F Series Network Speed Dome

User Manual

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

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

Trademarks

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

Disclaimer

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

Contents

Chapter 1 Overview 1
1.1 Product Introduction 1
1.2 Key Function 1
1.3 System Requirement 1
Chapter 2 Device Activation and Accessing 3
2.1 Activate Device 3
2.1.1 Activate Device via Web Browser 3
2.1.2 Activate via SADP 4
2.2 Access Device via Web Browser 5
2.2.1 Plug-in Installation 5
2.2.2 Admin Password Recovery 6
2.2.3 Illegal Login Lock 6
Chapter 3 Face Capture 7
3.1 Set Auto Face Capture Rule 7
3.1.1 Normal Mode Settings 7
3.1.2 Expert Mode Settings 8
3.2 Operate Manual Face Capture 9
3.3 Overlay and Capture 9
3.4 Face Capture Algorithm Parameters 9
Chapter 4 Road Traffic 12
4.1 Set Vehicle Detection Rule 12
4.2 Picture Settings 13
4.3 Display Road Information 14
Chapter 5 PTZ 15
5.1 PTZ Control 15
5.2 Set Preset 17

5.2.1 Special Presets 17
5.3 Set Patrol Scan 18
5.3.1 Set One-Touch Patrol 19
5.4 Set Pattern Scan 19
5.5 Set Limit 20
5.6 Set Initial Position 20
5.7 Set Scheduled Tasks 21
5.8 Set Park Action 21
5.8.1 Set One-Touch Park 21
5.9 Set Privacy Mask 22
5.10 Set Smart Tracking 22
5.11 Set Device Position 23
5.11.1 Set Auto Compass 23
5.11.2 Set Manual Compass 24
5.12 Set Power Off Memory 24
5.13 Set PTZ Priority 24
5.14 Set Rapid Focus 25
Chapter 6 Live View 26
6.1 Live View Parameters 26
6.1.1 Start and Stop Live View 26
6.1.2 Aspect Ratio 26
6.1.3 Live View Stream Type 26
6.1.4 Quick Set Live View 26
6.1.5 Select the Third-Party Plug-in 27
6.1.6 Start Digital Zoom 27
6.1.7 Conduct Regional Focus 27
6.1.8 Conduct Regional Exposure 27
6.1.9 Count Pixel 28

6.1.10 Light 28
6.1.11 Operate Wiper 28
6.1.12 Lens Initialization 28
6.1.13 Track Manually 29
6.1.14 Conduct 3D Positioning 29
6.2 Set Transmission Parameters 29
6.3 Smart Display 30
Chapter 7 Video and Audio 31
7.1 Video Settings 31
7.1.1 Stream Type 31
7.1.2 Video Type 31
7.1.3 Resolution 31
7.1.4 Bitrate Type and Max. Bitrate 32
7.1.5 Video Quality 32
7.1.6 Frame Rate 32
7.1.7 Video Encoding 32
7.1.8 Profile 33
7.1.9 I-Frame Interval 34
7.1.10 SVC 34
7.1.11 Smoothing 34
7.2 Audio Settings 34
7.2.1 Audio Input 34
7.2.2 Environmental Noise Filter 35
7.3 Two-way Audio 35
7.4 ROI 35
7.4.1 Set ROI 35
7.4.2 Set Target Tracking ROI 36
7.4.3 Set Face Tracking ROI 36

7.4.4 Set License Plate Tracking ROI 37
7.5 Display Info. on Stream 37
7.6 Display Settings 37
7.6.1 Scene Mode 38
7.6.2 Image Parameters Switch 41
7.6.3 Mirror 42
7.6.4 Video Standard 42
7.7 OSD 43
Chapter 8 Video Recording and Picture Capture 44
8.1 Storage Settings 44
8.1.1 Set Memory Card 44
8.1.2 Set FTP 45
8.1.3 Set NAS 46
8.2 Video Recording 47
8.2.1 Record Automatically 47
8.2.2 Record Manually 48
8.2.3 Playback and Download Video 48
8.3 Capture Configuration 49
8.3.1 Capture Automatically 49
8.3.2 Capture Manually 50
8.3.3 View and Download Picture 50
Chapter 9 Event and Alarm 51
9.1 Basic Event 51
9.1.1 Set Motion Detection 51
9.1.2 Set Video Tampering Alarm 53
9.1.3 Set Exception Alarm 54
9.1.4 Set Alarm Input 55
9.2 Smart Event 55

9.2.1 Detect Audio Exception 55
9.2.2 Set Intrusion Detection 56
9.2.3 Set Line Crossing Detection 57
9.2.4 Set Region Entrance Detection 58
9.2.5 Set Region Exiting Detection 59
9.2.6 Set Object Removal Detection 60
9.2.7 Set Unattended Baggage Detection 62
Chapter 10 Arming Schedule and Alarm Linkage 63
10.1 Set Arming Schedule 63
10.2 Linkage Method Settings 63
10.2.1 Trigger Alarm Output 63
10.2.2 FTP/NAS/Memory Card Uploading 64
10.2.3 Send Email 65
10.2.4 Notify Surveillance Center 66
10.2.5 Smart Tracking 66
10.2.6 Trigger Recording 66
Chapter 11 Network Settings 67
11.1 TCP/IP 67
11.1.1 Multicast Discovery 68
11.2 Port 68
11.3 Port Mapping 69
11.3.1 Set Auto Port Mapping 69
11.3.2 Set Manual Port Mapping 70
11.3.3 Set Port Mapping on Router 70
11.4 SNMP 71
11.5 Access to Device via Domain Name 72
11.6 Access to Device via PPPoE Dial Up Connection 72
11.7 Accessing via Mobile Client 73

11.7.1 Enable Hik-Connect Service on Camera 73
11.7.2 Set Up Hik-Connect 74
11.7.3 Add Camera to Hik-Connect 74
11.8 Set ISUP 75
11.9 Set ONVIF 76
11.10 Set Network Service 76
11.11 Set HTTP Listening 77
11.12 TCP Acceleration 77
11.13 Traffic Shaping 77
Chapter 12 System and Security 78
12.1 View Device Information 78
12.2 Restore and Default 78
12.3 Search and Manage Log 78
12.4 Import and Export Configuration File 79
12.5 Export Diagnose Information 79
12.6 Reboot 79
12.7 Upgrade 79
12.8 View Open Source Software License 80
12.9 Set Live View Connection 80
12.10 Time and Date 80
12.10.1 Synchronize Time Manually 80
12.10.2 Synchronize Time by Satellite 80
12.10.3 Set NTP Server 81
12.10.4 Set DST 81
12.11 Set RS-485 81
12.12 Security 82
12.12.1 Authentication 82
12.12.2 Set IP Address Filter 83

12.12.3 Set HTTPS 83
12.12.4 Security Audit Log 84
12.12.5 Set QoS 85
12.12.6 Set IEEE 802.1X 86
12.12.7 User and Account 86
Appendix A. Device Command 88
Appendix B. Device Communication Matrix 89

Chapter 1 Overview

1.1 Product Introduction

The F Series Network Speed Dome is an integration of HD camera, PTZ motion control module, and video content analysis algorithms, ideal for remote monitoring.

The device has basic PTZ functions, such as presets, scans, and target tracking, and smart functions, such as Road Traffic, Face Capture and Smart Event.

The device is well suited for HD monitoring in various places, such as rivers, forests, roads, railways, airports, ports, oil fields, posts, squares, parks, scenic areas, streets, stations, stadiums, residential blocks, prisons, libraries, shopping malls, hotels, government buildings, museums, and banks.

1.2 Key Function

The key functions of the device are as follows. Actual functions may vary for different models.

Face Capture

The device captures human faces according to set pupil distance or capture threshold and uploads the pictures to the center.

Road Traffic

The device captures vehicles on road and upload related vehicle information, such as license plates.
License plate recognition of multiple countries and regions are supported.

Event

The device detects basic events and multiple smart events, such as line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

PTZ

The device supports PTZ functions, such as presets, scans, patrol, smart tracking and power-off memory.

1.3 System Requirement

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

	Recommended Specifications
Operating System	Microsoft Windows XP/ Windows 7/ Windows 8/ Windows 10

	Recommended Specifications
	Mac OS 10.13 or later
CPU	Intel® Pentium® IV 3.0 GHz or higher
RAM	1 G or higher
Display	1024 × 768 resolution or higher
Web Browser	Internet Explorer 8.0 to 11.0, 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 need 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.

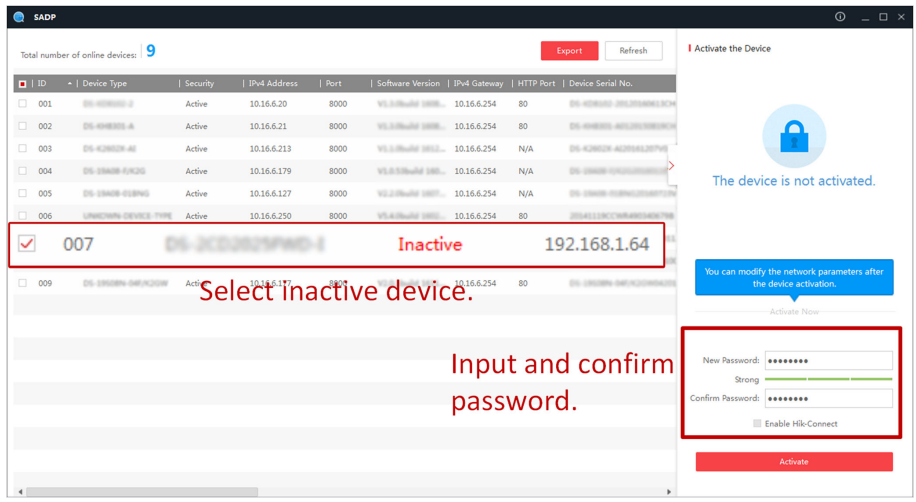
Steps

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 ™ are optional. For non-IE based web browser, webcomponents, ™, 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 8 to 11	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 → Network Service** to enable WebSocket or Websockets for normal view. Display and operation of certain functions

Operating System	Web Browser	Operation
		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**.

With the function enabled, the device is locked if the admin user inputs the wrong password for 7 times continuously when login, and other users inputs the wrong password for 5 times continuously when login.

Chapter 3 Face Capture

Face capture function detects and captures faces in surveillance scenes. When the grading of the detected face exceeds an algorithm-defined value, the PTZ camera channel captures the face and triggers linkage actions. Set up rule and parameters before using the function.

Note

- For certain device models, you need to select **Face Capture** on **VCA Resource** page first.
- This function is only supported by certain device models.

3.1 Set Auto Face Capture Rule

After set the face capture rules and algorithm parameters, the device captures faces and trigger linkage actions automatically.

Steps

1. Go to **Configuration → Face Capture → Rule** .
2. Check **Enable**.
3. Select a configuration mode.

Normal	One detection scene is allowed to set. The device captures face in the scene in set arming schedule. See ***Normal Mode Settings*** for details.
Expert	The device can patrol among the detection scenes and capture face images. Detection scenes and patrol schedule should be set in advance. See ***Expert Mode Settings*** for details.

4. Click **Save**.

What to do next

Go to **Picture** to search and view the captured pictures.
Go to **Smart Display** to see currently captured face pictures.

3.1.1 Normal Mode Settings

Steps

1. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
2. Use PTZ control panel or click to locate a scene with a face.
3. Click , and draw a detection area on live image.

4. Input **Mounting Height** of the device.
5. Input the min. pupil distance in the text field, or click draw min. pupil distance.

   Min. Pupil Distance

   The min. pupil distance refers to the minimum area between two pupils, and it is basic for the device to recognize a face.
6. Click **Save**.
7. Set arming schedule. See ***Set Arming Schedule*** .
8. Set linkage method. See ***Linkage Method Settings*** .

3.1.2 Expert Mode Settings

Steps

1. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
2. Set detection scenes and detection areas.
   1) Select a detection scene.
   2) Adjust the live image to a desired scene. You can use PTZ control buttons or click to locate a scene with a face.
   3) Click , and draw a detection area on live image.
   4) Click **Save**.
   5) Repeat above steps to set other detection scenes and areas.
3. Input **Mounting Height** of the device.
4. Input the min. pupil distance in the text field, or click draw min. pupil distance.

   Min. Pupil Distance

   The min. pupil distance refers to the minimum area between two pupils, and it is basic for the device to recognize a face.
5. Set patrol schedule.
   1) Click **Patrol Schedule**.
   2) Draw time bars as desired.
   3) Click a time bar and click **Configuration**.
   4) Edit patrol path and input dwell time for each detection scene.

+	Add a detection scene to the patrol path.
↓ ↑	Adjust the order of the scenes.
×	Delete the detection scene.

6. Set linkage method. See ***Linkage Method Settings*** .
7. Click **Save**.

3.2 Operate Manual Face Capture

Capture the target face manually in live view image.

Steps

1. Click **Live View**.
2. Click to start manual face capture.
3. Draw a frame to select the target face in live view image.

   The captured picture can be uploaded to the center.
4. Click the icon again to stop manual face capture.

3.3 Overlay and Capture

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

Display on Stream

Display smart information on stream, including the target and rules information.

Display on 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**.

Camera Information

Enter **Device No.** and **Camera Info** in order to manage the monitoring device.

Text Overlay

You can check desired items and adjust their order to display on captured pictures by clicking .

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.

Detection Parameters

Generation Speed

The speed to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the faster the target will be recognized. The default value is recommended.

Sensitivity

The sensitivity to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the easier a face will be detected, and the higher possibility of misinformation would be. The default value of 3 is recommended.

Capture Parameters

Upload Feature

Feature stands for the feature information the algorithm can tell from face pictures. For example, gender, facial expression, wearing glasses or not, etc. Check the function to upload the information.

Best Shot

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

Capture Times

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

Capture Threshold

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

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 a face will be captured during its stay in the configured area.

Unlimited

The device keeps capturing the target face, which exceeds the **Quick Shot Threshold** during the **Max. Capture Interval**.

Limited

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.

Restore Default

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

Chapter 4 Road Traffic

The device captures the passing vehicles and uploads the vehicle information together with the captured picture.

Note

- For certain device models, you need to select **Road Traffic** on **VCA Resource** page first.
- This function is only supported by certain device models.

4.1 Set Vehicle Detection Rule

In Vehicle Detection, the device detects and capture the passed vehicles and the license plates. The vehicle color, type and other information can be recognized automatically.

Steps

1. Go to **Configuration → Road Traffic → Detection Configuration** .
2. Select **Vehicle Detection**, and enable the function.
3. Click **Area Settings** to set the detection rule.
4. Select a detection scene from the drop-down list and change the **Scene Name** as required.

   The device supports multiple detection scenes with independent detection parameters.
5. Draw lane area in the scene.
   1) Click **Lock** to avoid accidental PTZ changing during configuration.
   2) Adjust the pan, tilt, and zoom position to obtain the target scene.
   3) Select the **Total Number of the Lanes** according to the actual lane number you want to monitor in your scene.

      Yellow lane lines, a blue detection line and a red frame are displayed on live image.
   4) Adjust the zoom ratio of the device so that the size of the vehicle in the image is close to that of the red frame. The position of red frame is adjustable.
   5) Click and drag the lane lines or the endpoints to set the positions according to the actual lane lines on the road.
   6) **Optional:** Click and drag the blue detection line to adjust the position. The vehicle detection triggers when target vehicles hit the line.
   7) Set the vehicle moving direction for every lane in the scene.
   8) Click **Save**.
6. **Optional:** Repeat to set other detection scenes if needed.
7. Select the **Country/Region**.
8. Click **Save** to finish area settings.
9. Set the arming schedule of vehicle detection.
   1) Click **Arming Schedule**, and check **Enable**.
   2) Select a detection scene and draw the time bar in the time table. Different scenes are marked with different colors on schedule.

3) **Optional:** Move the mouse to the end of each day, a copy icon pops up, and you can click to copy the current settings to other days.
4) Click **Save** after finishing schedule settings.

10. Set linkage method. See ***Linkage Method Settings*** .

4.2 Picture Settings

Captured vehicle pictures are uploaded. Picture size, quality and overlay information are configurable.

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

Picture Quality Vs Picture Size

Both **Picture Quality** and **Picture Size** influence the size and quality of pictures for uploading. They cannot be set at the same time.

Picture Quality

The quality of the uploaded picture is accordance with the set value. To keep the quality, the size of the pictures may vary according to the image complexity. Higher value means clearer image.

Picture Size

The size of the uploaded picture is accordance with the set value. To keep the size, picture with more complex contents might be less satisfactory in quality than that with simpler contents.

Overlay

With **Overlay** enabled, every uploaded picture has an additional part to display the overlaid information.

Font Color

The font color of overlaid texts.

Background

The background color for the overlaid texts.

Text Overlay

Check the desired item to display on the picture. Display sequence is adjustable.

Note

- Vehicle Color, Brand, and Type are not supported in this firmware version.
- Device No., Camera No., and Camera info. are set on **Configuration → Road Traffic → Camera** .

4.3 Display Road Information

Display a road sign with configurable texts to indicate the location on live image.

Steps

1. Go to **Configuration → Image → Road Information** .
2. Check **Display Road Information** to enable the function.
3. Select a intersection number and adjust the scene to the desired intersection by controlling PTZ.
4. Check and input desired information in the test fields.
5. Click **Save**.
6. **Optional:** Repeat to set other intersections. Up to 4 intersections are supported.

Result

When the device turns to the saved intersection, the road sign displays on the live image.

Chapter 5 PTZ

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

5.1 PTZ Control

In live view interface, you can use the PTZ control buttons to control the device panning, tilting, and zooming.

PTZ Control Panel

	Click and hold the directional button to pan/tilt the device. **Note** • You can set **Keyboard Control Speed** in **Configuration → PTZ → Basic Settings** . The speed of pan/tilt movement in live view is based on this speed level. • You can set **Max. Tilt-angle** in **Configuration → PTZ → Basic Settings** to limit tilt movement range.
↺	Click the button, then the device keeps panning. **Note** You can set **Auto Scan Speed** in **Configuration → PTZ → Basic Settings** . The higher the value you set, the faster the device pans.
	Drag the slider to adjust the speed of pan/tilt movement.

Note

You can set **Manual Control Speed** in **Configuration → PTZ → Basic Settings** .

Compatible	The control speed is same as **Keyboard Control Speed**.
Pedestrian	Choose **Pedestrian** when you monitor the pedestrians.

Non-motor Vehicle	Choose **Non-motor Vehicle** when you monitor the non-motor vehicles.
Motor Vehicle	Choose **Motor Vehicle** when you monitor the motor vehicles.
Auto	You are recommended to set it as **Auto** when the application scene of the speed dome is complicated.

To avoid blurred image resulted from fast zoom, you can check **Enable Proportional Pan** in **Configuration → PTZ → Basic Settings** . If you enable this function, the pan/tilt speed change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.

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

5.2 Set Preset

A preset is a predefined image position. For the 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 PTZ 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** . Click **Clear All Presets**, and click **Save**.

What to do next

Go to **Configuration → PTZ → Basic Settings** to set preset freezing and preset speed.
After enabling preset freezing, the live image switches directly from one preset to another, without showing the areas between these two scenes. It also guarantees the masked area will not be seen when the device is moving.

5.2.1 Special Presets

You can call the following presets with special demands to enable corresponding functions.

Preset No.	Function	Preset No.	Function
33	Auto flip	92	Set manual limits
34	Back to origin	93	Save manual limits
35	Call patrol 1	94	Remote reboot
36	Call patrol 2	95	Call OSD menu
37	Call patrol 3	96	Stop a scan
38	Call patrol 4	97	Start random scan

Preset No.	Function	Preset No.	Function
39	Day mode	98	Start frame scan
40	Night mode	99	Start auto scan
41	Call pattern 1	100	Start tilt scan
42	Call pattern 2	101	Start panorama scan
43	Call pattern 3	102	Call patrol 5
44	Call pattern 4	103	Call patrol 6
45	One-touch patrol	104	Call patrol 7
46	Day/Night Mode	105	Call patrol 8

5.3 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**.

5.3.1 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.

5.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

1. Click to show the PTZ control panel, and click .
2. Select one pattern scan path that needs to be set.
3. Click to start recording pattern scan.
4. Click PTZ control buttons as demands.

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**.

5.5 Set Limit

The device can only move within the limited range.

Steps

1. Go to **Configuration → PTZ → Limit** .
2. Select **Limit Type**.

   Manual Stops

   It refers to the movement range limit when you control the device manually.

   Scan Stops

   It refers to the movement range limit when the device scans automatically.

   Note

   Scan limit is only supported by the device that has scan function.

3. Click **Set** and set limits according to the prompt on the live image.
4. **Optional:** Click **Clear** to clear the limit settings of the selected mode.
5. Click **Save**.
6. Check **Enable Limit**.

   Note

   If you need to cancal all the set patrol paths, go to **Configuration → PTZ → Clear Config** , select **Clear All PTZ Limited**, and click **Save**.

Result

The device can only move within the set region after saving the settings.

5.6 Set Initial Position

Initial position refers to the relative initial position of the device azimuth. You can set the initial position if you need to select one point in the scene as the base point.

Steps

1. Go to **Configuration → PTZ → Initial Position** .
2. Move the device to the needed position by manually controlling the PTZ control buttons.
3. Click **Set** to save the information of initial position.

Call The device moves to the set initial position.

Clear Clear the set initial position.

5.7 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**.

5.8 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. For setting patrols, refer to ***Set Patrol Scan*** .

Steps

1. Go to **Configuration → PTZ → Park Action** and check **Enable Park Action**.
2. Set **Park Time**, the inactive time before the device starts the park action.
3. Select **Action Type** according to your needs.
4. Click **Save**.

5.8.1 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.

5.9 Set Privacy Mask

Privacy mask enables you to cover certain areas on the live image to prevent certain spots in the surveillance area from being live viewed and recorded.

Steps

1. Go to **Configuration → PTZ → Privacy Mask** .
2. Check **Enable Privacy Masks**.
3. Adjust the live image to the target scene via PTZ control buttons.
4. 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.

5. Click **Add**.

   It is listed in **Privacy Mask List**.
6. 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.
7. Repeat the steps above to set other privacy masks.
8. Click**Save**.

5.10 Set Smart Tracking

The function allows the device detecting and tracking the moving targets in the scene. The target stays in the center of the live image with a predefined size during the tracking process.

Steps

1. Go to **Configuration → PTZ → Smart Tracking** .
2. Check **Enable Smart Tracking**
3. Set the **Duration**. The device stops tracking when the duration time is up.
4. Select a target in the live image and adjust the PTZ buttons to see the target at desired size.
5. Click **Set Zoom Ratio**. The device tracks the target at a fixed zoom ratio.
6. Click **Save**.

5.11 Set Device Position

Before You Start
Go to **Configuration → PTZ → Basic Settings → PTZ OSD** to enable **PT Status** display.

Steps
1. Go to the setting page: **Configuration → PTZ → Position Settings** .
2. Select a **PT Mode**.

   Manual Use a direction indicating device to determine the North at the device location, and set the North for the device. For details, see ***Set Manual Compass*** .

   Auto For the device that has built-in e-compass, the compass can automatically tell the north direction for the device. For details, see ***Set Auto Compass*** .
3. Set Vandal-proof alarm.

   After enabling the function, the device triggers alarms once its position changes because of shock or vandalism.

   Sensitivity

   The higher the value is, the easier the alarm will be triggered.

   Upload Vandal-proof Alarm

   The device uploads the alarm information when the alarm is triggered.

   Vandal-proof Alarm Voice Warning

   The camera triggers the alarm with audible warning.
4. Select a **Longitude-Latitude Mode** to set the geographic location of the device.

   Auto For device with a built-in positioning module, select **Auto** to automatically obtain the longitude and latitude of the device location.

   Manual Get the device location information in advance, and input the longitude and latitude manually.
5. Click **Save**.

What to do next
If you lost direction when operating the device, you can click **Point to North** to call the north position that is saved in the device.

5.11.1 Set Auto Compass

For the device that has built-in e-compass, the compass can automatically tell the north direction for the device.

Before You Start
Electromagnetic interference may affact the accuracy of the e-compass. Use manual compass if electromagnetic interference occurs in the device installation environment.

Steps
1. Select the **PT Mode** as **Auto**.
2. Click **Calibrate** to synchronize the north of the device with that of the e-compass.

5.11.2 Set Manual Compass

Use a direction indicating device to determine the North at the device location, and set the North for the device.

Before You Start
Use a direction indicating device to determine the north at the device location.

Steps
1. Select the **PT Mode** as **Manual**.
2. Adjust the tilt position of the device to 0 by controling the up arrow and down arrow on the PTZ panel.
3. Adjust the pan position to show the live view of the north direction by controling the left arrow and right arrow on the PTZ panel.
4. Click **Set as North**.

5.12 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**.

5.13 Set PTZ Priority

The function can set the PTZ priority of different signals.

Steps
1. Go to **Configuration → PTZ → Prioritize PTZ** .
2. Set the priority signal and delayed time.

   Network

   The network signal controls the device with priority.

   RS-485

   The RS-485 signal controls the device with priority.

Delay

It refers to the time interval of PTZ operation controlled by different signals. When the operation with high priority is finished, the low priority signal controls the device after the setting interval.

3. Click **Save**.

5.14 Set Rapid Focus

Rapid focus is a function to reduce time of focusing comparing with that of normal focusing. To use the function, calibration should be done first. Rapid focus may not be supported by certain device models.

Steps

1. Go to **Configuration → PTZ → Rapid Focus** .
2. Add scenes for calibration.
   1) Adjust the live image to a desired scene via PTZ control buttons, and click **Add**.
   2) Set the **Rate** and the **Calibration Point Amount** of the added scene.

   Note

   More calibration points may increase calibration accuracy, but more focusing time is required. The default amount is recommended.

3. Select the scene to display the calibration line.

   A red line displays on live image.

4. Adjust the length and position of the line by dragging its two endpoints.

   Note

   The red line is recommended to stay in the center of the scene and to cover ground at the same time.
   Double click the image to enter full screen mode.

5. Click **Start Calibration**.

   Calibration status displays on the live image.

6. Repeat to add other scenes and complete the calibration.
7. Check **Enable Height Compensation** if the mounting height of the device is lower than 3 meters.
8. Check **Enable** after successful calibration.
9. Click **Save**.

Chapter 6 Live View

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

6.1 Live View Parameters

6.1.1 Start and Stop Live View

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

6.1.2 Aspect Ratio

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

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

6.1.3 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*** .

6.1.4 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*** .

6.1.5 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.

6.1.6 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.

6.1.7 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.

6.1.8 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.

6.1.9 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.

6.1.10 Light

Click to turn on or turn off the illuminator.

6.1.11 Operate Wiper

For the device that has a wiper, you can control the wiper via web browser.

Steps

1. Go to wiper setting page: **Configuration → PTZ → Wiper** .
2. Select a wiper mode.

One Time	The wiper wipes one time when you click on live view page.
Cycle	The wiper works on schedule at set wiping interval. Click on live view to start wiping. **Duration** The schedule in which the wiper is ready to work. **Interval** The interval between two secessive wiping actions.
Auto	**Note** Auto mode is only available for device that supports rain-sensing auto wiper. In auto mode, the wiper works when rain drops on the window.

6.1.12 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.

6.1.13 Track Manually

In live view, manually select a target for the device to track.

Steps

1. Click on the toolbar of the live view page.
2. Click a moving object in the live image.

   The camera tracks the target and keep it in the center of live view image.

6.1.14 Conduct 3D Positioning

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

Steps

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

6.2 Set Transmission Parameters

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

Steps

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

   Protocol

   TCP

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

   UDP

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

MULTICAST

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

Note

For detailed information about multicast, refer to .

HTTP

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

Play Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

3. Click **OK**.

6.3 Smart Display

This function displays real time images captured by certain smart functions.

Note

To use this function, you should first enable and configure certain smart functions.

- You can view the live image in one or two windows. Click or to switch.
- You can choose a live view. Click to choose a live view camera channel to display.
- You can change the layout of the display page. Click and check the display content you need to add it to the layout.

Chapter 7 Video and Audio

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

7.1 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** .

7.1.1 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.

7.1.2 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.

7.1.3 Resolution

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

7.1.4 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.

7.1.5 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.

7.1.6 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.

7.1.7 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.

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.

7.1.8 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.

7.1.9 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.

7.1.10 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.

7.1.11 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.

7.2 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** .

7.2.1 Audio Input

If built-in microphone or external audio pick-up device is available, audio encoding, audio input mode and input volume are configurable.

Audio Encoding

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

Audio Input

LineIn and MicIn are available. Select MicIn for the built-in microphone, and LineIn for external audio pick-up device.

Input volume

Adjust the volume of the audio input.

7.2.2 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.

7.3 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 and select , move the slider to adjust the volume.
4. Click , disable the two-way audio function.

7.4 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.

7.4.1 Set ROI

ROI (Region of Interest) encoding helps to assigns 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 **Drawing**.
   2) Click and drag the mouse on the view screen to draw the fixed region.
   3) Click **Stop Drawing**.

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

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

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

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

7.4.2 Set Target Tracking ROI

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

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

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

7.4.3 Set Face Tracking ROI

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

Steps

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

Note

ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

4. Click **Save**.

7.4.4 Set License Plate Tracking ROI

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

Steps

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

Note

ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

4. Click **Save**.

7.5 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**.

7.6 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

7.6.1 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.

Set Supplement Light

Steps

1. Go to **Configuration → Maintenance → System Service** .
2. Check **Enable Supplement Light**.

3. Click **Save**.
4. Go to **Configuration → Image → Display Settings → Day/Night Switch** to set supplement light parameters.

   Smart Supplement Light

   This feature uses smart image processing technology to reduce overexposure caused by supplement light.

   IR Light Mode

   When the mode is set to **Auto**, the supplement light is automatically enabled or disabled according to the image brightness.

   Brightness Limit

   Adjust the upper limit of IR light power.

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.

OIS

OIS (Optical Image Stabilization) reduces the effects of vibration in a video in order to increase the stability of the video.

Normal

The camera enable OIS automatically, which can modify most unstable situations.

Expert

You can customize the level and sensitivity of OIS as needed.

7.6.2 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**.

Set Link to Preset

You can set a preset to switch the image to a linked scene.

Steps

1. Check **Link to Preset**.
2. Select a preset.
3. Check and set a time period and a linked scene mode.
4. Click **Save**.

7.6.3 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.

7.6.4 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.

7.7 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.

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 8 Video Recording and Picture Capture

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

8.1 Storage Settings

This part introduces the configuration of several common storage paths.

8.1.1 Set Memory Card

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

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

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

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

Detect Memory Card Status

It helps to detect the memory card status of Hikvision memory card. You receive notifications when your memory card is detected abnormal.

Before You Start
Memory card should be installed to the device.

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

   Remaining Lifespan

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 authority 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 camera that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of users.
     - If you use the memory card (with a lock) on a different camera, you can go to **HDD Management** interface to unlock the memory card manually. Select the memory card, and click the **Unlock** button shown next to the **Format** button. Then 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 write when it is unlocked.
- If the camera, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** interface to unlock the memory card.

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

8.1.2 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**.

8.1.3 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**.

8.2 Video Recording

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

8.2.1 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**.

8.2.2 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.

8.2.3 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.

8.3 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.

8.3.1 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**.

8.3.2 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.

8.3.3 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 9 Event and Alarm

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

9.1 Basic Event

9.1.1 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:** Check **Enable Motion Detection in PTZ Control**, and the device detects moving targets in PTZ movement.
4. **Optional:** Highlight moving objects in green.
   1) Check **Enable Dynamic Analysis for Motion**.
   2) Go to **Configuration → Local** to enable **Rules**.
5. 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*** .
6. Set the arming schedule. See ***Set Arming Schedule*** for details.
7. Set linkage methods. See ***Linkage Method Settings*** for details.
8. 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.

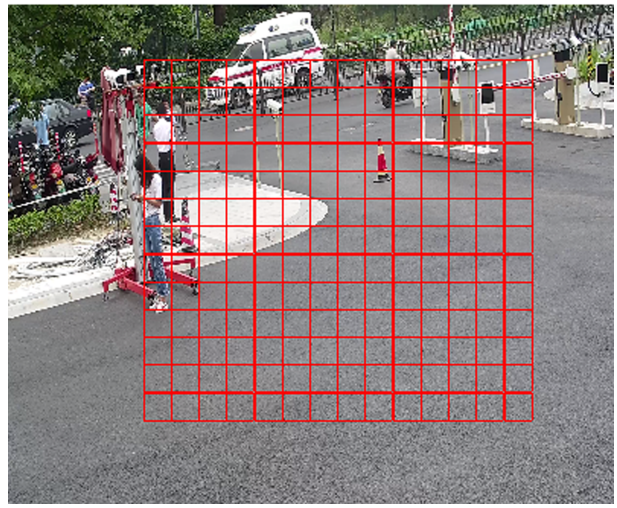


Figure 9-1 Set Rules

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.

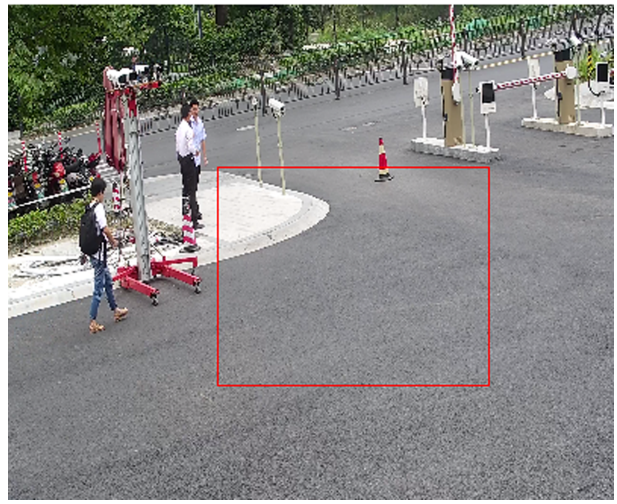


Figure 9-2 Set Rules

Stop Drawing	Finish drawing one area.
Clear All	Delete all the areas.

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

9.1.2 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.

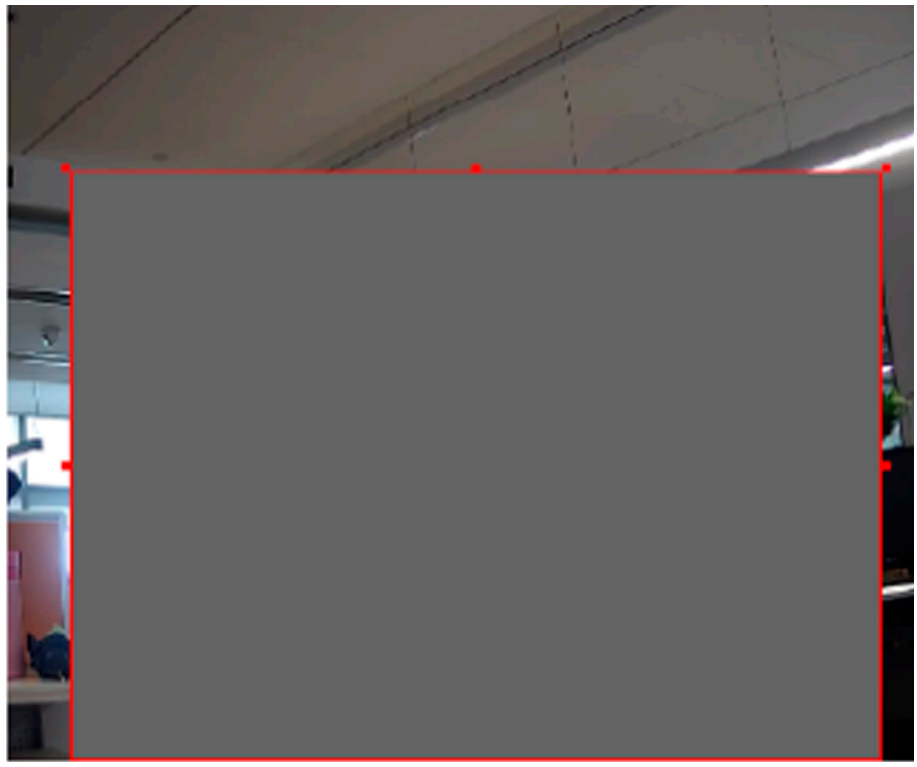


Figure 9-3 Set Video Tampering Area

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

9.1.3 Set Exception Alarm

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

Steps

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

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

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

9.1.4 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 cables connection.

Steps
1. Go to **Configuration → Event → Basic Event → Alarm Input** .
2. Check **Enable Alarm Input Handing**.
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**.

9.2 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.

9.2.1 Detect Audio Exception

Audio exception detection function detects the abnormal sound in the surveillance 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.

9.2.2 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.

Steps

1. Go to **Configuration → Event → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. 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.
6. 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 she/he stays 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.

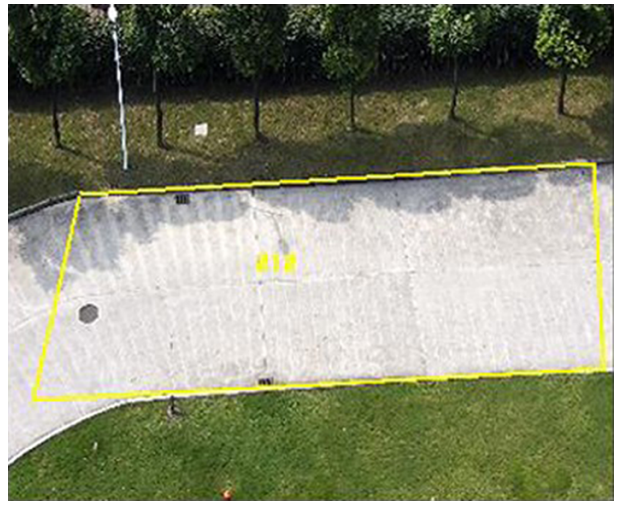


Figure 9-4 Draw Area

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

9.2.3 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.

Steps

1. Go to **Configuration → Event → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw 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 object going across the line from both directions can be detected and alarms are triggered.

A->B

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

B->A

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

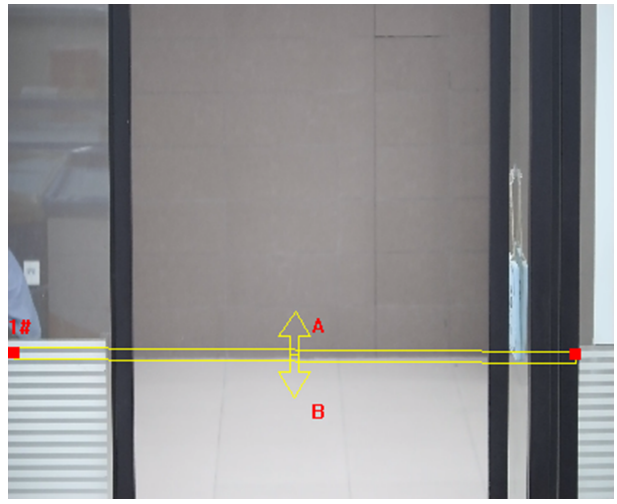


Figure 9-5 Draw Line

6. 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.

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

9.2.4 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.

Steps

1. Go to **Configuration → Event → Smart Event → Region Entrance Detection** .
2. Check **Enable**.

3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. 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.
6. 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 9-6 Draw Area

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

9.2.5 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.

Steps

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

2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. 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.
6. 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 9-7 Draw Area

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

9.2.6 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.

Steps

1. Go to **Configuration → Event → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. 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.
6. 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.

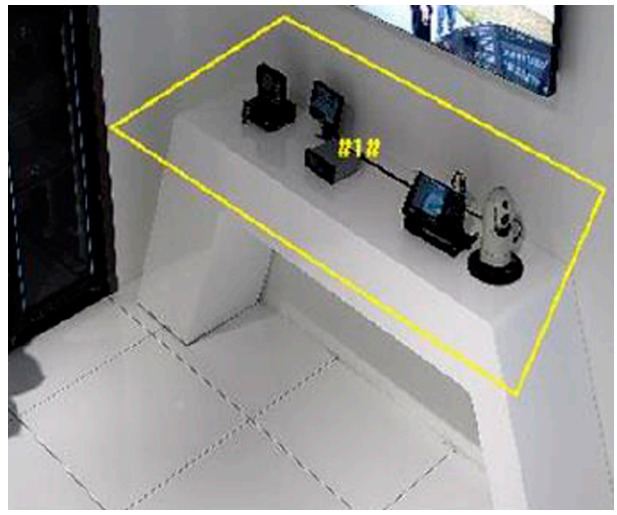


Figure 9-8 Draw Area

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

9.2.7 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.

Steps

1. Go to **Configuration → Event → Smart Event → Unattended Baggage Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

   Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. 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.
6. 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.

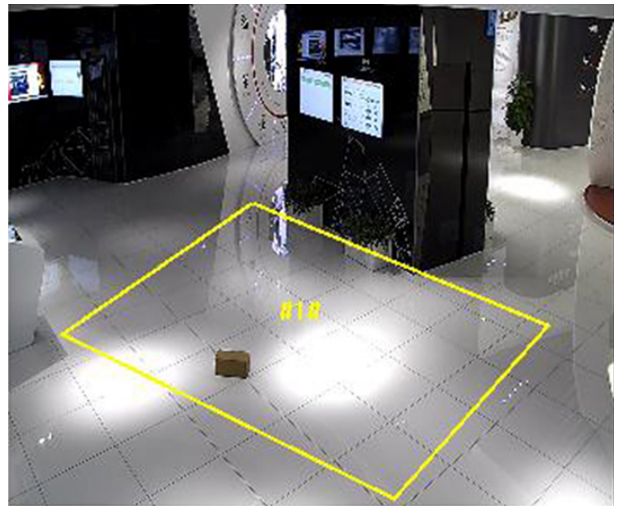


Figure 9-9 Draw Area

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

Chapter 10 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.

10.1 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**.

10.2 Linkage Method Settings

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

10.2.1 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

   Custom a name for the alarm output.

   Delay

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

10.2.2 FTP/NAS/Memory Card Uploading

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

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

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

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

10.2.3 Send Email

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

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

Set Email

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

Before You Start

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

Steps

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

      Note

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

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

10.2.4 Notify Surveillance Center

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

10.2.5 Smart Tracking

Check **Smart Tracking**, and the device tracks the target when an alarm event is detected.

10.2.6 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 11 Network Settings

11.1 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 → Basic Configuration → Network → TCP/IP** for parameter settings.

NIC Type

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

IPv4

Two IPv4 modes are available.

DHCP

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

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with 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.

11.1.1 Multicast Discovery

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

11.2 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.

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.

11.3 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**.

11.3.1 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.

11.3.2 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.

11.3.3 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.

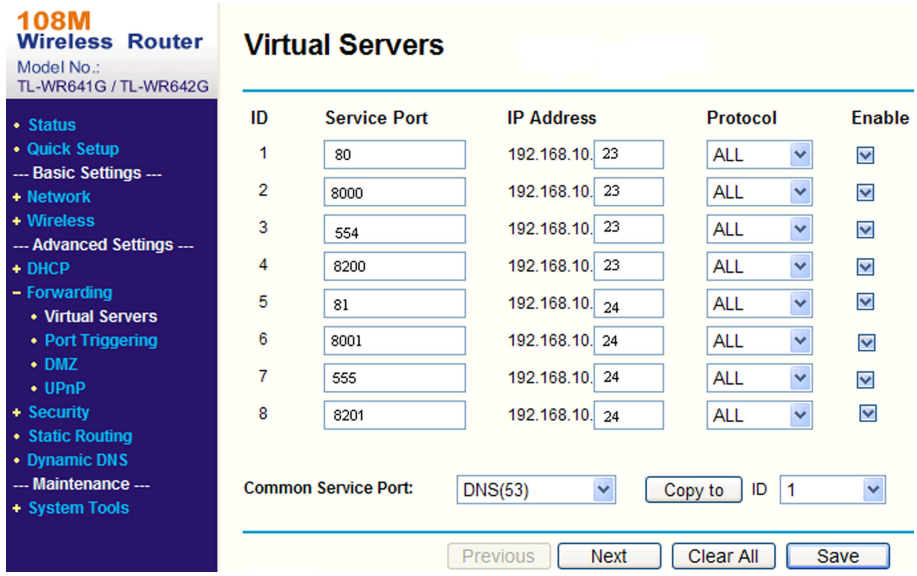


Figure 11-1 Port Mapping on Router

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.

11.4 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**.

11.5 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.

11.6 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.

11.7 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.

11.7.1 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.

11.7.2 Set Up Hik-Connect

Steps

1. Download and install the Hik-Connect app by searching "Hik-Connect" in App Store or ™.
2. Launch the app and register for a Hik-Connect user account.
3. Log in after registration.

11.7.3 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 three meters from the router when setting up the Wi-Fi.)
Wired Connection	Connect the camera to the router with a network cable and tap **Connected** in the 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.

11.8 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.

11.9 Set ONVIF

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

Steps

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

   Delete Delete the selected ONVIF user.

   Modify Modify the selected ONVIF user.
4. Click **Save**.
5. **Optional:** Repeat the steps above to add more ONVIF users.

11.10 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, and digital zoom function cannot be used.

   If the device uses HTTP, enable WebSocket.

   If the device uses HTTPS, enable WebSockets.

   SDK Service & Enhanced SDK Service

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

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

   Note

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

3. Click **Save**.

11.11 Set HTTP Listening

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

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTP Listening** .
2. Input **Destination IP** or **Host Name**, **URL**, and **Port**.
3. Select **Protocol**.

Note

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

4. Click **Test**.
5. Click **Save**.

11.12 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.

11.13 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.

Chapter 12 System and Security

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

12.1 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.

12.2 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.

12.3 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.

12.4 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**.

12.5 Export Diagnose Information

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

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

12.6 Reboot

You can reboot the device via browser.

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

12.7 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**.

12.8 View Open Source Software License

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

12.9 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.

12.10 Time and Date

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

12.10.1 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**.

12.10.2 Synchronize Time by Satellite

Note

This function varies depending on different devices.

Steps

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

4. Click **Save**.

12.10.3 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**.

12.10.4 Set DST

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

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

12.11 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**.

12.12 Security

You can improve system security by setting security parameters.

12.12.1 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.

12.12.2 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 to the list.

   Modify Modify the selected IP address in the list.

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

12.12.3 Set HTTPS

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

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable** .
3. Click **Delete** to recreate and install certificate.

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

   Create certificate request and install certificate Refer to ***Install Authorized Certificate***
4. Click **Save**.

Create and Install Self-signed Certificate

Steps

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

Result

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

Install Authorized Certificate

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

Steps

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

12.12.4 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.

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

Note

Install certificates according to the requirement of the log server. If two-way authentication is required, install the CA certificate and the client certificate. If one-way authentication is required, install the CA certificate.

1. **Optional:** Install client certificate.
   1) Click **Create** to create the certificate request. Fill in the required information in the pop-up window.
   2) Click **Download** to download the certificate request and submit it to the trusted authority for signature.
   3) Install the authorized certificate to the device.
6. Install the CA certificate to the device.

   Note

   Prepare a CA certificate in advance.

   1) Click **Browse**, and select the CA certificate file.
   2) Click **Install**.

12.12.5 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**.

12.12.6 Set IEEE 802.1X

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

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

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

Protocol

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

EAP-LEAP and EAP-MD5

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

EAP-TLS

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

EAPOL Version

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

12.12.7 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.

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

UD18066B