

«Carevision™

User Manual

Page 1 | 60

Safety Instructions

This manual is intended to ensure that user can use the product properly without danger or any property loss. Please read it carefully and do not discard for future reference. Precaution measures are divided into "WARNINGS" and "CAUTIONS" as below:

WARNING: Neglecting any of the warnings may cause serious injury.

CAUTIONS: Neglecting any of the CAUTIONS may cause injury or equipment damage.



Warning Follow these safeguards to avoid death or serious injury



Caution Follow these precautions to Prevent potential injury or Property loss



- Enclosure could be hot during operation in high ambient temperature environments
- NEC safety regulations must be followed during the installation of this product.
- Please use a power supply that meets the power requirements found in the data sheet.
- Do not connect multiple cameras with a single power adapter
- Shut down the power while connecting or dismounting the device.
- The device should be firmly fixed when installed onto the wall or beneath the ceiling.
- Shut down the power and unplug the power cable immediately when there is smoke, odor, or noise rising from the CAMERA.



- Make sure the power supply voltage is correct before using the camera.
- Do not drop objects onto the device or vibrate the device vigorously.
- keep the device away from locations where magnetic interference is present.
- Avoid installing the device where the surface is vibrating or subject to shock (ignoring this may damage the device).
- Do not aim the camera lens at a strong light source such as the sun or incandescent lamp. The strong light source can cause damage to the camera.
- Do not touch the heat sink in the product directly.
- When cleaning, wipe off the dirt on the casing with a soft cloth. When cleaning the dirt, it should be cleaned with a dry cloth. When the dirt is not easy to remove, it can be wiped clean with a neutral detergent. Do not use alkaline cleaner to wash. If there is dust on the lens, wipe the lens with a lens cloth.
- Properly configure all passwords and other related product security settings and keep your username and password in a safe place.

Contents

6.3.2 Storage management26
6.4 Network
6.4.1 Basic Setup
6.4.2 Advanced Setup29
6.5 Video
6.5.1 Video
6.5.2 Audio
6.6 Image
6.6.1 Image
6.6.2 OSD
6.7 Events
6.7.1 Ordinary Events
6.7.2 Smart Event
Chapter 7: Wi-Fi Cameras55
7.1 Setting Up Wi-Fi Cameras
7.1.1 Connect the Camera to the Home LAN55
7.1.2 Connect to Wi-Fi56
7.2 Changing the WiFi Password on a WiFi Camera57
7.2.1 Connect the Camera to the Home LAN57
7.2.2 Change Wi-Fi Password58
7.3 Configure WiFi Settings
7.3.1 Configure WiFi Settings59

Chapter 1: Product Introduction

1.1 Product Manual

ClareVision cameras video and audio recording capabilities, intelligent motion detection, notifications, alerts, and transmits video over your network.

You can use the ClareVision App for standalone camera viewing or using it with the ClareHome App and ClareOne Panel to view and manage live video feeds and recordings. For advanced configuration settings, you can use a web browser to set camera parameters such as system parameter settings, OSD display settings and other parameters. This manual provides instructions on all pertinent camera uses and settings.

1.2 Product Features

This section introduces the camera product features:

- System functions
- Video and capture functions

The cameras support video recording and capture. You can install a micro-SD card, configure a network storage disk, or connect the camera to a Network Video Recorder (NVR).

User management

You can manage multiple different users through the system administrator "**admin**" user. There are multiple permission levels available to control access to certain camera features.

• Video playback

You can playback video from the local memory card, network storage, or an NVR.

• Event detection function

There are two camera series: Value Series and Performance Series. The Value Series supports basic event detection. The Performance Series supports advanced event detection.

Basic event

Basic events include Motion Detection, Privacy Mask, Video Tampering, Exception, Alarm Input/Output, Flash alarm, Audible alarm output, and ROI.

Advanced event

Advanced events include Human Body Detection, Intrusion Detection, Line Cross Detection, Loiter Detection, and People Gather Detection.

• Internet protocols

The camera supports TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, RTP, RTSP, NTP, SMTP, UDP, TCP, DNS, DDNS and other network communication protocols. Additional support includes ONVIF2.4, CGI, mainstream manufacturers agreement and other Internet protocols.

• Cloud storage function

All camera support cloud storage. Cloud storage allows the storage of recorded video and events to your choice of cloud storage providers. For now, the cameras support Google Drive and Dropbox for cloud storage.

Chapter 2: Operating instructions

2.1 Network Connections

2.1.1 Wired network connection

Connect the camera to the Local Area Network (LAN) via switch or a router as shown in Figure 2-1:



Figure 2-1

2.1.2 Wireless internet access

Some cameras support wireless network connectivity. Figure 2-2 shows a camera in a wireless network environment connected to a computer.



Figure 2-2

2.2 Detecting and Changing the IP Address

To access the IP address of a ClareVision camera, proceed as follows:

Step 1: Search for the cameras IP address.

Using the <u>IP Search Tool which can be downloaded from the Clare Help Center by following the ling HERE</u> or from the resources tab on the SnapAV device page, you can search for the online cameras on the LAN and display the IP, MAC address, version, port, and other information of the cameras, as shown in Figure 2-3:

SEARCH TOOL								₹	-	Ξ×	
Online	Device		Onvif MultimodelN	etmast 🕞 Import		O Refresh					
	Index	Model	Device Name	Firmware Ver	sion	IP Address	Subnet Mask	GateV	NetWork Param Upgr	ade	٦
	001	IPCAMERA	CLR-V200-8T28W	RV1126_IMX415_TKH0L1A3T1Q	0_W_A00036070_2	192.168.1.187	255.255.255.0	192.168.	IP Address		
	002	IPCAMERA	CLR-V100-4B36W	FH8856_K05_B1T1A1M0C0P1_	W_A00036070_21	192.168.1.100	255.255.255.0	192.168.	SubnetMask		
									GateWay		
								>	DNS		
									HTTP Port		
									RTSP Port		
									DHCP		
									SECURITY VERIFY		
									Password		
									Modify Forget Password		

Figure 2-3

Use the IP Search Tool to discover all available online devices found on the network.

Step 2: Modify the IP address of the IP camera and connect the computer to the same network segment.

In the IP Search Tool, select the camera IP address you would like to modify. On the right-side window, modify the IP address and gateway as needed and enter the camera password (by default, this password is the first 6 characters of the UUID unless it was changed before). Tap "**Modify**" to confirm changes.

Step 3: Open the web browser and navigate to the IP address of the camera and enter the camera login information into the web console.



IMPORTANT NOTES:

When setting the IP address of the camera, please keep the device IP address and the computer IP address on the same LAN segment.

DHCP is enabled by default for the cameras.

The default administrator username is "admin".

The default password is the **first six characters of the UUID** found on the camera, packaging box, and Quick Start Guide. You will be prompted to change the password once the default login information is entered.

2.3 Setting the Camera over the Wireless Access Network (WAN)

This section explains how to connect the camera to the WAN with a static IP or a dynamic IP.

2.3.1 Static IP Connection

Before you start:

Please apply a static IP address from an ISP (Internet Service Provider). With the static IP address, you can connect the camera via a router or connect it to the WAN directly.

Ensure the router is connected to the camera as shown in Figure 2-5:





Specific steps are as follows:

- 1. Connect the camera to the router.
- 2. Assign a LAN IP address, the sub net mask, and the gateway. For details, please refer to 7.3.1.
- 3. Save the static IP in the router.
- 4. Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to different routers. Please call the router manufacturer for assistance with port mapping.
- 5. Access the camera through a web browser.

2.3.2 Dynamic IP Connection

Before you start:

Please apply a dynamic IP from the ISP. With the dynamic IP address, you can connect the camera to a modem or router.

The router is connected to the camera:

- 1. Connect the camera to the router.
- 2. Assign a LAN IP address, the subnet mask, and the gateway. For details, please refer to 7.3.1.
- 3. In the router, set the PPPOE username, password and confirm the password.
- 4. Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary with different routers. Please call the router manufacturer for assistance with port mapping.
- 5. Apply a domain name from a domain name provider.
- 6. Configure the DDNS settings in the setting interface of the router.
- 7. Visit the camera via the applied domain name.

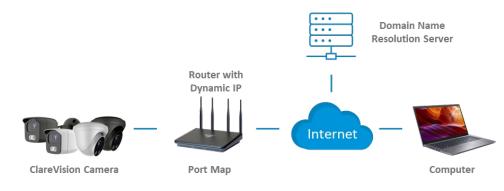


IMPORTANT NOTE:

The obtained dynamic IP address is assigned via PPPOE. The IP address will always change after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name

from the DDNS provider (E.g., DynDns.com). Please follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

Normal Domain Name Resolution as shown in Figure 2-5:

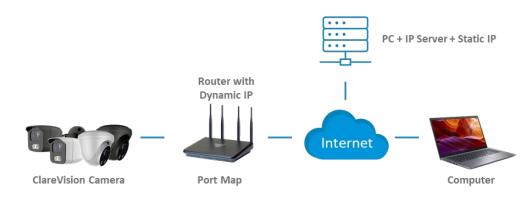




Specific steps are as follows:

- 1. Apply a domain name from a domain name provider.
- 2. Configure the DDNS settings in the DDNS Settings interface of the camera.
- 3. Visit the camera via the applied domain name.

Private Domain Name Resolution, as shown in Figure 2-6:





Specific steps are as follows:

- 1. Install and run the IP Server software in a computer with a static IP.
- 2. Access the camera through the LAN with a web browser or the client software.
- 3. Enable DDNS and select IP Server as the protocol type.

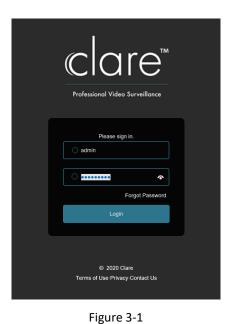
Chapter 3: Accessing ClareVision Cameras VIA Web Console

3.1 Login and Exit

3.1.1 Login

Open a browser (for optimal experience and to view video playbacks in the browser, Internet Explorer is recommended) on your computer and enter the camera IP address in the web address bar.

Enter "admin" for the username and the first six characters of the UUID for the password.





IMPORTANT NOTE:

If you have modified the IP address of the camera, please log in with the newly set IP address.

3.1.2 Change password

After a successful login, the interface will prompt you to change the password, as shown in Figure 3-2 and 3-3:

Tips 🔘 admin
The current password is too simple, please modify the
password!
Modify

Figure 3-2

IP Camera	Configuration		admin	⑦ Help	🗈 Logout
System	User Management				~
Security					
	Users to edit				
	Username	admin			
	User Type	Admin 🔽			
	Old Password	•••••			
	Modify Password				
	Password				
	Confirm Password				
	Do you want to set a new security	question			
	Security issue1				
	Answer1				
	Security issue2				
	Answer2				
	Security issue3				
	Answer3				
	key export				
	Save				
	IP Camera System Security	System User Management Security User So eat Username User	System User Management Security Users to set Users to set users to set Old Passeord users Old Passeord users Order Passeord users Do you want for its one security question users Society suited users Araser 2 users Araser 2 users Araser 3 users It properties to society problem and bort have the kap file, you need to refum the expegnentet to the factory.	System Lear Management Security Lear Note User how at non at non User how at non at non Old Passeord at non Old Passeord at non Order no associal guestion at non Do you want to be at non exoluting usetion at non Security issue1 at non Acces1 at non	System Let Management Security Let a latin User type Let a latin User type Let a latin Of Dissord Internet Baserd Internet

Figure 3-3

To change your password, follow these steps:

- 1. Enter the old password and enter the new password in the Password and Confirm Password fields.
- 2. Set security questions 1, 2, and 3, and enter the answers.
- 3. Click "**key export**" to save the key file to your computer. It is recommended to have the customer save this key file in their email or on their computer.
- 4. Click "Save" to complete the password modification.



IMPORTANT NOTE:

When setting a new password, you must set at least 8 characters and contain both letters and numbers.

3.1.3 Forgot password

If you forget your password, you can reset the password by using the security question verification or security key verification.

Security question verification

- 1. On the login interface, click "Forgot Password".
- 2. Select the verification method as "Security question validation" (as shown in Figure 3-4), enter the answers to security questions 1, 2, and 3, and click "Next"
- 3. Enter the new password and confirm the password (as shown in Figure 4-4) and click "Next".

U Verify Identity	Set New Password	Carry Out
Authentication Mode	Security question validation]
Security issue1]
Answer1		
Security issue2	¥	1
Answer2		
Security issue3		1
Answer3		
	Next Clear	

Figure 3-4

Verify Identity		Set New F		Carry Out	
	Set New Password Confirm Password	•••••			
		Next	Clear		

Figure 3-5

4. Click "Re-login" to return to the login interface (as shown in Figure 3-5).

Verify Identity	Set New Password	Carry Out
Dear user, the pass	word has been reset.Please click on " re-login "to ente	er the login interface
	re-login	

Figure 3-6

Security Key verification

- 1. On the login interface, click "Forgot Password".
- 2. Select the verification method as "Security Key Verification" (as shown in Figure 3-7) and click "Import" to import the key file exported when the password is modified.





3. Enter the new password and confirm the password (as shown in Figure 3-8) and click "Next".

Verify Identity		Carry Out			
	Set New Password Confirm Password	•••••			
		Next	Clear		



4. Click "Re-login" to return to the login interface (as shown in Figure 3-9).

Verify Identity	Set New Password	Carry Out
Dear user, the pas	ssword has been reset.Please click on " re-login "to enter	r the login interface
	re-login	

Figure 3-9



IMPORTANT NOTE:

When selecting "Security question validation", enter the correct answers to 2 questions to enter the "Set New Password" interface and proceed to the next step.

When setting a new password, you must set at least 8 digits and contain both letters and numbers to set it successfully.

A camera key file can be used multiple times to reset the password if you forget it.

3.1.4 Exiting Web Console

When you access the camera web console, you can quickly log out of the console by tapping on the "**Logout**" button in the top-right corner of the screen.

3.2 Install the necessary browser plugins

IMPORTANT NOTE:



When you use the IE browser, you need to download and install the prompted plugin.

The plugin of smart camera is "HsIPCCtl.exe".

Open Internet Explorer and log into the camera to be prompted to download and install the web plugin, as shown in Figure 3-10.

IP Camera Live View		Playback	Configuration	admin	⑦ Help	🔁 Logout		
💷 💷		Main Stream	Sub Stream	Tertiary Stream				
日	l e							Turn on/Sound off

Figure 3-10

Click "Please download the browser plugin here, please close the browser when the download is complete."

Do you want to run or save HsIPCCtLexe (1.85 MB) from 192.168.1.187?				×
It is type of file could harm your computer.	Run	Save	•	Cancel

Figure 3-11



IMPORTANT NOTE:

If the system prompts "Installation Failure", please uncheck the "Cancel Protection Mode" in the "Internet Options" security settings under Internet Options and enter the "Custom Level" ActiveX control Settings as show in Figure 3-12. Reinstall the plugin.

General Security Privacy Co	Enable Denable Orable Orable One of the second seco
🧶 🔩 🗸 🚫	Disable Enable (not secure) Prompt (recommended)
Internet Local intranet Trusted sites Restricted sites Internet This zone is for Internet websites, except those listed in trusted and restricted zones.	Download unsigned ActiveX controls (not secure) Disable (recommended) Enable (not secure) Prompt Initialize and script ActiveX controls not marked as safe for s Disable (recommended)
Allowed levels for this zone: Medium to High	Enable (not secure) Prompt
Appropriate for most websites Prompts before downloading potentially unsafe content	Only allow approved domains to use ActiveX without prompt Disable Enable
- Unsigned ActiveX controls will not be downloaded	< H
Enable Protected Mode (requires restarting Internet Explo	*Takes effect after you restart your computer
Custom level Default le	Reset custom settings
Reset all zones to default la	Reset to: Medium-high (default)

Figure 3-12

3.3 Main interface description

In the camera main interface, you can preview real-time video, playback, configure and use PTZ controls.

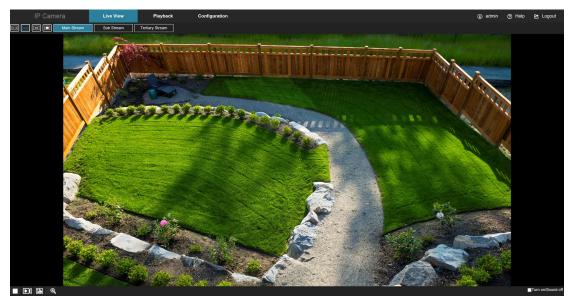


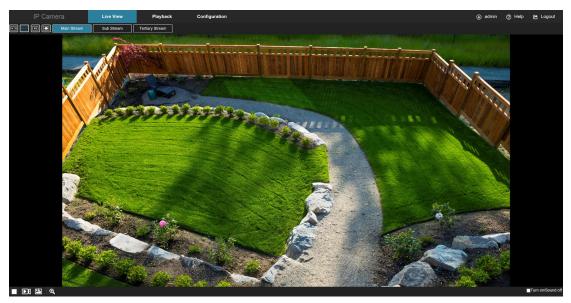
Figure 3-13

- [Live View] In the camera Live View, you can modify the aspect ratio, change the encoding (H.264, H.265 etc.), and capture video.
- [Playback] Playback live video or events stored on the camera memory card.
- **[Configuration]** All camera configuration parameters can be found under the Configuration tab.

Chapter 4: Live View

4.1 Live preview

Tap "Live View" to enter the camera live view interface, as shown in Figure 4-1:



- [Aspect Ratio Controls] In the real-time preview interface on the top left of the preview ratio option, click "4: 3", "16: 9", "X1", "Full Screen" to change the aspect ratio.
- [Stream Controls] You can access any of the streams (two or three depending upon the model) by selecting "Main Stream", "Sub Stream", and "Tri Stream"

Icon	Description
E:	The window size is 4:3.
×	The preview screen is displayed in its original size.
16:9	The window size is 16:9.
	Self-adaptive window size.
Main Stream Sub Stream Tertiary Stream	To switch the real-time preview stream (the mainstream is a high- definition stream, and the sub-stream is a standard definition stream).
	Start/Stop live view.
	Manually start/stop recording.
E1	Manually capture the picture.
Q	Turn on / off the electronic zoom function. To use the electronic zoom function in the preview image, hold down the left mouse button to select the electronic zoom area.
Open/Close Sound	Turn on/off Sound.

The preview interface operation buttons are shown in Table 5-1.

Table 4-2

4.2 Camera Settings, PTZ, Zoom, Cruise

Tap " I on the right side of the window to display the PTZ control interface. Tap " I to hide the PTZ control interface, where you can set the direction of the PTZ rotation of the camera, zoom in / out, focus - / focus +, one-key focus, lens initialization, cruise, as shown in Figure 4-3:

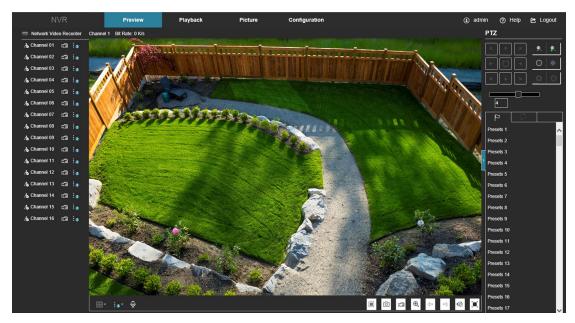


Figure 4-3

The PTZ control menu is shown in Figure 4-4 below:

ĸ	 ↑	7		
+	Ö	->	0	0
K	÷		$\eta_{q_{\rm R}^{\rm eq}}^{\rm eq}$	0

Figure 4-4

The PTZ control interface operation buttons are shown in Table 4-5 below.

k + × k + ×	Long press the arrow keys to control the horizontal and vertical direction, such as vertical rotation.		
	"Zoom-" and "Zoom +".		
2 R			
	"Focus-" and "Focus +".		
• •	• •		
8	One Key Focus.		

3	Init Camera.		
	Adjust the speed of rotation of the pan / tilt.		
Table 4-5			

Chapter 5: Playback

In the main interface, click "**Playback**" to enter the video playback interface. Playback video can be stored in the camera SD card for query, playback, and download operations as show in Figure 5-1:

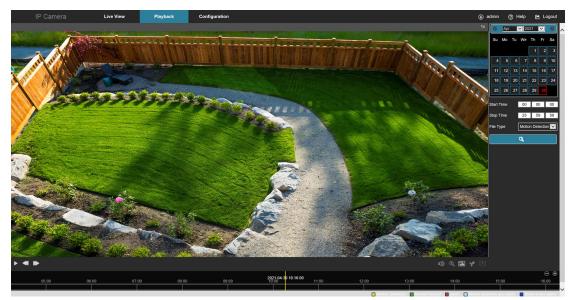


Figure 5-1

Here you can select the video type (ordinary video, event video) and time/date to retrieve the video or events of interest.

- [Play/Stop] After searching for the video, click " >" to start playing the video. Use the stop button " " to stop playing the video.
- [Slow Play/Fast Forward] When playing a video, click " I to slow down the video playback speed, click " I > " to speed up the video playback speed. See the upper right corner of the interface for the specific playback speed.
- [Drag and Drop] Use the timeline at the bottom of the video to move the video to the desired time in the time window.





Q



 $(\mathbf{+})$

F 1



[Prev Page] Click to switch to the previous page. •

• [Next Page] Click to switch the next page.



IMPORTANT NOTE:

This interface works with SD card storage only

Chapter 6: Configuration

Click "Configuration" to enter the local configuration interface. Here you can configure the camera system settings, network parameters, video and images settings, events, and more.

6.1 Local Configuration

In the main interface, click "Configuration \rightarrow Local Configuration" to enter the local configuration settings. Here you can set the "Record File Settings", "Picture and Clip Settings", "Export Configuration", and "Import Configuration" storage path. Change the path by selecting Browse, as shown in Figure 6-1.

Local Configuration			
Record File Settings			
Save record files to	C:\IPC\Record	Browse	
Save downloaded files to	C:\IPC\Download	Browse	
Picture and Clip Settings			
Save capture files in live view to	C:\IPC\Capture	Browse	
Save capture files when playback to	C:\IPC\PlaybackPics	Browse	
Save clips to	C:\IPC\PlaybackFiles	Browse	
Export Configuration			
Configuration Export Path	Export file		
Import Configuration			
Configuration Import Path	Import file		
Save			



- [Record File Settings] Set the path for the recorded video files.
 - \circ [Save record files to] Set the path for the manually recorded video files.
 - [Save downloaded files to] Set the path for the download files.
- [Picture and Clip Settings] Set the paths of the captured pictures and clipped video files. Valid for the pictures you captured with the web browser.
 - **[Save capture files in live view to]** Set the path of the manually captured pictures in live view mode.
 - [Save capture files when playback to] Set the path of the captured pictures in playback mode.
 - **[Save clips to]** Set the path of the clipped video files in playback mode.
- [Configure Export Path] Configure the storage path for camera export parameters.
- [Configure Import Path] Configure the storage path for the camera import parameters.

6.2 System

In the main interface, click "**Configuration** \rightarrow **System**" to enter the system configuration interface. The system consists of System Configuration, Scheduled Reboot, Log Query, and Security.

6.2.1 System Configuration

In the main interface, click "Configuration \rightarrow System \rightarrow System Configuration" to enter the system configuration interface.

	IP Camera	Live View	Playback	Configuration		
Ţ	Local Configuration		Time Settings	Dst	Maintenance	
	System	Basic Information				
	System Configuration					
	Scheduled Reboot	Device Name		CLR-V200-8T28W		
	Log Search	Firmware Version	H0L1A3T1Q0_W_A00036070_21.1			
	Security	Software Version		20.1.42.5		
63	Storage	Web UI version		21.1.03.210121		
۲	Network	Save				
	Video					
	Image					
١	Events					

Figure 6-2

Device Information

In the System Configuration interface, click "**Device Information**" to enter the device information configuration settings. Here you can view the basic information of the current camera, as shown in Figure 6-3:

Ţ	Local Configuration	Device Information	Time Settings	Dst	Maintenance
	Local Configuration				
	System	Basic Information			
	System Configuration	Device Name		CLR-V200-8T28W	
	Scheduled Reboot	Firmware Version		RV1126_IMX415_TKH0L	1A3T1Q0_W_A00036070_21.1
	Log Search	Software Version		20.1.42.5	
	Security	Web UI version		21.1.03.210121	
60	Storage				
0	Network	Save			
	Video				
	Image				
۱	Events				

Figure 6-3

- [Device Name] The name of the current camera.
- [Firmware Version] The current camera firmware version.
- [Software Version] The current software control version for the camera.
- [WEB UI Version] The current page version of the camera.

Time Settings

In the System Configuration interface, click "**Time Settings**" to enter the time settings interface, where you can set the device time, as shown in Figure 6-4.

Ţ	Local Configuration	Device Information	Time Settings	Dst	Maintenance	
	Local Configuration					
	System	Time Settings				
	System Configuration	Time Zone		GMT-05 Eastern Time (U	S & Canada), Indiana(East), Bogota, 🔽	
	Scheduled Reboot	Time Sync.				
	Log Search					
	Security	Time in Camera		2021-04-30 10:47:53		
Ð	Storage	O NTP				
۲	Network	SNTP Server		time.nist.gov	×	
	Video			time.nist.gov		
	Image	NTP auto-time		Off		
▣	Events	Time interval		0		mins
		Set Manually				
		Time Settings		2021-04-30 10	✓ 47 ✓ 51 ✓	
		Synchronize with cor	nputer time			
		Computer time		2021-04-30 10:47:53		
		NVR prohibit modifica	tion IPC Time			
		Save				

Figure 6-4

- [Time Zone] Displays the selected time zone.
- [Time in Camera] Displays the current device time.
- [NTP] Check to enable NTP synchronization.
- [SNTP Sever] Select the SNTP server address, including "time.windows.com", "time.nist, gov", "timenw.nist.gov", "time-a.nist.gov", "time-b.nist.gov".

- [NTP auto-time] Select to synchronize the time with the network time server. If this is "OFF", the camera will synchronize with the NTP server on bootup only.
- [Time interval] The time synchronization interval.
- [Set Manually] Manually overrides the camera time upon saving.
- [Synchronize with computer time] The camera will synchronize with the computer time and date.
- [NVR prohibit modification CAMERA time] Select this to block the NVR from updating the camera time.

DST

In the System Configuration interface, click "**DST**" to enter the daylight-saving time setting interface, where you can enable daylight saving time.





Maintenance

In the System Configuration interface, click "**Maintenance**" to enter the system maintenance settings interface, where you can restart the device, restore factory settings, manual upgrade, online upgrade, as shown in Figure 6-6.





- [Reboot System] Reboot the camera.
- [Default] There are two options: Simple recovery and Full recovery.
 - **Simple recovery:** resets all parameters EXCEPT network parameters to factory default.
 - Full recovery: resets all parameters INCLUDING network parameters to factory default.
- [Upgrade] Upgrade the firmware from a file located on your computer.

6.2.2 Scheduled Reboot

In the main interface, click "**Configuration** \rightarrow **System** \rightarrow **Schedule Reboot**" to enter the scheduled reboot settings interface, where you can set the period and time for the device to restart.



Figure 6-7

6.2.3 Log Search

In the main interface click on the "Configuration \rightarrow System \rightarrow Log Search" the log to search the camera log file.

P	Local Configuration						
=	System						
		ID 🔺	Time \$	Detail \$		Start Time :	
	System Configuration	1	2021-04-30 11:13:43	Motion Alarm	~	2021-02-01 00:00:00	1
	Scheduled Reboot	2	2021-04-30 11:12:20	Motion Alarm		End Time:	-
		3	2021-04-30 11:08:18	Motion Alarm			
	Security	4	2021-04-30 11:08:06	Motion Alarm		2021-04-30 23:59:59	1
B	Storage	5	2021-04-30 10:53:21	Motion Alarm			
	Siorage	6	2021-04-30 10:42:51	Motion Alarm		Search	
0	Network	7	2021-04-30 10:32:48	Motion Alarm			
	Video	8	2021-04-30 10:20:07	Motion Alarm		Clear	
	VIGEO	9	2021-04-30 10:18:30	Motion Alarm		Log export	
	Image	10	2021-04-30 10:17:26	Motion Alarm		Eog oxport	_
-		11	2021-04-30 10:16:23	Motion Alarm			
	Events	12	2021-04-30 10:16:11	Motion Alarm			
		13	2021-04-30 10:15:49	Motion Alarm			
		14	2021-04-30 10:15:39	Motion Alarm			
		15	2021-04-30 10:15:25	Motion Alarm			
		16	2021-04-30 10:14:38	Motion Alarm			
		17	2021-04-30 10:14:28	Motion Alarm	~		



- [Search] Set the date and start time of the log query, click "Search".
- [Clear] Clicking clear will clear the log search.
- [Log Export] Save the contents of the current log to the location you specified in txt format.

6.2.4 Security

In the main interface, click "**Configuration** \rightarrow **System** \rightarrow **Security**" to enter the user management settings interface, where you can add, edit, delete a user. You can also query the current user information. The admin user must be used to add users. You can add up to 10 users.

Ţ	Local Configuration	User Management			
	System	Username	User Role	Edit	Delete
	System Configuration	admin	Admin	Edit	
	Scheduled Reboot				
	Log Search				
61	Storage				
\odot	Network				
	Video				
	Image				
▣	Events				
				Ad	d User

Figure 6-9

Adding a User

- 1. Click "Add User" to add a user.
- 2. Input the Username, select "User Type" and input Password.
- 3. Click "**OK**" to complete.

Add User as shown in Figure 6-10.

Users to ed	lit			×
Use	rname Richard			
Use	r Type Admin	×		
Pa	esword			
Confirm Pa	esword			
	ок	Ca	ncel	
	Add	User		

Figure 6-10



IMPORTANT NOTE:

The admin user cannot be deleted, and you can only change the admin password.

User permission descriptions:

Administrator: All permissions.

Operator: All permissions (cannot make system security parameter settings).

Viewer: Only preview permission.

When setting the camera password, the password length is 8-31 characters and must contain numbers and letters.



IMPORTANT NOTE:

When modifying the administrator password, after setting the security question, click "**Browse**" to select the path, and click "**Export**" to export the key file, so that the password can be reset if the

password is forgotten.

After modifying the administrator password, when the PC and the camera are on the same LAN segment, click "**Forget**" to reset the password by answering the security question or importing the key.

When you change your password again, you do not have to set a new security question. When you forget your password, you can reset it with the last security question you set.

Edit the User

- 1. In the user list, select the user to be modified, and click "Edit" to enter the user editing interface.
- 2. Edit the user type or password, enter the confirm password.
- 3. Click "**OK**" to finish editing the user.

Delete Users

1. Click to select the user you want to delete and click "Delete".

2. Click "**OK**" on the pop-up dialogue box to delete the user.

6.3 Storage

6.3.1 Plan configuration

Rec Setup

1. In the main interface, click "**Configuration** → **Storage** → **Plan Configuration** → **Rec Setup**" to enter the recording setting interface, as shown in Figure 6-11

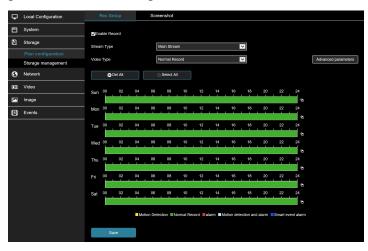


Figure 6-11

- 2. To enable record, select the stream type (Main Stream, Sub Stream, Tri-Stream), video type (Normal Record, Motion Detection, Alarm, Motion detection and alarm).
- 3. Set the recording time period.
 - **Method 1**: Click the arming time period, manually fill in the start time and end time, set up and click Save. If you need to delete the time period, click the "**Delete**" button and then reset the time period.
 - **Method 2**: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.
- 4. Repeat step 3 to set up a complete recording plan.
- 5. Click "Save" to complete the setting of the arming time.

You can set up more than one time period for up to 8 time periods.

"Select All" to enable 24/7 recording.

"Select all" to enable 24 hours of daily video recording throughout the week.

This feature requires an onboard SD card.

IMPORTANT NOTE

- [Stream Type] Select to set the stream type of recording, including Main Stream, Sub Stream, Tri-Stream.
- [Video Type] Including Normal Record, Motion Detection, Alarm, Motion Detection and Alarm.
- [Advance parameters] You can set the Pre-recorded time (Unlimited, 10s, 15s, 20s, 25s, 30s) and Video delay (5s, 10s, 30s, 1 min, 2 min, 5 min, 10 min), as shown in Figure 6-12.

<u>Yideo Type</u>	Normal Pacard	
Advanced parameters		×
✓Loop write		
Pre-recorded time	55	3
Video delay	10S	
		3
	ОК	Cancel





IMPORTANT NOTE

The pre-recording time and recording delay can be used for motion detection recording, alarm recording, motion detection and alarm recording.

Screenshot

The snapshot is used to set the relevant parameters such as the image format, resolution, and capture interval

1. In the main interface, click "**Configuration** → **Storage** → Plan **configuration** → **Screenshot**" to enter the screenshot parameter setting interface, as shown in Figure 6-13.

Ţ	Local Configuration	Rec Setup	Scree	nshot		
	System	Snapshot parameters				
6	Storage	Image Format	JF	PEG		$\mathbf{\mathbf{x}}$
	Storage management	Resolution	19	920*1080		
\odot	Network	Event trigger				
	Video	Enable event snapsho				
*	Image	Interval time	10)S		>
▣	Events	Number of screenshots	1			
		Save				

Figure 6-13

- 2. To enable event snapshot, select the image format, resolution, snapshot interval, and number of snapshots through the drop-down box.
- 3. Click "Save" to complete the configuration.

6.3.2 Storage management

Storage

In the main interface, click "**Configuration** \rightarrow **Storage** \rightarrow **Storage management** \rightarrow **Storage**" to enter the SD Card management settings interface. Here you can view the SD card related information and format the SD card as shown in Figure 6-14:

Ţ	Local Configuration	St	torage	Cloud Storage		
	System	Memory of	ard type	SD Card		
63	Storage		Status \$	Total Capacity \$	Residual Capacity \$	Device Type \$
	Plan configuration		Using	30417MB	26368MB	SD Card
\odot	Network					
	Video					
	Image					
▣	Events					
						Format



SD card format steps are as follows :

- 1. Select the disk to be formatted, click "Format".
- 2. Click "**OK**".
- 3. Wait for the format to complete then verify Total Capacity = Residual Capacity

Cloud Storage

When the device triggers an alarm, you can store the alarm picture taken by the device on a cloud server.

Prerequisites:

- You need to have a Google or Dropbox cloud storage account.
- To use this function, the device must be connected to the external network.
- In the main interface, click "Configuration → Storage → Storage Management → Cloud Storage" to enter the cloud storage configuration interface, as shown in Figure 6-15.

Ţ	Local Configuration	Storage	Cloud Storage	
	System	Cloud		
60	Storage	Cloud Storage Type	None	Not connected
	Plan configuration	Web		
		Auth Code		
\odot	Network	Username		
	Video	Total Capacity		
	Image	Used Capacity		
۵	Events	Bind		
		IPEYE		
		Enable IPEYE		
		Save		

Figure 6-15

2. Select the cloud storage type, such as "Google Drive" or "Dropbox".

- 3. Follow the prompts to log into the website with a browser on the computer to obtain the "Verification Code".
- 4. Enter the verification code in the "Auth code" field of the cloud storage interface.
- 5. Click "Bind".
 - **[Cloud Storage Type]** Select the cloud storage type: Dropbox or Google Drive in the drop-down menu.
 - [Auth Code] Enter the authorization code provided by the web service.

Click on the "Bind" after the success. "Username", "Total Capacity" and "Used Capacity" that information will be automatically displayed.

6.4 Network

6.4.1 Basic Setup

TCP/IP

The TCP/IP interface is used to view and configure network parameters such as the camera's IP address. You can enable DHCP or manually modify the camera network parameters. DHCP is ENABLED by default.

Enable DHCP:

Connect the camera to a router with DHCP enabled. The camera will obtain the corresponding IP address, subnet mask, default gateway, and preferred DNS server information.

The specific steps for manually modifying network parameters are as follows:

 In the main interface, click "Configuration → Network → Basic Setup → TCP / IP" to enter the TCP / IP interface, as shown in Figure 6-16.

Ţ	Local Configuration	TCP/IP	Port	
	System	NIIO 0-41		
Ð	Storage	NIC Settings		
\odot	Network	IPv4 Address	✓DHCP 192.168.1.187	Image: Second
	Basic Setup	IPv4 Subnet Mask	255.255.255.0	
	Advanced Setup	IPv4 Default Gateway	192.168.1.1	 Ø
	Video		192.100.1.1	`
	Image	DNS Server		
	Events	Preferred DNS Server	192.168.1.1	S
		Save		

Figure 6-16

- 2. Set the IP address, subnet mask, gateway, and DNS.
- 3. Click "Test" to make sure the modified IP address is available in the LAN.
- 4. Click "Save" to save the configuration.

Port

In the main interface, click "**Configuration** \rightarrow **Network** \rightarrow **Basic Setup** \rightarrow **Port**" to enter the port setting interface, where you can set the camera network port and protocol port. The network port has:

- HTTP port (default is 80)
- RTSP port (default is 554)
- HTTPS port (default is 443)

Protocol Ports include:

- ONVIF port (enabled default is 8999)
- HIK port (default is 8000)
- XM port (default is 34567)

See Figure 6-17.

Ţ	Local Configuration	TCP/IP	Port
	Local Configuration	-	
	System	Port	
	System Configuration	HTTP Port	80
	Scheduled Reboot	RTSP Port	554
	Log Search	HTTPS Port	443
	Security	Protocol Port	
61	Storage		
	Plan configuration	ONVIF Port	8999
	Storage management	HIK Port	8000 Enable HIK Protocol
\odot	Network	XM Port	34567 Enable XM Protocol
	Basic Setup	Save	
	Advanced Setup		

Figure 6-17

6.4.2 Advanced Setup

In the main interface click on the "**Configuration** \rightarrow **Network** \rightarrow **Advance Setup**" to enter the advanced configuration interface. Here, you can set the device DDNS, FTP, SMTP, P2P, PPPOE and other functions.

DDNS

After the DDNS (Dynamic Domain Name Server) parameter is set, when the IP address of the camera changes, the system can dynamically update the relationship between the domain name and the IP address on the DNS server. You can use the domain name to access the camera directly without recording the changing IP address.

Prerequisites:

Before configuring DDNS settings, make sure that the device supports the type of domain name resolution server, and log in to the DDNS service provider's website to register a username, password, domain name, and other information on the PC.

In the main interface, click "Configuration → Network → Advance Setup → DDNS" to enter the DDNS function settings screen, as shown in Figure 6-18:

Ţ	Local Configuration	DDNS	FTP	SMTP	P2P	Other	PPPOE
	System	DDNS					
60	Storage						
٢	Network	DDNS DDNS Type	Oray	~	1		
	Basic Setup	Site Name			1		
		DDNS User			Ī		
	Video	DDNS Password					
F	Image	Confirm Password					
١	Events	Status	Login failed				
		Service Type	Ordinary User				
		Links to service providers					
		Save					

Figure 6-18

- 2. Enable DDNS, select the DDNS type, and enter the username, password, and site name.
- 3. Click "**Save**" to save the configuration.
- 4. Enter the domain name in the PC web browser and press "**Enter**". If you can display the web interface of the device, the configuration is successful. If it is not displayed, the configuration failed.



IMPORTANT NOTE

Access via DDNS domain requires internet access.

FTP

Use FTP service to store alarm pictures.

Prerequisites:

You need to purchase or download the FTP service tool and install the software on your PC.



IMPORTANT NOTE:

To create an FTP user, you need to set the FTP folder write permission, otherwise the image will not be uploaded successfully.

 In the main interface, click "Configuration → Network → Advance Setup → FTP" to enter the FTP server settings interface, as shown in Figure 6-19.

Ţ	Local Configuration	DDNS	FTP	SMTP	P2P	Other	PPPOE
	System						
£	Storage	FTP				•	
0	Network	FTP Server Port	192.168.1.1		Test	J	
	Basic Setup	Usemame	admin		Anonymous		
		Password	••••				
	Video	Confirm Password	••••				
E	Image	FTP Server Upload Direct	-				
١	Events	Automatically Overwrite	When Server Full				
		Save					
		Save					

Figure 6-19

- 2. Enter the server address, port, username, password, password, file upload path, check "Auto Cover", and select to upload the FTP server file format AVI or JPEG.
- 3. Click "Save" to save the configuration.
- 4. Click "**Test**" to confirm whether the network connection and FTP configuration are correct.



IMPORTANT NOTE:

If the test fails, please recheck the network or FTP configuration.

SMTP

Enabling SMTP allows the camera to send alarm information to an email address.

 In the main interface, click "Configuration → Network → Advance Setup → SMTP" to enter the mail settings interface, as shown in Figure 6-20.

Ģ	Local Configuration	DDNS	FTP	SMTP	P2P	Other	PPPOE
	System	Sender					
B	Storage						
٩	Network	Sender SMTP Server	user@domain.com smtp.domain.com		_		
	Basic Setup	Port	25				
		Upload Via SMTP	Message		\sim		
D	Video	Authentication required					
	Image	Username	user@domain.co	n			
▣	Events	Password	•••••				
u=u	Lvents	Confirm Password	•••••				
		Email recipient(s)					
		Email 1	user@domain.co	n	Test)	
		Email 2			Test]	
		Email 3			Test]	
		Save					

Figure 6-20

- 2. Configure Sender, SMTP Server, Port, Username, Password, and Receiver.
- 3. Click "Test" to confirm whether the network connection and SMTP configuration are correct.
- 4. Click "**Save**" to save the configuration.

Sender

- [Sender] Enter the full address of the sender mailbox.
- [SMTP Server] Enter your email server address.
- [Port] Enter your email server port.
- [Upload Via SMTP] In the drop-down menu, select SMTP file format, JPEG image format, AVI video and message for selection.
- [Alarm Duration] Set the sending interval.
- [My Server Requires Authentication] When enabled, the server and user are authenticated to ensure that the data is sent to the correct client and server.
- [User Name] Enter the send mailbox user name.
- **[Password]** Enter the send mailbox password.
- [Confirm Password] Enter the send mailbox password.

6.5 Video

In the main interface, click "**Configuration** \rightarrow **Video**" to enter the video and audio configuration interface, where you can set the device video, audio, and other functions.

6.5.1 Video

In the main interface click "**Configuration** \rightarrow **Video** \rightarrow **Video**" into the video configuration interface, where you can set the camera device name, stream type, encoding and other video parameters, as shown in Figure 6-21.

Ţ	Local Configuration	Video			
	System	Stream Type	Main Stream	~	1
£	Storage				1
\odot	Network	Profile	Main Profile	×	1
		Video Encoding	H.264	×	
	Video	Resolution	2560x1440	×	
		Framerate	15	V	fps
	Audio	Tuniciate] '93
	Image	Bit Rate	4096		
▣	Events	Rate Control	VBR	×]
		I-Frame Interval	75		
		H264+	off]
		Watermark	Off	~	
		Watermark name			
		Save			



- [Stream Type] Default is the Main Stream, you can select Sub Stream or Tri-Stream.
- [Profile] Default is the Main Profile; you can select Basic Profile or High Profile.
- [Video Encoding] Switch the encoding method in the drop-down menu.
- **[Resolution]** Switch the output resolution in the drop-down menu.
- [Framerate] Set the frame rate of the current output video of the device.
- [Bit Rate] Support 64-12000kbps. A higher the bit rate equates better video quality but consumes the greater network bandwidth.
- [Rate Control] Set to variable or fix bit rate.
- [I-Frame Interval] Camera acquisition key frame interval
- [H265+/H264+] Turn on/off the camera H265+/H264+.
- [Watermark] Turn on/off the watermark function. It can prevent the video from being tampered after it is turned on.
- [Watermark name] Enter a watermark name.

6.5.2 Audio

In the main interface, click "**Configuration** \rightarrow **Video** \rightarrow **Audio**" to enter the audio configuration interface where you can set the device audio input mode, select the audio code, and set the input volume as shown in Figure 6-22.

Ţ	Local Configuration	Audio Configuration	
	System	✓Enable Audio	
60	Storage	_	
0	Network	Audio input Audio Encoding	Mic input
	Video	Volume	
	Video		
		Input volume	50
	Image		
۵	Events	Save	

Figure 6-22

- [Audio Enable] Turn on / off device audio input.
- [Audio Input] Select the audio input method.
- [Audio Output] Select the audio output method.
- [Audio Encode] Choose audio encoding, G711U/ G711A /AAC.
- [Input Volume] Set the device input volume.
- [Output Volume] Set the device output volume.

6.6 Image

In the main interface, click "**Configuration** \rightarrow **Image**" to enter the image configuration interface. Here you can control the device image settings and OSD text.

6.6.1 Image

In the main interface, click "**Configuration** \rightarrow **Image** \rightarrow **Image**" to enter the image configuration interface, where you can adjust the related image parameters such as Image Adjustment, Exposure Settings, Focus, Backlight Settings, Day and night switch, White Balance, Video Adjustment, Image Enhancement, Defog Mode, Distortion, and Image rotation as shown in Figure 6-23.

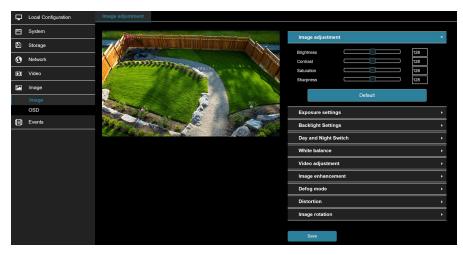


Figure 6-23

• [Image adjustment] You can manually set brightness, contrast, saturation, sharpness. The scope of valid values is from 0 to 255, you can drag the slider to set, and the default value is 128, as shown in Figure 6-24.

Image adjustment		-
Brightness Contrast Saturation Sharpness	Default	128 128 128 128
Exposure settings		•
Backlight Settings		•



• **[Exposure settings]** The default is automatic exposure. To set specific exposure settings, select Manual, and the Exposure Time and Gain Control is activated, click "**Save**". As shown in Figure 6-25

lmage adjustme	nt	×
Exposure settin	gs	•
Exposure settings Exposure time Automatic gain Gain Control	Auto Manual 1/25 125 128	
Backlight Settin	gs	•
Day and Night S	witch	•

Figure 6-25

 [Backlight Settings] Used to set backlight compensation and strong light suppression. The default is OFF, it can be turned on manually, allowing backlight, strong light suppression intensity, and dark area boost strength settings to be configured, as shown in Figure 6-27.

Exposure settings		•
Backlight Settings		
Backlight Compensation	O Off On	
Backlight	min	
Strong light suppression	O Off On	
Strong light suppression intensity		0
Dark area boost strength		0
Day and Night Switch		Þ
White balance		•



[Day and night switch] The fill light mode defaults to automatic with sensitivity set to 3. Filter time is 3 seconds, light mode is manual, light brightness is 100, as shown in Figure 6-28. When the fill mode is "Automatic", the device will turn on the fill light according to the actual environment. The user can switch the fill mode to "Daytime ", "Night" and "Time" according to the actual environment of the site and switch the sensitivity and filter time of the device according to the fill mode.

Backlight Settings		×
Day and Night Switch		-
Fill light mode	automatic	
Sensitivity	3	
Filter time	3	
light brightness	1/	00
White balance		×
Video adjustment		×

Figure 6-28

- **Time:** set the time the camera will switch into and out of night mode.
- **Daytime:** camera will not enter night mode.
- Night: camera will enter night mode.
- **Filtering time:** sets the time period the camera will use to determine it needs to switch modes.
- Light brightness: It is used to adjust the brightness of the fill light. The adjustable range is 0-100.
- [White balance] Default auto, switchable Manual, Fluorescent Lamp, Incandescent, Warm Light, Natural Light, as shown in Figure 6-29.

Day and Night	Switch			•
White balance				-
White balance Red gain Green gain Blue gain	Auto		128 128 128	
Video adjustme	ent			×
Image enhance	ement			•

Figure 6-29

- Manual White Balance: Use manual adjustment to adjust Red, Green, Blue gain controls.
- [Video adjustment] Here you can turn on and set 2D or 3D digital noise reduction, as shown in Figure 6-30.

White balance)	×
Video adjustn	nent	-
DNR model 2D 3D	off 32 32	
Image enhand	ement	×
Defog mode		۰.

Figure 6-30

• [Image enhancement] Including flicker control, wide dynamic switch, HDR, as shown in Figure 6-31.

Video adjustment		×
Image enhancement		-
Flicker control Sensor linear WDR	NTSC(60HZ)	
Defog mode		×
Distortion		×



- **Flicker control:** The flash mode is selected according to the camera installation environment and the flicker standard. The default setting is NTSC (60HZ).
- Sensor linear WDR: The default is Shut Down (off). You can switch select: Automatic, Weak, Moderate, Strong, Super.
- [Defog mode] Used to set the defog mode and strength, as shown in Figure 6-32.

Image enhancement		×
Defog mode		-
Defog mode Defog strength	Off 0	
Distortion		×
Image rotation		•



- **Defog Mode:** The default is off; you can choose from the drop-down menu to On or Auto.
- **Defog Strength:** The default is 0, when the fog mode is open, you can set the fog strength, can be set to a value range of 0-255.

• [Distortion] Used to set image distortion correction, as shown in Figure 6-33.

Defog mode		•
Distortion		-
Distortion mode Distortion intensity	Off	128
Image rotation		•



- **Distortion mode:** The default is OFF. You can select ON from the drop-down menu.
- **Distortion intensity:** The default is 128. When the distortion mode is on, the distortion correction strength can be set, and the value range can be set from 0-255.
- [Image rotation] Used to set image mirroring and corridor pattern, as shown in Figure 6-34.

Image rotation		-
Mirroring	off 🛛 🔽	
Corridor Pattern	off 🛛 🗹	



6.6.2 OSD

The OSD is information displayed on the real-time monitoring screen. The name, date, and day of the camera can be displayed on the monitor screen.

In the main interface, click "**Configuration** \rightarrow **Image** \rightarrow **OSD**" to enter the OSD configuration interface where you can set the preview interface to display time, OSD text and other information, as shown in Figure 6-35.





- [Time] Turn on / off the preview interface time display.
- **[Text]** Turn on / off the preview interface OSD text display.
- **[Date Format]** Set the preview interface to display the date format, default day / month / year, switchable month / day / year, and year / month / day options.
- **[OSD Position]** Set the preview interface to display the time or OSD text position, the default is the Top Left You can switch the Bottom Left.

• [OSD Text] Enter the preview interface to display text information

6.7 Events

In the main interface, click "**Configuration** \rightarrow **Events**" to enter the event configuration interface including basic events and smart events.

6.7.1 Ordinary Events

In the Ordinary event interface, you can set the device's Motion Detection, Privacy Mask, Video Tampering, Alarm Input, Alarm Output, Exception, Flash alarm, Audible alarm output, ROI, and other events.

Motion Detection

The motion detection function is used to detect whether there is a moving object in a certain area within a certain period of time. When there is a moving object, the camera will alarm according to the setting.

 In the main interface click on the "Configuration → Events → Motion Detection" to enter the motion detection settings interface, as shown in Figure 6-36.

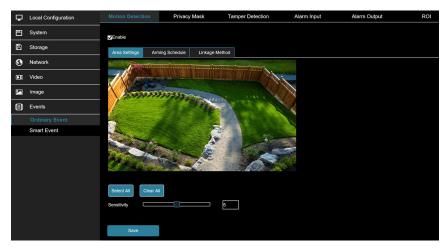


Figure 6-36

- 2. Click "Enable" to turn on the motion detection alarm.
- 3. Select the area to set the motion detection sensitivity, click "Save".
 - [Select All] Motion detection range to monitor all of the area, which consists of 396(22*18) squares.
 - [Manually draw the alarm area] Move the mouse to the preview screen, click the left mouse button to select the range of motion detection, release the left mouse button to complete the alarm area selection. A camera can select multiple motion detection zones at the same time.
 - [Clear All] Clears all the motion detecting area that selected currently.
 - **[Sensitivity]** The default is 5 with a range of 0-10. The larger the value, the more sensitive the camera will be to motion.
- 4. Set the arming schedule.

As shown in Figure 6-37, you can view, edit, and delete the arming time of motion detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

You can set up more than one time period for up to 8 time periods.



After the day of deployment time is set, the other time also need to set the same.

Figure 6-37

5. Set the linkage method.

Alarm linkage methods include general linkage (Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning) and linkage alarm output (IO Output), as shown in Figure 6-38.

- **[Upload Via SMTP]** Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.
- **[Upload Via FTP]** Select and the system is configured with the FTP server, will send the alarm information to the FTP server.
- **[Upload Via Cloud]** Select and the system is configured with the cloud server, will send the alarm information to the cloud account.
- o [Flash Warning] After selection, the device will link the alarm light to flash when alarming.
- **[IO Output]** Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

✓Enable								
Area Settings	Arming Schedu	e	Linkage Method					
General Linkage			Linkage Alarm Output					
Upload Via SMTP			Output					
Upload Via FTP								
Upload Via Cloud								
Save								

Figure 6-38

Privacy Mask

Privacy function is a privacy protection feature that blocks a portion of the camera view from being viewed and recorded.

In the main interface, click "**Configuration** \rightarrow **Event** \rightarrow **Privacy Mask**" to enter the privacy mask settings interface. As shown in Figure 6-39.





Here you can choose up to 3 privacy areas. Hold down the left mouse button and drag to select the area in the area. Region 1, Region 2, and Region 3 will show the corresponding coordinates, width, and height of the region. If you want to delete a region, click on the corresponding "**Delete**" button. Click on the "**Save**" after completing the setting.

Video Tampering

The occlusion alarm function is used to detect whether a monitoring area is blocked by human factors and other factors during a certain period of time. When the area of the device is blocked, the camera will alarm according to the settings. When the occlusion alarm is generated, the occlusion alarm cause can be quickly discharged, and the monitoring screen can be restored.

In the main interface click on the "Configuration → Events → Video Tampering" to enter the video tampering settings interface, as shown in Figure 6-40.

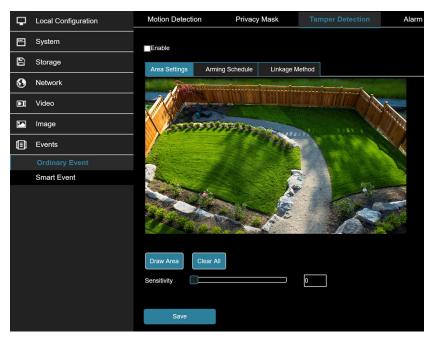


Figure 6-40

- 2. Click "Enable" to turn on the video tampering alarm.
- 3. Set the video tampering sensitivity, click "Save".
 - [Drawing Area] Move the mouse to the preview screen, click the left mouse button to select the range of motion detection, release the left mouse button, click "Stop Drawing" to complete the alarm area selection.
 - [Clear All] Clearing all the video tampering area currently selected.
 - **[Sensitivity]** The default is 0, can switch the range of 0-2, the greater the value of the more sensitive equipment alarm.
- 4. Set the arming schedule.

As shown in Figure 6-41, you can view, edit, and delete the arming time for video tampering. The default is 0 arming 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

You can set up more than one time period for up to 8 time periods.

After the day of deployment time is set, the other time also need to set the same.

Are	a Set	tings	\$	A	ming	Sch	nedule	e	Li	nkaç	ge Me	thod													
	6	De	I All					@ S	Select	All															
Sun	00	_1	02		04		06		08		10		12		14		16		18		20		22	24	0
Mon	00		02		04		06		08 I		10 '		12		14		16 '		18 '		20 1		22 1	24	
Tue	00		02 I		04		06	,	08 I		10 1		12 1	,	14	,	16 1		18 1		20 1	,	22	24	
Wed	00	1	02		04		06		08	1	10 1	1	12		14		16 1		18 1		20	1	22	24	Ū.
Thu	00	-	02	_1_	04		06	_	08 I	_1	10 1	_	12		14		16 1		18 1		20 I	_1	22	24	Ū,
Fri	00	1	02	1	04 1	1	06 I		08	1	10 '	1	12		14		16 1	-1	18 1	,	20	1	22	24	0
Sat	00		02	-	04		06	-	08		10 '	-	12		14		16 '	-	18 '	•	20		22	24	Ð,
		Save																							

Figure 6-41

5. Set the linkage method.

Alarm linkage methods include general linkage (Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning) and linkage alarm output (IO Output), as shown in Figure 6-42.

Enable						
Area Settings	Arming Schedu	le	Linkage Method			
General Linka	ge		Linkage Alarm Output			
Upload Via SM	/TP	Output				
Upload Via FT	P					
Upload Via Cl	bud					
Save						



- **[Upload Via SMTP]** Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.
- [Upload Via FTP] Select and the system is configured with the FTP server, will send the alarm information to the FTP server.
- **[Upload Via Cloud]** Select and the system is configured with the cloud server, will send the alarm information to the cloud account.
- [Flash Warning] After selection, the device will link the alarm light to flash when alarming.
- **[IO Output]** Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

Alarm Input Prerequisites

Before configuration, the device needs to be connected to the alarm input device. By configuring the alarm input, the alarm signal received by the alarm input device can be passed to the camera for further processing.

- In the main interface click on the "Configuration → Events → Alarm Input" to enter the Alarming Input settings interface.
- 2. Select the alarm input and alarm type (Normally open, Normally closed).
- 3. Set the arming schedule.

As shown in Figure 6-43, you can view, edit, and delete the arming time of the alarm input. The default is 0 arming 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

You can set up more than one time period for up to 8 time periods.

After the day of deployment time is set, the other time also need to set the same.

Ţ	Local Configuration	Motion Dete	ection	Privacy M	lask	Tampe	r Detectio	on		arm Inpu		Alarm Output	ROI
	System	Alarm Input											
63	Storage	Alarm type	Normally oper	1									
٢	Network	Arming Sche	edule Linka	age Method									
	Video	8 De	el All	Se	lect All	1							
5	Image					J							
۵	Events	Sun ⁰⁰	02 04	06	08 10	12	14	16	18	20	22	24 0	
		Mon ⁰⁰	02 04	06	08 10	12	14	16	18	20	22	24	
	Smart Event												
		Tue ⁰⁰	02 04	06	08 10	12	14	16	18	20	22	24	
												•	
		Wed 00	02 04	06	08 10	12	14	16	18	20	22	24	
		Thu ⁰⁰	02 04	06	08 10	12	14	16	18	20	22	24	
						. ï.	-ï-i			للتب		-Т.	
		Fri ⁰⁰	02 04	06	08 10	12	14	16	18	20	22	24	
												o	
		Sat 00	02 04	06	08 10	12	14	16	18	20	22	24	
												o	
		Save	e										

Figure 6-43

4. Set the linkage method.

Alarm linkage methods include general linkage (Upload Via SMTP, Upload Via FTP, Upload Via Cloud, Flash Warning) and linkage alarm output (IO Output), as shown in Figure 6-44.

v
· Method
Linkage Alarm Output
O Output



- **[Upload Via SMTP]** Select and the system is configured with SMTP, the alarm information will be sent to the SMTP recipient mailbox.
- [Upload Via FTP] Select and the system is configured with the FTP server, will send the alarm information to the FTP server.
- [Upload Via Cloud] Select and the system is configured with the cloud server, will send the alarm information to the cloud account.
- [Flash Warning] After selection, the device will link the alarm light to flash when alarming.
- **[IO Output]** Select and the IO output port is connected to the alarm device. During the alarm, the device will link the device to alarm.

Alarm Output

Prerequisites

Before configuration, the device needs to be connected to the alarm output device. By configuring the alarm output, the alarm signal received by the alarm input device can be passed to the camera for further processing.

- In the main interface click on the "Configuration → Events → Alarm Output" to enter the Alarming Output settings interface.
- 2. Set the delay time.
- 3. Set the arming schedule.

As shown in Figure 6-45, you can view, edit, and delete the arming time of the alarm input. The default is 0 arming 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the arming time period, two arrows will be displayed at both ends of the time period. Move the adjustment arrow left or right to adjust the arming time.

You can set up more than one time period for up to 8 time periods.

4. Click "Save" to complete the setting of the arming time.

₽	Local Configuration	Motion Detection	Privacy Mask	Tamper Detection	Alarm Input	Alarm Output	ROI
8	System	duration 10S	V				
8	Storage	Arming Schedule					
٢	Network						
	Video	🛿 Del All	C Select All				
	Image	Sun 00 02 04	06 08 10	12 14 16	18 20 22	24	
۵	Events	Mon 00 02 04	06 08 10	12 14 16	18 20 22	© 24	
	Ordinary Event					_ •	
	Smart Event	Tue 00 02 04	06 08 10	12 14 16	18 20 22	 24 	
		Wed 00 02 04	06 08 10	12 14 16	18 20 22	0 24 	
		Thu 00 02 04	06 08 10	12 14 16	18 20 22	@ 	
		Fri 00 02 04	06 08 10	12 14 16	18 20 22	0	
		Sat 00 02 04	06 08 10	12 14 16	18 20 22	 24 	
		Manual alarm	Save				

Figure 6-45

• **[Manual alarm]** Manually control the alarm output device on the alarm output interface to link the alarm.

ROI

ROI is the area of interest setting, users can set the most important area in the video screen through this function. When used the camera will improve the video image quality of the corresponding area when video encoding and reduce the encoding quality of other areas,

 In the main interface, click "Configuration → Events → ROI" to enter the ROI setting interface, as shown in Figure 6-46.





- [Region Settings] Move the mouse to the preview screen, hold down the left mouse button to select the ROI area range, and release the left mouse button to complete the area drawing. You can also enter the X, Y, W, and H corresponding positions in the corresponding area to set the area.
- 3. [Set "Relative QP value" or "Absolute QP value"] Select "Relative QP value" or "Absolute QP value" in the corresponding area position and enter the corresponding value.
- 4. Slide the scroll bar to set the frame rate of the Non-ROI region.
- 5. Click "Save" to complete the ROI setting.



IMPORTANT NOTE:

The ROI configuration is more effective when using a lower non-ROI frame rate setting

Click "Delete" in the corresponding setting area to delete the corresponding ROI area.

6.7.2 Smart Event

Smart event interface, which can set face recognition, intrusion detection, line cross detection, loiter detection and people gather detection.

Intelligent Detection

The face recognition function is used to detect the face appearing in the face database in the monitoring screen, and to perform frame selection tracking on the monitoring interface. The specific operation steps are as follows:

 In the main interface click on the "Configuration → Events → Smart Event" to enter the Face Recognition settings interface, as shown in Figure 6-47.

	IP Camera	Live View	Playback	Configuration		
Ţ	Local Configuration	Intelligent detection	Intrusion Detection	Line Cross Detection	Loiter Detection	People Gather Detection
8	System	Detection mode off	Y			
63	Storage					
٩	Network	Save				
	Video					
	Image					
۵	Events					
	Ordinary Event					

Figure 6-47

- 2. Check "Enable" to enable face recognition.
- 3. Set the arming area, move the mouse to the preview screen, hold down the left mouse button to select the area of the face recognition, and release the left mouse button to complete the area drawing.
 - **[Select all areas]** is used to set all areas under the monitor screen as the guard area.
 - [Delete Selection Area] is used to delete the selected alert area.

Intrusion Detection

The area intrusion detection is used to detect whether an object enters the set area in the video setting area, and the alarm is linked according to the judgment result.

 In the main interface click on the "Configuration → Events → Smart Event → Intrusion Detection" to enter the Intrusion Detection settings interface, as shown in Figure 6-48.

Ţ	Local Configuration	Intelligent detection	Intrusion Detection	Line Cross Detection	Loiter Detection	People Gather Detection
	System	Enable				
6	Storage		ning Schedule Linkage M	lethod		
٩	Network	Warn Region 1	· · ·			
	Video	And the second second		State and state		
	Image			THE WORLD'S AND	2	
۲	Events	1000000	10000		112	
	Ordinary Event		1 976	A STATE OF		
		and the second	- SAN SA			
		Draw Area Clear Time Threshold(S) Sensitivity				
		Save				

Figure 6-48

- 2. Check "Enable" to enable intrusion detection.
- 3. Select "Warn Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Save".
 - **[Drawing Area]** Click "**Drawing Area**", move the mouse to the preview screen, click the left mouse button and draw the endpoint of the quadrilateral guard area, then click the preview interface to complete the area drawing.
 - [Clear All] Used to delete the selected alert area.
 - **[Time threshold(s)]** Indicates that the target enters the alert zone and continues to stay for this time to generate an alarm. If set to 5s, the target intrusion area will trigger an alarm after 5s.
 - [Sensitivity] Used to set the sensitivity of detected area intrusion. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.
- 4. When you need to set other Warn Region, repeat step 3 to complete the setup.
- 5. Set the arming schedule.

As shown in Figure 6-49. You can view, edit, and delete the arming time of the intrusion detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, will show the left and right direction of the adjustment arrow, and move the adjustment arrow to adjust the arming time.

You can set up more than one time period for up to 8 time periods.

Ð

After setting, click "Save" to complete the setting of the arming time.

Ţ	Local Configuration	Intelligent detection	Intrusion	Detection	Line Cross Detection	Loiter Detection	People Gather Detection
	System	Enable					
6	Storage	Area Settings	Arming Schedule	Linkage Meth	od		
0	Network						
	Video	S Del All	G	Select All			
S	Image	Sun 00 02	04 06	08 10	12 14 16	18 20 22	24
۵	Events	Mon 00 02	04 06	08 10	12 14 16	18 20 22	24
	Ordinary Event						e
		Tue 00 02	04 06	08 10	12 14 16	18 20 22	24
		Wed 00 02	04 06	08 10	12 14 16	18 20 22	24
		Thu 00 02	04 06	08 10	12 14 16	18 20 22	24
		Fri 00 02	04 06	08 10	12 14 16	18 20 22	24
		Sat 00 02	04 06	08 10	12 14 16	18 20 22	24
		Save					

Figure 6-49



IMPORTANT NOTE

When the arming time is set, there can be no overlap between any two time periods.

Step 6: Set the linkage method as needed.

• [Linkage Method] refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

Line Cross Detection

The line cross detection function is used to detect whether there is an object in the video that crosses the set warning surface, and the alarm is linked according to the judgment result.

The specific operation steps are as follows:

 In the main interface click on the "Configuration → Events → Smart Event → Line Cross Detection" to enter the Line Cross Detection settings interface, as shown in Figure 6-50.

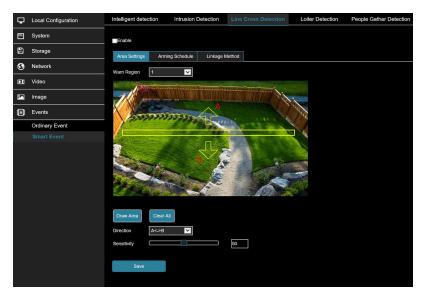


Figure 6-50

- 2. Check "Enable" to enable intrusion detection.
- 3. Select "Warn Line": The system supports setting up to 4 warn line. After selecting a warn line, you need to make the following settings. After setting, please click "Save" below.
 - **[Warn Line]** Click "**Drawing Area**" and a line segment with an arrow will appear on the screen. Click on the line segment, click and drag one of the endpoints to modify the length of the line segment; or click and drag the position of the line segment with the arrow in the picture to complete the drawing of a warning surface.
 - [Clear All] Used to delete the selected alert area.
 - [Direction] There are three options: "A<->B", "A->B", and "B->A", indicating the direction in which the object crosses the interface to trigger an alarm. "A->B" means that the alarm will be triggered when the object crosses from A to B; "B->A" means that the alarm will be triggered when the object crosses from B to A; "A<->B" means that the object crosses from A to B, or from B to B, the alarm is triggered, that is, the alarm is triggered in both directions.
 - [Sensitivity] Used to set the sensitivity of detected area intrusion. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.
- 4. When you need to set other Warn Line, repeat step 3 to complete the setup.
- 5. Set the arming schedule.

As shown in Figure 6-51. You can view, edit, and delete the arming time of the Line Cross detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, will show the left and right direction of the adjustment arrow, and move the adjustment arrow to adjust the arming time.

You can set up more than one time period for up to 8 time periods.



After setting, click "Save" to complete the setting of the arming time.

Intelligent	detec	tion		Int	rusio	n De	etect	ion									Loii	ter D	etec	tion		Peop	ple Gather De	tection
Enable	tinas		Arming	1 Scł	nedule		Lir	nkage	e Me	thod														
				,						נווים ר														
Ë	Del A					⊖ Se	elect	All																
Sun ⁰⁰	0:	2	04		06		08		10		12		14		16		18		20	2	2	24		
Mon ⁰⁰	0:	2	04		06		08		10	,	12		14		16		18		20	2	2	24	0	
Tue ⁰⁰	0	2	04		06		08		10		12		14		16		18		20	2	2	24	0	
					- 1													-	-	<u> </u>	I		0	
Wed 00	0:	2	04		06	-	08	-	10		12		14		16	-	18		20	2	2	24	0	
Thu 00	0	2	04	,	06	,	08 1		10 1	,	12 1		14 1	ļ	16 1	,	18 1		20	2	2	24		
Fri ⁰⁰	0	2	04		06		08		10		12		14		16		18	. :	20	2	2	24	•	
Sat ⁰⁰	0:	2	04		06	_	08		10		12		14		16		18	_	20	2	2	24	Ō	
				_		_		_	<u> </u>	_		_	- 11								-			





IMPORTANT NOTE

When the arming time is set, there can be no overlap between any two time periods.

- 6. Set the linkage method as needed.
 - [Linkage Method] refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

Loiter Detection

The loiter detection function is used to detect that the target stays within the set area for more than the set time threshold, and then alarms according to the judgment result.

 In the main interface click on the "Configuration → Events → Smart Event → Loiter Detection" to enter the Loiter Detection settings interface, as shown in Figure 6-52

Ţ	Local Configuration	Intelligent detection	Intrusion Detection	Line Cross Detection	Loiter Detection	People Gather Detection
	System	Enable				
63	Storage		ng Schedule Linkage M	Aethod		
٩	Network	Warn Region 1				
	Video				Page 199	
	Image	11			NA.	
▣	Events	10000000	MERON		and the second s	
	Ordinary Event		and the second			
		1 and the second	and the		14 M	
		Draw Area Clear A	1			
		Time Threshold(mins) 🔲		1		
		Sensitivity		50		
		Save				

Figure 6-52

- 2. Check "Enable" to enable intrusion detection.
- 3. Select "Warn Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Save" below.
 - **[Drawing Area]** Click "**Drawing Area**", move the mouse to the preview screen, click the left mouse button and draw the endpoint of the quadrilateral guard area, then click the preview interface to complete the area drawing.
 - [Clear All] Used to delete the selected alert area.
 - **[Time threshold(min)]** Indicates that the target generates an alarm after continuous movement in the detection area. The larger the time threshold, the longer the target continues to move in the detection area to trigger an alarm.
 - [Sensitivity] Used to set the sensitivity of detected area intrusion. The default is 50. Drag the progress bar or enter the value directly in the value box to modify the sensitivity. The greater the sensitivity, the easier it is to trigger an alarm.
- 4. When you need to set other Warn Region, repeat step 3 to complete the setup.
- 5. Set the arming schedule.

As shown in Figure 6-53. You can view, edit, and delete the arming time of the Loiter detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, will show the left and right direction of the adjustment arrow, and move the adjustment arrow to adjust the arming time.

You can set up more than one time period for up to 8 time periods.

Þ

After setting, click "Save" to complete the setting of the arming time.







IMPORTANT NOTE

When the arming time is set, there can be no overlap between any two time periods.

- 6. Set the linkage method as needed.
 - [Linkage Method] refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

People Gather Detection

The people gather detection function is used to detect that the density of the personnel in the set area exceeds the set threshold, and the alarm is linked according to the judgment result.

 In the main interface click on the "Configuration → Events → Smart Event → People Gather Detection" to enter the People Gather Detection settings interface, as shown in Figure 6-54.

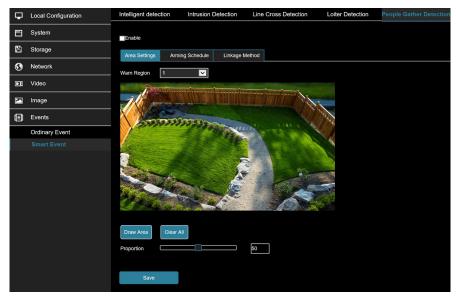


Figure 6-54

- 2. Check "Enable" to enable intrusion detection.
- 3. Select "Warn Region": The system supports setting up to 4 warn region. After selecting a warn region, you need to make the following settings. After setting, please click "Save" below.
 - **[Drawing Area]** Click "**Drawing Area**", move the mouse to the preview screen, click the left mouse button and draw the endpoint of the quadrilateral guard area, then click the preview interface to complete the area drawing.
 - [Clear All] Used to delete the selected alert area.
 - [Proportion] Indicates the proportion of personnel in the entire alert area. When the proportion of personnel exceeds the set percentage, the system will generate an alarm. The percentage is 50% by default. The larger the value, the more people can be accommodated in the alert area, and the less likely it is to trigger an alarm.
- 4. When you need to set other Warn Region, repeat step 3 to complete the setup.
- 5. Set the arming schedule.

As shown in Figure 6-55. You can view, edit, and delete the arming time of the People gather detection. The default is to arm the alarm 24 hours a day. You can adjust the arming time as follows:

Method 1: Click the arming time period, manually fill in the start time and end time, set up and click "**Save**". If you need to delete the time period, click the "**Delete**" button and then reset the time period.

Method 2: Click the time of deployment, the time period will display two circles at both ends, the mouse moves to the circle, will show the left and right direction of the adjustment arrow, and move the adjustment arrow to adjust the arming time.

You can set up more than one time period for up to 8 time periods.

Þ

After setting, click "Save" to complete the setting of the arming time.



Figure 6-55



IMPORTANT NOTE

When the arming time is set, there can be no overlap between any two time periods.

- 6. Set the linkage method as needed.
 - [Linkage Method] refers to the response made by the device when an alarm event occurs. The linkage includes "General Linkage", "Upload Via SMTP" and "Upload Via FTP".

Chapter 7: Wi-Fi Cameras

WiFi cameras do not currently support AP mode. This will be made available at a later date.

WiFi cameras must be plugged into the local area network to add or change WiFi settings.

7.1 Setting Up Wi-Fi Cameras

7.1.1 Connect the Camera to the Home LAN

The camera must be hooked up to a switch, router, or modem on the LAN to configure Wi-Fi settings.

1. Using an Ethernet cable, connect the Wi-Fi camera to a router, switch, or modem that is on the network the camera should be connected to. Power up the camera using the included power supply.

- 2. Once the camera is connected to the network, use the IP Search Tool to discover the Camera IP Address (Please reference Chapter 2).
- 3. Using Edge or Chrome, connect to the camera Web Console and finish camera setup (Please reference Chapter 3).

7.1.2 Connect to Wi-Fi

Connect to the desired WiFi network from the WiFi Configuration tab on the home page.

IP Camera	Live View	Playback	Configuration	Wifi Configuration
4:3 📧 🗙 💼 Main Stream	Sub Stream			

- 1. Select WiFi Configuration or navigate to Configuration > Network > Advanced Setup > WiFi.
- 2. Tap Scan to discover available WiFi networks.

Live View	Playback	Configuration	
DDNS	FTP	SMTP	P2P
Wifi			Scan
SSID 🔺	Encryptio	n 💠 🛛 Signal Strength 🗘	Channel \$
Clare-B	eta WPA-P	SK 100	0

3. Select the desired 2.4GHz WiFi network.

Live	e View	Playback	Configuration		
D	DNS	FTP	SMTP	Р	2P
Wifi			(Scan	
	SSID ▲	Encryptio	n 💠 🛛 Signal Strengtt	h ⇔ Channel ≎	
	Clare-Beta	WPA-P	SK 100	0	*
V	Clare-Dev1	WPA-P	SK 18	0	
	Clare-Dev2	WPA-P	SK 100	0	
	Clare-Jenova	WPA-P	SK 66	0	
	Clare-Longevity	WPA-P	SK 88	0	
	Clare-Smoke_1	WPA-P	SK 0	0	
	Clare-Smoke_2	WPA-P	SK 90	0	
	Clare-Smoke_5	WPA-P	SK 100	0	
	Clare-Smoke_6	WPA-P	SK 58	0	
	Clare-System1	WPA-P	SK 62	0	*

4. Input the WiFi password in the **Key Field**.

Status	Connection Failed	
SSID	Clare-Dev1	
Кеу		
Encryption	WPA-PSK Y	
DHCP		
IP Address		

 Check DHCP if you would like the network to assign the network parameters automatically. Leave this unchecked if you would like to configure settings such as IP Address, Netmask, Default Gateway, Preferred DNS Server.

Status	Connection Failed	
SSID	Clare-Dev1	
Кеу		
Encryption	WPA-PSK	~
DHCP		
IP Address		

6. Tap **Save**.

Default Gateway Preferred DNS Server	
Save	

7.2 Changing the WiFi Password on a WiFi Camera

7.2.1 Connect the Camera to the Home LAN

The camera must be hooked up to a switch, router, or modem on the LAN to configure Wi-Fi settings.

- 4. Using an Ethernet cable, connect the Wi-Fi camera to a router, switch, or modem that is on the network the camera should be connected to. Power up the camera using the included power supply.
- 5. Once the camera is connected to the network, use the IP Search Tool to discover the Camera IP Address (Please reference Chapter 2).
- 6. Using Edge or Chrome, connect to the camera Web Console and finish camera setup (Please reference Chapter 3).

7.2.2 Change Wi-Fi Password

Connect to the desired WiFi network from the WiFi Configuration tab on the home page.

IP Camera	Live View	Playback	Configuration	Wifi Configuration
4:3 📧 🗙 💽 🛛 Main Stream	Sub Stream			

- 7. Select WiFi Configuration or navigate to Configuration > Network > Advanced Setup > WiFi.
- 8. Tap **Scan** to discover available WiFi networks.

Live View	Playback	Configurati	on		
DDNS	FTP	SMT	þ		P2P
Wifi				Scan	
SSID 🔺	Encryptio	n 💠 Signal Stre	ength ≎	Channel \$	
Clare-Bet	a WPA-PS	SK 100)	0	*

9. Select the existing WiFi network or a new network to connect to.

Live Vie	ew	Playback	Configuration		
DDNS	\$	FTP	SMTP	P:	2P
Wifi			(Scan	
	SSID 🔺	Encryptio	n \$ Signal Strength	Channel \$	
	55ID ¥	Encryption	n 🗢 Signai Suengui		
	Clare-Beta	WPA-PS	SK 100	0	^
	Clare-Dev1	WPA-PS	SK 18	0	_
	Clare-Dev2	WPA-PS	SK 100	0	
	Clare-Jenova	WPA-PS	SK 66	0	
	Clare-Longevity	WPA-PS	SK 88	0	
	Clare-Smoke_1	WPA-PS	SK 0	0	
	Clare-Smoke_2	WPA-PS	SK 90	0	
	Clare-Smoke_5	WPA-PS	SK 100	0	
	Clare-Smoke_6	WPA-PS	SK 58	0	
	Clare-System1	WPA-PS	SK 62	0	-

10. Change the WiFi password in the **Key Field**.

Status	Connection Failed	
SSID	Clare-Dev1	
Кеу	•••••	
Encryption	WPA-PSK	~
DHCP		
IP Address		

11. Check **DHCP** if you would like the network to assign the network parameters automatically. Leave this unchecked if you would like to configure settings such as **IP Address, Netmask, Default Gateway, Preferred DNS Server**.

Status	Connection Failed	
SSID	Clare-Dev1	
Кеу	•••••	
Encryption	WPA-PSK V	
OHCP		
IP Address		

12. Tap Save.

Default Gateway Preferred DNS Server	
Save	

7.3 Configure WiFi Settings

7.3.1 Configure WiFi Settings

Several settings can be configured for WiFi cameras. The can be found under **Configuration > Network > Advanced Setup > WiFi**.

- [Scan Button] Scans all available WiFi networks
- [WiFi Window] Displays all available WiFi networks
- [Wireless WiFi Management Button] Displays a window that shows all programmed networks
- [Status] Displays the current connected or disconnected status of the WiFi network
- [SSID] Displays the currently selected WiFi network name
- **[Key]** Input the password for the selected WiFi network
- **[Encryption]** Change the encryption settings for the WiFi network
- [DHCP] When checked (Enabled), it allows the network to manage the configuration settings for the camera
- [IP Address] Input the desired IP address for the camera (disabled when DHCP is checked)

- [Netmask] Input the desired Netmask settings for the camera (disabled when DHCP is checked)
- [Default Gateway] Input the desired Gateway settings for the camera (disabled when DHCP is checked)
- [Preferred DNS Server] Input the desired DNS settings for the camera (disabled when DHCP is checked)