



Auto Tracking PTZ Camera

User Manual

Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

Contents

Chapter 1 Overview.....	1
1.1 Product Introduction	1
1.2 Key Function	1
Chapter 2 Device Activation and Accessing	1
2.1 Activate Device	1
2.1.1 Activate Device via Web Browser	1
2.1.2 Activate via SADP	2
2.2 Access Device via Web Browser	3
2.2.1 Plug-in Installation	4
2.2.2 Admin Password Recovery	5
2.2.3 Illegal Login Lock.....	5
Chapter 3 PTZ.....	6
3.1 PTZ Control	6
3.2 Set Preset	8
3.2.1 Special Presets	9
3.3 Set Patrol Scan	9
3.3.1 Set One-Touch Patrol	10
3.4 Set Pattern Scan	11
3.5 Set Power Off Memory	11
3.6 Set Sound Source Localization	11
Chapter 4 Live View.....	12
4.1 Live View Parameters.....	12
4.1.1 Start and Stop Live View	12
4.1.2 Aspect Ratio.....	12
4.1.3 Live View Stream Type	12
4.1.4 Select the Third-Party Plug-in	12
4.1.5 Start Digital Zoom	13
4.1.6 Conduct Regional Focus	13
4.1.7 Count Pixel.....	13

4.1.8 Lens Initialization	13
4.1.9 Track Manually	14
4.2 Set Transmission Parameters	14
4.3 Display Target Information	15
Chapter 5 Video and Audio.....	1
5.1 Video Settings.....	1
5.1.1 Stream Type.....	1
5.1.2 Video Type	1
5.1.3 Resolution.....	1
5.1.4 Bitrate Type and Max. Bitrate	2
5.1.5 Video Quality	2
5.1.6 Frame Rate	2
5.1.7 Video Encoding.....	2
5.1.8 Profile.....	3
5.1.9 I-Frame Interval	3
5.1.10 SVC	4
5.1.11 Smoothing	4
5.2 Audio Settings.....	4
5.2.1 Audio Input.....	4
5.2.2 Audio Output	5
5.2.3 Environmental Noise Filter	5
5.3 Two-way Audio.....	5
5.4 ROI.....	5
5.4.1 Set ROI	5
5.5 Display Settings	6
5.5.1 Scene Mode	6
5.5.2 Image Parameters Switch	9
5.5.3 Mirror.....	10
5.5.4 Video Standard	10
5.5.5 Local Video Output.....	10
5.6 Set Privacy Mask.....	11

Chapter 6 Network Settings.....	11
6.1 TCP/IP	11
6.2 Port Mapping.....	13
6.2.1 Set Auto Port Mapping.....	13
6.2.2 Set Manual Port Mapping.....	13
6.2.3 Set Port Mapping on Router	13
6.3 SNMP	14
6.4 Access to Device via Domain Name.....	15
6.5 Access to Device via PPPoE Dial Up Connection	16
6.6 HTTP(S).....	17
6.7 Multicast	17
6.7.1 Multicast Discovery	18
6.8 RTSP	18
6.9 Set SRTP	19
6.9.1 Multicast	19
6.9.2 Multicast Discovery	20
6.10 Bonjour	20
6.11 WebSocket(s).....	20
6.12 TCP Acceleration.....	20
6.13 Traffic Shaping	21
6.14 Set SDK Service	21
6.15 Set ONVIF.....	21
Chapter 7 System and Security	23
7.1 View Device Information	23
7.2 Reboot.....	23
7.3 Upgrade	23
7.4 Restore and Default	24
7.5 Search and Manage Log	24
7.6 Import and Export Configuration File.....	24
7.7 Export Diagnose Information.....	25
7.8 Search and Export Data Aware Information	25

7.9 View Open Source Software License	25
7.10 Set Live View Connection.....	26
7.11 Time and Date	26
7.11.1 Synchronize Time Manually	26
7.11.2 Synchronize Time by Satellite.....	26
7.11.3 Set NTP Server	27
7.11.4 Set DST	27
7.12 Set RS-485.....	27
7.13 Security	28
7.13.1 Set IP Address Filter	28
7.13.2 Set MAC Address Filter	28
7.13.3 Security Audit Log	29
7.13.4 Set QoS.....	30
7.13.5 Set IEEE 802.1X	30
7.13.6 SSH	31
7.13.7 Control Timeout Settings	31
7.13.8 Certificate Management	31
7.13.9 TLS	34
7.13.10 User and Account	34

Chapter 1 Overview

1.1 Product Introduction

The PTZ camera is an integration of HD camera, PTZ motion control module, and it is ideal for remote monitoring. The device has basic PTZ functions, such as presets, scans, and target tracking.

1.2 Key Function

You can quickly learn how to use the camera by the key functions.



Note

Actual functions may vary for different models.

PTZ

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

Chapter 2 Device Activation and Accessing

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



Note

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

2.1 Activate Device

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

2.1.1 Activate Device via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use

SADP software or PC client to activate the device.

Before You Start

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

Steps

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

The default IP address of the device is 192.168.1.64.

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



Caution

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

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

2.1.2 Activate via SADP

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

Before You Start

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

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

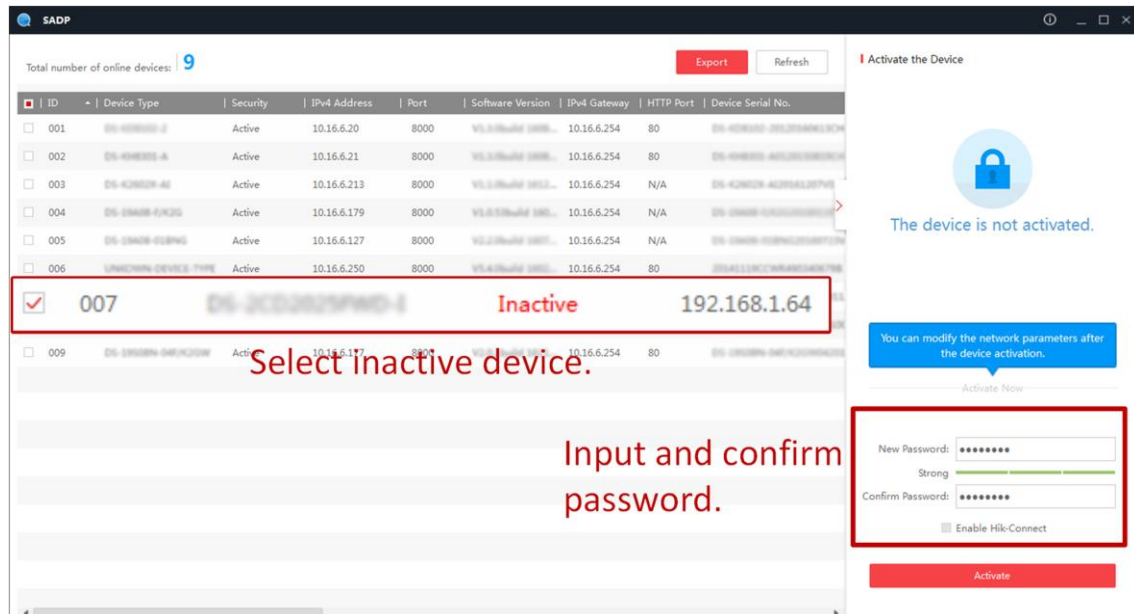
Steps

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

Caution

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

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



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

5. Modify IP address of the device.

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

2.2 Access Device via Web Browser

Before You Start

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

Steps

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

 Note

Illegal login lock is activated by default. If admin user performs seven failed password attempts (five attempts for user/operator), the IP address is blocked for 30 minutes.

If illegal login lock is not needed, go to **Configuration** → **System** → **Security** → **Security Service** to turn it off.

4. Click **Login**.

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

For IE based web browser, webcomponents and QuickTime^(TM) are optional. For non-IE based web browser, webcomponents, QuickTime^(TM), VLC and MJPEG 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	- 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 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 **Maintenance and Security → Security → Login Management**, and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

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

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 PTZ

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

3.1 PTZ Control

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

PTZ Control Panel

	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 camera 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.

3.2 Set Preset

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

Steps

1. Click  to show the setting panel, and click .
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.

3.2.1 Special Presets

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

Preset No.	Function	Preset No.	Function
33	Auto flip	92	Set manual limits
34	Back to origin	93	Save manual limits
35	Call patrol 1	94	Remote reboot
36	Call patrol 2	95	Call OSD menu
37	Call patrol 3	96	Stop a scan
38	Call patrol 4	97	Start random scan
39	Day mode	98	Start frame scan
40	Night mode	99	Start auto scan
41	Call pattern 1	100	Start tilt scan
42	Call pattern 2	101	Start panorama scan
43	Call pattern 3	102	Call patrol 5
44	Call pattern 4	103	Call patrol 6
45	One-touch patrol	104	Call patrol 7
46	Day/Night Auto	105	Call patrol 8
90	Wiper		

3.3 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 patrolling.



Delete the patrol.

Note

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

3.3.1 Set One-Touch Patrol

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

Steps

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.

3.4 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**.

3.5 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**.

3.6 Set Sound Source Localization

When you enable the function, the lens can follow the target which makes continuous sound.

 Note

Sound source localization and human body following cannot be enabled at the same time. Please disable human body following first.

Chapter 4 Live View

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

4.1 Live View Parameters

The supported functions vary depending on the model.

4.1.1 Start and Stop Live View

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

4.1.2 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.

4.1.3 Live View Stream Type

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

4.1.4 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.

4.1.5 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.

4.1.6 Conduct Regional Focus

You can enable the function to focus on certain area.

Steps



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.

4.1.7 Count Pixel

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

Steps

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

4.1.8 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.

4.1.9 Track Manually

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



The function may not be supported by certain device models.

Steps

1. Click  on the toolbar of the live view page.
2. Click a moving object in the live image.
The device tracks the target and keeps it in the center of live view image.

4.2 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.



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 real-time. In poor network environment, the device cannot ensure 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 not display.

3. Click **Save**.

4.3 Display Target Information

You can display target information on the live view image and view the target and its motion.

Steps

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

Rules

You can enable or disable the rules of dynamic analysis for motion here.

Display POS Info

Enable the function, feature information of the detected target is dynamically displayed near the target in the live image.

Display Rules Info on Capture

When this function is enabled, rules information is overlaid on the manually captured pictures.

Chapter 5 Video and Audio

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

5.1 Video Settings

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

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

5.1.1 Stream Type

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

Main Stream

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

Sub Stream

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

Other Streams

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

5.1.2 Video Type

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

Video Stream

Only video content is contained in the stream.

Video&Audio

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

5.1.3 Resolution

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

and storage.

5.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

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

Variable Bitrate

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

5.1.5 Video Quality

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

5.1.6 Frame Rate

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

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

5.1.7 Video Encoding

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



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.

5.1.8 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.

5.1.9 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

5.1.10 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 to decode high quality video stream.

5.1.11 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.

5.2 Audio Settings

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

5.2.1 Audio Input

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

Audio Encoding

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

Audio Input

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



Note

MicIn is only supported by certain models.

Input Volume

Adjust the volume of the audio input.

Environmental Noise Filter

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

5.2.2 Audio Output

You can output audio through line out. You can adjust the output volume according to your needs.

Note

- Connect audio output device according to your needs.
 - This function is only supported by certain models.
-

5.2.3 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.

5.3 Two-way Audio

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

Before You Start

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

Steps

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

5.4 ROI

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

5.4.1 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resource to the region of interest,

thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

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

Steps

1. Go to **Configuration** → **Video/Audio** → **ROI**.
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** and click  to draw ROI region on the live view.

Note

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

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

Note

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

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

5.5 Display Settings

It offers the parameter settings to adjust image features.

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

Click **Default** to restore settings.

5.5.1 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.

Compatible

This mode is only recommended for indoor devices with a bubble when you cannot get a clear image with other options.

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.

BLC

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

HLC

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

WDR

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

When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the

whole image and provides clear images with more details.

Note

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

DNR

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

Normal

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

Expert

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

White Balance

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

Defog

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

5.5.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

Go to image parameters switch setting page: **Configuration** → **Image** → **Display Settings** → **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.



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**.

5.5.3 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.



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

5.5.4 Video Standard

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

5.5.5 Local Video Output

If the device is equipped with video output interfaces, such as BNC, CVBS, HDMI, and SDI, you can preview the live image directly by connecting the device to a monitor screen.

Select the output mode as ON/OFF to control the output.

5.6 Set Privacy Mask

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

Steps

1. Go to **Configuration** → **Image** → **Privacy Mask**.
2. Check **Enable**.
3. Click . Drag the mouse in the live view to draw a closed area.

Drag the corners of the area Adjust the size of the area.

Drag the area Adjust the position of the area.

Click  Clear all the areas you set.

4. Click **Add** to add a privacy mask and set **Region Name** and **Mask Type**.
5. Click **Save**.

Chapter 6 Network Settings

6.1 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 SADP to get the device IP address.



Note

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

Manual

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

IPv6

Three IPv6 modes are available.

Route Advertisement

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

Note

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

DHCP

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

Manual

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

MTU

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

The valid value range of MTU is 1280 to 1500.

DNS

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

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.

6.2 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**.

6.2.1 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**.



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

6.2.2 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.

6.2.3 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 Servers**, and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

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

108M Wireless Router
Model No.: TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- + Network
- + Wireless
- Advanced Settings ---
- + DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- + Security
 - Static Routing
 - Dynamic DNS
- Maintenance ---
- + System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☒
2	8000	192.168.10.23	ALL	☒
3	554	192.168.10.23	ALL	☒
4	8200	192.168.10.23	ALL	☒
5	81	192.168.10.24	ALL	☒
6	8001	192.168.10.24	ALL	☒
7	555	192.168.10.24	ALL	☒
8	8201	192.168.10.24	ALL	☒

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

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.

6.3 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**.

6.4 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.

6.5 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.

6.6 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**.

6.7 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.

6.7.1 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.

6.8 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**.

6.9 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**.



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

6.9.1 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.

6.9.2 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.

6.10 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.

6.11 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.

6.12 TCP Acceleration

TCP acceleration is used to improve latency and reduce packet loss caused by network congestion

in poor network condition, and guarantee the fluency of live view.

6.13 Traffic Shaping

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

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

6.14 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**.

6.15 Set ONVIF

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

Steps

1. Go to **Configuration** → **Network** → **Platform Access** → **ONVIF**.
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 ONVIF user.
5. Click **Save**.
6. Optional: Repeat the steps above to add more ONVIF users.

7. Optional: Manage the user.

- Click  to delete the selected ONVIF user.
- Click  to modify the selected ONVIF user.

Chapter 7 System and Security

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

7.1 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.

7.2 Reboot

You can reboot the device via browser.

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

7.3 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**.

7.4 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.

7.5 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.

7.6 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**.

7.7 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.

7.8 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.

7.9 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.

7.10 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.

7.11 Time and Date

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

7.11.1 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**.

7.11.2 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**.

7.11.3 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**.



Server Address is NTP server IP address.

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

7.11.4 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**.

7.12 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.



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

3. Click **Save**.

7.13 Security

You can improve system security by setting security parameters.

7.13.1 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**.

7.13.2 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**.

7.13.3 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



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**.

7.13.4 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**.

7.13.5 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**.

7.13.6 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.

7.13.7 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.

7.13.8 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.

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**.

7.13.9 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.

7.13.10 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**.



See Far, Go Further