



SECURING YOUR WORLD



USER MANUAL

IP CAMERA

Table of Contents

Chapter 1 Overview and Default Settings.....	7
1.1 About This Manual.....	7
1.2 Default Settings at a Glance.....	7
1.3 Product Description.....	7
Chapter 2 Connecting the Camera.....	8
2.1 Direct Connection to a Computer.....	8
2.2 Connection Through a Router, Switch, or NVR.....	8
Chapter 3 Assigning an IP Address with the Discovery Tool.....	8
Chapter 4 Accessing the Camera from the Web Client.....	9
4.1 Locating the Camera and Opening the Web Client.....	9
4.2 First-Time Access: Activating the Camera.....	10
4.3 Routine Login.....	12
4.4 Recovering a Forgotten Password.....	12
4.4.1 Security Questions.....	12
4.4.2 Authorization Certificate.....	13
4.4.3 Super Code (not recommended).....	14
Chapter 5 Installing the Browser Plug-in.....	15
Chapter 6 Live View.....	18
6.1 Live Menu.....	18
6.2 Recording Status Indicators.....	19
6.3 Fisheye Display.....	20
6.3.1 Ceiling Mode.....	20
Chapter 7 Playback and Search.....	25
7.1 General Playback.....	25
7.2 Image Search.....	27
7.3 Playback by Tag.....	27
7.4 Smart Playback.....	28
7.5 AI Search.....	29
7.6 License Plate Detection Search.....	29
7.7 Pedestrian and Vehicle Search.....	30
7.8 Line Crossing Search.....	31
7.9 Intrusion Detection Search.....	31
7.10 Region Entrance Search.....	32
7.11 Region Exiting Search.....	33

Chapter 8 Local Settings.....	33
Chapter 9 Image and Video Settings.....	36
9.1 Preview and On-Screen Display.....	36
9.2 Image Control.....	36
9.2.1 Day and Night Mode.....	37
9.2.2 Orientation and Rotation.....	38
9.2.3 Exposure and Backlight.....	38
9.2.4 White Balance and Shutter.....	38
9.2.5 Image Enhancement.....	38
9.3 Privacy Mask.....	39
9.4 Video Parameters.....	39
9.4.1 Recording Parameters.....	40
9.4.2 Coding Parameters.....	40
9.4.3 Audio Management.....	41
9.5 Capture Settings.....	42
9.6 PTZ and RS-485 Settings.....	43
Chapter 10 Recording, Storage, and Schedules.....	44
10.1 Schedule Setup.....	44
10.1.1 Record Schedule.....	44
10.1.2 Capture Schedule.....	46
10.2 Disk Management.....	47
Chapter 11 Events and AI Detection.....	48
11.1 Common Detection Settings.....	48
11.2 Face Detection.....	49
11.3 Pedestrian and Vehicle.....	50
11.4 License Plate.....	50
11.5 Line Crossing.....	51
11.6 Intrusion.....	52
11.7 Enter Region.....	53
11.8 Exit Region.....	53
11.9 Object Detection.....	54
11.10 Cross Counting.....	54
11.11 Heat Map.....	55
11.12 Queue Length.....	55
11.13 Crowd Density.....	56
11.14 Special Sound.....	57

11.15 Motion Detection.....	58
11.16 Video Tampering.....	58
11.17 Event Schedule.....	59
11.18 Alarm Linkage Settings.....	59
Chapter 12 Alarm Actions and Deterrence.....	60
12.1 I/O Settings.....	61
12.1.1 Alarm Input Settings.....	61
12.1.2 Alarm Output Settings.....	62
12.2 Deterrence Settings.....	63
12.3 Siren Settings.....	64
12.4 Disarming.....	64
Chapter 13 Recognition Lists and Statistics.....	65
13.1 List Management.....	65
13.1.1 Face Recognition.....	65
13.1.2 License Plate Recognition.....	67
13.2 Statistics.....	70
13.2.1 Face Recognition.....	70
13.2.2 Pedestrian and Vehicle.....	71
13.2.3 Cross Counting.....	72
13.2.4 Heat Map.....	72
Chapter 14 Network and Services.....	73
14.1 FTP Settings.....	73
14.2 Network Settings.....	74
14.2.1 General Settings.....	74
14.2.2 PPPoE.....	76
14.2.3 SNMP.....	76
14.2.4 IEEE 802.1X.....	77
14.2.5 Port Settings.....	77
14.3 Cloud Service.....	78
14.4 Mail Settings.....	79
14.4.1 Parameters.....	79
14.4.2 Schedule.....	80
14.5 RTSP.....	80
14.6 Dynamic DNS.....	81
14.7 HTTPS.....	81
14.8 IP Filter.....	82

14.9 Platform Access.....	82
14.9.1 RTMP.....	83
14.9.2 Event Push Platform.....	83
14.9.2.1 HTTP Push.....	83
14.9.2.2 UDP Push.....	84
Chapter 15 System and Maintenance.....	85
15.1 General System Setup.....	85
15.1.1 Date and Time.....	85
15.1.2 Daylight Saving Time.....	85
15.2 Multi-user Management.....	86
15.3 Maintenance.....	87
15.3.1 Log Management.....	87
15.3.2 Restore Factory Settings.....	88
15.3.3 System Upgrade.....	89
15.3.4 Parameter Import and Export.....	90
15.3.5 Auto Maintenance.....	90
15.3.6 Developer Mode.....	90
15.4 System Information.....	91
15.4.1 Device Information.....	91
15.4.2 Privacy Statement.....	91
Chapter 16 PTZ Cameras.....	94
16.1 Basic Functions.....	94
16.1.1 Preset Cruise.....	94
16.1.2 Watch Mode.....	94
16.1.3 Linear Scan.....	95
16.1.4 Track Cruise.....	95
16.1.5 Pattern Scan.....	96
16.1.6 Pigtail Specification.....	96
Chapter 17 Thermal Cameras.....	96
17.1 Fire Detection.....	97
17.1.1 Temperature Measurement.....	97
17.1.2 Temperature Measurement Area Setting.....	98
17.1.3 Thermal Alarm Schedule.....	100
17.1.4 Thermal Alarm Linkage.....	101
17.2 Emissivity of Common Substances.....	102
Chapter 18 Multi-Lens Cameras.....	102

Getting Started

Bring the camera online — from physical connection and network addressing to your first secure login.

Chapter 1 Overview and Default Settings

This manual describes the installation, configuration, and operation of the network (IP) camera through its built-in web client. It applies to the full IPC product line; because features differ between models, some functions described here may not be available on every device.

1.1 About This Manual

The camera is administered entirely from a web browser — no dedicated client software is required for day-to-day use. Each chapter follows the same order you will encounter on screen, so the manual can be read start to finish during commissioning or used as a reference for a single feature.

- **Terminology.** The terms “IP camera,” “network camera,” and “IPC” are used interchangeably throughout this document.
- **Model differences.** Where a function depends on specific hardware (for example, PTZ, thermal imaging, audio, or I/O), the text notes that it is supported on selected models only.
- **Screenshots.** Interface images are provided as a guide. The exact layout and available options vary with firmware version and model.

1.2 Default Settings at a Glance

A new camera ships with the following defaults. Review them before installation so the device can be reached on your network and secured on first use.

Setting	Default value
Network addressing	DHCP (an address is obtained automatically)
Static fallback address	10.0.0.6 (used only when no DHCP server responds)
Web (HTTP) port	80
ONVIF	Enabled; the ONVIF port follows the web port
Administrator user name	admin (lowercase, cannot be changed)
Administrator password	None — must be created at first login

NOTE Because addressing is DHCP by default, the quickest way to find a new camera on the network is the Discovery Tool (Chapter 3), which lists every device together with its current IP address.

1.3 Product Description

The camera integrates high-definition imaging, efficient video compression, and on-board intelligent analytics in a single compact unit. It is designed for both residential and commercial surveillance and is managed remotely over a standard IP network.

Principal capabilities include:

- **Efficient high-definition streaming.** Modern H.265/H.264 compression delivers detailed images while minimizing bandwidth and storage demand.
- **Browser-based remote access.** The live view, playback, and configuration are all reached by entering the camera's address in a web browser.
- **Role-based multi-user access.** Multiple accounts can be created, each with a defined set of permissions for viewing and administration.
- **Intelligent detection and alerts.** On detecting a relevant event, the camera can send email notifications with snapshots or clips and push alerts to the mobile application.
- **On-board recording.** Event and continuous recordings are stored locally on a memory card, with optional upload to FTP, network storage, or the cloud.

Chapter 2 Connecting the Camera

The camera can be connected in two ways, depending on whether it will be accessed from a single computer or integrated into a local network for everyday use and remote viewing.

2.1 Direct Connection to a Computer

Use this method for bench testing or initial configuration, without a router or internet connection.

1. Connect an Ethernet cable between the camera's network port and the computer's network port.
2. Connect the camera to power using the supplied 12 V adapter.
3. Set the computer's IP address to the same subnet as the camera's default address, so the two can communicate.
4. Wait approximately one minute for the camera to start. It will then be reachable from the computer.

2.2 Connection Through a Router, Switch, or NVR

Use this method for normal operation. Connecting the camera to your local network allows access from other devices and, once port forwarding or a cloud account is configured, remote access over the internet.

1. Connect both the camera and the computer to LAN ports on the router, switch, or NVR.
2. Connect the camera to its power adapter.
3. Set the camera's gateway to match the router's IP address. This allows the camera to route its video stream through the router and, if enabled, out to the internet.

TIP On a network with DHCP, steps 1 and 2 are usually sufficient — the router assigns the address automatically. Set the gateway manually only when the camera uses a static address.

Chapter 3 Assigning an IP Address with the Discovery Tool

The Discovery Tool locates every camera on the local network and lets you view and change its network settings before you log in for the first time.



Launch the Discovery Tool from its desktop shortcut.

1. Run the Discovery Tool and click **Search**. The tool lists all cameras on the local network with their IP address, ports, device model, MAC address, and P2P ID.
2. Identify your camera by its MAC address or P2P ID (printed on the device label).
3. Select the camera and, in the **Device Info** fields at the bottom of the window, enter the required IP address, subnet mask, and gateway.
4. Enter the administrator user name and password, then click **Modify** to apply the new settings.

DISCOVERY TOOL														
Search Upgrade Config Import/Export Stream Config OSD Config Recovery Initialization Reboot Change Password														
Filtering IP														
No.	IP	Media Port	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	P2P ID	Initialized	Status
1	192.168.2.4	8080	80	1	PN20P5MP-AI	PN20P5MP-AI	V1.35.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-94-CB	Static	X135P60ZBC	true	
2	192.168.2.20	0	80	64	GSD-NVRPNC-AK-64NP-N	GSD-NVRPNC-AK-64NP-N	VC1.3.0-260407	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-94-CB	DHCP	ACT75D0TNC	true	
3	192.168.2.21	0	80	256	GSD-NVRPNC-AK-256NP-N	GSD-NVRPNC-AK-256NP-N	VC1.3.0-260413	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-94-C3	Static	neny5d0ctng	true	
4	192.168.2.25	9000	80	1	TEBDAIPMP28-AI	TEBDAIPMP28-AI	V21.45.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-54-41	Static	C523W3A4N	true	
5	192.168.2.26	9000	80	1	TEBDAIPMP28-AI	TEBDAIPMP28-AI	V21.45.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-55-28	Static	B3JNLNTUUS	true	
6	192.168.2.27	9000	80	1	TEBDAIPMP28-AI	TEBDAIPMP28-AI	V21.45.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-53-E2	Static	JK75EOKLBP	true	
7	192.168.2.28	9000	80	1	TEBDAIPMP28-AI	TEBDAIPMP28-AI	V21.45.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-54-67	Static	Y8P92EP2LR	true	
8	192.168.2.29	9000	80	1	TEBDAIPMP28-AI	TEBDAIPMP28-AI	V21.45.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-54-83	DHCP	91AN4CZCH	true	
9	192.168.2.30	0	80	32	GSD-NVRPNC-AK-32NP-N	GSD-NVRPNC-AK-32NP-N	VC1.3.0-260227	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-F3-A0	Static	nen5dmg6Vr	true	
10	192.168.2.42	0	80	1	KVS-GBA20PMP-POE-R	KVS-GBA20PMP-POE-R	VC51.57.1.2.3-260	255.255.255.0	192.168.2.1	F4-79-9C-C5-F3-40	Static	nen4thmspk	true	
11	192.168.2.43	0	80	1	KVS-GBA20PMP-POE-R	KVS-GBA20PMP-POE-R	VC51.57.1.2.3-260	255.255.255.0	192.168.2.1	F4-79-9C-C5-F3-42	Static	nen52m6bdc	true	
12	192.168.2.45	0	80	1	KVS-GBA20PMP-POE-R	KVS-GBA20PMP-POE-R	VC51.57.1.2.3-260	255.255.255.0	192.168.2.1	F4-79-9C-C5-F3-19	Static	nen5v4q3uq	true	
13	192.168.2.46	0	80	4	QUADZ8P18MP-AI	QUADZ8P18MP-AI	VC52.57.1.3-251	255.255.255.0	192.168.2.1	F4-79-9C-C5-89-E1	DHCP	cbny6c854y	true	
14	192.168.2.115	0	80	1	XEBATVPMP28-AI-64G	XEBATVPMP28-AI-64G	VC30.85.1.2.0-241	255.255.255.0	192.168.2.1	F4-79-9C-C5-93-16	Static	MZV768NCH	true	
15	192.168.2.200	90	80	32	GSD-NVRPNC-AK-32NP-N	GSD-NVRPNC-AK-32NP-N	V8.2.4.1-20240627	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-79-C2	Static	JF4UPJP3531	true	
16	192.168.2.202	0	80	1	SPTZDAIPMP-AI	SPTZDAIPMP-AI	VC55.57.1.3.4-260	255.255.255.0	192.168.2.1	F4-79-9C-C1-1F-4E	DHCP	cbm6cbz72g	true	
17	192.168.2.203	0	80	1	XEBATVPMP28-AI	XEBATVPMP28-AI	VC49.57.1.3.0-260	255.255.255.0	192.168.2.1	F4-79-9C-C1-9F-86	Static	namppnrm4u	true	
18	192.168.2.204	9000	80	1	TEBDAIPMP28-AI	TEBDAIPMP28-AI	V21.45.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-55-2E	Static	GL9RKC13KA	true	
19	192.168.2.214	0	80	4	FE30P128MP-AI	FE30P128MP-AI	VC49.57.1.3.1-251	255.255.255.0	192.168.2.1	F4-79-9C-C5-FD-89	Static	nen5p6ac7bc	true	
20	192.168.2.216	0	80	2	BIT4P5MP-AI-V2	BIT4P5MP-AI-V2	VC47.55.1.3.0-250	255.255.255.0	192.168.2.1	F4-79-9C-C5-F7-11	Static	nen6p9c4d53	true	
21	192.168.2.217	0	80	1	XEBATVPMP28-AI-E	XEBATVPMP28-AI-E	V1.9.2-240429	255.255.255.0	192.168.2.1	F4-79-9C-C5-F1-4F	Static	GM1N68XKH	true	
22	192.168.2.218	0	80	1	XT2FPAN20P5MP-AI	XT2FPAN20P5MP-AI	VC30.85.1.2.0-250	255.255.255.0	192.168.2.1	F4-79-9C-C5-E3-1A	Static	nenmsuc2m7	true	
23	192.168.2.219	0	80	1	ALPFBK232P18MP-AI	ALPFBK232P18MP-AI	VC48.55.1.3.0-260	255.255.255.0	192.168.2.1	F4-79-9C-C5-A8-67	Static	nen5gpcutcm	true	
24	192.168.2.220	0	80	1	BLZ50P5MP-AI	BLZ50P5MP-AI	VC30.85.1.3.0-260	255.255.255.0	192.168.2.1	F4-79-9C-C5-AA-DA	Static	cbm6adw7bzg	true	
25	192.168.2.221	0	80	1	XPTZ37XIPMP-AI-N	XPTZ37XIPMP-AI-N	VC46.55.1.3.0-260	255.255.255.0	192.168.2.1	F4-79-9C-C5-90-14	Static	XEKCT31LYPT	true	
26	192.168.2.222	90	80	16	HQ-S8	GSD-NVRPNC-AK-16-N	V8.2.4.1-20250711	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-58-EA	Static	VAPCCUNFJR	true	
27	192.168.2.223	0	80	1	KVS-GBA20PMP-POE-R	KVS-GBA20PMP-POE-R	VC51.57.1.2.3-260	255.255.255.0	192.168.2.1	F4-79-9C-C5-F3-44	Static	nen6d5drnge	true	
28	192.168.2.251	0	80	1	DBWLMP-POE-R	DBWLMP-POE-R	VC54.24.1.3.3-251	255.255.255.0	192.168.2.1	F4-79-9C-C5-E5-4B	DHCP	nen5w32zcp	true	
29	192.168.2.254	9000	80	1	TEBDAIPMP28-AI	TEBDAIPMP28-AI	V21.45.8.2.4.1.24	255.255.255.0	192.168.0.0/1	F4-79-9C-C5-54-A4	Static	SL5HL90NHT	true	

Figure 3-1. Discovery Tool — device list and network settings.

NOTE On a new camera the default user name is **admin** and no password has been set yet. Addressing is DHCP by default; assign a static address here only if your network requires one.

Chapter 4 Accessing the Camera from the Web Client

This chapter describes how to open the web client, activate the camera on first use, log in for routine operation, and recover or renew the administrator password. All procedures are performed in a supported web browser.

4.1 Locating the Camera and Opening the Web Client

The web client can be reached in two ways: by selecting the camera in the Discovery Tool, or by entering its address directly in a browser.

Method 1 — Discovery Tool. Run the Discovery Tool and click Search, then double-click the camera's IP address to open the web client in your default browser.

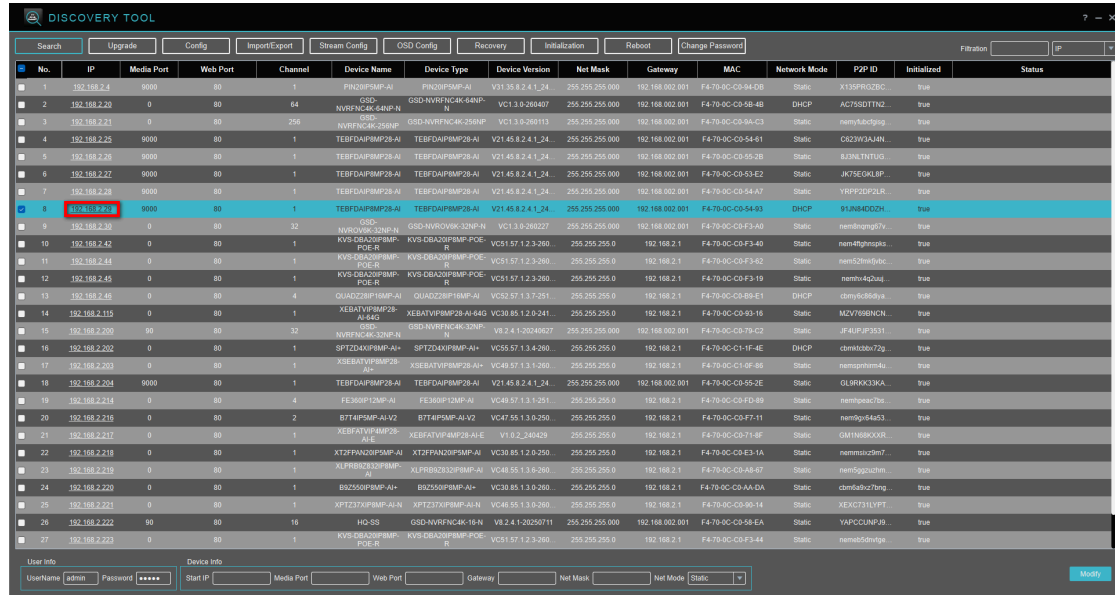


Figure 4-1. Selecting a camera in the Discovery Tool.

Method 2 — Direct browser access. In the browser address bar, enter the camera address in the form `http://<IP address>:<web port>`. For example, a camera at 172.20.58.41 using the default web port 80 is reached at `http://172.20.58.41:80`.

NOTE The default web (HTTP) port is 80. If the port has been changed, substitute the current value in the address.

4.2 First-Time Access: Activating the Camera

A new camera ships without a password and must be activated before use. On first access, the web client opens the Password screen and prompts you to create the administrator password.

The image shows the 'Password' configuration screen. It has a title 'Password' at the top. Below it are four sections: 'Default Username' with a text field containing 'admin'; 'New Password' with a text field and a password strength indicator; 'Password Strength' with a progress bar; and 'Confirm Password' with a text field. A tooltip is visible over the 'New Password' field, listing four rules: 1. Length must be 8 ~ 16; 2. The password cannot be the same as the username; 3. Only uppercase letters, lowercase letters, digit, special characters allowed. Must contain 2 of them; 4. Special characters include '~!@#%&*()-_+=~\|{};:~.,<.>/?'. An 'OK' button is at the bottom right.

Figure 4-2. Activation — creating the administrator password.

The password must meet the following requirements:

- **Length:** 8 to 16 characters.
- **Composition:** at least two of the following character types — uppercase letters, lowercase letters, digits, and special characters.
- **Uniqueness:** the password must not be identical to the user name.

Enter and confirm the password, then click OK. The default administrator user name is **admin** (all lowercase).

Immediately after the password is set, the web client offers optional password-recovery methods. Configuring at least one now allows you to regain access if the password is later lost. If none is selected, password recovery is disabled and a lost password cannot be reset from the web client.

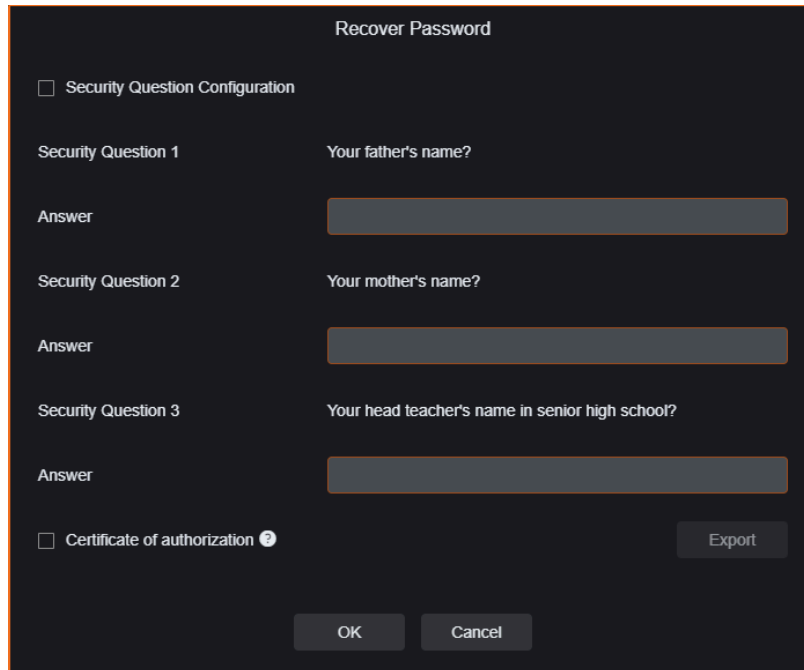


Figure 4-3. Optional password-recovery setup, presented during activation.

Security questions. Select three of the fifteen available questions and provide an answer for each (up to 64 characters). The answers are used later to authorize a password change.

Authorization certificate. Click Export to download a certificate file (certificate.txt), which is later imported to authorize a password change. Store it in a secure location.

Super code (Recommended). Derives a recovery code from the camera's MAC address and system clock.

WARNING When password recovery is enabled, keep the security answers or the certificate file secure. Either one grants the ability to reset the administrator password.

4.3 Routine Login

Once the camera is activated, the login screen appears on each subsequent visit. Enter the user name and password, select the interface language if required, and click Login.

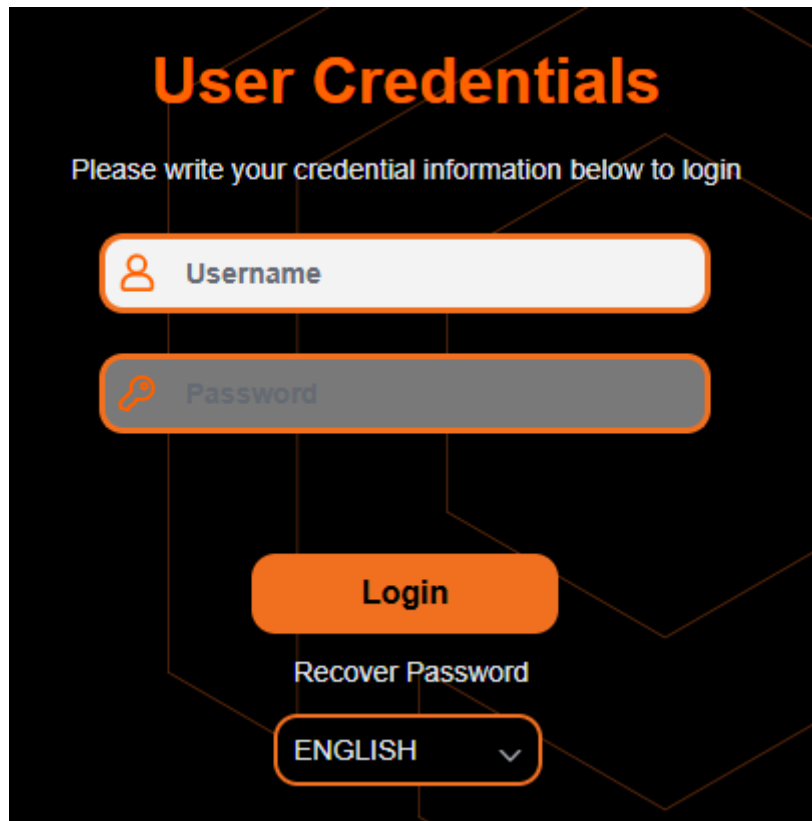
The image shows a web client login screen with a dark background and orange accents. At the top, the title "User Credentials" is displayed in large orange font. Below it, a subtitle reads "Please write your credential information below to login". There are two input fields: the first is labeled "Username" with a person icon, and the second is labeled "Password" with a key icon. Below these fields is an orange "Login" button. Under the "Login" button is a "Recover Password" link. At the bottom is a language selection dropdown menu currently showing "ENGLISH" with a downward arrow.

Figure 4-4. Web client login screen.

TIP Choose the interface language from the drop-down menu before logging in. It can be changed again at any time from the login screen.

4.4 Recovering a Forgotten Password

If password recovery was configured during activation, click **Recover Password** on the login screen to reset the administrator password using the method you set up.

4.4.1 Security Questions

Set Verification Mode to Security Question Verification, answer the three configured questions, and enter a new password. If the answers are correct, the password is changed immediately.

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

Figure 4-5. Password recovery using security questions.

4.4.2 Authorization Certificate

Set Verification Mode to Certificate of authorization, click Import, and select the certificate.txt file exported during activation. Once the certificate is accepted, enter a new password to complete the change.

Recover Password

Verification Mode: Certificate of authorization

Certificate of authorization: Import

OK Cancel

Figure 4-6. Password recovery using an authorization certificate.

CAUTION Each certificate can be used only once. After a successful recovery, the existing certificate is invalidated and the web client prompts you to export a replacement at the next login. If a new certificate is not exported, this recovery method becomes unavailable.

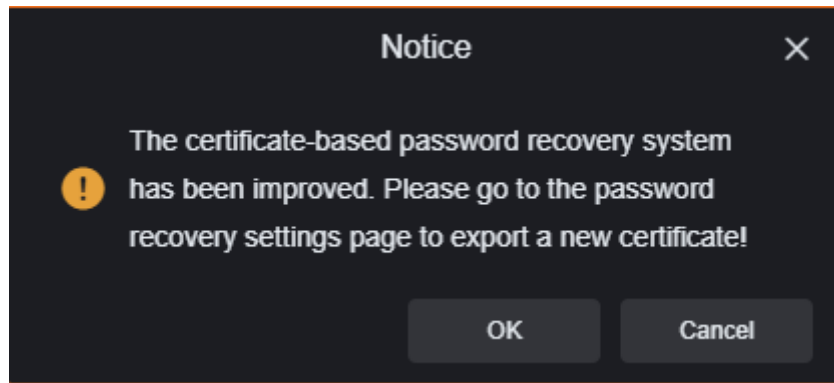


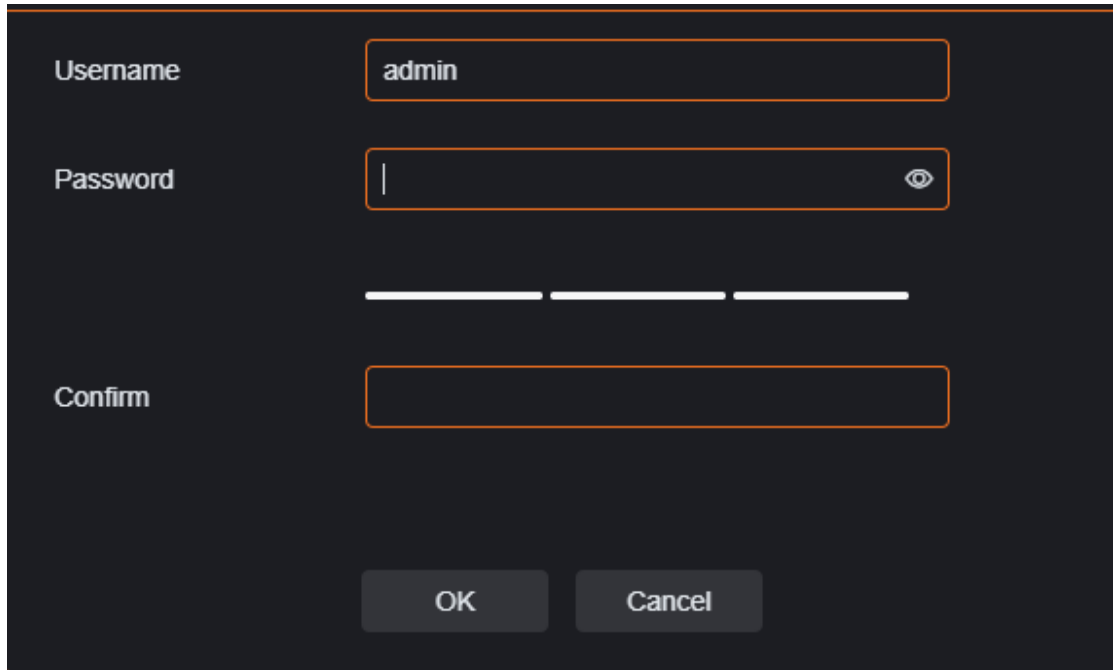
Figure 4-7. Prompt to export a replacement certificate after use.

4.4.3 Super Code (not recommended)

Super Code derives a one-time recovery code from the camera's MAC address and current system time. Enter the code to authorize a new password. Because the underlying values are easily observed, this method provides little security and should be avoided when the other options are available.

A dark-themed "Recover Password" dialog box. It features a "Verification Mode" dropdown menu currently set to "Super Code". Below this is a "Super code" field displaying a green-generated code: "2026-04-22 11:28:01 MAC Address: F4-70-0C-C0-C6-92". Further down are input fields for "New Password" and "Confirm Password". A "Password Strength" indicator is shown as a horizontal bar with three segments. At the bottom are "OK" and "Cancel" buttons.

Figure 4-8. Password recovery using Super Code.



A dark-themed dialog box for password renewal. It contains three input fields: 'Username' with the text 'admin', 'Password' with a single character and a toggle icon, and 'Confirm'. Below the fields are 'OK' and 'Cancel' buttons.

Figure 4-9. Password-renewal prompt shown after 90 days.

Chapter 5 Installing the Browser Plug-in

Some browsers require a small plug-in to display the camera's live video. When it is needed, the live view area shows a prompt in place of the image.

1. Open the **Live** view. If the plug-in is required, the video area displays: “Live video can be played only after the player plug-in is installed.”
2. Click **Download and install the player** and run the downloaded installer.
3. Restart the browser and, if prompted, allow the plug-in to run. The live image then appears.

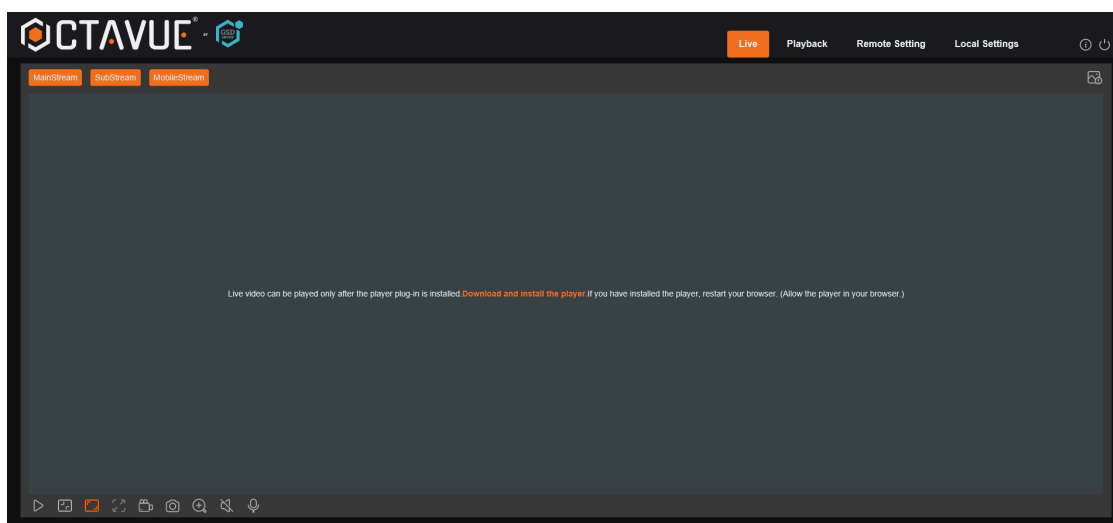


Figure 5-1. Live view prompting for the player plug-in.

NOTE The plug-in is only needed on older browsers. It can be skipped on Safari 12+, Chrome 57+, Firefox 52+, and Microsoft Edge 41+, which display live video without it.

PART II

Live View and Playback

Watch live video, review recordings, and search footage by event, image, or tag.

Chapter 6 Live View

After you log in, the web client opens the live view. This chapter describes the on-screen toolbar, the recording-status indicators, and the display options available on fisheye cameras.

NOTE Available functions differ between models. Some controls described here appear only on cameras that have the corresponding hardware, such as I/O terminals, PTZ, audio, or a fisheye lens.

6.1 Live Menu

The live view shows the current video stream together with a toolbar of controls. Its layout is shown below.

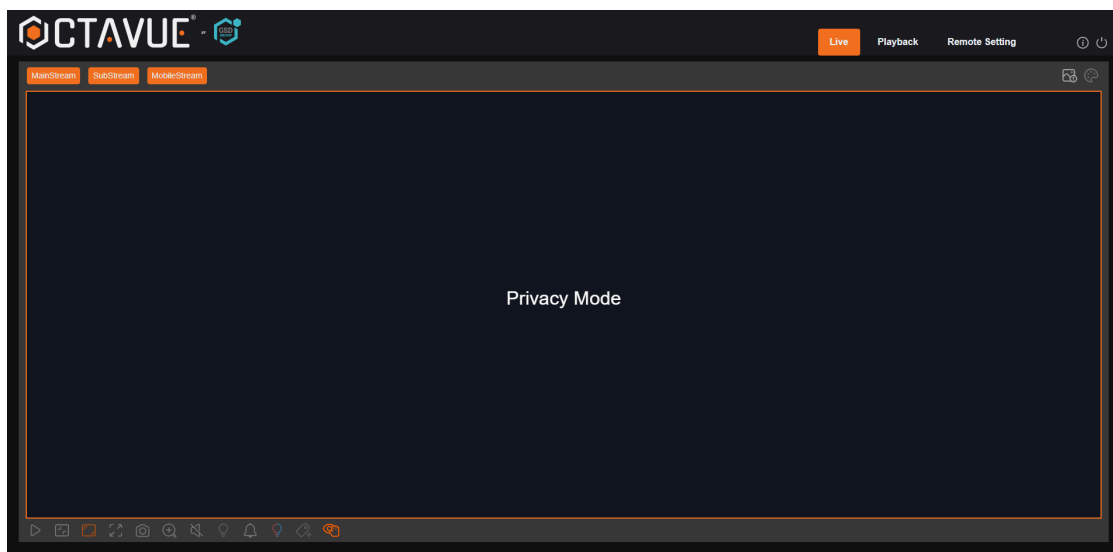


Figure 6-1. Live view and its on-screen toolbar.

The stream selector in the upper-left corner sets the quality of the live image. Three streams are available:

- **Main stream.** High-definition image, with the greatest demand on network bandwidth and computer performance.
- **Sub stream.** Moderate demand on bandwidth and performance, with lower image quality than the main stream.
- **Mobile stream.** The lowest demand on bandwidth and performance, and the lowest image quality.

The main menu bar switches between the four web-client screens: **Live**, **Playback**, **Remote Setting**, and **Local Settings**.

The live-view toolbar provides the following controls:

- 📘 **Info.** Displays details of the active user, the web-client version, and the plug-in version.

-  **Manual Alarm.** Enables or disables the manual alarm. Available on cameras with I/O terminals only.
-  **AI Alarm.** Opens the alarm push panel on the right, where snapshots from face detection and from human and vehicle detection are displayed.
-  **Color.** Adjusts image settings for the current stream, such as saturation and sharpness.
-  **PTZ Setting.** Opens the PTZ controls and refocusing options.
-  **Exit.** Logs out of the current session.
-  **Play / Stop.** Starts or stops playback of the current stream.
-  **Original Proportions.** Displays the live image at its native aspect ratio.
-  **Stretch.** Expands the live image to fill the display area.
-  **Full Screen.** Displays the live view in full screen. Double-click the image to toggle full screen, and press Esc to exit.
-  **Record.** Manually records the stream currently shown in live view.
-  **Capture.** Manually captures a still image from the current stream.
-  **Digital Zoom.** Magnifies a selected area of the image.
-  **Audio.** Enables, disables, or adjusts the live audio.
-  **Voice Intercom.** Opens two-way audio with the camera.
-  **Light.** Turns the white light on or off.
-  **Siren.** Turns the siren on or off.
-  **Warning Light.** Enables or disables the red-and-blue warning lights.
-  **Pixel Counter.** Selects an area to measure its size in pixels within the stream.
-  **Add Tag.** Adds a label to the live stream at the current moment.
-  **Fisheye.** Enters or exits fisheye mode; see the Fisheye Display section.
-  **Privacy Mode.** Turns privacy mode on or off. While it is on, the remaining toolbar options are grayed out.

6.2 Recording Status Indicators

A status letter in the live view reports the camera's current alarm state and whether recording is taking place. Several alarms can be active at the same time, so more than one indicator may appear. The same letter is used in two forms to distinguish an alarm whose recording is disabled from an alarm that is being recorded.

Indicator	Meaning
(no icon)	The memory card is normal, but no recording is in progress.
R	Normal (continuous) recording is in progress.
H	The memory card is in an abnormal state. Check and confirm the card.
M	A motion alarm is active, but motion-triggered recording is disabled.
M	A motion alarm is active and is being recorded.

I	An I/O alarm is active, but I/O-triggered recording is disabled.
I	An I/O alarm is active and is being recorded.
PIR	A PIR alarm is active, but PIR-triggered recording is disabled.
PIR	A PIR alarm is active and is being recorded.
S	A smart alarm is active, but smart-triggered recording is disabled.
S	A smart alarm is active and is being recorded.

NOTE Smart alarms include intelligent detections such as faces and people and vehicles.

6.3 Fisheye Display

On a fisheye camera, fisheye mode corrects the lens distortion and offers combinations of mounting method and display mode, so the image can be adapted to the installation scenario for the best result.



Figure 6-2. Fisheye mode, showing the installation-method and display-mode selectors.

- **Installation method.** Select the mounting mode - ceiling, wall, desktop, or tilt - to match how the camera is installed. Choosing the calibration mode that matches the mounting produces the best correction.
- **Display method.** Select how the corrected image is presented. Options include the fisheye view, 360-degree and 180-degree panoramas, PTZ views, a 3D cylinder, and VR, as well as combinations of these. The modes available depend on the installation method.

The base display modes are defined as follows:

- **Fisheye image.** The full wide-angle image captured by the fisheye lens.
- **Panoramic image.** The fisheye image corrected to a rectangular view.
- **PTZ image.** A corrected close-up of a selected area within the fisheye or panoramic image.
- **3D cylinder image.** The corrected image presented in the form of a cylinder.
- **VR image.** A 3D correction of the fisheye image that you navigate by dragging with the mouse. The scroll wheel zooms the view, and double-clicking a selected area with the right mouse button roams to that area and presents its PTZ image.

6.3.1 Ceiling Mode

In ceiling mode the camera is mounted overhead, for scenarios that require a top-down view. This mounting method provides twelve display modes.

 **Ceiling.** Ceiling mounting mode, for the fisheye camera installed overhead and other scenarios that need an overhead view.

NOTE The other fisheye mounting methods are configured in the same way.

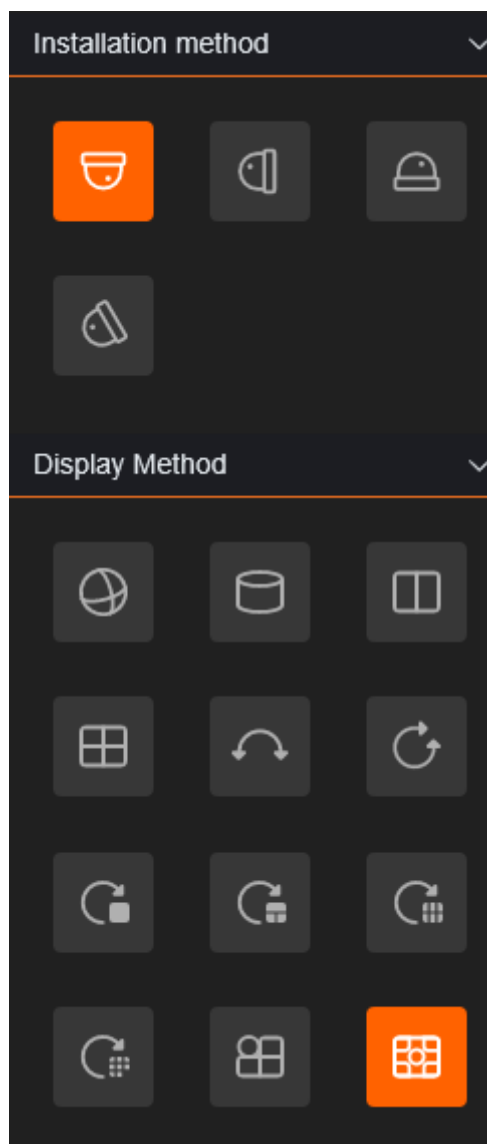


Figure 6-3. Ceiling mode - mounting selector and display-mode buttons.

The available display modes are selected with the following buttons:

 **VR.** Navigate the 3D-corrected image by dragging with the mouse. The scroll wheel zooms, and double-clicking a selected area roams to it and presents its PTZ image.

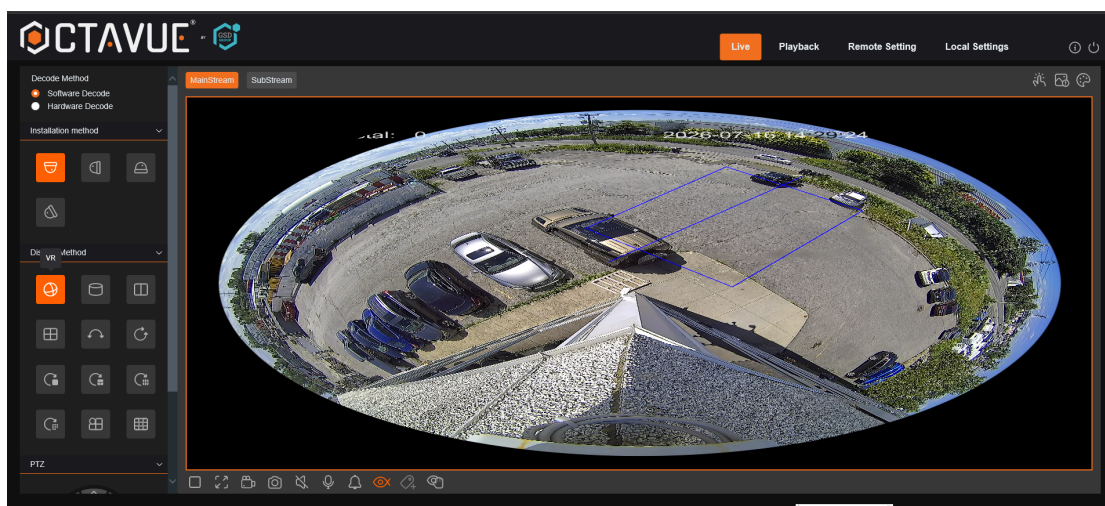


Figure 6-4. VR display mode.

Cylinder. Presents the corrected image as a 3D cylinder.

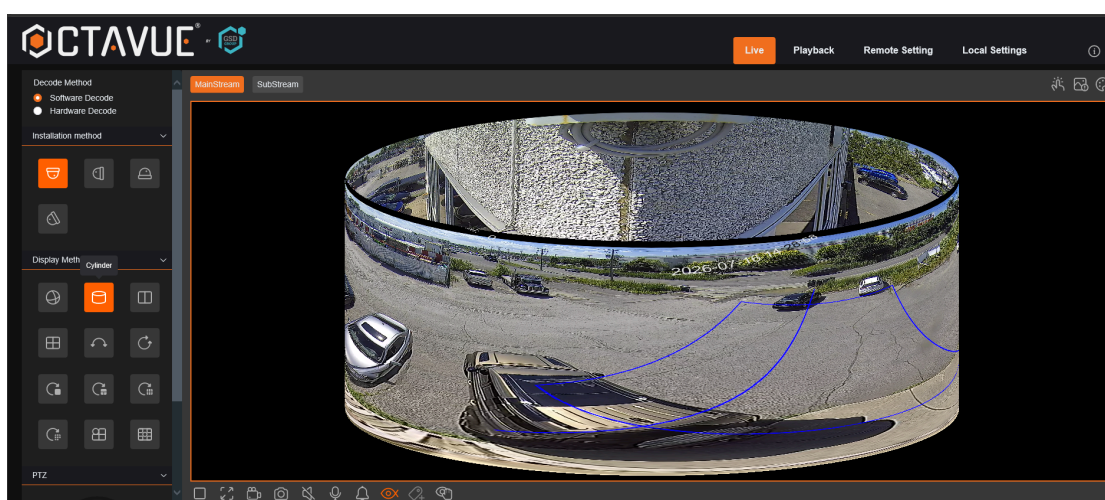


Figure 6-5. 3D cylinder display mode.

PTZ Image. Shows a corrected close-up of a single selected region.

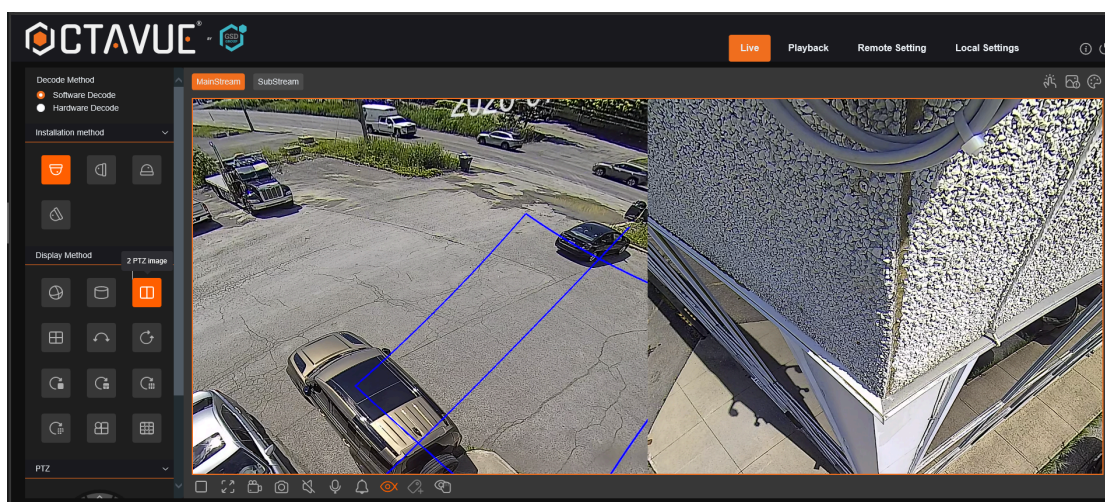


Figure 6-6. Single-region PTZ display mode.

2 PTZ Image. Shows corrected close-ups of two selected regions.

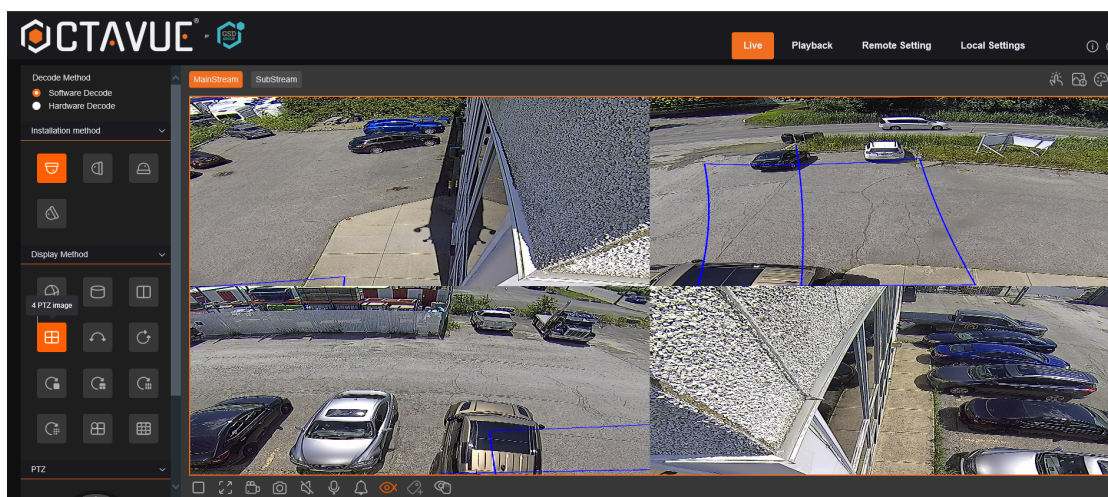


Figure 6-7. Two-region PTZ display mode.

4 PTZ Image. Shows corrected close-ups of four selected regions.

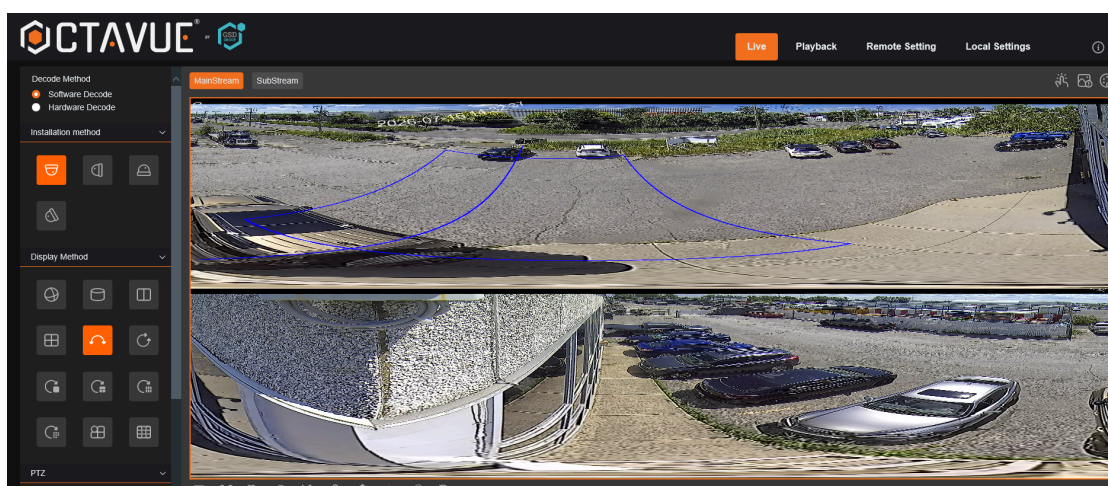


Figure 6-8. Four-region PTZ display mode.

180-Degree Panorama. Presents the scene as a 180-degree panorama.

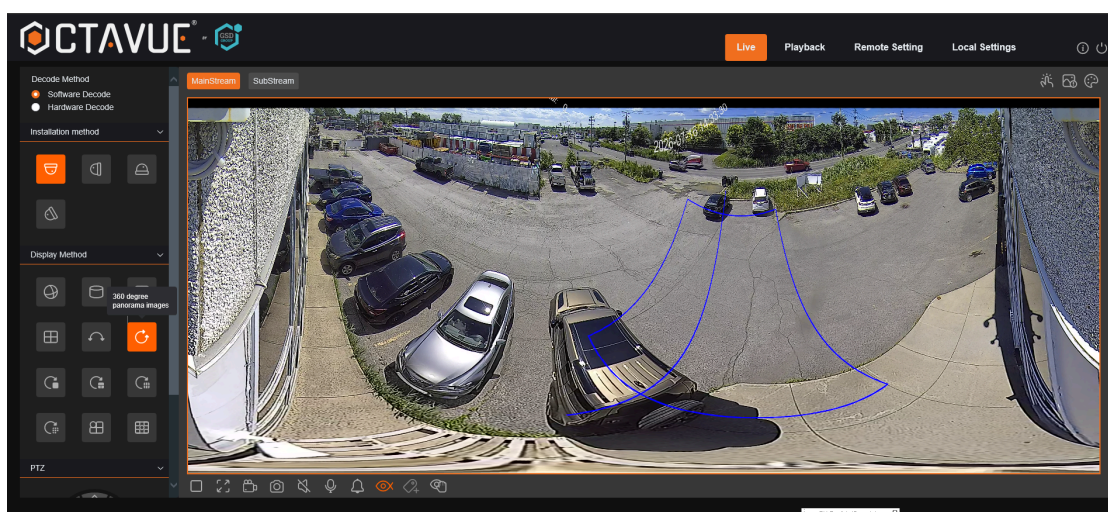


Figure 6-9. 180-degree panorama display mode.

360-Degree Panorama. Presents the scene as a 360-degree panorama.

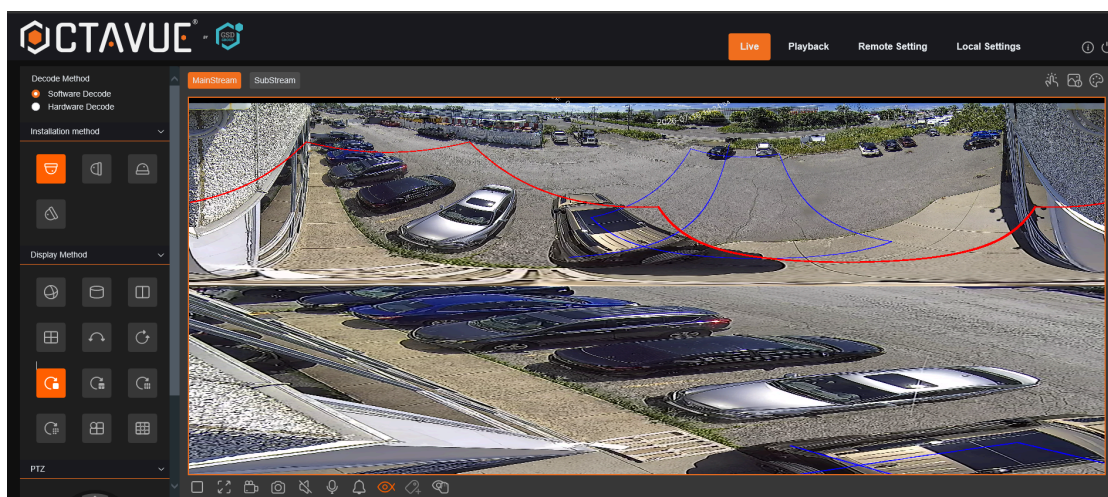


Figure 6-10. 360-degree panorama combined with a PTZ view.

- 360-Degree Panorama and 3 PTZ.** A 360-degree panorama with three corrected close-ups. Each colored band on the panorama marks a PTZ viewing range, which can be dragged to reposition its view.

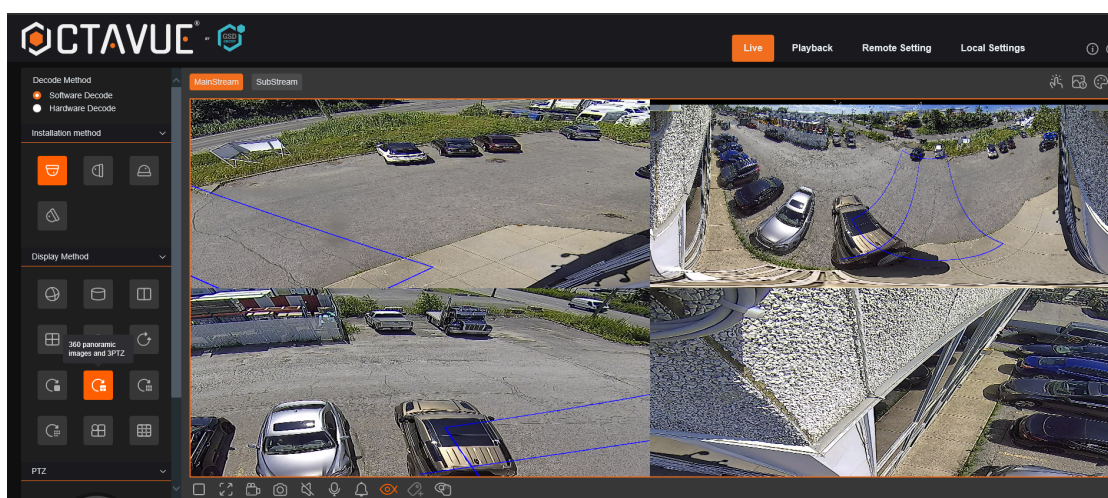


Figure 6-11. 360-degree panorama with three PTZ regions.

- 360-Degree Panorama and 6 PTZ.** A 360-degree panorama with six corrected close-ups, each mapped to a colored viewing range.

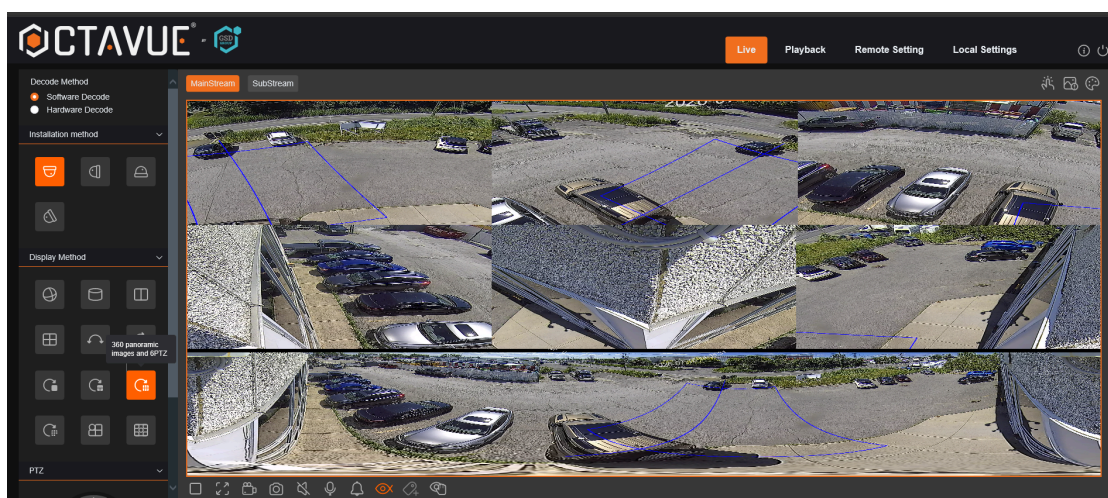


Figure 6-12. 360-degree panorama with six PTZ regions.

-  **360-Degree Panorama and 8 PTZ.** A 360-degree panorama with eight corrected close-ups, each mapped to a colored viewing range.

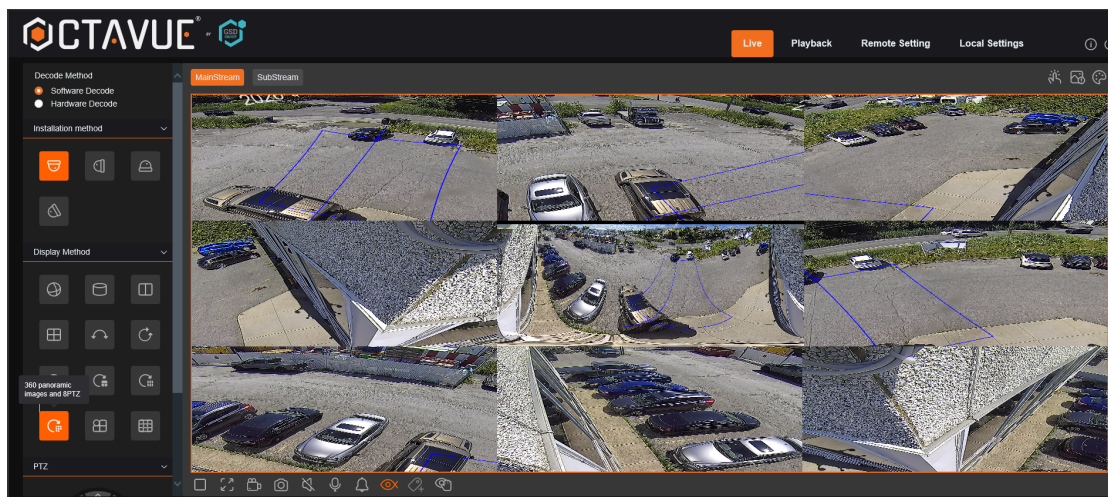


Figure 6-13. 360-degree panorama with eight PTZ regions.

-  **Fisheye and 3 PTZ.** The fisheye image with three corrected close-ups, each mapped to a colored viewing range.

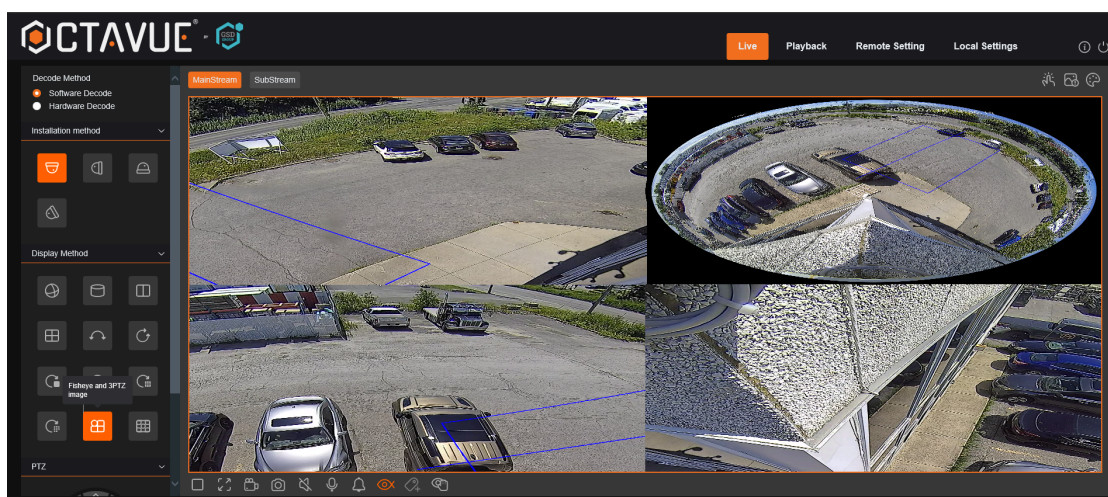


Figure 6-14. Fisheye with three PTZ regions.

-  **Fisheye and 8 PTZ.** The fisheye image with eight corrected close-ups, each mapped to a colored viewing range.

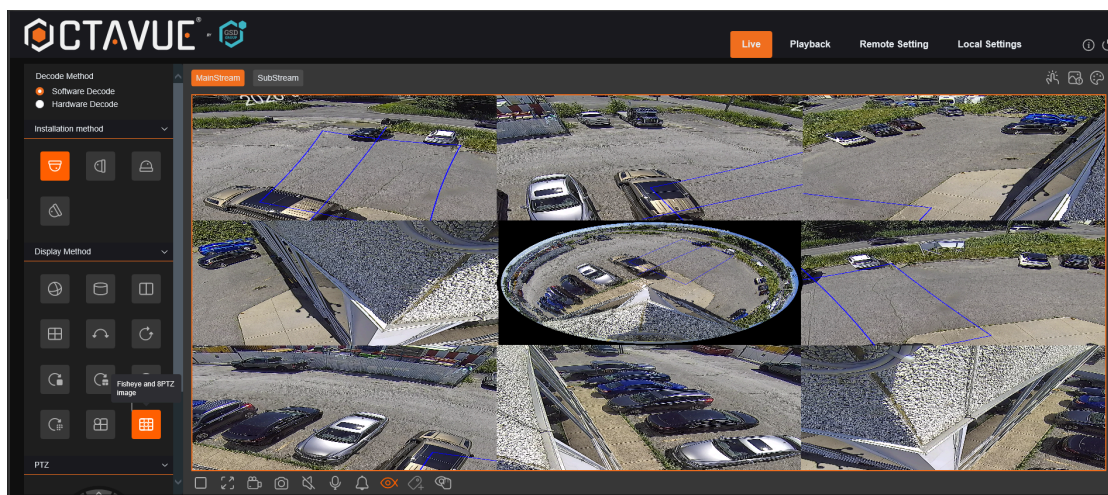


Figure 6-15. Fisheye with eight PTZ regions.

Chapter 7 Playback and Search

Beyond live viewing, the camera stores video so that it can be retrieved and reviewed later. This chapter describes general playback, image and tag searches, smart playback, and the AI searches that locate footage by event type.

7.1 General Playback

General playback searches the recordings held on the memory card and plays them back in the browser.

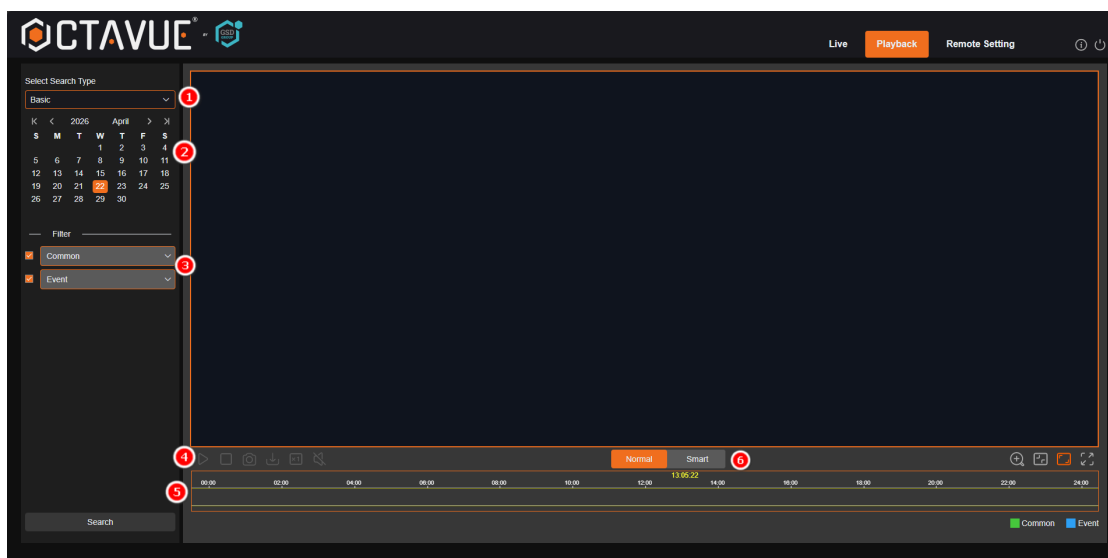


Figure 7-1. General playback and recording search.

1. Select the search mode. **General** is selected by default for standard recordings; to search AI-captured images instead, see the AI Search section.
2. Set the date and click **Search**. Dates for which recordings exist are indicated.
3. Choose one or more search types to limit the results to specific recording categories.
4. Click **Search** to list the matching recordings stored on the memory card.
5. Use the progress bar to locate and play a recording.
6. Switch between **Normal** and **Smart** search. In Smart search, select the human and vehicle buttons in the lower-left corner; the progress bar then marks clips triggered by people or vehicles in blue. These include Pedestrian and Vehicle, Intrusion, Region Entrance, Region Exiting, and Line Crossing detections.

The playback toolbar provides the following controls:

- Pause / Play.** Pauses or resumes the stream.
- Stop.** Stops playback.
- Forward by One Frame.** Advances the recording one frame per click.
- Record.** Manually records the stream being played.
- Capture.** Captures a still image from the current stream.
- Download.** Downloads the selected recording.

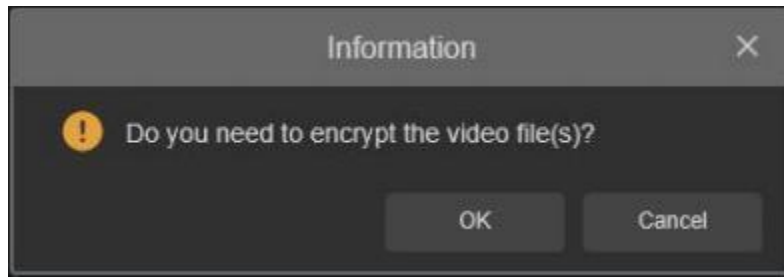


Figure 7-2. Encryption prompt shown when downloading a recording in AVF format.

-  **Speed.** Sets the playback speed to 1/8, 1/4, 1/2, 1, 2x, 4x, 8x, or 16x.
-  **Audio.** Enables, disables, or adjusts the stream audio.
-  **Add Default Tag.** Adds a tag using the default name, Tag.
-  **Add Tag.** Adds a custom tag; the name may be 1 to 39 characters.
-  **Digital Zoom.** Magnifies a selected area of the stream.
-  **Original Proportions.** Displays the stream at its native aspect ratio.
-  **Stretch.** Expands the stream to fill the display area.
-  **Full Screen.** Displays playback in full screen. Double-click the image to toggle full screen, and press Esc to exit.

NOTE Downloading a recording in AVF format prompts you to choose whether to encrypt the file. Downloads in AVI and MP4 format are not encrypted and produce no prompt.

7.2 Image Search

When automatic image capture is enabled, snapshots are searched and viewed on this screen.

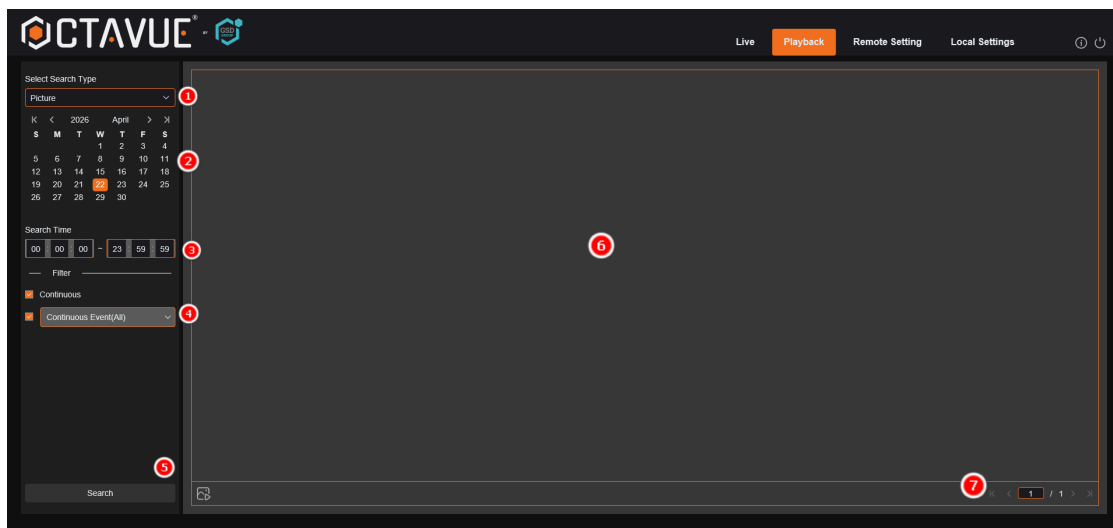


Figure 7-3. Image search screen.

1. Confirm that the search mode is set to **Picture**.
2. Set the search date and click **Search**. Dates that contain captured images are indicated.
3. Set the time range to narrow the search to a specific period.
4. Select the capture type to search. All types are selected by default.

5. Click **Search** to begin.
6. Review the results in the display area. Double-clicking an image plays the recording from shortly before and after the capture.
7. Use the page controls in the lower-right corner to move through additional results.

7.3 Playback by Tag

This screen lists tags added previously, and lets you play back, rename, or delete them.

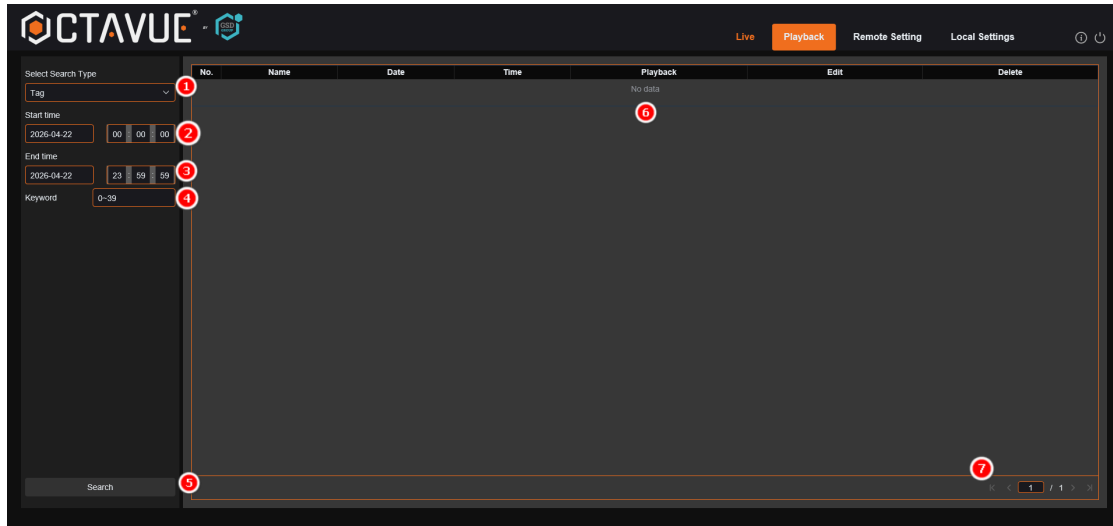


Figure 7-4. Playback by tag.

1. Confirm that the search mode is set to **Tag**.
2. Set the start time of the search.
3. Set the end time of the search.
4. Enter a keyword to match against tag names.
5. Click **Search** to begin.

Each entry in the results area provides the following controls:

- Play.** Plays back the tagged event.
- Edit.** Opens the event name for editing. Click **Save** to store the change; a confirmation message is shown.
- Delete.** Removes the tagged event.

Use the page controls in the lower-right corner to move through additional results.

7.4 Smart Playback

Smart playback runs in the browser without a plug-in. It identifies clips in which an alarm was triggered by a person and marks them in blue on the timeline at the bottom of the screen.

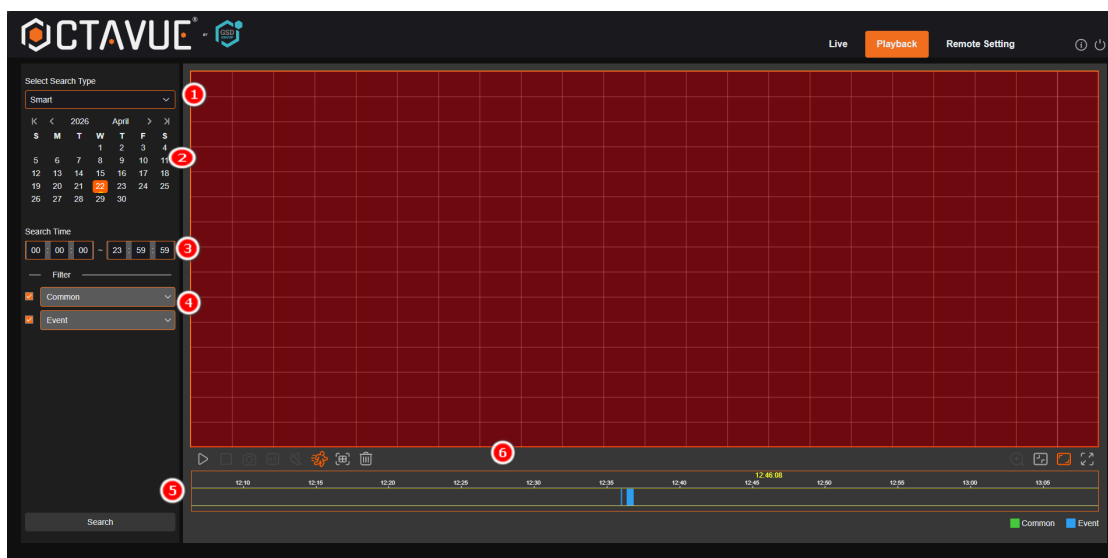


Figure 7-5. Smart playback.

1. Confirm that the search mode is set to **Smart**.
2. Set the date and click **Search**. Dates for which recordings exist are indicated.
3. Set the time range for the search.
4. Choose the search type to limit the results.
5. Click **Search** to begin.
6. Review the results in the display area.

The smart-playback toolbar provides the following controls:

-  **Stop.** Stops the playback stream.
-  **Capture.** Captures a still image from the current stream.
-  **Speed.** Sets the playback speed to 1/8, 1/4, 1/2, 1, 2x, 4x, 8x, or 16x.
-  **Audio.** Enables, disables, or adjusts the stream audio.
-  **Add Default Tag.** Adds a tag using the default name, Tag.
-  **Add Tag.** Adds a custom tag; the name may be 1 to 39 characters.
-  **Smart.** Opens the smart-area setup.
-  **All.** Sets the entire image as the smart-detection area.
-  **Clear All.** Clears the entire smart-detection area.
-  **Digital Zoom.** Magnifies a selected area of the stream.
-  **Original Proportions.** Displays the stream at its native aspect ratio.
-  **Stretch.** Expands the stream to fill the display area.
-  **Full Screen.** Displays playback in full screen. Double-click the image to toggle full screen, and press Esc to exit.

7.5 AI Search

When intelligent detection is enabled on the camera, matching events are recorded as images and video clips that can be searched by category. The following sections describe each AI search; the detections themselves are enabled and tuned under the events and AI detection settings (see Events and AI Detection).

7.6 License Plate Detection Search

When license plate detection is enabled, the camera triggers an alarm for recognized plates and records images and video for later search.

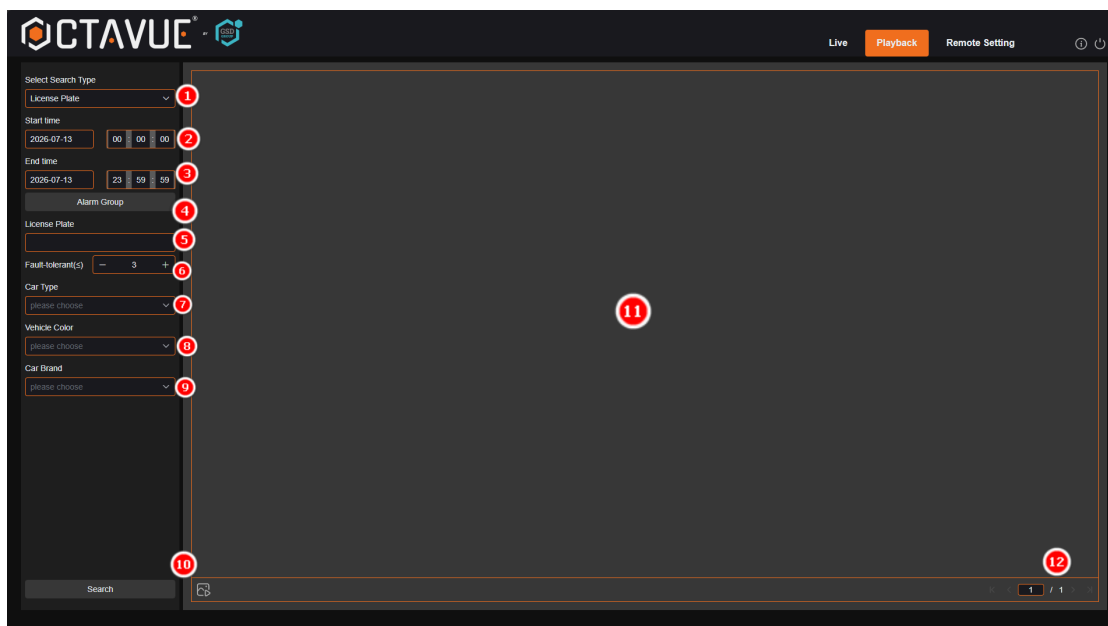


Figure 7-6. License plate detection search.

- **Search mode.** Confirm that the mode is set to License Plate.
- **Start time and end time.** Set the period over which to search for captured plates.
- **Alarm Group.** Restrict recognition to specific plate groups in the database. When no group is set, all images are searched and the similarity setting applies; when a group is set, unrecognized plates are ignored.
- **License Plate.** Filter the results by plate number.
- **Fault tolerance.** Set the number of characters, from 0 to 3, that may differ from a stored plate and still register a match. For example, with a tolerance of three, a vehicle with plate B734KB triggers an alarm against the stored plate B594SB.
- **Search.** Runs the search according to the settings.
- **Results.** Matches appear in the display area. Double-click an image to play the video from before and after the capture, and use the lower-right page controls to browse further results.

7.7 Pedestrian and Vehicle Search

Similar to face capture, this search distinguishes people from vehicles and records them separately, so results can be filtered by target type.

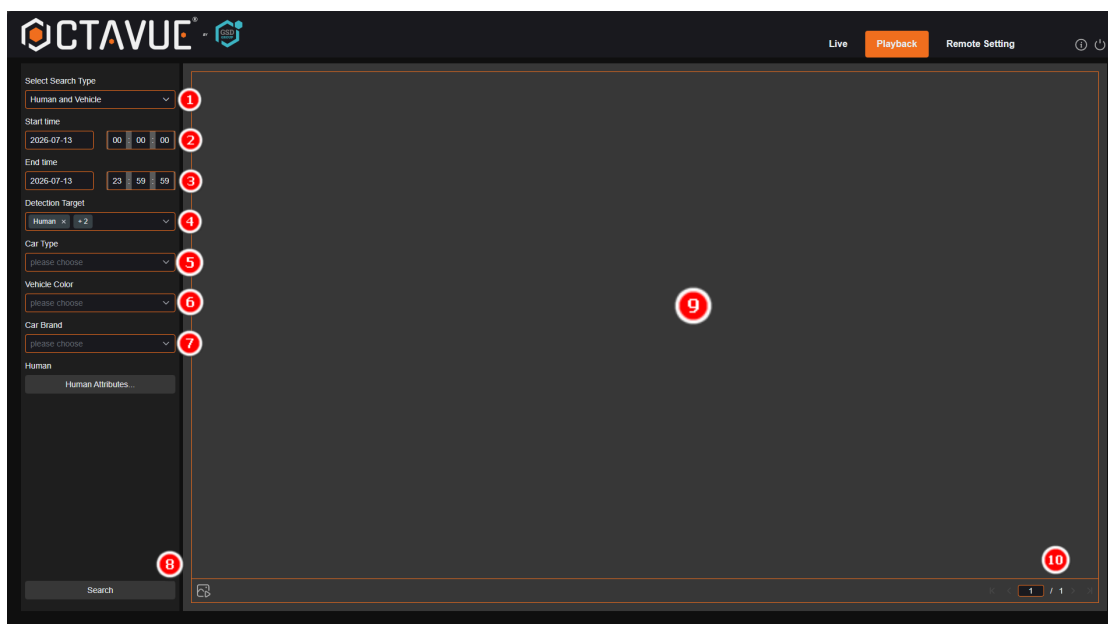


Figure 7-7. Pedestrian and vehicle search.

- **Search mode.** Confirm that the mode is set to Pedestrian and Vehicle.
- **Start time and end time.** Set the period over which to search for captured images.
- **Detection type.** Search for people, vehicles, or both.
- **Results.** Click Search to display matches. Double-click an image to play the surrounding video, and use the lower-right page controls to browse further results.

7.8 Line Crossing Search

Line-crossing detection alarms when a target crosses a defined line. It can be restricted to people or vehicles, and records images and video for later review.

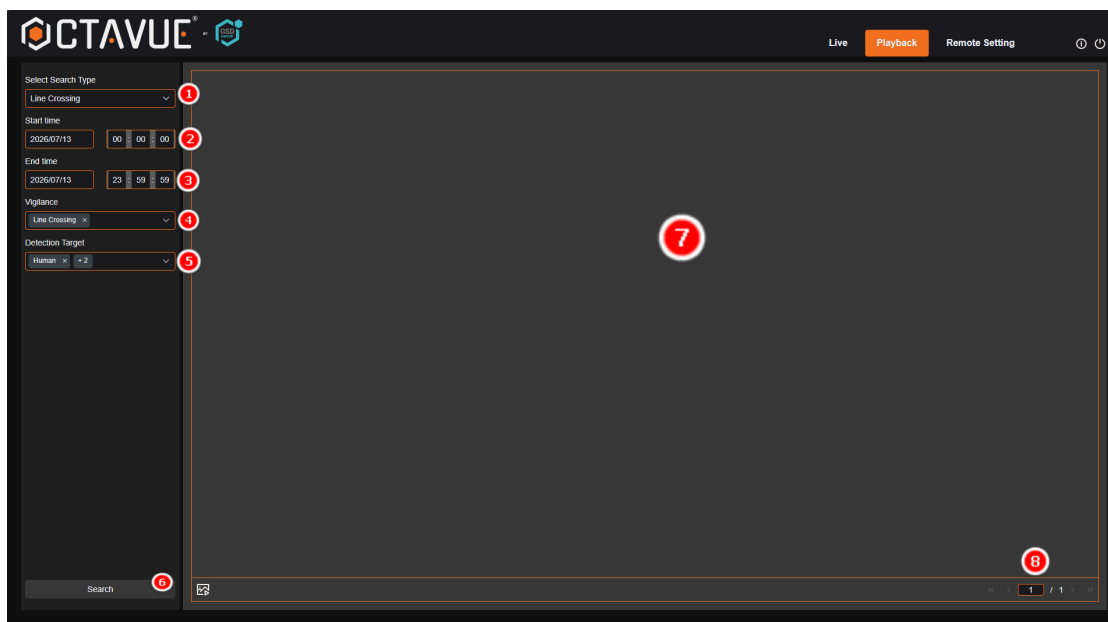


Figure 7-8. Line crossing search.

- **Search mode.** Confirm that the mode is set to Line Crossing.
- **Start time and end time.** Set the period over which to search for captured images.
- **Vigilance.** Set how the line-crossing alarm is captured.
- **Detection target.** Search for people, vehicles, or both.

- **Results.** Click Search to display matches. Double-click an image to play the video from shortly before and after the detection, and use the lower-right page controls to browse further results.

7.9 Intrusion Detection Search

When intrusion detection is enabled, the camera alarms when a target enters the guarded area, and records images and video for later review.

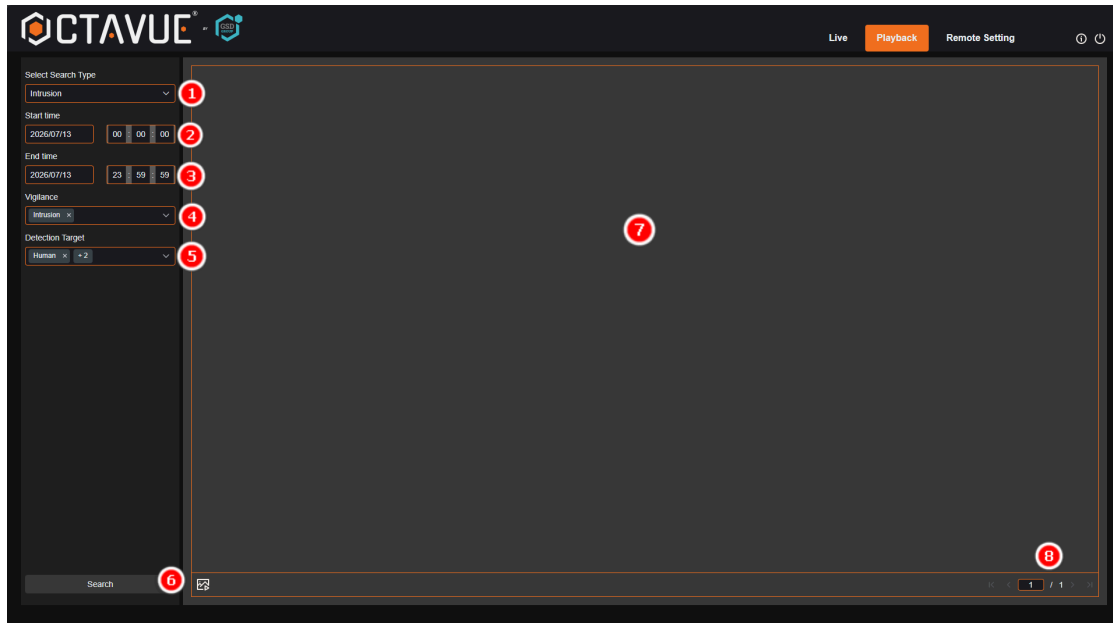


Figure 7-9. Intrusion detection search.

- **Search mode.** Confirm that the mode is set to Intrusion.
- **Start time and end time.** Set the period over which to search for captured images.
- **Vigilance.** Select Intrusion as the capture method.
- **Detection type.** Search for people, vehicles, or both.
- **Results.** Click Search to display matches. Double-click an image to play the surrounding video, and use the lower-right page controls to browse further results.

7.10 Region Entrance Search

When region-entrance detection is enabled, the camera alarms when a target enters the guarded area, and records images and video for later review.

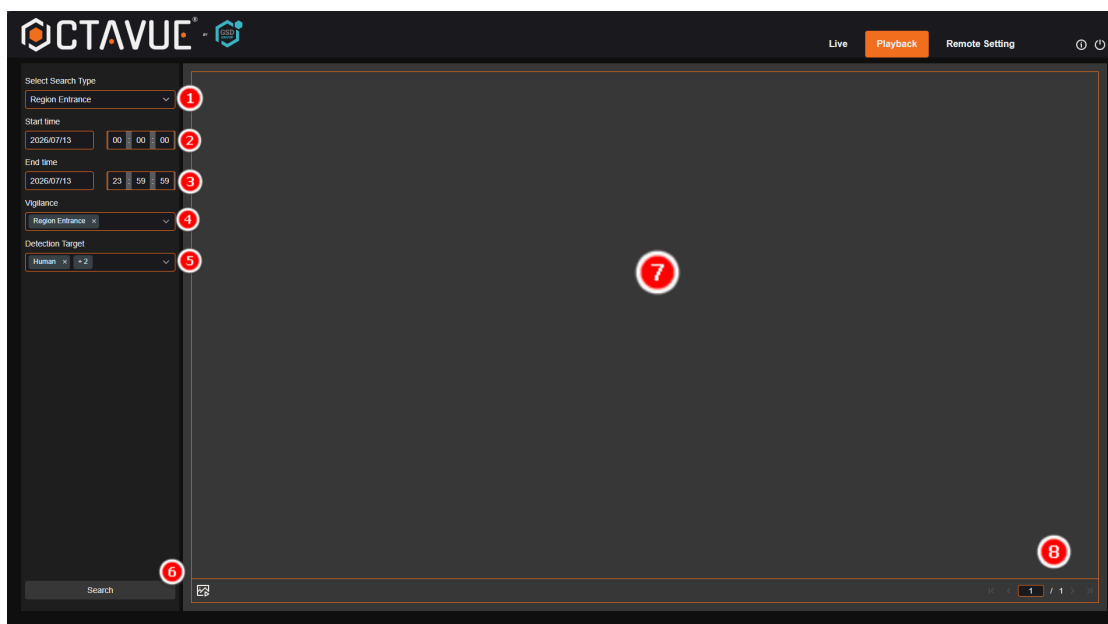


Figure 7-10. Region entrance search.

- **Search mode.** Confirm that the mode is set to Region Entrance.
- **Start time and end time.** Set the period over which to search for captured images.
- **Vigilance.** Set how the region-entrance alarm is captured.
- **Detection target.** Search for people, vehicles, or both.
- **Results.** Click Search to display matches. Double-click an image to play the video from shortly before and after the detection, and use the lower-right page controls to browse further results.

7.11 Region Exiting Search

When region-exiting detection is enabled, the camera alarms when a target leaves the guarded area, and records images and video for later review.

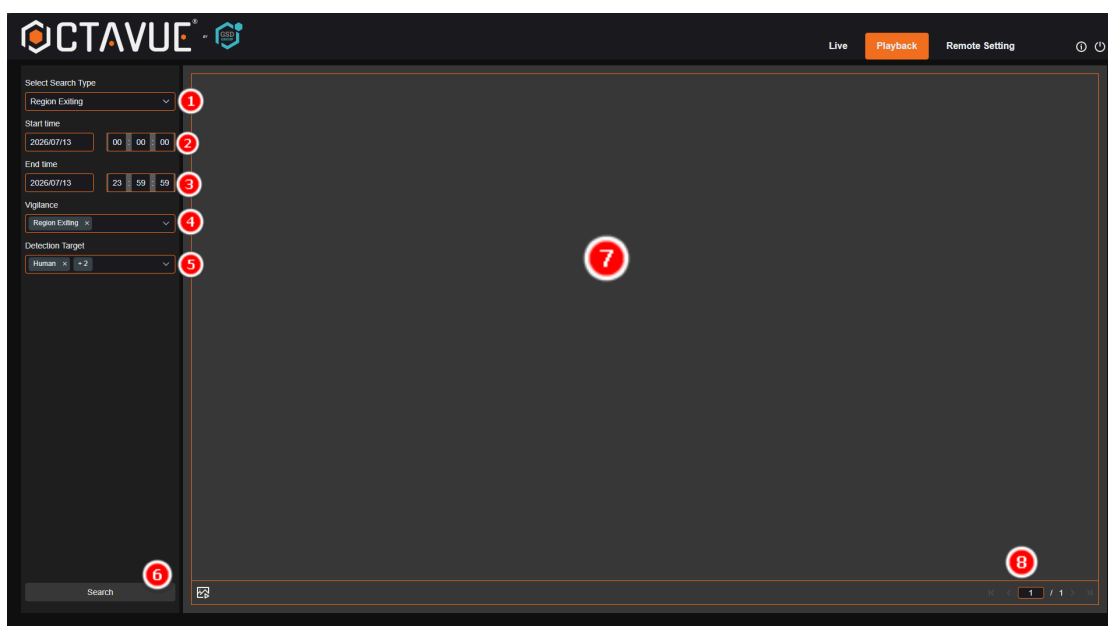


Figure 7-11. Region exiting search.

- **Search mode.** Confirm that the mode is set to Region Exiting.
- **Start time and end time.** Set the period over which to search for captured images.
- **Vigilance.** Select Region Exiting as the capture method.

- **Detection type.** Search for people, vehicles, or both.
- **Results.** Click Search to display matches. Double-click an image to play the surrounding video, and use the lower-right page controls to browse further results.

Chapter 8 Local Settings

Local Settings define where the web client saves files on your computer and in what format. They cover the folders used for recordings, downloads, and captured images, and the file formats for saved video and images.

NOTE This page does not appear when the web client is opened in Safari 12 or later, Chrome 57 or later, Firefox 52 or later, or Microsoft Edge 41, which handle these settings without it.

The screenshot shows a 'Path configuration' window with a dark background. It contains several settings:

- Record Path:** A text field containing 'D:\Device\Record' with a folder icon to its right.
- Download Path:** A text field containing 'D:\Device\Download' with a folder icon to its right.
- Snapshot Path:** A text field containing 'D:\Device\Capture' with a folder icon to its right.
- File type:** A dropdown menu currently showing 'MP4'.
- Interval:** A dropdown menu showing '10' with a 'Minute' label to its right.
- Capture Type:** A dropdown menu currently showing 'JPG'.
- Save:** A button located at the bottom center of the configuration area.

Figure 8-1. Local Settings - storage paths and file formats.

- **Storage paths.** Set the local folders where recorded video, downloaded recordings, and captured images are saved.
- **File formats.** Choose the format used for saved video and for captured images.

Configuration

Configure every aspect of the camera through the Remote Setting menu — imaging, recording, detection, alarms, network, and system administration.

Chapter 9 Image and Video Settings

This chapter covers the settings that determine how the camera captures and displays its scene: the information overlaid on the live image, the exposure and color behavior of the sensor, privacy masking, the resolution and compression of each stream, snapshot timing, and PTZ control. Each section corresponds to a page in the Image and Video area of the web client.

9.1 Preview and On-Screen Display

The Preview page controls the channel name, date and time, and other information overlaid on the live image, along with the position of each overlay element. Use it to label a channel and to decide what appears on screen during live view and playback.

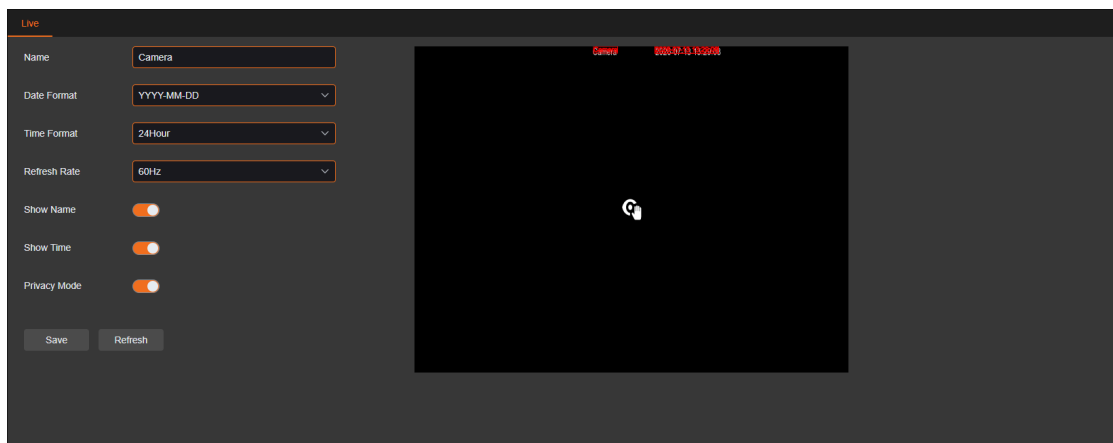


Figure 9-1. Preview page — overlay text, formats, and positions.

- **Channel Name.** Sets the name assigned to the camera channel.
- **Date Format.** Sets the date format shown in the on-screen display (OSD). Three formats are available: MM/DD/YYYY, YYYY-MM-DD, and DD/MM/YYYY.
- **Time Format.** Sets the OSD time format: 12-hour or 24-hour.
- **Refresh Rate.** Sets the image refresh rate to 60 Hz or 50 Hz, corresponding to the N and P systems respectively.
- **Show Name.** Displays the channel name on the live image.
- **Show Time.** Displays the camera time on the live image.
- **Privacy Mode.** When enabled, no image is shown in live view or playback, and the preview image is also hidden on the Settings page.
- **Show Channel Name Position.** Sets where the channel name appears; drag the name on the image to reposition it.
- **Display Time Position.** Sets where the time appears; drag the time on the image to reposition it.

- **Display Alarm Statistics Position.** Sets where alarm statistics appear; drag the statistics on the image to reposition them. This option is shown only when a function that supports alarm-statistics display is enabled.

Click **Save** to store the changes, or **Refresh** to reload the current values from the camera.

9.2 Image Control

Image Control provides direct access to the image-quality parameters of the sensor, including day/night behavior, supplemental lighting, exposure and backlight compensation, white balance, shutter, and noise reduction. Adjust these settings to suit the lighting and mounting conditions of the installation site.

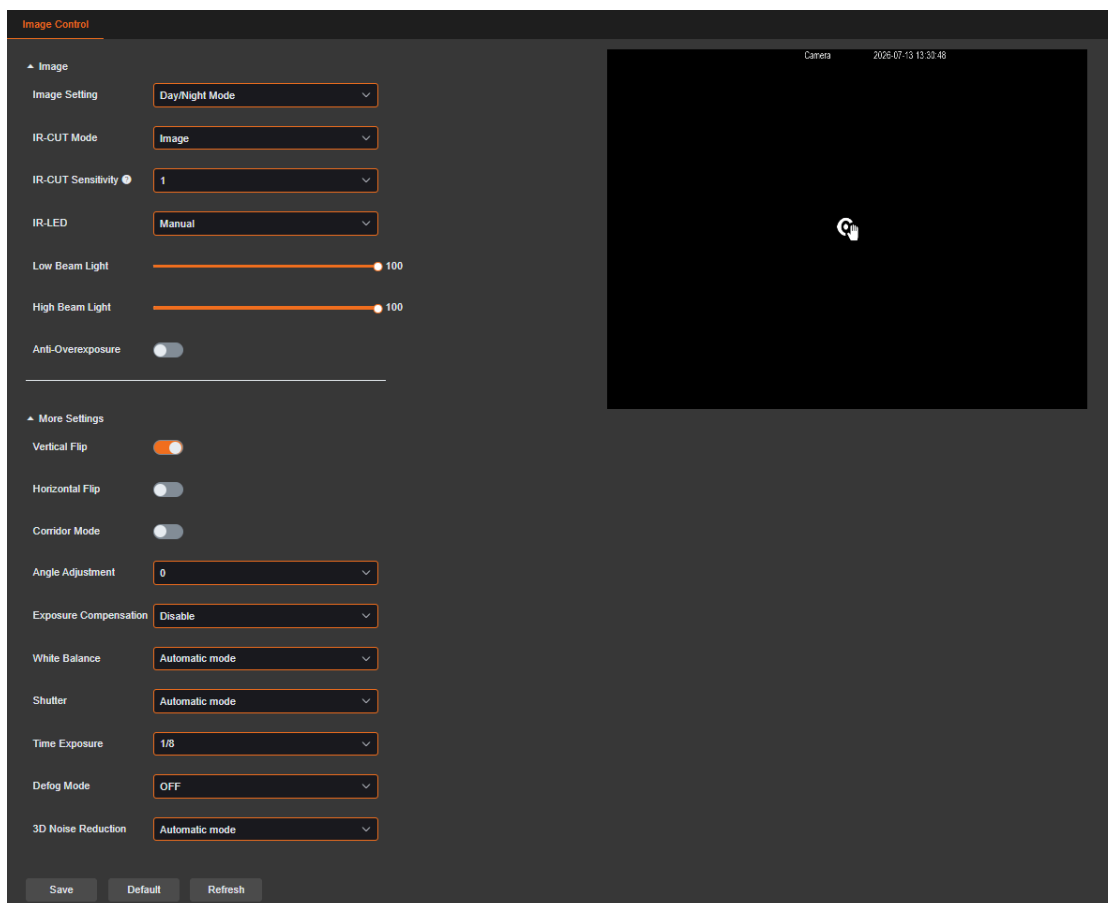


Figure 9-2. Image Control page — sensor and image-quality parameters.

9.2.1 Day and Night Mode

- **Image Setting.** Selects the image mode. Three modes are available.
- **Full Color Mode.** The camera remains in full color.
- **Day/Night Mode.** The camera switches between day (color) and night (black-and-white) operation.
- **Smart Illumination.** While in night vision, an alarm activates the warm light for supplemental illumination and the image becomes color; when the alarm ends, the camera returns to night vision.
- **White Light.** In Full Color Mode, sets the behavior of the camera's warm supplemental light. Four modes are available.
- **Automatic.** The camera adjusts the supplemental-light intensity according to ambient illumination.
- **Manual.** Applies a fixed brightness value to the scene.
- **Schedule.** Switches the warm light on and off according to a defined time schedule.
- **OFF.** Turns the warm light off.
- **Sensitivity.** Sets the camera's responsiveness to ambient light, from 0 to 3; a higher value is more sensitive.

- **Light Distance.** In Manual mode, sets the brightness of the white supplemental light, from 0 to 100; a higher value is brighter.
- **IR-CUT Mode.** In Day/Night Mode, sets how the camera switches between day and night. Five modes are available.
- **Auto / GPIO Auto.** Automatic switching: color to black-and-white is judged from the image, and the return to color is judged by the photosensor.
- **Day / Color Mode.** Forces color mode without switching to black-and-white.
- **Night / Black White Mode.** Forces black-and-white mode without switching to color.
- **Image / Image Mode.** Similar to Auto, but the transition between color and black-and-white is controlled from the image only.
- **Schedule / Schedule (B/W).** Switches between color and black-and-white by schedule. Set the start and end times for entering night vision to use this mode.
- **IR LED Control.** Sets the behavior of the camera's infrared LED during night vision. Three modes are available.
- **Smart IR.** Automatically controls infrared intensity based on focal length and whether the image is overexposed.
- **Manual.** Applies the configured IR brightness.
- **OFF.** Disables the infrared supplemental light.
- **Low / High Beam Light.** Manually adjusts infrared brightness, from 0 to 100. At 0 the IR light is off; at 100 it is at maximum brightness.
- **Anti-Overexposure.** When enabled in any image mode, prevents overexposure in high-brightness environments.

9.2.2 Orientation and Rotation

- **Corridor Mode.** Rotates the image 90 degrees clockwise for tall, narrow scenes. Supported on selected models.
- **Angle Adjustment.** Rotates the image to correct the camera's mounting orientation — for example, when a camera designed for inverted mounting is installed in a flat position.
- **Vertical Flip.** Flips the image top to bottom.
- **Horizontal Flip.** Mirrors the image left to right.

9.2.3 Exposure and Backlight

- **Exposure Compensation.** Sets how the camera responds to backlit scenes. Four modes are available.
- **WDR.** Wide Dynamic Range balances the image so that both bright and dark areas remain clearly distinguishable. Referred to as DWDR on some models.
- **HLC.** Highlight compensation makes objects in very bright areas clearer, according to the configured HLC Level. Not supported on some models.
- **Back Light.** Makes dark areas of the image clearer, according to the configured BLC Level and BLC Area.
- **Disable.** Applies no exposure compensation.

9.2.4 White Balance and Shutter

- **White Balance.** Adjusts color rendition. Two modes are available.
- **Automatic.** Uses default parameters to balance white light.
- **Manual.** Sets the red, green, and blue gains that combine to form white.
- **Shutter.** Sets the exposure duration. Models with aperture support offer additional modes; models without it offer only automatic and manual modes.
- **Automatic.** Selects an appropriate exposure time and aperture value based on the configured Time Exposure and Iris ranges.
- **Manual.** Uses the configured Time Exposure and Iris values directly.

- **Shutter First.** Uses a manually defined shutter value while the camera meters the corresponding aperture value.
- **Iris First.** Uses a manually defined aperture value while the camera meters the corresponding shutter value.

NOTE Manual shutter mode removes the flickerless option; automatic shutter mode enables it. If you switch back to manual mode, the exposure time reverts automatically to 1/100 or 1/120.

- **Exposure Time.** Sets the exposure time, used together with the Shutter setting. A long exposure time can overexpose the image, while a short exposure time darkens it.

9.2.5 Image Enhancement

- **Defog Mode.** When enabled, improves image clarity in rain and fog.
- **3D Noise Reduction.** Reduces image noise for a clearer picture. Three modes are available.
- **Automatic.** The camera selects the noise-reduction level algorithmically.
- **OFF.** Disables noise reduction.
- **Manual.** Applies the manually configured noise-reduction coefficient.
- **DIS.** Digital Image Stabilization uses software to reduce blur and instability caused by vibration or shaking, producing a smoother image according to the configured DIS Level. Supported on selected models.
- **Lens Distortion Correction.** When enabled, reduces distortion near the edges of the image. Supported on selected models.
- **FoV Adjustment.** Sets the distortion-correction intensity, from 0 to 5.

Click **Save** to store the parameters, **Default** to restore the image-control settings to their factory values, or **Refresh** to reload the current values.

9.3 Privacy Mask

The Privacy Mask function conceals specific areas of the scene, such as windows or keypads, that should not be recorded or displayed. You can create up to four privacy zones — six on some models — of any size and position.

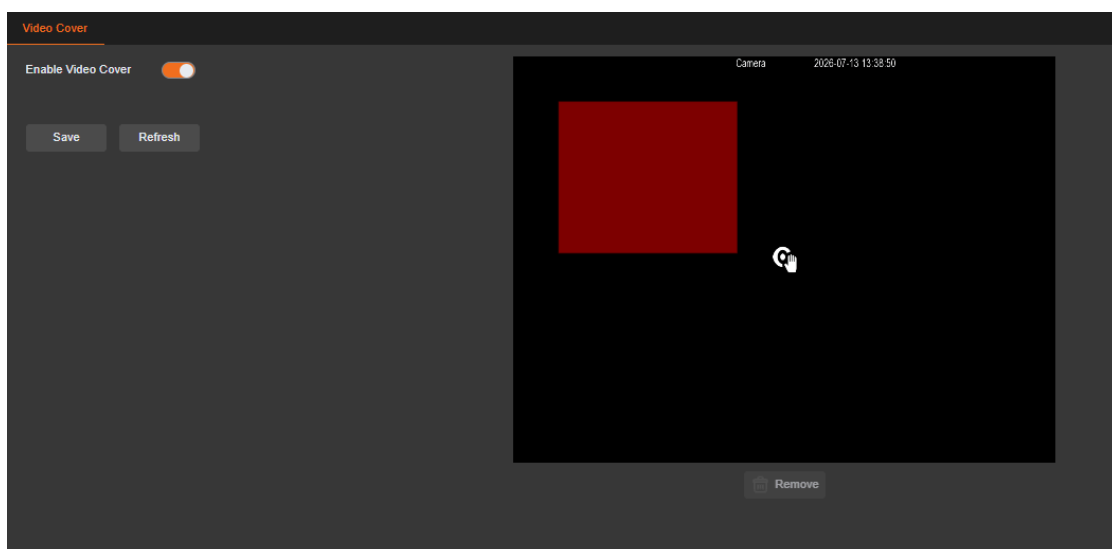


Figure 9-3. Privacy Mask page — defining covered areas.

To create a zone, enable the function and draw an area on the image. Each area appears as a red box while you edit it; click and drag the edges of the box to resize it. Once the settings take effect, the masked areas are rendered as solid black blocks.

- **Enable.** Enables or disables the Privacy Mask function.

- **Video Cover Area Setting.** Defines the areas to be masked in the monitored scene. Masked blocks appear red while being set and turn black once they take effect.
- **Remove.** Deletes the selected masked blocks.

NOTE Areas covered by a privacy mask are not visible during live view or playback.

9.4 Video Parameters

The Video Parameters page configures the resolution, frame rate, and compression of each video stream, together with the recording and audio behavior of the camera. Settings are grouped into recording, coding, and audio management.

9.4.1 Recording Parameters

These settings determine how the camera records to its memory card.

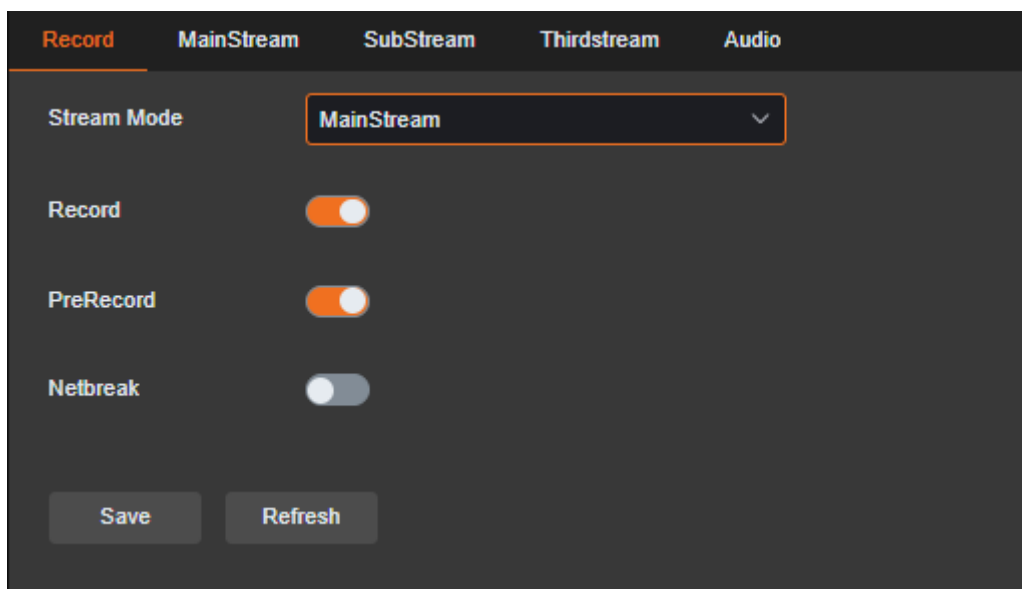


Figure 9-4. Recording parameters.

- **Stream Mode.** Selects the stream recorded to the memory card. The default is the main stream.
- **Record.** Enables recording.
- **PreRecord.** When enabled, the camera begins recording a few seconds before an alarm event. This is recommended when recording is based primarily on motion detection or I/O alarms.
- **Netbreak.** Continues event recording when the network is disconnected or the connection fails.

9.4.2 Coding Parameters

These settings define the image-quality parameters used for recording and for network transmission. The main stream is the quality of the recording stored on the memory card; the sub stream is the quality of the preview accessed remotely, for example by web clients and video management software; and the mobile stream, which can be turned off, defines the quality of the preview viewed remotely on a mobile device.

The screenshot shows a configuration window for video encoding. The 'MainStream' tab is selected. The settings are as follows:

Parameter	Value	Unit/Range
Resolution	2688 x 1520	
FPS	30	
Video Code Type	H.265	
Video Code Level	Main Profile	
Bitrate Control	CBR	
Bitrate Mode	Predefined	
Bitrate	4096	Kbps
I Frame Interval	60	(1 ~ 120)
Audio	Enabled (Toggle)	

Buttons at the bottom: Save, Default, Refresh.

Figure 9-5. Coding parameters for the main, sub, and mobile streams.

- **Resolution.** Sets the resolution of the recorded image.
- **Frame Rate.** Sets the number of frames per second the camera records.
- **Encoding Format.** Selects the compression type: H.264, H.265, H.264+, H.265+, or MJPEG. MJPEG is available for the sub stream only.
- **Video Code Level.** Sets the video quality profile: Baseline, Main Profile, or High Profile. Main Profile applies only when H.265 is selected.
- **Encoding Mode.** Selects the bitrate strategy. Constant Bit Rate (CBR) suits simple scenes such as a plain wall; Variable Bit Rate (VBR) suits complex scenes such as busy streets.
- **Config Mode.** Choose User Defined to set the bitrate manually, or Preset Mode to select a preset bitrate.
- **Bitrate.** Sets the data rate used to record the video. A higher bitrate yields better image quality.
- **I Frame Interval.** Sets the interval between I-frames.
- **Audio.** Enable this option to record audio together with video when a microphone is connected to the camera or the camera has built-in audio.

Click **Save** to store the encoding parameters, **Default** to restore them to their factory values, or **Refresh** to reload the current values.

9.4.3 Audio Management

These settings control the audio input and output of the camera.

Figure 9-6. Audio Management — input type, volume, and codec.

- **Audio Input Type.** Selects the audio input: MicIn uses the camera's built-in microphone; LineIn uses the audio input on the camera's tail lead. Supported on selected models.
- **Output Volume.** Sets the output audio volume.
- **Input Volume.** Sets the input audio volume.
- **Audio Code Type.** Sets the audio codec: G.711A or G.711U.

9.5 Capture Settings

The Capture Settings page configures the automatic snapshot function, which saves still images at defined intervals during normal recording and when an alarm occurs.

Figure 9-7. Capture Settings — snapshot intervals.

- **Normal Interval.** Sets the interval between snapshots during normal recording.
- **Alarm Interval.** Sets the interval between snapshots when motion detection or an I/O alarm is triggered.
- **Auto Capture.** Enables or disables automatic snapshots.

9.6 PTZ and RS-485 Settings

On models with an RS-485 interface, the PTZ page configures communication with a pan-tilt-zoom head and controls its movement. Match these serial parameters to the connected head; a mismatch prevents PTZ control.

PTZ	
Scheduled Tasks	
Protocol	Pelco-D
Baudrate	9600
Data Bit	8
Stop Bit	1
Parity	None
Address	1
Focus mode	Semi-auto
Zoom Status	5 S
Pan & Tilt Status	5 S
Preset Status	5 S
Min. Focus Distance	Auto

Save Refresh

Figure 9-8. PTZ page — RS-485 protocol and control parameters.

- **Protocol.** Selects the communication protocol used between the camera and the PTZ head.
- **Baudrate.** Sets the speed at which the camera sends information to the head. This value must match the head's baud rate.
- **DataBit / StopBit.** Messages between the camera and the head are sent as separate packets. DataBit sets the number of data bits per packet (8, 7, 6, or 5; the default 8 is recommended); StopBit marks the end of a packet and the start of the next (1 or 2; the default 1 is recommended).
- **Parity.** Sets the parity used for error checking. Refer to the head's documentation to configure this value. The default is None.
- **Address.** Sets the address code. When several devices share an analog protocol, each address code must be unique.
- **Focus Mode.** Sets how the lens focuses.
- **Auto.** Focuses automatically as the scene changes.

- **Semi-auto.** Focuses once after the head is moved or the lens is zoomed, and does not refocus when the scene changes. This is the default.
- **Manual.** Focuses only when you operate the focus control in the preview interface; movement, zoom, and scene changes do not trigger focusing.
- **Zoom Status.** Sets whether — and for how long — the lens magnification is shown in the lower-left corner of the preview.
- **Pan & Tilt Status.** Sets whether — and for how long — the horizontal and vertical position of the head is shown in the lower-left corner of the preview.
- **Preset Status.** Sets whether — and for how long — the number of the called preset is shown in the lower-left corner of the preview.
- **Min. Focus Distance.** Sets the minimum focus distance. Objects closer than this distance are ignored, and the lens focuses in preference on objects beyond it. For example, with a minimum focus distance of 6 m and a baffle placed at 1.5 m blocking part of the field of view, the camera focuses on the distant scene beyond 6 m.

Chapter 10 Recording, Storage, and Schedules

This chapter describes when the camera records and captures images, and where that data is stored. Schedule Setup defines the times at which recording and snapshots occur, while Disk Management prepares the memory card and connects network storage. Other chapters refer to the schedule configuration described here as the Schedule Setup section.

10.1 Schedule Setup

Schedule Setup defines the periods during which the camera records video and captures snapshots. Schedules can be built for normal (continuous), motion, and I/O event types, and reusable templates simplify applying the same schedule across channels.

10.1.1 Record Schedule

Use the Record Schedule to define continuous and alarm recording over a repeating weekly period.

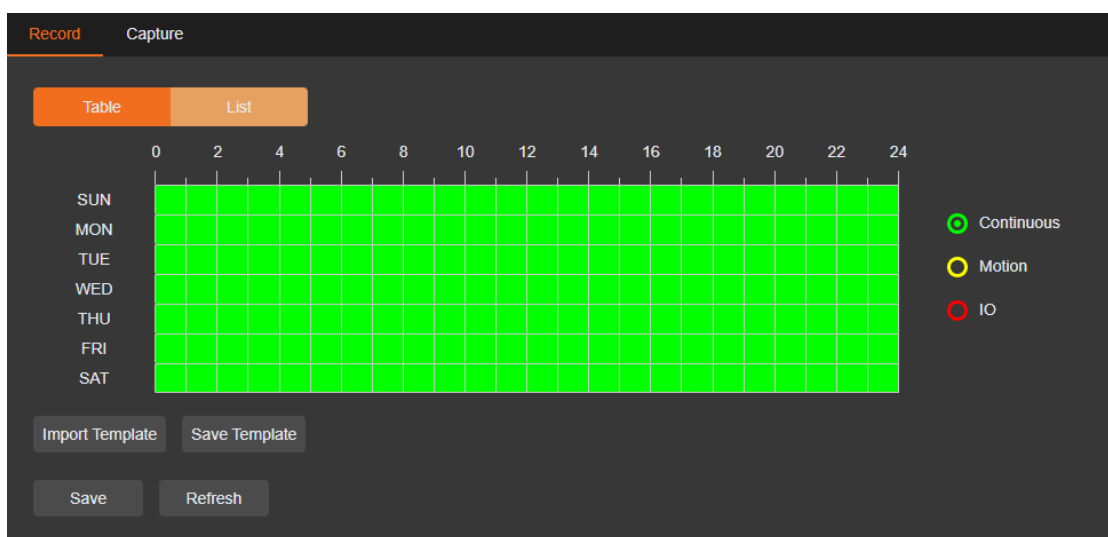


Figure 10-1. Record Schedule — weekly recording grid.

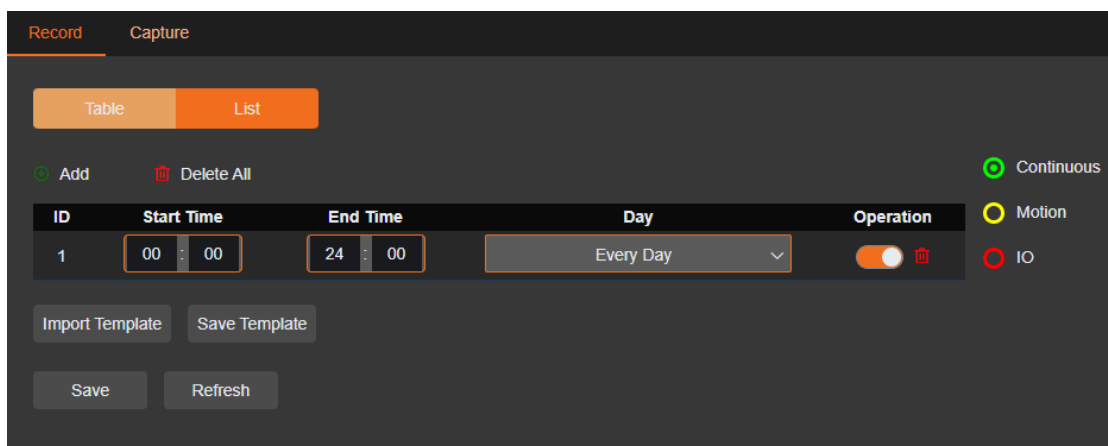


Figure 10-2. Editing a recording rule by time period and day.

- **Table / List.** Presents the schedule as a grid or as a list. Use the **Normal**, **Motion**, and **I/O** buttons on the right to switch between recording types. In Table form, drag or select the relevant time cells to set the schedule; in List form, add rules manually and enter the start and end times.
- **Add.** Adds a schedule rule.
- **Delete All.** Deletes all schedule rules.
- **Start Time.** Sets the start time of a schedule rule.
- **End Time.** Sets the end time of a schedule rule.
- **Day.** Sets the days on which the schedule rule takes effect.

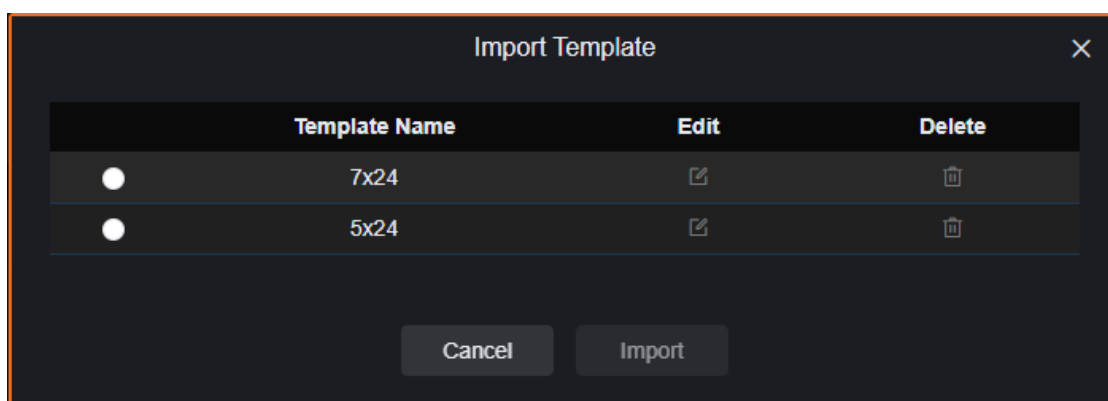


Figure 10-3. Applying and managing schedule templates.

- **Import Template.** Imports a custom or system-default schedule template.
- **Edit.** Edits a schedule template to change its name and rules.
- **Delete.** Deletes a schedule template.

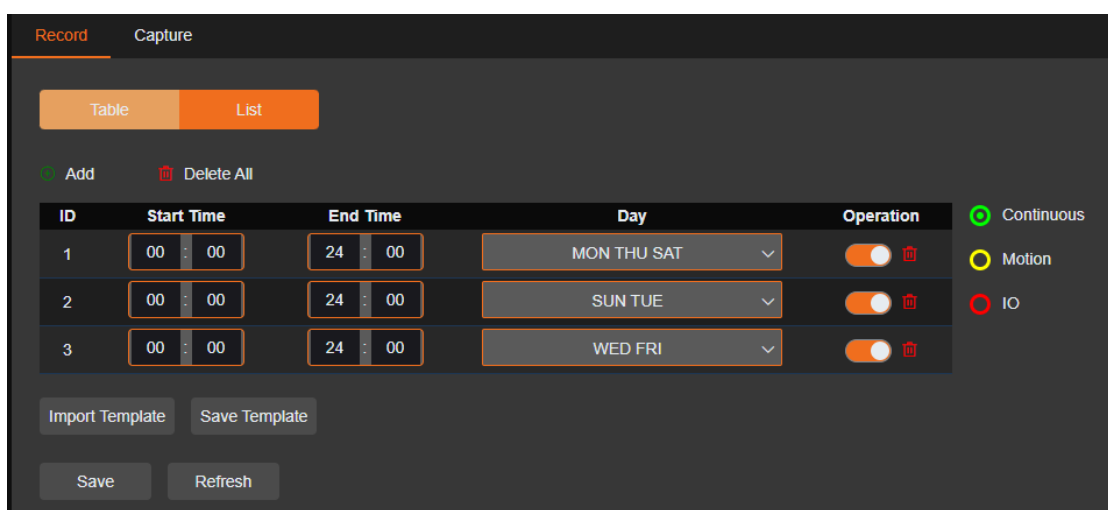


Figure 10-4. Built-in and custom schedule templates.

NOTE The system provides two default templates, 7x24 and 5x24, which cannot be edited or deleted.

- **Save Template.** Saves the current schedule rules as a custom template that can be imported on other schedule pages.

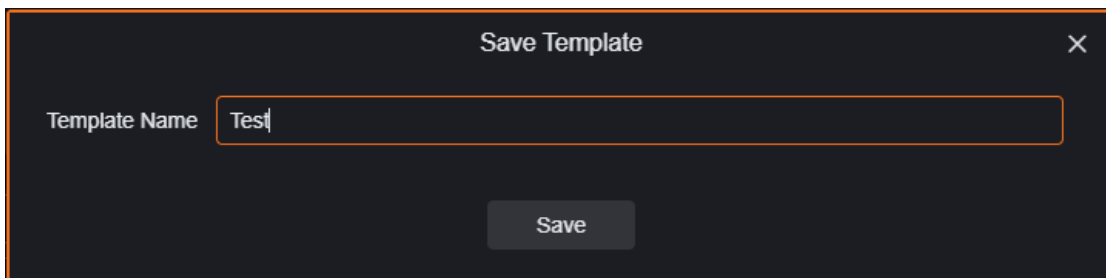
A dark-themed dialog box titled "Save Template" with a close button (X) in the top right corner. It contains a text input field labeled "Template Name" with the text "Test" entered. Below the input field is a "Save" button.

Figure 10-5. Saving the current schedule as a custom template.

Click **Save** to store the schedule, **Copy** to apply the same parameters to other channels, or **Refresh** to reload the current values.

10.1.2 Capture Schedule

Use the Capture Schedule to define continuous and alarm snapshots, so that capture actions run only during the set periods. It is configured in the same way as the Record Schedule, using the grid, rules, and templates described above.

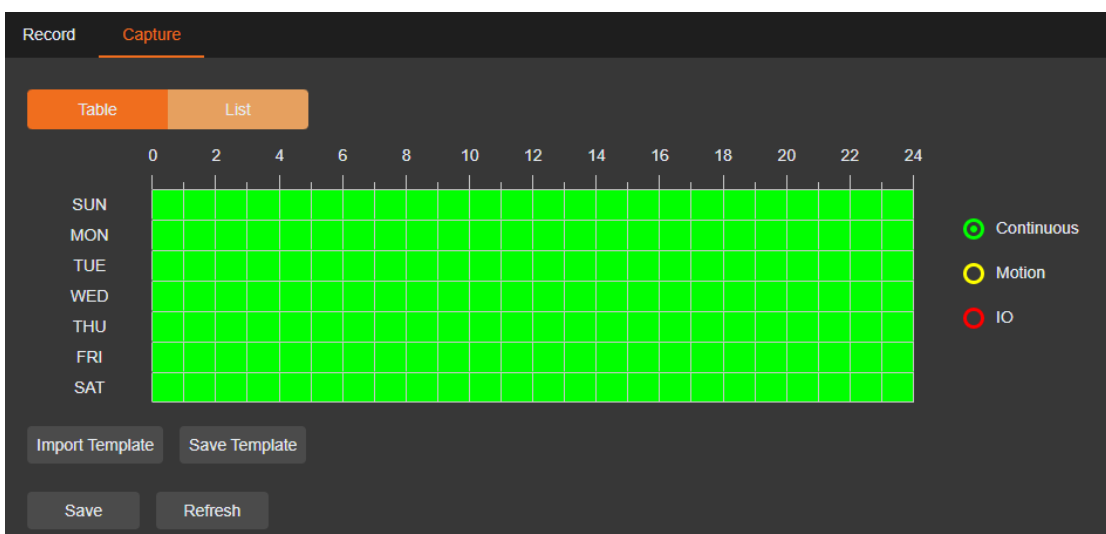
A screenshot of the "Capture" tab in a software interface. It shows a weekly snapshot grid with days of the week (SUN to SAT) on the y-axis and time slots (0 to 24) on the x-axis. The grid cells are highlighted in green, indicating a continuous capture schedule. To the right of the grid is a legend with three options: "Continuous" (green circle), "Motion" (yellow circle), and "IO" (red circle). Below the grid are buttons for "Import Template", "Save Template", "Save", and "Refresh".

Figure 10-6. Capture Schedule — weekly snapshot grid.

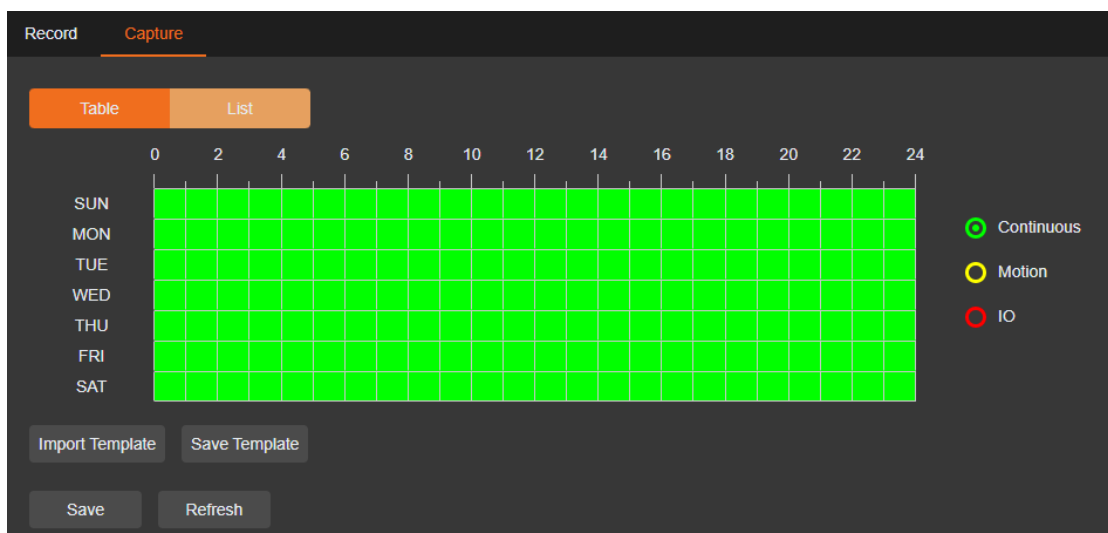


Figure 10-7. Editing a capture rule by time period and day.

10.2 Disk Management

Disk Management lets you check and prepare the camera's internal memory card and connect network storage. Format the card on first use and whenever it is replaced.

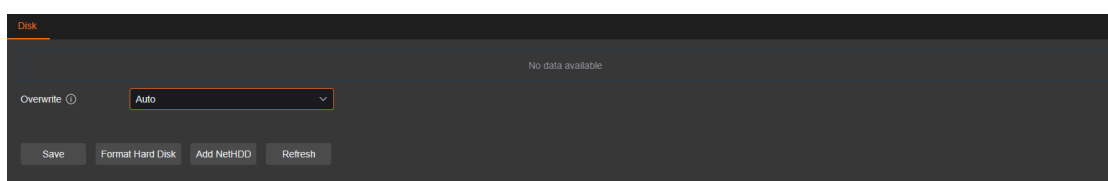
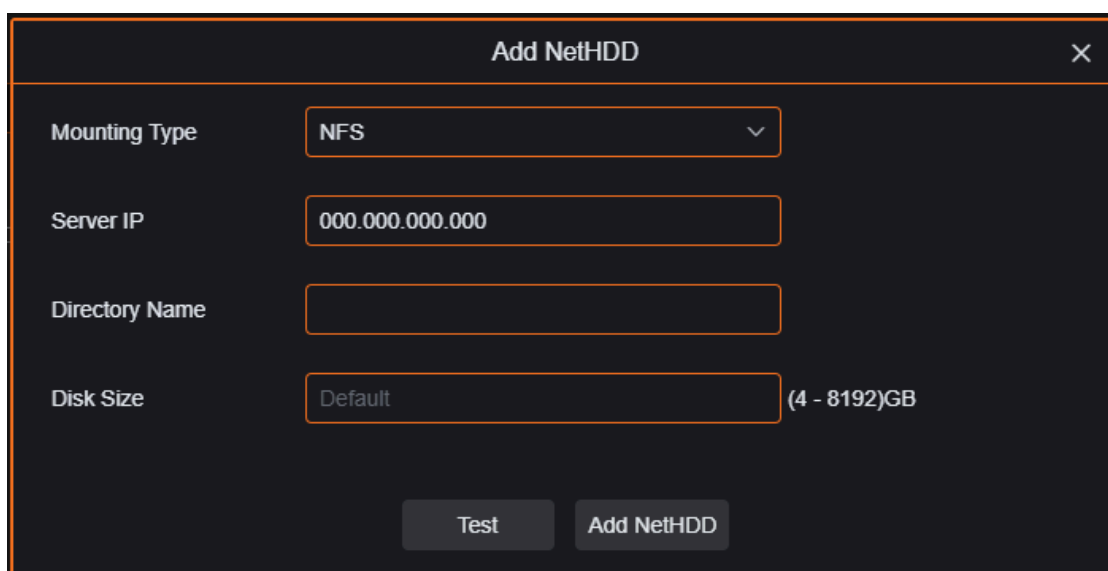


Figure 10-8. Disk Management — memory-card status and formatting.

- **Format Hard Disk.** Select the memory card to format, then click **Format SD Card**. To begin, enter your user name and password and click **OK**.
- **Overwrite.** Controls how the camera reuses card space when the card is full. Select **Auto** to automatically overwrite the oldest data, or **OFF** to keep all recordings. When overwrite is disabled, check the card periodically to ensure it does not fill up.

CAUTION Formatting erases all recordings and snapshots on the memory card. Back up any data you need before formatting.



Network storage lets the camera record video and capture images to a network hard disk. Once a network HDD (NAS) is configured, keep it connected to the network so recordings and snapshots can be written to it. The AI face database can be stored only on a network HDD.

- **Mounting Type.** Selects the protocol: NFS or SMB/CIFS. NFS does not require a user name and password; SMB/CIFS does.
- **User Name.** The NAS user name. Not used in NFS mode.
- **Password.** The NAS password. Not used in NFS mode.
- **Server IP.** The IP address of the NAS.
- **Directory Name.** The folder on the NAS in which to store data.
- **Disk Size.** The size of the network HDD.
- **Test.** Tests connectivity to the NAS.
- **Add NetHDD.** Adds the configured NAS.

Chapter 11 Events and AI Detection

The camera includes a suite of AI-based detection functions that analyze the video stream in real time and raise an alarm when a defined event occurs. Each function is turned on individually from the setup menu before it can be used.

AI detection consumes on-board processing power, and the camera's performance is finite. As a result, some AI functions cannot run at the same time. The combinations available on a given model are stated by the on-screen prompts for that model, which take precedence over the general descriptions in this chapter.

11.1 Common Detection Settings

Most detection types share the same core controls. They are described once here; the sections that follow list only the settings that are unique to each detection type and refer back to this section for everything else.

- **Min Pixel.** Sets the minimum pixel frame. A target must be larger than this frame to be recognized. Moving the pointer onto the slider shows the actual frame size in the preview on the right, where the frame can also be dragged; the preview frame disappears five seconds after the pointer leaves it.
- **Max Pixel.** Sets the maximum pixel frame. A target must be smaller than this frame to be recognized. As with the minimum, the frame is previewed and can be dragged on the right, and disappears five seconds after the pointer leaves it.
- **Sensitivity.** Governs how readily a target triggers an alarm. Higher sensitivity reduces missed alarms but increases false alarms. For area-based rules, the value corresponds to the proportion of the target that must enter the area: at 100% the alarm fires as the target touches the boundary, and at 50% it fires once half of the target has crossed it.
- **Target Validity.** Sets how closely a target must match the selected detection type. Level 1 requires a similarity of 80% or more, level 2 requires 60% or more, level 3 requires 40% or more, and level 4 requires 20% or more.
- **Detection Target.** Selects which object classes trigger the alarm — typically pedestrian, motor vehicle, and non-motorized vehicle (some types also offer an all-objects option).
- **Bounding Box.** Displays the detection box and the rule-line switch overlaid on the live image (supported on some models).
- **Rule Number.** Selects which of the detection rules is being edited. Up to four rule areas or lines are supported per detection type.
- **Rule Switch.** Enables the currently selected rule. Each rule has its own switch, tied to the active Rule Number.

- **Rule Type.** Selects the behavior a rule detects, where the detection type offers a choice (for example, a trigger direction or a class of event).
- **Detection Area.** Defines where detection applies. **Full Screen** monitors the entire field of view; **User-defined** limits detection to areas you outline, and supports polygons of three to eight sides.
- **Add / Draw / Remove / Remove All.** Manage rules in the setting area: **Add** inserts a default rule, **Draw** lets you draw one manually, **Remove** deletes the selected rule, and **Remove All** clears every rule.

NOTE The rule-line setting area on the right of each page is where detection areas and trigger lines are placed. The controls above operate on whichever rule is currently selected by **Rule Number**.

11.2 Face Detection

Face Detection captures faces that meet the configured requirements, computes their feature data with the face-model algorithm, and compares the result against the face database to raise an alarm. Enable the function before configuring it.

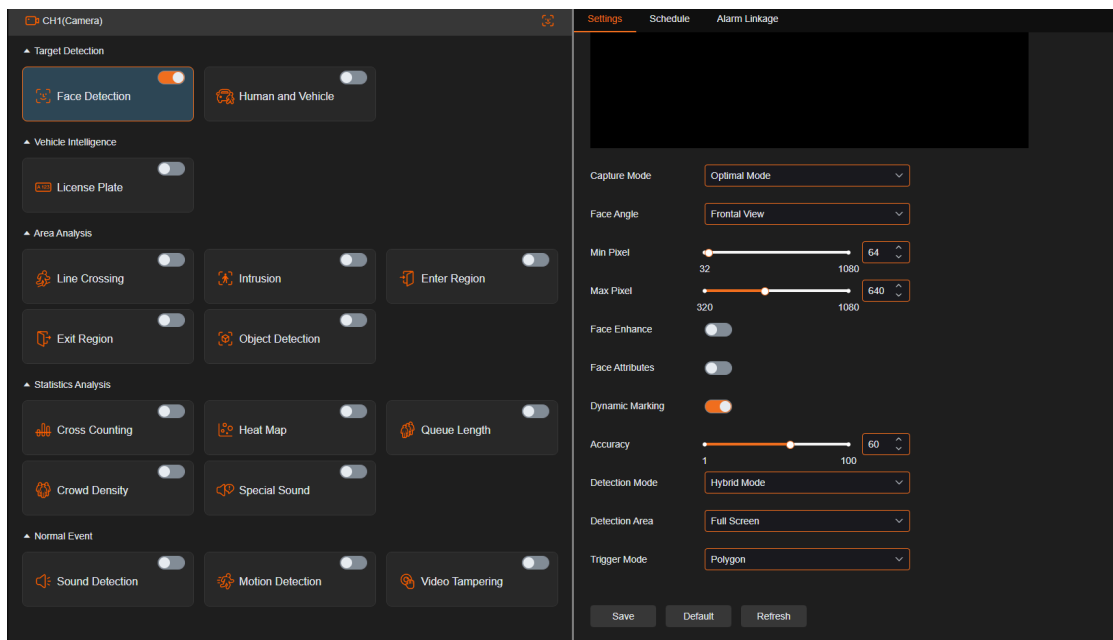


Figure 11-1. Face Detection settings.

Pixel size, sensitivity, bounding box, detection area, and rule controls behave as described in Common Detection Settings. The settings specific to Face Detection are:

- **Capture Mode.** Determines when captured images are pushed to live view or an attached NVR. In **Optimal Mode** the camera pushes only the single best image from the moment the face is detected until it disappears. In **RealTime Mode** the camera pushes an image immediately on detection and then pushes the best image when the face disappears.
- **Capture Interval.** Sets how many images are pushed and how often. **Snap Num** can be 1, 2, 3, or unlimited, and **Snap Frequency** ranges from 1 s to 255 s. At a frequency of 5 s, for example, images are pushed at 5 s, 10 s, and 15 s while the face remains in view.
- **Face Angle.** Filters captures by orientation so that only images meeting the angle criteria are pushed. **Frontal View** pushes only frontal faces; **Multi Angle** pushes side-facing views; **Customize** exposes the Roll Range, Pitch Range, Yaw Range, and Picture Quality controls together with the Frontal Default and Multi Default buttons.
- **Roll / Pitch / Yaw Range.** Set the permitted roll, pitch, and yaw of the captured face within the 3D model. A face outside these limits is still detected but its image is not pushed.
- **Picture Quality.** Raises the quality threshold; higher values help filter out captures that are not clear faces.

- **Frontal Default.** Under Customize, applies Roll Range 30, Pitch Range 30, Yaw Range 45, and Picture Quality 100.
- **Multi Default.** Under Customize, applies Roll Range 180, Pitch Range 180, Yaw Range 180, and Picture Quality 100.
- **Face Enhance.** Improves capture of moving faces and adjusts brightness to suit the face nearest the camera (supported on some models).
- **Face Attribute.** Identifies attributes of detected faces — age, gender, mask, glasses, and expression. This must be enabled to use the Face Features alarm.
- **Detection Mode.** **Hybrid Mode** detects faces on all objects in view; **Motion Mode** filters out motionless faces such as portraits and statues.
- **Trigger Mode.** Sets the rule-line type. **Rectangle** detects faces only within the defined area; **Line** tracks faces only when they cross the detection line.

11.3 Pedestrian and Vehicle

Pedestrian and Vehicle detection recognizes people and vehicles in the field of view, raises an alarm, and records captured images according to the configured settings.

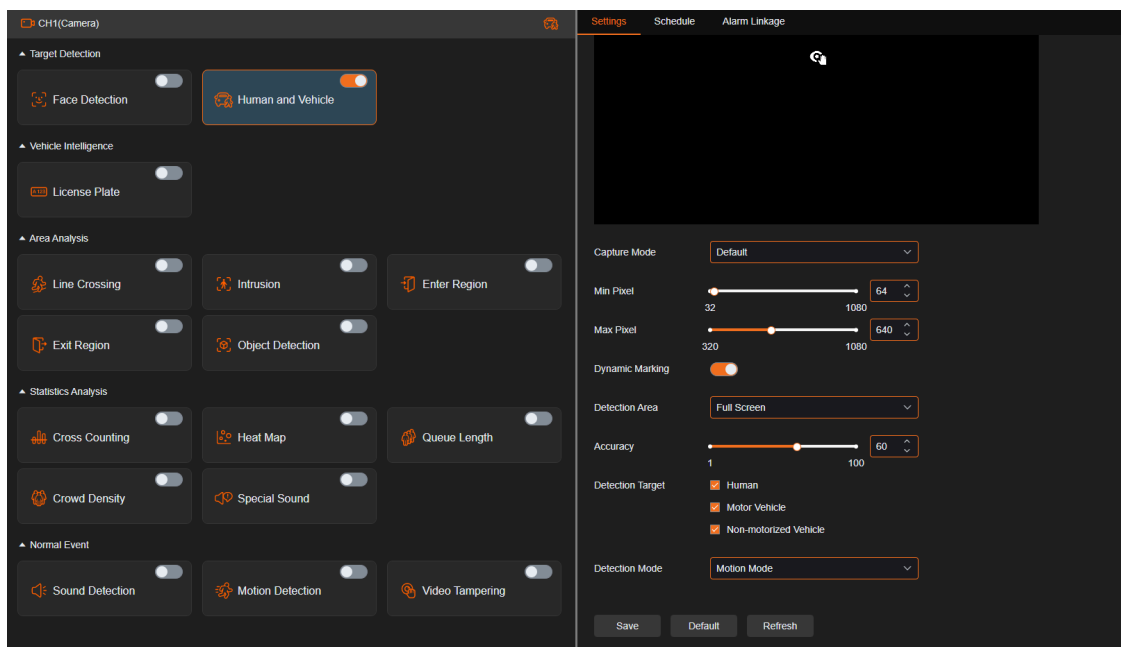


Figure 11-2. Pedestrian and Vehicle settings.

Pixel size, sensitivity, bounding box, detection area, and rule controls behave as described in Common Detection Settings. The settings specific to this type are:

- **Capture Mode.** **Default** pushes a single image per object from detection until it disappears; **RealTime Mode** pushes one image on detection and another when the object disappears; **Interval Mode** pushes images repeatedly at a set interval.
- **Snapshot Qty.** In Interval Mode, sets how many images are pushed for the same target — 1, 2, 3, or unlimited.
- **Capture Interval.** In Interval Mode, sets the time between pushes, measured from the target's appearance or the last push.
- **Detection Target.** Selects pedestrian, motor vehicle, non-motorized vehicle, or all.
- **Detection Mode.** **Hybrid Mode** detects all pedestrians and vehicles in view; **Motion Mode** filters out motionless ones.

11.4 License Plate

License Plate detection reads the plate of a passing vehicle and determines whether the vehicle is unknown or already recorded in the database, raising an alarm accordingly. Enable the function before configuring it.

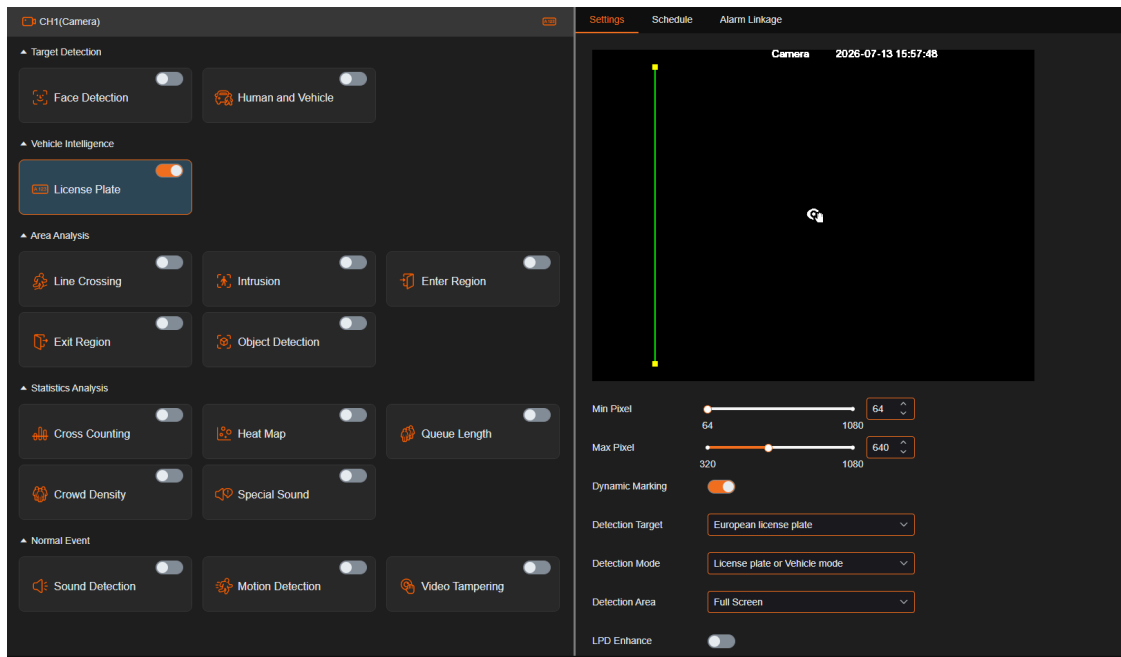


Figure 11-3. License Plate settings.

Pixel size, bounding box, detection area, and rule controls behave as described in Common Detection Settings. The settings specific to License Plate are:

- **Detection Target.** Selects the plate style to read — **European license plate** for European regions or **American license plate** for American regions.
- **Detection Mode.** **Vehicle priority mode** detects the vehicle first and then captures the plate for analysis; **License plate or Vehicle mode** analyzes the plate at the same time the vehicle is detected.
- **License Plate Enhancement.** Available only while License Plate detection is enabled. When on, the camera switches to IR-CUT image mode in Day/Night operation and hides the Exposure Compensation, Shutter, and Exposure Time settings.
- **Select Mode.** Chooses the application scenario. **Entrance/Exit** alarms when a vehicle passes through the area and crosses the detection line; **City Street** alarms when a vehicle or plate crosses the detection line; **Alarm Input** alarms when a vehicle or plate is within the area after an I/O input alarm is triggered (supported on some models).

NOTE With fault-tolerant matching, a plate is treated as a match to a database entry even when a limited number of characters differ, which allows for occasional misreads.

11.5 Line Crossing

Line Crossing detection raises an alarm when a pedestrian or vehicle crosses a defined virtual line in the configured direction.

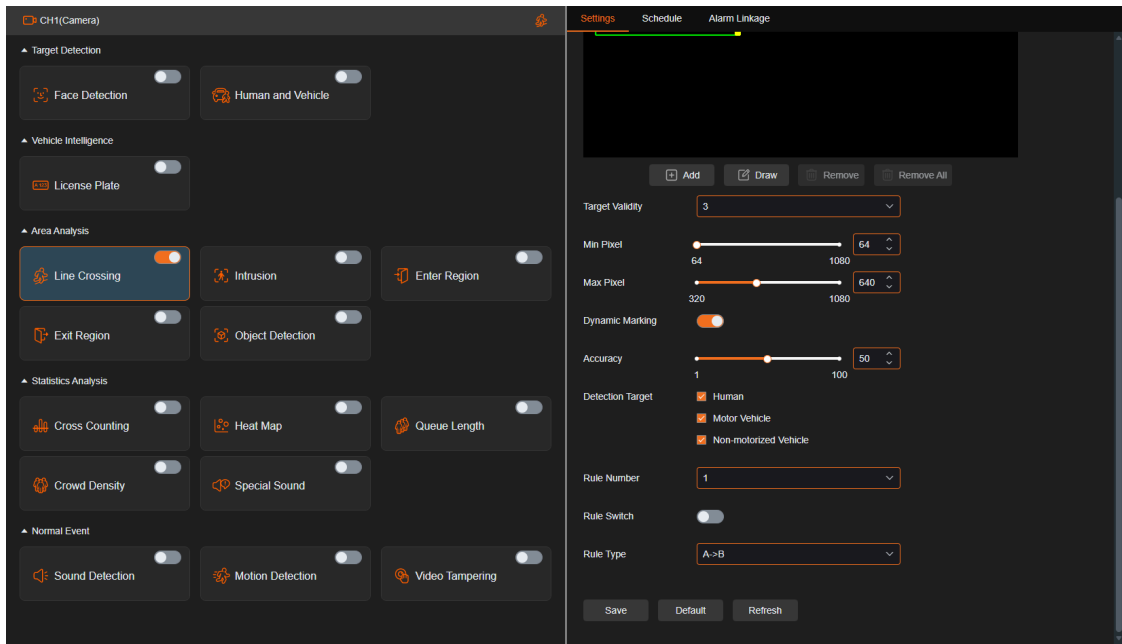


Figure 11-4. Line Crossing settings.

Pixel size, sensitivity, target validity, detection target, bounding box, and rule controls behave as described in Common Detection Settings. Up to four detection lines are supported, and **Rule Type** sets the crossing direction that triggers each line.

11.6 Intrusion

Intrusion detection determines whether an object enters a defined restricted area and raises a linked alarm based on the result.

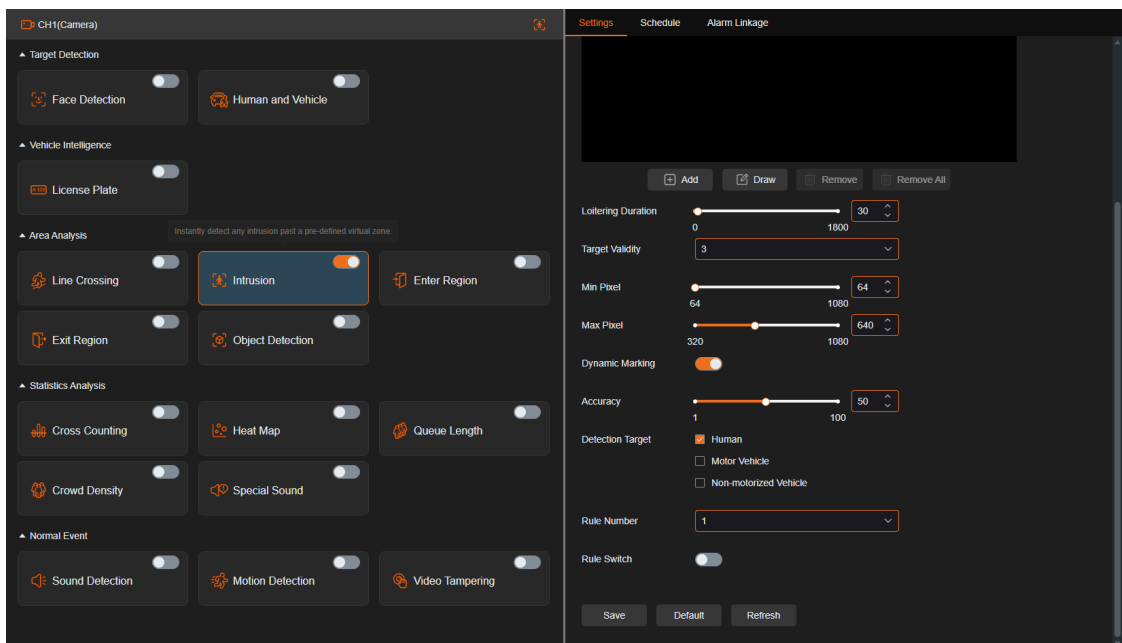


Figure 11-5. Intrusion settings.

Pixel size, sensitivity, target validity, detection target, bounding box, detection area, and rule controls behave as described in Common Detection Settings. The setting specific to Intrusion is:

- Loitering Duration.** The time a target must remain in the alert area before the alarm is raised. A value of 1 triggers the alarm one second after the target enters the area; the maximum is 1800 s.

11.7 Enter Region

Enter Region detection raises an alarm when a target crosses into the defined area from outside it. A target that first appears inside the area does not generate an alarm.

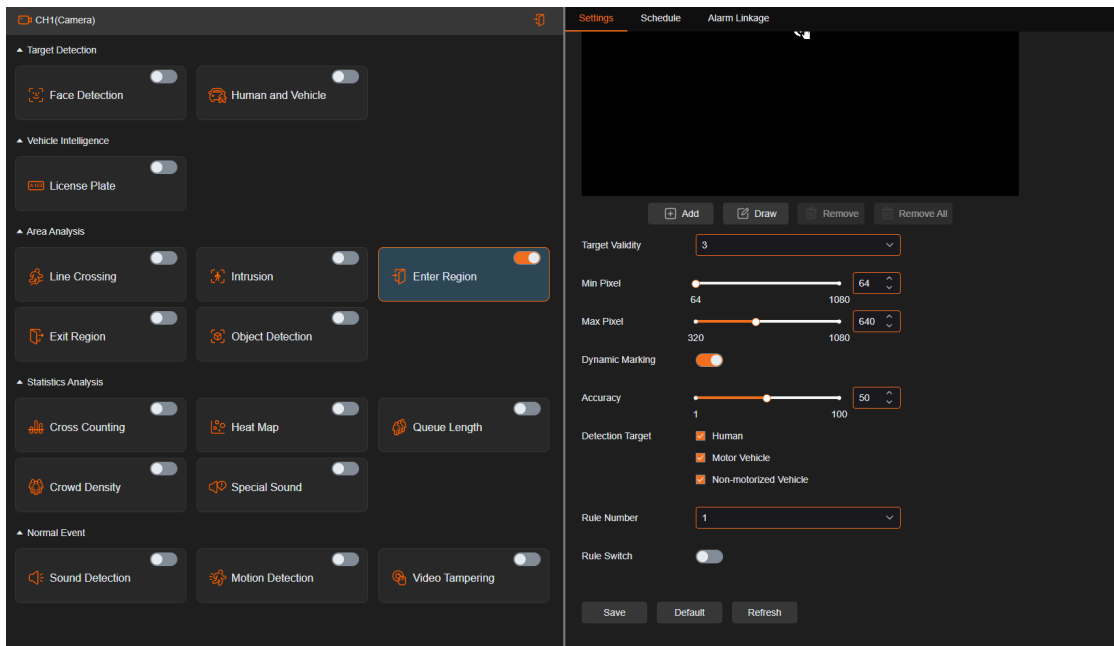


Figure 11-6. Enter Region settings.

Pixel size, sensitivity, target validity, detection target, bounding box, detection area, and rule controls behave as described in Common Detection Settings. Up to four detection rules are supported.

11.8 Exit Region

Exit Region detection raises an alarm when a target crosses out of the defined area. A target that first appears outside the area does not generate an alarm.

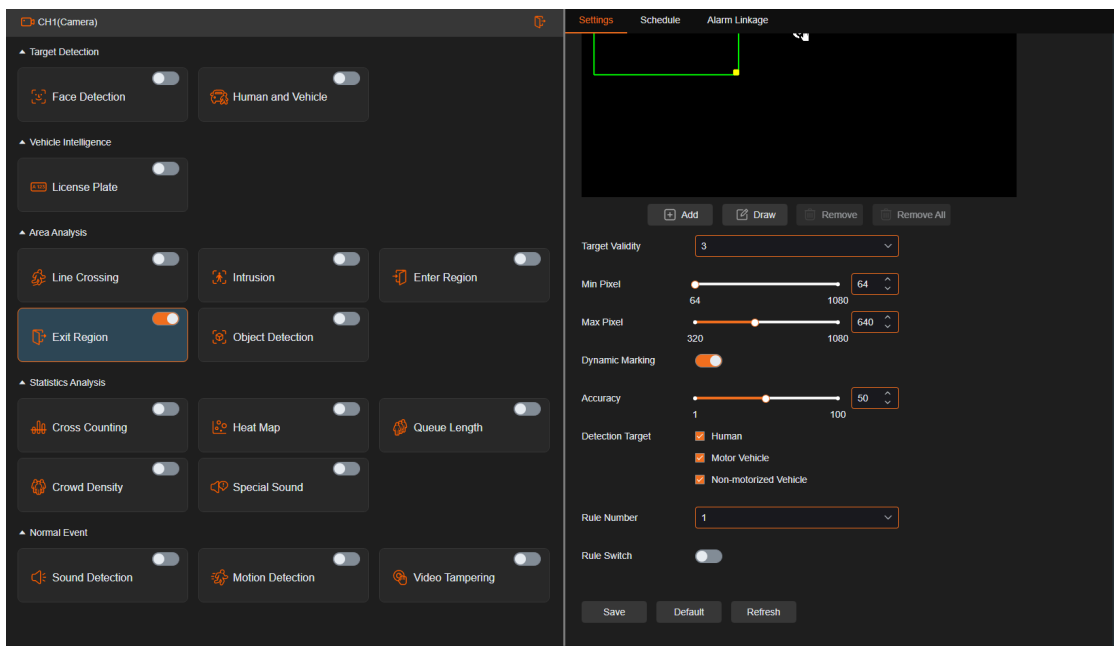


Figure 11-7. Exit Region settings.

Pixel size, sensitivity, target validity, detection target, bounding box, detection area, and rule controls behave as described in Common Detection Settings. Up to four detection rules are supported.

11.9 Object Detection

Object Detection raises an alarm when an object is left behind in the monitored scene or when a previously present object is removed.

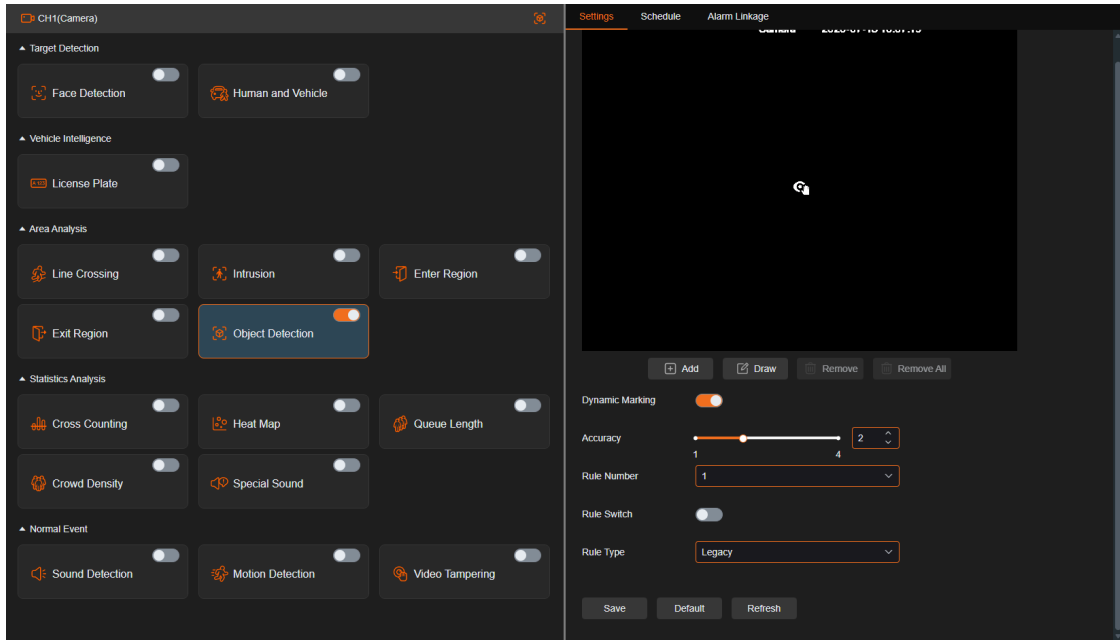


Figure 11-8. Object Detection settings.

Bounding box and rule controls behave as described in Common Detection Settings. The settings specific to Object Detection are:

- **Sensitivity.** Filters small interfering targets; higher sensitivity allows smaller objects to be detected.
- **Rule Type.** Sets what the rule reports for the selected area — **Legacy** for objects left behind, **Lost** for objects removed, or **Lost & Legacy** for both. The choice is tied to the active Rule Number.

11.10 Cross Counting

Cross Counting tallies specific objects that cross a line between two adjacent regions, A and B, and raises an alarm when the net count is high enough.

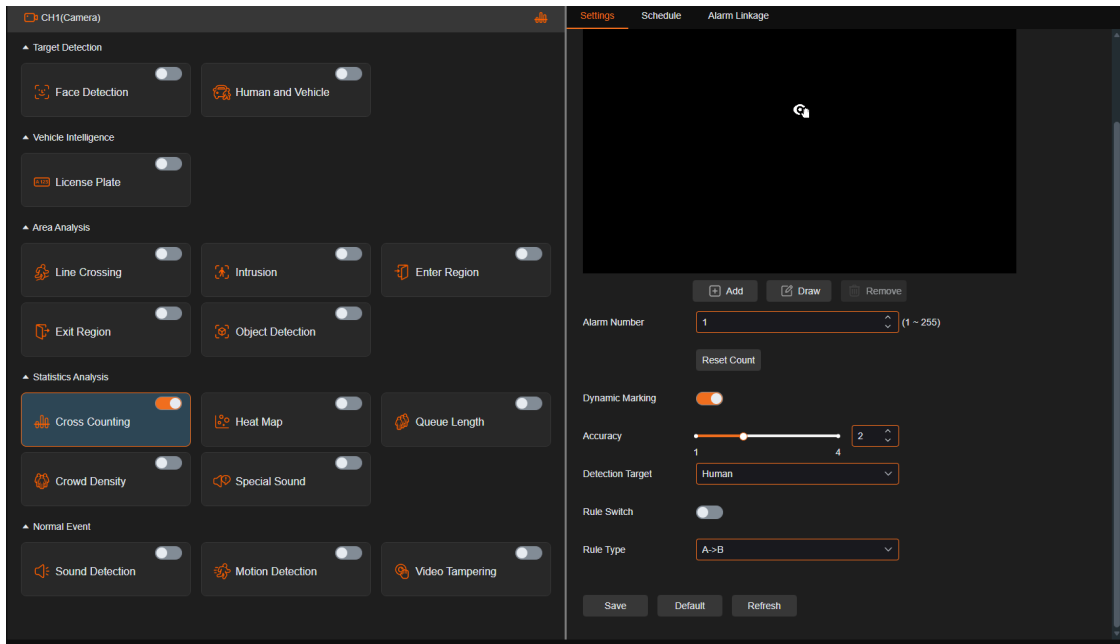


Figure 11-9. Cross Counting settings.

An object that enters from region A, crosses the detection line, and leaves through region B increases the **in** count by one; an object that enters from region B and leaves through region A increases the **out** count by one. Sensitivity and bounding box behave as described in Common Detection Settings. The settings specific to Cross Counting are:

- **Detection Target.** Selects what is counted — **Motion** (all objects, including people, vehicles, and boxes), **Pedestrian**, **Motor Vehicle**, or **Non-motorized Vehicle**. Changing this and saving clears the current count.
- **Alarm Number.** Sets the alarm threshold. The alarm fires when the count updates and the in count minus the out count is greater than or equal to this value.
- **Reset Count.** Clears the currently displayed count.
- **Rule Type.** Sets which crossing direction increases the in and out counts, as described above.
- **Count area.** Displays the running Cross Counting totals on the image. Adjust its position as described in the OSD and image overlay settings.

11.11 Heat Map

Heat Map records where people are active within all or part of the scene and saves the data every ten minutes. The resulting report presents the distribution of activity across time and space, making it easy to gauge how busy each area is. This function records data only and does not raise an alarm.

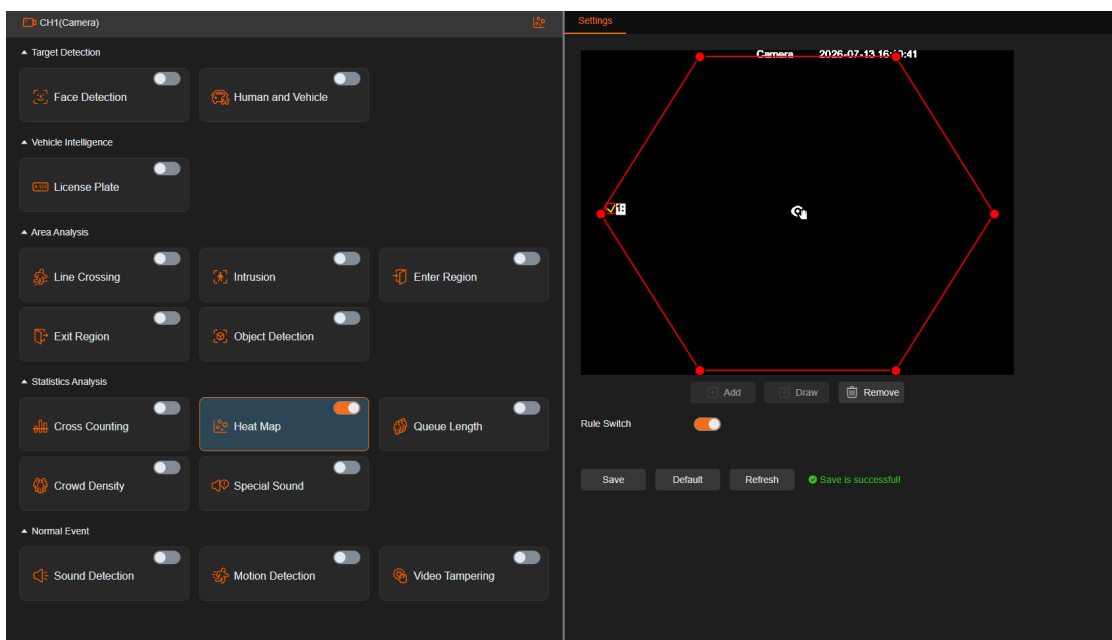


Figure 11-10. Heat Map settings.

Rule switch and the Add, Draw, and Remove controls behave as described in Common Detection Settings. The setting specific to Heat Map is:

- Monitoring Area Settings.** Defines the area for which activity is counted. By default the entire scene is selected.

11.12 Queue Length

Queue Length detection monitors the number of people waiting in a defined queue area and how long they wait, raising an alarm when the queue is too long or the wait too great.

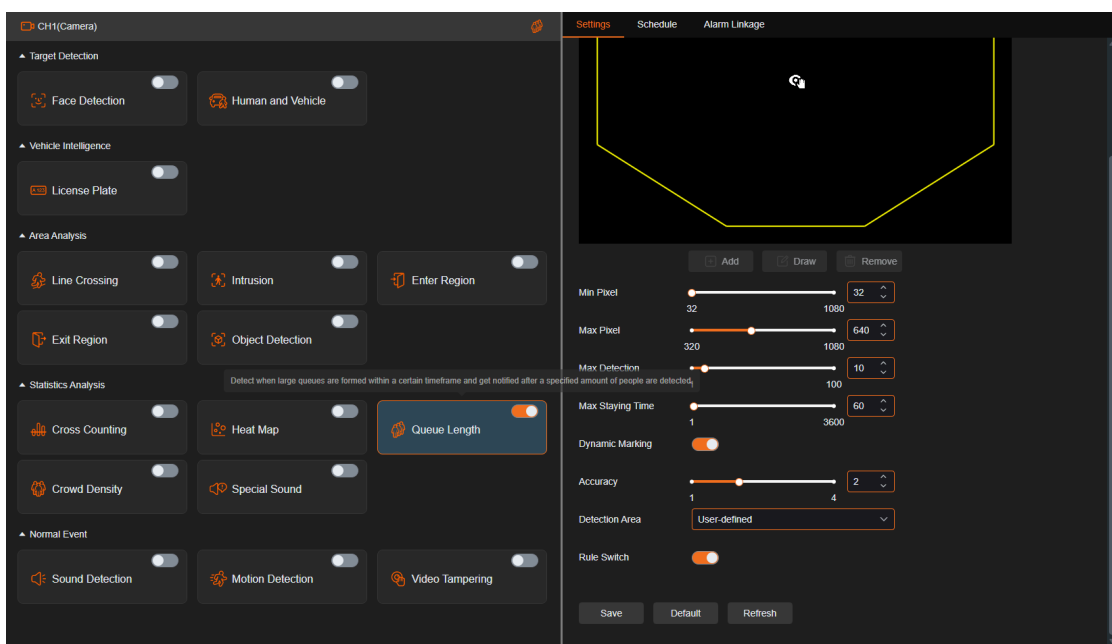


Figure 11-11. Queue Length settings.

Sensitivity, bounding box, detection area, and rule controls behave as described in Common Detection Settings. Pixel sizes here filter by head size relative to a 1080P image. The settings specific to Queue Length are:

- **Min / Max Pixels.** Based on a 1080P resolution, filter out heads smaller or larger than the set size. The frame is previewed and can be dragged on the right, and disappears five seconds after the pointer leaves it.
- **Max Detection.** The maximum number of heads allowed in the area; exceeding it raises an alarm.
- **Max Staying Time.** The maximum time people may remain in the area. Timing starts when the last person leaves; if no one has left by the set time, the wait is treated as a timeout and an alarm is raised. Counting restarts only when a detected target leaves the area — a target that simply disappears within the area is ignored, and counting occurs only while a target is present.
- **Count Display Area.** Shows the current number of people and the wait time for the person being served. Adjust its position as described in the OSD and image overlay settings.

11.13 Crowd Density

Crowd Density detection counts people by recognizing their heads and raises an alarm when the number in the monitored area exceeds a preset value.

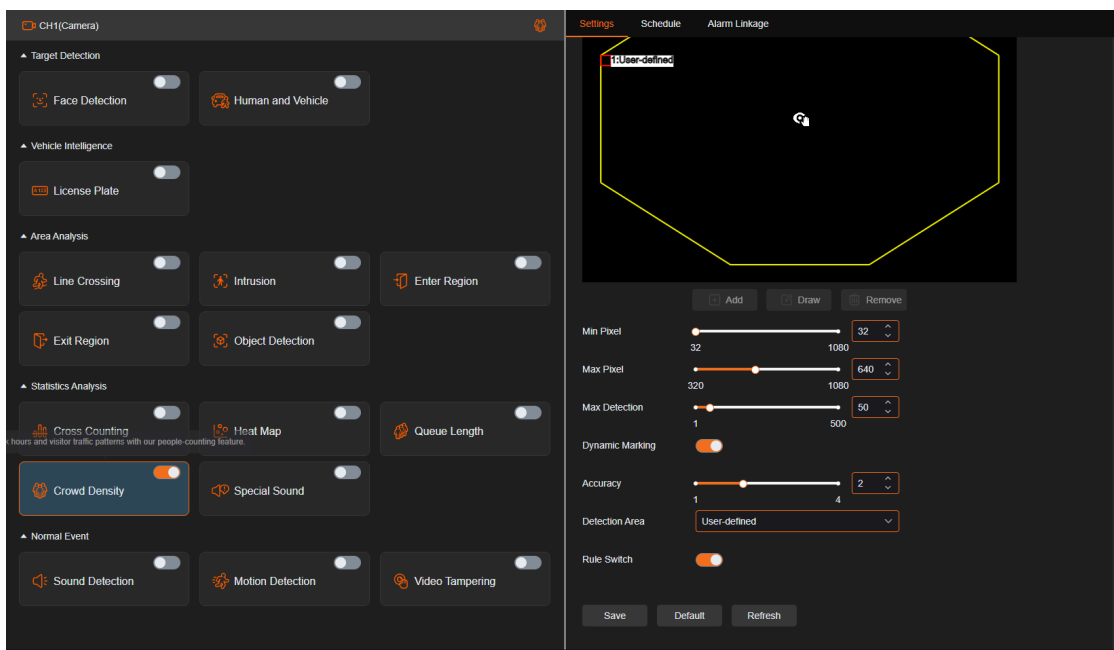


Figure 11-12. Crowd Density settings.

Sensitivity, bounding box, detection area, and rule controls behave as described in Common Detection Settings. As with Queue Length, pixel sizes filter by head size relative to a 1080P image. The settings specific to Crowd Density are:

- **Min / Max Pixels.** Based on a 1080P resolution, filter out heads smaller or larger than the set size, with the same preview behavior as other detection types.
- **Max Detection.** The maximum number of heads allowed in the area; exceeding it raises an alarm.
- **Count Display Area.** Shows the current number of people in the area. Adjust its position as described in the OSD and image overlay settings.

11.14 Special Sound

Special Sound detection listens for uncommon sounds chosen to suit the scene and raises an alarm when a selected sound is detected.

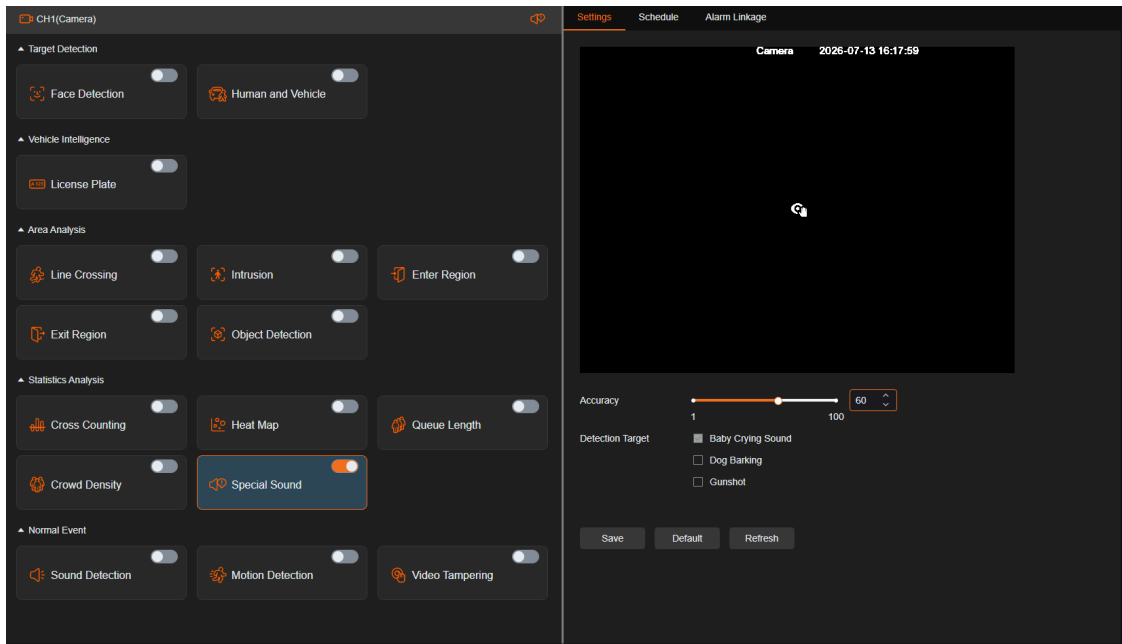


Figure 11-13. Special Sound settings.

The settings specific to Special Sound are:

- **Sensitivity.** Sets detection sensitivity, in the range 1 to 100.
- **Detection Target.** Selects the sound types to detect: baby crying, dog barking, and gunshot. Any combination can be enabled.

11.15 Motion Detection

Motion Detection raises an alarm when movement is detected within a defined zone of the image. On an alarm the camera can, for example, send an email with a snapshot to a specified address and push a notification through the mobile application.

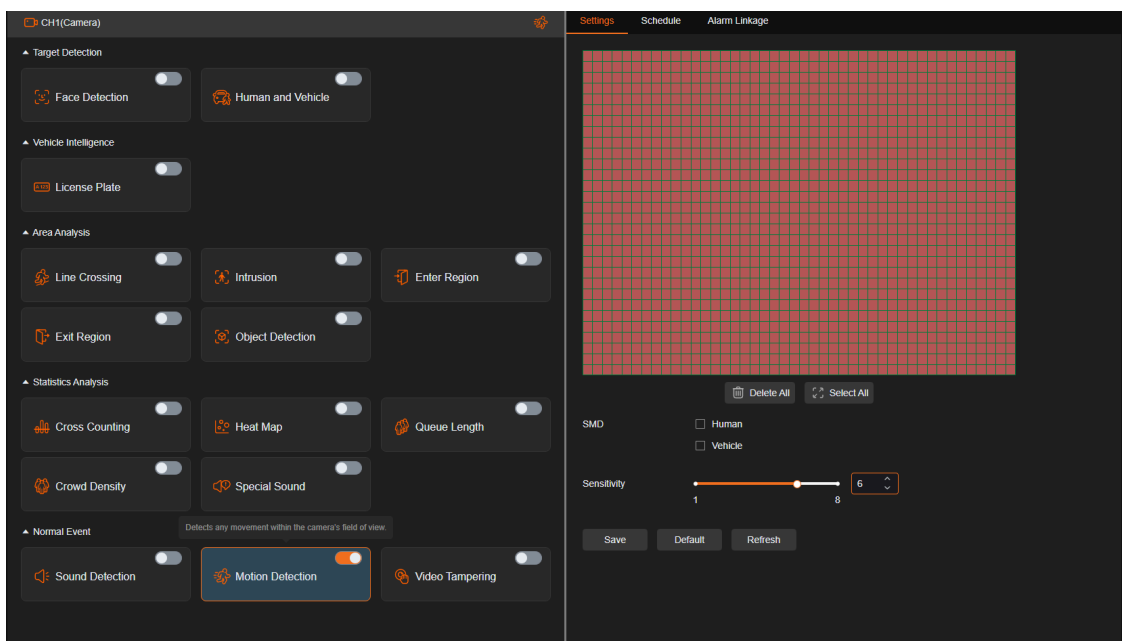


Figure 11-14. Motion Detection settings.

Drag with the left mouse button to outline the detection zone in the viewport on the right; only movement inside the zone triggers the alarm. The settings specific to Motion Detection are:

- **SMD.** Restricts motion detection to a target type — **Pedestrian** for human targets only or **Vehicle** for vehicle targets only.
- **Sensitivity.** Sets how readily motion triggers the alarm; higher values are more sensitive.

11.16 Video Tampering

Video Tampering detection raises an alarm when the live view is obscured, for example by covering or blocking the lens.

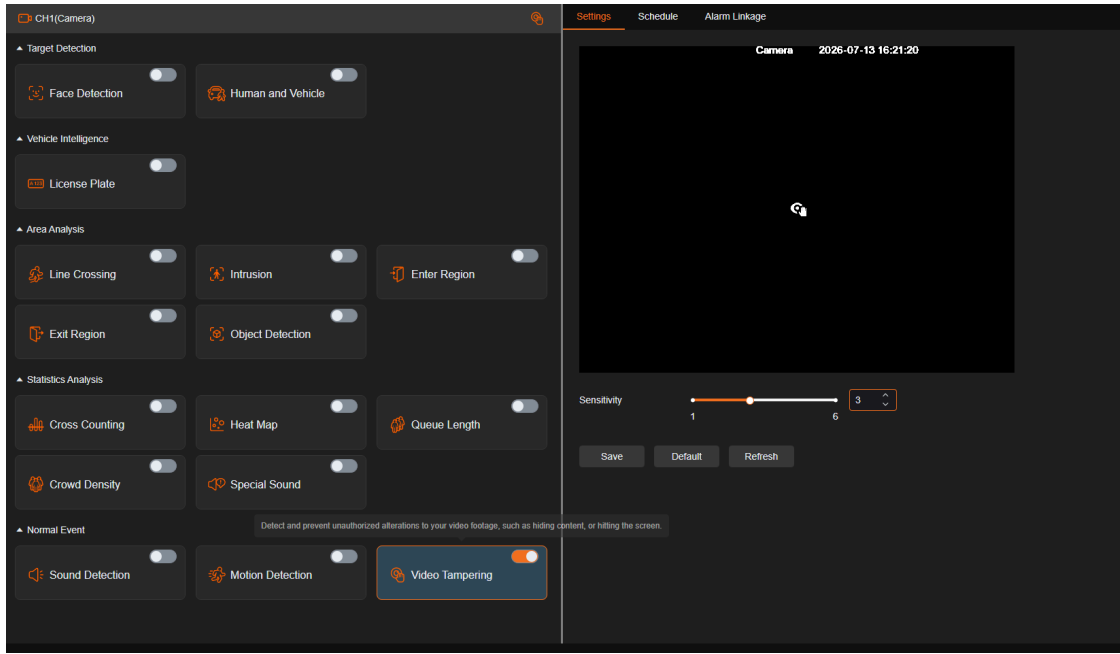


Figure 11-15. Video Tampering settings.

The setting specific to Video Tampering is:

- **Sensitivity.** Sets how readily lens occlusion triggers the alarm; higher values are more sensitive.

11.17 Event Schedule

Each event is active only during the periods defined in its schedule, so detection and its linked actions apply during the hours you choose.

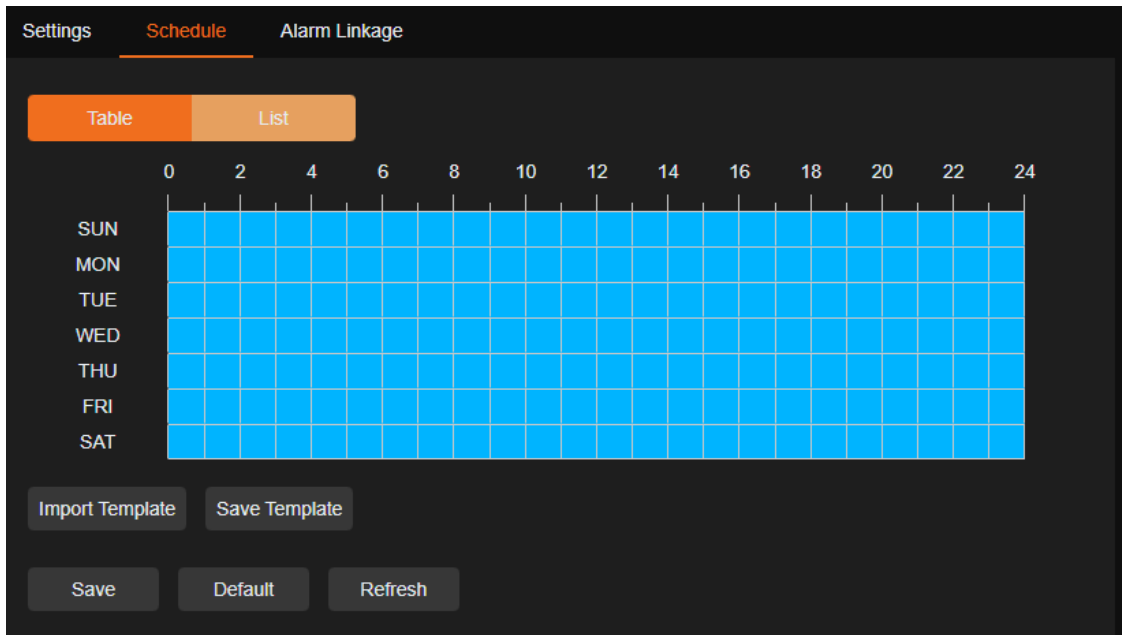


Figure 11-16. Event schedule.

To define when each event takes effect, see the Schedule Setup section.

11.18 Alarm Linkage Settings

Alarm linkage defines the actions the camera performs when any event raises an alarm. The same set of actions is available across the detection types described in this chapter.

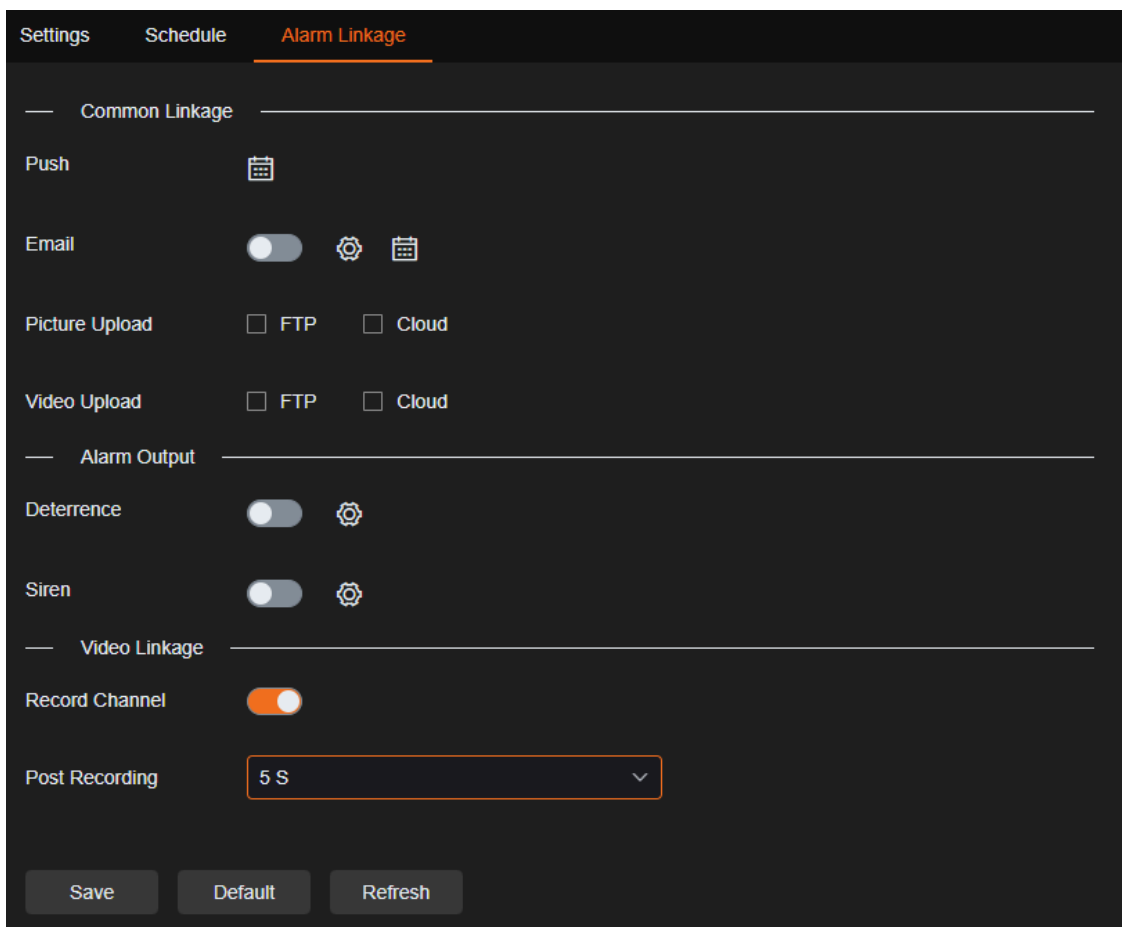


Figure 11-17. Alarm linkage settings.

- **Email.** Sends an email when an event alarm is triggered. Use the setup and schedule controls on the right to configure the message; see Mail Settings.
- **Picture Upload.** When FTP is selected, uploads a snapshot to the associated FTP server on an alarm. Associate the server first, as described in FTP Settings, then use the setup control to choose which channel's alarm image is uploaded.
- **Video Upload.** When FTP is selected, uploads a video clip to the associated FTP server on an alarm. As with picture upload, associate the server first in FTP Settings, then choose the channel to upload.
- **I/O Output.** Activates the camera's linked I/O alarm output on an alarm. Use the setup control to select the output source; configure the output duration and schedule in the alarm output settings.
- **Deterrence.** Triggers the light deterrent on an alarm, using the warm-light and red-and-blue-light parameters defined in Alarm Actions and Deterrence. Set them directly from the control on the right.
- **Siren.** Triggers the siren deterrent on an alarm, using the siren parameters defined in Alarm Actions and Deterrence. Set them directly from the control on the right.
- **Wiegand.** Transmits data to a control system or data center over the Wiegand interface when a license plate is recognized (supported on some models).
- **Recording Channel.** Records the alarm on the selected channel when an alarm is triggered. Use the setup control to choose the linked channel.
- **Recording Delay.** Sets how long the camera continues to record after the alarm ends.

Chapter 12 Alarm Actions and Deterrence

This chapter describes how the camera responds when an event is detected. It defines the physical alarm input and output terminals, the visual deterrents (white light and red/blue warning light), the audible siren, and the disarming controls that suppress selected responses. The actions configured here are the ones that other detection features reference by name when they link an event to an alarm.

12.1 I/O Settings

The I/O settings govern the camera's hardware alarm terminals: a sensor input that lets an external device trigger the camera, and a relay output that lets the camera drive an external device. These features are available only on models fitted with I/O terminals and require a compatible external device to be wired to them.

12.1.1 Alarm Input Settings

The alarm input accepts a signal from an external sensor — for example, a door contact or a passive infrared detector — and uses it to trigger the camera's alarm responses. This is an optional feature, available only when the camera provides I/O terminals and an external alarm device is connected to them.

Alarm Input

Alarm Output

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

Save

Refresh

Figure 12-1. Alarm input list.

Advance

Alarm Input No. Local<-1 Settings Input

Alarm Type Normally-Open Post Recording 5 S

☒ Schedule ☐ Linkage

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

Figure 12-2. Alarm input parameters.

Click **Edit** to open the setup page, then configure the following:

- **Alarm Input No.** Selects the input source used for the I/O alarm.
- **Settings.** Enables or disables the I/O input alarm function.
- **Alarm Type.** Selects the type of input signal that constitutes an alarm.
- **Post-recording.** Sets how long the camera continues recording after an alarm is triggered. The default is 5 seconds.
- **Schedule.** Defines the periods during which the alarm input is active. See the Schedule Setup section.

Advance

Alarm Input No. Local<-1 Settings Input

Alarm Type Normally-Open Post Recording 5 S

☐ Schedule ☒ Linkage

☐ Normal Linkage

- ☐ Email
- ☐ FTP Picture Up...
- ☐ FTP Video Up...
- ☐ Picture to Cloud
- ☐ Video to Cloud
- ☐ Event Push Platform
- ☒ Record Channel
- ☒ Warning Light
- ☒ Siren

☐ Alarm Output

- ☐ Local->1

PTZ Linkage

- ☐ Preset
 - 1
- Dwell Time
 - 5 (1 ~ 20) s
- ☐ Tour
 - 1
- ☐ Pattern Scan
 - 1

Figure 12-3. Alarm input linkage options.

Under **Linkage**, select the responses the camera performs when the input is triggered:

- **Email.** Sends a message to the configured address when the alarm is triggered. See Mail Settings.
- **FTP Picture Upload.** Uploads a snapshot to the FTP server when the alarm is triggered. See FTP Settings.
- **FTP Video Upload.** Uploads a video clip to the FTP server when the alarm is triggered. Click the adjacent **Settings** button to configure the upload. See FTP Settings.
- **Light.** When enabled, illuminates the white light as a deterrent when the alarm is triggered. See the Deterrence Settings section.
- **Warn Light.** When enabled, illuminates the red and blue warning light as a deterrent when the alarm is triggered. See the Deterrence Settings section.
- **Siren.** When enabled, sounds the siren as a deterrent when the alarm is triggered. See the Siren Settings section.
- **Alarm Output.** Selects the alarm output source to activate when the alarm is triggered. See the Alarm Output Settings section.

12.1.2 Alarm Output Settings

The alarm output is a relay terminal the camera activates in response to an alarm, allowing it to drive an external device such as a lamp or an audible annunciator.

Alarm Output No.	Latch Time	Edit
Local->1	NaN Hour	

Save Refresh

Figure 12-4. Alarm output list.

Advance

Alarm Output No. Local->1 Latch Time please choose

Alarm Status Close

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 Trigger

Figure 12-5. Alarm output parameters.

Click **Edit** to open the setup page, then configure the following:

- **Alarm Output No.** Selects the I/O output source used for alarm linkage.
- **Latch Time.** Sets how long the output remains active after the alarm is triggered.
- **Schedule.** Defines the periods during which the alarm output is active. See the Schedule Setup section.

12.2 Deterrence Settings

On cameras equipped with a white light and a red and blue warning light, the deterrence settings define how those lights behave when an alarm links to them. When a linked event is triggered, the camera illuminates the lights according to the parameters configured here.

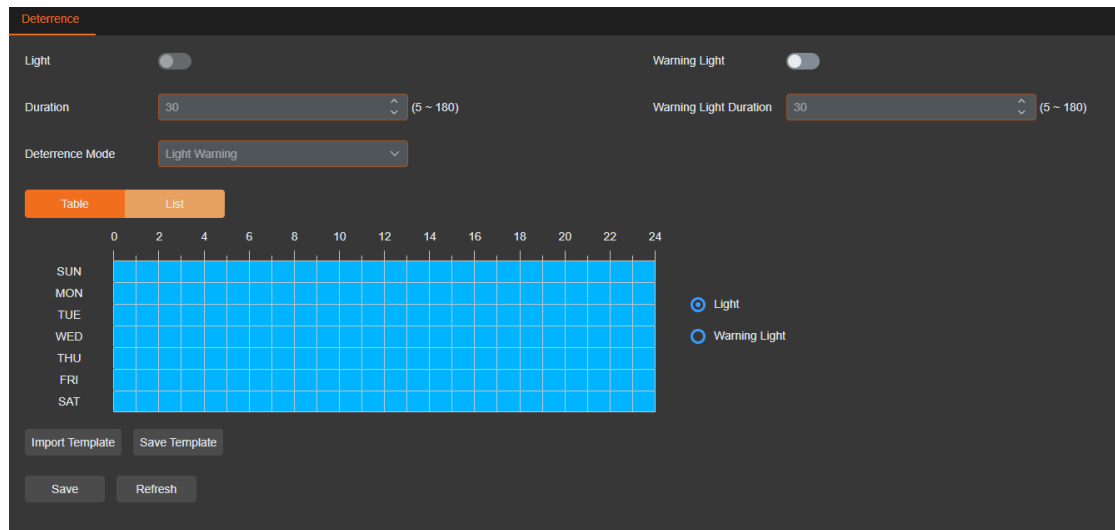


Figure 12-6. Deterrence settings.

NOTE The available parameters depend on the image control mode. In full-color mode the white light parameters are grayed out and cannot be set; in day/night mode all parameters can be set; in smart night light mode the warning light parameter is grayed out and cannot be set.

- **Light.** Turns the white light deterrent on or off.
- **Light Duration (s).** Sets how long the white light remains illuminated.
- **Light Mode.** Selects how the white light behaves during deterrence. Two modes are available.
- **Steady Mode.** The white light stays continuously on for the duration of the deterrence.
- **Flashing Mode.** The white light flashes at a set frequency for the duration of the deterrence.
- **Warning Light.** Turns the red and blue warning light on or off.
- **Warning Light Duration (s).** Sets how long the red and blue warning light remains illuminated.
- **Schedule.** Defines the periods during which the white light and the red and blue warning light are active. See the Schedule Setup section.

12.3 Siren Settings

On cameras equipped with a siren, these settings define the audible deterrent. When an alarm links to the siren, the camera sounds it automatically according to the parameters configured here.

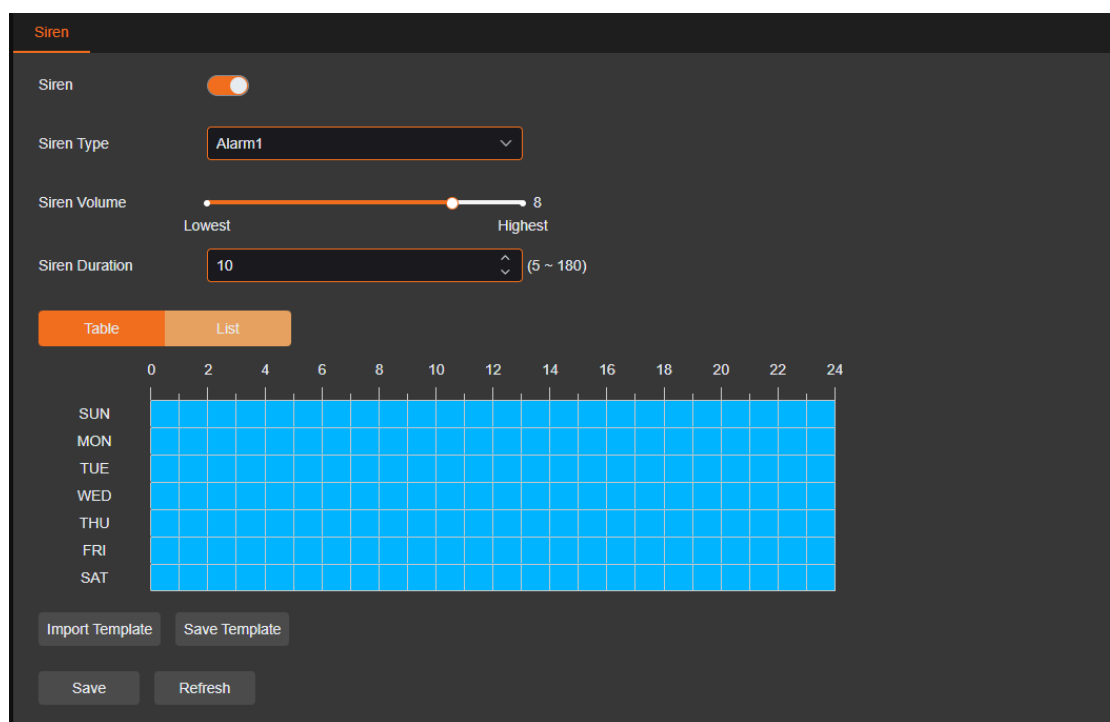


Figure 12-7. Siren settings.

- **Siren.** Enables or disables the siren.
- **Siren Type.** Selects the audio file the siren plays. Two built-in files are provided. On supported models you can also import up to three custom PCM or WAV files; each imported file must have a sampling rate no higher than 8000 Hz and a size no larger than 256 k. To remove a custom file, select it and click the **Delete** button beside it.
- **Siren Volume.** Sets the loudness of the siren, adjustable from 1 to 10.
- **Siren Duration (s).** Sets how long the siren sounds, adjustable from 5 to 180 seconds.
- **Schedule.** Defines the periods during which the siren is active. See the Schedule Setup section.

12.4 Disarming

Disarming suppresses the camera's response to alarm linkages. When it is active, the alarm actions you select below are withheld even though the underlying event is still detected. Use it to silence responses temporarily without disabling detection.

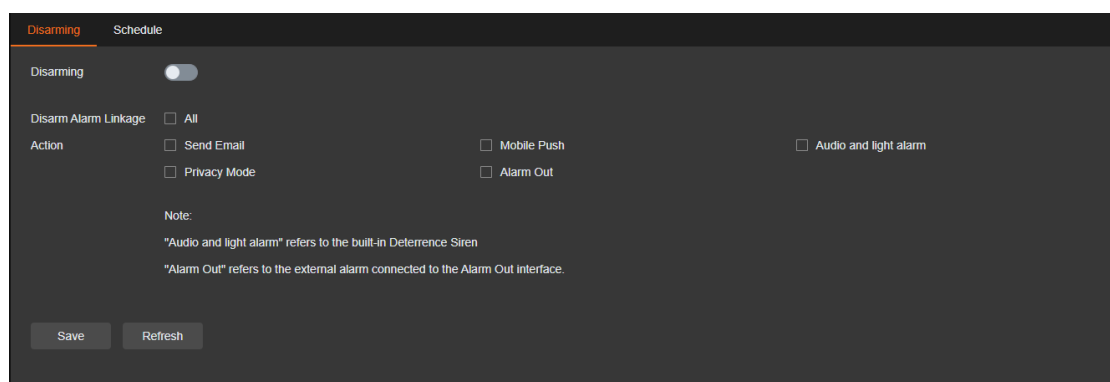


Figure 12-8. Disarming settings.

- **Disarming.** Enables or disables the disarming function.
- **Action.** Selects the local alarm linkage types to suppress.
- **All.** Selects or clears all action types at once.
- **Email.** When selected, a triggered alarm does not send an email notification. See Mail Settings.

- **Mobile Push.** When selected, a triggered alarm is not pushed to the RXCamView and OVConnect mobile applications.
- **Audio and light alarm.** When selected, a triggered alarm does not activate the red and blue warning light, the white light, or the siren.
- **Privacy Mode.** When selected, the camera enters privacy mode. On multi-channel devices, the channel can be specified.
- **Alarm Out.** When selected, a triggered alarm does not activate the external alarm output device.
- **Schedule.** Defines the periods during which disarming is active. See the Schedule Setup section.

CAUTION While disarming is active for a given action, the camera does not send that alert or drive that deterrent, even when an event occurs. Confirm that disarming is turned off before relying on the alarm responses again.

Chapter 13 Recognition Lists and Statistics

This chapter covers the reference databases that the camera's recognition features compare captured targets against, and the statistical reports it generates from the resulting data. List management defines the face and license-plate groups and their alarm policies; statistics turns the recorded detections into charts and exportable reports.

13.1 List Management

The camera compares each recognized target against reference data organized into groups. Each group carries an alarm policy — white list, black list, or stranger — that determines how a match is treated. Manage these groups here before enabling face or license-plate recognition.

NOTE Changes to a database take effect only after a short system reload.

13.1.1 Face Recognition

Face recognition identifies a detected person by comparing the captured face against the reference images stored in the database. Use the group management controls to build and maintain that database.

Group Name	Delete	Edit	Enable	Alarm	Policy	Similarity	Alarm	Alarm Schedule
Allow List					Allow	≥ 70 %		
Block List					Deny	≥ 70 %		
Stranger					Stranger	< 70 %		

Figure 13-1. Face recognition group list.

- **Alarm Policy Display.** Indicates each group's policy as a visual prompt only: green marks a white list, red marks a black list, and no color marks the stranger group.
- **Group Name.** Edits the name of the current group. This name is included in the notification when an alarm is pushed.
- **Delete.** Removes a group. The first three groups cannot be deleted.
- **Edit.** Opens the reference-image settings for the group, described below.
- **Enable.** Uses the group's data for face-recognition comparison.
- **Alarm.** Master switch that enables the group's alarm response.
- **Police.** Sets the alarm policy. The first three groups cannot be changed; other groups can be set to Allow or Deny.
- **Similarity.** Sets the matching threshold. An alarm is generated when the match similarity exceeds this value.

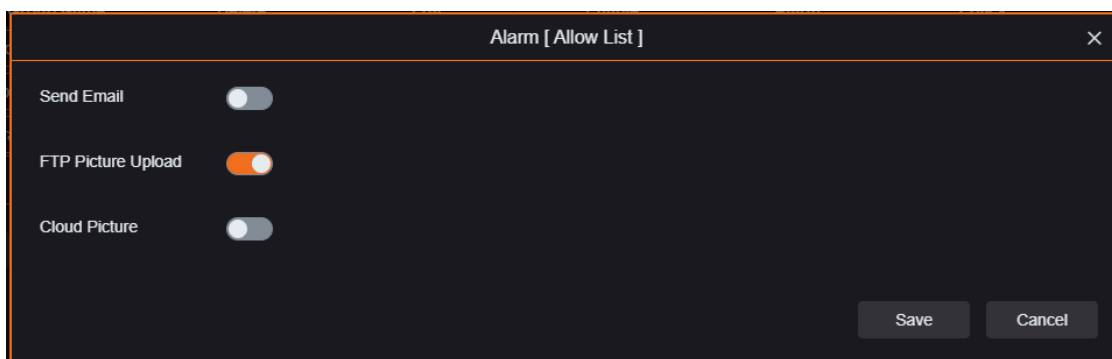


Figure 13-2. Face group alarm linkage settings.

Under **Alarm Linkage**, configure the responses for a successful group match:

- **Latch Time.** Sets how long the I/O alarm output continues after the camera captures and matches an image. The camera must support the I/O output function, and the active period is governed by the corresponding schedule.
- **Alarm Out.** Enables the alarm output.
- **Email.** Sends an email when a group match succeeds. See Mail Settings.
- **FTP Picture Upload.** Uploads the matched image to the associated FTP server. The active period is governed by the schedule, and the FTP server must be configured first. See FTP Settings.

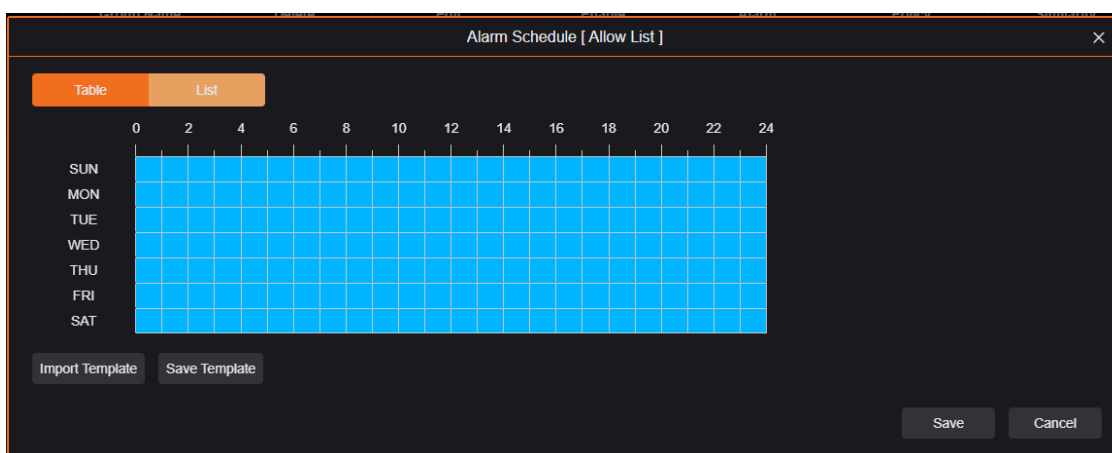


Figure 13-3. Alarm schedule for a face group.

- **Alarm schedule.** Sets the effective time for the alarm output, email, and FTP picture upload of the group alarm. See the Schedule Setup section.

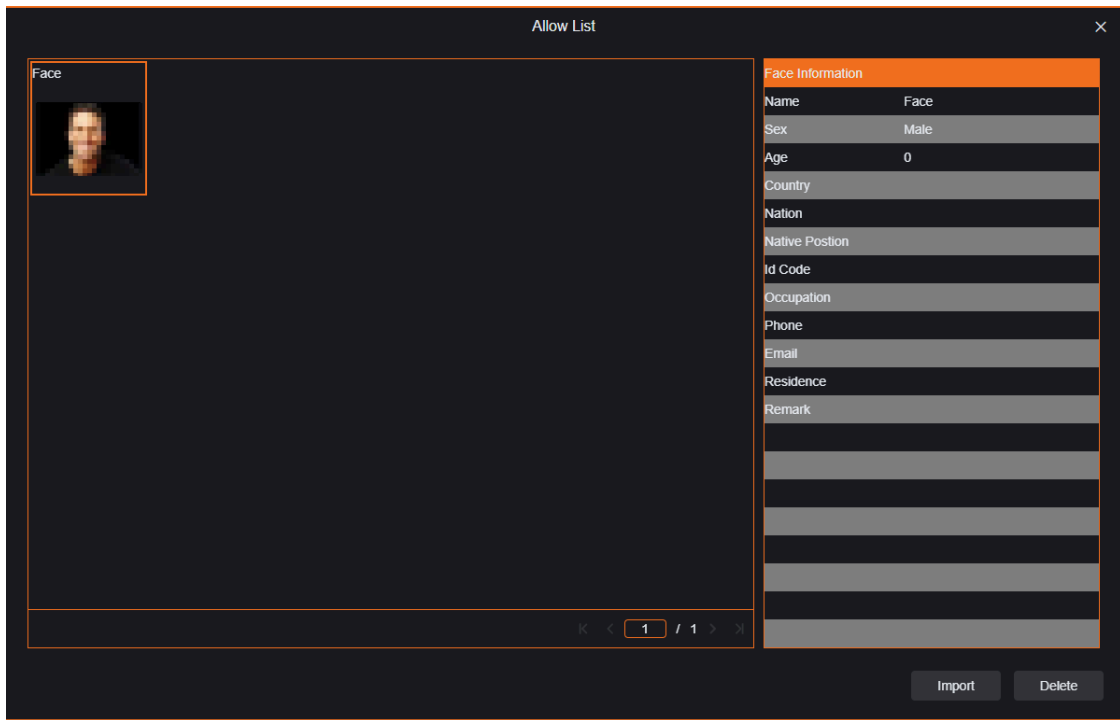


Figure 13-4. Reference-image editing for a face group.

Click **Add Group** to create a new database group; up to 16 groups are supported. Click the **Edit** icon to set the reference data for a group. The editing interface provides the following:

- **Added Picture Display Area.** Shows the face images already added to the group.
- **Info.** Displays the details of the currently selected image.
- **Detail Information.** Right-click an image to view its full details.
- **Move To.** Right-click an image to move it to another group.
- **Edit.** Right-click an image to reopen its editing interface and revise its information.
- **Delete.** Right-click an image to delete it.
- **Import.** Adds new face data to the group from local images or from images already captured by the camera.
- **Delete (batch).** Removes face data in bulk. Activate the control, select the images to remove, then click **Delete** again.

13.1.2 License Plate Recognition

License-plate recognition identifies a detected vehicle by comparing the captured plate against the reference data stored in the database. Use the group management controls to build and maintain that database.

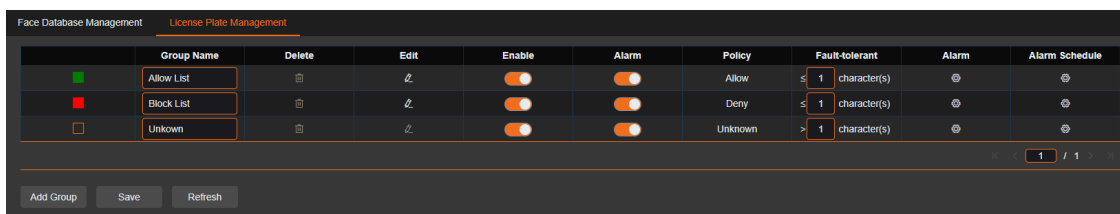


Figure 13-5. License-plate recognition group list.

- **Alarm strategy display.** Indicates each group's policy as a prompt only: green marks a white list, red marks a black list, and no color marks the stranger plate list.
- **Group Name.** Edits the name of the current group. This name is included in the notification when an alarm is pushed.
- **Delete.** Removes a group. The first three groups cannot be deleted.
- **Edit.** Opens the reference-image settings for the group, described below.
- **Enable.** Uses the group's data for license-plate comparison.

- **Alarm.** Master switch that enables the group's alarm response.
- **Police.** Sets the alarm policy. The first three groups cannot be changed; other groups can be set to Allow or Deny.
- **Fault-tolerant.** Sets the number of characters that may differ between a searched plate and the stored plate. A lower value produces closer matches.

TIP To search for a plate when only a few characters are known, set the fault tolerance to its maximum. Many unrelated plates are returned, but results are ranked by similarity, so the closest matches appear first.

Figure 13-6. License-plate group alarm linkage settings.

Under **Alarm Linkage**, configure the responses for a successful group match:

- **Latch Time.** Sets how long the I/O alarm output continues after the camera captures and matches a plate. The camera must support the I/O output function, and the active period is governed by the corresponding schedule.
- **Alarm Out.** Enables the alarm output.
- **Email.** Sends an email when a group match succeeds. See Mail Settings.
- **FTP Picture Upload.** Uploads the matched image to the associated FTP server. The active period is governed by the schedule, and the FTP server must be configured first. See FTP Settings.

Figure 13-7. Alarm schedule for a license-plate group.

- **Alarm schedule.** Sets the effective time for the alarm output, email, and FTP picture upload of the group alarm. See the Schedule Setup section.

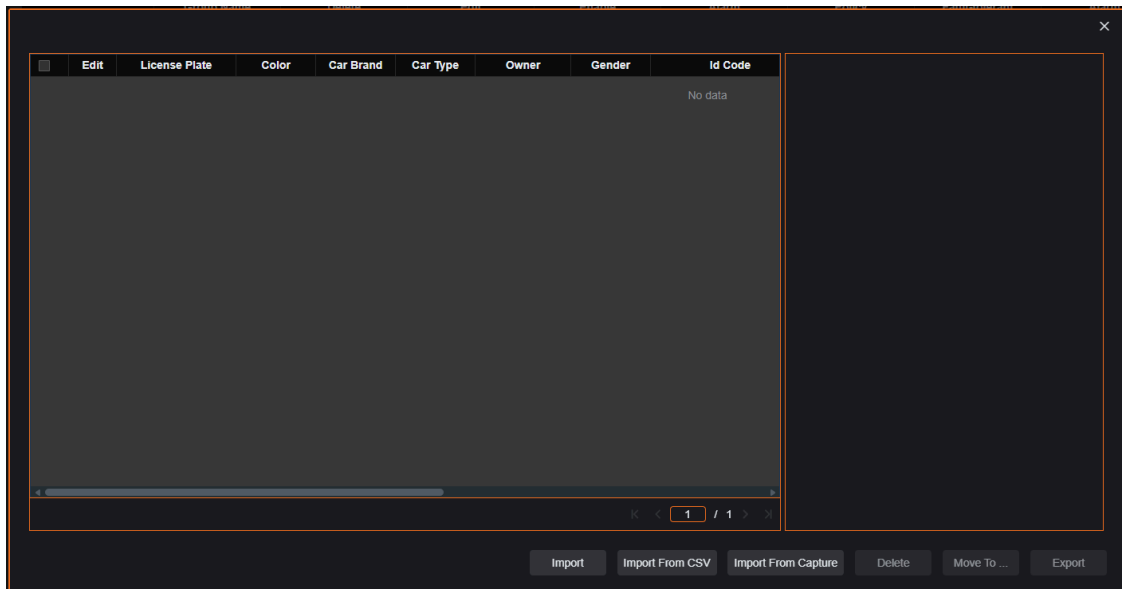


Figure 13-8. Reference-data editing for a license-plate group.

Click the **Edit** icon to set the reference data for a group. License-plate information can be added in three ways: **Import**, **Import From CSV**, and **Import From Local Capture**. When a group reaches 5000 entries, a message reports that the group has reached its upper limit.

1. Click **Import** to add a single license plate manually.
2. Click **Import From CSV** to import one or more entries from a CSV file, formatted as shown 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											

Figure 13-9. CSV import format for license-plate data.

Select the CSV file to import and click the import button to add its entries to the group. Use the **Delete** button to remove unwanted entries.

1. Click **Import From Capture** to import plates recorded locally. Select the date, duration, and alarm group, then click **Search** to list every plate saved by all devices during that period.

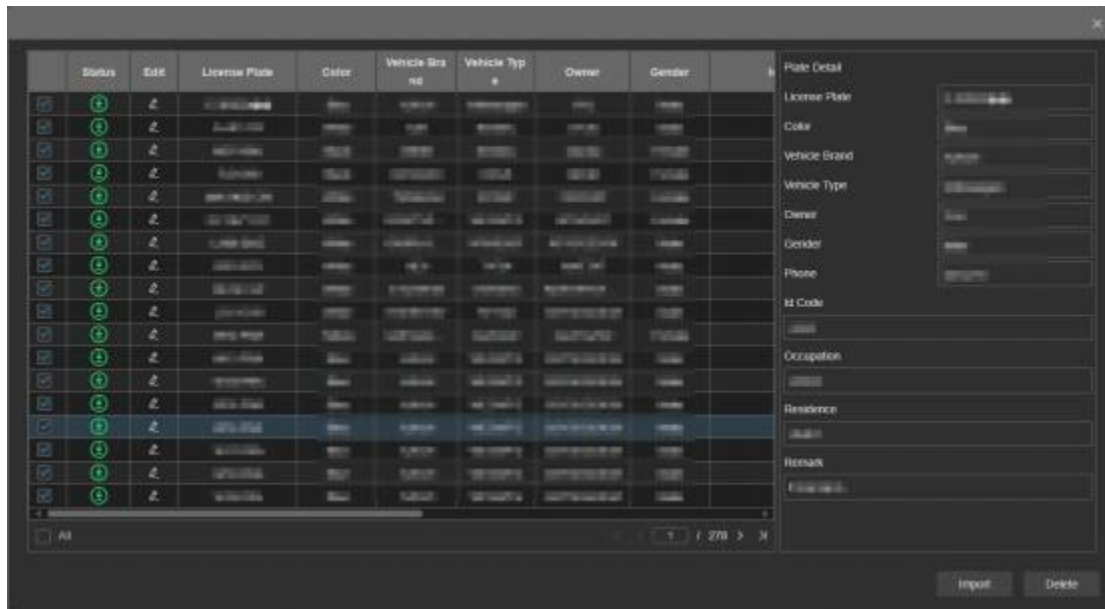


Figure 13-10. Importing plates from local capture.

- **All.** Selects all listed license-plate entries.
- 📌 Click an entry to edit its information, then click **Save**. The status icon changes once the entry is saved.
- 1. Select entries and click **Delete** to remove the chosen license-plate information.
- 2. Select entries and click **Move to** to move the chosen plates to another group.
- 3. Click **Export** to save the information for the entire group.

Click **Enable** to use the group's data for comparison. Click **Add Group** to create a new database group; up to 16 groups are supported.

13.2 Statistics

The statistics feature analyzes the data produced by the camera's intelligent detection and presents it as charts and reports. Each report is searched over a selected time range and can be exported to an Excel file.

13.2.1 Face Recognition

This report searches and counts the face data stored on the memory card according to the search settings.

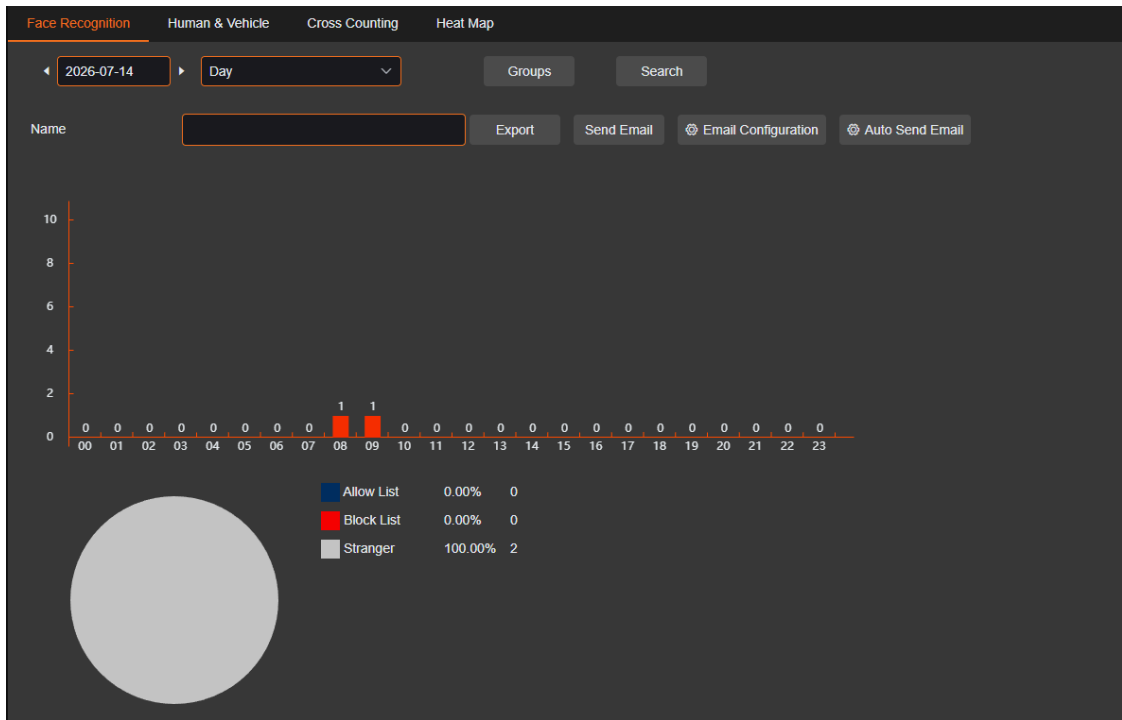


Figure 13-11. Face recognition statistics.

- **Time.** The reference time for the search.
- **Search Mode.** Selects the time range: Day, Week, Month, Quarter, or Year.
- **Group.** The group to include in the search.
- **Search.** Runs the search using the current settings.
- **Export.** Exports the current results to an Excel file. Provide a file name before exporting.
- **Display Area.** Presents the results as bar and pie charts.

13.2.2 Pedestrian and Vehicle

This report counts pedestrian and vehicle detections, including line-crossing, intrusion, region-entrance, and region-exiting events.



Figure 13-12. Pedestrian and vehicle statistics.

- **Time.** The reference time for the search.
- **Search Mode.** Selects the time range: Day, Week, Month, Quarter, or Year.
- **Intelligent.** Filters by capture type. A total of 18 types are available, spanning pedestrian, motor vehicle, and non-motorized vehicle across the line-crossing, intrusion, region-entrance, and region-exiting events.

- **Search.** Runs the search using the current settings.
- **Export.** Exports the current results to an Excel file. Provide a file name before exporting.
- **Display area.** Presents the results as a graph.

13.2.3 Cross Counting

Cross Counting searches and tallies the targets that cross a defined line.

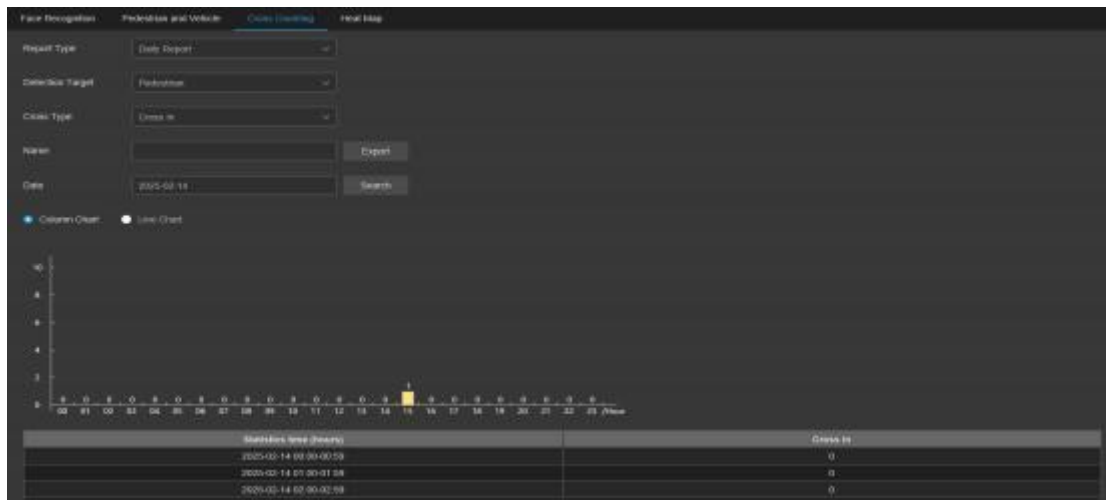


Figure 13-13. Cross counting statistics.

- **Report Type.** Selects the time range: Daily report, Weekly report, Monthly report, or Annual report.
- **Detection Target.** Selects the detection model whose data is counted — Motion, Person, or Vehicle. Data can be searched only by the model that triggered it; for example, motion-triggered data cannot be searched under another type.
- **Cross Type.** Filters the crossing direction: Cross In or Cross Out.
- **Export.** Exports the current results to an Excel file. Provide a file name before exporting.
- **System time.** The reference time for the selected report type.
- **Mode.** Selects whether the display area shows a bar chart or a line chart.
- **Display Area.** Presents the results as charts.
- **Search.** Runs the search using the current settings.

13.2.4 Heat Map

The heat map report visualizes how people are distributed across the scene, either by space or by time. In the space heat map, red marks the busiest areas and blue the least active. In the time heat map, the vertical value is an activity index derived from the number of people and their dwell time; a higher value indicates greater activity and does not represent an exact head count. The camera must have a usable memory card, on which the heat map data is stored.

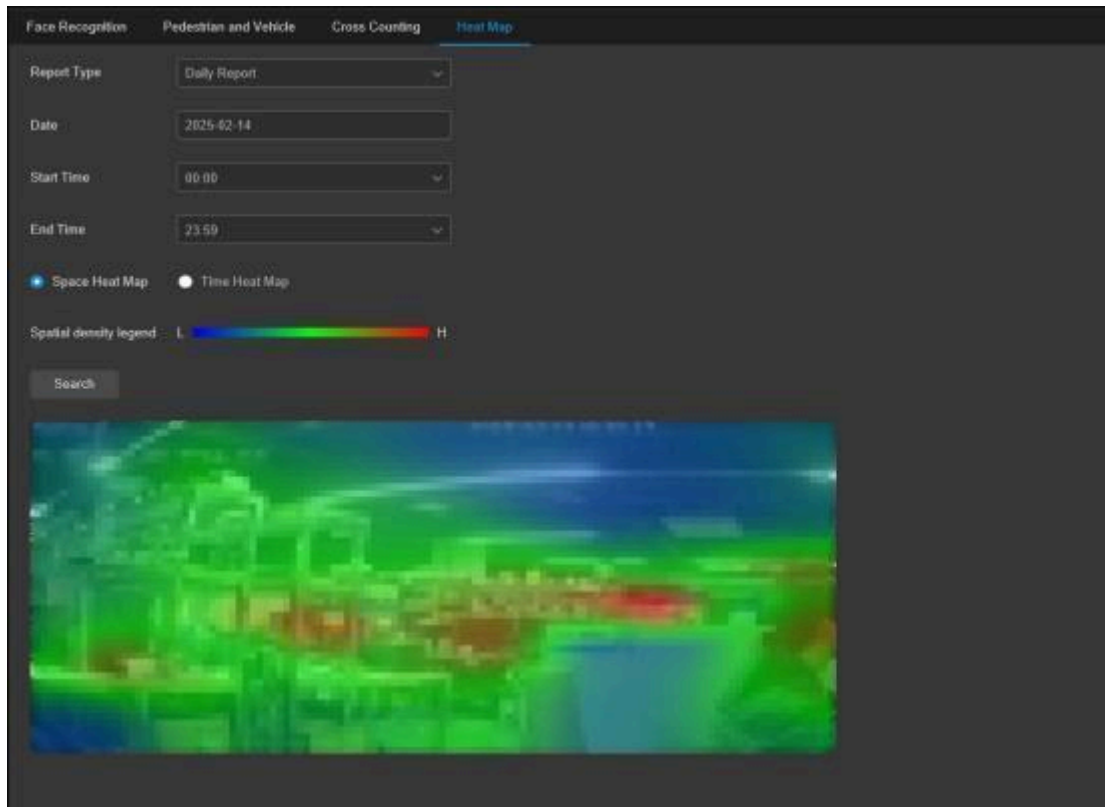


Figure 13-14. Heat map report.

- **Report Type.** Selects the time range: Daily report, Weekly report, Monthly report, or Annual report.
- **Date.** The date the search refers to.
- **Start Time.** Shown only for a daily report; sets the hour at which the search begins.
- **End Time.** Shown only for a daily report; sets the hour at which the search ends.
- **Mode.** Selects how the results are shown: as a graph or as a table.
- **Display Area.** Presents the frequency of activity in the monitored area as a graph, and, for different time periods, as a table.
- **Search.** Runs the search using the current settings.

Chapter 14 Network and Services

This chapter covers the camera's network configuration and its connected services: file transfer, core network addressing and ports, cloud access, email notifications, streaming, dynamic addressing, encrypted connections, address filtering, and third-party platform integration. Configure these settings so the camera can be reached on your network and can deliver images, video, and event data to the destinations you choose.

14.1 FTP Settings

The camera can upload event snapshots and recordings to an FTP server, providing off-camera storage of alarm evidence. Enable this feature and supply your server details to have the camera transfer images and video automatically when an event occurs.

Figure 14-1. FTP server settings.

- **FTP Enable.** Turns the FTP upload function on.
- **FTP Protocol.** Selects the transfer protocol. Two options are available: FTP and SFTP.
- **Server.** The IP address or domain name of your FTP server.
- **Port.** The port used to reach the FTP server.
- **Username / Password.** The credentials for your FTP server account.
- **Transfer Images.** When selected, alarm images are uploaded to the FTP server.
- **Transfer Videos.** When selected, alarm video is uploaded to the FTP server.

14.2 Network Settings

The network settings define how the camera obtains its address and communicates on the network. Most installations use DHCP, in which the router assigns all parameters automatically; configure a static address only when your network requires one. Where the camera authenticates with a user name and password to reach the network, use PPPoE.

14.2.1 General Settings

These settings control the camera's basic addressing. When the camera is connected to a router that provides DHCP, select the DHCP option and the router assigns all network parameters automatically. Set the following parameters manually only when the network requires a static configuration.

Figure 14-2. General network settings.

- **IP Address.** The camera's identifier on the network. It consists of four numbers between 0 and 255 separated by periods, for example 192.168.1.100.
- **Subnet Mask.** A network parameter that defines the range of addresses available on the network. It also consists of four numbers separated by periods, for example 255.255.0.0.
- **Gateway.** The address through which the camera reaches the wider network. It uses the same format as an IP address, for example 192.168.1.1.
- **IPv6 Address.** The camera's IPv6 identifier on the network. It consists of eight groups of hexadecimal values between 0 and FFFF, separated by colons.
- **DNS1 / DNS2.** DNS1 is the primary DNS server and DNS2 is the standby server. In most cases only the DNS1 address needs to be entered.
- **Main Stream (multicast).** When enabled, the main stream is made available for multicast.
- **Multicast Address.** The multicast address to use. A third-party player can request the camera to send a multicast media stream over RTSP.

 Video encryption transmission control — enables encryption of the audio and video streams.

Figure 14-3. Duplicate IP address warning.

Video Encryption Transmission. Enables encrypted transmission of the audio and video streams. On models that support it, the camera also warns you when a duplicate IP address is detected in the same network segment, displaying a message when the settings are applied.

14.2.2 PPPoE

The camera supports network connectivity through PPPoE dial-up. Use this method when your connection requires authentication with a user name and password.

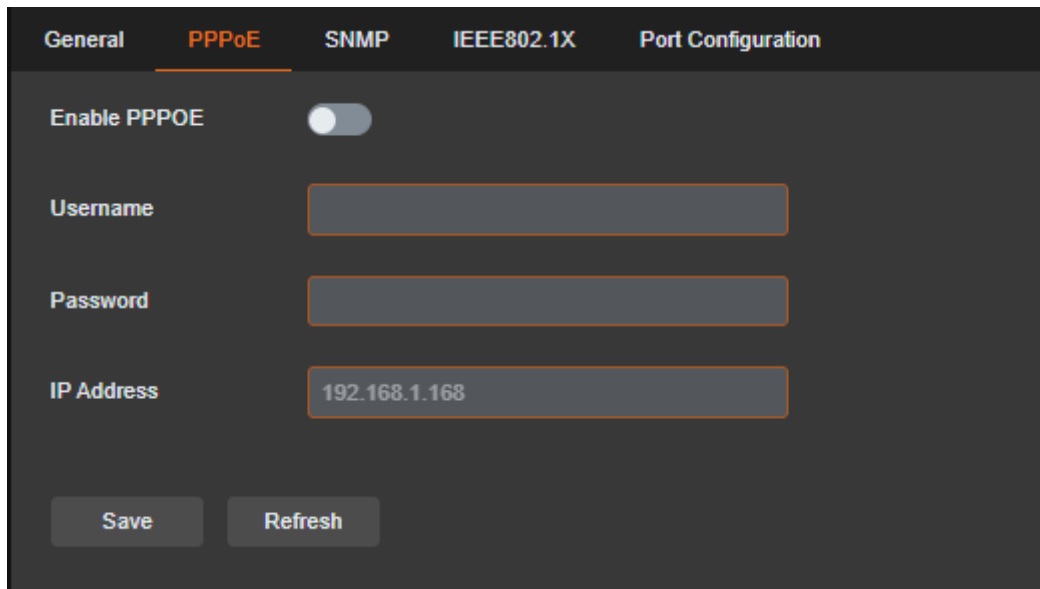


Figure 14-4. PPPoE settings.

1. Select **Enable PPPoE**.
2. Enter the PPPoE user name and password.
3. Click **Save**. The camera restarts to apply the PPPoE settings.

14.2.3 SNMP

Simple Network Management Protocol (SNMP) is an application-layer protocol for managing network nodes such as servers, workstations, routers, switches, and hubs across an IP network. Enable it to integrate the camera with an SNMP management system.

The screenshot shows the SNMP configuration interface. The 'SNMP' tab is active. The 'Enable' toggle is currently off. The 'SNMP Version' is set to 'V2'. The 'SNMP Port' is set to '161'. The 'Read Community' is set to 'public'. The 'Write Community' is set to 'private'. The 'Trap IP Address' is set to '127.0.0.1'. The 'Trap Port' is set to '162'. The 'Save' and 'Refresh' buttons are at the bottom.

Figure 14-5. SNMP settings.

- **Enable.** Turns SNMP on or off.
- **SNMP Version.** Sets the protocol version. V1, V2, and V3 are available.
- **SNMP Port.** The port used by the SNMP server.
- **Read Community.** The SNMP read community value.
- **Write Community.** The SNMP write community value.
- **Trap IP Address.** The destination address for SNMP traps.
- **Trap Port.** The destination port for SNMP traps.

14.2.4 IEEE 802.1X

IEEE 802.1X is a port-based network access control protocol widely used on Ethernet networks to authenticate and secure LAN port access. A device connected to a controlled port can reach resources on the LAN only after it passes authentication; if authentication fails, access is denied.

Figure 14-6. IEEE 802.1X settings.

- **Enable IEEE 802.1X.** Turns 802.1X authentication on or off.
- **Authentication Methods.** Selects the 802.1X authentication method.
- **Username.** The 802.1X authentication user name.
- **Password.** The 802.1X authentication password.

14.2.5 Port Settings

These settings define the ports used to reach the camera and the behavior of related services. Change a port only when another application on the network already uses the default value.

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 Port	554	554	TCP	Inactive	Auto	☐

Multicast Port: 10000 (1024-65535)

P2P Switch: ☒

Auto Redirect to HTTPS: ☐

Figure 14-7. Port settings.

- **HTTP Port.** The port used to log in to the camera remotely, for example from the web client. The default is 80. If another application already uses port 80, change this value.
- **HTTPS Port.** The port for secure connections. The default is 443. HTTPS is a secure HTTP channel that protects the transmission through encryption and authentication.
- **RTSP Port.** The port used for RTSP streaming. The default is 554. If another application already uses port 554, change this value.
- **UPnP.** To reach the camera remotely through the web client, port forwarding must be configured on the router. If the router supports UPnP, enable this option and the camera arranges port forwarding automatically. If the router does not support UPnP, configure port forwarding manually on the router.
- **Multicast Port.** Sets the port used for multicast.
- **P2P Switch.** Enables the peer-to-peer service. When turned off, P2P connectivity is unavailable.

14.3 Cloud Service

The cloud service lets you add the camera to the OVConnect mobile application for remote management. Enable the service, select your region, and generate a dynamic QR code; scanning the code in the OVConnect app binds the camera to your account.

Figure 14-8. Cloud service setup.

- **Cloud Service.** Turns the cloud service on or off.
- **Privacy Statement.** You must read and agree to the privacy statement before the cloud service can be enabled.
- **Region.** Selects the cloud service region. It must match the region in which the OVConnect app is registered.
- **QR Code.** After the cloud service is enabled and the region is set, a dynamic QR code is generated automatically. Scan it with the OVConnect app to add the camera. The code is valid for 300 seconds; once it expires, generate a new one.
- **Unbind.** Removes the binding between the camera and the OVConnect account. After unbinding, the camera appears offline and is no longer accessible in the app.

NOTE The cloud service communicates with a cloud server, so the camera must be connected to the internet for this feature to work.

14.4 Mail Settings

The camera can send email notifications when an event is triggered or the storage is full. Configure the mail parameters below, then define when notifications are sent using the schedule.

14.4.1 Parameters

These settings define the mail account the camera uses to send notifications and the recipients that receive them.

Email Configuration

Email Schedule

Email

☒

Type

Other

Encryption

OFF

SMTP Port

25

(1 ~ 65535)

SMTP Server

SMTP server cannot be empty !

Username

Passkey

Sender

Sender Error!

Receiver 1

Receiver 2

Receiver 3

Interval

3Min

Save

Test

Refresh

Figure 14-9. Mail parameter settings.

- **Email.** Turns email notifications on.
- **Type.** The mailbox type. Two options are available: Outlook and Other.
- **Encryption.** Enable this if the mail server requires SSL or TLS. If you are unsure, set it to Automatic.
- **SMTP Port.** The SMTP port of the mail server.
- **SMTP Server.** The address of the SMTP server.
- **Username.** Your email address.
- **Password.** The password for your email account.
- **Receiver 1 to 3.** The email addresses that receive event notifications from the camera.
- **Interval.** The minimum time between notification emails.

TIP Click **Test Email** to confirm the configuration. A message is sent to your inbox; if it arrives, the parameters are correct.

14.4.2 Schedule

Define when the mail function is active so that notifications are sent only during the selected time periods. Configure the periods as described in the Schedule Setup section.

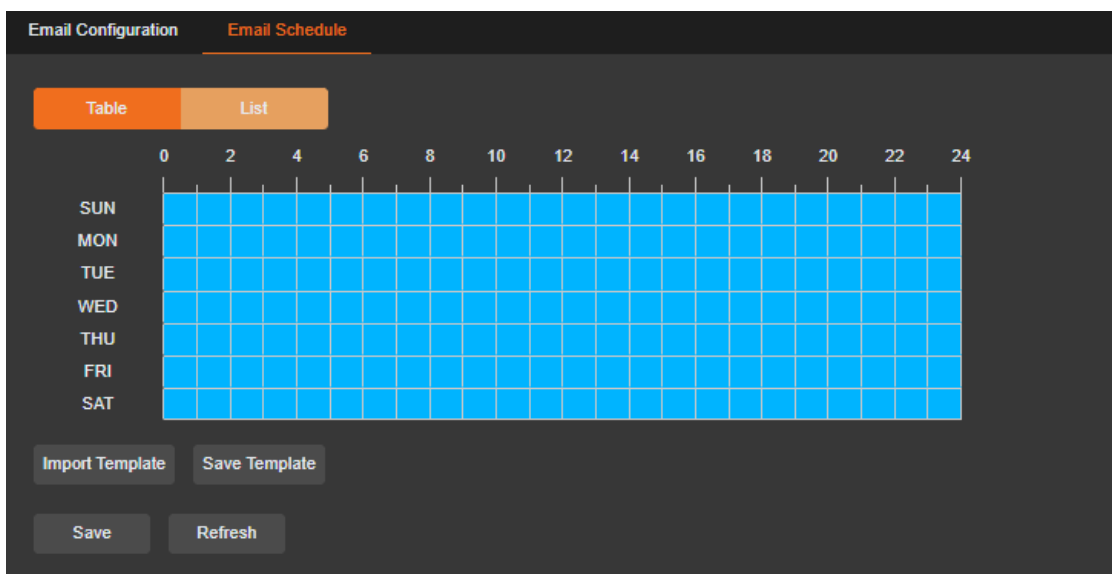
The image shows the 'Email Schedule' configuration page. At the top, there are two tabs: 'Email Configuration' and 'Email Schedule', with the latter being selected. Below the tabs are two buttons: 'Table' (highlighted in orange) and 'List'. The main area is a grid representing a weekly schedule. The columns are numbered from 0 to 24 in increments of 2, representing hours of the day. The rows are labeled with the days of the week: SUN, MON, TUE, WED, THU, FRI, and SAT. All cells in the grid are currently filled with a solid blue color, indicating that the email function is active for the entire week. At the bottom of the grid, there are four buttons: 'Import Template', 'Save Template', 'Save', and 'Refresh'.

Figure 14-10. Mail schedule.

14.5 RTSP

The Real Time Streaming Protocol (RTSP, RFC 2326) is an application-layer protocol in the TCP/IP family that defines how multimedia data is transmitted efficiently over an IP network. It allows you to view the live image in a compatible video player.

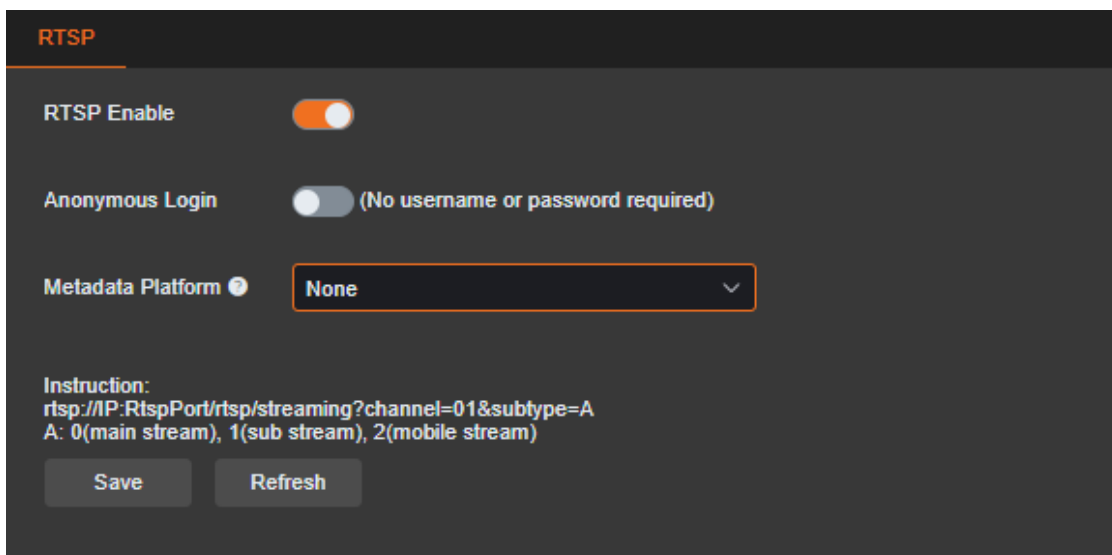
The image shows the 'RTSP' settings configuration page. The title 'RTSP' is at the top. Below it, there are three settings: 'RTSP Enable' with a toggle switch that is currently turned on (orange); 'Anonymous Login' with a toggle switch that is currently turned off (grey) and a note '(No username or password required)'; and 'Metadata Platform' with a dropdown menu currently set to 'None'. Below these settings is an 'Instruction' section with the text: 'rtsp://IP:RtspPort/rtsp/streaming?channel=01&subtype=A' and 'A: 0(main stream), 1(sub stream), 2(mobile stream)'. At the bottom, there are two buttons: 'Save' and 'Refresh'.

Figure 14-11. RTSP protocol settings.

- **RTSP Enable.** Turns the RTSP service on. Enable it to use the protocol.
- **Anonymous Login.** When enabled, no authentication is required to use the protocol.
- **Metadata Platform.** Controls how event alarm data is pushed to a third-party platform when the camera is connected using ONVIF. Options are:
 - **None.** No external metadata is pushed.
 - **General.** Pushes common-format metadata, suitable for third-party platforms without special requirements.
 - **Milestone.** Pushes metadata formatted for the Milestone platform.

14.6 Dynamic DNS

Dynamic DNS (DDNS) provides a stable host name that simplifies remote connection to the camera when its public IP address changes. To use DDNS, first create an account with a DDNS service provider.

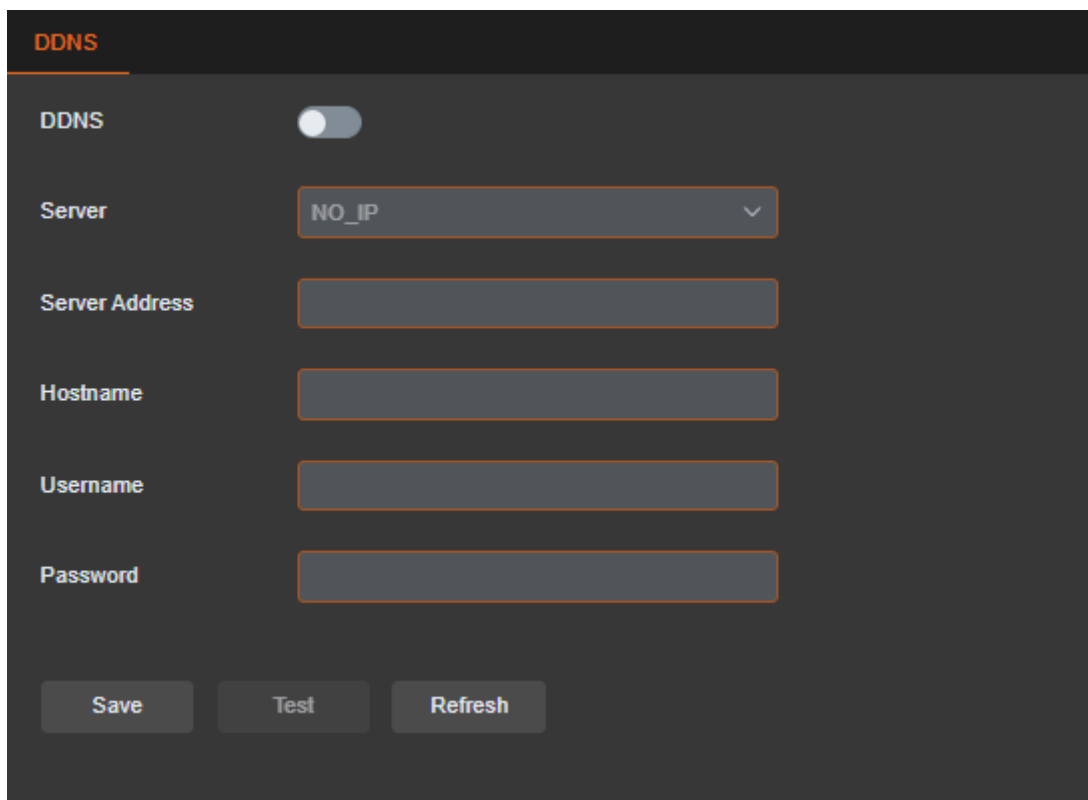


Figure 14-12. Dynamic DNS settings.

- **DDNS.** Turns the DDNS function on.
- **Server.** Selects the DDNS provider. DYNDNS and NO-IP are supported, with partial support for CHANGEIP and DNSEXIT.
- **Hostname.** The domain name you created on the provider's website. This is the address you enter in a browser to reach the camera remotely.
- **User / Password.** The credentials obtained when creating the account with the DDNS provider.

TIP After entering the parameters, click **Test DDNS** to verify the settings. If the result reports a network or DNS error, check that the network is functioning and that the DDNS details are correct.

14.7 HTTPS

HTTPS provides an encrypted connection to the camera. Use these settings to enable HTTPS and, optionally, to supply your own certificate.

Figure 14-13. HTTPS protocol settings.

- **Certificate Type.** Selects the certificate source. Two options are available: Default and Custom. The Custom option allows you to connect using your own certificate.
- **Certificate.** Selects the custom certificate file when the Custom option is chosen.
- **Key.** Selects the custom key file when the Custom option is chosen.

14.8 IP Filter

The IP filter controls which devices may connect to the camera by maintaining an allow list or a block list of addresses.

Figure 14-14. IP filter settings.

- **Enable.** Turns the IP filter on. When enabled, choose whether to apply the block list or the allow list.
- **Edit Filtering List.** Selects the list to edit — the block list or the allow list.
- **Single Add.** Adds a single address to the list.
- **Network Segment Add.** Adds a range of addresses to the list.
- **Start Address.** The first address in the range.
- **End Address.** The last address in the range.
- **Delete.** Removes a selected address from the block list or allow list.

14.9 Platform Access

Platform access lets the camera push its stream or its event data to external services. RTMP streams live video to a media server, while the event push platform delivers alarm notifications over HTTP or UDP.

14.9.1 RTMP

When RTMP is enabled and a valid server address is supplied, the camera pushes its audio and video stream to a live-streaming server such as YouTube Live.

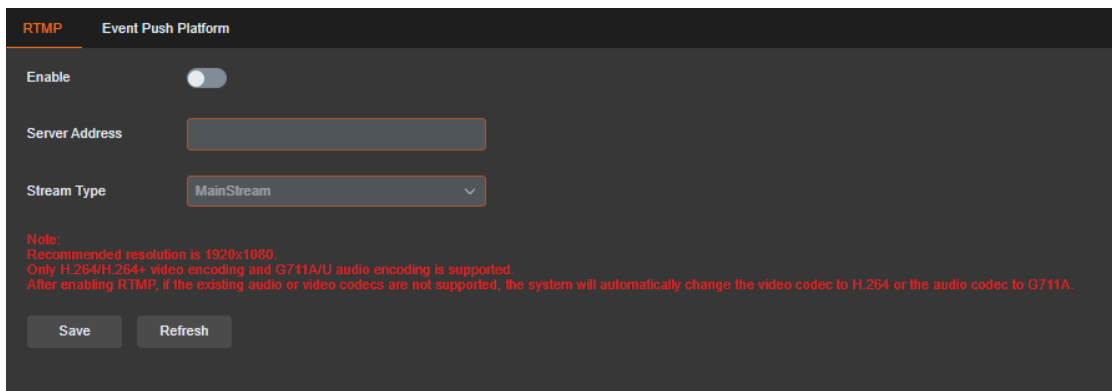


Figure 14-15. RTMP settings.

- **Enable.** Turns the RTMP function on or off.
- **Server Address.** The address of the server to which the stream is pushed.
- **Stream Type.** Selects which video stream is pushed to the server.

14.9.2 Event Push Platform

The event push platform sends alarm notifications to an external server. It supports two transport methods: HTTP, with POST and GET; and UDP, with unicast, multicast, and broadcast. This feature is available on selected models only.

14.9.2.1 HTTP Push

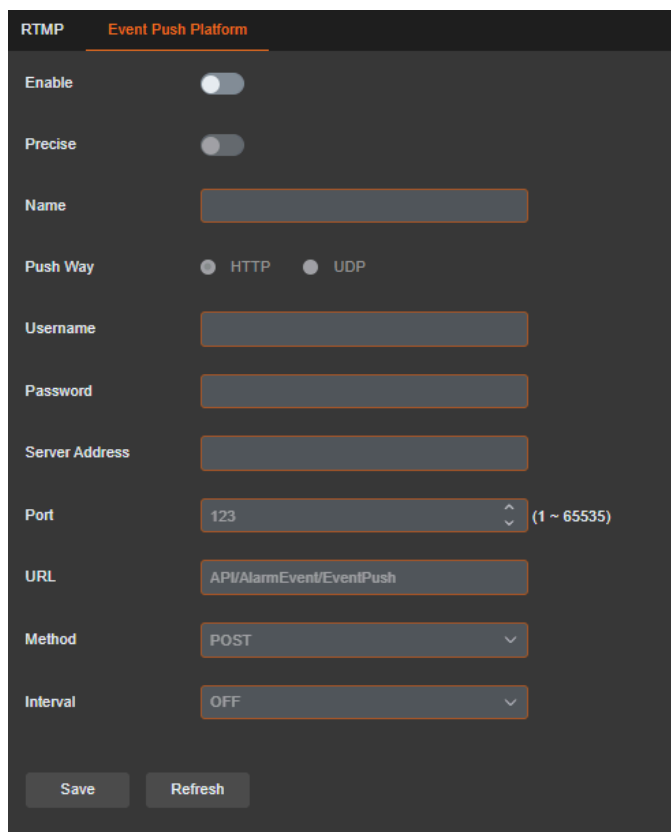


Figure 14-16. Event push over HTTP.

- **Enable.** Turns the event push function on or off.

- **Precise.** When enabled, the camera pushes once when an alarm is triggered and again when it ends. When disabled, it pushes only once at the start of the alarm.
- **Name.** The channel name. Chinese characters are not supported.
- **Push Method.** Selects the transport. Both HTTP and UDP are supported; choose HTTP here.
- **Username.** The user name. Leave it empty if none is required.
- **Password.** The password. Leave it empty if none is required.
- **Server Address.** The address of the receiving server.
- **Port.** The server port, in the range 1 to 65535.
- **URL.** The server API path. Leave it empty if none is required.
- **Method.** The HTTP method. Both POST and GET are supported. Only HTTP POST can push images; other methods push notifications only. The alarm types included in image push match those shown in the alarm column of the live view in the web client.
- **Interval.** The keep-alive interval. The keep-alive mechanism periodically confirms the connection without affecting normal alarm push. There is no keep-alive mechanism in UDP mode.

14.9.2.2 UDP Push

The screenshot shows the 'Event Push Platform' configuration window. At the top, there are two tabs: 'RTMP' and 'Event Push Platform', with the latter being selected. Below the tabs, there are several configuration options:

- Enable:** A toggle switch that is currently turned on (orange).
- Precise:** A toggle switch that is currently turned off (grey).
- Name:** An empty text input field.
- Push Way:** Two radio buttons labeled 'HTTP' and 'UDP'. The 'UDP' button is selected (orange).
- UDP Method:** A dropdown menu showing 'Broadcast' with a downward arrow.
- UDP Address:** A text input field containing '255.255.255.255'.
- UDP Port:** A text input field containing '5000' with up and down arrows on the right. To the right of the field is the range '(1 ~ 65535)'.

At the bottom of the configuration area, there are two buttons: 'Save' and 'Refresh'.

Figure 14-17. Event push over UDP.

- **Enable.** Turns the event push function on or off.
- **Precise.** When enabled, the camera pushes once when an alarm is triggered and again when it ends. When disabled, it pushes only once at the start of the alarm.
- **Name.** The channel name. Chinese characters are not supported.
- **Push Method.** Selects the transport. Choose UDP here.
- **UDP Method.** The UDP delivery type. Three modes are supported:
- **Unicast.** Messages are sent to a single client at the configured UDP server address and port; only that address receives them.
- **Multicast.** Multiple clients on the same network segment that use the same UDP address and port receive the message; other addresses do not.
- **Broadcast.** All UDP servers on the same network segment receive the message.

- **UDP Address.** The UDP server address.
- **UDP Port.** The UDP server port, in the range 1 to 65535.

Chapter 15 System and Maintenance

This chapter describes the camera's system-level configuration and upkeep: setting the clock and daylight saving time, managing user accounts and permissions, performing routine maintenance such as logging and firmware upgrades, and reviewing device and privacy information.

15.1 General System Setup

These settings establish the camera's date, time, and daylight saving behavior. An accurate clock is essential so that recordings, event logs, and notifications carry correct timestamps.

15.1.1 Date and Time

Set the camera's clock either manually or by synchronizing it with a network time source.

Figure 15-1. Date and time settings.

- **Time Settings Mode.** Selects how the clock is set. In Static mode you enter the time yourself; in NTP synchronization mode the time is calibrated over the network.
- **Date Format.** Sets the format used to display dates.
- **Time Zone.** Selects the time zone for your region or city.
- **Time Format.** Selects the preferred time format.
- **System Time.** Click in the field to set the date and time.
- **Synchronize Computer Time.** Sets the camera's clock to match the computer's time. This is unavailable when NTP synchronization mode is selected.
- **Server Address.** The optional NTP server used for automatic timekeeping.

15.1.2 Daylight Saving Time

Daylight Saving Time (DST) lets the camera adjust its clock automatically for regions that observe seasonal time changes.

Figure 15-2. Daylight saving time settings.

- **Daylight Saving Time.** Enable this option if your time zone observes daylight saving time.
- **Set by Week.** Selects the month, day of the week, and time at which DST begins and ends — for example, 2:00 a.m. on the first Sunday of a given month.
- **Set by Date.** Selects the exact date and time at which DST begins and ends.
- **Start Time / End Time.** Sets the start and end of the daylight saving period.
- **Time Offset.** Selects how much time DST adds to your time zone — the difference between Coordinated Universal Time (UTC) and local time.

15.2 Multi-user Management

Multi-user management lets you create accounts with individual user names, passwords, and permissions. The camera supports two account types:

- **ADMIN (system administrator).** Has full control of the camera. The administrator can configure every function, change the administrator and user passwords, and enable or disable password protection.
- **USER (standard user).** Has access to functions such as live view, search, and playback. Multiple users can be created, each with its own set of access rights.

NO.	Username	Group Name	Password	Delete User
1	admin			
2	user1	Advanced		

Figure 15-3. Multi-user management.

To change an account's password, click the **Password Edit** icon. The password must be 8 to 16 characters and combine at least two of the following: digits, uppercase letters, lowercase letters, and special characters. Re-enter the new password to confirm it. When you save the change, the camera asks for the current administrator password for authentication.

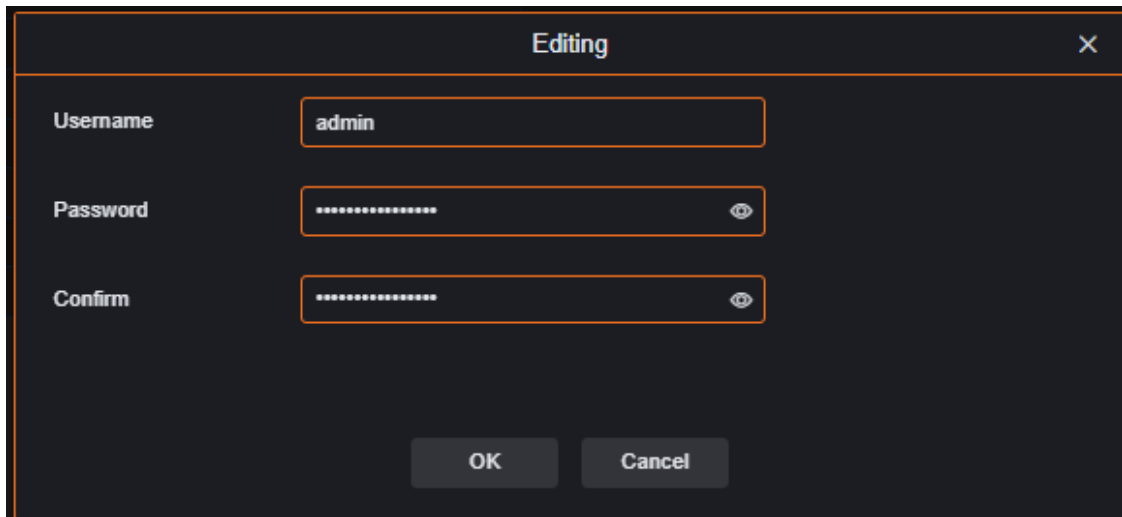

 A dark-themed dialog box titled "Editing" with a close button (X) in the top right corner. It contains three input fields: "Username" with the text "admin", "Password" with masked characters and a visibility icon, and "Confirm" with masked characters and a visibility icon. At the bottom are "OK" and "Cancel" buttons.

Figure 15-4. Editing a user account.

To enable and configure a standard user:

1. Select one of the inactive users and click the **Password Edit** icon.
2. Select **Enable** to activate the user.
3. Click **UserName** to edit the user name.
4. Click the field next to **Password** and enter the desired password.



Policy icon — opens the permissions page for the selected user.

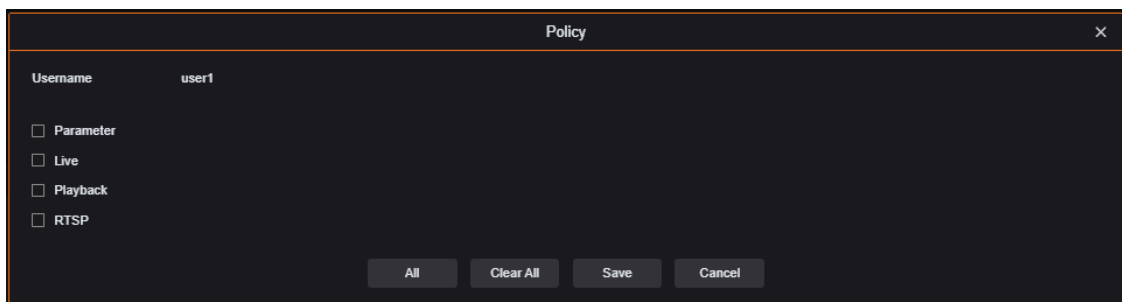

 A dark-themed dialog box titled "Policy" with a close button (X) in the top right corner. It shows "Username" as "user1". Below are four checkboxes: "Parameter", "Live", "Playback", and "RTSP", all of which are currently unchecked. At the bottom are "All", "Clear All", "Save", and "Cancel" buttons.

Figure 15-5. Setting sub-user permissions.

1. Click the field next to **Confirm** and re-enter the password, then click **OK**. The camera requires the administrator password for authentication.

To set permissions for a standard user, open the **Policy** page and select the box for each function you want to grant. Click **All** to select every permission or **Clear** to clear them all.

15.3 Maintenance

The maintenance tools let you review system activity, restore or upgrade the camera, back up and restore its configuration, schedule automatic upkeep, and collect diagnostic information.

15.3.1 Log Management

The system log records significant events such as motion alerts and system warnings. You can search the log by type and time period and export a backup to your computer.

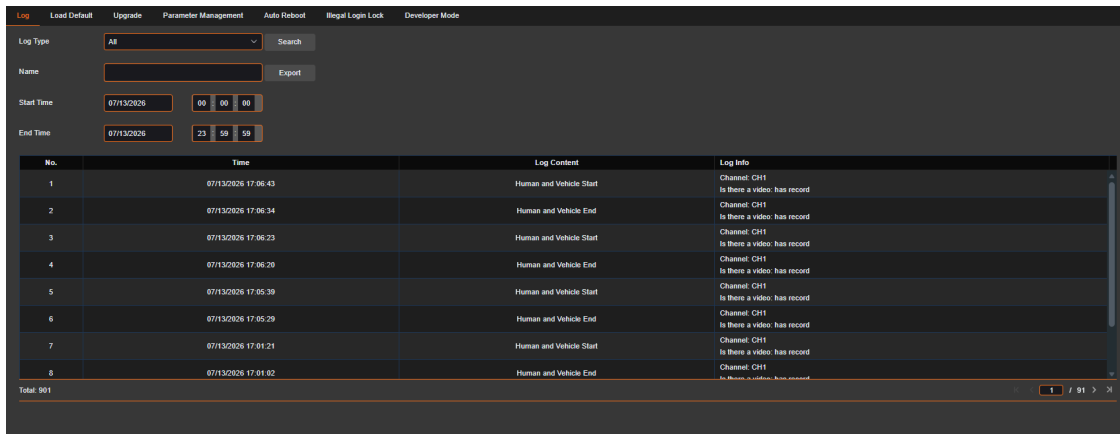


Figure 15-6. Log search and backup.

Select the category to search from the **Log Type** list, or choose **All** to view the entire log for the selected period. The available types are:

- **System.** System settings, reboot, auto reboot, upgrade, time settings, and NTP calibration.
- **Configuration.** Changes to camera settings, including live control, privacy areas, recording mode and schedule, main/sub/mobile stream, network, email, color, motion detection, storage, multi-user, NTP, image control, RTSP, IP filter, restore factory settings, sound detection, import/export, event push, capture, deterrent, AI, FTP, DDNS, HTTPS, audio, siren, system maintenance, video masking, I/O alarms, and cloud service setup.
- **Alarm.** The start and end of detection events such as motion, I/O alarm, video tampering, line crossing, object detection, pedestrian and vehicle, face detection, cross counting, crowd density, queue length, license plate detection, intrusion, region entrance, region exiting, rare sound, and sound alarm.
- **Account.** Login, logout, lock, and user switching.
- **Recording.** Search, playback, and backup.
- **Storage.** Format memory card, memory card full, and memory card error.
- **Network.** Network down, network up, network error, and network mode change.

To search and export the log:

1. Select the event subtype from the **Minor Type** list. This list is unavailable when Log Type is set to All.
2. Enter a file name in the **Name** field. Click **Export** to create a backup of the log.
3. Click the **Start Time** field and select the start date and time from the calendar.
4. Click the **End Time** field and select the end date and time from the calendar.
5. Click **Search**.
6. Review the log entries for the selected period, using the page navigation controls in the lower-right corner to move between pages.

15.3.2 Restore Factory Settings

This page restores the camera's configuration to its factory state. Restoring the factory settings does not format the data on the memory card.

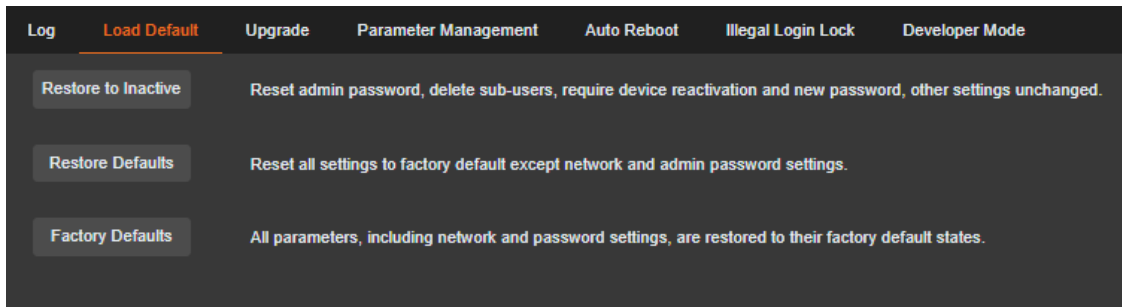


Figure 15-7. Restore factory settings.

- **Restore to Inactive.** Resets the administrator password and deletes all sub-users; the camera must be reactivated. All other settings remain unchanged.
- **Restore Defaults.** Restores all settings to factory values except the network configuration and the administrator password.
- **Factory Defaults.** Restores every camera setting to its factory value.

CAUTION Restoring factory settings is irreversible. Export a configuration backup first if you may need the current settings again.

15.3.3 System Upgrade

This page updates the camera's firmware. You can detect an upgrade online or install a firmware file from your computer.

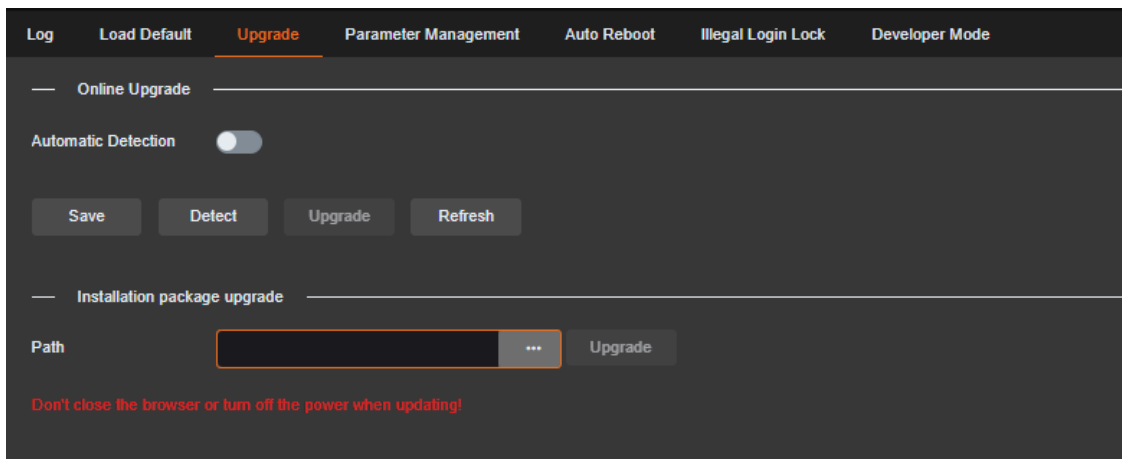


Figure 15-8. System upgrade.

- **Automatic Detection.** When enabled, the camera checks for online upgrade files automatically.
- **Username / Password.** The credentials for the upgrade server. HTTP upgrades do not require them.
- **Server Address.** The address of the online upgrade server.
- **Save.** Stores the current settings.
- **Detect.** Checks the server for a new firmware version. When one is found, a prompt appears.

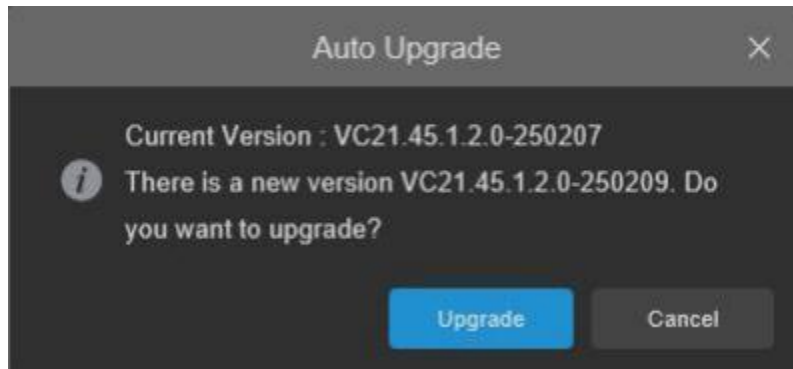


Figure 15-9. New firmware version detected.

To upgrade from a local file, place the firmware file (a .bin file) on your computer, click the button next to **Path** to select it, then click **Upgrade** to begin. The upgrade takes about 2 to 3 minutes.

CAUTION Do not power off the camera or close the browser during the firmware upgrade. Interrupting the process can leave the camera inoperable.

NOTE To detect the latest firmware from the cloud server, enable the cloud service to bind the OVConnect app and clear the online upgrade settings on this page.

15.3.4 Parameter Import and Export

You can export the camera's configuration to a file on your computer and later import that file to restore the settings or apply them to another camera.

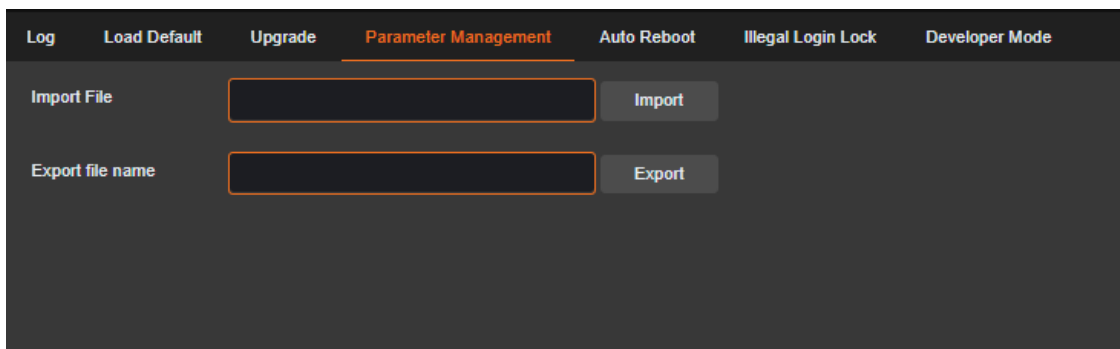


Figure 15-10. Parameter management.

- **Import File.** Click the field to open the file browser, select a parameter file, and click **Import** to load the settings.
- **Export File Name.** Enter a name for the exported file, then click **Export** to save the current parameters.

15.3.5 Auto Maintenance

Automatic maintenance reboots the camera on a defined schedule to keep it running reliably over long periods.

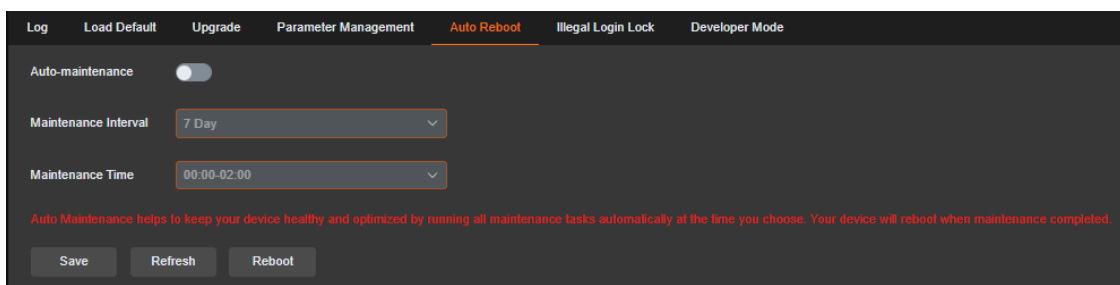


Figure 15-11. Auto maintenance.

- **Auto Maintenance.** Turns the automatic maintenance feature on or off.
- **Maintenance Interval.** Sets how often automatic maintenance runs.
- **Maintenance Time.** Sets the period during which maintenance takes place. The camera reboots at a random point within this period.

15.3.6 Developer Mode

Developer mode collects and records diagnostic log information to support device debugging.

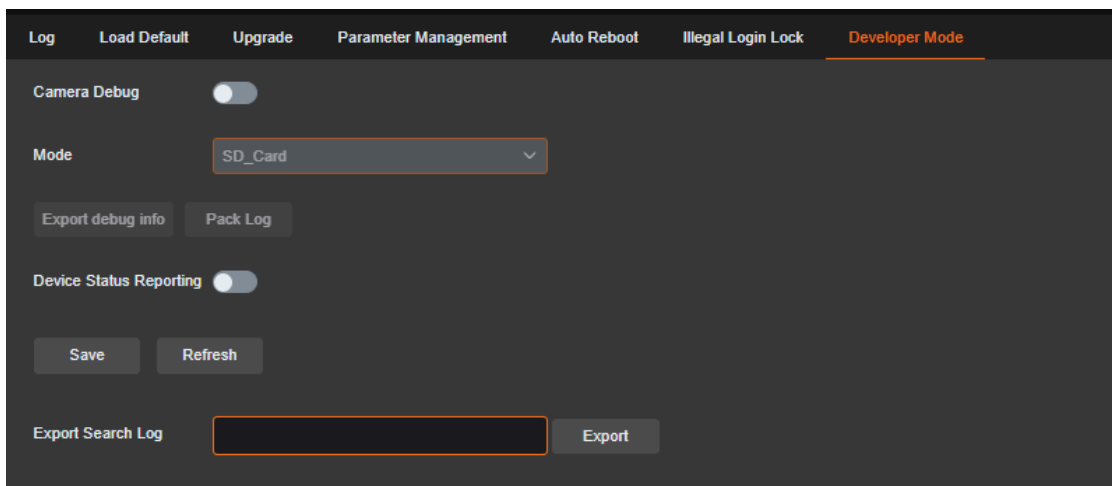


Figure 15-12. Developer mode.

- **Camera Debug.** Enables the collection of debug information.
- **Mode.** Selects where debug information is recorded. Three modes are available: NVR, SD_Card, and FTP.
- **Download Debug Logs.** Exports debug information. In SD_Card mode, click the button and enter the correct password to download the information to your computer.
- **Pack Log.** Packages the logs. In NVR or FTP mode, click this button to upload the packaged log information to the FTP server.
- **Device Status Reporting.** When enabled, uploads the storage status, channel status, and device information to the P2P server.
- **Export Search Log.** Exports the search log. Enter a file name and click Export to save all stored log files to your computer.

15.4 System Information

The system information pages let you review the camera's identity and read its privacy statement.

15.4.1 Device Information

This page displays system details such as the device ID, model name, MAC address, and firmware version.



Figure 15-13. Device information.

15.4.2 Privacy Statement

This page presents the full text of the device's privacy statement for review.

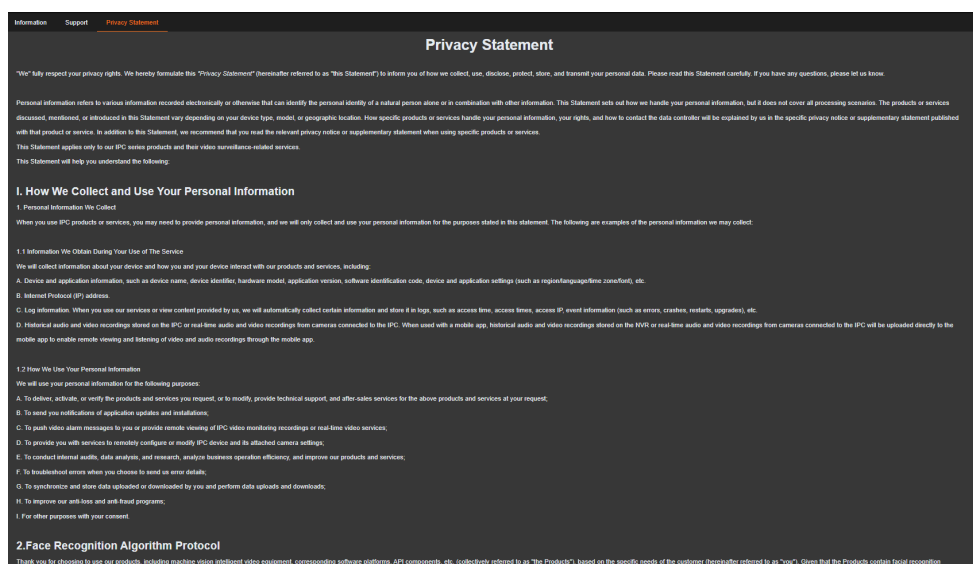


Figure 15-14. Privacy statement.

Camera Types

Model-specific features for PTZ, thermal, and multi-lens cameras.

Chapter 16 PTZ Cameras

This chapter describes the pan-tilt-zoom (PTZ) features available on selected camera models, including the self-test performed at startup and the cruise modes used for automated patrol.

When a PTZ camera is powered on, it performs a Power-On Self-Test (POST). The camera rotates clockwise at a constant speed until it detects the zero point, then moves vertically and settles at a 45° downward angle, with the lens aligned to the identification mark on the enclosure. The lens focuses to the near end, extends to the far end, and returns to the near end to complete the test. Depending on the model, the camera may instead return to the position it held before power-off.

16.1 Basic Functions

A PTZ camera provides several automated movement features:

- **Cruise modes.** The camera supports preset points, a watch position, track cruise, pattern scan, and line scan.
- **Automatic speed adjustment for zoom.** The pan and tilt speed changes automatically with the zoom ratio. At higher zoom the camera moves more slowly, and at lower zoom it moves faster, which improves tracking of a target.
- **Power-off memory.** If the camera is cruising when power is lost, it resumes the cruise after completing the self-test at the next startup. Some models instead return to the position held before power-off, depending on the model.



Click the control icon in the top-right corner of the live view to show or hide the PTZ control panel. The buttons are described in the sections that follow.

16.1.1 Preset Cruise

A preset point stores a specific pan, tilt, and zoom position that the camera can return to on demand.



Aim the camera with the arrow keys, then click to save the current position as a preset point.



Click to recall a preset point and move the camera to that position.



Click to delete a preset point.

Click the **point1** text box to rename a preset point.

NOTE You can store up to 255 preset points.

16.1.2 Watch Mode

In Watch Mode, the camera automatically performs a preset action when it receives no control signal for the configured waiting time.

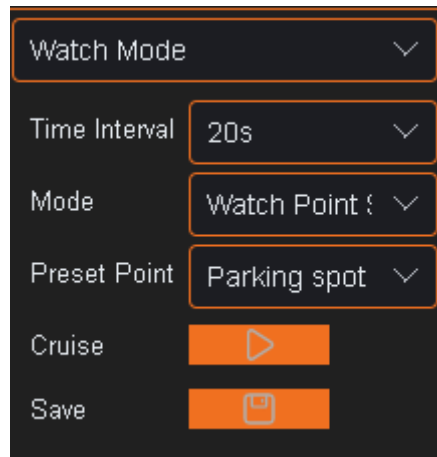


Figure 16-1. Watch Mode configuration.

1. Set the cruise mode to **Watch Mode**.
2. Set the time interval. This is the delay after you stop manually operating the camera before the watch action resumes. It can be set from 15 to 240 seconds.
3. Set the watch action to one of the available modes: default cruise, a preset point, line scan, track cruise, or pattern scan.

With default cruise selected, the camera rotates continuously 360° counterclockwise at a constant speed when the watch action is called.

NOTE Only one watch point can be configured at a time.

16.1.3 Linear Scan

Line scan moves the camera back and forth between two horizontal positions at a constant speed.

1. Set the cruise mode to **Line Scan**.

 Aim the camera at the required start position and click to record it as the scan start point.

 Rotate the camera to the required end position and click to record it as the scan end point.

Click **Cruise** to begin scanning. The camera then travels between the two points at a constant speed.

16.1.4 Track Cruise

In track cruise, the camera patrols a sequence of preset points in order. You can define up to four tracks, and each track can include up to 32 preset points, each with its own dwell interval.

1. Set the cruise mode to **Tour**.



Figure 16-2. Selecting the track to configure.

1. Select the track to which preset points will be added.



Figure 16-3. Adding and ordering the preset points on a track.

1. Add or remove preset points for the track. Use the up and down arrow buttons to change the order in which the points are visited.
-  Set the dwell interval between preset points during the cruise.
1. Click **Cruise** to start the patrol. The camera visits the preset points in the configured order.

NOTE After adding preset points, you must click **Cruise** to save the track path.

16.1.5 Pattern Scan

Pattern scan records a sequence of manual operations — horizontal movement, vertical movement, and zoom changes — and replays them on demand. The camera supports four pattern-scan paths, numbered 1 to 4, each stored on the camera.

1. Set the cruise mode to **Pattern Scan**.



Figure 16-4. Selecting the pattern-scan path.

1. Select a path.



Figure 16-5. Recording control for a pattern-scan path.

1. Click the record button, perform the required PTZ operations, then click the button again to stop recording. Click the call button to replay the recorded path.

16.1.6 Pigtail Specification

The following figure identifies the connectors on the camera's cable tail (pigtail).

Label	Corresponding Pigtail Color
AUDIO IN	Pink
AUDIO OUT	White/Yellow
AUDIO GND	Purple
RS485+	Brown/White
RS485-	Brown
GROUND	Yellow/Green
ALARM IN	Blue
ALARM GND	Green/Purple
ALARM OUT+	Green
ALARM OUT-	Gray

The pigtails depend on the actual model.

Figure 16-6. Pigtail connector specification.

Chapter 17 Thermal Cameras

Thermal cameras detect heat rather than visible light, which allows them to identify fire points and measure surface temperatures across the scene. The features in this chapter apply to models equipped with a thermal channel.

17.1 Fire Detection

Fire detection monitors areas where a fire hazard may exist and raises an alarm when a fire point is detected.



Figure 17-1. Fire detection settings.

- **Enable.** Turns fire detection on or off.
- **Sensitivity.** Sets how readily a fire point triggers the alarm. A lower sensitivity requires a higher temperature to trigger the alarm; a higher sensitivity triggers at a lower temperature.

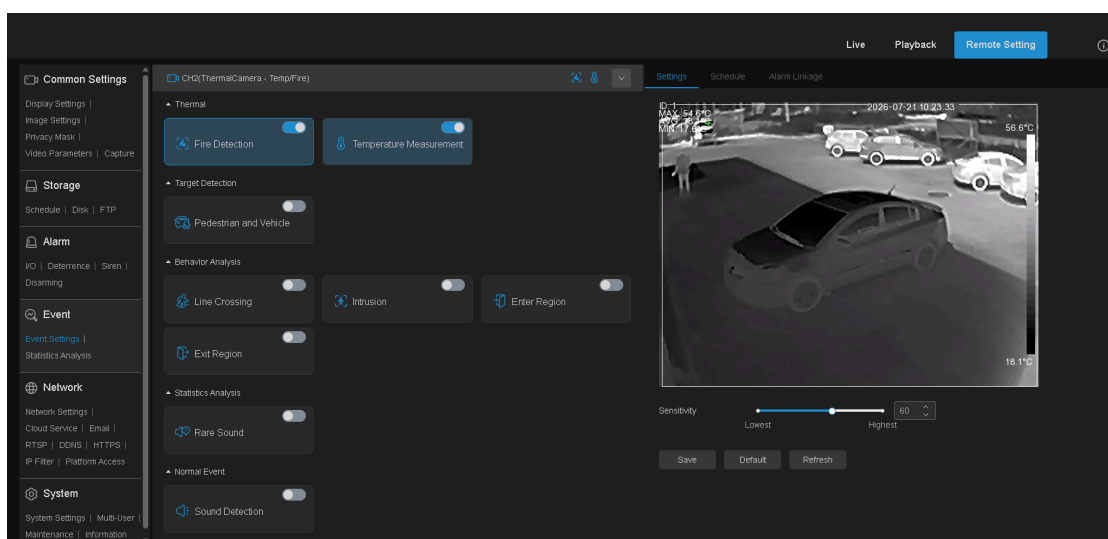


Figure 17-2. Fire detection sensitivity.

17.1.1 Temperature Measurement

Temperature measurement displays and overlays temperature readings taken from the thermal channel. Enable the feature and configure how the readings are shown.

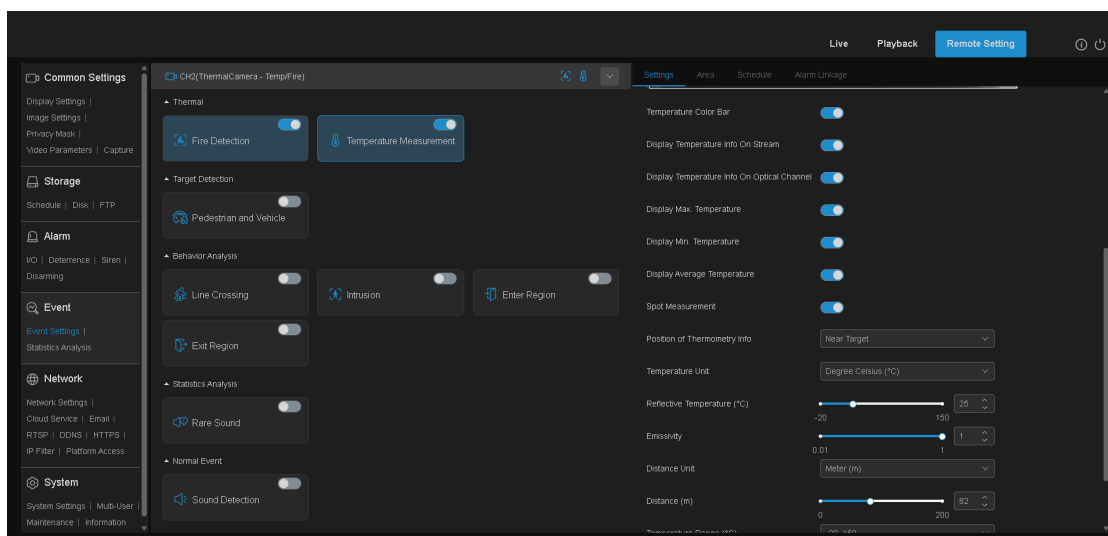


Figure 17-3. Temperature measurement settings.

- **Enable.** Turns the temperature measurement function on or off.
- **Temperature Color Bar.** Displays a color bar on the right of the thermal live view, scaled between the maximum and minimum temperatures.
- **Display Temperature Info On Stream.** Overlays the measurement areas and their temperatures on the thermal channel live view.
- **Display Temperature Info On Optical Channel.** Overlays the measurement areas and their temperatures on the optical channel live view at the same time.
- **Display Max. Temperature.** Shows the maximum measured temperature in the live view. The temperature-info overlay must be enabled first.
- **Display Min. Temperature.** Shows the minimum measured temperature in the live view. The temperature-info overlay must be enabled first.
- **Display Average Temperature.** Shows the average measured temperature in the live view. The temperature-info overlay must be enabled first.
- **Spot Measurement.** When enabled, clicking any point in the thermal live view with the left mouse button measures the temperature at that spot.
- **Position of Thermometry Info.** Sets where the temperature information appears: **Near Target** places it beside each measurement area, and **Top Left** places it in the top-left corner of the live view.
- **Temperature Units.** Selects the unit used for temperature values: Celsius, Fahrenheit, or Kelvin.
- **Reflected Temperature.** Sets the ambient temperature reflected by the target's surface. Setting it correctly lets the camera separate the radiation emitted by the object from the radiation reflected off it, which improves measurement accuracy.
- **Emissivity.** Sets the target material's ability to emit infrared radiation. Because different materials emit and reflect radiation differently, an incorrect value causes measurement error. See the Emissivity of Common Substances table.
- **Distance Unit.** Selects meters or inches for the distance value.
- **Distance.** Sets the straight-line distance between the target and the camera, according to the actual installation.

NOTE When a measurement area is defined as a point, only the average temperature is displayed; the maximum and minimum temperatures are not shown.

17.1.2 Temperature Measurement Area Setting

Temperature-measurement rules define where in the scene the camera samples temperature. To create a rule:

1. Click **Add** to create a rule. Up to 20 rules can be defined.

2. Select the rule and set **Enable** to activate it.
3. Enter a name for the rule in the **Name** column.
4. Choose the rule type — point, line, or area — then draw it on the configuration screen at the right. To remove a rule, select its check box and click **Delete**.

The three rule types behave as follows:

- **Point.** Click a location to measure the temperature at that spot. The preview screen shows the rule and its average temperature.
- **Line.** Click and drag to draw a line; the camera measures temperature along the segment. Select the line's check box to adjust its length, angle, and position. The preview screen shows the rule and the temperature along the line.
- **Area.** Click and drag to draw a quadrilateral region; the camera measures the temperature within it. Select the region's check box to adjust its size and position. The preview screen shows the rule and the area's temperature.

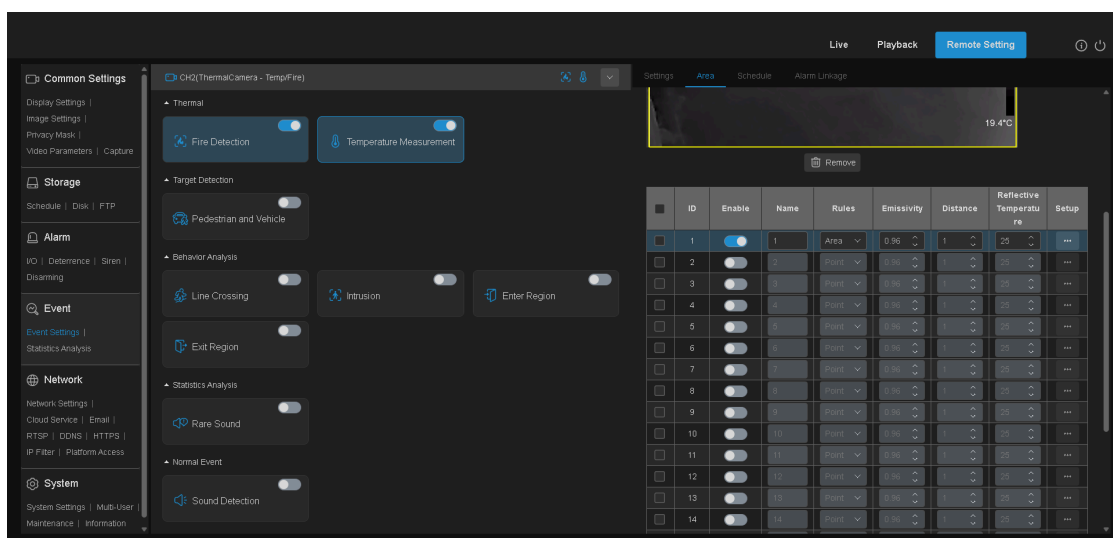


Figure 17-4. Drawing point, line, and area temperature-measurement rules.

For each rule, set the parameters that ensure an accurate reading:

1. Set the **Emissivity** to match the target material.
2. Set the **Distance** to the straight-line distance between the target and the camera.
3. Set the reflected (ambient) temperature of the camera's surroundings.

Finally, define how each rule raises an alarm.

- Click to open the alarm rule configuration page.

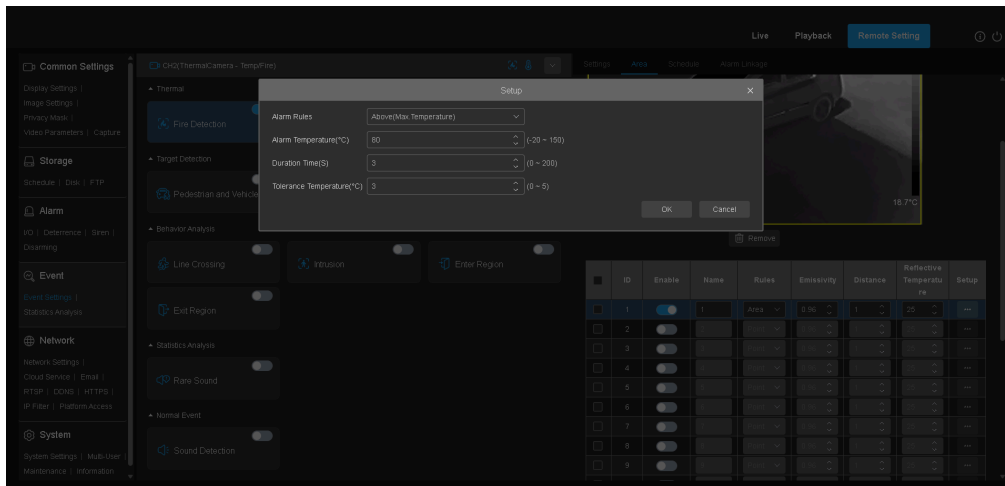


Figure 17-5. Alarm rule configuration for a temperature-measurement rule.

An alarm rule compares a measured value against a threshold. The available conditions are:

- **Maximum temperature.** The maximum temperature is above, or below, the threshold.
- **Minimum temperature.** The minimum temperature is above, or below, the threshold.
- **Average temperature.** The average temperature is above, or below, the threshold.
- **Temperature difference.** The spread between the highest and lowest temperature is above, or below, the threshold.

NOTE Point rules support only the average-temperature conditions (above or below the threshold).

- **Alarm Temperature.** The temperature threshold that triggers the alarm.
- **Duration Time.** How long the measured temperature must exceed the threshold before the alarm is triggered.
- **Tolerance Temperature.** A margin that prevents minor temperature fluctuations from repeatedly toggling the alarm.

NOTE Example: with the condition set to average temperature above 40°C, a duration of 3 s, and a tolerance of 3°C, the alarm triggers when the monitored area's average temperature exceeds 40°C for more than 3 seconds, and clears when the average falls to 37°C or below.

To remove a rule, select its check box and click **Delete**.

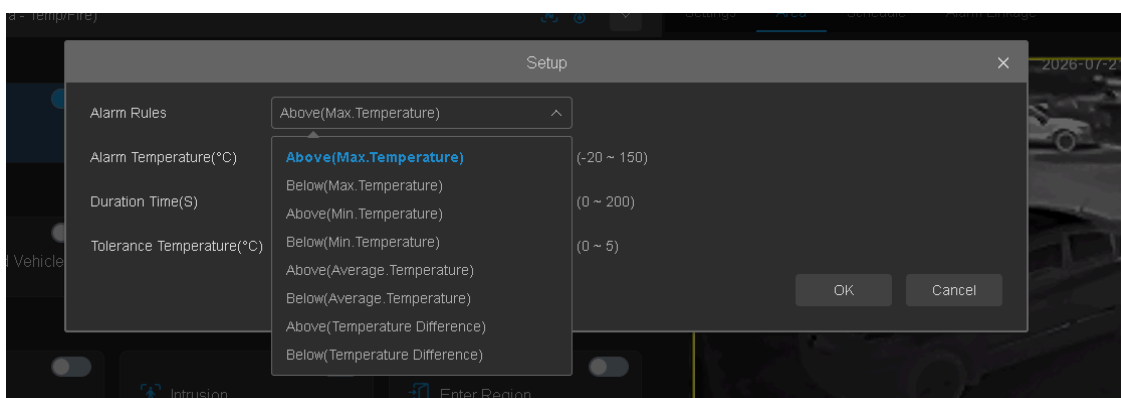


Figure 17-6. Alarm rule thresholds and duration.

17.1.3 Thermal Alarm Schedule

When the schedule is enabled, the camera performs fire detection and temperature-measurement alarms only during the time periods you define. Configure the periods as described in the Schedule Setup section.

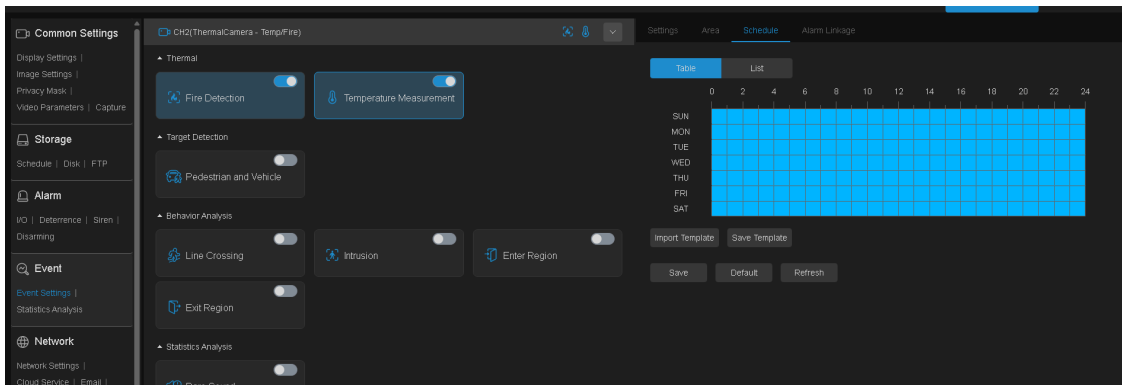


Figure 17-7. Thermal alarm schedule.

17.1.4 Thermal Alarm Linkage

Define the actions the camera performs when a fire-detection or temperature-measurement alarm is triggered.

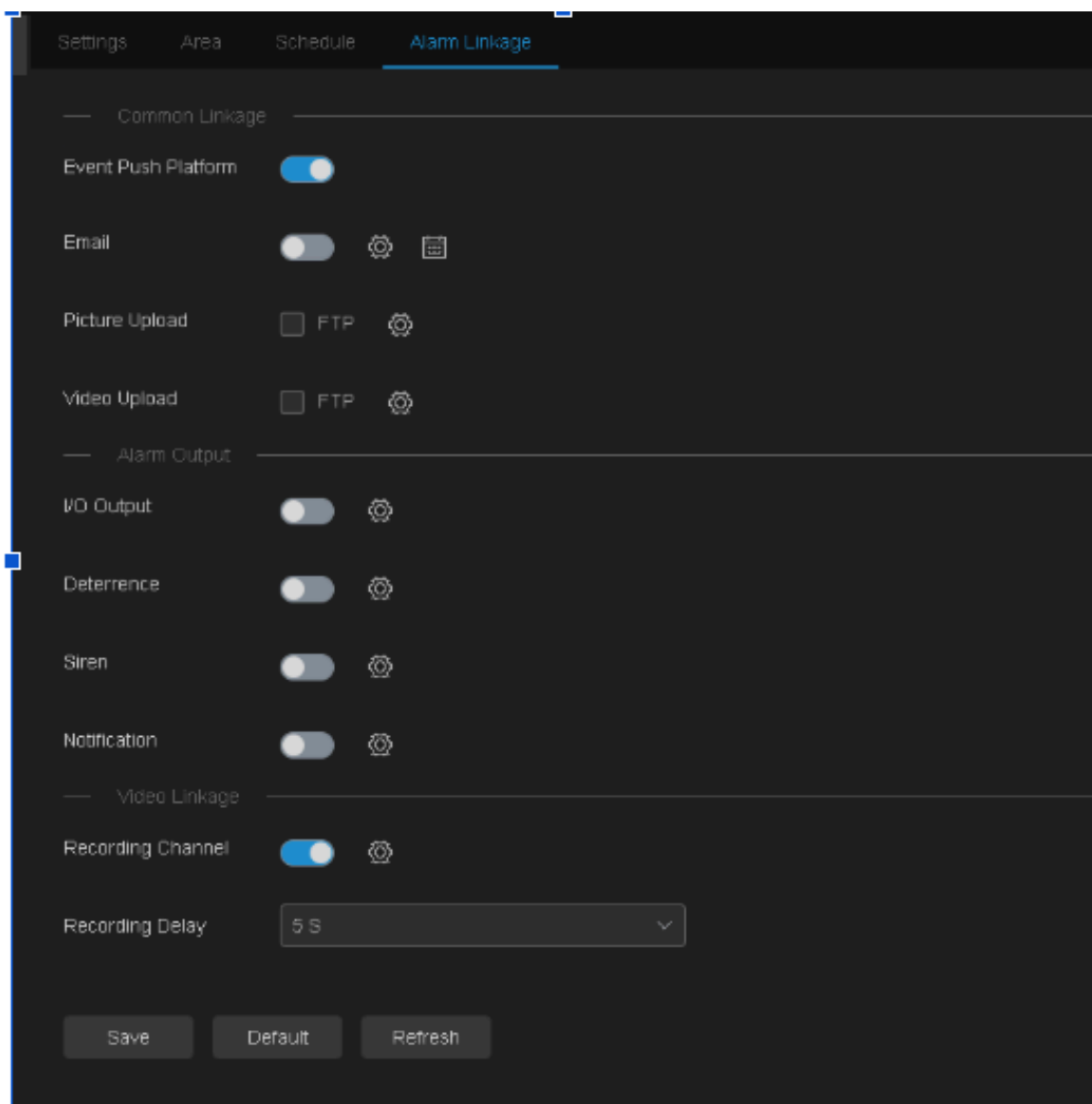


Figure 17-8. Thermal alarm linkage actions.

- **Send Email.** Sends an email notification when an alarm is triggered.
- **Event Push Platform.** When enabled, alarm information is pushed to the connected client.
- **Alarm In/Out.** Enables the alarm output and its latch time. It is not shown on cameras without an I/O output.

- **Light.** When enabled, the white light turns on for deterrence when an alarm is triggered.
- **Warn Light.** When enabled, the warning light turns on for deterrence when an alarm is triggered.
- **Siren.** When enabled, the siren sounds for deterrence when an alarm is triggered.
- **FTP Picture Upload.** Uploads alarm images to the FTP server for the selected channels when an alarm is triggered.
- **Record Channel.** Records video on the selected channels when an alarm is triggered.

17.2 Emissivity of Common Substances

Use these representative emissivity values as a starting point when configuring temperature measurement. Adjust them to match the specific target material where a more accurate reading is required.

Substance	Emissivity
Human skin	0.98
Cotton fabric	0.98
Water	0.96
Asphalt	0.96
Concrete	0.95
Brick	0.95
Rubber	0.95
Paint	0.93
Ceramics	0.92
Soil	0.92
Printed circuit board	0.91
Paper	0.90
Cardboard	0.90
Sand	0.90
Wood	0.85

Chapter 18 Multi-Lens Cameras

Multi-lens cameras — panoramic, quad-lens, and dual-lens models such as QUADZ2812IP32MP-AI, QUADF28IP16MP-AI, and DD2F28IP10MP-AI — house several independent lenses in a single unit, under a single IP address.

These models share the same platform, web client, video and image settings, and AI feature set as the rest of the IP camera line. The key difference is architectural: multiple lenses, each exposed as its own channel, are managed through one login.

- **Single IP, multiple channels.** The camera is managed from one web login and one IP address, but each physical lens appears internally as its own channel (for example, Channel 1 to Channel 4). Video, image, and AI pages include a channel selector, and settings are applied per channel. A **Copy to other channels** option applies the same settings to every lens at once.
- **Independent AI settings per channel.** Each channel can have its own AI detection rules — face, license plate, motion, cross-line, and cross-counting — enabled, tuned, and scheduled independently of the others.

- **Independent deterrence and siren per channel.** Active deterrence (light) and siren responses are configured per channel, since each lens covers a different field of view and may require a different response.
- **Recording and alarm linkage per channel.** Alarm actions such as recording and FTP or cloud upload let you choose which channels they apply to; an alarm on one lens need not trigger a response on the others.
- **NVR integration.** When added to an NVR, the device appears as a single network entry with multiple channels, in the same way as a multi-channel encoder. The NVR lists and lets you preview or record each lens as a separate channel, without a separate device entry per lens.

In short, treat these models as standard IP cameras for setup, firmware, network, and AI configuration. The only meaningful difference is that one camera now represents several channels behind a single IP address, so any setting that is normally global becomes per-channel.