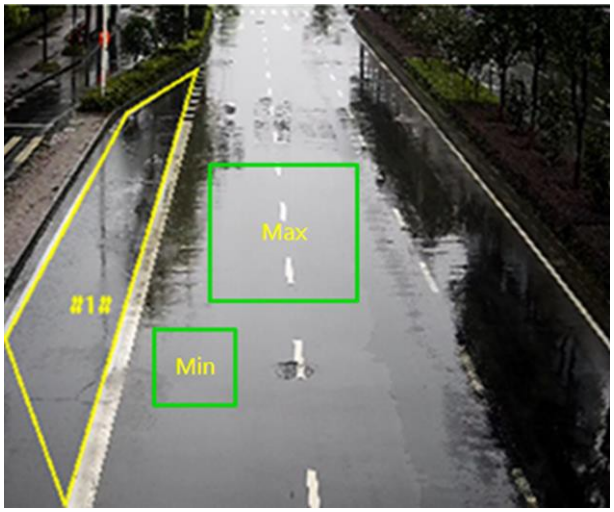


Figure 7, Set Rule

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

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

7. Click **Save**.

6.2.10 Set Unattended Baggage Detection

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

Steps

1. Go to Configuration → Event → Smart Event → Unattended Baggage Detection.

2. Check **Enable**.

3. Select one **Region**. For the detection region settings, refer to *Draw Area*.

4. Set rules.

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

- **Threshold**: The time objects are left in the region. An alarm is triggered after an object is left and stays in the region for the set time period.

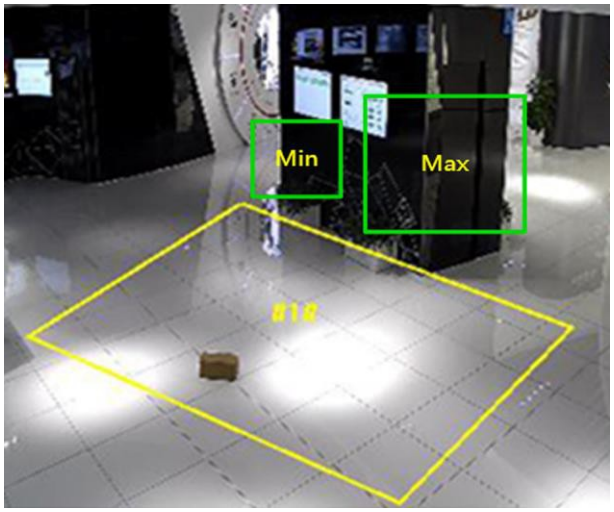


Figure 8, Set Rule

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

6.2.11 Set Object Removal Detection

Detects if objects are removed from the pre-defined detection region such as exhibits on display. If it occurs, the device can take linkage actions and the staff can take measures to reduce property loss.

Steps

1. Go to Configuration → Event → Smart Event → Object Removal Detection.
2. Check **Enable**.
3. Select a **Region**. For the region settings, see *Draw Area*.
4. Set the rule.
   - **Sensitivity:** Range [1–100]. The percentage of the body part of an acceptable target that leaves the pre-defined region. Sensitivity = 100 – S1/ST*100. S1 stands for the target body part that leaves the pre-defined region. ST stands for the complete target body.

     EXAMPLE: If you set the value as 60, a target will be counted as a removed object only when 40 percent of the body part leaves the region.
   - **Threshold:** Range [5–100s], the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.

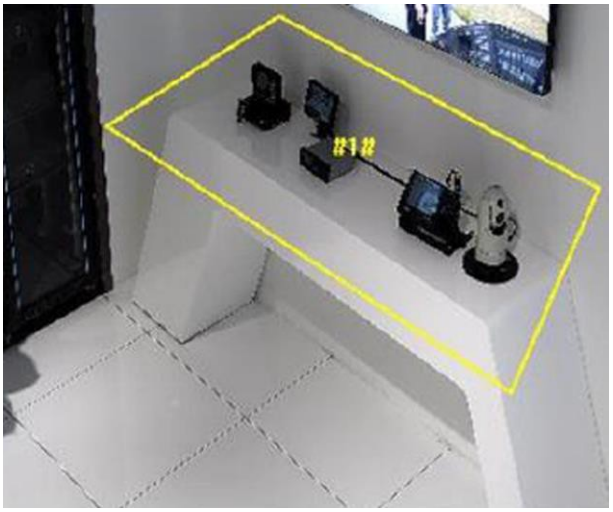


Figure 9, Set Rule

5. Optional: Repeat the above steps to set more regions.
6. For the arming schedule settings, see *Set Arming Schedule*. For the linkage method settings, see *Linkage Method Settings*.
7. *Click* **Save**.

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

6.2.12 Draw Area

This section introduces the configuration of area.

Steps

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

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

6.2.13 Set Size Filter

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

Steps

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

Chapter 7 Network Settings

7.1 TCP/IP

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

Go to **Configuration → Basic Configuration → Network → 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 a domain name. It is also required for some applications (e.g., sending e-mail). Set Preferred DNS Server and Alternate DNS server properly if needed.**

7.1.1 Multicast

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

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

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

7.1.2 Multicast Discovery

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

7.2 SNMP

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

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

Steps

1. Go to the settings page: Configuration → Network → Advanced Settings → SNMP.
2. Check Enable SNMP v1, Enable SNMP v2c, or Enable SNMP v3.

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

   You also need to use the version according to the security level required. SNMP v1 is not secure, and SNMP v2 requires password for access. SNMP v3 provides encryption and HTTPS protocol must be enabled.
3. Configure the SNMP settings.
4. Click **Save**.

7.3 Set SRTP

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

Steps

1. Go to Configuration → Network → Advanced Settings → SRTP.

2. Select Server Certificate.
3. Select Encrypted Algorithm.
4. Click **Save**.

NOTE: Only certain device models support this function.

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

7.4 Port Mapping

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

Before You Start

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

Steps

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

7.4.1 Set Auto Port Mapping

Steps

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

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

7.4.2 Set Manual Port Mapping

Steps

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

What To Do Next

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

7.4.3 Set Port Mapping on Router

The following settings are for a specific router. The settings vary depend router model.

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.

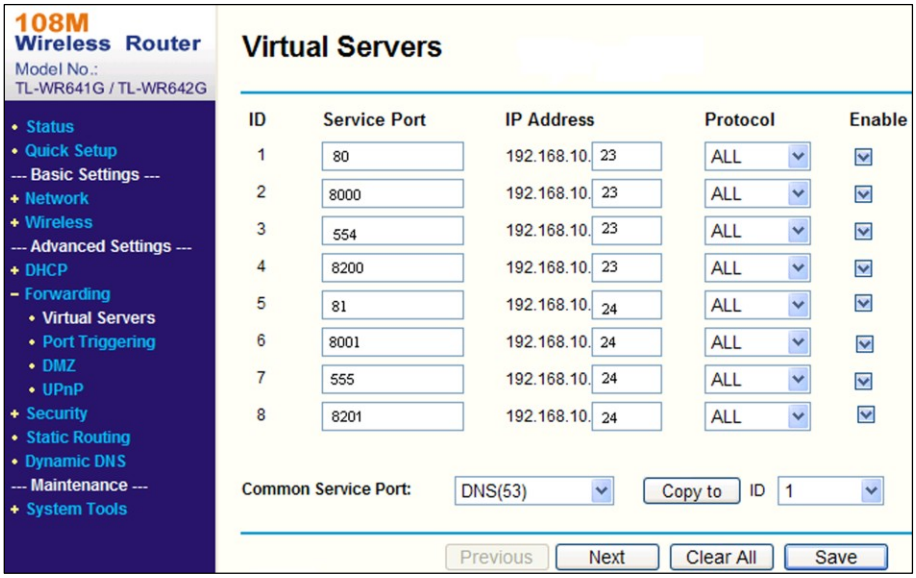


Figure 10, Port Mapping on Router

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

7.5 Port

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

CAUTION: Do not modify the default port parameters at will, otherwise the device may be inaccessible. Go to **Configuration** → **Network** → **Basic Settings** → **Port** for port settings.

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

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

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

7.6 Access to Device via Domain Name

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

Before You Start

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

Steps

1. Refer to *TCP/IP* to set DNS parameters.
2. Go to the DDNS settings page: Configuration → Network → Basic Settings → DDNS.
3. Check **Enable DDNS** and select **DDNS** type.
   - **DynDNS**: Dynamic DNS server is used for domain name resolution.
   - **NO-IP**: NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to *Port* to check the device port,and refer to *Port Mapping* for port mapping settings.
6. Access the device.

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

7.7 Access to Device via PPPoE Dial Up Connection

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

Steps

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

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

7.8 Wireless Dial

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

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

7.8.1 Set Wireless Dial

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

Before You Start

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

Steps

1. Go to Configuration → Network → Advanced Settings → Wireless Dial.
2. Check to enable the function.
3. Click **Dial Parameters** to configure and save the parameters.
4. Click **Dial Plan**. See *Set Arming Schedule* for detailed information.
5. Optional: Set **White List**. See *Set White List* for detailed information.
6. Click Dial Status.
   - **Click Refresh:** Refresh the dial status.
   - **Click Disconnect:** Disconnect the 3G/4G wireless network.

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

7.8.2 Set White List

Add the mobile phone number of administrator to the white list in order to receive alarm messages from the device.

Steps

1. Go to the white list settings page: Configuration → Advanced Configuration → Wireless Dial → White List.
2. Check Enable SMS Alarm.
3. Click + in the white list.
   1) Input the mobile phone number to receive alarm messages.
   2) Check **Reboot via SMS**.
   3) Select events, and the mobile phone will receive the alarm message when an event happens.
   4) Click **Save**.
4. Optional: Repeat the steps above to set multiple recipients.
   - Modify the white list parameters.

- × Delete the white list that already set.
- **Send Test SMS** Send a message to the mobile phone for test.

5. Click **Save**.

7.9 Wi-Fi

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

This function is supported only by certain device models.

7.9.1 Connect Wi-Fi Manually

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

Steps

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

   NOTE: For stable use of Wi-Fi, it is not recommended to use DHCP.

3. Go to the Wi-Fi settings page: Configuration → Network → Advanced Configuration → Wi-Fi.
4. Set and save the parameters.
   1) Click **Search**.
   2) Select a **SSID**, which should be the same as that of the wireless router or AP. The network parameters are automatically shown in **Wi-Fi**.
   3) Set the **Network Mode** to **Manage**.
   4) Input the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

What To Do Next
Go to TCP/IP settings page: **Configuration** → **Network** → **Basic Configuration** → **TCP/IP**, and click **Wlan** to check the **IPv4 Address** and log in the device. See *Login* for detailed information.

7.9.2 Connect Wi-Fi Automatically

The device can connect the Wi-Fi automatically via WPS or QSS protocols, which both support PBC mode and PIN mode.

Use PBC: Set PBC to connect Wi-Fi automatically. PBC refers Push-Button-Configuration, in which the user simply has to push a button, either an actual or virtual one (as the **Connect** button on the configuration interface of the IE browser), on both the Access Point (and a registrar of the network) and the new wireless client device.

Before You Start

Complete the operation within 120 seconds, otherwise the connection will fail.

Steps

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

   NOTE: For stable use of Wi-Fi, it is not recommended to use DHCP.
3. Go to the Wi-Fi settings page: Configuration → Network → Advanced Configuration → Wi-Fi.
4. Set the Wi-Fi parameters.
   1) Check **Enable WPS**.
   2) Select **PBC connection**.
   3) Check the Wi-Fi router to see if there is a WPS button. If there is, push the button and you will see the indicator near the button start flashing, which means the WPS function of the router is enabled. For detailed operation, see the router user guide.
   4) Push the WPS button to enable the function on the camera. If there is not a WPS button on the camera, you can also click the virtual button to enable the PBC function on the Web interface.
   5) Click **Connect**.
5. Click **Save**.
6. Set PBC code for wireless router or AP.
   - Press the WPS or QSS button on the wireless router or AP within 120 seconds to quickly complete the connection.
   - Refer to the router or AP user guide to set PBC code.
7. Go to TCP/IP setting page: **Configuration → Network → Basic Configuration → TCP/IP**, and click **Wlan** to check the **IPv4 Address** and log in the device.
   - Input the IP address in the browser to access the device.
   - Add the device in the client application. Select **IP/Domain**, and input the IP address and other parameters to access the device.

Use PIN on Device: The device can automatically connect the network by setting the device PIN code parameters in wireless router or AP via WPS or QSS protocols.

Steps

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

NOTE: For stable use of Wi-Fi, it is not recommended to use DHCP.

3. Go to the Wi-Fi setting page: Configuration → Network → Advanced Configuration → Wi-Fi.
4. Check Enable WPS.
5. Click **Generate** to generate a device PIN code.
6. Refer to the wireless router or AP user manual to input the code to the router or AP.
7. Go to the TCP/IP settings page: **Configuration** → **Network** → **Basic Configuration** → **TCP/IP**, and click **Wlan** to check the **IPv4 Address** and log in to the device.
   - Input the IP address in the browser to access the device.
   - Add the device in the client application. Select **IP/Domain**, and input the IP address and other parameters to access the device.

Use PIN on Router: The device can automatically connect the network by setting the PIN code of the wireless router or AP in device via WPS or QSS protocols.

Before You Start

Get the PIN code and SSID of the router or AP.

Steps

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

   NOTE: For stable use of Wi-Fi, it is not recommended to use DHCP.
3. Go to the Wi-Fi settings page: Configuration → Network → Advanced Configuration → Wi-Fi.
4. Set Wi-Fi parameters.
   1) Check **Enable WPS**.
   2) Select **Use router PIN code**.
   3) Enter the PIN code and SSID you get from the router side in the **SSID** and **Router PIN code** field.
   4) Click **Connect**.
5. Click **Save**.
6. Go to the TCP/IP setting page: **Configuration** → **Network** → **Basic Configuration** → **TCP/IP**, and click **Wlan** to check the **IPv4 Address** and log in the device.
   - Input the IP address in the browser to access the device.
   - Add the device in client application. Select **IP/Domain**, and input the IP address and other parameters to access the device.

7.10 Set Network Service

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

Steps

NOTE: This function varies by model.

Go to **Configuration** → **Network** → **Advanced Settings** → **Network Service**.

1. Set network service.
   - **WebSocket & WebSockets**: WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 or above version or Mozilla Firefox 52 or above version to visit the device. Otherwise, live view, image capture, and the digital zoom function cannot be used.
     - If the device uses HTTP, enable WebSocket.
     - If the device uses HTTPS, enable WebSockets and select the server certificate.
   - **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.

     NOTE: If you enable Enhanced SDK Service, you should select the server certificate.

     When set up a connection between the device and the client software, it is recommended to use Enhanced SDK Service and set the communication in Arming Mode to encrypt the data transmission.
   - TLS (Transport Layer Security): The device offers TLS1.1 and TLS1.2. Enable one or more protocol versions according to your need.
2. Click **Save**.

7.11 Set ONVIF

If you need to access the device through ONVIF protocol, you can configure the ONVIF user to enhance the network security.

Steps

1. Go to Configuration → Network → Advanced Settings → Integration Protocol.
2. Check Enable ONVIF.
3. Click **Add** to configure the ONVIF user.
   - **Delete:** Delete the selected ONVIF user.
   - **Modify:** Modify the selected ONVIF user.

4. Click **Save**.

5. Optional: Repeat the steps above to add more ONVIF users.

7.12 Set Alarm Server

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

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

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

5. Click **Save**.

7.13 Access Camera via Hik-Connect

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

Before You Start
Connect the camera to a network with network cables.

Steps

1. Get and install the Hik-Connect app in the following ways.

   - Visit *https://appstore.hikvision.com* to download the application according to your mobile phone system.

   - Visit the official site of our company. Then go to **Support** → **Tools** → **Hikvision App Store**. Scan the QR code below to download the application.

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

   - Visit *https://appstore.hikvision.com/static/help/index.html* and refer to the troubleshooting.

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

3. Start the application and register for a Hik-Connect user account.
4. Log in after registration.
5. 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.
6. Follow the prompts to set the network connection, and add the camera to your Hik-Connect account.

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

7.13.1 Enable Hik-Connect Service on Camera

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

Enable Hik-Connect Service via Web Browser

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

Before You Start

Activate the camera before enabling the service.

Steps

1. Access the camera via a Web browser.
2. Enter platform access configuration interface. Configuration → Network → Advanced Settings → Platform Access.
3. Select Hik-Connect as the Platform Access Mode.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in 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 section introduces how to enable Hik-Connect service via SADP software of an activated camera.

Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.

3. Check Enable Hik-Connect.
4. Create a verification code or change the old verification code.

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

5. Click and read "Terms of Service" and "Privacy Policy."
6. Confirm the settings.

Set Up Hik-Connect

Steps

1. Get and install the 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 (e.g., "Unknown app") occur during installation, refer to the following:

   Visit *https://appstore.hikvision.com/static/help/index.html* and refer to the troubleshooting.

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

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

Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi hot spot.
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 the camera body or on the *Quick Start Guide* cover.

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

5. Input the verification code of your camera.

   NOTE: The required verification code is the code you create or change when you enable Hik-Connect service on the camera.

   If you forget the verification code, you can check the current verification code on the **Platform Access** configuration page via a Web browser.

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

7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

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

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

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

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

Chapter 8 Arming Schedule and Alarm Linkage

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

8.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

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

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

8.2 Linkage Method Settings

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

8.2.1 Trigger Alarm Output

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

Steps

1. Go to Configuration → Event → Basic Event → Alarm Output.
2. Set alarm output parameters.
   - **Automatic Alarm:** For information about the configuration, see *Automatic Alarm*.
   - **Manual Alarm:** For 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**: Customize 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**: Customize a name for the alarm output.
    - **Delay**: The time duration that the alarm output remains after an alarm occurs.
2. Set the alarming schedule. For information about the settings, see *Set Arming Schedule*.
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

8.2.2 FTP/NAS/Memory Card Uploading

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

- Refer to *Set FTP* to set the FTP server.
- Refer to *Set NAS* for NAS configuration.
- Refer to *Set Memory Card* for memory card storage configuration.

8.2.3 Send Email

Check **Send Email**, and the device sends an e-mail to the designated addresses with alarm information

when an alarm event is detected.

NOTE: For e-mail settings, refer to *Set Email*.

Set Email

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

Before You Start

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

Steps

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

      NOTE: To use STARTTLS, make sure that the protocol is supported by your e-mail server. If you check **Enable STARTTLS** and the protocol is not supported by your e-mail server, the e-mail is sent with no encryption.
   4) Optional: To receive notifications with alarm pictures, check **Attached Image**. The notification e-mail has three attached alarm pictures about the event with configurable image capturing interval.
   5) Input the receiver's information, including the receiver's name and address.
   6) Click **Test** to see if the function is properly configured.
3. Click **Save**.

8.2.4 Notify Surveillance Center

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

8.2.5 Trigger Recording

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

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

8.2.6 Flashing Light

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

Set Flashing Alarm Light Output

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

Steps

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

NOTE: Only certain device models support this function.

8.2.7 Audible Warning

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

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

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

Set Audible Alarm Output

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

Steps

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

files can be uploaded.

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

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

Chapter 9 System and Security

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

9.1 View Device Information

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

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

9.2 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to Configuration → System → Maintenance → Log.
2. Set search conditions Major Type, Minor Type, Start Time, and End Time.
3. Click **Search**. The matched log files will be displayed on the log list.
4. Optional: Click **Export** to save the log files in your computer.

9.3 Simultaneous Login

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

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

9.4 Import and Export Configuration File

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

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

9.5 Export Diagnose Information

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

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

9.6 Reboot

You can reboot the device via a browser.

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

9.7 Restore and Default

Restores the device parameters to the default settings.

Steps

1. Go to Configuration → System → Maintenance → Upgrade & Maintenance.
2. Click **Restore** or **Default** according to your needs.
   - **Restore:** Reset device parameters, except user information, IP parameters, and video format to the default settings.
   - **Default:** Reset all the parameters to the factory default.

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

9.8 Upgrade

Before You Start
You need to obtain the correct upgrade package.

CAUTION: DO NOT disconnect power during the process. The device will reboot automatically after the 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 the upgrade file belongs to.
3. Click **Browse** to select the upgrade file.
4. Click **Upgrade**.

9.9 View Open Source Software License

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

9.10 Time and Date

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

9.10.1 Synchronize Time Manually

Steps

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

9.10.2 Set NTP Server

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

Before You Start
Set up an NTP server or obtain NTP server information.

Steps

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

   NOTE: Server Address is NTP server IP address.
5. Click **Test** to test server connection.
6. Click **Save**.

9.10.3 Synchronize Time by Satellite

NOTE: This function varies by device.

Steps

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

4. Click **Save**.

9.10.4 Set DST

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

Steps

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

9.11 Set RS-485

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

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

Steps

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

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

3. Click **Save**.

9.12 Set RS-232

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

Before You Start
Connect the device to a computer or terminal with an RS-232 cable.

Steps

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

9.13 External Device

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

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

9.13.1 Supplement Light Settings

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

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

9.14 Security

You can improve system security by setting security parameters.

9.14.1 Authentication

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

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

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

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

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

9.14.2 Set IP Address Filter

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

IP address refers to IPv4.

Steps

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

9.14.3 Set HTTPS

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

Steps

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

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

9.14.4 Set QoS

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

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

Steps

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

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

3. Click **Save**.

9.14.5 Set IEEE 802.1x

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

Go to **Configuration → Network → Advanced Settings → 802.1x**, and enable the function. Set **Protocol** and **EAPOL Version** according to router information.

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

- **EAP-LEAP and EAP-MD5**: If you use EAP-LEAP or EAP-MD5, the authentication server must be configured. Register a user name and password for 802.1x in the server in advance. Input the user name and password for authentication.
- EAP-TLS: If you use EAP-TLS, input Identify, Private Key Password, and upload CA Certificate, User Certificate, and Private Key.
- **EAPOL Version**: The EAPOL version must be identical with that of the router or the switch.

9.14.6 Control Timeout Settings

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

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

9.14.7 Search Security Audit Logs

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

Steps

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

1. Go to Configuration → System → Maintenance → Security Audit Log.
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**. The log files that match the search conditions will be displayed on the Log List.
4. Optional: Click **Export** to save the log files to your computer.

9.14.8 Security Reinforcement

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

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

9.15 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.

9.15.1 Create Self-signed Certificate

Steps

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

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

9.15.2 Create Certificate Request

Before You Start

Select a self-signed certificate.

Steps

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

9.15.3 Import Certificate

Steps

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

   NOTE: Up to 16 certificates are allowed.

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

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

   You cannot create a certificate that has the same ID as that of the existing certificate and import a certificate that has the same content with that of the existing certificate.

9.15.4 Install Server/Client Certificate

Steps

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

- **Create certificate request**: Refer to *Create Certificate Request*
- **Import Certificate**: Refer to *Import Certificate*

9.15.5 Install CA Certificate

Steps

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

NOTE: Up to 16 certificates are allowed.

9.15.6 Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an e-mail 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 daybefore 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 thecertificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

9.16 User and Account

9.16.1 Set User Account and Permission

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

CAUTION: To increase security of using the device on a network, change your account password regularly. Changing the password every three months is recommended. If the device is used in a high-risk environment, it is recommended that the password be changed monthly or weekly.

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 permissions.
   - **User**: Users can be assigned permission to view live video, set PTZ parameters, and change their own passwords, but no permission for other operations.
   - **Operator**: Operators can be assigned all permissions except for operations on the administrator and creating accounts.
   - **Modify:** Select a user and click **Modify** to change the password and permission.
   - **Delete:** Select a user and click **Delete**.

     NOTE: The administrator can add up to 31 user accounts.
3. Click **OK**.

9.16.2 Simultaneous Login

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

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

9.16.3 Online Users

The information of users logging into the device is shown.

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

Chapter 10 Allocate VCA Resource

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

Steps

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

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

10.1 Face Capture

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

NOTE: For device that supports face capture, you need to enable the function in **VCA Resource**. Referto *Allocate VCA Resource* for details.

Face capture is supported only by certain models.

10.1.1 Set Face Capture

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

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

Steps

1. Go to Configuration → Face Capture.
2. For shield region settings, refer to *Set Shield Region*.
3. Select **Rule** and check **Rule**.
4. Click ⬡ to draw the detection area. It is recommended that the drawn area occupies 1/2 to 2/3 of the live view image.
5. Click ▭ and draw a rectangle based on the pupil distance of the face on the live view.

Figure 11, Set Face Capture

NOTE: The device will detect whether there is a human face in the area by the set minimum pupil distance.

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

7. Click **Save**.

8. For overlay and capture settings, refer to *Overlay and Capture*. For advanced parameters settings, refer to *Face Capture Algorithms Parameters*.

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

10.1.2 Overlay and Capture

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

- **Display VCA info. on Stream**: Display smart information on stream, including the target and rules information.
- **Display Target info. on Alarm Picture**: Overlay the alarm picture with target information.
- **Target Picture Settings**: Custom, Head Shot, Half-Body Shot, and Full-Body Shot are selectable.

  NOTE: If you select **Custom**, you can customize **width**, **head height** and **body height** as required.You can check **Fixed Value** to set the picture height.

- **Background Picture Settings**: Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image needs to be uploaded to surveillance center, check **Background Upload**.
- **People Counting Overlay**: Select flow overlay type.

  NOTE: Select the daily reset time. Click **Manual Reset** to reset immediately.

- **Camera**: Set **Device No.** and **Camera Info.** for the camera, which can be overlaid on capturedpicture.

- **Text Overlay**: You can check desired items and adjust their order to display on captured pictures by using . The content of **Device No.** and **Camera Info** should be on the same page.

10.1.3 Face Capture Algorithms Parameters

Set and optimize the parameters of the algorithm library for face capture. Go to **Configuration** → **Face Capture** → **Advanced Configuration** → **Parameters**.

- **Face Capture Version**: It lists the version of the algorithms library.
- Detection Parameters
  - **Generation Speed**: The speed to identify a target. The higher the value, the faster the target will be recognized. Setting the value quite low, and if there was a face in the configured area from the start, this face will not be captured. It can reduce the misinformation of the faces in the wall painting orposters. The default value of 3 is recommended.
  - **Sensitivity**: The sensitivity to identify a target. The higher the value, the easier a face will be recognized, and the higher possibility of misinformation. The default value of 3 is recommended.
- Capture Parameters
  - **Best Shot**: The best shot after target leave the detection area.
  - **Capture Times**: Number of times a face will be captured during its stay in the configured area. The default value is 1.
  - **Capture Interval**: The frame interval to capture a picture. If you set the value as 1, which is the default value, the camera captures the face in every frame.
  - **Capture Threshold**: The quality of the face to trigger capture and alarm. A higher value means better quality must be met to trigger capture and alarm.
  - **Quick Shot**: Defines quick shot threshold and maximum capture interval.
  - **Quick Shot Threshold**: The quality of face to trigger quick shot.
  - **Face Exposure**: Check the checkbox to enable the face exposure.
  - **Reference Brightness**: The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value set. The higher the value, the brighter the face.
  - **Minimum Duration**: The minimum duration of the camera exposures of the face. The default value is 1 minute.

    NOTE: If face exposure is enabled, make sure the WDR function is disabled, and manual iris is selected.
  - **Face Filtering Time**: The time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the

detected face when the face stays in the scene for 5 seconds.

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

- **Restore Default**: Click **Restore** to restore all the advanced configuration settings to the factory defaults.

10.1.4 Set Shield Region

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

Steps

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

10.2 Road Traffic

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

NOTE: Only certain device models support this function.

10.2.1 Set Vehicle Detection

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

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

Steps

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

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

7. Select Region and Country/Region.

8. Select the license plate information upload mode.

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

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

9. Select the **Detection** mode.

10. Check Remove Duplicated License Plates and set the Time Interval (default is 4 minutes).

    NOTE: Up to eight license plates are supported.

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

12. Click **Save**.

10.2.2 Set Mixed-Traffic Detection Rule

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

Before You Start

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

Steps

1. Go to Configuration → Road Traffic → Detection Configuration, and select Mixed-traffic Detection as detection type.

2. Check **Enable**.

3. Select the lane number.

4. Select Region and Country/Region.

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

6. Click **Save**.

10.2.3 Uploading Pictures Settings

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

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

- **Picture Quality**: The larger the value, the clearer the picture, but more storage space is also required.
- **Picture Size**: The larger the value, the larger the storage space needed, and the level of network transmission requirement is also higher.
- **Overlay**: You can overlay camera, device, or vehicle information on the captured image and click ↑ ↓ to adjust the order of overlay texts.

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

10.2.4 Camera Settings

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

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

10.2.5 Import or Export Blacklist & Whitelist

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

Steps

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

NOTE: The file to import should correspond with the file template that is required by the camera. You are recommended to export an empty Blacklist & Whitelist file from the camera as a template and fill in the content. The file should be in.xls format and the cell format should be "text."

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

10.3 Multi-Target-Type Detection

Multi-Target-Type Detection is to detect, capture, and upload data of targets in multiple types such as human faces, human bodies, and vehicles.

NOTE: For certain device models, you need to enable **Multi-Target-Type Detection** on the **VCA Resource** page first.

10.3.1 Set Multi-Target-Type Detection Rule

After setting the multi-target-type detection rules and algorithm parameters, the device captures targets of multiple types and triggers linkage actions automatically.

Steps

1. Go to Configuration → Multi-Target-Type Detection → Rule.
2. Check **Rule**.
3. Click ⬡, and draw a detection area on the live image.
4. Enter the min. pupil distance in the text field, or click ▣ to draw the min. pupil distance.

Min. Pupil Distance
The min. pupil distance refers to the minimum area between two pupils, and it is basic for the device to recognize a face.

1. Set arming schedule. See *Set Arming Schedule*.
2. Set linkage method. See *Linkage Method Settings*.
3. Click **Save**.

What To Do Next
Go to **Picture** to search for and view the captured pictures.

Go to **Smart Display** to see currently captured target pictures.

10.3.2 Overlay and Capture

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

- **Display VCA info. on Stream**: Display smart information on stream, including the target and rules information.
- **Display Target info. on Alarm Picture**: Overlay the alarm picture with target information.
- **Target Picture Settings**: Custom, Head Shot, Half-Body Shot, and Full-Body Shot are selectable.

NOTE: If you select **Custom**, you can customize **width**, **head height**, and **body height** as required.You can check **Fixed Value** to set the picture height.

- **Background Picture Settings**: Compared to the target picture, the background picture is the scene image that offers extra environmental information. You can set the background picture quality and resolution. If the background image needs to be uploaded to the surveillance center, check **Background Upload**.

- People Counting Overlay

  - Select flow overlay type.

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

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

- **Text Overlay**: You can check desired items and adjust their order to display on captured pictures by using . The content of **Device No.** and **Camera Info** should be on the same page.

10.3.3 Multi-Target-Type Detection Algorithm Parameters

Used to set and optimize the parameters of the algorithm library for Multi-Target-Type Detection.

Go to the **Configuration** → **Multi-Target-Type Detection** → **Advanced Configuration** for configuration.

- **HMS Version**: The current algorithm version, which cannot be edited.

- **Restore Defaults**: Click **Restore** to restore all the advanced configuration settings to the factory defaults.

- Detection Parameters

  - **Generation Speed**: The speed of deciding whether an object in detection area is a target or not. The higher the value, the faster the target will be detected. The default value is recommended.

  - **Sensitivity**: The sensitivity of recognizing a target. The higher the value, the easier a target will be recognized, and the higher possibility of misinformation. The default value is recommended.

- Capture Parameters

  - Best Shot

  - **Capture Threshold:** The quality of a face to trigger capture and alarm. A higher value means better quality must be met to trigger capture and alarm.

  - **Face Exposure**: Enable the function, and the device automatically adjusts the exposure level when human faces appear in the scene.

  - **Reference Brightness**: The reference brightness of a face in face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lowers the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.

  - **Minimum Duration**: The extra time the device keeps the face exposure level after the face disappears in the scene.

- **Face Filtering Time**: The time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face stays in the scene for 5 seconds.

10.3.4 Set Shield Region

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

Steps

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

10.4 Face Counting

Face counting detection can remove duplicate faces and calculate the number of objects entering or exiting a configured area.

NOTE: Certain device models require selecting **Face Counting** on the **VCA Resource** page first.

Only certain camera models support this function.

10.4.1 Set Face Counting Detection Rule

After setting the face counting detection rules and algorithm parameters, the device captures targets and triggers linkage actions automatically.

Steps

1. Go to Configuration → Face Counting → Rule.
2. Check **Rule**.
3. Enter the min. pupil distance in the text field, or click ⊡ to draw the min. pupil distance. The distance of the drawn pupil will be displayed on the box below the live view.
   - **Min. Pupil Distance**: The min. pupil distance refers to the minimum square size composed by the area between two pupils, and it is the basic standard for a camera to identify a target.
   - **Max. Pupil Distance**: The max. pupil distance refers to the maximum square size composed by the area between two pupils, and it is the basic standard for a camera to identify a target.
     1) Enter the max. pupil distance in the text field, or click ⊡ to draw the max. pupil distance.
     2) Click ⬡ to draw the detection area. Draw an area by left-clicking end-points in the live view

window, and right-clicking to finish the area drawing.

3) Click ⟋ to draw the detection line. The arrow shows entering direction, you can click ⇌ to change the direction.

   - If the target crosses the counting area from the entering direction and crosses the detection line, then it is counted as the entering number.
   - If the target crosses the counting area from the exiting direction and crosses the detection line, then it is counted as the exiting number.

4) Click A and B to draw region A and B. Make sure the two areas don't overlap. You can click ⇌ to change the direction.

   - If the target enters from A region to B region, then it is counted as the entering number.
   - If the target enters from B region to A region, then it is counted as the exiting number.

5) Set arming schedule. See *Set Arming Schedule*.

6) Set linkage method. See *Linkage Method Settings*.

10.4.2 Overlay and Capture

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

- **Display VCA info. on Stream**: Display smart information on stream, including the target and rules information.
- **Display Target info. on Alarm Picture**: Overlay the alarm picture with target information.
- **Target Picture Settings**: Custom, Head Shot, Half-Body Shot, and Full-Body Shot are selectable.

  NOTE: If you select **Custom**, you can customize **width**, **head height**, and **body height** as required. You can check **Fixed Value** to set the picture height.

- **Background Picture Settings**: Compared to the target picture, the background picture is the scene image offering extra environmental information. You can set the background picture quality and resolution. If the background image needs to be uploaded to the surveillance center, check **Background Upload**.
- **People Counting Overlay**: Select flow overlay type. Select the daily reset time. Click **Manual Reset** to reset it immediately.
- **Camera**: You can set **Device No.** and **Camera Info.** for the camera, which can be overlaid on captured picture.
- **Text Overlay**: You can check desired items and adjust their order to display on captured pictures by using ↓ ↑. The content of **Device No.** and **Camera Info** should be on the same page.

10.4.3 Face Counting Algorithm Parameters

Sets and optimizes the parameters of the algorithm parameters for Face Counting.

NOTE: These functions vary by models.

- **Face Capture Mode**: The current algorithm version, which cannot be edited.
- **Best Shot**: The best shot after the target leaves the detection area.
- **Capture Times**: The capture times a face will be captured during its stay in the configured area. The default value is 1.
- **Capture Threshold**: The quality of face to trigger capture and alarm. A higher value means better quality must be met to trigger capture and alarm.
- **Face Exposure**: The device adjusts the face brightness when it detects a face in the image.
- **Reference Brightness**: The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value set. The higher the value, the brighter theface.
- **Min. Duration**: The minimum duration the camera exposes the face.

  NOTE: If face exposure is enabled, make sure the WDR function is disabled, and manual iris is selected.
- **Real-Time Update Data**: If enabled, the real-time people counting data will be uploaded to the platform.
- **Data Statistics Cycle**: Select the data statistics cycle as required.
- **Algorithm Validity**: The higher the value, the more difficult it is to detect the target, but the higher the detection accuracy.
- **Restore Defaults**: Click **Restore**to restore all the advanced configuration settings to the factory defaults.

10.4.4 View Face Counting Result

Steps

1. Go to Application.
2. Set search condition and click **Counting**. Matched results are shown in the **Face Picture Comparison Statistics** and **People Counting Statistics** area.

10.5 Queue Management

Counts queuing-up people number and waiting time of each person.

NOTE: Queue management is supported only by certain models.

10.5.1 Set Regional People Queuing-Up

Counts queuing-up persons in defined regions. Alarms are triggered when the alarm threshold condition and the alarm trigger are both met.

Before You Start

To enable the function, go to **VCA Resource**, and select **Queue Management**.

Steps

1. Go to Configuration → Queue Management.
2. Select Regional People Queuing-Up.
3. Click **Add Region** to draw the detection area and set **Region Name** and **Alarm Interval**. Repeat this step above to set more areas.
   - **Alarm Interval**: During the set alarm interval, alarms of the same type only trigger one notification.

Figure 12, Set Regional People Queuing-Up

4. Optional: Check **OSD** to display the region name and its real-time queuing-up people number.
5. Set **Alarm threshold**. An alarm is triggered when the alarm threshold condition is met.
6. For arming schedule settings, refer to *Set Arming Schedule*. For linkage method settings, refer to *Linkage Method Settings*.
7. Click **Save**.

10.5.2 Set Waiting Time Detection

Counts the waiting time of each person that enters the detection area. Alarms are triggered when the alarm threshold condition and the alarm trigger are both met.

Before You Start

To enable the function, go to **VCA Resource**, and select **Queue Management**.

Steps

1. Go to Configuration → Queue Management.
2. Select Waiting Time Detection.

3. Click **Add Region** to draw the detection area and set **Region Name** and **Alarm Interval**. Repeat this step above to set more areas.

    - **Alarm Interval**: During the set alarm interval, alarms of the same type trigger only one notification.

Figure 13, Set Waiting Time Detection

4. Set **Alarm threshold**. An alarm is triggered when the alarm threshold condition is met.

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

6. Click **Save**.

7. Optional: Enable Display POS Information and Rule in Configuration → Local.

The detection area and the time people staying in the detection area can be viewed on the live view.

10.5.3 Queue Management Statistics

Queue management supports data analysis and report output.

Before You Start

For queue management settings, refer to *Set Regional People Queuing-Up* and *Set Waiting Time Detection*.

- Select **Queuing-Up Time Analysis** and **Regional Comparison** to compare queuing-up people number of different regions.
- Select **Queuing-Up Time Analysis** and **Multi-Level Comparison** to compare queuing-up people number of different waiting time levels.
- Select **Queue Status Analysis** and **Regional Comparison** to compare the time and duration that a queue stays at a certain length in different regions.
- Select **Queue Status Analysis** and **Multi-Level Comparison** to compare the time and duration of the queue at different queue length levels.

Steps

NOTE: With an on-board memory card installed, the device can save up to one mouth's data. With no memory card installed, the device can save only up to one week's data.

1. Select the analysis mode.
   - **Queuing-Up Time Analysis**: Queuing-Up time analysis calculates people number of different waiting time levels.
   - **Queue Status Analysis**: Queue status analysis calculates the time and duration that a queue stays a certain length.
2. Select Statistic Type.
   - **Regional Comparison**: Multiple regions and one level can be selected for analysis, and an analysis chart can be drawn.
   - **Multi-Level Comparison**: Multiple levels and regions can be selected for analysis, and one analysis chart is drawn for each region.
3. Check one or more regions.
4. Set the queue length level. Check one or more desired range checkboxes and input values.
5. Select Report Type and Statistics Time.
6. Click **Counting** to generate the report.

10.6 Counting

Calculates the number of people entering or exiting a configured area.

NOTE: Counting is supported only by certain models.

10.6.1 Set Counting

Calculates the objects entering and exiting the region, alarm events, and uploads data.

Steps

1. Go to Configuration → Counting.
2. Check Enable Counting.
3. Optional: Check **Enable OSD Overlay**, and the real-time number of people entering and exiting the region is displayed on the live video.

   NOTE: The overlay information counts only the number of the current day. The number is cleared when the device is restarted or midnight comes. You can also click 0 to clear the number manually.
4. Set the detection line and the objects across the line will be detected and counted.

- Draw a detection line.
- Delete the detection line.
- Change the direction.

Figure 14, Set Counting

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

10.6.2 View Counting Statistics

You can view and export the counting statistics stored in the device or memory card.

Before You Start
Go to *Set Counting* to set queue management first.

Steps

1. Go to Application.
2. Select Report Type.
3. Select Statistics Type.
4. Select Start Time.
5. Click Counting.
6. Optional: Click **Export** to export the counting statistics.

The counting statistics can be viewed in table, line chart, and bar chart.

10.7 Hard Hat Detection

Detects targets in the monitoring region who do not wear a hard hat, and triggers an alarm.

NOTE: Only certain device models support the function.

10.7.1 Set Hard Hat Detection

Before You Start
Go to **Configuration** → **System** → **System Settings** → **VCA Resources** to enable **Hard Hat Detection**.

Steps

1. Go to Configuration → Hard Hat Detection, and check Enable Hard Hat Detection.
2. Optional: Set Target Generation Speed.

Target Generation Speed
The target generation speed of a face entering the detection region. The greater the value, the quicker the generation speed.

1. Set detection region.
    1) Select detection region.
    2) Click **Draw Area**, and click and draw the endpoints of the region in the live view image.
    3) Right click to finish the drawing.
    - **Click Stop Drawing:** Finish drawing the region.
    - **Click Clear All:** Draw the region again.
2. For arming schedule settings, refer to *Set Arming Schedule*. For linkage method settings, refer to *Linkage Method Settings*.
3. Click **Save**.

10.8 Face Comparison and Modeling

For certain device models, you need to enable **Multi-Target-Type Detection** or **Face Capture** on **VCA Resource** page first.

10.8.1 Face Comparison

Face comparison serves the purpose of face recognition by comparing the captured faces with those in the face picture library.

Set Face Picture Library
Face picture library is used to store modeled human faces and information.

Steps

1. Go to Configuration → Face Picture Library.
2. Create a face picture library.

1) Click + to add a face picture library.

2) Input library name, threshold and remarks.

   - **Threshold**: Face similarity higher than the set threshold triggers face picture comparison alarm uploading.

3) Click **OK**.

4) Optional: Modify a face picture library. Select the desired library and click ⚙ and change related parameters.

5) Optional: Delete a library. Select the desired library and click ×.

3. Add face pictures to the library.

   NOTE: The picture format should be JPEG, and the size no larger than 300 KB per file.

   - **Add one face picture:** Click **Add** and upload the face picture with detailed face information.
   - **Import face picturesin batch:** Click **Import** and select picture path.

     NOTE: When you import face pictures in batch, the picture name is saved as the face name. For other face information, modify one-by-one manually.

     The verification code for exporting and importing should be a combination of 8 to 16 digits, containing numerics, upper case, and lower case letters.

4. Optional: Modify face information.

   1) Select a face picture library.

   2) Select the target face picture. You can use the search function to locate the picture by inputting search conditions such as name and gender, and clicking **Search**.

   3) Click **Modify**.

   4) Edit detailed information.

      NOTE: Face picture is not allowed to change.

   5) Click **OK**.

5. Create models for each face picture in library.

   NOTE: Modeling process builds up a face model for each face picture. Face model is required for face picture comparison to take effect.

   - **Modeling:** Select one or more face pictures, and click **Modeling**.
   - **Batch Modeling:** Select a face picture library, and click **Batch Modeling**.

6. Optional: Repeat to create more face libraries.

7. Click **Save**.

Set Face Picture Comparison

Compares captured pictures with face pictures in a library and outputs comparison result. Comparison result can trigger certain actions when arming schedule and linkage method are set.

Before You Start

You should first create a face picture library and add face pictures. See *Set Face Picture Library*.

Steps

1. Go to Configuration → Comparison and Modeling → Face Comparison and Modeling.
2. Select Face Picture Comparison.
3. Check Enable Face Picture Comparison.
4. Select a face picture library as the reference.
5. Optional: Check **Report Face Comparison Information During Multi-Target-Type Capture Alarm**, if you want to receive face comparison information during multi-target-type capture alarm.
6. Select desired face information to upload.
7. Select a face comparison mode.
    - **Best Comparison:** The device captures and compares the target face continuously when the face target stays in the detection area, and uploads the best scoring face picture and related alarm information when the target face leaves the area.
    - **Quick Comparison:** The device captures and compares the target face when the face grading exceeds the set **Face Grading Threshold for Capture**.
    - **Face Grading Threshold for Capture**: The face grading threshold for the device to judge whether to capture and upload the face or not.
    - **Max. Capture Interval**: The maximum interval between two captures when the target is in the detection area. The camera takes the capture when it reaches the **Max. Capture Interval** even if the face grading does not reach the set threshold.
    - **Quick Setup Mode**: Select the mode according to actual using scenarios. In custom mode, you can set **ComparisonTimeout** and **Comparison Times**.
8. Set arming schedule. See *Set Arming Schedule*.
9. Set linkage method. See *Linkage Method Settings*.

View Face Comparison Result

Steps

1. Go to Application.

2. Set search condition and click **Counting**. Matched results are shown in **Face Picture Comparison Statistics** area.

10.8.2 Face Modeling

Collects face pictures, creates face models, and uploads data to the surveillance center.

Before You Start

Configure Face Capture or Multi-Target-Type detection for face picture collection. See *Face Capture* or *Multi-Target-Type Detection* for configuration instructions.

Steps

1. Go to Configuration → Comparison and Modeling → Face Comparison and Modeling.
2. Select **Face Modeling** to start.
3. Check Enable Face Modeling.
4. Set parameters for modeling.
   - **Report Face Modeling Information in Multi-Target-Type Capture Alarm**: When a person triggers the multi-target-type detection, the alarm information includes the face modeling information of the detected face if checked.
   - **Quick Capture**: The device starts face modeling when it detects a face that scores higher than the set face grading threshold for capture.
   - **Face Grading Threshold for Capture**: The face grading threshold for the device to judge whether to capture and upload the face or not. A higher value means better picture quality.
   - **Max. Capture Interval**: The maximum interval between two captures when the target is in the detection area. The camera takes the capture when it reaches the **Max. Capture Interval** even if the face grading does not reach the set threshold.
5. Set arming schedule. See *Set Arming Schedule*.
6. Set linkage method. See *Linkage Method Settings*.

Chapter 11 Open Platform

Open platform allows you to install the application for a third-party to develop and run its function and service.

NOTE: Only certain device models support this function.

11.1 Set Open Platform

Steps

1. Go to Configuration → Open Platform.

   NOTE: Before installing the application, read the Disclaimer at the bottom and 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 of the available memory and computing power of the device.

2. In **Install Apps**, click **Browse** and select the imported application package.

3. Click **Import** to complete the installation.

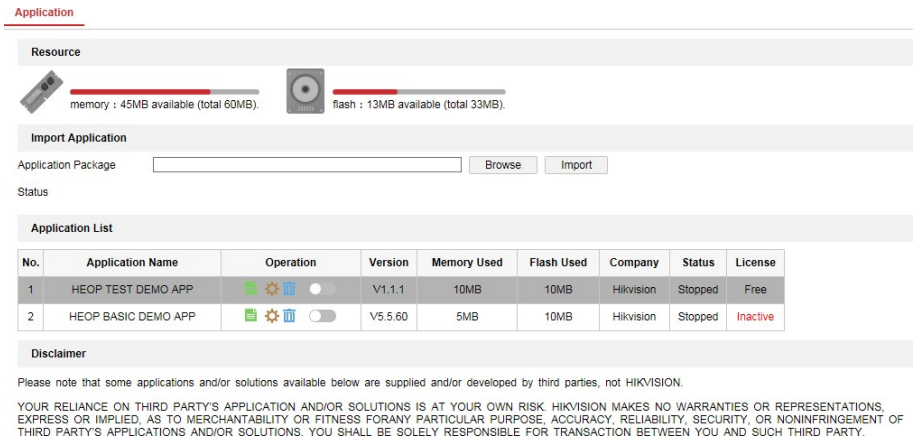


Figure 15, Open Platform

The installed applications and their related information are displayed in the **Application List** such as application name, operation, version, memory used, flash used, company, status, and license.

4. Optional: Set application.

   - Export log.
   - Set permission.

- Delete the application.
- Enable or disable the application.

5. Optional: In application display, click **Browse** and import the application certificate.

Chapter 12 Set EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement.

Before You Start

To use the EPTZ function, select **Fourth Stream** in live view. Fourth stream and EPTZ must be both enabled simultaneously.

Steps

1. Go to Configuration → EPTZ.
2. Check Enable EPTZ.
3. Check Fourth Stream.
4. Select the **Application**. **Patrol** and **Auto-tracking** are selectable.

Chapter 13 Smart Display

Displays captured pictures when enabling smart functions.

- **Layout Preview**: Click and select **Layout Preview**. Select the contents according to your needs. When you select real-time analysis, you can select the contents only for real-time analysis.
- **Detection Attribute**: Click and select **Detection Attribute**. When you enable this function, the attribute information of target analysis can be displayed and the information you select will be displayed in the attribute analysis area.

Device Commands

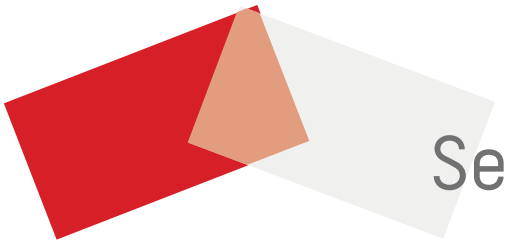
Scan the following QR code to get device common serial port commands.

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

Device Communication Matrix

Scan the following QR code to get device communication matrix.

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



See Far, Go Further