

advidia

Network Camera

User Manual

User Manual

About this Manual

This Manual is applicable to Network Camera.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only.

The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website.

Please use this user manual under the guidance of professionals.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL OUR COMPANY, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET

SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



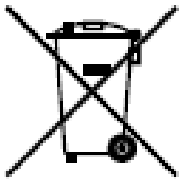
This product and - if applicable - the supplied accessories too are

marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see:

www.recyclethis.info.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.



Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into 'Warnings' and 'Cautions':

Warnings: Serious injury or death may be caused if any of these warnings are neglected.

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.

	
Warnings Follow these safeguards to prevent serious injury or death.	Cautions Follow these precautions to prevent potential injury or material damage.



Warnings:

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. And source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- Please make sure that the ceiling can support more than 50(N) Newton gravities if the camera is fixed to the ceiling.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Cautions:

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.

- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -30°C to +60°C, or -40°C to +60°C if the camera model supports heater), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, ensure there is good ventilation to the device.
- Keep the camera away from water and any liquids.
- While shipping, pack the camera in its original, or equivalent, packing materials. Or packing the same texture.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

Notes:

For the camera supports IR, you are required to pay attention to the following precautions to prevent IR reflection:

- Dust or grease on the dome cover will cause IR reflection. Please do not remove the dome cover film until the installation is finished. If there is dust or grease on the dome cover, clean the dome cover with clean soft cloth and isopropyl alcohol.
- Make certain the installation location does not have reflective surfaces of objects too close to the camera. The IR light from the camera may reflect back into the lens causing reflection.
- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDS. Fasten the dome cover to camera body so that the foam ring and the dome cover are attached seamlessly.

Table of Contents

Chapter 1	System Requirement.....	9
Chapter 2	Network Connection.....	10
2.1	Setting the Network Camera over the LAN	10
2.1.1	Wiring over the LAN	10
2.1.2	Activating the Camera	11
Chapter 3	Access to the Network Camera.....	15
3.1	Accessing by Web Browsers	15
Chapter 4	Live View	17
4.1	Live View Page	17
4.2	Starting Live View	17
4.3	Recording and Capturing Pictures Manually	18
Chapter 5	Network Camera Configuration	19
5.1	Configuring Local Parameters.....	19
5.2	Configure System Settings.....	21
5.2.1	Configuring Basic Information	21
5.2.2	Configuring Time Settings.....	21
5.2.3	Configuring RS232 Settings.....	24
5.2.4	Configuring RS485 Settings.....	24
5.2.5	Configuring DST Settings.....	25
5.3	Maintenance.....	26
5.3.1	Upgrade & Maintenance.....	26
5.3.2	Log	27
5.3.3	System Service	28
5.4	Security Settings	29
5.4.1	Authentication	29
5.4.2	IP Address Filter	29
5.4.3	Security Service.....	31
5.5	User Management	32
5.5.1	User Management	32
5.5.2	Online Users.....	37
Chapter 6	Network Settings	38
6.1	Configuring Basic Settings.....	38
6.1.1	Configuring TCP/IP Settings	38
6.1.2	Configuring DDNS Settings.....	40
6.1.3	Configuring Port Settings	41
6.1.4	Configure NAT (Network Address Translation) Settings.....	42

6.2	Configure Advanced Settings	43
6.2.1	Configuring SNMP Settings	43
6.2.2	Configuring FTP Settings	45
6.2.3	Configuring Email Settings	47
6.2.4	HTTPS Settings	50
6.2.5	Configuring QoS Settings	51
6.2.6	Configuring 802.1X Settings	52
Chapter 7	Video/Audio Settings	54
7.1	Configuring Video Settings	54
7.2	Configuring Audio Settings	57
7.3	Configuring ROI Encoding	58
7.4	Display Info. on Stream	59
7.5	Configuring Target Cropping	60
Chapter 8	Image Settings	61
8.1	Configuring Display Settings	61
8.1.1	Day/Night Auto-Switch	61
8.1.2	Day/Night Scheduled-Switch	65
8.2	Configuring OSD Settings	66
8.3	Configuring Privacy Mask	68
8.4	Configuring Picture Overlay	69
Chapter 9	Event Settings	70
9.1	Basic Events	70
9.1.1	Configuring Motion Detection	70
9.1.2	Configuring Video Tampering Alarm	77
9.1.3	Configuring Alarm Input	78
9.1.4	Configuring Alarm Output	79
9.1.5	Handling Exception	80
9.2	Smart Events	81
9.2.1	Configuring Audio Exception Detection	81
9.2.2	Configuring Defocus Detection	83
9.2.3	Configuring Scene Change Detection	84
9.2.4	Configuring Face Detection	85
9.2.5	Configuring Intrusion Detection	87
9.2.6	Configuring Line Crossing Detection	88
9.2.7	Configuring Region Entrance Detection	90
9.2.8	Configuring Region Exiting Detection	92
9.2.9	Configuring Unattended Baggage Detection	93
9.2.10	Configuring Object Removal Detection	95

9.3	VCA Configuration.....	96
9.3.1	Counting	97
Chapter 10	<i>Storage Settings.....</i>	99
10.1	Configuring Record Schedule	99
10.2	Configure Capture Schedule.....	102
10.3	Configuring Net HDD.....	103
Chapter 11	<i>Playback.....</i>	106

Chapter 1 System Requirement

Operating System: Microsoft Windows XP SP1 and above version

CPU: 2.0 GHz or higher

RAM: 1G or higher

Display: 1024×768 resolution or higher

Web Browser: Internet Explorer 8.0 and above version, Apple Safari 5.0.2 and above version, Mozilla Firefox 5.0 and above version and Google Chrome 18 and above version.

Chapter 2 Network Connection

Note:

- You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.
- To ensure the network security of the network camera, we recommend you to have the network camera assessed and maintained termly. You can contact us if you need such service.

Before you start:

- If you want to set the network camera via a LAN (Local Area Network), please refer to *Section 2.1 Setting the Network Camera over the LAN*.

2.1 Setting the Network Camera over the LAN

Purpose:

To view and configure the camera via a LAN, you need to connect the network camera in the same subnet with your computer, and install the SADP or Guarding Expert software to search and change the IP of the network camera.

Note: For the detailed introduction of SADP, please refer to Appendix 1.

2.1.1 Wiring over the LAN

The following figures show the two ways of cable connection of a network camera and a computer:

Purpose:

- To test the network camera, you can directly connect the network camera to the computer with a network cable as shown in Figure 2-1.
- Refer to the Figure 2-2 to set network camera over the LAN via a switch or a router.

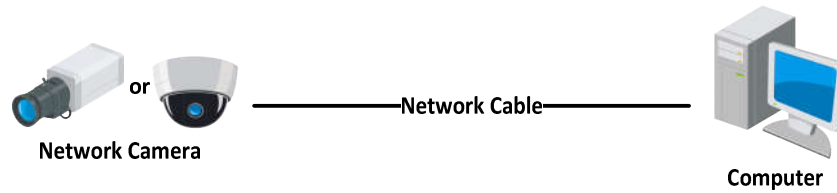


Figure 2-1 Connecting Directly

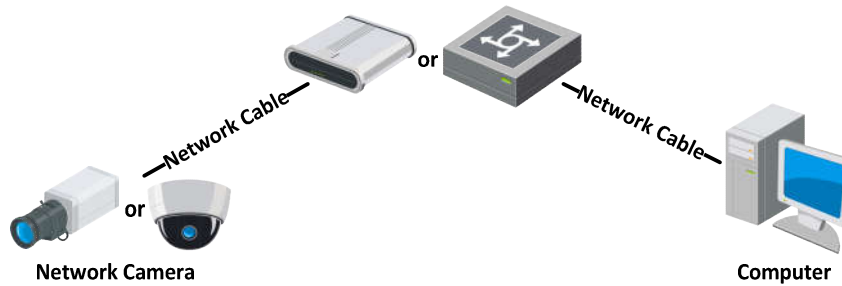


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Activating the Camera

You are required to activate the camera first by setting a strong password for it before you can use the camera.

Activation via Web Browser, Activation via SADP, and Activation via Client Software are all supported.

❖ Activation via Web Browser

Steps:

1. Power on the camera, and connect the camera to the network.
2. Input the IP address into the address bar of the web browser, and click Enter to enter the activation interface.

Notes:

- The default IP address of the camera is 192.0.0.64.

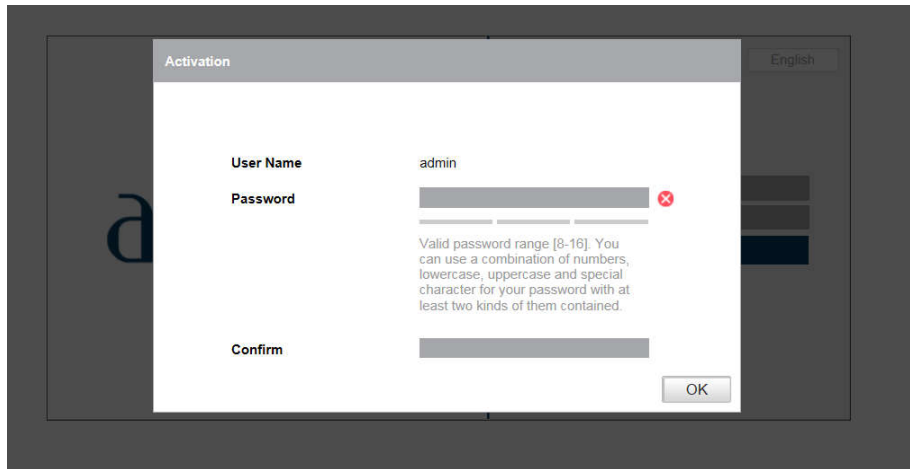


Figure 2-3 Activation via Web Browser

3. Create a password and input the password into the password field.



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

4. Confirm the password.
5. Click OK to save the password and enter the live view interface.

❖ Activation via Advidia Camera Finder Utility

Advidia Camera Finder Utility is used for detecting the online device, activating the camera, and resetting the password.

Get the Advidia Camera Finder Utility from the supplied disk or the official website, and install the Advidia Camera Finder Utility according to the prompts. Follow the steps to activate the camera.

Steps:

1. Run the Advidia Camera Finder Utility software to search the online devices.
2. Check the device status from the device list, and select the inactive device.

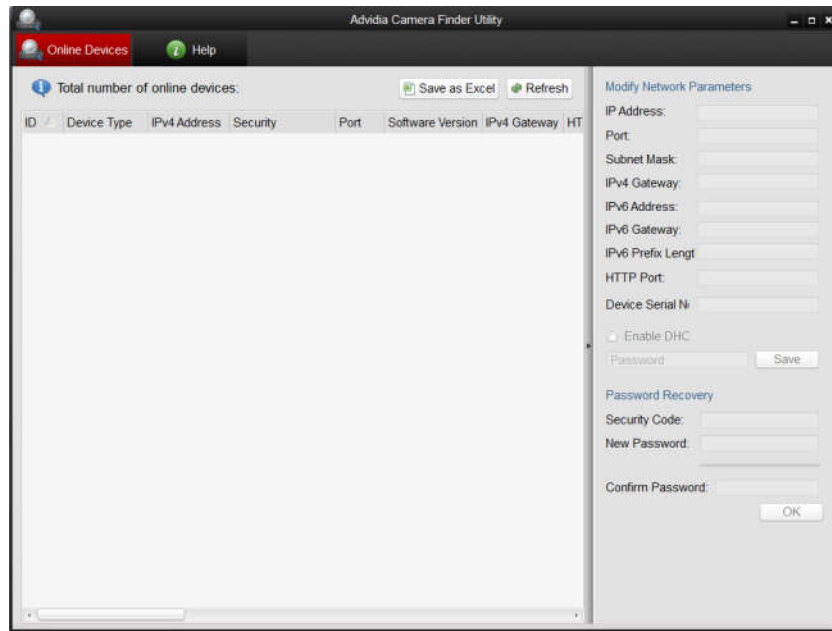


Figure 2-4 Advidia Camera Finder Utility Interface

3. Create a password and input the password in the password field, and confirm the password.



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

4. Click **OK** to save the password.

You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

Modify Network Parameters

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

☐ Enable DHCP

Password

Figure 2-5 Modify the IP Address

6. Input the password and click the **Save** button to activate your IP address modification.

Chapter 3 Access to the Network Camera

3.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the browser address bar, input the IP address of the network camera, and press the **Enter** key to enter the login interface.
3. Activate the network camera for the first time using, refer to the Section 2.1.2 for details.

Note:

- The default IP address is 192.0.0.64.
 - If the camera is not activated, please activate the camera first according to Chapter 2.1.2.
4. Select English as the interface language on the top-right of login interface.
 5. Input the user name and password and click **Login**.

The admin user should configure the device accounts and user/operator permissions properly. Delete the unnecessary accounts and user/operator permissions.

Note:

The IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).

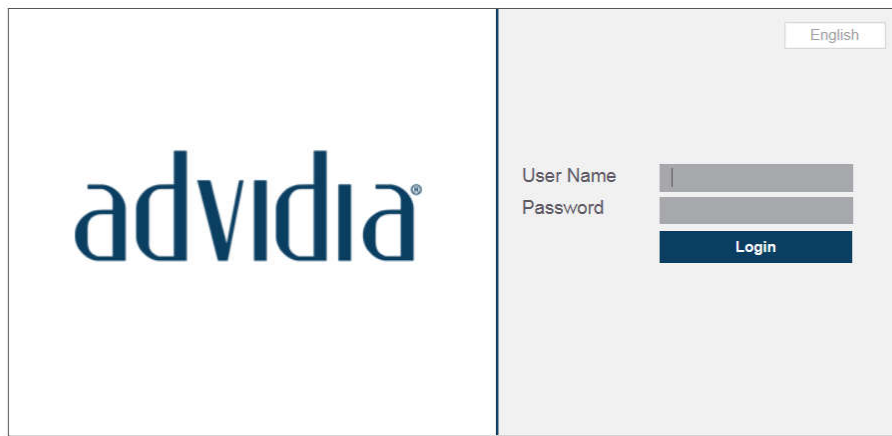


Figure 3-1 Login Interface

6. Install the plug-in before viewing the live video and operating the camera. Please follow the installation prompts to install the plug-in.

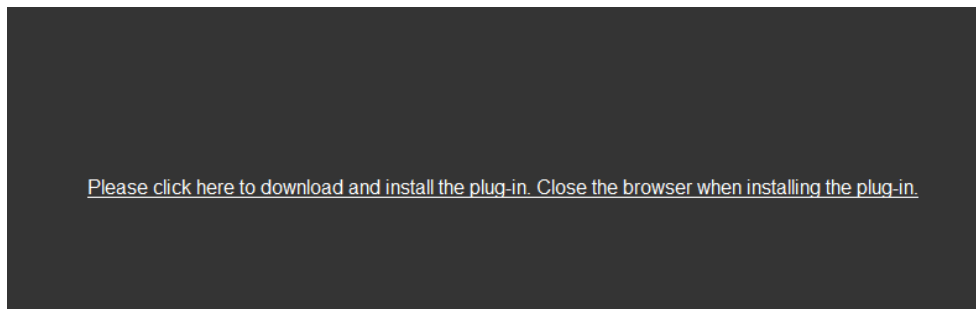


Figure 3-2 Download and Install Plug-in

Note: You may have to close the web browser to install the plug-in. Please reopen the web browser and log in again after installing the plug-in.

Chapter 4 Live View

4.1 Live View Page

Purpose:

The live view page allows you to view the real-time video, capture images, realize PTZ control, set/call presets and configure video parameters.

Log in the network camera to enter the live view page, or you can click **Live View** to enter the live view page.

Descriptions of the live view page:

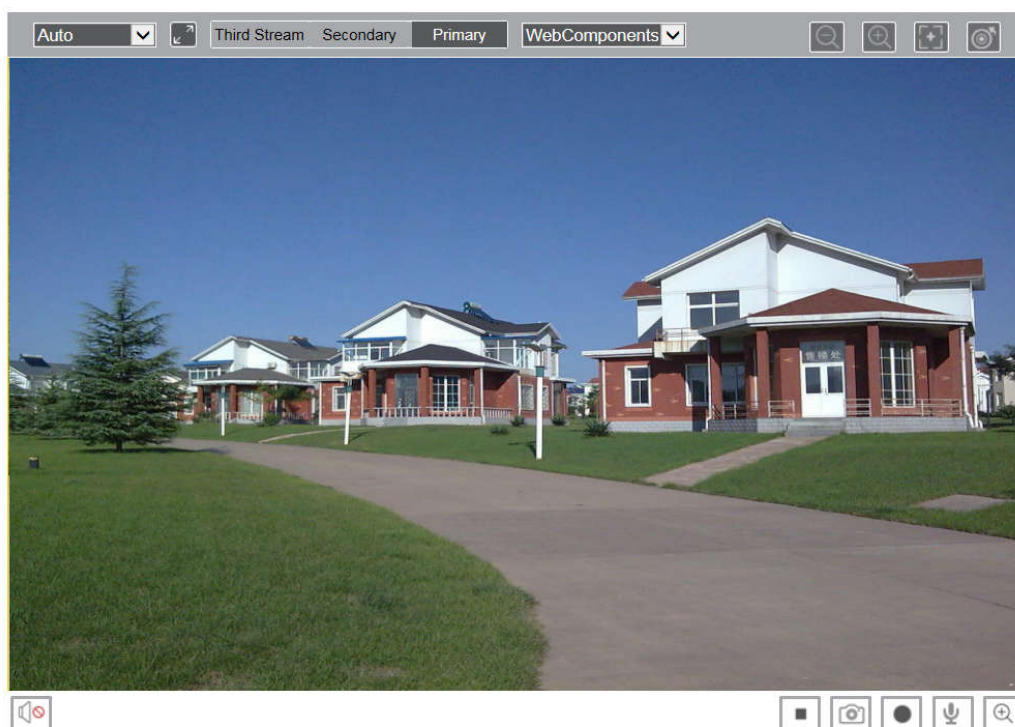


Figure 4-1 Live View Page

4.2 Starting Live View


In the live view window as shown in Figure 4-2, click  on the toolbar to start the live view of the camera.





Figure 4-2 Live View Toolbar

Table 4-1 Descriptions of the Toolbar

Icon	Description
	Start/Stop live view.
	The window size, 4:3, 16:9, X1 and Auto are optional.
	Full screen.
	Live view with main, sub, third stream.
	Click to select the third-party plug-in.
	Zoom in and out
	Auto focus
	Lens initialization
	Audio on and adjust volume /Mute.
	Manually capture the picture.
	Manually start/stop recording.
	Turn on/off microphone.
	Start/stop digital zoom function.

Note: The icons vary according to the different camera models.

4.3 Recording and Capturing Pictures Manually

In the live view interface, click on the toolbar to capture the live pictures or click to record the live view. The saving paths of the captured pictures and clips can be set on the **System > Local** page.

Note: The captured image will be saved as JPEG file or BMP file in your computer.

Chapter 5 Network Camera Configuration

5.1 Configuring Local Parameters

Purpose:

The local configuration refers to the parameters of the live view, record files and captured pictures. The record files and captured pictures are the ones you record and capture using the web browser and thus the saving paths of them are on the PC running the browser.

Steps:

1. Enter the Local Configuration interface: **System > Local**.

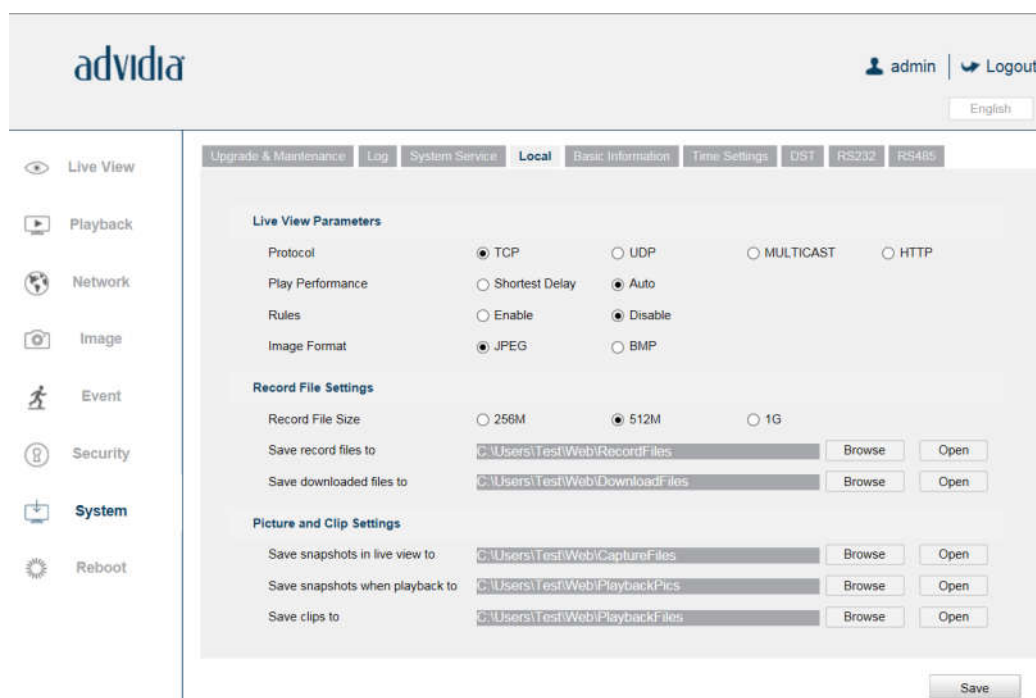


Figure 5-1 Local Configuration Interface

2. Configure the following settings:

- **Live View Parameters:** Set the protocol type and live view performance.

- ◆ **Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable.

TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.

UDP: Provides real-time audio and video streams.

HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.

MULTICAST: It's recommended to select MCAST type when using the Multicast function.

- ◆ **Play Performance:** Set the play performance to Shortest Delay or Auto.
- ◆ **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g., enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.
- ◆ **Image Format:** Choose the image format for picture capture.
- **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.
 - ◆ **Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.
 - ◆ **Save record files to:** Set the saving path for the manually recorded video files.
 - ◆ **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you capture with the web browser.
 - ◆ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.
 - ◆ **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
 - ◆ **Save clips to:** Set the saving path of the clipped video files in playback mode.
 - ◆ **Note:** You can click **Browse** to change the directory for saving the clips and pictures, and click Open to open the set folder of clips and picture saving.

3. Click **Save** to save the settings.

5.2 Configure System Settings

Purpose:

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

5.2.1 Configuring Basic Information

Enter the Device Information interface: **System > Basic Information**.

In the **Basic Information** interface, you can edit the Device Name and Device No..

Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.

Upgrade & Maintenance	Log	System Service	Local	Basic Information	Time Settings	DST	RS232	RS485
-----------------------	-----	----------------	-------	-------------------	---------------	-----	-------	-------

Device Name	IP CAMERA
Device No.	88
Model	
Serial No.	20170309AAWR727863684
Firmware Version	V5.4.0 build 170329
Encoding Version	V7.3 build 170330
Web Version	V4.0.51 build 161221
Plugin Version	V3.0.6.1
Number of Channels	1
Number of HDDs	0
Number of Alarm Input	1
Number of Alarm Output	1

Save

Figure 5-2 Basic Information

5.2.2 Configuring Time Settings

Purpose:

You can follow the instructions in this section to configure the time synchronization and DST settings.

Steps:

1. Enter the Time Settings interface, **System> Time Settings**.

Upgrade & Maintenance Log System Service Local Basic Information **Time Settings** DST RS232 RS485

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore ▼

NTP

☐ NTP

Server Address time.windows.com

NTP Port 123

Interval 1440 min

Test

Manual Time Sync.

☒ Manual Time Sync.

Device Time 2017-04-17T21:26:44

Set Time 2017-04-17T21:26:28 ☐ Sync. with computer time

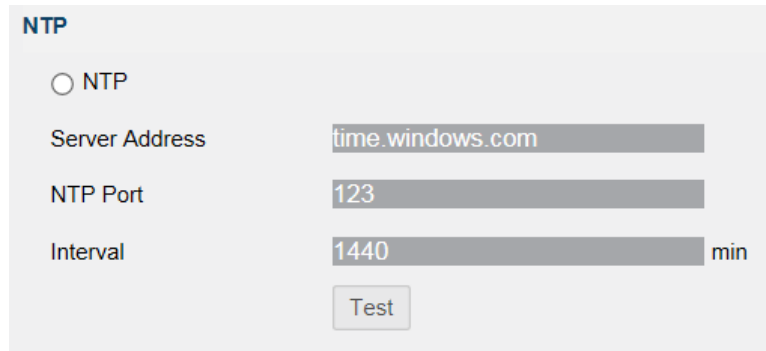
Figure 5-3 Time Settings

2. Select the Time Zone of your location from the drop-down menu.
3. Configure the NTP settings.
 - (1) Click to enable the **NTP** function.
 - (2) Configure the following settings:

Server Address: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions with NTP server.
 - (3) (Optional) You can click the **Test** button to test the time synchronization function via NTP server.



NTP

☐ NTP

Server Address: time.windows.com


NTP Port: 123

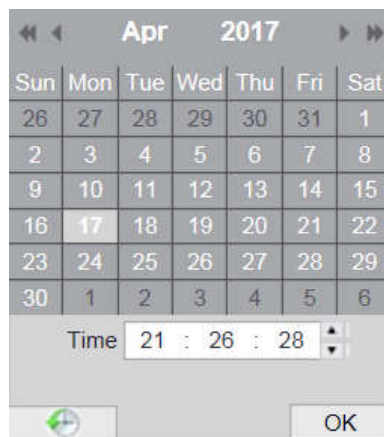
Interval: 1440 min

Test

Figure 5-4 Time Sync by NTP Server

Note: If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

- Configure the manual time synchronization.
 - (1) Check the **Manual Time Sync.** item to enable the manual time synchronization function.
 - (2) Click the icon  to select the date, time from the pop-up calendar.
 - (3) (Optional) You can check **Sync. with computer time** item to synchronize the time of the device with that of the local PC.



Calendar view for April 2017. The date 17 is selected. Below the calendar, the time is set to 21 : 26 : 28. There is a green circular icon with a refresh symbol and an OK button.

Figure 5-5 Time Sync Manually

- Click **Save** to save the settings.

5.2.3 Configuring RS232 Settings

The RS232 port can be used in two ways:

- **Parameters Configuration:** Connect a computer to the camera through the serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the serial port parameters of the camera.
- **Transparent Channel:** Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

Steps:

1. Enter RS232 Port Setting interface: **System > RS232**.
2. Configure the Baud Rate, Data Bit, Stop Bit, Parity, Flow Control, and Usage.

Label	Value
Baud Rate	115200
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
Usage	Console

Figure 5-6 RS232 Settings

Note: If you want to connect the camera by the RS232 port, the parameters of the RS232 should be exactly the same with the parameters you configured here.

3. Click **Save** to save the settings.

5.2.4 Configuring RS485 Settings

Purpose:

The RS485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

Steps:

1. Enter RS-485 Port Setting interface: **System > RS485**.

Figure 5-7 RS-485 Settings

2. Set the RS485 parameters and click **Save** to save the settings.

By default, the Baud Rate is set as 9600 bps, the Data Bit is 8, the stop bit is 1 and the Parity and Flow Control is None.

Note: The Baud Rate, PTZ Protocol and PTZ Address parameters should be exactly the same as the PTZ camera parameters.

5.2.5 Configuring DST Settings

Purpose:

Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Configure the DST according to your actual demand.

Steps:

1. Enter the DST configuration interface.

System > DST

Figure 5-8 DST Settings

2. Select the start time and the end time.
3. Select the DST Bias.
4. Click **Save** to activate the settings.

5.3 Maintenance

5.3.1 Upgrade & Maintenance

Purpose:

The upgrade & maintenance interface allows you to process the operations, including reboot, partly restore, restore to default, export/import the configuration files, and upgrade the device.

Enter the Maintenance interface:

System > Upgrade & Maintenance

- **Restore:** Reset all the parameters, except the IP parameters and user information, to the default settings.
- **Default:** Restore all the parameters to the factory default.

Note: After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.

- **Export/Import Config. File:** Configuration file is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

Steps:

1. Click **Device Parameters** to export the current configuration file, and save it to certain place.
2. Click **Browse** to select the saved configuration file and then click **Import** to start importing configuration file.

Note: You need to reboot the camera after importing configuration file.

- **Upgrade:** Upgrade the device to a certain version.

Steps:

1. Select firmware or firmware directory to locate the upgrade file.
Firmware: Locate the exact path of the upgrade file.
Firmware Directory: Only the directory the upgrade file belongs to is required.
2. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.

Note: The upgrading process will take 1 to 10 minutes. Please don't disconnect power of the camera during the process, and the camera reboots automatically after upgrade.

5.3.2 Log

Purpose:

The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:

Please configure network storage for the camera or insert a SD card in the camera.

Steps:

1. Enter log searching interface: **System > Log**.

Upgrade & Maintenance **Log** System Service Local Basic Information Time Settings DST RS232 RS485

Major Type: All Types Minor Type: All Types

Start Time: 2017-04-17 00:00:00 End Time: 2017-04-17 23:59:59 Search

Log List Export

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
-----	------	------------	------------	-------------	-------------------	----------------

Total 0 Items << < 0/0 > >>

Figure 5-9 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.
3. Click **Search** to search log files. The matched log files will be displayed on the log list interface.
4. To export the log files, click **Export** to save the log files.

5.3.3 System Service

Purpose:

System service settings refer to the software and hardware service the camera supports. Supported functions vary according to the different cameras. For the cameras support IR LED, ABF (Auto Back Focus), Auto Defog, or Status LED, you can select to enable or disable the corresponding service according to the actual demands.

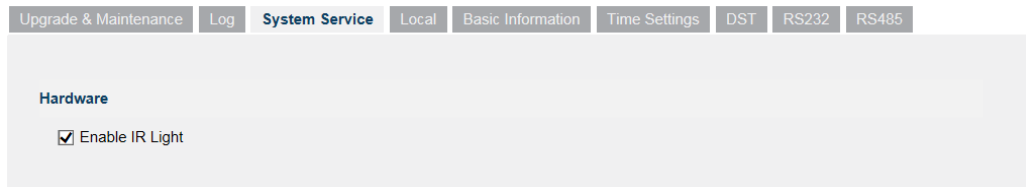


Figure 5-10 Enable IR Light

5.4 Security Settings

Configure the parameters, including Authentication, Anonymous Visit, IP Address Filter, and Security Service from security interface.

5.4.1 Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface: **Security > Authentication**.

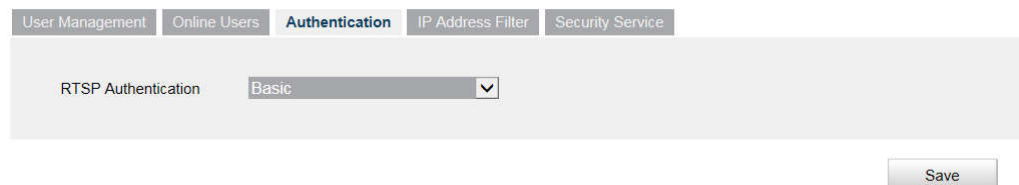


Figure 5-11 RTSP Authentication

2. Select the RTSP **Authentication** type **basic** or **disable** in the drop-down list to enable or disable the RTSP authentication.

Note: If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol via the IP address.

3. Click **Save** to save the settings.

5.4.2 IP Address Filter

Purpose:

This function makes it possible for access control.

Steps:

1. Enter the IP Address Filter interface: **Security > IP Address Filter**

Figure 5-12 IP Address Filter Interface

2. Check the checkbox of **Enable IP Address Filter**.
3. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
4. Set the IP Address Filter list.
 - Add an IP Address

Steps:

- (1) Click the **Add** to add an IP.
- (2) Input the IP Address.

Figure 5-13 Add an IP

(3) Click the **OK** to finish adding.

- Modify an IP Address

Steps:

(1) Left-click an IP address from filter list and click **Modify**.

(2) Modify the IP address in the text filed.



Figure 5-14 Modify an IP

(3) Click the **OK** to finish modifying.

- Delete an IP Address or IP Addresses.

Select the IP address(es) and click **Delete**.

5. Click **Save** to save the settings.

5.4.3 Security Service

To enable the remote login, and improve the data communication security, the camera provides the security service for better user experience.

Steps:

1. Enter the security service configuration interface: **Security > Security Service**.



Figure 5-15 Security Service

2. Check the checkbox of **Enable SSH** to enable the data communication security, and uncheck the checkbox to disable the SSH.

3. Check the checkbox of **Enable Illegal Login Lock**, and then the IP address will be locked if the admin user performs 7 failed user name/password attempts (5

times for the operator/user).

Note: If the IP address is locked, you can try to login the device after 30 minutes.

5.5 User Management

5.5.1 User Management

Purpose:

The admin user can add, delete or modify user accounts, and grant them different permissions. We highly recommend you manage the user accounts and permissions properly.

Steps:

1. Enter the User Management interface: **Security > User Management**

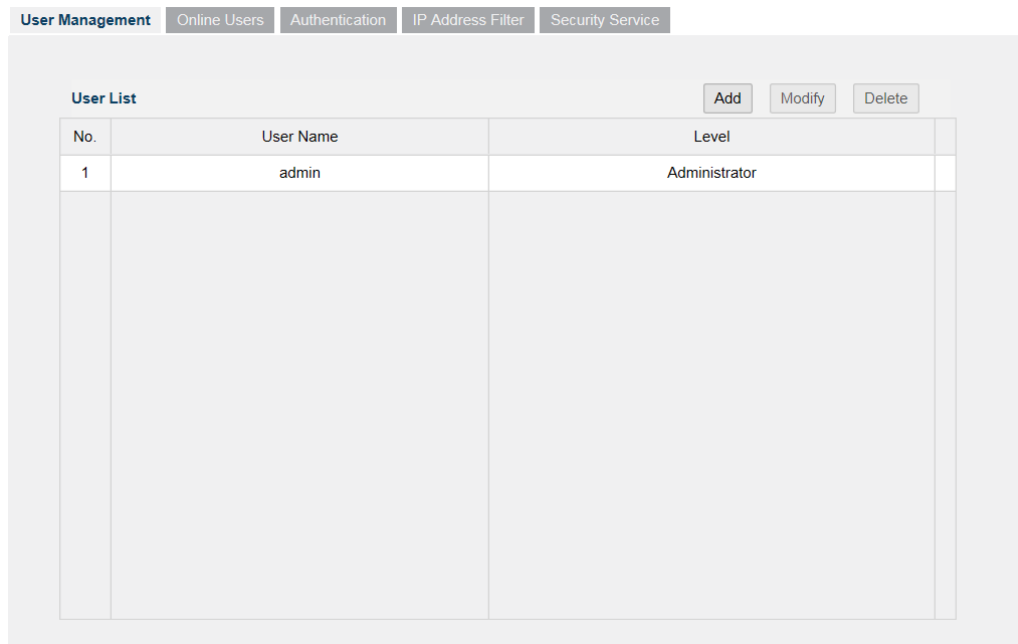


Figure 5-16 User Management Interface

- **Adding a User**

The *admin* user has all permissions by default and can create/modify/delete other accounts.

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

Steps:

1. Click **Add** to add a user.
2. Input the **User Name**, select **Level** and input **Password**.

Notes:

- Up to 31 user accounts can be created.
- Users of different levels own different default permissions. Operator and user are selectable.

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

3. You can check or uncheck the permissions for the new user.
4. Click **OK** to finish the user addition.

Add user [X]

User Name: [Text Box]

Level: [Operator] [v]

Password: [Text Box]

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm: [Text Box]

☐ Select All

- ☐ Remote: Parameters Settings
- ☒ Remote: Log Search / Interrogate Wor...
- ☐ Remote: Upgrade / Format
- ☒ Remote: Two-way Audio
- ☐ Remote: Shutdown / Reboot
- ☐ Remote: Notify IP Server / Trigger Ala...
- ☐ Remote: Video Output Control
- ☐ Remote: Serial Port Control
- ☒ Remote: Live View
- ☒ Remote: Manual Record
- ☒ Remote: PTZ Control
- ☒ Remote: Playback

[OK] [Cancel]

Figure 5-17 Add a User

- **Modifying a User**

Steps:

1. Left-click to select the user from the list and click **Modify**.
2. Modify the **User Name**, **Level** and **Password**.

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

4. You can check or uncheck the permissions.
5. Click **OK** to finish the user modification.

Modify user

User Name: admin

Level: Administrator

Password: •••••

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm: •••••

- ☒ Select All
- ☒ Remote: Parameters Settings
- ☒ Remote: Log Search / Interrogate Wor...
- ☒ Remote: Upgrade / Format
- ☒ Remote: Two-way Audio
- ☒ Remote: Shutdown / Reboot
- ☒ Remote: Notify IP Server / Trigger Ala...
- ☒ Remote: Video Output Control
- ☒ Remote: Serial Port Control
- ☒ Remote: Live View
- ☒ Remote: Manual Record
- ☒ Remote: PTZ Control
- ☒ Remote: Playback

OK Cancel

Figure 5-18 Modify a User

• Deleting a User

Steps:

1. Click to select the user you want to delete and click **Delete**.
2. Click **OK** on the pop-up dialogue box to confirm the deletion.

Purpose:

Click **Refresh** to refresh the list.

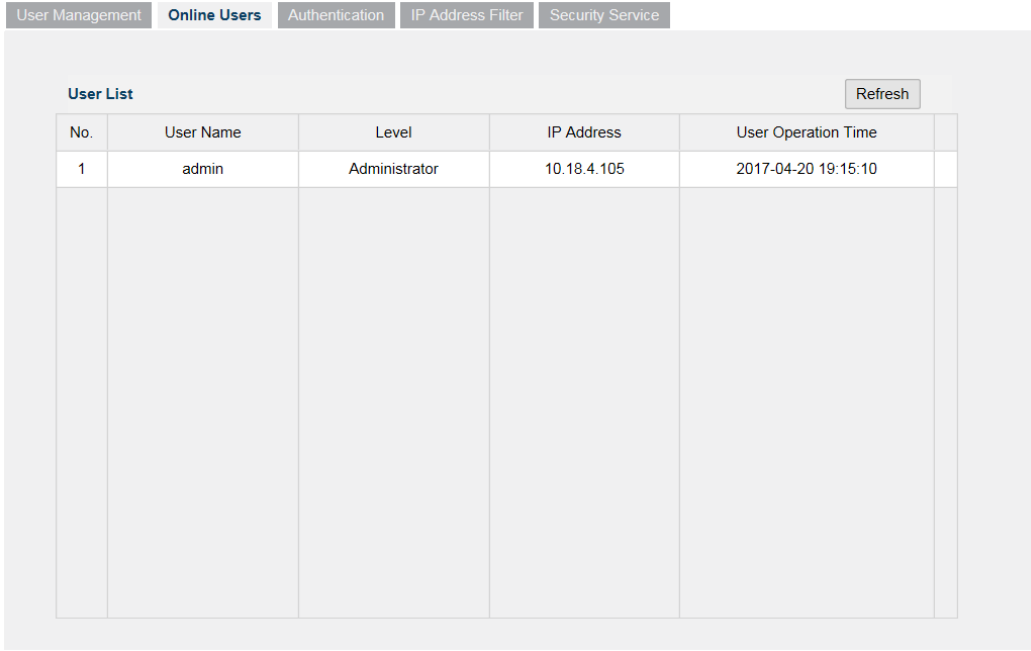


Figure 5-19 View the Online Users

Chapter 6 Network Settings

Purpose:

Follow the instructions in this chapter to configure the basic settings and advanced settings.

6.1 Configuring Basic Settings

Purpose:

You can configure the parameters, including TCP/IP, DDNS, PPPoE, Port, and NAT, etc., by following the instructions in this section.

6.1.1 Configuring TCP/IP Settings

Purpose:

TCP/IP settings must be properly configured before you operate the camera over network. The camera supports both the IPv4 and IPv6. Both versions can be configured simultaneously without conflicting to each other, and at least one IP version should be configured.

Steps:

1. Enter TCP/IP Settings interface: **Network > TCP/IP**

TCP/IP DDNS PPPoE Port NAT SNMP FTP Email HTTPS QoS 802.1x

NIC Type

☒ DHCP

IPv4 Address

IPv4 Subnet Mask

IPv4 Default Gateway

IPv6 Mode

IPv6 Address

IPv6 Subnet Mask

IPv6 Default Gateway

Mac Address

MTU

Multicast Address

☒ Enable Multicast Discovery

DNS Server

Preferred DNS Server

Alternate DNS Server

Figure 6-1 TCP/IP Settings

2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.
3. (Optional) Check the checkbox of **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.
4. Configure the DNS server. Input the preferred DNS server, and alternate DNS server.
5. Click **Save** to save the above settings.

Notes:

- The valid value range of MTU is 1280 to 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.
- A reboot is required for the settings to take effect.

6.1.2 Configuring DDNS Settings

Purpose:

If your camera is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

Before you start:

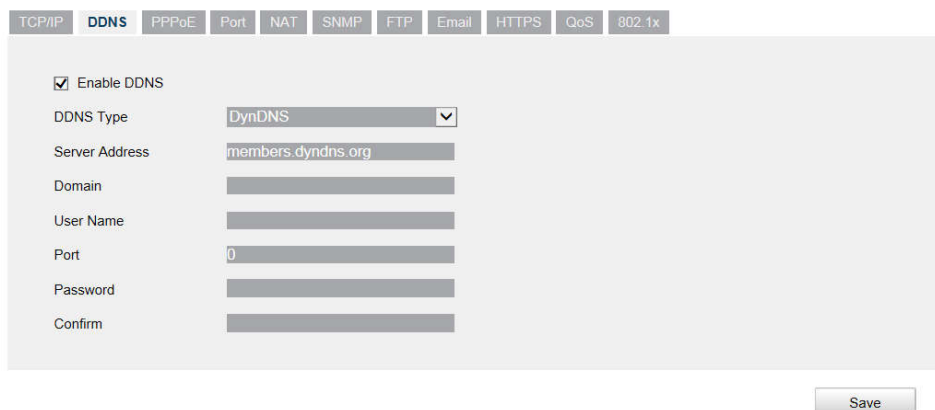
Registration on the DDNS server is required before configuring the DDNS settings of the camera.

Steps:

1. Enter the DDNS Settings interface: **Network > DDNS**.
2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Two DDNS types are selectable: DynDNS and NO-IP.
 - DynDNS:

Steps:

- (1) Enter **Server Address** of DynDNS (e.g. members.dyndns.org).
- (2) In the **Domain** text field, enter the domain name obtained from the DynDNS website.
- (3) Enter the **User Name** and **Password** registered on the DynDNS website.
- (4) Click **Save** to save the settings.



The screenshot shows the DDNS Settings interface. At the top, there is a navigation bar with tabs: TCP/IP, **DDNS**, PPPoE, Port, NAT, SNMP, FTP, Email, HTTPS, QoS, and 802.1x. Below the tabs, the 'Enable DDNS' checkbox is checked. The 'DDNS Type' dropdown menu is set to 'DynDNS'. The 'Server Address' field contains 'members.dyndns.org'. The 'Domain', 'User Name', 'Port' (set to 0), 'Password', and 'Confirm' fields are empty. A 'Save' button is located at the bottom right of the form.

Figure 6-2 DynDNS Settings

- NO-IP:

Steps:

(1) Choose the DDNS Type as NO-IP.

TCP/IP **DDNS** PPPoE Port NAT SNMP FTP Email HTTPS QoS 802.1x

☒ Enable DDNS

DDNS Type: NO-IP

Server Address:

Domain:

User Name:

Port: 0

Password:

Confirm:

Save

Figure 6-3 NO-IP DNS Settings

(2) Enter the Server Address as www.noip.com

(3) Enter the Domain name you registered.

(4) Enter the User Name and Password.

(5) Click **Save** and then you can view the camera with the domain name.

6.1.3 Configuring Port Settings

Purpose:

You can set the port No. of the camera, e.g., HTTP port, RTSP port and HTTPS port.

Steps:

1. Enter the Port Settings interface, **Network >Port**

TCP/IP DDNS PPPoE **Port** NAT SNMP FTP Email HTTPS QoS 802.1x

HTTP Port: 80

RTSP Port: 554

HTTPS Port: 443

Server Port: 8000

Save

Figure 6-4 Port Settings

2. Set the HTTP port, RTSP port, HTTPS port and server port of the camera.

HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.

RTSP Port: The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.

HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.

Server Port: The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

3. Click **Save** to save the settings.

Note: A reboot is required for the settings to take effect.

6.1.4 Configure NAT (Network Address Translation) Settings

Purpose:

NAT interface allows you to configure the UPnP™ parameters.

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

With the function enabled, you don't need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

Steps:

1. Enter the NAT settings interface. **Network > NAT.**
2. Check the checkbox to enable the UPnP™ function.
3. Choose a nickname for the camera, or you can use the default name.
4. Select the port mapping mode. Manual and Auto are selectable. And for manual port mapping, you can customize the value of the external port.
5. Click **Save** to save the settings.

Save

Note: The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the SNMP Settings interface: **Network > SNMP**.

Figure 6-6 SNMP Settings

2. Check the checkbox of Enable SNMPv1, Enable SNMP v2c, Enable SNMPv3 to enable the feature correspondingly.
3. Configure the SNMP settings.

Note: The settings of the SNMP software should be the same as the settings you configure here.

4. Click **Save** to save and finish the settings.

Notes:

- A reboot is required for the settings to take effect.
- To lower the risk of information leakage, you are suggested to enable SNMP v3 instead of SNMP v1 or v2.

6.2.2 Configuring FTP Settings

Purpose:

You can configure the FTP server related information to enable the uploading of the

captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

Steps:

1. Enter the FTP Settings interface: **Network > FTP**.

Figure 6-7 FTP Settings

2. Input the FTP address and port.
3. Configure the FTP settings; and the user name and password are required for the FTP server login.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4. Set the directory structure and picture filing interval.

Directory: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you

have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

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

Picture Name: Set the naming rule for captured picture files. You can choose **Default** in the drop-down list to use the default rule, that is,

IP address_channel number_capture time_event type.jpg
(e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg).

Or you can customize it by adding a **Custom Prefix** to the default naming rule.

5. Check the Upload Picture checkbox to enable the function.

Upload Picture: To enable uploading the captured picture to the FTP server.

Anonymous Access to the FTP Server (in which case the user name and password won't be required.): Check the **Anonymous** checkbox to enable the anonymous access to the FTP server.

Note: The anonymous access function must be supported by the FTP server.

6. Click **Save** to save the settings.

6.2.3 Configuring Email Settings

Purpose:

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video tampering, etc.

Before you start:

Please configure the DNS Server settings under **Network > TCP/IP** before using the Email function.

Steps:

1. Enter the TCP/IP Settings (**Network > TCP/IP**) to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

Note: Please refer to *Section 7.1.1 Configuring TCP/IP Settings* for detailed information.

2. Enter the Email Settings interface: **Network > Email**.
3. Configure the following settings:

Sender: The name of the email sender.

Sender's Address: The email address of the sender.

SMTP Server: IP address or host name (e.g., smtp.263xmail.com) of the SMTP Server.

SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.

Email Encryption: None, SSL, and TLS are selectable. When you select SSL or TLS and disable STARTTLS, e-mails will be sent after encrypted by SSL or TLS. The SMTP port should be set as 465 for this encryption method. When you select SSL or TLS and enable STARTTLS, emails will be sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

Note: If you want to use STARTTLS, make sure that the protocol is supported by your e-mail server. If you check the Enable STARTTLS checkbox when the protocol is not supported by your e-mail sever, your e-mail will not be encrypted.

Attached Image: Check the checkbox of Attached Image if you want to send emails with attached alarm images.

Interval: The interval refers to the time between two actions of sending attached pictures.

Authentication (optional): If your email server requires authentication, check this checkbox to use authentication to log in to this server and input the login user name and password.



- For your privacy and to better protect your system against security risks, we

strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

The **Receiver** table: Select the receiver to which the email is sent. Up to 3 receivers can be configured.

Receiver: The name of the user to be notified.

Receiver's Address: The email address of user to be notified.

TCP/IP DDNS PPPoE Port NAT SNMP FTP **Email** HTTPS QoS 802.1x

Sender

Sender's Address

SMTP Server

SMTP Port

E-mail Encryption

☐ Attached Image

Interval s

☐ Authentication

User Name

Password

Confirm

Receiver

No.	Receiver	Receiver's Address	Test
1			<input type="button" value="Test"/>
2			
3			

Figure 6-8 Email Settings

4. Click **Save** to save the settings.

6.2.4 HTTPS Settings

Purpose:

HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.

E.g., If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting https://192.168.1.64:443 via the web browser.

Steps:

1. Enter the HTTPS settings interface. **Network > HTTPS**.
2. Check the checkbox of Enable to enable the function.

Figure 6-9 HTTPS Configuration Interface

3. Create the self-signed certificate or authorized certificate.
 - Create the self-signed certificate
 - (1) Select **Create Self-signed Certificate** as the Installation Method.
 - (2) Click **Create** button to enter the creation interface.

Figure 6-10 Create Self-signed Certificate

- (3) Enter the country, host name/IP, validity and other information.
- (4) Click **OK** to save the settings.

Note: If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

- Create the authorized certificate

- (1) Select **Create the certificate request first and continue the installation** as the Installation Method.
 - (2) Click **Create** button to create the certificate request. Fill in the required information in the popup window.
 - (3) Download the certificate request and submit it to the trusted certificate authority for signature.
 - (4) After receiving the signed valid certificate, import the certificate to the device.
4. There will be the certificate information after your successfully creating and installing the certificate.



Figure 6-11 Installed Certificate

5. Click the **Save** button to save the settings.

6.2.5 Configuring QoS Settings

Purpose:

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

Steps:

1. Enter the QoS Settings interface: **Network > QoS**

Figure 6-12 QoS Settings

2. Configure the QoS settings, including Video/Audio DSCP, Event/Alarm DSCP and Management DSCP.

The valid value range of the DSCP is 0 to 63. The bigger the DSCP value is, the higher the priority is.

Note: DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.

3. Click **Save** to save the settings.

Note: A reboot is required for the settings to take effect.

6.2.6 Configuring 802.1X Settings

Purpose:

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

Before you start:

The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.



- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a*

minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Enter the 802.1X Settings interface, **Network > 802.1X**

Figure 6-13 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including Protocol, EAPOL version, User Name, Password and Confirm.

Note: The **EAPOL version** must be identical with that of the router or the switch.

4. Enter the user name and password to access the server.
5. Click **Save** to finish the settings.

Note: A reboot is required for the settings to take effect.

Chapter 7 Video/Audio Settings

Purpose:

Follow the instructions below to configure the video setting, audio settings, ROI, and Display info. on Stream.

7.1 Configuring Video Settings

Steps:

1. Enter the Video Settings interface, **Image > Video**

Setting	Value
Stream Type	Main Stream(Normal)
Video Type	Video Stream
Resolution	1920*1080P
Bitrate Type	Variable
Video Quality	Medium
Frame Rate	25 fps
Max. Bitrate	4096 Kbps
Video Encoding	H.264
H.264+	OFF
Profile	Main Profile
I Frame Interval	50
SVC	OFF
Smoothing	50 [Clear<->Smooth]

Save

Figure 7-1 Video Settings

2. Select the Stream Type of the camera to main stream (normal), sub-stream or third stream.

Notes:

- The main stream is usually for recording and live view with good bandwidth, and the sub-stream can be used for live view when the bandwidth is limited.
3. You can customize the following parameters for the selected stream type.

Video Type:

Select the stream type to video stream, or video & audio composite stream. The

audio signal will be recorded only when the **Video Type** is **Video & Audio**.

Resolution:

Select the resolution of the video output.

Bitrate Type:

Select the bitrate type to constant or variable.

Video Quality:

When bitrate type is selected as Variable, 6 levels of video quality are selectable.

Frame Rate:

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

Max. Bitrate:

Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Note: The maximum limit of the max. bitrate value varies according to different camera platforms. For certain cameras, the maximum limit is 8192 Kbps or 12288 Kbps.

Video Encoding:

If the Stream Type is set to main stream, H.264 and H.265 are selectable, and if the stream type is set to sub stream or third stream, H.264, MJPEG, and H.265 are selectable. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate and image quality.

Note: Selectable video encoding types may vary according to different camera modes.

H.264+ and H.265+:

- **H.264+:** If you set the main stream as the stream type, and H.264 as the video encoding, you can see H.264+ available. H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.264,

H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

- **H.265+:** If you set the main stream as the stream type, and H.265 as the video encoding, you can see H.265+ available. H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

You need to reboot the camera if you want to turn on or turn off the H.264+/H.265+. If you switch from H.264+ to H.265+ directly, and vice versa, a reboot is not required by the system.

Notes:

- Upgrade your video player to the latest version if live view or playback does not work properly due to compatibility.
- The bitrate type must be variable if you want to use H.264+ or H.265+.
- With H.264+/H.265+ enabled, the parameters such as profile, I frame interval, video quality, and SVC are greyed out if the bitrate type is variable.
- With H.264+/H.265+ enabled, some functions are not supported. For those functions, corresponding interfaces will be hidden.
- H.264+/H.265+ can spontaneously adjust the bitrate distribution according the requirements of the actual scene in order to realize the set maximum average bitrate in the long term. The camera needs at least 3 days to adapt to a fixed monitoring scene.

Max. Average Bitrate:

When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the Max. Average Bitrate box. You can also set the maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.

Profile:

Basic profile, Main Profile, and High Profile for coding are selectable.

I Frame Interval:

Set I Frame Interval from 1 to 400.

SVC:

Scalable Video Coding is an extension of the H.264/AVC standard. Select OFF/ON to disable/enable the SVC function. Select Auto and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

Smoothing:

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

- Click **Save** to save the settings.

Note:

The video parameters vary according to different camera models. Refer to the actual display page for camera functions.

7.2 Configuring Audio Settings

Steps:

- Enter the Audio Settings interface: **Image > Audio**.

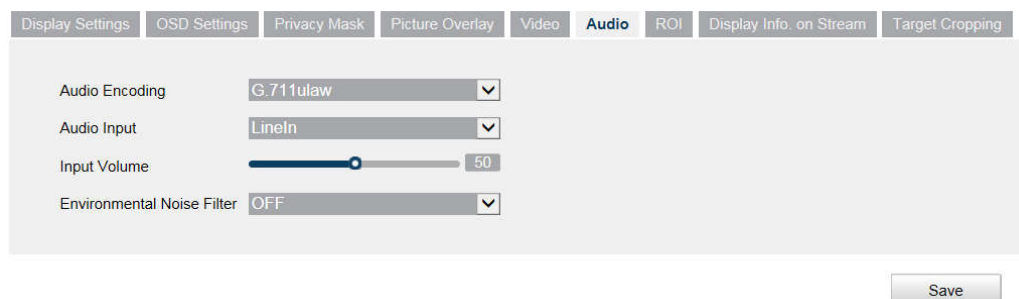


Figure 7-2 Audio Settings

- Configure the following settings.

Note: Audio settings vary according to different camera models.

Audio Encoding: G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 and PCM are

selectable. For MP2L2, the Sampling Rate and Audio Stream Bitrate are configurable. For PCM, the Sampling Rate can be set.

Audio Input: MicIn and LineIn are selectable for the connected microphone and pickup respectively.

Input Volume: 0-100 adjustable.

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

3. Click **Save** to save the settings.

7.3 Configuring ROI Encoding

Purpose:

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

Note: ROI function varies according to different camera models.

Display Settings

OSD Settings

Privacy Mask

Picture Overlay

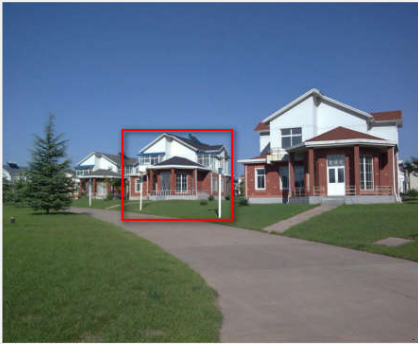
Video

Audio

ROI

Display Info. on Stream

Target Cropping



Draw Area

Clear

Stream Type

Stream Type

Main Stream(Normal)

Fixed Region

☐ Enable

Region No.

1

ROI Level

3

Region Name

Dynamic Region

☐ Enable Face Tracking

ROI Level

3

Save

Figure 7-3 Region of Interest Settings

Steps:

1. Enter the ROI settings interface: **Image > ROI**.
2. Select the Stream Type for ROI encoding.
3. Check the checkbox of **Enable** under Fixed Region item.
4. Set **Fixed Region** for ROI.
 - (1) Select the Region No. from the drop-down list.
 - (2) Check the **Enable** checkbox to enable ROI function for the chosen region.
 - (3) Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.
 - (4) Select the ROI level.
 - (5) Enter a region name for the chosen region.
 - (6) Click **Save** to save the settings of ROI settings for chosen fixed region.
 - (7) Repeat steps (1) to (6) to setup other fixed regions.
5. Set **Dynamic Region** for ROI.
 - (1) Check the checkbox to enable **Face Tracking**.
6. Click **Save** to save the settings.

Note: To enable face tracking function, the face detection function should be supported and enabled.

(2) Select the ROI level.

Note: ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

7.4 Display Info. on Stream

Check the checkbox of **Enable Dual-VCA**, and the information of the objects (e.g. human, vehicle, etc.) will be marked in the video stream. Then, you can set rules on the connected rear-end device to detect the events including line crossing, intrusion, etc.

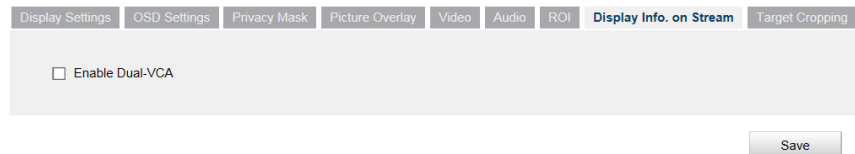


Figure 7-4 Display Info. on Stream

7.5 Configuring Target Cropping

Purpose:

You can specify a target area on the live video, and then the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.

Note: Target cropping function varies according to different camera models.

Steps:

1. Enter the **Target Cropping** settings interface.
2. Check **Enable Target Cropping** checkbox to enable the function.
3. Set Third Stream as the stream type.
4. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
5. Click **Save** to save the settings.

Chapter 8 Image Settings

Purpose:

Follow the instructions in this chapter to configure the image parameters, including display settings, OSD settings, privacy mask, and picture overlay.

8.1 Configuring Display Settings

Purpose:

Configure the image adjustment, exposure settings, day/night switch, backlight settings, white balance, image enhancement, video adjustment, and other parameters in display settings.

Note: The display parameters vary according to the different camera models. Please refer to the actual interface for details.

8.1.1 Day/Night Auto-Switch

Steps:

1. Enter the Display Settings interface, **Image > Display Settings**.

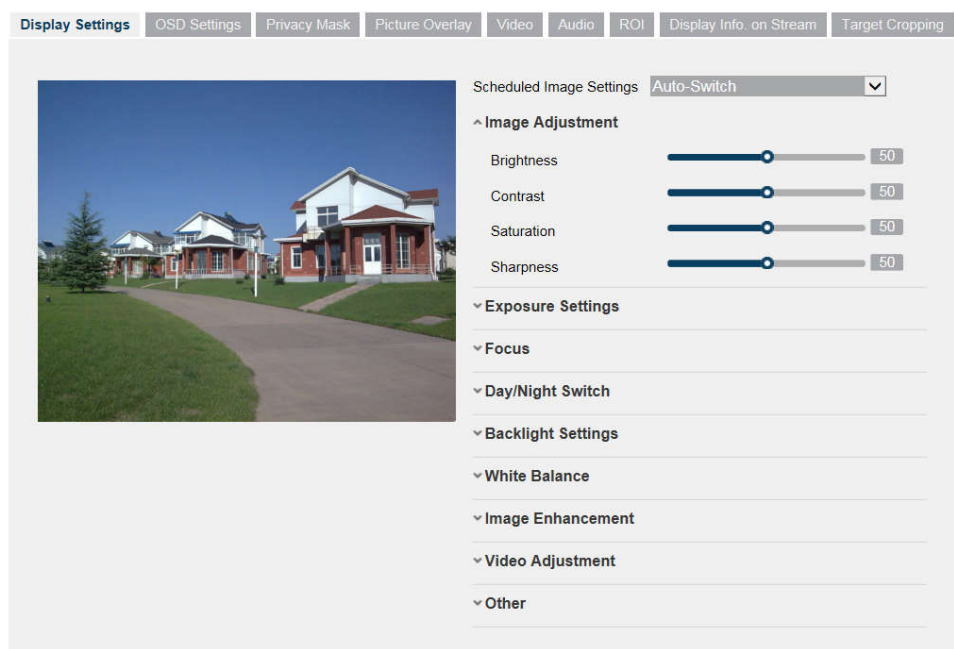


Figure 8-1 Display Settings of Day/Night Auto-Switch

2. Set the image parameters of the camera.

Note: In order to guarantee the image quality in different illumination, it provides two sets of parameters for users to configure.

- **Image Adjustment**

Brightness describes bright of the image, which ranges from 1 to 100.

Contrast describes the contrast of the image, which ranges from 1 to 100.

Saturation describes the colorfulness of the image color, which ranges from 1 to 100.

Sharpness describes the edge contrast of the image, which ranges from 1 to 100.

- **Exposure Settings**

If the camera is equipped with the fixed lens, only **Manual** is selectable, and the iris mode is not configurable.

If **Auto** is selected, you can set the auto iris level from 0 to 100.

The **Exposure Time** refers to the electronic shutter time, which ranges from 1 to 1/100,000s. Adjust it according to the actual luminance condition.

Gain of image can also be manually configured from 0 to 100. The bigger the value is, the brighter would the image be, and the noise would also be amplified to a larger extent.

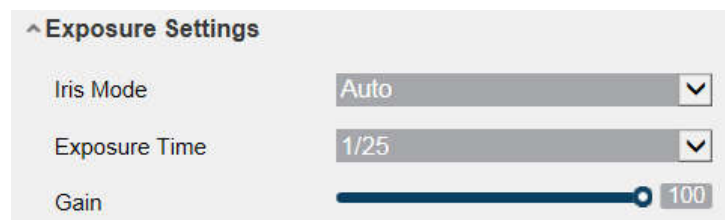


Figure 8-2 Exposure Settings

- **Day/Night Switch**

Select the Day/Night Switch mode according to different surveillance demand.

Day, Night, Auto, Scheduled-Switch, and Triggered by alarm input are selectable for day/night switch.

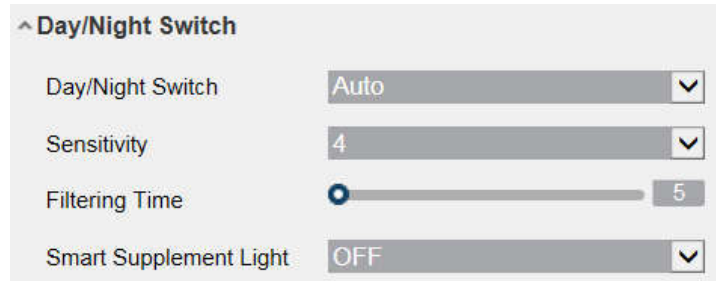


Figure 8-3 Day/Night Switch

Day: the camera stays at day mode.

Night: the camera stays at night mode.

Auto: the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0 to 7, the higher the value is, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5s to 120s.

Scheduled-Switch: Set the start time and the end time to define the duration for day/night mode.

Triggered by alarm input: The switch is triggered by alarm input. You can set the triggered mode to day or night.

Smart Supplement Light: Set the supplement light as ON, and Auto and Manual are selectable for light mode.

Select Auto, and the supplement light changes according to the actual luminance. E.g., if the current scene is bright enough, then the supplement light adjusts itself to lower power; and if the scene is not bright enough, the light adjusts itself to higher power.

Select Manual, and you can adjust the supplement by adjusting the distance. E.g., if the object is near the camera, the device adjusts the supplement light to lower power, and the light is in higher power if the object is far away.

- **Backlight Settings**

BLC Area: If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. OFF, Up, Down, Left, Right, Center, Auto, and Custom are

selectable.

Note: If BLC mode is set as Custom, you can draw a red rectangle on the live view image as the BLC area.

WDR: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

HLC: High Light Compression function can be used when there are strong lights in the scene affecting the image quality.

- **White Balance**

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



Figure 8-4 White Balance

- **Image Enhancement**

Digital Noise Reduction: DNR reduces the noise in the video stream. OFF, Normal and Expert are selectable. Set the DNR level from 0 to 100 in Normal Mode. Set the DNR level from both space DNR level [0-100] and time DNR level [0-100] in Expert Mode.

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

EIS (Electrical Image Stabilizer): EIS reduces the effects of vibration in a video.

Grey Scale: You can choose the range of the grey scale as [0-255] or [16-235].

- **Video Adjustment**

Camera Rotation: It mirrors the image so you can see it inversed. Mirror, Flip, 180, and Normal are selectable.

Rotate: To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene.

When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.

Scene Mode: Choose the scene as indoor or outdoor according to the real environment.

Video Standard: 50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

Capture Mode: It's the selectable video input mode to meet the different demands of field of view and resolution.

Lens Distortion Correction: For cameras equipped with motor-driven lens, image may appear distorted to some extent. Turn on this function to correct the distortion.

- **Others**

Some camera models support CVBS, SDI, or HDMI output. Set the local output ON or OFF according to the actual device.

8.1.2 Day/Night Scheduled-Switch

Day/Night scheduled-switch configuration interface enables you to set the camera parameters for day and night separately, guaranteeing the image quality in different illumination.

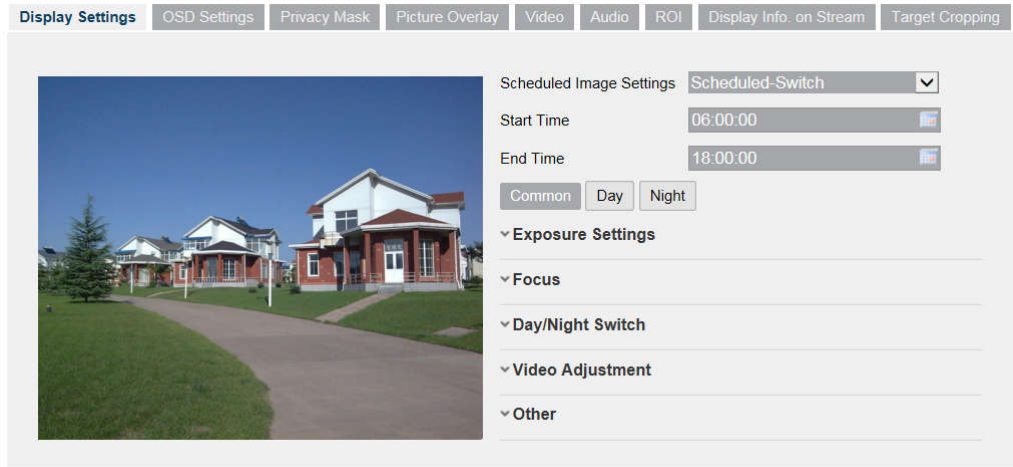


Figure 8-5 Day/Night Scheduled-Switch Configuration Interface

Steps:

1. Click the calendar icon to select the start time and the end time of the switch.

Notes:

- The start time and end time refer to the valid time for day mode.
- The time period can start and end on two days in a row. For example, if you set start time as 10:00 and end time as 1:00, the day mode will be activated at 10 o'clock in the morning and stopped at 1 o'clock early in the next morning.

2. Click Common tab to configure the common parameters applicable to the day mode and night mode.

Note: For the detailed information of each parameter, please refer to *Section 9.1.1 Day/Night Auto-Switch*.

3. Click Day tab to configure the parameters applicable for day mode.
4. Click Night tab to configure the parameters applicable for night mode.

Note: The settings saved automatically if any parameter is changed.

8.2 Configuring OSD Settings

Purpose:

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.

Figure 8-6 OSD Settings

Steps:

1. Enter the OSD Settings interface: **Image > OSD Settings**.
2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format and date format.
5. Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.
6. Configure the text overlay settings.
 - (1) Check the checkbox in front of the textbox to enable the on-screen display.
 - (2) Input the characters in the textbox.

Note: Up to 8 text overlays are configurable.

7. Adjust the position and alignment of text frames.

Left align, right align and custom are selectable. If you select custom, you can use the mouse to click and drag text frames in the live view window to adjust their positions.

Note: The alignment adjustment is only applicable to Text Overlay items.

8. Click **Save** to save the settings.

8.3 Configuring Privacy Mask

Purpose:

Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

Steps:

1. Enter the Privacy Mask Settings interface: **Configuration** > **Image** > **Privacy Mask**.
2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click **Draw Area**.

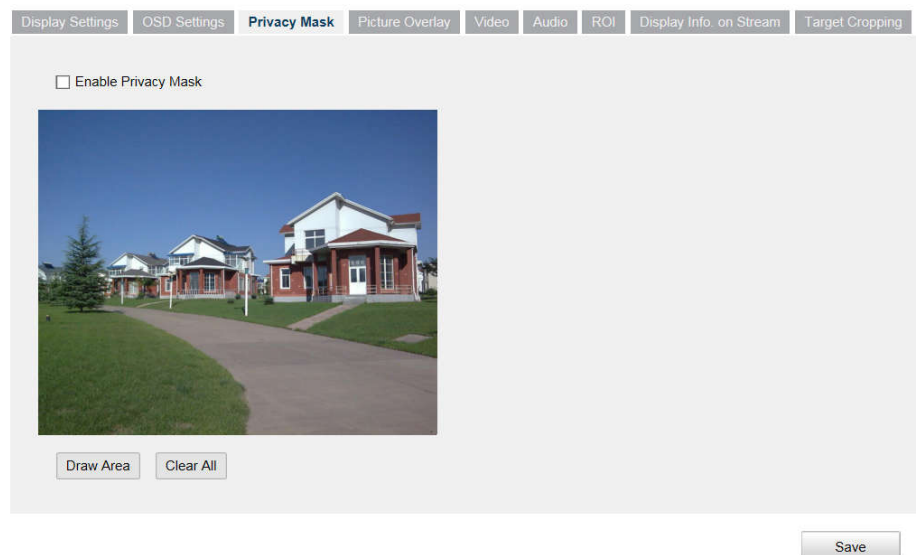


Figure 8-7 Privacy Mask Settings

4. Click and drag the mouse in the live video window to draw the mask area.
- Note:** You are allowed to draw up to 4 areas on the same image.
5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
 6. Click **Save** to save the settings.

8.4 Configuring Picture Overlay

Purpose:

Picture overlay enables you to overlay a picture on the image. This function enables a certain enterprise or users to overlay their logo on the image.

Steps:

1. Enter the Picture Overlay Settings interface, **Configuration > Image > Picture Overlay**.



Figure 8-8 Picture Overlay

2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Check **Enable Picture Overlay** checkbox to enable the function.
5. Set X Coordinate and Y Coordinate values adjust the picture position on the image. Adjust Picture Width and Picture Height to the desired size.
6. Click **Save** to save settings.

Note: The picture must be in RGB24 bmp format and the maximum picture size is 128*128.

Chapter 9 Event Settings

This section explains how to configure the network camera to respond to alarm events, including basic event and smart event.

9.1 Basic Events

You can configure the basic events by following the instructions in this section, including motion detection, video tampering, alarm input, alarm output, and exception, etc. These events can trigger the linkage methods, such as Notify IP Server, Send Email, Trigger Alarm Output, etc.

Note: Check the checkbox of Notify IP Server if you want the alarm information to be pushed to PC or mobile client software as soon as the alarm is triggered.

9.1.1 Configuring Motion Detection

Purpose:

Motion detection detects the moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.

In order to detect the moving objects accurately and reduce the false alarm rate, normal configuration and expert configuration are selectable for different motion detection environment.

● Normal Configuration

Normal configuration adopts the same set of motion detection parameters in the daytime and at night.

Tasks 1: Set the Motion Detection Area

Steps:

1. Enter the motion detection settings interface: **Event > Motion Detection**.
2. Check the checkbox of **Enable Motion Detection**.
3. Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles.

Note: Select Disable for rules if you don't want the detected objects displayed with the green rectangles. Select disable rules from **Configuration > Local Configuration > Live View Parameters-rules**.

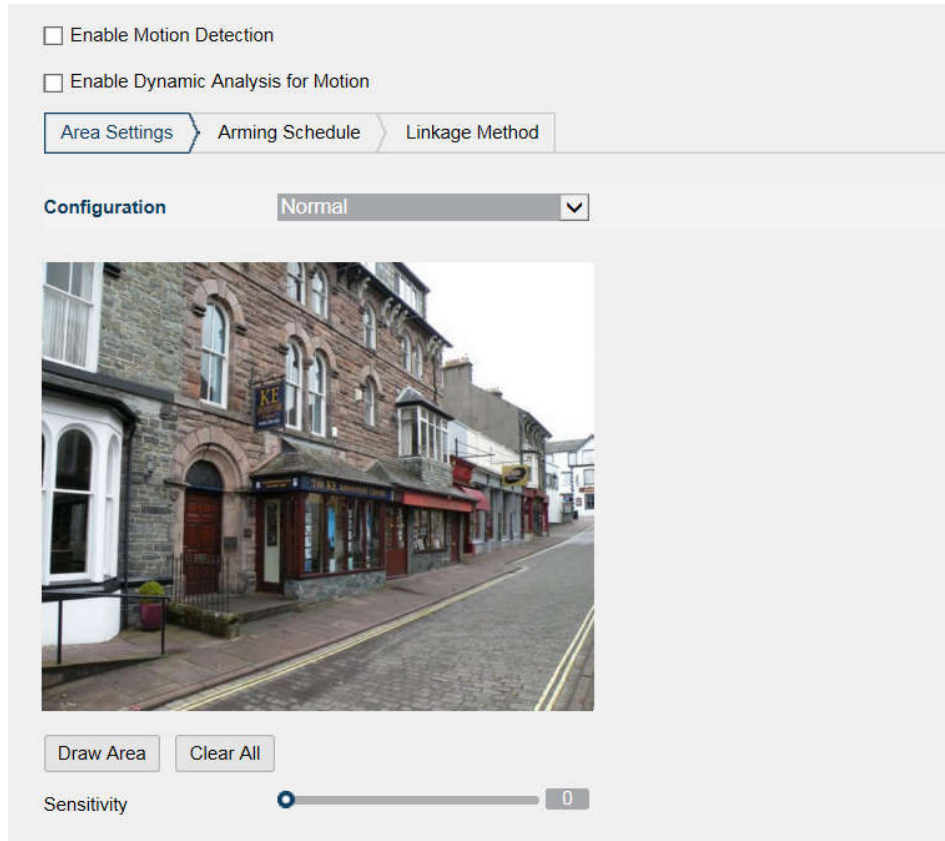


Figure 9-1 Enable Motion Detection

4. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area.
5. (Optional) Click **Clear All** to clear all of the areas.
6. (Optional) Move the slider to set the sensitivity of the detection.

Task 2: Set the Arming Schedule for Motion Detection

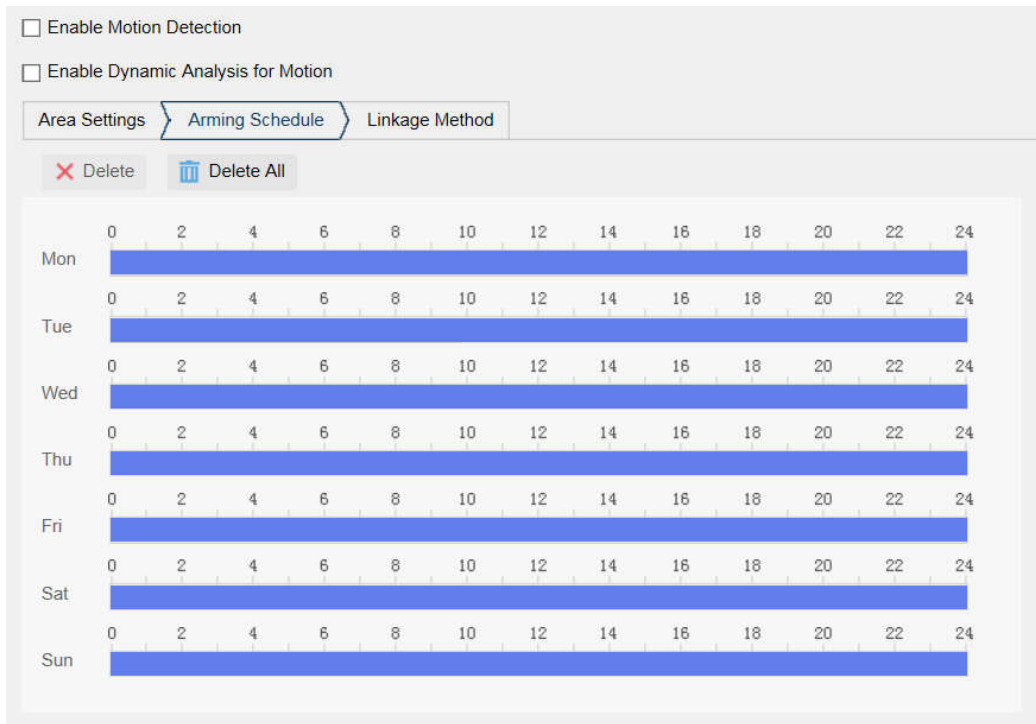


Figure 9-2 Arming Schedule

Steps:

1. Click **Arming Schedule** to edit the arming schedule.
2. Click on the time bar and drag the mouse to select the time period.

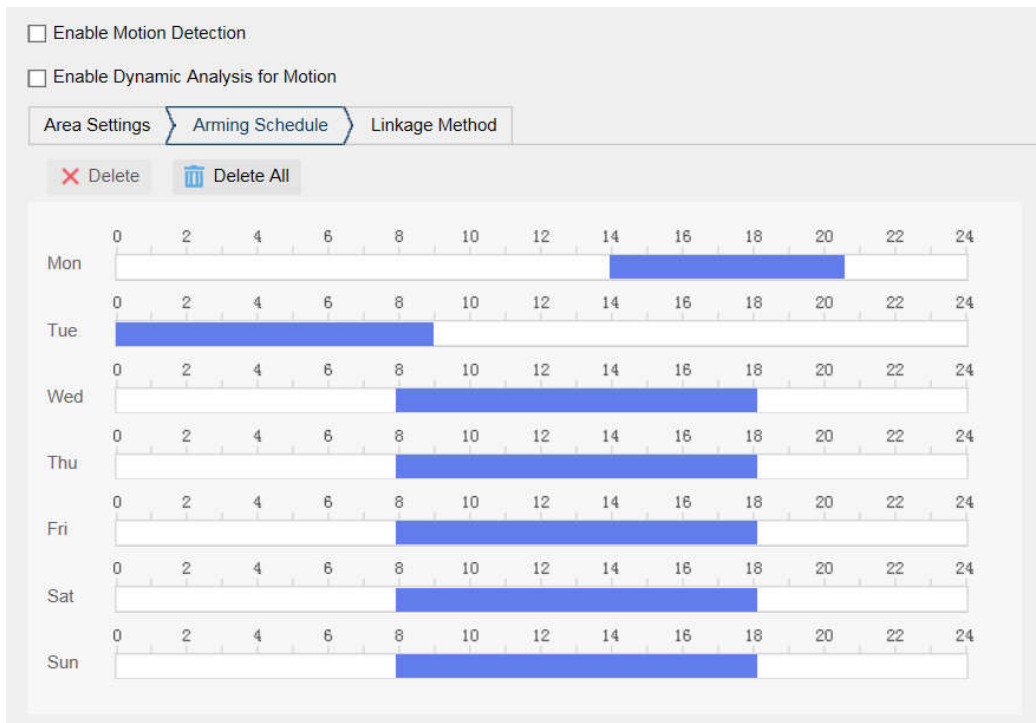


Figure 9-3 Arming Schedule

Note: Click on the selected time period, you can adjust the time period to the desired time by either moving the time bar or input the exact time period.

3. (Optional) Click Delete to delete the current arming schedule, or click Save to save the settings.
4. Move the mouse to the end of each day, a copy dialogue box pops up, and you can copy the current settings to other days.
5. Click **Save** to save the settings.

Note: The time of each period can't be overlapped. Up to 8 periods can be configured for each day.

Task 3: Set the Linkage Method for Motion Detection

Check the checkbox to select the linkage method. Audible Warning, Send Email, Notify IP Server, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output are selectable. You can specify the linkage method when an event occurs.

<input type="checkbox"/> Enable Motion Detection		
<input type="checkbox"/> Enable Dynamic Analysis for Motion		
Area Settings > Arming Schedule > Linkage Method		
<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Recording
<input type="checkbox"/> Send Email	<input type="checkbox"/> A->1	<input type="checkbox"/> A1
<input checked="" type="checkbox"/> Notify IP Server		
<input type="checkbox"/> Upload to FTP/Memory Card/NAS		

Figure 9-4 Linkage Method

Note: The linkage methods vary according to the different camera models.

- **Audible Warning**

Trigger the audible warning locally. And it only supported by the device that have the audio output.

- **Notify IP Server**

Send an exception or alarm signal to remote management software when an event occurs.

- **Send Email**

Send an email with alarm information to a user or users when an event occurs.

Note: To send the Email when an event occurs, please refer to *Section 7.2.3* to complete Email setup in advance.

- **Upload to FTP/Memory Card/NAS**

Capture the image when an alarm is triggered and upload the picture to a FTP server.

Notes:

- Set the FTP address and the remote FTP server first. Refer to *Section 7.2.2 Configuring FTP Settings* for detailed information.
- Go to **Event > Capture > Capture Parameters** page, enable the event-triggered snapshot, and set the capture interval and capture number.
- The captured image can also be uploaded to the available SD card or network disk.

- **Trigger Channel**

The video will be recorded when the motion is detected. You have to set the recording schedule to realize this function. Please refer to *Section 11.1* for detailed information.

- **Trigger Alarm Output**

Trigger one or more external alarm outputs when an event occurs.

Note: To trigger an alarm output when an event occurs, please refer to *Section 10.1.4 Configuring Alarm Output* to set the related parameters.

● Expert Configuration

Expert mode is mainly used to configure the sensitivity and proportion of object on each area for different day/night switch.



Figure 9-5 Expert Mode of Motion Detection

● Day/Night Switch OFF

Steps:

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **OFF** for **Switch Day and Night Settings**.
3. Select the area by clicking the area No.
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area.
5. Set the arming schedule and linkage method as in the normal configuration mode.

6. Click **Save** to save the settings.

- Day/Night Auto-Switch

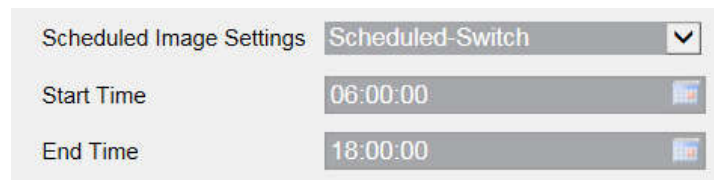
Steps:

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **Auto-Switch** for **Switch Day and Night Settings**.
3. Select the area by clicking the area No..
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.
6. Set the arming schedule and linkage method as in the normal configuration mode.
7. Click **Save** to save the settings.

- Day/Night Scheduled-Switch

Steps:

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **Scheduled-Switch** for **Switch Day and Night Settings**.



The screenshot shows a configuration window titled "Scheduled Image Settings". It contains three rows of settings:

Scheduled Image Settings	Scheduled-Switch	▼
Start Time	06:00:00	📅
End Time	18:00:00	📅

Figure 9-6 Day/Night Scheduled-Switch

3. Select the start time and the end time for the switch timing.
4. Select the area by clicking the area No..
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
6. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.
7. Set the arming schedule and linkage method as in the normal configuration mode.

8. Click **Save** to save the settings.

9.1.2 Configuring Video Tampering Alarm

Purpose:

You can configure the camera to trigger the alarm when the lens is covered and take certain alarm response actions.

Steps:

1. Enter the video tampering Settings interface, **Event > Video Tampering**.

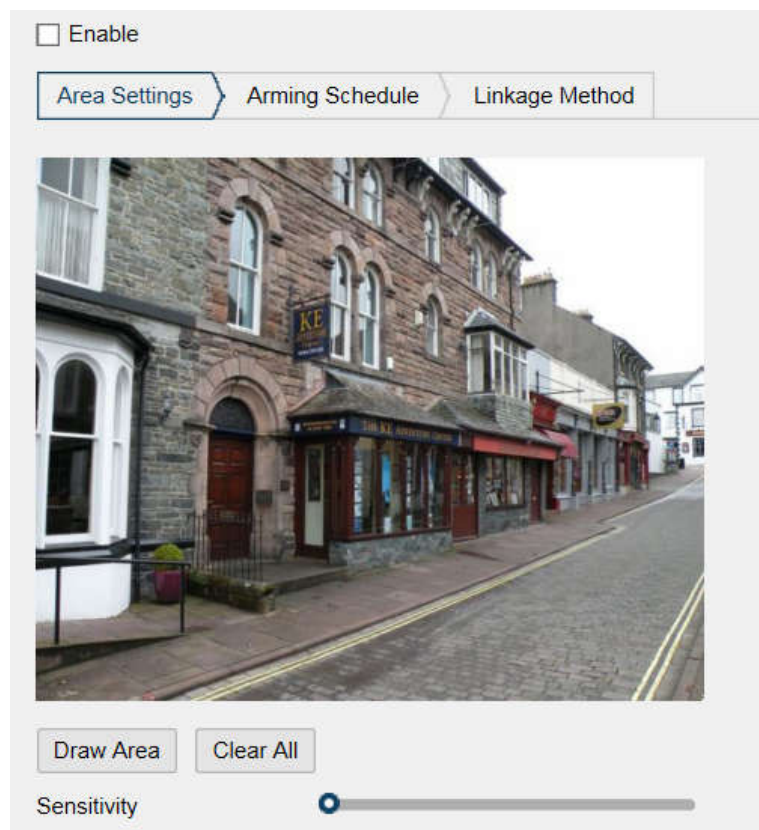


Figure 9-7 Video Tampering Alarm

2. Check **Enable Video Tampering** checkbox to enable the video tampering detection.
3. Set the video tampering area. Refer to *Task 1: Set the Motion Detection Area* in *Section 10.1.1*.
4. Click **Edit** to edit the arming schedule for video tampering. The arming schedule

configuration is the same as the setting of the arming schedule for motion detection. Refer to **Task 2: Set the Arming Schedule for Motion Detection** in *Section 10.1.1*.

5. Check the checkbox to select the linkage method taken for the video tampering. Audible warning, Notify IP Server, send email and trigger alarm output are selectable. Please refer to **Task 3: Set the Linkage Method for Motion Detection** in *Section 10.1.1*.
6. Click **Save** to save the settings.

9.1.3 Configuring Alarm Input

Steps:

1. Enter the Alarm Input Settings interface: **Event > Alarm Input**.
2. Choose the alarm input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed). Edit the name to set a name for the alarm input (optional).

Alarm Input No. IP Address

Alarm Type Alarm Name

☒ Enable Alarm Input Handling

Arming Schedule | Linkage Method

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figure 9-8 Alarm Input Settings

3. Click **Arming Schedule** to set the arming schedule for the alarm input. Refer to

Task 2: Set the Arming Schedule for Motion Detection in Section 10.1.1.

4. Click **Linkage Method** and check the checkbox to select the linkage method taken for the alarm input. Refer to **Task 3: Set the Linkage Method for Motion Detection** in Section 10.1.1.
5. You can copy your settings to other alarm inputs.
6. Click **Save** to save the settings.

9.1.4 Configuring Alarm Output

Alarm Output No. IP Address

Delay Alarm Name

Alarm Status (cannot copy)

Arming Schedule

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figure 9-9 Alarm Output Settings

Steps:

1. Enter the Alarm Output Settings interface: **Event > Alarm Output**.
2. Select one alarm output channel in the **Alarm Output** drop-down list. You can also set a name for the alarm output (optional).
3. The Delay time can be set to 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min or Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.

4. Click **Arming Schedule** to enter the Edit Schedule Time interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to *Task 2: Set the Arming Schedule for Motion Detection* in *Section 10.1.1*.
5. You can copy the settings to other alarm outputs.
6. Click **Save** to save the settings.

9.1.5 Handling Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflicted and illegal login to the cameras.

Steps:

1. Enter the Exception Settings interface: **Event > Exception**.
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to *Task 3: Set the Linkage Method for Motion Detection* in *Section 10.1.1*.

Exception Type: HDD Full	
<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output
<input type="checkbox"/> Send Email	<input type="checkbox"/> A->1
<input checked="" type="checkbox"/> Notify IP Server	

Figure 9-10 Exception Settings

3. Click **Save** to save the settings.

9.2 Smart Events

You can configure the smart events by following the instructions in this section, including audio exception detection, defocus detection, scene change detection, intrusion detection, and line crossing detection, etc. These events can trigger the linkage methods, such as Notify IP Server, Send Email, Trigger Alarm Output, etc.

9.2.1 Configuring Audio Exception Detection

Purpose:

Audio exception detection function detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken when the alarm is triggered.

Note: Audio exception detection function varies according to different camera models.

Steps:

1. Enter the Audio Exception Detection settings interface, **Event > Audio Exception Detection**.

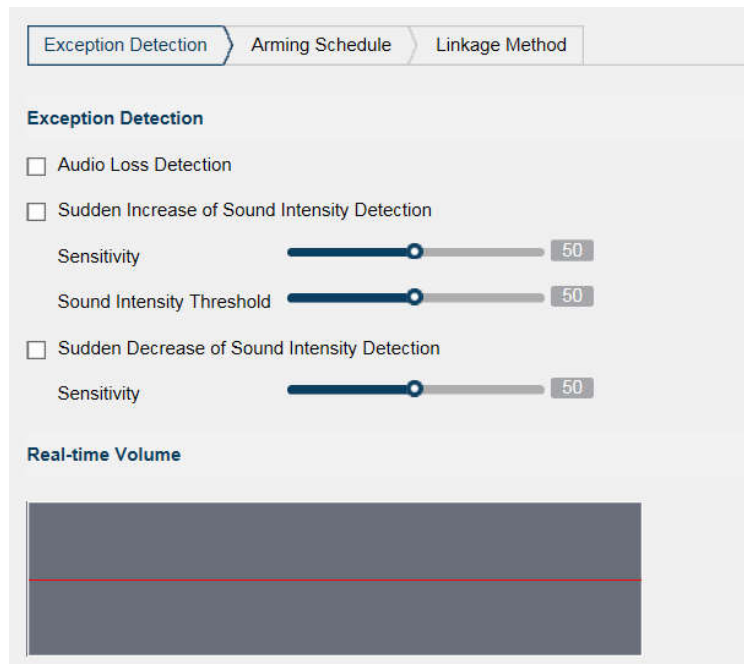


Figure 9-11 Audio Exception Detection

2. Check the checkbox of **Audio Loss Exception** to enable the audio loss detection function.
3. Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
4. Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity and threshold for sound steep drop.

Notes:

- Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.
 - Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
 - You can view the real-time volume of the sound on the interface.
5. Click **Arming Schedule** to set the arming schedule. Refer to **Task 2 Set the Arming Schedule for Motion Detection** in Section 10.1.1 for detailed steps.

6. Click **Linkage Method** and select the linkage methods for audio exception, including Notify IP Server, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel for recording and Trigger Alarm Output.
7. Click **Save** to save the settings.

9.2.2 Configuring Defocus Detection

Purpose:

The image blur caused by defocus of the lens can be detected, and some certain actions can be taken when the alarm is triggered.

Note: Defocus detection function varies according to different camera models.

Steps:

1. Enter the Defocus Detection settings interface, **Configuration > Event > Smart Event > Defocus Detection**.

☐ Enable

Sensitivity 50

<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output
<input type="checkbox"/> Send Email	<input type="checkbox"/> A->1
<input checked="" type="checkbox"/> Notify IP Server	

Figure 9-12 Configuring Defocus Detection

2. Check the checkbox of **Enable** to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100, and the higher the value is, the more easily the defocus image can trigger the alarm.
4. Select the linkage methods for defocus, including Notify IP Server, Send Email and Trigger Alarm Output.
5. Click **Save** to save the settings.

9.2.3 Configuring Scene Change Detection

Purpose:

Scene change detection function detects the change of surveillance environment affected by the external factors, such as the intentional rotation of the camera. Some certain actions can be taken when the alarm is triggered.

Note: Scene change detection function varies according to different camera models.

Steps:

1. Enter the Scene Change Detection settings interface, **Event > Scene Change Detection**.

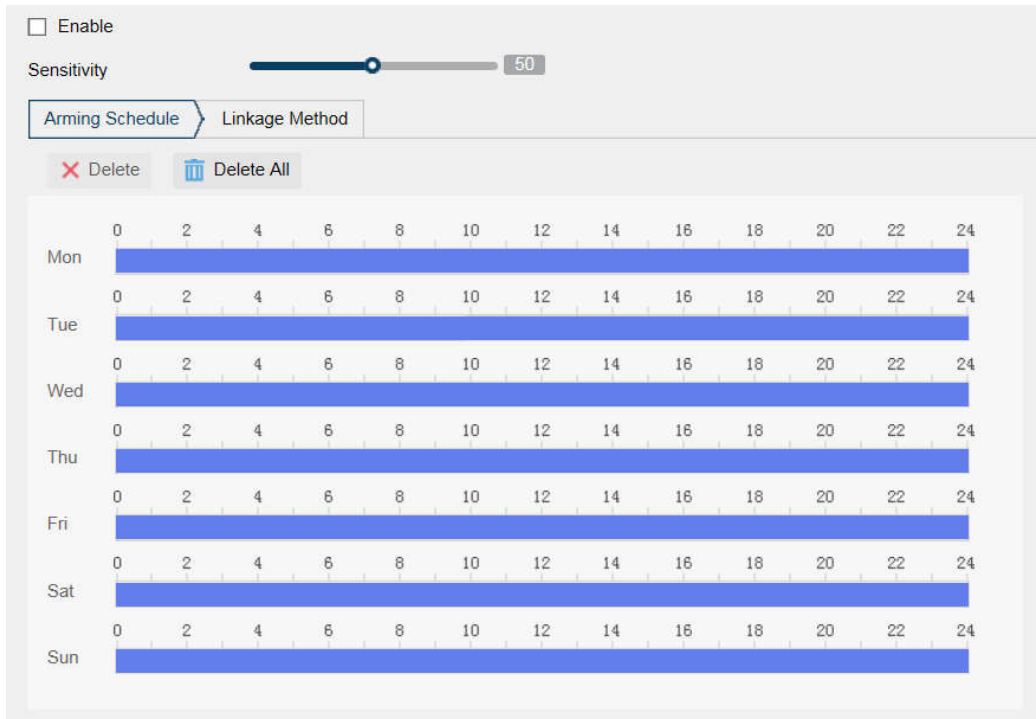


Figure 9-13 Scene Change Detection

2. Check the checkbox of **Enable** to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100, and the higher the value is, the more easily the change of scene can trigger the alarm.
4. Click **Arming Schedule** to set the arming schedule. Refer to *Task 2 Set the Arming Schedule for Motion Detection* in *Section 10.1.1* for detailed steps.
5. Click **Linkage Method** to select the linkage methods for scene change, including Notify IP Server, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output.
6. Click **Save** to save the settings.

9.2.4 Configuring Face Detection

Purpose:

Face detection function detects the face appears in the surveillance scene, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Face Detection settings interface, **Event > Face Detection**.
 2. Check the **Enable Face Detection** checkbox to enable the function.
 3. Check the checkbox of **Enable Dynamic Analysis** for Face Detection, and then the detected face is marked with green rectangle on the live video.
- Note:** To mark the detected face on the live video, go to **System > Local** to enable the **Rules**.
4. Click-and-drag the slider to set the detection sensitivity. The Sensitivity ranges from 1 to 5. The higher the value is, the more easily the face can be detected.
 5. Click **Arming Schedule** to set the arming schedule. Refer to ***Task 2 Set the Arming Schedule for Motion Detection*** in *Section 10.1.1* for detailed steps.
 6. Click **Linkage Method** to select the linkage methods for face detection. Refer to ***Task 3: Set the Linkage Method Taken for Motion Detection*** in *Section 10.1.1*.

☐ Enable Face Detection
☐ Enable Dynamic Analysis for Face Detection
 Sensitivity: 3

Arming Schedule
Linkage Method

✖ Delete
Delete All

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

Figure 9-14 Face Detection

7. Click **Save** to save the settings.

9.2.5 Configuring Intrusion Detection

Purpose:

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Note: Intrusion detection function varies according to different camera models.

Steps:

1. Enter the Intrusion Detection settings interface, **Configuration> Event > Smart Event > Intrusion Detection**.

☐ Enable

Area Settings | Arming Schedule | Linkage Method

Region: 1

Draw Area | Clear

Threshold(s): 0

Sensitivity: 50

Percentage: 1

Figure 9-15 Intrusion Detection

2. Check the checkbox of **Enable Intrusion Detection** to enable the function.

3. Select the region from the drop-down list for detection settings.
4. Click **Area Settings** tab and click **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the time threshold, detection sensitivity and object percentage for intrusion detection.

Threshold: Range [0s-10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.

Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. When the sensitivity is high, a very small object can trigger the alarm.

Percentage: Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.

7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click **Arming Schedule** to set the arming schedule.
9. Click **Linkage Method** to select the linkage methods for intrusion detection, including Notify IP Server, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output.
10. Click **Save** to save the settings.

9.2.6 Configuring Line Crossing Detection

Purpose:

Line crossing detection function detects people, vehicle or other objects which cross a pre-defined virtual line, and some certain actions can be taken when the alarm is triggered.

Note: Line crossing detection function varies according to different camera models.

Steps:

1. Enter the Line Crossing Detection settings interface, **Event > Line Crossing Detection**.

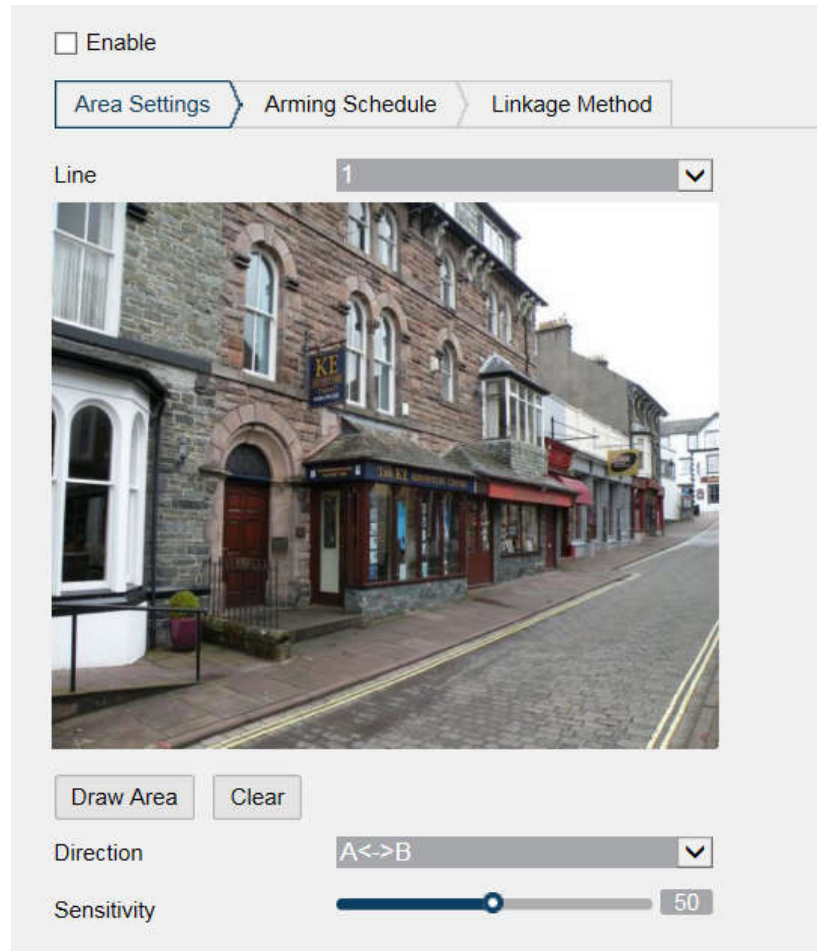


Figure 9-16 Line Crossing Detection

2. Check the checkbox of **Enable Line Crossing Detection** to enable the function.
3. Select the line from the drop-down list for detection settings.
4. Click **Area Settings** tab and click **Draw Area** button, and a virtual line is displayed on the live video.
5. Click-and-drag the line, and you can locate it on the live video as desired. Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.
6. Select the direction for line crossing detection. And you can select the directions

as A<->B, A->B, and B->A.

A<->B: Only the arrow on the B side shows; when an object going across the plane with both direction can be detected and alarms are triggered.

A->B: Only the object crossing the configured line from the A side to the B side can be detected.

B->A: Only the object crossing the configured line from the B side to the A side can be detected.

7. Click-and-drag the slider to set the detection sensitivity.
Sensitivity: Range [1-100]. The higher the value is, the more easily the line crossing action can be detected.
8. Repeat the above steps to configure other lines. Up to 4 lines can be set. You can click the **Clear** button to clear all pre-defined lines.
9. Click the **Arming Schedule** to set the arming schedule.
10. Select the linkage methods for line crossing detection, including Notify IP Server, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output.
11. Click **Save** to save the settings.

9.2.7 Configuring Region Entrance Detection

Purpose:

Region entrance detection function detects people, vehicle or other objects which enter a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Region Entrance Detection settings interface, **Event > Region Entrance Detection**.

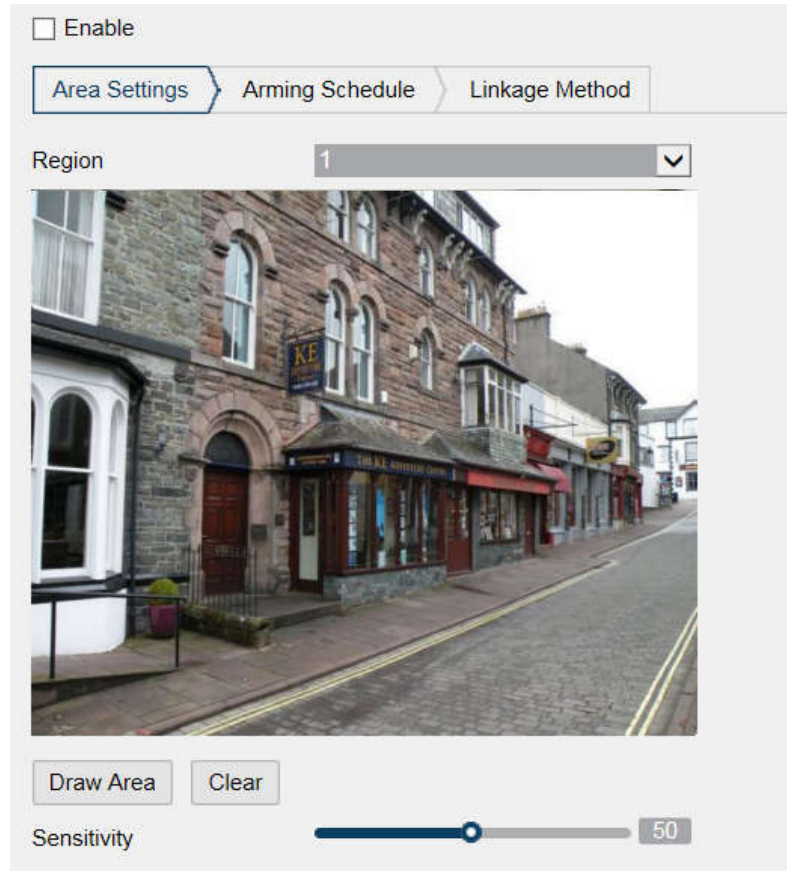


Figure 9-17 Region Entrance Detection

2. Check the **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Click-and-drag the slider to set the detection sensitivity.
Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. When the sensitivity is high, a very small object entering the region can trigger the alarm.
7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click **Arming Schedule** to set the arming schedule.
9. Click **Linkage Method** to select the linkage methods.

10. Click **Save** to save the settings.

9.2.8 Configuring Region Exiting Detection

Purpose:

Region exiting detection function detects people, vehicle or other objects which exit from a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Region Exiting Detection settings interface, **Event > Region Exiting Detection**.

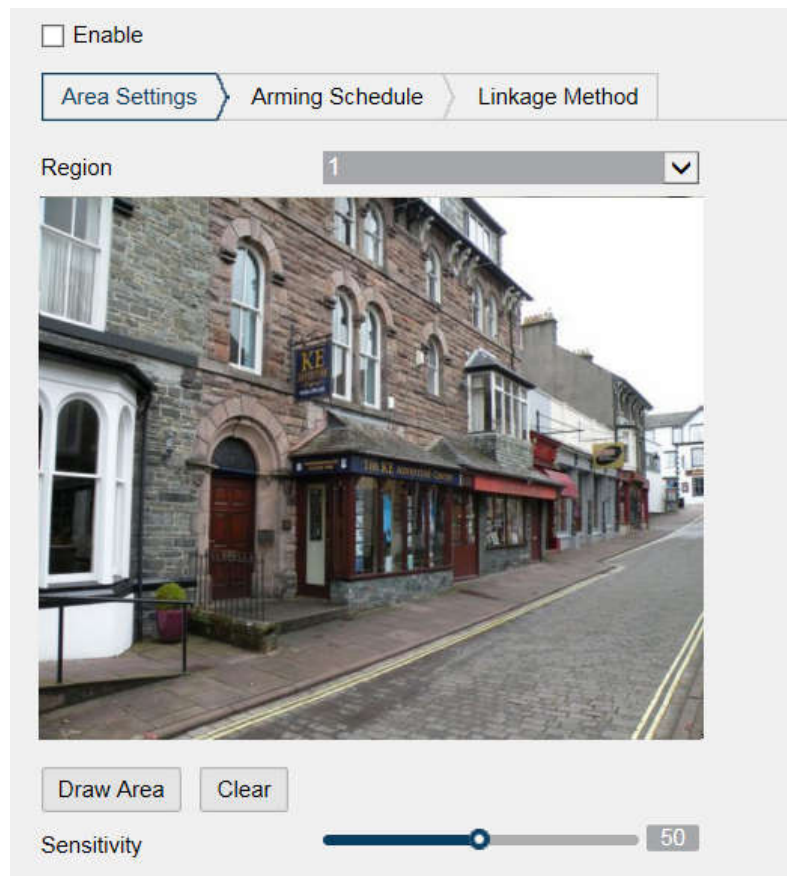


Figure 9-18 Region Exiting Detection

2. Check **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.

5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Click-and-drag the slider to set the detection sensitivity.
Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. When the sensitivity is high, a very small object exiting from the region can trigger the alarm.
7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click **Arming Schedule** to set the arming schedule.
9. Click **Linkage Method** to select the linkage methods.
10. Click **Save** to save the settings.

9.2.9 Configuring Unattended Baggage Detection

Purpose:

Unattended baggage detection function detects the objects left over in the pre-defined region such as the baggage, purse, dangerous materials, etc. A series of actions can be taken when the alarm is triggered.

Steps:

1. Enter the Unattended Baggage Detection settings interface, **Event > Unattended Baggage Detection**.

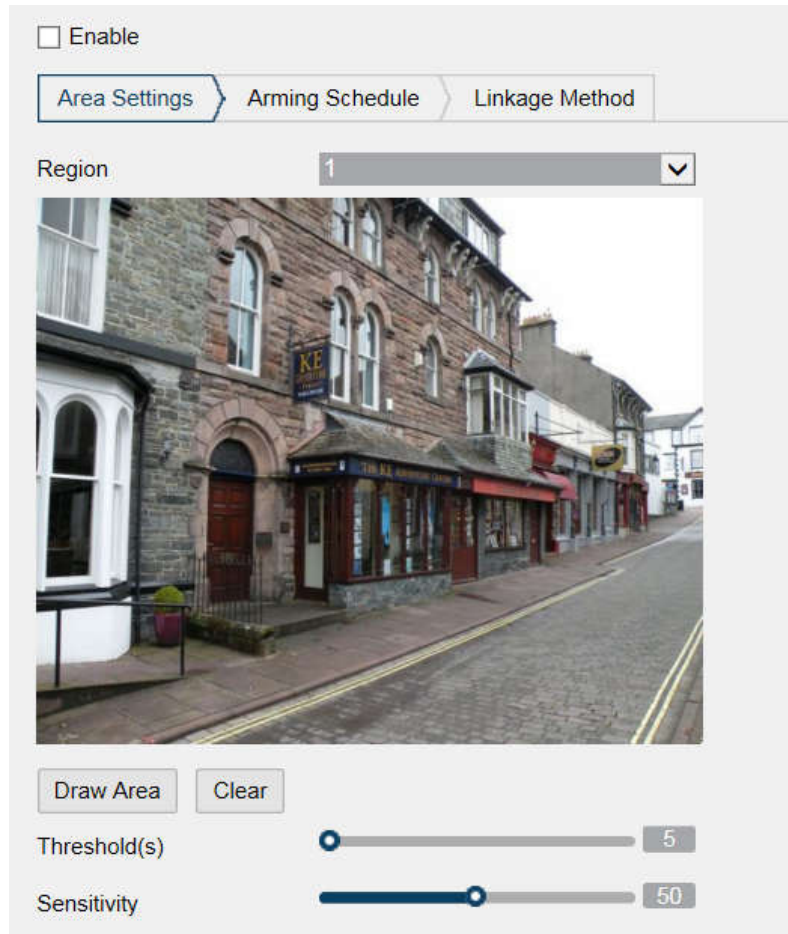


Figure 9-19 Unattended Baggage Detection

2. Check **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the time threshold and detection sensitivity for unattended baggage detection.
Threshold: Range [5-20s], the threshold for the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object is left and stay in the region for 10s.
Sensitivity: Range [1-100]. The value of the sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object left in the region can trigger the alarm.
7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You

can click the **Clear** button to clear all pre-defined regions.

8. Click **Arming Schedule** to set the arming schedule.
9. Click **Linkage Method** to select the linkage methods.
10. Click **Save** to save the settings.

9.2.10 Configuring Object Removal Detection

Purpose:

Object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.

Steps:

1. Enter the Object Removal Detection settings interface, **Configuration > Event > Smart Event > Object Removal Detection**.

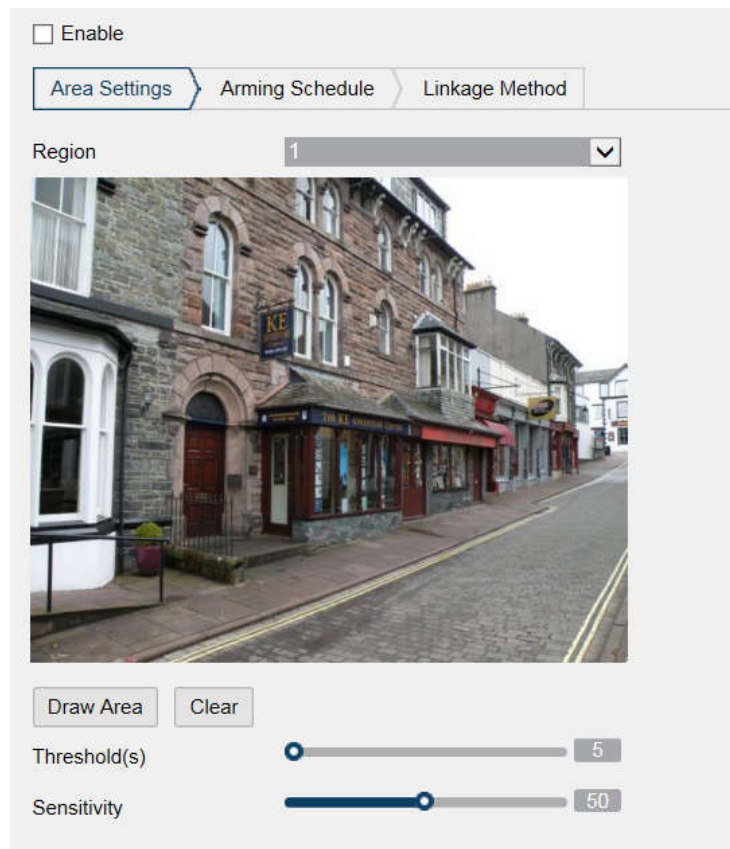


Figure 9-20 Object Removal Detection

2. Check **Enable** checkbox to enable the function.
3. Select the **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the time threshold and detection sensitivity for object removal detection.

Threshold: Range [5-20s], the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.

Sensitivity: Range [1-100]. The value of the sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.
7. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
8. Click **Arming Schedule** to set the arming schedule.
9. Click **Linkage Method** to select the linkage methods.
10. Click **Save** to save the settings.

9.3 VCA Configuration

9.3.1 Counting

Counting function helps to calculate the number of people entered or exited a certain configured area and is widely applied to the entrances or exits.

Notes:

It is recommended to install the camera as right above the entrance/exit as possible, and make sure it is horizontal to improve the counting accuracy.

Steps:

1. Enter the Counting Configuration interface: **Event > Counting**.

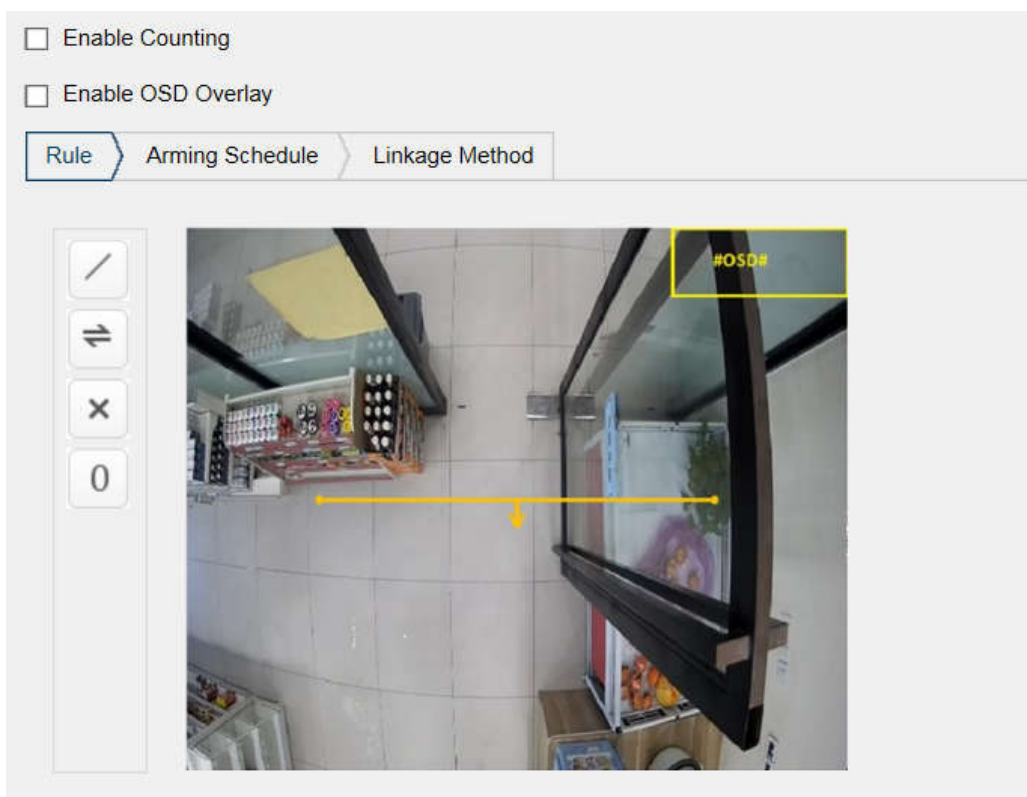






Figure 9-1 Counting Configuration

2. Check the **Enable Counting** checkbox to enable the function.
3. Check the **Enable OSD Overlay** checkbox, and the real-time number of people entered and exited is displayed on the live video.
4. Set the detection line.

An orange line, named as detection line can be set on the live video, and the object entering or exiting through the line will be detected and counted.

- 1) Click  to draw a detection line, and an orange detection line will appear on the image.

Note:

- The detection line should be drawn at the position right below the camera, and it should cover the whole entrance / exit.
 - Draw the detection line at the position don't have many people lingering.
- 2) Click-and-drag the detection line to adjust its position.
 - 3) Click-and-drag the two end points of the detection line to adjust its length.
 - 4) Click  delete the detection line.
 - 5) Click  to change the direction.
5. Click the  button, and the number of the people entered and exited will be cleared to zero.
 6. Click **Arming Schedule** to enter the arming schedule interface, and click-and-drag the mouse on the time bar to set the time.
 7. Check **Linkage Method** tab to select the linkage method.
 8. Click **Save** to save the settings.

Note:

The counting statistics will be calculated under **People Counting Statistics** tab.

Chapter 10 Storage Settings

Before you start:

To configure record settings, please make sure that you have the network storage device or local storage device configured.

10.1 Configuring Record Schedule

Purpose:

There are two kinds of recording for the cameras: manual recording and scheduled recording. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of scheduled recording are stored in the local storage or in the network disk.

Steps:

1. Enter the Record Schedule Settings interface: **Event > Record Schedule**.

☐ Enable

Continuous

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													
Sun													

☐ Continuous
☐ Motion
☐ Alarm
☐ Motion | Alarm
☐ Motion & Alarm
☐ Event

Figure 10-1 Recording Schedule Interface

2. Check the checkbox of **Enable** to enable scheduled recording.
3. Click **Advanced** to set the camera record parameters.

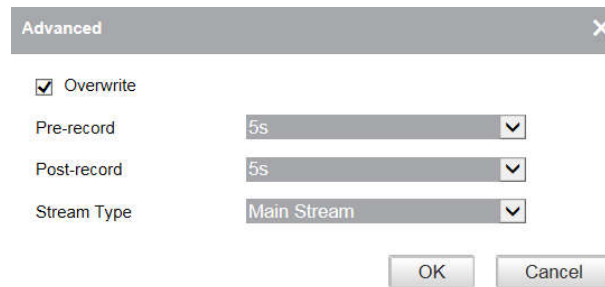


Figure 10-2 Record Parameters

- **Pre-record:** The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.
The Pre-record time can be configured as No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s or not limited.
- **Post-record:** The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.
The Post-record time can be configured as 5s, 10s, 30s, 1 min, 2 min, 5 min or 10 min.
- **Stream Type:** Select the stream type for recording.

Note: The record parameter configurations vary depending on the camera model.

4. Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event.

- **Continuous**

If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.

- **Record Triggered by Motion Detection**

If you select **Motion Detection**, the video will be recorded when the motion is detected.

Besides configuring the recording schedule, you have to set the motion

detection area and check the checkbox of **Trigger Channel** in the **Linkage Method of Motion Detection Settings** interface. For detailed information, please refer to the ***Task 1: Set the Motion Detection Area*** in the *Section 10.1.1*.

- **Record Triggered by Alarm**

If you select **Alarm**, the video will be recorded when the alarm is triggered via the external alarm input channels.

Besides configuring the recording schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** in the **Linkage Method of Alarm Input Settings** interface. For detailed information, please refer to *Section 10.1.3*.

- **Record Triggered by Motion & Alarm**

If you select **Motion & Alarm**, the video will be recorded when the motion and alarm are triggered at the same time.

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 10.1.1* and *Section 10.1.3* for detailed information.

- **Record Triggered by Motion | Alarm**

If you select **Motion | Alarm**, the video will be recorded when the external alarm is triggered or the motion is detected.

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 10.1.1* and *Section 10.1.3* for detailed information.

- **Record Triggered by Events**

If you select **Event**, the video will be recorded if any of the events is triggered.

Besides configuring the recording schedule, you have to configure the event settings.

5. Select the record type, and click-and-drag the mouse on the time bar to set the record schedule.
6. Click **Save** to save the settings.

10.2 Configure Capture Schedule

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the local storage or network storage.

Steps:

1. Enter the Capture Settings interface: **Event > Capture**.

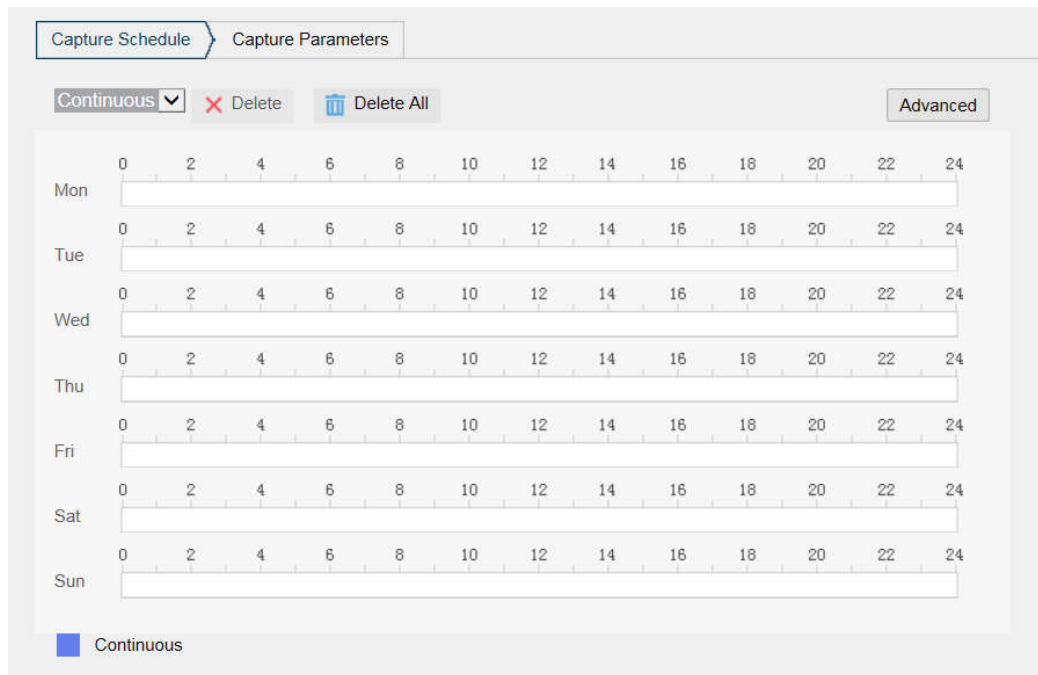


Figure 10-3 Capture Configuration

2. Go to **Capture Schedule** tab to configure the capture schedule by click-and-drag the mouse on the time bar. You can copy the record schedule to other days by clicking the green copy icon on the right of each time bar.
3. Click **Advanced** to select stream type.

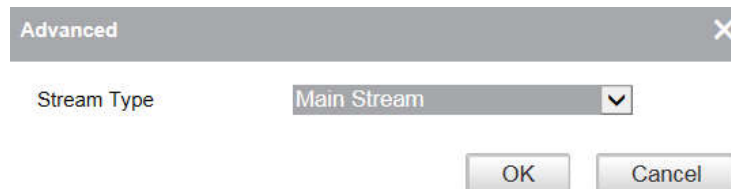
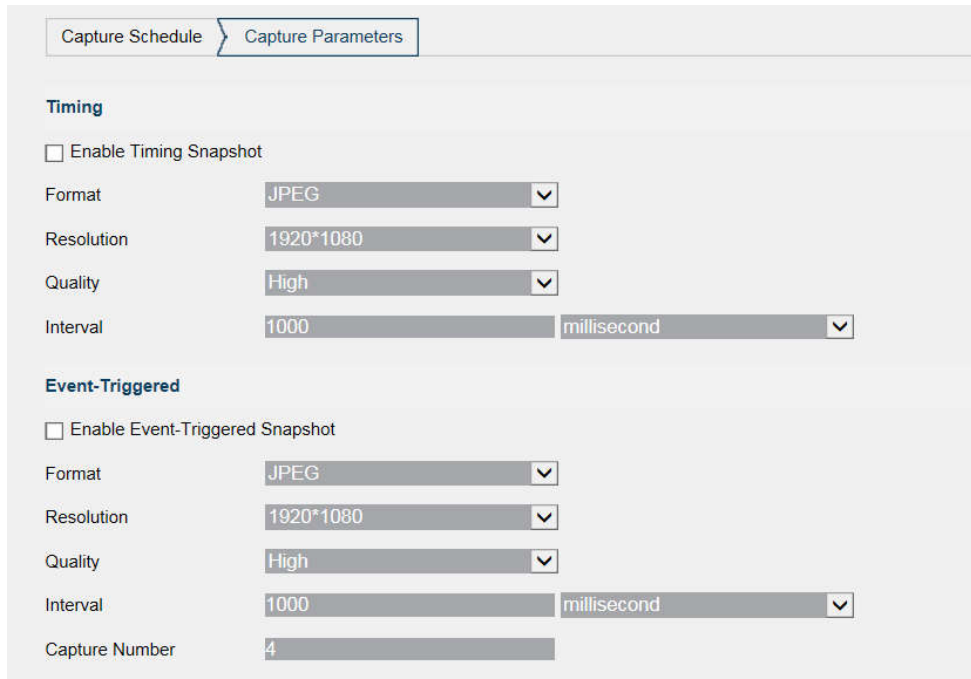


Figure 10-4 Advanced Setting of Capture Schedule

4. Click **Save** to save the settings.

5. Go to **Capture Parameters** tab to configure the capture parameters.
 - (1) Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot.
 - (2) Select the picture format, resolution, quality and capture interval.
 - (3) Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.
 - (4) Select the picture format, resolution, quality, capture interval, and capture number.



The screenshot shows the 'Capture Parameters' configuration page. It features two main sections: 'Timing' and 'Event-Triggered'. Both sections have a checkbox to enable their respective snapshot types, which are currently unchecked. Each section contains dropdown menus for 'Format' (set to JPEG), 'Resolution' (set to 1920*1080), and 'Quality' (set to High). The 'Interval' is set to 1000 milliseconds in both sections. The 'Event-Triggered' section also includes a 'Capture Number' field set to 4.

Figure 10-5 Set Capture Parameters

6. Set the time interval between two snapshots.
7. Click **Save** to save the settings.

10.3 Configuring Net HDD

Before you start:

The network disk should be available within the network and properly configured to store the recorded files, log files, pictures, etc.

Steps:

1. Add Net HDD.

(1) Enter the Net HDD settings interface, **Event > Net HDD**.

HDD No.	Server Address	File Path	Type	Delete
1			NAS	✗
2			NAS	✗
3			NAS	✗
4			NAS	✗
5			NAS	✗
6			NAS	✗
7			NAS	✗
8			NAS	✗

Mounting Type: NFS ▼ User Name: Password: Test

Figure 10-6 Add Network Disk

(2) Enter the IP address of the network disk, and enter the file path.

(3) Select the mounting type. NFS and SMB/CIFS are selectable. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

Note: Please refer to the *NAS User Manual* for creating the file path.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

(4) Click **Save** to add the network disk.

2. Initialize the added network disk.

(1) Enter the HDD Settings interface, **Event > HDD Management**, in which

you can view the capacity, free space, status, type and property of the disk.

HDD Management							Format
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress

Figure 10-7 Storage Management Interface

- (2) If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.

When the initialization completed, the status of disk will become **Normal**.

HDD Management							Set	Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress	
<input checked="" type="checkbox"/>	9	20.00GB	0.00GB	Formatting	NAS	R/W		

Figure 10-8 View Disk Status

3. Define the quota for record and pictures.
- (1) Input the quota percentage for picture and for record.
 - (2) Click **Save** and refresh the browser page to activate the settings.

Quota	
Max.Picture Capacity	4.75GB
Free Size for Picture	4.75GB
Max. Record Capacity	14.50GB
Free Size for Record	14.50GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figure 10-9 Quota Settings

Note:

Up to 8 NAS disks can be connected to the camera.

Chapter 11 Playback

Purpose:

This section explains how to view the remotely recorded video files stored in the network disks or memory cards.

Steps:

1. Click **Playback** on the menu bar to enter playback interface.

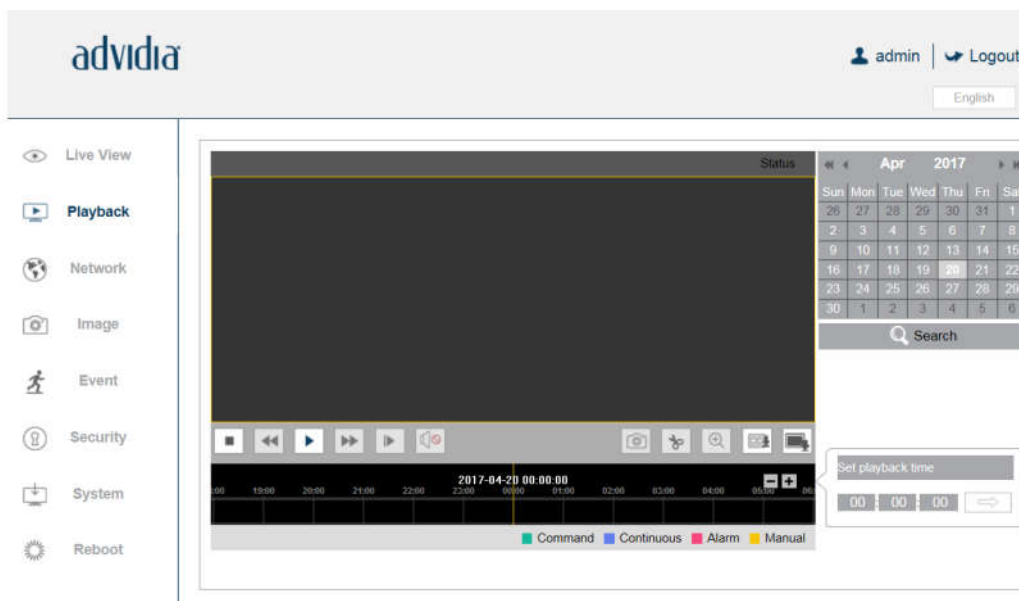


Figure 11-1 Playback Interface

2. Select the date and click **Search**.

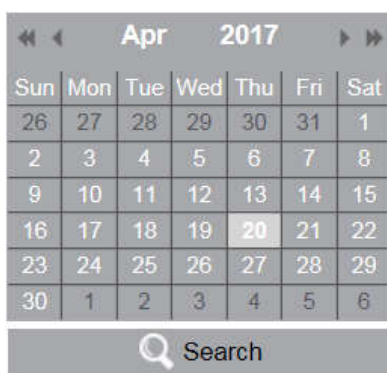


Figure 11-2 Search Video

3. Click ► to play the video files found on this date.

The toolbar on the bottom of Playback interface can be used to control playing

process.



Figure 11-3 Playback Toolbar

Table 11-1 Description of the buttons

Button	Operation	Button	Operation
	Play		Capture a picture
	Pause		Start/Stop clipping video files
	Stop		Audio on and adjust volume/Mute
	Speed down		Download Recording
	Speed up		Download images
	Enable/Disable digital zoom		Playback by frame

Note: You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface.

You can also input the time and click to locate the playback point in the **Set playback time** field. You can also click to zoom out/in the progress bar.



Figure 11-4 Set Playback Time

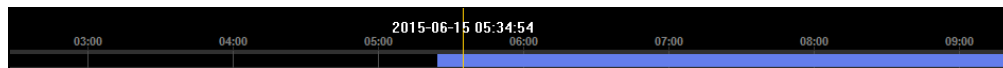


Figure 11-5 Progress Bar

The different colors of the video on the progress bar stand for the different video types.

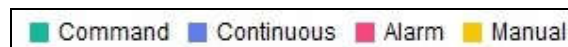


Figure 11-6 Video Type

