ZKiVision Client Software User Manual

Document version: 4.5

Software version: Pro V3.0

Date: 2013.07

Overview

This document describes the installation, functions, user interface and operations of ZKiVision Client Software.

General Instructions

Thank you for choosing our video surveillance product. Please read this manual carefully before using this product.

All functions of the product in this manual are for reference only. The actual product may differ from what is described in this manual due to updates from time to time. We disclaim liability for any dispute rising out of the unconformity between technical parameters and descriptions in this manual. We reserve the right to make any changes or amendments without prior notice.

For more details, visit our website www.zkivision.com or your local service outlets.

Table of Contents

1 Overview 1

1.1 Function 1

1.2 Operating Environment 1

1.3 Procedure for Use of ZKiVision 1

1.4 Conventions 2

2 Installation and Removal 3

2.1 Installation 3

2.2 Removal 5

3 Quick Start Guide 6

4 User Interface 7

4.1 Preview 7

4.1.1 System Button Bar 8

4.1.2 Tab Bar 8

4.1.3 Device List/Group List 9

4.1.4 Control Panel 11

4.1.5 Preview Window 14

4.1.6 Event Panel 18

4.2 Login/Logout 20

4.3 E-map 22

4.3.1 Map List 22

4.3.2 PTZ Control Panel 26

4.3.3 E-Map Window 26

4.3.4 Toolbar 28

4.4 Playback 29

4.4.1 Local Playback 29

4.4.2 Remote Playback 32
4.4.3 Server Playback 33
4.4.4 Local Backup 34
4.4.5 Server Backup 35
4.5 Event Query 36
4.5.1 General Event 36
4.5.2 Access Event 38
4.5.3 Face Event 41
4.5.4 Face Searching 43
4.5.5 System Event 47
4.6 Settings 49
4.6.1 Local Device Management 50
4.6.2 Platform Devices Download 52
4.6.3 Group Management 53
4.6.4 Audio and Video Parameter Settings 54
4.6.5 Alarm Settings 56
4.6.6 PTZ Parameter Settings 60
4.6.7 Device Information View 61
4.6.8 Network Settings 61
4.6.9 Advanced Settings 67
4.6.10 System Settings 68
4.6.11 Storage Management 70
4.6.12 User Management 72
4.6.13 Input / Output Signal Settings 73
4.6.14 Local Linkage Settings 74
4.7 Access Function 76
4.7.1 Personnel 76

4.7.2 Device 81

4.7.3 Access Control 86

4.7.4 Reports 102

4.8 Face Function 107

4.8.1 Face Registration 108

4.8.2 User Management 110

4.8.3 Parameter Setting 111

4.9 Logout 112

5 Configuration 113

5.1 How to Search and Add Camera/NVR/Access Controller to an Area 113

5.2 Manually Add a Device to the System 114

5.3 Modify Local Device Information 115

5.4 Group Cameras 116

5.5 Modify Network Parameters of a Camera 117

5.6 How to Set Timed Recording 119

5.7 Set Motion Detection 120

5.8 Enable Arming 121

5.9 Set Alarm Linkage 122

5.10 How to Set Email Linkage Alarm 125

5.11 Configure Preset Locations and Cruise Routes 127

5.12 Search and Playback Videos by Date 128

5.13 Back Up Videos 129

5.14 Create a New User 130

5.15 How to Modify User Info or User Permission 131

5.16 Back Up and Recover Configuration Data 132

5.17 How to set WIFI 132

5.18 Search for System Logs 133

5.19 Playback Associated Videos Through Alarm Logs....135
5.20 Apply for and Use a Dynamic Domain Name for Visiting IPC on Internet....135
5.21 Set Audio and Video Parameters Appropriate for Your Network....141
5.22 How to Set E-map....142
5.23 How to Set and Apply the Association of the IP Camera with the Access Controller....144
5.24 How to Set and Apply Face Function....146
5.25 How to Use Vendors DDNS for Visiting Surveillance Device on Internet....150
6 FAQs....153
6.1 No Image at Preview....153
6.2 No Audio at Preview....153
6.3 No Audio in Playback....154
6.4 Failure to Enable Manual Recording....154
6.5 Failure to Disable Videotaping at Preview....155
6.6 Pan-Tilt Abnormality....155
6.7 Failure to Implement Audio Intercom....156
6.8 Failure to Play Back Videos Displayed on the Timeline Panel After a Video Search....156
6.9 Failure to Search for Video Files....156
6.10 Failure to Set the Motion Detection Area....156
6.11 Failure to Achieve Alarm Linkage....157
6.12 Failure to Display the Alarm Window After Enabling Arming....157
6.13 Video Image Exception at Preview....158
6.14 Incorrect System Time....159
7 Others....160

1 Overview

1.1 Function

ZKiVision Client Software is a piece of network video surveillance software provided by ZK Technology free of charge. It supports multiple functions such as monitoring, videotaping, and alarm linkage of multiple IP cameras over the LAN and Internet.

As the video surveillance system is complex, it is strongly recommended to read the corresponding user manual before the first use of this software and confirm the device can be visited by browser on the LAN and Internet. This document describes how to use ZKiVision client software for video surveillance.

1.2 Operating Environment

Operating system: Windows XP, Windows 7

CPU: I3 series or above

Graphics: 1G or above discrete graphics

Memory: 4G

NIC: 1000 Mbps NIC

System disk: SATA500G

As a better computer can bring better effect of surveillance, it is recommended to use a better computer for video surveillance.

1.3 Procedure for Use of ZKiVision

Before using, proceed as follows:

Perform planning and installation of all IP cameras used for surveillance.

Change the IP addresses and ports of the IP cameras through the search software on the CD.

Access the IP camera from the browser and set the user name, password, alarm trigger mode (external alarm or motion detection), and system time for these IP cameras.

If you intend to access these IP cameras over the Internet, set dynamic domain names for them and perform port mapping on the corresponding routers.

The following takes the superuser as an example to describe the use of the software. The operation procedures vary with users of different operation authorities. Users only need to operate the items displayed on the operation interface by following the procedure below.

Run this client software.

Log in to the system as a superuser (“admin” and its default password “123456”) and change the default password.

Search and add devices to the system.

Modify device parameters (including device information and network parameters).

Set code stream.

Set arming (alarm linkage settings and storage management).

Preview the image.

Set users (assign authorities).

1.4 Conventions

To simplify the description in this manual, the following conventions are made:

Network video surveillance software is called software/system for short.

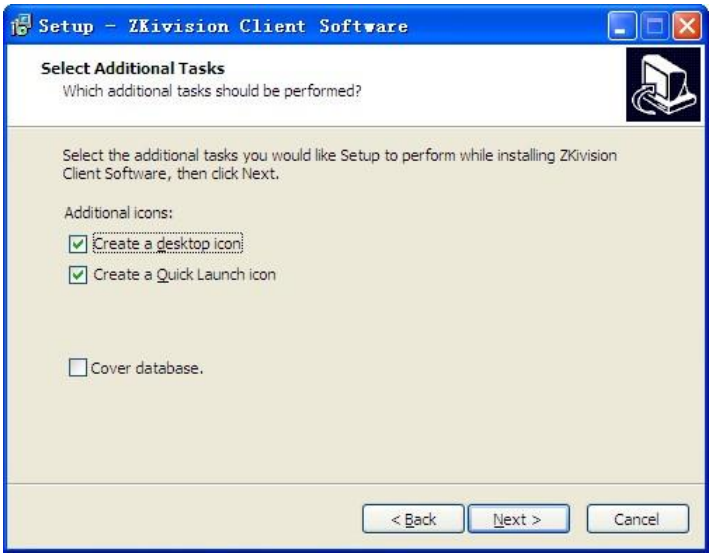
Click indicates left click of mouse button.

Double click indicates double left click of mouse button.

Right click indicates click with the right button of the mouse.

Some of the figures in this manual are for reference only.

Step 4: Confirm the installation is correct and click **Next** to wait for the completion of installation. Click **Finish** to exit.



☺**Note**: If the installation folder already exists, there will be a prompt box pops up. If you want to install to the existed folder, there will be an additional selection "cover database". Select it to use new database, or use the original database.

Step 5: For reconfiguration, please click **Back**, click **Install** to begin the installation process.

Step 5: After installation is completed, click **Finish** to exit.

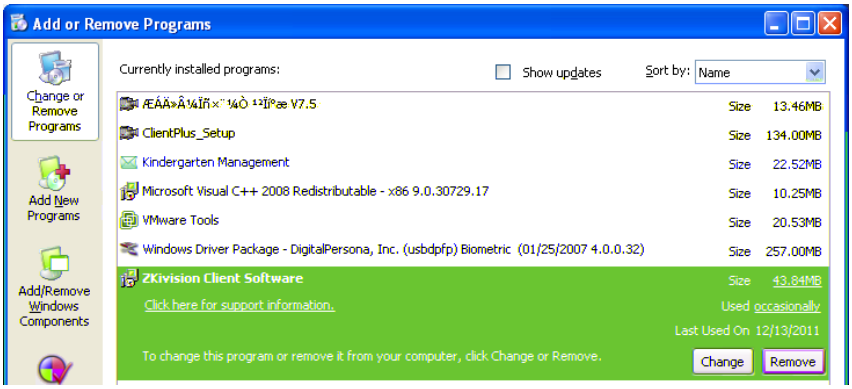
2.2 Removal

If you do not need to use anymore, you can delete it in the following two ways.

Close all the related programs before deletion.

Mode 1: Choose *Start* > *All programs* > *ZKTechnology* > *ZKiVision Client Software* > *Uninstall* to delete related documents.

Mode 2: Open the system control panel and choose ZKiVision Client Software. Click **Delete** to delete related documents.



☺**Notes:** 1. The above two modes are not available for deleting all the documents. Deleting related documents under installation directory is necessary.

2. When the software is uninstalled, the database and user's setting will be kept.

3 Quick Start Guide

By means of the following procedures, you can perform a fast setting on the client software.

1 Install the client software and the **Monitor client** icon is displayed on the desktop.

2 Double-click the **Monitor client** icon to enter the system.

3 Choose **Settings** > **Device Management** > **Search**. Click

to display the **Search** interface.

4 Click **Search all device** to search all camera devices produced by our company on the LAN.

5 Choose camera in the search list. Change the remote device information (such as IP address and device port) on this interface.

6 In the search list, select one or more cameras or tick off **Select All** to select all cameras.

7 Click **OK** to finish adding cameras to the system.

8 Choose camera channel in the device list on the **Search** interface to modify the local device information (device names and user names). Partition the device.

9 Enter **Preview** interface. Double-click the camera channel in the device list or drag the channel into the preview cell to connect the device. Then the video can be previewed.

10 Choose **Video** from the shortcut menu or click to start the videotaping.

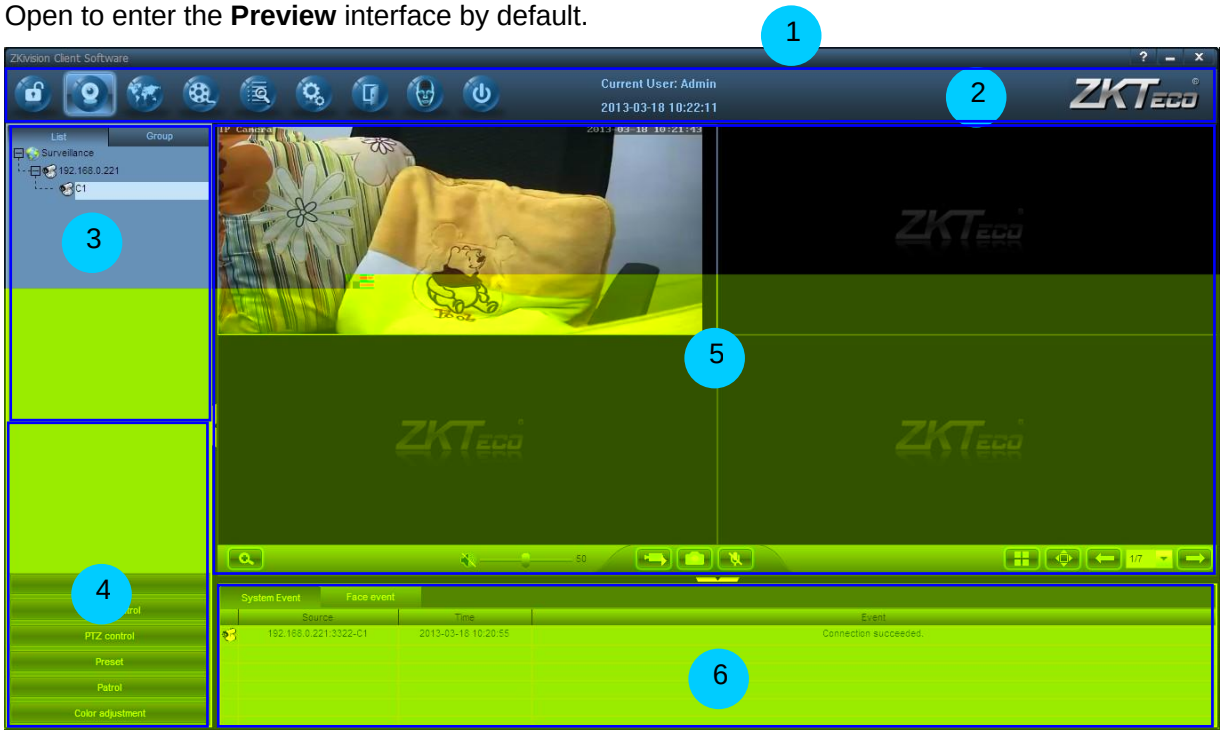
11 For more information of other functions such as user configuration, video playback, access management and alarm linkage configuration, see 5 Configuration.

4 User Interface

The user interface of ZKiVision is easy to operate. It is divided into the following 9 working areas, which switch over in tag page: **Lock user, Preview, E-map, Playback, Event Search, Setting, Access Management, Face Function and Exit**.

4.1 Preview

Open to enter the **Preview** interface by default.



The description of software interface is shown in the following table:

Area	Description	Area	Description
1	Button bar	4	Control panel
2	Tab bar	5	Preview window
3	Device list/Group list	6	Event list

When the device is added to the system, it will automatically display in the device tree on the preview page. After the parameter setting is completed, you can operate video monitoring, camera preset and color conditioning on the preview page.

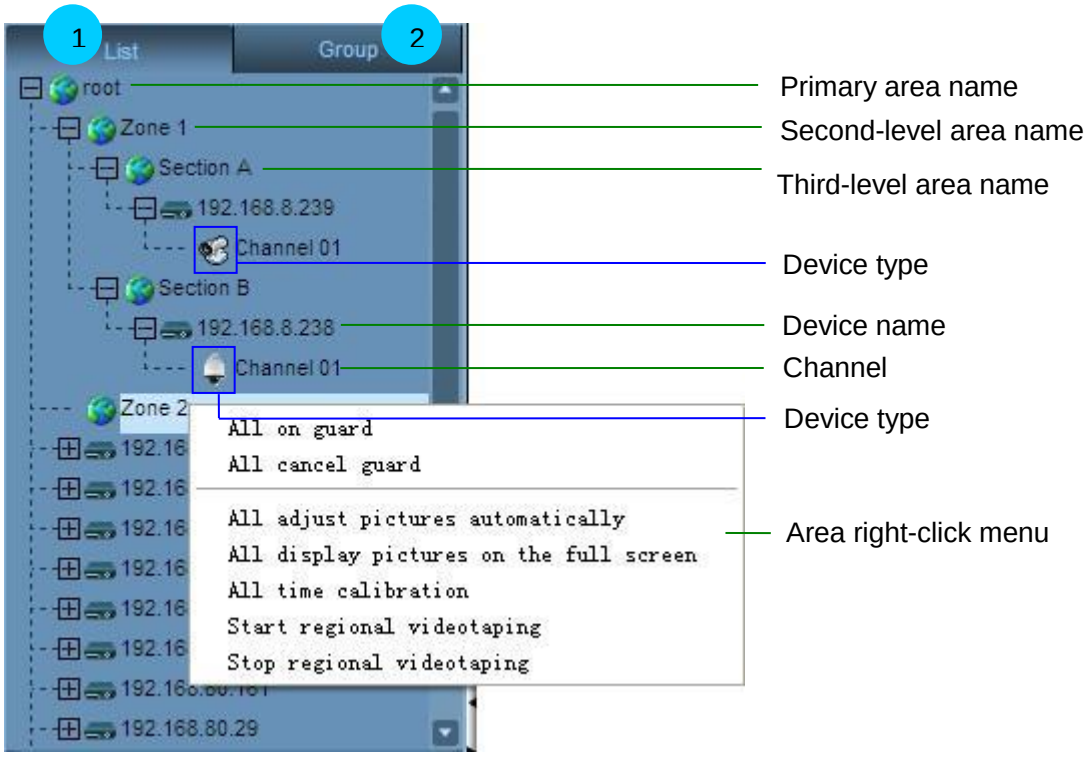
4.1.1 System Button Bar

Icon	Name	Function description
ZKivision Client Software	Version name	
?	**Help** button	Click ? to display user manual.
–	**Minimize** button	Click – to minimize the window to the system tray.
X	**Exit** button	Click X to pop up the exit prompt.

4.1.2 Tab Bar

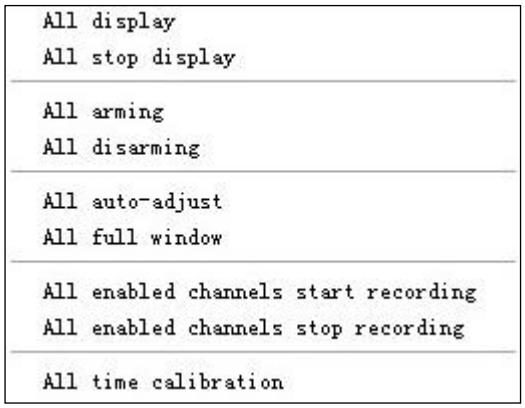
Icon	Name	Function description
/	Lock/Unlock	It is used for locking, unlocking, current operator modification, or password modification.
	Preview	Click to display the **Preview** interface. It is used for camera and video surveillance, control, and management.
	E-map	Click to enter the **E-map** interface and you can watch live pictures of a passage while viewing its location. The e-map also supports viewing multi-passages and pan tilt zoom of live pictures.
	Playback	Click to display the **Playback** interface. It is used for video search and playback.
	Event Search	Click to display the **Event Search** interface. You can set different conditions for querying normal events, access events, face events, face searching and system events.
	Setting	Click to display the **Setting** interface. It is used for device management, audio video settings, and alarm linkage settings.
	Access Management	Click to enter the **Access Management** interface, where functions like personnel registration, access control, and report query and export are available for the access control device.
	Face Function	Click to display the **Face Function** interface. You can register faces, manage user information and set parameters for face detection.
	Exit	Click to exit the interface.
Current User: Admin 2011-12-01 16:19:39	User profile	It is used for displaying the current user name and current date and time on the system.
	Logo	ZKTeco Logo

4.1.3 Device List/Group List



Icon	Name	Function description
List	List mode	Display area, device, and channel according to the list hierarchy of user configuration.
Group	Group mode	Display group and channel according to the group hierarchy of user configuration.
	Area/Group	Area: Divide cameras into different areas according to their different locations to facilitate centralized monitoring against different areas for users. Group: Divide cameras into different groups according to their different monitoring types to facilitate centralized monitoring against different monitoring types for users.
/	Device type	IP Camera/ Network Video Recorder (NVR)/ Digital Video Recorder (DVR)/ access controller

Right-click the area name to pop up the following function menu:



Enable alarm linkage of all enabled channels in the area.

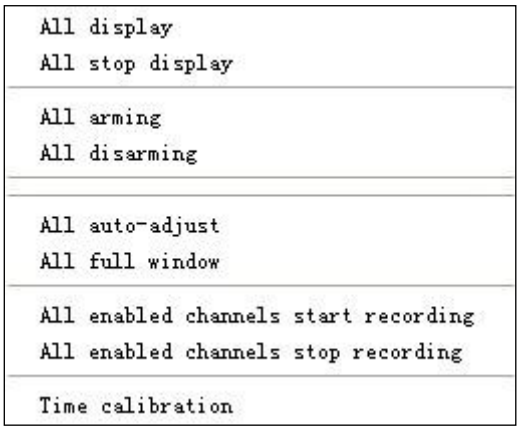
All enabled channels in the area display pictures with original proportions.

All enabled channels

All enabled channels in the area stop videotaping.

Calibrate the time on all devices in the area to the software system time.

Right-click the device name to pop up the following function menu:



Right-click the channel to pop up the following function menu:

☺**Note:** For related devices added, device name modification and partition, see Search for and Add a Camera to an Area. All

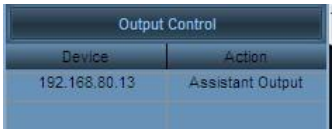
4.1.4 Control Panel

- **Blacklist**

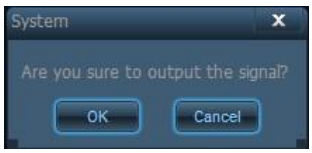
Unfold the blacklist panel of face detection by clicking the "**Blacklist**" bar and the system will display in the blacklist the blacklist users that it identifies: On the left are face images that it detects and on the right are reference images at registration, as shown in the above figure.

Note: For the setting and application of face identification, see 错误!未找到引用源。 How to Set and Apply Face Function.

- **Output Control**



Unfold the output control panel by clicking **Output Control,** select the camera channel from which the output is to be controlled. The output actions that can be controlled will display in the panel: If this camera is not associated with the access controller, only the **Assistant Output** of the camera can be controlled; if it is associated with the access controller, both the **Assistant Output** of the camera and **Open the Door** by the access controller can be controlled. Double-click the action to be controlled and a confirmation box will display, as shown in the following figure:



Note: For the association of the IP camera and the access controller, see How to Set and Apply the Association of the IP Camera with the Access Controller.

- **PTZ control panel**

Icon	Name	Function description
	Direction control	Control the rotation direction of the Pan-tilt by following the arrows (up, upper right, upper left, left, right, lower right, lower left, and down). Click to control the automatic horizontal rotation of the Pan-tilt. Cancel this operation by another click.
	Narrow aperture	Click to stop down if the camera lens has a power driven aperture control function.
	Widen the aperture	Click to widen the aperture if the camera lens has a power driven aperture control function.
	The focal distance becomes smaller.	Click to make the camera zoom in on distant pictures to implement monitoring if the camera lens has a power zoom function.
	The focal distance becomes larger.	Click to make the camera zoom in on nearby pictures to implement monitoring if the camera lens has a power zoom function.
	Focus forward	Click to make focus forward to obtain a clear picture if the camera lens has a power focus function.
	Focus backward	Click to make focus backward to obtain a vague picture if the camera lens has a power focus function.
	Pan-tilt speed	Drag the slider left to slow down the pan-tilt speed or drag the slider right to accelerate the pan-tilt speed.
	Light	Click to open the light when the external light devices are connected in a dark lighting condition. Close the light by another click.

	Windscreen wiper	Click to enable the windscreen wiper when the cover is dirty. Disable the windscreen wiper by another click. It is recommended to adopt this function to avoid scrape on the lens when it is rainy or the cover is wet.

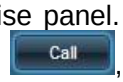
Note: The above functions are available only when they are supported by camera lens and external devices.

- **Preset Panel**

Click **Preset** bar to display the preset panel. Click , the Pan-tilt will rotate to the preset.

Note: For the preset settings, see Configure Preset Locations and Cruise Routes.

- **Cruise Panel**

Click **Cruise** bar to display the cruise panel. Select the required camera channel. In the cruise drop-down list, select a cruise. Click  , the Pan-tilt will rotate along the cruise.

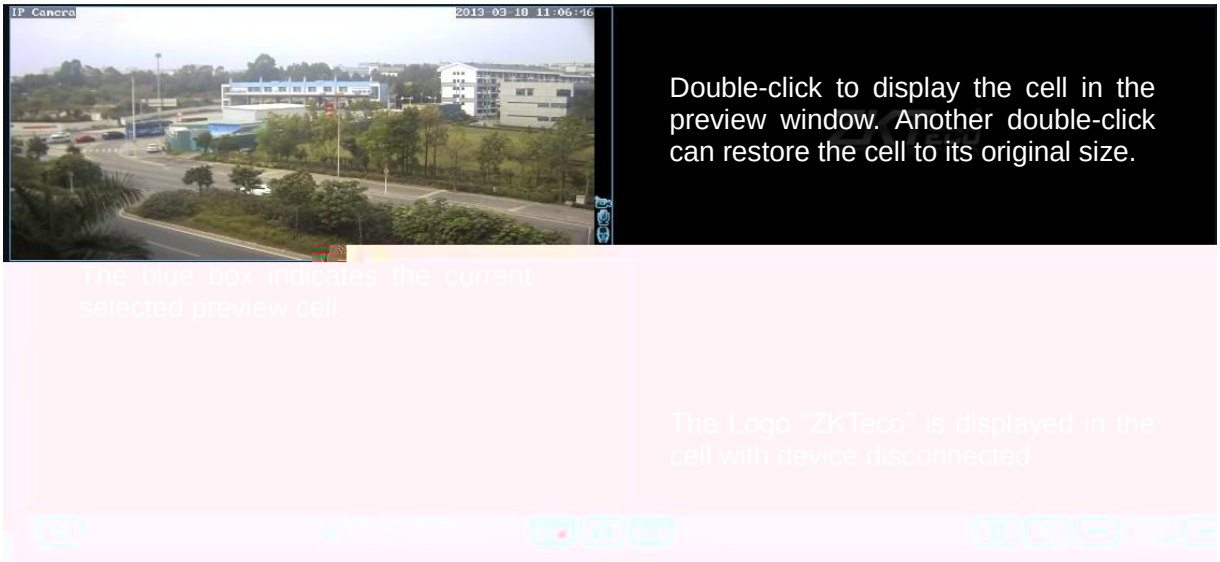
Note: For the preset settings, see Configure Preset Locations and Cruise Routes.

- **Color Adjustment Panel**

Icon	Name	Function description
	Brightness	The picture turns brighter from a left drag to a right drag (0–255).
	Saturation	The picture turns brighter from a left drag to a right drag (0–255).
	Contrast	The picture contrast can be enhanced from a left drag to a right drag. HD camera: 0–6. SD video camera: 0–255.
	Chromaticity	The picture color turns darker from a left drag to a right drag. This function is only applicable to the SD video camera (0–255).
	Shutter	1. When a monitored object is moving fast, a greater shutter value will reduce the blurring effects. 2. Applicable only to wide dynamic devices (0~255)
	Sensitivity	1. In poor lighting conditions, the camera with a higher sensitivity will be more sensitive to light. 2. Applicable only to wide dynamic devices (0~255)
	Illumination	1. In poor lighting conditions, better video effects will be achieved by adjusting to a greater value. 2. Applicable only to wide dynamic devices (0~255)
Default		Click Default to restore the brightness, saturation, contrast, shutter, and sensitivity to the default value 80, 50, 0, 1, 17 respectively for WDR HD device. Click Default to restore the picture brightness, saturation, and contrast to the default value 80, 50, and 0 respectively for HD device. Click Default to restore the picture brightness, saturation, contrast, and chromaticity to the default value 120, 150, 140, and 255 respectively for SD device.

4.1.5 Preview Window

In the device list, double-click channel or drag the channel into the cell when a device is need to be connected.



Right-click the cell in list mode to pop up the following function menu:

Full screen display of the **Preview** window.

Automatically adjust the picture to its original size.

Opening the door is the output action of the access controller associated with this IP device.

After choosing the **Enable face function**, **Disable face function** will be automatically displayed.

After ticking this option, face will be collected and displayed on the face event panel only when its template quality is higher than template quality threshold. When registering user online, enable this option because quality of faces collected this way will be higher.

Snapshoot the current picture.

Videotape the current picture.

Disconnect the device. Click the camera channel or drag the channel to the picture to reconnect the device and display pictures.

Right-click the cell in group mode to pop up the following function menu:

Icon	Name	Function description
	Electronic magnification	Click the button and scroll the mouse to zoom in and zoom out. Drag the box to an area to view relevant contents.
/	Sound on/off	Click to open the audio and click to close the audio after a channel or a picture is selected.

/ Videotape/

/	Expand/Fold	Click to fold the preview window. Click to expand the preview window.
	Surveillance	Surveillance is enabled on the channel.
	Face recognition	The face recognition function is enabled on the channel.
	Video recording	A video is being recorded on the channel.
	Sound playing	The sound playing function is enabled on the channel.
	Audio collection	The audio collection function is enabled on the channel.

For example: There are 3 groups (group 1-[1], group 2-[6], and group 3-[16]) in the current configuration. The cycling time is set to 5s. Select 6-split-cell display. 16 camera channels are connected in total.

List mode: The first page of preview window displays CH1–CH6 cells. Click to switch to the second page on which displays CH7–CH12 cells.

Group mode: Click to display one full screen, to display 6-spit-cell picture after 5s, and to display 16-split-cell after another 5s. The 6-split-cell display will jump to the 16-split-screen display when you click .

Note: 1. If you need to set the video storage disk, choose **Settings** > **Local settings** > **Storage management**.

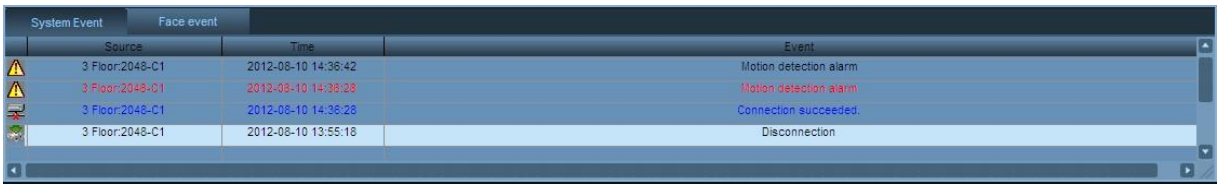
2. If you need to modify the format or storage location of the capturing pictures, choose **Settings** > **Local settings** > **System settings**.

3. Dividing cameras into different groups is a prerequisite to group switching, see Group Cameras for details.

4. If you need to modify the group polling time, choose **Settings** > **Local settings** > **System settings**.

4.1.6 Event Panel

4.1.6.1 System Event



Event information are color coded:

• **Red** — Alarm event

• **Blue** — General event

• **Black** — Already browsed information

Source The names of cameras that the message comes from

Time The time at which events occur

Event Brief description of event type

Icon	Description
	Connection succeeded
	Connection failed
	Alarming
	Alarm stopped

4.1.6.2 Face Event

The system can display detected faces on the face event information panel. If the face it identifies is that of a registered user, “user name and face identification marks” will be displayed under the face image; if the face is that of an unregistered user, a question mark (?) will be displayed under the image. You can tick any or all face images and add them to the face registration list.

Click **Pause** to suspend the rolling display of the face identification results and the button automatically switches over to **Play**.

After pause, you can manually tick the detected images or tick **Select all** to select all the images displayed in the identification results.

Click this button to add the ticked images to the face registration list.

4.2 Login/Logout

On this page, you can switch over from user to user and modify user password.

User Select the user name for login system.

User password Type in the user password.

Remember If it is selected, the user name and password are remembered. You do not need to enter the password if you log in to the system from the same computer.

Login Click **Login** to log in to the system after selecting the user name and typing in password.

Exit Click **Exit** to exit the **Login** interface.

Modify P.W. Click **Modify P.W.** after selecting an existing user name to modify the password.

Old password Type in the old password.

New password Type in the new password.

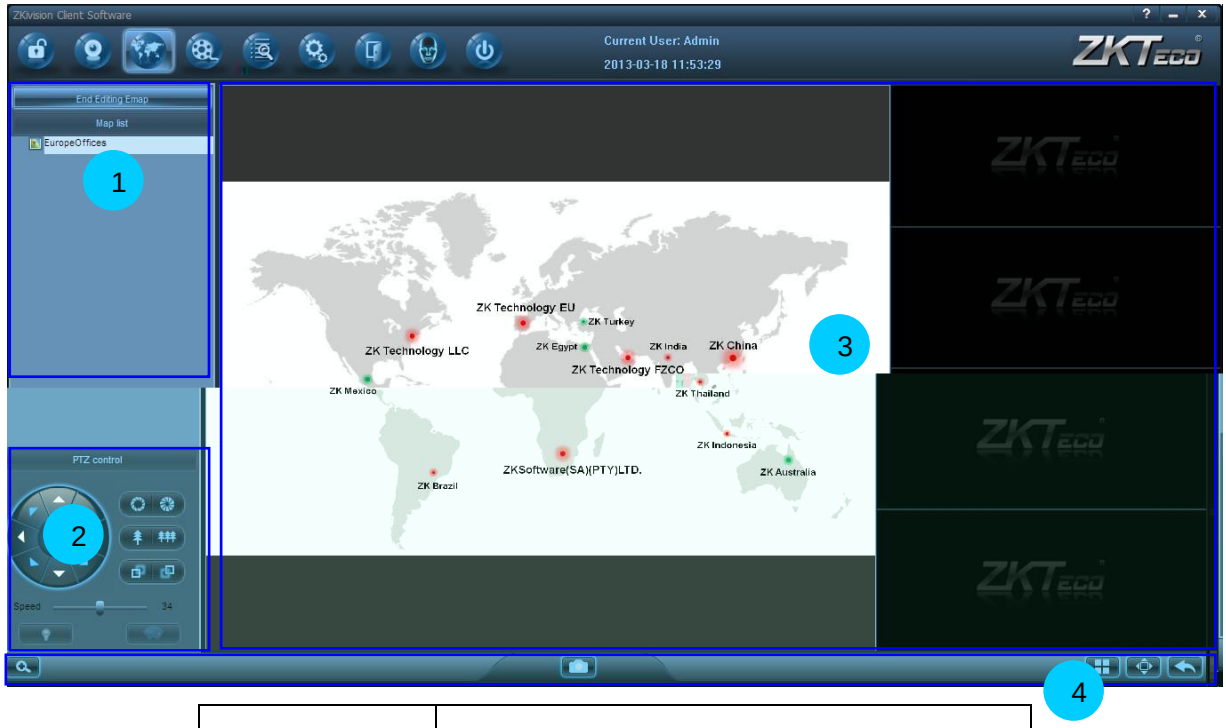
Confirm password Type in the new password again.

OK Click **OK** to submit the new password.

Delete Click **Delete** to cancel this operation.

Note: Superuser **admin** exists in the system by default and the default password is "**123456**". This superuser cannot be deleted and his user level cannot be modified.

4.3 E-map



Region	Description	
1	Map List	
2	PTZ Control Panel	
3	E-Map Window	
	Map Display Window	Video Play Window
4	Toolbar	

The system supports electronic maps. It allows users to upload electronic maps and conveniently and visually deploy cameras on the electronic maps, facilitating unified management of devices.

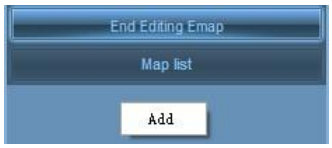
Note: Refer to How to Set E-map for e-map settings.

4.3.1 Map List

Access the map editing interface by clicking **Click and Edit Emap** and the button switches over to **End Editing Emap**.

Click **End Editing Emap** to exit emap editing and the button switches over to **Click and Edit Emap**.

In the initial state, when you right click on the blank of the map list after accessing the map editing interface, the **Add** map page will be displayed.



Right-click the name of map to pop up the following functional menu:

Edit Status non-editing status

1. Add map: Click to enter the interface of adding map.

Click **Browser** to find the images in BMP in the local computer, input the map name and then click **OK** to complete the map adding.

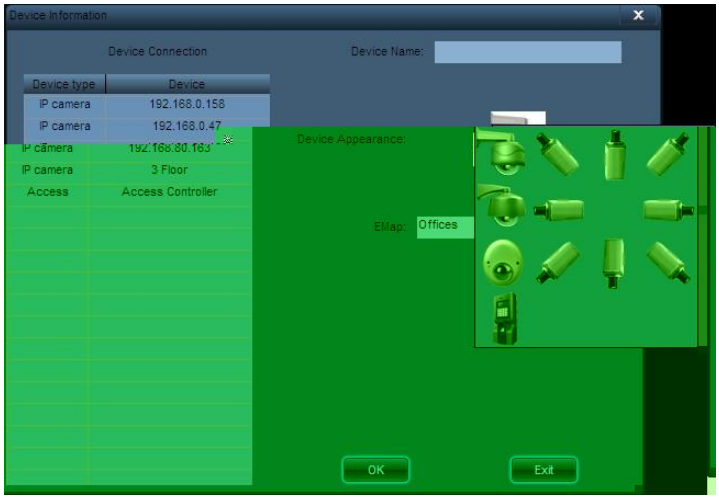
Note: It only supports the images in BMP.

2. Add device: Click to enter the interface of adding device.

You can mark the location of a device on the map by adding the device icon on the map.

Select the device to be linked, set the name and appearance of the device, etc., and then click

to complete the adding.



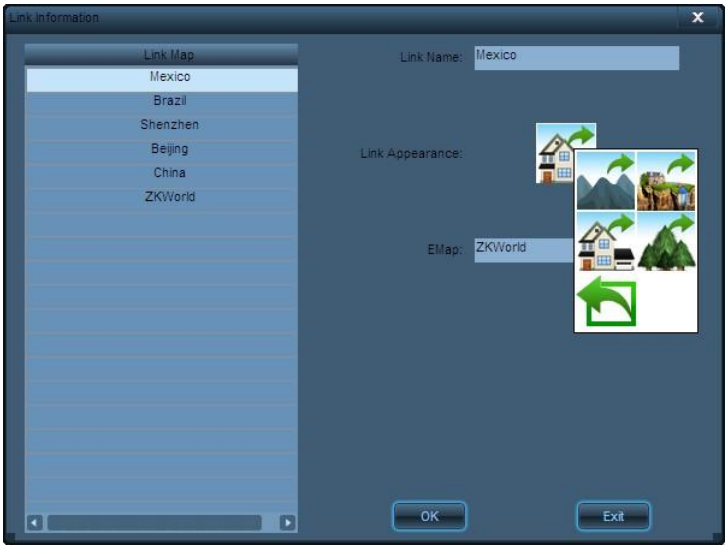
When adding device succeeds, the chosen visual icon for the device will be displayed on the map. You can drag the location of the device icon by moving the mouse cursor to the device icon, pressing and holding the left button of the mouse. Exit editing. After the device is armed, the device icon will blink when there is an alarm input signal. You can double-click the device icon or drag the icon to the video play window to play the video in real time.

3. Add link: Click to enter the interface of adding link.

By adding link icon on a map, a user can conveniently and expediently enter and check the map whenever he wants to.

Select the map to be linked, set the name and appearance of the link, etc., and then click

to complete the adding.

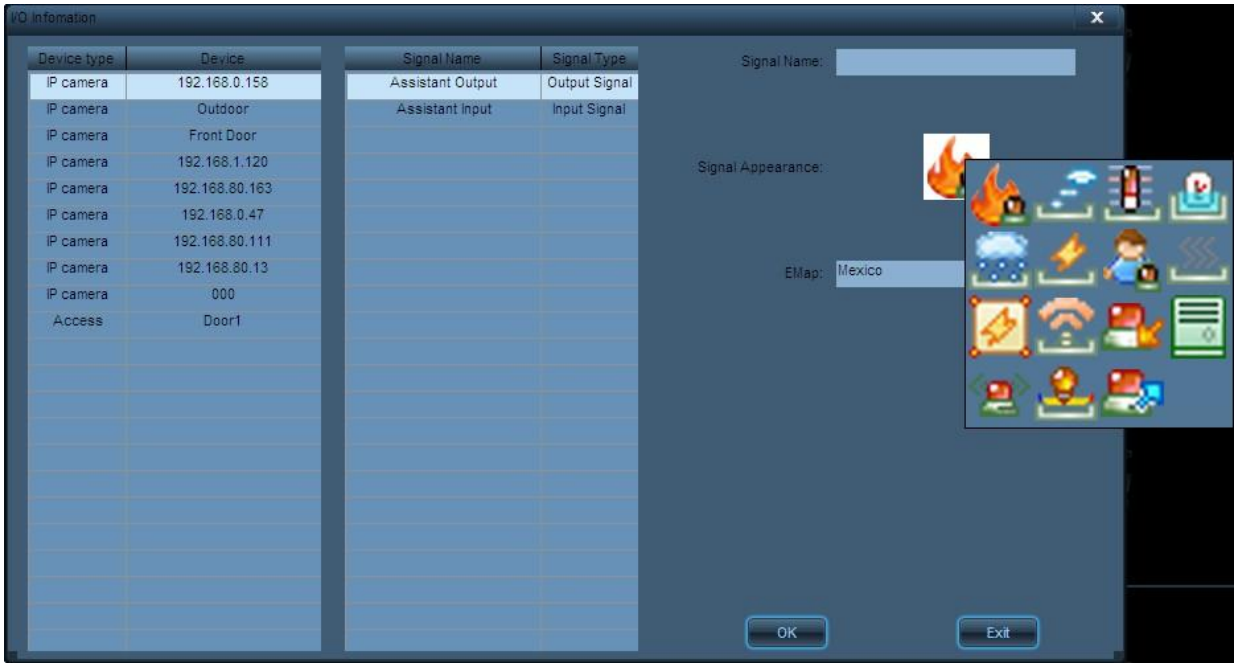


After successfully adding link, the selected icon of link appearance appears on the map. Move the cursor to the icon, and hold down the left button to move the location of link icon. After exiting the condition of editing, double-click the icon to enter the linked e-map.

4. Add I/O Signal: Click to enter the interface of adding I/O signal.

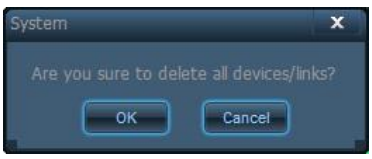
When an alarm input device is connected to the IP camera or to the access controller associated with the camera, auxiliary input will be generated and when an alarm output device or an exit switch is connected to the IP camera or to the access controller associated with the camera, auxiliary output signals will be generated. By adding input-output signal icons, you can mark on the map the locations of the devices that are connected to the IP camera or the access controller.

After selecting the devices to be connected, the signal type, setting signal name and signal appearance, click **OK** to finish the adding.

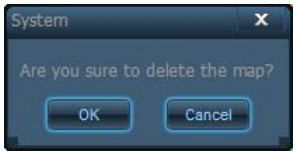


When adding signals succeeds, the chosen visual icons for the signals will be displayed on the map. You can drag the locations of the signal icons by moving the mouse cursor to the signal icons, pressing and holding the left button of the mouse. Exit editing. After the device is armed, the input signal icon will blink when an external alarm signal comes in. After confirming on site, the security guard can right click the icon to confirm the alarm. Then the icon will stop blinking. The guard also can double-click the output signal icon to control the output.

5. Delete all devices/links: Click to delete all device icons and map icons linked on the map.



6. Delete the map: Click to delete the map.

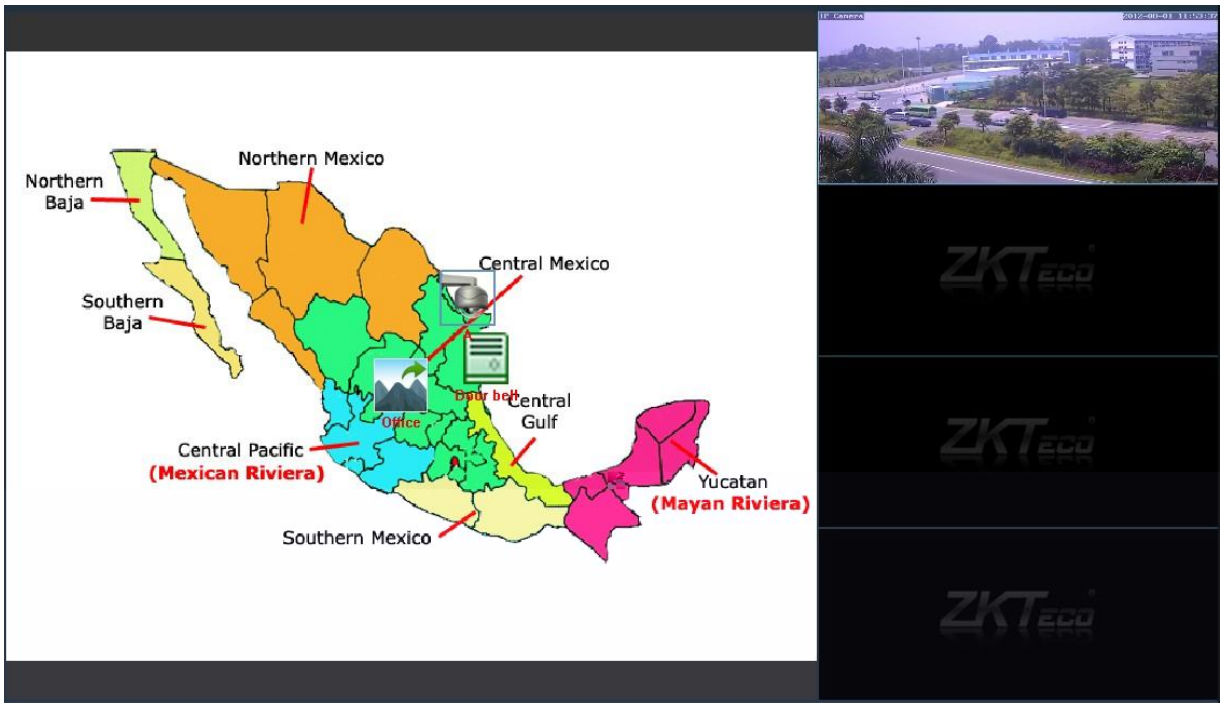


7. Attribute: Click to display the attributes of the map. The attributes cannot be edited in the no edit status.

4.3.2 PTZ Control Panel

Note: For details, see 4.1.4 Control Panel.

4.3.3 E-Map Window



4.3.3.1 Map Display Window

- In edit status, right-click a map to pop up a functional menu as shown in the above figure:

Add devices — Enter the interface of adding device
Add links — Enter the interface of adding link
Add I/O signal — Enter the interface of adding I/O signal
Delete all devices/links — Delete all icons linked to the map
Attribute — Display the attributes of the map

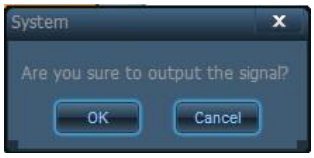
- In non-editing status, right-click the link/device icon to pop up the following functional menu:

Delete — Delete the icon
Attribute — Display the attribute of the icon

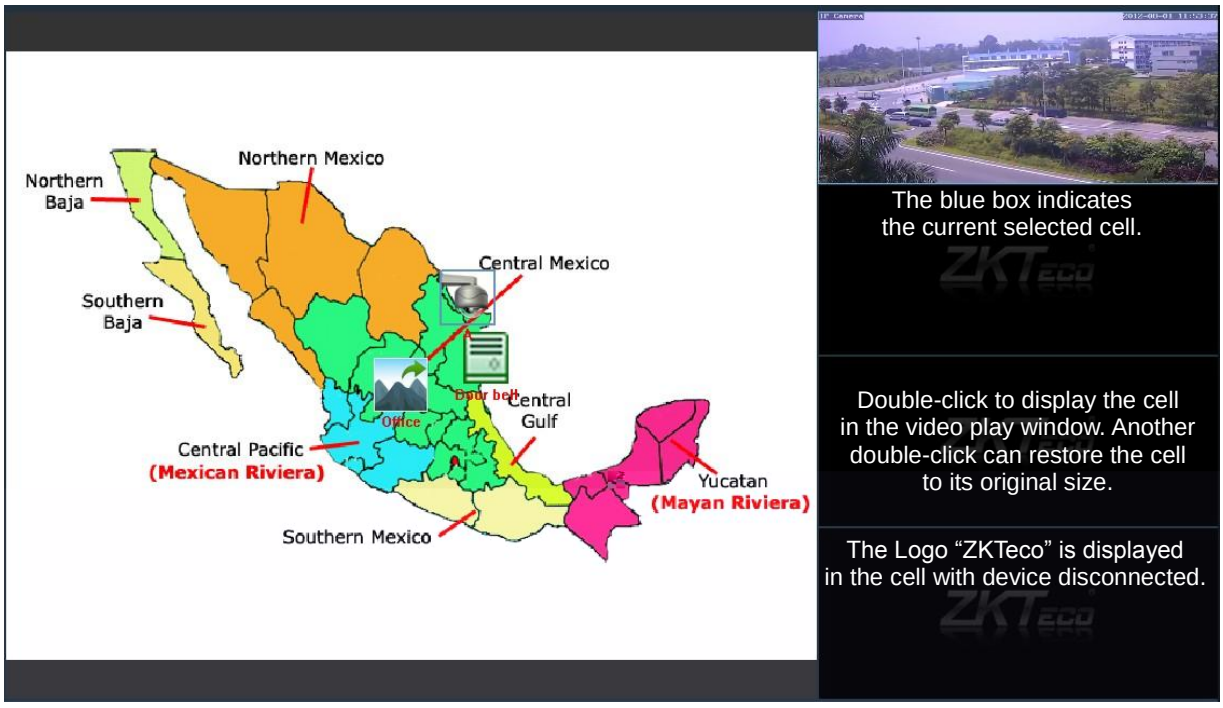
- In non-editing status, you can right click the map or the link icon to view its attribute.
- In non-editing status, when there is alarm input, the device or input signal icon will blink. When you right click, the function menu shown as follows will be displayed:

Confirm alarm — Click to confirm the alarm and the icon will stop blinking
Attribute — Display the attributes of this icon

- In non-editing status, when you double-click the output signal icon, the function menu shown as follows will be displayed:

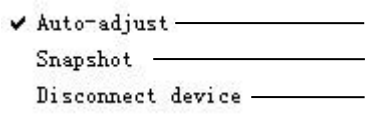


4.3.3.2 Video Play Window



You can double-click the device icon or drag the icon to the video play window to play the video in real time.

Right click on the play cell, the function menu shown as follows will be displayed:



Automatically adjust the image to its original size.

Capture the current image

Disconnect the device. Double-click the device icon or drag the icon to the cell to reconnect the device and display image.

4.3.4 Toolbar

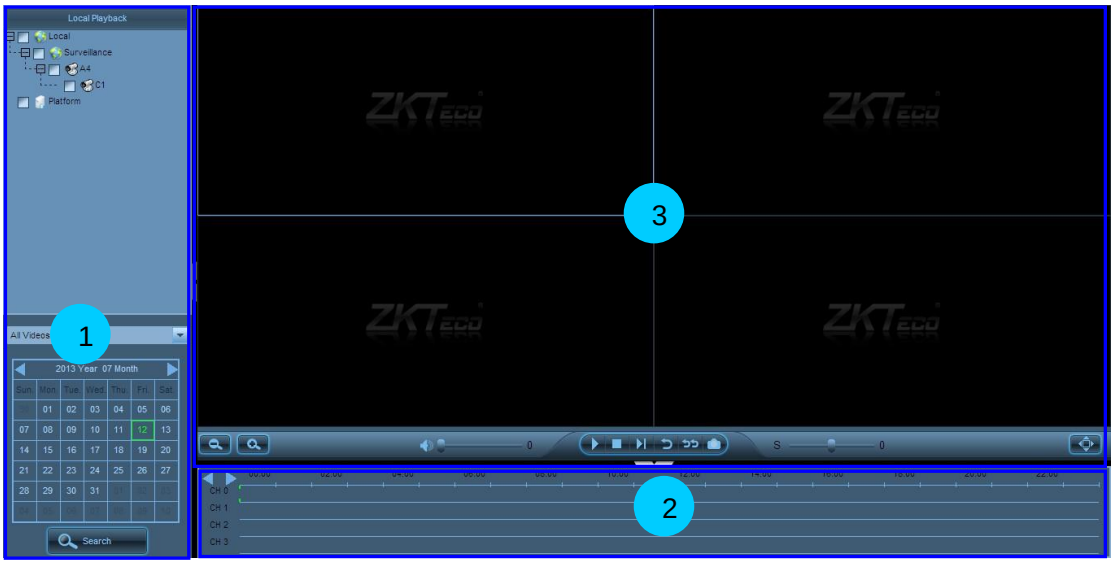
Icon	Description	Function
	Electronic magnification	Click the button and scroll the mouse to zoom in and zoom out. Drag the box to an area to view relevant contents.
	Snap-shot	After choosing the cell, click this button to snap-shot the scene. The default storage path is C:\Picture.
	Select cells	1. You can choose a video play window to display the number of cells. The system supports one-, two- or four-cell display. 2. By default, the video is displayed in four cells.
	Full Screen	1. Click the button to have the map display in full screen, and click again to exit the full screen. 2. During full screen, move the cursor to the bottom of the screen to show the toolbar.
	Back	Click the button and back to the previous map.

Notes: 1. The setting of map must be performed in edit status, and the map cannot be edited in non-editing status.

2. In non-editing status, right-click the map, link, I/O signal or device to check its attributes.

4.4 Playback

4.4.1 Local Playback



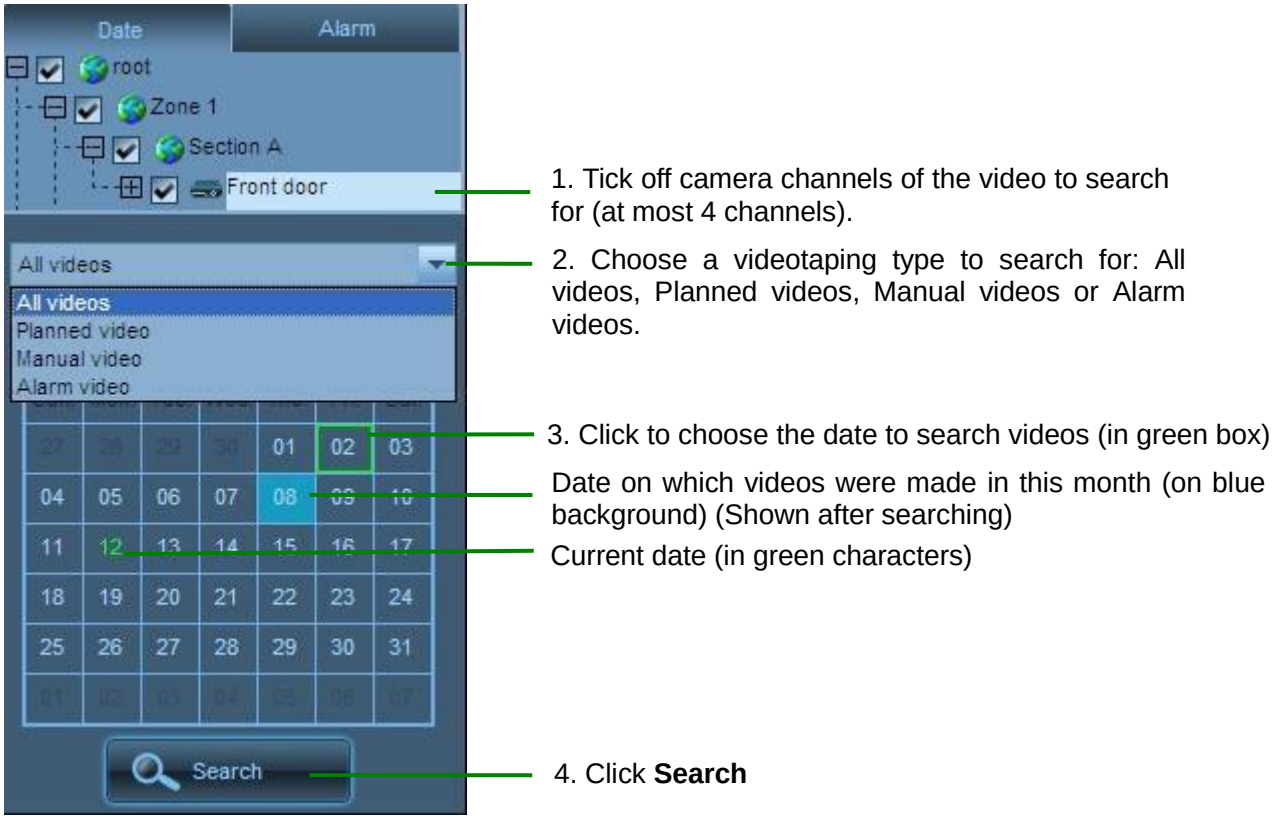
Area	Description
1	Video search panel
2	Timeline panel
3	Playback window

Local Video: is stored in the local computer.

After setting search conditions by date on the video search panel, click **Search**, and the search result will be displayed on the timeline panel. You can play back the video by choosing the start time for playback on the timeline panel and clicking **Play** on the playback window.

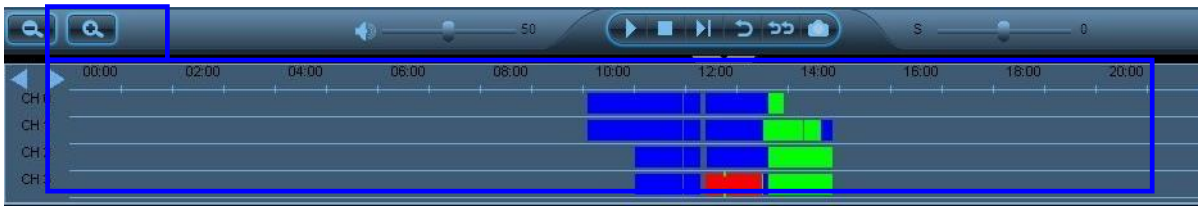
Note: See Search and Playback Videos by Date for information regarding to video search by date.

4.4.1.1 Video Search Panel



4.4.1.2 Timeline Panel

The search results are displayed on **Timeline** panel after you choose the date on which the videos were made.



Icon	Name	Function description
	Zoom out	Click to scale down the timeline in **Timeline** panel and display the video records in a long period of time.
	Zoom in	Click to scale up the timeline in **Timeline** panel and display the video records in a long period of time.
	Leftward	Click to move the timeline leftward when the timeline ratio is displayed.
	Rightward	Click to move the timeline rightward when the timeline ratio is displayed.
CH0–CH3	Channel	ZKiVision supports concurrent search and video playback in four channels.
00:00–24:00	Temporal scale	Divide the time of the day into 48 equal portions, and the minimum scale is half an hour. The time point of the current position will be displayed on the **Timeline** panel when you move the mouse on the **timeline**. Click the time point to accurately position the video.
	Manual video	
	Planned video	
	Alarm video	
		The starting point of video playback.

4.4.1.3 Playback Window

Icon	Name	Function description
/	Sound on / off	After the camera is connected, click to turn the sound on, and click again to turn the sound off.

	Volume	Drag the volume slider left to turn down the volume or drag the volume slide right to turn up the volume (1–100).
	Play/Pause	After you a camera channel is selected, click to play back the video, and click again to pause the video.
	Stop	Click to stop the video during the video playback.
	Single-frame play	Click to perform a single-frame play during the video playing. Each frame image will be displayed by every single click.
	Replay	Click to replay the video in the current channel.
	All replay	Click to replay all the videos in four channels.
	Image capture	Click to capture the image and save it to hard disks.
	Play speed	Drag the speed slider left to slow down the play speed or drag the volume slide right to accelerate the play speed (1–100). Speed adjustment range includes -2 (1/4 speed), 0 (normal speed), and 2 (2 times speed). The device uses normal speed (0) by default.
	Expand/Fold	Click to fold the **Playback** window, and click to expand it.

4.4.2 Remote Playback

Remote Video: is stored in NVR/DVR and other remote device hard disks, other than that stored locally.

After specifying search conditions on the remote video search panel, click Search. Then, search results are displayed on the time axis panel. Select the playback start time on the time axis panel and click Play in the playback window to play back a remote video.

Notes: 1) The remote video search and playback page is similar to the local video search and playback page. For details, see 4.4.1 "Local Playback".

2) The remote video search and playback operations are similar to the local video search and playback operations. For details, see 5.12 "Search and Playback Videos by Date."

4.4.3 Server Playback

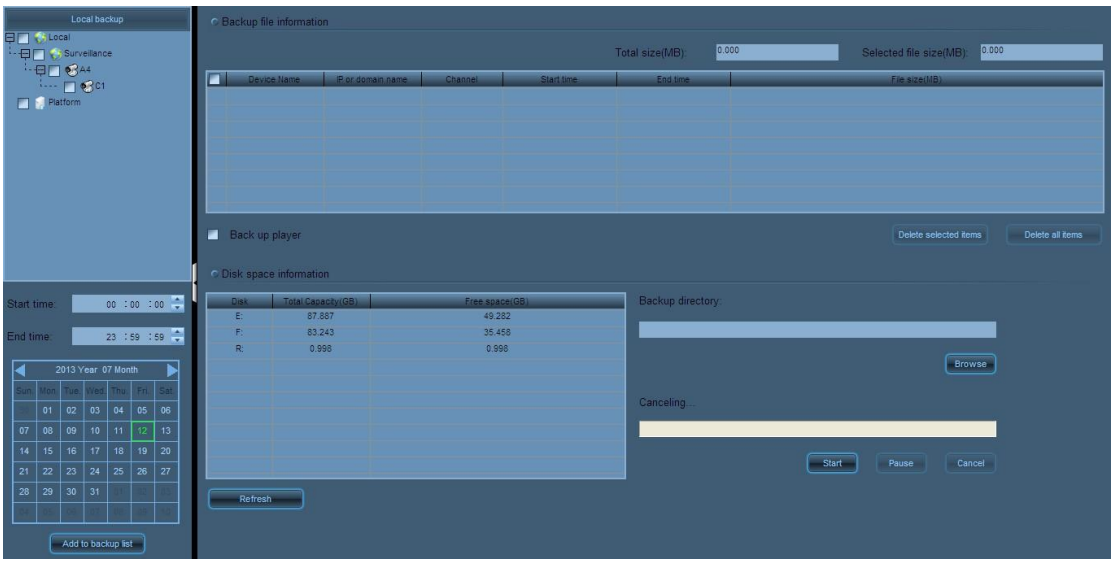
Server Video: is stored in MTS and other servers, other than that stored locally.

After specifying search conditions on the remote video search panel, click Search. Then, search results are displayed on the time axis panel. Select the playback start time on the time axis panel and click Play in the playback window to play back a remote video.

Notes: 1) The server video search and playback page is similar to the local video search and playback page. For details, see 4.4.1 "Local Playback".

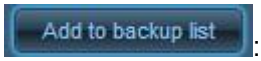
2) The server video search and playback operations are similar to the local video search and playback operations. For details, see 5.12 "Search and Playback Videos by Date."

4.4.4 Local Backup



Local Video Backup: is to back up videos stored locally to the specified disk.

After setting search conditions by date on the video search panel, click **Add to backup list**, and the search results will be displayed on the backup file list. Click the video to be backed up on the backup file list, set the backup path, and click **Start** to back up the video.

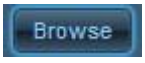


: Click the button after selecting the camera and the search time. If there is a video from the selected camera for the set search time, the search results will be displayed in the backup list on the right.

: Select one message in the backup list, and click the button to delete the message.

: Click the button to delete all the messages in the backup list.

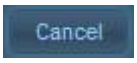
: Tick this option to back up the media player during video backup.



: Click the button to select the backup catalogue.

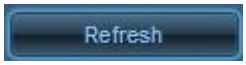
: Click the button to start backup.

: Click the button to pause backup.



: Click the button to cancel backup.

: Click once to select a disk in the disk list, and click the button to format the selected disk.

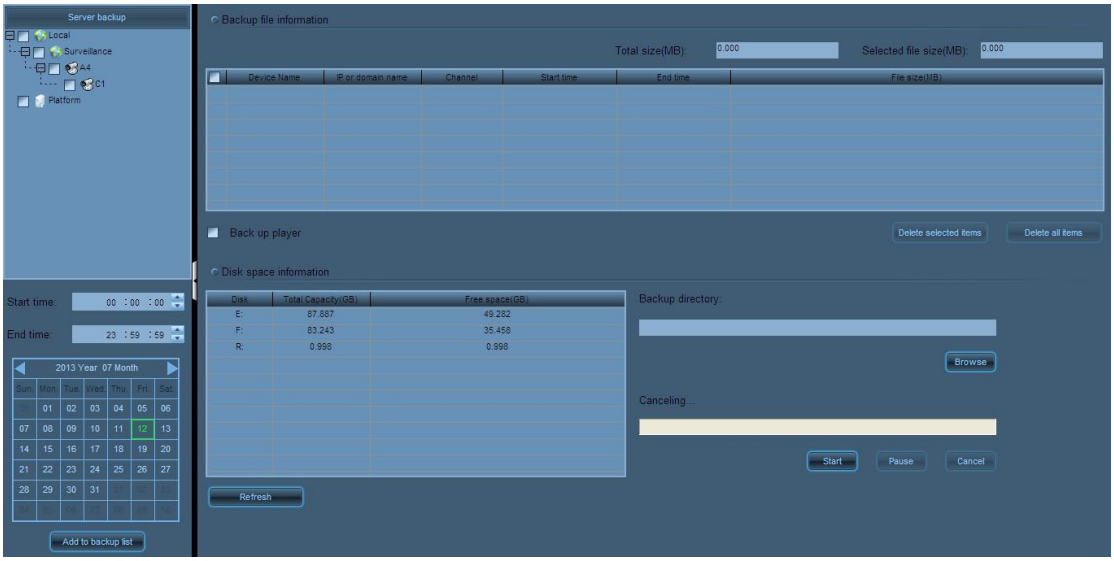


: Click to refresh the disk information.

Note: Refer to Back Up Videos for how to back up the video.

4.4.5 Server Backup

Server Video Backup: is to back up videos stored in the server to the specified disk.



Note:

① The server video backup interface is similar to the local video backup interface. See 4.4.4 Local Backup for details.

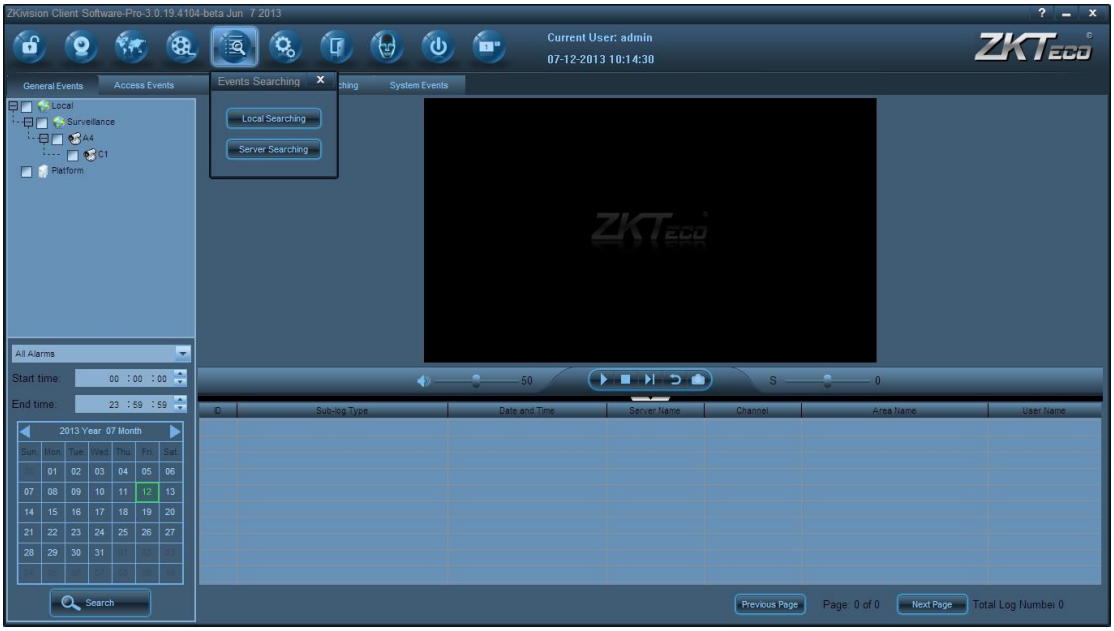
② The server video backup operation is similar to the local video backup operation. See 5.13 How to Back up Video for details.

4.5 Event Query

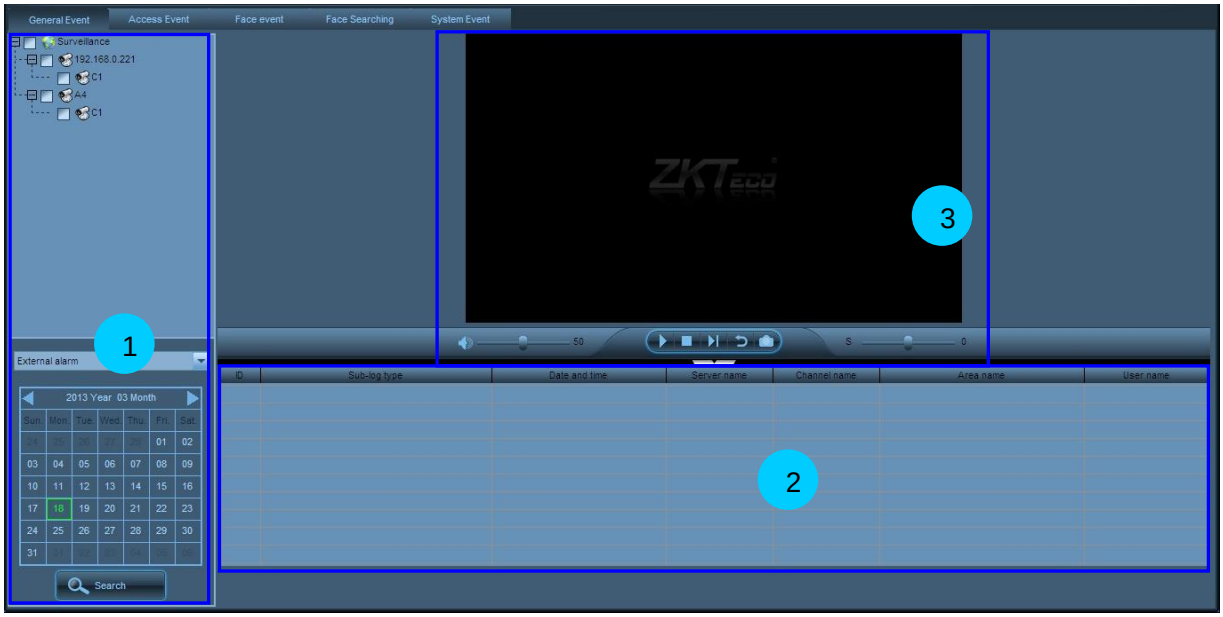
After setting search conditions on the log search panel, click **Search** or **Query**, and the search results will be displayed on the log list. You can query or play back the associated video.

Local Searching: is to search general events, access events, face events, face searching and system events in the local client.

Server Searching: is to search general events, access events and face events in the server.

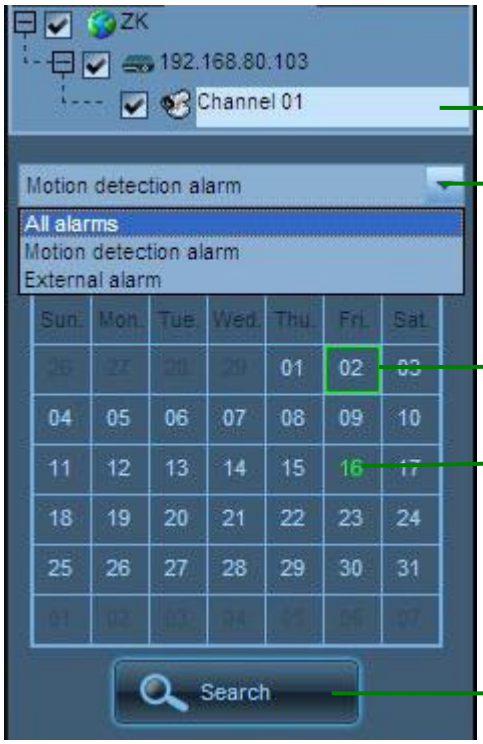


4.5.1 General Event



Area	Description
1	Log search panel
2	Log list
3	Playback window

4.5.1.1 Log Search Panel



1. Tick off the camera channels of alarm log to search for.

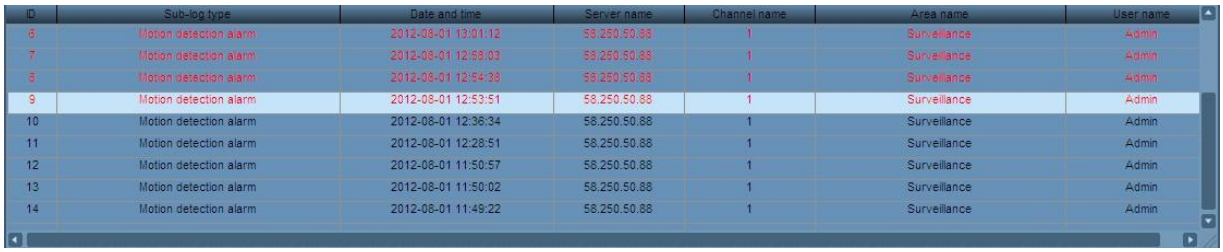
2. Choose a videotaping type to search for: All alarms, Motion detection alarm, or External alarm.

3. Click to choose the date to search videos (in green box)

Current date (in green characters)

4. Click **Search**.

4.5.1.2 Log List



Different colors indicate different types of log:

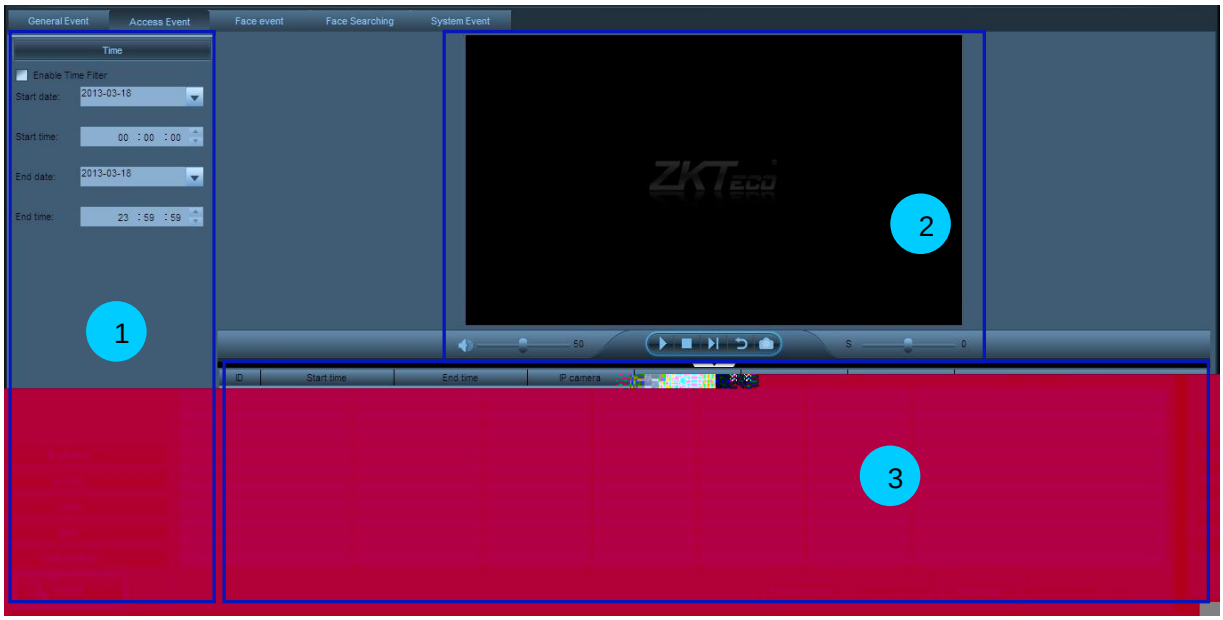
• Red -- Alarm log with associated video

• Black -- Alarm log without associated video

4.5.1.3 Playback Window

Note: For details about the icon and functions of the playback window, see 4.4.1.3 Playback Window.

4.5.2 Access Event



Area	Description
1	Log search panel
2	Log list
3	Playback window

Access event: records and stores access event logs after the access control and video linkage function is configured. For example, the access event sets whether to start video recording linkage

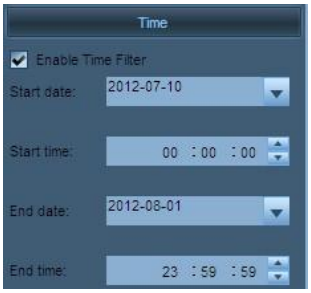
based on the alarm setting for alarm linkage and door opening linkage. The access event also displays video-contained events in red. You can double-click a log to play the contained video.

4.5.2.1 Log Search Panel

To search access controller event logs, you can set several filtering conditions, such as time, IP camera, access controller, alarm pattern, user ID and verification mode.

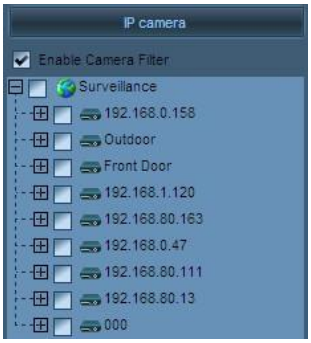
Note: The combination of various filtering conditions will filter the search results. If none of the filtering conditions is enabled, then all the current day's logs of all the devices will be searched by default.

- **Enable Time Filter**



After ticking **Enable Time Filter**, you can set the start time and end time for log searching.

- **Enable Camera Filter**



After clicking **Enable Camera Filter**, you can select the IP cameras of which the logs are to be searched for.

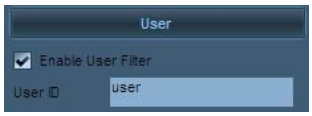
- **Enable Access Filter**

After clicking **Enable Access Filter**, you can select the access controllers of which the logs are to be searched for.

- **Enable Alarm Filter**

After ticking "**Enable Alarm Filter**", you can select types of alarm log to be searched for.

- **Enable User Filter**

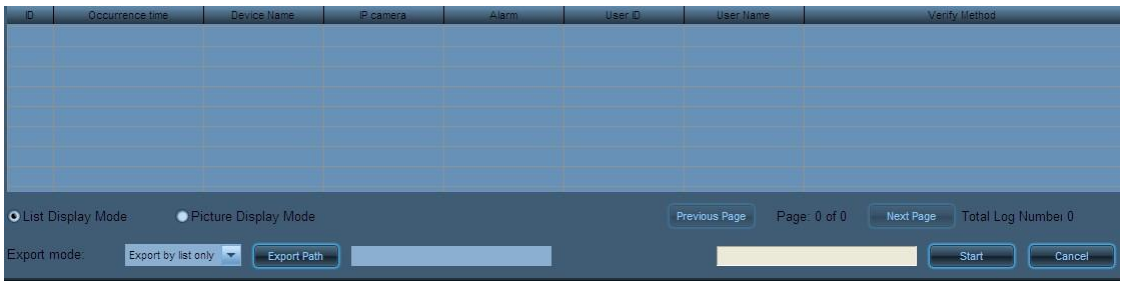


After clicking **Enable User Filter**, you can search for logs by user ID.

- **Enable Verification Mode Filter**

After **clicking Enable Verify Mode Filter**, you can search for logs by verify mode.

4.5.2.2 Log List



- **List Display Mode**

Search results are displayed by list, and different colors indicate different types of logs:

•Red – alarm logs with linked videos

•Black – alarm logs without linked videos

- **Picture Display Mode**

If captured pictures of access events are enabled in the Alarm Linkage Settings interface, search results can be displayed by picture. Click to view related pictures and double-click to play linked videos.

Previous Page: Click to view the search results in the previous page.

Next Page: Click to view the search results in the next page.

Total Log Number: is the number of searched logs.

Export Mode: includes Export by list only, Export by picture only, or Export all.

Export Path: Click the button to set the export path.

Browse: Click the button to select the backup directory.

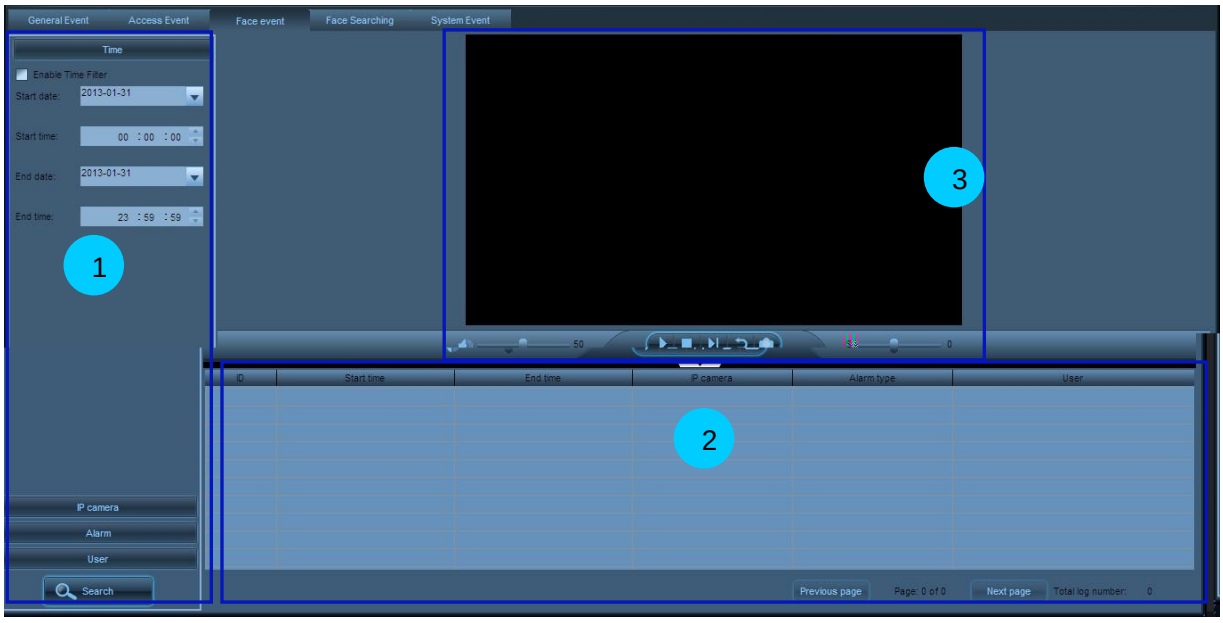
Start: Click the button to start exporting.

Cancel: Click the button to cancel exporting.

4.5.2.3 Playback Window

Note: The playback window of access controller events is the same as that of common events. For details, see 4.4.1.3 Playback Window.

4.5.3 Face Event



Area	Description
1	Log search panel
2	Log list
3	Playback window

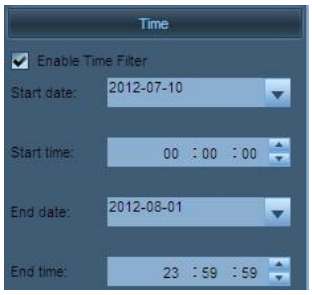
Face event: records and stores face event logs after the face recognition function is enabled. For example, the face event sets whether to start video recording linkage based on the alarm setting for unrecognized faces, common users, and blacklisted users. The face event also displays video-contained events in red. You can double-click a log to play the contained video.

4.5.3.1 Log Search Panel

To search for face event logs, you can set several filtering conditions, such as time, IP camera, door controller, alarm pattern, user ID and verification mode.

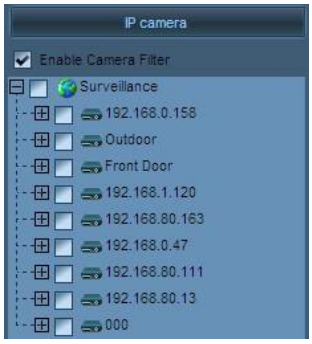
Note: The combination of various filtering conditions will filter the search results. If none of the filtering conditions is enabled, then all the current day's logs of all the devices will be searched for by default.

- **Enable Time Filter**



After ticking **Enable time filter**, you can set the start time and end time for log searching.

- **Enable Camera Filter**



After clicking **Enable camera filter**, you can select the IP cameras of which the logs are to be searched for.

- **Enable Alarm Filter**

After ticking "**Enable alarm filter**", you can select types of alarm log to be searched for.

- **Enable User Filter**

After clicking **Enable user filter**, you can search for logs by ID of face registered user.

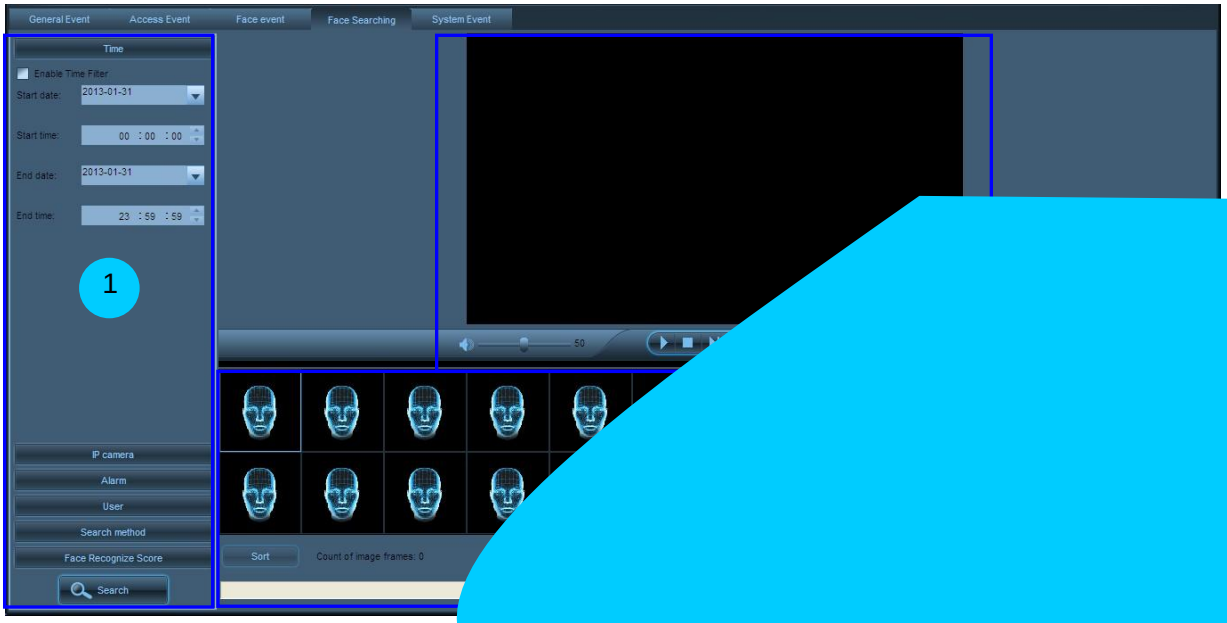
4.5.3.2 Log List

Note: The log list of face events is the same as that of common events. For details, see 4.5.1.2 Log List.

4.5.3.3 Playback window

Note: The playback window of face events is the same as that of common events. For details, see 4.4.1.3 Playback Window.

4.5.4 Face Searching



Area	Description
1	Log search panel
2	Face list
3	Playback window

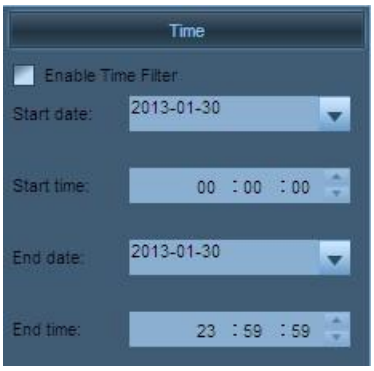
You can widely search for videos of all people that ever appear on the recording screen and specify query conditions to search for videos quickly and accurately, making face recognition to be applied more widely.

4.5.4.1 Log Search Panel

When searching for faces, you can specify multiple filter conditions: time, network camera, alarming mode, user, search method, and face recognition score.

Note: Search results are filtered based on multiple added filter conditions. If no filter condition is specified, all faces in videos of all devices on the current day are searched out by default.

- **Filter by time**



After selecting **Enable Time Filter,** you can set the start time and end time for log search.

- **Filter by camera**

After selecting **Enable Camera Filter**, you can select the network camera for log search.

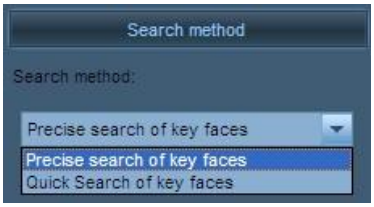
- **Filter by alarm**

After selecting **Enable Alarm Filter**, you can set the type of alarm logs for search.

- **Filter by user**

After selecting **Enable User Filter**, you can enter the user ID for log search.

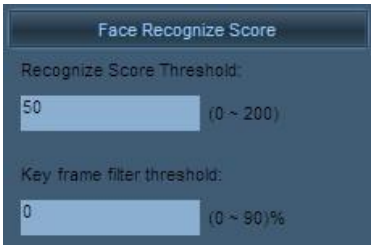
- **Filter by search method**



After you select **Precise search of key faces** from the drop-down list, all faces that ever appear in videos will be searched accurately and comprehensively.

After you select **Quick search of key faces** from drop-down list, faces that ever appear in videos will be searched quickly.

- **Filter by face recognition score**



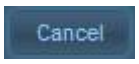
The value of **Recognize Score Threshold** affects the rate of faces that can be searched out. The larger the value is, the more accurately faces are searched and the fewer faces can be recognized. The default value is recommended.

If **Key frame filter threshold** is set to a larger value, the system filters out faces with great similarities, and consequently fewer faces are searched out.

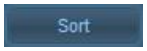
4.5.4.2 Face List

Face images that are searched out from videos are displayed in the face list.

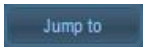
If it is clicked, face search is paused.



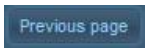
If it is clicked, face search is cancelled.



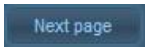
If it is clicked, search results are sorted by face recognition score in descending order.



Enter a number in the box, and click the bottom to directly jump to this page.



If it is clicked, the search results on the previous page are displayed.



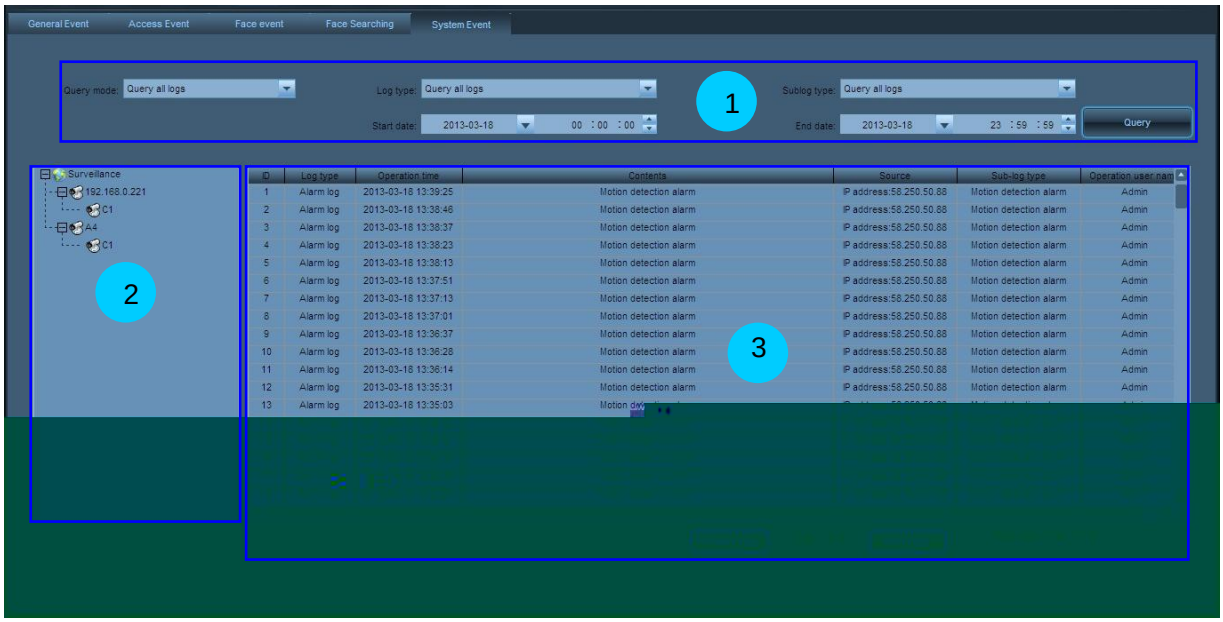
If it is clicked, the search results on the next page are displayed.

If it is clicked, selected faces will be added to the template of faces to be registered.

4.5.4.3 Playback Window

Note: The playback window of face search is similar to the playback window of common events. For details, see 4.4.1.3 "Playback Window."

4.5.5 System Event



Area	Description
1	Log query panel
2	Device list/User list
3	Log list

Query mode Query logs based on a specified type of data.

Query all logs Query all logs of all devices.

Query based on device Select a device from the device list to query its logs.

Query based on user Select a user with operation logs from the user list.

Log type

	Log Type	Description	Sub-log Type
All logs: Record all information of the system.	Operation log	Record all operation information of a user.	Network preview
			Voice intercom
			Guard
			PTZ control
			Remote setting

			Time calibration
			Others
	Alarm log	Record the alarm information of a device.	Disk full alarm
			Video loss alarm
			Motion detection alarm
			Hard disk read/write error alarm
			Standard mismatch alarm
			External alarm
			Others
	System log	Record information such as user login, logout and related information.	Login
			Logout
			Local settings
			Others

Start date Indicates the start time of a log search.

End date Indicates the end time of a log search.

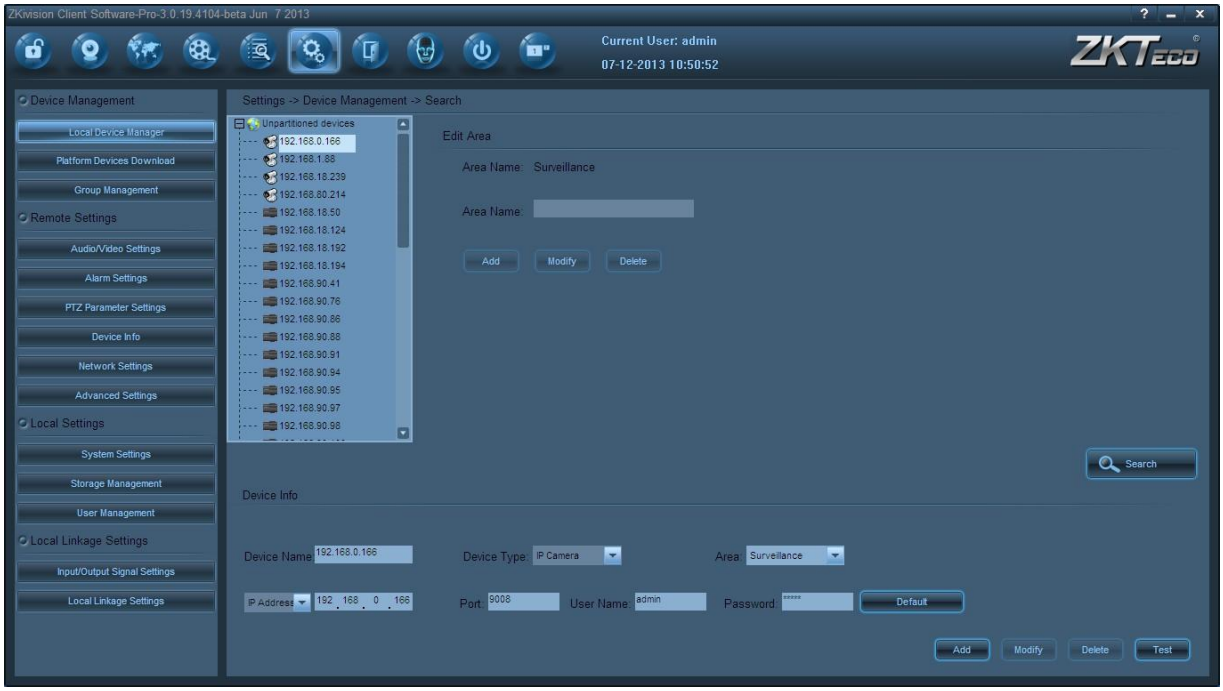
Query Select a camera channel from the device list, or a user from the user list. Then set query conditions on the **Log query** panel and click the **Query** button. Eligible results are displayed in the log list.

Previous page View the query results on the previous page.

Next page View the query results on the next page.

Total log number Indicates the number of all log query results.

4.6 Settings



The **Settings** menu contains 12 submenus and allows settings of multiple devices (for example, the IP cameras).

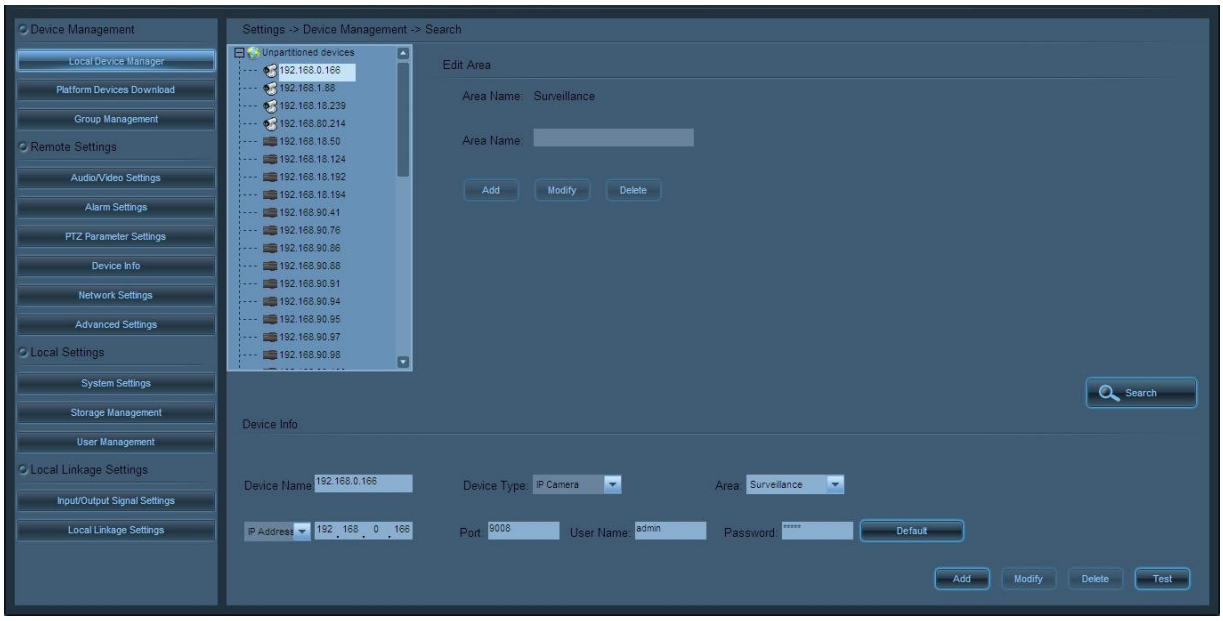
- **Common operations and icon functions in the Settings menu**

Camera selection: Select a channel in the device list by clicking the channel name. **Camera connection**: Connect a camera by double-clicking the channel name in the device list.

Icon	Function description
Add	Add devices/areas/groups/camera presets/cruise paths/users.
Modify	Save modified parameters or switch to modification state.
Delete	Delete existing devices/areas/groups/camera presets/cruise paths/users.
Apply	Synchronize the modified parameters with the remote device.
Reset	Restore the parameters to their values in the last saving.
Default	Restore parameters to their default values
Test	Test whether the device can be connected properly

Save	Save the modified information to local database
Cancel	Cancel modification
Duplicate	Copy the setting to other devices

4.6.1 Local Device Management



- **Area Information**

Area name The name of the upper level area of the currently chosen area.

Area name Areas that can be set.

- **(Local) Device Information**

Device name Device names displayed in the software. After the **Device name** is set, the device list displays only the device name rather than the device IP address.

Device type Includes IP camera, access control device or NVR/DVR.

Select areas The area where the device belongs to.

IP address/Domain name The device cannot be connected successfully unless the device IP and domain name are consistent with that in the remote device.

Port The device's communication port. The device cannot be successfully connected unless the device communication port is consistent with that in the remote device.

User name The user name that used to visit the front-end device. The device cannot be successfully connected unless you enter a correct user name.

Password The password that is used to access front-end device, and the device cannot be successfully connected unless you enter a correct password.

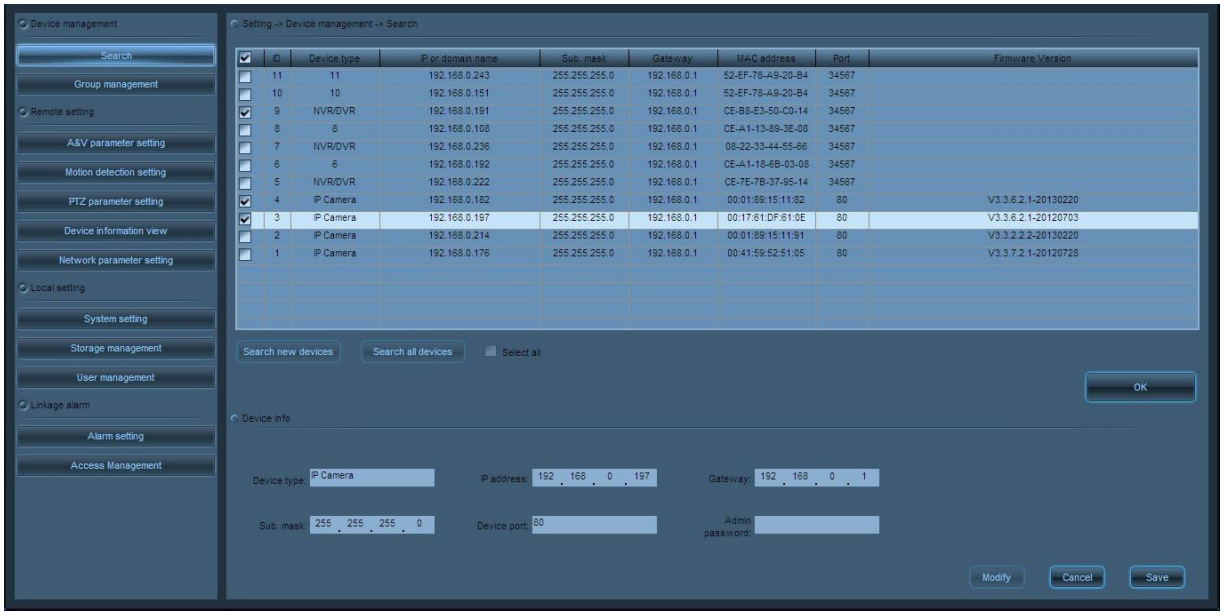
Default: The password is used as the default password for connections if **Default** is ticked.

Note: 1. There are at most 128 areas can be added.

2. After device search is completed, the camera cannot videotape or capture images unless it is added to an area. An un-partitioned device cannot be used.

- **Device Search**

Click **Search** to display the search interface:



Search all devices over the LAN.

Search new devices over the LAN.

Select all devices in the search list.

- **(Remote) Device Information**

Device Type Includes IP camera, access control device or NVR/DVR.

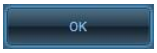
IP address The default IP address is 192.168.1.88. It can be modified as needed.

Gateway The default gateway is 192.168.1.1. It needs to be reset if the device and the PC are not in the same network segment.

Subnet mask The default subnet mask is 192.168.1.88. It can be modified as needed.

Device port The device port number is 80 by default. To modify it, please contact the network administrators or network professionals. The camera will be restarted after the port is successfully modified.

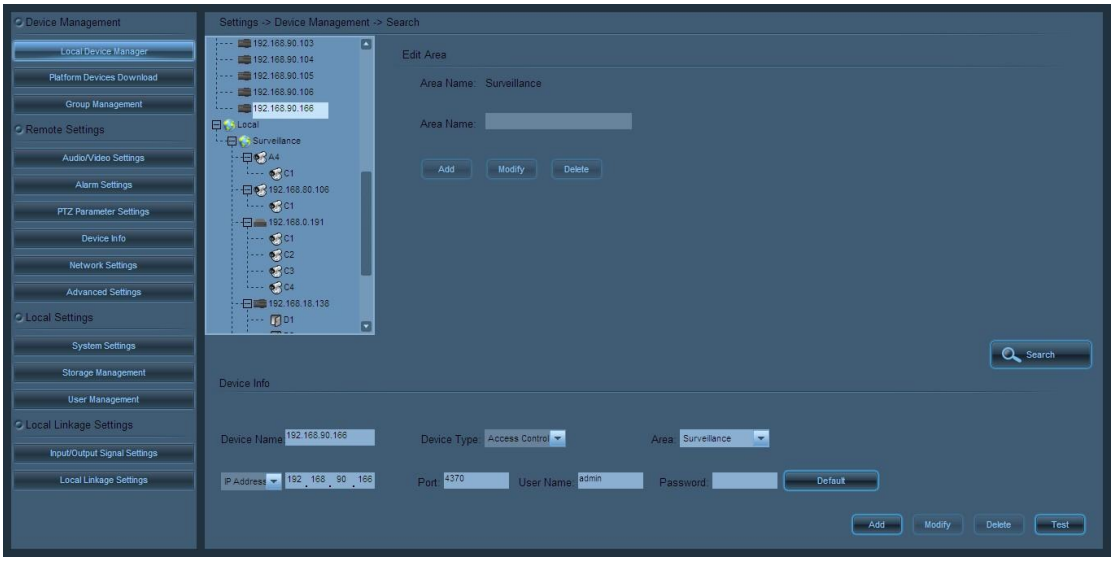
Administrator password To modify the IP address, gateway, subnet mask or port, a correct administrator password must be entered.

Click 

to go back to the upper interface.

Note: For information regarding to device remote parameters (IP address and port) modification, see 5.4 Modify Network Parameters of a Camera.

4.6.2 Platform Devices Download



Server IP: is the IP address of CMS server.

Server Port: is the port of CMS server.

User Name: is the name of CMS operator with permission to access the client.

Password: is the operator's password.

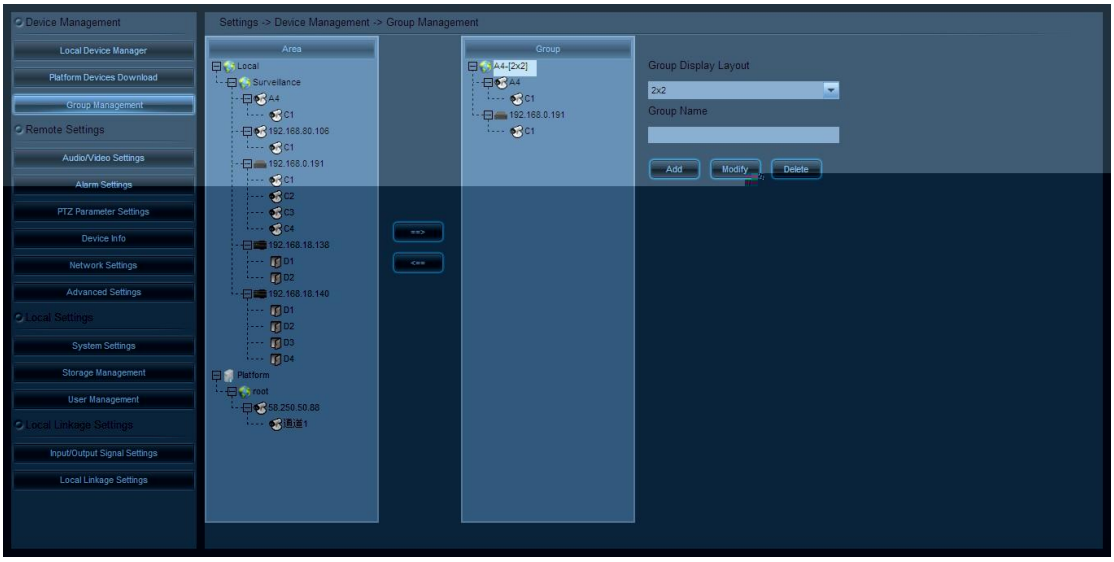
: Click the button to login the CMS server after inputting correct server information.

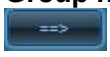
: Click the button to clear all local server data, including the platform device tree and related linkage information.

: Click the button to clear local server data and synchronize server data locally, which is applicable for logging in different servers to obtain different device trees.

: Click the button to synchronize server data directly and locally, which is applicable for logging in the same server to update data.

4.6.3 Group Management

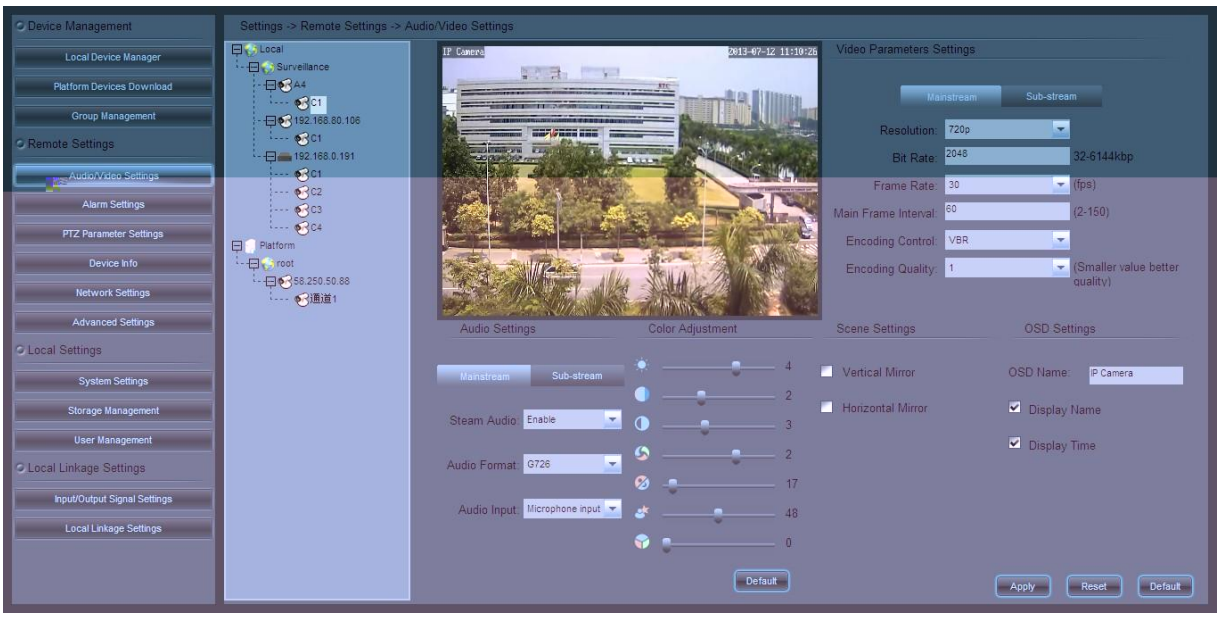


Group Type	The number of images and includes 1-image, 4-image, 5-image, 6-image, 8-image, 9-image, 16-image, 17-image, 19-image, and 22-image.
Group type	Choose group type (according to picture quantities), including single picture, 4-picture, 6-picture, 8-picture, 9-picture or 16-picture.
Group name	Set group names.
	Click a channel to be grouped in the device list. Then, click a group in the group list and click to add the channel to the group.
	Click a channel to be deleted in the group list and click to delete the channel from the group.

Note: 1. The device only can be operated after partition.

2. There are at most 20 groups can be added.

4.6.4 Audio and Video Parameter Settings



Double-click a camera channel in the device tree, and set the audio and video parameters after connection.

- **Video Parameter Settings**

Resolution Resolution is a standard to measure the image definition (unit: pixels). The higher the value is, the clearer the image is.

The main stream definition of HD cameras is 720P (1280*720 pixels), and the secondary stream definition is QVGA (320*420 pixels). For the main stream definition of HD cameras, you can choose one from D1, CIF, and QCIF. For the secondary stream definition of HD cameras, you can choose one from CIF and QCIF. D1 image resolution: 704*576 pixels, CIF image resolution: 352*288 pixels, and QCIF image resolution: 176*144 pixels.

Bit rate Indicates the transmission of data traffic per second. Generally bit rate is the multiple of 128 Kbit/s. The higher the bit rate is, the clearer the definition is. You can set an appropriate bit rate based on the network condition.

Frame rate indicates the number of pictures displayed on the screen per second. Frame rate can be set, and the higher the frame rate is, the better the video effect is. Generally, a frame rate that exceeds 24 frames per second is called all realtime images.

Main frame interval An image would be used as the main image in video compression. The rest images will be compared with this one and only the different images will be saved. When videotaping scenes with fast moving

objects, shorten the frame interval to avoid blurred streaks or motion blur. When videotaping scenes with slow moving objects, lengthen the frame interval to reduce the data volume and improve the compression ratio.

Video coding control You can select **Fixed stream** for a scenario in which surveillance activities are gentle, and the video encoder shall encode as the stream velocity set in the stream settings. You can select **Variable bit rate** for a scenario in which surveillance activities are intense, and the video encoder can operate at a variable bit rate without losing image quality. Encode based on the set stream velocity, but the encoding will not follow this velocity completely. **Video encoding quality** You can choose any video encoding quality from 1 to 6. The smaller the value is, the better the image quality is, and the greater the stream control is.

- **Audio Parameter Settings**

Audio acquisition **Enable** indicates that transmitting audio signals is available. **Disable** indicates that transmitting audio signals is unavailable.

Audio format You can choose G711 or G726 as the audio format.

	Code rate	Sound quality	Application condition
G711	Larger	Higher	The network is in good condition
G726	Medium	Intermediate	The network is in intermediate condition

Audio input mode When a microphone is functioned as the external audio acquisition device, choose **Microphone input** to use an external amplification device to amplify the audio signal because the microphone has a low output power. When the recording volume and the output power of the audio acquisition device are high, choose **Linear input** to get a better recording effect.

- **Color Adjustment**

See the **Color Adjustment panel** in 4.1.4 Control panel for details.

- **Scene Settings**

Image up/down rotation Select it to rotate the image up and down. This is only for HD cameras.

Image left/right rotation Select it to rotate the image right and left. This is only for HD cameras.

- **OSD Settings**

Name Overlap Select it to overlap the camera name to the upper left corner of the video.

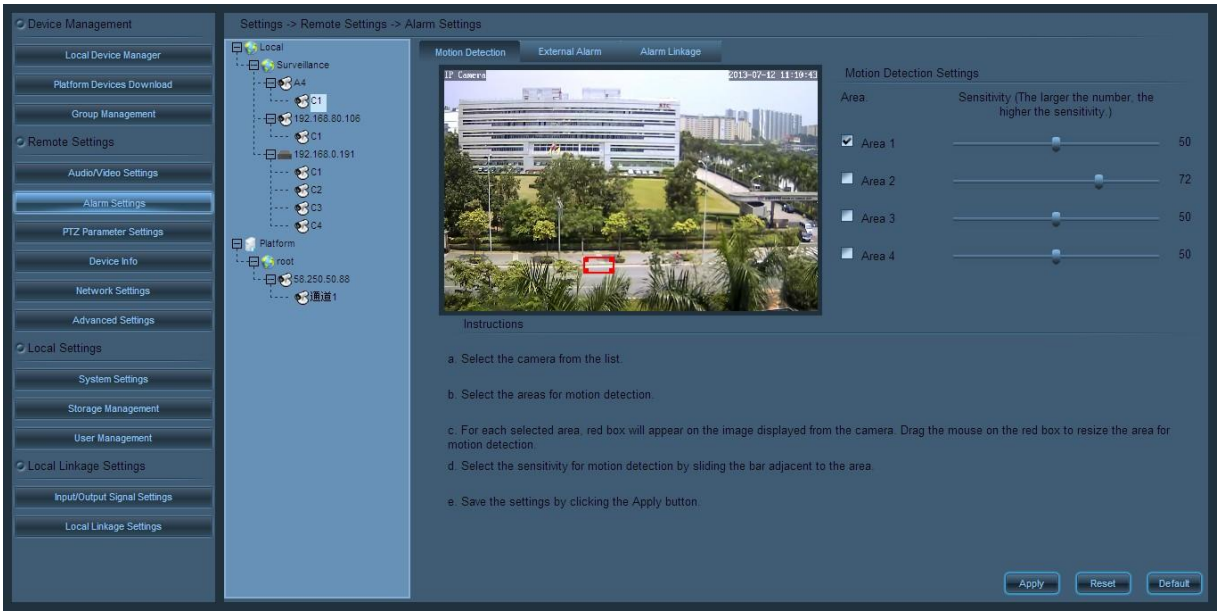
Time Overlap Select it to overlap the camera time to the upper right corner of the video.

OSD name The camera name, with a maximum number of characters of 17 that can be entered

4.6.5 Alarm Settings

Double-click a camera channel in the device tree, and set the audio and video parameters after connection.

- **Motion Detective**



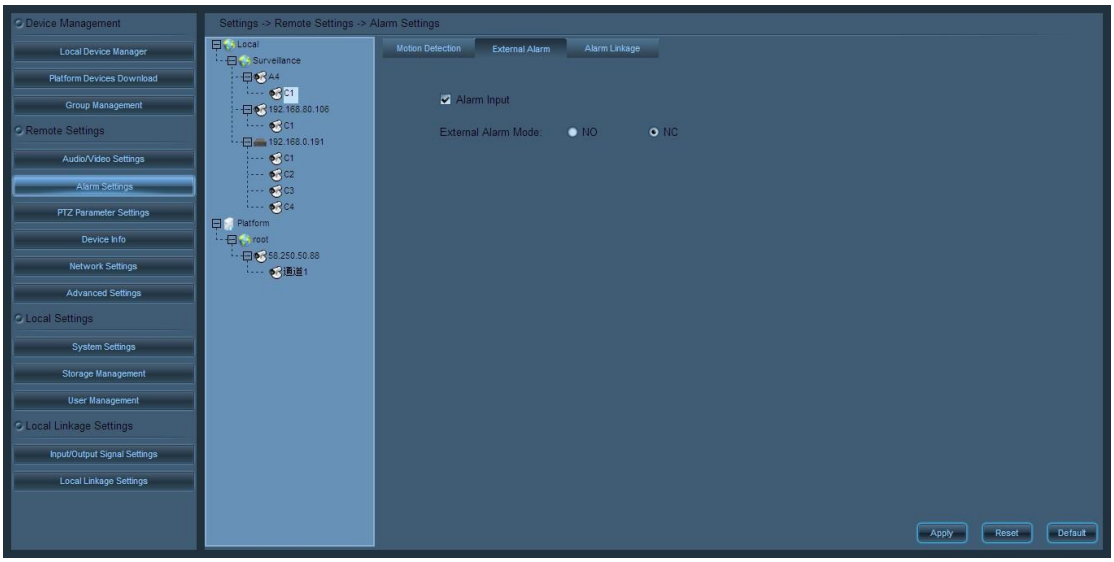
To monitor a specific area and ensure the alarm can be automatically activated when abnormal motion occurs, you can select and activate motion detection. Double-click the camera channel in the device tree and set the motion detection of the camera after connection. The camera supports 4-motion-detection-area setting. Tick off the option box on the right side of the interface to activate the corresponding options.

Detection area Tick off the option box on the right side of the interface to activate the corresponding options. The 4-motion-detection-area setting is supported on the camera.

After an area is activated, the area box and the area number will be displayed on the screen. Move the mouse into the area box. Left-click the mouse to drag the area box into any place on the image. You can also move the mouse to the lower right corner of the area box. Left-click the mouse to adjust its size.

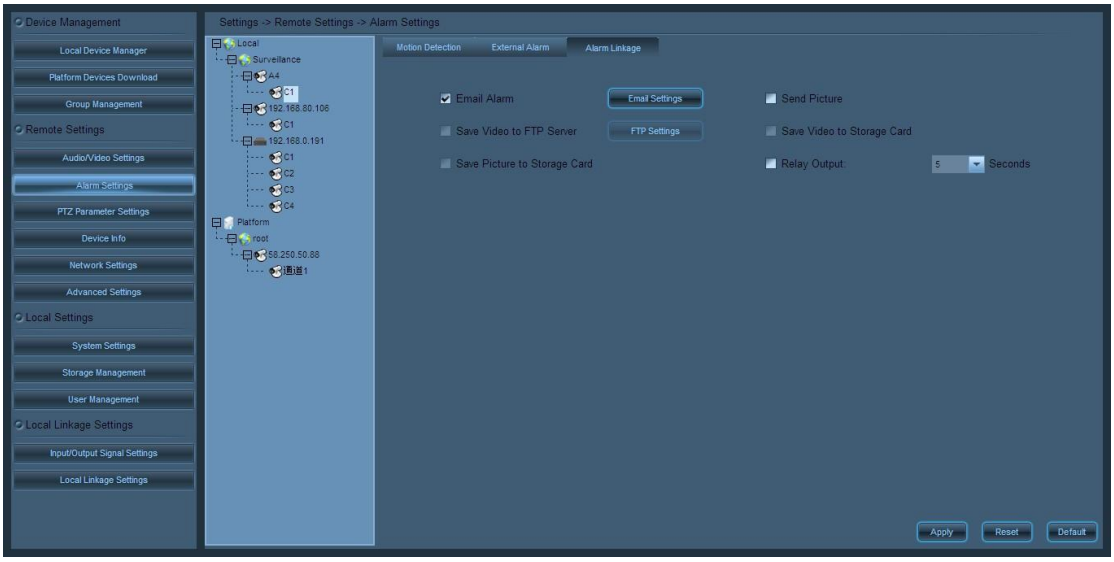
Sensitivity The sensitivity ranges from 0 to 100. The larger the number is, the higher the sensitivity is.

- **External Alarm**



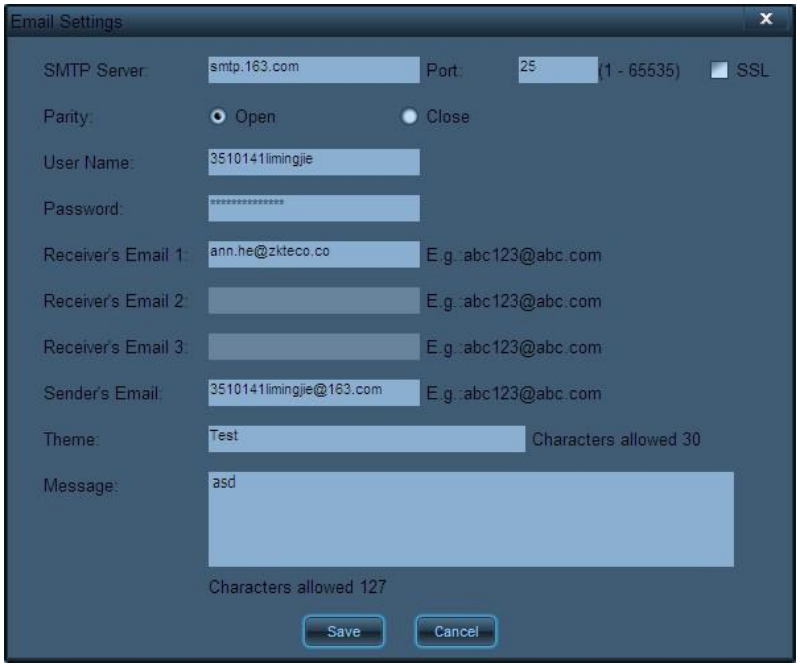
If the device is equipped with an external alarm input device, check "Alarm Input" to enable external alarm input. If the alarm input device is a normally open device, select "NO"; if the alarm input device is a normally close device, select "NC".

- **Alarm Linkage**



Once an alarm is triggered, several modes of alarm are available:

Email Alarm: is to send an alarm email to the preset mailbox; click "Email Settings" to enter the Email Settings interface.



SMTP Server: is the IP address of SMTP server. See your mailbox settings for details.

Port: is 25 by default. To modify the port, please contact your network administrator or consult professionals.

SSL: Check the option to enable secure connection. See your mailbox settings for details.

Parity: If you select "Open", you need to input the user name and password for communications upon successful authentication; if you select "Close", you do not need to input the user name and password for authentication.

User Name: is the name of email.

Password: is the password of email.

Receiver's Email: is the email address to receive alarm emails. Please input at least one address.

Sender's Email: is the address displayed in the alarm emails.

Theme: is the subject of the alarm emails.

Message: is the content of the alarm emails and only supports English input.

Note:

1) The SMTP server should support POP3 Protocol. Because may mail servers disable this protocol to strength security and reduce spam mails, you need to verify whether your selected SMTP server supports POP3, or email sending may fail.

2) Check the SSL option for some mail servers with SSL certification.

3) Set correct DNS in the "Network Settings" interface to send emails successfully.

Send Picture: is to send captured pictures to the preset email.

Save Video to FTP Server: is to transmit video caches in the storage card to the FTP server (only available if the storage card is inserted); click "FTP Settings" to enter the FTP Server Settings interface.

FTP Server: is the IP address or domain name of FTP server.

Port: is 21 by default. To modify the port, please contact your network administrator or consult professionals.

User Name: is the user name applied in the FTP server.

Password: is the password applied in the FTP server.

Passive Mode: Data connection is initiated by the client program under this mode. Select "Open" to open the passive mode; select "Close" to close the passive mode.

Path: Add any subfolder path in the FTP server (the subfolder must be created in the FTP server in advance).

Test FTP Settings: Click "Test" to see whether the FTP server can be successfully connected.

Note: To use the FTP function, apply for a user name and password in the FTP server and for a storage space. The user must have permission to write in and create a subdirectory in the storage space.

Save Video to Storage Card: Record a 30s video and save it to the storage card (including a 5s clip before the alarm).

Save Picture to Storage Card: Save snapshot pictures to the storage card.

Relay Output: Close the relay to enable alarm output. The optional alarm durations are 5s, 10s, 20s or 30s.

Note: The function of "Save Video to FTP Server" can be enabled only when the storage card is inserted into the device, and the function of "Save Video to Storage Card" is enabled at the same time.

4.6.6 PTZ Parameter Settings

Double-click the camera channel in the device tree, and set the PTZ parameter after connection.

- **PTZ Control**

See the **PTZ control** panel in 4.1.4 Control panel for details.

- **Pan-tilt Settings**

Address code It is used to distinguish various pan-tilts. The address code of the pan-tilt can be modified by using pan-tilt internal code. Please set the address code to match it with the pan-tilt address code.

Protocol You can choose PELCO-D or PELCO-P as the communication protocol of pan-tilt motor control. This protocol must be consistent with the pan-tilt internal control protocol.

Baud rate For the transmission frequency of RS-485 signal, the higher the baud rate is, the faster the transmission speed is, and the error rate rises accordingly. The baud rate must be consistent with that of the internal pan-tilt.

Data bits, stop bits, and **calibration** The transmission parameters of RS-485 protocol must be consistent with that of the internal pan-tilt.

Note: 1. Due to different production standards of manufactures, when the incomplete match of the address codes occurs, try to add 1 or minus 1 to implement complete match.

2. For pan-tilt related parameters, see *Pan-tilt User Manual.*

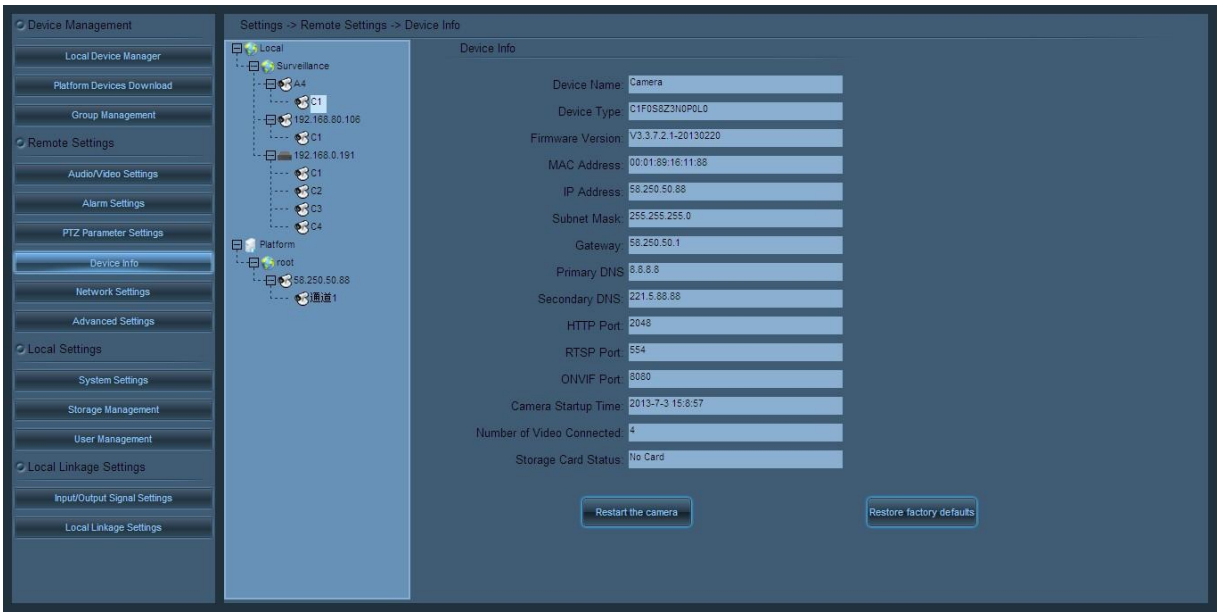
- **Preset and Cruise**

When the motion pan-tilt arrives at the place you focused on. Click and choose the preset number in the preset list. Set the preset name and click **Add** to add the preset**.**

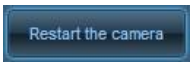
After adding two or more presets to the camera channel, you can configure a cruise based on the presets.

After setting the cruise, click **Add** to add a cruise. Click and select a **Preset** in the preset list, Select the cruise that will be added to from the drop-down list, Click to add this preset to the selected cruise. Click and choose the unnecessary preset. Click to delete it from the cruise. After saving the cruise path, click "Test" to test the cruise path.

4.6.7 Device Information View



Double-click the camera in the device list. Check the configuration information of important parameters of the camera in the right side of the interface.

Click 

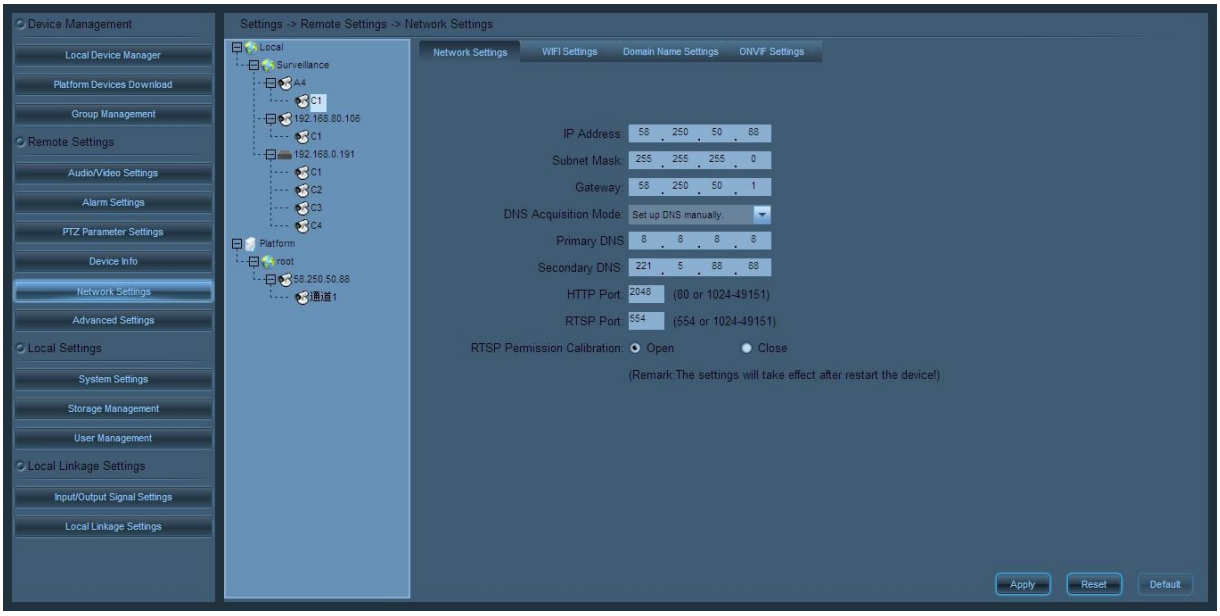
to restart the camera.

Click

to restore the camera parameters to its factory defaults.

4.6.8 Network Settings

Double-click the camera channel in the device tree. After successful connection, the system obtains the network parameters which can be set.



IP address The default IP address is 192.168.1.88. It can be modified as needed.

Subnet mask The default subnet mask is 192.168.1.88. It can be modified as needed.

Gateway The default gateway is 192.168.1.1. It needs to be reset if the device and the PC are not in the same network segment.

DNS acquisition mode Domain Name Server (DNS) can translate the domain name into an IP address. In **Manually set the DNS** mode, you need to enter the primary and secondary DNS addresses manually. When select "Automatically obtain the DNS", the DNS address will be obtained automatically when the camera is connected with the LAN.

Primary DNS The primary DNS is 192.168.1.88 by default. It can be modified as needed.

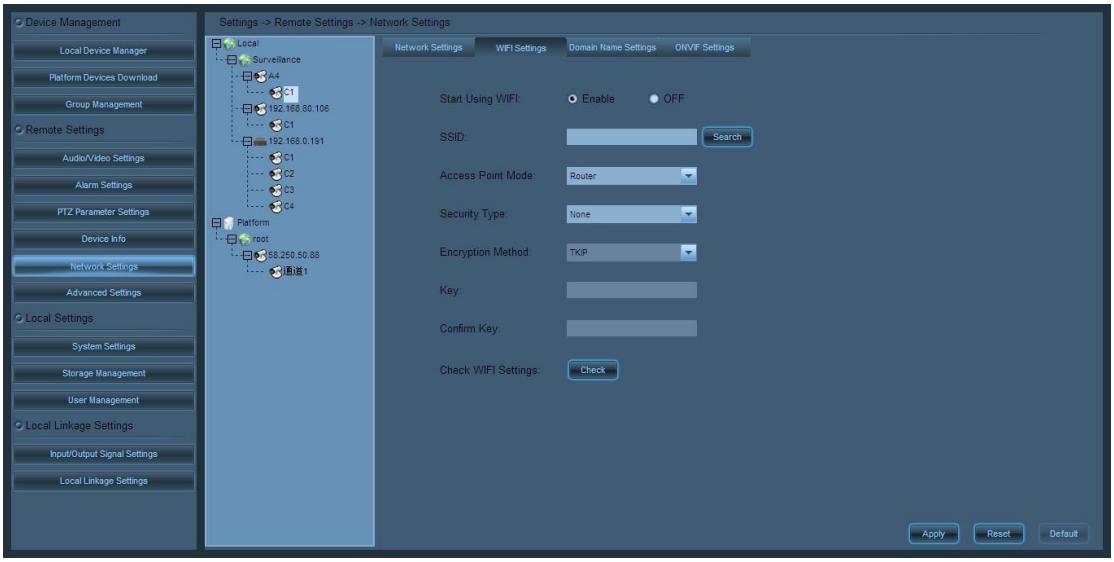
Secondary DNS The system will connect the secondary DNS when the connection failure or error of the primary DNS occurs.

HTTP port The device port number is 80 by default. To modify it, contact the network administrators or network professionals. The camera will restart after the port is successfully modified.

RTSP Port 554 by default. If a player that supports RTSP Protocol is needed to connect the device and play videos, input the URL address "rtsp://IP address/stream code"; if the RTSP port is modified, input "rtsp://IP address: port/stream code". The device is restarted after successful modification of the port.

Parity If you select "Open", you need to login to connect the device when using a player that supports RTSP Protocol; if you select "Close", you do not need to login.

- **WIFI Settings**



Start Using WIFI: Select "Enable" to allow WIFI connection; select "OFF" to disable WIFI connection.

SSID: is the login name (case sensitive) for WLAN authentication. Only users who pass authentication can access WIFI. Click "Search", and a WIFI webpage will pop up to list all available WIFIs.

Access Point Mode: includes two options. "Router" mode corresponds to a star structure network, and "Point-to-point" mode corresponds to a point-to-point peer-to-peer network. Select a network in the WIFI search results to automatically obtain the access point mode of the network.

Security Type: is set in the router, including five types: none, WEP64, WEP128, WPA-PSK and WPA2-PSK. Select a network in the WIFI search results to automatically obtain the security type of the network.

Encryption Method: is used for wireless connection, including TKIP and AES. Select a network in the WIFI search results to automatically obtain the encryption method of the network.

Key: Input the key if it is set in the router.

Confirm Key: Input the key again to confirm.

Check WIFI Settings: Click "Check" to check whether the WIFI settings are correct.

☺ **Note:**

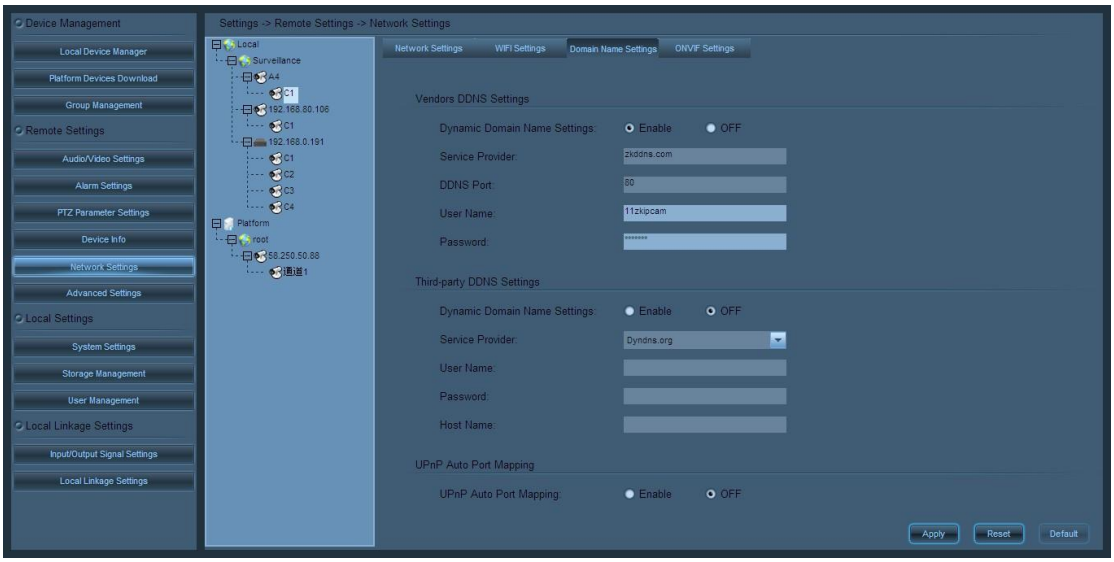
1) Only a device with built-in wireless module can support WIFI connection. Before configuring the WIFI network, please verify whether the device has the built-in wireless module.

2) When the device is connected with a network cable and enables WIFI connection, wired connection is the first choice when the device is started. If wired connection fails, wireless connection is selected. The IP address and port for wireless connection are the same as those for wired connection.

3) To ensure network security, it is strongly recommended the security settings be enabled and that the encryption method of WPA-PSKWPA2-PSK AES be used.

4) Please see the *User Manual for WEB Surveillance* – 4.11 How to Configure WIFI Connection for using WIFI to access device.

- **Domain Name Settings**



Register a domain name for use in constantly IP changing environment such as ADSL.

After Dynamic Domain Name Settings are enabled, select the "Service Provider" that provides DDNS service, and input the service provider's user name and password applied in the server.

- **Vendors DDNS Settings**

Dynamic Domain Name Settings: Click "Enable" to enable Vendors DDNS; click "OFF" to disable Vendors DDNS.

Service Provider: provides DDNS service.

DDNS Port: is 80 by default, and cannot be modified if Vendors DDNS is used.

User Name: is the service provider's user name applied in the server.

Password: is the service provider's password applied in the server.

- **Third-party DDNS Settings**

  Dynamic Domain Name Settings: Click "Enable" to enable Third-party DDNS; click "OFF" to disable Third-party DDNS.

  Service Provider: provides DDNS service. Dyndns.org, 3322.org and Dynddns.us are supported.

  User Name: is the service provider's user name applied in the server.

  Password: is the service provider's password applied in the server.

  Host Name: is the domain name assigned in the server.

- **UPnP Port Mapping**

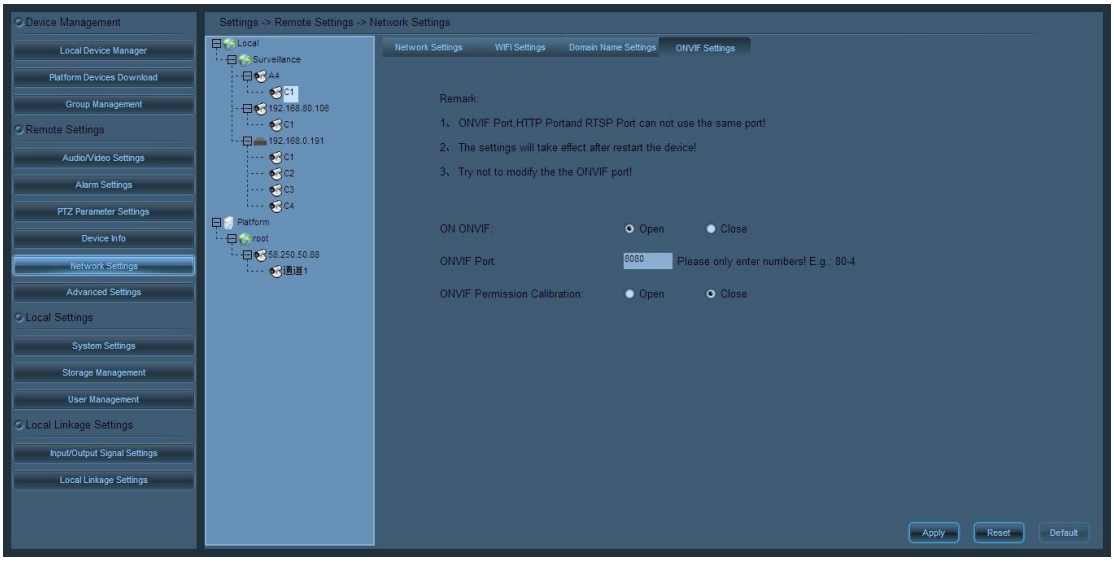
  UPnP Port Mapping: UPnP refers to "Universal Plug-n-Play". If UPnP is enabled, the device automatically communicates with the router in the LAN upon being connected to the LAN, and makes the router open a port to map with its port. So you do not need to login the router for port mapping.

Note:

1) To use the UPnP function, first confirm UPnP is enabled in the router.

2) Because routers have various models, not all of them can support UPnP well. Please test whether UPnP can work with the matched router. Otherwise, UPnP is not recommended. According to the current test, UPnP can work well with the TP-LINK router.

- **ONVIF Settings**



Our network surveillance device supports the ONVIF function. Once the function is enabled, the client software that supports ONVIF Protocol can be used for monitoring, recording and PTZ control of the network surveillance device.

ON ONVIF: Select "Open" to enable ONVIF; select "Close" to disable ONVIF.

ONVIF Port: is 8080 by default. Please do not modify the ONVIF port if not necessary. The device is restarted after successful modification of the port.

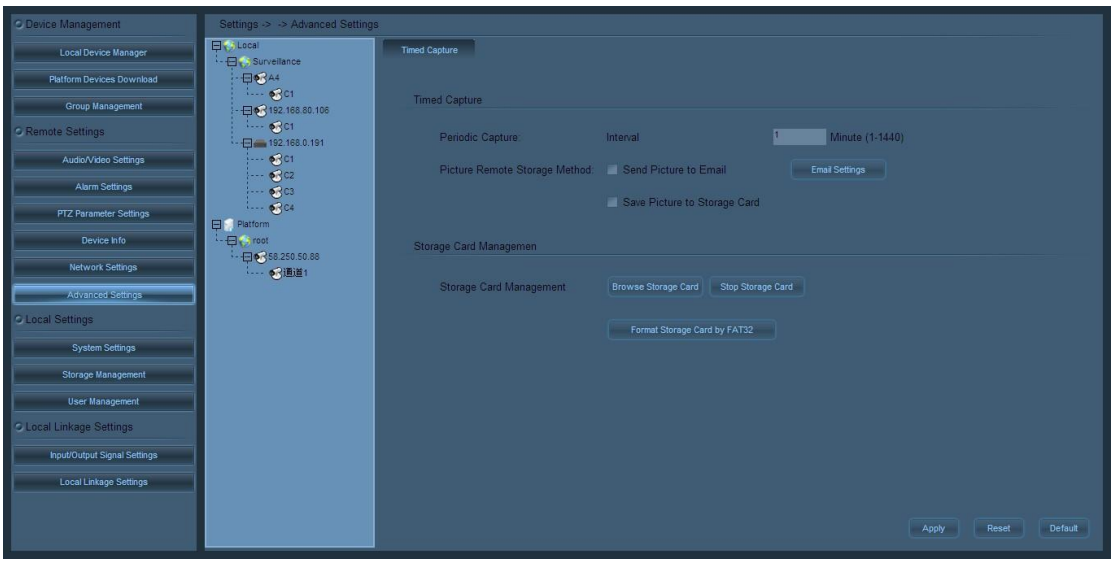
ONVIF Permission Calibration: If you select "Open", you need to login to connect the device when using the client software that supports ONVIF Protocol; if you select "Close", you do not need to login.

Note:

1) ONVIF port, HTTP port and RTSP port shall not be the same!

2) ONVIF settings take effect after the device is restarted.

4.6.9 Advanced Settings



- **Timed Capture**

Periodic Capture: Set an interval for timed capture.

Picture Remote Storage Method: Check "Save Picture to Storage Card" to save captured pictures to the storage card; check "Send Picture to Email" to send captured pictures to the preset email.

- **Storage Card Management**

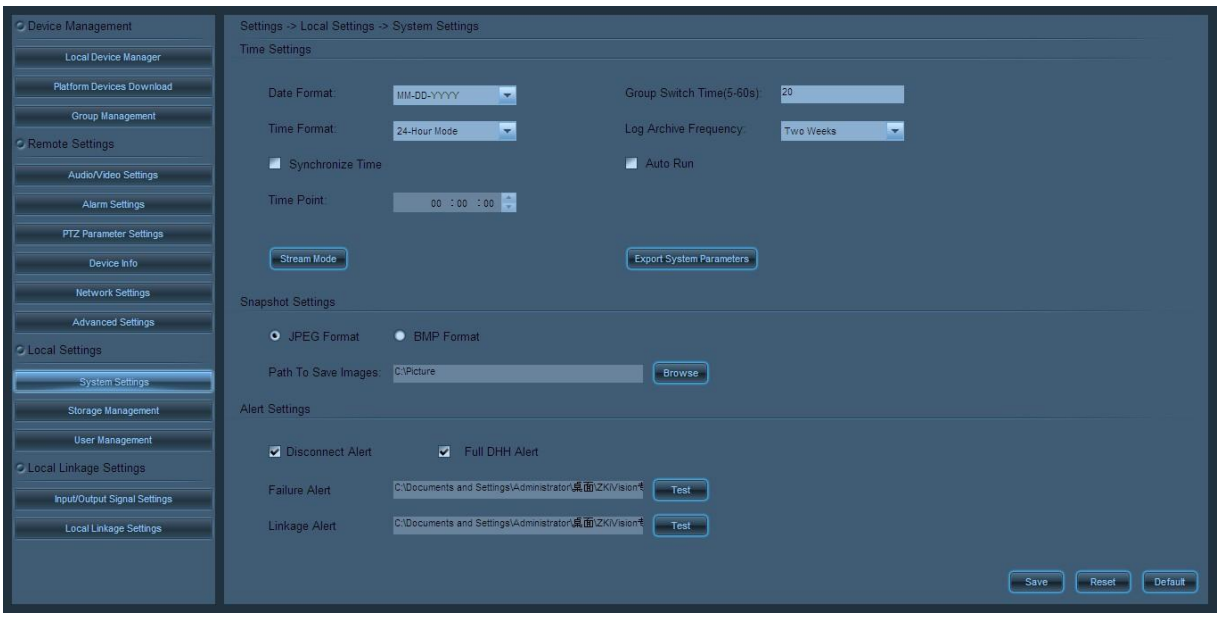
Storage Card Management: Click "Browse Storage Card" to browse the storage card on the device; click "Stop Storage Card" to stop the storage card; click "Format Storage Card by FAT32" to format the storage card.

☺ **Note:** The system supports the storage card up to 32G. Please format the storage card to FAT32. Storage cards made by some manufactures may not be compatible with the device. Please test the storage card before usage.

- **Export System Parameters**

Click the button to export system parameters to the local computer.

4.6.10 System Settings



- **Time Settings**

Date format It includes year-month-day, month-day-month, or day-month-year. The default format is year-month-day.

Time format It includes 12 hours or 24 hours. The default format is 24 hours.

Auto-calibration time Select it to calibrate the time of all connected devices during the given time, that is, synchronize the time of all devices with the PC.

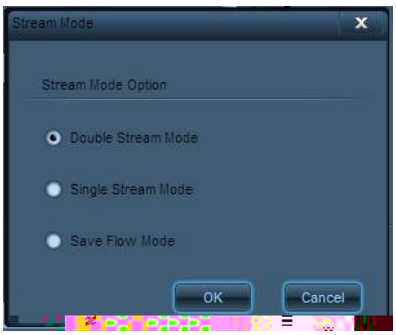
Auto-calibration time Calibrate the time automatically.

Group switch time The time interval of group switching. The group switch time is 20s by default. It can be set from 5s to 60s.

Log storage time The logs can be saved for a week, two weeks, or a month. The default storage time is a week.

Auto run The software automatically starts upon computer startup after this option is selected.

- **Stream Mode**



Double Stream Mode When the preview window displays screens of multiple channels, the watched video, snapshot, and recorded video are sub-stream images. If you double-click one video for magnification, the watched video, snapshot, and recorded video are all main stream images.

Single Stream Mode If sub-stream image is set in the video recording setting, the watched video, snapshot, and recorded video are sub-stream images; if main stream image is set in the video recording setting, the watched video, snapshot, and recorded video are main stream images regardless of whether videos of one or more channels are displayed in the preview window.

Save Flow Mode When the preview window displays screens of multiple channels, the watched video, snapshot, and recorded video are sub-stream images. If you double-click one video for magnification, the watched video, snapshot, and recorded video are all main stream images and they are all in flow saving mode.

Note: If you select **Single Stream Mode**, enter **Setting** > **Local Setting** > **Storage Management** interface to set the stream mode of videos.

- **Export System Parameters**

Click the button to export system parameters to the local computer.

- **Capture Settings**

Image format The formats of system captured pictures include JPEG and BMP. The default format is JPEG.

Image storage path The default storage path of the captured pictures is **C:\Picture**.

- **Alert Settings**

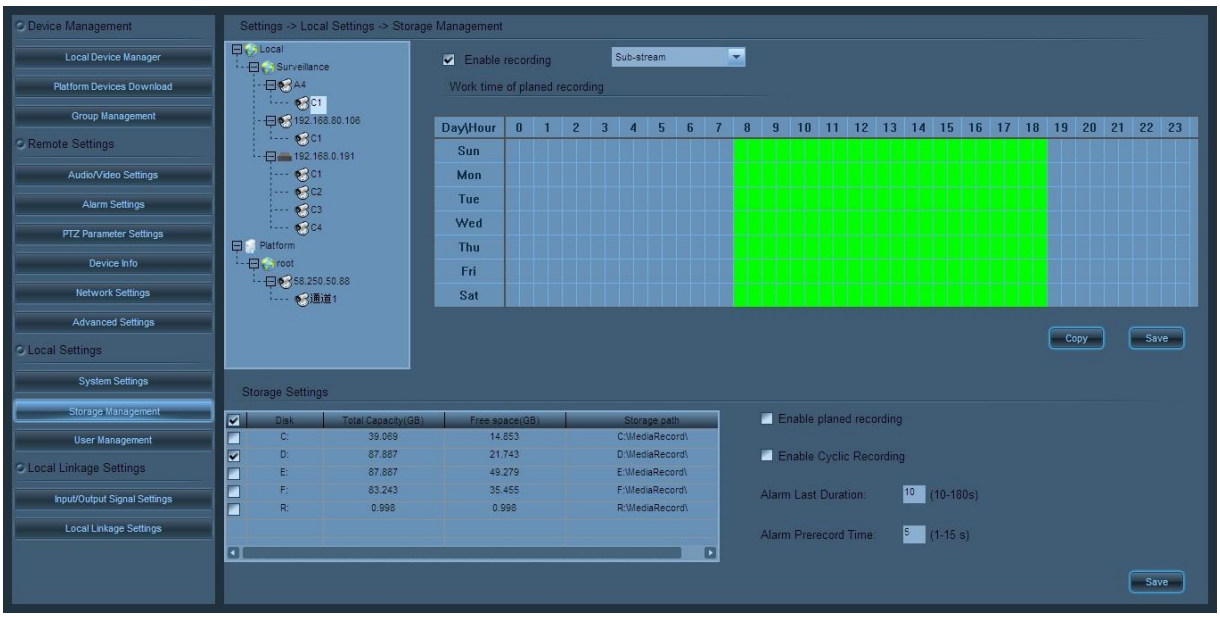
Disconnect Alert Alert is generated when the device is disconnected.

Full HDD Alert Alert is generated when the hard disk is full.

Failure Alert Click **Test** to choose a sound for failure alerts.

Linkage Alert Click **Test** to choose a sound for linkage alerts.

4.6.11 Storage Management



Double-click a camera channel in the device tree and complete the video recording configuration after successful connection.

- **Time management**

Enable recording Set the stream format of recording, such as main-stream or sub-stream.

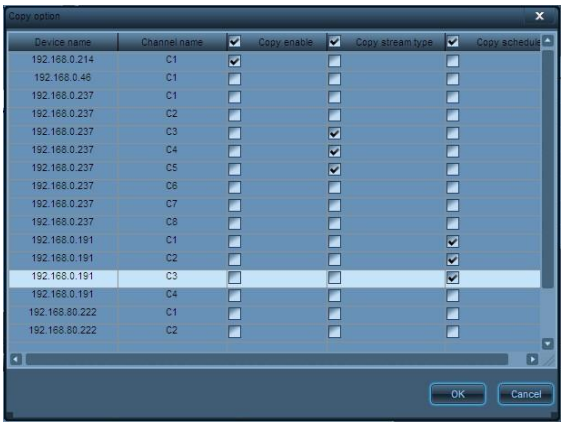
- **Work time of planned recording**

Sunday Saturday Indicates a week (unit: day).

0 23 Indicates one day (unit: half an hour).

Work time of planned recording Click in the plan chart to drag a green area as shown above. The green area indicates the work time of planned recoding opened by the channel.

- **Copy**



Copy enable If this option is selected, the video recording enabling status of the channel is copied.

Copy stream type If this option is selected, the stream type of the channel is copied.

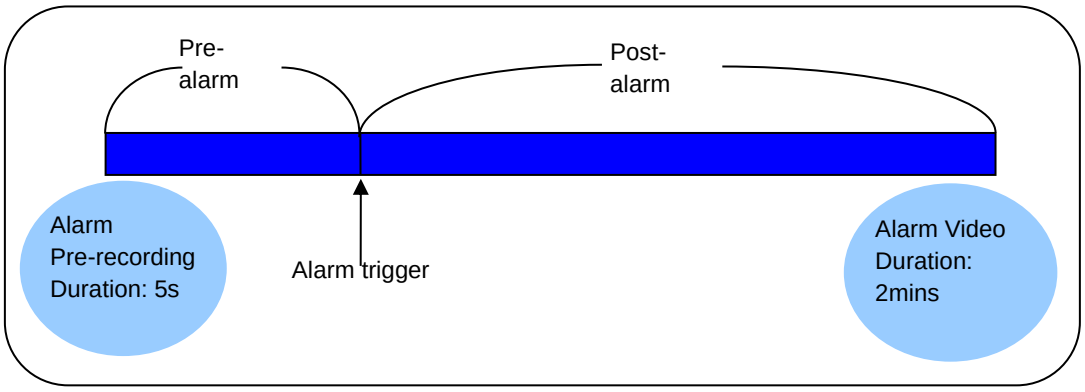
Copy schedule If this option is selected, the planned video recording schedule of the channel is copied.

Enable planned recording If this option is selected, the video recording planned in the schedule in green in the **Time management** area is enabled.

Video storage path After Surveillance client software is installed, it will automatically detect the computer disk and displays the test results in the list. The default storage path is **D:\MediaRecord\.** When the space of the first selected disk is less than 5G, the second selected disk will begin to videotape.

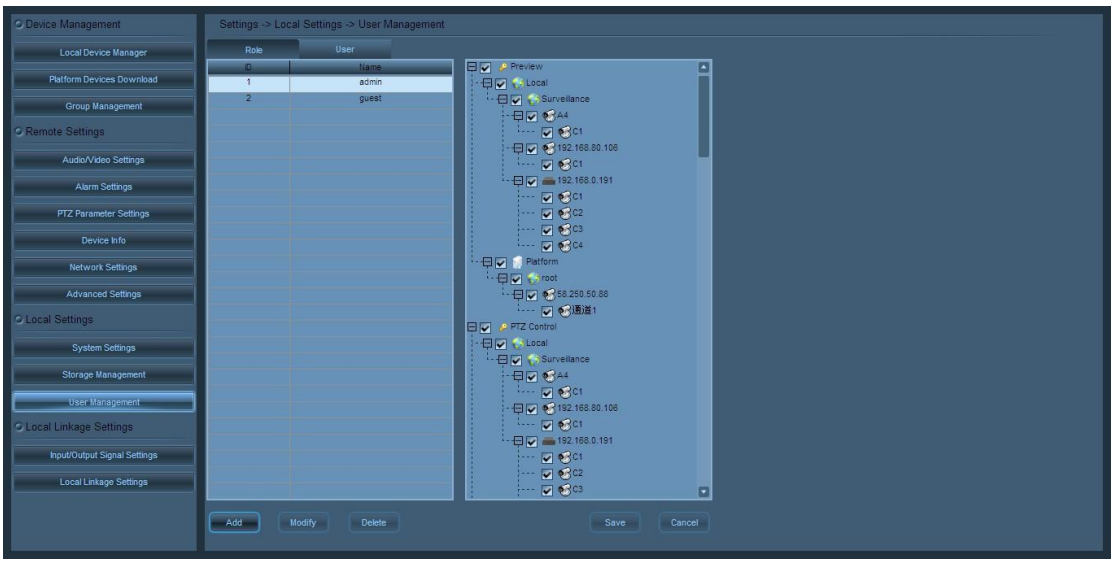
Alarm duration The duration of the alarm videotaping is 5s by default. It can be set from 10s to 180s.

Alarm pre-recording duration The pre-recording duration of the alarm videotaping is 5s by default. It can be set from 1s to 15s.



Video cyclic cover If you select it, the system will automatically overwrite the earliest videotaping when all the configured videotaping disk spaces are less than 5G. If you clear it, the **Disk cleanup** interface will pop out when all the configured videotaping disk spaces are less than 5G. As long as one of the configured videotaping disk spaces is more than 5G, the scheduled videotaping will restart.

4.6.12 User Management



- **Role**

Role	Default Permission
admin	All permissions to perform all settings, which cannot be modified or deleted
guest	No permissions by default, which can be modified as required
custom	Role added by the user, which can be assigned by role

Add: Click the button to add a new role (only admin user or custom user with "User Management" permission can add a new role); assign permissions to the new role in the right permission list and click "Save".

Modify: Click a role in the role list and click the button to modify the role name.

Delete: Click a role in the user list and click the button to delete the role.

- **User**

Name: is the name of user logging in the system.

Role: is the user role, whose permissions can be viewed in the right permission list.

User State: Click "Permit" to allow the user to login the system; click "Forbid" to prohibit the user logging in the system.

Add: Click the button to add a new user.

Modify: Click a user in the user list and click the button to modify the user information.

Delete: Click a user in the user list and click the button to delete the user.

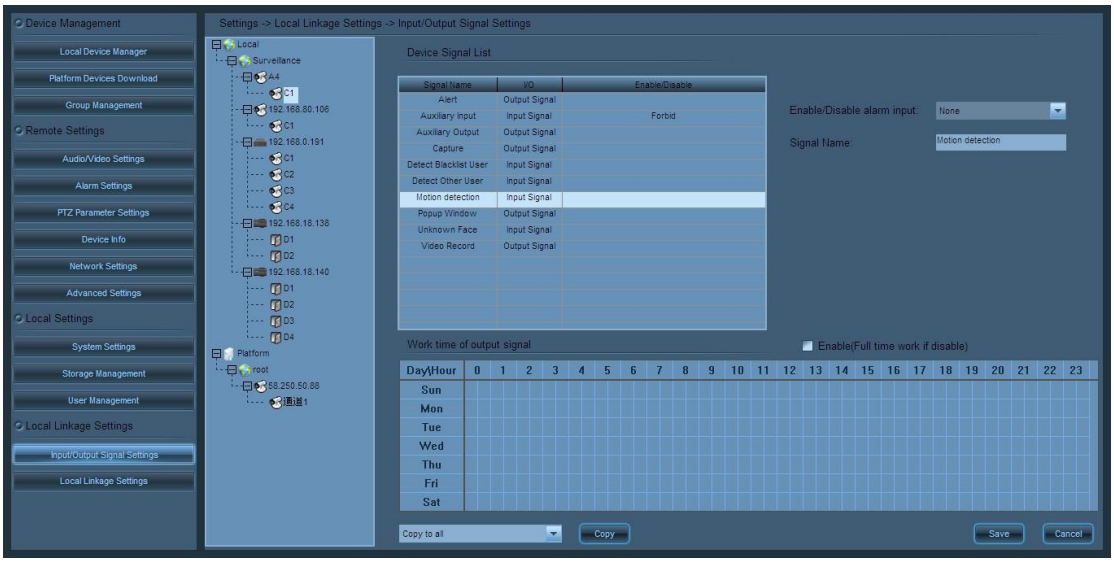
Note:

① The default super user of the system is "admin" and the default password is "123456". The super user cannot be deleted, and its user level cannot be modified.

② A user level can only be modified by the same user.

③ The system login password of an existing user can be modified in the "Lock User/Log off User" interface.

4.6.13 Input / Output Signal Settings



Double-click a camera channel in the device list. Set the input/output signal of the device upon successful connection.

Device Signal List: The system automatically lists all signals of the channel, and click to select a signal.

Enable/Disable alarm input: When there is an external alarm input device, select an auxiliary input signal in the Device Signal List. Select "Enable" to enable the external alarm input; click "Disable" to disable the external alarm input.

Signal Name: Select a signal in the Device Signal List to set the signal name.

Enable: Check the option to enable local alarm linkage during the preset period; uncheck the option to enable local alarm linkage all day long.

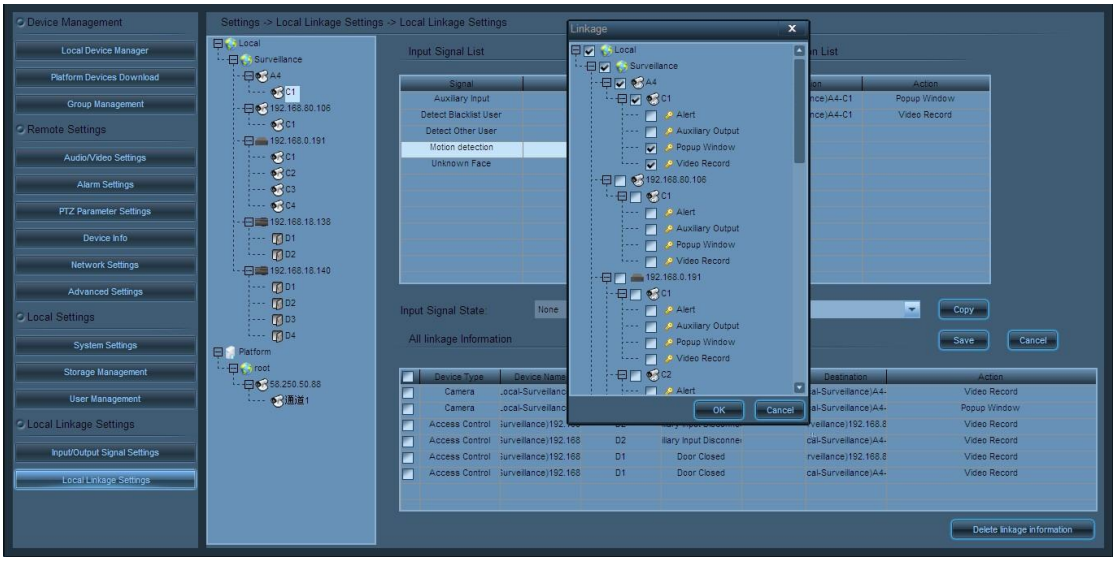
Sun ~ Sat: is a week period with the unit of day.

0 ~ 23: is a day with the unit of half an hour.

Work time of output signal: Click in the plan chart to drag a green area as shown above. The green area indicates the work time of signal alarm linkage.

Copy: If the work time of alarm linkage of Signal B is the same as that of Signal A, set the work time of Signal A and select Signal B in the dropdown list. Then, click Copy and Save. If the work time of alarm linkage of all signals is the same, set the work time of a signal and select "Copy to all". Then, click Copy and Save.

4.6.14 Local Linkage Settings



Double-click a camera channel in the device tree. Modify or set the alarm linkage options of the channel upon successful connection.

Input Signal List: The system automatically lists all input signals of alarm linkage of the channel, and click to select a signal.

Linkage: Click to select an input signal. Click the button to set output actions for flexible and convenient linking: IP camera <--> IP camera, IP camera <-->Access control device, Access control device <-->Access control device.

Linkage Action List: The system automatically lists the alarm linkage actions of the set linked input signal.

Input Signal State: includes "NO" and "NC" for auxiliary input signals. If the alarm input device is a normally open device, select "NO"; if the alarm input device is a normally close device, select "NC". This setting option is not available for other input signals.

Copy Input Signal Alarm Linkage: If the linkage action and linkage time of Alarm B input signal are the same as those of Alarm A input signal, set the options of Alarm A input signal and select Alarm B input signal in the dropdown list. Then, click

and

. If the linkage action and linkage time of all input signals are the same, set the options of an input signal and select "Copy to all input terminals". Then, click

and

. In this way, all input signals of the camera are set with alarm linkage.

All linkage information: The system automatically lists the linkage information of all devices, and click to select the information.

: Select a linkage action in the linkage information list and click the button to delete it.

Note:

① The alarm linkage of all signals can only work if the device (camera) surveillance is enabled in the preview interface. No linkage alarm is generated if the device surveillance is disabled.

② If a new alarm message is generated within the alarm duration, the alarm duration is prolonged.

4.7 Access Function

4.7.1 Personnel

To use the access control function of the system, enter the personnel system: 1. Set the company's organization structure in the department management settings; 2. Register personnel in the system and assign departments in the personnel management settings. Then, maintain and manage the personnel, and perform related access control settings.

4.7.1.1 Department

To manage the company's personnel, describe and manage the company's department organization structure. When you first use the system, the system has a default department with the name of **[Company Name]** and the number of Level **[1]**, which can be modified but not deleted.

The main functions of department management include Add Department and Maintain Department.

1. **Add Department:**

(1) Click [Personnel] – [Department] – [Add] to display the Add Department interface:

Description for each field:

Department Name: contains up to any 50 characters.

Department Number: shall not be the same as other department number, with a length of up to 50 digits.

Parent Department: Select a department in the tree controls as the parent department, or select a department in the dropdown list and click [OK].

(2) After all fields are completed, click [OK] to finish operation or click [Cancel] to cancel operation.

Alternatively, click [Import] to import the department information in other software or materials to the system. See Appendix 1 Common Operations for details. [Parent Department] is an important parameter to determine the company's organization structure. The company's organization structure chart is displayed in the form of department tree on the right side of the interface.

- **Maintain Department:**

The functions of department maintenance include Maintain Department and Cancel Department.

In case of any change in a department or the organization structure, click [Edit] to modify the Department Name, Department Number or the Parent Department. Click the Department Name directly or click the [Edit] button behind the department to enter the Edit interface.

To cancel a department, click the check box before the department and click [Delete], or directly click the [Delete] button behind the department.

✍**Note:** Any department cannot be modified or deleted at will, or the department's personnel will lose their department. Besides, some history materials cannot be queried. If modification or deletion is required, transfer the department's personnel to another department.

4.7.1.2 Personnel

To use the management system, register personnel in the system, or import the personnel information in other software or materials to the system. See Appendix 1 Common Operations for details.

1. Add Personnel

(1) Click [Personnel] – [Personnel] – [Add] to display the Personnel Profile interface:

Description for each field:

Personnel Number: is up to 9 non-repeated digits by default.

Department: Click the dropdown box to double-click relevant department or select relevant department and click [OK].

ID Card Number:

To use these functions, directly click the personnel number in the personnel list to enter the Edit interface, or double-click [Edit]. After editing, click [OK] to save and exit.

1. Personnel Issue Card

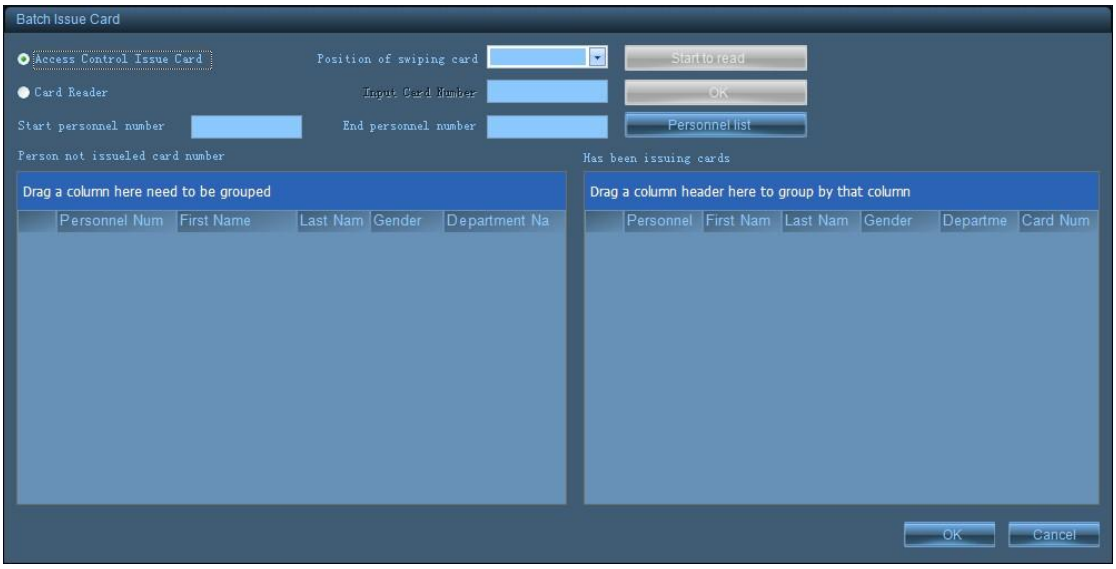
Assign the personnel with card number, including batch issue card and single person issue card.

(1) Instructions of Card Reader:

The card reader is connected with PC through USB interface. Click the card number entry column and swipe the card on the card reader. Then, the card number is automatically displayed in the entry column.

(2) Operating Steps of Batch Issue Card

Click [Personnel] – [Personnel Issue Card] – [Batch Issue Card] to display the Batch Issue Card editing interface:



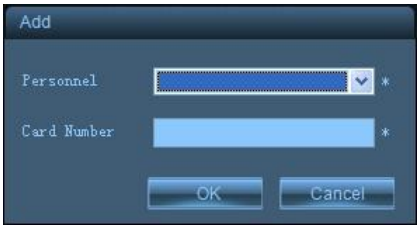
Personnel list: shows all personnel without cards within the personnel number range.

Input Card Number (or **Position of swiping card**): Click OK to assign card numbers to the personnel in the list from the top down, until all personnel are assigned with card numbers.

Click [OK] to finish card issue and return. The personnel and their card numbers are displayed in the list.

(3) Operating Steps of Single Person Issue Card

Click [Personnel] – [Personnel Issue Card] and select [Add], or select a person in the Single Person Issue Card interface and double-click – [Add], to pop up the following dialog box:



Select a person and input the card number. Then, click [OK] to finish.

✍**Note:** The system supports card issue by card reader and manual entry of card number.

- **Personnel Adjustment**

Personnel adjustment refers to daily maintenance of existing personnel, mainly including adjusting department and deleting personnel.

(1) Adjust Department

Click [Personnel] – [Personnel]. Select personnel and click [Adjust Department] to display the editing interface.

Select the adjusted department.

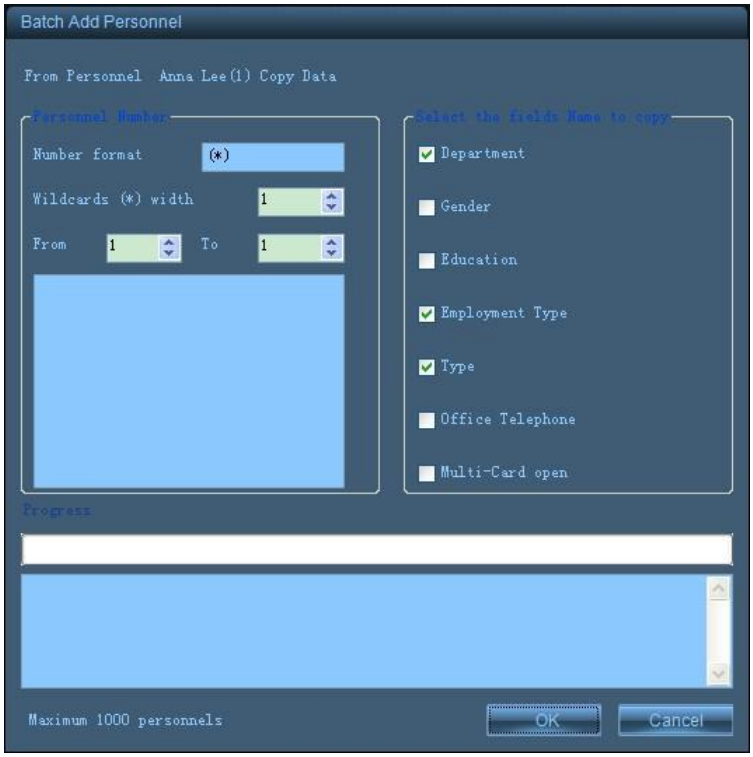
After editing, click [OK] to save and exit.

(2) Delete Personnel

Click [Personnel] – [Personnel]. Select personnel and click [Delete], or double-click to select [Delete] and click [OK] to delete the person.

✍**Note:** The database of the person is deleted at the same time when the person is deleted.

(3) Batch Add Personnel



To batch add personnel, select the personnel to be copied. The Batch Add Personnel function is not available without personnel information. The length of number of personnel to be batch added shall not exceed 8 digits. A maximum of 1000 people are allowed to be added in a batch.

Number format: is the personnel number format and "(*)" refers to wildcards.

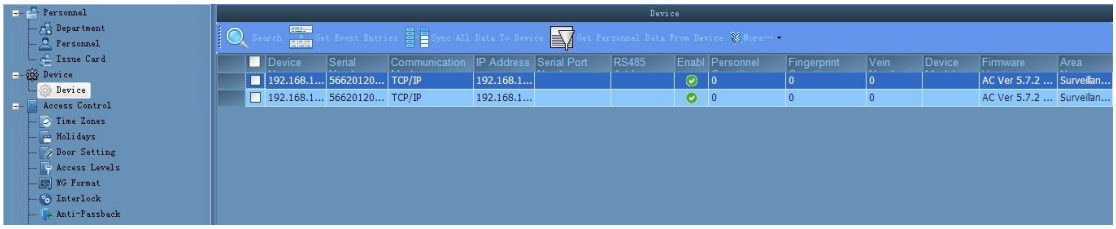
Wildcards (*) width: is the valid width of wildcards, and limits the number of digits in "From" and "To" edit boxes.

Select the fields name to copy: Select the same information of batch added personnel as that of the personnel to be copied.

4.7.2 Device

The system needs to be connected with the access control panel to realize the access control function. To use the function, first install the device and connect it with network. Then, set relevant parameters in the system to manage the device, upload user access control data, download configuration information, enter various reports and realize digital management of a company.

Set communications parameters of the connection equipment. Correct communications parameters ensure normal communications with the device, including system settings and device settings. Upon successful communications, the information of the connected device can be viewed, and remote surveillance, uploading and downloading can be performed.

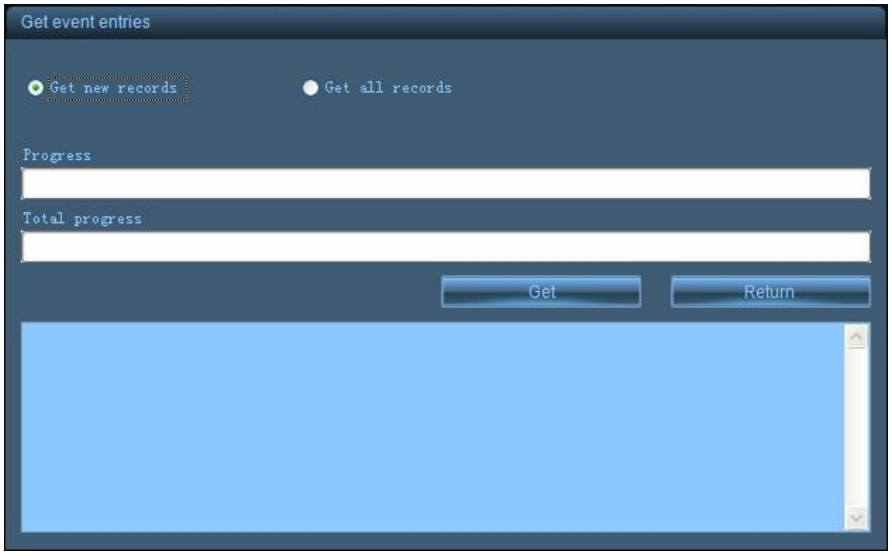


4.7.2.1 Device Maintenance

To realize communications, data uploading and configuration information downloading between the system and the device, set parameters of the device and the system. The user can view access control panels with all permission in the system. To add or delete the device, go to the Device Management interface.

Search: Click [Device] – [Device] – [Search] to pop up the following interface. Enter the device name to search.

Get events entries: Get event records of the device to the system. Three options are available: Get new records, Get all records, and Get records through SD card.



Get new records: The system only gets new event records generated after last got records and record them into the database. Repeated records are not written in.

Get all records: The system gets all event records in the current panel again. Repeated records are not written in.

Get records through SD card: The system reads data in the SD card and gets panel event records. Then, the software saves SD card backup records to the system after analysis.

In the event that the event records in the device are not uploaded to the system in real time as a result of network interruption or communications interruption due to other factors, manually get event records in the device by reading SD card. Alternatively, you can set timed getting.

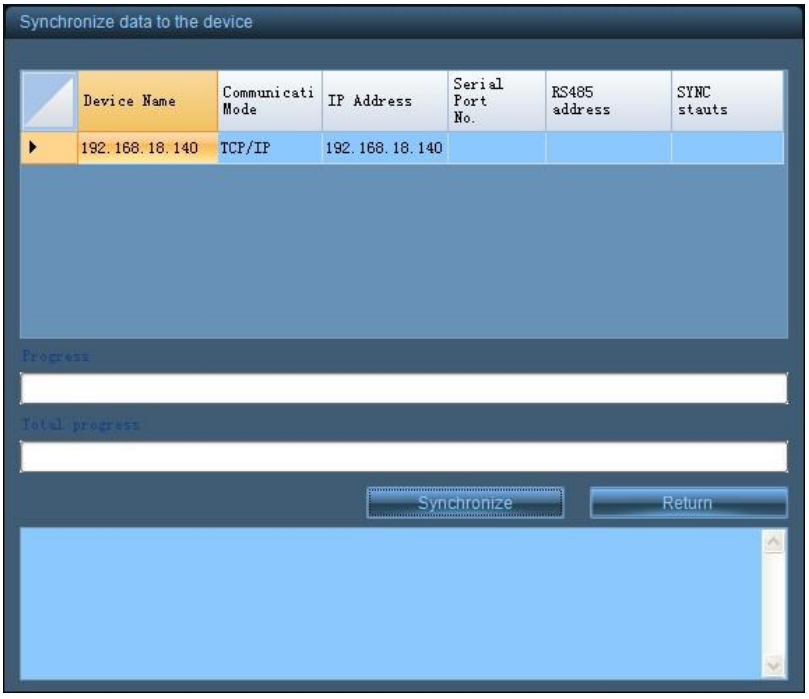
✍**Note:** A maximum of 100,000 event records are stored in the access control panel. The earliest saved records are automatically deleted (10,000 records to be deleted by default) in case of more than 100,000 event records.

Synchronize data to the device: Synchronize new data to the device, such as new personnel and new access control settings. This is called increment synchronization.

See the device adding operation for the definitions of the preceding parameters and related settings. The items in grey are not editable. The device name cannot be same as other device name.

The device type of the access control panel shall not be modified. In case of wrong type, delete the device manually and add a device again.

Get data from device: Save source information from the device to the software, as shown in the figure:



More: includes Modify IP address, Disable auxiliary output, Disable, Enable, Modify Communication password, Synchronize time, Get event records, Upgrade firmware, and Log.

(5) **Disable auxiliary output:** Disable external devices connected with the device auxiliary output interface. Only one device is selected a time for this operation.

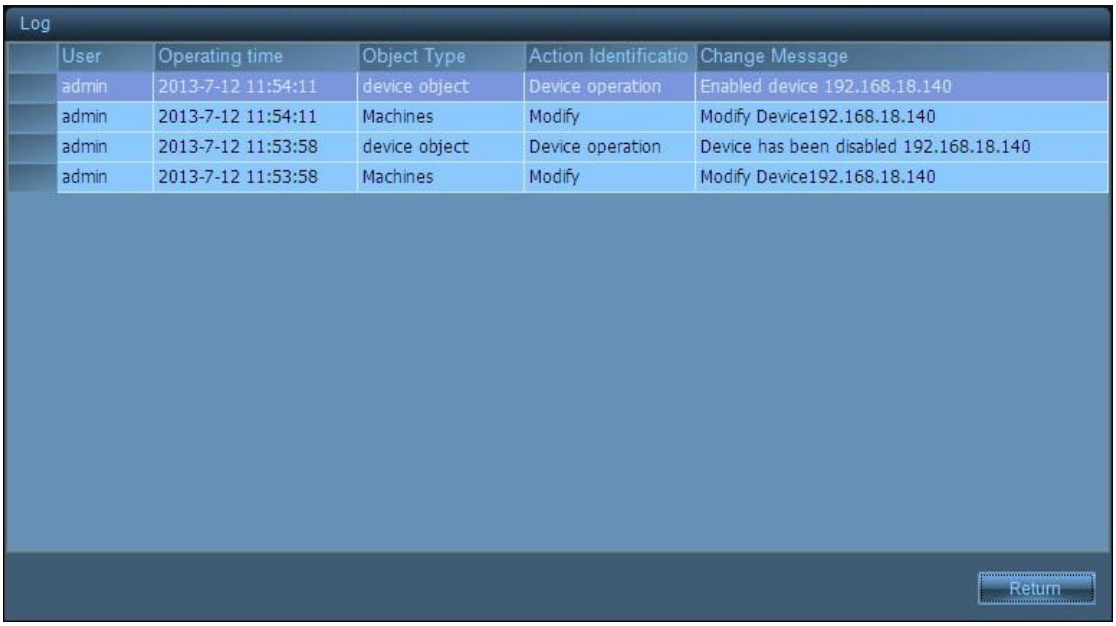
(6) **Modify Communication password:** To modify the communication password, enter old communication password and pass verification. Then, enter a new password twice and click [OK].

✍**Note:** The communication password shall not contain spaces, and combination of numbers and letters is recommended. To set the communication password can improve the device security, and is recommended for each device.

(7) **Get personnel data:** Get the number of current personnel and total fingerprints from the device. The data is displayed in the device list.

(8) **Modify fingerprint match threshold:** The user can modify the fingerprint match threshold in the device. The threshold ranges 35 ~ 70 and is 55 by factory default. When a device is added, the system reads the threshold of the device. Upon successful reading, the user can view the current fingerprint match threshold in the device list. Fingerprint match thresholds of several devices can be batch modified.

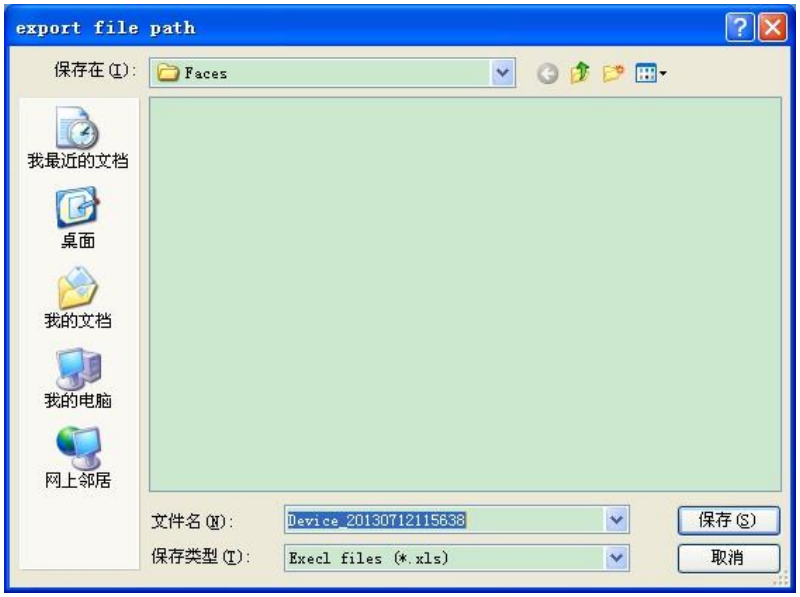
(9) **Log:** records and lists all history operations of the software. There are Log buttons in the Personnel, Department and Personnel Issue Card interfaces. Click the Log button to display relevant records.



(10) **Synchronize data to the device:** Synchronize system data to the device, including door data, access levels (personnel and time zone), anti-passback, interlock, linkage, first-card opening and multi-card opening. Select the device and click [Synchronize data to the device] to synchronize data.

✍**Important:** Before all data is synchronized to the device, all existing data (excluding event records) in the device is deleted and all settings data is synchronized again. You should ensure smooth network connection and avoid outage. In addition, when the device works normally, be careful to perform the operation. You can synchronize data to the device during a period when few people use the device, to not affect normal use.

(11) **Export:** Click [Device] – [Device] – [Export] to pop up the following interface. Click [Save] to export the device data to your computer in EXCEL, PDF or txt. format.



4.7.3 Access Control

1. **System Working Principle:**

   The access control system is a management system based on the C/S architecture, and can consistently manage personnel access by controlling network access control panels with computer.

   The access control system can set access levels of registered users who are allowed to access some doors within a certain time period.

   The system supports several databases (such as Access and SQL Server) and multiple languages. It is designed based on multi-business integration and supports business expansion such as attendance check.

- **System Parameters Description:**

  256 time zones;

256 access levels;

Three types of 96 holidays;

Anti-passback;

Interlock;

Linkage;

First-card normal open;

Multi-card opening;

Remote opening and closing;

Real-time monitoring.

- **Introduction to Operating Functions of Access Control System:**

  Click to enter the [Door Control] system and [Real-Time Monitoring] is displayed on the homepage.

  The access control system management mainly includes: time zones, holidays, door setting, access levels and real-time monitoring.

  ✍**Note:** See the "Terminology" for definitions of parameters of the Section.

4.7.3.1 Time Zones

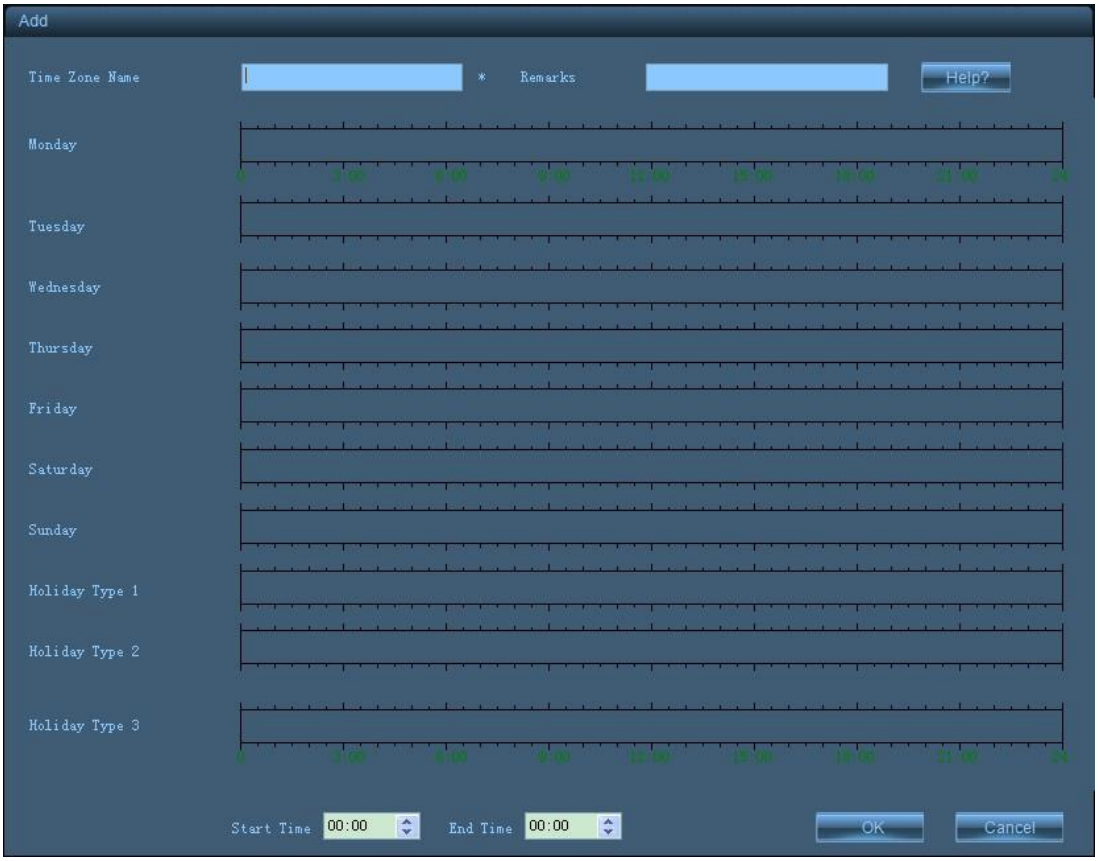
Time zones can be used to set access time. Enable read heads within valid time zones of specified doors and disable read heads within other time zones, or set normally open time zones of doors. Time zones can also be used to set access levels. Specified users can access specified doors within preset time zones (including access levels and first-card normal open settings).

The system controls the access as per preset time zones. The system can define a maximum of 255 time zones. Each time zone can be defined in a week, and each day of three holiday types can have a maximum of three time intervals in valid time within 24 hours. The format of each time interval of time zone is HH:MM – HH:MM as per 24-hour system and accurate to minute.

A default time zone named **[24-hour Pass]** is in the initial system, which can be modified but not deleted. The user can add new time zones which can be modified or deleted.

1. **Add Time Zone:**

   (1) Click [Access Control] – [Time Zones] – [Add] to set possible time zones in the time zone settings interface.



Description for each parameter:

Time Zone Name: contains up to any 50 characters.

✍**Remarks:** contain a maximum of 70 characters, and describe details of the current time zone, including explanations and main application occasions, which facilitate the user or others with the same access level to view the time zone information.

Time Interval and **Start Time and End Time**: A time zone includes three time intervals a day within a week, and three time intervals each of three holidays. Set the start time and end time of each time interval.

Setting Method: If the time zone is normal open, enter 00:00 ~ 23:59 in the time interval, or click to drag the whole time frame; if the time zone is empty by default, it is normal close. Three time intervals are set for a time zone, so use the mouse to drag only three time zones in each time frame.

Holiday Type: Three holiday types in the time zone are irrelevant with any day of a week. If a time zone coincides with a holiday type, the three time intervals of the holiday type shall prevail. The holiday type in the time zone is optional. If the user leaves the holiday type empty, the system gets the default value.

After setting the time zone, click [OK] and save. The time zone is displayed in the list.

- **Maintenance of Time Zone:**

Edit Time Zone: In the time zone list, double-click a time zone or select a time zone and click [Edit] in the menu, to modify the time zone in the time zone editing interface. Click [OK] to save the modified time zone which is displayed in the time zone list.

Delete Time Zone: In the time zone list, select a time zone and click [Delete]. Click [Yes] to delete the time zone; click [No] to cancel. The time zone in use cannot be deleted.

Click the check box before one or several time zones in the time zone list. Click [Delete] at the top of the list. Click [Yes] to delete the selected time zones; click [No] to cancel.

4.7.3.2 Holidays

The access control time of holidays may not be the same as normal. The system supports holiday access control time settings to facilitate operation.

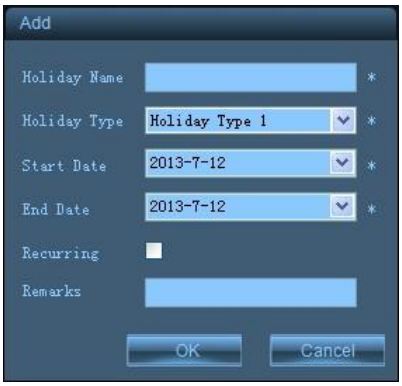
The holiday management includes Add Holiday, Modify Holiday, and Delete Holiday.

1. **Add Holiday:**

   Holidays support three types. Each type contains up to 32 holidays. To set special access levels on some particular dates, use the Holidays function.

   Operating steps:

   (1) Click [Access Control] – [Holidays] – [Add] to enter the Add Holiday editing interface:



   Description for each field:

   Holiday Name: contains up to any 50 characters.

   Holiday Type: includes Holiday Type 1, Holiday Type 2 and Holiday Type 3. A newly added holiday record must be any of the three types. Each type contains up to 32 holidays.

   Start Date and End Date: The start date shall not be later than the end date, or the system prompts error. The year of the start date shall not be smaller than the current year, and the holiday dates shall be within a year.

   Recurring: includes Yes and No. The default is "No". For holidays not to be modified for the next year, such as the New Year's Day dated January 1 of each year, select "Yes". For the Mother's Day dated the second Sunday in each May, select "No" as the date is uncertain.

For example, if the date of "New Year's Day" is set at January 1, 2012 and to be Holiday Type 1, January 1 is not subject to access control by "Friday", but subject to access control by "Holiday Type 1", such as the 8:00 ~ 20:00 access control as indicated in 6.1 Time Zones.

(2) Click [OK] to save and display the added holiday in the holiday list.

- **Modify Holiday:**

  To modify the existing holiday, select the holiday and click [Edit] or double-click the holiday to enter the editing interface. Click [OK] to save and quit.

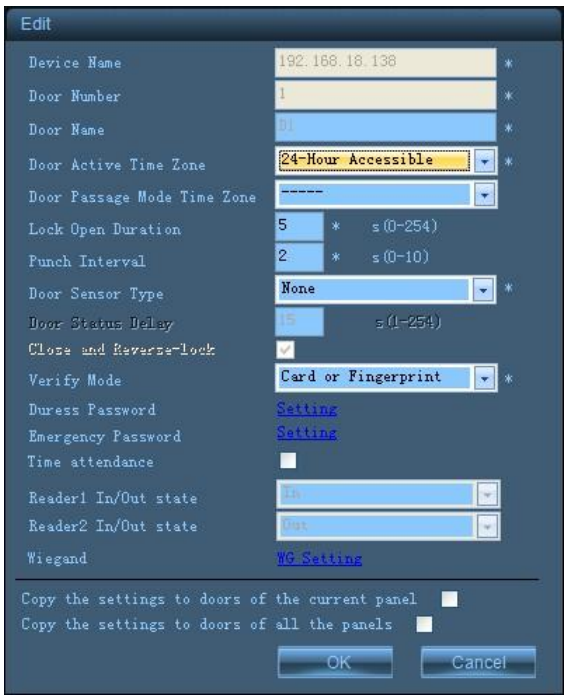
- **Delete Holiday:**

  In the holiday list, select a holiday and click [Delete]. Select [Yes] to delete the holiday; click [No] to cancel. The holiday in use cannot be deleted.

4.7.3.3 Door Setting

Operation steps for modifying 4FEE door parameters:

Enter the [Access Control] – [Door Setting] interface to select the door whose parameters need to be modified, click the [Edit] button in the menu, or double-click the door to be modified. The edit interface is displayed;



Description for each field:

Device Name: is a non-editable item (can be edited and modified in 5.2.1 Modify Network Parameters of a Camera);

Door Number: The system automatically numbers the doors based on the number of doors of the device (for example, the number of each door in a four-door panel is respectively 1, 2, 3, and 4). Each door number in the system is consistent with that of the device.

✍**Note:** By default, the number following the underline in the door name is consistent with the door number. But the 1/2/3/4 in Anti-Passback and Interlock refers to the door number, not the number in the door name. No positive connection between the two, and the system allows the user to modify the door name, so the two cannot be mixed up.

Door Name: is "device name_door number" by default, allowing the user to modify the door name as required, and at most 50 any characters allowed to fill in this field.

Door Active Time Zone and **Door Passage Mode Time Zone:** By default the two fields are null. The lock open duration after the initialization and that added by the user are displayed here for the user to select. In door editing, Door Active Time Zone is a required item. A door can be normally open and closed only if its door active time zone is set up. The door passage mode time zone is effective only if it is included within the door active time zone. It is recommended to include the door passage mode time zone within the door active time zone.

✍**Note:** Swipe the card with access permission to a door for 5 times in succession, the intraday passage mode of the door can be disabled (including the first-card normal open), and the door is closed immediately.

Punch Interval: is measured by second (ranges from 0–10s), 2s by default.

Door Sensor Type: includes None, Normal Open, and Normal Closed. By default this field is None. In door editing, the user can select Normal Open or Normal Closed. If Normal Open or Normal Closed is selected, Door Status Delay and Close and Reverse-lock need to be selected. By default, once the Door Sensor Type is set to Normal Open or Normal Closed, the Door Status Delay is 15s by default, and the Close and Reverse-lock is enabled by default.

Close and Reverse-lock: reverse-locks a door after it is closed. Select this item to reverse-lock a door;

Verify Mode: supports Card Only, Card and Password, Password Only, Card and Fingerprint, and Card or Fingerprint. By default this field is Card or Fingerprint. If Card and Password is selected, please ensure that the door uses a read head with keyboard.

Duress Password and Emergency Password: Use **Duress Password** to open a door under duress (use it cooperatively with a registered card), and the duress password gives an alarm when opening the door. Use **Emergency Password** (also called "super password") to open a door under an emergency. The emergency password opens a door normally, and is effective in any time zone and in any verify mode, usually used by administrator.

In using **Duress Password** to open a door (using it cooperatively with a registered card), if the verify mode is "Card Only", press "ESC" first, then input the set password and click OK, and swipe the registered card. The door is opened and an alarm is generated. If the verify mode is "Card and Password", swipe the registered card first, then input the set password and click OK (the same

with opening a door normally under the mode of Card and Password). The door is opened and an alarm is generated.

In using **Emergency Password** to open a door, the password must be numbers (whole number) that are less than or equal to 8 digits. Input the password to open the door. Each time press "ESC" first, then input the password and click OK to open a door by emergency password.

When the duress password or emergency password is used, the time interval to input each number cannot be longer than 10s. It is recommended that the two passwords be different.

Time Attendance: Select this item to make the punch card record of a door used for attendance checking.

✍**Note:** To perform attendance checking, at least one door must be selected in "Door Setting". If no door is selected, no record will be displayed in the attendance checking software report module.

Copy the settings to doors of the current panel: Select this item to apply the settings to all doors of the current panel;

Copy the settings to doors of all the panels: Select this item to apply the settings to all doors of all the panels within the scope of the current user's permissions;

After editing the parameters, click [OK] to save and exit.

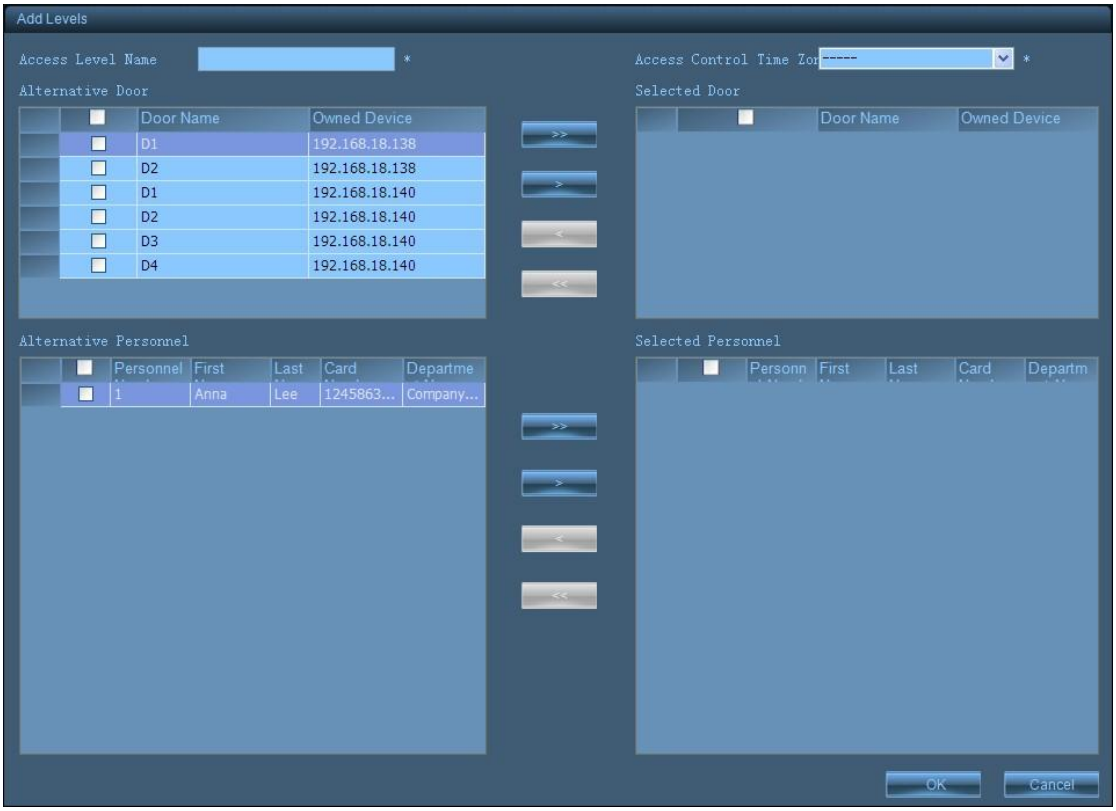
See the "Terminology" in the first page of this user manual for other parameter description.

4.7.3.4 Access Levels

Access levels refer to one selected door or several selected doors that can be opened by verification within certain time zones.

Add Levels:

1. Click [Access Control] – [Access Levels] – [Add Levels] to enter the Add Levels editing interface;



- Set each parameter: the Access Level Name (unrepeatable), Access Control Time Zone, Selected Door, and Selected Personnel;
- Click [OK] to finish the settings and exit. The added access level is displayed in the list.

Note:

(1) Different doors of different panels can be selected and added to an access level;

(2) In adding personnel, if the selected personnel are included in the current access level, the system will not re-add them.

(3) The system does not allow two access levels with the same time zone and selected doors.

Personnel Access Permission Settings: Select the target personnel in the right column, click "<<" to remove the personnel from this access level.

4.7.3.5 Interlock

Interlock can be implemented among two (multiple) doors of a panel. When one door is open, the other doors are closed. When a door needs to be opened, other corresponding doors must be closed; otherwise the door cannot be opened.

Before the interlock, please ensure that the door sensors are connected according to the panel *Installation Guide*, and set the door sensor type to Normal Open or Normal Closed in Door Setting.

Operation steps for adding interlock:

1. Click [Access Control] – [Interlock] – [Add] to enter the interlock Add edit interface;
2. Select a device to display its interlock rule. Because one device corresponds to only one interlock rule, the devices that are already interlocked cannot be viewed in the drop-down list of Device during adding interlock. Delete the set interlock, and the corresponding device will return to the drop-down list of Device. The settings interface is different based on the number of doors of the selected device:

   One-door panel cannot implement interlock;

   Two-door panel can implement 1-2 two-door interlock;

   Four-door panel can implement 1-2 two-door interlock, 3-4 two-door interlock, 1-2-3 three-door interlock, and 1-2-3-4 four-door interlock;

- Select one item in the drop-down list of Interlock Rule (the interlock rules with different doors can be multi-selected). Click [OK] to finish the settings. The added interlock is displayed in the list.

For example, if 1-2-3-4 four-door interlock is selected, Door 3 can be opened only if Doors 1, 2, and 4 are closed.

Note: In the editing, only the interlock rule can be modified, and the device cannot be changed. If a device needs to disable its interlock function, delete its corresponding interlock rule. In deleting a device record, its interlock record will be deleted together.

4.7.3.6 Anti-Passback

Anti-Passback supports entrance and exit anti-passback. In some special circumstances, the personnel using an access card have to exit through the same door where they swipe the card to come in. The card swiping record must be strict corresponding in pairs of entrance and exit. If you come in by following someone without swiping the card, you cannot go out by swiping the card. Similarly, if you go out by following someone without swiping the card, you cannot come in by swiping the card. Or if you give the card to someone else after you swipe the card and come in, he/she cannot come in with your card. If you swipe the card but do not come in, you cannot come in by swiping the card a second time. The same rule applies to going out. The user can enable this function in settings. This function usually applies to prisons, armed forces, national defense, scientific research sites, and vaults in banks and so on.

Operation steps for adding anti-passback:

1. Click [Access Control] – [Anti-Passback] – [Add] to enter the anti-passback Add edit interface;

2. Select the target device (N-door panel). Because one device corresponds to only one anti-passback record, the devices that are already set with anti-passback function cannot be viewed in the drop-down list of Device during the anti-passback adding. If a set anti-passback record is deleted, the corresponding device will return to the drop-down list of Device. The settings are different if the number of doors controlled by the panel is different.

   Anti-passback can be set for read heads and doors by the panels. If a cardholder comes in through Door A, he/she must go out through Door B. This function mainly applies to passage control and entrance ticket control.

Anti-passback for one-door panel and that for read heads;

Anti-passback for two-door panel:

Anti-passback for the read heads of Door-1, anti-passback for the read heads of Door-2, and anti-passback for Door-1 and Door-2;

Anti-passback for four-door panel:

Anti-passback for Door-1 and Door-2, anti-passback for Door-3 and Door-4, anti-passback for Door-1/Door-2 and Door-3/Door-4, anti-passback for Door-1 and Door-2/Door-3, anti-passback for Door-1 and Door-2/Door-3/Door-4, anti-passback for the read heads of Door-1, anti-passback for the read heads of Door-2, anti-passback for the read heads of Door-3, and anti-passback for the read heads of Door-4;

✍**Note:** The read heads above include the Wiegand read heads and inBIO read heads connected to access control panels. The Wiegand read heads of one-door panel and two-door panel are divided into entrance read heads and exit read heads, and the read heads of four-door panel are all entrance read heads. Among the inBIO read heads, the read heads 1 and 2 (RS485 address (or device number) is 1 and 2, the same below) correspond to Door 1, the read heads 3 and 4 correspond to Door 2, the read heads 5 and 6 correspond to Door 3, and the read heads 7 and 8 correspond to Door 4. In anti-passback settings for the doors or the read heads, whether the read head is Wiegand read head or inBIO read head does not matter. Set the anti-passback as required by determining it is entrance or exit status (the current read head is entrance read head or exit read head).If the number of a Wiegand read head or the RS485 address is odd number, it is an entrance read head; if an even number, an exit read head.

- Select one rule in the drop-down list of Anti-Passback (the anti-passback with different doors or read heads can be multi-selected). Click [OK] to finish the settings. The added anti-passback is displayed in the list.

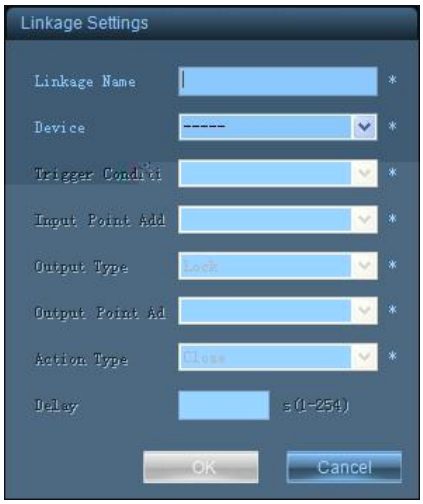
  ✍**Note:** In the editing, only the anti-passback can be modified, and the device cannot be changed. If a device needs to disable its anti-passback function, delete its corresponding anti-passback record. In deleting a device record, its anti-passback record will be deleted together.

4.7.3.7 Linkage

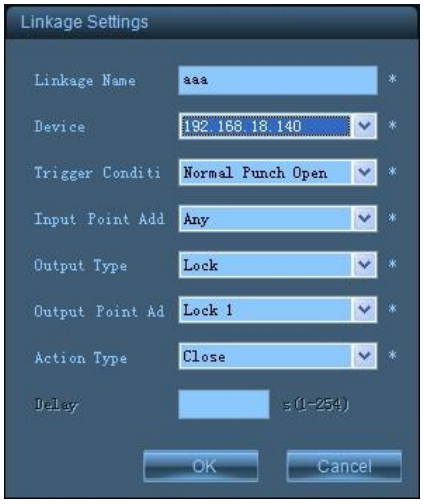
Linkage refers to a linkage action generated at an appointed output point after a specific event happening at an input point in the access control system. Linkage actions control the verification, door opening, alarm generating, and abnormalities in the system. The actions can be viewed in the monitored event list.

Operation steps for adding linkage:

1. Click [Access Control] – [Linkage] – [Add] to enter into the Linkage Settings interface;



- Input the linkage name (a device can be selected only if the linkage name is input), and select a device. The Linkage Settings interface is displayed. (The system prejudges if the device is connected and reads the device extended parameters, such as the auxiliary input number, auxiliary output number, number of doors, and number of read heads. If no device extended parameters are available, the user will be prompted that the linkage failed. Otherwise, the items for linkage settings will be displayed based on the number of doors, auxiliary input number, and auxiliary output number of the selected device.)



Description for each field:

Trigger Condition: Please refer to the *Description for Real-Time Events*, among which except for the linkage-trigger events, alarm cancelation, auxiliary output enabling, auxiliary output disabling, and device starting, the others can all be trigger conditions.

Input Point Add: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary input 1, Auxiliary input 2, Auxiliary input 3, Auxiliary input 4, Auxiliary input 9, Auxiliary input 10, Auxiliary input 11, and Auxiliary input 12. (Please refer to the specific device parameters of a device for its specific input point addresses);

Output Point Add: Door lock 1, Door lock 2, Door lock 3, Door lock 4, Auxiliary output 1, Auxiliary output 2, Auxiliary output 3, Auxiliary output 4, Auxiliary output 6, Auxiliary output 8, Auxiliary output 9, and Auxiliary output 10; (please refer to the specific device parameters of a device for its specific input point addresses);

Action Type: Close, Open, Normal Open. By default this field is Close. If Open is selected, the Delay field needs to be set. Or select Normal Closed.

Delay: ranges from 1-254s (effective only when the action type is Open);

- After editing, click [OK] to save and exit. The added linkage is displayed in the linkage list.

For example, if "Open a door by card" is selected as the trigger condition, the input point: Door 1, the output point: Door lock 1, the action type: Open, and the Delay range: 60s, then when you "open the door by swiping a card", a linkage action "Open" will be generated at Door lock 1, and the door will be open for 60s.

✍**Note:** In the editing, only the linkage name and configuration items can be modified, and the device cannot be changed. In deleting a device, its linkage record will be deleted together.

If the system appoints a specific door as the input point for a device under certain trigger condition or sets up the auxiliary input point for the device, it does not allow to add (or edit) a linkage with the same trigger condition, with its input point set to "Any", and for the same device.

Otherwise, if the device and trigger condition are the same, and in the system exists a linkage with the input point "Any", the system does not allow to add (or edit) a linkage with its input point being a specific door or an auxiliary input point.

In addition, the system does not allow a device to have a linkage with the same input point and output point under specific trigger conditions.

One device allows multiple times of logical (as stated above) linkage settings.

4.7.3.8 First-Card Normal Open

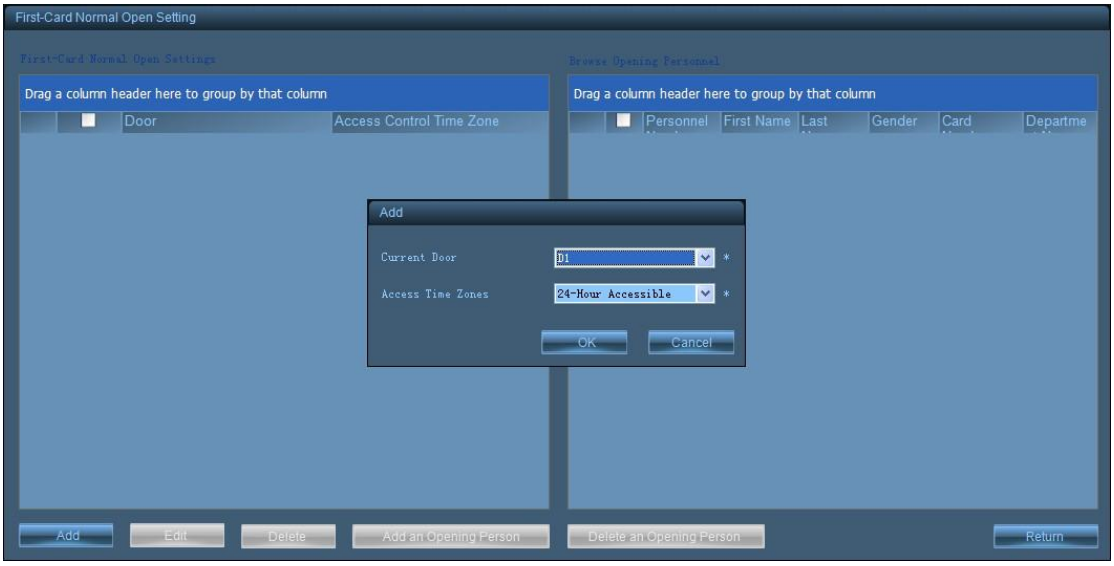
First-Card Normal Open: In certain access time zone, after the personnel with the First-Card Normal Open permission open a door by swiping a card, the door will be normally open and automatically close at the end of the effective access time zone.

The user can perform the First-Card Normal Open settings for a specific door. The settings determine the door, the access time zone for door opening, and the personnel with the First-Card

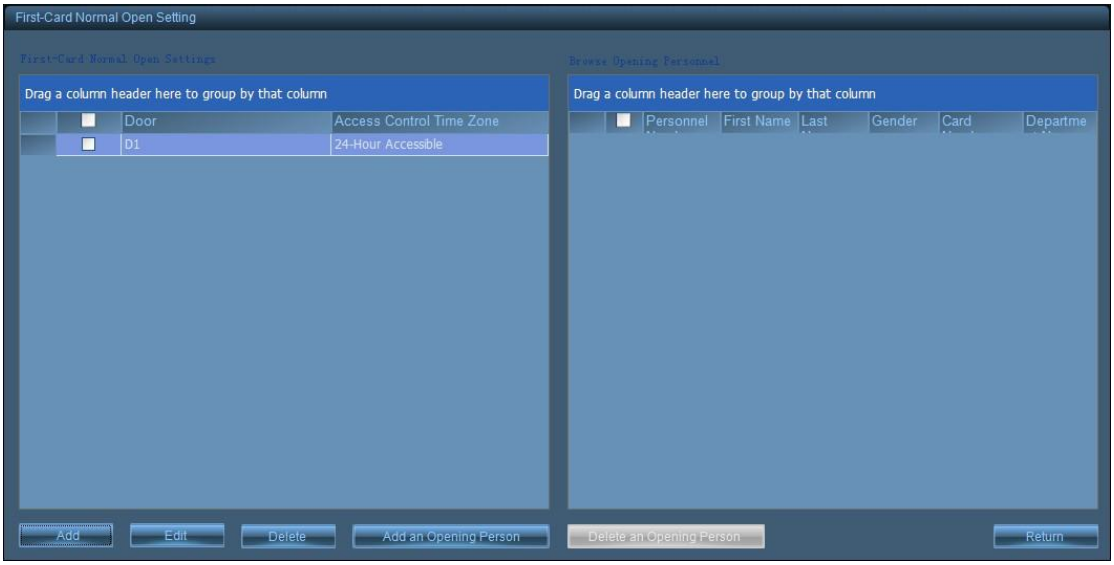
Normal Open permission. The First-Card Normal Open settings in several access time zones can be performed for a door. The interface of each door displays the existing number of First-Card Normal Open settings. In the First-Card Normal Open settings for a door, the "Current Door" does not need to be modified in adding or editing. You only need to select the access time zones. After successfully adding the access time zones, add the personnel with First-Card Normal Open permission. You can view the personnel with the First-Card Normal Open permission and delete them on the right side of the interface to revoke their First-Card Normal Open permission.

Operation steps for adding First-Card Normal Open:

1. Click [Access Control] – [First-Card Normal Open] to enter the First-Card Normal Open Setting interface;
2. Click [Settings] – [Add], select the Access Time Zones for First-Card Normal Open, and click [OK] to save and exit;



- Select the door for First-Card Normal Open, click [Add an Opening Person] to set personnel with First-Card Normal Open permission. The personnel must have access permission to perform First-Card Normal Open. Click [OK] to save and exit.



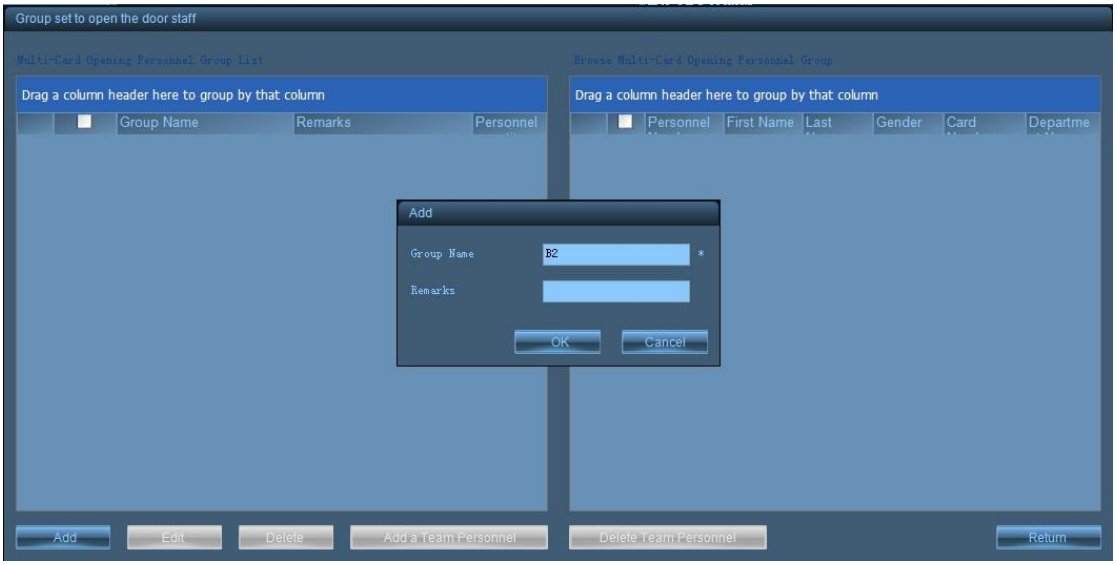
✍**Note:** Swipe the card with access permission to a door under Normal Open status for 5 times in succession (the time interval among each card swiping cannot exceed 5s), the Normal Open status is disabled and the door is closed. After the fifth card swiping, the door can be opened by normal card swiping. This function must be performed within the effective access time zones, and performing it disables all other First-Card Normal Open settings and all other access time zones with First-Card Normal Open settings.

4.7.3.9 Multi-Card Opening

1. Multi-Card Opening Personnel Group:

The function of Group set to open the door staff groups the staff. The groups are used for Multi-Card Opening combination settings.

(1) Click [Access Control] – [Multi-Card Opening] – [Multi-Card Opening Personnel Group] – [Add] to enter the Multi-Card Opening Personnel Group editing interface;



Group Name: can be any characters, allowing at most 50 any characters, and not allowing repeating the existing group names;

After editing, click [OK]. The added multi-card opening personnel group is displayed in the list.

(2) Select a group, and click [Add a Team Personnel] to add this group;

(3) After adding the personnel, click [OK] to save and return.

✍**Note:** One person belongs to only one group, and cannot be assigned to several groups.

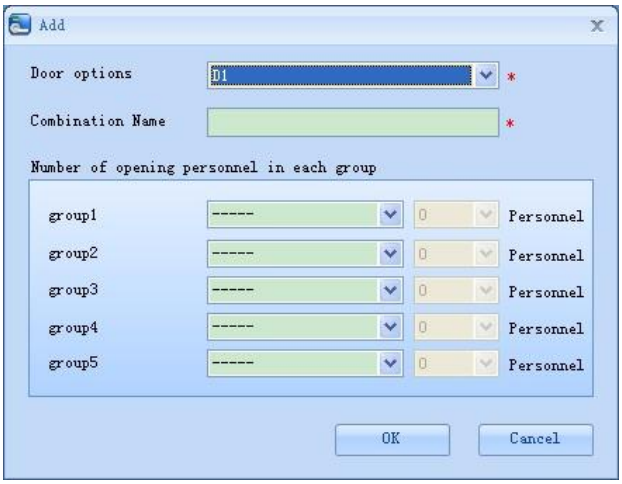
- **Multi-Card Opening:** sets permission for the personnel in [Multi-Card Opening Personnel Group].

  Under some specific access control circumstances this function needs to be enabled. It demands the appointed personnel in a multi-card opening combination to be present. Each one of them swipes their cards in proper order to pass the verification. Before passing the verification, other cards cannot be inserted (even if it is a valid card of other combinations for the same door); otherwise a second time of verification can be done after 10s. Only one person cannot open the door by swiping his/her card.

  Multi-Card Opening combination refers to the combination comprising one or several multi-card opening personnel groups and the personnel in the groups. In determining the number of opening personnel in each group, one (for example, 2 persons in one group open a door simultaneously) or several groups (for example, each group has 2 persons, and the 4 persons of two groups open a door simultaneously) can be set. At least the number of opening personnel in one group cannot be 0, and the total number of all opening personnel cannot exceed 5.In addition, if the number of opening personnel input by the user exceeds that of the current groups, the Multi-Card Opening function cannot be performed.

  Operation steps for adding multi-card opening:

  (1) Click [Access Control] – [Multi-Card Opening] – [Add] to enter the multi-card opening Add interface;



(2) The maximum number of opening personnel for simultaneous multi-card opening is 5. The number in the brackets is the current actual number of opening personnel in each group. Set the number of opening personnel in a group for simultaneously opening a door, and click [OK] to finish the settings.

4.7.3.10 Real-Time Monitoring

The status of doors of access control panels in the system and real-time events are monitored, including normal events and abnormal events (including alarm events) and so on.

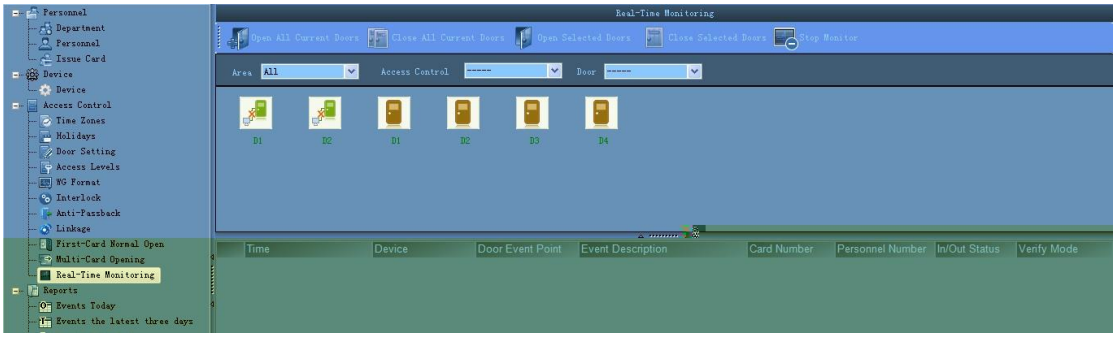
Monitoring All: By default the home page of the Real-Time Monitoring interface displays all doors of the panels within the user's permission scope. The user can monitor one (or several) door by setting the [Area], [Access Control], or [Door].

Remote Opening/Closing a Door: controls one door or all doors. To control a single door, place the cursor onto the icon of the door, and click [Remote Opening/Closing a Door] in the pop-up dialog box. To control all doors, click [Open/Close All Current Doors].

In remote opening a door, the user can define the duration of a door being open in the pop-up dialog box. The default duration is 15s. You can select [Enable the Intraday Door Passage Mode Time Zone] to enable the intraday door passage mode time zones set by the system. You can also set the door status to Normal Open, so the door is not limited by any time zones (open for 24 hours).

To close a door, select [Disable the Intraday Door Passage Mode Time Zone] first to avoid enabling other normal open time zones to open the door, and then select [Remote Closing a Door].

✍**Note:** If the remote opening or closing a door always fails, please view the Device list to check if many devices are disconnected. If any, please check the network; otherwise the operation cannot be performed.



Place the cursor onto the icon of a door, the relevant parameters of the door will be shown, including the Owned Device, Door Number, and Door Name, and three operations for a single door, including remote opening a Door, remote closing a door, and alarm cancelation. The state indicated by each icon is as follows:

Icon							
State	Door alarm	Door closed under the on-line state	Door opened under the on-line state	No door sensor	Device forbidden	Door under the off-line state	Door opened over time

Personnel Photo Display:

If the real-time monitoring involves personnel and the personnel set up their photos, their photos will be displayed in the monitoring. The event name, time, and the names of personnel are shown in the photos.

Event Monitoring:

The system automatically acquires the monitored device event records, including normal door events and abnormal door events (including alarm events). The alarm events are marked in red, the door abnormal events except for the alarm events are marked in orange, and normal door events are marked in green.

The latest record of the currently monitored events is at the top. You can view the latest monitoring record without dragging the scroll bar. The maximum records simultaneously displayed in the interface are about 100.

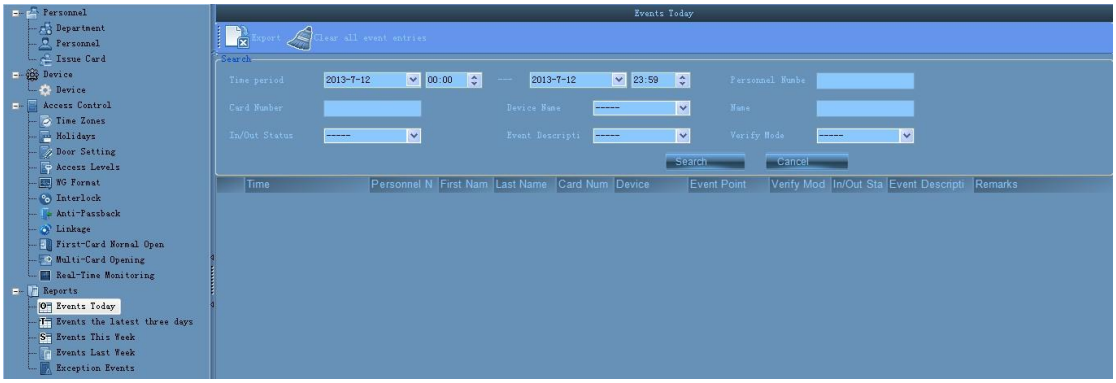
4.7.4 Reports

Include [Events Today], [Events the Latest Three Days], [Events This Week], [Events Last Week], and [Exception Events] reports. You can select Export All or Export after Query. A can perform statistical analysis based on the reports, including card verification, door operation, and normal card swiping.

✍**Note:** Only the event record generated when the user uses Emergency Password to open a door contains the verify mode [Password Only].

4.7.4.1 Events Today

Click [Report] – [Events Today] to enter the following interface. The record of the intraday door events is displayed.



4.7.4.2 Events the Latest Three Days

Click [Report] – [Events the Latest Three Days] to display the record of the door events of the latest three days.

4.7.4.3 Events This Week

Click [Report] – [Events This Week] to display the record of the door events of the nearest week.

4.7.4.4 Events Last Week

Click [Report] – [Events Last Week] to display the record of the door events of the last week.

4.7.4.5 Exception Events

Exception events under specified requirements can be viewed.

Clear All Exception Event Entries: clears all the exception event lists.

Door Status Real-Time Monitoring: displays not only the e-map, but also the event monitoring (consistent with the door status monitoring data, including alarm sound and so on).

Door Operation: Place the cursor onto a door icon and the system automatically filters and displays the operation type based on the door status. The user can perform remote opening/closing a door, and alarm cancelation and so on.

Annex: *Description for Real-Time Events*

1. 1. Normal Events

Normally open a door by card: refers to normal events triggered by the personnel with opening permission using a card and passing the verification under the "Card Only" verify mode.

Normally open a door by fingerprint: refers to the normal event triggered by the personnel with opening permission using his/her fingerprint and passing the verification under the "Fingerprint Only" or the "Card or Fingerprint" verify mode. **Open a door by card and fingerprint:** refers to the normal event triggered by the personnel with opening permission using a card and his/her fingerprint and passing the verification under the "Card and Fingerprint" verify mode.

Open a door by button switch: refers to the normal event triggered by pressing the button switch to open a door in effective time zones.

Swipe a card in door passage mode time zone: refers to the normal event triggered by swiping a card to a door when the personnel with opening permission have already opened the door by remote normal open operation in the door passage mode time zone and the door is being open.

First-card normal open card swiping: refers to the normal event triggered by the personnel with the First-Card Normal Open permission swiping a card and passing the verification in the first-card normal open time zone when the door is closed and under the "Card Only" verify mode.

Door passage mode time zone ended: When the set door passage mode time zone is over, the door will be closed automatically. The door passage mode time zone includes the door passage mode time zone of a door and the time zone with the First-Card Normal Open settings.

Remote normal open: refers to the normal event triggered when a door is opened by remote opening and is set to normal open.

Disable the intraday door passage mode time zone: refers to the normal event triggered by swiping a valid card (must be the same user's card) for 5 times in succession on a read head or using the [Disable the Intraday Door Passage Mode Time Zone] operation in remote closing a door when a door is under the normal open status.

Enable the intraday door passage mode time zone: refers to the normal event triggered by swiping a valid card (must be the same user's card) for 5 times in succession on a read head or using the [Enable the Intraday Door Passage Mode Time Zone] operation in remote opening a door when the intraday door passage mode time zone of a door is disabled.

Open a door by multi-card opening: refers to the normal event triggered when the last card passing the verification in multi-card opening under the "Card Only" verify mode.

Open a door by emergency password: refers to the normal event triggered by using the emergency password (also called "super password") of a door to open it and passing the verification.

Open a door in door passage mode time zone: refers to the normal event triggered when a door is automatically opened at the set time if it is set with door passage mode time zone.

Event to trigger linkage: refers to the normal event triggered when a set linkage in the system becomes effective.

Alarm cancelation: refers to the normal event triggered when the user successfully cancels the alarm operation of a door.

Remote opening a door: refers to the normal event triggered when the user successfully opens a door remotely.

Remote closing a door: refers to the normal event triggered when the user successfully closes a door remotely.

Enable auxiliary output: refers to the normal event triggered when a linkage becomes effective, of which the output point address is set to an auxiliary output point and the action type is set to Open.

Disable auxiliary output: refers to the normal event triggered when a linkage becomes effective, of which the output point address is set to an auxiliary output point and the action type is set to Open. In addition, the normal event will also be triggered if the user uses [Door Setting] – [Disable the Auxiliary Output] to disable an enabled auxiliary output point.

Door opened: refers to the normal event triggered when the door sensor senses the door being opened normally.

Door closed: refers to the normal event triggered when the door sensor senses the door being closed normally.

Auxiliary input point disconnected: refers to the normal event triggered when an auxiliary input point is disconnected.

Short circuit of auxiliary input point: refers to the normal event triggered when short circuit of an auxiliary input point happens.

Start a device: refers to the normal event triggered when a device is started. This event is not displayed in the real-time monitoring and can be viewed in the event log of the Record.

- **Abnormal Events**

Too short card swiping interval: refers to the abnormal event triggered when the interval between two times of card swiping is shorter than the set interval of the door.

Door non-active time zone (card): refers to the abnormal event triggered by swiping a card with opening permission to the current door in its non-active time zone under the "Card Only".

Door non-active time zone (button switch): refers to the abnormal event triggered by pressing the button switch to open a door in its non-active time zone, by which the door cannot be opened.

Invalid time zone: refers to the abnormal event triggered by swiping a card with opening permission to a door in the time zone beyond those set with access control of the door.

Illegal access: refers to the abnormal event triggered by swiping a registered card to a door that does not set with access control.

Anti-passback: refers to the abnormal event triggered when an anti-passback set in the system becomes effective.

Interlock: refers to the abnormal event triggered when an interlock set in the system becomes effective.

Multi-card verification: refers to the abnormal event triggered by the verification of the cards (regardless of passing or not) except for the last card in multi-card opening.

Card unregistered: refers to the abnormal event triggered by a card number unregistered in the system.

Door opened over time: refers to the abnormal event triggered when a door is detected being open by the door sensor and its opening duration is over time.

Overdue card: refers to the abnormal event triggered when the personnel who set the access control period swipe a card and cannot pass the verification beyond the access control period.

Wrong password: refers to the abnormal event triggered by wrong password in opening a door by the Card and Password verify mode, or the duress password or the emergency password.

Unable to close a door in its door passage mode time zone: refers to the abnormal event triggered when a door in the normal open status cannot be closed by the [Remote Closing a Door] operation in the remote closing a door.

4.8 Face Function

On this page, you can register face users and set face identification parameters.

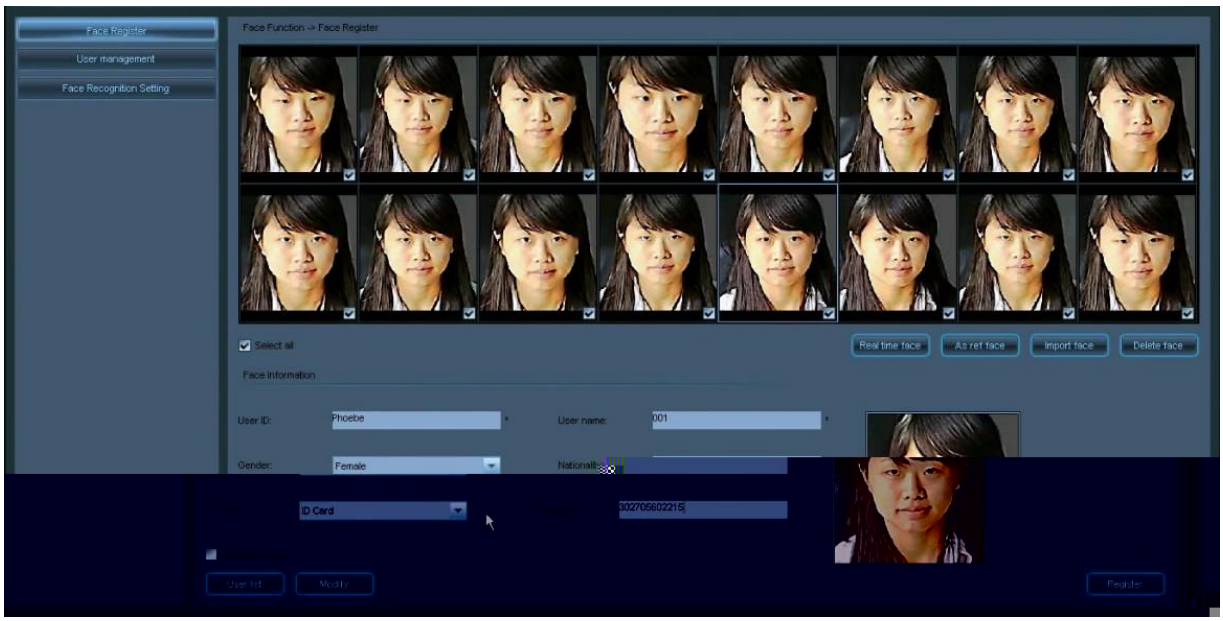
- **Description of the icon functions in the Face Function working area**

Icon	Function Description
Add	Add face user
Modify	Save modified information
Delete	Delete the ticked users
Default	Restore parameters to the default values.
Save	Save modified parameters
Cancel	Cancel the modification

Notes:

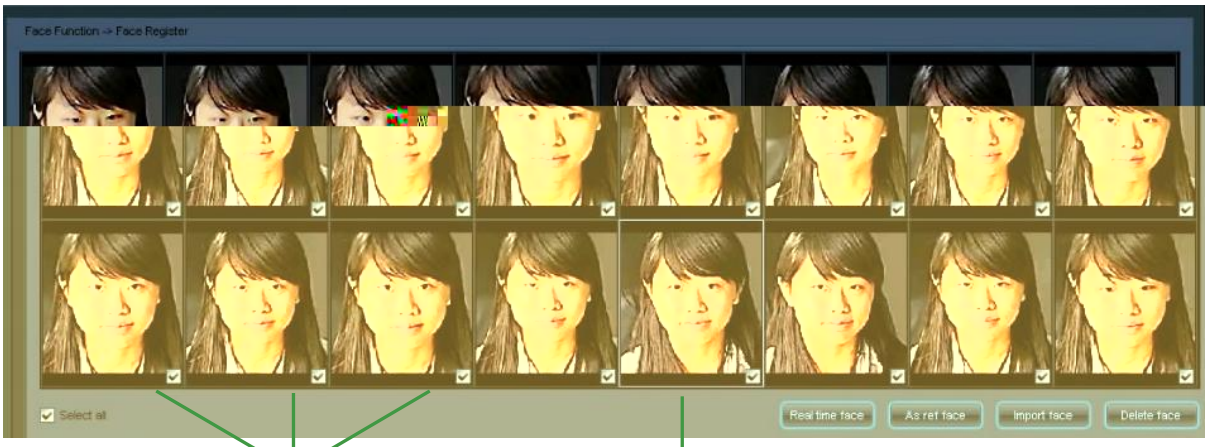
1. Face identification function is available for a maximum of one video device.
2. For the configuration and application of face identification function, see 5.24 How to Set and Apply Face Function.

4.8.1 Face Registration



- **Face Template List**

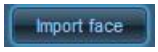
After right clicking **Enabling Face Identification** on the preview page, you can add the detected faces to this list, or you can manually import face pictures to this list. The system will extract a face template from the ticked picture on the template list and use it as the face template for the currently registered user.



Currently ticked face images The blue cell indicates currently chosen position or face image

Tick all the pictures on the list.

The previously detected face images are used as face templates. The system can store a maximum of 500 real-time face images. If there are more than 500 face images, the earliest ones will be replaced.



You can manually import local face pictures. The picture must be in the JPG format and its size must be the multiple of 16, for example, 320*480. There can only be one face in the picture and the face should be as regular as possible.

If you click this button, the currently chosen face picture (in blue cell) will be used as the reference picture for the currently registered user.

Delete currently ticked pictures.

. **Face Registration Information**

User ID It is the ID of a user; the IDs that have already been added to the system cannot be changed; the unregistered IDs can be added to the system.

User name It is the name of a user, which can be changed according to actual circumstances.

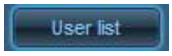
User gender Female or male.

User native place It is the native place of a user, which can be changed according to actual circumstances.

ID type ID card, passport, driving license or other certificates.

Certificate number The certificate number can be changed according to actual circumstances.

Blacklist user Ticking this option, you can set this user as a blacklist user.

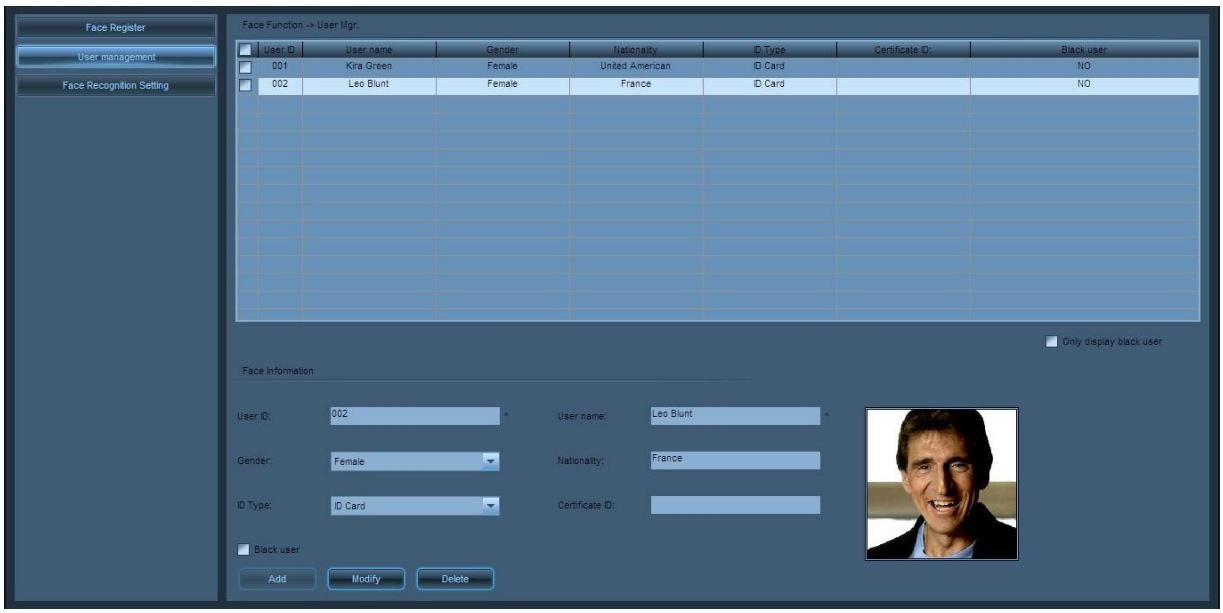


Click to access the registered user list.

Click to select one user on the registered user list, click **Confirm** and this user's face registration information will be displayed on the face registration page. Now you can modify this user's information. Click **Modify** to save the modification.

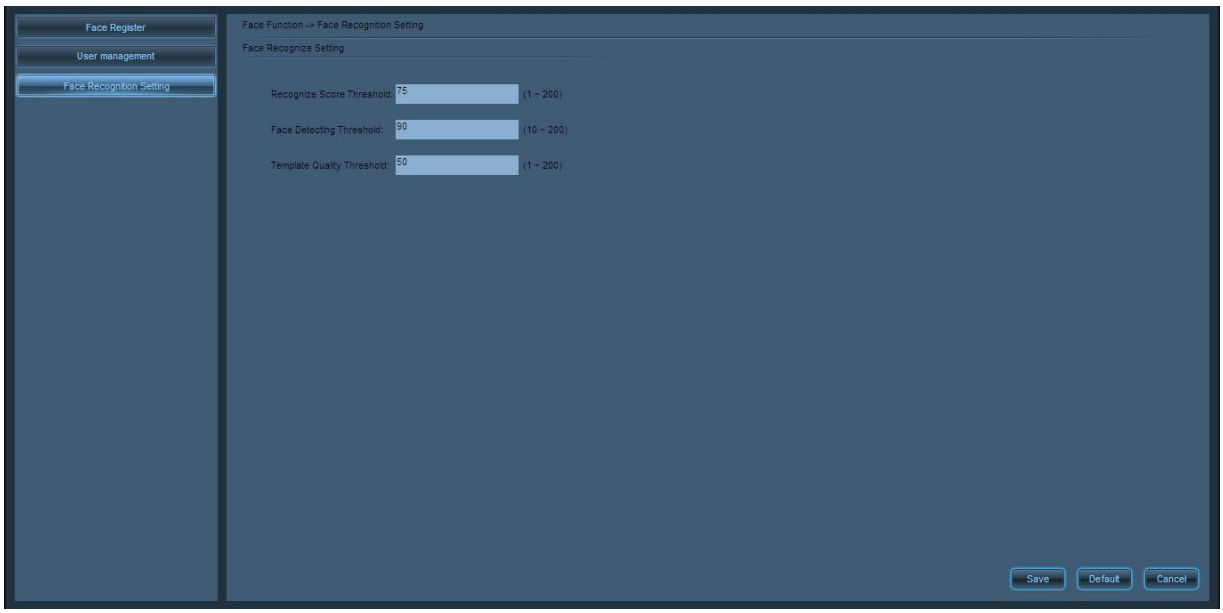
After setting face registration information, click this button to register the user.

4.8.2 User Management



Display blacklist users only	If you click this option, only blacklist users will be displayed on the user list.
User ID	It is the ID of the user; the IDs that have already been added to the system cannot be changed; the unregistered IDs can be added to the system.
User name	It is the name of a user, which can be changed according to actual circumstances.
User gender	Female or male.
User native place	It is the native place of a user, which can be changed according to actual circumstances.
ID type	ID card, passport, driving license or other certificates.
Certificate number	The certificate number can be changed according to actual circumstances.
Blacklist user	Ticking this option, you can set this user as a blacklist user.

4.8.3 Parameter Setting



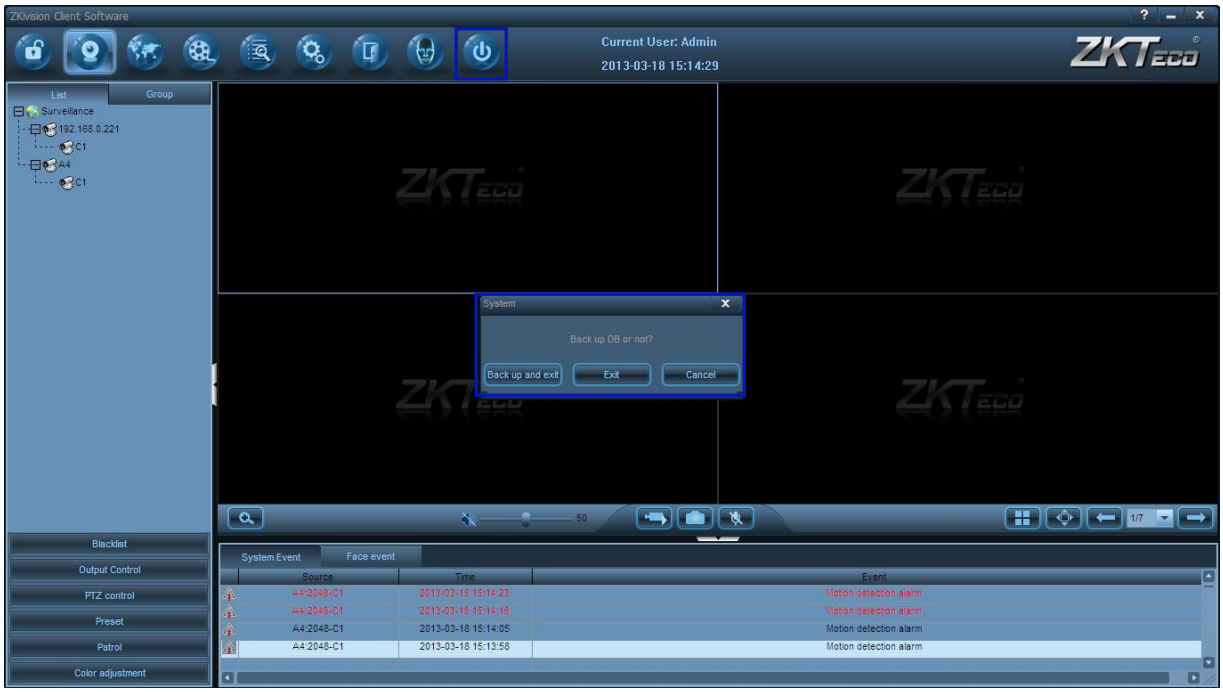
Threshold value for face identification marks It is the similarity threshold value of a detected object compared with the user face template in the database. A smaller threshold value makes it easier for the system to identify a face; however, misjudgment is apt to occur. A greater value ensures a more accurate identification of a face, but it is possible that the system cannot identify the face. So a moderate value is recommended.

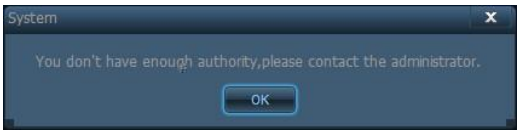
Face detection quality threshold value It is the similarity threshold between the detected object and the face. A smaller threshold value makes identification more sensitive, but it is likely for the system to identify a similar face as the exact face. A greater value makes it possible for the system to miss detecting faces. So a moderate value is recommended.

Template quality threshold value It is the threshold value for face features. A greater threshold value ensures a clearer contour of a detected face.

Min face size The minimum size of captured face images. The width and height cannot be smaller than 160 and 200 respectively.

4.9 Logout





Back up and exit The system backs up the configuration and exits. The default backup path is Installation Path\Database_Backup.

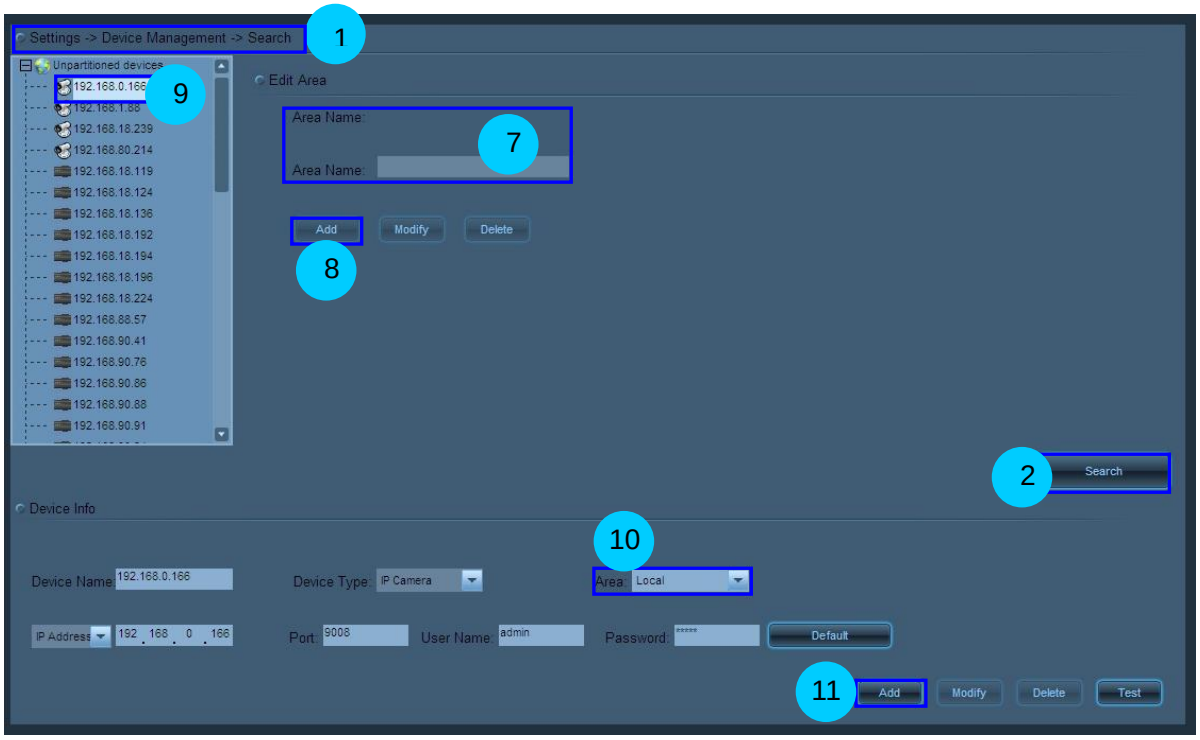
Exit The system exits directly if you click Exit.

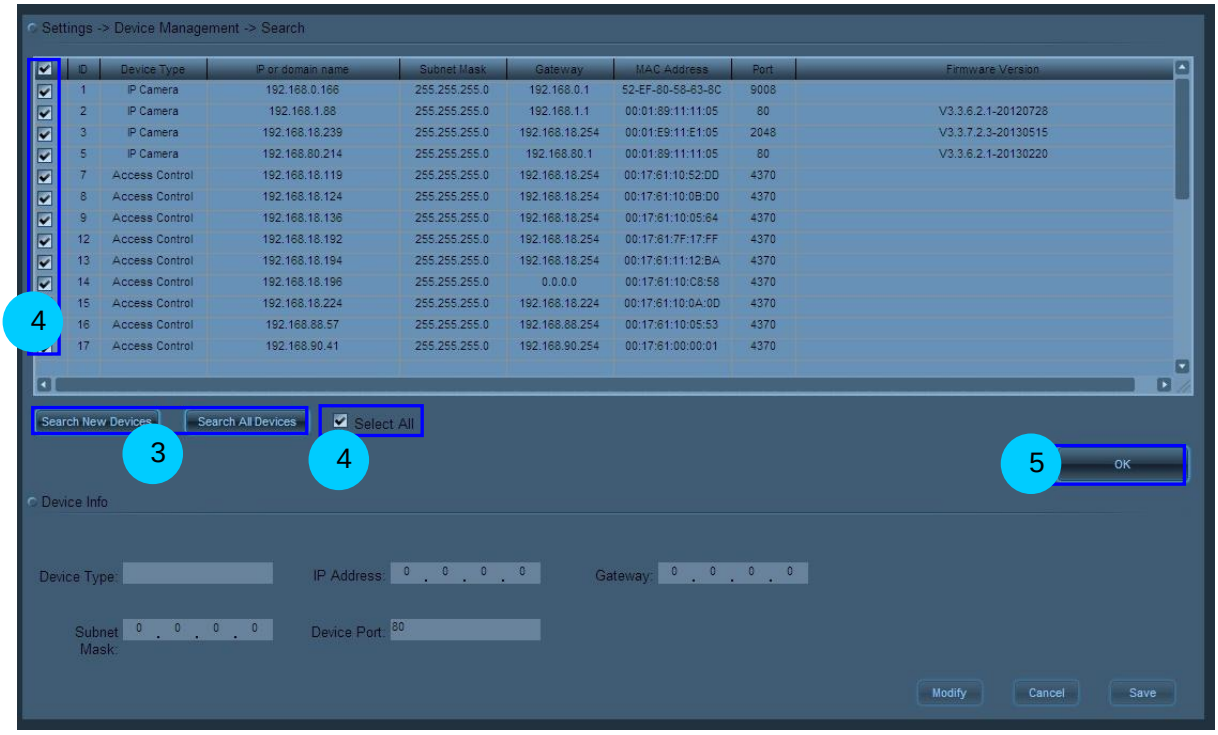
Cancel The system cancels exiting if you click Cancel.

Note: Only superusers and the custom users with a system shutdown authority can exit the client software.

5 Configuration

5.1 How to Search and Add Camera/NVR/Access Controller to an Area



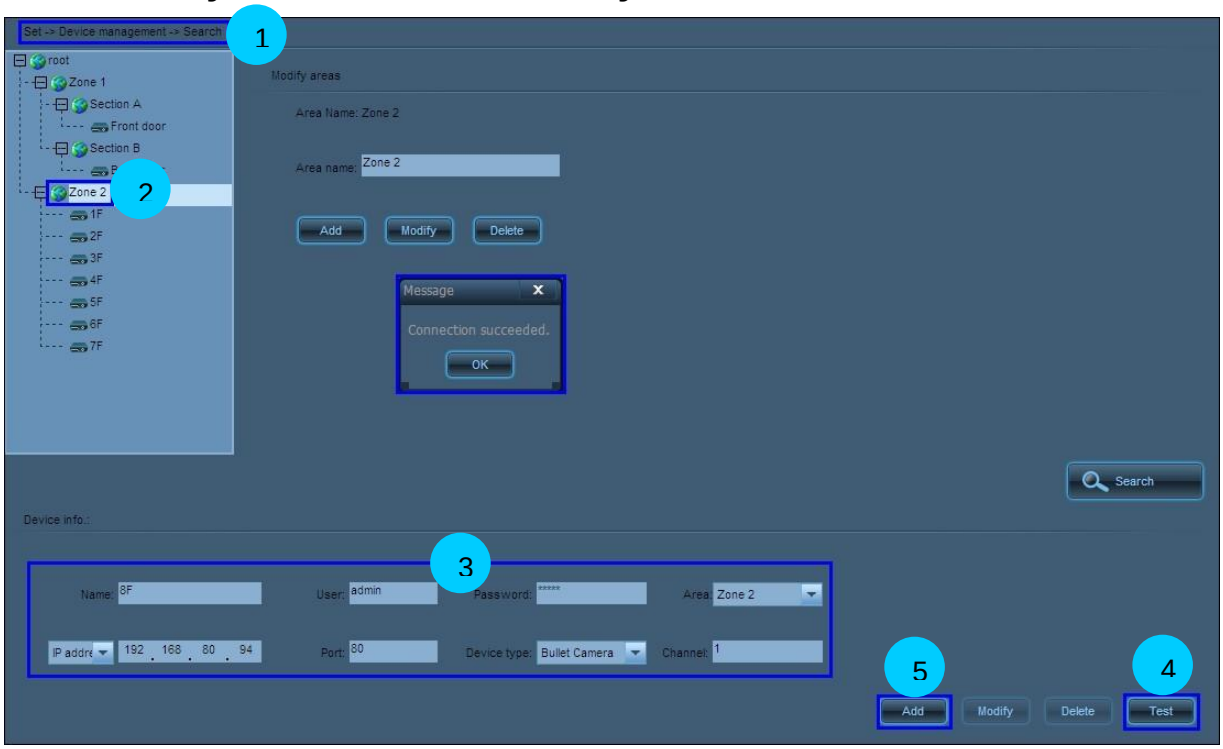


1. Enter the "Settings" -> "Device Management" -> "Search" interface.
2. Click to enter the device search interface.
3. Click or to search devices.
4. Select the device to be added or select "Select All" to select all devices in the search list.
5. Click to finish the device searching.
6. Click and select the parent area in the device list.
7. Set the field of Area Name.
8. Click to add this named area to the parent area.
9. Select an unpartitioned device in the device list.
10. Set the field of Area in "Device Info".
11. Click to add this device to the area.

Note: 1. Up to 128 areas can be added.

2. After device search is completed, the camera cannot videotape or capture images unless it is added to an area. Unpartitioned devices cannot be used.

5.2 Manually Add a Device to the System



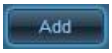
1 Choose Set > Device Management > Search.

2 Click a parent area in the device list.

3 Manually fill in information about the to-be-added device in the **Device info** pane.

4 Click

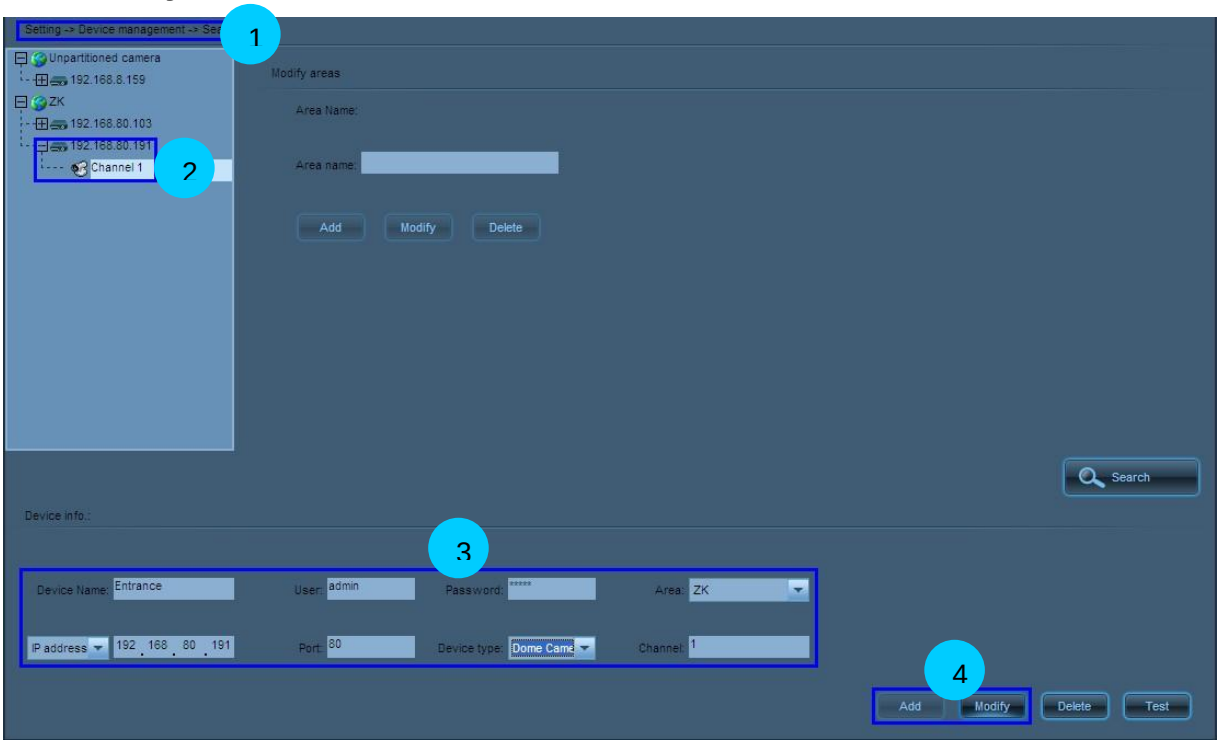
to check whether connection succeeds.

5 After confirming the connection succeeds, click 

to add the camera to the system.

Note: If a device has no fixed IP address on a public network, you can gain access to this device by using a domain name provided by the domain name supplier. In this case, you must manually add this device to the system. For details of domain name registration and device configuration, see 5.20 Apply for and Use a Domain Name for Device Access.

5.3 Modify Local Device Information

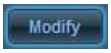


1 Choose Settings > Device management > Search.

2 Click a camera channel in the device list.

3 Modify the device information in the **Device info** pane.

4 Click

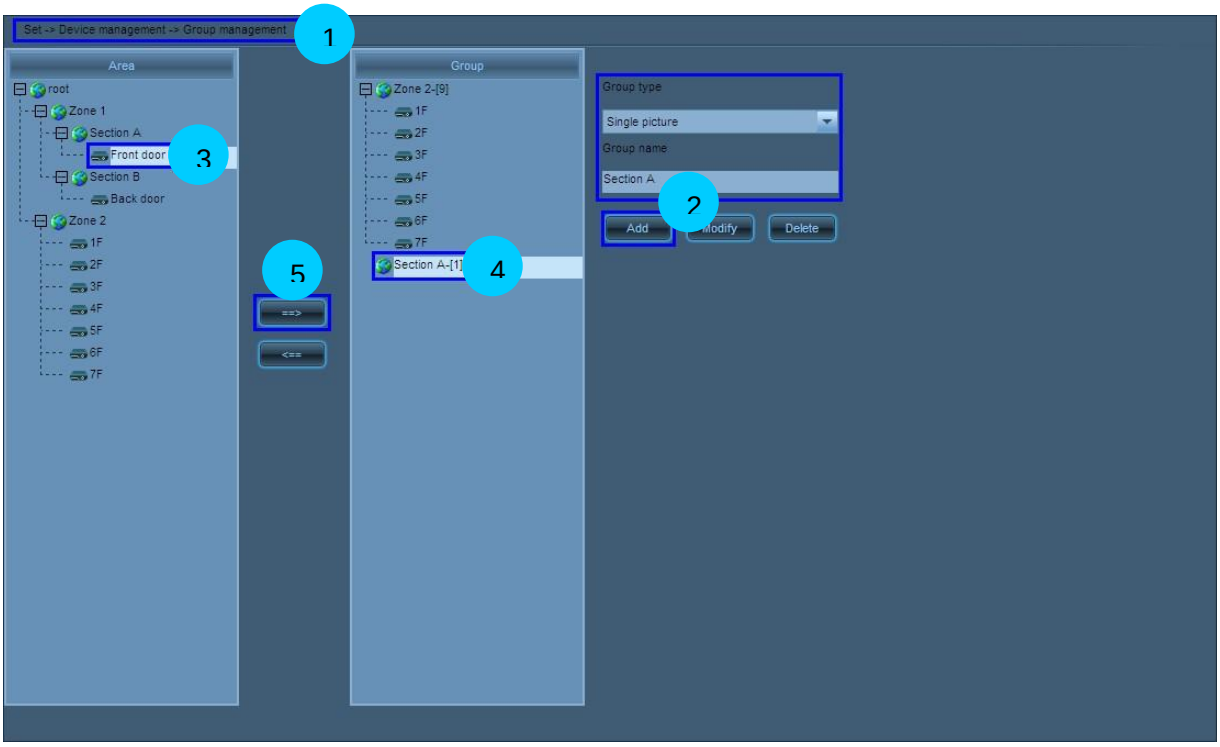
or 

to save modification.

Note: 1. After a device name is set, the device list displays only the name instead of the IP address of the device.

2. This section describes the procedure for modifying related local device information. For details of modifying remote device parameters (such as IP addresses and port numbers), see Modify Network Parameters of a Camera.

5.4 Group Cameras



1 Choose Set > Device management > Group management.

2 Set the group type and group name and click

to add a new group.

3 Click a camera channel in the device list.

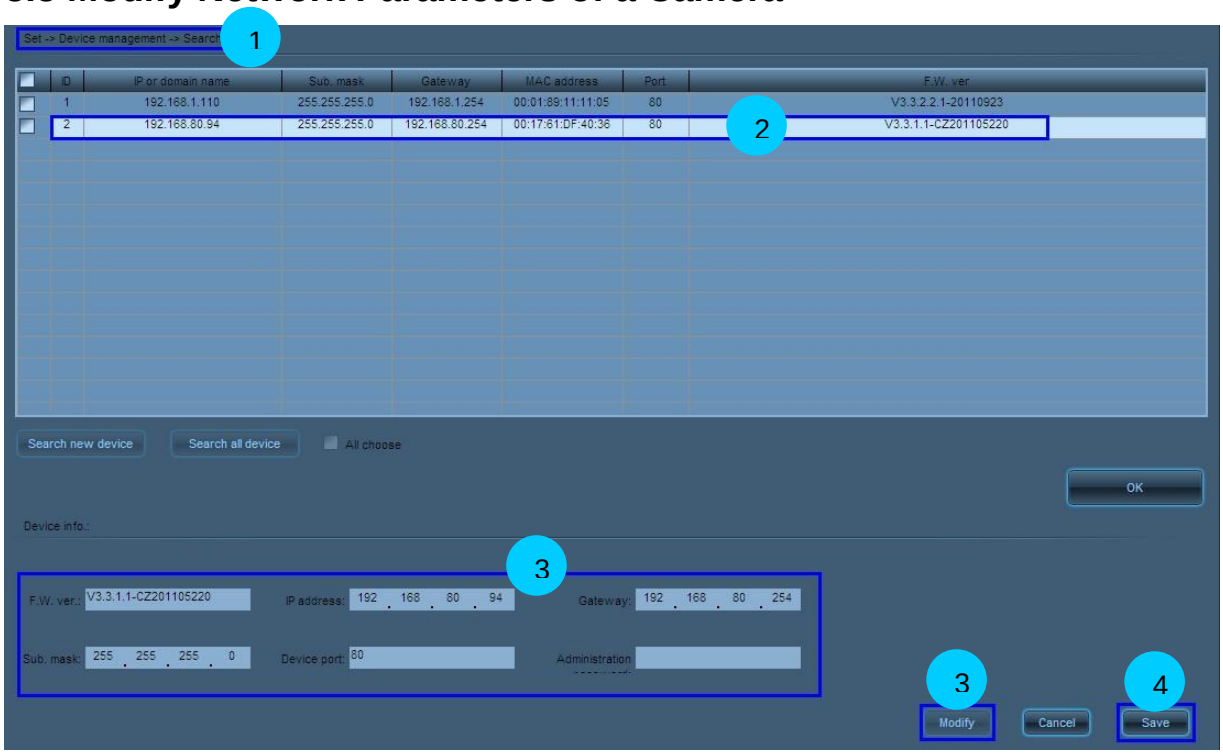
4 Click a group in the group list.

5 Click

to add the selected camera channel to this group.

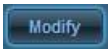
Note: Up to 20 groups can be added.

5.5 Modify Network Parameters of a Camera



1 Choose Set > Device management > Search.

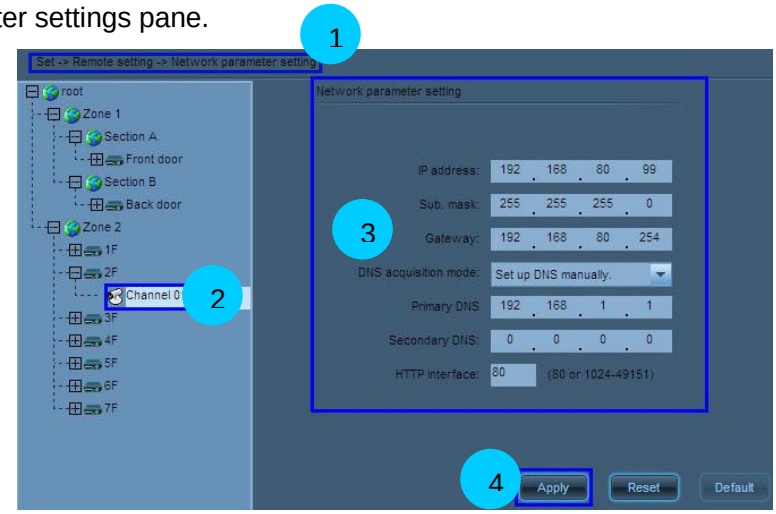
2 Select a camera from the search result list.

3 Click  and then modify the remote device information of this camera.

4 Enter a correct admin password and click to save your settings.

☺**Note:** You can also modify network parameters of a camera in the following two methods.

Method 1: Choose Set > Remote settings > Network parameter settings and perform setting in the Network parameter settings pane.



1 Choose Set > Remote settings > Network parameter settings.

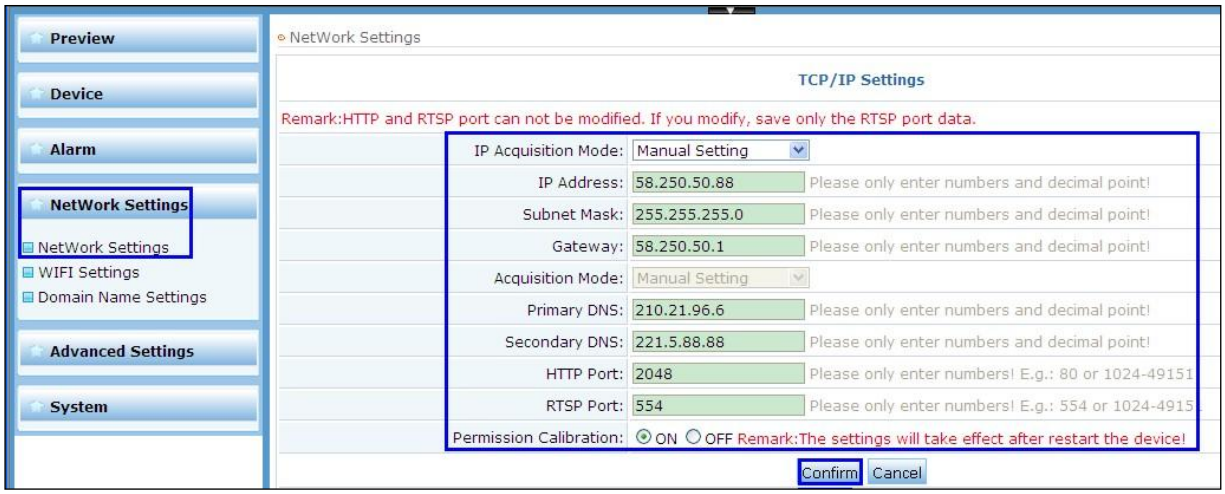
2 Double-click a camera channel in the device list.

3 Modify the network parameters of the camera, including the IP address, DNS acquisition mode, and DNS addresses.

4 Click

to apply your settings.

Method 2: Access a camera through browser and choose **Network settings** > **Network settings** to modify network parameters of the camera in the **Network settings** pane. For details, see Network Settings in the *User Manual--Using Browser for Video Surveillance* in the delivery-attached CD.



5.6 How to Set Timed Recording

2. Enter the "Settings" -> "Local Settings" -> "Storage Management" interface.
3. Double-click the camera channel to be set to timed recording in the device list to connect it.
4. Select "Enable recording" to enable the recording function. Choose the stream format of recording.
5. Drag the left mouse button to set the work time of planed recording (0~23 indicates one day, measured in half an hour).Drag again to cancel.
6. Click

to save the settings.
7. Select "Enable planed recording".
8. Click

to save the settings.
9. Disable the planed recording: Deselect "Enable planed recording", and click

to save. Or cancel the green squares in the work time of planed recording and click

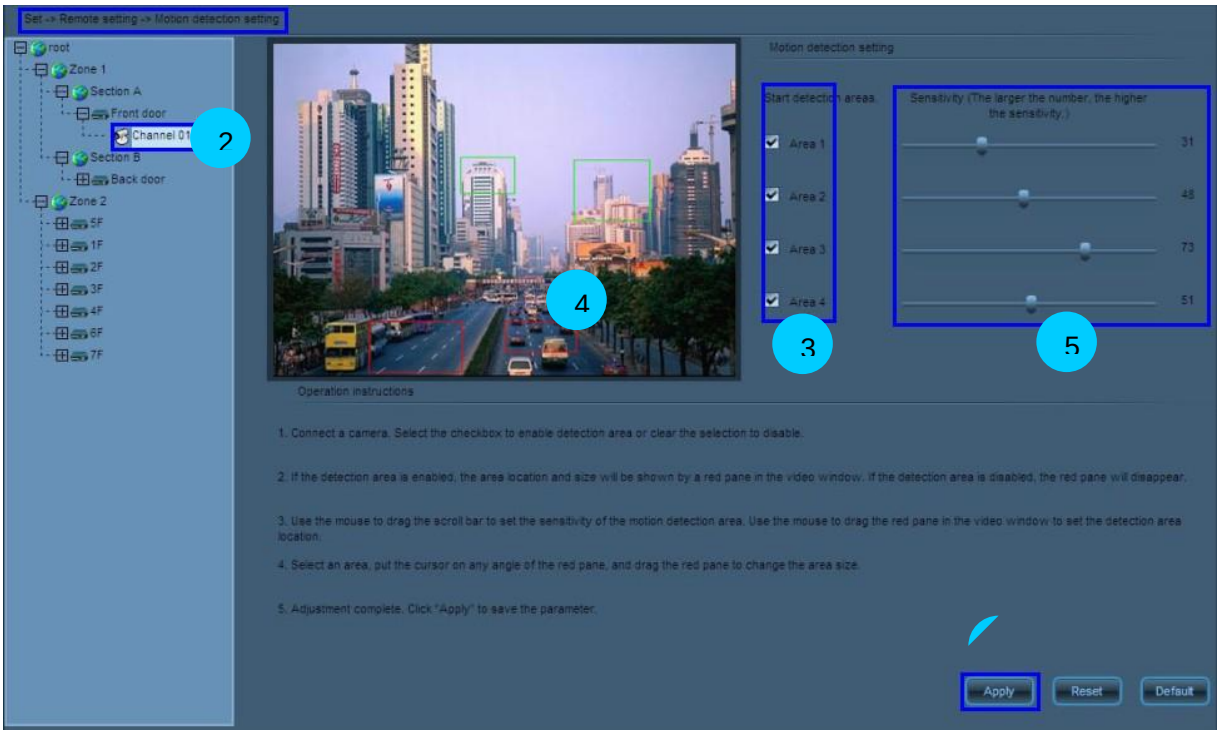
to save.

Note: If the work time of planed recording of all devices is the same, set the work time of planed recording for one device, click

to set the copied content, and click

to save the settings. Then all devices enable planed recording.

5.7 Set Motion Detection



1 Choose Set > Remote settings > Motion detection settings.

2 Double-click a camera channel in the device list.

3 Select one or more areas for motion detection.

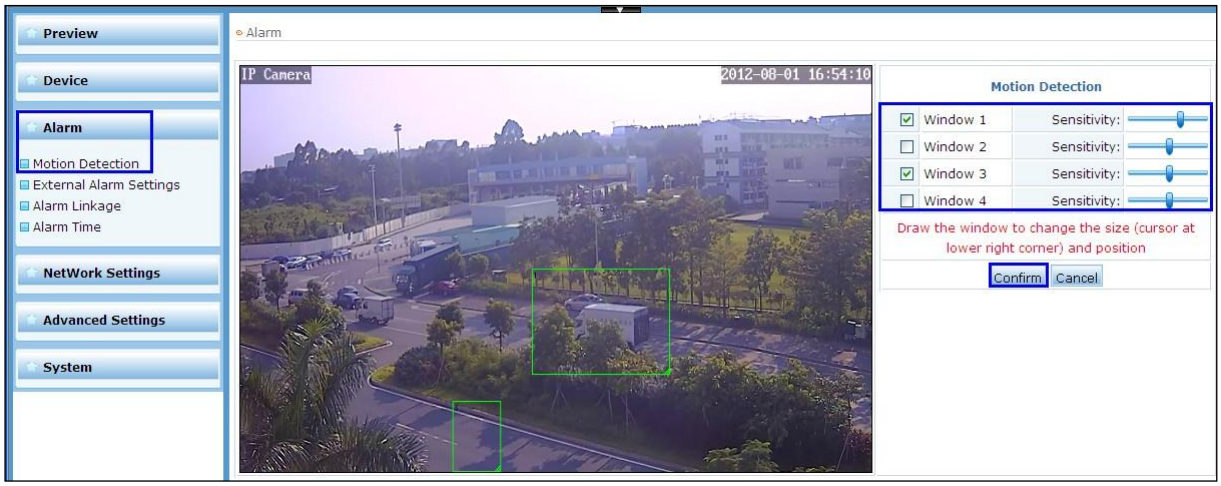
4 Set the locations and sizes of these areas.

5 Set the detection sensitivity of these areas.

6 Click

to apply your settings.

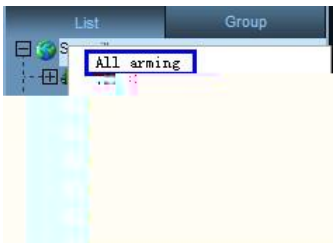
Note: You can also access a camera through BROWSER and choose **Alarm** > **Motion Detection** to set motion detection parameters. For details, see Motion Detection in the *User Manual--Using Browser for Video Surveillance* in the delivery-attached CD.

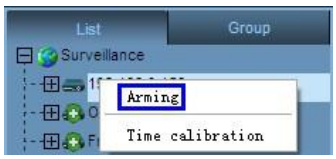


5.8 Enable Arming

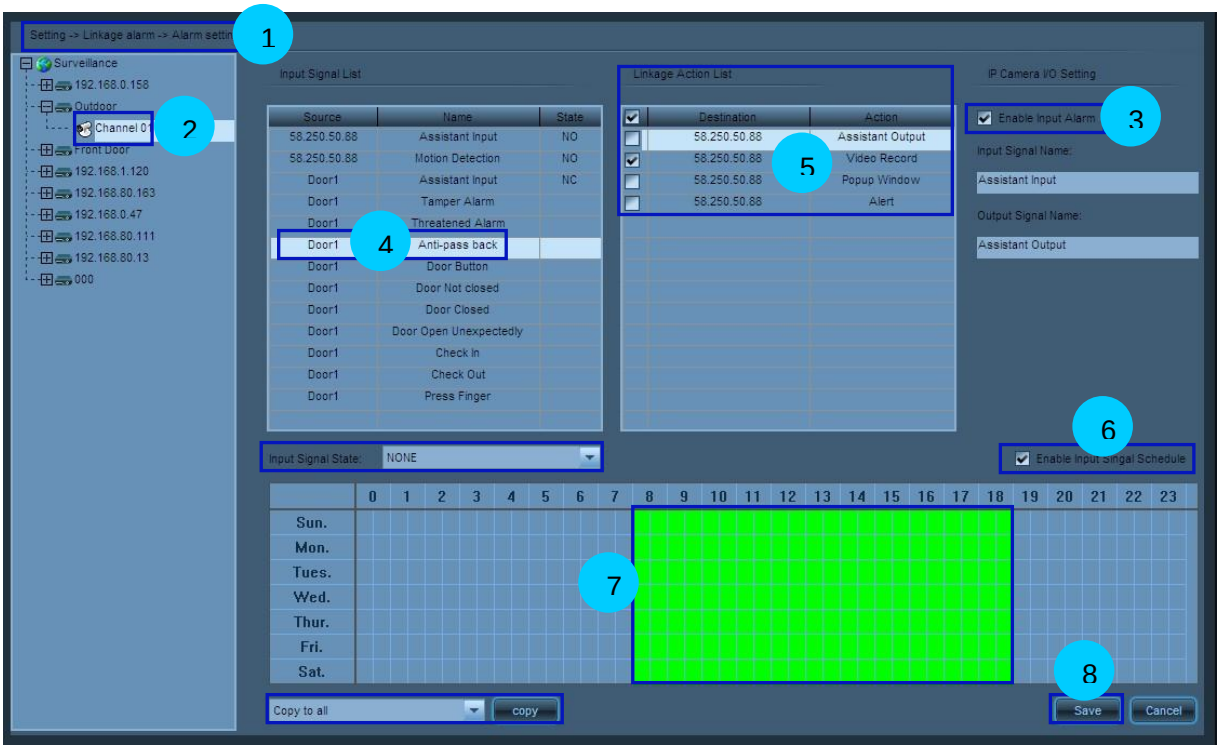
The alarm linkage of all signals will work only after the device (the camera) is armed. If the device is disarmed, it cannot produce alarm linkage.

Enter Preview interface, right click on the area name in the device list, and choose **All Arming** in the fuction menu to enable all alarm linkage of all devices in this area. Right click on the device name in the device list, and choose **Arming** in the fuction menu to enable all alarm linkage of all channels in this device.





5.9 Set Alarm Linkage



1 Access the **Setup** --> **Alarm Linkage** --> **Alarm Setup** page.

2 Double-click on the device list the camera channel for which alarm linkage is to be set. When the connection is successful, the input-output signals of the associated alarm will be displayed on the list.

3 Click **Enable alarm input** to start using alarm input signals.

4 Click to select alarm input signals on the input signal list.

5 Tick linkage actions on the linkage action list. You can select more than one.

6 Tick **Enable input signal setting** to start setting the time for input signal alarm linkage.

7 Press the left mouse button and drag the cursor to set the time period for input signal alarm linkage (0 ~ 23 indicates a day, with half an hour as the unit). If you want to cancel it, you can drag the cursor again.

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

9 Set the storage location and time length for the alarm linkage video.

9.1 Access the **Settings** --> **Local Settings** --> **Storage Management** interface to set alarm linkage video.

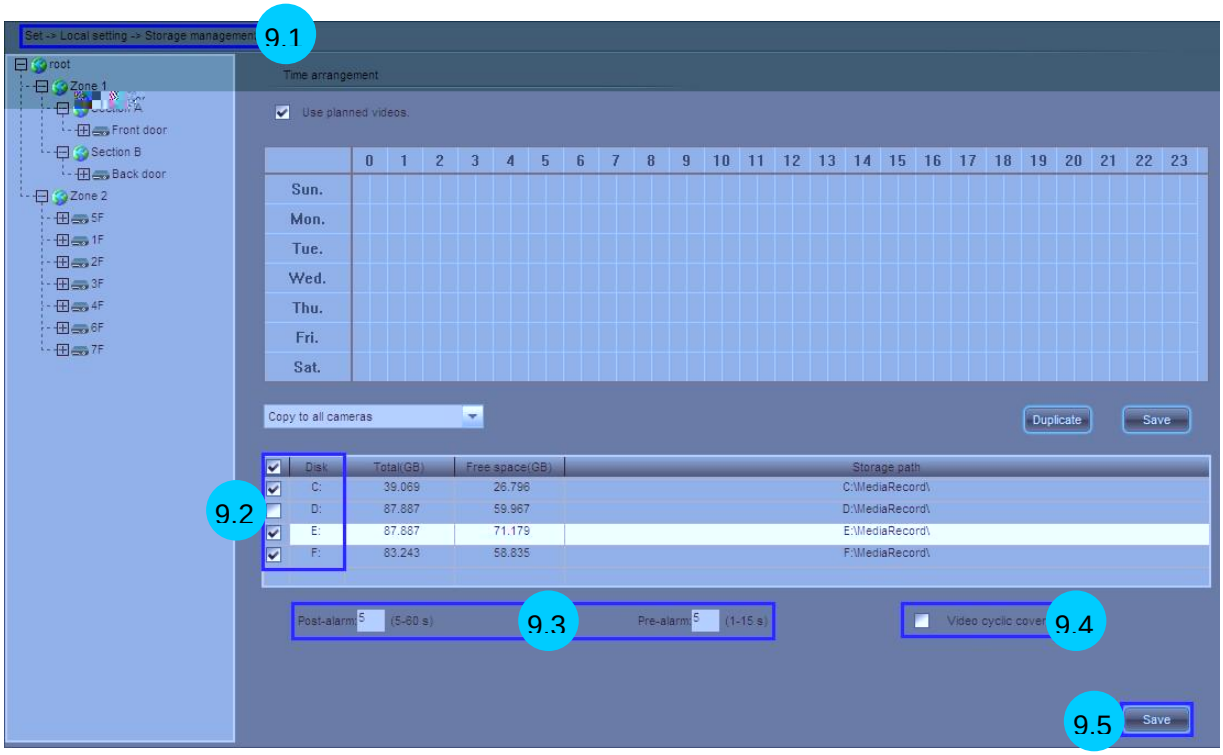
9.2 Tick the storage location for the video (After the installation, the software will automatically detect the hard disks of the computer and display them on the list).

9.3 Set alarm video: the lasting time of the alarm and the time for pre-recording an alarm.

9.4 If you tick **Video Cyclic Cover**, then when all the space of the disk is occupied, the earlier 5G video file will be deleted. If you cancel the tick, then when the disk is full, the video recording will stop.

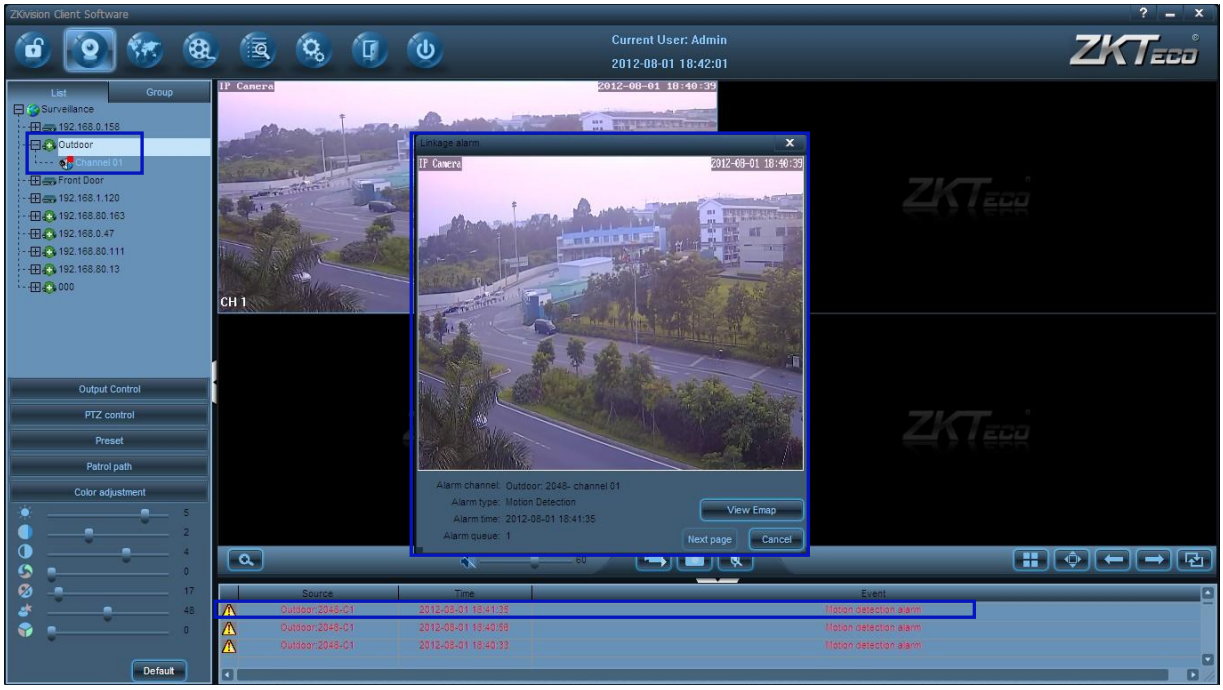
9.5 Click **Save** to save the setting.

10 You can select other camera channels and click **Copy** to copy the alarm linkage setting to other cameras.



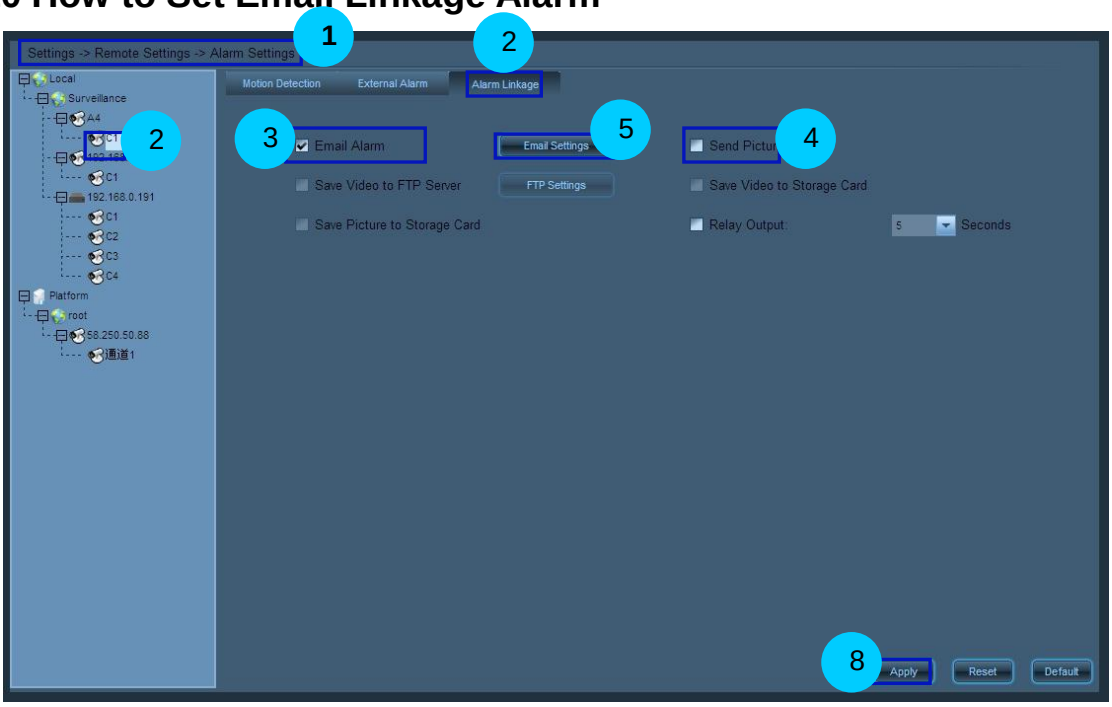
Note: After arming, an alarm will trigger the alarm linkage options.

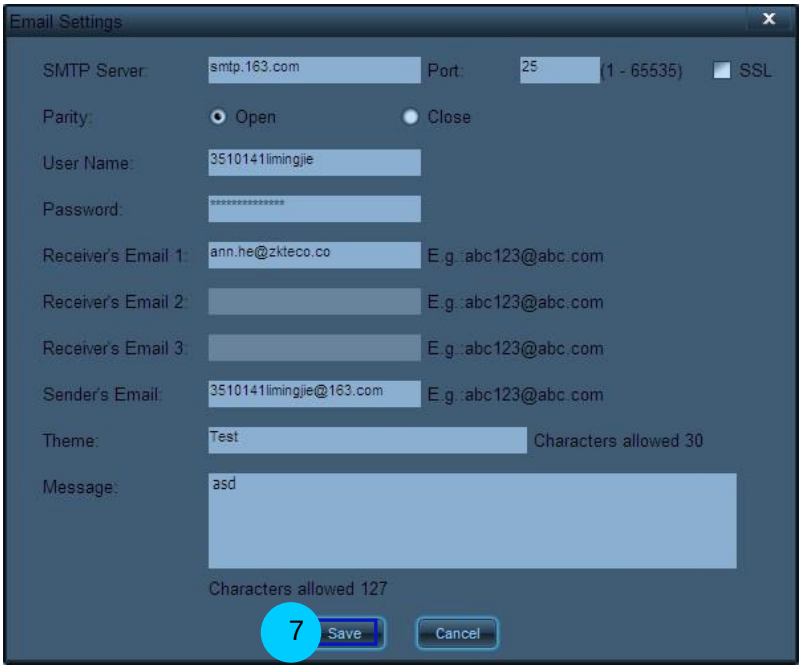
Pop up video window :



Linkage video alarm:

5.10 How to Set Email Linkage Alarm





1. Enter the "Settings" -> "Remote Settings" -> "Alarm Settings" interface.
2. Double-click the camera channel to connect it, and shift to "Alarm Linkage".
3. Select "Email Alarm" to enable email alarm function.
4. After enabling the email alarm function, select "Send Picture" to send the captured pictures to the preset email.
5. Click "Email Settings" to directly enter the email settings interface linked to this interface.

6. Set the following items based on actual needs.

SMTP Server: is the IP address of SMTP server. See your mailbox settings for details.

Port: is 25 by default. To modify the port, please contact your network administrator or consult professionals.

SSL: Select the box to enable secure connection. See your mailbox settings for details.

Parity: If you select "Open", you need to input the user name and password for communications upon successful validation; if you select "Close", you do not need to input the user name and password for validation.

User Name: is the name of email.

Password: is the password of email.

Receiver's Email: is the email address to receive alarm emails. Please input at least one email address.

Sender's Email: is the address displayed in the alarm emails.

Theme: is the subject of the alarm emails.

Message: is the content of the email.

10. After finishing the settings, click

to save the email settings, and click "X" to exit from the email settings interface.
11. Click

to enable the email alarm linkage settings.

5.11 Configure Preset Locations and Cruise Routes

1 Choose Set > Remote settings > PTZ parameter settings.

2 Double-click a camera channel in the device list.

3 Adjust the camera to the desired location.

4 Select the ID of a preset location.

5 Set the name of the preset location.

6 Click

to add the preset location.

7 Set the name of a cruise route.

8 Click

to add the cruise route.

9 Click a preset location in the preset location list.

10 Select a cruise route from the **Cruise route** drop-down list.

11 Click

to add the preset location to this cruise route.

12 Click

to save your settings.

5.12 Search and Playback Videos by Date

1 Click to enter **Playback** interface.

2 Select devices based on date type.

3 Select a video type from the drop-down list.

4 Select a date.

5 Click to search for videos and the search results are displayed on the Timeline panel.

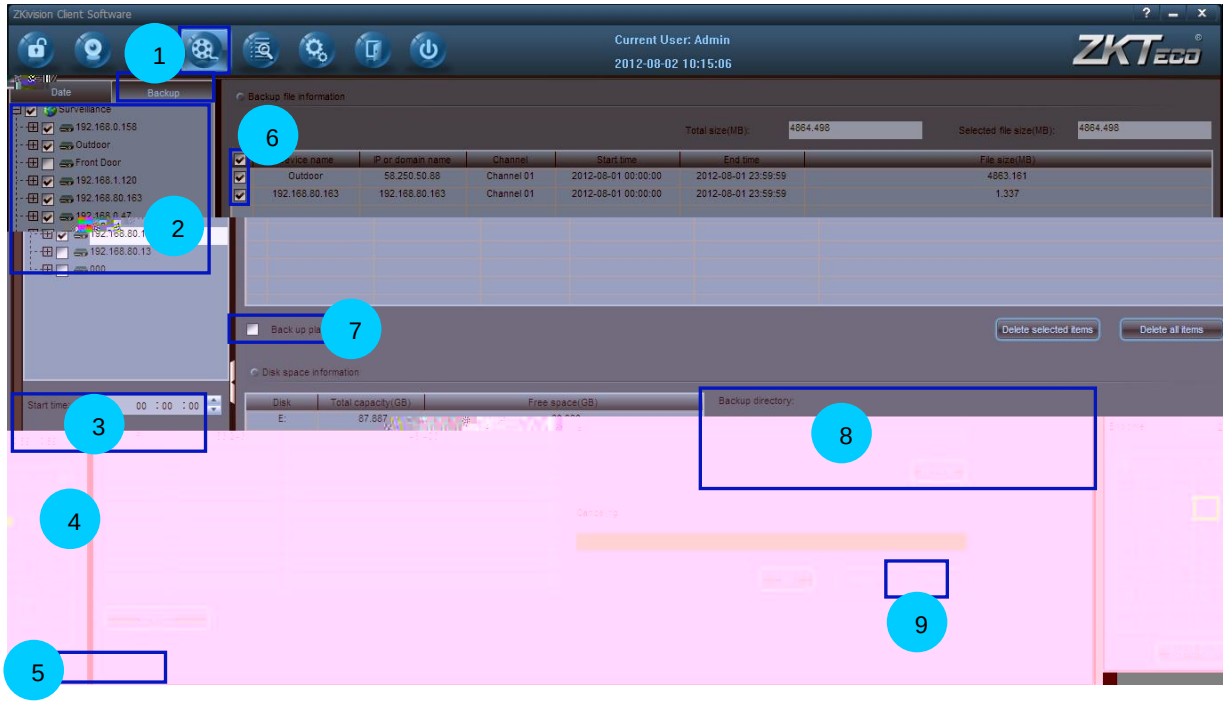
6 Click on the Timeline panel as the start point for playback.

7 Click to start playing back videos.

Note: 1. A maximum of four channels can be selected for video search and playback by date.

2. When replaying a video, the replay will be stopped if changing the page.

5.13 Back Up Videos



1. Enter **Playback** interface and click “Backup” to enter the page of video backup.

2. Tick the cameras for video search.

3. Set the specific period.

4. Select the date.

5. Click

to add the searched videos to the backup list.

6. Tick the videos to be backed up.

7. Select whether to back up the media player.

8. Click the button

to set the path of backup.

9. Click the button

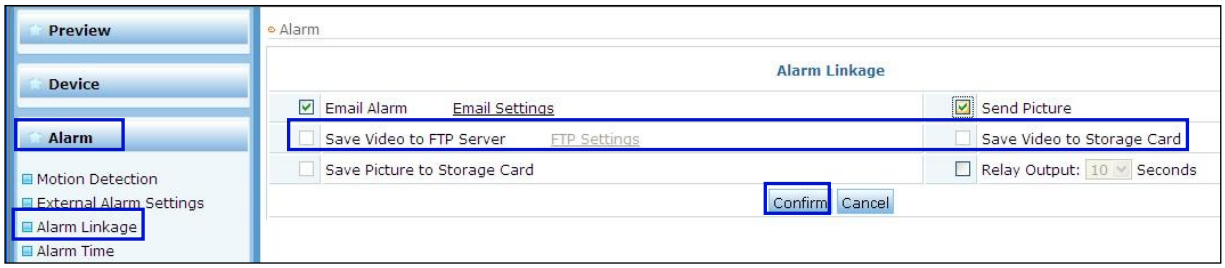
to start the video backup.

Notes: 1. The total files to be backed up should not be larger than 8G every time.

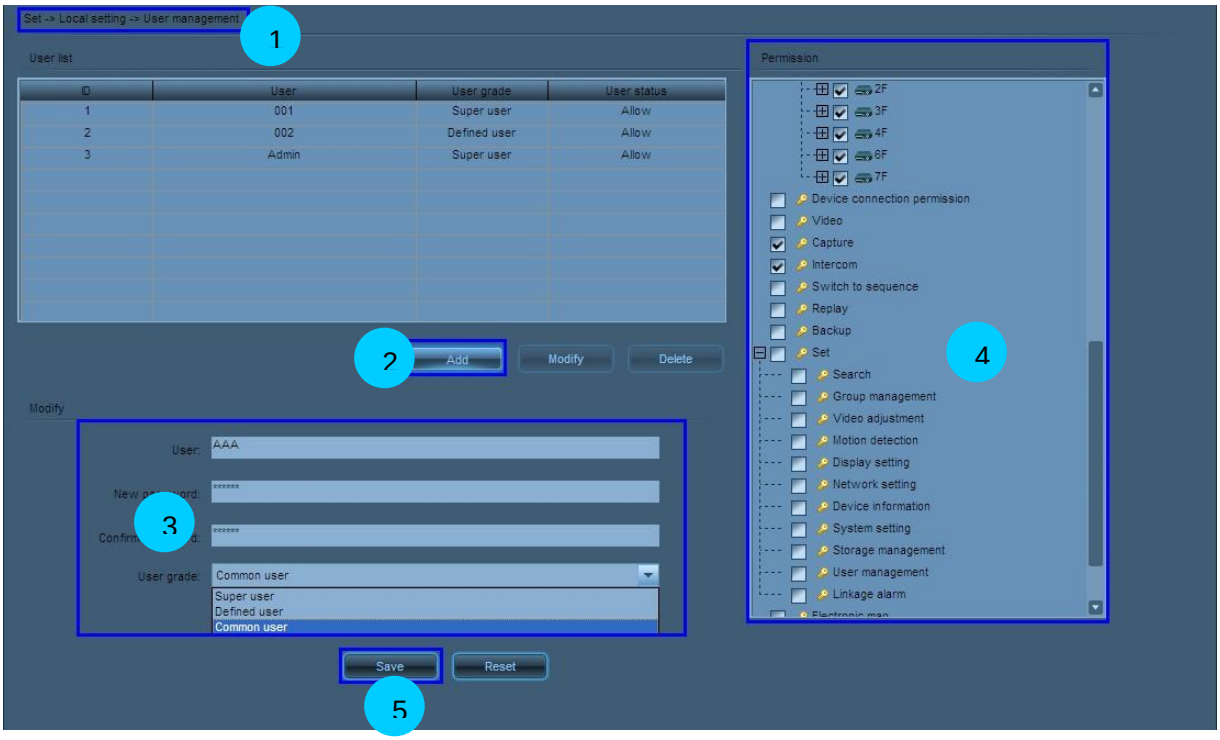
2. The path of backup should be neither the system disk, e.g. disk C, nor the video storage disk.

3. You can also access a camera through BROWSER and choose **Alarm** > **Linkage alarm** and select the **Save Video to Storage Card** option to back up the video to a storage card or select the **Save Video FTP Server** option to back up the video to

an FTP server and a storage card concurrently. For details, see Alarm Linkage in the *User Manual--Using Browser for Video Surveillance* in the delivery-attached CD.



5.14 Create a New User



1 Choose Set > Local settings > User management.

2 Click

.

3 Set a user name, a password, and a user level.

4 Set the user authority.

5 Click

to save the profile of the new user.

5.15 How to Modify User Info or User Permission

1. Enter the "Settings" -> "Local Settings" -> "User Management" interface, and shift to "User".
2. Select the user to be modified from the user list.
3. Click

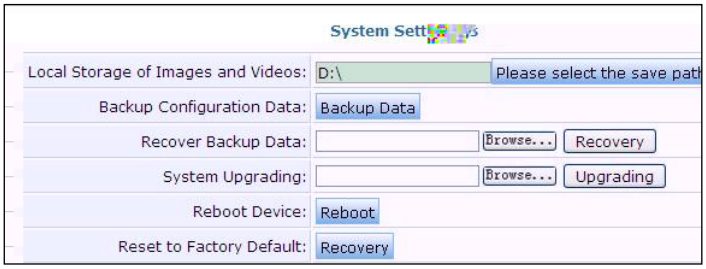
to enter the modification interface.
4. Modify the user name, role, user status or password.
5. Click

and click

to save the modified user information.

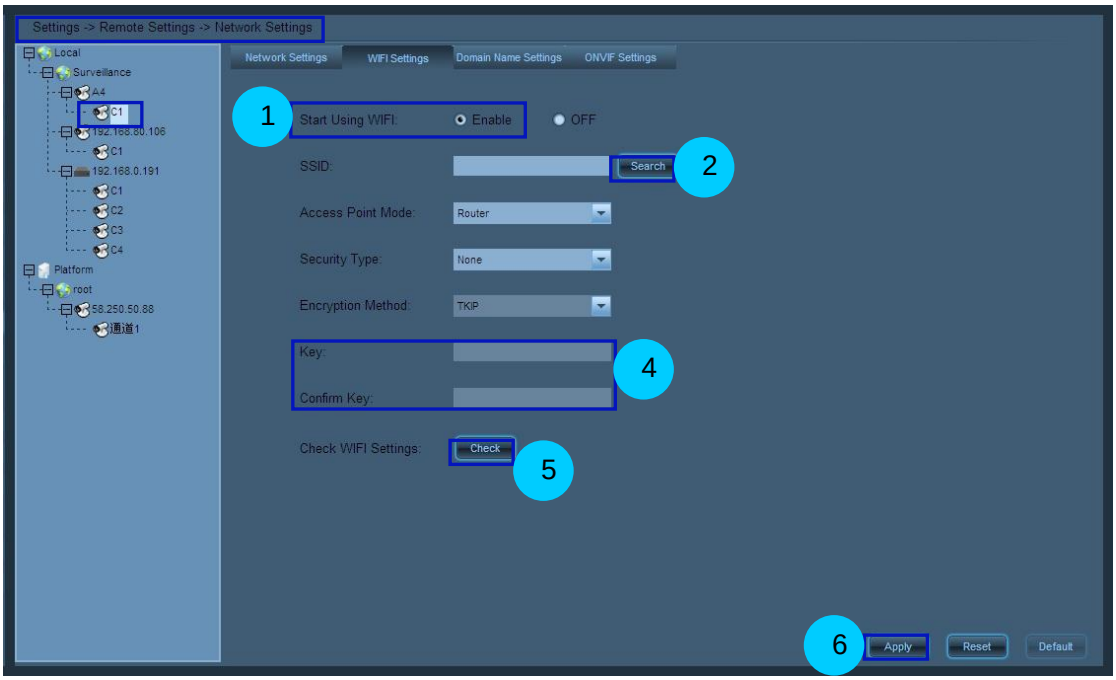
5.16 Back Up and Recover Configuration Data

To back up or recover configuration data, access to a camera through browser and choose **System** > **System Settings** to perform system settings. For details, see System Settings in the *User Manual--Using Browser for Video Surveillance* in the delivery-attached CD.



5.17 How to set WIFI

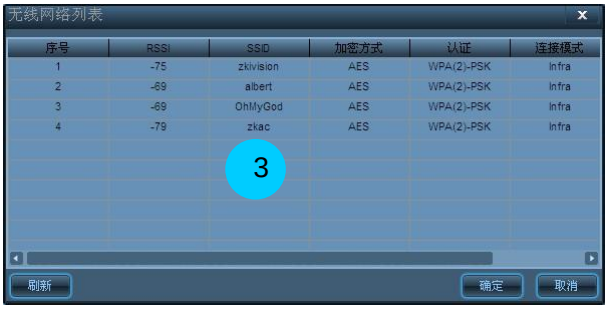
Before enabling the wireless network, use network cable to connect the device with the network. Enter the "Setting" "Remote Settings" "Network Settings" "WIFI Settings" submenu, and double-click a camera channel to connect it. Please configure WIFI connection by following the steps as follows:



1. Start using WIFI.
2. Click

to search available WIFI.

3. Select a WIFI network in the pop-up WIFI list. All the parameters of the selected WIFI will be automatically filled in each parameter bar (such as the access point mode and way of encryption).

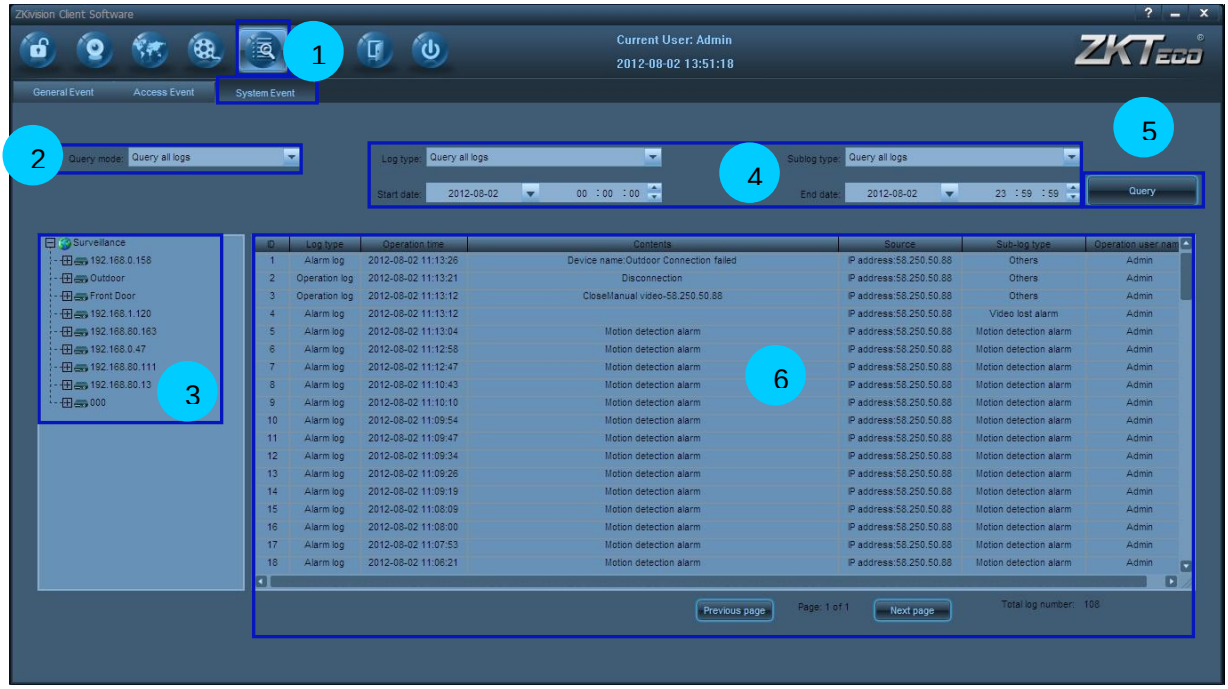


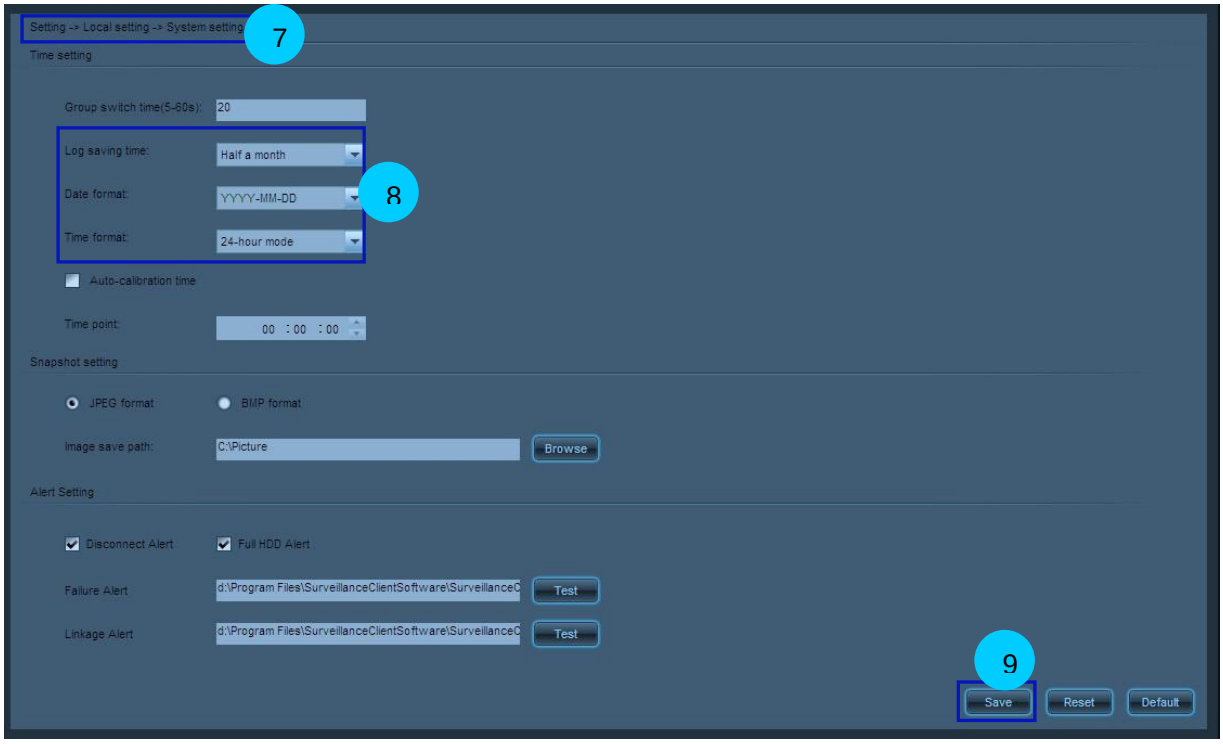
4. If a key is set to the router, input the key.
5. Click

to check if the WIFI is connected normally.
6. After successful connection, click

to enable the settings.
7. Pull up the network cable, and restart the device.
8. Access the camera by the browser, and enter the "Settings" -> "System" -> "Device Info" interface, you can see the network connection type displayed as "Wireless Connection".

5.18 Search for System Logs



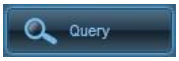


1 Click the button.

2 Select a data type.

3 Select the log type, sublog type, start date and end date.

4 Select a camera channel or a user.

5 Click 

to query the logs of a specified type within the defined time period.

6 Query results are displayed in the log list. Drag the scroll bar on the rightmost side or at the bottom of the interface to view the details. Click

or

to view the query results on the previous or next page.

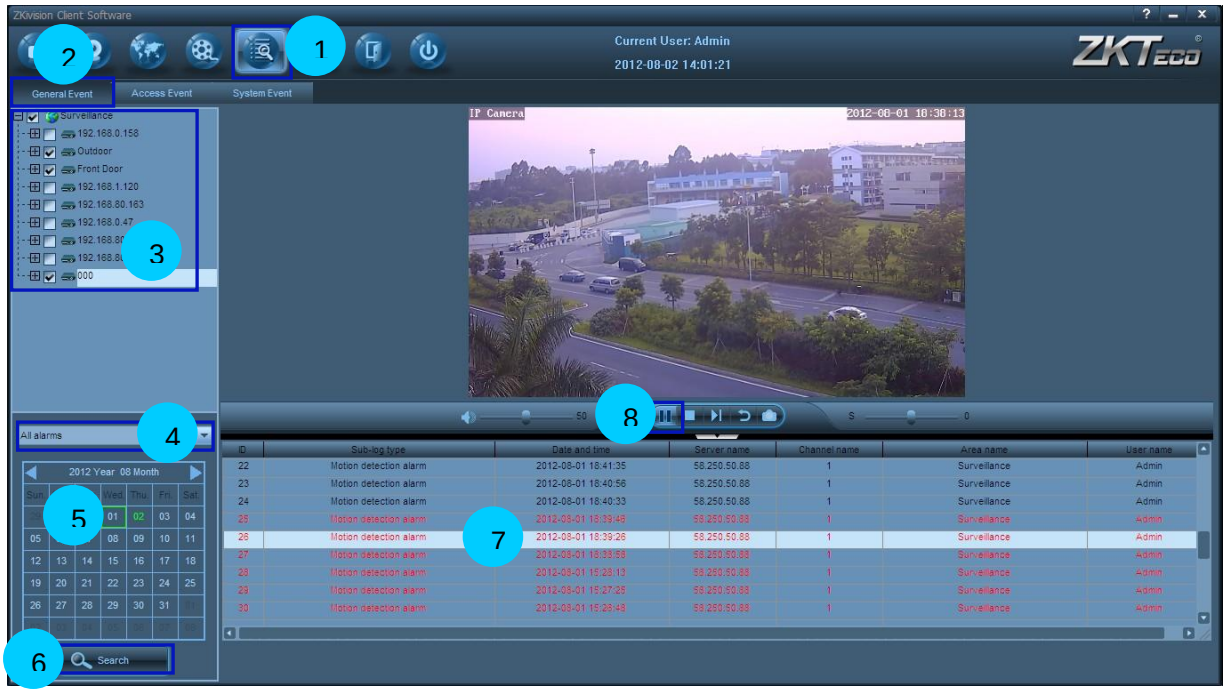
7 To modify the log saving time, date format, or time format, choose **Set** > **Local settings** > **System settings**.

8 In the **Time settings** pane, modify the log saving time, date format, or time format.

9 Click

to save your settings.

5.19 Playback Associated Videos Through Alarm Logs



1 Click the button.

2 Click the **Alarm** tab to search for videos based on alarm type.

3 Select the camera channels for query.

4 Select an alarm type.

5 Select a date.

6 Click to find out the alarm logs on that date. Query results are be displayed in the log list.

7 Select one of the alarm logs in the log list.

8 Click to play the associated videos of this alarm log.

Note: The video playback will stop if you change the page.

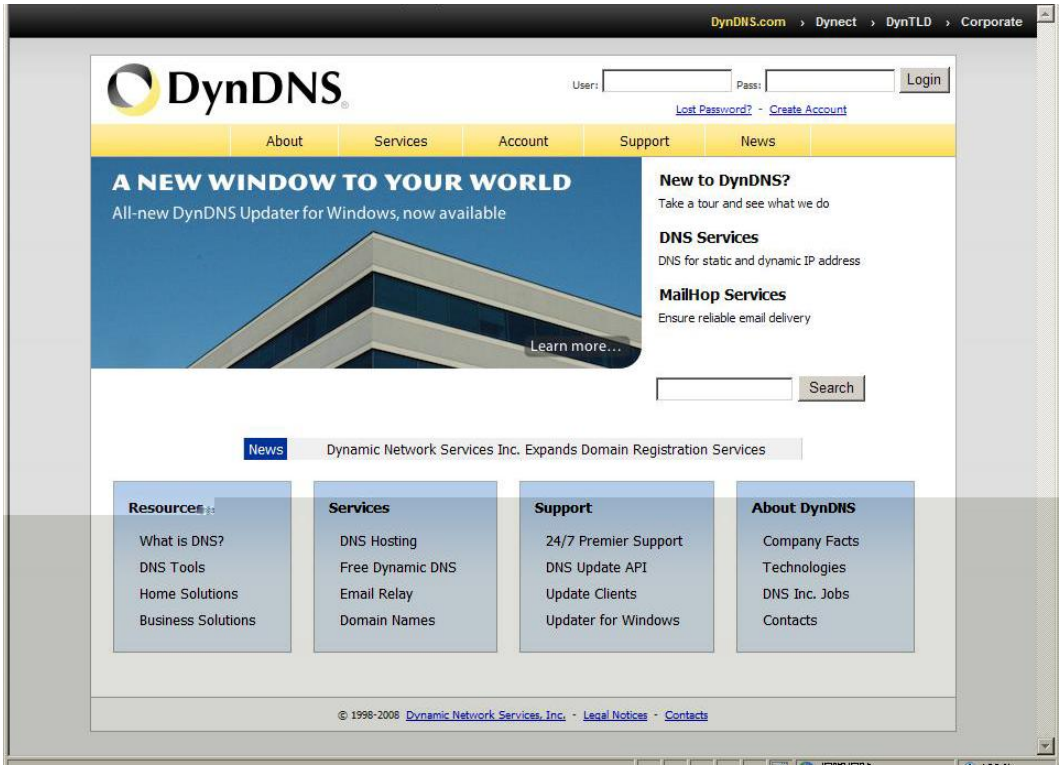
5.20 Apply for and Use a Dynamic Domain Name for Visiting IPC on Internet

If it is necessary to visit a camera on the internet, set the dynamic domain name of the camera and enable the port mapping on the corresponding router. Firstly, there must be a router with DDNS (Dynamic Domain Name Service). The following is an example of TP-Link router.

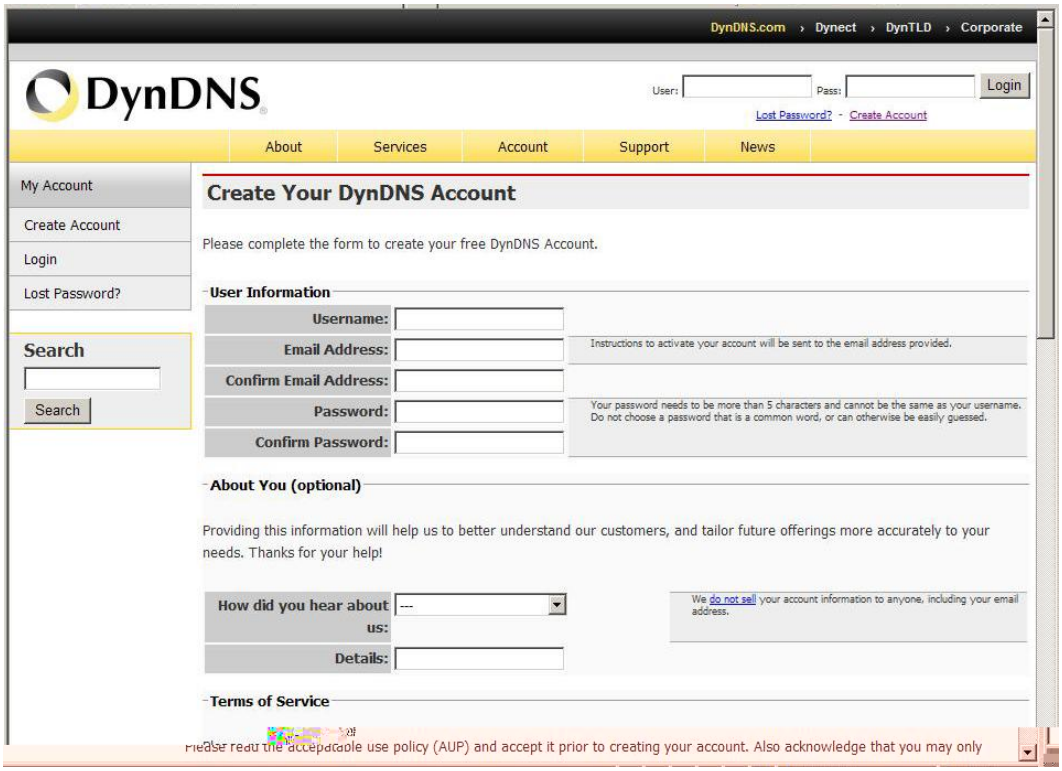
A Apply the dynamic domain username and host name for the camera.

Currently our company's IPC supports the dynamic domain name by Dyndns.org, 3322.org and Dynddns.us. Before applying the dynamic domain name, register an email address to receive the verification email. For example, the application for a Dyndns dynamic domain names is in the following procedure:

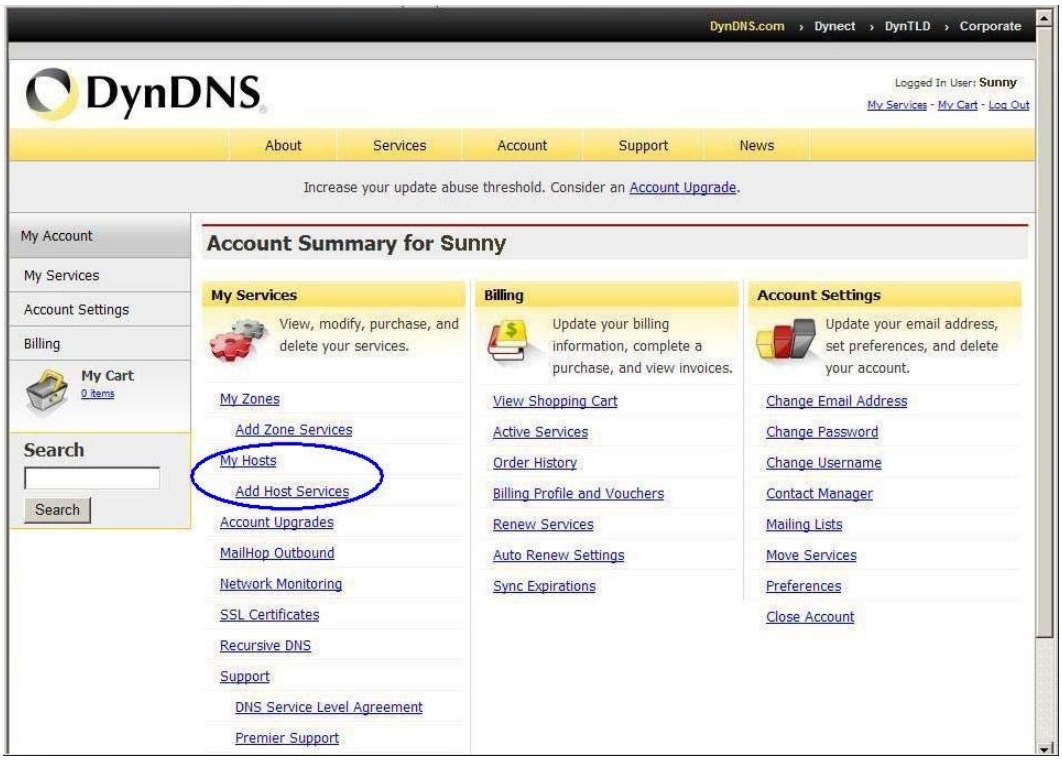
1. Log in http://www.dyndns.org, click the "**Create Account"**.



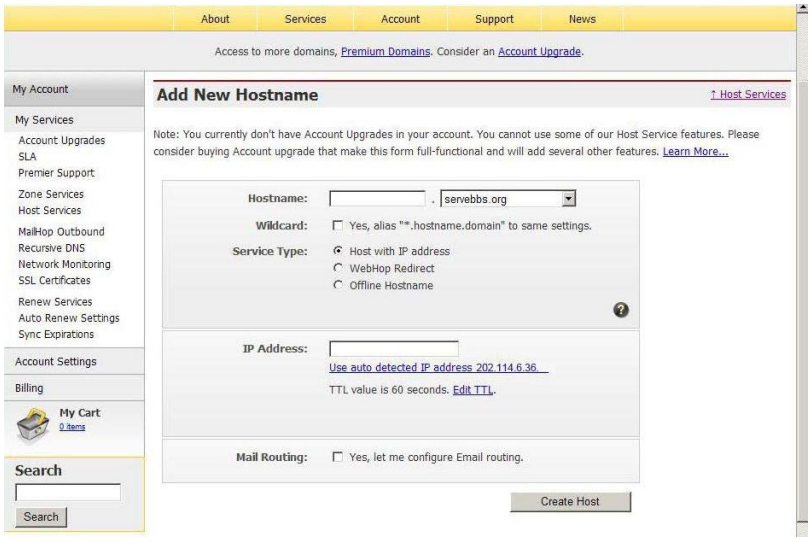
2. Input all information and follow step by step with DynDNS.



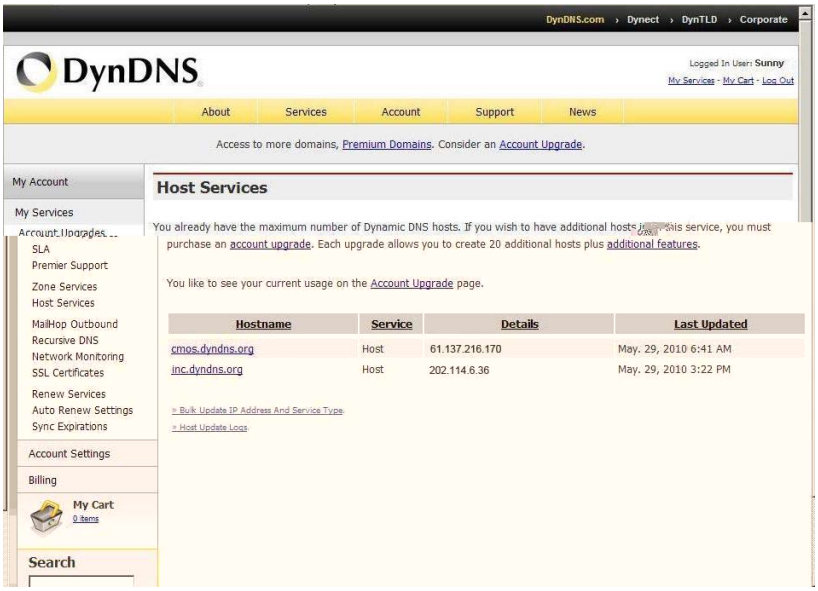
3. Log in with new account and click "**Account My Hosts Add Host Services**".



4. Type domain in the Hostname field and select sub-domain.

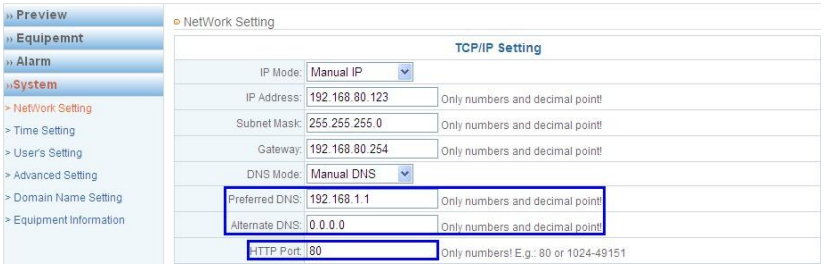


5. After typing in information, check your DDNS service.

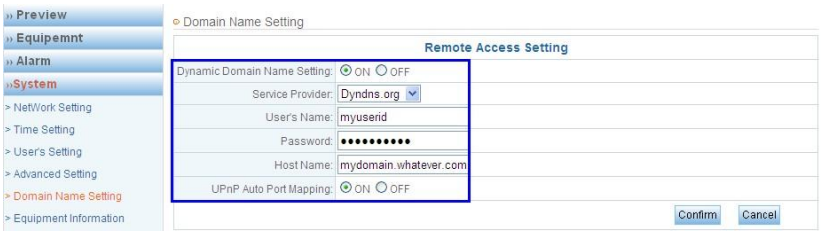


B Visit and configure the camera through browser.

1. Enter “System”--“Network Setting”, fill the correct LAN gateway and HTTP port. The DNS and port settings of the router are used here.

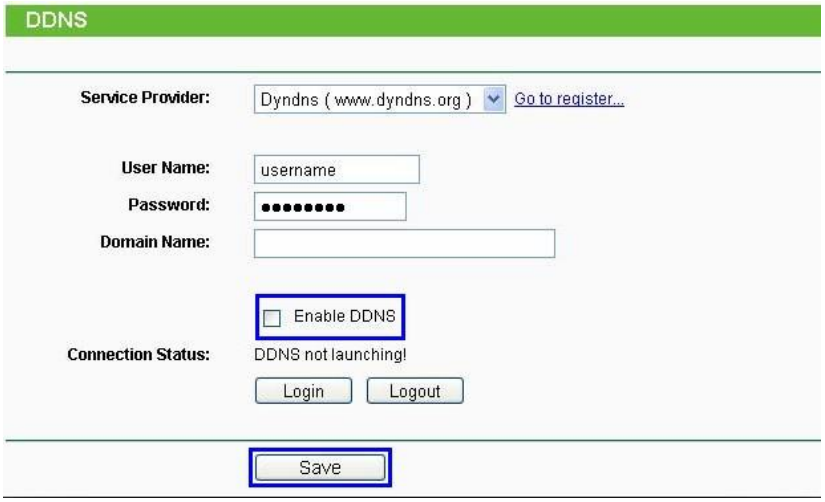


2. Enter “System”--“Domain Name Setting”, and configure the domain name of the camera.

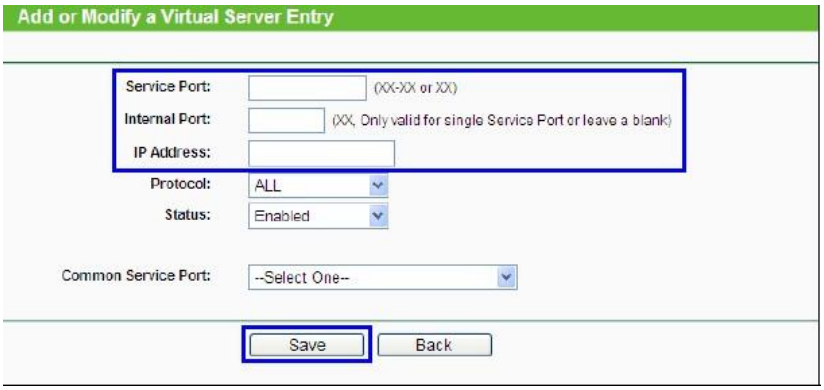


C Login and configure the router

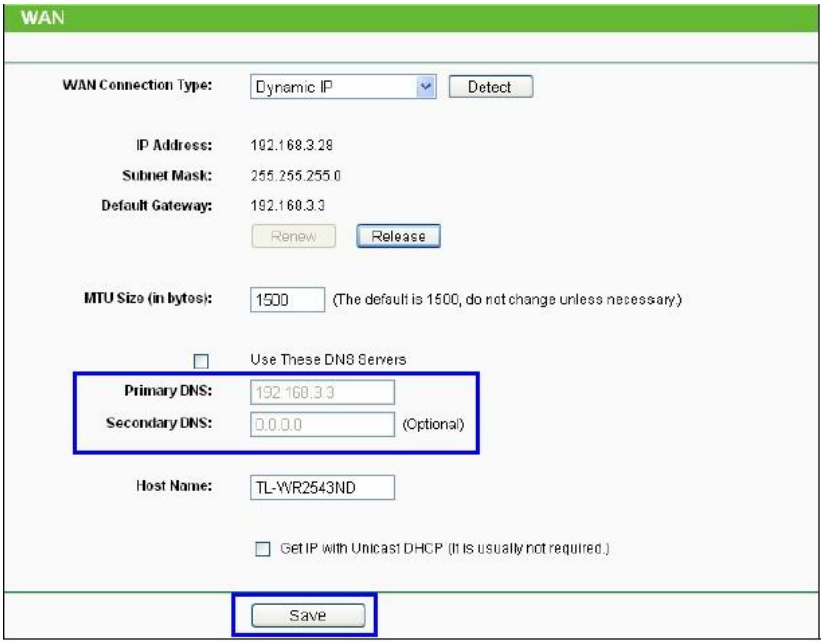
1. Enter the “Dynamic DNS” setting of the router, set and enable the DDNS.



2. Port Mapping: Enter “Forward Rules”--“Virtual Server Setting”, click “Add a new link”, add the IP address of the IPC in LAN and the corresponding port number, and enable the function. The port setting of the camera is used here.



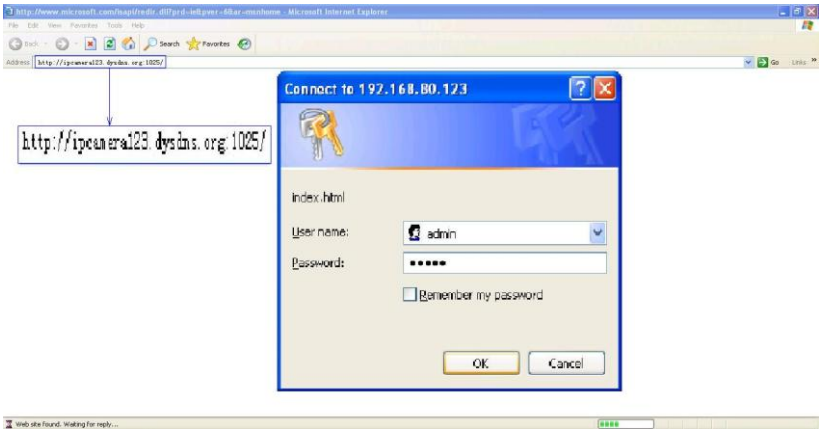
3. Configure DNS address: Enter “Network Parameters”--“WAN Port Setting” and manually set the DNS address of the router. The DNS setting of the camera is used here.



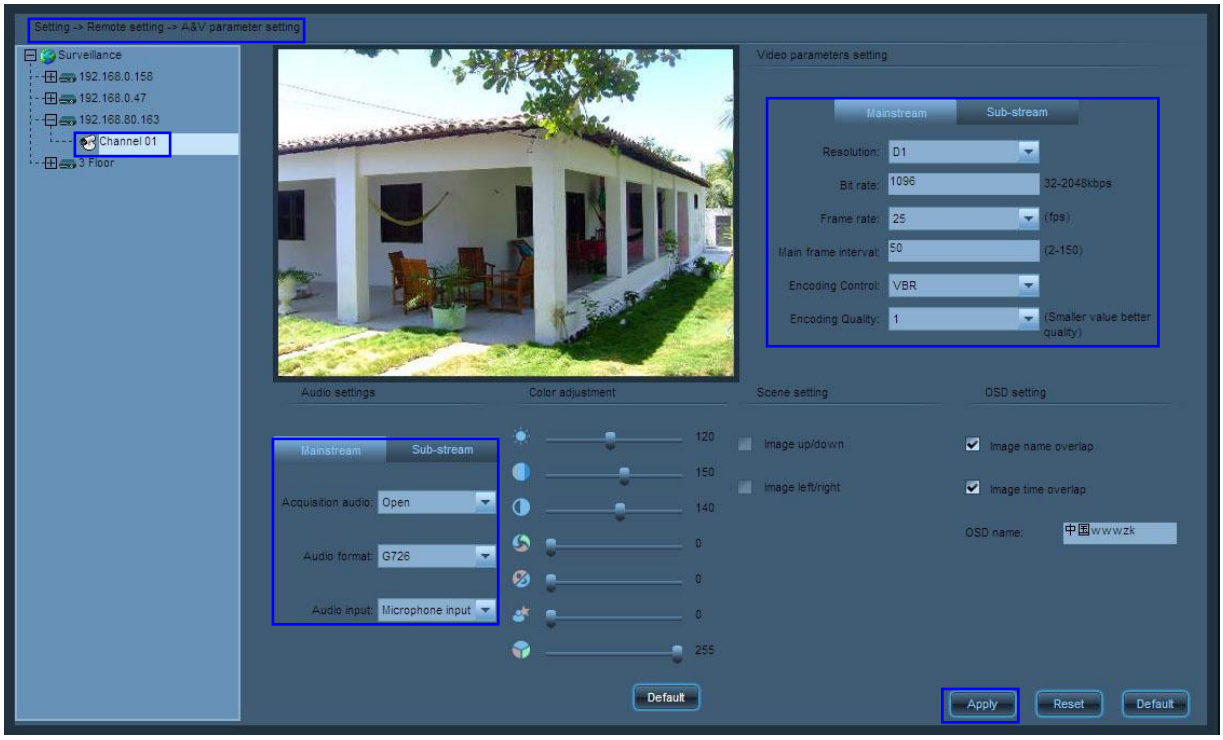
D Use the domain name to check whether can visit the IP camera on internet.

Choose **Set** > **Device management** > **Search**. Click to choose a parent area, manually add this IP camera to the system. Click Test, then the "Connection succeeded" dialog window pops up.

Or type in “http://domain name: port number” in the address bar of browser, e.g. “http://ipcamera123.dysdns.org:1025”, and log in the system to browse the videos of the IPC.



5.21 Set Audio and Video Parameters Appropriate for Your Network



1 Choose Set > Remote settings > A&V parameter settings.

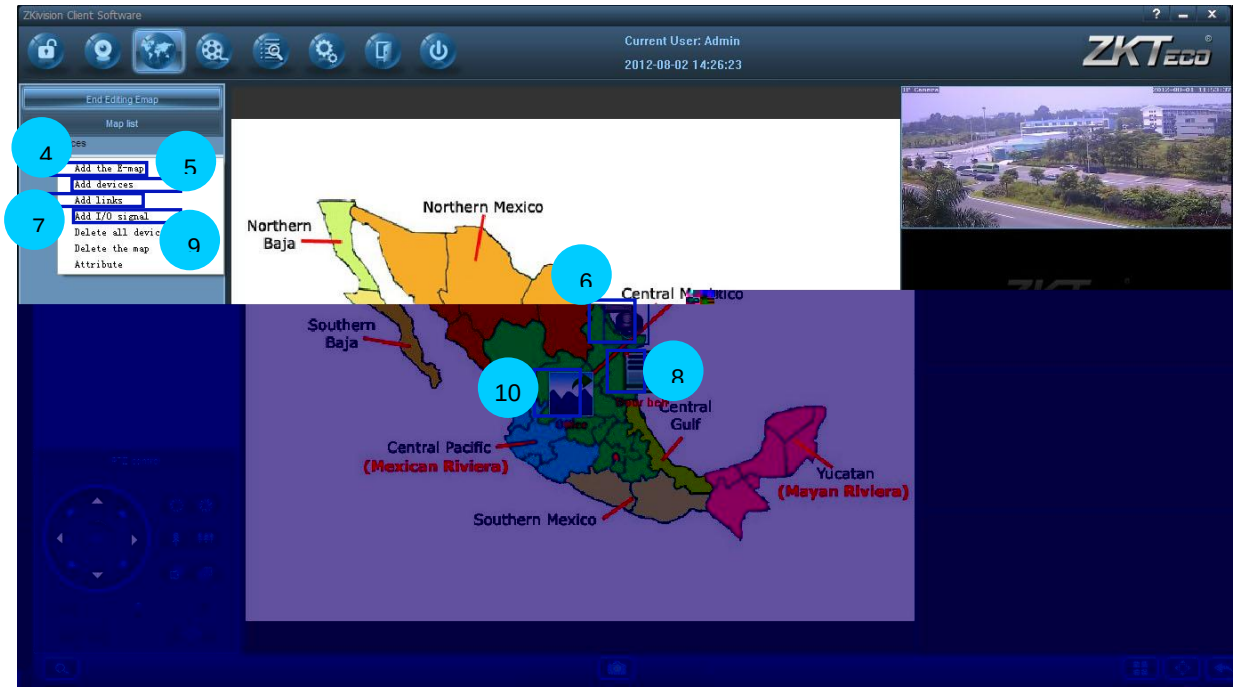
2 Double-click a camera channel in the device list.

3 Set audio and video parameters. See 4.6.3 Audio and Video Parameters settings.

4 Click

to apply your settings.

5.22 How to Set E-map



1. Access the **E-Map** tag page.
2. Click **Edit E-Map** to access the map editing page.
3. Click the right mouse button on the map list and choose **Add** to add e-maps.

4. If you want to add multi-level scenario maps, first choose the upper level map on the map list, and right click to choose **Add E-map**. Then set the attributes for the map that you want to add.
5. If you want to deploy a camera on the map, first choose the map on the map list, and right click to choose **Add devices**. Then set the attributes for the device that you want to add.
6. Or you can right click the map on the map display window and choose **Add devices**.
7. Drag the mouse cursor to the device icon, press the left button and drag the device icon to where you want to place it.
8. If you want to add link on the map, first choose the map on the map list, and right click to choose **Add link**. Then set the attributes for the link that you want to add.

   Or you can right click the map on the map display window and choose **Add link**.
9. Drag the mouse cursor to the link icon, press the left button and drag the link icon to where you want to place it.
10. If you want to add input-output signals on the map, first choose the map on the map list, and right click to choose **Add I/O Signals**. Then set the attributes for the input-output signals that you want to add
11. Or you can right click the map on the map display window and choose **Add I/O Signals**.
12. Drag the mouse cursor to the signal icon, press the left button and drag the signal icon to where you want to place it.
13. Click **End Editing E-map** to exit map editing.
14. After the device is armed, when an external alarm signal comes in, the input signal icon will blink. After confirming the alarm on site, the security guard can right click the icon to confirm the alarm and then the icon will stop blinking.
15. You can access the linked e-map by clicking the link icon on the map.
16. You can double-click the device icon or drag the icon to the video play window to play the video in real time.
17. You can control the output by double-clicking the output signal icon on the map.

Notes:

1. The alarm linkage of all signals will work only after the device (the camera) is armed. If the device is disarmed, it cannot produce alarm linkage. For arming the device, see Enable Arming.

2. For setting signal alarm linkage, see Set Alarm Linkage.

3. For associating the IP camera with the access controller, see 5.23 How to Set and Apply the Association of the IP Camera with the Access Controller.

5.23 How to Set and Apply the Association of the IP Camera with the Access Controller

1. Set the association of the camera with the access controller.

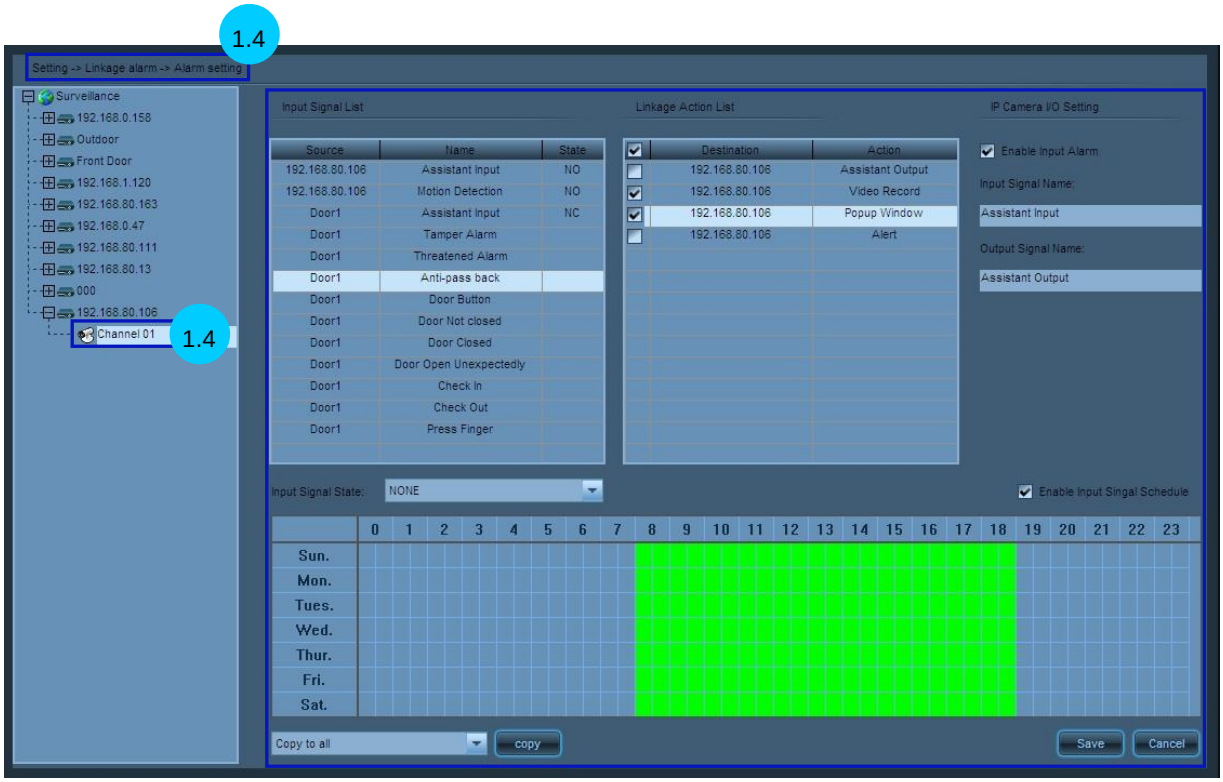
   1.1 Access the **Settings** --> **Linkage Alarm** --> **Access Management** interface.

   1.2 Manually add the access controller to the system. When adding succeeds, the access controller will be displayed on the access controller list.(You can click **Test** to check whether the access controller is successfully connected)

   1.3 Double-click the camera channel to be associated with on the device tree to connect the camera.

   1.4 Tick the access controller to be associated with on the access controller list. You may select more than one access controller.

   1.5 Click **Save** to save the setting and finish associating the camera with the access controller.



2. Set door controller event alarm linkage.

   2.1 Access the **Setup** --> **Alarm Linkage** --> **Alarm Setup** page.

   2.2 Double-click the camera associated with the door controller. When the connection is successful, set the alarm linkage items for door controller events. For details, see **错误!未找到引用源。错误!未找到引用源。**.

   2.3 Click Preview to start arming the device. For details, see Enable Arming.

3. You can implement video surveillance on the **Preview** page. If there is a door controller input signal, the system will perform linkage actions such as video recording and opening the door according to the alarm linkage settings.

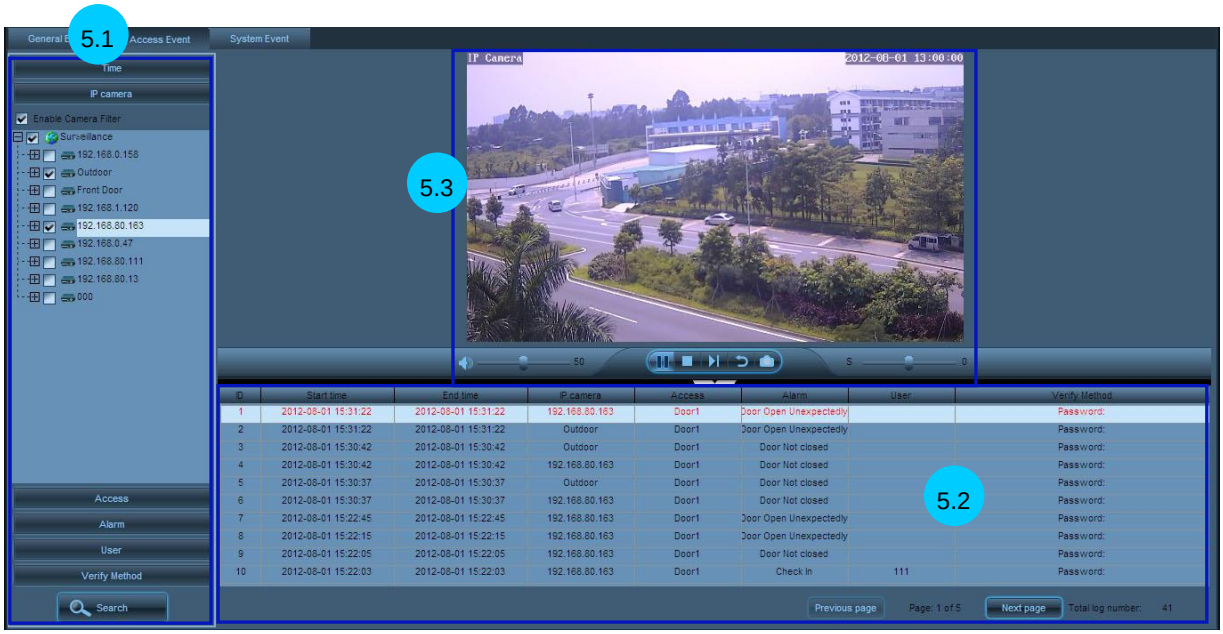
4. On the e-Map page, you can add input-output signal icons on the map and operate video surveillance and output control. For details, see **错误!未找到引用源。 错误!未找到引用源。**.

5. Search for door controller events and play back the linkage video.

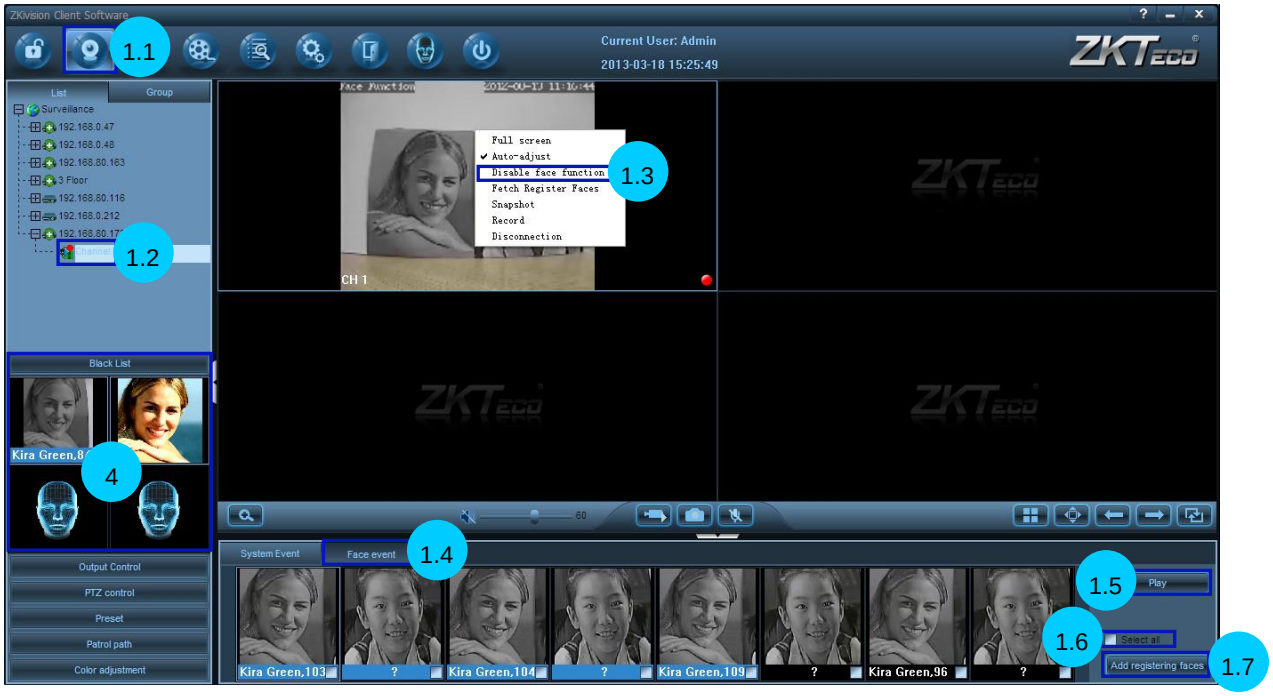
   5.1. Access the **Event Query** –**Access Events** page.

   5.2. Set query conditions, click **Search**, and the search results will be displayed on the log list.

   5.3. View the log, double-click the log with associated video (font in red), and the associated video will be played in the playback window.



5.24 How to Set and Apply Face Function



1. You can register a user in two ways: collecting a photo on line and manually importing a picture.

. Registering by Collecting a Photo online

1.1 Access the **Preview** page.

1.2 Connect the camera for which the face identification function is to be enabled.

1.3 Right click to choose **Enable Face Function** on the cell.

1.4 Switch to the **Face Event** information panel.

1.5 Click **Pause** to suspend the rolling display of the identification results on the left.

1.6 Tick the face images to be registered, or tick **Select all** to select all the images on the face event information panel.

1.7 Click **Add registering faces** to add the ticked images to the face template list on the face registration page.

1.8 Access the **Face Function—Face Registration** page.

1.11 Select the face image to be registered or click Real time face to select the real-time face image.

1.12 Click to select one picture on the list as a reference picture for the currently registered user.

1.13 Fill in the user information and set whether the user is a blacklist user or not.

1.14 Click **Register** to add the user to the system, and the registration is finished.

. Registering by Manually Importing a Picture

1.8 Access the **Face Function—Face Registration** page.

1.9 On the face template list, tick to select the location to which you want to import the picture.

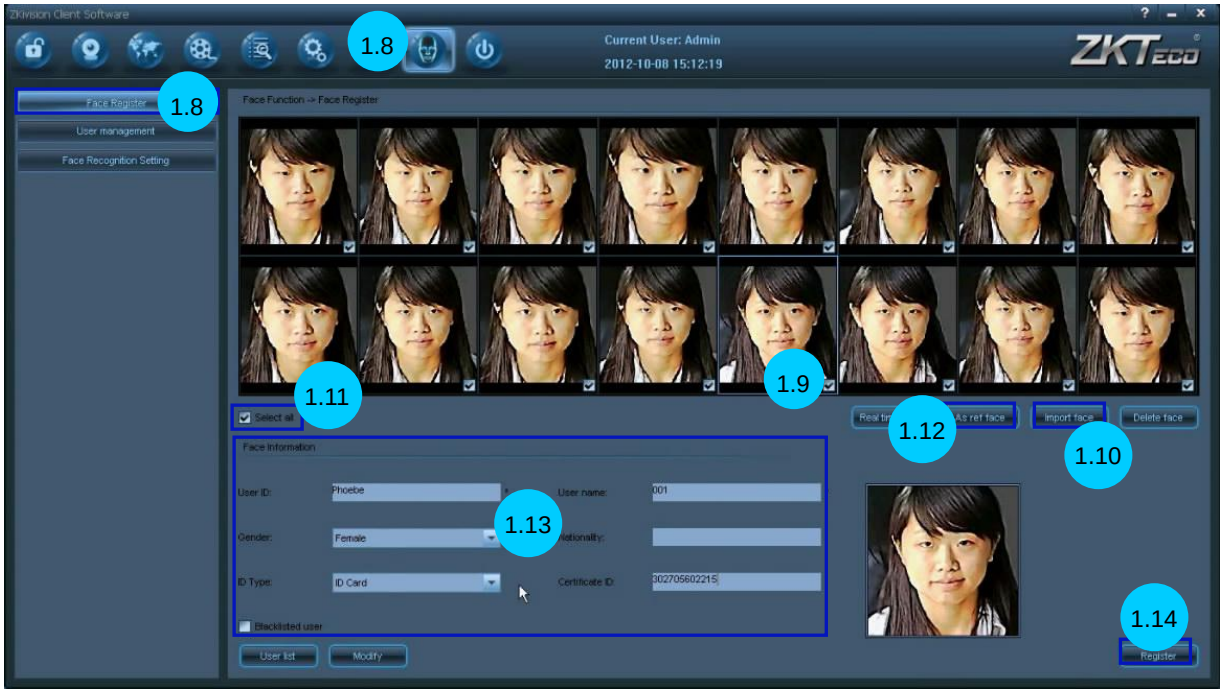
1.10 Click **Import Face** to manually import face pictures.

1.11 Tick the face images to be registered or tick **Select all** to select all the pictures on the list.

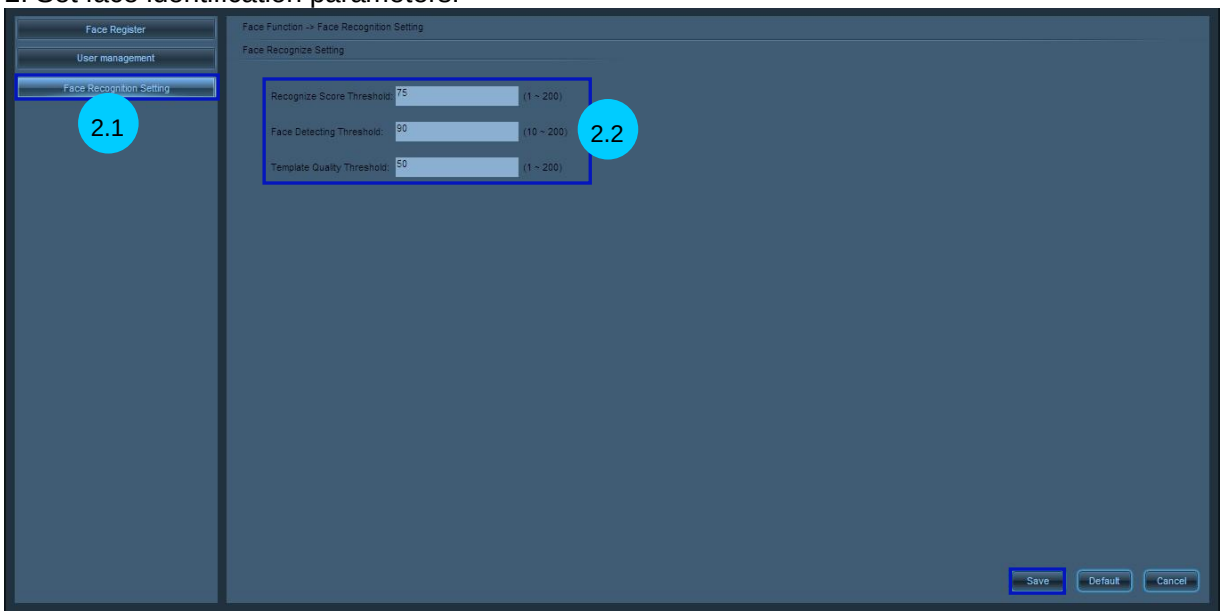
1.12 Click to select one picture on the list as a reference picture for the currently registered user.

1.13 Fill in the user information and set whether the user is a blacklist user or not.

1.14 Click **Register** to add the user to the system, and the registration is finished.



2. Set face identification parameters.



2.1 Access the **Face Identification—Parameter Settings** page

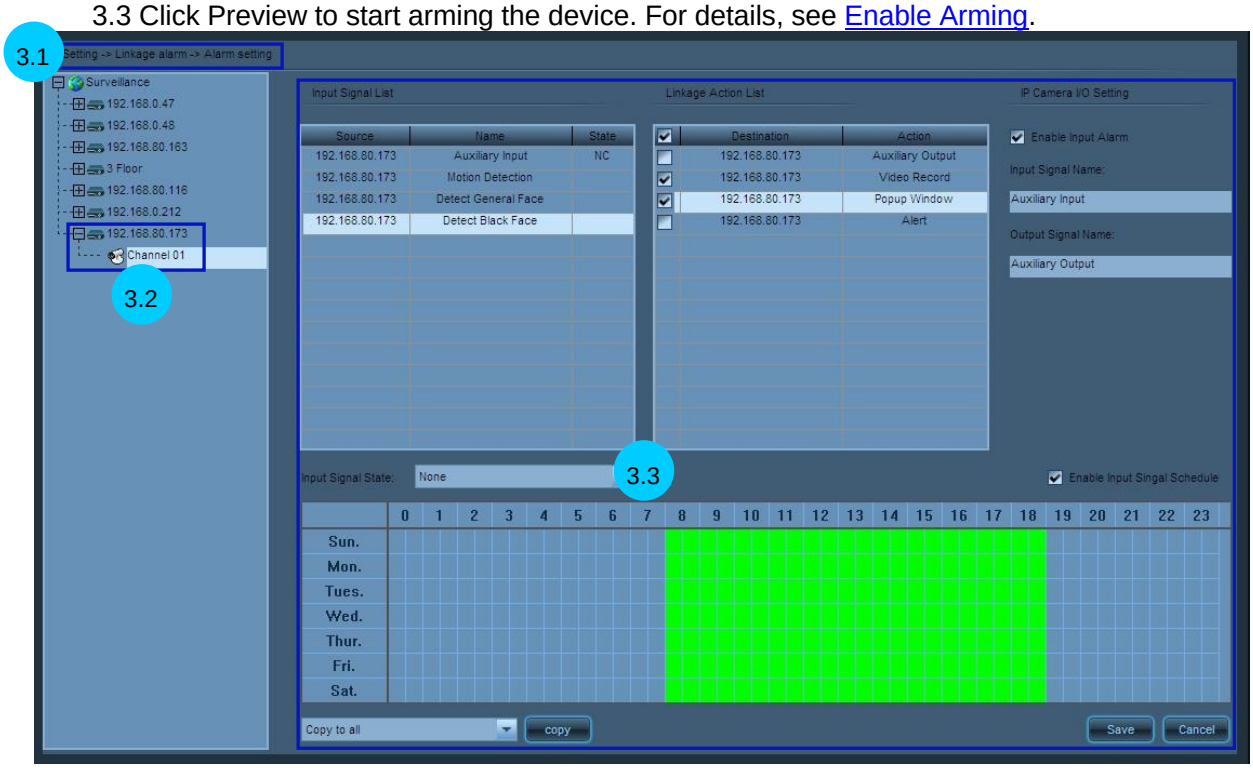
2.2 Set face identification parameters. For description of parameters, see 4.8.3Parameter Setting.

3. Set face event alarm linkage.

3.1 Access the **Setup—Alarm Settings** page.

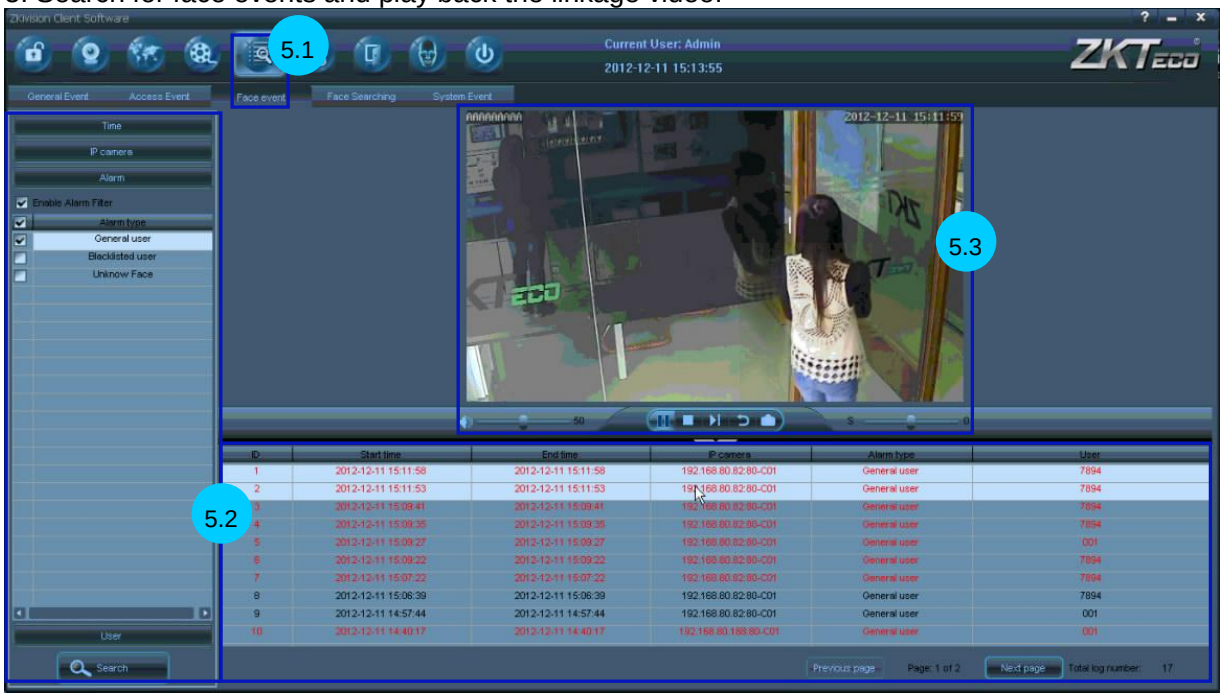
3.2 Double-click the camera for which face identification function is enabled. When the connection is successful, set alarm linkage items for face events. For details, see 5.9How to Set Alarm Linkage.

3.3 Click Preview to start arming the device. For details, see Enable Arming.



4. You can implement video surveillance on the **Preview** page. If the system identifies a face, the system will perform alarm linkage actions according to the alarm linkage settings; if it identifies a blacklist user, the user will be displayed on the **Blacklist**.

5. Search for face events and play back the linkage video.



5.1 Access the **Event Query** – **Face Events** page.

5.2 Set query conditions, click **Search,** and the search results will be displayed on the log list.

5.3 View the log, double-click the log with associated video (font in red), and the associated video will be played in the playback window.

6. You can also search for and play back face videos.

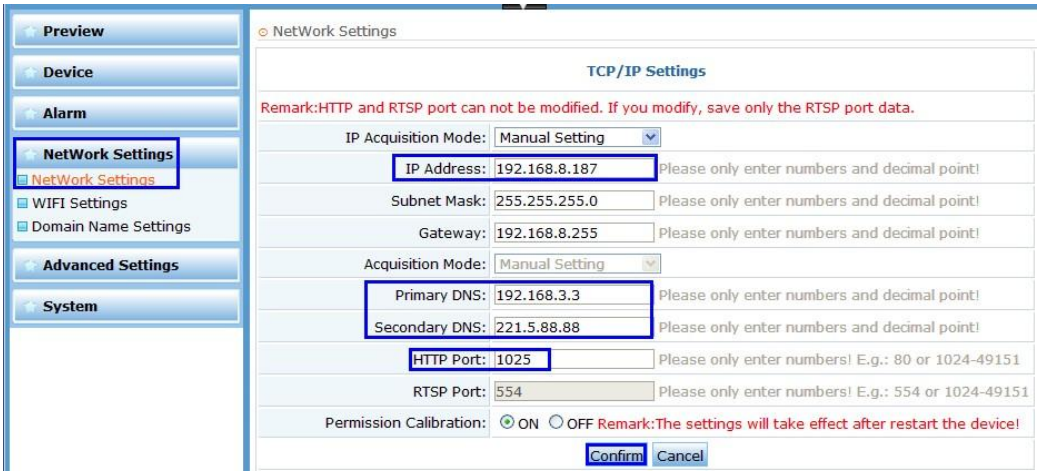
6.1 Choose **Event Search** > **Face Searching**.

6.2 Specify query conditions and click **Search**.

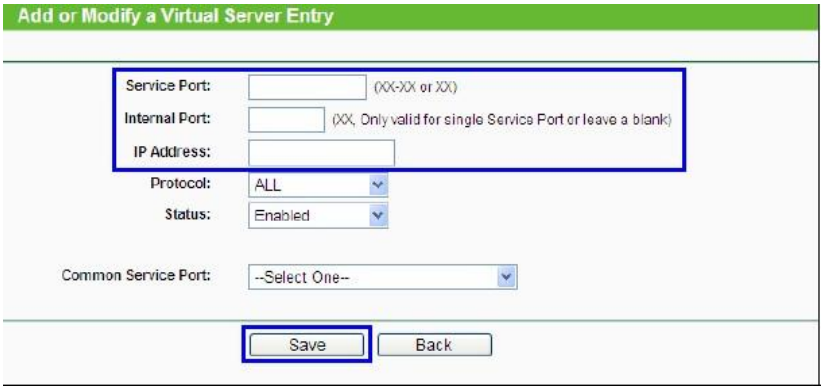
6.3 Double-click a face image that is searched out. Then, the playback window plays the video associated with the face image.

Note: The system will extract a face template from the ticked picture on the template list and use it as the face template for the currently registered user. When you register a user, it is

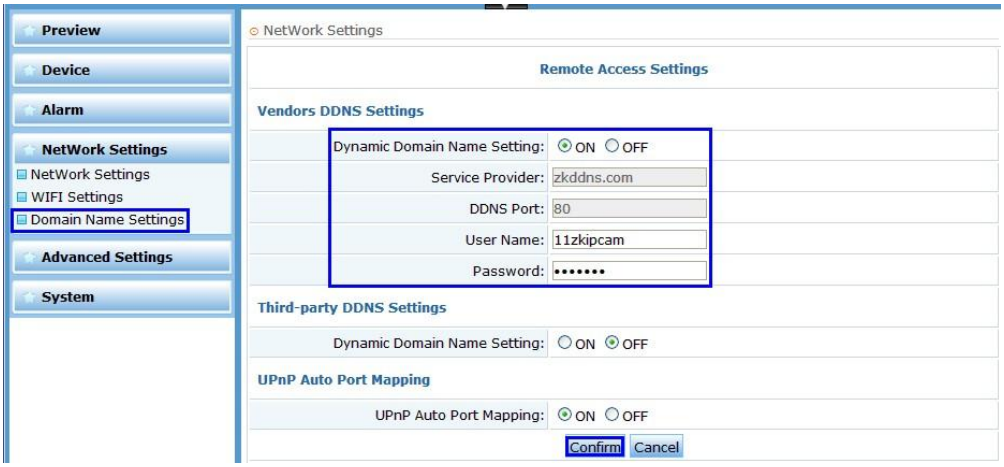
A Use a browser to access a device. Open the **Network Settings** page. Set the DNS address of the device (this DNS address must be consistent with the one set on the router) and the HTTP port.



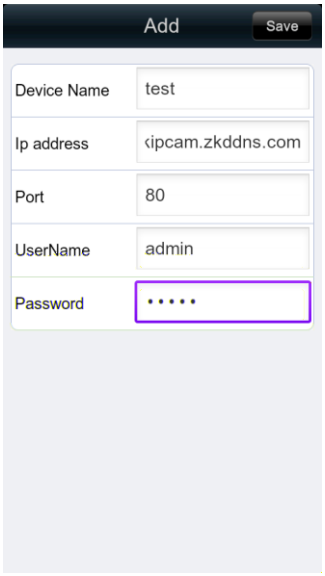
B Use the browser to access the router. Open the **Forward Rules** > **Virtual Server Setting** page. Click **Add a new link**. Add the IP address of the device in a LAN and the corresponding service port, and enable this function. The settings here must be consistent with the settings of the IP address and HTTP port of the device.



C Use the browser to access the device. Open the **Network Settings** > **Domain Name Settings** page. Set the Vendors DDNS.



D Use the dynamic domain name to access the device. (e.g.: access the device by a mobile phone)



6 FAQs

6.1 No Image at Preview

Possible causes:

1 Incorrect device information such as the user name and password

2 MAC address conflicts between the camera and other devices

3 Too many users connected to the camera

4 Camera hardware failure

Solutions:

1 Choose **Set** > **Device management** > **Search**. Correct the device information such as the user name and password. Click **Test** until the connection succeeds.

2 Choose **Set** > **Device management** > **Search**. Click

and then

. On the search list, check whether the camera has a MAC address that conflicts with that other devices. If such a conflict exists, consult professionals or our technical support team.

3 Access to the camera through browser. Choose **System** > **Device information** to view the number of connected videos (a camera can support a maximum of four users to browse main stream videos at the same time or ten users to browse secondary stream videos at the same time). When the maximum number of video connections is reached, wait for a few minutes until the number falls below the maximum, and then try connecting again. After these operations, you can properly play the videos.

4 Contact our commercial personnel or technical support team.

6.2 No Audio at Preview

Possible causes:

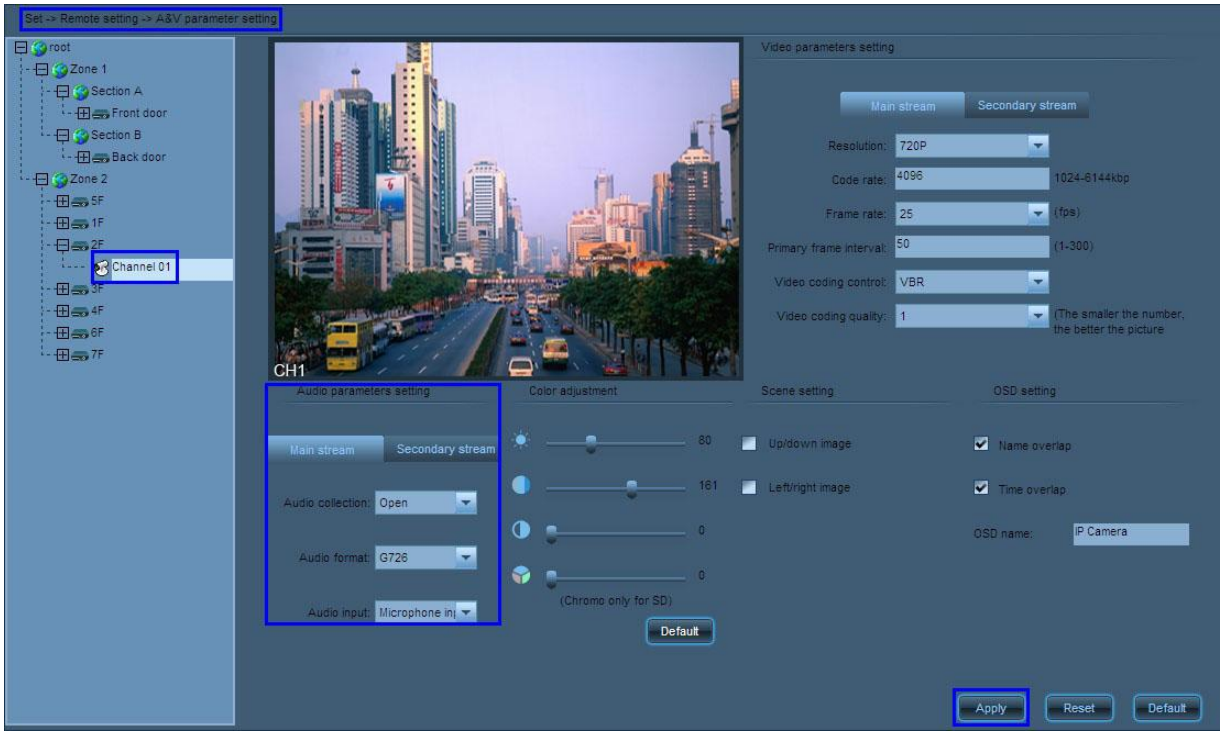
1 No external audio collecting devices

2 Incorrect audio/video parameter settings

Solutions:

1 Connect an audio collecting device to the camera before connecting the camera to your PC to make sure that you can properly hear the audio.

2 Choose Set > Remote settings > A&V parameter settings. On the A&V parameter settings interface, set Audio collection to Open.



6.3 No Audio in Playback

Possible cause: The audio collection function is disabled when you videotape the images.

6.4 Failure to Enable Manual Recording

Possible causes:

1 Equipment disconnected

2 Disk space insufficient

Solutions:

1 Choose **Set** > **Device management** > **Search**. Click **Test** until the connection succeeds.

2 Choose **Set** > **Local settings** > **Storage management**. Tick off **Disk full cover**. Then the video files of the earliest date will be deleted when all disk space is less than the preset reclaimable space. Or you can enter the video storage path and manually delete unwanted videos to free up the disk space.

6.5 Failure to Disable Videotaping at Preview

Possible causes:

The device performs scheduled videotaping within a specified period.

The device performs linkage alarm videotaping within a specified period.

6.6 Pan-Tilt Abnormality

Abnormal conditions:

1 Lighting out of order

2 Wiper out of order

3 Pan-tilt out of order

(1) The device has no built-in pan-tilt.

(2) The device cannot work with a pan-tilt.

Solutions:

1 Check whether any external light fixtures are connected. This function applies when there are external fixtures.

2 Check whether any external wipers are connected. This function applies when there are external wipers.

3 (1) An external pan-tilt is required.

(2) Choose **Set** > **Remote Settings** > **PTZ Parameter Settings**. Set PTZ parameters such as the address, baud rate, and stop bit on the **PTZ Parameter Settings** interface. Ensure that these parameter settings are consistent with the PTZ settings.

6.7 Failure to Implement Audio Intercom

Possible cause: The device has no external audio input devices or no headsets or microphones are connected to the PC.

Solution: Connect an external audio input device to the device and connect a microphone headset to the PC.

6.8 Failure to Play Back Videos Displayed on the Timeline Panel After a Video Search

Possible cause: The video files are missing or the user has manually deleted the video files within a specified period.

6.9 Failure to Search for Video Files

Possible cause: The video file for this time period has been deleted or has been overwritten by circulating video recording.

6.10 Failure to Set the Motion Detection Area

Possible causes:

1 When **Resolution** is set to **QCIF**, the system does not respond your request for motion detection area settings.

2 If you log in to the front-end device with a non-admin account, the system does not respond your request for motion detection area settings.

Solutions:

1 Choose **Settings** > **Remote Settings** > **A&V Parameter Settings**. In the Video parameters settings pane, set the resolutions on the Main stream and Secondary stream tab pages separately.

2 Switch to log in to the front-end device as a superuser, and then set the motion detection area.

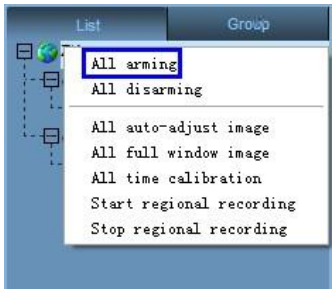
6.11 Failure to Achieve Alarm Linkage

Possible cause: The **Arming** function is not enabled.

Solutions:

1 On the equipment list of the preview interface, right-click a desired area and choose **All arming** from the shortcut menu. Then the guard function is enabled for all devices in this area.

2 On the equipment list of the preview interface, right-click a desired device and choose **Arming** from the shortcut menu. Then the guard function is enabled for this device in this area.



6.12 Failure to Display the Alarm Window After Enabling Arming

Possible causes:

1 The **Pop up video window** option is not selected.

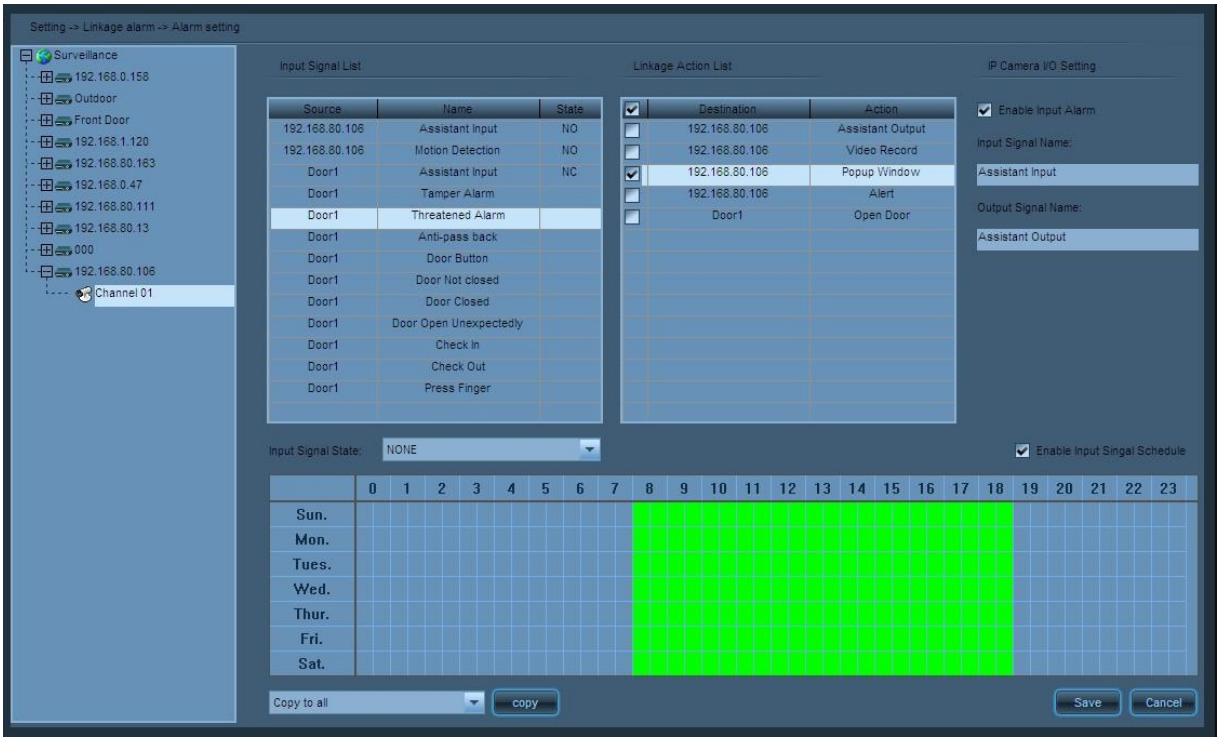
2 No alarm signals are detected.

3 When **Resolution** is set to **QCIF**, the system does not support motion detection alarms.

4 If you log in to the system as a non-admin user (namely, a superuser), the system does not support motion detection alarms.

Solutions:

1 Choose **Settings** > **Linkage Alarm** > **Alarm Settings**. In the Alarm linkage pane, select **Pop up Window**.



2 Check the motion detection area and input alarm settings. For relevant motion detection settings, see 5.7 Set Motion Detection. For relevant external alarm inputs, see Set Alarm Linkage.

3 Choose Set > Remote settings > A&V parameter settings. In the Video parameters settings pane, set the resolutions on the Main stream and Secondary stream tab pages separately.

4 Switch to log in to the system as a superuser.

6.13 Video Image Exception at Preview

Possible causes:

1 Incorrect video parameter settings

2 Unstable camera connection

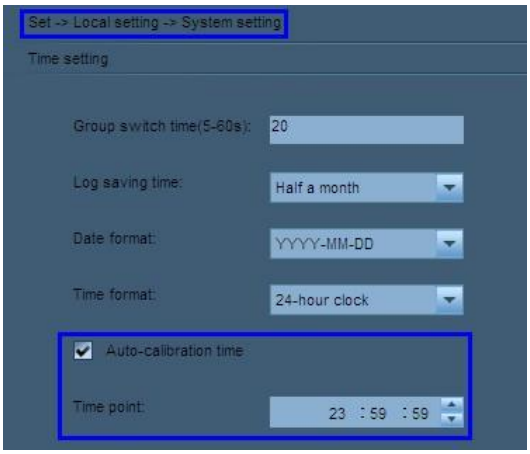
Solutions:

1 Choose **Set** > **Remote settings** > **A&V parameter settings**. In the **Video parameters settings** pane, set parameters on the **Main stream** and **Secondary stream** tab pages according to actual bandwidth.

2 Check to ensure that the camera is properly connected.

6.14 Incorrect System Time

Solution: Choose **Set** > **Local settings** > **System settings**. Tick off **Auto-calibration time** and set the calibration time. When the calibration time arrives, the system automatically calibrates the time.



7 Others

1 To monitor the devices in a centralized manner, enable **Task Manager** to check the CPU usage. The CPU may function improperly with more than 80% resources occupied. See 5.21 Set Audio and Video Parameters Appropriate for Your Network to decrease the device bit rate, or lower the resolution.

2 Check the manufacturer website regularly for the latest software version.

3 Know the factory default parameters of cameras produced by our company.

IP Acquisition Mode	Manual settings
IP Address	192.168.1.88
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
HTTP Interface	80
UPnP	Disabled
DNS Acquisition Mode	Manual settings
Primary DNS	192.168.1.1
Motion Detection	Disabled
Alarm Input	Disabled
Wireless	Disabled
User name	admin
Password	admin