

IP Camera

User Manual

Table of Contents

1. Overview.....	6
1.1.Scope of Application	6
1.2.Product Description.....	7
1.3.Operational Environment	7
2. Device Connection	8
2.1.Connecting to PC	8
2.2.Connection via router/switch	8
3. Setting the IP Address of an IPC using Risco Search Tool	9
4. Login from Web Client.....	10
4.1.Accessing Camera from Web Client.....	10
4.2.Login for the First Time.....	10
4.3.General Login.....	13
4.4.Recover Password.....	13
4.4.1.Security Question Configuration.....	14
4.4.2.Certificate of Authorization	15
4.4.3.Super Code.....	15
4.5.Password Expire.....	16
5. Installing Plug-in	17
6. Preview screen.....	18
6.1.Live menu	18
6.2.Video Status.....	20
7. Playback	21
7.1.General playback.....	21
7.2.Image Search.....	23
7.3.Playback by Tag.....	24
7.4.Smart.....	24
7.5. AI	26
7.5.1.License Plate Detection Search	26
7.5.2.Pedestrian and Vehicle Search	27
7.5.3.Line Crossing.....	28
7.5.4.Instrusion Detection.....	29
7.5.5.Region Entrance.....	29
7.5.6.Region Exiting.....	30
8. Remote Settings.....	32
8.1.Preview	32
8.2.Image Control.....	33
8.3.Video Cover.....	36
8.4.Video Parameters.....	37
8.4.1.Recording Parameters	37
8.4.2.Coding Parameters.....	37

8.4.3.Audio Management.....	39
8.5.Capture Settings.....	41
8.6.Schedule Setup.....	41
8.6.1.Record Schedule.....	41
8.6.2.Capture Schedule.....	44
8.7.Disk Management.....	45
8.8.FTP server settings.....	46
8.9.I/O Settings	48
8.9.1.Alarm input settings.....	48
8.9.2.Alarm Output Settings.....	50
8.10.Deterrence Settings.....	51
8.11.Siren Settings.....	52
8.12.Disaming.....	53
8.13.Event Settings.....	54
8.13.1. Face Detection.....	54
8.13.2. Pedestrian and Vehicle.....	58
8.13.3. License Plate.....	60
8.13.4. Line Crossing.....	62
8.13.5. Intrusion.....	63
8.13.6. Enter Region.....	65
8.13.7. Exit Region.....	67
8.13.8. Object Detection	69
8.13.9. Cross Counting	70
8.13.10. Heat Map.....	71
8.13.11. Queue Length.....	72
8.13.12. Crowd Density.....	74
8.13.13. Rare Sound.....	76
8.13.14. Motion Detection.....	76
8.13.15. Video Tampering.....	77
8.13.16. Event Schedule.....	78
8.13.17. Alarm linkage settings.....	79
8.14.List Management.....	80
8.14.1. License plate recognition.....	80
8.15.Statistics.....	83
8.15.1. Pedestrian & Vehicle.....	84
8.15.2. Cross Counting	85
8.15.3. Heat Map.....	86
8.16.Network Settings.....	87
8.16.1. General Settings.....	88
8.16.2. PPPoE	89
8.16.3. SNMP	90
8.16.4. IEEE802.1X.....	91
8.16.5. Port Settings.....	92
8.17.Cloud Service Setup.....	93
8.18.Mail Settings.....	93
8.18.1. Parameter settings.....	93
8.18.2. Schedule Setup.....	95
8.19.RTSP Protocol Settings	95

8.20.Dynamic Domain Name Settings.....	96
8.21.HTTPS protocol settings.....	97
8.22.IP Filter.....	98
8.23.Platform Access	99
8.23.1. RTMP	99
8.23.2. Event Push Platform	99
8.24.General system setup	102
8.24.1. Date and time	102
8.24.2. Daylight Saving Time.....	103
8.25.Multi-user management.....	104
8.26.Maintenance	106
8.26.1. Log Management.....	106
8.26.2. Restoring factory settings	108
8.26.3. System upgrades	108
8.26.4. Parameter management.....	110
8.26.5. Auto Maintenance.....	110
8.26.6. Developer Mode.....	111
8.27.System Information.....	112
8.27.1. Device information	112
9. Local settings	113
Standard Limited Product Warranty (“Limited Warranty”)	114
Contacting RISCO Group	116

Statement

Thanks for using our series of IP cameras that are integrated IP cameras developed for network video surveillance, including IP box camera, bullet camera, dome camera, PTZ cameras, etc. A powerful SoC (System on a Chip) is used as the media processor to automate audio and video acquisition, compression, and transmission. The standard H.264/H.265 coding algorithm guarantees a clearer and smoother video transmission. The embedded web server allows users to easily and instantaneously monitor and remotely control front-end cameras from Internet Explorer.

This series of IP cameras are suitable for large and medium-sized enterprises, government projects, shopping malls, chain supermarkets, intelligent buildings, hotels, hospitals, schools and other customer groups, and all kinds of places where remote network video transmission and monitoring will be applied. This product is easy to install and user friendly.

Introduction

- In this manual, IP cameras refer to network cameras.
- Click indicates click on the left mouse button.
- Double click indicates double click on the left mouse button.
- By default, an IP camera uses DHCP to automatically obtain an IP address; the default IP address is 192.168.1.168.
- Upon initial use, users must set a password as instructed, logging in with the username "admin" (in lowercase) and configuring the password as outlined in Section 4.2.
- The default web port number is 80. The ONVIF port number aligns with the web port number.

Note: Some information contained in this manual may different from the actual product. For any problems that cannot be solved using this manual, please feel free to contact our technical support or authorized agent. This manual is subject to change without prior notice.

1. Overview

1.1. Scope of Application

IP cameras with powerful image processing capabilities can be applied in various public places such as shopping malls, supermarkets, schools, factories and workshops, as well as environments requiring high-definition video images such as banks and traffic control systems, as shown in the image below.



1.2. Product Description

The IP camera is a digital network monitoring camera that can operate independently with a built-in web server, and can be used for real-time monitoring from all over the world by using a web browser or client software. The IP camera, based on the state-of-the-art digital solution, is an integrated media processing platform for audio/video acquisition, compression and network transmission on a single board. It complies with H.264/H.265 High Profile coding standard. By typing the IP camera's IP address or domain name into a web browser, any remote user can perform real-time monitoring. The IP camera solution is suitable for residential or commercial environments, as well as a variety of places requiring remote network video surveillance and transmission. The product is easy to install and user friendly.

The IP camera Allow to set multiple users with different permissions for easy management.

The IP camera has the motion detection function, and will actively send E-mail, captured images or alarm video when an event occurs and store the alarm video in the TF card for easy retrieval.

1.3. Operational Environment

System: Windows XP/Windows 7/ Windows 8/ Windows 10/ Windows 11/MacOS 10 or above

CPU: Intel I3 or higher

Memory: 2G or higher

Video Memory: 1G or higher

Display: 1024 × 768 or higher resolution

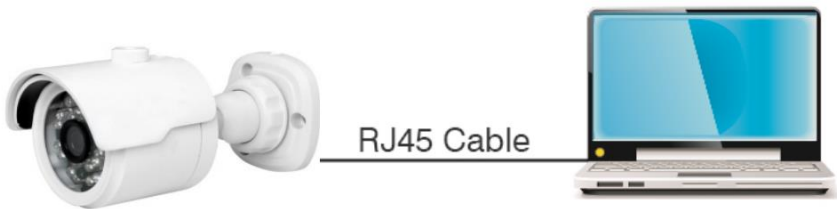
Browser: IE10 and higher version, Chrome 57 and higher version, Firefox 52 and higher version, Edge 41 and higher version, and Safari 12 and higher version.

2. Device Connection

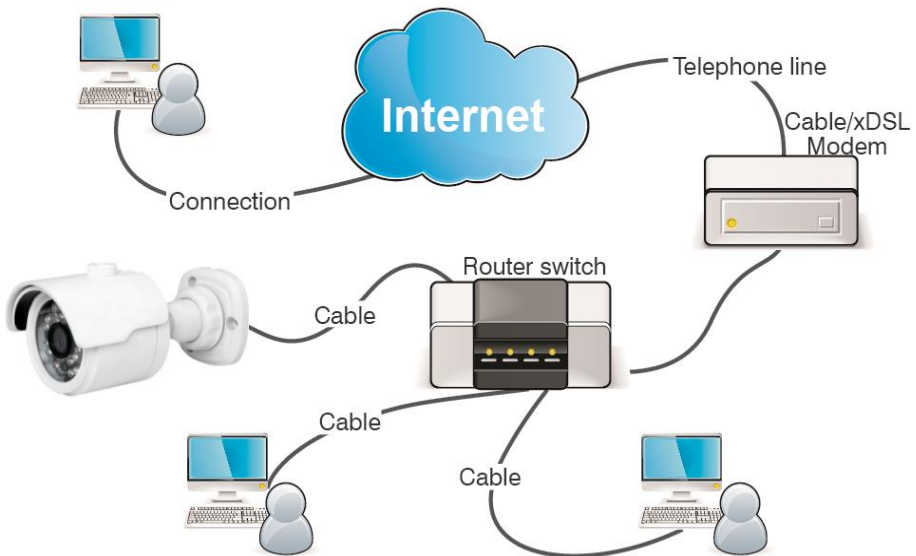
You can set up the IP camera in two selectable modes

2.1. Connecting to PC

Directly connect an IP camera to a PC through a network cable, connect the power input to the DC 12V adapter, and set the IP addresses of the PC and the IP camera on the same network segment. If the network is running properly, the IP camera will communicate with the PC within one minute after turned on.



2.2. Connection via router/switch



3. Setting the IP Address of an IPC using Risco Search Tool

Step 1 Run Risco Search Tool  , click Search to get the information of the IPCs in this LAN as shown in the figure below, and locate your desired IPC based the P2P or MAC address of the camera

RISCO

7 - 31

Search

Upgrade

Config

Stream Config

OSD Config

Recovery

Initialization

Import/Export

Reboot

Change Password

Filter: IP

IP

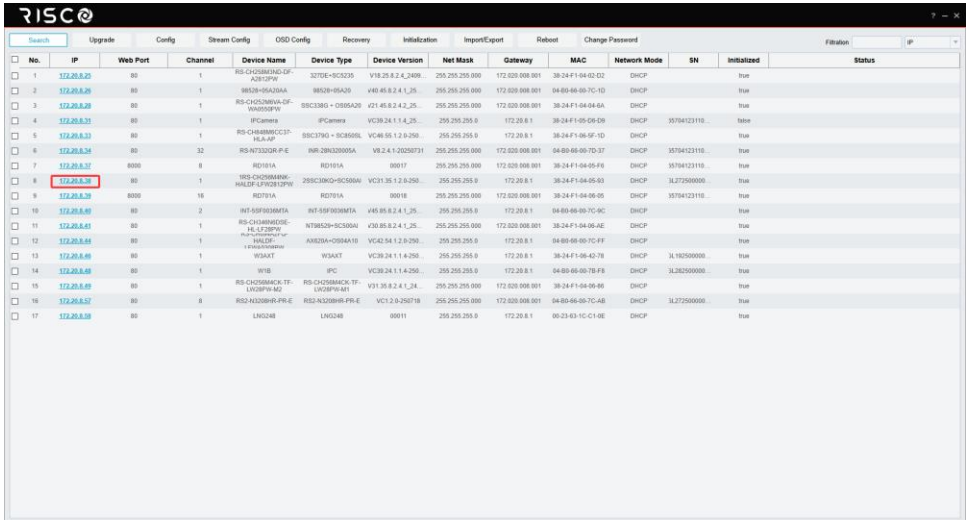
☐	No.	IP	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	SN	Initialized	Status	
☐	1	172.20.8.27	80	1	RS-C10582H4G-DF-A013PW	2170E-SC325	V10.25.8.2.4_2009	255.255.255.0	172.0.0.0/01	38-24-F1-60-02-C2	DHCP		true		
☐	2	172.20.8.28	80	1	9803B-98A0MA	9803B-H5A20	V40.45.8.2.4_1_25	255.255.255.0	172.0.0.0/01	94-80-66-90-7C-10	DHCP		true		
☐	3	172.20.8.29	80	1	RS-C10520BWA-DF-WA013PW	SBC3360 + D905A20	V71.45.8.2.4_1_25	255.255.255.0	172.0.0.0/01	38-24-F1-64-04-A4	DHCP		true		
☐	4	172.20.8.31	80	1	IPCcamera	VC39.24.1.1.4_25	255.255.255.0	172.20.8.1	38-24-F1-60-09-09	DHCP		35704123110	false		
☐	5	172.20.8.33	80	1	RS-C10480MC3P-HA-AP	SBC3790 + SC3505	VC40.56.1.2.0_250	255.255.255.0	172.20.8.1	38-24-F1-66-9F-1D	DHCP		true		
☐	6	172.20.8.34	80	32	RS-N7332QR-P-E	NR-28K32005A	V8.2.4.1.2003731	255.255.255.0	172.0.0.0/01	94-80-66-00-7D-37	DHCP		35704123110	true	
☐	7	172.20.8.37	8000	8	RD701A	RD701A	00017	255.255.255.0	172.0.0.0/01	38-24-F1-64-05-F9	DHCP		35704123110	true	
☐	8	172.20.8.38	80	1	RS-C10580MBK-HALF-LP0303PW	255C10KQ-SC3500A	VC31.35.1.2.0_250	255.255.255.0	172.20.8.1	38-24-F1-64-05-93	DHCP		31273200000	true	
☐	9	172.20.8.39	8000	16	RD701A	RD701A	00018	255.255.255.0	172.0.0.0/01	38-24-F1-64-06-06	DHCP		35704123110	true	
☐	10	172.20.8.40	80	2	INT-S0F003M51A	INT-S0F003M51A	V45.85.8.2.4_1_25	255.255.255.0	172.20.8.1	94-80-66-00-7C-9C	DHCP		true		
☐	11	172.20.8.41	80	1	RS-C10480MC3P-HA-AP	NT9852H-SC300A	V30.85.8.2.4_1_25	255.255.255.0	172.0.0.0/01	38-24-F1-64-06-AE	DHCP		true		
☐	12	172.20.8.44	80	1	AN820A+O9AA10	VC42.54.1.2.0_250	255.255.255.0	172.20.8.1	94-80-66-00-7C-FF	DHCP		true			
☐	13	172.20.8.46	80	1	WSAXT	VC39.24.1.1.4_250	255.255.255.0	172.20.8.1	38-24-F1-66-42-78	DHCP		31182500000	true		
☐	14	172.20.8.49	80	1	W1B	IPC	VC38.24.1.1.4_250	255.255.255.0	172.20.8.1	94-80-66-00-7B-F8	DHCP		31282500000	true	
☐	15	172.20.8.49	80	1	RS-C10580MC3P-LV03PW-M0	RS-C10580MC3P-LV03PW-M0	V31.35.8.2.4_1_24	255.255.255.0	172.0.0.0/01	38-24-F1-64-06-06	DHCP		true		
☐	16	172.20.8.57	80	8	RS2-N3208R-PR-E	RS2-N3208R-PR-E	VC1.2.0-250718	255.255.255.0	172.0.0.0/01	94-80-66-00-7C-AB	DHCP		31273200000	true	
☐	17	172.20.8.59	80	1	LN524B	LN524B	00011	255.255.255.0	172.20.8.1	00-23-43-1C-C1-0E	DHCP		true		

Note: The default IP address of the camera is 192.168.1.168, the default username is admin.

4. Login from Web Client

4.1. Accessing Camera from Web Client

Use Risco Search Tool to search the IPCs in the current network. As shown in the following figure, directly click an IP address and use your IE browser to login to the corresponding camera.



No.	IP	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	SN	Initialized	Status
1	172.20.8.25	80	1	RS-CH25M4ND-CP-AS0CPW	327DE-SC3235	V18.25.8.2.4_2409...	255.255.255.000	172.828.008.001	38-24-F1-04-02-02	DHCP		true	
2	172.20.8.26	80	1	8852B-ISA200A	8852B-ISA20	V40.45.8.2.4_1_25...	255.255.255.000	172.828.008.001	04-80-66-66-7C-1D	DHCP		true	
3	172.20.8.28	80	1	RS-CH25M4VA-CP-V00000TV	SBC3385 + DB85A20	V21.45.8.2.4_1_25...	255.255.255.000	172.828.008.001	38-24-F1-04-04-6A	DHCP		true	
4	172.20.8.33	80	1	IPCamera	IPCamera	VC38.24.1.1.4_25...	255.255.255.0	172.20.8.1	38-24-F1-05-08-09	DHCP	357841231110...	false	
5	172.20.8.33	80	1	RS-CH25M4VC3P-ISA-A2P	SBC3390 + BC3605L	VC46.55.1.2.0_250...	255.255.255.0	172.20.8.1	38-24-F1-06-07-1D	DHCP		true	
6	172.20.8.34	80	32	RS-N7320R-P-E	NR-28N32000A	V8.2.4.1-20200731	255.255.255.000	172.828.008.001	04-80-66-66-7D-37	DHCP	357841231110...	true	
7	172.20.8.37	8080	8	RD781A	RD781A	00017	255.255.255.0	172.828.008.001	38-24-F1-04-05-F6	DHCP	357841231110...	true	
8	172.20.8.38	80	1	RS-CH25M4VA-CP-V00000TV	285C3M0-SC3500A	VC31.35.1.2.0_250...	255.255.255.0	172.20.8.1	38-24-F1-04-05-63	DHCP	31272500000...	true	
9	172.20.8.38	8080	16	RD781A	RD781A	0001E	255.255.255.0	172.828.008.001	38-24-F1-04-05-05	DHCP	357841231110...	true	
10	172.20.8.40	80	2	RS-CH25M4VA-CP-V00000TV	NR750P-SC3500A	V46.85.8.2.4_1_25...	255.255.255.0	172.20.8.1	04-80-66-66-7C-9C	DHCP		true	
11	172.20.8.41	80	1	RS-CH25M4VA-CP-V00000TV	NR750P-SC3500A	V46.85.8.2.4_1_25...	255.255.255.0	172.828.008.001	38-24-F1-04-05-4E	DHCP		true	
12	172.20.8.46	80	1	RS-CH25M4VA-CP-V00000TV	NR750P-SC3500A	V46.85.8.2.4_1_25...	255.255.255.0	172.20.8.1	04-80-66-66-7C-F9	DHCP		true	
13	172.20.8.46	80	1	RS-CH25M4VA-CP-V00000TV	NR750P-SC3500A	V46.85.8.2.4_1_25...	255.255.255.0	172.20.8.1	04-80-66-66-7C-F8	DHCP	31282500000...	true	
14	172.20.8.46	80	1	W848T	W848T	VC38.24.1.1.4_250...	255.255.255.0	172.20.8.1	38-24-F1-04-02-78	DHCP	31282500000...	true	
15	172.20.8.48	80	1	IPC	IPC	VC38.24.1.1.4_250...	255.255.255.0	172.20.8.1	04-80-66-66-7C-F8	DHCP	31282500000...	true	
16	172.20.8.48	80	1	RS-CH25M4VC3P-ISA-A2P	SBC3390 + BC3605L	V21.45.8.2.4_1_24...	255.255.255.000	172.828.008.001	38-24-F1-04-04-60	DHCP		true	
17	172.20.8.52	80	8	RS-N320MR-P-E	RS-N320MR-P-E	VC1.2.0-250719	255.255.255.000	172.828.008.001	04-80-66-66-7C-AB	DHCP	31272500000...	true	
18	172.20.8.58	80	1	LN6204H	LN6204H	00011	255.255.255.0	172.20.8.1	00-23-63-10-01-0E	DHCP		true	

As an alternative, you can open your IE browser and type the following information into the address bar: <http://ip:web port>. As shown in the figure above, the IP address of the device to be accessed is 172.20.8.38, the web port No. is 80, and the combined URL is <http://172.20.8.38:80>.

Note: In practical applications, the default HTTP access mode is port 80.

4.2. Login for the First Time

Firstly, access the camera from a web client, you need to set a password for the camera in order to complete the activation operation. The web client will display the screen as shown in the image below. Hover over the password entry box to prompt for the password requirement.

The length of the password should be 8~16 characters. It should contain at least two combinations of uppercase letters, lower case letters, numbers and special characters.

Password and username cannot be set the same.

Password

Default Username

admin

New Password

Password Strength

Confirm Password

OK

Set a new password and click OK to save your change. The web client will display the screen as shown in below picture. Users can open the corresponding recover password method by checking the box, or cancel the setting directly without checking the box, and do not enable the recover password function.

Recover Password

☐ Security Question Configuration

Security Question 1

Your father's name?

Answer

Security Question 2

Your mother's name?

Answer

Security Question 3

Your head teacher's name in senior high school?

Answer

☐ Certificate of authorization ?

Export

☐ Super code(Not recommended) ?

OK

Cancel

④ Security Question Configuration: To change the user password by question verification, check the Security Question Configuration, select three questions among 15 questions, and set the answers at a maximum length of 64 characters to recover your password.

② Certificate of authorization: To change the user password by using a certificate, check the Certificate of authorization, and click Export to download the certificate.txt file.

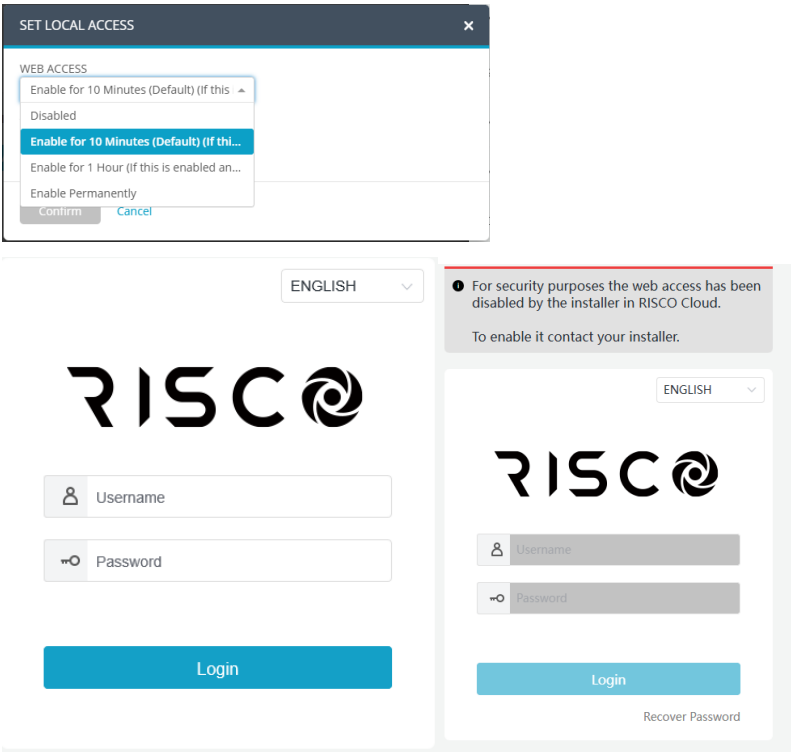
③ Super code(Not recommended): This method is to calculate a super code allowing to changing the user password by using the MAC address of the camera and camera time. You are not advised to enable this function as the MAC address of the camera is broadcast over the network, and the system time of the camera can be directly obtained when you login from the web client and use Super code to change the user password.

Note: Keep your verification information properly when the recover password function is enabled.

4.3. General Login

After accessing from the web client, you will be directed to the login screen as shown in below picture. Then input your username and password, and click Login to access the operation screen. At the same time, you can select your desired language upon login.

The RISCO server can set the web login time, When the login times out, IPC can't login to the web client.



4.4. Recover Password

When the recover password function is enabled, if you forget the login information, you can click Recover Password to enter the Recover Password screen. You can check security question configuration, certificate of authorization, or super code upon first login to recover your password.

4.4.1. Security Question Configuration

You can change the user password by setting security questions on the Recover Password screen, as shown in the screen below. Fill in the answers to security questions. You can directly change the user password.

Recover Password

Verification Mode

Security Question Verification

Security Question 1

Your father's name?

Answer

Security Question 2

Your mother's name?

Answer

Security Question 3

Your head teacher's name in senior high school?

Answer

New Password

Password Strength

Confirm Password

OK

Cancel

4.4.2. Certificate of Authorization

When you set security questions upon first login, you will be asked to download the certificate.txt when you choose to recover the user password by using Certificate of authorization. On the Recover Password screen, click the Recover Password and import the certificate.txt file to reset the password, as shown in below picture. Click **Import** and select the certificate.txt file. Then, enter a new password to change the user password.

Recover Password

Verification Mode

Certificate of authorization

Certificate of authorization

Import

OK

Cancel

Note: After using this method to change the password, the key file will be invalidated and a pop-up window will prompt the user to re-export the key file after logging. If the user does not choose to re-export the key file, the user will no longer be allowed to change the password by this method after that. The prompt is shown in the screen below.

Notice

X

!

The certificate-based password recovery system has been updated. The current certificate has expired and can no longer be used. Please export a new certificate to ensure continued security.

OK

Cancel

4.4.3. Super Code

The super code is an insecure way to recover the password. The super code is calculated based on the MAC address of the camera and the time of the super verification code according to certain rules. Then the user password can be changed by entering the verification code.

The 'Recover Password' dialog box features a light blue header. It contains several input fields: 'Verification Mode' with a dropdown menu set to 'Super Code', 'Super code' (empty), 'New Password' (empty), and 'Confirm Password' (empty). A green status message reads '2025-07-30 11:10:54 MAC Address: 38-24-F1-10-95-EA'. A 'Password Strength' indicator shows three segments, with the first two filled. At the bottom are 'OK' and 'Cancel' buttons.

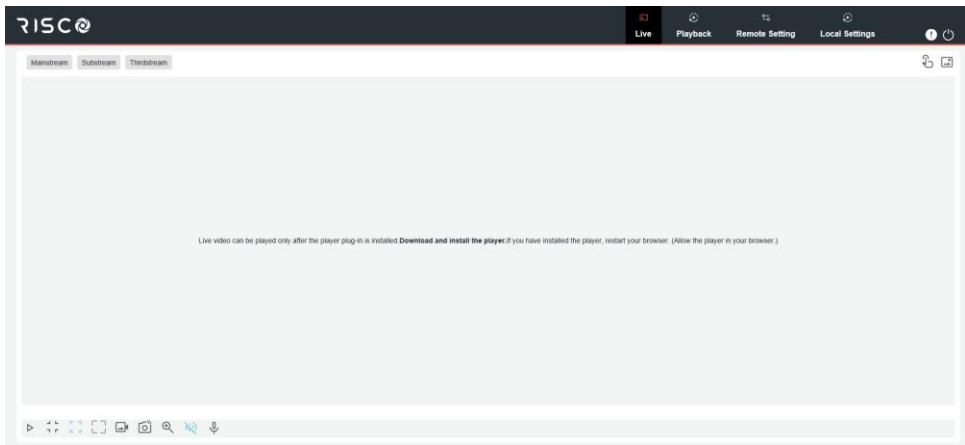
4.5. Password Expire

Security risks may arise if you use the same password for a long period of time. To this end, the program records the time when the password was changed last time. The system will ask you whether to change the password again if the current login time is 90 days later after the last password change time. When you decide to change the password, the screen as shown in the image below. As instructed on the screen, use your old password for verification and set a new password.

The 'Password' dialog box has a light blue header. It includes a 'Default Username' field with 'admin' entered. Below it is a 'New Password' field with a red border and a toggle icon. A 'Password Strength' indicator shows three segments, with the first two filled. There is a 'Confirm Password' field (empty) and a red error message: '[New Password] Please provide valid input'. An 'OK' button is at the bottom right.

5. Installing Plug-in

Images can be normally previewed only when the plug-in is installed when you login from your IE browser. Download and install the plug-in as instructed on the screen as shown in the screen below.



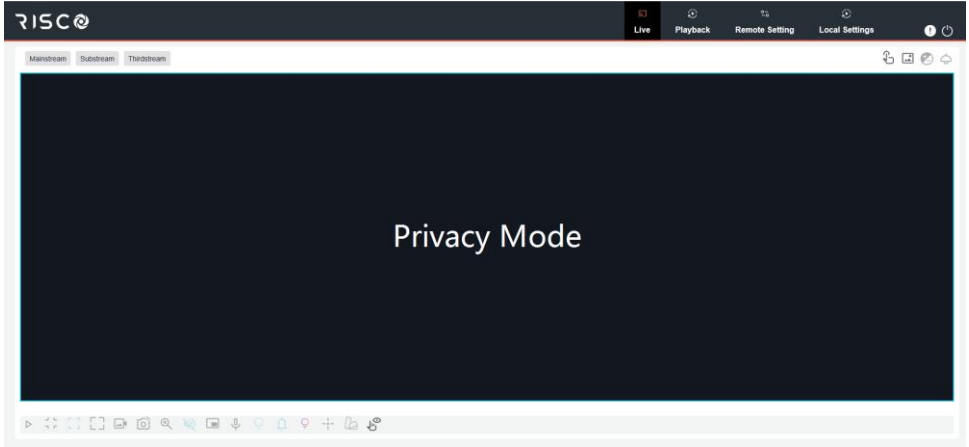
Note: Skip the plugin installation when you access the web client from Safari 12 and higher version, Chrome 57 and higher version, Firefox 52 and higher version, and Edge 41.

6. Preview screen

6.1. Live menu

After successful login, the web end enters the login preview interface, whose interface is shown in the following figure.

Note: Functions vary from product to product, please refer to actual.



Stream switch menu: Adjust the current live view quality from the upper-left corner.

- Main stream: HD picture, but higher requirements on bandwidth and PC performance.
- Sub stream: Moderate requirements on bandwidth and PC performance, but lower picture quality when compared with main stream.
- Mobile stream: Lowest requirements on bandwidth and PC performance, and lowest picture quality.

Main switch bar: Switches web function screens. The web client provides four menus: Live, Playback, Remote Setting, Local Settings.



Info: Display the information about the active user, web version and plugin version.



Manual Alarm: Enable/disable the manual alarm. (Note: for cameras with I/O function only)



AI alarm: Open the alarm push bar on the right and push images during face detection and human & vehicle detection.



Color: Adjust current image settings, such as image saturation and sharpness.



PTZ Setting: PTZ settings and re-focusing.



Exit: Log out of the current login.



Stop/Play: Play and stop the preview of the current stream.



Original Proportions: Display the current live view in its original proportion.



Stretch: Display the current live view in a way that stretches the display area.



Full Screen: Display the live view in full screen. double-click the screen to enable or disable the function, and press Esc to exit the full screen mode.



Record: Manually record the stream in preview.



Capture: Manually capture the image of the current stream.



Digital Zoom: Zoom in a certain area of the display.



Audio: Enable or disable or adjust the audio in preview.



Voice Intercom: Communicate with the camera.



Light: Manually turn on/off the white light.



Siren: Manually turn on/off the siren.



Warning Light: Enable or disable the red and blue lights



Pixel Counter: Select an area to check its pixel size in the stream.



Add Tag: Add a label, click to add a label.



Privacy Mode: Turn on/off the privacy mode. When it is turned on, the other options in the menu bar will be greyed out.

6.2. Video Status

The recording status is a simple indication on the web side of the current alarm of the camera and whether the recording is normal or not. Multiple alarms can exist at the same time, as described below:

No icon: The device SD card is normal, but no recording is taking place.

R: The camera is recording in general.

H: The SD card is in an abnormal state, please check and confirm the SD card.

M: The camera is in MOTION alarm, but MOTION alarm recording is disabled.

M: The camera is in MOTION alarm and MOTION alarm recording.

I: The camera is in IO alarm, but IO alarm recording is disabled.

I: The camera is in IO alarm and makes IO alarm recordings

S: The camera is in Smart Alarm, but no Smart Alarm recording is disabled.

S: The camera is in Smart alarm and smart alarm recording.

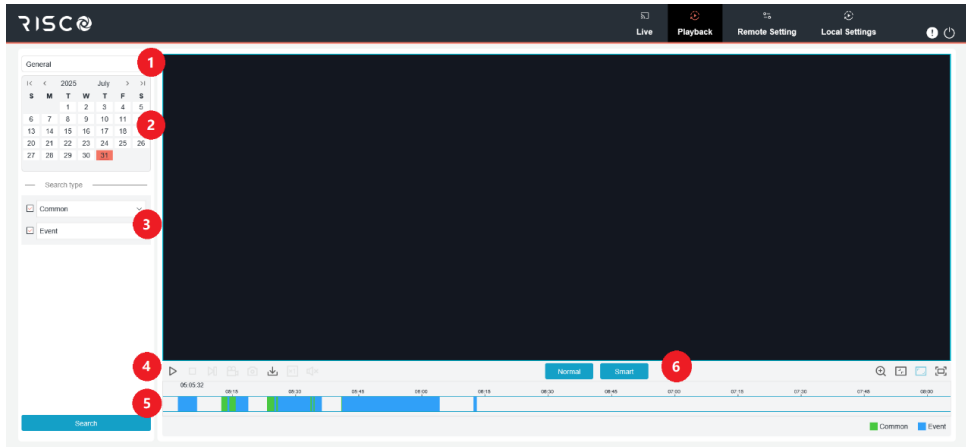
Note: Intelligent alarms include alarms for faces, people & cars, etc

7. Playback

Cameras not only need to be able to allow us to see live images, but they also need to be able to save the image information so that it can be retrieved and viewed when needed.

7.1. General playback

The playback function is mainly composed of general video search, AI search function, as shown in the figure below for video search.



1.Switch search mode: Switch search functions, as shown in the figure above. General is selected by default to search for general recording files. switch to AI image search by referring to the following part in this section.

2.Date: Set the date to search for recording files, click Search, you will be prompted with the dates with available recording files.

3.Search type: Display the search types supported by the camera. search for only part of recording files as required.

4.Playback process bar: Display and search for recording files stored in the memory card according to search settings.



Pause/Play: Pause/play streams.



Stop: Stop playing streams.



Forward by One Frame: Play one frame with one click.



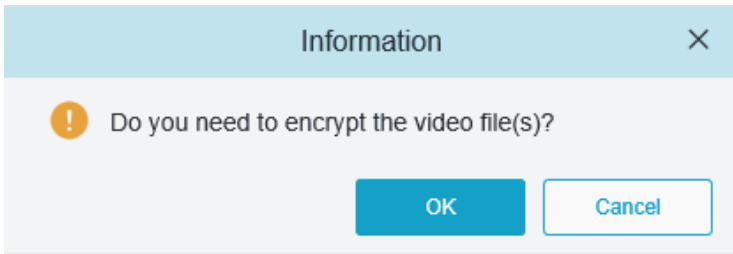
Record: Manually record the stream in preview.



Capture: Manually capture the image of the current stream.



Download: Download the searched recording file. (Note: When downloading AVF format records, a Pop-up window will ask if encryption is required. AVI and MP4 formats will not have a pop-up window.)



Speed: Supports playing at a speed of 1/8, 1/4, 1/2, 1, X2, X4, X8, X16.



Audio: Enable or disable or adjust stream sound.



Add Default Tag: Add a default tag. Default name Tag.



Add Tag: Add a custom tag, customizable the name of the tag, the length of the name is 1~39 characters.



Digital Zoom: Zoom in a certain area of the stream.



Original Proportions: Display the current live view in its original proportion.



Stretch: Display the current live view in a way that stretches the display area.



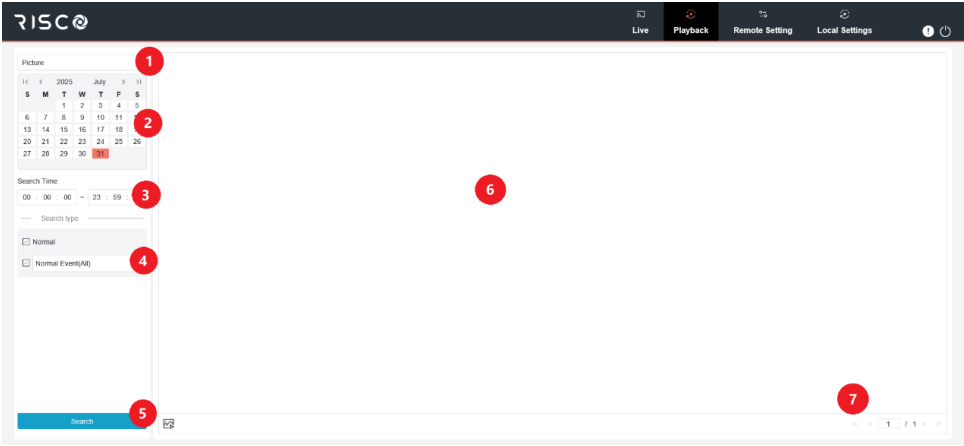
Full Screen: Display the playback stream in full screen. double-click the screen to enable or disable the function, and press Esc to exit the full screen mode.

5.Search: Display the video search in the SD card according to the search settings.

6.Normal/Smart search: Switch Normal or Smart search. After selecting Smart search, click the button of human type and car type in the lower left corner, the video progress bar will mark the alarm video triggered by human and car type on the same day in blue. Alarm videos of people and car types include: Pedestrian & Vehicle, Intrusion, Enter Region, Exit Region and Line Crossing detected videos of people and car types.

7.2. Image Search

When the camera turns on the automatic picture capture function, Search and play pictures in this interface.



1.Search mode switching: Switch the current search function, the current search mode is Picture.

2.Search date: Set the date of searching pictures, click search, it will prompt the date of having video files.

3.search time: Set the time to search for pictures, to facilitate users to query the specific time period of the picture.

4.Search type: Select the type of image capture to search, the default selection of all.

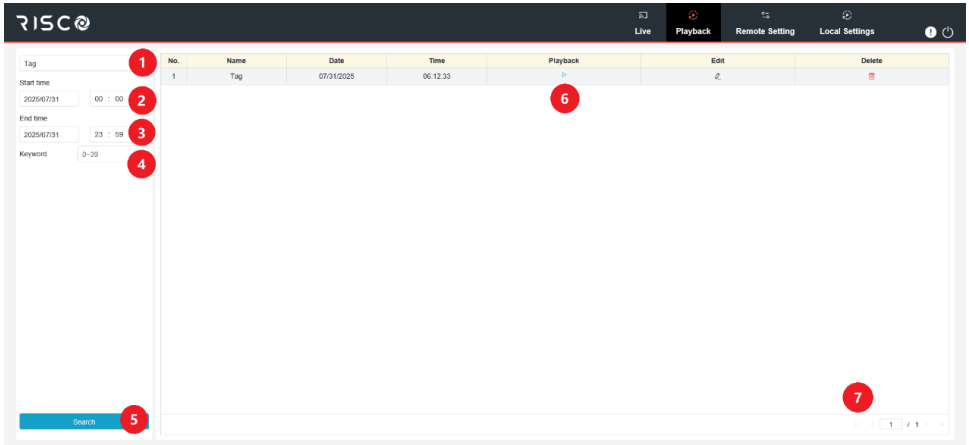
5.Search: Click Search, start searching for pictures.

6.Search results display area: Display the pictures searched by the user. When you double-click a picture, it will play the playback video of the time period before and after the picture.

7.Search results page: In the lower right corner of the search results can be turned.

7.3. Playback by Tag

This screen allows you to view all previously added tags and edit, playback or delete them.



1. search mode switching: switch the current search function, the current search mode is Tag.

2.Start time: Set the start time of the search tag.

3.End time: Set the end time of the search tag.

4.Keyword: Enter the keyword to search.

5. Search: Click Search, start searching.

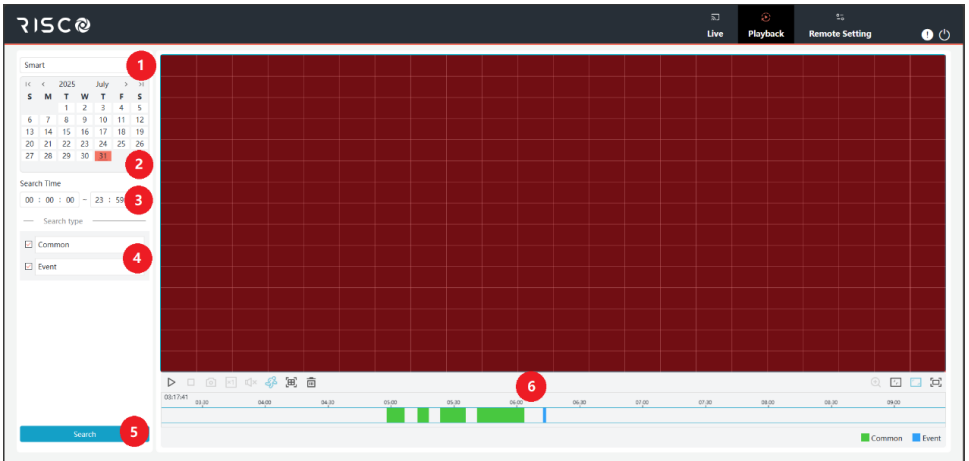
6.the search results display area: display the user set up to meet the search conditions of the search results.

Click  button to play back the event; click  button to modify the event name; click the Save button to pop up the Modify success prompt box; click  button to delete the event.

7. search results page: in the lower right corner of the search results can be turned page.

7.4. Smart

Login from a browser without the need of plugin to start smart playback, as shown in the screen below.



This function can identify whether an alarm is triggered by human in daily life. If yes, the alarm will be shown in blue in the playback time bar on the bottom.

1.Switch search mode: Switch the current search function. The current search mode is Smart.

2.Date: Set the date to search for smart events. By clicking Search, you will be prompted with the dates for which recording files are available.

3.Search time: Set the time for searching for events.

4.Search type: Display the search types supported by the camera. search for only part of recording files as required.

5.Search: Click Search to start searching.

6.Search Result Display Area: Display the desired search results.



Stop: Turns off the playback stream.



Capture: Manually capture the image of the current stream.



Speed: Variable speed playback, support 1/8, 1/4, 1/2, 1, X2, X4, X8, X16 speed adjustment.



Audio: Switch on/off, adjust the sound of the playback stream.



Add Default Tag: Add a default tag. Default name Tag.



Add Tag: Add a custom tag, customizable tag name, name length 1 to 39 characters.



Smart: Click to enter the smart area setting interface.



All: Click All to set the entire screen of the camera as the Smart detection area;



Delete: Click Clear All to clear the entire area.



Digital Zoom: An electronic zoom function that zooms in to show a certain area of the playback stream.



Original Proportions: Displays the current preview screen in its original proportions.



Stretch: Displays the current preview screen in a way that spreads the display area.

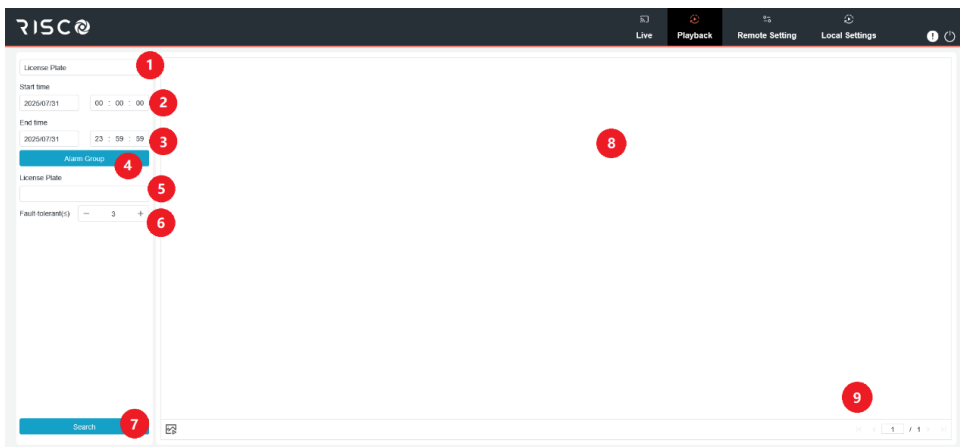


Full Screen: Display the playback stream in full screen, double click the screen to open/close the function, press Esc to exit the full screen when the function is opened.

7.5. AI

7.5.1. License Plate Detection Search

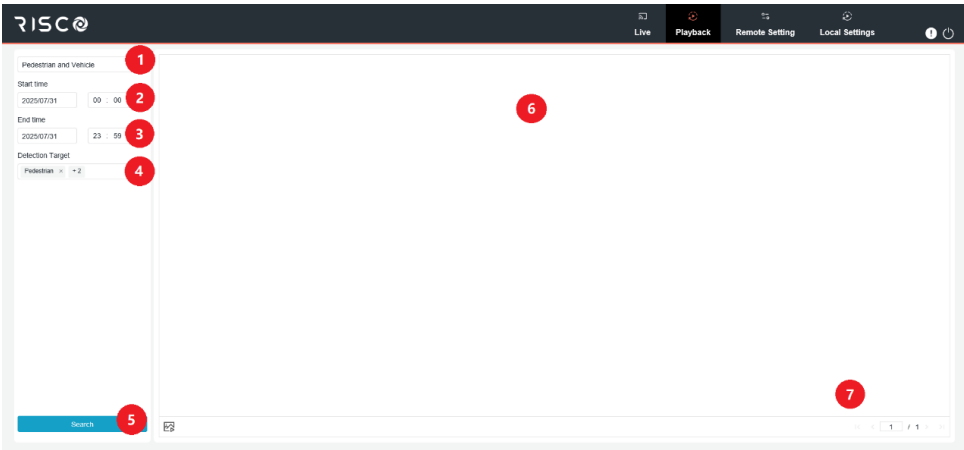
When the License Plate detection function is enabled for the IPC, an alarm will be triggered for recognized License Plates, and images or videos will be recorded for easy search and viewing. The screen is shown in the screen below.



- 1.**Switch search mode:** Switch the current search function. The current search mode is License Plate.
 - 2.**Start time:** Set the start time to search for captured License Plates.
 - 3.**End time:** Set the end time to search for captured License Plates.
 - 4.**Alarm Group:** Recognize License Plates by groups in the database.
- Note:** All images will be searched when no group limitations are set. In this case, the similarity setting takes effect. Unknown License Plates will be ignored when group limitations are set.
- 5.**License Plate:** Filter and query License Plates.
 - 6.**Fault-tolerant:** Fault-tolerant rate. For example, three characters are set as the querying criteria. When the License Plate number is B594SB in the allow list in the group, an alarm will also be triggered when the vehicle with License Plate number B734KB approaches the surveillance area. That is, a License Plate number has 0-3 characters different from that in the database will be recognized.
 - 7.**Search:** Search for captured License Plates according to settings.
 - 8.**Search Result Display Area:** Display the desired search results. Double-click the picture will play the video after and before the picture.
 - 9.**Search results Flip:** Scroll through search results at the lower right corner.

7.5.2. Pedestrian and Vehicle Search

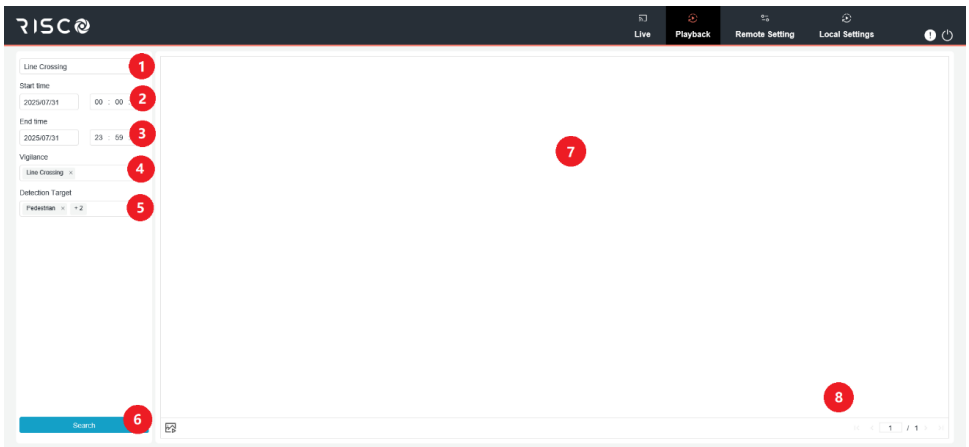
Similar to the Face Capture function, the camera can differentiate between people or cars and record them according to the desired situation, which is used to search for the desired record. The interface effect is shown in the screen below.



- 1.Switch search mode:** Switch the current search function. The current search mode is Pedestrian & Vehicle.
- 2.Start time:** Set the start time to search for Pedestrian and Vehicle images.
- 3.End time:** Set the end time to search for Pedestrian and Vehicle images.
- 4.Detection Target:** Select human or vehicle images as needed, or select both.
- 5.Search:** Search for Pedestrian and Vehicle images according to search settings.
- 6.Search Result Display Area:** Display the desired search results. Double-click the picture will play the video after and before the picture.
- 7.Search results Flip:** Scroll through search results at the lower right corner.

7.5.3. Line Crossing

With the development of technology, Line Crossing is not only compatible with the old way of alarming targets entering the guarded area, but also adds the function of human-vehicle detection, which alarms only human or vehicle targets and records pictures or video information for easy searching and viewing, and its interface effect is shown in the following screen.

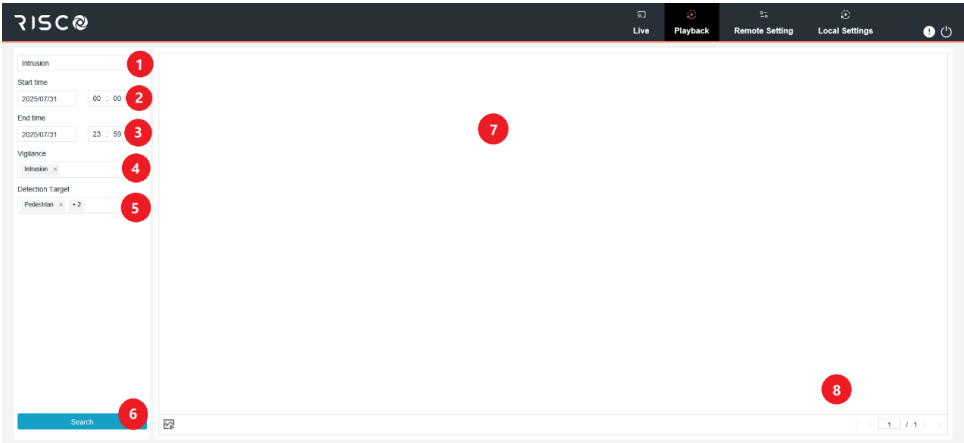


- 1.Search mode switching:** Switch the current search function, the current search mode is Line Crossing.
- 2.Start time** Set the start time of searching for human car shape capture.
- 3.End time** Set the end time of searching for human car shape capture.
- 4.Vigilance** Set the way of capturing the alarm triggered as Line Crossing, also set it at the same time.
- 5.Detection Target** According to the need, set the search of the person or the car to catch the picture, also search at the same time.
- 6.Search:** According to the search settings to search for humanoid models to capture the map.

- 7.The search results display area:** Display the customer's desired search results. Double-click on the picture to access a small period of time before and after the detection of playback.
- 8.Search results page:** In the lower right corner of the search results can be turned.

7.5.4. Intrusion Detection

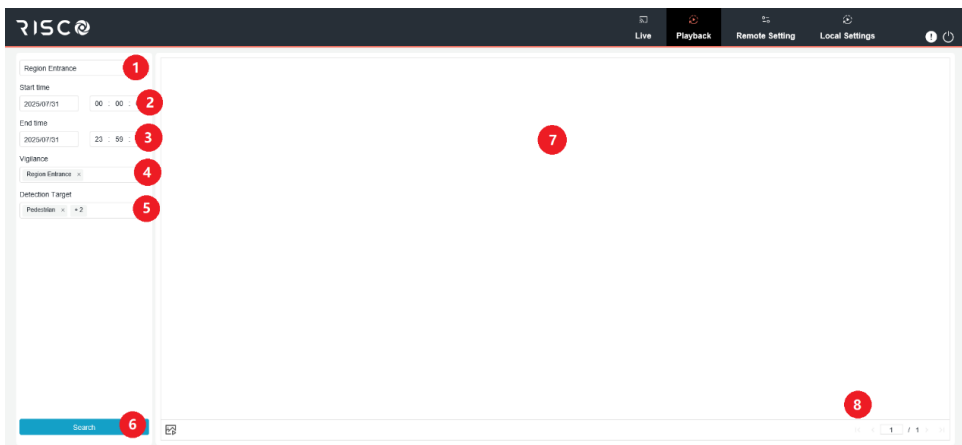
When the camera enables the Intrusion function, it will alarm the target that enters into the intrusion of the alert area. Record video or capture picture information for easy search and view. Its interface is shown in the following screen.



- 1.Switch search mode:** Switch the current search function. The current search mode is Intrusion.
- 2.Start time:** Set the start time to search for Intrusion snapshot.
- 3.End time:** Set the end time to search for Intrusion snapshot.
- 4.Vigilance:** Select Intrusion as the capture method.
- 5.Detection Target:** Select Intrusion images as needed, or select both.
- 6.Search: Search for Intrusion** Images according to search settings.
- 7.Search Result Display Area:** Display the desired search results. Double-click the picture will play the video after and before the picture.
- 8.Search results Flip:** Scroll through search results at the lower right corner.

7.5.5. Region Entrance

After the camera opens the entry area detection function, it will alarm the detected targets entering the alert area, record pictures or video information for easy search and view, and its interface effect is shown in the following screen.



1.Search mode switching: Switch the current search function, the current search mode is Region Entrance.

2.Start time Set the start time of searching into the area to capture the map.

3.End time: Set the end time of searching into the area to capture the map.

4.Vigilance: Set the way of capturing the alarm triggered to enter the area.

5.Detection Target: According to the need, set the search of the person or the car to catch the picture, also search at the same time.

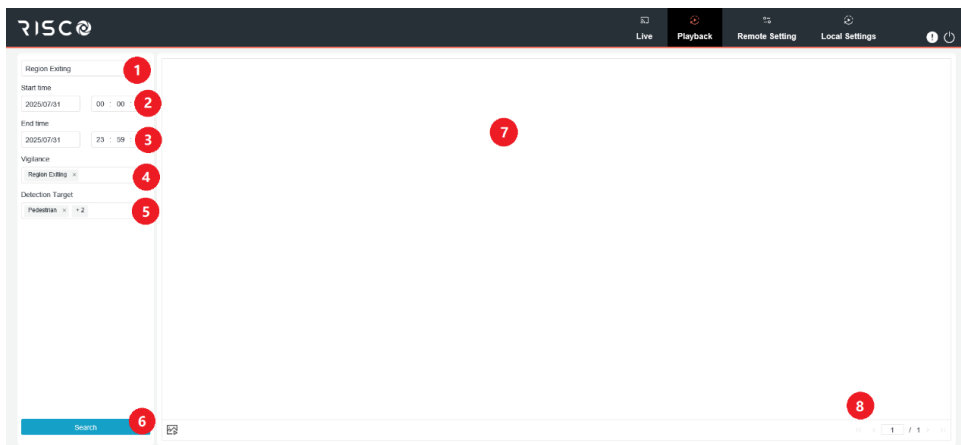
6. Search: according to the search settings to search for humanoid models to capture the picture.

7.The search results display area: Display the customer's desired search results. Double-click on the picture to access a small period of time before and after the detection of playback.

8.Search results page: In the lower right corner of the search results can be turned.

7.5.6. Region Exiting

When the camera turns on Region Exiting function, Alarm triggered and detect targets leaving the guarded area. Record video or capture picture information for easy search and view. Its interface is shown in the following figure.



1.Switch search mode: Switch the current search function. The current search mode is Region Exiting.

2.Start time: Set the start time to search for Region Exiting images.

3.End time: Set the end time to search for Region Exiting images.

4.Vigilance: Select Region Exiting as the capture method.

5.Detection Target: Select Region Exiting images as needed, or select both.

6.Search: Search for Region Exiting images according to search settings.

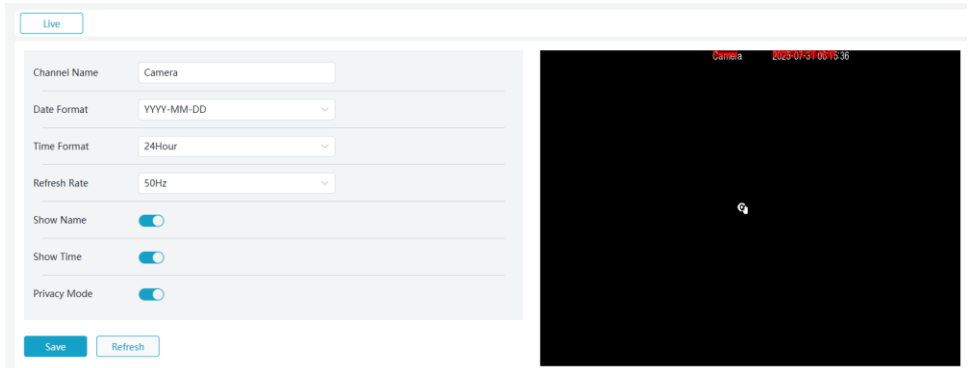
7.Search Result Display Area: Display the desired search results. Double-click the picture will play the video after and before the picture.

8.Search results Flip: Scroll through search results at the lower right corner.

8. Remote Settings

8.1. Preview

The Live interface is to set the channel name, device time, Cross Counting and other intelligent function statistics and image overlay position, its interface is shown in the following screen.



Channel Name: Set the camera channel name

Date Format: Set the date format displayed by the camera OSD, there are three types: MM/DD/YYYYY, YYYY-MM-DD and DD/MM/YYYYY.

Time Format: Set the time format of the camera's OSD display, there are two types: 12-hour and 24-hour.

Refresh Rate: Set the refresh rate of the camera, there are two options, 60Hz and 50Hz, corresponding to N and P system.

Show Name: The preview shows the camera channel name.

Show Time: The preview shows the camera time.

Privacy Mode: Privacy Mode. When Privacy Mode is enabled, there is no image in preview and playback, and the preview image is not displayed in the Settings page.

Show Channel Name Position: Set the position where the channel name is displayed by dragging the channel name on the image.

Display Time Position: Set the position of the channel time display by dragging the channel time on the image.

Display Alarm Statistics Position: Set the position of the channel alarm statistics display by dragging the channel alarm statistics on the image. This setting is only displayed when the function that supports alarm statistics display is turned on.

Save: Save the current changes

Refresh: Retrieve the current interface parameters.

8.2. Image Control

Image control is the direct control to modify the graphic parameters, such as color-to-black mode, wide dynamic, backlight supplement, etc. The interface is shown in the following screen.

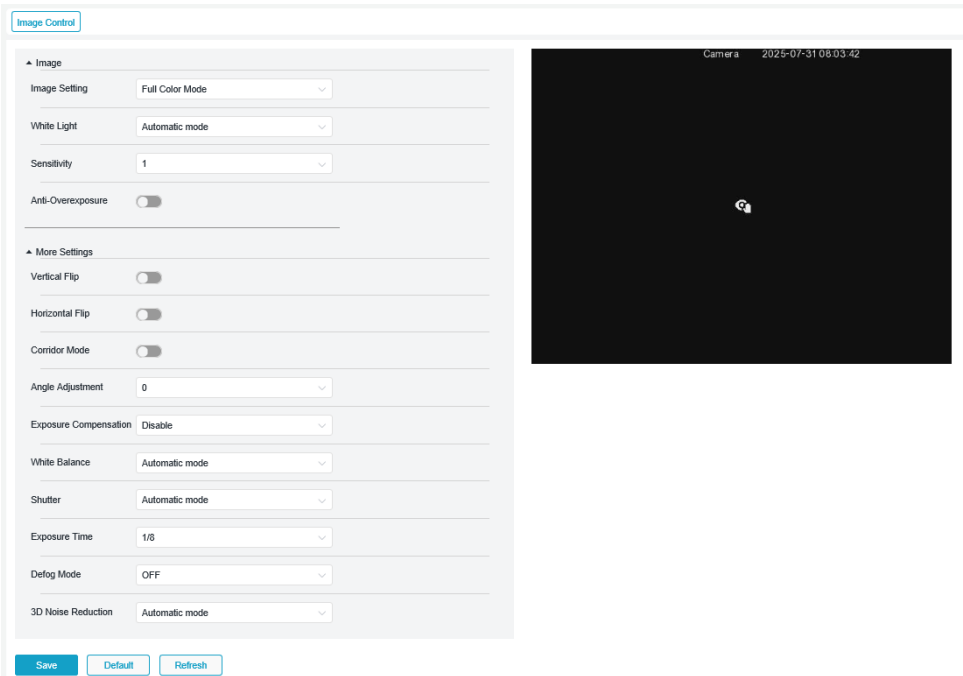


Image Setting: Set the camera image mode, there are 3 modes.

Full Color Mode: The camera is in full Color mode.

Day/Night Mode: The camera is in Day/Night mode.

Smart Illumination: The camera in night vision mode when the camera triggers an alarm will be linked to the warm light for fill light, the image is in color; the end of the alarm the camera back to night vision mode.

White Light: Under Full Color Mode, set the fill light effect of the camera's warm light, there are 4 modes in total.

Automatic mode: automatic mode, the camera automatically adjusts the strength of the fill light according to the ambient illumination.

Manual: Fill in the environment with a fixed brightness value.

Schedule: automatically switch on/off the warm light for fill light by setting the time schedule.

OFF: Turns off the warm light lamp.

Sensitivity: Sensitivity 0 to 3, the camera's perception of ambient light, the higher the value the more sensitive.

Light Distance: range 0 to 100, **White Light** is the brightness of the fill light in **Manual** mode, the higher the value, the higher the brightness.

IR-CUT Mode: Set the camera **day/night** switching mode under Day/Night Mode, there are 5 modes.

Auto/GPIO Auto: auto control switching mode, color switching black and white by image judgement, black and white conversion color by photosensitive judgement.

Day/Color Mode: Forces color mode without switching between black and white.

Night/Black White Mode: Forces black and white mode without switching color.

Image/Image Mode: Similar to Auto Mode, control the mode of color to black and black to color by image.

Schedule/Schedule(B/W): Switch between black and white and color by schedule setting. To turn on this function, you need to set the start and end time of entering night vision.

IR LED Control: Sets the fill light effect of the camera's IR LED in night vision, with 3 modes.

Smart IR: Intelligent control of infrared lamp fill light intensity, according to the focal length, whether the screen is over the explosion of dynamic control of infrared lampsThe fill light.

Manual: Manual mode to fill in the light with the set IR lamp brightness.

OFF: No light is used for fill.

Low/High Beam Light: Manually adjust the brightness of the IR lamp (0 to 100, when set to 0 the IR lamp does not light up, and when set to 100 it is the brightest).

Anti-Overexposure: When turned on in all image modes, this function prevents overexposure of images in high-brightness environments.

Corridor Mode: The image is rotated 90 degrees clockwise. (Some models support corridor mode)

Angle Adjustment: Image rotation setting, the camera can be adjusted by this value in certain usage scenarios where the camera is inverted from the preset, e.g. designed to be used upside down, but in reality it is used in a flat position.

Vertical Flip: To make the image of the screen interact up and down.

Horizontal Flip: Mirror mode in horizontal direction so that the images of the screen interact left and right.

Exposure Compensation: Sets how the program behaves when backlit, with 4 modes:

WDR: Wide Dynamic Range in which the picture is uniformly balanced based on the setting and both light and dark areas can be clearly distinguished. (DWDR in some models)

HLC: Strong light rejection function, which makes objects in the high light area clearer in the picture according to the set HLC Level value. (Not supported by some models)

Back Light: Make the dark areas of the screen clearer according to the set BLC Level value and BLC Area.

Disable: No exposure compensation optimisation is performed on the picture frame.

White Balance: White balance setting with two modes:

Automatic mode: Adjust the white light using default parameters

Manual: Actively set the synthetic gained white light of red, green, and blue.

Shutter: Set the length of shutter exposure. (Some models have support for aperture setting; those that do not have support for aperture setting have only automatic and manual modes)

Automatic mode: The program automatically selects an appropriate exposure time and aperture value according to the currently set Time Exposure and Iris range.

Manual: Directly uses the currently set Time Exposure time and Iris aperture value.

Shutter First: Shutter First is the aperture value obtained by metering the camera with a manually defined shutter.

Iris First: Aperture priority, where the size of the aperture is defined manually and the camera's metering is used to obtain the corresponding shutter value.

Note: The exposure time in shutter manual mode removes the flickerless option, the exposure time in shutter auto mode opens the flickerless option, and if you switch to manual mode again, the exposure time will automatically switch to 1/100 or 1/120.

Exposure Time: Set the exposure time of the camera, used in combination with Shutter. When the exposure time is long, the image will be overblown, and when the exposure time is short, the image will be dark.

Defog Mode: Defog mode. Turn it on to make the picture clearer in rainy and foggy weather.

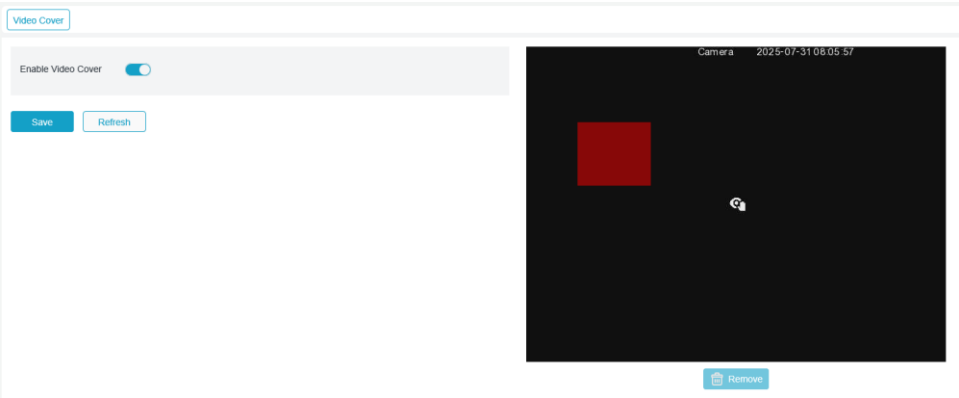
3D Noise Reduction: Reduces noise in the image to make the picture clearer, with three modes:

- Automatic mode:** The camera automatically selects the noise reduction effect according to the algorithm.
- OFF:** Noise cancellation is not switched on.
- Manual:** Noise reduction is performed according to the manually set noise reduction coefficient.
- Save:** Saves the parameters for image editing.
- Default:** Restores the image control parameters to the default.
- Refresh:** reacquiring image parameters

8.3. Video Cover

If you want to cover some specific areas of the image screen, this function will allow you to create 4 or 6 (some models support the creation of 6) privacy zones of any size and location.

Enable the switch and select the area where privacy needs to be enabled. The area appears as a "red box". Click on the edge of the red box and drag it to any size to create the privacy area.



- Enable:** Enable/Disable the Video Cover function.
- Video Cover Area Setting:** Set the areas to be tampered in the monitoring screen. The tampered blocks are red while setting and will turn to black after they take effect. set four tampering blocks.
- Remove:** Delete selected video cover blocks.
- Note:** With the privacy area set, the screen covered by the privacy area is not visible during preview and playback.

8.4. Video Parameters

This menu allows the user to configure the parameters of the screen preview and the recording parameters.

8.4.1. Recording Parameters

This menu configures the parameters related to system recording.

RecordMainstreamSubstreamThirdstreamAudio

Stream ModeMainstream

Record

PreRecord

Netbreak

Save

Refresh

Stream Mode: Select the recording mode. The video stream saved in the SD card. The default is Mainstream.

Record: Check to enable recording.

PreRecord: If this option is enabled. The camera will start recording a few seconds before an alarm event occurs. This option is recommended for users whose main type of recording is based on motion detection or I/O alarms.

Netbreak Event recording is also performed when the network is disconnected or the connection fails.

8.4.2. Coding Parameters

This menu allows the user to configure the image quality parameters for recorded video or network transmission. Typically, the Master Stream is the quality of the recorded video that will be saved in the HDD; the Sub Stream is the quality of the preview video that will be accessed remotely (e.g. by web clients and VMS). The Mobile Stream (Mobile Stream can be optionally turned off) defines the quality of the preview viewed via remote access using a mobile device.

Record
Mainstream
Substream
Thirdstream
Audio

Resolution
2880 x 1620

Frame Rate
25

Encoding Format
H.265

Video Code Level
Main Profile

Encoding Mode
CBR

Config Mode
Predefined

Bitrate
3072
Kbps

I Frame Interval
50
(1 ~ 100)

Audio
☒

Save
Default
Refresh

Resolution: This parameter indicates the resolution of the recorded image.

Frame Rate: This parameter indicates the number of frames recorded by the camera.

Encoding Format: Channel decoding type, there are H264, H265, H264+, H265+ and MJPEG.

(MJPEG mode exists only in sub-stream mode)

Video Code Level: Video quality level with Bestline, Main Profile and High Profile.

(Main Profile only when H265).

Encoding Mode: Select the bitrate level. For simple scenes, such as a grey wall, Constant Bit Rate (CBR) is appropriate. For more complex scenes, such as busy streets, Variable Bit Rate (VBR) is appropriate.

Config Mode: If you want to set the bitrate yourself, select "User Defined" mode. If you want to select a preset bitrate, select "Preset Mode".

Bitrate: This parameter corresponds to the data transfer speed that the camera uses to record the video. Higher bitrate videos will have better quality.

I Frame Interval: Sets the I frame interval of the camera.

Audio: Enable this option if the user wants to record audio and video at the same time and connect a microphone to the camera or use a camera with audio capabilities.

Save: Save the parameters of the video encoding.

Default: restores the video encoding parameters to the default.

Refresh: recapture the video encoding parameters.

8.4.3. Audio Management

This menu sets the volume of the device.

RecordMainstreamSubstreamThirdstreamAudio

Audio Input TypeMicIn

Output Volume9

Input Volume9

Audio Code TypeG711A

Save

Refresh

Audio Input Type: select the audio input type, there are Mic In and Line In. Mic In means the audio is input through the microphone of the device, Line In means the audio is input through the tail line of the device (supported by some models).

Output Volume: Set the volume of the output audio.

Input Volume: Set the volume of the input audio.

Audio Code Type: Set the audio decoding type, support G711A and G711U.

8.5. Capture Settings

This menu allows the user to configure the parameters related to the Auto Capture function.

Capture

Normal Interval5 S

Alarm Interval5 S

Auto Capture

Save

Refresh

- Normal Interval:** the interval between captures in normal recording.
- Alarm Interval:** alarm interval, the time interval to capture images when motion detection is triggered and IO alarm is triggered.
- Auto Capture:** Enable/disable auto capture.

8.6. Schedule Setup

8.6.1. Record Schedule

Set up regular and alarm recording schedules for a set period of time.

Record

Capture

Table

List

	0	2	4	6	8	10	12	14	16	18	20	22	24
SUN													
MON													
TUE													
WED													
THU													
FRI													
SAT													

Import Template

Save Template

Save

Refresh

☒ Normal
 ☐ Motion
 ☐ I/O

Record

Capture

Table

List

+

 Add

✖

 Delete All

☒ Normal
 ☐ Motion
 ☐ I/O

ID	Start Time	End Time	Day	Operation
1	00 : 00	24 : 00	Every Day	☒ ✖

Import Template

Save Template

Save

Refresh

Table/List: The schedule is presented in table form or list form. Click on Normal, Motion or I/O on the right side to switch between different types of video schedules.

Select Table form and drag or tick the corresponding time period in the table to set the corresponding time schedule.

Select the List form to set the corresponding time schedule by manually adding rules and entering the start and end time periods.

Add: Adds a schedule rule.

Delete All: Delete all schedule rules.

Start Time: Set the schedule rule start time.

End Time: Set the end time of the schedule rule.

Day: Set the period for the schedule rule to take effect.

Import Template: Import a custom or system default schedule template.

Import Template

	Template Name	Edit	Delete
☐	7x24		
☐	5x24		
☐	Test		

Cancel

Import

Edit: Edit this schedule template to modify the template name and specific schedule rules.

Delete: Delete this schedule template.

Note: The system supports two schedule templates, 7x24 and 5x24, by default, which cannot be edited or deleted.

Test

Template Name

Test

Add

Delete All

ID	Start Time	End Time	Day	Operation
1	00 : 00	24 : 00	SUN FRI SAT	
2	00 : 00	03 : 00	MON TUE WED THU	
3	08 : 00	24 : 00	MON TUE WED THU	

Cancel

Apply

Save Template: Save the schedule template, save the currently set schedule rule as a custom template, and import the template in other schedule setting pages.

Record

Capture

Table

List

Add

Delete All

Normal

Motion

I/O

ID	Start Time	End Time	Day	Operation
1	00 : 00	24 : 00	Every Day	

Import Template

Save Template

Save

Refresh

Reference can be made to chapter [8.6.1 Video recording schedule](#).

8.7. Disk Management

This menu allows the user to check and configure the internal TF card. Formatting is only required for initial access and when replacing a new TF card.

Disk

No data available

Overwrite

Auto

Save

Format Hard Disk

Add NetHDD

Refresh

Format Hard Disk: Select the SD card to be format, and then click Format SD Card. To start format, enter your username and password and then click OK.

Overwrite: This option to overwrite old records in the SD card when the SD card is full. If Auto is selected, the oldest data will be automatically overwritten when the SD card is full. Select OFF if you do not want to overwrite any old videos. If this function is disabled, check the status of the SD card periodically to ensure that the SD card is not full.

ADD NetHDD: This function Allow to add a network HDD. After a network HDD (NAS) is configured, connect the NAS to the Internet to record channel videos or capture images. The AI face database can only be stored in the HDD.

Add NetHDD

Mounting Type

SMB/CIFS

Username

Username cannot be empty!

Password

Password cannot be empty!

Server IP

000.000.000.000

IP format error...!

Directory Name

Can not be empty

Disk Size

Default

(4 - 8192)GB

Test

Add NetHDD

Mounting type: There are two options, Including NFS and SMB/CIFS. Among them, NFS does not need username and password, but SMB/CIFS needs.

User Name: Specifies the username of NAS (unavailable in NFS mode).

Password: Specifies the password of NAS (unavailable in NFS mode).

Server IP: Specifies the IP address of NAS.

Directory Name: Specifies the folder where you want to store data in the NAS.

Disk Size: Specifies the size of the network HDD.

Test: Test the connectivity of NAS.

Add NetHDD: Click this option to add NAS.

8.8. FTP server settings

This menu allows the user to enable the FTP server in order to view pictures and videos uploaded from the camera to FTP on the FTP server.

FTP

FTP Enable

☐

FTP Protocol

FTP

Server

Port

21

(1 ~ 65535)

Username

Password

DIR Name ?

Transfer images

☐

Save

Test

Refresh

FTP Enable: Click to enable the FTP function.

FTP Protocol: modify the FTP protocol, there are two protocols: FTP and SFTP.

Server: Enter the IP address or domain name of the user's FTP server.

Port: Enter the FTP port.

Username/ Password: Enter the user's FTP server username and password.

Transfer images: When checked, the alarm images will be uploaded to the FTP server.

Transfer Videos: Ticked will upload the alarm video to FTP server.

8.9. I/O Settings

8.9.1. Alarm input settings

This is an optional feature that is only available if the user's device supports I/O sensors and an external I/O alarm device is connected.

Alarm Input

Alarm Output

Alarm Input No.	Type	Enable	Settings	Edit
Local-1	Normally-Open	Disable	Disable	Edit

Save

Refresh

To set the I/O input alarm parameters, click Edit to enter the setting page.

✕

Alarm Input No.

Settings

Local<-1

Input

Alarm Type

Post Recording

Normally-Open

5 S

☒ Schedule ☐ Linkage

	Table	List
SUN		
MON		
TUE		
WED		
THU		
FRI		
SAT		

Import Template
Save Template

Alarm Input No.: Selects the input source for I/O alarms.

Settings: Enables or disables the I/O input alarm function.

Alarm Type: Select the input alarm type.

Post Recording: Set the length of time the device continues to record after triggering an alarm, the default is 5 seconds.

Schedule: Set the schedule for the I/O input alarm function to take effect. Refer to [8.6 Schedule Setting](#).

Linkage: Set the I/O input alarm linkage function.

Advance

Alarm Input No.

Local<-1

Settings

Input

Alarm Type

Normally-Open

Post Recording

5 S

Schedule

Linkage

Normal Linkage

Email

Risco Cloud Push

FTP Picture Upload

Recording Channel

Warning Light

Siren

Alarm Output

Local->1

Email: Sends an email to the configured mailbox when an alert is triggered.

RISCO Cloud Push: Set whether the device will push to the RISCO server after the I/O alarm occurs.

FTP Picture Upload: Uploads the alarm picture to the FTP server after the alarm is triggered.

FTP Video Upload: Uploads the alarm video to an FTP server after the alarm is triggered.

Clicking on the Settings button next to it gives you the option to upload to an FTP server after an alarm is triggered.

Light: When switched on, a warm light will illuminate for warm light deterrence when an alarm is triggered.

Warn Light: When turned on, a red and blue light will be illuminated as a deterrent when an alarm is triggered.

Siren: When on, an alarm will sound for deterrence when triggered.

Alarm Output: Check the alarm output source, the I/O alarm output will be performed when the alarm is triggered. Refer to [8.9.2 Alarm Output Settings](#).

8.9.2. Alarm Output Settings

To set the alarm linkage I/O output parameters, click Edit to enter the setting page.

Alarm InputAlarm Output

Alarm Output No.	Latch Time	Edit
Local->1	5 S	

SaveRefresh

Advance

Alarm Output No.

Local->1

Latch Time

5 S

Alarm Status

Close

TableList

024681012141618202224

SUN

MON

TUE

WED

THU

FRI

SAT

Import Template

Save Template

Trigger

- Alarm Output No.:** Select the I/O output source for alarm linkage.
- Latch Time:** Set the duration of I/O linkage output when the alarm is triggered.
- Schedule:** Set the schedule for the alarm linkage I/O output function to take effect. Refer to chapter [8.6 Schedule Setting](#).

8.10. Deterrence Settings

When the camera supports white light, red and blue light function, this menu can be configured deterrent parameters; when the alarm is triggered linked to the deterrent, the light will be lit in accordance with the configured parameters of the way to alarm. See the following screen:

Deterrence

Light

Warning Light

Light Duration(s)

60

(5 ~ 180)

Warning Light Duration(s)

60

(5 ~ 180)

Light Mode

Steady Mode

Table

List

024681012141618202224

SUN

MON

TUE

WED

THU

FRI

SAT

Import Template

Save Template

Save

Refresh

Note: When the camera supports white light and the image control is set to full-color mode, the white light parameters such as Light are greyed out and cannot be set; when the image control is set to day/night mode, this interface parameter can be set; when the image control is set to smart night light mode, the Warning Light parameter is greyed out and cannot be set.

Light: Turns the light warning on or off.

Light Duration (s): The duration of the white light.

Light Mode: Set the white light mode, there are 2 modes:

Steady Mode: Always on mode, the white light is always on when deterring.

Flashing Mode: Flashing mode, the white light flashes at a set frequency during deterrence.

Warning Light: Turns the red and blue warning lights on and off.

Warning Light Duration (s): The duration of the red and blue lights.

Schedule: Setting up the schedule for when the warm-up and red and blue lights will take effect. Refer to [8.6 Schedule Setting](#).

8.11. Siren Settings

When the camera supports siren This menu allows you to configure alarm-related parameters; when the alarm is triggered by the linkage deterrent, the alarm will be automatically turned on for deterrence. See the following screen:

Siren

Siren

Siren Type

Alarm1

Siren Volume

1

9

10

Siren Duration(s)

10

(5 ~ 180)

Table

List

0

2

4

6

8

10

12

14

16

18

20

22

24

SUN

MON

TUE

WED

THU

FRI

SAT

Import Template

Save Template

Save

Refresh

Siren Type: Changes the audio file of the siren.

Default provides two audio files, in addition to support the import of three custom pcm and wav audio file types, the imported file audio sampling rate can not exceed 8000HZ, the file size can't exceed 256k; selected custom imported audio file on the right side of the Delete button, click on the current audio file can be deleted (Note: Some models support this feature).

Siren Volume: Alarm sound volume level, supports 1 to 10 adjustable levels.

Siren Duration(s): The duration of the alarm sound, support 5 ~ 180 seconds adjustable.

Schedule: Set the schedule of the effective time of the alarm. Refer to [8.6 Schedule Setting](#).

8.12. Disarming

Enabling the disarm function can revoke the response of the device to all kinds of alarm linkage, this menu can set the disarm switch, type, schedule and other related parameters.

Disarming

Schedule

Disarming

Action

☐ All

☐ Email

☐ Alarm Out

☐ Audio and light alarm

☐ Risco Cloud Push

☐ Privacy Mode

Note:

"Audio and light alarm" refers to the built-in Deterrence Siren

"Alarm Out" refers to the external alarm connected to the Alarm Out interface.

Save

Refresh

Disarming: Enables or disables the disarming function.

Action: IPC local alarm linkage type.

All: Select or clear all types.

Email: When disarming function is enabled, tick the mailbox alarm to trigger the alarm without sending alarm email.

Audio and light alarm: When disarming function is enabled, the alarm is triggered when this option is ticked, and the red and blue lights, warm-up light and siren do not respond.

Privacy Mode: When disarming function is enabled, tick Privacy Mode and IPC will enable privacy mode. (Only multi-channel devices support channel setting)

Alarm Out: When disarming function is enabled, check Alarm Out to trigger alarm, external alarm output device is not effective.

RISCO Cloud Push: Enable to prevent the NVR from automatically pushing to the RISCO server when an alarm is triggered while one-click disarming is enabled.

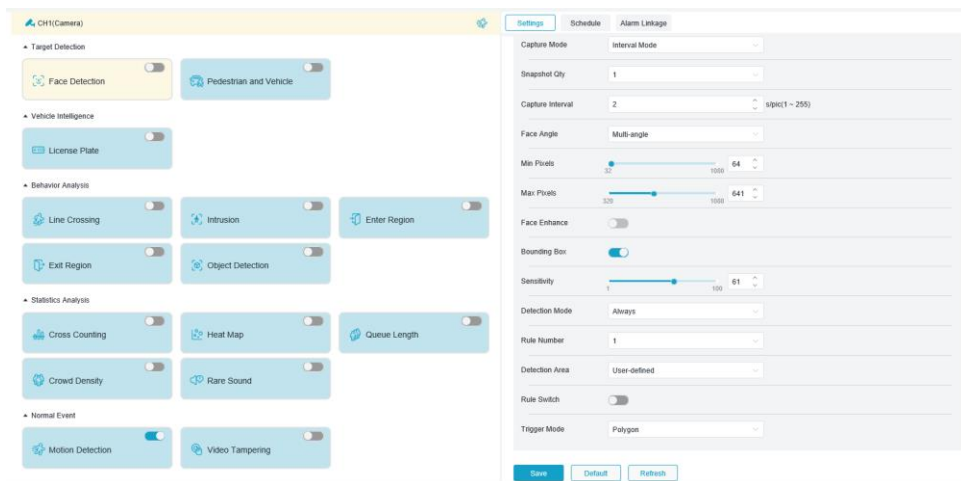
Schedule: Set the schedule for the effective time of disarming. [Refer to 8.6 Schedule Setup.](#)

8.13. Event Settings

The camera uses AI intelligent alarm, you need to open the corresponding alarm function in the Setup menu first. Opening the function needs to consume the computing power of the camera, due to the limitations of the performance of the camera. Some of the AI functions do not support simultaneous opening, please refer to the relevant limitations of the specific model prompt shall prevail.

8.13.1. Face Detection

The face detection function is to detect the face target through the camera first, get the captured image that meets the requirements, then calculate the face feature data of the captured image through the face model algorithm, and then compare it with the face database for alarm. To do this, you need to enable the face detection function first.



Face Detection: Enable the face detection function.

Capture Mode: Set the snap mode. receive push notifications in live view or connect an NVR to check the image effect. The program supports three Snap Modes.

Optimal Mode: The camera only pushes an image that it considers best from detecting an object until the object disappears.

RealTime Mode: When detecting an object, the camera immediately pushes an image, and then pushes the best image when the object disappears.

Capture Interval: set the snap number and the snap and push interval as required. The options for Snap Num include 1, 2, 3, and unlimited. The Snap Frequency ranges from 1s to 255s. For example, when the snap frequency is set to 5s, an image is pushed at 5s, 10s and 15s when the object is detected.

Face Angle: Screen the captured images. That is, only the captured images that meet angle setting will be pushed. There are three mode options.

Frontal View: Only the frontal view of an object is pushed.

Multi Angle: Choose to push images containing only side faces.

Customize: Customize the angle of an object for which images can be pushed. If this function is enabled, Roll Range, Pitch Range, Yaw Range, and Picture Quality options, as well as Frontal Default and Multi Default buttons will be available.

Roll Range: Set the roll range of the captured face image in the 3D model. When the angle does not meet the setting limit, face detection can be carried out but the image will not be pushed.

Pitch Range: Set the pitch range of the captured face image in the 3D model. When the angle does not meet the setting limit, face detection can be carried out but the image will not be pushed.

Yaw Range: Set the yaw angle of the captured face image in the 3D model. When the angle does not meet the setting limit, face detection can be carried out but the image will not be pushed.

Picture Quality: High quality images are good for filtering out detected non-face images.

Frontal Default Apply Mode: Selecting Customize displays the control, setting the values for Push Angle to Range: 30, Pitch Range: 30, Yaw Range: 45, and Picture Quality: 100.

Multi Default Apply Mode: Selecting Customize displays the control, setting the values for Push Angle to Range: 180, Pitch Range: 180, Yaw Range: 180, and Picture Quality: 100.

Min Pixels: Set the minimum recognition pixel frame. The face has to be larger than the set pixel to be recognition. When the mouse moves to the progress bar, the image preview on the right side will show the actual size of the pixel frame, and drag the pixel frame to set it at the same time, and the pixel frame in the image preview disappears when the mouse moves away for 5 seconds.

Max Pixels: Set the maximum recognition pixel frame. The face has to be smaller than the set pixel to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame disappears in the image preview.

Sensitivity: The higher the sensitivity, the missed alarms will decrease, but the false alarms will increase.

Face Enhance: Face Enhance switch to increase the capture effect on moving targets. It also adjusts the brightness according to the face closest to the camera to optimise the capture effect (supported by some models).

Face Attribute: Identify the attributes of the detected faces, including age, gender, mask, glasses, and expression. Note: You need to open this function to use Face Features alarm.

Detection Mode: Filter the performance of detected objects in the camera. There are two mode options.

Hybrid Mode: Allow do face detection for all objects in the view.

Motion Mode: Allow to filter out motionless faces, such as such as portraits and statues in the scene.

Bounding Box: Display face detection box, detect rule line switch (supported by some models).

Trigger Mode: Set the detection rule line type. There are two rule types.

Rectangle: Allow to detect only face objects in the set area.

Line: Face objects are tracked only when the detection line is crossed according to settings.

Detection Area: Setting options are changed when the detection area is used to recognize objects by default. There are two modes.

Full Screen: All areas that can be monitored by the camera are detected.

User-defined: Only user-defined boxed areas are detected.

Rule Number: Rule number selection, support to set 4 detection rule areas.

Rule Switch: Rule enable switch, each detection rule has an independent enable switch, associated with the currently selected Rule Number.

Rule Type: The setting item is available only when using the over-line detection mode, and there are two detection trigger modes: $A \rightarrow B$ and $B \rightarrow A$.

Rule Line Setting Area: According to the parameter setting, set the detection area or detection trigger line in this area.

Add: Add a default detection rule in the setting area.

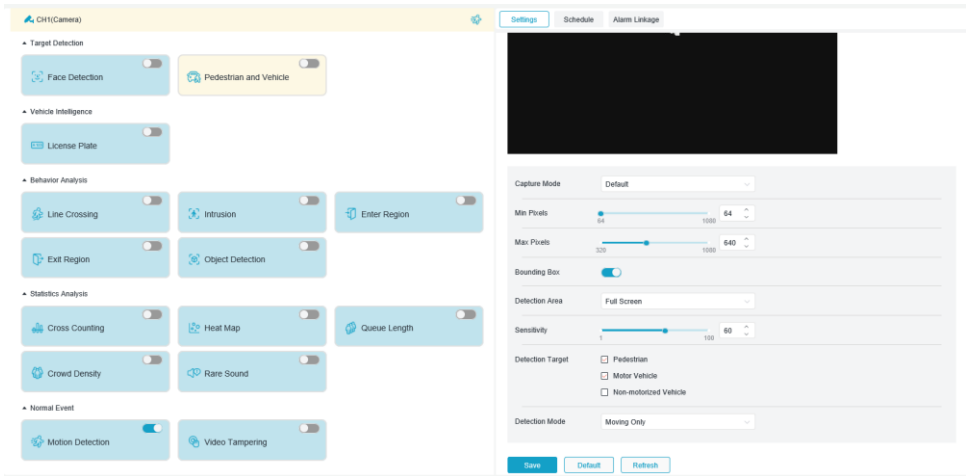
Draw: Manually draw a detection rule in the setting area.

Remove: Removes a detection rule from the setting area.

Remove All: Remove all detection rules in the setting area

8.13.2. Pedestrian and Vehicle

Pedestrian detection and vehicle detection function, used to recognize pedestrian or vehicles in the view, generate an alarm, and record capture images, according function settings.



Pedestrian & Vehicle: Enable Pedestrian & Vehicle detection function.

Capture Mode: set the snap mode. receive push notifications in live view or connect NVR to check the image effect. The program supports three Snap Modes.

Default: The camera pushes only one pedestrian or vehicle image from detecting an object until the object disappears.

RealTime Mode: When detecting an object, the camera immediately pushes one image, and then pushes another image when the object disappears.

Interval Mode: Push pictures for a set number of times according to the set push interval. When using Snapshot Mode as Interval Mode, there are Snapshot Qty and Capture Interval settings:

Snapshot Qty: according to the interval set by Capture Interval, push the image 1, 2, 3, infinite times for the camera thinks it is the same target.

Capture Interval: Push the image according to the set time from the target appearance or last push time.

Min Pixel: Set the minimum recognition pixel frame. The pedestrian and vehicle has to be larger than the set pixel to be recognition. When the mouse moves to

the progress bar, the image preview on the right side will show the actual size of the pixel frame, and drag the pixel frame to set it at the same time, and the pixel frame in the image preview will disappear after the mouse moves away for 5 seconds.

Max Pixel: Set the maximum recognition pixel frame. The pedestrian and vehicle has to be smaller than the set pixel to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview disappears.

Sensitivity: With higher detection sensitivity, pedestrian or vehicle objects can be detected easier, but false alarms may be easily generated.

Detection Target: The options include pedestrian, motor vehicle, non-motorized vehicle, and all.

Detection Mode: Filter object behaviors in the detection area. There are two mode options.

Hybrid Mode: Allow to detect all pedestrians or vehicles in the view.

Motion Mode: Allow to filter out motionless pedestrians or vehicles.

Bounding Box: A detection box that displays the shape of pedestrian vehicle and detects rule line switches.

Detection Area: Detection area setting, there are two modes.

Full Screen: All areas that can be monitored by the camera are detected.

User-defined: detect only the area selected by user-defined box.

Rule Number: Rule Number selection, supports setting 4 detection rules.

Rule Switch: Rule Enable Switch, each rule has its own enable switch, associated with the currently selected Rule Number.

Rule Line Setting Area: When using the custom detection area mode, setting the detection area of 3-8 sides is supported.

Add: Add a default detection rule in the setting area.

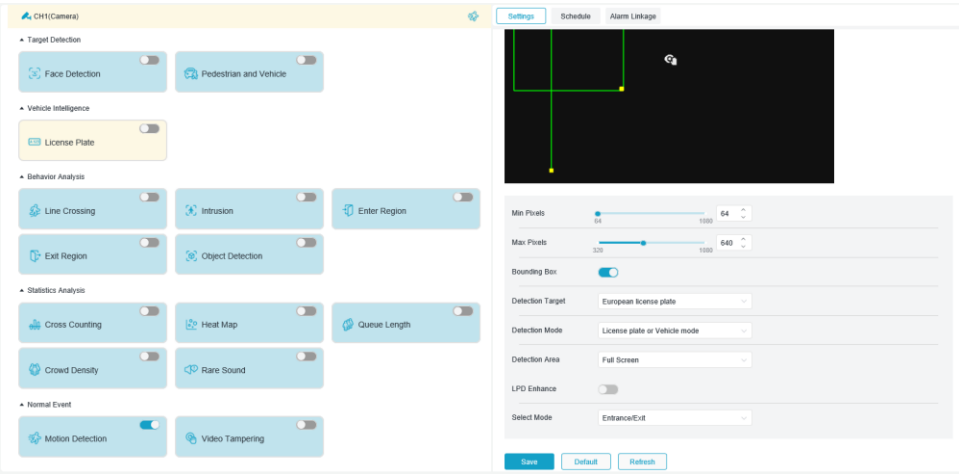
Draw: Manually draw a detection rule in the setting area.

Remove: Removes a detection rule from the setting area.

Remove All: Remove all detection rules in the setting area.

8.13.3. License Plate

License Plate Detection Function by detecting the license plate of the passing vehicle, it identifies whether the vehicle is an unfamiliar vehicle or a vehicle that has been entered into the database and alarms it, so it is necessary to turn on the number plate detection function first.



License Plate : Enable the License Plate detection.

Min pixel: The minimum pixel box, the license plate must be larger than the set minimum pixel to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview will disappear.

Max pixel: Maximum pixel frame, the license plate has to be smaller than the set maximum pixel in order to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview will disappear.

Detection Target: Type of license plates to be detected. There are two type options.

European license plate: License plates in European regions.

American license plate: License plates in American regions.

Detection Mode: Set the detection mode options, there are two kinds as below:

Vehicle priority mode: Vehicle priority mode will detect the vehicle first, and then capture the license plate for analysis.

License plate or Vehicle mode: The license plate will be detected and analysis at the same time when the vehicle is detected.

Bounding Box: Display the detection box and detect the rule line switch.

Detection Area: Set the area for license plate detection, there are two kinds as below:

Full Screen: Detect the whole area monitored by the camera.

User-defined: custom set the detection area.

Rule Switch: Enable switch for the current numbered rule, displayed when setting the custom detection area.

Rule Line Setting Area: According to the parameter setting, set the detection area or detection trigger line in this area.

Add: Add a default detection rule in the setting area.

Draw: Manually draw a detection rule in the setting area.

Remove: Removes the rule selected in the Rule Settings area.

License Plate Enhancement: License Plate Enhancement can only be turned on when the License Plate Detection function is enabled. When License Plate Enhancement is on, the unit will automatically switch to IR-CUT image mode in Day/Night mode, and the settings for Exposure Compensation, Shutter and Exposure Time will be hidden.

Select Mode: Application scenario selection items for license plate detection, there are three kinds as below:

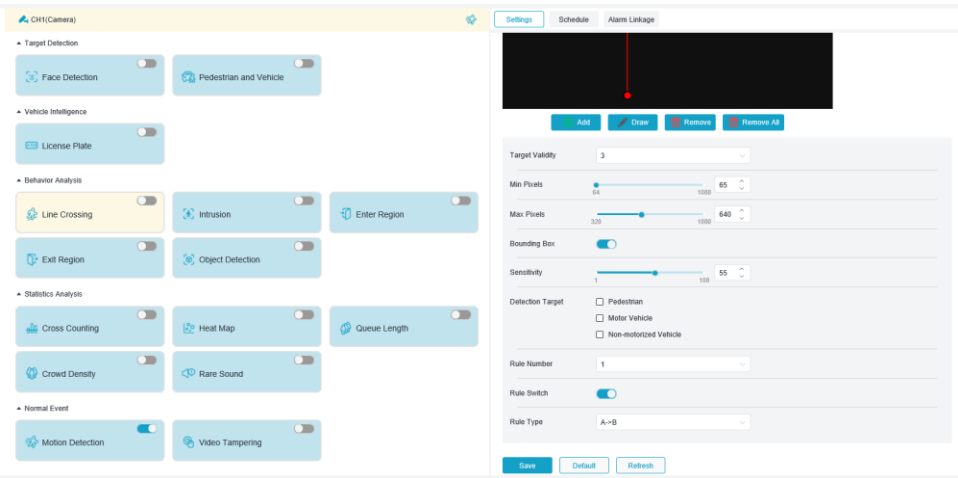
Entrance/Exit: After setting the detection line, the alarm will be triggered when the vehicle passes through the detection area and crosses the detection line.

City Street: After setting the detection line, the alarm will be triggered when the vehicle or license plate passes through the detection area and crosses the detection line.

Alarm Input: Trigger the alarm when the vehicle or license plate is located in the detection area after triggering the I/O input alarm. (Supported by some models).

8.13.4. Line Crossing

The line-crossing detection function detects Pedestrian and vehicles that cross the set virtual line. When a specific target passes through the preset detection line, an alarm signal is generated.



Line Crossing: Enable the Line Crossing detection.

Target Validity: The similarity between the detection target and the set detection type.1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a similarity of 20% or more.

Min Pixel: Set the minimum recognition pixel box, the target has to be larger than the set pixel to be recognition. When the mouse moves to the progress bar, the image preview on the right side will show the actual size of the pixel frame, and drag the pixel frame to set it, and the pixel frame disappears in the image preview after the mouse moves away for 5 seconds.

Max Pixel: Set the maximum pixel frame to be recognition, the target has to be smaller than the set pixel to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview disappears.

Sensitivity: The sensitivity is related to the proportion of the detection target entering the area, the larger the sensitivity setting is for crossing the line, the easier it is to trigger the alarm. For example, if it is set to 100%, the alarm will be

triggered when the detection target just touches the boundary of the set area. If it is set to 50%, the alarm will be triggered after 50% of the detection target has crossed the boundary of the set area.

Detection Target: set objects for perimeter intrusion detection:

Pedestrian: Line crossing alarm is triggered only for pedestrians.

Motor Vehicle: Line crossing alarm is triggered only for motor vehicles.

Non-motorized Vehicle: Line crossing alarm is triggered only for non-motorized vehicles.

Bounding Box: Display the detection rule line switch.

Rule Number: Rule number selection, Line Crossing function supports to set 4 inspection rule lines.

Rule Switch: Enable switch for rule line, each rule line has its own enable switch, which is related to the currently selected Rule Number.

Rule Type: the rule to be triggered by the rule line, there are three kinds of crossing rules: $A \rightarrow B$, $B \rightarrow A$ and $A \leftrightarrow B$. The setting is related to the currently selected Rule Number.

Rule Line Setting Area: According to the parameter setting, set the detection area or detection trigger line in this area.

Add: Add a default detection rule in the setting area.

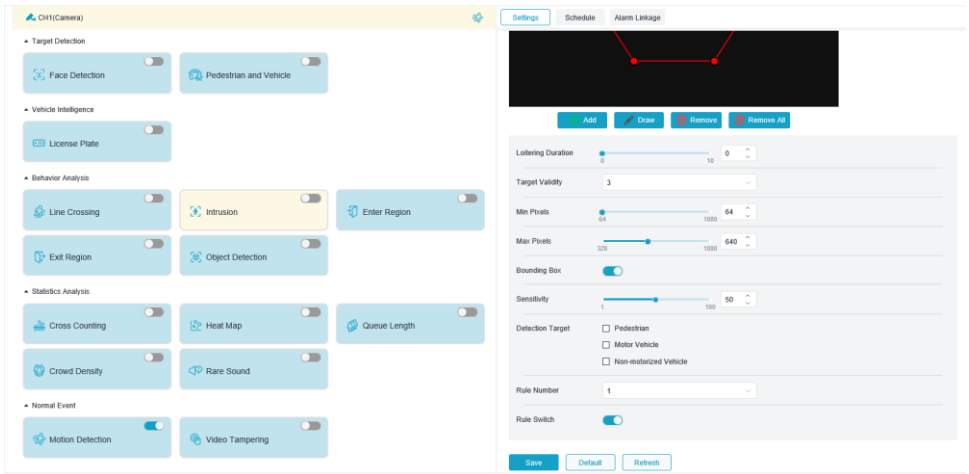
Draw: Manually draw a detection rule in the setting area.

Remove: Removes the rule selected in the Rule Settings area.

Remove All: Remove all rule lines.

8.13.5. Intrusion

Intrusion detection can detect whether there are objects in the video invade the set restricted area, according to the judgement results linkage alarm.



Intrusion: Enable or disable the Intrusion detection function.

Loitering Duration: Indicates that the alarm is generated after the target enters the alert area and stays there continuously for that amount of time. For example, if it is set to 1, the alarm will be triggered immediately after the target has invaded the area for 1s, and the maximum length of time can be set to 10s.

Target Validity: The similarity between the detection target and the set detection type. 1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a similarity of 20% or more.

Min Pixel: Set the minimum recognition pixel box, the target has to be larger than the set pixel to be recognition. When the mouse moves to the progress bar, the image preview on the right side will show the actual size of the pixel frame, and drag the pixel frame to set it, and the pixel frame disappears in the image preview after the mouse moves away for 5 seconds.

Max Pixel: Set the maximum pixel frame to be recognition, the target has to be smaller than the set pixel to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview disappears.

Sensitivity: Trigger the sensitivity setting for area intrusion detection, the larger the sensitivity setting, the easier it is to trigger the alarm. The larger the sensitivity setting, the more likely the alarm will be triggered. The sensitivity is related to the percentage of the detection target entering the area. For example, if

it is set to 100%, the alarm will be triggered when the target just touches the boundary of the set area. If it is set to 50%, the alarm will be triggered after 50% of the target has already passed the boundary of the set area.

Detection Target: set objects for perimeter intrusion detection:

Pedestrian: Intrusion alarm is triggered only for pedestrians.

Motor Vehicle: Intrusion alarm is triggered only for motor vehicles.

Non-motorized Vehicle: Intrusion alarm is triggered only for non-motorized vehicles.

Bounding Box: Display the detection rule line switch.

Rule Number: Rule number selection, intrusion function supports setting 4 detection rules.

Rule Switch: Enable switch for rule line, each rule line has its own enable switch, which is related to the currently selected Rule Number.

Rule Line Setting Area: According to the parameter setting, set the detection area or detection trigger line in this area.

Add: Add a default detection rule in the setting area.

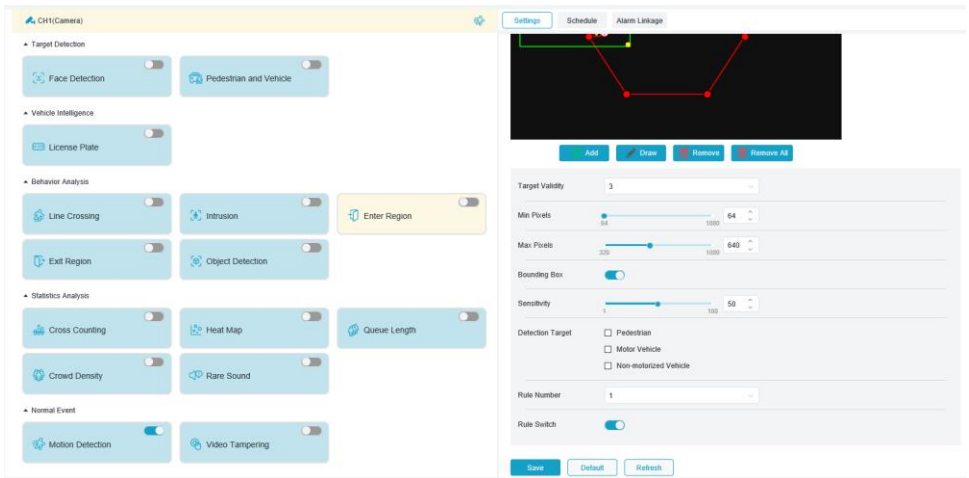
Draw: Manually draw a detection rule in the setting area.

Remove: Removes the rule selected in the Rule Settings area.

Remove All: Remove all rule lines.

8.13.6. Enter Region

Enter Region detection, can detect the target from outside the area into the area, the target generated in the area will not generate alarm, according to the results of the judgement linkage alarm.



Enter Region Enable or disable the Region Entrance detection function.

Target Validity: The similarity between the detection target and the set detection type. 1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a similarity of 20% or more.

Min Pixel: Set the minimum recognition pixel box, the target must be larger than the set pixels to be recognition. When the mouse moves to the progress bar, the image preview on the right side will show the actual size of the pixel box, and drag the pixel box to set it at the same time, and the pixel box in the image preview will disappear after the mouse moves away for 5 seconds.

Max Pixels: Set the maximum pixel frame to be recognition, the target has to be smaller than the set pixels to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview disappears.

Sensitivity: Trigger the sensitivity setting for area entry detection, the larger the sensitivity setting, the more likely to trigger the alarm. The sensitivity is related to the percentage of the detection target entering the area, For example, if it is set to 100%, the alarm will be triggered when the detection target just touches the boundary of the set area. If it is set to 50%, the alarm will be triggered after 50% of the target has already passed the boundary of the set area.

Detection Target: Set objects for Region Entrance detection.

Pedestrian: Region Entrance alarm is triggered only for pedestrians.

Motor Vehicle: Region Entrance alarm is triggered only for motor vehicles.

Non-motorized Vehicle: Region Entrance alarm is triggered only for non-motorized vehicles.

Bounding Box: Display the detection rule line switch.

Rule Number: Region Entrance function supports setting 4 detection rules.

Rule Switch: Each rule line has its own enable switch, which is related to the currently selected Rule Number.

Rule Line Setting Area: According to the parameter setting, set the detection area or detection trigger line in this area.

Add: Add a default detection rule in the setting area.

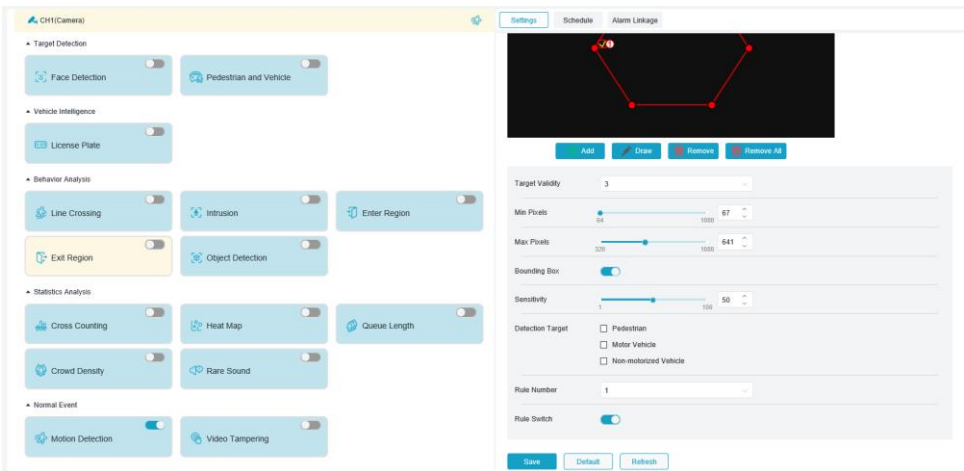
Draw: Manually draw a detection rule in the setting area.

Remove: Removes the rule selected in the Rule Settings area.

Remove All: Remove all rule lines.

8.13.7. Exit Region

Exit Region detection, can detect the target from the area to go outside the area, the target generated outside the area will not generate alarm, according to the results of the judgement linkage alarm.



Exit Region Enable or disable the Region Exiting detection function.

Target Validity: The similarity between the detection target and the set detection type. 1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a similarity of 20% or more.

Min Pixels: Set the minimum recognition pixel box, the target must be larger than the set pixels to be recognition. When the mouse moves to the progress bar, the image preview on the right side will show the actual size of the pixel box, and drag the pixel box to set it at the same time, and the pixel box in the image preview will disappear after the mouse moves away for 5 seconds.

Max Pixels: Set the maximum pixel frame to be recognition, the target has to be smaller than the set pixels in order to be recognition. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview disappears.

Sensitivity: Trigger the sensitivity setting of area region exiting, the larger the sensitivity setting, the more likely to trigger the alarm. Sensitivity correlates with the proportion of the detection target that exits the area. For example, if it is set to 100%, the alarm will be triggered when the detected target has just touched the boundary of the set area. If it is set to 50%, the alarm will be triggered after 50% of the target has already passed the boundary of the set area.

Detection Target: Set objects for perimeter region exiting detection:

Pedestrian: Region Exiting alarm is triggered only for pedestrians.

Motor Vehicle: Region Exiting alarm is triggered only for motor vehicles.

Non-motorized Vehicle: Region Exiting alarm is triggered only for non-motorized vehicles.

Bounding Box: Display the detection rule line switch.

Rule Number: intrusion function supports setting 4 detection rules.

Rule Switch: Each rule line has its own enable switch, which is related to the currently selected Rule Number.

Rule Line Setting Area: According to the parameter setting, set the detection area or detection trigger line in this area.

Add: Add a default detection rule in the setting area.

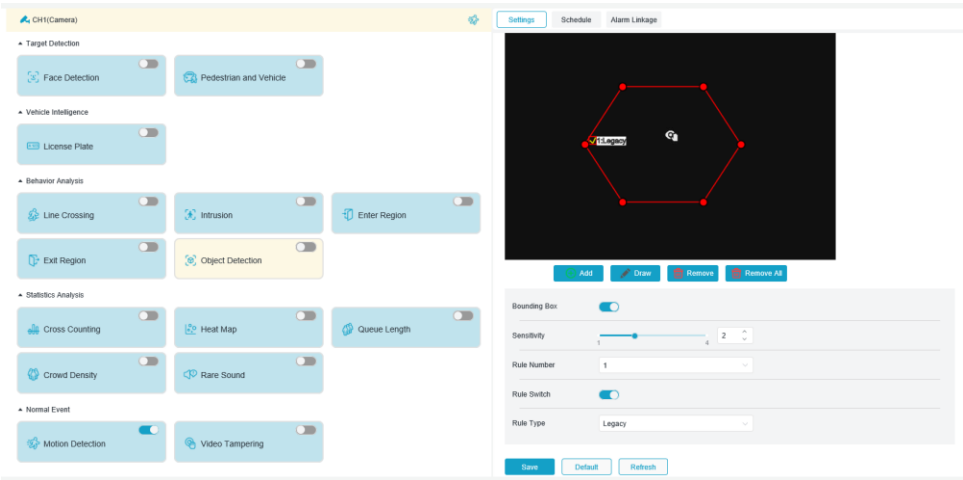
Draw: Manually draw a detection rule in the setting area.

Remove: Removes the rule selected in the Rule Settings area.

Remove All: Remove all rule lines.

8.13.8. Object Detection

Object detection, generating an alarm when an object is found to have been left behind in a supervised scene or when an object is lost.



Object Detection: Enable the Object Detection alarm function switch.

Sensitivity: Filter small interference target settings, the higher the sensitivity, the smaller the detectable object.

Bounding Box: Detection rule line switch.

Rule Number: Support to set 4 detection rules.

Rule Switch: Each rule has an independent enable switch, associated with the currently selected Rule Number.

Rule Type: Set the detection area to be left or lost items to generate an alarm, there are three kinds of rules, Legacy, Lost, Lost & Legacy, and the settings are related to the currently selected Rule Number.

Rule Setting Area: Set, modify and display edited rules.

Add: Add a default detection rule to the setting area.

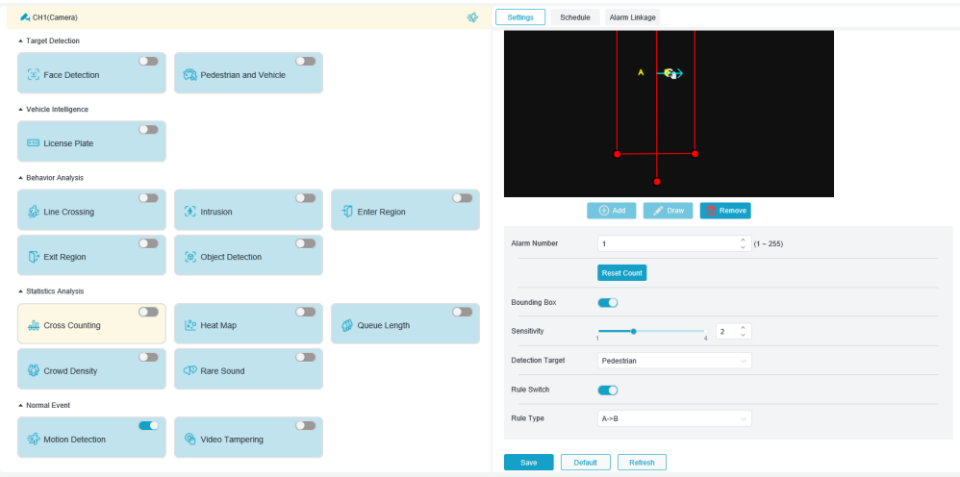
Draw: Manually draw an inspection rule in the setting area.

Remove: Removes the rule selected in the rule setup area.

Remove All: Remove all rules.

8.13.9. Cross Counting

Cross Counting function to make a cross line record of specific objects in the monitoring area. Set the crossing line with two areas AB on both sides of the set line. For example, if the trigger rule of the rule line is $A \rightarrow B$, when the object enters from the area of A and passes through the detection line, and leaves the area of B, the count of in is increased by 1. when the object enters from the area of B and passes through the detection line, and leaves the area of A, the count of out is increased by 1. In the case of triggering the increase of the counting, an alarm will be generated only when the in count minus out of the current counting is greater than or equal to the Alarm Number count of the setup, and the interface is shown in the following figure. The interface is shown in the screen below.



Cross Counting: Enable or disable the Cross Counting function.

Sensitivity: Filter small interference target settings, the higher the sensitivity, the smaller the detectable object, can also be used to detect more distant targets in the scene.

Detection Target: Set the type of target to be recognition by Cross Counting over the line detection, there are 4 modes, switching to save will clear the current count.

Motion: detect all objects, including people, cars, cartons and other objects.

Pedestrian: only identify the target in human form.

Motor Vehicle: Only motorized vehicles are identified.

Non-motorized Vehicle: Identify only non-motorized vehicles.

Alarm Number: Set the conditions for triggering the alarm. The camera will trigger the Cross Counting alarm when the trigger count is updated and the in count minus the out count is greater than or equal to the current setting.

Reset Count: Clear the currently displayed count.

Bounding Box: Detect rule line switch.

Rule Switch: Enable the switch for the current numbered rule line.

Rule Type: set the direction to increase the trigger count of in and out counts, there are two kinds: $A \rightarrow B$ and $B \rightarrow A$. For example, if $A \rightarrow B$ is selected, the in count will be increased when the monitoring target enters the region A and leaves the region B, and the out count will be increased when the target enters the region B and leaves the region A.

Cross Line Setting Area: Set the rule line for Cross Counting detection in this area.

Add: Add a default detection rule in the setting area.

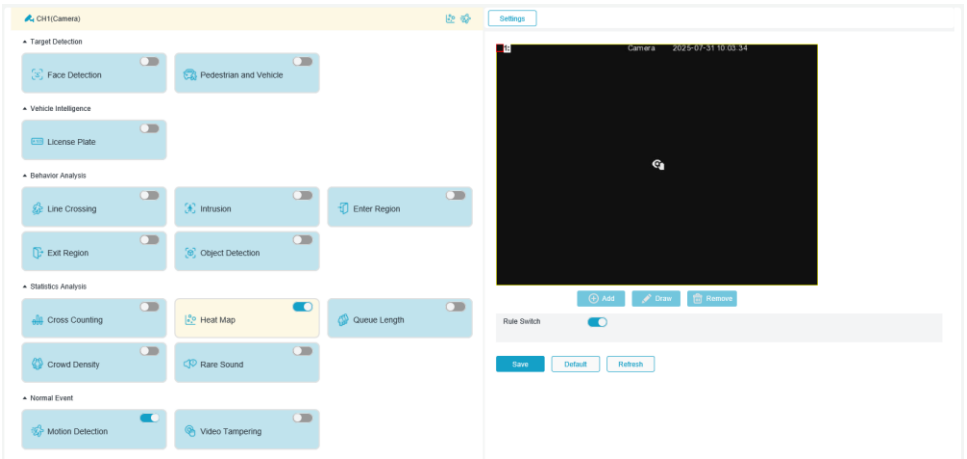
Draw: Draw a detection rule manually in the setting area.

Remove: Removes the rule line selected in the Rule Line Setup area.

Count area: display the count of Cross Counting statistics. refer to section 8.1 to adjust the display position.

8.13.10. Heat Map

Heat map, the user can set all or specific areas, used to detect the specified area of the personnel active information. And the changes will be saved and uploaded at 10-minute intervals. Through the heat map report, the distribution of personnel can be visually presented for both time or space dimensions, which makes it easy to understand the activity level of each area in the scene. This function only supports data recording, not alarm.



Heat Map: Enable or disable Heat Map statistics function.

Rule Switch: Enable the rule switch for the current number.

Monitoring Area Settings: Sets the area where the camera's Heat Map function will count the heat, by default all areas are checked.

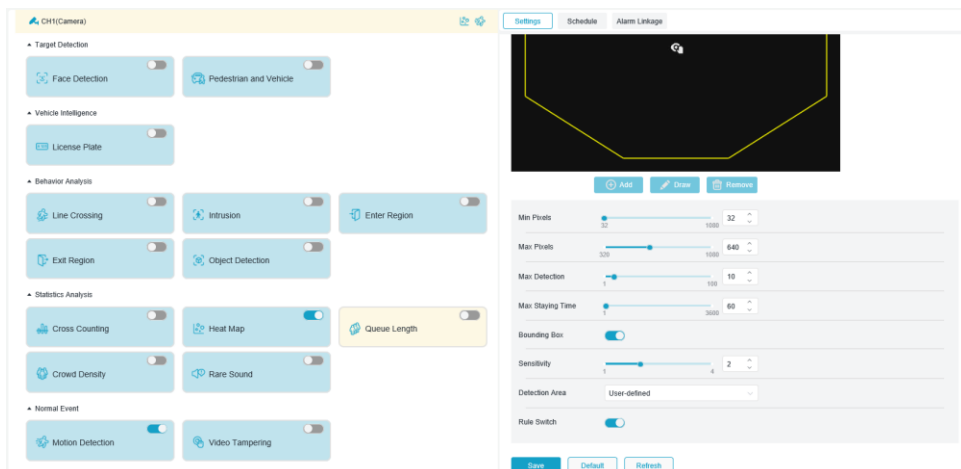
Add: Add a default detection rule to the setting area.

Draw: Manually draw a detection rule in the setting area.

Remove: Removes the rule selected in the Rule Settings area

8.13.11. Queue Length

Queuing detection function, by monitoring the number of people queuing in the set queue area, as well as the queuing waiting time, generates an alarm when the queue is too long or the queuing time is long.



Queue Length: Enable or disable Queue Length detection function.

Min Pixels: Based on the resolution of 1080P, filter out the targets with head smaller than the setting in the screen. When the mouse moves to the progress bar, the image preview on the right side will show the actual size of the pixel frame, and drag the pixel frame to set it at the same time, and the pixel frame in the image preview will disappear after the mouse moves away for 5 seconds.

Max Pixels: Based on the resolution of 1080P, filter out the targets with head larger than the setting in the screen. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and at the same time, drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview disappears.

Max Detection: Maximum value of heads allowed to be detected in the detection area, exceeding this value generates an alarm.

Max Staying Time: the maximum length of time allowed to stay in the detection area, when more than the set length of time, no personnel to leave the detection area to generate an alarm. (This time length statistics from the last person to leave the region to start timing, to reach the set length of time has not yet left the personnel, it will be considered processing timeout, triggering an alarm)

Note: Only when there is a target to leave the detection area to restart counting, the sudden disappearance of the target in the region is ignored. only in the region when there is a detected target to count.

Sensitivity: Filter the smaller interference target settings, the higher the sensitivity, the smaller the target can be detected.

Bounding Box: display the detection box, detect the rule line switch.

Detection Area: Set the area to be detected by the queuing detection function, there are two modes.

Full Screen: Detect the whole area monitored by the camera.

User-defined: Custom the detection area.

Rule Switch: Enable switch for the current numbered rule, displayed when setting the custom detection area.

Detection area setting: Open the setting when opening the custom detection area, support to set the detection area of 3-8 sides.

Add: Add a default detection rule to the setting area.

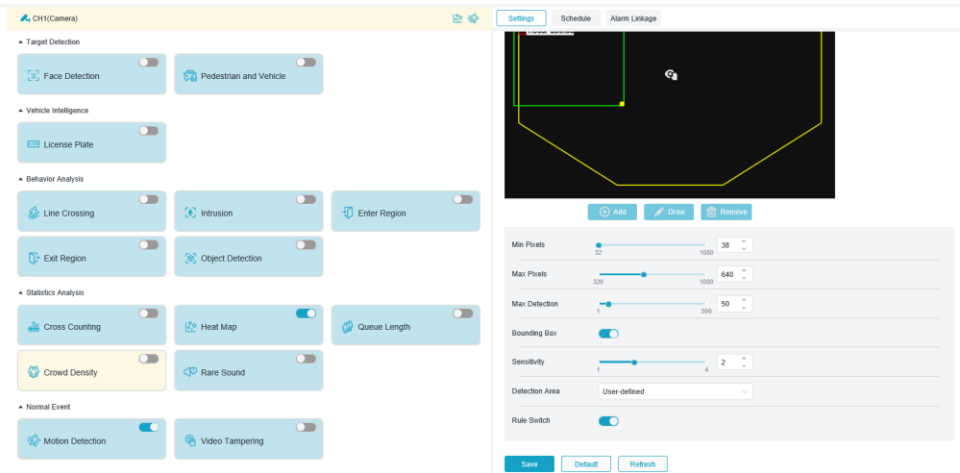
Draw: Manually draw an inspection rule in the setting area.

Remove: Delete the selected rule in the rule setting area.

Count Display Area: Display the number of people in the current monitoring area and the time the queue is waiting for the person who is serving to finish the service, please refer to section 8.1 for the adjustment of the display position.

8.13.12. Crowd Density

Crowd density detection function, through the human figure recognition function to identify the way the human head, identify the number of people appearing in the monitoring area, when the number of people over the preset value to produce an alarm.



Crowd Density: Enable the Crowd Density detection function.

Min Pixels: Based on the resolution of 1080P, filter out the targets with head smaller than the setting in the screen. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview will disappear.

Max Pixels: Based on the resolution of 1080P, filter out the targets with head larger than the setting in the screen. When the mouse moves to the progress bar, the right image preview will show the actual size of the pixel frame, and at the same time, drag the pixel frame to set it, when the mouse moves away for 5 seconds, the pixel frame in the image preview disappears.

Max Detection: the maximum value of head detection allowed in the detection area, exceeding this value generates an alarm.

Sensitivity: filtering smaller interference target settings, the higher the sensitivity, the smaller the target can be detected

Bounding Box: display the detection box, detection rule line switch.

Detection Area: Set the detection area of crowd density detection function, there are two modes:

Full Screen: Detect the whole area monitored by the camera.

User-defined: Custom the detection area.

Rule Switch: The current numbered Rule Enable switch, displayed when setting the custom detection area.

Detection Area Setting: Open the setting when opening the custom detection area, support to set the detection area with 3-8 sides.

Add: Add a default detection rule to the setting area.

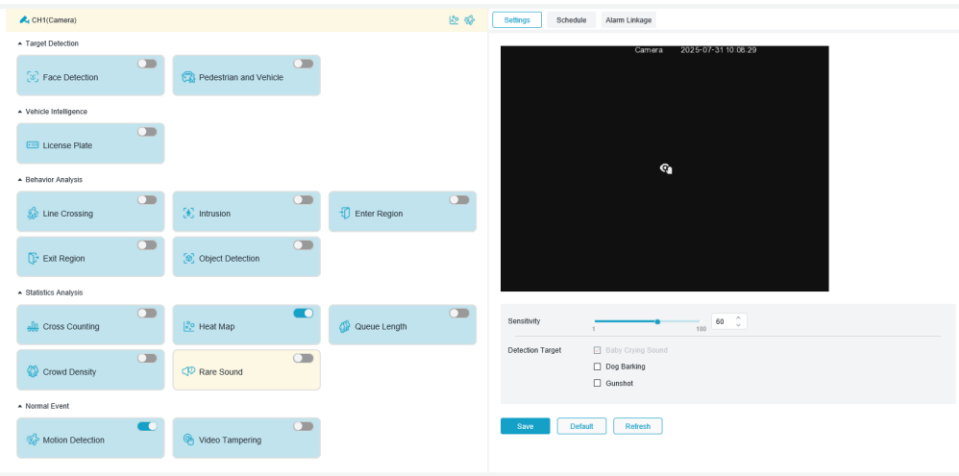
Draw: Manually draw an inspection rule in the setting area.

Remove: Delete the selected rule in the rule setting area.

Count Display Area: Display the number of people in the current monitoring area, please refer to section 8.1 for adjusting the display position.

8.13.13. Rare Sound

Rare Sound detection, according to the needs of the application scene can be set to different detection types, such as children crying, gunshots, dog barking, etc. When the camera detects the set sound alarm.



Rare Sound: Enable or disable Rare Sound detection function.

Sensitivity: Sensitivity, range 1~100.

Detection Target: Detection types.

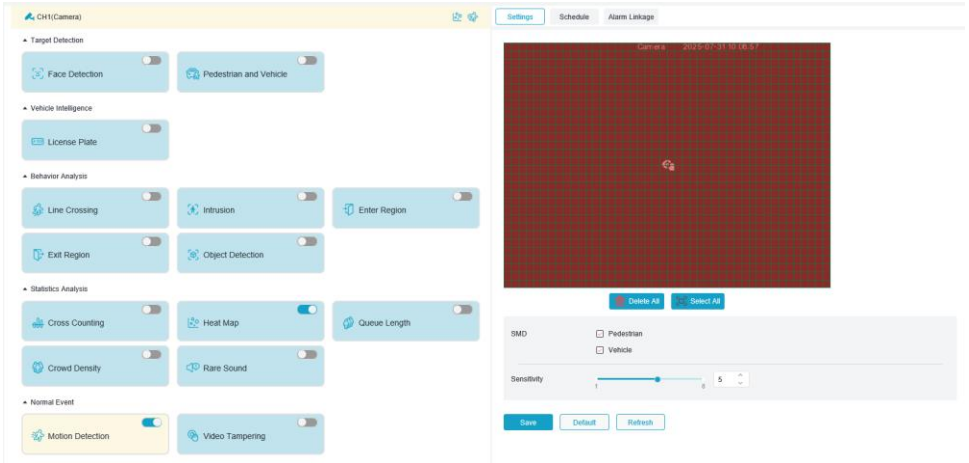
Baby Crying Sound: Check the box to detect baby crying sound.

Dog Barking: Check the box to detect dog barking sound.

Gunshot: Check the box to detect gunshot sound.

8.13.14. Motion Detection

Configure the parameters related to motion detection on this page. When the camera detects motion of a detected target within the frame, the camera will trigger a series of alarms. For example, it will send an email alert containing an additional image of the camera that triggered the alarm to a user-specified email address (if this option is enabled), as well as a push notification via the mobile application.



Drag the left mouse button to delineate the detection zone in the right viewport. Only movements within the zone will trigger the alarm.

Motion Detection: Activate or deactivate motion detection.

SMD: Set the object of motion detection.

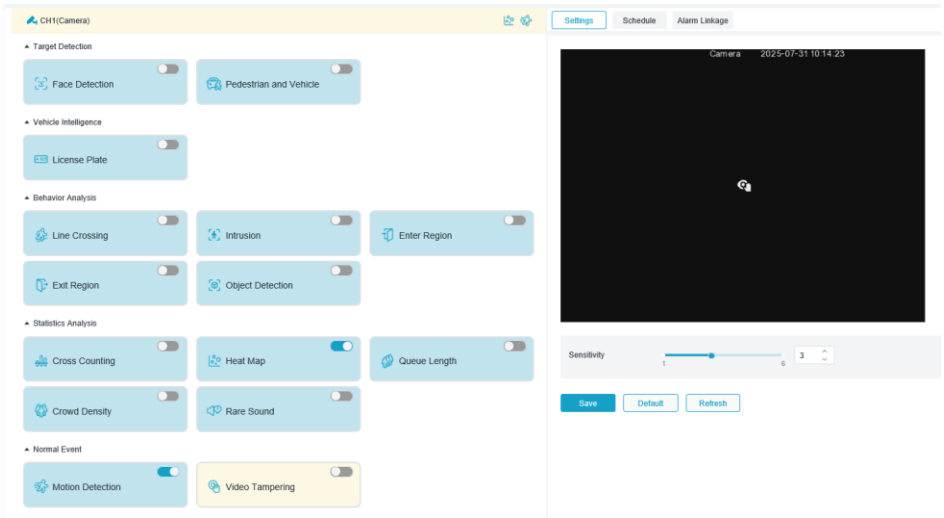
Pedestrian: Only detect the alarm for human targets.

Vehicle: Detect and alarm only vehicle targets.

Sensitivity: Set the sensitivity of motion detection, the larger the value, the more sensitive it is.

8.13.15. Video Tampering

Detects live view screen occlusion and alerts.

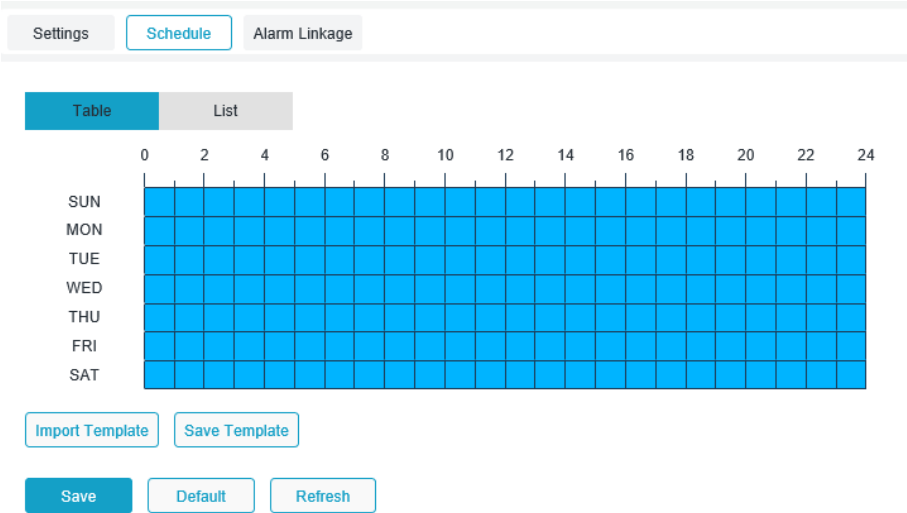


Video Tampering: Switch for camera occlusion detection.

Sensitivity: set the sensitivity of lens occlusion detection, the larger the value the more sensitive.

8.13.16. Event Schedule

To set the schedule for each event to take effect, refer to [8.6 Schedule Setup](#).



8.13.17. Alarm linkage settings

Set the function to be linked when each event triggers an alarm

SettingsScheduleAlarm Linkage

Common Linkage

Event Push Platform

Risco Cloud Push

Email

Picture Upload

FTP

Alarm Output

I/O Output

Deterrence

Siren

Video Linkage

Recording Channel

Recording Delay

5 S

Save

Default

Refresh

Event Push Platform: If the Event Push Platform switch is turned on, the camera sends a message to the third-party platform when the event alarm is triggered. Refer to [8.23.2 Event Push Platform Setting](#).

Risco Cloud Push: Set whether the device will push to the RISCO server after an event alarm occurs.

Email: Whether the camera sends an email when an event alarm is triggered. Click on the Setup button or the Schedule button on the right to set the email parameters, see 8.18 Email Settings.

Picture Upload: If FTP is checked, the camera sends a picture to the associated FTP server when an event alarm is triggered. The FTP server needs to be associated first. Refer to chapter [8.8 FTP Server Settings](#). Click on the Setup

button on the right to select which channel's corresponding alarm picture should be uploaded to the FTP server.

Video Upload: Check FTP to send the video to the associated FTP server when the camera triggers an event alarm. An FTP server needs to be associated with the camera first. Refer to 8.8 FTP Server Settings. Click on the Setup button on the right to select which channel should be uploaded to the FTP server.

I/O Output: The alarm output of the camera's linked I/O when the camera triggers an event alarm. Click the Setup button on the right to tick the I/O alarm output source. The output duration and schedule can refer to [8.9.2 Alarm Output Settings](#).

Deterrence: Light deterrent linkage switch, when alarm is triggered, alarm response will be performed according to the warm light and red and blue light setting parameters in 8.10 Light Deterrence Setting Page. set the parameters directly by clicking the setting button on the right side.

Siren: Siren Deterrent switch, when the alarm is triggered, the alarm response will be made according to the parameter of 8.11 Siren Deterrent Setting Page. set the parameters directly by clicking the setting button on the right side.

Wiegand: Wiegand linkage switch, which transmits to the control system or data center via the Wiegand interface when a license plate is recognised (supported by some models)

Recording Channel: Recording channel linkage switch, click the right setup button to select the linkage channel. When an alarm is triggered, the selected channel will record the corresponding alarm type.

Recording Delay: The delay time for the camera to record after the alarm ends.

8.14. List Management

8.14.1. License plate recognition

The license plate recognition function, which focuses on identifying the identity of the detection target, requires basic data for comparison. The program establishes the database base for license plate matching through the database management function.

Note: Changes to the database require a small system reload to take full effect

License Plate Management									
	Group Name	Delete	Edit	Enable	Alarm	Policy	Fault-tolerant	Alarm Linkage	Alarm Schedule
	Allow List					Allow	< 1 character(s)		
	Block List					Deny	< 1 character(s)		
	Unknown					Unknown	> 1 character(s)		

Add Group
Save
Refresh

Alarm strategy display: In the camera, it only serves as a strategy reminder. Green for white list, red for black list, colorless for unfamiliar license plate list.

Group Name: Edit and modify to show the current group name, the specific group name will be prompted when the alarm is pushed.

Delete: group delete function, the first 3 groups are not allowed to delete.

Edit: Open the picture settings of the grouping reference, for more information, please continue with the content of the following figure.

Enable: license plate recognition using grouped data for comparison.

Alarm: Enable alarm response setting master switch.

Police: Alarm policy, the first 3 groups can not be modified, other groups can be customised as Allow, Deny.

Fault-tolerant: Fault-tolerant characters, allows the search results to display the number of inconsistent characters between the license plate number and the set number of characters, the lower the setting, the higher the match of the search results.

Note: If you want to search the target license plate with only few characters, set the error tolerance rate to the maximum, at this time, many irrelevant license plates will be searched, but the search results are sorted by similarity, and the license plates with high similarity are in the front, so that find the desired target license plate.

Alarm Linkage: Group alarm settings:

Alarm Linkage [Allow List]

Email 

FTP Picture Upload 

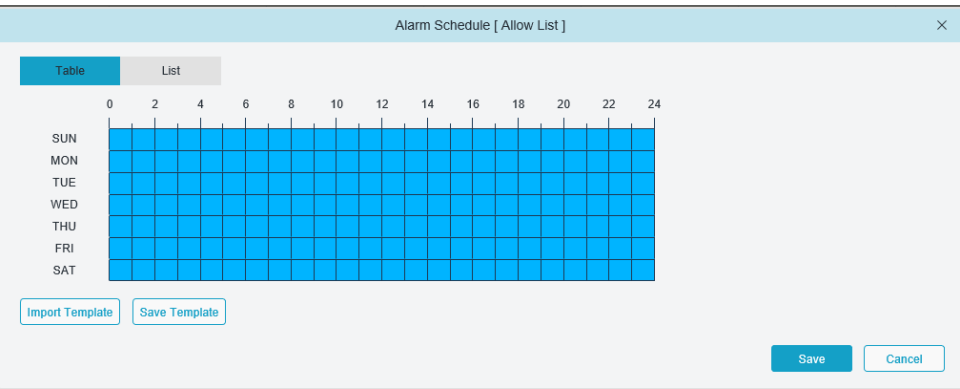
Save
Cancel

Email: Switch to send an email when the grouped face recognition matches are successful.

FTP Picture Upload: Switch to send the picture to the associated FTP server when the group face recognition match is successful.

Note: At the same time by the schedule control effective time, you need to associate FTP server first.

Alarm schedule: Set the effective time of Alarm Out, Email and FTP Picture Upload for group alarm, please refer to chapter 8.6 Schedule Settings.



Click the **Edit** con to set the specific reference data of the corresponding group. The interface is shown in the figure below



There are three ways to add license plate information: Import, Import From CSV, Import From Local Capture. When you add more than 5000 pieces of data, a pop-up box will appear with the content 'Add data has reached the upper limit of the group'.

- (1) Click **Import** button to manually add a single license plate.
- 2) Click **Import From CSV** button to import single or multiple data from CVS form, the format of CVS form is as below.

#	A	B	C	D	E	F	G	H	I	J	K
1	License Plate	Color	Car Brand	Car Type	Owner	Sex	Id Code	Phone	Occupation	Residence	Remark
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27											
28											
29											
30											

Click a piece of data to edit the information of this license plate, after editing, click **Save** button to save, if the modification is successful.  will become .

- 4) **Delete**: Check the checkbox of the license plate information and click the button to delete the license plate information.
- (5) **Move to...**: Tick the checkbox of the license plate information and then click the button to move the license plate information to other groups.
- 6) Click **Export** button to export and save the information of the whole group.

Enable: The license plate recognition uses grouped data for comparison.

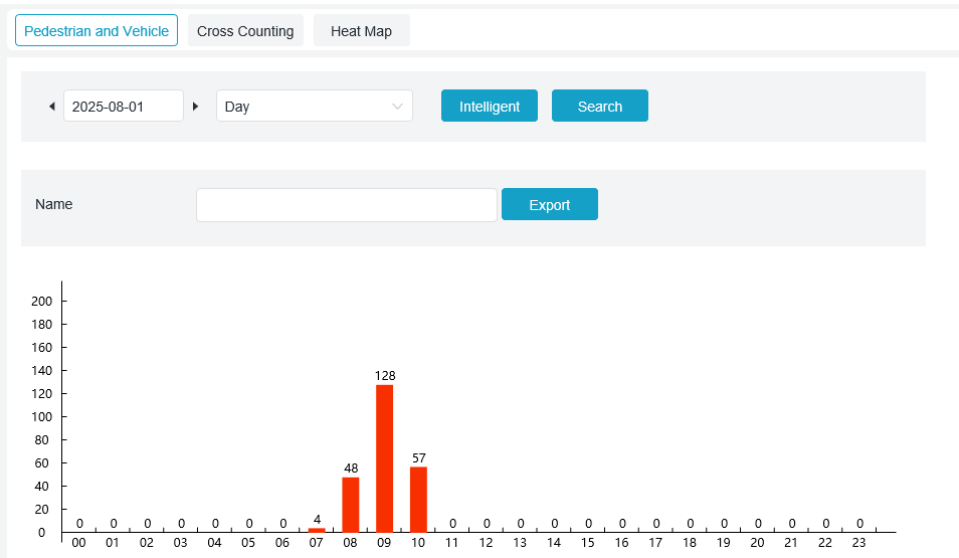
Add Group: Add a new database group, support up to 16 database groups.

8.15. Statistics

AI data statistical analysis function.

8.15.1. Pedestrian & Vehicle

Pedestrian & Vehicle data statistics. Includes alarms for Pedestrian & Vehicle, Line Crossing, Intrusion, Region Entrance, Region Exiting, with the interface shown below.



Time: The reference time for the search pattern.

Search Mode: Data search supports 5 time ranges: Day, Week, Month, Quarter, Year.

Intelligent: search according to the type of marker at the time of capture acquisition, Pedestrian, Motor Vehicle, Non-motorized Vehicle, Line Crossing [Pedestrian], Line Crossing [Motor Vehicle], Line Crossing [Non-motorized Vehicle], Intrusion [Pedestrian], Intrusion [Motor Vehicle], Intrusion [Non-motorized Vehicle], Region Entrance [Pedestrian], Region Entrance[Motor Vehicle], Region Entrance[Non-motorized Vehicle], Region Exiting[Pedestrian], Region Exiting[Motor Vehicle], Region Exiting [Motor Vehicle], Region Exiting [Non-motorized Vehicle], and a total of 18 types of grips.

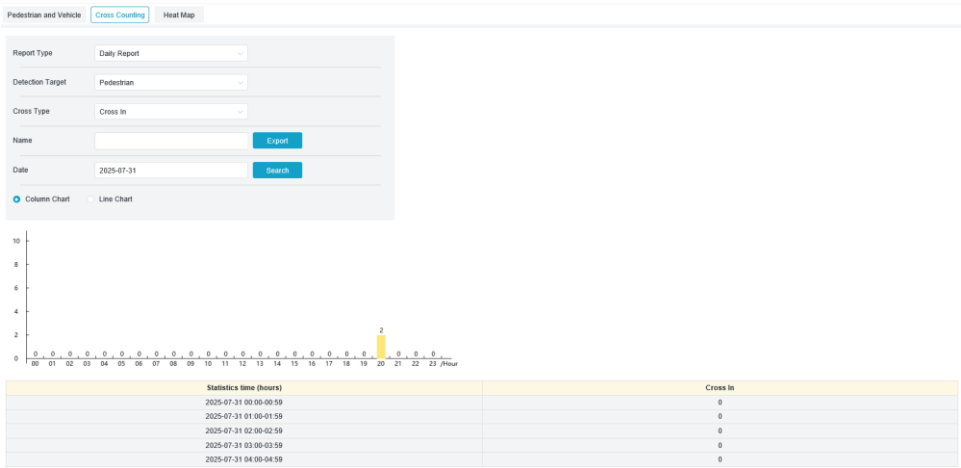
Search: Re-search the data based on the current search settings.

Export: You need to add an export file name to export the current search data using an Excel document.

Display area: Show the current search results in the form of a graph.

8.15.2. Cross Counting

Cross Counting is a function of searching and counting the data across the line, and its function interface is shown in the figure.



Report Type: The data search supports 4 types of time ranges: Daily report, Weekly report, Monthly report and Annual report.

Detection Target: Set the corresponding alarm model that the data needs, for example, the data triggered by Motion cannot be searched by other types. For example, Motion triggered data cannot be searched by other types. There are three types of models, Motion, Person and Vehicle, corresponding to the function settings.

Cross Type: Search data according to the crossing statistics, there are two types of models: Cross In and Cross Out.

Export: You need to add export file name to export the current search data using Excel file.

System time: the reference time of current Report Type.

Mode: Whether the chart in the icon display area is displayed as a bar chart or a line chart.

Display Area: Show the current search results in the form of charts.

Search: Search data according to the current settings.

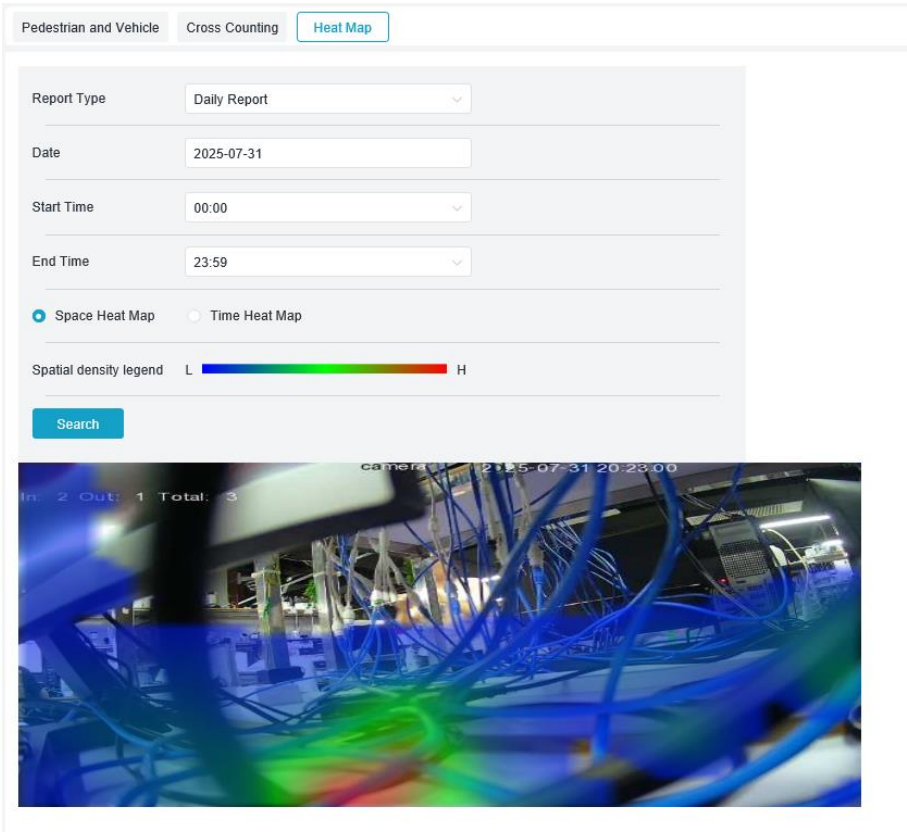
8.15.3. Heat Map

The heat map report allows you to visualize the distribution of people in two dimensions: time or space.

Space heat map: the different areas in the screen of the personnel active situation. The red color is the densest area, i.e. the most active, and the blue color is the least densely populated area.

Time heat map: people's activity at different times in the screen. The vertical coordinate value is the index calculated according to the number of people, stay time and other comprehensive calculation, the larger the value the higher the activity, does not represent the number of people.

The camera must be equipped with a usable SD card, the heat map information will be stored in the SD card, the interface effect is shown in the figure.



Report Type: The data search supports the search of Daily report, Weekly report, Monthly report and Annual report in 4 time ranges.

Date: The date to which the data search refers.

Start Time: only shown in Daily report setting, set the specific hour to start the search.

End Time: Displayed only when setting up a daily report, sets the specific hour at which the search ends.

Mode: Set the way to display the data when searching, there are two ways: graph and table.

Display Area: display the frequency of changes in the monitoring area in the form of a graph, and display the frequency of changes in the monitoring area in the form of a table for different time periods.

Search: search data according to the current settings.

8.16. Network Settings

This menu allows users to configure network parameters such as PPPoE, DHCP, and SNMP. the most common type is DHCP. unless a static IP is set manually. most of the time the network type is DHCP. if the user needs to authenticate a username and password to connect to the network, select PPPoE.

8.16.1. General Settings

General

PPPoE

SNMP

IEEE802.1X

Port Configuration

DHCP

IP Address

172.20.25.27

Test

Subnet Mask

255.255.255.0

Gateway

172.020.025.001

IPv6 DHCP

IPv6 Address

fe80::3824:f1ff:fe10:95ea

Subnet Prefix Length

64

(1 ~ 128)

IPv6 Default Gateway

fe80::3824:f1ff:fe10:95ea/64

DNS 1

172.018.001.222

DNS 2

008.008.008.008

IPv6 DNS 1

2606:4700:4700::1111

IPv6 DNS 2

2606:4700:4700::1122

Multicast

Multicast

Multicast Address

239.255.255.255

(224.0.0.0~239.255.255.255)

Stream Encryption

Audio-Video Encrypted Transmission

Intercom Encrypted Transmission

Save

Refresh

If connecting to a router that allows DHCP, tick the DHCP box. The router will automatically assign all network parameters to the device. Unless the following parameters are set manually for the network:

IP Address: The IP address is the identifier of IPC on the network. It consists of four numbers between 0 and 255 separated by periods.for example, "192.168.001.100".

Subnet Mask: A subnet mask is a network parameter that defines the range of IP addresses that can be used in the network. If the IP address is likened to the street you live on, then the subnet mask is the community. A subnet address also consists of four numbers separated by periods, for example, "255.255.000.000".

Gateway: This address allows IPC to access the network. The format of a gateway address is the same as that of an IP address, for example, "192.168.001.001".

IPv6 Address: The IPv6 address is the identifier of IPC on the network. It consists of eight numbers between 0 and FFFF, separated by colons, for example, "ABCD: EF01: 2345: 6789: ABCD: EF01: 2345: 6789".

DNS1/DNS2: DNS1 is the active DNS server and DNS2 is the standby DNS server. Usually you just need to enter the DNS1 server address.

Main Stream: If this option is enabled, the main stream can be used for multicast.

Multicast Address: Specify a multicast address. A third-party player can request the camera to send a multicast media stream through the RTSP protocol.

Video Encryption Transmission: Indicates audio/video encryption transmission.

If the IPC is capable of warning you of repeated IP addresses in the same network segment, when IP addresses are repeatedly used, the following message will pop up when you click the Test

IP Address	172.20.25.27	Test
Subnet Mask	255.255.255.0	

8.16.2. PPPOE

The device supports networking communication via PPPOE dial-up.

General **PPPoE** SNMP IEEE802.1X Port Configuration

Enable PPPOE ☐

Username

Password

IP Address

Save Refresh

Check the "Enable PPPoE" box and enter the PPPoE username and password. Click "Save" to save and the system will reboot to activate the PPPoE settings.

8.16.3. SNMP

Simple Network Management Protocol (SNMP) is a standard protocol specifically designed to manage network nodes (servers, workstations, routers, switches, and HUBS, etc.) in an IP network and is an application layer protocol.

General
PPPoE
SNMP
IEEE802.1X
Port Configuration

Enable
☐

SNMP Version
V2

SNMP Port
161
(1 ~ 65535)

Read Community
public

Write Community
private

Trap IP Address
127.0.0.1

Trap Port
162
(1 ~ 65535)

Save
Refresh

Enable: Enable or disable SNMP.

SNMP Version: Set the version of SNMP server, V1, V2 and V3 are available.

SNMP Port: Set the port of the SNMP server.

Read Community: Set the SNMP server Read Community value.

Write Community: Set the SNMP server Write Community value.

Trap IP Address: Set the SNMP server Trap IP address.

Trap Port: Set the SNMP server Trap port.

8.16.4. IEEE802.1X

The 802.1x protocol is widely used in Ethernet as the access control mechanism for LAN ports, which mainly solves the problems of authentication and security in Ethernet. The 802.1x protocol is a port-based network access control protocol. "Port-based network access control" refers to the authentication and control of accessed user devices at the port level of the LAN access device. User devices connected to the port can access resources on the LAN if they can pass authentication. If it cannot pass authentication, it cannot access resources on the LAN.

General
PPPoE
SNMP
IEEE802.1X
Port Configuration

Enable IEEE802.1X
☐

Authentication methods
EAP-MD5

EAPOL Version
IEEE802.1X-2010

Username
username

Password
••••••••••••••••

Save
Refresh

- Enable IEEE802.1X:** Enable or disable IEEE802.1X.
- Authentication Methods:** Set the authentication methods of IEEE802.1X.
- Username:** Set the IEEE802.1X authentication username.
- Password:** Set the IEEE802.1X authentication password.

8.16.5. Port Settings

General
PPPoE
SNMP
IEEE802.1X
Port Configuration

Server	Internal Port	External Port	Protocol	UPNP Status	Mapping Strategy	UPNP
HTTP Port	80	80	TCP	Inactive	Auto	☐
HTTPS Port	443	443	TCP	Inactive	Auto	☐
RTSP	554	554	TCP	Inactive	Auto	☐
Multicast Port	10000	(1024-65535)				

Save
Default
Refresh

- HTTP Port:** This is the port that the user uses to log in to the camera remotely (e.g. using a web client). If other applications already use port 80, change it.
- HTTPS Port:** Default value is 443, Https is an HTTP channel aiming at security, which guarantees the security of the transmission process by transmission encryption and authentication on the basis of HTTP.
- RTSP Port:** The default value is 554, if other applications already use the default port 554, change it.

UPNP: If you want to use Web Client to log in to the device remotely, port forwarding needs to be done in the router. If the user's router supports UPnP, please enable this option. In this case, users do not need to manually configure port forwarding in the router. If the user's router does not support UPnP, please ensure that port forwarding is done manually in the router.

Multicast port: Allows you to set the multicast port.

P2P Switch: P2P switch, P2P will not take effect when it is turned off.

8.17. Cloud Service Setup

By enabling the cloud service function, adding the device to RISCO server.

Risco Cloud Configuration

Risco Cloud

☒

Save

Refresh

Cloud Services: Cloud service switch.

8.18. Mail Settings

8.18.1. Parameter settings

This menu allows the user to configure email settings. To receive system notifications on email when an alarm is triggered and the hard disc is full, complete these settings.

Email

Schedule

Email

Other

Outlook

Other

25

(1 ~ 65535)

SMTP Server

SMTP server cannot be empty !

Username

Username cannot be empty!

Passkey

Sender's Name

Sender Error!

Receiver 1

Receiver 2

Receiver 3

Interval

3Min

Save

Test

Refresh

Email: Tick to enable.

Type: mailbox type, there are two types: Outlook and Other.

Encryption: Enable if the user's email server requires SSL or TLS authentication. If you are not sure, set it to "Automatic".

SMTP Port: Enter the SMTP port of the email server.

SMTP Server: Enter the address of the SMTP server for e-mail.

Username: Enter the user's email address.

Password: Enter the user's email password.

Receiver 1~3: Enter the e-mail address where the user wants to receive event notifications from the camera.

Interval: Configures the time interval between the camera's notification e-mails.

To ensure that all settings are correct, click on "**Test Email**". An email will be sent to the user's inbox. If the user receives the test email, the configuration parameters are correct.

8.18.2. Schedule Setup

Set the schedule for the mail function to take effect, so that the mail function will take effect only during the schedule time period. refer to [8.6 Schedule Settings](#).

EmailSchedule

TableList

	0	2	4	6	8	10	12	14	16	18	20	22	24
SUN													
MON													
TUE													
WED													
THU													
FRI													
SAT													

Import Template

Save Template

Save

Refresh

8.19. RTSP Protocol Settings

RTSP (Real Time Streaming Protocol), RFC2326, Real Time Streaming Transport Protocol, is an application layer protocol in the TCP/IP protocol family. The protocol defines how a one-to-many application can efficiently transmit multimedia data over an IP network. allows users to view live images through a video player.

RTSP

RTSP Enable

☒

Anonymous Login

☐ (No username or password required)

Metadata Platform ⓘ

None ▼

Instruction:
rtsp://IP:RtspPort/rtsp/streaming?channel=01&subtype=A
A: 0(main stream), 1(sub stream), 2(mobile stream)

Save

Refresh

RTSP Enable: the RTSP switch. Enable to use the protocol.

Anonymous Login: Anonymous login. When enabled, no authentication is required to use this protocol.

Metadata Platform: Used to control the pushing of event alarm data to the third-party platform when the device is interfaced to the third-party monitoring platform using the onvif protocol.

None: no external metadata push

General: Push common format metadata externally, available for third-party platforms without special requirements

Milestone: pushing metadata externally for the Milestone platform

8.20. Dynamic Domain Name Settings

This menu allows the user to configure the DDNS settings. DDNS provides a static address to simplify the remote connection to the camera. To use DDNS, the user first needs to open an account on the webpage of the DDNS service provider.

DDNS

DDNS

☐

Server

NO_IP

Hostname

Username

Password

Save

Test

Refresh

DDNS: DDNS switch, check to enable DDNS.

Server: Select the preferred DDNS server (DYNDNS, NO_IP, partial support for CHANGEIP, DNSEXIT).

Hostname: Enter the domain name that the user created on the web page of the DDNS service provider. This is the address that the user types in the URL box when they want to connect to the camera remotely via a PC.

User/Password: Enter the user name and password obtained when creating an account on the DDNS service provider's web page.

After entering all parameters, click "Test DDNS" to test the DDNS settings. If the test result is "Network unreachable or DNS error", please check whether the network is normal or the DDNS information is correct.

8.21. HTTPS protocol settings

This menu allow to set HTTPS.connect your device over HTTPS.

HTTPS

Certificate Type

Custom

Certificate not installed

Certificate

...

Key

...

Install

Save

Refresh

Certificate Type: There are two options, including default and custom. The Custom option Allow to connect devices using your own certificate.

Certificate: Select a custom certificate when the Custom option is selected.

Key: Select a custom key file when the Custom option is selected.

8.22. IP Filter

The IP Filter function allows you to set a black and white list of connected devices.

IP Filter

Enable

☐

Edit Filtering List

Allowed

Add Single IP Address

Add IP Address Range

No.	☐	Start Address	End Address	CON.
No data available				

Save

Remove List

Refresh

Enable: Enable or disable the IP filter. choose to enable the block list or allow list if this option is turned on.

Edit Filtering List: Select the list you want to set (black list or white list).

Single Add: Single Add.

Network Segment Add: Network Segment Add

Start Address: Enter the start address.

End Address: Enter the end address.

Delete: Delete the added user IP from the black/white list.

8.23. Platform Access

8.23.1. RTMP

RTMP function page, when you turn on the enable switch and fill in the correct server address, push the audio and video stream of the device to the YouTube live server.

RTMP

Event Push Platform

Enable

☐

Server Address

Stream Type

Mainstream

Note:

The recommended resolution is 1920x1080.
The supported video encoding formats are H.264 and H.264+.The supported audio encoding formats are G711A and G711U.
After enabling RTMP, if the current audio or video codecs are not supported, the system will automatically switch the video codec to H.264 or the audio codec to G711A.

Save

Refresh

Enable: Enable or disable the RTMP function.

Server Address: The address of the server to be pushed.

Stream Type: Select the video stream to be pushed to the server.

8.23.2. Event Push Platform

Event push is divided into HTTP push method and UDP push method: HTTP method has POST method and GET method; UDP method has unicast, multicast and broadcast three methods. (Note: some models support event push function).

1. HTTP Push

RTMP

Event Push Platform

Enable

☒

Precise

☐

Name

Push Method

☒ HTTP ☐ UDP

Username

Password

Server Address

192.168.1.168 or example.com

Port

123

^
v

(1 ~ 65535)

URL

API/AlarmEvent/EventPush

Method

POST

v

Interval

OFF

v

Save

Refresh

Enable: Enable or disable the Event Push function.

Precise: Enable or disable the Precise function. When on, pushes once when an alarm is triggered and again when the alarm ends. When it is off, it will only push once when the alarm is triggered.

Name: Set the channel name. Do not support Chinese display.

push method: Set the push mode. Both HTTP push mode and UDP push mode are supported. select **HTTP** or **UDP** as required.

Username: Set the username. It can be set to NULL if there is not any.

Password: Set the password. It can be set to NULL if there is not any.

Server Address: Set the server address.

Port: Set the server port. (port number range: 1–65535.)

URL: Set the server API. It can be set to NULL if there is not any.

Method: Set the HTTP push method. Both POST and GET methods are supported. Only the HTTP-POST method supports image push. Other methods push notifications only. The alarm type of image push is the same as that in the alarm column of live view on the Web client.

Interval: Set the keep-alive interval. The keep-alive mechanism ensures that a notification is periodically pushed to the client in accordance with the preset time while normal alarm push is not affected. There is no keep-alive mechanism in UDP mode.

2. UDP Push

RTMP

Event Push Platform

Enable

☒

Precise

☐

Name

Push Method

☐ HTTP☒ UDP

UDP Method

Broadcast

UDP Address

255.255.255.255

UDP Port

5000

(1 ~ 65535)

Save

Refresh

Enable: enable or disable the event push function.

Precise: Enable or disable Precise Push. When it is on, push once when alarm is triggered and again when the alarm is over. When it is off, it will only push once when the alarm is triggered.

Name: Channel name, does not support Chinese display.

Push Method: Support HTTP push method and UDP push method. Check HTTP for HTTP push method, check UDP for UDP push method.

UDP Method: UDP push type, supports Unicast, Multicast and Broadcast methods:

Unicast: Enter the IP address and port of the client's UDP server to receive push messages, and only this address can receive messages

Multicast: Multiple client UDP servers on the same network segment using the same UDP address and port can receive the message, while other non-UDP addresses will not receive it.

Broadcast: All UDP servers under the same network segment can receive the message.

UDP Address: UDP server address.

UDP Port: UDP server port (port range 1-65535)

8.24. General system setup

8.24.1. Date and time

The screenshot displays a web-based configuration interface for 'Date and Time'. It features two tabs: 'Date and Time' (which is selected and highlighted with a blue border) and 'Daylight Saving Time'. Below the tabs, there are two dropdown menus. The first, labeled 'Date Format', is set to 'YYYY-MM-DD'. The second, labeled 'Time Format', is set to '24Hour'. At the bottom of the interface, there are two buttons: 'Save' and 'Refresh'.

Hide Date, Time, Time Zone and NTP when the Risco Cloud switch is **open**.

Date Format: Set the date format.

Time Format: Select the preferred time format.

Off Risco Cloud switch :

Date and Time Daylight Saving Time

Time setting mode ☒ Static ☐ NTP server synchronization

Date Format YYYY-MM-DD

Time Zone GMT+8:00

Time Format 24Hour

System time 2025-08-01 14 : 15 : 09

System time: change the system date and time.

Date Format: Set the system date display format.

Time Format: Set the system time display format.

Time Zone: Set up the time zone of the device.

8.24.2. Daylight Saving Time

If the RISCO Cloud switch is on, settings cannot be modified.

Off the Risco Cloud switch, If the DST daylight time is implemented in the user area, relevant parameters can be set in this interface and DST can be enabled.

Date and Time **Daylight Saving Time**

This Feature is not Supported!

The DST (Daylight Saving Time) feature gives the user the option to add daylight saving time to a specific time zone or region.

Date and Time

Daylight Saving Time

Daylight Saving Time

☒ Set by week ☐ Set by date

Start Time

March

The 2nd

SUN

19 : 00 : 00

End Time

November

The 1st

SUN

19 : 00 : 00

Time Offset

1Hour

Save

Refresh

Daylight Saving Time: Enable this option if the user's time zone uses daylight saving time.

Set by week: Selects the month, specific day of the week and time when Daylight Saving Time begins and ends. For example, 2: 00 a.m. on the first Sunday of a particular month.

Set by date: Select the date and time when daylight saving time starts and ends.

Start Time / End Time: Set the start time and end time for daylight saving time.

Time Offset: Selects the amount of time Daylight Saving Time adds to the user's time zone. This is the difference between Coordinated Universal Time (UTC) and local time.

8.25. Multi-user management

This menu is user configurable with user name, password and user rights.

The system supports the following user types:

ADMIN - System Administrator: The administrator can fully configure the system and change the administrator and user passwords.

and enable/disable password protection.

USER - Normal User: User can only access Preview, Search, Playback and other functions. Users can set up multiple users with different system access rights.

Multi-User						
NO.	Username	Level	Enable	Password	Policy	
1	admin	ADMIN	Enable	z		
2	user1	USER	Disable	z		
3	user2	USER	Disable	z		
4	user3	USER	Disable	z		
5	user4	USER	Disable	z		
6	user5	USER	Disable	z		
7	user6	USER	Disable	z		

Refresh

To change the password for an administrator or user, click the "Password Edit" icon. The password must be 8-16 digits and at least 2 combinations of numbers, uppercase letters, lowercase letters and special characters. Enter the new password again to confirm. Save the new password and the system will ask the user to enter the old password for authentication.

Editing

Enable

☒

Username

Password

☐

Confirm

☐

OK

Cancel

1. One of the currently inactive users and click the Password Edit icon.
2. Tick "Enable" to enable users.
3. Click "Username" to edit the username.
4. Click the field next to Password to enter the desired password.
5. Click the field next to Confirm to re-enter your password.

Click OK. The user will be required to enter the administrator password for authentication.

To set the permissions for sub users: Click  enter the Policy page and tick the box corresponding to the function to enable the sub user's permissions in this area. Click [All](#) to check all boxes and Clear to [clear](#) all boxes.

Policy

Username

user1

☐ Parameter

☐ Live

☐ Playback

☐ PTZ

☐ RTSP

All

Clean All

Save

Cancel

8.26. Maintenance

The system log displays important system events such as motion alerts and system warnings. Users can easily import a backup file of the system log to their computer for a set period of time.

8.26.1. Log Management

The system log displays important system events such as motion alerts and system warnings. Users can easily import a backup file of the system log to their computer for a set period of time.

Log

Load Default

Upgrade

Parameter Management

Auto Maintenance

Developer Mode

Log Type

All

Search

Name

Export

Start Time

07/31/2025

00 : 00 : 00

End Time

07/31/2025

23 : 59 : 59

No.	Time	Log Content	Log Info
1	07/31/2025 13:55:21	Multi-User	Operation result: The operation was successful User Name: admin IP: 172.20.25.3
2	07/31/2025 13:50:50	Login	Operation result: The operation was successful User Name: admin IP: 172.20.25.3
3	07/31/2025 13:47:37	Change Time	
4	07/31/2025 13:44:43	System Startup	
5	07/31/2025 13:44:29	Network Connect	
6	07/31/2025 12:27:03	Cloud Server	Type: Cloud Service Save Operation result: The operation was successful User Name: admin IP: 172.20.25.3
7	07/31/2025 12:25:52	Cloud Server	Type: Cloud Service Save Operation result: The operation was successful User Name: admin

Total: 58

1

Log Search and Backup.

Select log **type** of event to search for from the drop-down list next to Log Type, or select **All** to view the entire system log for the selected time period. The available types are: System Log, Configuration Log, Warning Log, Account Log, Recording Log, Storage Log, and Network Log.

System: System Settings, Reboot, Auto Reboot, Upgrade, Time Settings, and NTP Calibration.

Configuration: IPC live control , private area settings , recording mode settings , recording plan settings , main stream settings , network settings, Sub Stream settings, email settings, color settings, motion detection settings, hard disk settings, multi-user settings, NTP settings, image control, mobile stream settings, RTSP settings, IP filter settings, restore factory settings, rare sound detection settings, export settings, and import settings. Event Push settings, Capture settings, Deterrent settings, AI settings, FTP settings, DDNS settings, HTTPS settings, audio settings, Siren settings, system maintenance, video masking, IO alarms, cloud service setup.

Alarm: Start of motion detection, end of motion detection. start of I/O alarm, end of I/O alarm. start of Video Tamper, end of Video Tamper. start of Line Crossing, end of Line Crossing.start of Object Detection, end of Object Detection.start of Pedestrian & Vehicle, end of Pedestrian & Vehicle.start of Face Detection, end of Face Detection.start of Cross Counting, end of Cross Counting.start of Crowd Density, end of Crowd Density.start of Queue Length, end of Queue Length.start of License plate detection, end of License plate detection. start of Intrusion, end of Intrusion. start of Region Entrance, end of Region Entrance. start of Region Exiting, end of Region Exiting, tart of Rare Sound, end of Rare Sound. start of Sound Alarm, end of Sound Alarm.

Account: Log in, log out, lock and switch users.

Recording: Search, playback and backup.

Storage: Format hard disc, hard disc full and hard disc error.

Network: Network down, network up, network error and network mode change.

1. Select the event type to search for from the drop-down list next to **Minor Type** (if ALL is selected for Log Type, this menu will not be available).
2. Enter the export file name in the field next to **Name**. Click Export to create a backup of the syslog.

- 3. Click the area next to **Start Time** to select the start date and time of the search from the on-screen calendar.
- 4. Click the area next to **End Time** to select the end date and time of the search from the on-screen calendar.
- 5. Click **Search**.
- 6. Browse the system log from the selected time period:
- 7. Use the **⏪ < / > ⏩** button in the lower right corner of the menu to switch between pages of syslog events.

8.26.2. Restoring factory settings

Users can select different reset methods on this page to restore the device's configuration parameters to factory settings. Restoring the factory settings will not format the data of the TF card.

Log

Load Default

Upgrade

Parameter Management

Auto Maintenance

Developer Mode

Restore to Inactive

Reset admin password, delete sub-users, require device reactivation and new password, other settings unchanged.

Restore Defaults

Reset all settings to factory default except network and admin password settings.

Factory Defaults

All parameters, including network and password settings, are restored to their factory default states.

Restore to Inactive: Resets the administrator password, deletes all sub-users, the camera needs to be reactivated, and the parameters of the other pages remain unchanged.

Restore Defaults: Except for the network and administrator password, all other pages are restored to the factory settings.

Factory Defaults: All parameters of the camera are restored to the factory settings.

8.26.3. System upgrades

This menu allows you to upgrade the firmware of your device.

Log

Load Default

Upgrade

Parameter Management

Auto Maintenance

Developer Mode

Online Upgrade

Automatic Detection

☐

Username

Password

Server Address

Server Address example:

protocol://hostname[:port]/path

(s)ftp://192.168.1.100:23/device/upgradePackage

http(s)://192.168.1.100:80/device/upgradePackage

Save

Detect

Upgrade

Refresh

Installation package upgrade

Path

...

Upgrade

Don't close the browser or turn off the power when updating!

Automatic Detection: Automatic detection. Turn on this button to automatically detect online upgrade files.

Username: Server username.

Password: The server password.

Server Address: Enter the online upgrade address (HTTP upgrade does not require user name and password).

Save: click this button to save the current setting.

Detect: Detect, after uploading the upgrade file and setting the upgrade path, click Detect to manually detect the online upgrade file.

8.26.4. Parameter management

The user can export the configured main menu parameters to a computer or import the exported setup file from the computer to the device.

LogLoad DefaultUpgradeParameter ManagementAuto MaintenanceDeveloper Mode

Import File

Import

Export file name

Export

Import File: Click on the box to bring up the path window, select the parameter file and click **Import** to start importing parameters.

Export File Name: Click the box to enter the file name of the exported parameter. Click **Export** to export the parameters.

8.26.5. Auto Maintenance

The user can export the configured main menu parameters to the computer or import the exported setup file from the computer to the device.

LogLoad DefaultUpgradeParameter ManagementAuto MaintenanceDeveloper Mode

Auto Maintenance☐

Maintenance Interval7 Day

Maintenance Time00:00-02:00

Auto Maintenance helps to keep your device healthy and optimized by running all maintenance tasks automatically at the time you choose. Your device will reboot when maintenance completed.

SaveRefreshReboot

- Auto Maintenance:** Enables or disables the automatic maintenance feature
- Maintenance Interval:** Sets the automatic maintenance interval of the camera.
- Maintenance Time:** Sets the time period for automatic camera maintenance.
- Note:** the device will reboot at random times during this period.

8.26.6. Developer Mode

This menu enables developer mode, which is convenient for developers to collect and record log information for device debugging.

Log

Load Default

Upgrade

Parameter Management

Auto Maintenance

Developer Mode

Camera Debug

Mode

SD_Card

Download Debug Logs

Pack Log

Device Status Reporting

Save

Refresh

Export Search Log

Export

Camera Debug: Check to enable.

Mode: Select the mode of collecting and logging debugging information, there are three modes: NVR, SD_Card and FTP.

Download Debug Logs: Export debug information. Select SD_Card mode, click the button, enter the correct password, the device will export the debug information to the local computer.

Pack Log: Pack logs. Select NVR or FTP mode, click this button, the device will upload the pack log information to FTP server.

Device Status Reporting: Enable this function to upload the storage status, channel status and device information to P2P server.

Export Search Log: Export the search log. Enter the file name of the log to be exported and click the Export button to export all the log files stored on the device to the local computer.

8.27. System Information

8.27.1. Device information

This menu allows users to view system information, such as device ID, device model name, MAC address, firmware version, etc.

Information

Privacy Statement

Device ID	0000000000000000
Device Name	RO-00000000000000000000000000000000
Device Type	0000000000000000
Hardware Version	00000000
Software Version	00000000000000000000000000000000
Web Version	0000000000000000
MAC Address	0000000000000000
RISCO ID	0000000000000000

Refresh



9. Local settings

This menu allows to set the path for storing videos and downloaded and captured image files, as well as the format of videos and captured images.

Note: skip this page when you access the web client from Safari 12 and later, Chrome 57 and later, Firefox 52 and later, and Edge 41.

Path configuration

Record Path

D:\Device\Record

Download Path

D:\Device\Download

Snapshot Path

D:\Device\Capture

File type

MP4

Interval

10

Minute

Capture Type

JPG

Save

Standard Limited Product Warranty (“Limited Warranty”)

RISCO Ltd. (“**RISCO**”) guarantee RISCO’s hardware products (“**Products**”) to be free from defects in materials and workmanship when used and stored under normal conditions and in accordance with the instructions for use supplied by RISCO, for a period of (i) 24 months from the date of delivery of the Product (the “**Warranty Period**”). This Limited Warranty covers the Product only within the country where the Product was originally purchased and only covers Products purchased as new.

Contact with customers only. This Limited Warranty is solely for the benefit of customers who purchased the Products directly from RISCO or from an authorized distributor of RISCO. RISCO does not warrant the Product to consumers and nothing in this Warranty obligates RISCO to accept Product returns directly from end users who purchased the Products for their own use from RISCO’s customer or from any installer of RISCO, or otherwise provide warranty or other services to any such end user directly. RISCO’s authorized distributor or installer shall handle all interactions with its end users in connection with this Limited Warranty. RISCO’s authorized distributor or installer shall make no warranties, representations, guarantees or statements to its end users or other third parties that suggest that RISCO has any warranty or service obligation to, or any contractual privity with, any recipient of a Product.

Remedies. In the event that a material defect in a Product is discovered and reported to RISCO during the Warranty Period, RISCO shall accept return of the defective Product in accordance with the below RMA procedure and, at its option, either (i) repair or have repaired the defective Product, or (ii) provide a replacement product to the customer.

Return Material Authorization. In the event that you need to return your Product for repair or replacement, RISCO will provide you with a Return Merchandise Authorization Number (RMA #) as well as return instructions. Do not return your Product without prior approval from RISCO. Any Product returned without a valid, unique RMA # will be refused and returned to the sender at the sender’s expense. The returned Product must be accompanied with a detailed description of the defect discovered (“**Defect Description**”) and must otherwise follow RISCO’s then-current RMA procedure published in RISCO’s website at www.riscogroup.com in connection with any such return. If RISCO determines in its reasonable discretion that any Product returned by customer conforms to the applicable warranty (“**Non-Defective Product**”), RISCO will notify the customer of such determination and will return the applicable Product to customer at customer’s expense. In addition, RISCO may propose and assess customer a charge for testing and examination of Non-Defective Product.

Entire Liability. The repair or replacement of Products in accordance with this Limited Warranty shall be RISCO’s entire liability and customer’s sole and exclusive remedy in case a material defect in a Product is discovered and reported as required herein. RISCO’s obligation and this Limited Warranty are contingent upon the full payment by customer for such Product and upon a proven weekly testing and examination of the Product functionality.

Limitations. This Limited Warranty is the only warranty made by RISCO with respect to the Products. The warranty is not transferable to any third party. To the maximum extent permitted by applicable law, this Limited Warranty shall not apply and will be void if: (i) the conditions set forth above are not met (including, but not limited to, full payment by customer for the Product and a proven weekly testing and examination of the Product functionality); (ii) if the Products or any part or component thereof: (a) have been subjected to improper operation or installation; (b) have been subject to neglect, abuse, willful damage, abnormal working conditions, failure to follow RISCO’s instructions (whether oral or in writing); (c) have been misused, altered, modified or repaired without RISCO’s written approval or combined with, or installed on products, or equipment of the customer or of any third party; (d) have been damaged by any factor beyond RISCO’s reasonable control such as, but not limited to, power failure, electric power surges, or unsuitable third party components and the interaction of software therewith or (e) any failure or delay in the performance of the Product attributable to any means of communication provided by any third party service provider, including, but not limited to, GSM interruptions, lack of or internet outage and/or telephony failure. BATTERIES ARE EXPLICITLY EXCLUDED FROM THE WARRANTY AND

RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY. RISCO does not install or integrate the Product in the end user's security system and is therefore not responsible for and cannot guarantee the performance of the end user's security system which uses the Product or which the Product is a component of.

This Limited Warranty applies only to Products manufactured by or for RISCO. Further, this Limited Warranty does not apply to any software (including operating system) added to or provided with the Products or any third-party software, even if packaged or sold with the RISCO Product. Manufacturers, suppliers, or third parties other than RISCO may provide their own warranties, but RISCO, to the extent permitted by law and except as otherwise specifically set forth herein, provides its Products "AS IS". Software and applications distributed or made available by RISCO in conjunction with the Product (with or without the RISCO brand), including, but not limited to system software, as well as P2P services or any other service made available by RISCO in relation to the Product, are not covered under this Limited Warranty. Refer to the Terms of Service at: www.riscogroup.com/warranty for details of your rights and obligations with respect to the use of such applications, software or any service. RISCO does not represent that the Product may not be compromised or circumvented; that the Product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise, or that the Product will in all cases provide adequate warning or protection. A properly installed and maintained alarm may only reduce the risk of a burglary, robbery or fire without warning, but it is not insurance or a guarantee that such will not occur or will not cause or lead to personal injury or property loss. CONSEQUENTLY, RISCO SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR OTHER LOSS BASED ON ANY CLAIM AT ALL INCLUDING A CLAIM THAT THE PRODUCT FAILED TO GIVE WARNING. EXCEPT FOR THE WARRANTIES SET FORTH HEREIN, RISCO AND ITS LICENSORS HEREBY DISCLAIM ALL EXPRESS, IMPLIED OR STATUTORY, REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS WITH REGARD TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS, TO THE EXTENT PERMITTED BY LAW. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RISCO AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (i) THE OPERATION OR USE OF THE PRODUCT WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE; (ii) THAT ANY FILES, CONTENT OR INFORMATION OF ANY KIND THAT MAY BE ACCESSED THROUGH THE PRODUCT SHALL REMAIN SECURED OR NON-DAMAGED. CUSTOMER ACKNOWLEDGES THAT NEITHER RISCO NOR ITS LICENSORS CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, GSM OR OTHER MEANS OF COMMUNICATIONS AND THAT RISCO'S PRODUCTS, MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH MEANS OF COMMUNICATIONS. RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT IN ANY EVENT RISCO SHALL NOT BE LIABLE FOR ANY AMOUNTS REPRESENTING LOST REVENUES OR PROFITS, PUNITIVE DAMAGES, OR FOR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, EVEN IF THEY WERE FORESEEABLE OR RISCO HAS BEEN INFORMED OF THEIR POTENTIAL.

Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website (www.riscogroup.com) or at the following telephone and fax numbers:

United Kingdom

Tel: +44-(0)-161-655-5500

support-uk@riscogroup.com

Italy

Tel: +39-02-66590054

support-it@riscogroup.com

Spain

Tel: +34-91-490-2133

support-es@riscogroup.com

France

Tel: +33-164-73-28-50

support-fr@riscogroup.com

Belgium (Benelux)

Tel: +32-2522-7622

support-be@riscogroup.com

China (Shanghai)

Tel: +86-21-52-39-0066

support-cn@riscogroup.com

Israel

Tel: +972-3-963-7777

support@riscogroup.com

