

# **Network Speed Dome**

**User Manual** 

# **Initiatives on the Use of Video Products**

## Thank you for choosing Hikvision products.

Technology affects every aspect of our life. As a high-tech company, we are increasingly aware of the role technology plays in improving business efficiency and quality of life, but at the same time, the potential harm of its improper usage. For example, video products are capable of recording real, complete and clear images. This provides a high value in retrospect and preserving real-time facts. However, it may also result in the infringement of a third party's legitimate rights and interests if improper distribution, use and/or processing of video data takes place. With the philosophy of "Technology for the Good", Hikvision requests that every end user of video technology and video products shall comply with all the applicable laws and regulations, as well as ethical customs, aiming to jointly create a better community.

## Please read the following initiatives carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not be in conflict with this reasonable expectation. Therefore, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range, when installing video products in public areas. For non-public areas, a third party's rights and interests shall be evaluated when installing video products, including but not limited to, installing video products only after obtaining the consent of the stakeholders, and not installing highly-invisible video products.
- The purpose of video products is to record real activities within a specific time and space and under specific conditions. Therefore, every user shall first reasonably define his/her own rights in such specific scope, in order to avoid infringing on a third party's portraits, privacy or other legitimate rights.
- During the use of video products, video image data derived from real scenes will continue to be
  generated, including a large amount of biological data (such as facial images), and the data could
  be further applied or reprocessed. Video products themselves could not distinguish good from
  bad regarding how to use the data based solely on the images captured by the video products.
  The result of data usage depends on the method and purpose of use of the data controllers.
  Therefore, data controllers shall not only comply with all the applicable laws and regulations and
  other normative requirements, but also respect international norms, social morality, good
  morals, common practices and other non-mandatory requirements, and respect individual
  privacy, portrait and other rights and interests.
- The rights, values and other demands of various stakeholders should always be considered when processing video data that is continuously generated by video products. In this regard, product security and data security are extremely crucial. Therefore, every end user and data controller, shall undertake all reasonable and necessary measures to ensure data security and avoid data leakage, improper disclosure and improper use, including but not limited to, setting up access

control, selecting a suitable network environment (the Internet or Intranet) where video products are connected, establishing and constantly optimizing network security.

 Video products have made great contributions to the improvement of social security around the world, and we believe that these products will also play an active role in more aspects of social life. Any abuse of video products in violation of human rights or leading to criminal activities are contrary to the original intent of technological innovation and product development. Therefore, each user shall establish an evaluation and tracking mechanism of their product application to ensure that every product is used in a proper and reasonable manner and with good faith.

# Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

## About this Manual

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

### www.hikvision.com/).

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

## Trademarks

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

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

## Disclaimer

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

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

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

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

# Contents

Chapter 1 Overview	1
1.1 Product Introduction	1
1.2 Key Function	1
1.3 System Requirement	1
Chapter 2 Device Activation and Accessing	2
2.1 Activate Device	2
2.1.1 Activate Device via Web Browser	2
2.1.2 Activate via SADP	3
2.2 Access Device via Web Browser	4
2.2.1 Plug-in Installation	4
2.2.2 Admin Password Recovery	5
2.2.3 Illegal Login Lock	5
Chapter 3 PTZ	7
3.1 PTZ Control	7
3.2 Set Preset	9
3.2.1 Special Presets	9
3.3 Set Patrol Scan 1	0
3.3.1 Set One-Touch Patrol 1	1
3.4 Set Pattern Scan 1	1
3.5 Set Limit 1	2
3.6 Set Initial Position 1	3
3.7 Set Scheduled Tasks 1	3
3.8 Set Park Action 1	4
3.8.1 Set One-Touch Park 1	4
3.9 Set Privacy Mask 1	4
3.10 Set Smart Tracking 1	5

3.11 Set Power Off Memory 16
3.12 Set PTZ Priority 16
3.13 Set Rapid Focus 17
Chapter 4 Live View 18
4.1 Live View Parameters 18
4.1.1 Start and Stop Live View 18
4.1.2 Aspect Ratio 18
4.1.3 Live View Stream Type 18
4.1.4 Quick Set Live View 18
4.1.5 Select the Third-Party Plug-in 19
4.1.6 Count Pixel 19
4.1.7 Start Digital Zoom 19
4.1.8 Conduct Regional Focus 19
4.1.9 Conduct Regional Exposure 20
4.1.10 Light 20
4.1.11 Lens Initialization 20
4.1.12 Track Manually 20
4.1.13 Conduct 3D Positioning 20
4.1.14 Undervoltage Alarm 21
4.1.15 Display Target Information on Live View 21
4.2 Set Transmission Parameters 21
4.3 OSD Menu 22
Chapter 5 Video and Audio 23
5.1 Video Settings 23
5.1.1 Stream Type 23
5.1.2 Video Type 23
5.1.3 Resolution 23
5.1.4 Bitrate Type and Max. Bitrate 24

5.1.5 Video Quality 24
5.1.6 Frame Rate 24
5.1.7 Video Encoding 24
5.1.8 I-Frame Interval 26
5.2 Audio Settings 26
5.2.1 Audio Input
5.2.2 Environmental Noise Filter 27
5.3 Two-way Audio 27
5.4 ROI
5.4.1 Set ROI 28
5.5 Display Info. on Stream 28
5.6 Display Settings 28
5.6.1 Scene Mode 29
5.6.2 Image Parameters Switch 33
5.6.3 Mirror
5.6.4 Video Standard 34
5.6.5 Zoom Limit
5.7 OSD
5.8 Demist
Chapter 6 Video Recording and Picture Capture
6.1 Storage Settings 36
6.1.1 Memory Card 36
6.1.2 Set FTP 38
6.1.3 Set NAS
6.1.4 Set Cloud Storage 40
6.2 Video Recording 40
6.2.1 Record Automatically 40
6.2.2 Record Manually 42

6.2.3 Playback and Download Video 42
6.3 Capture Configuration 43
6.3.1 Capture Automatically 43
6.3.2 Capture Manually 43
6.3.3 View and Download Picture 43
Chapter 7 Event and Alarm 45
7.1 Basic Event 45
7.1.1 Set Motion Detection 45
7.1.2 Set Video Tampering Alarm 47
7.1.3 Set Exception Alarm 48
7.1.4 Set Alarm Input 49
7.2 Smart Event 49
7.2.1 Detect Audio Exception 49
7.2.2 Set Face Detection 50
7.2.3 Set Intrusion Detection 51
7.2.4 Set Line Crossing Detection 52
7.2.5 Set Region Entrance Detection 54
7.2.6 Set Region Exiting Detection 55
7.2.7 Set Object Removal Detection 56
7.2.8 Set Unattended Baggage Detection 58
Chapter 8 Arming Schedule and Alarm Linkage 60
8.1 Set Arming Schedule 60
8.2 Linkage Method Settings 60
8.2.1 Trigger Alarm Output 60
8.2.2 FTP/NAS/Memory Card Uploading 62
8.2.3 Send Email 62
8.2.4 Notify Surveillance Center 63
8.2.5 Smart Tracking 63

8.2.6 Trigger Recording 63
Chapter 9 Network Settings
9.1 TCP/IP
9.1.1 Multicast
9.1.2 Multicast Discovery
9.2 Port
9.3 Port Mapping 67
9.3.1 Set Auto Port Mapping67
9.3.2 Set Manual Port Mapping 67
9.3.3 Set Port Mapping on Router 68
9.4 SNMP
9.5 Access to Device via Domain Name 69
9.6 Access to Device via PPPoE Dial Up Connection 70
9.7 Accessing via Mobile Client 70
9.7.1 Enable Hik-Connect Service on Camera71
9.7.2 Set Up Hik-Connect 72
9.7.3 Add Camera to Hik-Connect 72
9.8 Wi-Fi
9.8.1 Connect Device to Wi-Fi 73
9.9 Set ISUP 73
9.10 Set Open Network Video Interface 74
9.11 Set Network Service 74
9.12 Set Alarm Server 75
9.13 TCP Acceleration 76
9.14 Traffic Shaping
9.15 Set SRTP 76
Chapter 10 System and Security77
10.1 View Device Information77

10.2 Restore and Default	77
10.3 Search and Manage Log	77
10.4 Import and Export Configuration File	78
10.5 Export Diagnose Information	78
10.6 Reboot	78
10.7 Upgrade	78
10.8 View Open Source Software License	79
10.9 Set Live View Connection	79
10.10 Time and Date	79
10.10.1 Synchronize Time Manually	79
10.10.2 Set NTP Server	79
10.10.3 Set DST	80
10.11 Set RS-485	80
10.12 Security	80
10.12 Security 10.12.1 Authentication	
, ,	81
10.12.1 Authentication	81 81
10.12.1 Authentication 10.12.2 Set IP Address Filter	81 81 82
10.12.1 Authentication 10.12.2 Set IP Address Filter 10.12.3 Set HTTPS	81 81 82 82
10.12.1 Authentication 10.12.2 Set IP Address Filter 10.12.3 Set HTTPS 10.12.4 Security Audit Log	81 81 82 82 83
10.12.1 Authentication 10.12.2 Set IP Address Filter 10.12.3 Set HTTPS 10.12.4 Security Audit Log 10.12.5 Set QoS	81 81 82 82 83 83
10.12.1 Authentication	81 81 82 82 83 83 84 84
10.12.1 Authentication 10.12.2 Set IP Address Filter 10.12.3 Set HTTPS 10.12.4 Security Audit Log 10.12.5 Set QoS 10.12.6 Set IEEE 802.1X 10.12.7 Certificate Management	81 81 82 82 83 83 84 84 84
10.12.1 Authentication 10.12.2 Set IP Address Filter 10.12.3 Set HTTPS 10.12.4 Security Audit Log 10.12.5 Set QoS 10.12.6 Set IEEE 802.1X 10.12.7 Certificate Management 10.12.8 Control Timeout Settings	81 81 82 83 83 84 84 87 87
10.12.1 Authentication 10.12.2 Set IP Address Filter 10.12.3 Set HTTPS 10.12.4 Security Audit Log 10.12.5 Set QoS 10.12.6 Set IEEE 802.1X 10.12.7 Certificate Management 10.12.8 Control Timeout Settings 10.12.9 User and Account	81 81 82 83 84 84 87 87 <b>89</b>

# **Chapter 1 Overview**

## **1.1 Product Introduction**

The Network Speed Dome is an integration of the HD zoom camera and the PT module, ideal for remote monitoring. The device is easy to install and operate. Through Ethernet control, the device is able to compress and transmit images to multiple users. With network attached storage (NAS), the device is able to store and retrieve data easily.

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, 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. You can enable the functions as you need.

## **Event Function**

The device detects basic events and multiple smart events.

### **PTZ Function**

The device supports PTZ functions, such as presets, scans, patrol, 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			
	Mac OS 10.13 or later			
CPU	Intel <sup>®</sup> Pentium <sup>®</sup> IV 3.0 GHz or higher			
RAM	1 G or higher			
Display	1024 × 768 resolution or higher			
Web Browser	Internet Explorer 10 and above version, Apple Safari 12 and above version, Mozilla Firefox 52 and above version, Google Chrome 57 and above version.			

# **Chapter 2 Device Activation and Accessing**

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

## **i**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.

# 

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 <u>http://</u> <u>www.hikvision.com/</u>, 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.

001       Active       10.16.6.20       8000       10.16.6.254       80         002       Active       10.16.6.21       8000       10.16.6.254       80         003       Active       10.16.6.213       8000       10.16.6.254       N/A         004       Active       10.16.6.217       8000       10.16.6.254       N/A         005       Active       10.16.6.217       8000       10.16.6.254       N/A         006       Active       10.16.6.20       8000       10.16.6.254       N/A         006       Active       10.16.6.20       8000       10.16.6.254       80         006       Active       10.16.6.20       8000       10.16.6.254       80         006       Active       10.16.6.20       8000       10.16.6.254       80         007       Inactive       192.168.1.64       192.168.1.64       194	SADP	(									0 _ 0
001 Active 10.16.6.20 800 10.16.6.254 80   002 Active 10.16.6.21 800 10.16.6.254 80   003 Active 10.16.6.213 800 10.16.6.254 N/A   004 Active 10.16.6.179 800 10.16.6.254 N/A   005 Active 10.16.6.250 800 10.16.6.254 N/A   006 Active 10.16.6.250 800 10.16.6.254 80   007 Inactive 192.168.1.64   009 ActiveSeleCtfinactive device 80	Total numb	ber of online devices: 9							Export	Refresh	Activate the Device
002 Active 10.16.6.21 800 10.16.6.254 80   003 Active 10.16.6.213 8000 10.16.6.254 N/A   004 Active 10.16.6.179 8000 10.16.6.254 N/A   005 Active 10.16.6.273 800 10.16.6.254 N/A   006 Active 10.16.6.250 800 10.16.6.254 N/A   006 Active 10.16.6.250 800 10.16.6.254 N/A   007 Inactive 192.168.1.64	I   ID	•   Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Po	rt   Device Se	rial No.	
a crive 10.16.6.213 8000 10.16.6.254 N/A a crive 10.16.6.177 8000 10.16.6.254 N/A a crive 10.16.6.127 8000 10.16.6.254 N/A a crive 10.16.6.127 8000 10.16.6.254 80 006 Active 10.16.6.250 8000 10.16.6.254 80 007 Inactive 192.168.1.64 a crive 10.16.6.251 80 192.168.1.64 192.168.1.64 b crite activated. Comparison of the device activation. Comparison of the device activation.	001	E0.4030302.2	Active	10.16.6.20	8000	V1.3.06ubl 1808	10.16.6.254	80	D5-KDRU	12-20120340413CH	
1       004       Active       10160.213       8000       10160.224       N/A         1       004       Active       10166.217       8000       10166.224       N/A         1       005       Active       10166.217       8000       10166.224       N/A         1       006       Active       10166.225       800       10166.224       80         1       006       Active       10166.224       80       10166.224       80         1       009       ActiveSeleCtlinactive device       192.168.1.64       N/A       Active touck parameters after the device activation.         1       009       ActiveSeleCtlinactive device       80       N/A       N/A         1       009       Active Selectlinactive device       80       N/A       N/A         1       009       Active Selectlinactive device       80       N/A       N/A         1       009       Active New Password.       80       N/A       N/A         1       009       Active Selectlinactive device       80       N/A       N/A         1       009       Active Selectlinactive device       80       N/A       N/A         1       009       Active Selectl	002	DS-404E303-A	Active	10.16.6.21	8000	V5.3.0build 1898	10.16.6.254	80	D5-10483	IL AUGUSTISTICS	4
a crive 10.16.6.127 8000 10.16.6.254 N/A 006 Active 10.16.6.250 8000 10.16.6.254 80 007 Inactive 192.168.1.64 009 ActiSeleCtt <sup>1</sup> inactive device <sup>10.16.6.254</sup> 80 Input and confirm password.	003	D5-828028-AI	Active	10.16.6.213	8000	VL1/Build 1812	10.16.6.254	N/A	D5-42802	X AL20141207VE	
Active 10.16.6.127 8000 10.16.6.254 N/A 1 006 Active 10.16.6.250 8000 10.16.6.254 80 0007 Inactive 192.168.1.64 1 009 ActiSeleCt Inactive device. 80 Input and confirm password.	004	DS-19A08-F/K2G	Active	10.16.6.179	8000	V1.0.53build 180	10.16.6.254	N/A	D1-1940	••••••••••••••••••••••••••••••••••••••	The device is not activated
OO7       Inactive       192.168.1.64         009       ActiSeleiCtinactive device.       80         Input and confirm password.       New Password:       New Password:	005	05-19408-018NG	Active	10.16.6.127	8000	V2.276whit 1807	10.16.6.254	N/A	D5-1868	10000201407274	The device is not delivated.
009       Acti Select Inactive device.       80         Input and confirm password.       New Password:       Strong	006	UNIDWN-DEVICE-TYPE	Active	10.16.6.250	8000	VSA Durid 1852	10.16.6.254	80	20141119	CCW84803406798	
Active device activation. Active device devi	/	007			4	Inactiv	/e	1	192.168	3.1.64	
password.	009	D5-19508N-045/K2GW	<sup>Actir</sup> Se	lectina	activ	ve devic	e.10.16.6.254	80	05-2002	N- MEX20H5423	the device activation.
										onfirm	New Password:
							pass	wo	rd.		

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.

# **i**Note

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

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

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

## 2.2.1 Plug-in Installation

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

Operating System	Web Browser	Operation
Windows	Internet Explorer 10+	Follow pop-up prompts to complete plug-in installation.
Windows 7 and above version	Google Chrome 57+ Mozilla Firefox 52+	Click <b>Download Plug-in</b> to download and install plug-in.
Mac OS	Google Chrome 57+ Mozilla Firefox 52+ Mac Safari 12+	Plug-in installation is not required. Go to Configuration → Network → Advanced Settings

Operating System	Web Browser	Operation
		→ Network Service to enable WebSocket or Websockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

## iNote

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.

## iNote

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**  $\rightarrow$  **System**  $\rightarrow$  **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**  $\rightarrow$  **System**  $\rightarrow$  **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** $\rightarrow$ **System** $\rightarrow$ **Security** $\rightarrow$ **Security Service**, and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

#### **Illegal Login Attempts**

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

#### **Locking Duration**

The device releases the lock after the setting duration.

# Chapter 3 PTZ

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

## **3.1 PTZ Control**

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

## **PTZ Control Panel**

	<ul> <li>Click and hold the directional button to pan/tilt the device.</li> <li>i Note</li> <li>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.</li> <li>You can set Max. Tilt-angle in Configuration → PTZ → Basic Settings to limit tilt movement range.</li> </ul>
U	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.
4	Drag the slider to adjust the speed of pan/tilt movement.

## **i**Note

You can set Manual Control Speed in Configuration  $\rightarrow$  PTZ  $\rightarrow$  Basic Settings .

Compatible	The control speed is same as <b>Keyboard Control</b> <b>Speed</b> .
Pedestrian	Choose <b>Pedestrian</b> when you monitor the pedestrians.
Non-motor Vehicle	Choose <b>Non-motor Vehicle</b> when you monitor the non-motor vehicles.
Motor Vehicle	Choose <b>Motor Vehicle</b> when you monitor the motor vehicles.
Auto	You are recommended to set it as <b>Auto</b> 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**  $\rightarrow$  **PTZ**  $\rightarrow$  **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

at a	Click the button, and the lens zooms in.
م	Click the button, and the lens zooms out.

## **i**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

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

## Iris

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

## **3.2 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  $\ F$  .
- 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.

## **i**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.

# iNote

You can delete all presets in **Configuration**  $\rightarrow$  **PTZ**  $\rightarrow$  **Clear Config**. Click **Clear All Presets**, and click **Save**.

### What to do next

Go to **Configuration**  $\rightarrow$  **PTZ**  $\rightarrow$  **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.

## 3.2.1 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
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

## 3.3 Set Patrol Scan

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

### **Before You Start**

# iNote

This function is only supported by certain models.

Make sure that you have defined more than one presets. See <u>Set Preset</u> for detailed configuration.

### Steps

- **1.** Click to show the setting panel, and click  $\varnothing$  to enter patrol setting interface.
- **2.** Select a patrol number from the list and click x.
- **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.

# **i**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.

# iNote

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

## 3.3.1 Set One-Touch Patrol

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

### Steps

Set two or more presets among preset No.1 to preset No.32. For setting presets, refer to <u>Set</u>
 <u>Preset</u>.

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.

## 3.4 Set Pattern Scan

The device can move as the recorded pattern.

#### Steps

## **i** Note

This function is only supported by certain models.

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

## **i**Note

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

- 5. Click on 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.

# iNote

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

# 3.5 Set Limit

The device can only move within the limited range.

### Steps

- **1.** Go to **Configuration**  $\rightarrow$  **PTZ**  $\rightarrow$  **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.

# iNote

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.

# iNote

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

## Result

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

# 3.6 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.

# 3.7 Set Scheduled Tasks

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

### Steps

- **1.** Go to **Configuration**  $\rightarrow$  **PTZ**  $\rightarrow$  **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.

# iNote

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

# 3.8 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. See *Set Patrol Scan* for details.

#### Steps

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

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

6. Click Save.

## 3.8.1 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.

## 3.9 Set Privacy Mask

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

#### Steps

### **1.** Go to **Configuration** $\rightarrow$ **PTZ** $\rightarrow$ **Privacy Mask** .

- 2. Adjust the live image to the target scene via PTZ control buttons.
- **3.** Draw the area.

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

## 4. Click Add.

It is listed in **Privacy Mask List**.

5. Edit Name, Type, and Active Zoom Ratio on your demand.

## Active Zoom Ratio

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

# **i**Note

Active zoom ratio is only supported for the PTZ channel.

- 6. Repeat the steps above to set other privacy masks.
- 7. Check Enable Privacy Masks.

# 3.10 Set Smart Tracking

The device detects and tracks moving targets in the scene and keeps the target in the center of the live image with a predefined size during the tracking process.

## Steps

## iNote

This function is only supported by certain device models.

## **1.** Go to **Configuration** $\rightarrow$ **PTZ** $\rightarrow$ **Smart Tracking** .

2. Check Enable Smart Tracking.

- **3.** Set the **Duration**. The device stops tracking when the duration time is up.
- 4. Set the zooming control and tracking parameters.

## **Zooming Control**

Two modes are available. Controlled by target frame or by tilt angle of the device.

## By Tilt Angle

The device calculates the tracking zoom ratio automatically according to the tilt angle of the device.

## iNote

The attitude of the device affects the accuracy of this zooming control mode. For the model with a built-in gyroscope, try to calibrate the attitude if some zooming problems happen during tracking. See for instructions.

## By Target Frame

The tracked target has a virtual frame around. The device calculates a suitable zoom ratio according to the frame and the set **Tracking Zoom Ratio**. Larger value means bigger zoom ratio.

### Wait to Stop Tracking If Low Validity

The validity is an internal parameter that helps judge whether the device should keep tracking or not. This parameter is the waiting time level before the device stops tracking when the validity is low. Larger value means longer waiting time.

### Wait to Lower Tracking Speed If Low Validity

The validity is an internal parameter that helps judge whether the PTZ channel should lower the tracking speed or not. This parameter is the waiting time level before the device lowers the tracking speed when the validity is low. Larger value means longer waiting time.

5. Optional: Check Tuning Mode.

# **i**Note

Tuning mode is to display the information that helps debugging the function. This mode is reserved for technical support.

6. Click Save.

## 3.11 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**  $\rightarrow$  **PTZ**  $\rightarrow$  **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.

# 3.12 Set PTZ Priority

The function can set the PTZ priority of different signals.

### Steps

- **1.** Go to **Configuration**  $\rightarrow$  **PTZ**  $\rightarrow$  **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.

# 3.13 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.

# iNote

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.

## iNote

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 4 Live View**

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

## 4.1 Live View Parameters

The supported functions vary depending on the model.

## 4.1.1 Start and Stop Live View

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

## 4.1.2 Aspect Ratio

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

- **us refers to 4:3 window size.**
- III refers to 16:9 window size.
- refers to original window size.
- 🔳 refers to self-adaptive window size.

## 4.1.3 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 **<u>Stream Type</u>**.

## 4.1.4 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 <u>OSD</u>.
- For parameter explanation and instructions of audio and video settings, see *Video and Audio*.

## 4.1.5 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.

## 4.1.6 Count Pixel

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

## Steps

- 1. Click 'L. 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.

## 4.1.7 Start Digital Zoom

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

### Steps

- **1.** Click **Q** 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.

## 4.1.8 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.

## 4.1.9 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  $\mathbb{X}$  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.

## 4.1.10 Light

Click 🌞 to turn on or turn off the illuminator.

## 4.1.11 Lens Initialization

The lens automatically adjusts the zoom and focus value to default settings.

You can initialize the lens in two ways:

- Click 
   on PTZ control panel to reset the lens parameters once.
- Select Lens Initialization as ON in Configuration → Image → Display Settings to reset the lens parameters once.

## 4.1.12 Track Manually

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

## **i**Note

The function may not be supported by certain device models.

## Steps

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

The device tracks the target and keeps it in the center of live view image.

## 4.1.13 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.

## 4.1.14 Undervoltage Alarm

It is used to monitor the device voltage and warns you when the voltage is alarmingly low.

## **i**Note

This function is only supported by certain models.

When the device voltage is too low, a sign  $\otimes$  appears in the live view image. You are recommended to optimize the power supply, so as to avoid device failure.

The function is on by default.

## 4.1.15 Display Target Information on Live View

Go to **Configuration**  $\rightarrow$  **Local**  $\rightarrow$  **Live View Parameters** for settings.

### **i** Note

Related smart function should be configured and enabled in advance.

#### **Display POS Information**

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

## 4.2 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

ТСР

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.

# iNote

For detailed information about multicast, refer to Multicast .

#### HTTP

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

#### **Play Performance**

#### **Shortest Delay**

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

#### Balanced

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

#### Fluent

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

### Custom

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

### 3. Click OK.

## 4.3 OSD Menu

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

Click direction buttons or  $\square$  and  $\square$  to move up and down. Click  $\bigcirc$  to confirm your selection.

# **Chapter 5 Video and Audio**

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

## 5.1 Video Settings

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

Go to setting page: Configuration  $\rightarrow$  Video/Audio  $\rightarrow$  Video .

## 5.1.1 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.

## 5.1.2 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.

## 5.1.3 Resolution

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

## 5.1.4 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.

## 5.1.5 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.

## 5.1.6 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.

## 5.1.7 Video Encoding

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

# iNote

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.

## iNote

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.

## **i**Note

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

## Profile

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

## SVC

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

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

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

## Smoothing

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

### MJPEG

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

### 5.1.8 I-Frame Interval

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

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

## 5.2 Audio Settings

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

Go to the audio settings page: Configuration  $\rightarrow$  Video/Audio  $\rightarrow$  Audio .

## 5.2.1 Audio Input

If a built-in microphone or an 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

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

```
iNote
```

MicIn is only supported by certain models.

## Input volume

Adjust the volume of the audio input.

## 5.2.2 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.

## 5.3 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.

## 5.4 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.

## 5.4.1 Set ROI

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

#### **Before You Start**

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

#### Steps

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

## iNote

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.

## iNote

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.

## 5.5 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  $\rightarrow$  Video/Audio  $\rightarrow$  Display Info. on Stream .
- 2. Check Enable Dual-VCA.
- 3. Click Save.

## 5.6 Display Settings

It offers the parameter settings to adjust image features.

#### Go to Configuration $\rightarrow$ Image $\rightarrow$ Display Settings .

Click **Default** to restore settings.

### 5.6.1 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.

## **i**Note

Day/Night Switch function varies according to models.

## Set Supplement Light

#### Steps

**1.** Go to **Configuration**  $\rightarrow$  **Maintenance**  $\rightarrow$  **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.

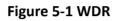
## iNote

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



WDR Off

WDR On



## White Balance

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



Cold





Auto White Balance

#### Figure 5-2 White Balance

Warm

#### DNR

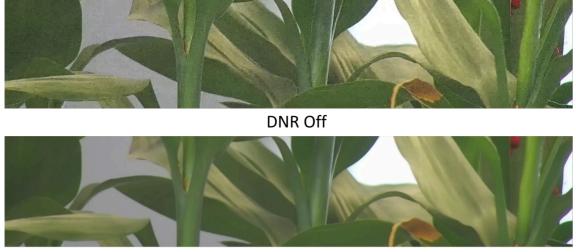
Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

#### Normal

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

#### Expert

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



DNR On Figure 5-3 DNR

## Defog

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



Defog On

**Figure 5-4 Defog** 

## EIS

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

## 5.6.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

Go to image parameters switch setting page: Configuration  $\rightarrow$  Image  $\rightarrow$  Image Parameters Switch , and set parameters as needed.

## Set Switch

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

#### Steps

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

## **i**Note

For the 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.

## 5.6.3 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.

## **i**Note

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

## 5.6.4 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/region.

## 5.6.5 Zoom Limit

You can set a certain value to limit the maximum value of zooming.

## 5.7 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  $\rightarrow$  Image  $\rightarrow$  OSD Settings . Set the corresponding parameters, and click Save to take effect.

## **Character Set**

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

### **Displayed Information**

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

## **Text Overlay**

Set customized overlay text on image.

## **OSD** Parameters

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

## 5.8 Demist

Demist is to remove the condensation on the lens and the glass window.

Enter the OSD menu and go to System Settings  $\rightarrow$  System Info Settings  $\rightarrow$  Demist to select a demist mode.

For OSD menu operations, see OSD Menu .

#### N.O

The function is turned on all the time.

#### Auto

The device automatically removes the condensation according to temperature changes.

#### N.C

The function is turned off all the time.

# **Chapter 6 Video Recording and Picture Capture**

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

## 6.1 Storage Settings

This part introduces the configuration of several common storage paths.

## 6.1.1 Memory Card

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

#### Set New or Unencrypted Memory Card

#### **Before You Start**

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

#### Steps

#### 1. Go to Configuration → Storage → Storage Management → HDD Management .

**2.** Select the memory card.

## **i**Note

If an **Unlock** button appears, you need to unlock the memory card first. See <u>Detect Memory</u> <u>Card Status</u> for details.

3. Click Format to initialize the memory card.

When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.

- **4. Optional:** Encrypt the memory card.
  - 1) Click Encrypted Format.
  - 2) Set the encryption password.
  - 3) Click **OK**.

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

## iNote

Keep your encryption password properly. Encryption password cannot be found if forgotten.

**5. Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.

6. Click Save.

### Set Encrypted Memory Card

#### **Before You Start**

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

#### Steps

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

## **i**Note

If an **Unlock** button appears, you need to unlock the memory card first. See <u>Detect Memory</u> <u>Card Status</u> for details.

- **3.** Verify the encryption password.
  - 1) Click Parity.
  - 2) Enter the encryption password.
  - 3) Click **OK**.

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

## iNote

If the encryption password is forgotten and you still want to use this memory card, see <u>Set New</u> <u>or Unencrypted Memory Card</u> to format and set the memory card. All existing contents will be removed.

- 4. Optional: Define the Quota of the memory card. Input the percentage for storing different contents according to your needs.
- 5. Click Save.

## **Detect Memory Card Status**

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

#### **Before You Start**

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

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

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

#### Health Status

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

## iNote

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

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

## iNote

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

## 6.1.2 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.

## 6.1.3 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.

## 6.1.4 Set Cloud Storage

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

#### Steps

If cloud storage is enabled, the pictures are stored in the cloud storage server preferentially.

#### 1. Go to Configuration → Storage → Storage Management → Cloud Storage .

- 2. Check Enable Cloud Storage.
- 3. Set basic parameters.

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

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

## 6.2 Video Recording

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

## 6.2.1 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.

## **i**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.

- Set schedule for the selected record type. Refer to <u>Set Arming Schedule</u> 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.

### **i**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.

## 6.2.2 Record Manually

#### Steps

- **1.** Go to **Configuration**  $\rightarrow$  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.

## 6.2.3 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.

## **i**Note

Go to **Configuration**  $\rightarrow$  **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**.

## **i**Note

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

## 6.3 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.

### 6.3.1 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 <u>Set Arming Schedule</u> for configuring schedule time.
- 5. Click Save.

## 6.3.2 Capture Manually

#### Steps

- **1.** Go to **Configuration**  $\rightarrow$  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.

#### 6.3.3 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.

## **i**Note

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

# **Chapter 7 Event and Alarm**

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

## 7.1 Basic Event

## 7.1.1 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**  $\rightarrow$  **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 <u>Set Arming Schedule</u> 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.

- 1. Select normal mode in Configuration.
- 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.

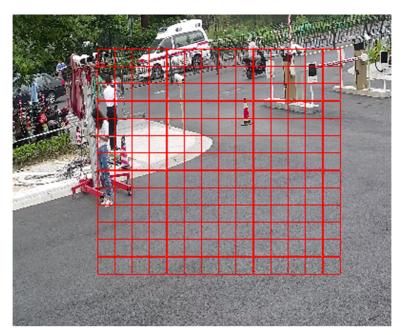


Figure 7-1 Set Rules

**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 7-2 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.

## 7.1.2 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**  $\rightarrow$  **Event**  $\rightarrow$  **Basic Event**  $\rightarrow$  **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 7-3 Set Video Tampering Area

- Refer to <u>Set Arming Schedule</u> for setting scheduled time. Refer to <u>Linkage Method Settings</u> for setting linkage method.
- 6. Click Save.

## 7.1.3 Set Exception Alarm

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

- **1.** Go to **Configuration**  $\rightarrow$  **Event**  $\rightarrow$  **Basic Event**  $\rightarrow$  **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.

## 7.1.4 Set Alarm Input

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

#### **Before You Start**

## **i**Note

This function is only supported by certain models.

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

#### Steps

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

## 7.2 Smart Event

**i**]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.

#### 7.2.1 Detect Audio Exception

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

- 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.

**i** 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.

- Refer to <u>Set Arming Schedule</u> for setting scheduled time. Refer to <u>Linkage Method Settings</u> for setting linkage methods.
- 4. Click Save.

## **i**Note

The function varies according to different models.

## 7.2.2 Set Face Detection

It helps to detect the face in the detection region. If a face is detected, the device triggers the linkage actions.

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

## 7.2.3 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. Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
  - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
  - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
- 7. 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.
  - DetectionYou can specify the object type, and the device only detects the selectedTargettype of objects.



Figure 7-4 Draw Area

- 8. Click Save.
- **9.** Repeat above steps to set other detection areas.
- 10. Set arming schedule. See <u>Set Arming Schedule</u>.
- 11. Set linkage method. See Linkage Method Settings .

## 7.2.4 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

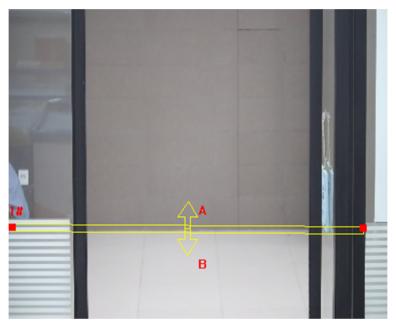
The object going across the line from both directions can be detected and alarms are triggered.

#### 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 7-5 Draw Line

- **6. Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
  - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
  - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
- 7. 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.
  - DetectionYou can specify the object type, and the device only detects the selectedTargettype of objects.
- 8. Click Save.

- 9. Repeat above steps to set other lines.
- 10. Set arming schedule. See Set Arming Schedule .
- 11. Set linkage method. See Linkage Method Settings .

## 7.2.5 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**  $\rightarrow$  **Event**  $\rightarrow$  **Smart Event**  $\rightarrow$  **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. Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
  - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
  - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
- 7. 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 7-6 Draw Area

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

## 7.2.6 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**  $\rightarrow$  **Event**  $\rightarrow$  **Smart Event**  $\rightarrow$  **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. Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
  - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
  - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
- **7.** 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.
  - DetectionYou can specify the object type, and the device only detects the selectedTargettype of objects.



Figure 7-7 Draw Area

8. Click Save.

- 9. Repeat above steps to set other regions.
- 10. Set arming schedule. See Set Arming Schedule .
- 11. Set linkage method. See Linkage Method Settings .

## 7.2.7 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. Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
  - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
  - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
- 7. 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.

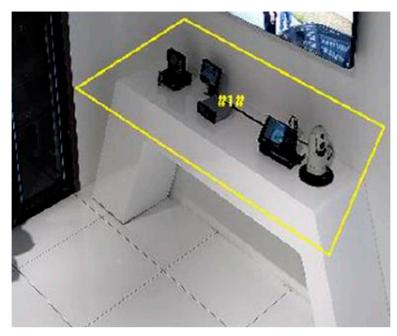


Figure 7-8 Draw Area

- 8. Click Save.
- **9.** Repeat above steps to set other regions.
- 10. Set arming schedule. See <u>Set Arming Schedule</u>.
- 11. Set linkage method. See Linkage Method Settings .

## 7.2.8 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**  $\rightarrow$  **Event**  $\rightarrow$  **Smart Event**  $\rightarrow$  **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. Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
  - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
  - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
- **7.** 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.

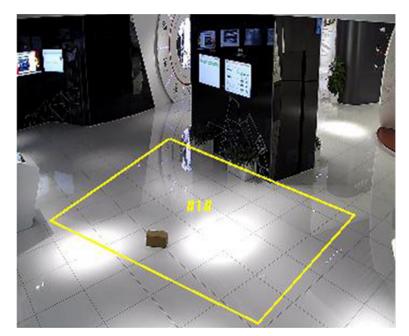


Figure 7-9 Draw Area

8. Click Save.

- 9. Repeat above steps to set other regions.
- 10. Set arming schedule. See Set Arming Schedule .
- 11. Set linkage method. See Linkage Method Settings .

# **Chapter 8 Arming Schedule and Alarm Linkage**

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

## 8.1 Set Arming Schedule

Set the valid time of the device tasks.

#### Steps

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



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.

## 8.2 Linkage Method Settings

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

## 8.2.1 Trigger Alarm Output

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

#### Steps

## **i** Note

This function is only supported by certain models.

#### **1.** Go to **Configuration** $\rightarrow$ **Event** $\rightarrow$ **Basic Event** $\rightarrow$ **Alarm Output**.

2. Set alarm output parameters.

Automatic Alarm For the information about the configuration, see <u>Automatic Alarm</u>.

Manual Alarm For the information about the configuration, see <u>Manual Alarm</u>.

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 <u>Set Arming Schedule</u>.
- **3.** Click **Copy to...** to copy the parameters to other alarm output channels.
- 4. Click Save.

#### **Manual Alarm**

You can trigger an alarm output manually.

#### Steps

1. Set the manual alarm parameters.

#### Alarm Output No.

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

#### Alarm Name

Edit a name for the alarm output.

#### Delay

#### Select Manual.

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

### 8.2.2 FTP/NAS/Memory Card Uploading

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

Refer to <u>Set FTP</u> to set the FTP server.

Refer to <u>Set NAS</u> for NAS configuration.

Refer to <u>Set New or Unencrypted Memory Card</u> for memory card storage configuration.

#### 8.2.3 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 <u>Set Email</u>.

#### 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**  $\rightarrow$  **Network**  $\rightarrow$  **Basic Settings**  $\rightarrow$  **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.

### iNote

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.

### 8.2.4 Notify Surveillance Center

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

### 8.2.5 Smart Tracking

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

### iNote

This function is only supported by certain models.

### 8.2.6 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 9 Network Settings**

## 9.1 TCP/IP

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

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

#### NIC Type

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

#### IPv4

Two IPv4 modes are available.

#### DHCP

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

## **i**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.

## **i**Note

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

#### DHCP

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

#### Manual

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

#### MTU

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

The valid value range of MTU is 1280 to 1500.

#### DNS

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

#### **Dynamic Domain Name**

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

## **i**Note

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

#### 9.1.1 Multicast

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

Go to **Configuration**  $\rightarrow$  **Network**  $\rightarrow$  **Basic Settings**  $\rightarrow$  **Multicast** for the multicast settings.

#### **IP Address**

It stands for the address of multicast host.

#### Stream Type

The stream type as the multicast source.

#### Video Port

The video port of the selected stream.

#### Audio Port

The audio port of the selected stream.

#### 9.1.2 Multicast Discovery

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

## 9.2 Port

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

# **A**Caution

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

#### Go to **Configuration** $\rightarrow$ **Network** $\rightarrow$ **Basic Settings** $\rightarrow$ **Port** for port settings.

#### **HTTP Port**

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

#### **HTTPS Port**

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

#### **RTSP Port**

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

#### SRTP Port

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

#### Server Port

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

#### **Enhanced SDK Service Port**

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

#### WebSocket Port

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

#### WebSockets Port

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

#### iNote

- 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.

## 9.3 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 <u>Port</u> to modify the device ports.

#### Steps

**1.** Go to **Configuration**  $\rightarrow$  **Network**  $\rightarrow$  **Basic Settings**  $\rightarrow$  **NAT**.

**2.** Select the port mapping mode.

Auto Port Mapping Refer to <u>Set Auto Port Mapping</u> for detailed information.

Manual Port Mapping Refer to <u>Set Manual Port Mapping</u> for detailed information.

3. Click Save.

### 9.3.1 Set Auto Port Mapping

#### Steps

- 1. Check Enable UPnP<sup>™</sup>, 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.

## iNote

UPnP<sup>™</sup> function on the router should be enabled at the same time.

### 9.3.2 Set Manual Port Mapping

#### Steps

- 1. Check Enable UPnP<sup>™</sup>, 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.

### 9.3.3 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.

108M Wireless Router Model No.: TL-WR641G / TL-WR642G	Virtu	ual Servers			
Status	ID	Service Port	IP Address	Protocol	Enable
Quick Setup	1	80	192.168.10. 23	ALL 🗸	~
Basic Settings + Network	2	8000	192.168.10. 23	ALL 🔽	~
+ Wireless Advanced Settings	3	554	192.168.10. 23	ALL 🔽	×
+ DHCP	4	8200	<b>192.168.10</b> . 23	ALL 🗸	~
<ul> <li>Forwarding</li> <li>Virtual Servers</li> </ul>	5	81	192.168.10. 24	ALL 🔽	⊻
Port Triggering	6	8001	192.168.10. 24	ALL 🗸	~
• DMZ • UPnP	7	555	192.168.10. 24	ALL 🔽	×
+ Security	8	8201	192.168.10. 24	ALL 🗸	~
<ul> <li>Static Routing</li> <li>Dynamic DNS</li> <li>Maintenance</li> <li>System Tools</li> </ul>	Common Service Port: DNS(53)  Copy to ID 1 Previous Next Clear All Save				

#### Figure 9-1 Port Mapping on Router

## **i**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.

## **9.4 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**  $\rightarrow$  **Network**  $\rightarrow$  **Advanced Settings**  $\rightarrow$  **SNMP**.
- 2. Check Enable SNMPv1, Enable SNMP v2c or Enable SNMPv3.

## iNote

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.

### 9.5 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**  $\rightarrow$  **Network**  $\rightarrow$  **Basic Settings**  $\rightarrow$  **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.
- Check the device ports and complete port mapping. Refer to <u>Port</u> to check the device port , and refer to <u>Port Mapping</u> 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.

## 9.6 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.
1.	

## **i**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 <u>Access to Device via Domain</u> <u>Name</u> for detail information.

## 9.7 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.

### **i**Note

Hik-Connect service should be supported by the camera.

### 9.7.1 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.

## iNote

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.

### **i**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.

### 9.7.2 Set Up Hik-Connect

#### Steps

1. Get and install Hik-Connect application by the following ways.

- Visit <u>https://appstore.hikvision.com</u> to download the application according to your mobile phone system.
- Visit the official site of our company. Then go to **Support** → **Tools** → **Hikvision App Store**.
- Scan the QR code below to download the application.

## **i**Note

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

- Visit *https://appstore.hikvision.com/static/help/index.html* to refer to the troubleshooting.
- Visit <u>https://appstore.hikvision.com/</u>, and click Installation Help at the upper right corner of the interface to refer to the troubleshooting.
- 2. Start the application and register for a Hik-Connect user account.
- 3. Log in after registration.

### 9.7.3 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.

## **i**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.

## **i**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.
- **8.** Connect the camera to the router with a network cable and tap **Connected** in the result interface.

## iNote

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

9. Tap Add in the next interface to finish adding.

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

## 9.8 Wi-Fi

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

### iNote

This function is only supported by certain device models.

### 9.8.1 Connect Device to Wi-Fi

#### **Before You Start**

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

#### Steps

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

## iNote

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

- 3. Go to Wi-Fi settings page: Configuration → Network → Advanced Configuration → Wi-Fi.
- **4.** Set and save the parameters.
  - 1) Click Search.
  - 2) Select a SSID, which should be the same as that of wireless router or AP.

The parameters of the network is automatically shown in Wi-Fi.

- 3) Select the Network Mode as Manage.
- 4) Input the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

#### What to do next

Go to TCP/IP settings page: Configuration  $\rightarrow$  Network  $\rightarrow$  Basic Configuration  $\rightarrow$  TCP/IP, and click Wlan to check the IPv4 Address and log in the device. See <u>Access Device via Web Browser</u> for detailed information.

## 9.9 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.

## 9.10 Set Open Network Video Interface

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

#### Steps

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

**Delete** Delete the selected Open Network Video Interface user.

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

## 9.11 Set Network Service

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

#### Steps

## iNote

This function varies according to different models.

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

2. Set network service.

#### WebSocket & WebSockets

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

If the device uses HTTP, enable WebSocket.

If the device uses HTTPS, enable WebSockets.

When you use WebSockets, select the Server Certificate.

## **i**Note

Complete certificate management before selecting server certificate. Refer to <u>Certificate</u> <u>Management</u> for detailed information.

#### SDK Service & Enhanced SDK Service

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

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

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

## **i**Note

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

#### **TLS (Transport Layer Security)**

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

#### Bonjour

Uncheck to disable the protocol.

3. Click Save.

## 9.12 Set Alarm Server

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

#### Steps

- **1.** Go to Configuration  $\rightarrow$  Network  $\rightarrow$  Advanced Settings  $\rightarrow$  Alarm Server .
- 2. Enter Destination IP or Host Name, URL, and Port.
- 3. Select Protocol.

## iNote

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

- 4. Click Test to check if the IP or host is available.
- 5. Click Save.

## 9.13 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.

## 9.14 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.

## 9.15 Set SRTP

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

#### Steps

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

## **i**Note

- Only certain device models support this function.
- If the function is abnormal, check if the selected certificate is abnormal in certificate management.

# **Chapter 10 System and Security**

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

## **10.1 View Device Information**

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

Enter Configuration  $\rightarrow$  System  $\rightarrow$  System Settings  $\rightarrow$  Basic Information to view the device information.

## **10.2 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.

iNote

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

## 10.3 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

- **1.** Go to **Configuration**  $\rightarrow$  **System**  $\rightarrow$  **Maintenance**  $\rightarrow$  **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.

## **10.4 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  $\rightarrow$  System  $\rightarrow$  Maintenance  $\rightarrow$  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.

## **10.5 Export Diagnose Information**

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

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

## 10.6 Reboot

You can reboot the device via browser.

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

## 10.7 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** $\rightarrow$ **System** $\rightarrow$ **Maintenance** $\rightarrow$ **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.

## **10.8 View Open Source Software License**

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

## **10.9 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**  $\rightarrow$  **System**  $\rightarrow$  **Maintenance**  $\rightarrow$  **System Service** to set the upper limit of the remote connection number.

## 10.10 Time and Date

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

### 10.10.1 Synchronize Time Manually

#### Steps

- **1.** Go to **Configuration**  $\rightarrow$  **System**  $\rightarrow$  **System** Settings  $\rightarrow$  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.

### 10.10.2 Set NTP Server

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

#### Before You Start

Set up a NTP server or obtain NTP server information.

#### Steps

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

## iNote

Server Address is NTP server IP address.

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

### 10.10.3 Set DST

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

#### Steps

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

## 10.11 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**  $\rightarrow$  **System**  $\rightarrow$  **System Settings**  $\rightarrow$  **RS-485**.
- 2. Set the RS-485 parameters.

## **i**Note

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

3. Click Save.

## 10.12 Security

You can improve system security by setting security parameters.

### 10.12.1 Authentication

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

Go to **Configuration**  $\rightarrow$  **System**  $\rightarrow$  **Security**  $\rightarrow$  **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.

#### **i** Note

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

#### 10.12.2 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**  $\rightarrow$  **System**  $\rightarrow$  **Security**  $\rightarrow$  **IP Address Filter**.
- 2. Check Enable IP Address Filter.
- 3. Select the type of IP address filter.

Forbidden IP addresses in the list cannot access the device.

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

- 4. Edit the IP address filter list.
  - Add Add a new IP address or IP address range to the list.
  - **Modify** Modify the selected IP address or IP address range in the list.
  - **Delete** Delete the selected IP address or IP address range in the list.
- 5. Click Save.

### 10.12.3 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. Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
- **4.** Select a server certificate.

## **i**Note

- Complete certificate management before selecting server certificate. Refer to <u>Certificate</u> <u>Management</u> for detailed information.
- If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
- 5. Click Save.

### 10.12.4 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

#### **i** Note

This function is only supported by certain camera models.

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

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

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

#### Set Log Server

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

#### **Before You Start**

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

#### Steps

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

### 10.12.5 Set QoS

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

## **i**Note

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

#### Steps

- **1.** Go to Configuration  $\rightarrow$  Network  $\rightarrow$  Advanced Configuration  $\rightarrow$  QoS .
- 2. Set Video/Audio DSCP, Alarm DSCP and Management DSCP.

## iNote

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.

### 10.12.6 Set IEEE 802.1X

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

Go to **Configuration**  $\rightarrow$  **Network**  $\rightarrow$  **Advanced Settings**  $\rightarrow$  **802.1X**, and enable the function.

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

### **i**Note

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

### 10.12.7 Certificate Management

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

### Server Certificate/Client Certificate

## **i**Note

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

### **Create and Install Self-signed Certificate**

#### Steps

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

## ĴiNote

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

4. Click OK to save and install the certificate.

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

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

5. Optional: Click Certificate Property to see the certificate details.

#### Install Self-signed Request Certificate

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

#### Before You Start

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

#### Steps

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

The certificate request details are displayed in a pop-up window.

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

## **i**Note

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

3) Click Browse to select the certificate file.

#### 4) Select Self-signed Request Certificate.

5) Click **OK**.

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

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

9. Optional: Click Certificate Property see the certificate details.

#### Install Other Authorized Certificate

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

#### Steps

- **1.** Go to Configuration  $\rightarrow$  System  $\rightarrow$  Security  $\rightarrow$  Certificate Management .
- 2. Click Import.

#### 3. Input Certificate ID.

#### **i**Note

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

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

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

#### 6. Click OK.

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

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

### **Install CA Certificate**

#### Before You Start

Prepare a CA certificate in advance.

#### Steps

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

## **i**Note

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

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

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

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

### **Enable Certificate Expiration Alarm**

#### Steps

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

## iNote

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

3. Click Save.

### **10.12.8 Control Timeout Settings**

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

Go to **Configuration**  $\rightarrow$  **System**  $\rightarrow$  **Security**  $\rightarrow$  **Advanced Security** to complete settings.

### 10.12.9 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**  $\rightarrow$  **System**  $\rightarrow$  **User Management**  $\rightarrow$  **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**.

## iNote

The administrator can add up to 31 user accounts.

3. Click OK.

### Simultaneous Login

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

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

#### **Online Users**

The information of users logging into the device is shown.

Go to **Configuration**  $\rightarrow$  **System**  $\rightarrow$  **User Management**  $\rightarrow$  **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.



# Appendix C. FAQ

Scan the following QR code to find the frequently asked questions of the device. Note that some frequently asked questions only apply to certain models.



