Zoom Camera and Zoom Camera Module

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's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Contents

Chapter 1 Overview

1.1 Product Introduction

Network zoom camera and zoom camera module are digital monitoring products with video capture, smart encoding compression, and network transmission functions. The device is equipped with embedded operation system and high-performance hardware that guarantee reliability.

The device is well suited for HD monitoring in various places, such as warehouses, residential blocks, ports, squares, schools, stations, and parks.

1.2 Key Function

The key functions of the device are as follows. Actual functions may vary for different models. You can enable the functions as you need.

Face Capture

The device captures human faces and uploads the pictures to the center.

Event Function

The device detects basic events and multiple smart events.

1.3 System Requirement

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

	Recommended Specifications
Operating System	Microsoft Windows XP/ Windows 7/ Windows 8/ Windows 10 Mac OS 10.13 or later
CPU	Intel® Pentium® IV 3.0 GHz or higher
RAM	1 GB or higher
Display	1024 × 768 resolution or higher
Web Browser	Internet Explorer 10 and above version, Apple Safari 12 and above version, Mozilla Firefox 52 and above version, Google Chrome 57 and above version.

Chapter 2 Device Activation and Accessing

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

Note

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

2.1 Activate Device

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

2.1.1 Activate Device via Web Browser

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

Before You Start

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

Steps

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

   The default IP address of the device is 192.168.1.64.
2. Open a web browser and input the default IP address.
3. Create and confirm the admin password.

   Caution

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Click **OK** to complete activation and enter **Live View** page.
5. Modify IP address of the camera.

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

   2) Change IP address.

   3) Save the settings.

2.1.2 Activate via SADP

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

Before You Start

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

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

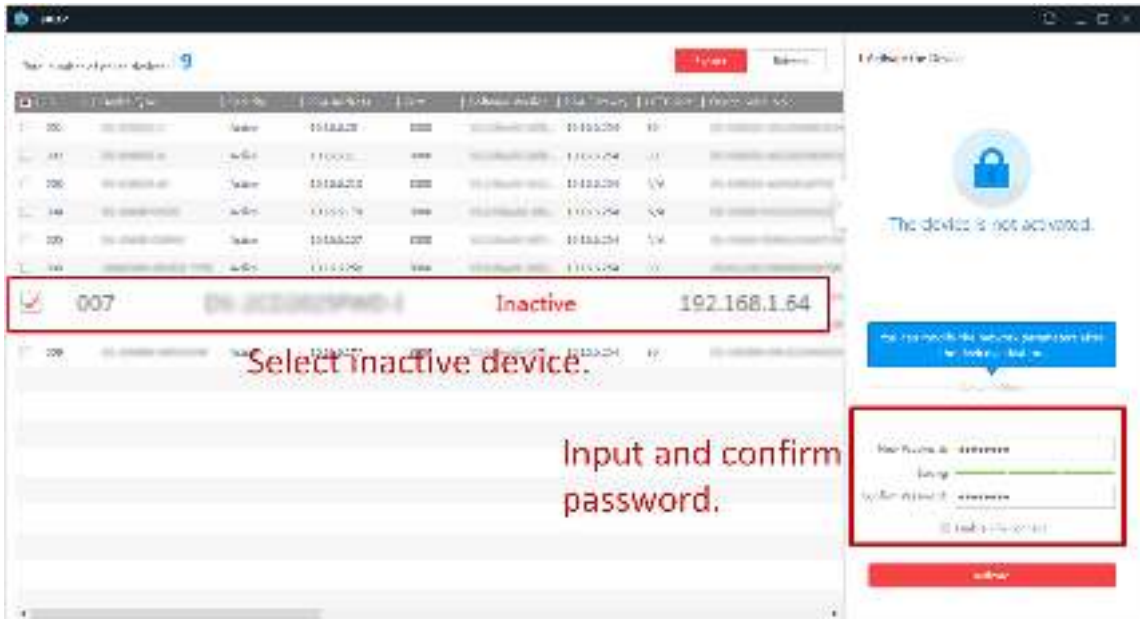
Steps

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

Caution

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

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



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

5. Modify IP address of the device.

1) Select the device.

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

2.2 Access Device via Web Browser

Before You Start

Check the system requirement to confirm that the operating computer and web browser meets the requirements. See ***System Requirement*** .

Steps

1. Open the web browser.
2. Input IP address of the device to enter the login interface.
3. Input user name and password.

Note

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

4. Click **Login**.
5. Download and install appropriate plug-in for your web browser.

   For IE based web browser, webcomponents and QuickTime™ are optional. For non-IE based web browser, webcomponents, QuickTime™, VLC and MJEPG are optional.

2.2.1 Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	Internet Explorer 10+	Follow pop-up prompts to complete plug-in installation.
Windows 7 and above version	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 12+	Plug-in installation is not required. Go to **Configuration → Network → Advanced Settings**

Operating System	Web Browser	Operation
		→ **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 device only supports Windows and Mac OS system and do not support Linux system.

2.2.2 Admin Password Recovery

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

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

Note

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

Security Question

You can set the account security during the activation. Or you can go to **Configuration → System → User Management** , click **Account Security Settings**, select the security question and input your answer.
You can click **Forget Password** and answer the security question to reset the admin password when access the device via browser.

Email

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

2.2.3 Illegal Login Lock

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

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

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Smart Function

3.1 Allocate VCA Resource

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

Steps

1. Go to **Open Platform → VCA Resource** .
2. Select desired VCA functions.
3. Save the settings.

Note

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

3.2 Set Camera Info

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

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

3.3 Face Capture

Face capture function detects faces and captures pictures. When the grading of the detected face exceeds an algorithm-defined value, the device captures the face and triggers linkage actions. Set up rule and parameters before using the function.

Note

- This function is only supported by certain device models.
- To enable this function, you may need to select **Face Capture** on **VCA Resource** page. See ***Allocate VCA Resource*** for details.

3.3.1 Set Face Capture

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

Before You Start

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

Steps

1. Go to **Open Platform → 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. Input or draw the min. pupil distance and the max. pupil distance.

   The **Min. Pupil Distance** and the **Max. Pupil Distance** are used to improve detection accuracy. Only targets whose pupil distance are between the maximum distance and the minimum distance trigger the capture.

   Click and to draw the distance on live image, or input values in the text fields of **Min. Pupil Distance** and **Max. Pupil Distance**.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the 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 Algorithm Parameters*** .

Result

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

3.3.2 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**.

3.3.3 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

You can set the face picture type by selecting **Custom**, **Head Shot**, **Half-Body Shot**, or **Full-Body Shot**. If you select **Custom**, you can define detailed picture width and height of a picture freely. If the captured pictures should have the same picture height, check **Fixed Value** and input desired picture height.

Background Picture Settings

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

Text Overlay

You can check desired items (Device No., Camera Info. and Capture Time) and adjust their order to display on captured pictures by .

See ***Set Camera Info*** to set **Device No.** and **Camera Info**.

3.3.4 Face Capture Algorithm Parameters

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

Face Capture Version

It refers to the current algorithm version, which cannot be edited.

Restore Defaults

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

Capture Parameters

Best Shot

The device captures the target picture with the highest score after setting the parameters.

Capture Times

It refers to the capture times that a face will be captured during its stay in the detection area.

Capture Threshold

It refers to the quality of face that triggers capture and alarm. Higher value means that better quality should be met to trigger capture and alarm.

Remove Duplicated Faces

This function can filter out repeated captures of a face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

Every face picture is kept in the duplicates removing library for the set update time.

Quick Shot

The device captures the target picture once the score of the captured face exceeds the **Quick Shot Threshold** during the **Max. Capture Interval**. Otherwise, the device selects and uploads the picture with the highest score during the **Max. Capture Interval**.

Quick Shot Threshold

It refers to the quality of face to trigger quick shot.

Max. Capture Interval

It describes the max. time occupation for one quick shot.

Capture Times

It refers to the capture times that a face will be captured during its stay in the configured area. The device captures the target face according to the set times.

Face Exposure

Enable the function, and the device automatically adjusts exposure level when human faces appear in the scene.

Reference Brightness

It refers to the reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lower 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

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be

triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Chapter 4 PTZ

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the camera.

4.1 Lens Control

On the live view page, you can use the lens control buttons to control the zooming, focusing, and aperture level of the device.

Zoom in/out

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

Note

- You can set **Zooming Speed** in **Configuration → PTZ → Basic Settings** . The higher the value is, the faster the zooming speed is.
- You can set **Zoom Limit** in **Configuration → Image → Display Settings → Other** to limit the maximum value of the total zoom (digital zoom and optical zoom).

Focus

	Click the button, the lens focuses near, and the object nearby gets clear.
	Click the button, the lens focuses far, and the object far away gets clear.

Iris

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

4.2 Set Preset

A preset is a predefined image position. For a defined preset, you can call the preset No. to view the position.

Steps

1. Click to show the setting panel, and click .
2. Use the lens control buttons to move the lens to the desired position.
3. Select a preset number from the preset list, and click to finish the setting.

Note

Some presets are predefined with special command. You can only call them but not configure them.

4. Repeat the steps above to set multiple presets.

Click the button to call the preset.

Click the button to delete the preset.

Note

You can delete all presets in **Configuration → PTZ → Clear Config** . Check **Clear All Presets**, and click **Save**.

4.3 Set Patrol Scan

Patrol scan is a function to automatically move among multiple presets.

Before You Start

Make sure that you have defined more than one presets. See ***Set Preset*** for detailed configuration.

Steps

1. Click to show the setting panel, and click to enter patrol setting interface.
2. Select a patrol number from the list and click .
3. Click to add presets.

Preset

Select predefined preset.

Speed

Set the speed of moving from one preset to another.

Time

It is the duration staying on one patrol point.

Delete the presets in patrol.

Adjust the preset order.

Note

A patrol can be configured with 32 presets at most, and 2 presets at least.

4. Click **OK** to finish a patrol setting.
5. Repeat the steps above to configure multiple patrols.
6. Operate patrols.

   Call the patrol.

   Stop patroling.

   Delete the patrol.

   Set the patrol.

Note

You can delete all patrols in **Configuration → PTZ → Clear Config** . Click **Clear All Patrols**, and click **Save**.

4.3.1 Set One-Touch Patrol

The device automatically adds presets to one patrol path and starts patrol scan.

Steps

1. Set two or more presets among preset No.1 to preset No.32. For setting presets, refer to ***Set Preset*** .

   The device will automatically add presets to patrol path No.8.
2. Choose one of the following methods to enable the function.
   - Click .
   - Call patrol path No.8.
   - Select and call preset No.45.

4.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

1. Click to show the setting panel, and click .
2. Select one pattern scan path that needs to be set.
3. Click to start recording pattern scan.
4. Click lens control buttons to move the device as you need.

Note

Recording stops when the space for pattern scan is 0%.

5. Click to complete one pattern scan path settings.

6. Click ▶ to call pattern scan.

   ■ Stop pattern scan.

   ◉ Reset pattern scan path.

   ✕ Delete the selected pattern scan.

Note

If you need to delete all the pattern scans, go to **Configuration → PTZ → Clear Config** , and check **Clear All Patterns**, and click **Save**.

4.5 Set Scheduled Tasks

You can set the device to perform a certain task during a certain period.

Steps

1. Go to **Configuration → PTZ → Scheduled Tasks** .
2. Check **Enable Scheduled Task**.
3. Select the task type and set the period. For setting the period, refer to ***Set Arming Schedule*** .
4. Repeat step 3 to set more than one scheduled tasks.
5. Set **Park Time**. During the set task period, if you operate the device manually, the scheduled task will be suspended. When the manual operation is over, the device will continue to perform the scheduled task after the set park time.
6. Click **Save**.

Note

If you want to clear all scheduled tasks, go to **Configuration → PTZ → Clear Config** , check **Clear All Scheduled Tasks**, and click **Save**.

4.6 Set Park Action

You can set the device to perform an action (for example, preset or patrol) or return to a position after a period of inactivity (park time).

Before You Start

Set the action type first. For example, if you want to select patrol as park action, you should set the patrol. See ***Set Patrol Scan*** for details.

Steps

1. Go to **Configuration → PTZ → Park Action** .
2. Check **Enable Park Action**.
3. Set **Park Time**: the inactive time before the device starts park action.
4. Select **Action Type** according to your needs.
5. Select an **Action Type ID**, if you select patrol or preset as action type.

When the action type is patrol, action type ID stands for patrol No. When the action type is preset, action type ID stands for preset No.

6. Click **Save**.

4.6.1 Set One-Touch Park

This function is used to start park instantly.

Steps

1. Refer to ***Set Park Action*** to set a park action.
2. Choose from the following methods to start one-touch park.
   - Click .
   - Call Preset No. 32.

4.7 Set Privacy Mask

Privacy masks cover certain areas on the live image to protect personal privacy from being live viewed and recorded.

Steps

1. Go to **Configuration → PTZ → Privacy Mask** .
2. Adjust the live image to the target scene via PTZ control buttons.
3. Draw the area.

Draw Area	Click **Draw Area**, and click on the live view image to determine the boundary of the mask.
Stop Drawing	Click**Stop Drawing** after drawing the mask.

4. Click **Add**.

   It is listed in **Privacy Mask List**.
5. Edit **Name**, **Type**, and **Active Zoom Ratio** on your demand.

   Active Zoom Ratio

   When the actual zoom ratio is less than the set active zoom ratio, the set area can not be covered. When the actual zoom ratio is greater than the set active zoom ratio, the privacy mask is valid. The maximum value of active zoom ratio depends on the camera module.

   Note

   Active zoom ratio is only supported for the PTZ channel.
6. Repeat the steps above to set other privacy masks.
7. Check **Enable Privacy Masks**.

4.8 Set Power Off Memory

This function can resume the previous PTZ status of device after it restarting from a power-off.

Steps

1. Go to **Configuration → PTZ → Basic Settings** .
2. Select **Resume Time Point**. When the device stays at one position for the set resume time point or more, the position is saved as a momory point. The device returns to the last memory point when it restarts.
3. Click **Save**.

Chapter 5 Live View

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

5.1 Live View Parameters

The supported functions vary depending on the model.

5.1.1 Start and Stop Live View

Click **Live View**. Click to start live view. Click to stop live view.

5.1.2 Aspect Ratio

Aspect Ratio is the display ratio of the width to height of the image.

- refers to 4:3 window size.
- refers to 16:9 window size.
- refers to original window size.
- refers to self-adaptive window size.
- refers to original ratio window size.

5.1.3 Live View Stream Type

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

5.1.4 Quick Set Live View

It offers the quick access to the display settings, OSD, and video/audio on live view page.

Steps

1. Click and click **General** to show quick setup page.

2. Set display settings, OSD, and video/audio.

- For parameter explanation and instructions of display settings, see ***Display Settings*** .
- For parameter explanation and instructions of OSD settings, see ***OSD*** .
- For parameter explanation and instructions of audio and video settings, see ***Video and Audio*** .

5.1.5 Select the Third-Party Plug-in

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

Steps

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

5.1.6 Start Digital Zoom

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

Steps

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

5.1.7 Conduct Regional Focus

You can enable the function to focus on certain area.

Steps

1. Click to enable regional focus.
2. Drag the mouse on the live view to draw a rectangle as the desired focus area.
3. Click to disable this function.

5.1.8 Conduct Regional Exposure

When the brightness of live view is not balanced, you can enable this function to optimize the exposure of the selected image region.

Steps

1. Click to enable regional exposure.
2. Drag the mouse on the live view to draw a rectangle as the desired exposure area.
3. Click to disable this function.

5.1.9 Count Pixel

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

Steps

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

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

5.1.10 Lens Initialization

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

Click to operate lens initialization.

5.1.11 OSD Menu

When network access is unavailable, you can call the Preset No.95 to show OSD menu to start device configuration.

Click direction buttons or and to move up and down.

Click to confirm your selection.

5.1.12 Display Target Information on Live View

Go to **Configuration → Local → Live View Parameters** for settings.

Note

Related smart function should be configured and enabled in advance.

Display POS Information

POS information refers to the target features, such as target ID, etc. Supported POS information types varies according to device models.

5.2 Set Transmission Parameters

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

Steps

1. Go to **Configuration → Local** .

2. Set the transmission parameters as required.

Protocol

TCP

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

UDP

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

MULTICAST

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

Note

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

HTTP

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

Play Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

3. Click **OK**.

5.3 Smart Display

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

Note

To use this function, your web browser version should be above IE11.0.9600.17843.

Live View Parameter

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

Download Display Pictures

Click  and the device stores captured pictures to the browser cache. Hover the pointer over the icon to see the number of pictures in the cache. Click  again to download the pictures in a package.

Note

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

Layout

Click  and choose **Layout**. Check the display content you need to add it to the smart display page. When real-time analyze is selected, you can choose the contents you want to display.

Chapter 6 Video and Audio

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

6.1 Video Settings

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

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

6.1.1 Stream Type

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

Main Stream

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

Sub Stream

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

Other Streams

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

6.1.2 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.

6.1.3 Resolution

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

6.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

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

Variable Bitrate

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

6.1.5 Video Quality

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

6.1.6 Frame Rate

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

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

6.1.7 Video Encoding

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

Note

Available compression standards vary according to device models.

H.264

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

H.264+

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

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

Note

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

H.265

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

H.265+

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

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

Note

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

Profile

This function means that under the same bitrate, the more complex the profile is, the higher the quality of the image is, and the requirement for network bandwidth is also higher.

SVC

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

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

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

Smoothing

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

MJPEG

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

6.1.8 I-Frame Interval

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

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

6.2 Audio Settings

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

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

6.2.1 Audio Input

External audio pick-up device is available for audio input, and audio encoding and input volume are configurable.

Audio Encoding

The device offers several compression standard. Select according to your need.

Audio Input

LineIn is supported for external audio pick-up device.

Input volume

Adjust the volume of the audio input.

6.2.2 Environmental Noise Filter

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

6.3 Two-way Audio

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

Before You Start

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

Steps

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

6.4 ROI

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

6.4.1 Set ROI

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

Before You Start

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

Steps

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

   Note

   Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.
5. Input the **Region Name** and **ROI Level**.
6. Click **Save**.

   Note

   The higher the ROI level is, the clearer the image of the detected region is.
7. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

6.5 Display Info. on Stream

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

Steps

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

6.6 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

6.6.1 Scene Mode

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

Image Adjustment

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

Exposure Settings

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

Exposure Mode

Auto

The iris, shutter, and gain values are adjusted automatically.

You can limit the changing ranges of iris, shutter and gain by setting **Max. Iris Limit**, **Min. Iris Limit**, **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Iris Priority

The value of iris needs to be adjusted manually. The shutter and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the shutter and gain by setting **Max. Shutter Limit**, **Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Shutter Priority

The value of shutter needs to be adjusted manually. The iris and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the iris by setting **Max. Iris Limit**, **Min. Iris Limit** and **Limit Gain** for better exposure effect.

Manual

You need to set **Iris**, **Shutter**, and **Gain** manually.

Slow Shutter

The higher the slow shutter level is, the slower the shutter speed is. It ensures full exposure in underexposure condition.

Focus

It offers options to adjust the focus mode and the minimum focus distance.

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

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

Day

The image is always in color.

Night

The image is always black/white

Auto

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

Scheduled-Switch

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

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 alarm input signal.

Note

Day/Night Switch function varies according to models.

BLC

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

HLC

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

WDR

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

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

Note

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

DNR

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

Normal

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

Expert

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

White Balance

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

Defog

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

EIS

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

Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.

Note

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

Video Standard

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

6.6.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

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

Set 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**.

6.7 OSD

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

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

Character Set

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

Displayed Information

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

Text Overlay

Set customized overlay text on image.

OSD Parameters

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

Chapter 7 Video Recording and Picture Capture

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

7.1 Storage Settings

This part introduces the configuration of several common storage paths.

7.1.1 Memory Card

You can view the capacity, free space, status, type, and property of the memory card. Encryption of memory card is supported to ensure data security.

Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.
3. Click **Format** to initialize the memory card.

   When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.
4. **Optional:** Encrypt the memory card.
   1) Click **Encrypted Format**.
   2) Set the encryption password.
   3) Click **OK**.

   When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

   Note

   Keep your encryption password properly. Encryption password cannot be found if forgotten.
5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

- Insert an encrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.
- You need to know the correct encryption password of the memory card.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management** .
2. Select the memory card.

   Note

   If an **Unlock** button appears, you need to unlock the memory card first. See ***Detect Memory Card Status*** for details.
3. Verify the encryption password.
   1) Click **Parity**.
   2) Enter the encryption password.
   3) Click **OK**.

      When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

   Note

   If the encryption password is forgotten and you still want to use this memory card, see ***Set New or Unencrypted Memory Card*** to format and set the memory card. All existing contents will be removed.
4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

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

Before You Start

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

Steps

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

   Remaining Lifespan

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

Health Status

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

Note

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

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

Note

- Only admin user can set the **R/W Lock**.
- The memory card can only be read and written when it is unlocked.
- If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.

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

7.1.2 Set FTP

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

Before You Start
Get the FTP server address first.

Steps

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

   Server Address and Port

   The FTP server address and corresponding port.

   User Name and Password

   The FTP user should have the permission to upload pictures.

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

   Directory Structure

   The saving path of snapshots in the FTP server.

   Picture Filling Interval

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

   Picture Name

   Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.
3. Click **Upload Picture** to enable uploading snapshots to the FTP server.
4. Click **Test** to verify the FTP server.
5. Click **Save**.

7.1.3 Set NAS

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

Before You Start

Get the IP address of the network disk first.

Steps

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

   Server Address

   The IP address of the network disk.

   File Path

   The saving path of network disk files.

   Mounting Type

Select file system protocol according to the operation system.

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

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

7.1.4 Set Cloud Storage

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

Steps

Caution

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

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

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.
Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

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

7.2 Video Recording

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

7.2.1 Record Automatically

This function can record video automatically during configured time periods.

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

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

Note
The record type is vary according to different models.

Continuous
The video will be recorded continuously according to the schedule.

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

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

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

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

Event
The video is recorded when configured event is detected.

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

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

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

Post-record

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

Stream Type

Select the stream type for recording.

Note

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

Recording Expiration

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

6. Click **Save**.

7.2.2 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.

7.2.3 Playback and Download Video

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

Steps

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

   The matched video files showed on the timing bar.
3. Click to play the video files.
   - Click to clip video files.
   - 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 search condition and click **Search**.
   2) Select the video files and then click **Download**.

Note

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

7.3 Capture Configuration

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

7.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

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

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

   Timing

   Capture a picture at the configured time interval.

   Event-Triggered

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

7.3.2 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.

7.3.3 View and Download Picture

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

Steps

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

   The matched pictures showed in the file list.
3. Select the pictures then click **Download** to download them.

Note

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

Chapter 8 Event and Alarm

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

8.1 Basic Event

8.1.1 Set Motion Detection

This function detects moving objects in the detection region and trigger linkage actions.

Steps

1. Go to **Configuration → Event → Basic Event → Motion Detection** .
2. Check **Enable Motion Detection**.
3. **Optional:** Highlight moving objects in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Go to **Configuration → Local** to enable **Rules**.
4. Select **Configuration Mode**. Normal mode and expert mode are selectable.
   - For the information about normal mode, see ***Normal Mode*** .
   - For the information about expert mode, see ***Expert Mode*** .
5. Set the arming schedule. See ***Set Arming Schedule*** for details.
6. Set linkage methods. See ***Linkage Method Settings*** for details.
7. Click **Save**.

Normal Mode

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

Steps

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

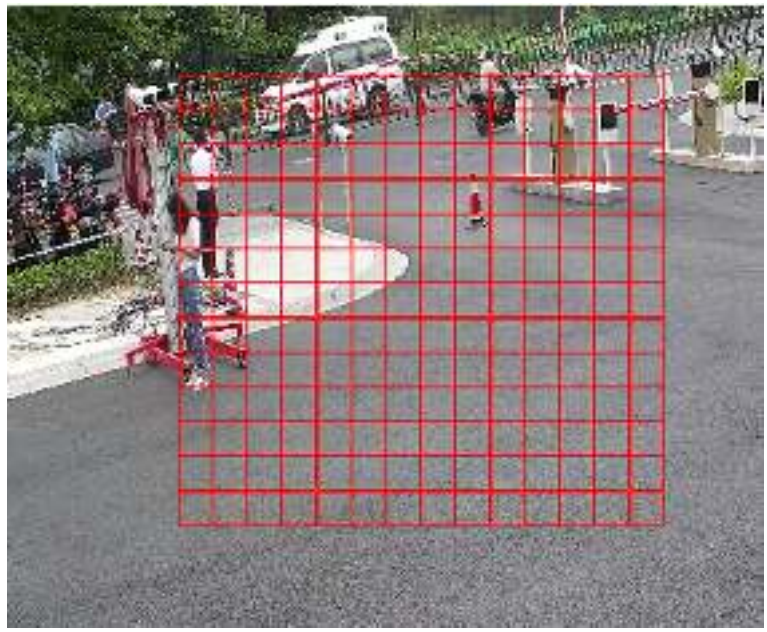


Figure 8-1 Set Rules

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.

Expert Mode

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

Steps

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

Scheduled Image Settings

OFF

Image switch is disabled.

Auto-Switch

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

Scheduled-Switch

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

Sensitivity

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

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

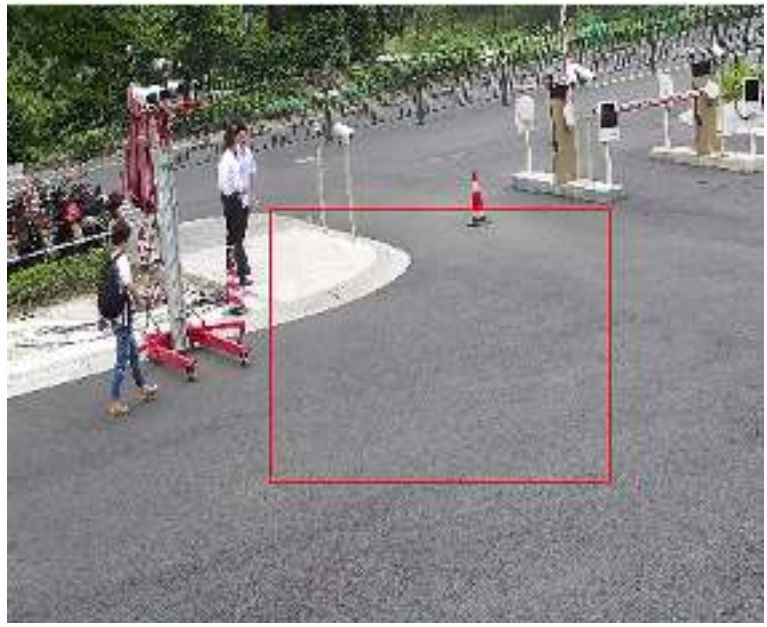


Figure 8-2 Set Rules

Stop Drawing Finish drawing one area.

Clear All Delete all the areas.

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

8.1.2 Set Video Tampering Alarm

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

Steps

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

Stop Drawing Finish drawing.

Clear All Delete all the drawn areas.

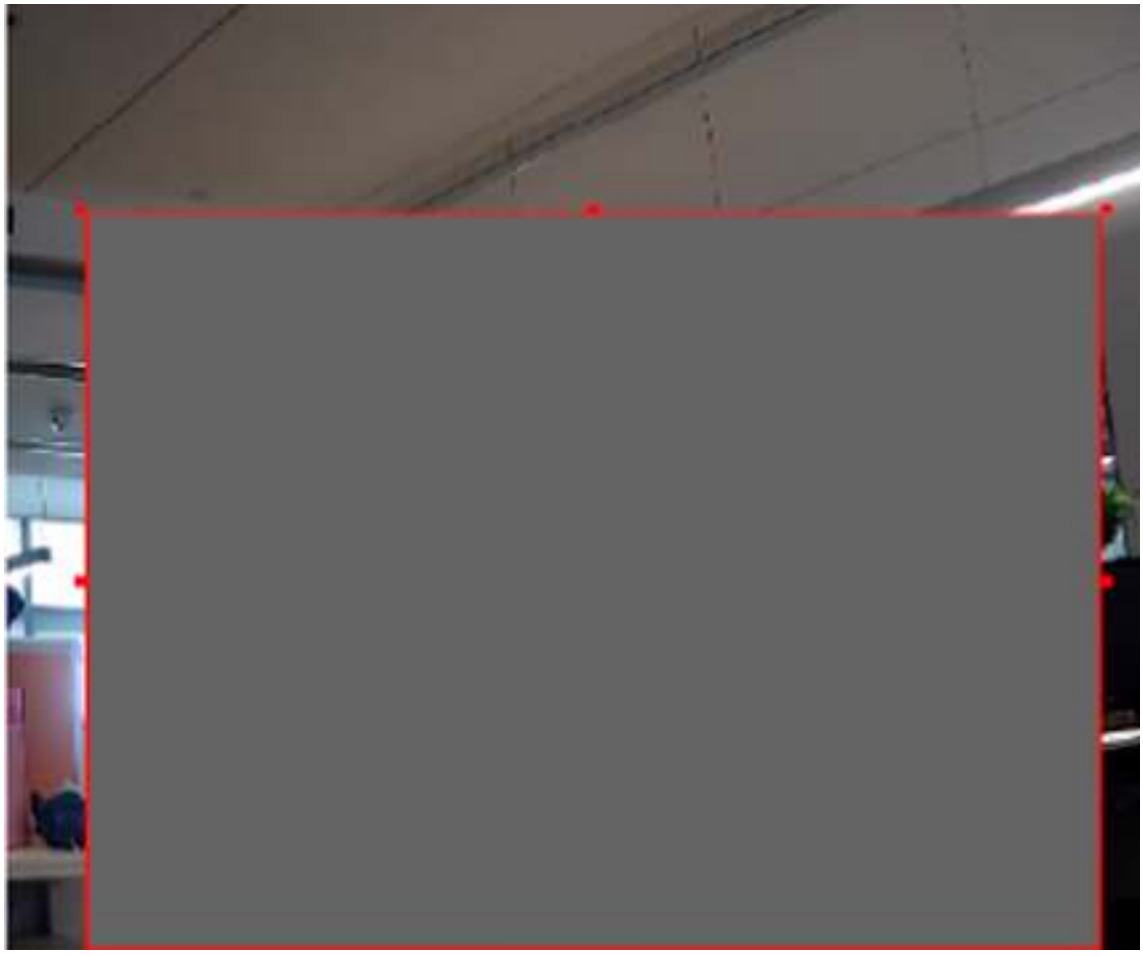


Figure 8-3 Set Video Tampering Area

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

8.1.3 Set Alarm Input

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

Before You Start

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

Steps

1. Go to **Configuration → Event → Basic Event → Alarm Input** .
2. Check **Enable Alarm Input Handling**.
3. Select **Alarm Input NO.** and **Alarm Type** from the dropdown list. Edit the **Alarm Name**.

4. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
5. Click **Copy to...** to copy the settings to other alarm input channels.
6. Click **Save**.

8.1.4 Set Exception Alarm

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

Steps

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

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.
Network Disconnected	The device is offline.
IP Address Conflicted	The IP address of current device is same as that of other device in the network.
Illegal Login	Incorrect user name or password is entered.

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

8.2 Smart Event

Note

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

8.2.1 Detect Audio Exception

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

Steps

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

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

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

Note

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

Sudden Decrease of Sound Intensity Detection

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

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

Note

The function varies according to different models.

8.2.2 Set Intrusion Detection

Intrusion detection detects the object movement of entering and loitering in a predefined area. When intrusion occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.
4. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.

5. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value of sensitivity is, the more easily the target is detected.
Threshold	Threshold stands for the time of the target loitering in the region. If the time that they stay in the region exceeds the threshold, the alarm is triggered.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.

Figure 8-4 Draw Area

6. Click **Save**.
7. Repeat above steps to set other detection areas.
8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .

8.2.3 Set Line Crossing Detection

Line crossing detection is used to detect the object movement of crossing a predefined line. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Line Crossing Detection** .

2. Check **Enable**.
3. Draw a detection line.
   1) Select a **Line No.**. Up to 4 lines can be set in the scene.
   2) Click **Detection Area**.

      A yellow line is displayed on live image.
   3) Click on the line, and drag its end points to adjust the length and position.
   4) Select the **Direction** for the detection line.

      Direction

      It stands for the direction from which the object goes across the line.

      A<->B

      The objects going across the line from both directions can be detected and alarms are triggered.

      A->B

      Only the objects crossing the configured line from side A to side B can be detected.

      B->A

      Only the objects crossing the configured line from side B to side A can be detected.

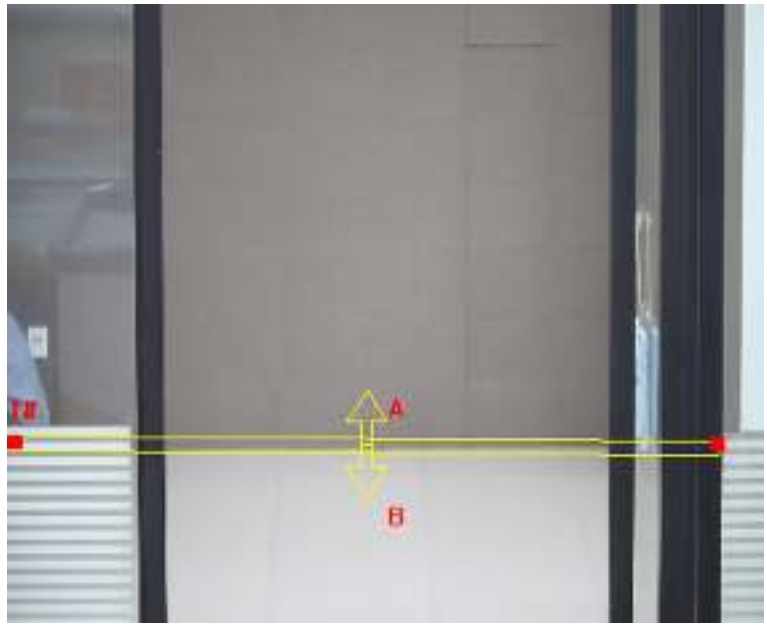


Figure 8-5 Draw Line

4. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.

2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.

5. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.

6. Click **Save**.
7. Repeat above steps to set other lines.
8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .

8.2.4 Set Region Entrance Detection

Region entrance detection is used to detect the object movement of entering a predefined area. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Region Entrance Detection** .
2. Check **Enable**.
3. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.
4. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
5. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.

Figure 8-6 Draw Area

6. Click **Save**.
7. Repeat above steps to set other regions.
8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .

8.2.5 Set Region Exiting Detection

Region exiting detection is used to detect the objects movement of exiting from a predefined area. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Region Exiting Detection** .
2. Check **Enable**.
3. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.

4. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
5. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.

Figure 8-7 Draw Area

6. Click **Save**.
7. Repeat above steps to set other regions.
8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .

8.2.6 Set Object Removal Detection

Object removal detection detects whether the objects are removed from the predefined detection area, such as exhibits on display. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.
4. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
5. Set detection parameters.

Sensitivity	The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
Threshold	The threshold is the time of the objects removed from the area. If you set the value as 10, alarm is triggered after the object disappears from the area for 10 seconds.

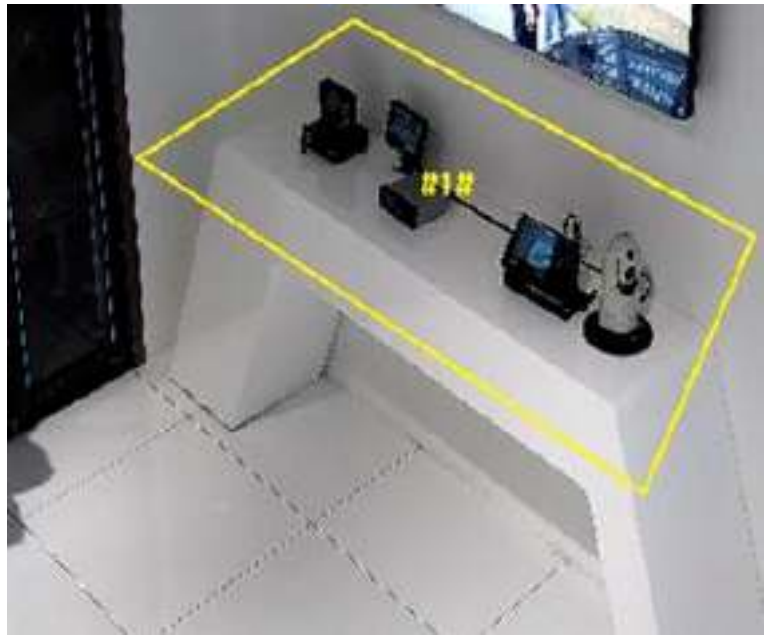


Figure 8-8 Draw Area

6. Click **Save**.
7. Repeat above steps to set other regions.
8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .

8.2.7 Set Unattended Baggage Detection

Unattended baggage detection is used to detect the objects left over in the predefined area. Linkage methods are triggered after the object is left and stays in the area for a set time period.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See ***Allocate VCA Resource*** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Unattended Baggage Detection** .
2. Check **Enable**.
3. Draw detection area.
   1) Select a **Region No.**. Up to 4 regions can be set.
   2) Click **Detection Area**.
   3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.

4. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
   1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
   2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
5. Set detection parameters.

   Sensitivity The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

   Threshold It stands for the time of the objects left in the area. Alarm is triggered after the object is left and stays in the area for the set time period.

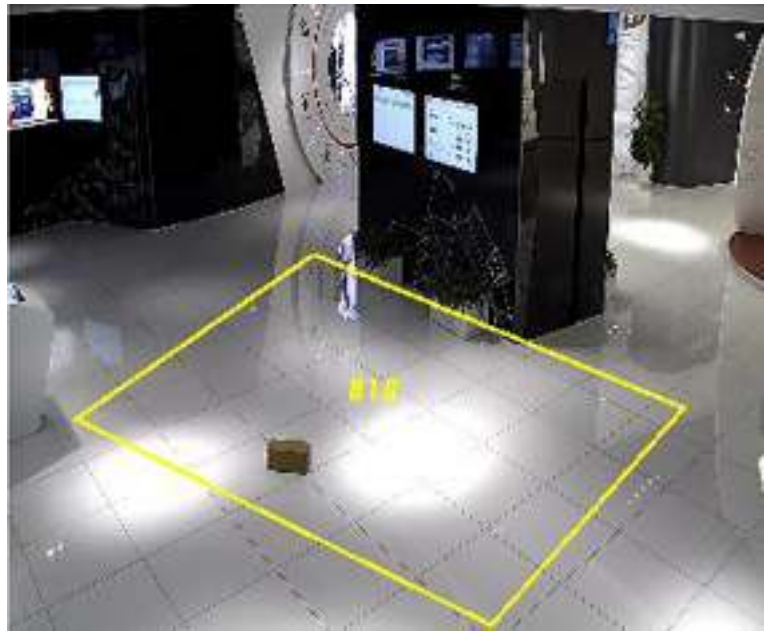


Figure 8-9 Draw Area

6. Click **Save**.
7. Repeat above steps to set other regions.
8. Set arming schedule. See ***Set Arming Schedule*** .
9. Set linkage method. See ***Linkage Method Settings*** .

Chapter 9 Arming Schedule and Alarm Linkage

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

9.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

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

   Note

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

9.2 Linkage Method Settings

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

9.2.1 Trigger Alarm Output

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

Steps

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

   Automatic Alarm For the information about the configuration, see ***Automatic Alarm*** .

   Manual Alarm For the information about the configuration, see ***Manual Alarm*** .
3. Click **Save**.

Automatic Alarm

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

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Custom a name for the alarm output.

   Delay

   It refers to the time duration that the alarm output remains after an alarm occurs.
2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule*** .
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

   Alarm Output No.

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

   Alarm Name

   Edit a name for the alarm output.

   Delay

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

9.2.2 FTP/NAS/Memory Card Uploading

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

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

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

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

9.2.3 Send Email

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

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

Set Email

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

Before You Start

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

Steps

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

      Note

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

9.2.4 Notify Surveillance Center

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

9.2.5 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***

Chapter 10 Network Settings

10.1 TCP/IP

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

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

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

Dynamic Domain Name

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

Note

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

10.1.1 Multicast

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

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

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

10.1.2 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.

10.2 Port

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

Caution

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

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

HTTP Port

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

HTTPS Port

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

RTSP Port

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

SRTP Port

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

Server Port

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

Enhanced SDK Service Port

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

WebSocket Port

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

WebSockets Port

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

Note

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

10.3 Port Mapping

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

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

Steps
1. Go to **Configuration → Network → Basic Settings → NAT** .
2. Select the port mapping mode.

Auto Port Mapping	Refer to ***Set Auto Port Mapping*** for detailed information.
Manual Port Mapping	Refer to ***Set Manual Port Mapping*** for detailed information.

3. Click **Save**.

10.3.1 Set Auto Port Mapping

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

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

10.3.2 Set Manual Port Mapping

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

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

10.3.3 Set Port Mapping on Router

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

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding → Virtual Severs** , and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

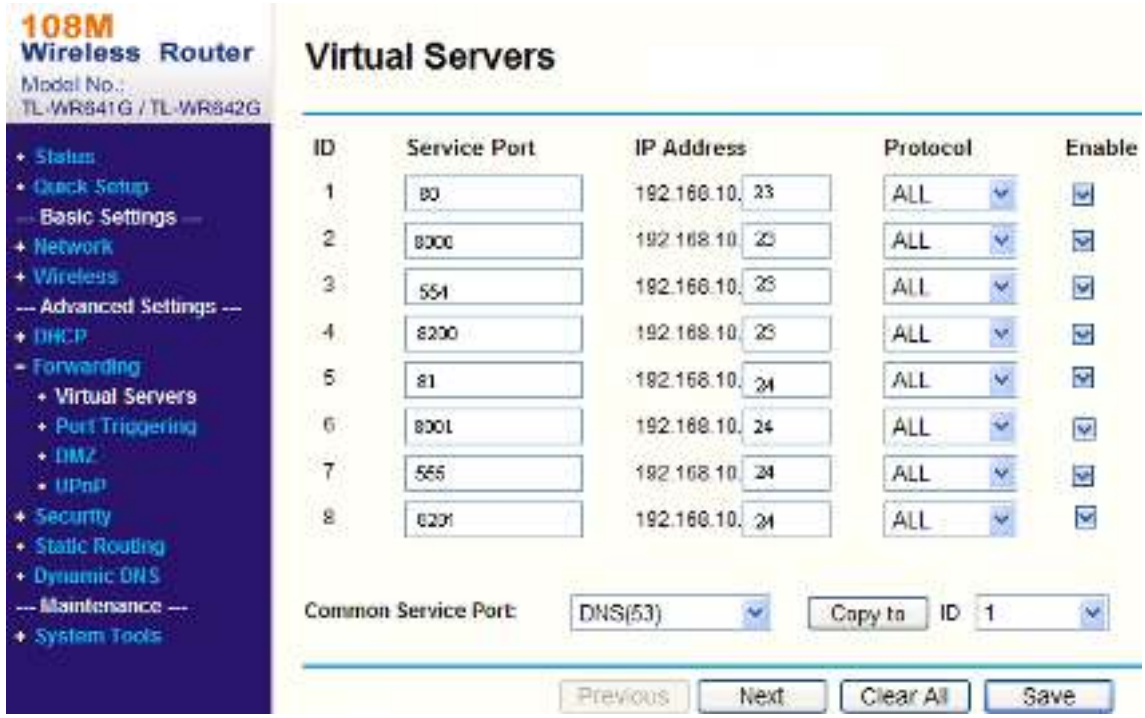


Figure 10-1 Port Mapping on Router

Note

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

10.4 SNMP

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

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

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

   Note

   The SNMP version you select should be the same as that of the SNMP software.
   And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.
3. Configure the SNMP settings.
4. Click **Save**.

10.5 Access to Device via Domain Name

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

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

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

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

   NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to ***Port*** to check the device port , and refer to ***Port Mapping*** for port mapping settings.
6. Access the device.

   By Browsers Enter the domain name in the browser address bar to access the device.

By Client Software Add domain name to the client software. Refer to the client manual for specific adding methods.

10.6 Access to Device via PPPoE Dial Up Connection

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

Steps

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

   Dynamic IP

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

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

   Input your dial-up password again.
4. Click **Save**.
5. Access the device.

   By Browsers Enter the WAN dynamic IP address in the browser address bar to access the device.

   By Client Software Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

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

10.7 Accessing via Mobile Client

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

Note

Hik-Connect service should be supported by the camera.

10.7.1 Enable Hik-Connect Service on Camera

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

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

Enable Hik-Connect Service via Web Browser

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

Before You Start

You need to activate the camera before enabling the service.

Steps

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

   Note

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

Enable Hik-Connect Service via SADP Software

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

Steps

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

   Note

   The verification code is required when you add the camera to Hik-Connect service.
5. Click and read "Terms of Service" and "Privacy Policy".

6. Confirm the settings.

10.7.2 Set Up Hik-Connect

Steps

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

Note

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

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

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

10.7.3 Add Camera to Hik-Connect

Steps

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

Note

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

5. Input the verification code of your camera.

Note

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

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

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

Note

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

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

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

10.8 Set ISUP

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

Steps

1. Go to **Configuration → Network → Advanced Settings → Platform Access** .
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.

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

10.9 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

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

   Delete Delete the selected Open Network Video Interface user.

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

10.10 Set Network Service

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

Steps

Note

This function varies according to different models.

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

   WebSocket & WebSockets

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

   If the device uses HTTP, enable WebSocket.

   If the device uses HTTPS, enable WebSockets.

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

   Note

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

   SDK Service & Enhanced SDK Service

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

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

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

   Note

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

   TLS (Transport Layer Security)

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

   Bonjour

   Uncheck to disable the protocol.
3. Click **Save**.

10.11 Set Alarm Server

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

Steps

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. 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**.

10.12 TCP Acceleration

TCP acceleration is used to improve latency and reduce packet loss caused by network congestion in poor network condition, and guarantee the fluency of live view.

10.13 Traffic Shaping

Traffic shaping is used to shape and smooth video data packet before transmission.

It helps to improve latency and reduce packet loss caused by network congestion and ensure the video quality as well. Shaping level is configurable.

10.14 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.

Chapter 11 System and Security

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

11.1 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.

11.2 Restore and Default

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

Steps

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

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

Default Reset all the parameters to the factory default.

Note

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

11.3 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.

11.4 Import and Export Configuration File

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

Steps

1. Export configuration file.
   1) Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
   2) Click **Device Parameters** and input the encryption password to export the current configuration file.
   3) Set the saving path to save the configuration file in local computer.
2. Import configuration file.
   1) Access the device that needs to be configured via web browser.
   2) Click **Browse** to select the saved configuration file.
   3) Input the encryption password you have set when exporting the configuration file.
   4) Click **Import**.

11.5 Export Diagnose Information

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

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

11.6 Reboot

You can reboot the device via browser.

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

11.7 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

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

Steps

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

Firmware	Locate the exact path of the upgrade file.

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

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

11.8 View Open Source Software License

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

11.9 Set Live View Connection

It controls the remote live view connection amount.

Live view connection controls the maximun live view that can be streamed at the same time.

Enter **Configuration → System → Maintenance → System Service** to set the upper limit of the remote connection number.

11.10 Time and Date

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

11.10.1 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**.

11.10.2 Set NTP Server

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

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

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

   Note

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

11.10.3 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**.

11.11 Set RS-485

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

Before You Start

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

Steps

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

   Note

   You should keep the parameters of the device and the computer or terminal all the same.
3. Click **Save**.

11.12 Set RS-232

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

Before You Start

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

Steps

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

11.13 Security

You can improve system security by setting security parameters.

11.13.1 Authentication

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

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

RTSP Authentication

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

RTSP Digest Algorithm

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

WEB Authentication

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

WEB Digest Algorithm

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

Note

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

11.13.2 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**.

11.13.3 Set MAC Address Filter

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

Steps

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

   Forbidden MAC addresses in the list cannot access the device.

   Allowed Only MAC addresses in the list can access the device.
4. Edit the MAC address filter list.

   Add Add a new MAC address to the list.

   Modify Modify the selected MAC address in the list.

   Delete Delete the selected MAC address in the list.
5. Click **Save**.

11.13.4 Set HTTPS

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

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable**.
3. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
4. Select a server certificate.

Note

- Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.
- If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

5. Click **Save**.

11.13.5 Security Audit Log

The security audit logs refer to the security operation 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.

Security audit logs can be saved on device internal storage. The log will be saved every half hour after device booting. Due to limited storage space, you can also save the logs on a log server.

Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

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

   The log files that match the search conditions will be displayed on the Log List.
4. **Optional:** Click **Export** to save the log files to your computer.

Set Log Server

The log server should support syslog (RFC 3164) over TLS.

Before You Start

- Install client and CA certificates before configuration. Refer to ***Certificate Management*** for detailed information.
- Select certificates according to the requirement of the log server. If two-way authentication is required, select the CA certificate and the client certificate. If one-way authentication is required, select the CA certificate only.

Steps

1. Check **Enable Log Upload Server**.
2. **Optional:** Check **Enable Encrypted Transmission** if you want the log data to be encrypted.
3. Input **Log Server IP** and **Log Server Port**.
4. **Optional:** Select client certificate.
5. Select CA certificate to the device.
6. Click **Test** to test the settings.
7. Click **Save**.

11.13.6 Set QoS

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

Note

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

Steps

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

   Note

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

11.13.7 Set IEEE 802.1X

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

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

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

Note

- If you set the **Protocol** to **EAP-TLS**, select the **Client Certificate** and **CA Certificate**.
- If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

11.13.8 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.

11.13.9 Certificate Management

It manages the server/client certificates and CA certificate of the device.

Server Certificate/Client Certificate

Note

The device has default self-signed server/client certificate installed. The certificate ID is ***default***.

Create and Install Self-signed Certificate

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Create Self-signed Certificate**.
3. Input certificate information.

   Note

   The input certificate ID cannot be the same as the existing ones.
4. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain functions, the function name is shown in the column **Functions**.
5. **Optional:** Click **Certificate Property** to see the certificate details.

Install Self-signed Request Certificate

You can send the self-signed certificate to a trusted third-party for the signature, and install the certificate to the device.

Before You Start
Create a self-signed certificate first. See ***Create and Install Self-signed Certificate*** for instructions.

Steps
1. Go to **Configuration → System → Security → Certificate Management** .
2. Select a self-signed certificate from the Server/Client Certificate list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **OK**.

   The certificate request details are displayed in a pop-up window.
6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
   1) Click **Import**.
   2) Input **Certificate ID**.

   Note

   The input certificate ID cannot be the same as the existed ones.

   3) Click **Browse** to select the certificate file.
   4) Select **Self-signed Request Certificate**.
   5) Click **OK**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.
9. **Optional:** Click **Certificate Property** see the certificate details.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps
1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Import**.
3. Input **Certificate ID**.

Note

The input certificate ID cannot be the same as the existed ones.

4. Click **Browse** to select the certificate file.
5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

Independent Key	If your certificate has a independent key, select this option. Browse to select the private key and input the private-key password.
PKCS#12	If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **OK**.

   The imported certificate is displayed in the **Server/Client Certificate** list.

   If the certificate is used by certain function, the function name is shown in the column **Functions**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Input **Certificate ID**.

Note

The input certificate ID cannot be the same as the existing ones.

3. Click **Browse** to select the certificate file.
4. Click **OK**.

   The imported certificate is displayed in the **CA Certificate** list.

   If the certificate is used by certain functions, the function name is shown in the **Functions** column.

11.13.10 User and Account

Set User Account and Permission

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

Caution

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

Steps

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

   Administrator

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

   User

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

   Operator

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

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

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

   Note

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

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.

Simultaneous Login

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

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

Appendix A. Device Command

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

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

Appendix B. Device Communication Matrix

Scan the following QR code to get device communication matrix.

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


See Far, Go Further