

Smart-Linkage PTZ Camera

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual on the company website.
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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". OUR COMPANY 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 OUR COMPANY 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 OUR COMPANY 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 OUR COMPANY 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, OUR COMPANY 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 Legal Informationi
Chapter 1 Overview1
1.1 Product Introduction1
1.2 Key Function1
1.3 System Requirement2
Chapter 2 Device Activation and Accessing3
2.1 Activate Device3
2.1.1 Activate Device via Web Browser3
2.1.2 Activate via IP PORTAL4
2.2 Access Device via Web Browser5
2.2.1 Plug-in Installation5
2.2.2 Admin Password Recovery6
2.2.3 Illegal Login Lock7
Chapter 3 Smart Function8
3.1 Allocate VCA Resource8
3.2 General Settings8
3.2.1 Set Camera Info9
3.3 Face Capture9
3.3.1 Set Auto Face Capture Rule9
3.3.1.1 Normal Mode Settings10
3.3.1.2 Expert Mode Settings10
3.3.2 Operate Manual Face Capture11
3.3.3 Overlay and Capture11
3.3.4 Face Capture Algorithm Parameters12
3.4 Display Alarm14
Chapter 4 PTZ16
4.1 PTZ Control16
4.2 Set Preset18
4.2.1 Special Presets19
4.3 Set Patrol Scan19
4.3.1 Set One-Touch Patrol20
4.4 Set Pattern Scan21
4.5 Set Limit21
4.6 Set Home Position22
4.7 Set Park Action22
4.7.1 Set One-Touch Park23
4.8 Set Scheduled Tasks23
4.9 Set Power Off Memory23

4.10 Set PTZ Priority24
4.11 Set Privacy Mask24
4.12 Set Rapid Focus25
4.13 Panorama Linkage25
4.13.1 Set Panorama Linkage - Auto Calibration26
4.13.2 Set Panorama Linkage - Manual Calibration26
4.14 GPS Calibration27
4.14.1 Set GPS Calibration27
4.14.2 Verify Calibration28
4.15 Set Device Position29
4.15.1 Set Manual Compass29
Chapter 5 Live View31
5.1 Live View Parameters31
5.1.1 Start and Stop Live View31
5.1.2 Aspect Ratio31
5.1.3 Live View Stream Type31
5.1.4 Select the Third-Party Plug-in31
5.1.5 Start Digital Zoom32
5.1.6 Conduct Regional Focus32
5.1.7 Conduct Regional Exposure32
5.1.8 Count Pixel32
5.1.9 Light33
5.1.10 Operate Wiper33
5.1.11 Lens Initialization34
5.1.12 Track Manually34
5.1.13 Conduct 3D Positioning34
5.2 Set Transmission Parameters34
Chapter 6 Video and Audio36
6.1 Video Settings36
6.1.1 Stream Type36
6.1.2 Video Type36
6.1.3 Resolution37
6.1.4 Bitrate Type and Max. Bitrate37
6.1.5 Video Quality37
6.1.6 Frame Rate37
6.1.7 Video Encoding37
6.1.7.1 H.26438
6.1.7.2 H.264+38
6.1.7.3 H.26538
6.1.7.4 H.265+38
6.1.7.5 MJPEG39

6.1.8 Profile39
6.1.9 I-Frame Interval39
6.1.10 SVC39
6.1.11 Smoothing39
6.2 Audio Settings39
6.2.1 Audio Input40
6.2.2 Audio Output40
6.2.3 Environmental Noise Filter40
6.3 Two-way Audio40
6.4 ROI40
6.4.1 Set ROI41
6.5 Target Cropping41
6.6 Display Info. on Stream42
6.7 Display Settings42
6.7.1 Scene Mode43
6.7.1.1 Image Adjustment43
6.7.1.2 Exposure Settings43
6.7.1.3 Focus43
6.7.1.4 Day/Night Switch44
Set Supplement Light44
6.7.1.5 BLC45
6.7.1.6 HLC45
6.7.1.7 WDR45
6.7.1.8 DNR46
6.7.1.9 White Balance46
6.7.1.10 Defog47
6.7.1.11 EIS47
6.7.2 Image Parameters Switch47
6.7.2.1 Set Scheduled-switch47
6.7.2.2 Set Link to Preset47
6.7.3 Mirror48
6.7.4 Video Standard48
6.8 OSD48
Chapter 7 Video Recording and Picture Capture49
7.1 Storage Settings49
7.1.1 Memory Card49
7.1.1.1 Set New or Unencrypted Memory Card49
7.1.1.2 Set Encrypted Memory Card50
7.1.1.3 Detect Memory Card Status50
7.1.2 Set FTP52
7.1.3 Set NAS53

7.1.4 eMMC Protection53
7.1.5 Set Cloud Storage54
7.2 Video Recording55
7.2.1 Record Automatically55
7.2.2 Record Manually56
7.2.3 Playback and Download Video56
7.3 Capture Configuration57
7.3.1 Capture Automatically57
7.3.2 Capture Manually58
7.3.3 View and Download Picture58
Chapter 8 Event and Alarm60
8.1 Basic Event60
8.1.1 Set Motion Detection60
8.1.1.1 Normal Mode60
8.1.1.2 Expert Mode61
8.1.2 Set Video Tampering Alarm62
8.1.3 Set Alarm Input63
8.1.4 Set Exception Alarm64
8.1.5 Set Audio Exception Detection64
8.2 Smart Event65
8.2.1 Set Intrusion Detection65
8.2.2 Set Line Crossing Detection67
8.2.3 Set Region Entrance Detection69
8.2.4 Set Region Exiting Detection70
8.2.5 Set Tracking Parameters72
8.2.6 Set Tracking Parameters73
Chapter 9 Arming Schedule and Alarm Linkage74
9.1 Set Arming Schedule74
9.2 Linkage Method Settings75
9.2.1 Trigger Alarm Output75
9.2.1.1 Automatic Alarm75
9.2.1.2 Manual Alarm75
9.2.2 FTP/NAS/Memory Card Uploading76
9.2.3 Send Email76
9.2.3.1 Set Email76
9.2.4 Notify Surveillance Center77
9.2.5 Smart Tracking77
9.2.6 Trigger Recording77
9.2.7 Audible Warning78
9.2.7.1 Set Audible Alarm Output78
9.2.7.2 Set Alarm Server79

9.2.8 Alarm Server79
9.2.8.1 Set Alarm Server79
Chapter 10 Network Settings80
10.1 TCP/IP80
10.2 Port Mapping81
10.2.1 Set Auto Port Mapping81
10.2.2 Set Manual Port Mapping82
10.2.3 Set Port Mapping on Router82
10.3 SNMP83
10.4 Access to Device via Domain Name84
10.5 Access to Device via PPPoE Dial Up Connection84
10.6 Accessing via Mobile Client86
10.6.1 Enable Guarding Vision Service on Camera86
10.6.1.1 Enable Guarding Vision Service via Web Browser86
10.6.1.2 Enable Guarding Vision Service via IP PORTAL Software86
10.6.2 Set Up Guarding Vision87
10.6.3 Add Camera to Guarding Vision87
10.7 HTTP(S)88
10.8 Multicast91
10.8.1 Multicast Discovery91
10.9 RTSP89
10.10 Set SRTP90
10.10.1 Multicast91
10.10.2 Multicast Discovery91
10.11 Bonjour91
10.12 WebSocket(s)91
10.13 TCP Acceleration92
10.14 Traffic Shaping92
10.15 Set ISUP92
10.16 Set Open Network Video Interface92
10.17 Set SDK Service93
Chapter 11 System and Security94
11.1 View Device Information94
11.2 Restart94
11.3 Upgrade94
11.4 Restore and Default95
11.5 Search and Manage Log95
11.6 Import and Export Configuration File95
11.7 Export Diagnose Information96
11.8 Search and Export Data Aware Information96
11.9 View Open Source Software License97

11.10 Set Live View Connection97
11.11 Time and Date97
11.11.1 Synchronize Time Manually97
11.11.2 Synchronize Time by Satellite97
11.11.3 Set NTP Server98
11.11.4 Set DST98
11.12 Set RS-48598
11.13 Security99
11.13.1 Set IP Address Filter99
11.13.2 Set MAC Address Filter99
11.13.3 Security Audit Log100
11.13.3.1 Search Security Audit Logs100
11.13.3.2 Set Log Server100
11.13.4 Set QoS101
11.13.5 Set IEEE 802.1X101
11.13.6 SSH102
11.13.7 Control Timeout Settings102
11.13.8 Certificate Management102
11.13.8.1 Server Certificate/Client Certificate102
Create and Install Self-signed Certificate102
Install Self-signed Request Certificate103
Install Other Authorized Certificate104
11.13.8.2 Install CA Certificate104
11.13.8.3 Enable Certificate Expiration Alarm105
11.13.9 TLS106
11.13.10 User and Account106
11.13.10.1 Set User Account and Permission106
11.13.10.2 Online Users107
11.13.10.3 Simultaneous Login107

Chapter 1 Overview

1.1 Product Introduction

The Smart-Linkage PTZ Camera is an HD camera for remote monitoring through network. It is easy to install with simple wiring and is easy to use.
The device consists of two channels: Camera 01 is the PTZ channel and Camera 02 is the panoramic channel. The integrated design combines the advantage of panoramic camera and PTZ camera to capture the whole picture and details at the same time. Based on deep learning technology, the device is able to filter out interference factors and get a clear image of the target. The device has multiple features and can be widely used in complicated environments such as entrances and exits, mixed-traffic roads, sidewalks, parks, scenic areas, streets, stations, residential blocks, and boundaries.

1.2 Key Function

The key functions of the device are as follows.

Audio Alarm

The device supports audio alarm to warn intruders off.

Linked Tracking and Capture

The panoramic channel and the PTZ channel work together to detect, locate and track targets in both overall pictures and adequate details.

Face Capture

The device detects, tracks, captures, grades, and filters moving faces, and outputs captured pictures.

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 visiting and operating the product.

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

Chapter 2 Device Activation and Accessing

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

Note

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

2.1 Activate Device

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

2.1.1 Activate Device via Web Browser

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

Before You Start

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

Steps

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

   The default IP address of the device is 192.168.1.64.

2. Open a web browser and input the default IP address.
3. Create and confirm the admin password.

Caution

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

4. Click **OK** to complete activation and enter **Live View** page.
5. Modify IP address of the camera.
   1) Enter IP address modification page. **Configuration** → **Network** → **TCP/IP**
   2) Change IP address.
   3) Save the settings.

2.1.2 Activate via IP PORTAL

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

Before You Start

- Get the IP PORTAL software from the supplied disk or the official website , and install the IP PORTAL according to the prompts.
- The device and the PC that runs the IP PORTAL 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 IP PORTAL* for details.

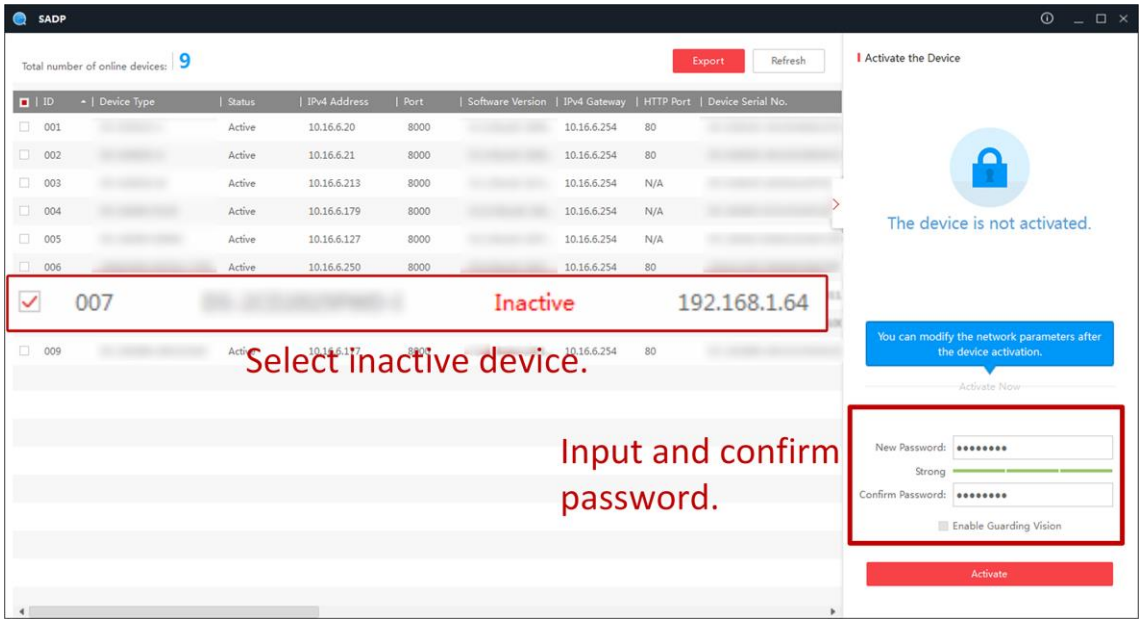
Steps

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

Caution

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

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



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

5. Modify IP address of the device.
   1) Select the device.

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

2.2 Access Device via Web Browser

Before You Start

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

Steps

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

Note

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

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

   For IE based web browser, webcomponents and QuickTime(TM) are optional. For non-IE based web browser, webcomponents, QuickTime(TM), 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 camera function. You should install plug-in or complete certain settings to ensure normal display and operation. For detailed restricted function, refer to the actual device.

Operating System	Web Browser	Operation
Windows	● Internet Explorer 10+ ● Google Chrome 57 and earlier version ● Mozilla Firefox 52 and earlier version	Follow pop-up prompts to complete plug-in installation.
	● Google Chrome 57+ ● Mozilla Firefox 52+	Click to download and

Operating System	Web Browser	Operation
		install plug-in.
Mac OS	● Google Chrome 57+ ● Mozilla Firefox 52+ ● Mac Safari 16+	Plug-in installation is not required. Go to **Configuration** → **Network** → **Network Service** → **WebSocket(s)** to enable WebSocket or WebSockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

Note

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

2.2.2 Admin Password Recovery

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

Note

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

Security Question

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

Email

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

verification code during the recovering operation process.

2.2.3 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.
Go to **Configuration** → **System** → **Security** → **Security Service**, and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Smart Function

3.1 Allocate VCA Resource

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

Steps

1. Click **VCA** on the left tab.
2. Enable the desired VCA function.
3. Click **Next** to finish settings.

Note

Certain VCA functions are mutually exclusive.

3.2 General Settings

Set the general parameters which are related to the smart applications.
Go to **VCA** → **Set Application** → **General Settings** to set the following parameters.

Camera Info.

For camera information settings, refer to ***Set Camera Info***.

FTP

For FTP settings, refer to ***Set FTP***.

Email

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

Alarm Output

For alarm output settings, refer to ***Automatic Alarm***.

Audible Alarm Output

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

Alarm Server

For alarm server settings, refer to ***Alarm Server***.

Tracking Parameters

For tracking parameter settings, refer to ***Set Tracking Parameters***.

3.2.1 Set Camera Info

Customize specific information for the device. It may help identify a certain device when multiple devices are under management.
Go **Open Platform** → **General VCA Resource** to set **Camera No.** and **Camera Info**.

3.3 Face Capture

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

Note

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

3.3.1 Set Auto Face Capture Rule

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

Before You Start

Go to **VCA** → **Select Application** to select **Face Capture**, and click **Next** to enable the function.

Steps

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

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

4. Click **Save**.

What to do next

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

Normal Mode Settings

Steps

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

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

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

   Click and to draw the distance on live image, or input values in the text fields of **Min. Pupil Distance** and **Max. Pupil Distance**.
5. Click **Save**.
6. Set arming schedule. See ***Set Arming Schedule***.
7. Set linkage method. See ***Linkage Method Settings***.

Expert Mode Settings

Steps

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

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

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

   Click and to draw the distance on live image, or input values in the text fields of **Min. Pupil Distance** and **Max. Pupil Distance**.

4. Set patrol schedule.
   1) Go to **VCA** → **Set Application** → **Face Recognition** → **Auto-Switch Schedule and Linkage Method**.
   2) Click **Modify**.
   3) Draw time bars as desired.
   4) Click a time bar and click **Set Scene Auto-switch**.
   5) Edit patrol path and input dwell time for each detection scene.

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

   6) Click **OK**.
5. Set linkage method. See ***Linkage Method Settings***.
6. Click **Save**.

3.3.2 Operate Manual Face Capture

Capture the target face manually in live view image.

Steps

1. Click **Live View**.
2. Click to start manual face capture.
3. Draw a frame to select the target face in live view image.
   The captured picture can be uploaded to the center.
4. Click the icon again to stop manual face capture.

3.3.3 Overlay and Capture

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

Display VCA Info. on Stream

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

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Target Picture Settings

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

Face Beautification

Check **Face Beautification** and adjust the beautification level as needed.

Note

Face Beautification slightly adjusts skin tone and reduces facial noise.

Background Picture Settings

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

Text Overlay

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

3.3.4 Face Capture Algorithm Parameters

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

Face Capture Version

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

Restore Defaults

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

Capture Parameters

Upload Feature

Feature stands for the feature information the algorithm can tell from face pictures. Check the function to upload the information.

Best Shot

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

Capture Times

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

Capture Threshold

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

Remove Duplicated Faces

This function can filter out repeated captures of certain face.

Note

Remove Duplicated Faces, **Face Picture Comparison**, and **Face Modeling** cannot be turned on simultaneously, and the device can support only one function at a time. The last one you turned on can eventually take effect, and the other two turn off automatically.

Similarity Threshold for Duplicates Removing

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

Duplicates Removing Library Grading Threshold

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

Duplicates Removing Library Update Time

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

Quick Shot

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

Quick Shot Threshold

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

Max. Capture Interval

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

Capture Times

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

Unlimited

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

Limited

The device captures the target face according to the set times.

Face Exposure

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

Reference Brightness

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

exposure level.

Minimum Duration

The extra time the device keeps the face exposure level after the face disappears in the scene.

Face Filtering

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

3.4 Display Alarm

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

Go to **Application Display** → **Display Alarm** to view the real-time images. Click  to go back to **Application Display**.

Note

- To use this function, you should first enable and configure certain smart functions.
- To use this function, your web browser version should be above IE11.0.9600.17843.

Live View

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

Download Display Picture

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

Note

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

Layout

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

Detect Features

Click and choose **Detect Features**. Check the corresponding checkbox to display the features of the detection target.

Chapter 4 PTZ

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

4.1 PTZ Control

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

PTZ Control Panel

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

Note

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

Compatible	The control speed is same as **Keyboard Control**

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

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

Zoom in/out

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

Note

- You can set **Zooming Speed** in **Configuration** → **PTZ** → **Basic Settings**. The higher the value is, the faster the zooming speed is.

You can set **Zoom Limit** in **Configuration** → **Image** → **Display Settings** → **Other** to limit the maximum value of the total zoom (digital zoom and optical zoom).

Focus

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

Iris

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

4.2 Set Preset

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

Steps

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

Note

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

4. Repeat the steps above to set multiple presets.

	Click the button to call the preset.
	Click the button to delete the preset.

Note

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

What to do next

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

4.2.1 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 Auto	105	Call patrol 8
90	Wiper		

4.3 Set Patrol Scan

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

Before You Start

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

Steps

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

Preset

Select predefined preset.

Speed

Set the speed of moving from one preset to another.

Time

It is the duration staying on one patrol point.

	Delete the presets in patrol.
	Adjust the preset order.

Note

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

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

	Call the patrol.
	Stop patroling.
	Delete the patrol.

Note

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

4.3.1 Set One-Touch Patrol

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

Steps

1. Set two or more presets among preset No.1 to preset No.32. For setting presets, refer to ***Set Preset***.
   The device will automatically add presets to patrol path No.8.
2. Choose one of the following methods to enable the function.
   – Click .
   – Call patrol path No.8.

Select and call preset No.45.

4.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

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

Note

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

5. Click to complete one pattern scan path settings.
6. Click to call pattern scan.

	Stop pattern scan.
	Reset pattern scan path.
	Delete the selected pattern scan.

Note

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

4.5 Set Limit

The device can only move within the limited range.

Steps

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

Manual Stops

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

Scan Stops

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

Note

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

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

Note

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

Result

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

4.6 Set Home Position

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

Steps

1. Go to **Configuration** → **PTZ** → **Home 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.

View	The device moves to the set initial position.
Clear	Clear the set initial position.

4.7 Set Park Action

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

Before You Start

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

Steps

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

5. Select an **Action Type ID**, if you select patrol or preset as action type.

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

6. Click **Save**.

4.7.1 Set One-Touch Park

This function is used to start park instantly.

Steps

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

4.8 Set Scheduled Tasks

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

Steps

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

Note

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

4.9 Set Power Off Memory

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

Steps

1. Go to **Configuration** → **PTZ** → **Basic Settings**.

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

4.10 Set PTZ Priority

The function can set the PTZ priority of different signals.

Steps

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

   Network

   The network signal controls the device with priority.

   RS-485

   The RS-485 signal controls the device with priority.

   Delay

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

4.11 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** → **Image** → **Privacy Mask**.
2. Select a channel.
3. Check **Enable**.
4. Adjust the live image to the target scene via PTZ control buttons.
5. Draw the area. Click , and click on the live view image to determine the boundary of the mask.
6. Click **Add**.
   It is listed in **Privacy Mask** list.
7. Edit **Name**, **Type**, and **Active Zoom Ratio** on your demand.

   Active Zoom Ratio

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

Note

Active zoom ratio is only supported for the PTZ channel.

8. Repeat the steps above to set other privacy masks.
9. Click **Save**.

4.12 Set Rapid Focus

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

Steps

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

   Note

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

3. Select the scene to display the calibration line.
   A red line displays on live image.
4. Adjust the length and position of the line by dragging its two endpoints.

   Note

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

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

4.13 Panorama Linkage

This function links panoramic channel with PTZ channel through calibration. The PTZ channel

tracks moving objects in panoramic channel and automatically adjusts its PTZ positions to keep the target in the center of PTZ view for more details.

Note

This function is only supported by certain device models.

4.13.1 Set Panorama Linkage – Auto Calibration

Before You Start

Avoid using auto calibration for vast similar scenes (for example, lake, lawn, or public square) or dark scenes (for example, night scenes).

Steps

1. Go to **Configuration** → **Calibrate** → **Panorama Linkage**.
2. Select the **Calibration Mode** as **Auto**. Click **Start Calibration**.
3. Select a method for auto calibration.

One-touch Calibration	If all scenes in panoramic channel have good stitching effect, it is recommended to use **One-touch Calibration** to calibrate all scenes. Click **One-touch Calibration**. When calibration for all scenes is complete, click **Stop Calibration** to exit.
Single Scene Calibration	If certain scenes in panoramic channel have bad stitching effect, it is recommended to use **Single Scene Calibration** to calibrate these scenes. Select a scene. Use the PTZ control buttons to adjust the close-up view to the same scene in the panorama view. Click **Single Scene Calibration**, and the calibration for the selected scene starts. When the calibration is complete, click **Stop Calibration** to exit. Select another scene and repeat the calibration.

4. Click **Save**.

4.13.2 Set Panorama Linkage – Manual Calibration

Steps

1. Go to **Configuration** → **Calibrate** → **Panorama Linkage**.
2. Select the **Calibration Mode** as **Manual Calibration**. Click **Start Calibration**.
3. Select a scene.
4. Add calibration points.
   1) Select a No. in **Calibration Parameter** list. Click +.
      A numbered green cross displayed on the live image.
   2) Drag the green cross to a certain position.

3) Repeat the steps above to add more calibration points.

Note

- It is recommended to add at least 9 calibration points in one scene. For higher tracking precision, up to 12 calibration points can be added. Calibration points should be distributed evenly in live image, for example, 3 points at far range, middle range, and close range each.
- It is recommended to put calibration points at distinct positions in live image (for example, corners). If no distinct position is available, you can place something (for example, box, stool, or people) to mark the position.

5. Link the PTZ channel to the calibration points in panorama view.
   1) Select a calibration point in panorama view.
   2) Adjust the PTZ channel to set the center of the close-up view at the same position as the calibration point in panorama view by using the PTZ control buttons.
   3) Click to link the current PTZ positions to the calibration point.
   4) Repeat the steps above to link other calibration points.
6. Click **Start Calibration** to finish the calibration for the current scene.
7. When calibration is complete, click **Stop Calibration** to exit.
8. Click **Save**.

4.14 GPS Calibration

GPS calibration is used to map the geographical location to the camera scene so that the device can calculate the real-time geographic information of targets. This function is only supported under certain VCA resource options.

4.14.1 Set GPS Calibration

Before You Start

Choose at least 4 calibration points on the ground in the monitoring scene and measure the precise longitude and latitude of the points. The calibration points should scatter in a 2 × 2 or 3 × 3 array.

Steps

1. Go to **Configuration** → **Calibrate** → **GPS Calibration** → **Calibration**.

Note

The PTZ control is automatically locked to avoid interruption during configuration.

2. Select the longitude and latitude type according to device location.
3. Set calibration points.
   1) Adjust the pan, tilt, and zoom to find the scene with a calibration point.

2) Click and click on the calibration point on the live image.
   The selected point is zoomed in and placed in the center of the image.
3) Click again.
   A green cross shows on the point.
4) Click **Add** and input the precise longitude and latitude of the point.

Note

You must add at least 4 points, otherwise you cannot save the points.

5) Click to save the pan, tilt, and zoom value of the point.
6) Click **Save**.
7) Repeat the steps to set other calibration points.

4.14.2 Verify Calibration

Before You Start

Choose verification points on the ground in the monitoring scene and measure the precise longitude and latitude of the points.

Steps

1. Go to **Configuration** → **Calibrate** → **GPS Calibration** → **Calibration Verification**.

Note

The PTZ control is automatically locked to avoid interruption during configuration.

2. Set verification points.
   1) Adjust the pan, tilt, and zoom to find the scene with a verification point.
   2) Click and click on the verification point on the live image.
      The selected point is zoomed in and placed in the center of the image.
   3) Click again.
      A red cross shows on the point.
   4) Click **Add** and input the precise longitude and latitude of the point.

Note

You must add at least 4 points, otherwise you cannot save the points.

   5) Click **Save**.
   6) Repeat the steps to set other verification points.
      Numbered green and blue rectangles are displayed on the image. The blue rectangle marks the PTZ position of the verification point you set and the green rectangle marks the calculated PTZ position based on the longitude and latitude you input. If the two rectangles are close to each other, then the GPS calibration succeeds.

4.15 Set Device Position

Before You Start

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

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Location**.
2. Select a **PT Mode**.

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

3. Click **Calibrate** to calibrate gyroscope attitude.

Note

Only devices with built-in gyroscope support this function.

4. Select a **Longitude-Latitude Mode** to set the geographic location of the device.

Auto	For device with a built-in positioning module, select **Auto** to automatically obtain the longitude and latitude of the device location.
Manual	Get the device location information in advance, and input the longitude and latitude manually.

5. Click **Save**.

What to do next

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

4.15.1 Set Manual Compass

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

Before You Start

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

Steps

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

4. Click **Set as North**.

Chapter 5 Live View

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

5.1 Live View Parameters

The supported functions vary depending on the model.

Note

For multichannel devices, select the desired channel first before live view settings.

5.1.1 Start and Stop Live View

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

5.1.2 Aspect Ratio

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

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

5.1.3 Live View Stream Type

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

5.1.4 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 or MJPEG.

5.1.5 Start Digital Zoom

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

Steps

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

5.1.6 Conduct Regional Focus

You can enable the function to focus on certain area.

Steps

Note

This function varies with the device model.

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

5.1.7 Conduct Regional Exposure

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

Steps

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

5.1.8 Count Pixel

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

Steps

1. Click  to enable the function.
2. Drag the mouse on the image to select a desired rectangle area.
   The width pixel and height pixel are displayed on the bottom of the live view image.

5.1.9 Light

Click to turn on or turn off the illuminator.

Caution

For the device with laser:

- DO NOT stare at operating light source. May be harmful to the eyes.
- If appropriate shielding or eye protection is not available, turn on the light only at a safe distance or in the area that is not directly exposed to the light.
- When assembling, installing or maintaining the device, DO NOT turn on the light, or wear eye protection.

5.1.10 Operate Wiper

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

Note

Wiper operation and settings vary on device models.

Steps

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

One Time The wiper wipes one time when you click on live view page.

Cycle The wiper works on schedule at set wiping interval. Click on live view to start wiping.

uration

The schedule in which the wiper is ready to work.

nterval

The interval between two successive wiping actions.

Auto

Note

Auto mode is only available for device that supports rain-sensing auto wiper.

In auto mode, the wiper works when rain drops on the window.

5.1.11 Lens Initialization

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

5.1.12 Track Manually

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

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.

5.1.13 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.

5.2 Set Transmission Parameters

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

Steps

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

Protocol

TCP

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

UDP

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

MULTICAST

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

Note

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

HTTP

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

Play Performance

Shortest Delay

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

Balanced

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

Fluent

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

Custom

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

Auto Start Live View

- **Yes** means the live view is started automatically. It requires a high performance monitoring device and a stable network environment.
- **No** means the live view should be started manually.

3. Click **Save**.

Chapter 6 Video and Audio

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

6.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.
Go to setting page: **Configuration** → **Video/Audio** → **Video**.

Note

For device with multiple camera channels, select a channel before other settings.

6.1.1 Stream Type

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

Main Stream

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

Sub Stream

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

Other Streams

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

6.1.2 Video Type

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

Video

Only video content is contained in the stream.

Video & Audio

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

6.1.3 Resolution

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

6.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

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

Variable Bitrate

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

6.1.5 Video Quality

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

6.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).
A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

6.1.7 Video Encoding

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

Note

Available compression standards vary according to device models.

H.264

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

H.264+

H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.
When H.264+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.

Note

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

H.265

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

H.265+

H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.
When H.265+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.

Note

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

MJPEG

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

6.1.8 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.

6.1.9 I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.
In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

6.1.10 SVC

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.
The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.
SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able decode high quality video stream.

6.1.11 Smoothing

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

6.2 Audio Settings

It is a function to set audio parameters such as audio encoding, environment noise filtering.
Go to the audio settings page: **Configuration** → **Video/Audio** → **Audio**.

6.2.1 Audio Input

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

Audio Encoding

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

Audio Input

LineIn is supported for external audio pick-up device.

Input volume

Adjust the volume of the audio input.

6.2.2 Audio Output

The device outputs audio by the built-in speaker. You can adjust the output volume according to your need.

6.2.3 Environmental Noise Filter

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

6.3 Two-way Audio

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

Before You Start

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

Steps

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

6.4 ROI

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in

video compression. The technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

6.4.1 Set ROI

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

Before You Start

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

Steps

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

Note

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

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

Note

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

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

6.5 Target Cropping

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

Steps

1. Go to **Configuration** → **Video/Audio** → **Target Cropping**.
2. Check **Enable**.
3. Select a **Cropping Resolution**.

Cropping Resolution

Cropping resolution is the main stream resolution after target cropping.

A red frame appears in the live view.

4. Drag the frame to the target area.
5. Click **Save**.

Note

- Some models support target cropping. Refer to the actual device for details.
- This function is mutually exclusive with some functions. After enabling target cropping, some functions will fail. Refer to the actual device for details.

6.6 Display Info. on Stream

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

Steps

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

6.7 Display Settings

It offers the parameter settings to adjust image features.

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

For device that supports multiple channels, display settings of each channel is required. The settings for different channels may be different. This part introduces all possible parameters among the channels.

Click **Default** to restore settings.

6.7.1 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.

Note

Day/Night Switch function varies according to models.

Set Supplement Light

Steps

1. Go to **Configuration** → **Maintenance** → **System Service**.
2. Check **Enable Supplement Light**.
3. Click **Save**.
4. Go to **Configuration** → **Image** → **Display Settings** → **Day/Night Switch** to set supplement light parameters.

Smart Supplement Light

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

IR Light Mode

When the mode is set to **Auto**, the supplement light is automatically turned in or off according to the image brightness.

Brightness Limit

Adjust the upper limit of supplement light power.

BLC

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

HLC

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

WDR

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

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

Note

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



Figure 6-1 WDR

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.



Figure 6-2 DNR

White Balance

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



Figure 6-3 White Balance

Defog

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



Defog Off Defog On

Figure 6-4 Defog

EIS

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

6.7.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

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

Set Scheduled-switch

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

Steps

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

> **Note**
>
> For Linked Scene configuration, refer to ***Scene Mode***.

3. Click **Save**.

Set Link to Preset

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

Steps

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

4. Click **Save**.

6.7.3 Mirror

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

Select the mirror mode as needed.

Note

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

6.7.4 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.

6.8 OSD

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

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

Character Set

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

Display

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

Format Settings

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

Text Overlay

Set customized overlay text on image.

Chapter 7 Video Recording and Picture Capture

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

7.1 Storage Settings

This part introduces the configuration of several common storage paths.

7.1.1 Memory Card

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

Set New or Unencrypted Memory Card

Before You Start

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

Steps

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

Note

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

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

Note

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

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

Set Encrypted Memory Card

Before You Start

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

Steps

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

Note

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

3. Verify the encryption password.
   1) Click **Parity**.
   2) Enter the encryption password.
   3) Click **OK**.
   When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.

Note

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

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

Detect Memory Card Status

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

Before You Start

The configuration page only appears when a certain type of memory card is installed to the device.

Steps

1. Go to **Configuration** → **Storage** → **Storage Management** → **Memory Card Detection**.

2. Click **Status Detection** to check the **Remaining Lifespan** and **Health Status** of your memory card.

Remaining Lifespan

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

Health Status

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

Note

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

3. Click **R/W Lock** to set the permission of reading and writing to the memory card.
    1. Add a LockSelect the **Lock Switch** as ON.
    2. Enter the password.
    3. 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.
    1. Remove the LockSelect the **Lock Switch** as OFF.
    2. Enter the password in **Password Settings**.
    3. Click **Save**.

Note

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

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

7.1.2 Set FTP

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

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration** → **Event** → **Alarm Setting** → **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.
3. Optional: Check **Upload Picture** to enable uploading snapshots to the FTP server.

   Picture Filing Interval

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

   Picture Name

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

Note

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

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

7.1.3 Set NAS

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

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration** → **Storage** → **Storage Management** → **Net HDD**.
2. Click **Add**.
3. Set **Mounting Type**.

   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.
4. Set 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.
5. Click **Test** to check whether the network disk is available.
6. Click **OK** to finish the steps to add a Net HDD.
7. Optional: Configure the Net HDD.

Edit	Click to edit the parameter setting.
Delete	Delete the Net HDD. ● Click . ● Select the Net HDD, click **Delete**.

8. Click **Save**.

7.1.4 eMMC Protection

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

Note

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

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

eMMC, short for embedded multimedia card, is an embedded non-volatile memory system. It is

able to store the captured images or videos of the device.

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

7.1.5 Set Cloud Storage

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

Steps

Caution

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

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

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

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

7.2 Video Recording

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

7.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

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

Steps

1. Go to **Configuration** → **Storage** → **Schedule Settings** → **Record Schedule**.
2. Select channel No.
3. Check **Enable**.
4. Select a record type.

Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

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

Alarm

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

Motion | Alarm

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

Motion & Alarm

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

Event

The video is recorded when configured event is detected.

5. Set schedule for the selected record type. Refer to ***Set Arming Schedule*** for the setting operation.

6. Set the advanced recording parameters.

Overwrite

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

Pre-record

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

Post-record

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

Stream Type

Select the stream type for recording.

Note

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

Recording Expiration

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

7. Click **Save**.

7.2.2 Record Manually

Steps

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

7.2.3 Playback and Download Video

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

Steps

1. Go to **Playback** → **Video**.
2. Select channel No.
3. Set search condition and click **Search**.
   The matched video files showed on the timing bar.
4. Click to play the video files.
   – Click to play video files in full screen. Press **ESC** to exit full screen.
   – Click to stop video playback for all channels.

5. Optional: Click to clip video files. Click again to stop clipping video files

Note

Go to **Configuration** → **Local** → **Save clips to**, view and change the saving path of clipped video files.

6. Optional: Click on the playback interface to download files.

Note

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

7.3 Capture Configuration

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

7.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

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

Steps

1. Go to **Configuration** → **Storage** → **Schedule Settings** → **Picture Capture**.
2. Select a channel to set capture parameters.
3. Set capture schedule. Refer to ***Set Arming Schedule*** for configuring schedule time.

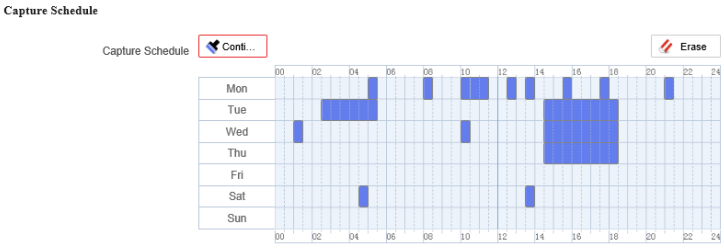


Figure 7-1 Set Capture Schedule

4. Set the capture type.

   Scheduled

   Capture a picture at the configured time interval.

   Event-Triggered

   Capture a picture when an event is triggered.

5. Set the **Format**, **Resolution**, **Quality**, **Interval**, and **Capture Number**.

> **Note**
>
> The resolution of the captured picture is the same as the resolution of the captured picture stream. You can select **Stream Type** in **Advanced**.

6. Click **Save**.

7.3.2 Capture Manually

Steps

1. Go to **Configuration** → **Local**.
2. Set the **Image Format** and saving path to for snapshots.

   JPEG

   The picture size of this format is comparatively small, which is better for network transmission.

   BMP

   The picture is compressed with good quality.

3. Click **Save**.
4. Click near the live view or play back window to capture a picture manually.

7.3.3 View and Download Picture

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

Steps

1. Go to **Playback** → **Picture**.

2. Select channel No.
3. Set search condition and click **Search**.
   The matched pictures showed in the file list.
4. Download the pictures.

   – Select the pictures then click **Download** to download them.
   – Click **Download This Page** to download the pictures of this page.
   – Click **Download All** to download all the pictures.

Note

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

Chapter 8 Event and Alarm

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

8.1 Basic Event

8.1.1 Set Motion Detection

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

Steps

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

Normal Mode

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

Steps

1. Select **Normal Mode** in **Configuration**.
2. Set the **Sensitivity** of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to ***0***, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle. This function allows alarm triggering by specified target types (human and vehicle).

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

4. Click . Click and drag the mouse on the live image, and then right click the mouse to finish drawing one area.
5. Optional: Click to clear all the areas.
6. 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 . Click and drag the mouse on the live image and then release the mouse to finish drawing one area.



Figure 8-1 Set Rules

4. Click to clear all the areas.
5. Click **Save**.
6. Optional: Repeat above steps to set multiple areas.

8.1.2 Set Video Tampering Alarm

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

Steps

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

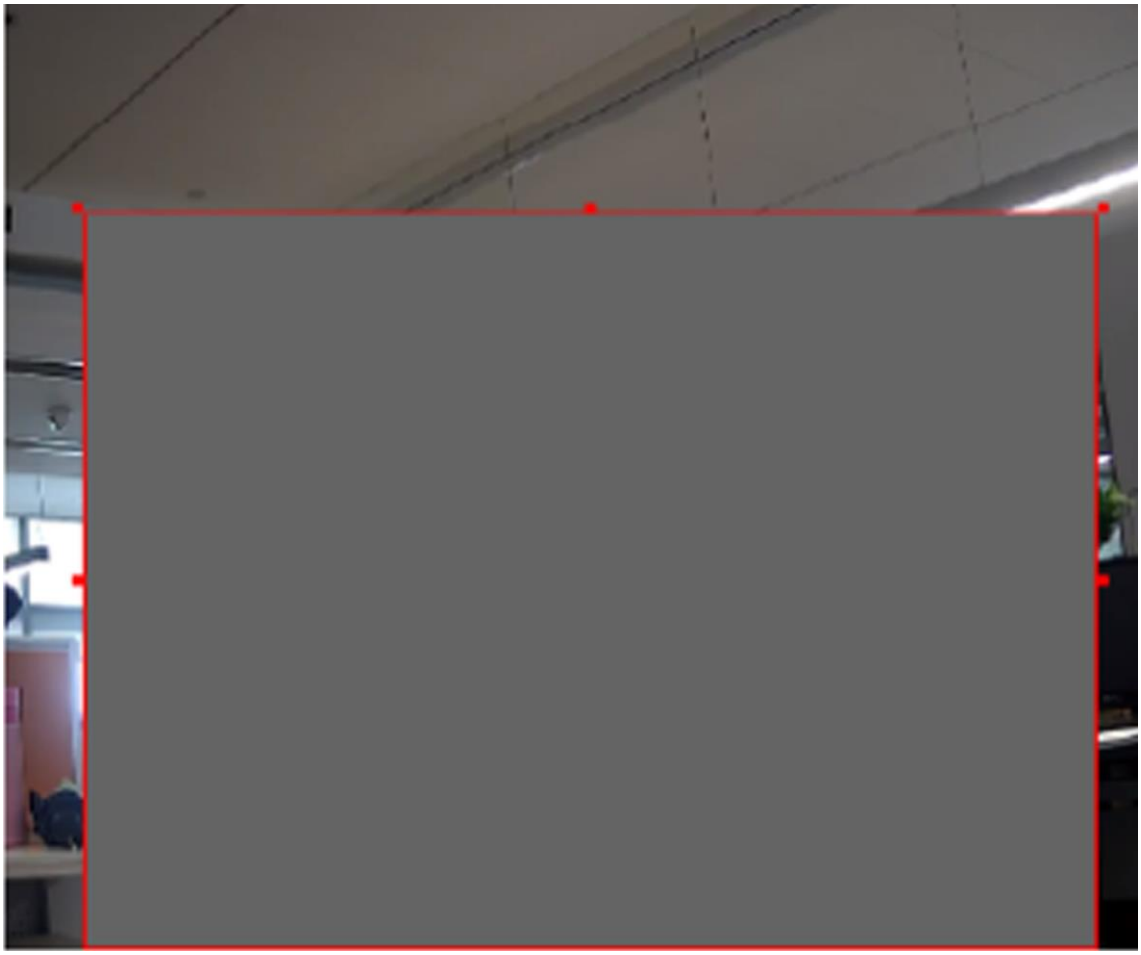


Figure 8-2 Set Video Tampering Area

6. Optional: Click to delete all the drawn areas.
7. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
8. Click **Save**.

8.1.3 Set Alarm Input

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

Before You Start

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** → **Event and Detection** → **Alarm Input**.
2. Select an **Alarm Input NO.** and click to set alarm input.

3. Select **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Check **Enable Alarm Input Handling**.
5. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
6. Click **Copy to...** to copy the settings to other alarm input channels.
7. Click **Save**.

8.1.4 Set Exception Alarm

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

Steps

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

   HDD Full

   The HDD storage is full.

   HDD Error

   Error occurs in HDD.

   Network Disconnected

   The device is offline.

   IP Address Conflicted

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

   Illegal Login

   Incorrect user name or password is entered.

   Abnormal Restart

   The device restarts abnormally.

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

8.1.5 Set Audio Exception Detection

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

Steps

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

   Audio Loss Detection

   Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

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

Note

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

Sudden Decrease of Sound Intensity Detection

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

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

Note

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

8.2 Smart Event

Note

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

8.2.1 Set Intrusion Detection

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

Before You Start

Go to **VCA** → **Select Application** to select Smart Event
, and click **Next** to enable the function.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Intrusion Detection**.

2. Select a channel.
3. Check **Enable**.
4. 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.
5. Adjust the live image to the desired scene by using PTZ control buttons.
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.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.



Figure 8-3 Draw Area

8. Click **Save**.
9. Optional: Click **Add**, and repeat above steps to set other rules.

Note

Up to 4 rules can be set.

10. Set arming schedule. See ***Set Arming Schedule***.
11. Set linkage method. See ***Linkage Method Settings***.

8.2.2 Set Line Crossing Detection

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

Before You Start

Go to **VCA** → **Select Application** to select Smart Event
, and click **Next** to enable the function.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Line Crossing Detection**.
2. Select a channel.
3. Check **Enable**.
4. 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.
5. Adjust the live image to the desired scene by using PTZ control buttons.
6. Draw detection line.
   1) Select a **Line No.**. Up to 4 lines can be set in the scene.
   2) Click .
      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.

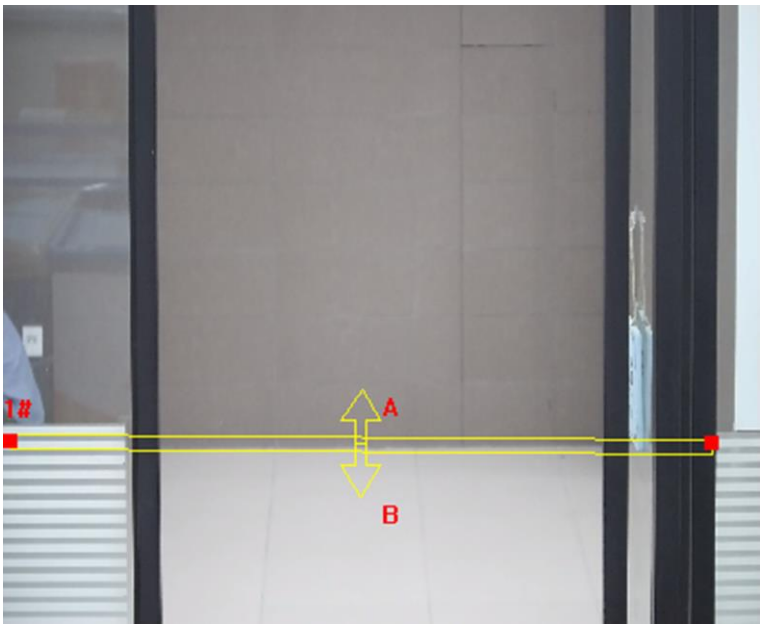


Figure 8-4 Draw Line

7. 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.
8. 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.

9. Click **Save**.
10. Optional: Click **Add**, and repeat above steps to set other rules.

Note

Up to 4 rules can be set.

11. Set arming schedule. See ***Set Arming Schedule***.
12. Set linkage method. See ***Linkage Method Settings***.

8.2.3 Set Region Entrance Detection

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

Before You Start

Go to **VCA** → **Select Application** to select Smart Event
, and click **Next** to enable the function.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Region Entrance Detection**.
2. Select a channel.
3. Check **Enable**.
4. 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.
5. Adjust the live image to the desired scene by using PTZ control buttons.
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 8-5 Draw Area

8. Click **Save**.
9. Optional: Click **Add**, and repeat above steps to set other rules.

Note

Up to 4 rules can be set.

10. Set arming schedule. See ***Set Arming Schedule***.
11. Set linkage method. See ***Linkage Method Settings***.

8.2.4 Set Region Exiting Detection

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

Before You Start

Go to **VCA** → **Select Application** to select Smart Event
, and click **Next** to enable the function.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Region Exiting Detection**.
2. Select a channel.
3. Check **Enable**.
4. 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.

5. Adjust the live image to the desired scene by using PTZ control buttons.
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 8-6 Draw Area

8. Click **Save**.
9. Optional: Click **Add**, and repeat above steps to set other rules.

Note

Up to 4 rules can be set.

10. Set arming schedule. See ***Set Arming Schedule***.
11. Set linkage method. See ***Linkage Method Settings***.

8.2.5 Set Tracking Parameters

The tracking parameters includes the initial tracking position, tracking zoom ratio, tracking duration, and advanced parameters.

Steps

1. Go to **VCA** → **Set Application** → **General Settings** → **Tracking Parameters**.
2. Set the initial tracking position of the PTZ channel.

   When the tracking task stops, the PTZ channel returns to the set initial position.

   1) Adjust the PTZ channel to the desired scene as the initial position.
   2) Click **Set Tracking Initial Position** to save the position.
3. Set the tracking zoom ratio.

Set a fixed zoom ratio	A fixed zoom ratio means the PTZ channel keeps the set zoom value throughout the tracking. Adjust the **Self-adaptive Ratio Coefficient** to ***0***. Adjust the zoom to a desired level. Click **Set Zoom Ratio** to save the zoom level.
Set auto zoom ratio control	The device determines the actual zoom ratio dynamically according to the detected target size and the set **Self-adaptive Ratio Coefficient**. Larger **Self-adaptive Ratio Coefficient** means larger zoomed target during tracking.

4. Set the tracking duration.
   - When you set the **Tracking Duration** as ***0***, the PTZ channel keeps tracking the target until it leaves the view of the panoramic channel.
   - When you set the **Tracking Duration** as a number other than 0, the PTZ channel tracks a target for the set time. The tracking stops when the time is up or when the target leaves the view of the panoramic channel.
5. Click **Save**.
6. Go to **Configuration** → **PTZ** → **Panorama Tracking** → **Advanced**.
7. Optional: Check to enable **Tracking Takeover**.
   When the target leaves the view of the panoramic channel, the PTZ channel takes over the leading role of the task and keeps tracking.
8. Optional: Check to enable **Track in Turn**.
   When multiple targets trigger events in the panoramic channel around the same time, the PTZ channel tracks the targets in turn. If this function is not enabled, the PTZ channel tracks a target until it leaves the view.
9. Click **Save**.

8.2.6 Set Tracking Parameters

Adjust the motion parameters of the device for better target tracking performance.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Advanced Settings**.
2. Optional: Check **Tuning Mode**.

Note

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

3. Set the **Tracking Duration**.

   The device stops tracking when it tracks a target uninterruptedly for the set duration.
4. Set the zooming control and other 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.

   Note

   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 ***Set Device Position*** 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: Click **Default** to restore the smart tracking parameters to default settings.
6. Click **Save**.

Chapter 9 Arming Schedule and Alarm Linkage

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

9.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. Optional: Click **Arming Schedule and Linkage Method** in the related event interface.
2. Click **Modify** behind **Arming Schedule**.
3. Click **Draw**, and drag the time bar to draw desired valid time.

Note

- Each cell represents 30 minutes.
- Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
- Up to 8 periods can be configured for one day.

4. Click **Erase**, and drag the time bar to clear selected valid time.
5. Click **OK** to save the settings.

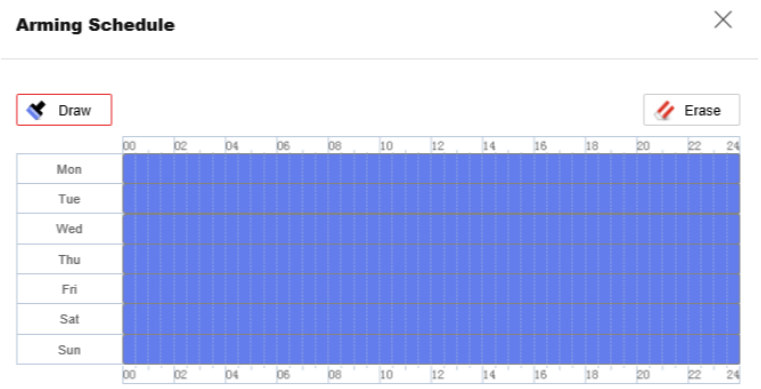


Figure 9-1 Set Arming Schedule

9.2 Linkage Method Settings

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

9.2.1 Trigger Alarm Output

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

Steps

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

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

Automatic Alarm

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

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click ✎ to set alarm parameters.

   Alarm Name

   Custom a name for the alarm output.

   Delay

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

Manual Alarm

You can trigger an alarm output manually.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click to set alarm parameters.

   Alarm Name

   Custom a name for the alarm output.
2. Click **Manual Alarm** to enable manual alarm output.
3. Optional: Click **Clear Alarm** to disable manual alarm output.

9.2.2 FTP/NAS/Memory Card Uploading

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

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

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

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

9.2.3 Send Email

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

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

Set Email

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

Before You Start

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

Steps

1. Go to email settings page: **Configuration** → **Network** → **Advanced Settings** → **Email**.
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) Optional: If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.

3) Set the **E-mail Encryption**.
   - When you select **SSL** or **TLS**, and disable STARTTLS, emails are sent after encrypted by SSL or TLS. The SMTP port should be set as 465.
   - When you select **SSL** or **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

   Note

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

4) Optional: If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has a certain number of attached alarm pictures about the event with configurable image capturing interval.

   Note

   The number of alarm pictures may vary according to different device models and different events.

5) Input the receiver's information, including the receiver's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

9.2.4 Notify Surveillance Center

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

9.2.5 Smart Tracking

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

Note

This function is only supported by certain models.

9.2.6 Trigger Recording

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

For device with more than one camera channels, you can set one or more channels to take

recordings if needed.

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

9.2.7 Audible Warning

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

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

Note

The function is only supported by certain camera models.

Set Audible Alarm Output

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

Steps

1. Go to **Configuration** → **Event** → **Alarm Setting** → **Audible Alarm Output**.
2. Select **Sound Type** and set related parameters.
   - Select **Prompt** and set the alarm times you need.
   - Select **Warning** and its contents. Set the alarm times you need.
   - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Set** → **Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
3. Optional: Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See ***Set Arming Schedule*** for details.
5. Click **Save**.

Note

The function is only supported by certain device models.

Set Alarm Server

Steps

1. Go to **Configuration** → **Event** → **Alarm Setting** → **Alarm Server**.
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol**.

Note

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

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

9.2.8 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.

Set Alarm Server

Steps

1. Go to **Configuration** → **Event** → **Alarm Setting** → **Alarm Server**.
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol**.

Note

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

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

Chapter 10 Network Settings

10.1 TCP/IP

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

Go to **Configuration** → **Network** → **Network 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 IP PORTAL to get the device IP address.

Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.
The valid value range of MTU is 1280 to 1500.

DNS

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

Domain Name Settings

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

Note

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

10.2 Port Mapping

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

Steps

1. Go to **Configuration** → **Network** → **Network Service** → **NAT**.
2. Select the port mapping mode.

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

3. Click **Save**.

10.2.1 Set Auto Port Mapping

Steps

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

Note

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

10.2.2 Set Manual Port Mapping

Steps

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

What to do next

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

10.2.3 Set Port Mapping on Router

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

Steps

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

Example

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

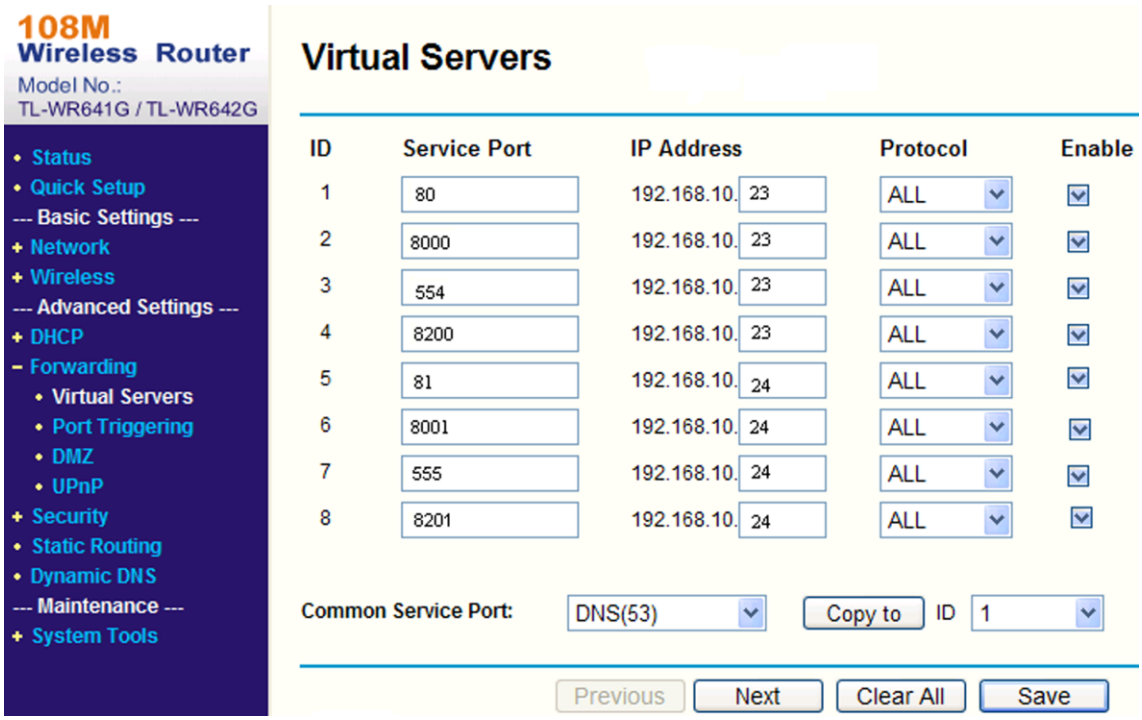


Figure 10-1 Port Mapping on Router

Note

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

10.3 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 **Configuration** → **Network** → **Network Settings** → **SNMP**.
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.

Note

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

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

10.4 Access to Device via Domain Name

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

Before You Start

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

Steps

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

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

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

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

10.5 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** → **Network Settings** → **PPPoE**.
2. Check **Enable**.
3. Set the PPPoE parameters.

   Dynamic IP

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

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

   Confirm

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

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

Note

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

10.6 Accessing via Mobile Client

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

Note

Guarding Vision service should be supported by the camera.

10.6.1 Enable Guarding Vision Service on Camera

Guarding Vision service should be enabled on your camera before using the service.

You can enable the service through IP PORTAL software or Web browser.

Enable Guarding Vision Service via Web Browser

Follow the following steps to enable Guarding Vision 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 Guarding Vision as the **Platform Access Mode**.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. Create a verification code or change the old verification code for the camera.

   Note

   The verification code is required when you add the camera to Guarding Vision service.

7. Save the settings.

Enable Guarding Vision Service via IP PORTAL Software

This part introduce how to enable Guarding Vision service via IP PORTAL software of an activated camera.

Steps

1. Run IP PORTAL software.

2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Guarding Vision**.
4. Create a verification code or change the old verification code.

Note

The verification code is required when you add the camera to Guarding Vision service.

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

10.6.2 Set Up Guarding Vision

Steps

1. Get and install Guarding Vision application by searching "Guarding Vision" in App Store or Google Play(TM).
2. Start the application and register for a Guarding Vision user account.
3. Log in after registration.

10.6.3 Add Camera to Guarding Vision

Steps

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

Note

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

5. Input the verification code of your camera.

Note

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

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

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

Note

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

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

   For detailed information, refer to the user manual of the Guarding Vision app.

10.7 HTTP(S)

HTTP is an application-layer protocol for transmitting hypermedia documents. 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** → **Network Service** → **HTTP(S)**.
2. Enter **HTTP Port**.

Note

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.

3. Check **Enable** in **HTTPS**.

Note

You can click **TLS Settings** to set the TLS version that the device supports. Refer to for details.

4. Enter **HTTPS Port**.
5. Optional: Check **HTTPS Browsing** to access the device only via HTTPS protocol.
6. Select **Server Certificate**.
7. Set **Web Authentication**.

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.

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.

8. Click **Save**.

10.8 Multicast

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

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

IP Address

It stands for the address of multicast host.

10.8.1 Multicast Discovery

Go to **Configuration** → **Network** → **Network Settings** → **TCP/IP** to enable this function.

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

10.9 RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

Steps

1. Go to **Configuration** → **Network** → **Network Service** → **RTSP**.
2. Enter **Port**.
3. Set **Multicast** parameters.

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.

4. Set **RTSP Authentication**.

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.

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.

5. Click **Save**.

10.10 Set SRTP

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

Steps

1. Go to **Configuration** → **Network** → **Network Service** → **SRTP**.
2. Enter the **Port** number.
3. Set **Multicast** parameters.

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.

4. Select **Server Certificate**.
5. Select **Encrypted Algorithm**.
6. Click **Save**.

Note

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

10.10.1 Multicast

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

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

IP Address

It stands for the address of multicast host.

10.10.2 Multicast Discovery

Go to **Configuration** → **Network** → **Network Settings** → **TCP/IP** to enable this function.

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

10.11 Bonjour

It is an implementation of zero-configuration networking (zeroconf), a group of technologies that includes service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

Go to **Configuration** → **Network** → **Network Service** → **Bonjour** to enable the function, and click **Save**.

After enabling the function, the device spread and receive service information in local area network.

10.12 WebSocket(s)

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.

Go to **Configuration** → **Network** → **Network Service** → **WebSocket(s)** to set parameters, and click **Save**.

WebSocket

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

WebSockets

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

10.13 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.

10.14 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.

10.15 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** → **Platform Access** → **ISUP**.
2. Optional: Select an access center.
3. Check **Enable**.
4. Select a protocol version and enter related parameters.
5. Click **Save**.
   Register status turns to **Online** when the function is correctly set.

10.16 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** → **Platform Access** → **Open Network Video Interface**.
2. Check **Enable**.
3. Select an authentication mode.
   – If you select **Digest**, the device only supports digest authentication.
   – If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication.
4. Click **Add** to configure the Open Network Video Interface user.
5. Click **Save**.
6. Optional: Repeat the steps above to add more Open Network Video Interface users.

7. Optional: Manage the user.
   – Click to delete the selected Open Network Video Interface user.
   – Click to modify the selected Open Network Video Interface user.

10.17 Set SDK Service

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

Steps

1. Go to **Configuration** → **Network** → **Platform Access** → **SDK Service**.
2. Set **SDK Service** parameters.
   1) Check **Enable** to add the device to the client software with SDK protocol.
   2) Enter the **Port** number.
3. Set **Enhanced SDK Service** parameters.
   1) Check **Enable** to add the device to the client software with SDK over TLS protocol.
   2) Optional: Click **TLS Settings** to enable the TLS version that the device supports. Refer to ***TLS*** for details.
   3) Enter the **Port** number.
   4) Select a server certificate to make sure the data transmission security. You can click **Certificate Management** to add a certificate. Refer to ***Certificate Management*** for details.
4. Click **Save**.

Chapter 11 System and Security

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

11.1 View Device Information

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

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

11.2 Restart

You can restart the device via browser.

Go to **Maintenance and Security** → **Maintenance** → **Restart**, and click **Restart**.

11.3 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 **Maintenance and Security** → **Maintenance** → **Upgrade**.
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 🗀 to select the upgrade file.
4. Click **Upgrade**.

11.4 Restore and Default

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

Steps

1. Go to **Maintenance and Security** → **Maintenance** → **Backup and Restore**.
2. Click **Restore** or **Default** according to your needs.

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

Note

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

11.5 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

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

11.6 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 **Maintenance and Security** → **Maintenance** → **Backup and Restore** → **Backup**.
   2) Click **Export** 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) Go to **Maintenance and Security** → **Maintenance** → **Backup and Restore** → **Reset**.
   3) Click 🗀 to select the saved configuration file.
   4) Input the encryption password you have set when exporting the configuration file.

5) Click **Import**.

11.7 Export Diagnose Information

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

Go to **Maintenance and Security** → **Maintenance** → **Device Debugging** → **Diagnose Information**. Click **Export**. In the pop-up window, check desired diagnose information and click **Export** to export corresponding diagnose information of the device.

11.8 Search and Export Data Aware Information

The data aware function is used to search and export the data of the restart, arming and capture alarm statistics.

Before You Start

Log in to the device via admin user account.

Steps

1. Go to **Application Display** → **Data Aware**.
2. Select the search condition.

Statistics Type	Options
Restart Records	Type of rebooting, start time and end time.
Arming	Arming type, start time and end time.
Capture Alarm Statistics	Report type, alarm target, protocol, arming IP address and start time.
Alarm Quality Statistics	Report type, alarm target and start time.

3. Click **Search**.
   The data information that match the conditions will be displayed.
4. Optional: Click **Export** to save the data information to the local device.

11.9 View Open Source Software License

On the top-right corner, click ⓘ and select **Open Source Software Description** to download the license. You can view the license in the editor.

11.10 Set Live View Connection

It controls the remote live view connection amount.

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

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

11.11 Time and Date

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

11.11.1 Synchronize Time Manually

Steps

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

Click **Sync. with computer time** to synchronize the time of the device with that of the local PC.

5. Click **Save**.

11.11.2 Synchronize Time by Satellite

Note

This function varies depending on different devices.

Steps

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

4. Click **Save**.

11.11.3 Set NTP Server

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

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

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

Note

Server Address is NTP server IP address.

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

11.11.4 Set DST

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

Steps

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

11.12 Set RS-485

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

Before You Start

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

Steps

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

Note

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

3. Click **Save**.

11.13 Security

You can improve system security by setting security parameters.

11.13.1 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 **Maintenance and Security** → **Security** → **IP Address Filter**.
2. Check **Enable**.
3. Select the type of IP address filter.

Blocklist	IP addresses in the list cannot access the device.
Allowlist	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 the selected IP address or IP address range in the list.
	Delete the selected IP address or IP address range in the list.

5. Click **Save**.

11.13.2 Set MAC Address Filter

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

Steps

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

Blocklist	MAC addresses in the list cannot access the device.

Allowlist	Only MAC addresses in the list can access the device.

4. Edit the MAC address filter list.

Add	Add a new MAC address to the list.
	Modify the selected MAC address in the list.
	Delete the selected MAC address in the list.

5. Click **Save**.

11.13.3 Security Audit Log

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

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

Search Security Audit Logs

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

Steps

Note

This function is only supported by certain camera models.

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

Set Log Server

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

Before You Start

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

Steps

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

11.13.4 Set QoS

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

Note

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

Steps

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

   Note

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

3. Click **Save**.

11.13.5 Set IEEE 802.1X

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

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

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

Note

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

11.13.6 SSH

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

Go to **Maintenance and Security** → **Maintenance** → **Device Debugging**, and click **Settings** of **SSH**. You can edit the number of the port. Click **Save**.

Caution

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

11.13.7 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 **Maintenance and Security** → **Security** → **Login Management** → **Control Timeout Settings** to complete settings.

11.13.8 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.

Note

The function is only supported by certain device models.

Server Certificate/Client Certificate

Note

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

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security** → **Security** → **Certificate Management**.

2. Click **Create Self-signed Certificate**.
3. Input certificate information.

Note

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

4. Click **Save** 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 **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 **Maintenance and Security** → **Security** → **Certificate Management**.
2. Select a self-signed certificate from the **Server/Client Certificate** list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **Save**.
   The certificate request details are displayed in a pop-up window.
6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
   1) Click **Import**.
   2) Input **Certificate ID**.

   Note

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

   3) Click to select the certificate file.
   4) Select **Self-signed Request Certificate**.
   5) Click **Save**.
   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 **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 **Maintenance and Security** → **Security** → **Certificate Management**.
2. Click **Import**in the **Server/Client Certificate** list.
3. Input **Certificate ID**.

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

4. Click 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 an 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 **Save**.
   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 **Maintenance and Security** → **Security** → **Certificate Management**.
2. Click **Import** in the **CA Certificate** list.
3. Input **Certificate ID**.

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

4. Click to select the certificate file.
5. Click **Save**.
   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)**.

Note

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

3. Click **Save**.

11.13.9 TLS

The Transport Layer Security (TLS) protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. TLS settings are effective for HTTP(S) and enhanced SDK service.

Go to **Maintenance and Security** → **Security** → **TLS**, and enable the desired TLS protocol. Click **Save**.

Caution

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

11.13.10 User and Account

Set User Account and Permission

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

Caution

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

Steps

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

   Administrator

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

   User

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

   Operator

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

Modify	Select a user and click ✎ to change the password and permission.
Delete	Select a user and click 🗑.

Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

Online Users

The information of users logging into the device is shown.

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

Simultaneous Login

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

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

