KBVISION
member of ADH Group

KBiVMS Client User's Manual

Version 6.08

Table of Contents

Welcome

Thank you for using our KBiVMS Client!

This user's manual is designed to be a reference tool for operation of your system.

Here you can find detailed operation information about KBiVMS Client.

Cybersecurity Statement and Recommendations

Cybersecurity Statement

- You are responsible for the risks resulting from connecting your product to the internet, including but not limited to, cyber-attacks, hacking attacks, computer viruses and malware, etc. Please protect your data and personal information by taking necessary actions, such as changing the default password and using a strong combination, changing your password periodically, keeping your firmware up-to-date, etc. KBVision is not responsible for any dysfunction, information leakage or other problems caused by failure to take necessary precautions to secure your devices. We will provide product maintenance services.
- To the extent not prohibited by applicable laws, KBVision and its employees, licensees, and

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for KBVision systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on KBiVMS:

Those using KBiVMS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for KBiVMS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:
Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:
Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:
If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:
Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:
Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network
The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

For latest information about KBVision, the cybersecurity statement and recommendations, please visit www.kbvision.vn

1 Overview

KBiVMS Client Platform is software for user to manage KBiVMS Client and it has the following functions:

- Multi-device, multi-channel real time monitoring and record playback
- Local snapshot, record mark and etc. of playback record
- E-map function allows user to position the device at any time.
- Audio intercom allows client to communicate with front-end device and broadcast.
- Video intercom, remote unlock and talk
- Easy management and Control TV Wall display synchronously.
- Customize monitoring plan and supports multi-channel/window video tour.
- Alarm activation with alarm video
- Mouse simulating rocker to control PTZ
- Fisheye and speed dome link
- Access control, alarm controller arm/disarm
- Behavior analysis, people count, heat map.

KBiVMS Client platform support download, installation and usage of 32bit/64bit Client. KBiVMS Client has four types:

- C/S Client
- B/S Client, see Ch 22.
- Android Client
- iOS Client

2 Configure System

2.1 Initialization Config

Before you use the platform, please follow the steps listed below to set the initialization information.

2.1.1 Startup

Connect the power supply and startup.

The first time you startup, system will format the hard disk automatic, may take you about 10 minutes, please be patient.

Note: KBiVMS Client Built-in one 1T corporate hard disk, if system start abnormal, need to check whether the hard disk is loose.

2.1.2 Set System IP Address

Before you use KBiVMS Client platform, please set system IP address.

KBiVMS Client default IP address:

- port 1：192.168.1.108
- port 2：192.168.2.108
- port 3：192.168.3.108
- port 4：192.168.4.108

2.1.3 Get IP Address

Step 1. If you forget KBiVMS Client platform IP, you can find it back via two methods:

- KBiVMS Client can view LCD panel of server, SV500, software server can connect to monitor.
- Use ConfigTool to search.

The latest version of ConfigTool can be downloaded from KBVision official website.

Open ConfigTool, you can see Figure 2-1.

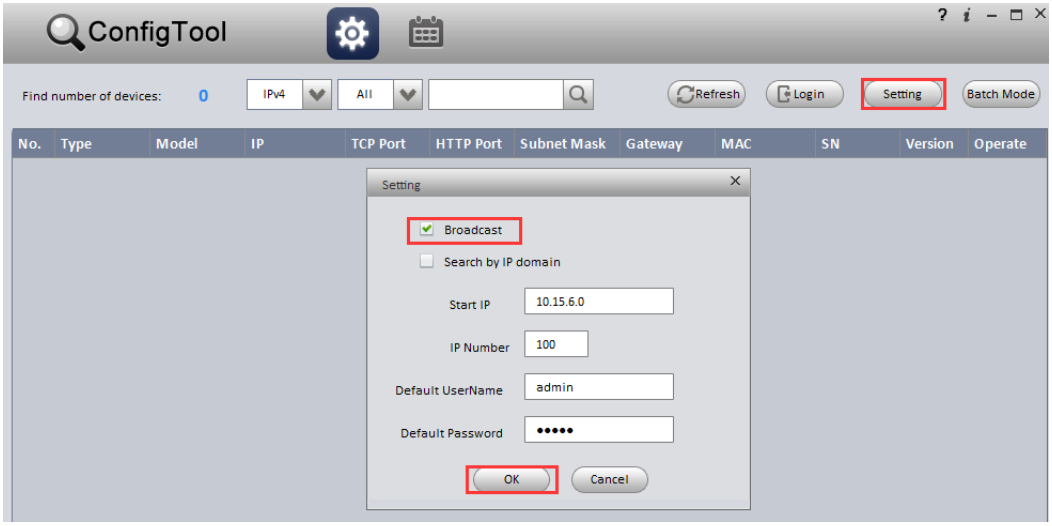


Figure 2-1

Step 2. Click Refresh, it will list out device list and details including KBiVMS Client server within LAN.

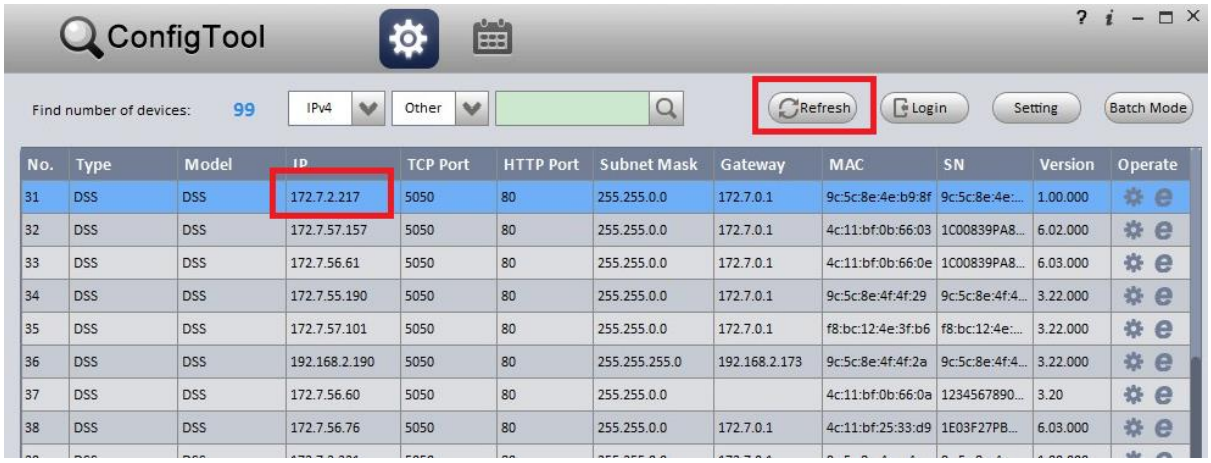


Figure 2-2

2.2 Quick Guide

Step 1. Please input http://ip/config on the IE and then click Enter button. System pops up the following dialogue box. See Figure 2-3.

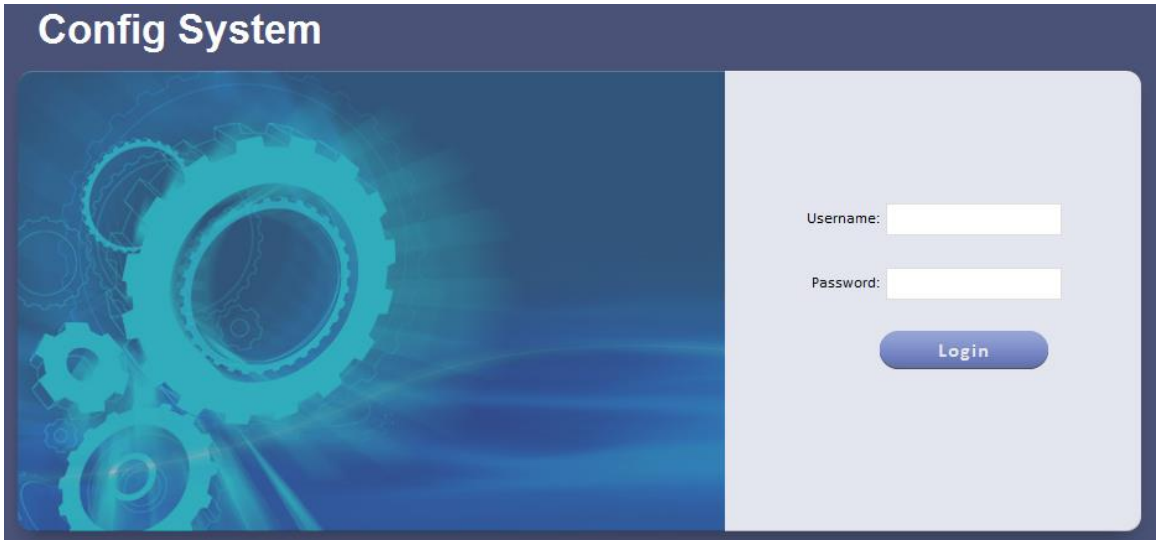


Figure 2-3

Step 2. Please input user name and password. System default user name is **admin** and password is **123456.**

Note: If you login in by using initial password, system pops up a password modification box, asking you to change password. You can login system only after you change password. Password can contains number, letter, underline and other symbols.

Step 3. Click Login. The system shows Quick Guide interface, see Figure 2-4.

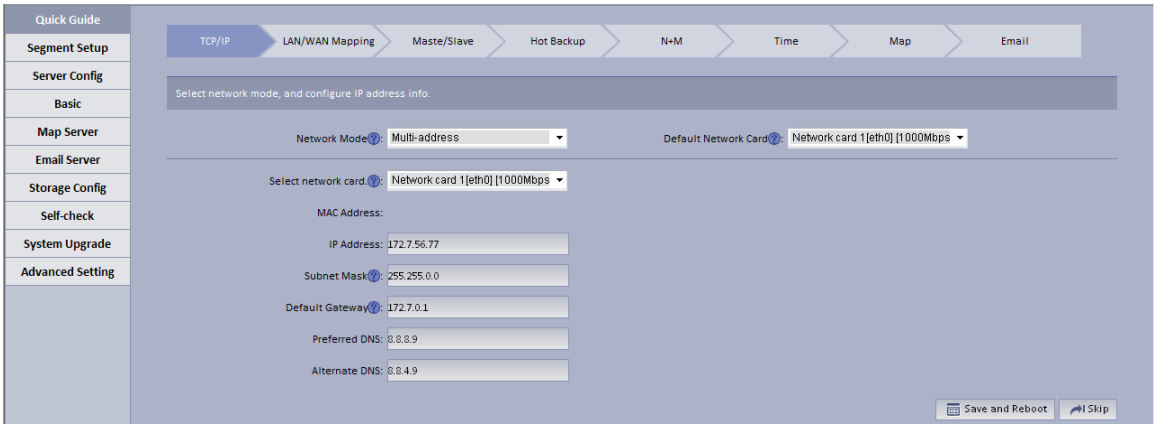


Figure 2-4

Step 4. Configure TCP/IP.

1. Select appropriate network mode, and set IP address, subnet mask, gateway and etc. for different Ethernet cards.
2. Click Save and Reboot. If you do not want to configure, please click Skip. If you click Skip, the system will operate according to current IP and perform next config.

Note:

- Multi-address mode：known as multi-Ethernet card mode, you have more than one segment can configure with different segments; this mode requires higher network reliability.
  Such as: configure hot spare, which requires Ethernet 2 with hot spare server beat IP; as well as being used in plan with ISCSI extended storage. While, under planning of Ethernet port: Ethernet port 1 as server communication, port 2 as reserved, port 3 and 4 as ISCSI storage.
- Load balancing: known as Ethernet card binding mode, suitable for condition that requiring higher network band width, and used in plan of high performance demand or non-ISCSI storage.
- Fault-tolerant mode：（master-spare strategy）Only one device is in active status, and when one device goes down, the another immediately switches from hot spare to master device. MAC address is visible from outside. Viewing from outside, bond MAC address is exclusive in order to switch disorder. This mode only provides fault tolerant function; so this algorithm may improve usability of network connection, but its resource utilization is low as there is only one port in working status and when there are N network ports, its resource utilization is 1/N.
- Advanced binding: used to let user select quantity of Ethernet card to be bound when the Ethernet card mode is load balancing, in order to achieve stream forwarding over 1K by one Ethernet card; for example: 2 IP bindings, plus 2 multi-addresses, this server can have 3 IPs, and bound IP bandwidth is 2K, the other 2 are 1K, suitable for pure stream forwarding scene (storage not recommended).

Step 5. LAN/WAN mapping config.

1. Configure IP address, router address and each type of server port. Click next to each server, and you can view definition of related server.

Note:

If the system access WAN via router LAN/WAN mapping, then you need to fill in WAN address and port info of related Ethernet port. If no port is mapping, then you can main port config. Address of router is the address accessed by WAN.

See Figure 2-5.

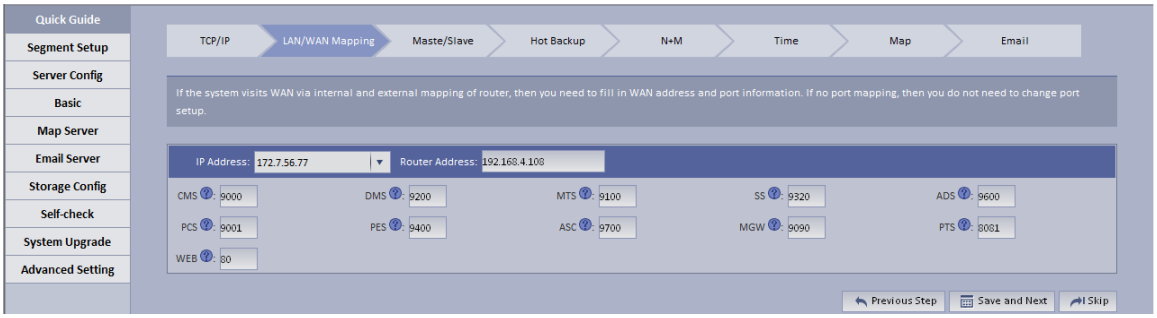


Figure 2-5

2. Click Save and Next. If you do not configure, then click Skip. See Figure 2-6.

Figure 2-6

Step 6. Master/slave server selection.

1. By default, the system uses master server, and if you want to set it to slave server, please select Slave.

Note:

Server in a distribute system has two types: master and slave. There is only one master server and the rest are slave servers. Master server is the only controller which manage data, device and dispatch other distribution work. In the system, only master server will enable database （mysql server）, tomcat and CMS and etc. Role of distribute server includes device input+forward+storage, only enable corresponding function services, such as DMS, MTS, SS, ARS, PCPS and etc. The entire system has only one port to user which is master server IP address.

2. Click Save and Next. If you do not configure, click Skip.

Step 7. Hot spare.

1. If the system configures hot spare, when master server goes down, hot spare server will replace master server and continue working, to main system stability. When master server recovers, the system will switch back to master server, see Figure 2-7.

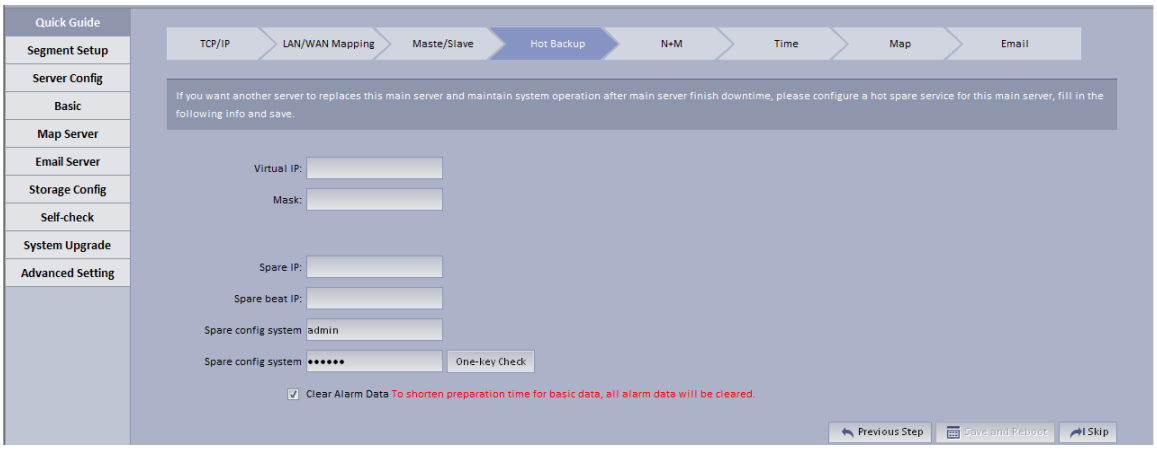


Figure 2-7

Parameter	Note
Virtual IP	An IP not used in network segment and is configured with virtual IP. No matter where master server or hot spare server works, they all can be accessed via virtual IP without distinguishing master and hot spare servers.
Mask	Mask info.
Spare IP	Hot spare server IP address, known as address of port 1 of hot spare server.
Spare beat IP	• Hot spare server beat IP address, known as address of port 2 of hot spare server.
Spare config system user (password)	Hot spare server CONFIG SYSTEM account and password.
Clear Alarm Data	After hot spare is configured, the system will auto sync master data with spare. If master alarm information is too much which causing long time for sync, it will clear alarm data on master server when hot spare is enabled by default.

2. Before the system starts hot spare, first make sure the master server and hot spare server are correctly configured physically and port 2 of both master and hot spare servers are connected via Ethernet cable within the same segment. Port 1 of both master and hot spare servers is configured to have different accessible addresses within the same segment. See Figure 2-8.

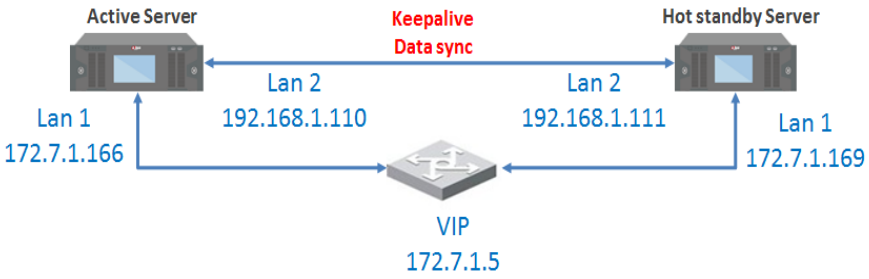


Figure 2-8

Note: During hot spare, we do not recommend to use master and hot spare servers as central storage.

3. Set virtual IP, spare IP and etc., click Save and Next.

Step 8. N+M.

The system shows “N+M” interface, see Figure 2-9.N+M backup is for mechanism of slave server in a distribute. After a distribute server add redundant server, if this slave server goes down and cannot reboot in 60s, CMS will allocate device and business of this slave server to redundant server, meantime it will save record on disk of redundant server.

1. First login config system of the slave server you want to configure, in distribute, select Slave, see Figure 2-9.

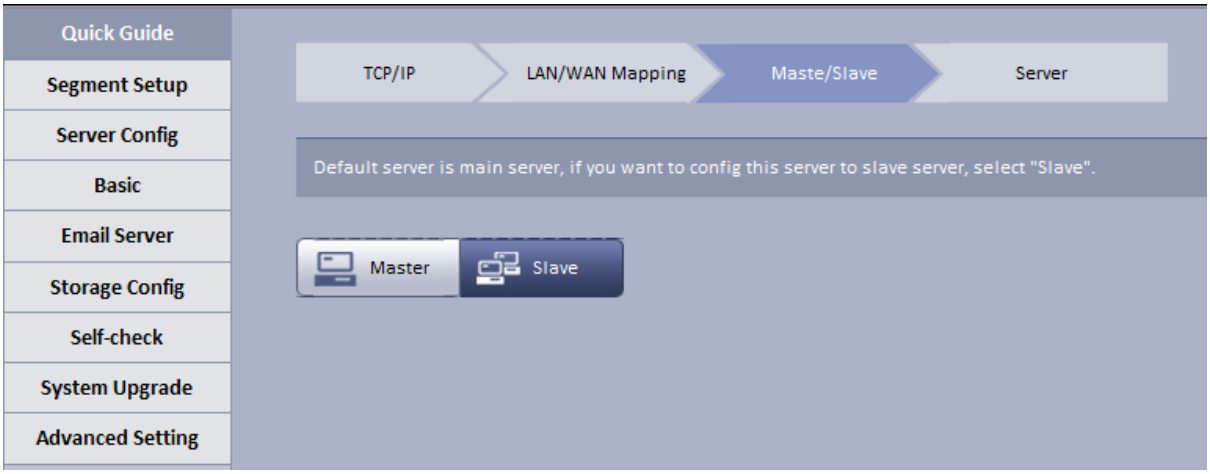


Figure 2-9

2. Fill in master server IP, see Figure 2-10.

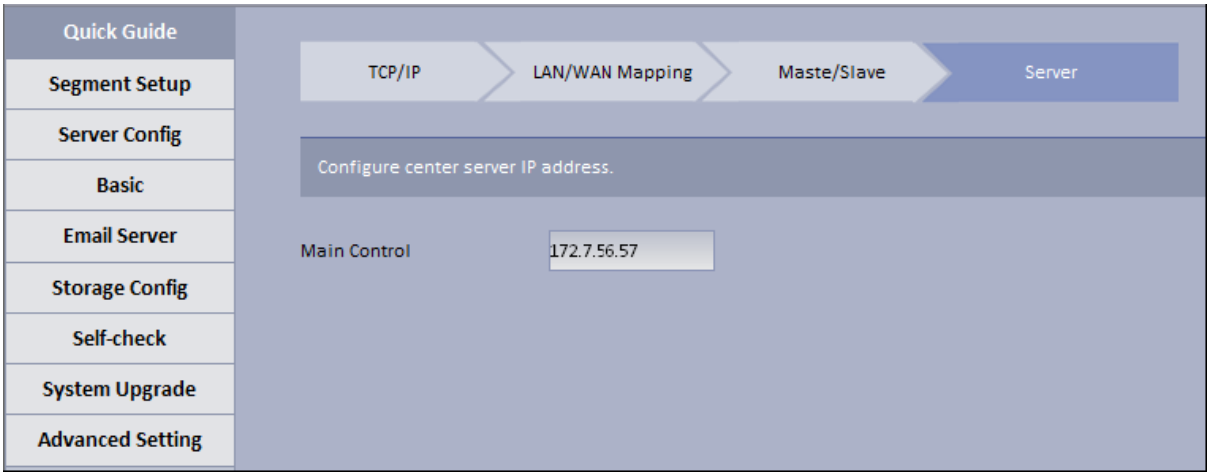


Figure 2-10

3. Login master server config system, in N+M interface, you can see all slave servers, see Figure 2-11.

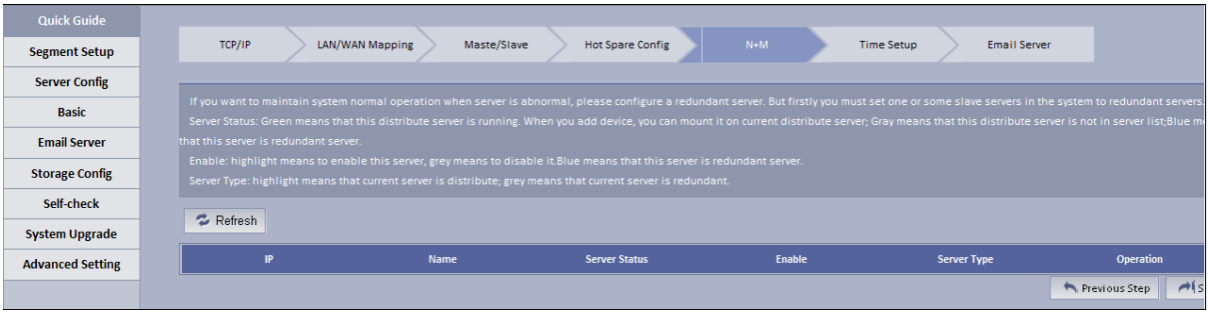


Figure 2-11

4. Select corresponding slave server, in “Enable” column, enable button, and after server reboots, Server Status shows which means that slave server can be used as normal, see Figure 2-12.

Figure 2-12

5. If you want to configure redundant server for slave server, select slave server you want to configure it to redundant server. In Enable column enable button, and in Server Type column modify server type to be non redundant server type.

6. Select one slave server, click button, the system pops up edit box, see Figure 2-13.

Select redundant server on the left, click Add to add it to the right, click OK.

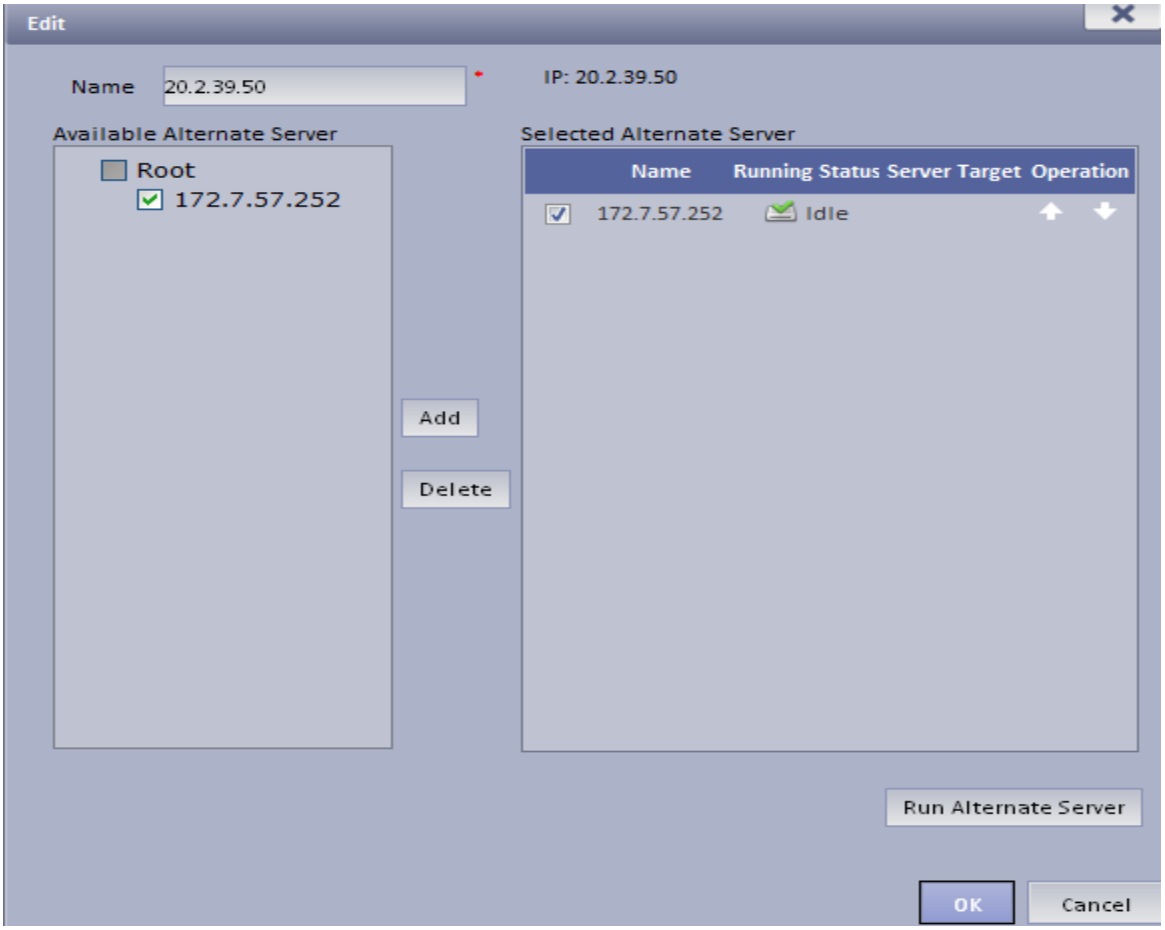


Figure 2-13

After set redundant server, you can see Figure 2-14.

Figure 2-14

When distribute server goes down, redundant server will replace it in 60s and you may view status of redundant server.

Click  button next to redundant server, to view info in home server mounted by redundant server and current operation status. See Figure 2-15.

Figure 2-15

Note:

- Server status: green means that distribute server is running, when you add device, you can mount it on current distribute server; grey means that the distribute server is not used, when you add device, this distribute will not be shown in server list; blue means that this server is redundant.
- Enable: highlight means that server is enabled. Grey means disabled.
- Server Type: highlight means that it is distribute server for now; grey means that it is redundant server for now.

Note:

- During N+M backup, certain data will be lost depending on size of stream.
- When redundant server is working, the record originally saved on slave server can be searched but cannot be played, but if original slave server has been recovered from abnormality but the device has not been moved back, those records on original distribute server can also be played.
- When distribute server recovers, you can manually move back device to original slave server. In Figure 2-16, click the red button, now you can search and playback record in both slave server and redundant server.

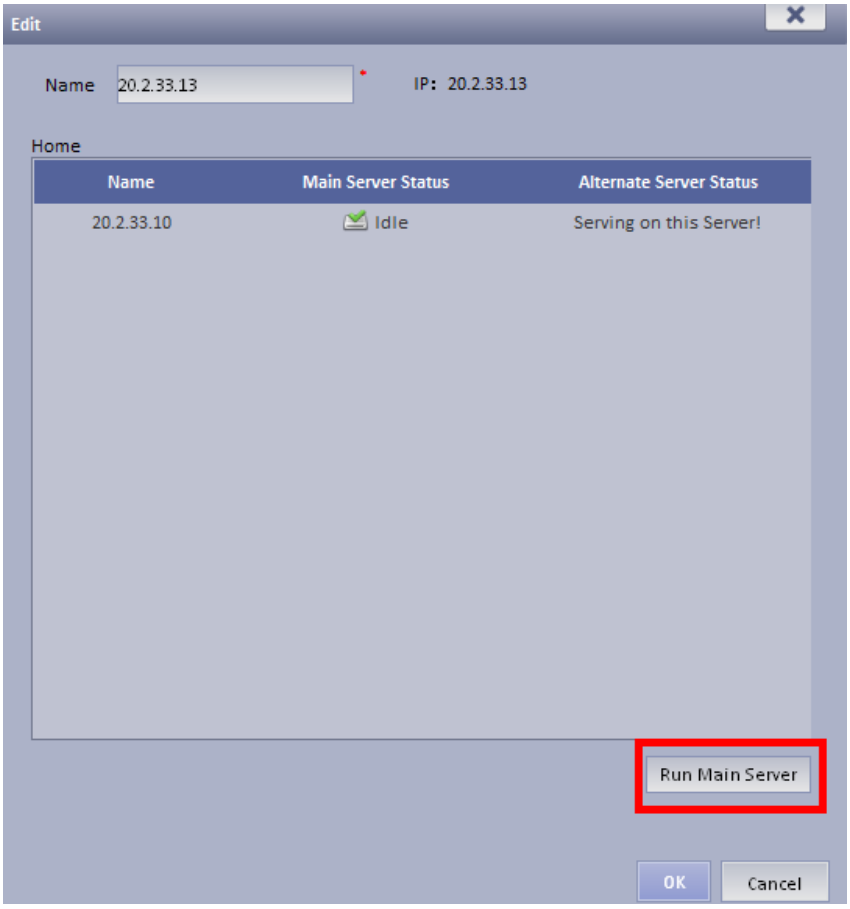


Figure 2-16

7. Click Save and Next, if not set, click Skip.

Step 9. Set Time. The system shows Time interface, see Figure 2-17.

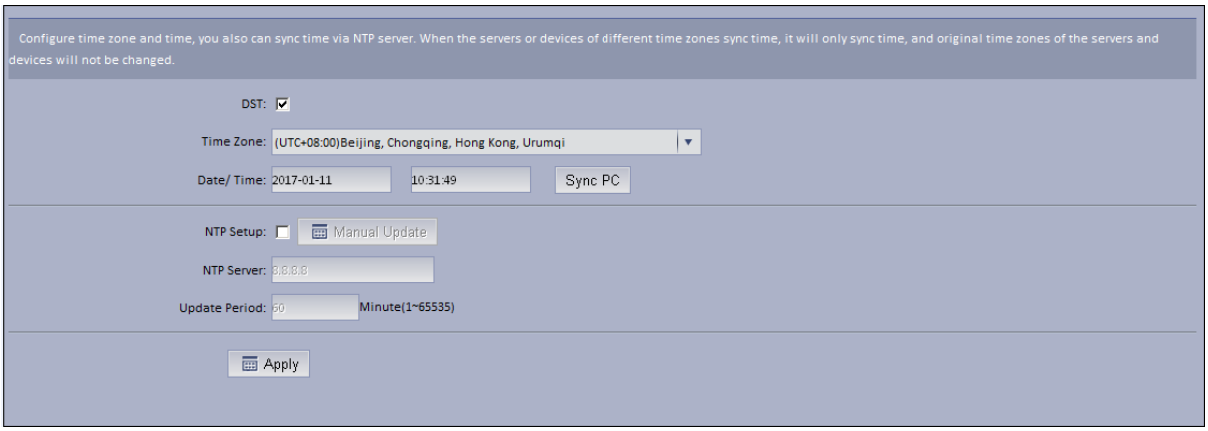


Figure 2-17

1. Check DST, then select time zone of DST. If you do not check DST, then you do not need to check time zone.
2. Configure time zone and time, default is UTC+08:00, it can quickly sync with PC.

   If there is NTP server, you may configure to ensure accuracy of KBiVMS Client time. Non-central servers do not have NTP function.
3. Click Save and Next, if you do not configure, please click Skip.

Note:

When NTP sync with server, scene are not the same.

NTP sync may target server at a specific server (has NTP function) to sync time, while only can remain syncing with one server.

Sync time on Manager-end, it sync serves of entire group related to this server.

Non-central servers do not have sync time function.

Hot spare, master/slave server time config, you can check NTP sync, enter identical server IP, see below:

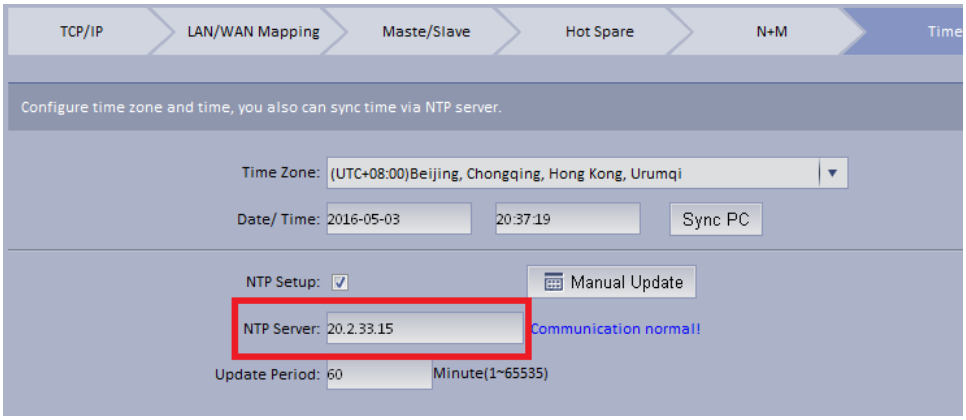


Figure 2-18

Step 10. Configure Email.

The system shows Email interface.

Support yahoo, gmail, hotmail. For yahoo and gmail mail box, it only supports SSL encryption, and for hotmail mail box, it only supports TLS encryption.

Configure email server. When alarm occurs, this email server may send email to specific user.

Parameter	Note
SMTP Address	Fill in email server address.
Port	Fill in email port.
Username and Password	Username and password of email box sends out email.
Sender Mail Address	● Email address.
Encryption Type	There are 3 types, 1. No encryption, 2. TLS encryption, 3. SSL encryption. Method of encryption can be used for inter-organization email server.
Test Recipient	Enter email address of a test receiver, click Mail Test. So he/she can receive a test email to check the email setup.

Step 11. Fill in all contents, click OK. Reboot server.

2.3 Segment

TCP/IP config, LAN/MAP mapping are same as config in wizard, skipped here.

2.4 Server

Click Server Config on the left, see Figure 2-19.

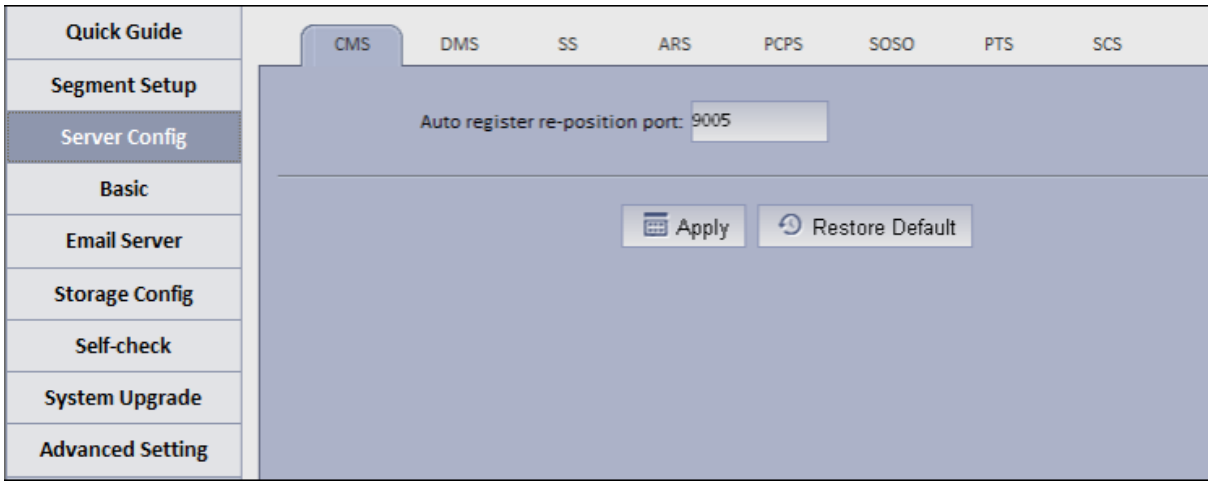


Figure 2-19

- CMS:

This function is mainly for registration of CMS device mount on N+M back.

Auto register device: need to fill in server IP and CMS port (by default ARS server port is 9500), if you directly write server IP, then when the server goes down, redundant server will replace, and the Auto register device cannot register to redundant server.

To prevent this situation, when you register it, fill in hot spare VIP for server IP, and fill in port as port of CMS (9500 by default).

By auto registering Auto register device, when server has redundant server replacement, it can be used as normal.

Note: This function requires specific device (please refer to the device).

- DMS

  Set Reset listening port, it is 80 be default.

- SS

Max locked record ratio: record lock function, currently only support to lock center record; after record is locked at client, when storage disk is full and overwrites, it skip locked record and overwrite non-locked record.

Default ratio is 10, and user can customize size of lock record.

- PES

  Control pos end string, end string is “Thank you!” by default.

- ARS:

Auto register server IP is server port, which is 9500 by default. It can be modified as long as identical with registration on device.

Stream type: self-adaptive, main stream and sub stream.

Self-adaptive: when access client, according to client setup, stream self adapts to change.

Main stream: when access client, do not affect by client setup, stream type shows main stream.

Sub stream: when access client, do not affect by client setup, stream type shows sub stream.

Currently stream type setup is valid for static connection auto registration device (device auto register type, please refer to device).

- PCPS

This option is for non-KBVision device connection. Pleas maintain default setup.

- SOSO server

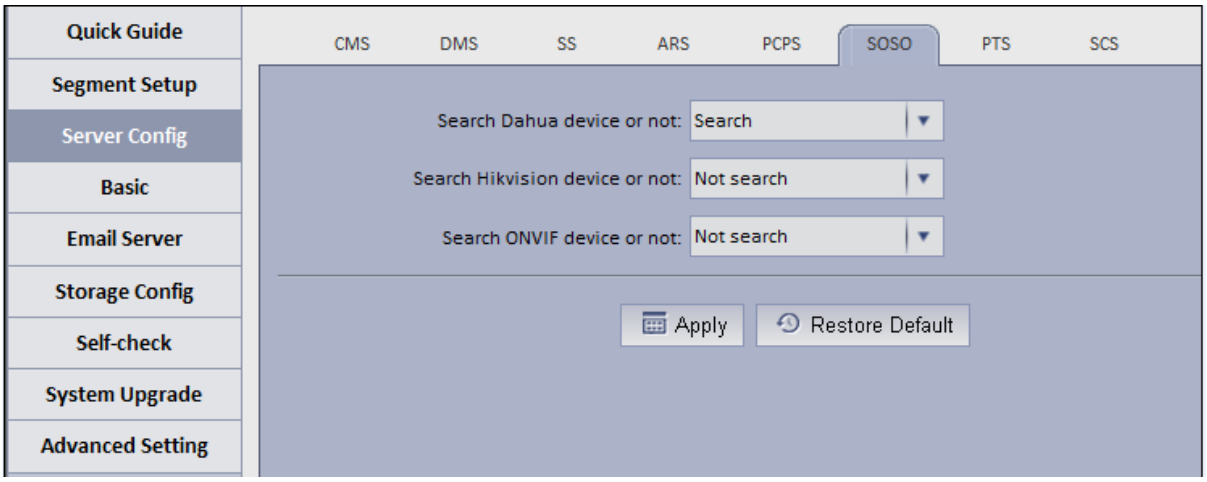


Figure 2-20

SOSO server config is to filter search content.

In KBiVMS Client Manager-end interface, add device, click auto search. See Figure 2-21.

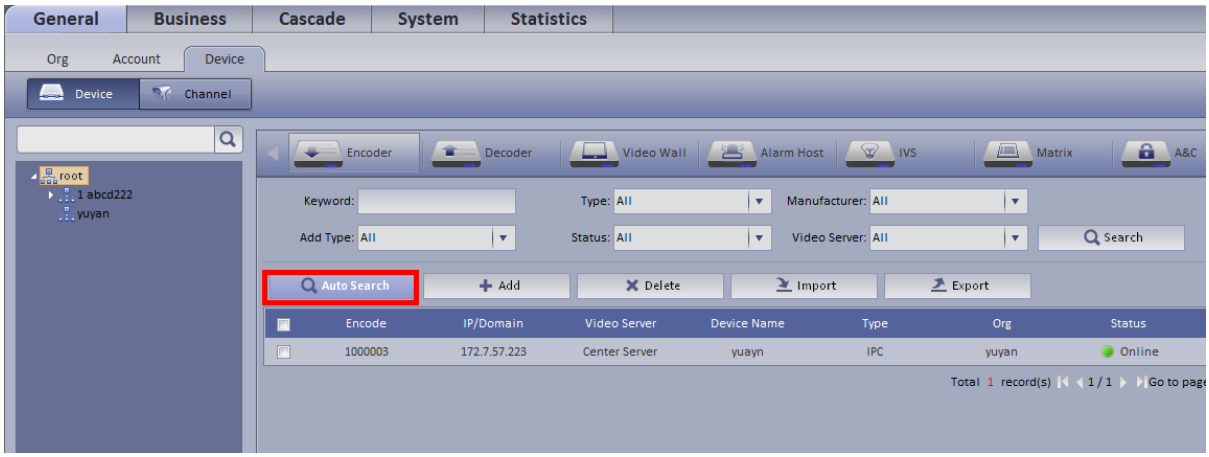


Figure 2-21

Server enables auto search of KBVision device by default and disables auto search of ONVIF device, see Figure 2-22.

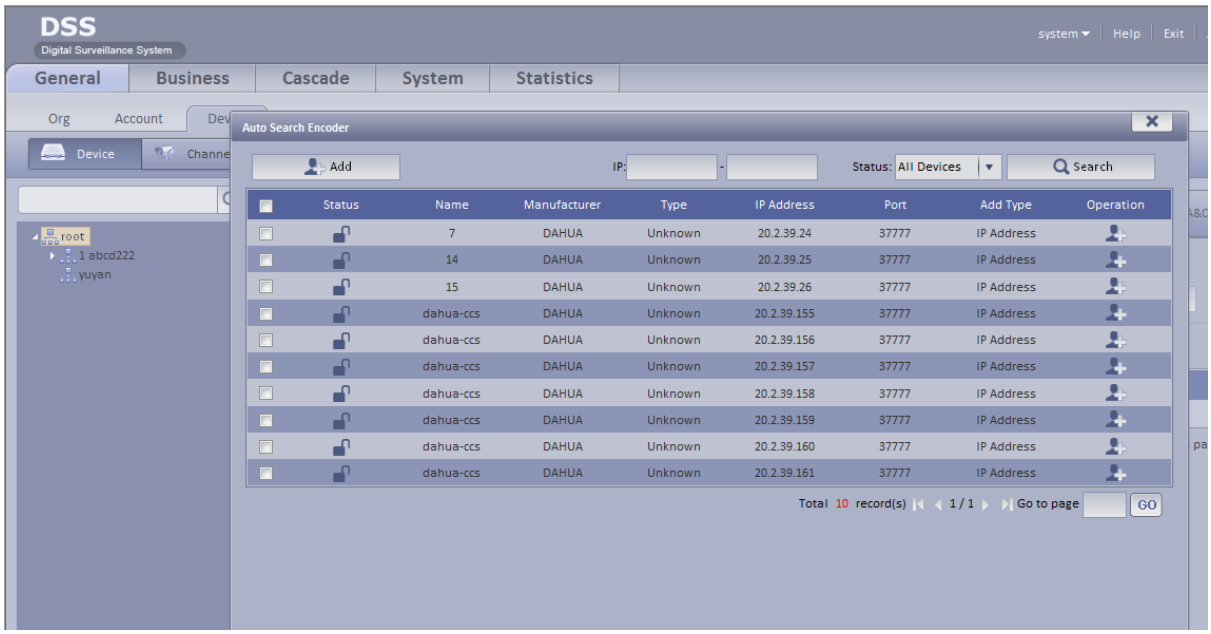


Figure 2-22

- PTS server

Picture storage server port, 8081 by default.

- SCS server

SCS server config, current version is config item of video talk server. Default is in Figure 2-23.

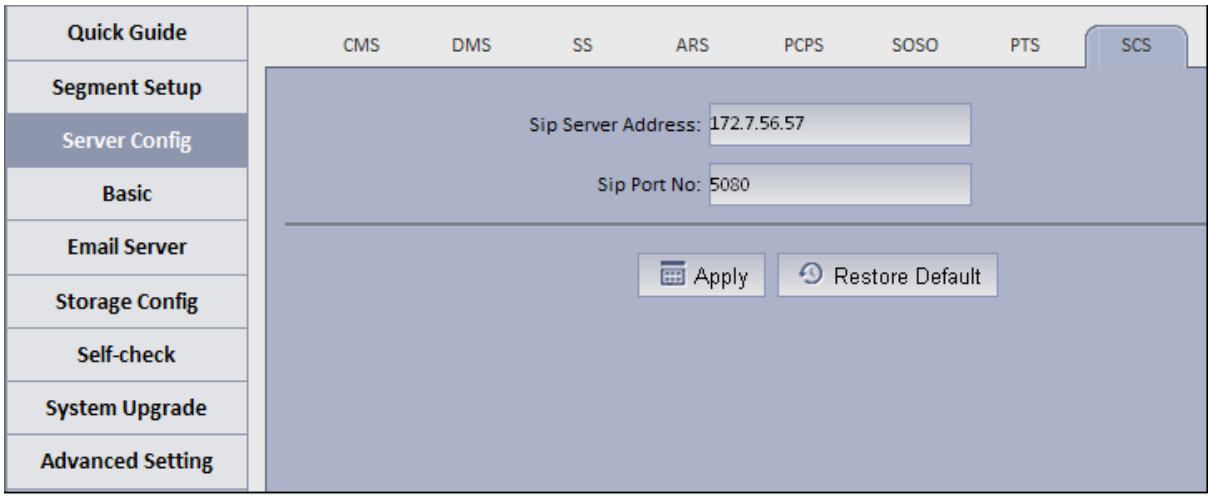


Figure 2-23

Server address: server IP, port is 5080 by default. On device registered via sip server, the port must be identical. See Figure 2-24.

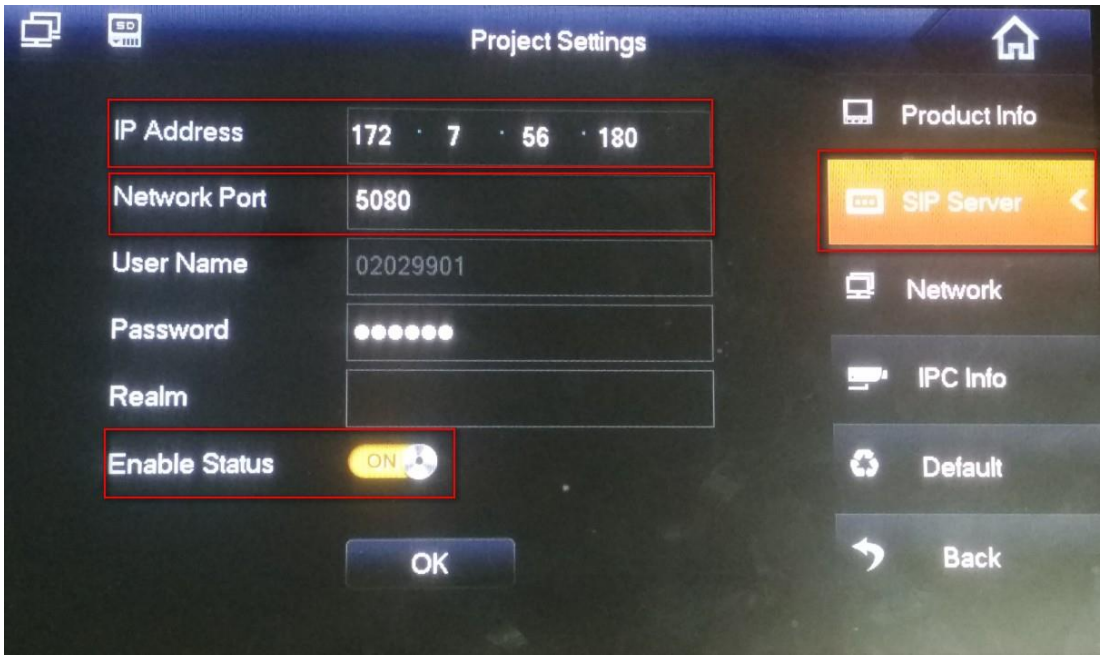


Figure 2-24

2.5 **Basic Config**

- Account modification: login config account, modify login password.
- System maintain: support to reboot, shut down and restore.

Restore default: it will clear database and restore default status.

Reset password: reset backstage config/system/root user login password.

- Time setup

Function in wizard, skipped here.

- Web access port setup

In case web port 80 is occupied, you must modify to other port and assess the system again by entering IP address plus port no.
i.e.: port no. is changed to 1000, the IP address shall be followed by “ip:1000”. See Figure 2-25.

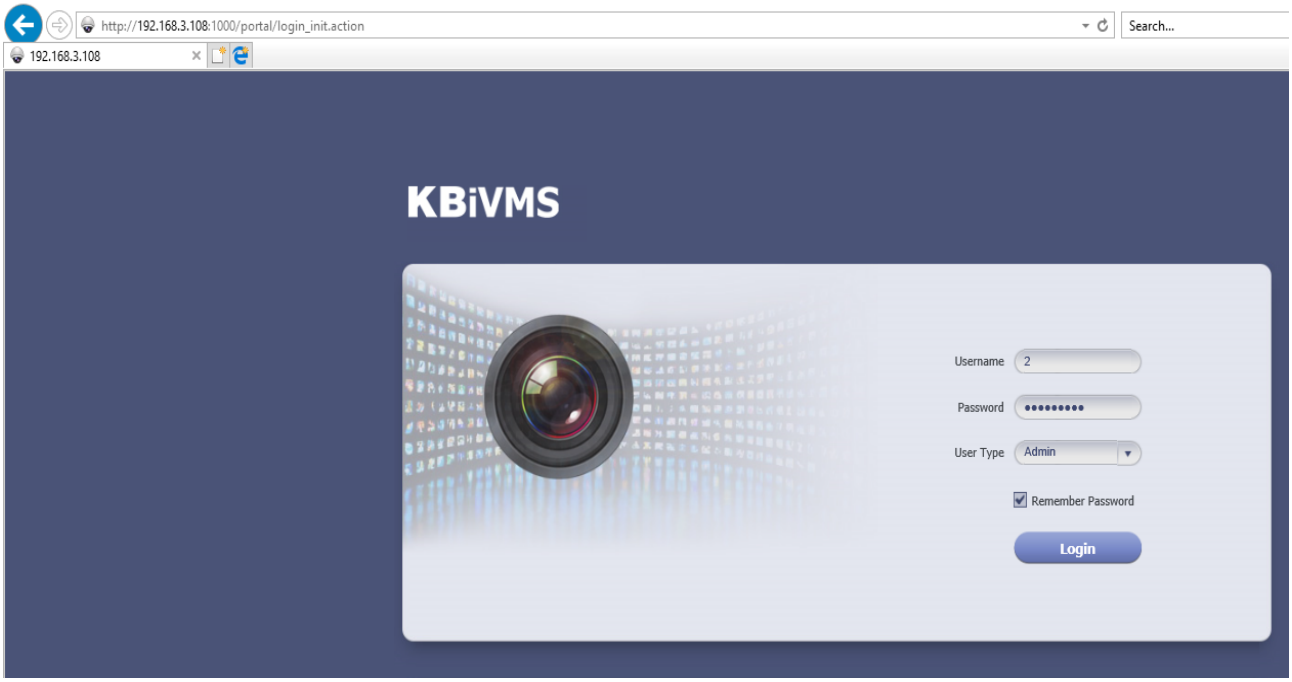


Figure 2-25

- Add static router

In environment of single Ethernet card or multi-Ethernet cards, you may be able to access more than one network segment via router, here add static router addresses of these routers to prevent network address error.

- Ping check

Enter IP, click Apply, test whether platform server and other network are the save, and ether loss of packet exists.

- Log

Support unit in day, to download server log of entire system.

2.6 **Email**

Email config is the same as in wizard, skipped here.

2.7 **Storage**

Storage config includes local config and network config.

- Local config: plug hard disk to local server, and you can directly format hard disk and set type of video or picture.

Set to picture, this disk only stores picture info; set to video, this disk only stores video info; see Figure 2-26.

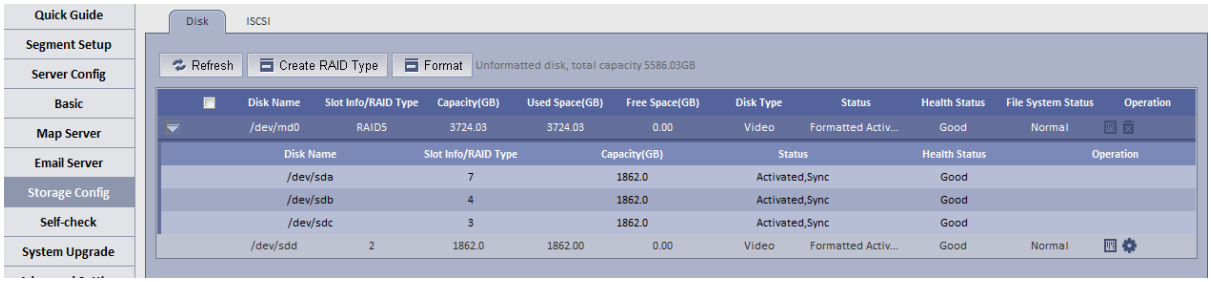


Figure 2-26

Click Create RAID Type, to create Raid and improve data security.

Note:

Raid is a simple technology which can improve external storage solution which can be selected according to actual scene need. Currently the platform supports setup of multiple Raid methods, and user can customize this.

See Figure 2-27.

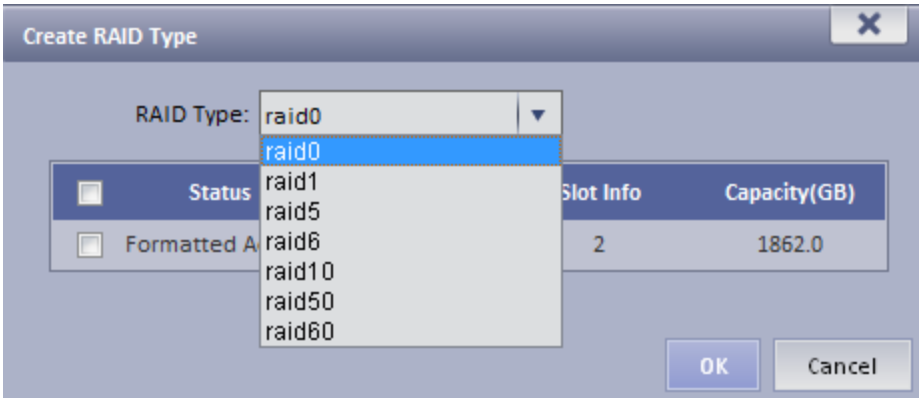


Figure 2-27

Local config can set hot spare: local hot spare and global hot spare. Local disk may be selected to be hot spare. When other disks in use are failed, it can replace any of them.

Local hot spare: select one designated Raid group. (current only supports Raid5).

Set hot spare:

1. Select hard disk: select button to set hot spare, see Figure 2-28.

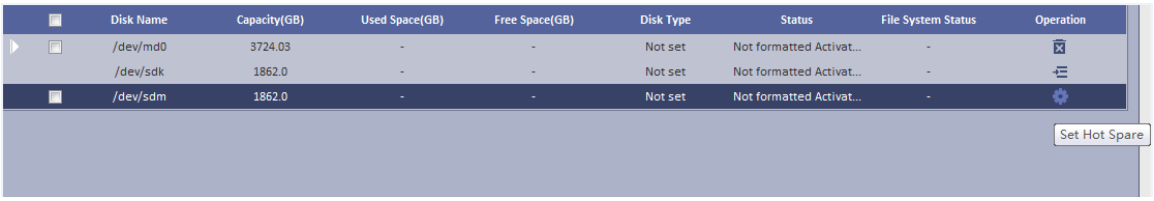


Figure 2-28

2. After click the button, see Figure 2-29 and select hot spare type.

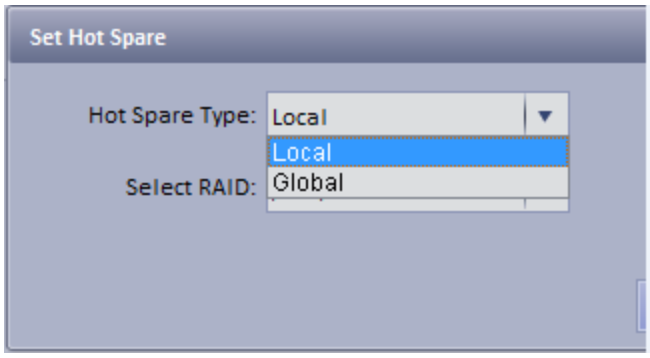


Figure 2-29

If you select local hot spare (only support Raid5): locally select one raid5 group.

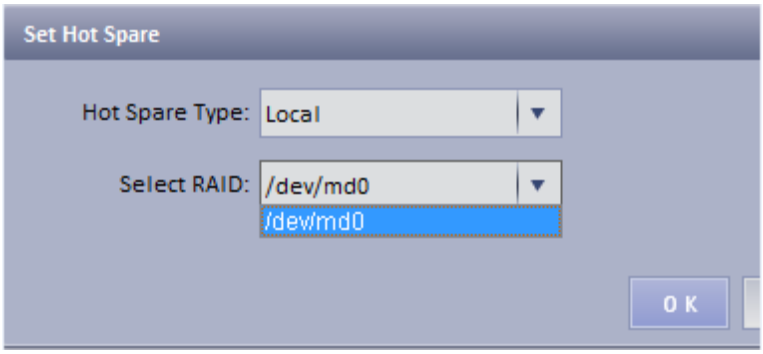


Figure 2-30

After setup is successful, view Raid5 group which has one additional hot spare disk. When any one of raid5 disk is broken, local hot spare will continue working.

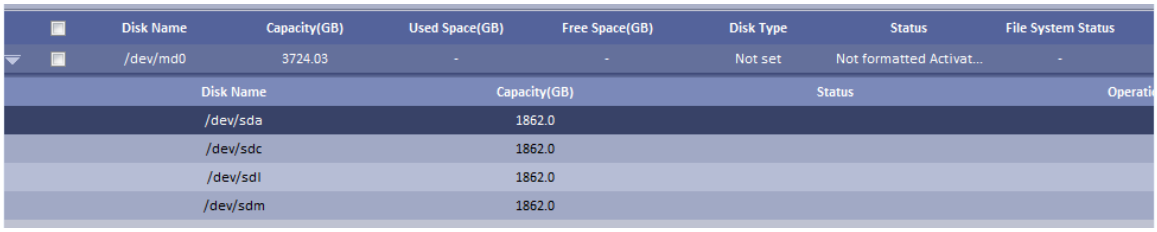


Figure 2-31

- If select global hot spare. See Figure 2-32 .

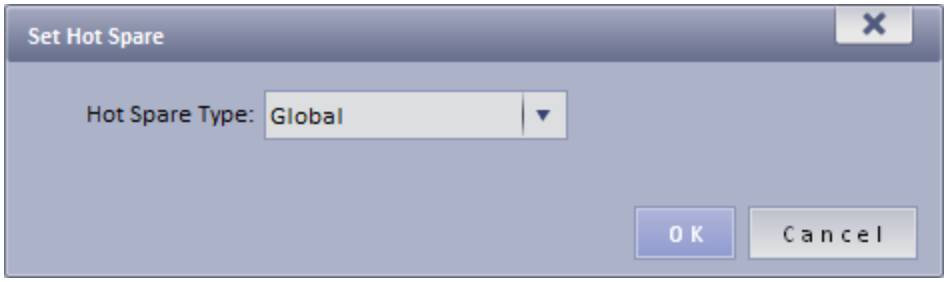


Figure 2-32

After setup is successful, when any one storage disk in server is broken, global hot spare disk will replace it and continue working.

Figure 2-33

- Network disk: via network add other storage server, such as ESS, EVS (before adding,

please configure Raid disk on storage server).

After you add it, you must format this disk, and set it to video or picture, same as “local disk config”, see Figure 2-34.

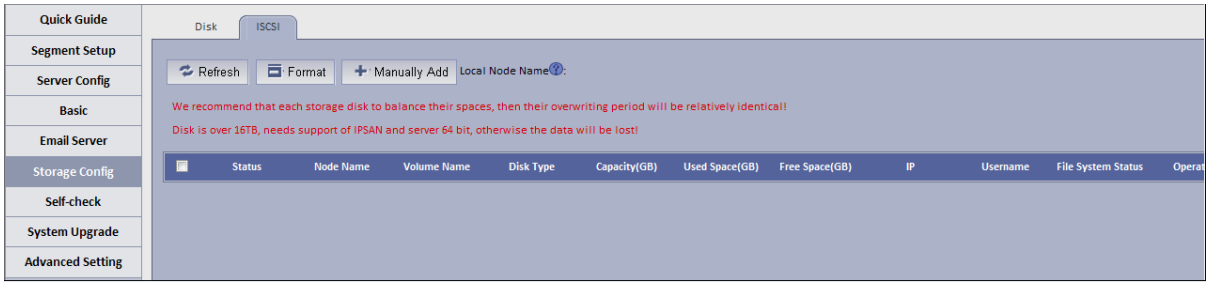


Figure 2-34

For the added storage server, it has been added and used by other server, then the Raid group info will be abnormal, see Figure 2-35.

Figure 2-35

If you have to use this disk, click Rob, and click  , when you see prompt, click OK.

See Figure 2-36.

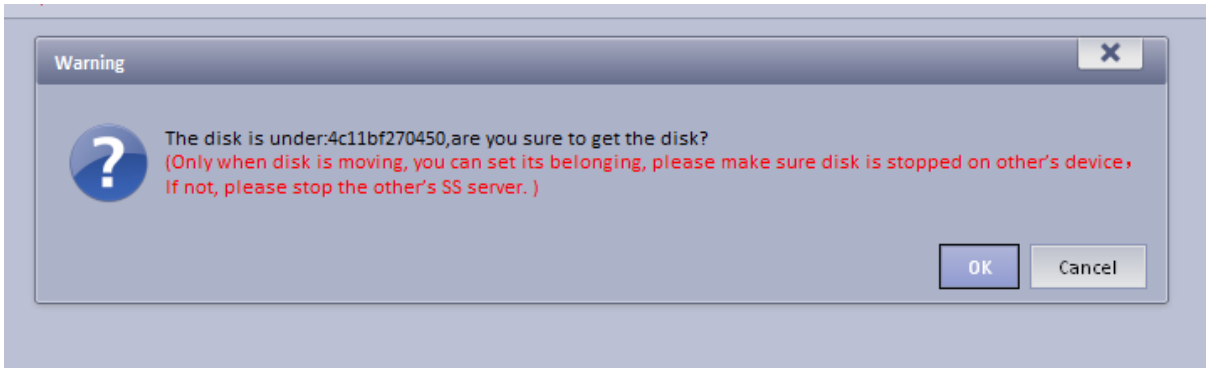


Figure 2-36

After robbery, the server can immediately use this disk to store.

2.8 System Self-Check

At the upper left corner of system self-check interface, it shows system real-time operation status.  means normal,  means abnormal, see Figure 2-37.

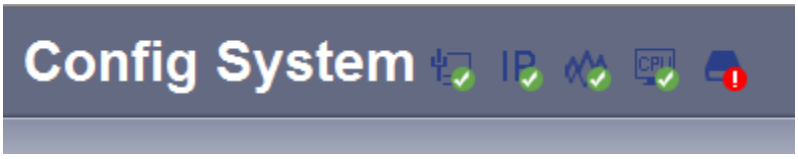


Figure 2-37

Click to see corresponding details.

- Application check: it shows current system running server, database, FTP server operation status, see Figure 2-38.

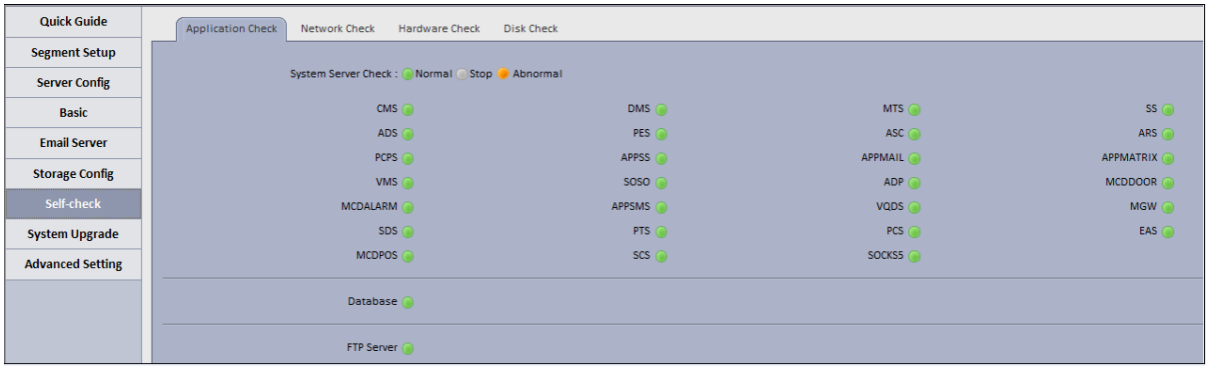


Figure 2-38

- Network check: it shows current Ethernet card status and real-time stream in/out flow, see Figure 2-39.

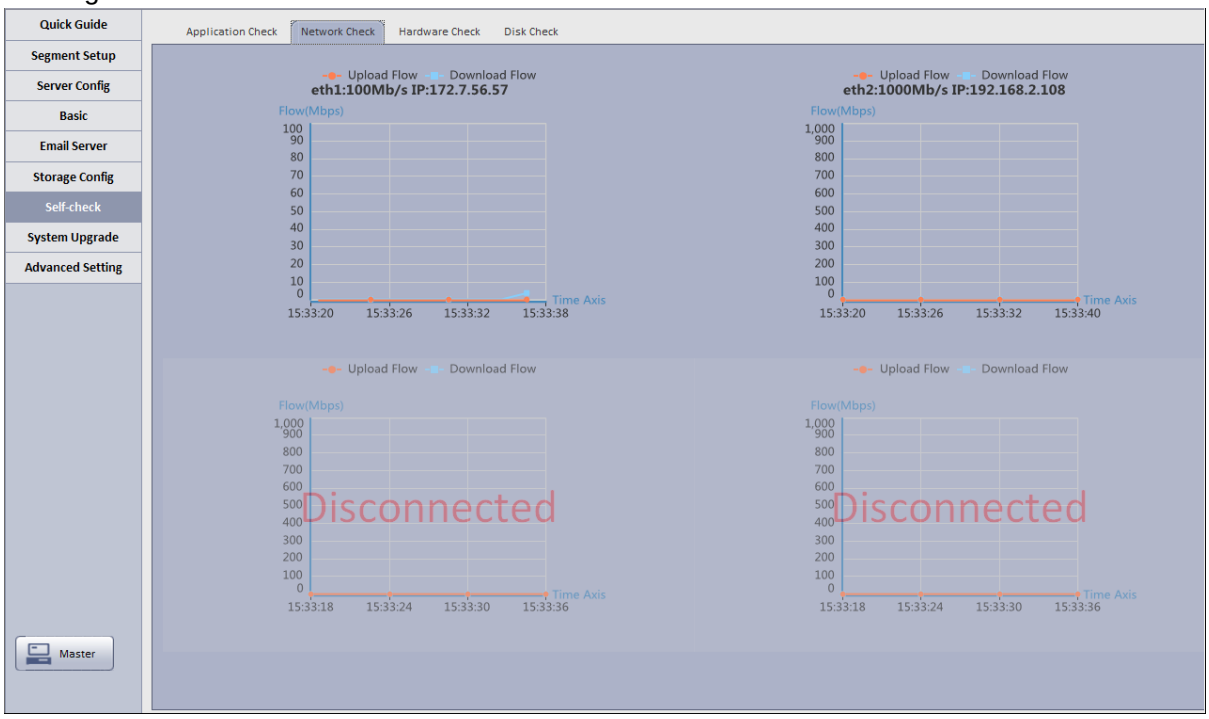


Figure 2-39

- Hardware check: it shows current system running status, and real-time data, see Figure 2-40.

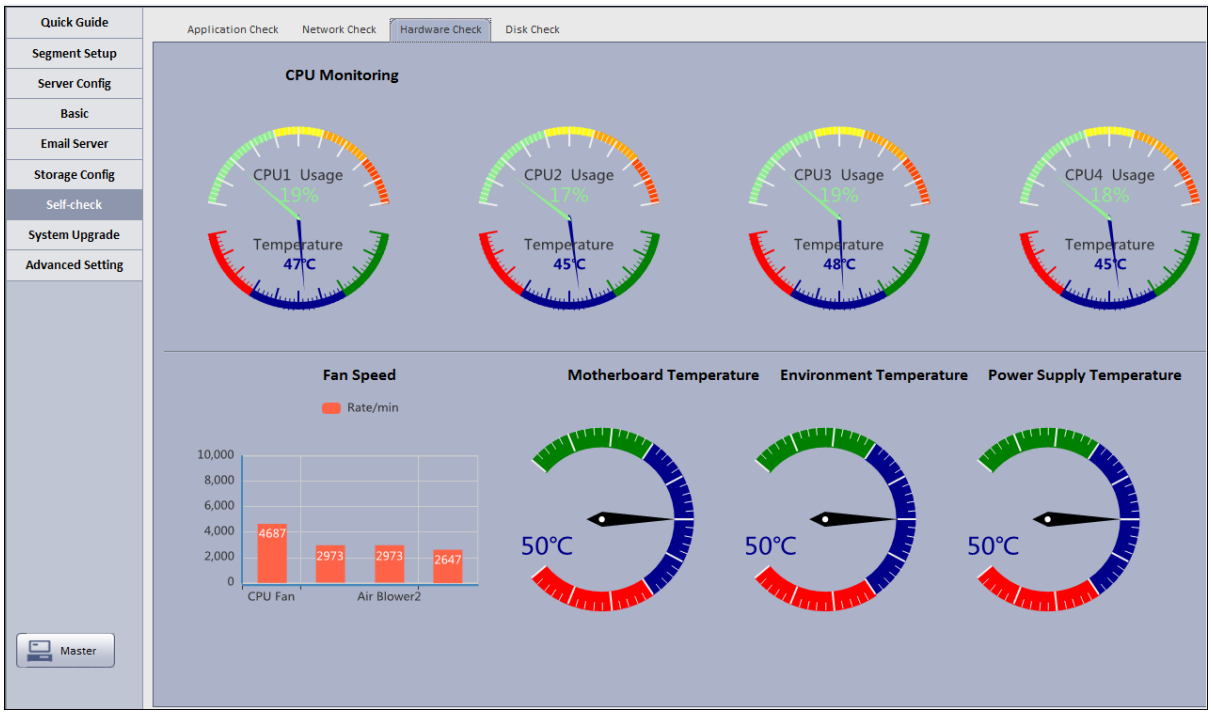


Figure 2-40

- Disk check: it shows current system real-time mounted HDD operation status, including mounted hard disk of Raid disk in network storage server, see Figure 2-41.

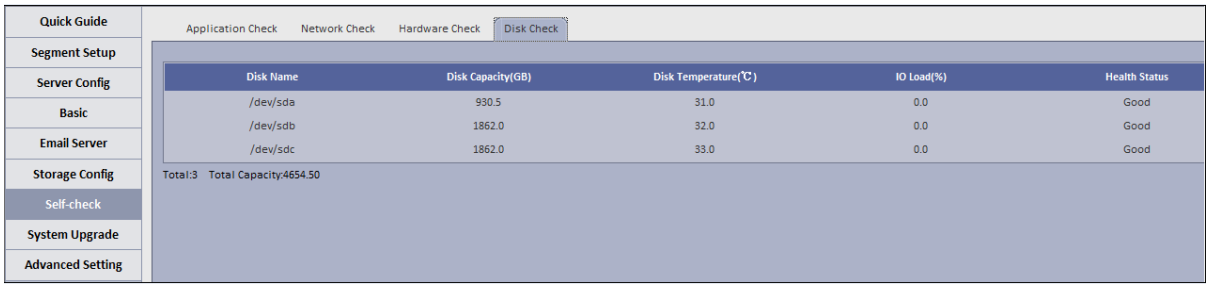


Figure 2-41

2.9 **System Upgrade**

The system supports one-click WEB upgrading, compatible with tool upgrading, see Figure 2-42.

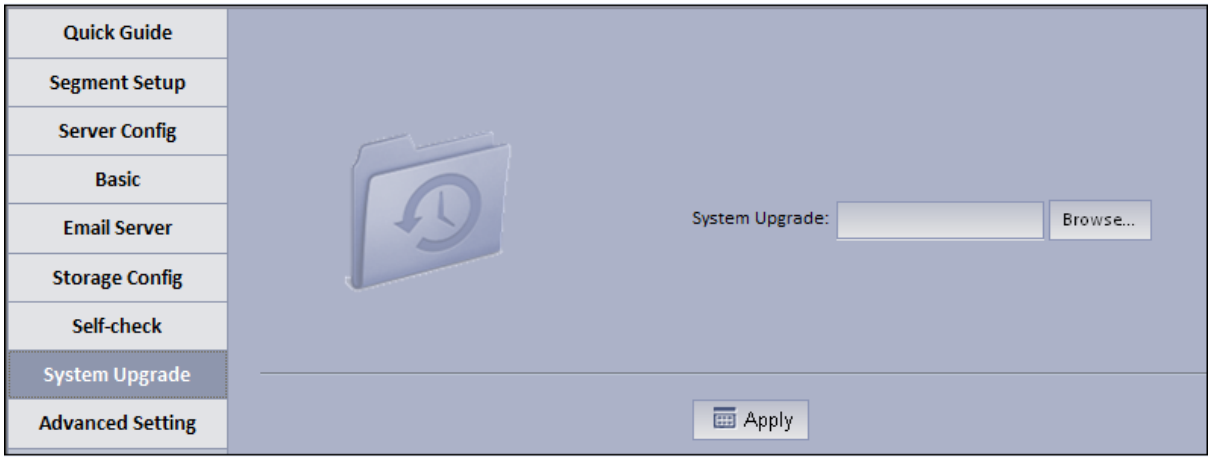


Figure 2-42

2.10 **Advanced Config**

Master/slave confic, hot spare config, N+M config are same as in wizard, so skipped here.

2.11 **WEB System Parameter Config**

2.11.1 **Login WEB**

You can refer to the following steps to login KBiVMS Manager. In Internet Explorer, input IP address of the Server, press Enter. You will see Figure 2-43.
Default username is **system**. Default password is **123456**.

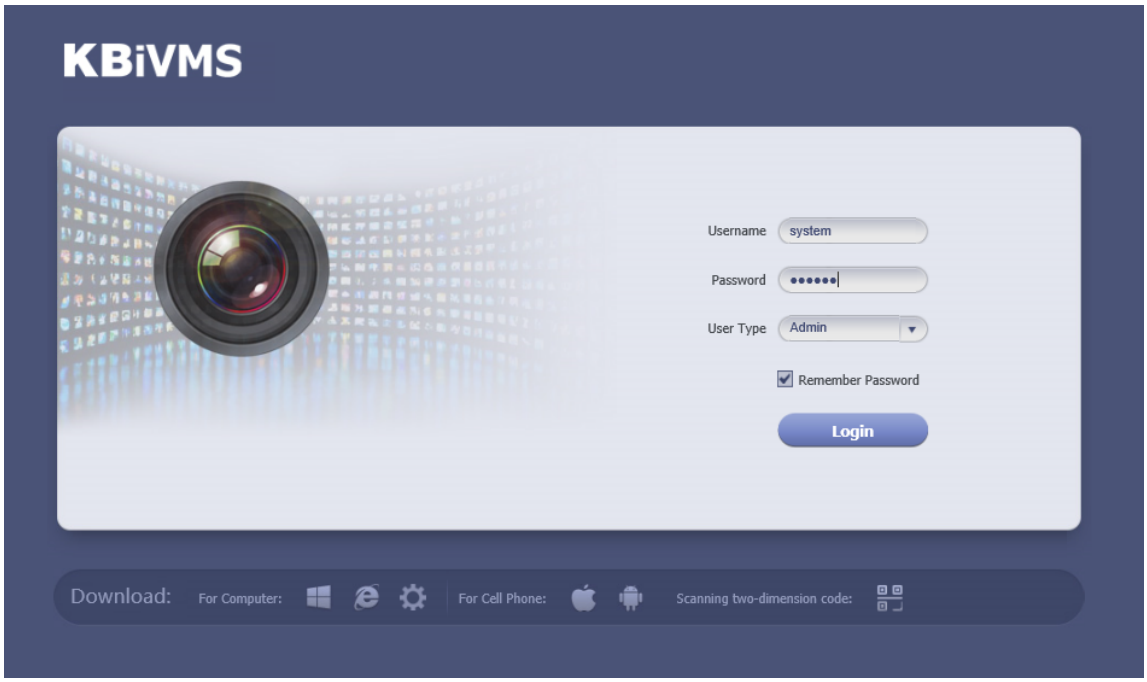
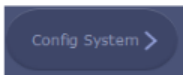


Figure 2-43

Parameter	Requirement
	Download C/S client.
	IE control download.
	Download iPhone version, Android version and scan QR code to download client.
	Download VTSS app, including iOS, Android and scanning via QR code.
	IE config tool download.
	Config tool download.

Parameter	Requirement
	Help manual download.
	Enter config system.

Note: You can download KBiVMS Client on this login page. If it is your first time login KBiVMS Client Manager, please add its IP address into the trusted site of your explorer.

2.11.2 System Parameter Config

When you first login the system, you shall configure system settings in order to make the system run properly.

Configure the system as follows:

Step 1. Select System > Parameters, you will see Figure 2-44.

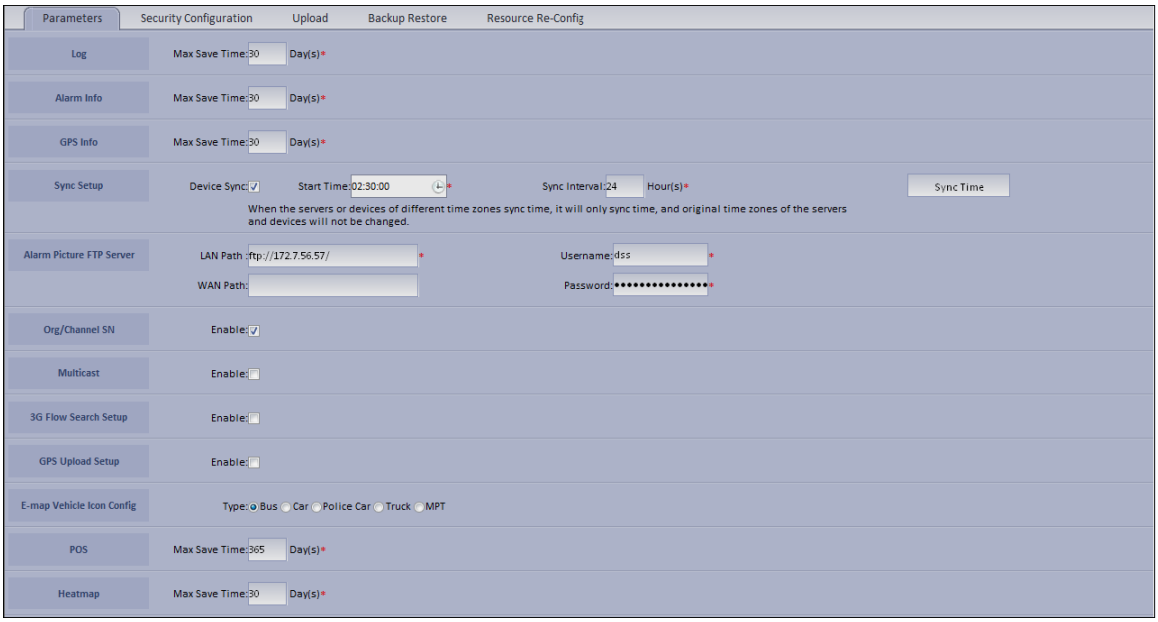


Figure 2-44

Parameter		Note
CMS	IP Address	IP address of manager server
	LAN Port	LAN port of manager server, default is 9000
	WAN Port	WAN port of manager server.
PCS	LAN IP	IP address of PCS
	LAN Port	LAN port of PCS, default is 9001
	WAN Port	WAN port of PCS.

Parameter		Note
WEB Server	LAN IP	LAN IP of WEB server.
	WAN IP	WAN IP of WEB server.
	LAN Port	LAN port of WEB server, default is 80.
	WAN Port	WAN port of WEB server.
Log	Max Save Time	Set max save time of log, default is 30 days
Alarm Info	Max Save Time	Set max save time of alarm info, default is 30 days
GPS Info	Max Save Time	Set max save time of GPS info, default is 30 days.
Sync Setup	Server Sync	If check this parameter, then enable server sync function.
	Device Sync	If check this parameter, then enable device sync function.
	Start Time	Set start time of time sync.
	Sync Interval	Subject to server time sync device and server time. Default is 2 hours as every 2 hours; system is subject to server time and sync time with server. Note: Device and server sync time via SDK.
	Sync Now	Click it to start time sync immediately.
Alarm Picture FTP Server	LAN Path	FTP LAN address where to save alarm picture.
	WAN Path	FTP WAN address where to save alarm picture.
	Username/Password	Username and password to login FTP server

Parameter	Note
Org/Channel SN	● If check Start, organization and channel will have this SN. ● If you do not check Start, this SN will not be display in organization manager and device manager.
Multicast	● If check Start, you can see multicast when add device. ● If you do not check Start, you cannot see multicast when add device.
3G Flow Search Setup	Check“Enable”, set time, search 3G flow usage.
GPS Upload Setup	Check“Enable”, and set interval time, as the time interval GPS info is uploaded
E-map Vehicle Icon Config	Set vehicle icon on e-map
POS	Set max save time of POS info
Heat Map	Set max save time of heat map

Step 2. Configure parameters.

Step 3. Click Submit.

2.11.3 **Security Configuration**

Step 1. Select System > Security Configuration, you will see Figure 2-45.

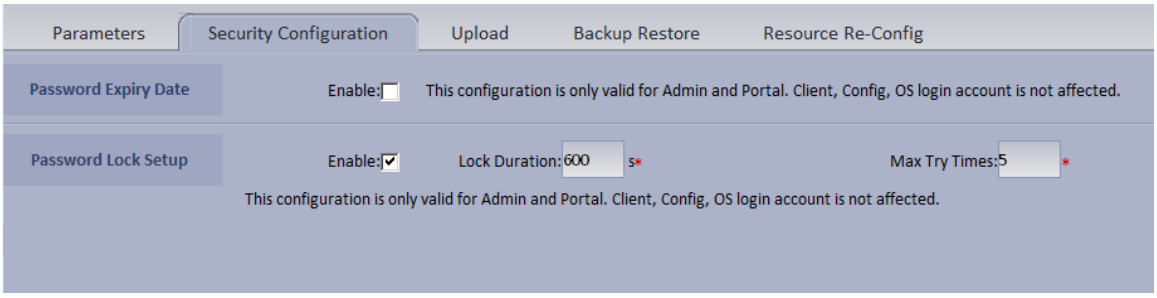


Figure 2-45

Step 2. Enable HTTPS, access web via https.

Step 3. Enable Password Expiry Date, once this date is reached, you must change password, otherwise, you cannot login.

Step 4. Enable Password Lock and set lock time, try times and duration. Once exceeding max try times, the password will be locked.

3 Add Organization and Login User

You can enter IP address of the Server platform in IE to login Manager.

3.1 Add Organization

Before you add device, you need to add organization of current device. You can arrange, organize and manage layer of device in Org.

The default first-level organization is root node. Newly added organization will be displayed below the root node.

Select General>

Select General> Org, Org includes basic organization and logic organization. When you configure user role, if you select different organizations in the right area of “Device Right>Device Tree Display Right”, then in Client Live Preview interface, it shows device under the corresponding organization.

- Select General> Org.

1. Click 

.

System pops up Add Org box, see Figure 3-1.

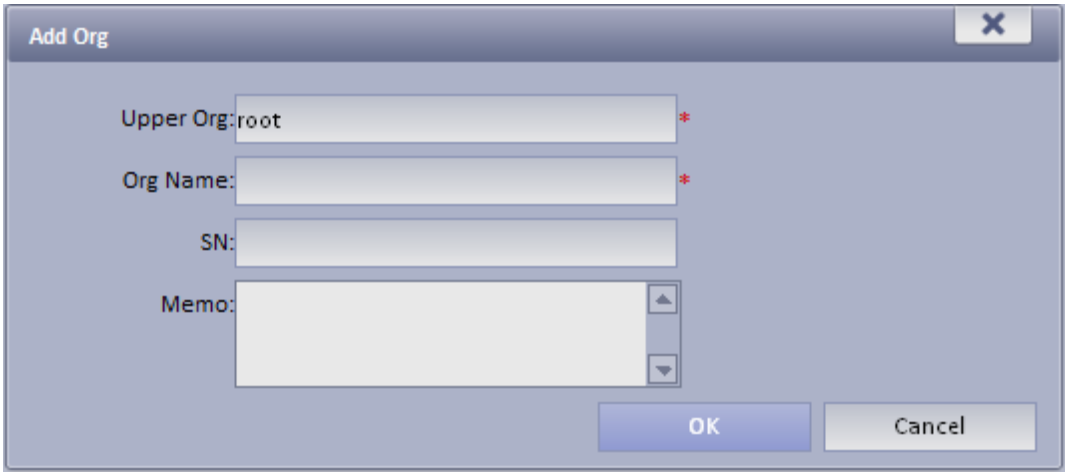


Figure 3-1

2. Select Upper Org, input Org Name, SN.
3. Click 

.

Note:You can only modify root node organization info, and you cannot delete this organization.

- Select Org>Logic Org, click Create Logic Org.

System shows Create Logic Org box, see Figure 3-2.

Figure 3-2

1. Enter org name, click OK.

2. After you add new logic org in the area on the left, click and select config.
   You also can click create login org in area on the left, then root node will be shown belw.
3. In channel Config Channels area , select alternative channel and add it to selected channel. See Figure 3-3.

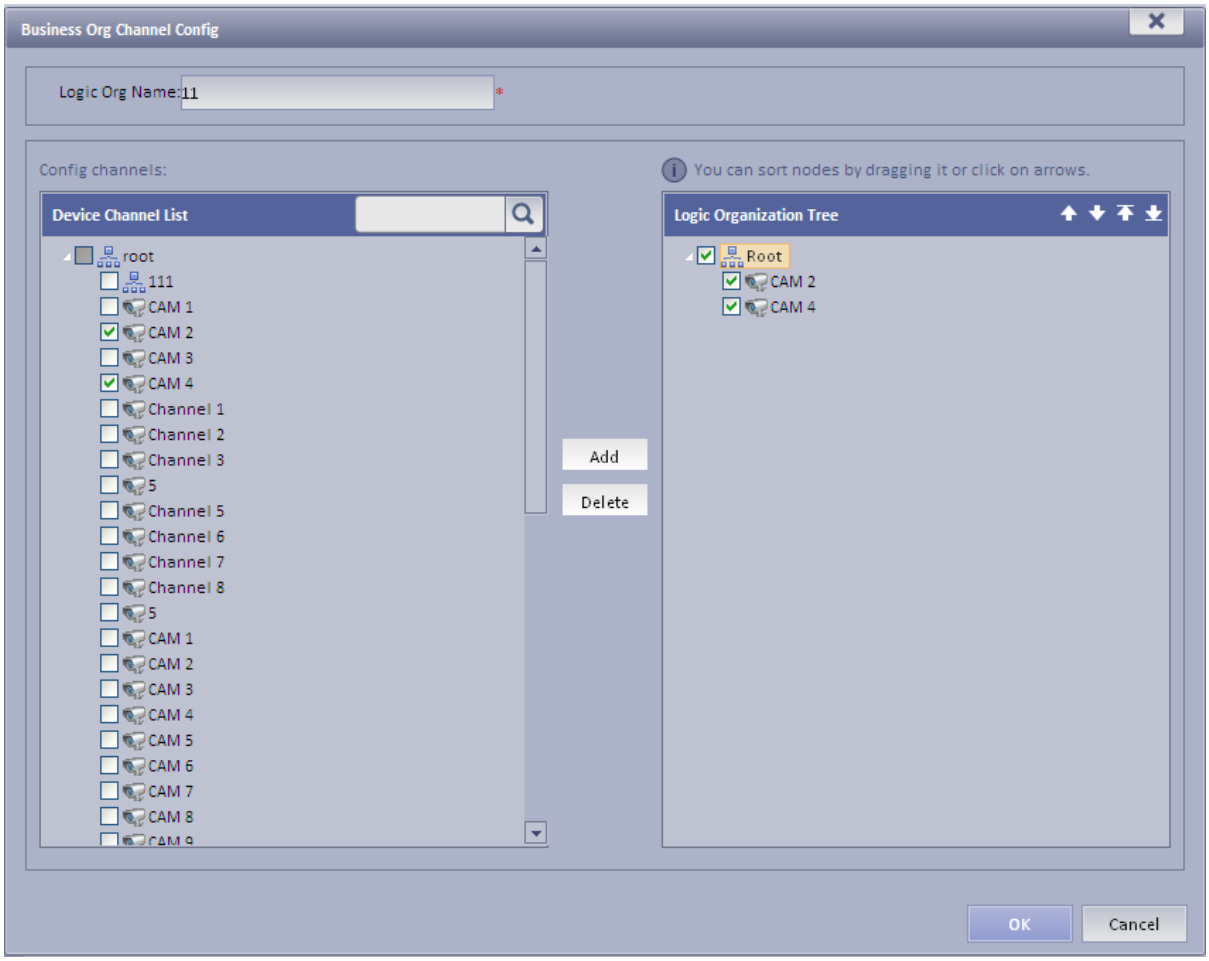


Figure 3-3

You can adjust channel selection via , , and .

3.2 Add User Role

KBiVMS Client Platform supports to add user role and then add user. Existing user can login Manager as well as Client. Different user roles lead to different operation rights.

Rights of user role includes Administrator Menu right, Operator Menu right and Device right. You must grand these rights before you can operate.

Step 1. Click General>Account. System displays Account interface.

Step 2. Click Role tab.

Step 3. Click Add. System pops up Add Role box.

Step 4. Input Role Name, and select Role Level.

Note: If you check Copy Role next to Role Name, and select one role from the dropdown box, then the info will be pasted to your selected role.

Step 5. Click Device Rights page, select right in Right Trees and select channel in Channel Tree on the right. See Figure 3-4.

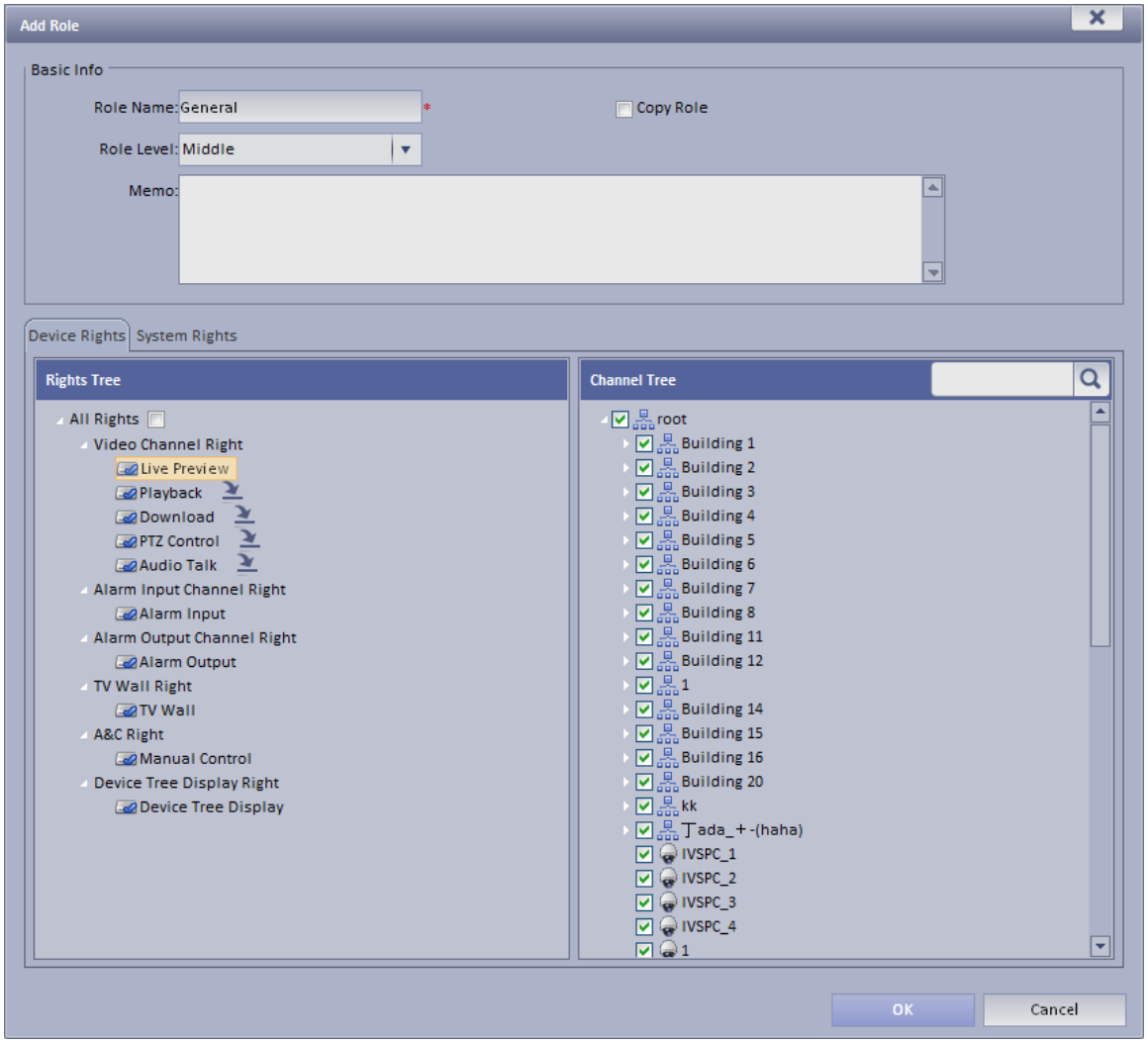


Figure 3-4

Note:

- Click  so you can copy setting from the selected node to current node.
- If you do not check corresponding device right, then all users under this role will have no corresponding rights.

Step 6. Click System Rights tag, select corresponding system rights. See Figure 3-5.

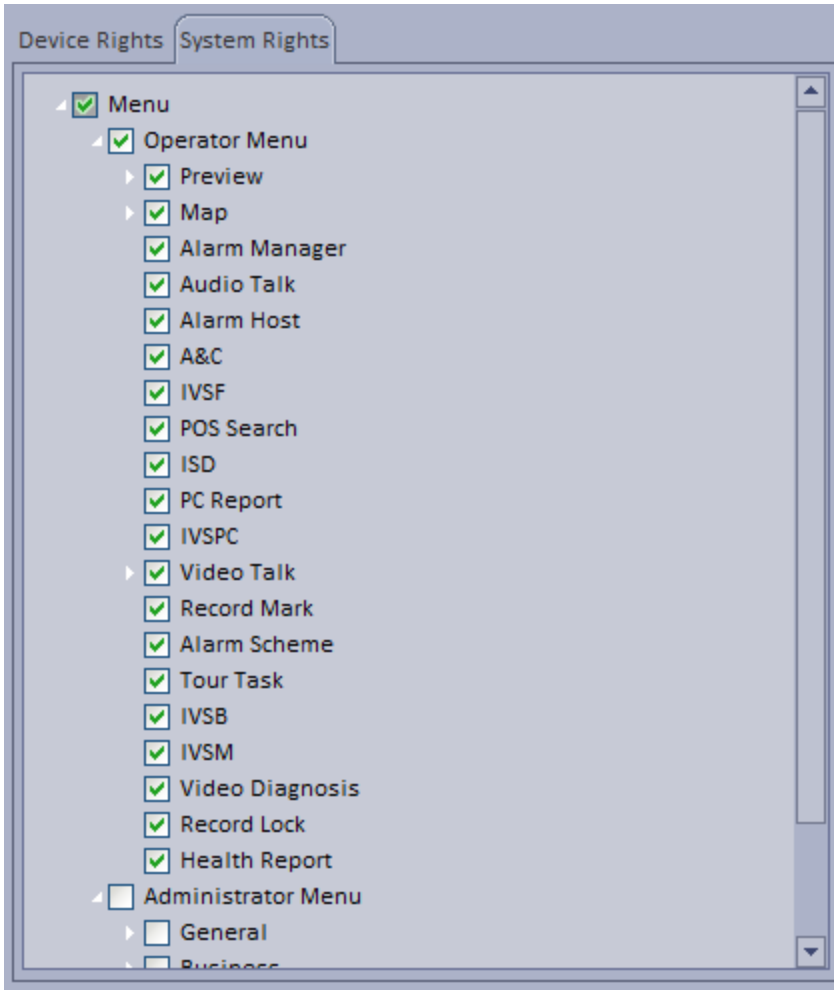


Figure 3-5

Step 7. Click OK to add the role.

3.3 Add User

If you have added user role, now you can add user of that role.

Step 1. Click User tab under Account.

Step 2. Click 

. System pops up Add User box.

Step 3. Create a username, a password and confirm password. Select Department and Role. See Figure 3-6.

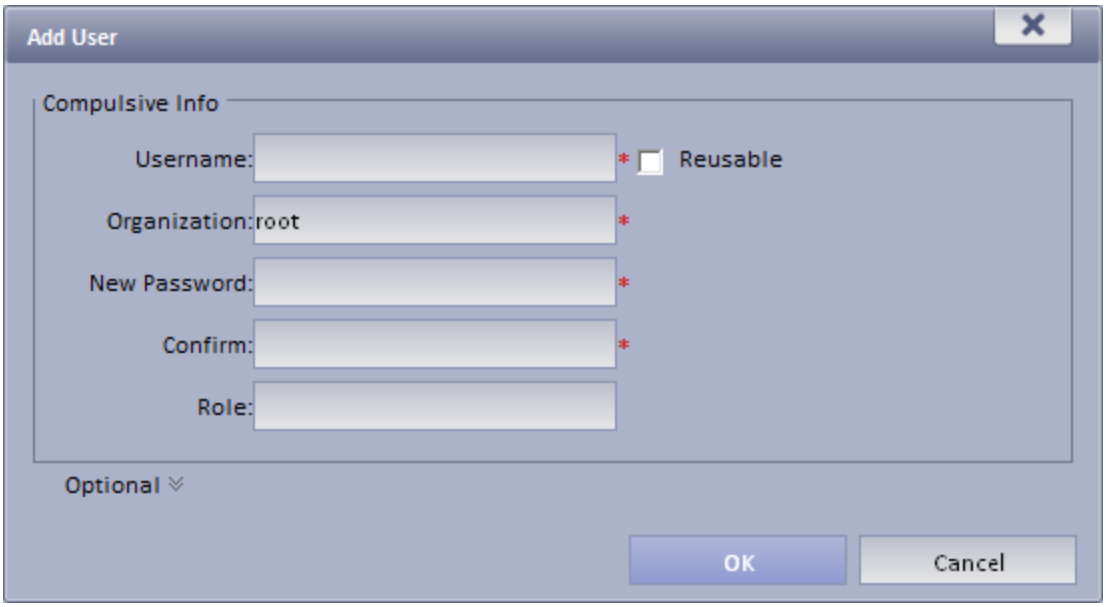


Figure 3-6

Note:

- If you check Reusable box next to Username, then you allows more than one user to login system with this Username at the same time.
- If you do not select a role, then the user will have no System Rights or Device Rights.
- You can select more than one role at a time.
- You can click Optional in the lower-left corner to fill in extra info.

Step 4. Click OK to add user.

4 KBiVMS Client Installation and Login

4.1 Requirement for PC

To install KBiVMS, your PC shall match the following requirements or higher. See Chart 4-1.

Parameter	Requirement
OS	Microsoft Windows XP SP3, Microsoft Windows 7
CPU	Core 2 dual-core 3.0 or higher
Hard Disk	At least 10GB free space
Video Card	DirectX 9.0c or higher
Memory	At least 2GB
Monitor	1024×768 or higher
Explorer	IE7, IE8 or higher

Chart 4-1

4.2 Install

Please follow these steps to install KBiVMS Client:

Step 1. Download and install the Client set up file

a) In Internet Explorer, input the IP address of Server. System displays login interface of KBiVMS Client Manager as in Figure 4-1.

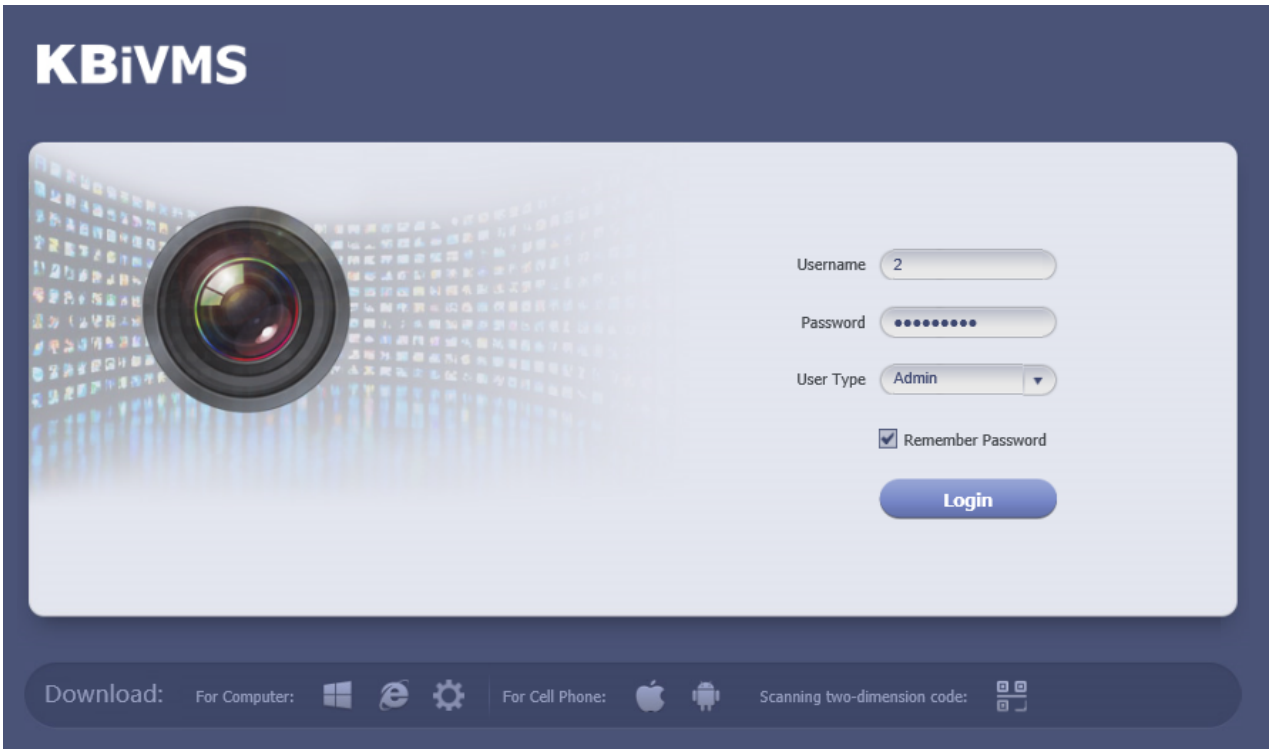


Figure 4-1

b) Click Download Client-end. System pops up a box.

c) Click Save. Download and save KBiVMS Client setup file to local PC.

Step 2. Install the Client, check Run KBiVMS Client, see Figure 4-2.

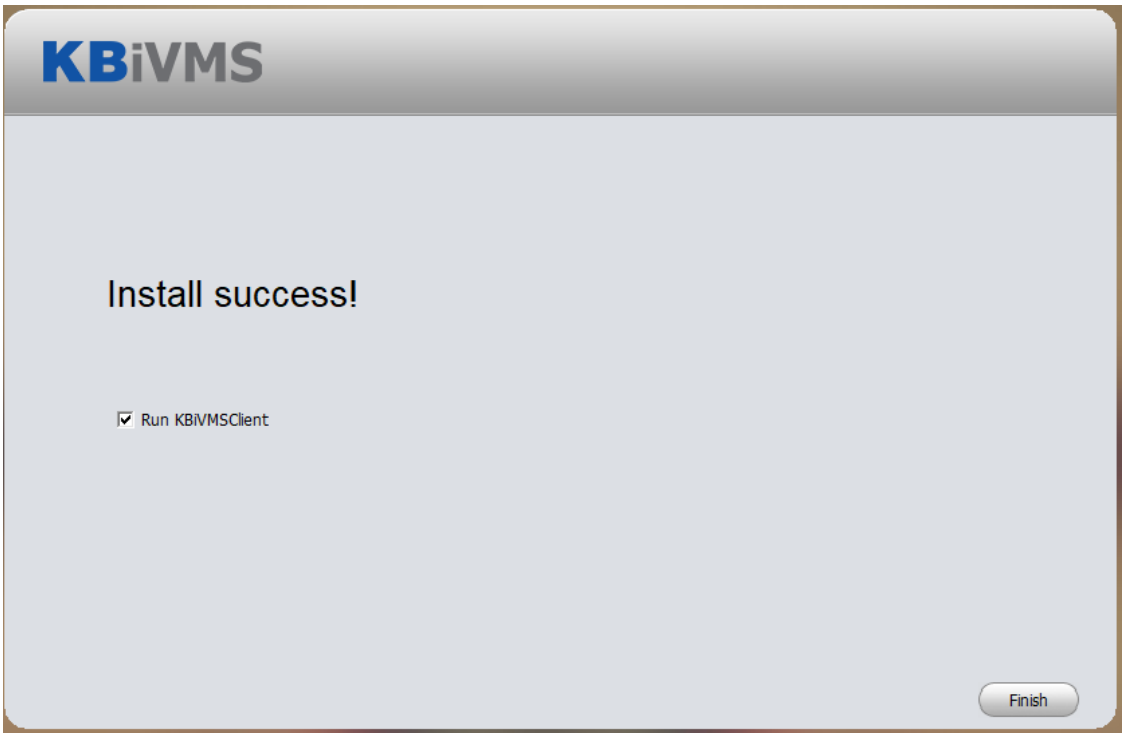


Figure 4-2

4.3 Login

KBiVMS Client interface is shown in Figure 4-3.

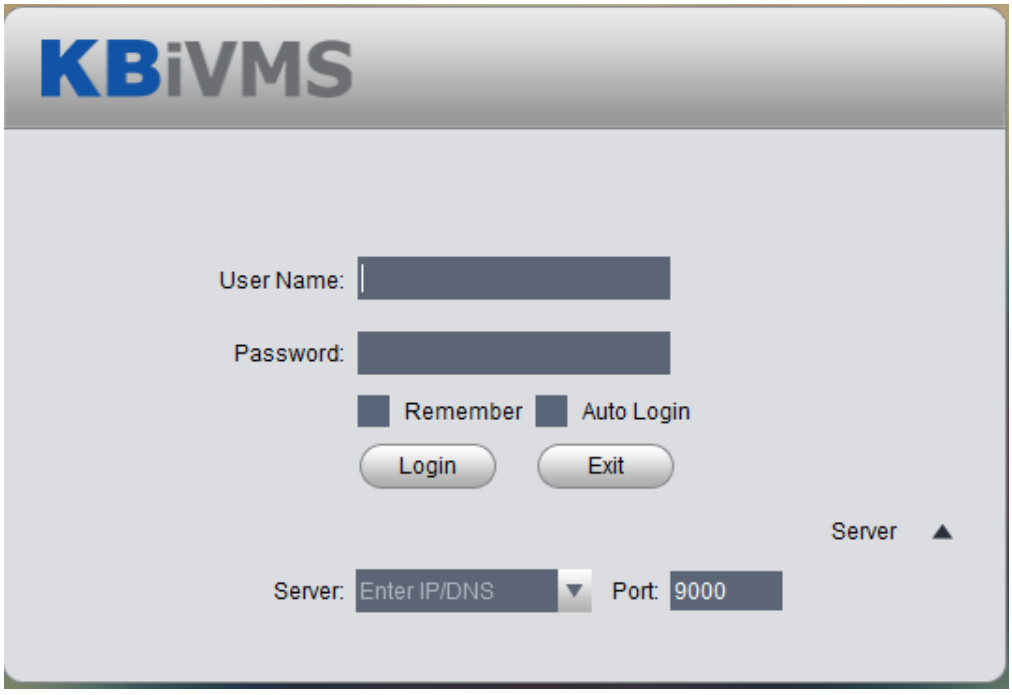


Figure 4-3

Step 1. Input Username and Password.

Step 2. Click Server, and input Server IP and Port. Server IP shall be the IP address of Server. Default port is 9000.

Step 3. Click Login. System pops up homepage as in Figure 4-4.

Figure 4-4

- Click Log Off on the right of interface to switch user.
- Click Password to modify login password.
- Click in the upper-right corner to lock account. To unlock, you need to input login password in box pops up.

4.4 Local Config

After you first login Client, you can Window Split, Connection Type, Bit Stream Type, Alarm Level Amount, Video Buffer Time, Snapshot Save Path, Max Record Path and Record Save Path and etc.

Step 1. Click 

in Setup Manager area. System enters Local Setup interface. See Figure 4-5.

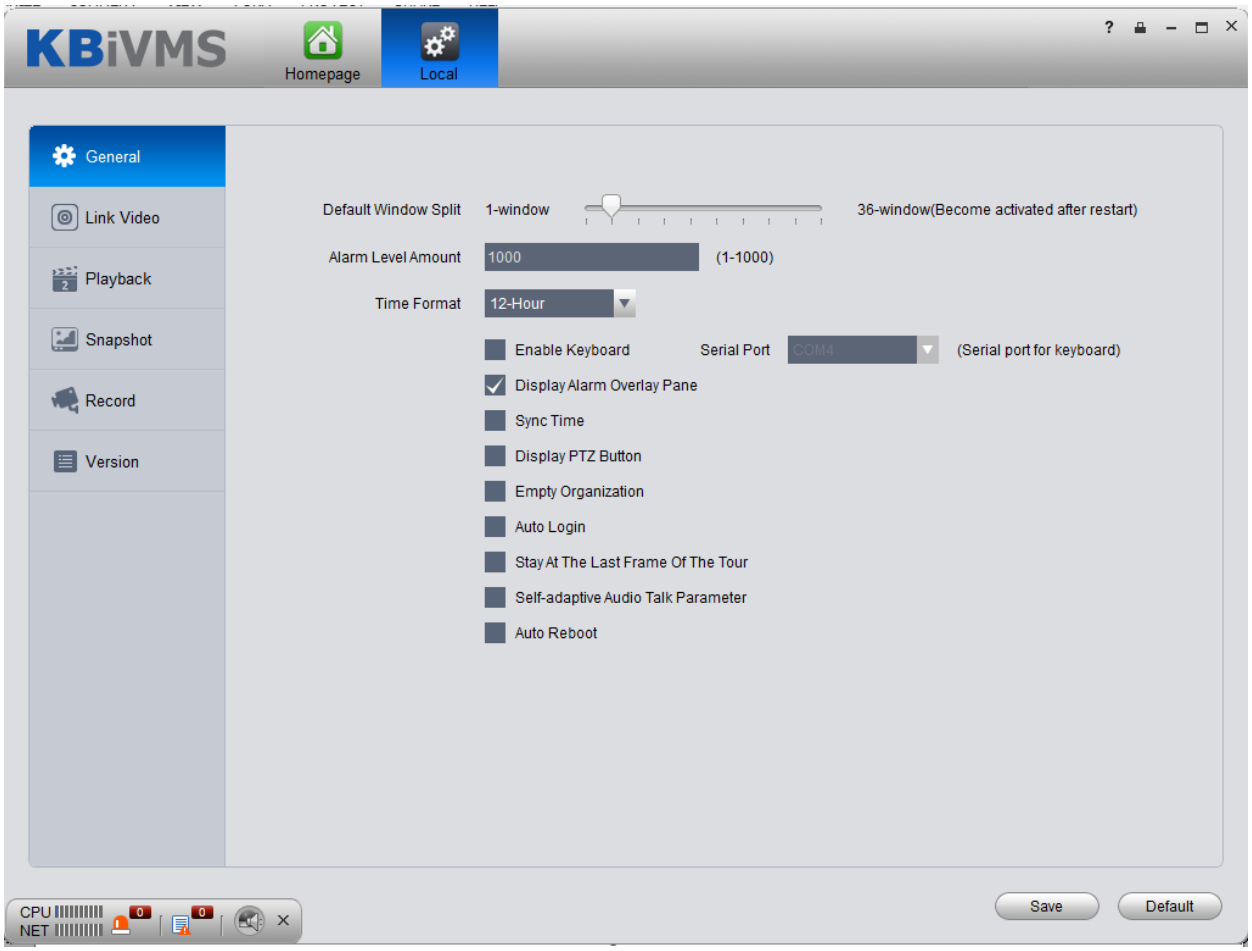


Figure 4-5

Parameter		Note
General	Default Window Split	Set preview, playback and others' default display modes.
	Default Auto Change Stream Type	i.e.: Select 4-split when window plays more than 4-split, it will switch to sub stream from main stream.
	Alarm Level Amount	Max alarms in Alarm Manager. Default is 1000 items.
	Time Format	Set "12 Hour" or "24 Hour" standard.
	Enable Keyboard	Check to enable keyboard.

Parameter		Note
	Serial Port	Select port (COM 1~COM10) For network keyboard use only.
	Display Alarm Overlay Pane	Display it or not  。 ●  : real time display CPU status ●  : Real time display net status ●  : Quickly enter Alarm Manager>Alarm List interface. ●  : Quickly enter Alarm Manager>System Event interface. Step 1.  : Prompt alarm device
	Sync Time	Respond sync time or not: ● Check: sync server time by Client. Step 1. Not check: Do not sync server time.
	Display PTZ Button	Check it to display 8 keys of PTZ in window.
General	Empty Organization	If you create more than one organization on Manager, and the organizations have no device. Select this parameter, so Client displays name of the organizations.
	Auto Login	If select this parameter, then you will automatically login the client when you open it.
	Stay at the Last Frame of the Tour	If you select this parameter, then image stops at the last frame during tour.
	Self-adaptive Audio Talk Parameter	During talk, system can auto match device sampling frequency, sampling bit, and audio format.

Parameter		Note
	Auto Reboot	If you select this parameter, when PC boots up, the client boots up automatically.
	Open Link Video of POS	If you select this parameter, then it will open
Video	Connection Type	Request video mode.
	Bit Stream Type	Bit stream type used when you open video, you can select default bit stream, or self-adaptive stream for window size.
	Play Mode	Select play mode accordingly. There are RT priority, fluency priority and balance first. Default video buffer time is 1500ms.
	Login Enable	Task enabled after login. Include：None, previous tour task, previous preview record.
	Double Click on Real Time Window to Switch to Main Stream	Double click window to switch to main stream. Note: When window split is more than 9, double click a window to maximize window. Video stream will be switched to main stream.
	Display Error Info	When system has error or user encounters operation error, it shows a message box or not.
	POS Width	Live preview interface POS display width.
	Display Video Info	Display real time video bit rate and etc. in monitoring window or not.

Parameter		Note
Playback	Instant Playback Enable	Select this parameter to enable instant playback.
	RT Playback Time	Select real time playback time, default is 15s.
	Select this parameter, playback enable.	Start playback
	Enable High Definition Adjustment	Check to prevent stuck high definition video.
Snapshot	Save Snapshot Picture Directly	Select this parameter, then you will not see a snapshot box pops up.
	Format of Save Capture	Picture storage format, as BMP and JEPG.
	Continuous Amount	Set amount of continuous snapshot. Min is 2, and max is 10.
	Continuous Interval	Set continuous snapshot interval.
	Snapshot Save Path	When you snapshot at local, storage path is set here.

Parameter		Note
	Picture ftp server	Enter FTP server address, username and password used to save picture
Record	Max Record Time	Max record time of local recording.
	Max Size of Single Record	When you record locally, you cannot record file over this max size
	Record Save Path	Record storage path of local recording.
	ANPR Linked Record Time	When ANPT device has alarm, linked record play time.
	Query Record Time Out	Set record search overtime time.
	POS Record Time	i.e. here set Before：1 min, Length：5 min, in“POS search” interface search for linked record of receipt, play record 1 min before and 5 after time when the receipt is generated.
Version		View version info of the software.

Chart 4-2

Step 2. Set General, Video, Playback, Snapshot and Record info.

Step 3. Click Save.

5 Live Preview

Live Preview function supports to view live video, and monitor PTZ, snapshot, record and etc. at the same time.

5.1 Video Preview for General Encoding Device

5.1.1 Manually Add

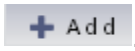
Before you can use functions of Client, you shall add organization and device on Manager.

Directly enter KBiVMS Client Platform IP address in IE, to login Manager,

Step 1. Select General>Device>Device, system displays device interface.

Step 2. If you click Add in Device interface, then you need to select device category first. Such as encoder, decoder, video wall. You also can add separately by clicking each device category tab.

Step 3. Click 

Step 4. Click 

. System displays Add Encoder box, see Figure 5-1.

Step 5. Enter IP address, device name and click Add. See Figure 5-2.

Step 6. Select device type, enter video channel, alarm input and output channel.

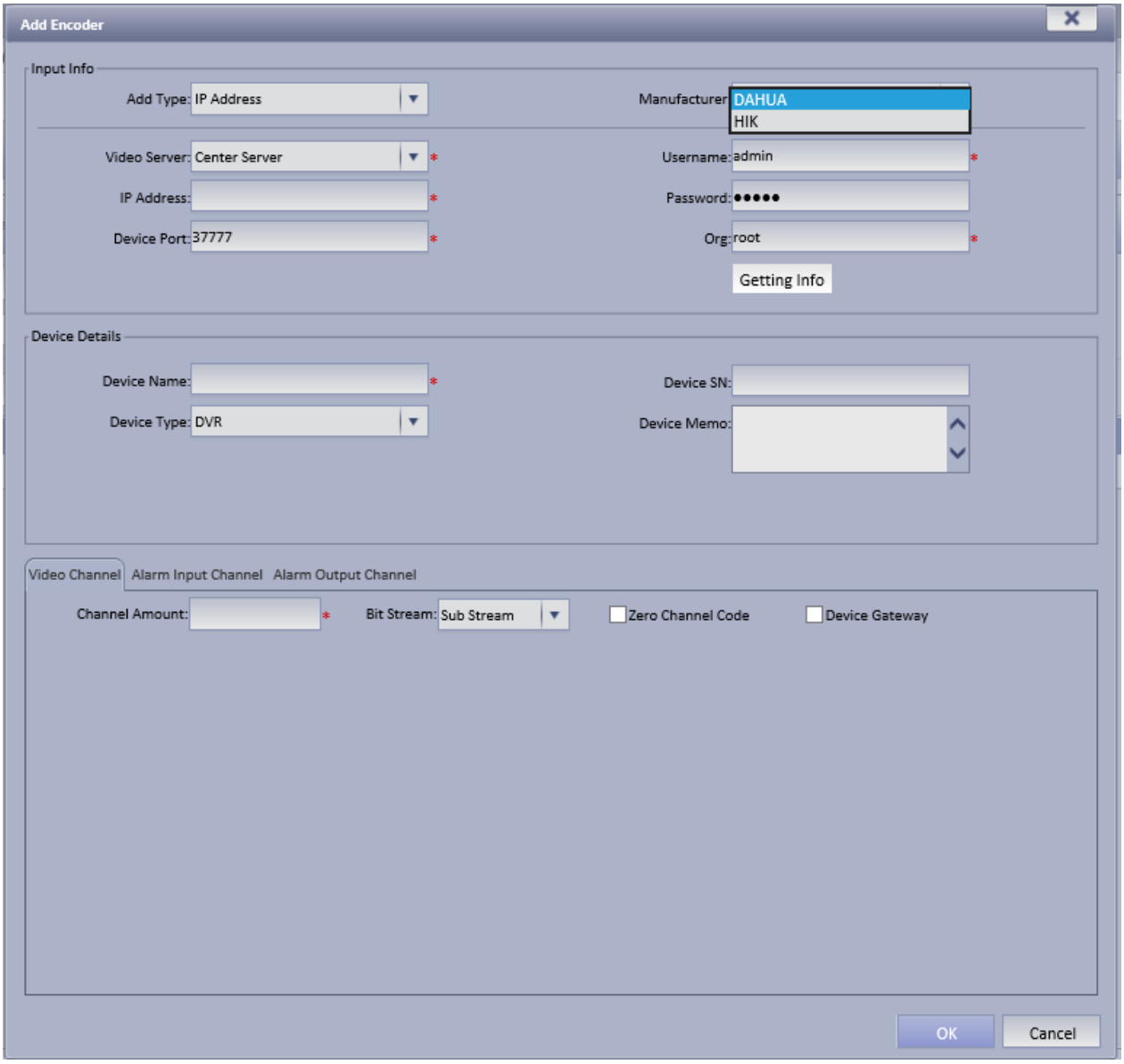


Figure 5-1

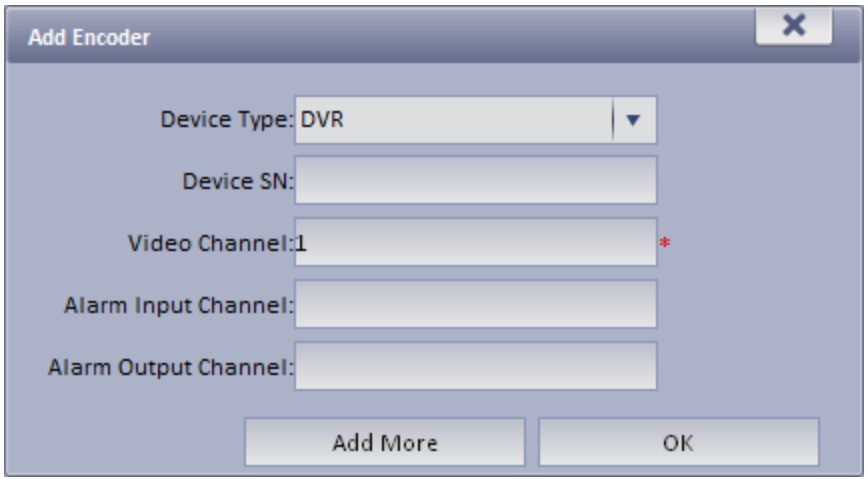


Figure 5-2

Parameter	Note
Add Type	You can add device via the following methods: ● IP Address: If the device has static IP address, you can add

Parameter	Note
	device with its IP address. ● IP Section: If there are multiple devices with continuous IP address, such as 192.168.1.50～192.168.1.100, and their port no., channel number and other parameters are the same, you can add these devices as batch by entering starting IP and end IP. ● Domain Name: If you do not know IP the device, you can its domain name. ● Auto Register: When front-end device has dynamic IP address or in LAN, you shall add device via auto register. For example, add mobile device via auto register. ● ONVIF: When device supports ONVIF protocol, you can add device via ONVIF.
Video Server	Server where the device belongs to. Click the box and you can select corresponding organization in prompt box.
Device Type	System supports to add device types including: DVR, IPC, NVS, MDVR, NVR, Smart NVR, MPT3000, EVS, Smart IPC, VIT.
Zero Channel Code	Combine multiple windows into one channel transmission.
Device Gateway	● If select this parameter, then enable device input gateway. When you select transcoding, you need transcoding server. ● If not select this parameter, then not enable this function.
Enable All	● If select this parameter, then enable all channels of the alarm output device. ● If not select this parameter, then not enable channel of the alarm output device and cannot preview at Client. By default, enable all is checked and is recommended.

Chart 5-1

Step 7. Click OK as finishing adding encoder.

If you want to continue adding encoder, please click Add More.

5.1.2 **Auto Search Encoder**

Channel in the same LAN with platform server can use Auto Search function to add.

Step 1. In Device interface, select one organization node.

Step 2. Click 

. See Figure 5-3.

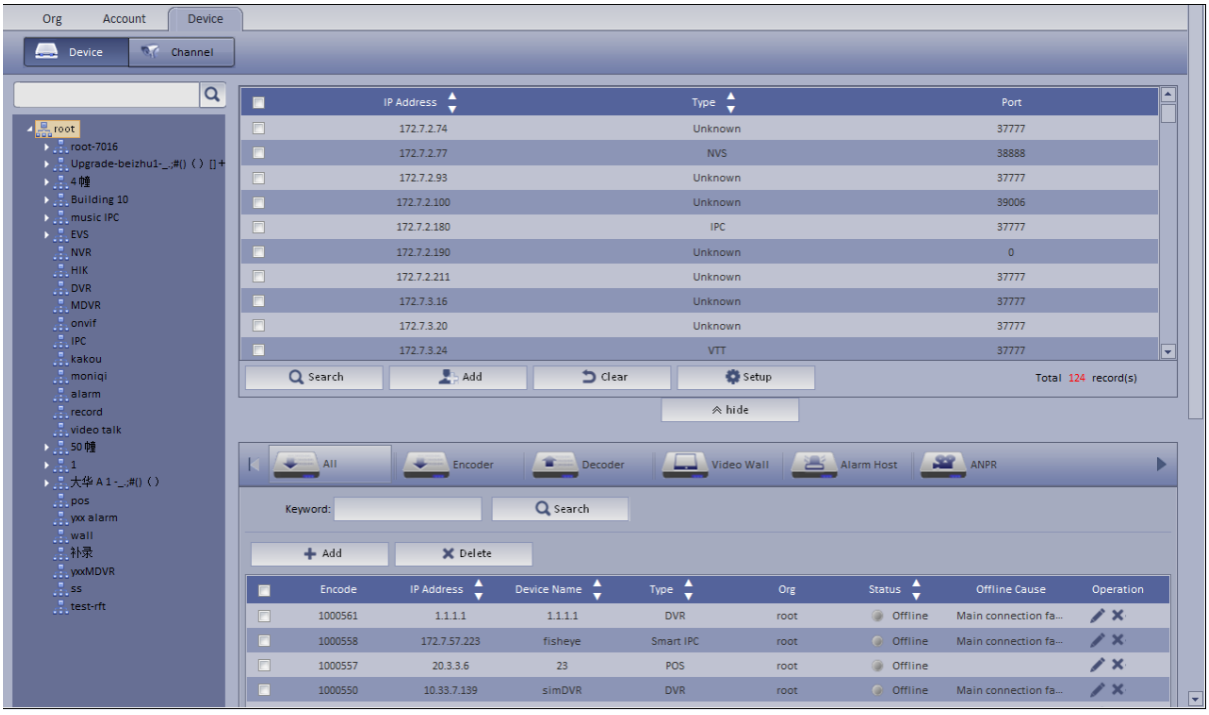


Figure 5-3

Step 3. Click 

, you can re-config IP segment and click Search to search all devices within this IP range.

Step 4. Check device you want to add and click 

.See

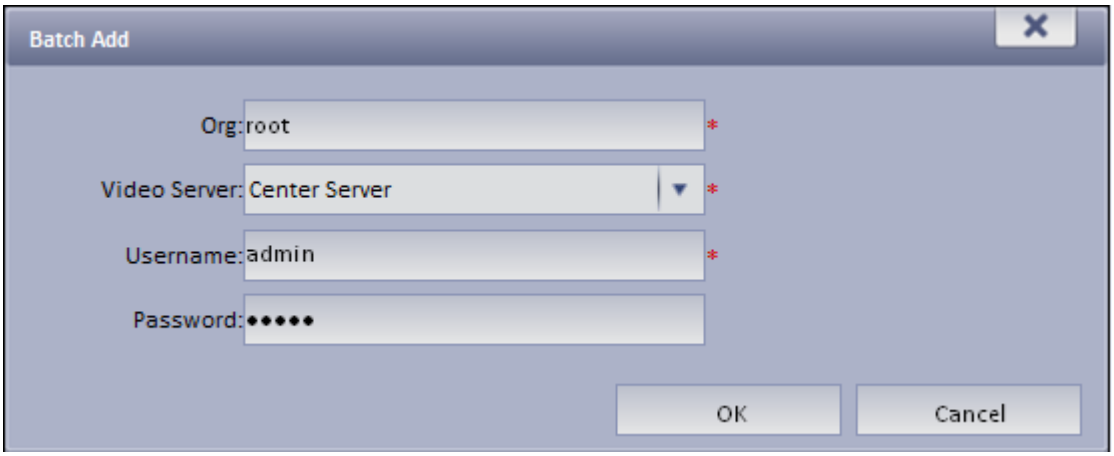


Figure 5-4

Step 5. Select Org, video server, enter username and password. Username and password are device login username and password, which shall both be “admin” by default.

Step 6. Click OK. System adds the device into corresponding organization.

5.2 **Preview**

Step 1. Login KBiVMS Client.

Step 2. Click  in Basic area. System shows Live Preview interface.

Step 3. In device list on the right, select channel and double click or drag it to video window. If you double click device, then all channels under this device will be open.

Video window shows live preview, see Figure 5-5.

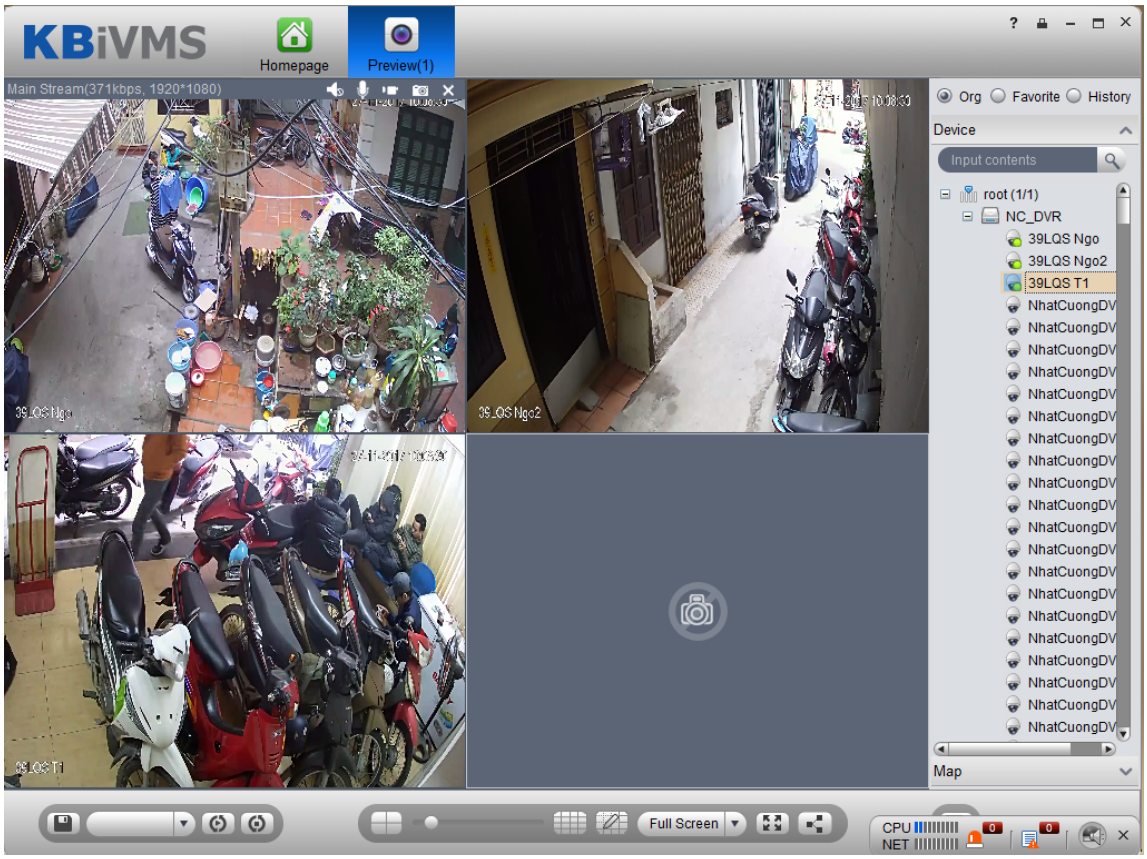


Figure 5-5

You can click  in video window to locally record; click  to snapshot. Record and snapshot can be set in Local Config under Setup Manager area.

Right click video window, select TV wall. You can output video to wall in two ways, one is to select window decoding in Live Preview, and the other is to select TV wall task layout and execute output.

➢ Via Live Preview window decoding, see Figure 5-6.

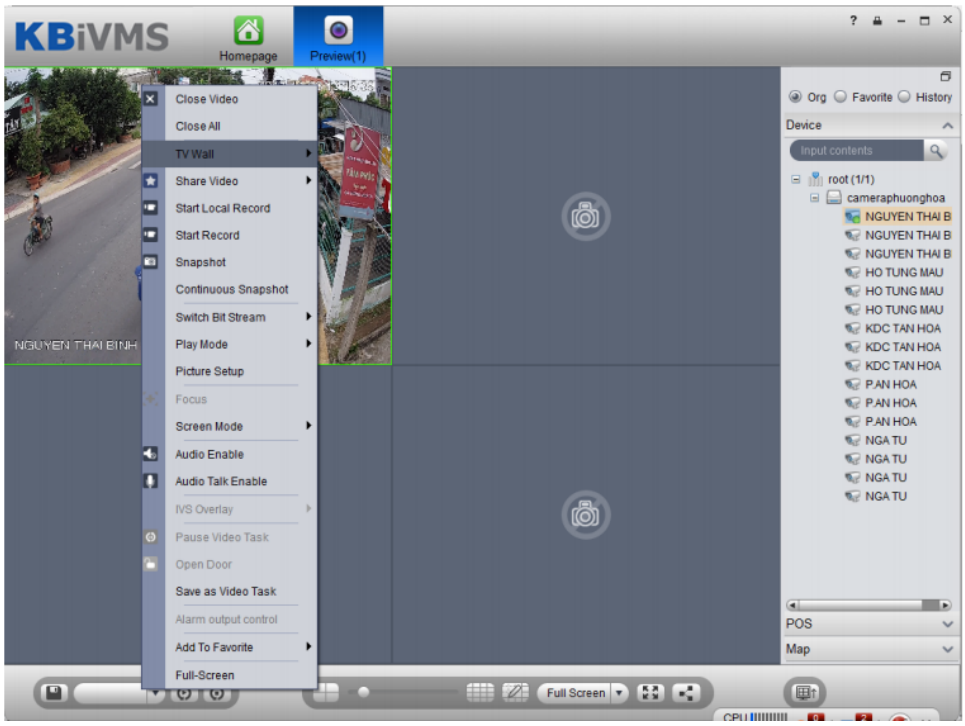


Figure 5-6

➢ Select layout set in TV wall task to execute wall task, see Ch 5.4

5.3 **Window Mode**

Client Live window supports general mode, 1+3 mode, 1+5 mode preview.

In Live window, right click and select Screen Mode, see Figure 5-7.

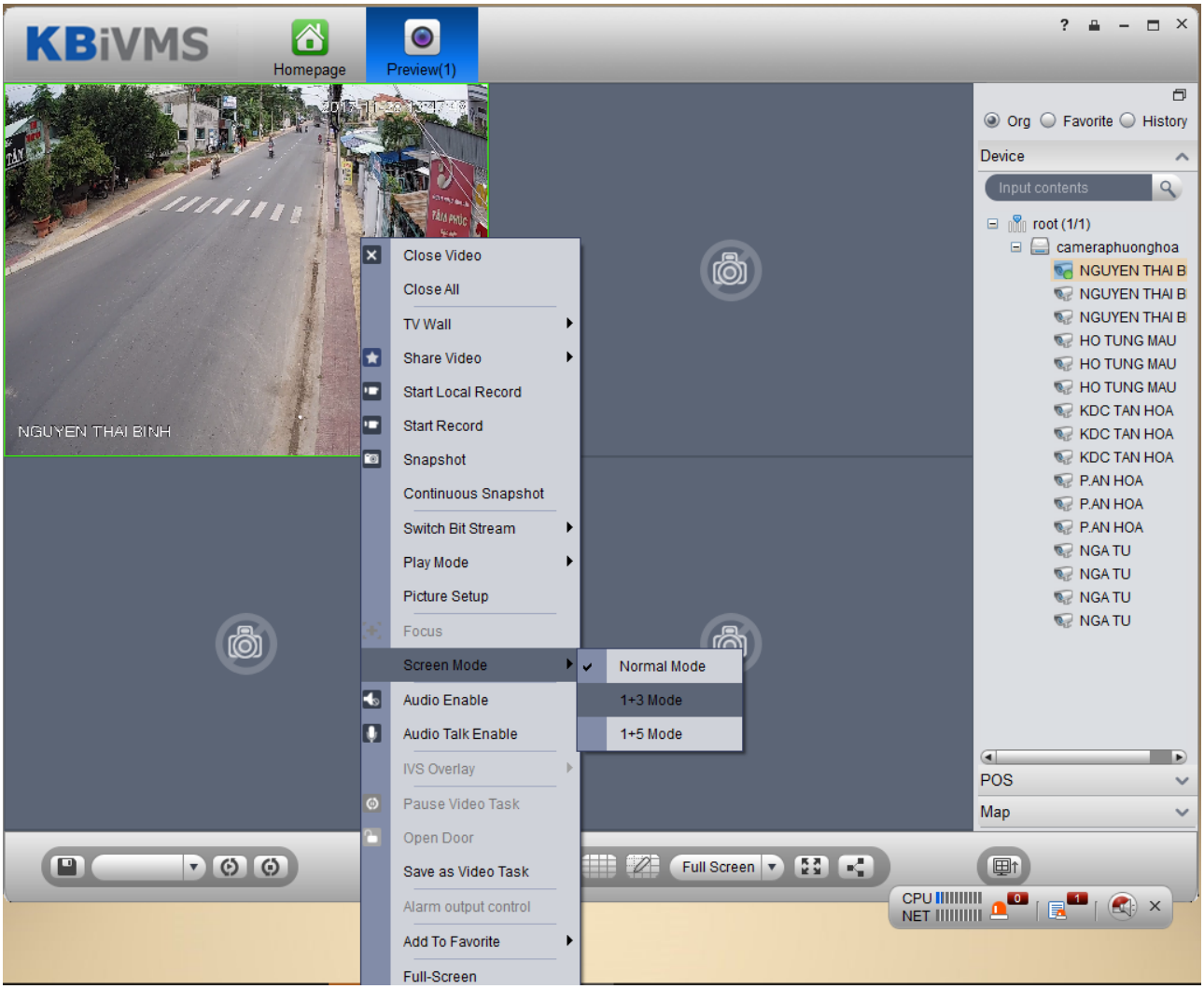


Figure 5-7

For example, select 1+3 mode, see Figure 5-8.

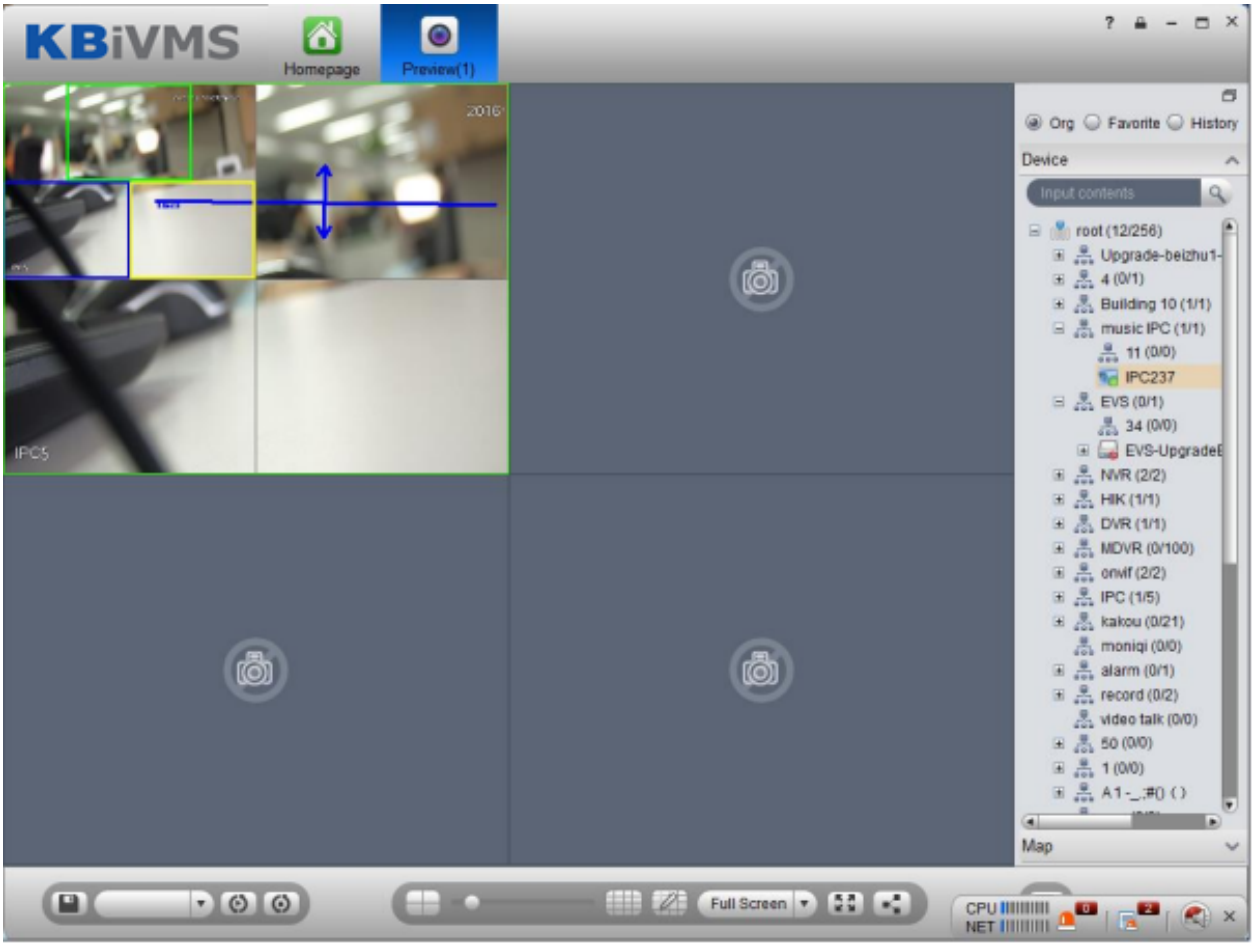


Figure 5-8

5.4 **Device Tree Pop-up**

Click  , see Figure 5-9.

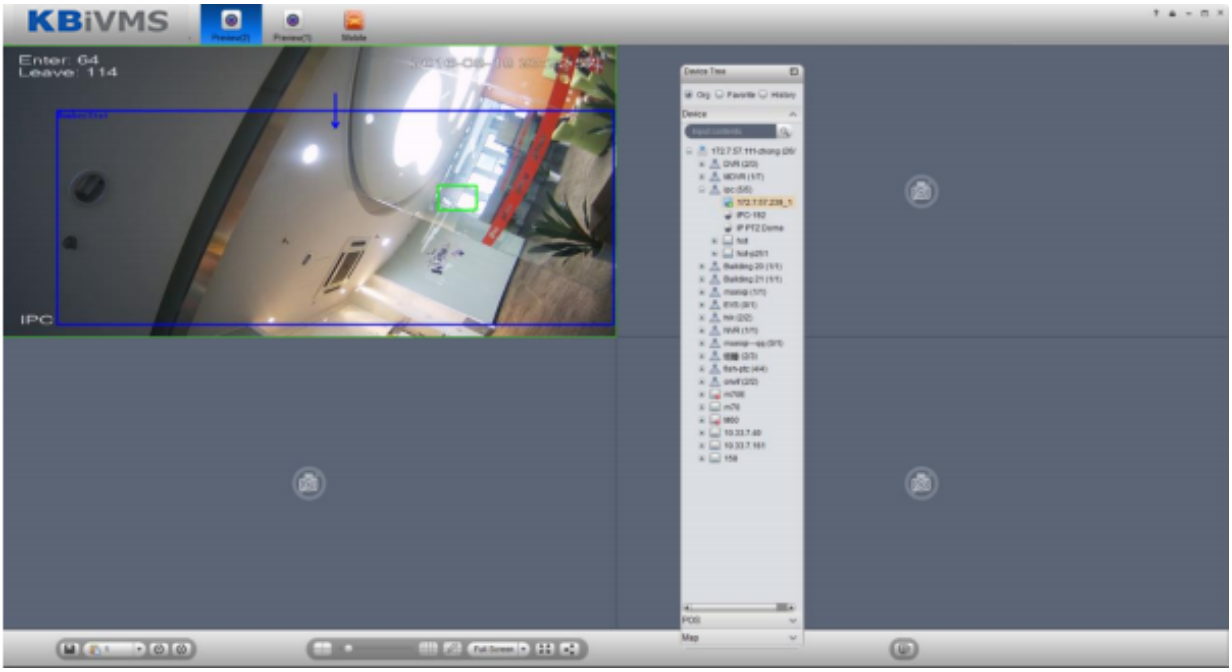


Figure 5-9

After device tree pops up, you can freely move position, and click  to restore, or drag device

tree to left or right side of client.

5.5 Live Video Wall

Note:

Before output video to video wall, make sure you have added TV wall and video wall task, please refer to Ch 9.2 and 9.3 for details.

Step 1. In Preview interface, click  at the lower right corner.

Step 2. Select TV wall, task. See Figure 5-10.

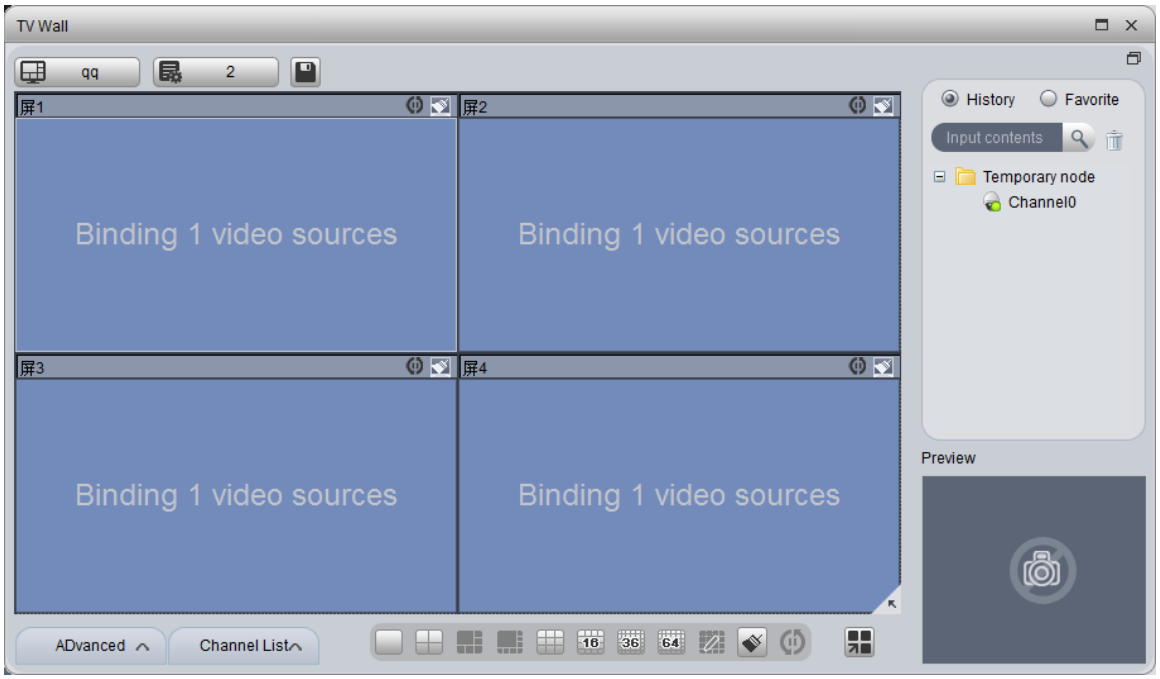


Figure 5-10

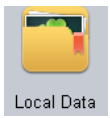
Step 3. Click  to output to wall.

In video window, right click mouse and select TV wall, you also can select wall layout to output.

5.6 Local Data

Snapshot picture and record will be saved in local disk.

You can search saved local data, as saved record and snapshot in Local Data interface.

Step 1. Click on 

in Setup Manager area. System pops up Local Data interface.

Step 2. On the right, select device channel.

Step 3. Config start time and end time. Select data type (picture, video) or use advanced search.

Step 4. Click on Search. See Figure 5-11.

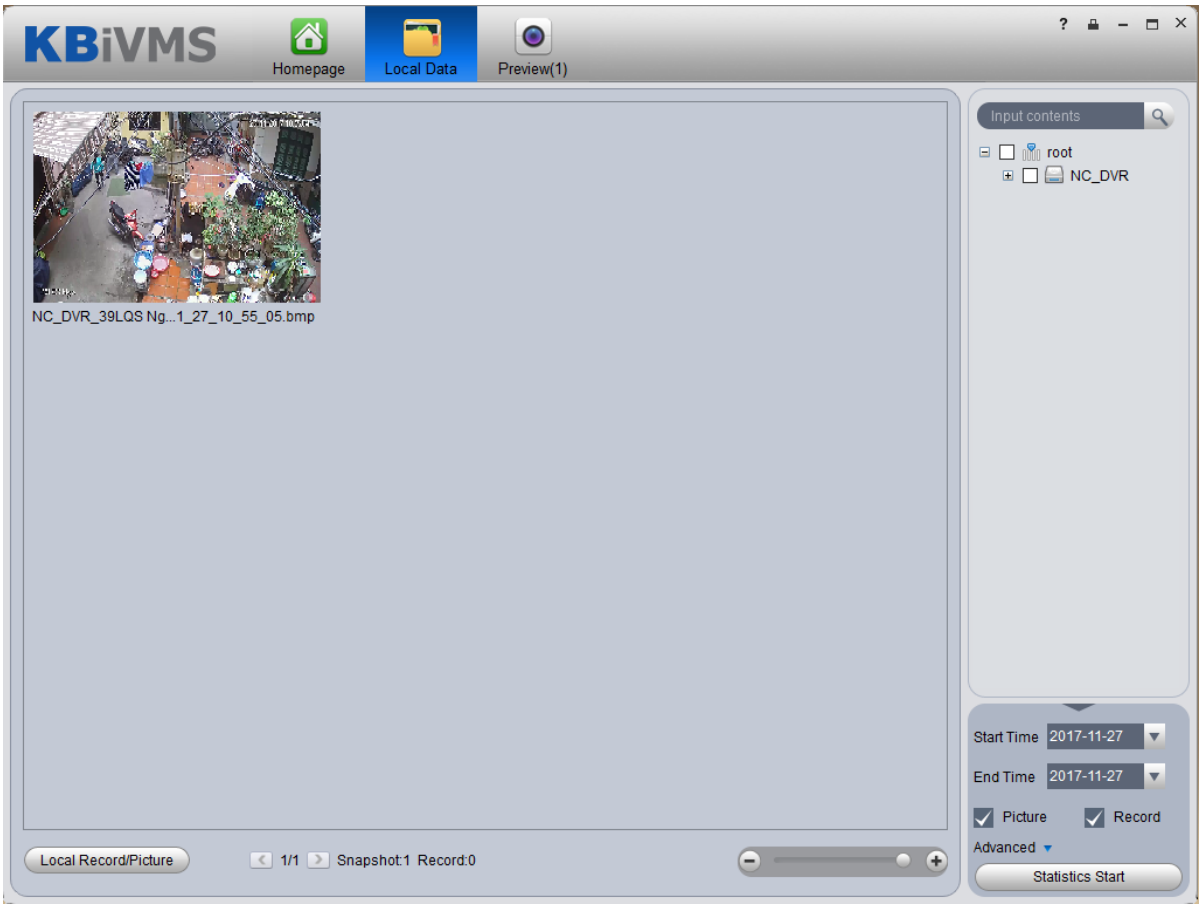


Figure 5-11

Step 1. Right click searched picture or record, you can copy, cut and delete the picture or record. You also can open path where the picture and record stored.

Step 2. Double click picture, you can view detailed info of picture.

Step 3. Double click record, you can view detailed info of record and playback the record.

Step 4. Click Local Record in the lower left corner, you can open local record storage path.

Step 5. Click  to adjust picture size.

5.7 **Fisheye**

KBiVMS Platform supports fisheye device installation, which includes ceiling, wall mount and grounding.

Step 1. Login KBiVMS Client Manager.

Step 2. Select General>Device>Device.

Step 3. Click Add. System pops up Add Encoder box, see Figure 5-12.

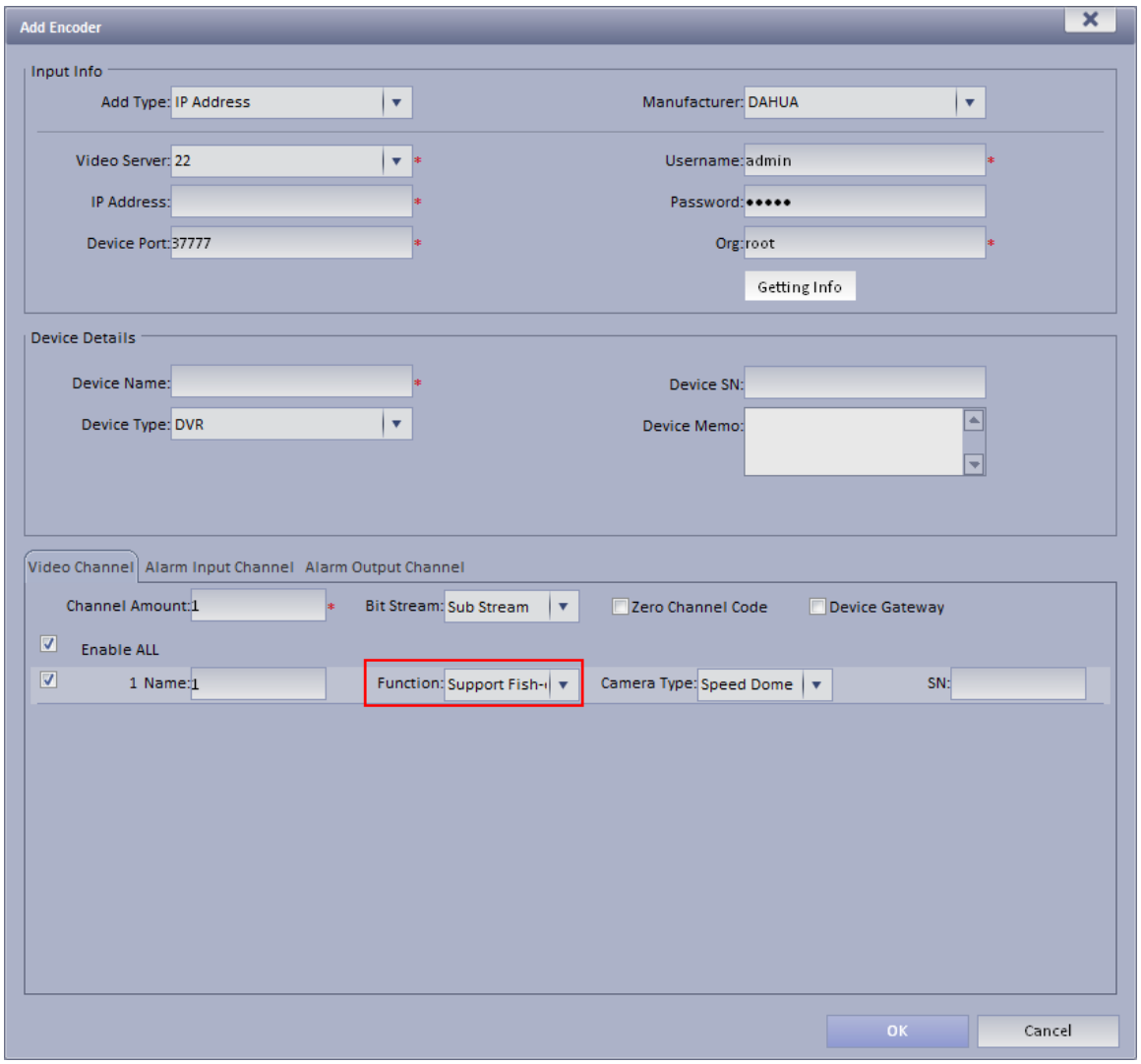


Figure 5-12

Step 4. Configure fisheye device parameter, for “function”, select support fisheye.

Step 5. Click OK. Login KBiVMS Client.

Step 6. Click  .

Step 7. Double click fisheye device on the right. Ceiling installation has 8 types, see Figure 5-13 as there are “1+8” types.

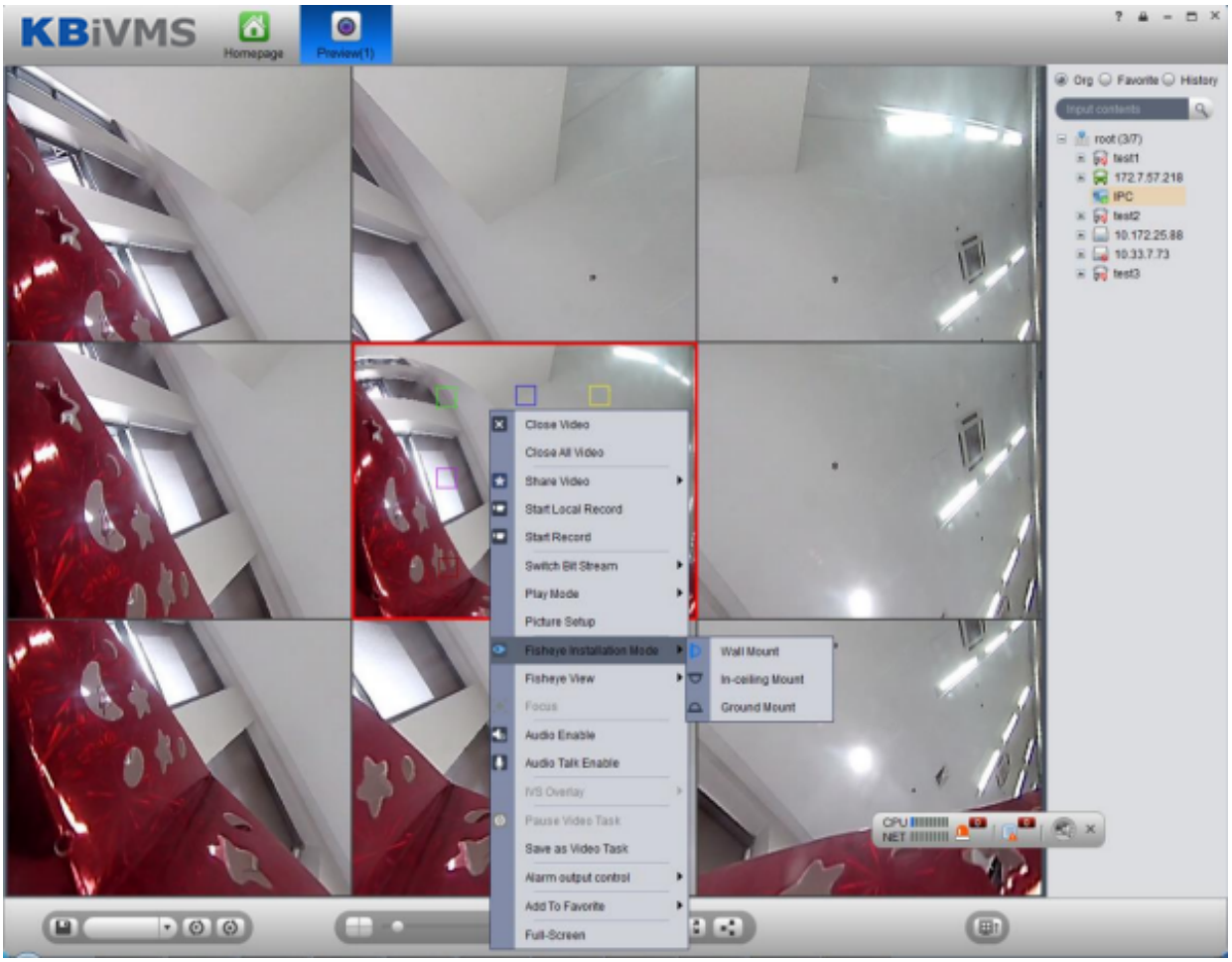


Figure 5-13

The fisheye in the center splits into 8 scenes. You can drag mouse to one of these blocks, such as: , and its corresponding box will rotate.

Wall mount includes 5 types while grounding includes 7 types.

5.8 Tour Task

5.8.1 Tour Task

You can set tour task to achieve tour over several windows. To set tour task:

Step 1. Click 

in Setup Manager area. System displays Tour Task interface.

Step 2. Click  . System displays add task interface.

Step 3. Input Task Name, Description and select Window No.

Step 4. Drag designated device on the right to left window for setup as in Figure 5-14.

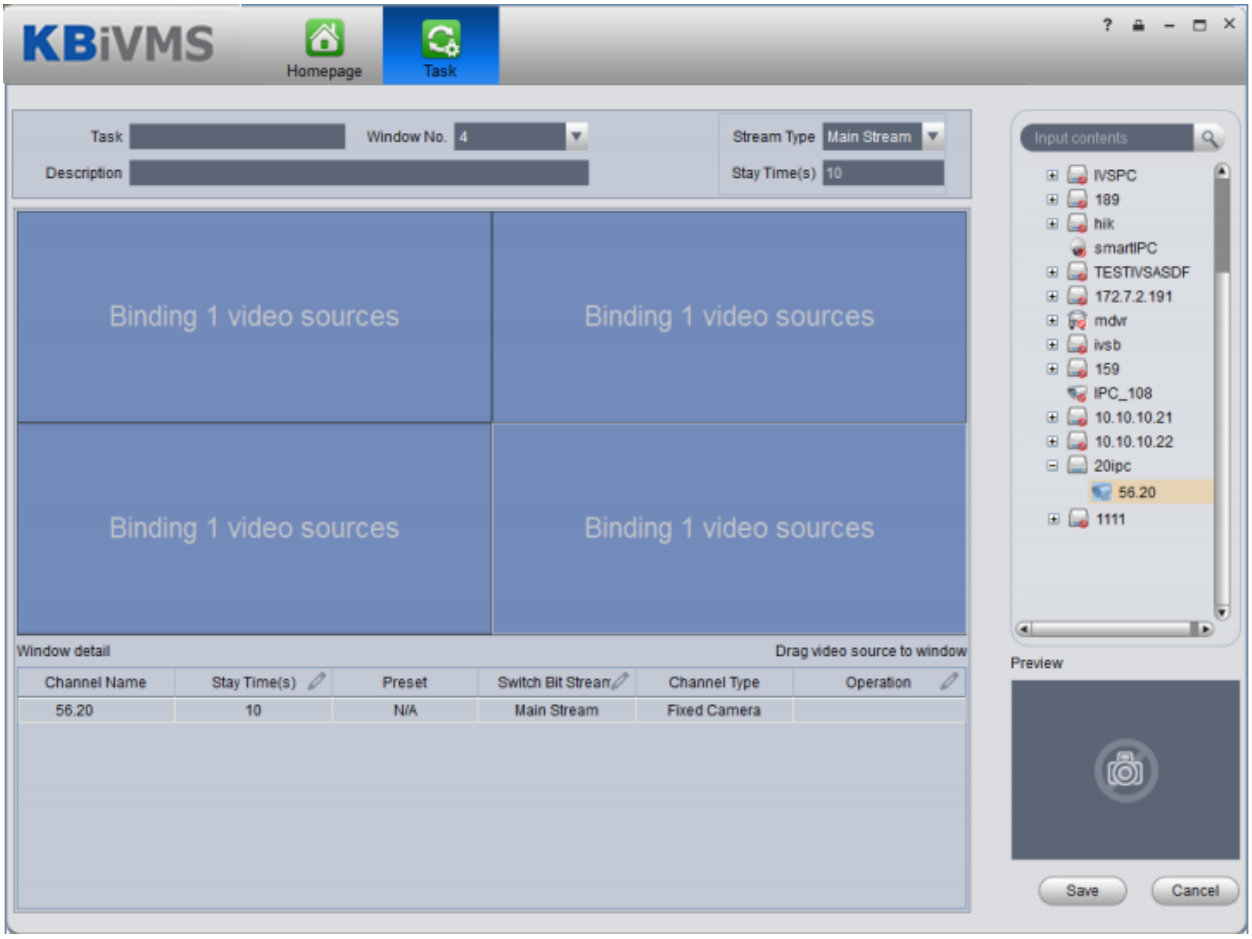


Figure 5-14

- Click , so you can viewo video in Preview in the lower right to view it.
- Click , to adjust sequence, or click to delete added channel on the left.

Step 5. Click Save.

See Figure 5-15.

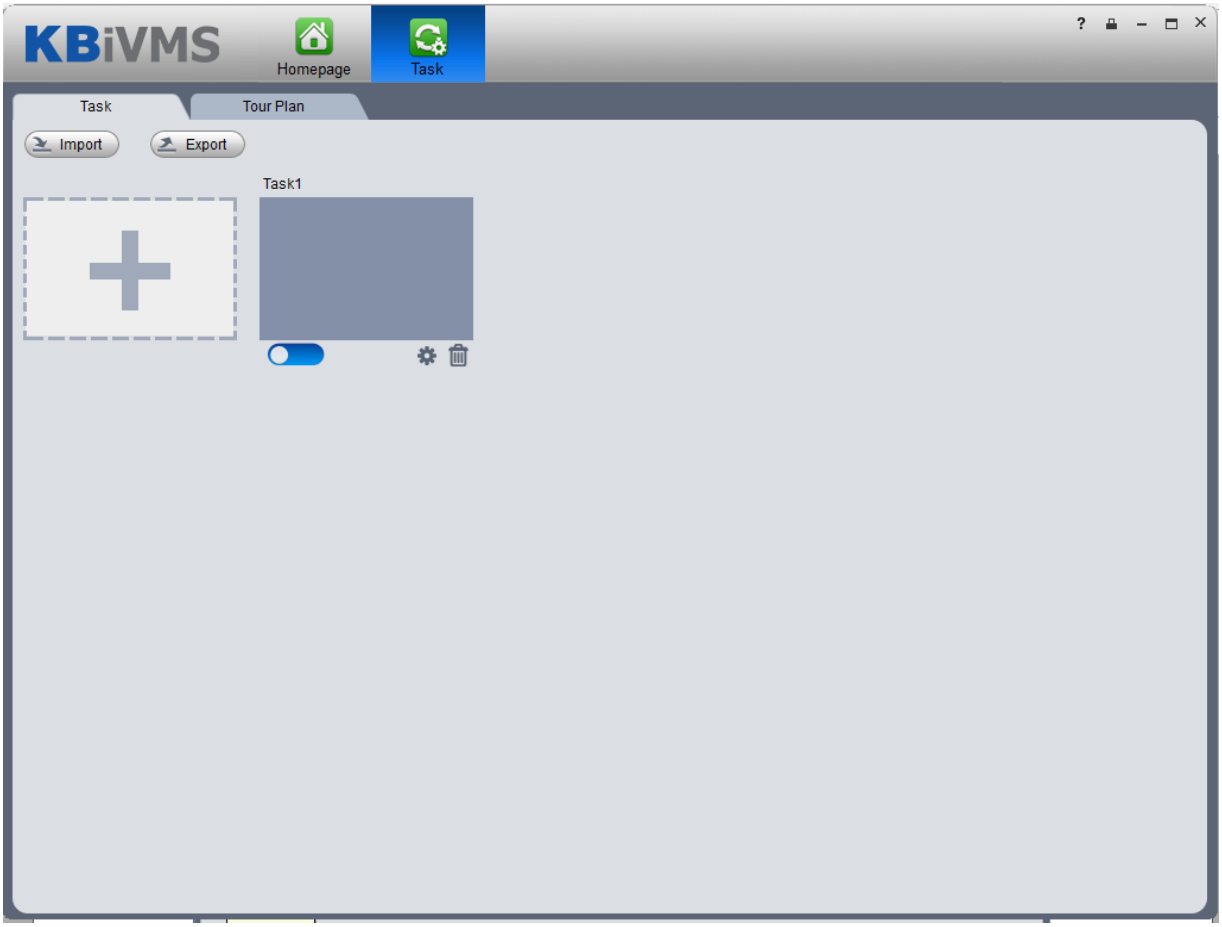


Figure 5-15

To enable tour task, there are two ways:

- In Tour Task interface, click  to turn on tour task. You can now view monitoring status of tour channel in Preview interface.
- In Preview interface, select tour task in the lower left, and click start.

5.8.2 Tour Plan

By configuring tour plan, you can achieve start time and end time of each tour plan.

Step 1. Click  in Setup Status area, select Tour Plan tab.

Step 2. Click  .

Select wither Schedule or Tour Plan.

Note:

: schedule, may specify time to execute plan.

: tour plan, may specify tour plan with interval period.

- Select schedule
  See Figure 5-16.

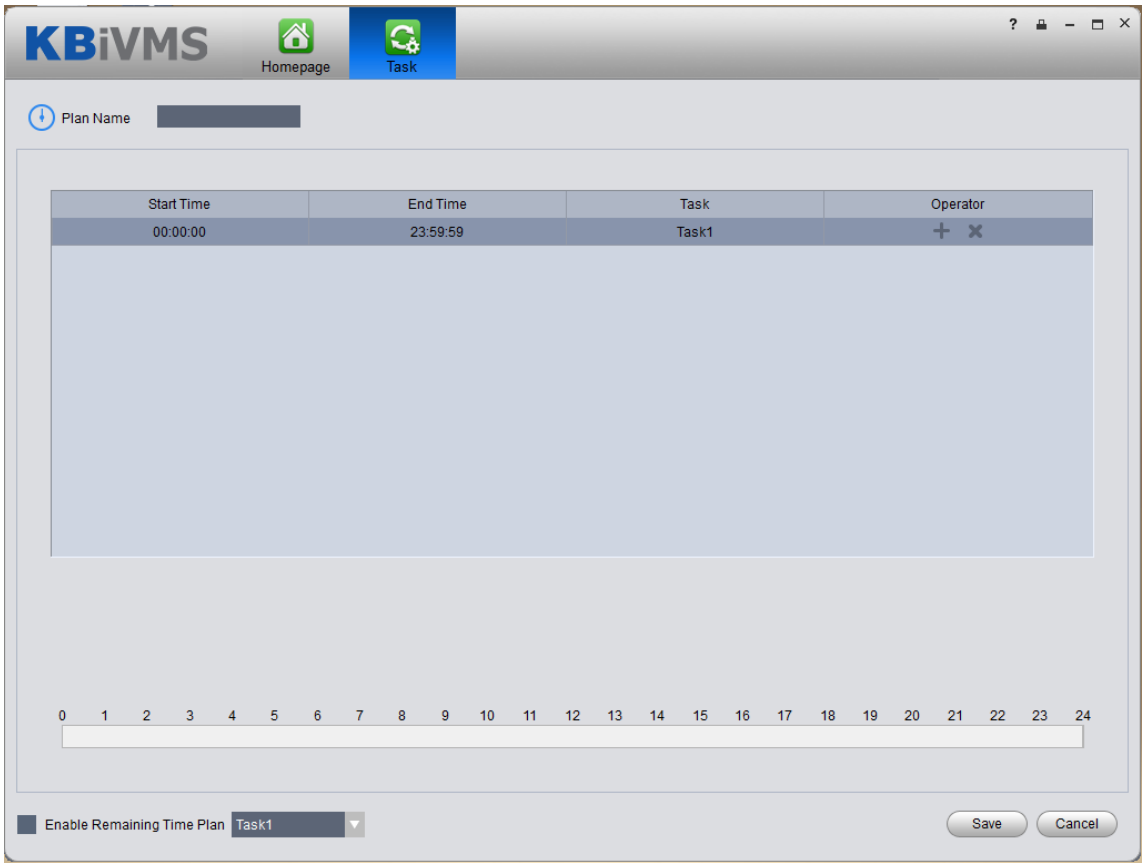


Figure 5-16

1. Input plan name, select start time and end time.
2. Click  to add tour plan.
3. Check Enable Remaining Time Plan, click Save.
   Note:
   Enable Temaining Time Plan: It means the plan to be executed at remaining time period other than absolute time period.

- Select tour plan

1. Configure corresponding parameter.
   See Figure 5-17.

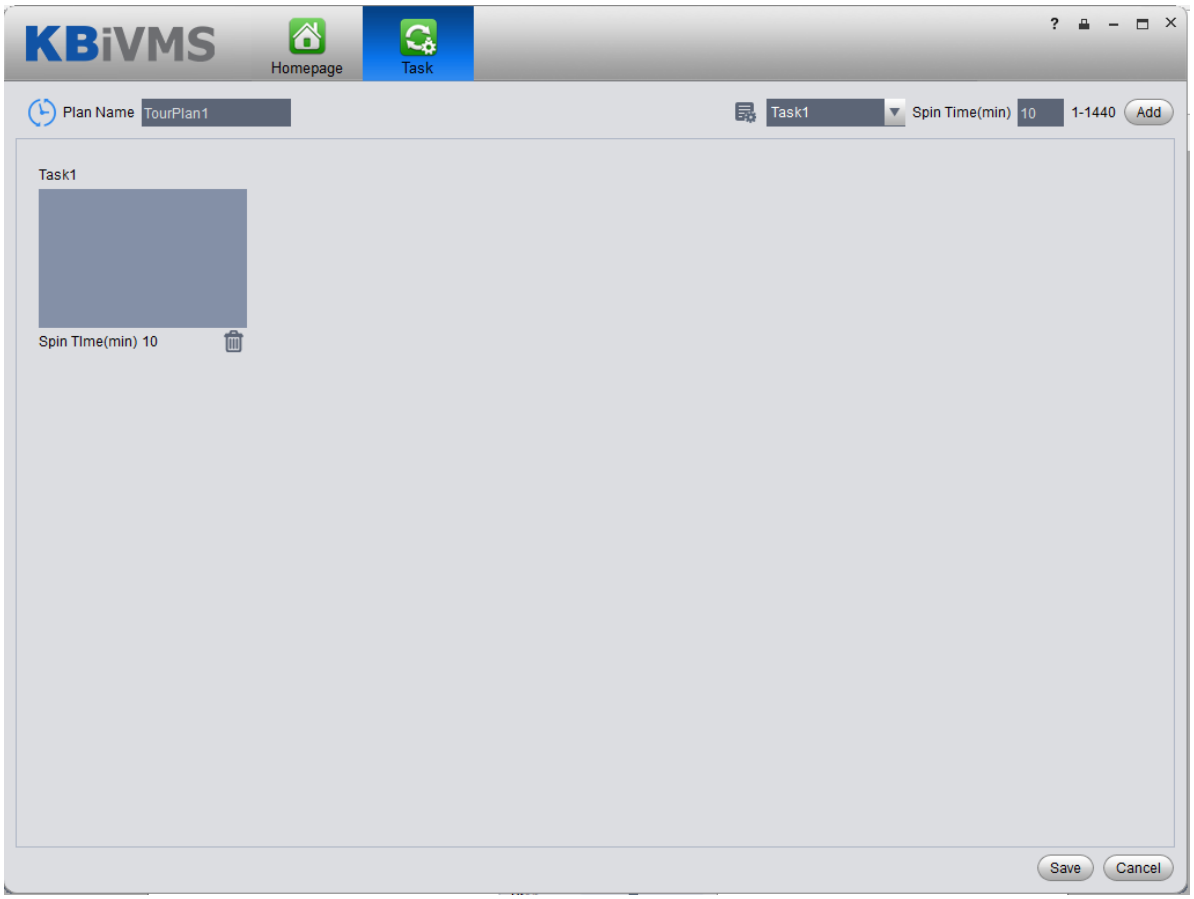


Figure 5-17

2. Click Save.
   See Figure 5-18.

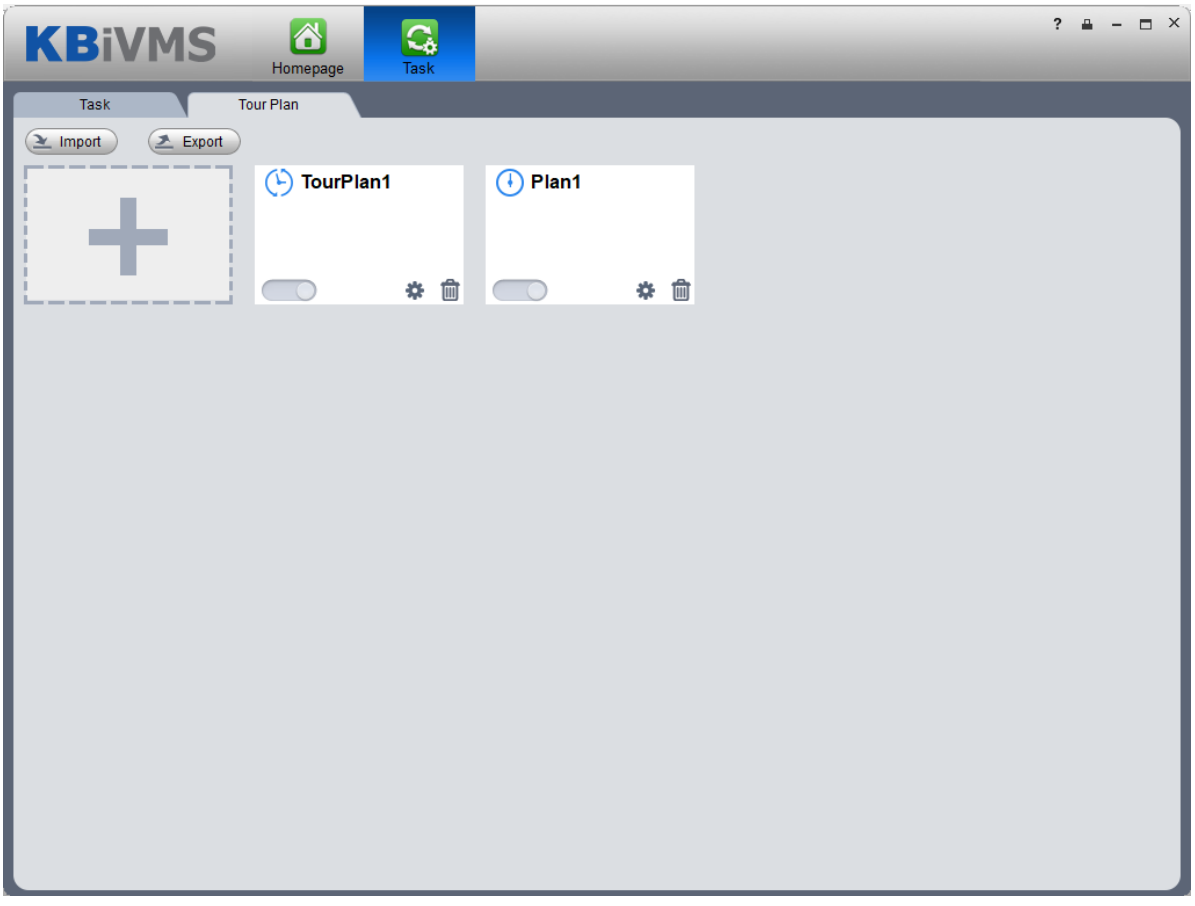


Figure 5-18

Click Import to import existing plan. Click Export to export plan.

5.9 PTZ

If device type is speed dome, then you can click PTZ tab in the interface to set PTZ as in Figure 5-19.

Figure 5-19

Parameter	Note
	Click to lock current PTZ. Lock status is . Based on current user level, control over PTZ may vary. ● When low-level user lock the PTZ, high-level user can click to unlock. ● When high-level user lock the PTZ, low-level user cannot unlock it until it is automatically unlocked. ● User of same level can unlock PTZ that lock by each other. **Note:** **PTZ default unlock time is 30s.**
	Control speed dome with mouse.
Direction key	It sets rotation direction of PTZ in eight directions as up, down, left, right, upper left, upper-right, lower-left, lower-right.

Parameter	Note
	Partial zoom for zoom in/out of certain area. **Note:** **This function can only be controller with mouse.**
Step Length	It controls rotation speed of PTZ in 1~ 8 directions with different step lengths.
Zoom	It controls zoom of speed dome.
Focus	It adjusts focus.
Iris	It adjusts brightness.
Preset	Via setting preset, you can rotate camera toward position of the preset.
Tour	Via setting tour, you can tour camera among different presets. **Note:** **This function does not require support from speed dome, but speed dome must support preset.**
Aux	It adjusts light, wiper, PTZ menu, auto rotation, aux 1, aux 2 and IR light.

- Preset

By setting preset, you can rotate camera toward position of preset. To add preset:

Step 1. Click direction key on PTZ to rotate camera.

Step 2. Click Preset tab.

Step 3. Click Add. System pops up Preset Setup interface.

Step 4. Input SN and Name as in Figure 5-20.

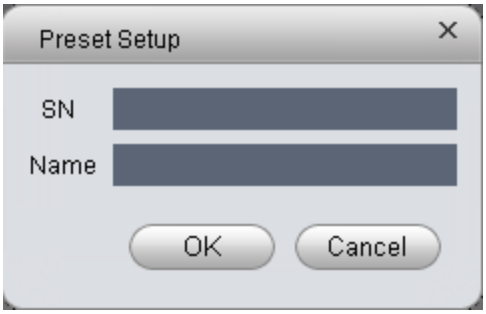


Figure 5-20

Step 5. Click OK.

When you need to rotate the camera toward designated position, you just need to select direction from the dropdown list, and click Go.

- Tour

Via set Tour, you can make camera tour among different presets.

Note: There must be at least two presets for tour.

To add tour:

Step 1. In PTZ interface, click Tour tab.

Step 2. Click Add. System pops up a new tour box.

Step 3. Input name and SN. In All Presets area on the left, select preset, and click Add. System adds presets on the left to list on the right as in Figure 5-21.

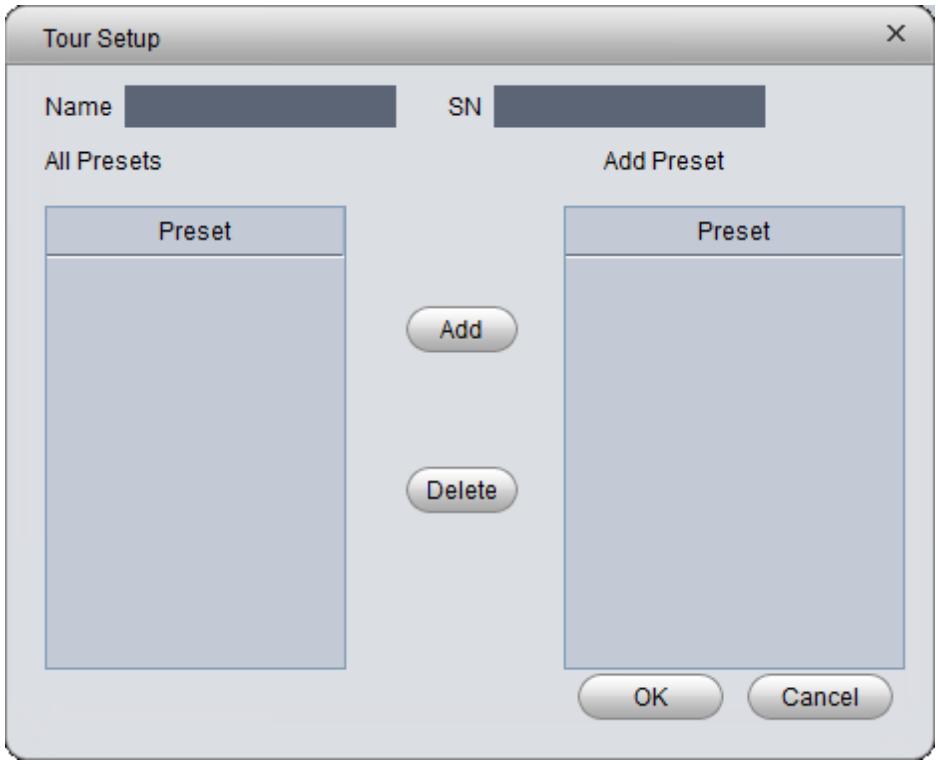


Figure 5-21

- Add Select preset on the left, click this button, presets will be added into list on the right.
- Delete Select preset on the right, click this button, presets will be deleted from the list on the right.
- Modify Stay Time, click Stay Time column of presets on the right to modify it. It ranges from 3s ~ 6000s.

Step 4. Click OK. System will say it is successfully saved.

Step 5. Click OK.

When you want to start tour, in Tour tab, select tour from dropdown list and click Start.

- Scan

Step 1. Select Scan from the dropdown list.

Step 2. Click PTZ button, rotate PTZ to a specific position toward left, click , set left border.

Step 3. Continue rotating PTZ to a specific position toward right, click , set right border.

Step 4. Click , to start scan, and PTZ will rotete back and forth within two borders.

- Pattern

Pattern is the path of scanning.

Step 1. In the dropdown list, click Pattern.

Step 2. In 

dropdown list, select pattern number, you can set 5 patterns.

Step 3. Click Setup>Start Record, operate 8 PTZ buttons, to start setup of pattern.

Step 4. Click Setup>Stop Record, setup is complete.

Step 5. Click Startup to start rotation according to setup.

5.10 **POS Function**

5.10.1 **Add POS Resource on Manager-end**

Before you can see POS transaction info on Client, you must add POS resource on KBiVMS Client Manager.

Two methods to add POS:

- Add POS signal to NVR, and NVR sends it to KBiVMS platform to save, so you can add NVR supporting POS.
- Install POS into conversion box, and match conversion box to platform.

Warning

Current POS info are all connected to NVR, and sent to KBiVMS Client Platform for storage via NVR later, so you just need to add NVR of POS.

Method 1:

Step 1. Login KBiVMS Client Manager.

Step 2. Select General>Device>Device.

System shows Device interface.

Step 3. Click 

.

Step 4. Click 

. System shows Add Encoder box, see Figure 5-22.

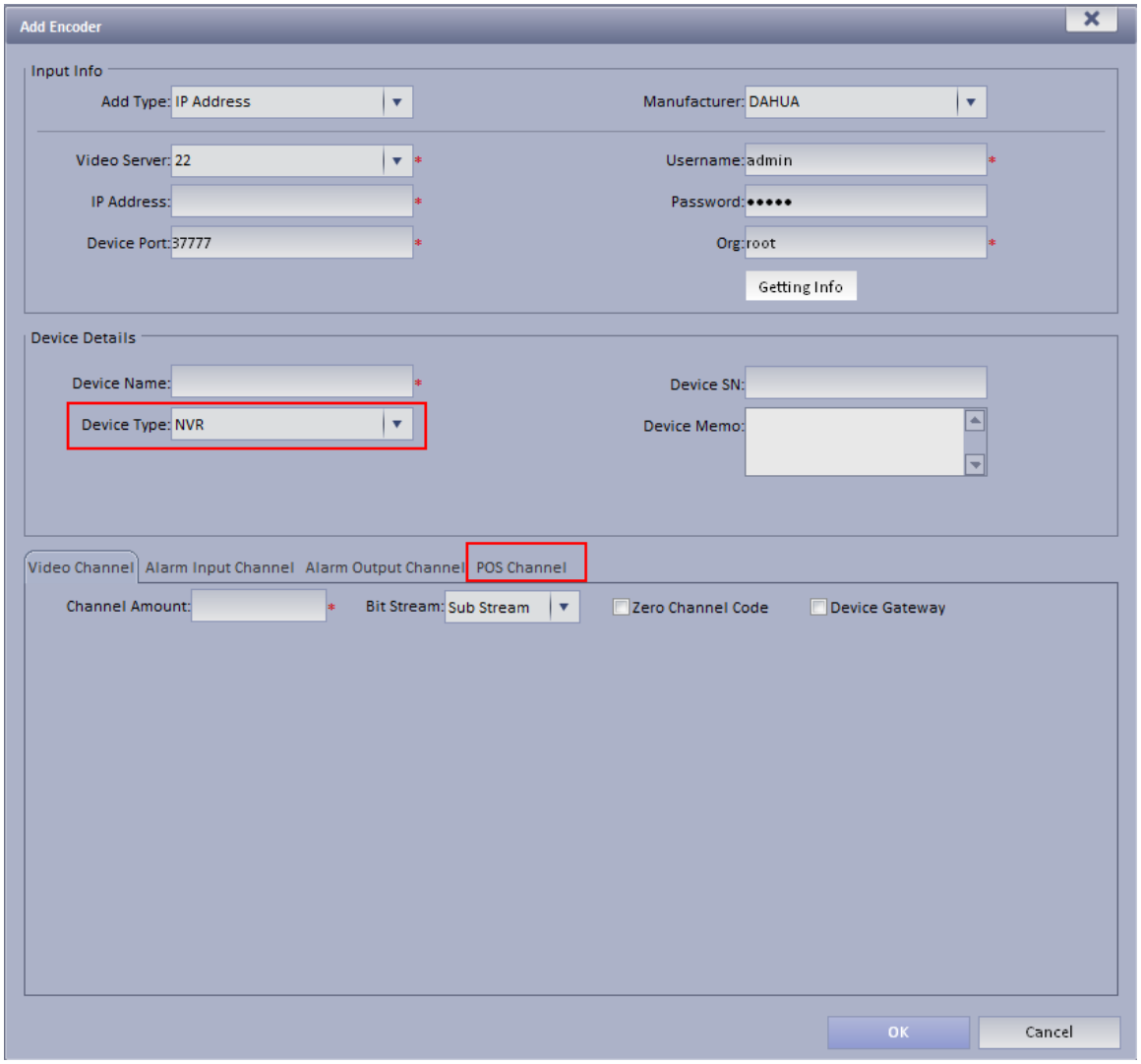


Figure 5-22

For device type, select NVR, then you will see POS tab.

Step 5. Configure POS device parameter, click OK.

Method 2:

Step 1. Select General>Device>POS.

Step 2. Click Add.

System pops up Add POS box, see Figure 5-23.

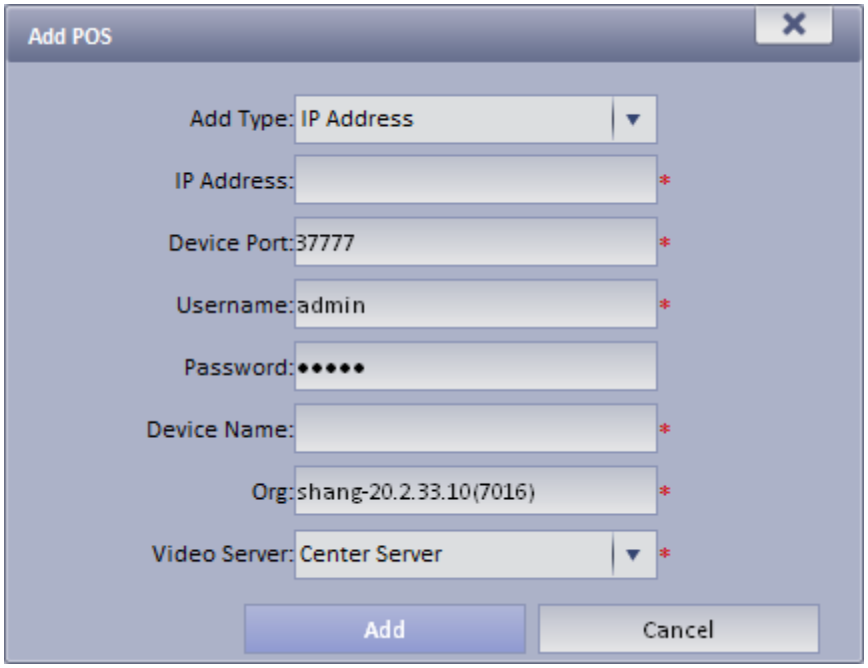


Figure 5-23

Step 3. Enter conversion box IP address, device name, click Add. See Figure 5-24.

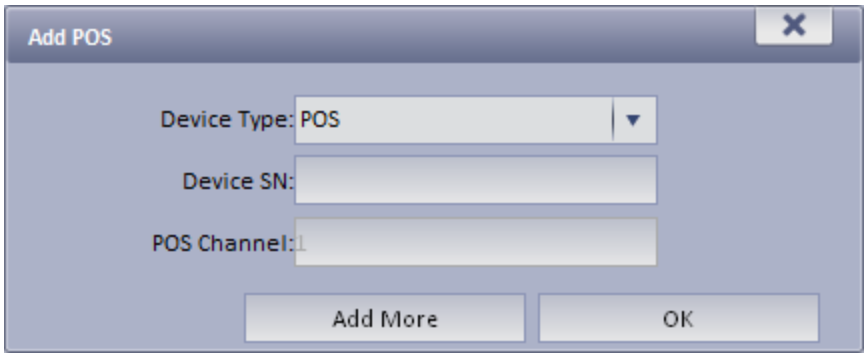


Figure 5-24

Step 4. Enter device SN, click OK. If you want to add multiple POS conversion boxes, click Continue to Add.

5.10.2 **Link POS Video Resource**

Step 1. Select Business>Resources Binding>POS.

Step 2. Click Setup. See Figure 5-25.

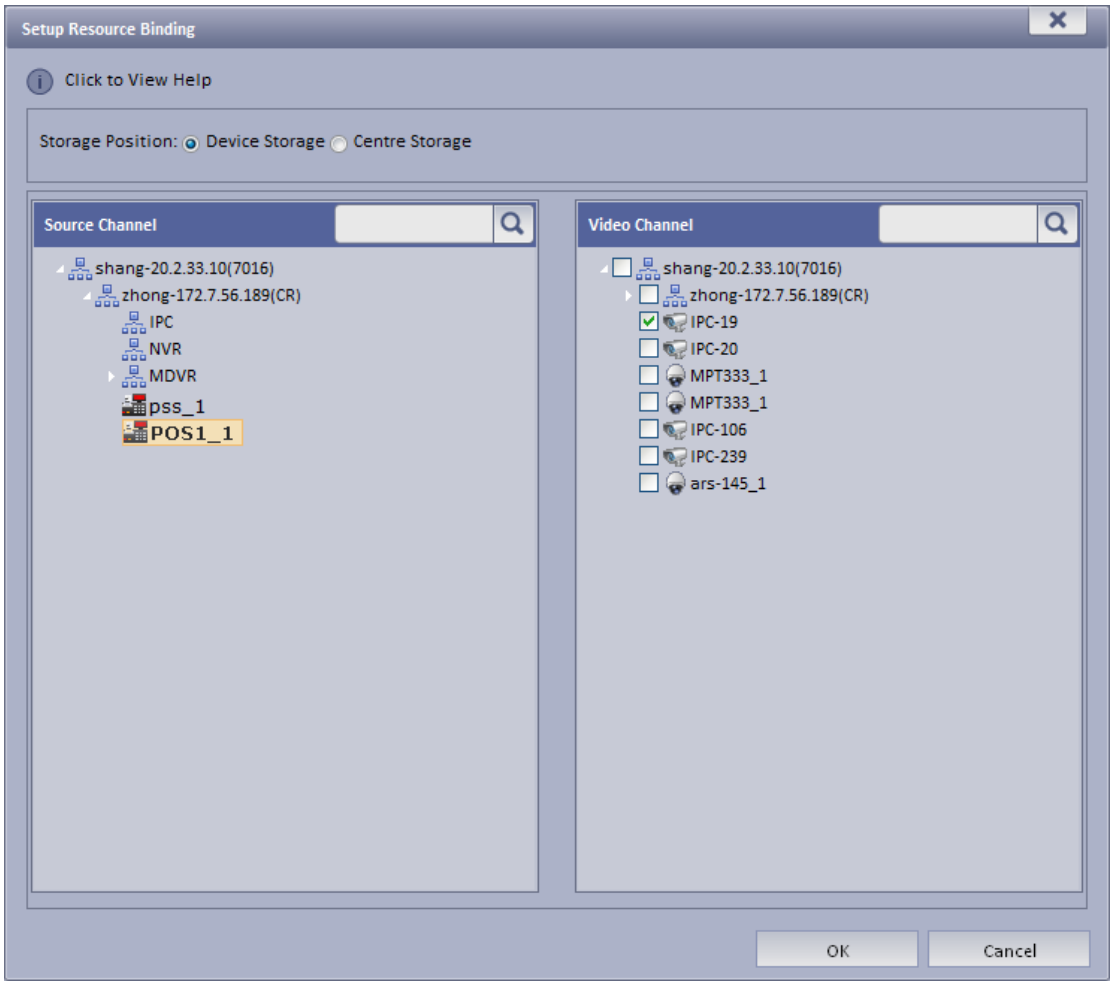


Figure 5-25

Step 3. In resource channel on the left, select POS device, and select link channel on the right.

Note:

One POS device can link up to 16 video channels.

Step 4. Click OK.

5.10.3 **Link POS Video Resource**

Step 1. Select Business> Resources Binding> POS.

Step 2. Click Setup.

See Figure 5-26.

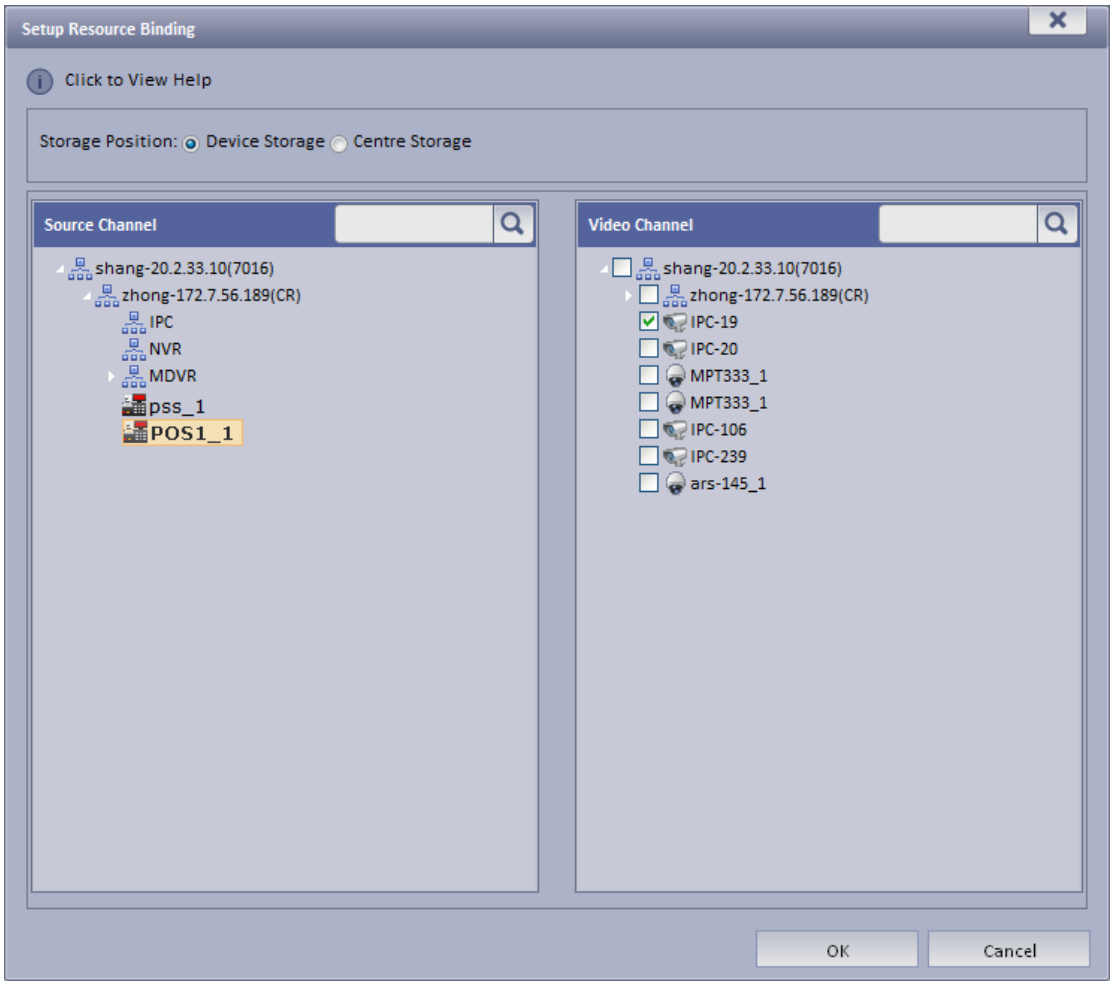


Figure 5-26

Step 3. In source channel on the left, select POS device, and bind channel in video channel on the right.

Note:

One POS device can bind up to 16 video channels.

Step 4. Click OK.

5.10.4 **Use POS Function on Client**

Step 1. Login KBiVMS Client.

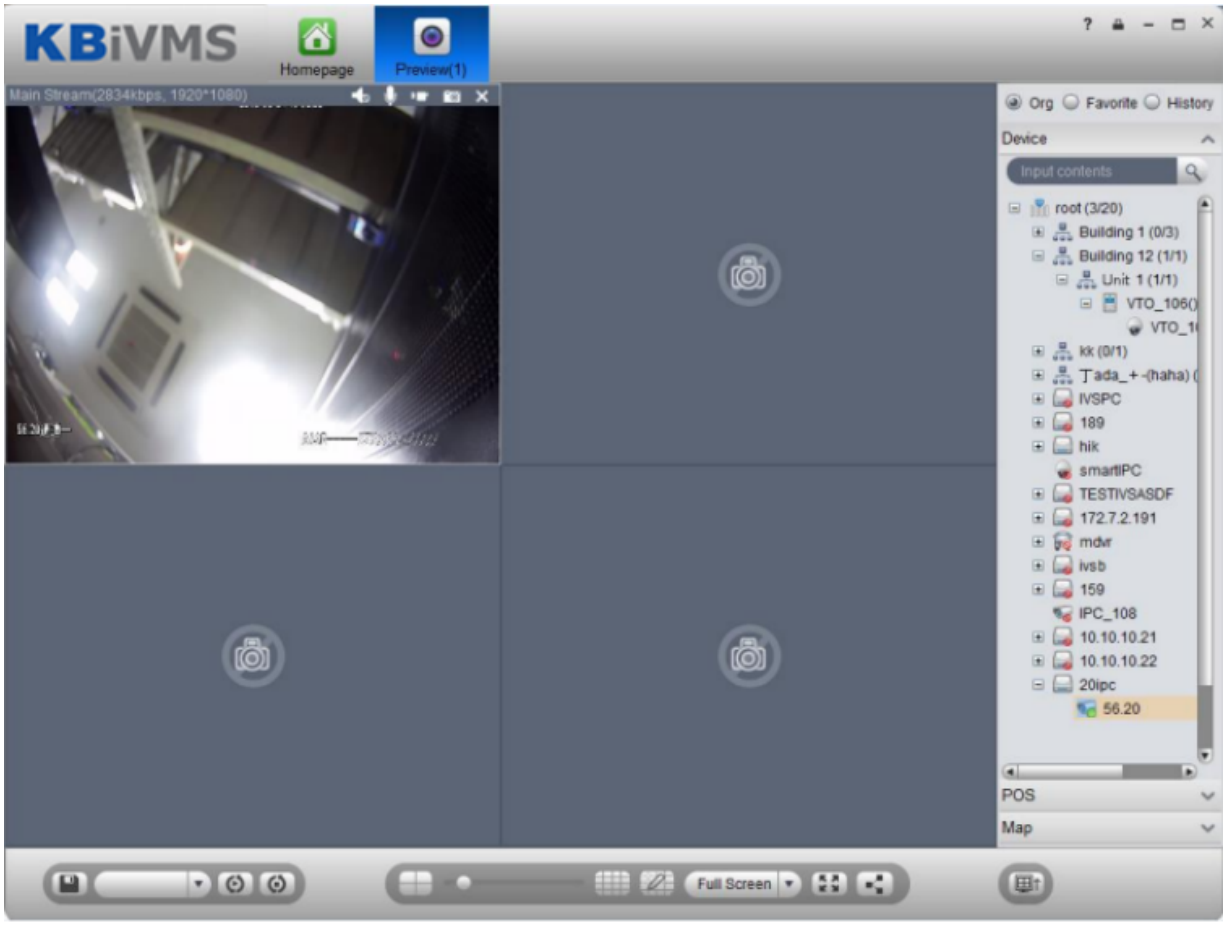


Figure 5-27

Step 2. In Live Preview, click POS tab on the right.

Step 3. If you swipe card on POS device, then it will refresh POS card record in window on the left and play linked video.

Note:

Linked video channel will all open, up tp 16 channels, in self-adaptive mode. See Figure 5-28.

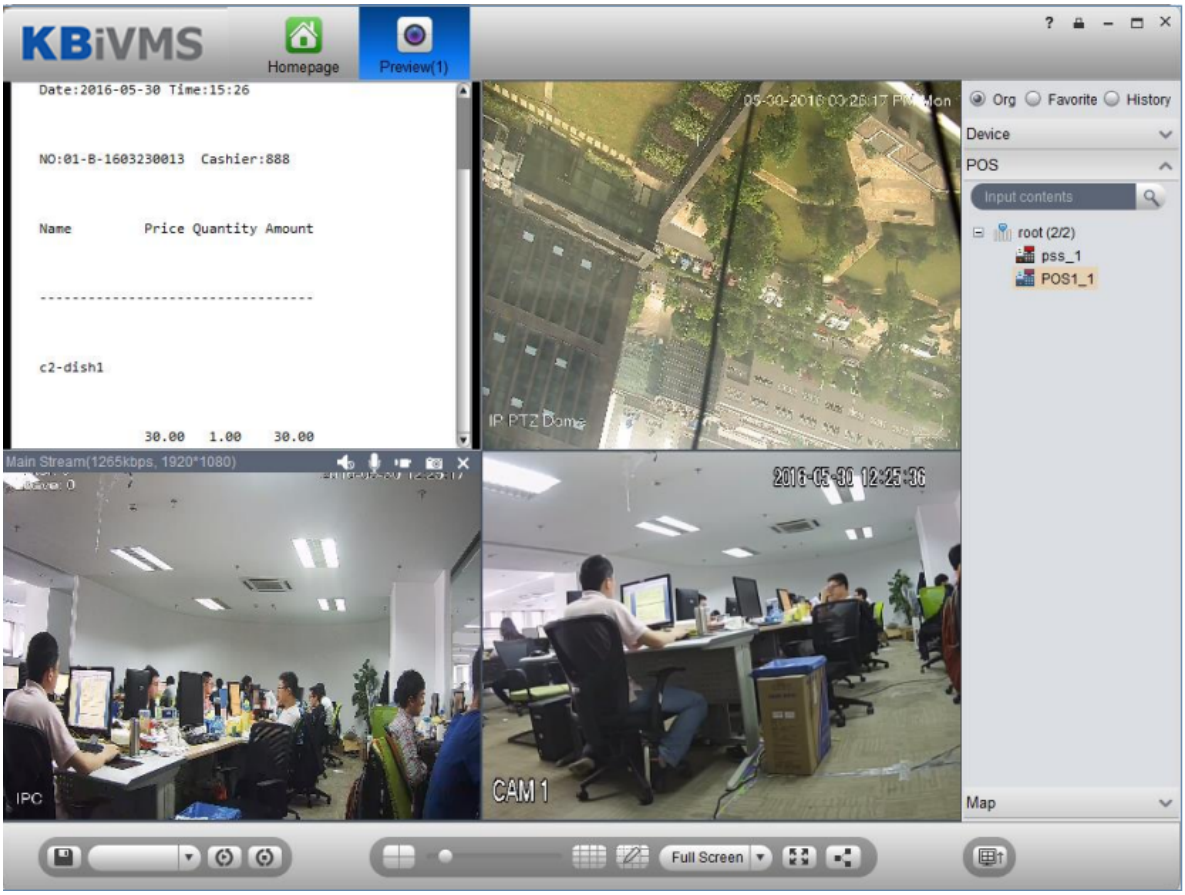


Figure 5-28

Step 4. Right click POS window, select save video as task.

Then you can directly select 

at the lower-left corner for touring.

5.10.5 **POS Search**

In POS interface, you can search POS info list and playback related record.

Step 1. Click  in More Extension area.

Step 2. Select search time and etc, click Search.

POS info list are shown on the left.

Step 3. Double click one item of info, the linked video of the selected info will be shown on the right. (1 min before the selected time, and 5 min after the selected time), see Figure 5-29.

Note:

POS receipt linked record time can be set in Local>Record.

Set new PES server in the system, control pos end string which is “Thank you!” by default.

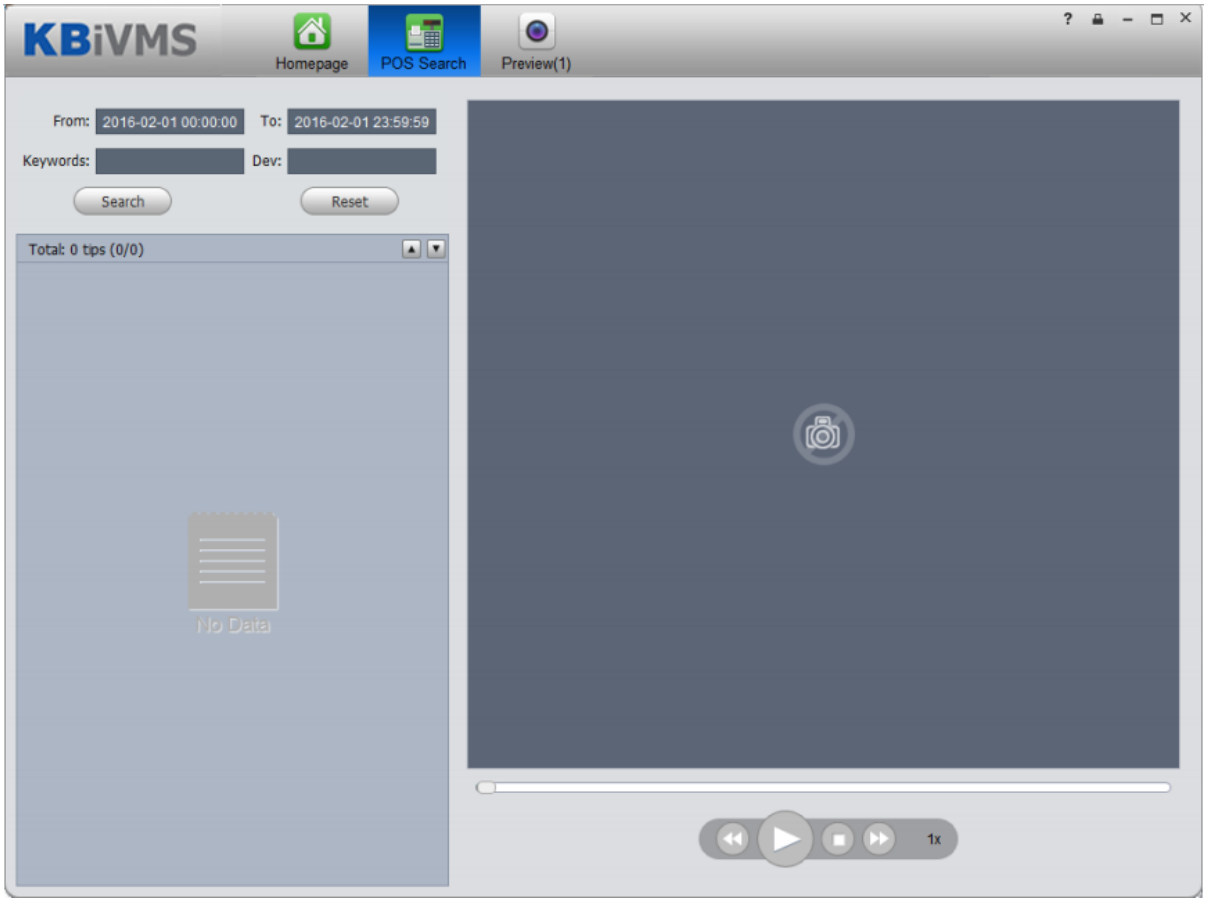


Figure 5-29

5.11 **Map**

Step 1. In Live Preview interface, click Map on the right.

Map tab shows map and hot spot map added on Manager-end.

Step 2. Double click map, on the left it shows map and added devices. On the map, you can see live preview, playback and video wall.

Step 3. Click  in video window to play live video. See Figure 5-30.

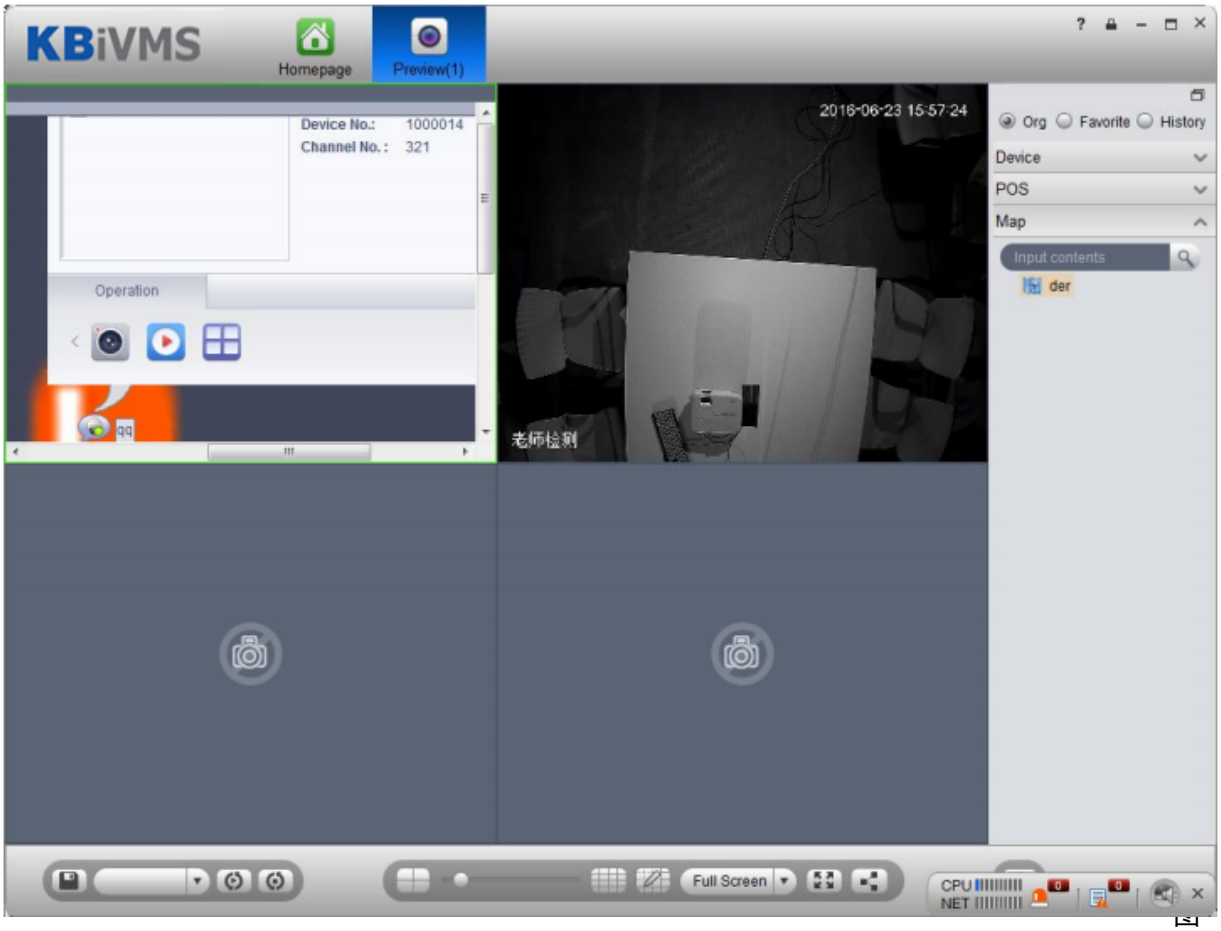

KBiVMS
Homepage
Preview(1)
Device No.: 1000014
Channel No.: 321
Operation
2016-06-23 15:57:24
老师检测
Org
Favorite
History
Device
POS
Map
Input contents
Full Screen
CPU
NET

Figure 5-30

6 Playback

The system can search and playback record from device or center storage media. You can search for different channels, different times, and different types of record on Client, playback and download them. If there is record found, it will show different colors in date selection area.

- Device storage: Record stored in SD card on front device or in DVR, NVR. Storage plan is configured on device.
- Center storage: Record stored on NVS, or Server hard disk. For detailed config, please refer to Storage config in System Config. Before you playback record from center, please configure normal plan first. Within the setup period, the system will store record file on NVS.

6.1 Configure Storage Plan

6.1.1 Time Template

Step 1. Login KBiVMS Manager.

Step 2. Select Business>Time Template.

Step 3. Click Add. See Figure 6-1.

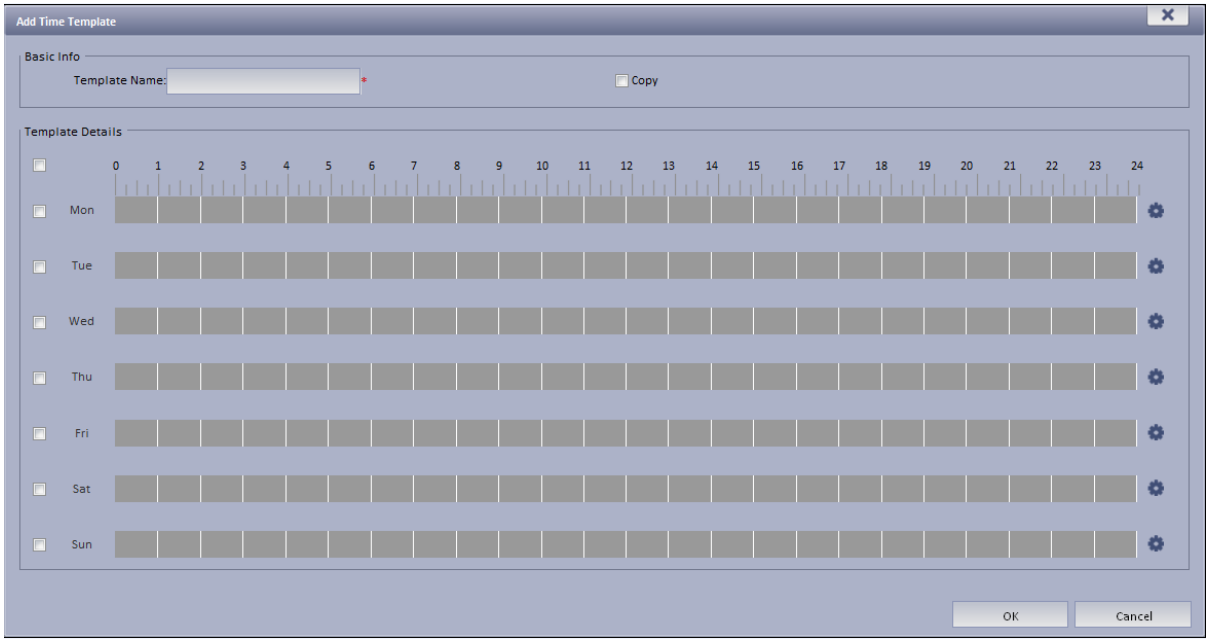


Figure 6-1

Step 4. Enter template name, use mouse to draw period, as well as you can click  .

System pops up period setup box, see Figure 6-2.

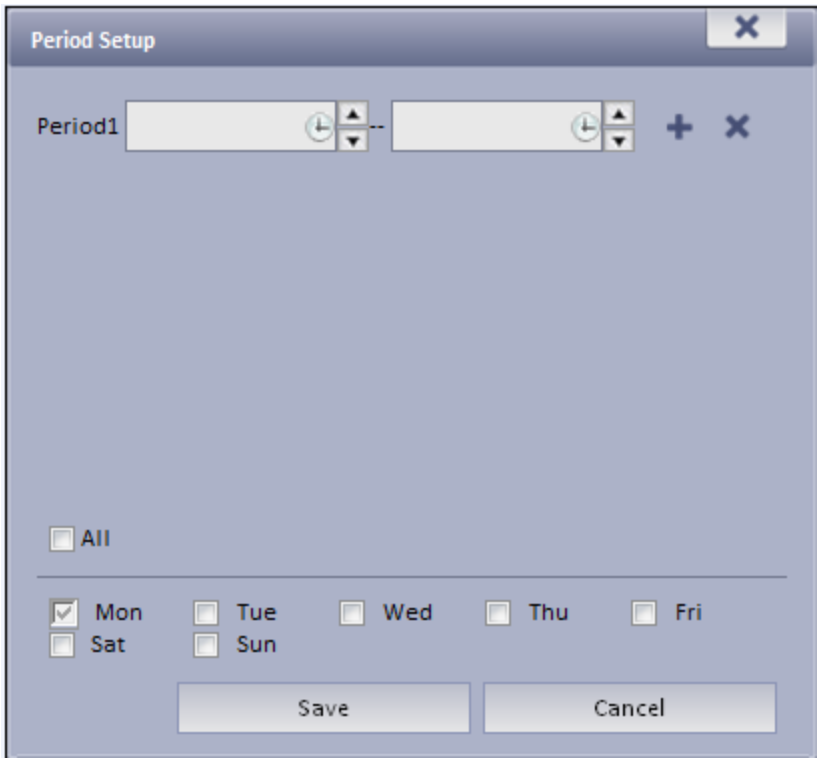


Figure 6-2

Step 5. Click Save. See Figure 6-3.

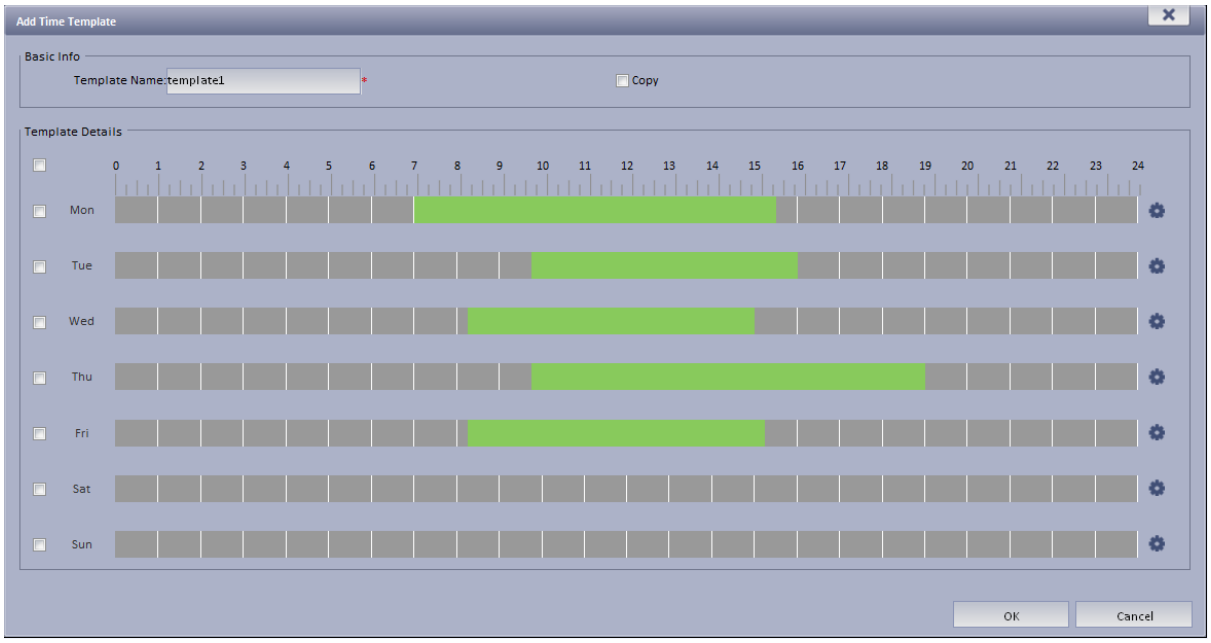


Figure 6-3

Note:

If you select Copy next to template name, and in dropdown list select existing template, then you can copy info in existing template into this template.

6.1.2 **Storage Config**

6.1.2.1 Add Normal Plan

Step 1. Select Business>Storage. System displays Storage interface as in Figure 6-4.

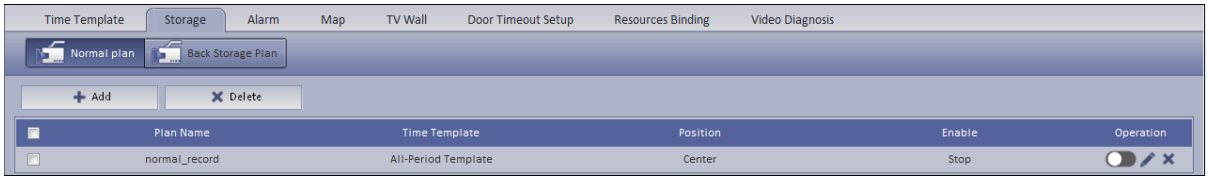


Figure 6-4

Step 2. Click Add . System pops a Add Time Template box. See Figure 6-5.

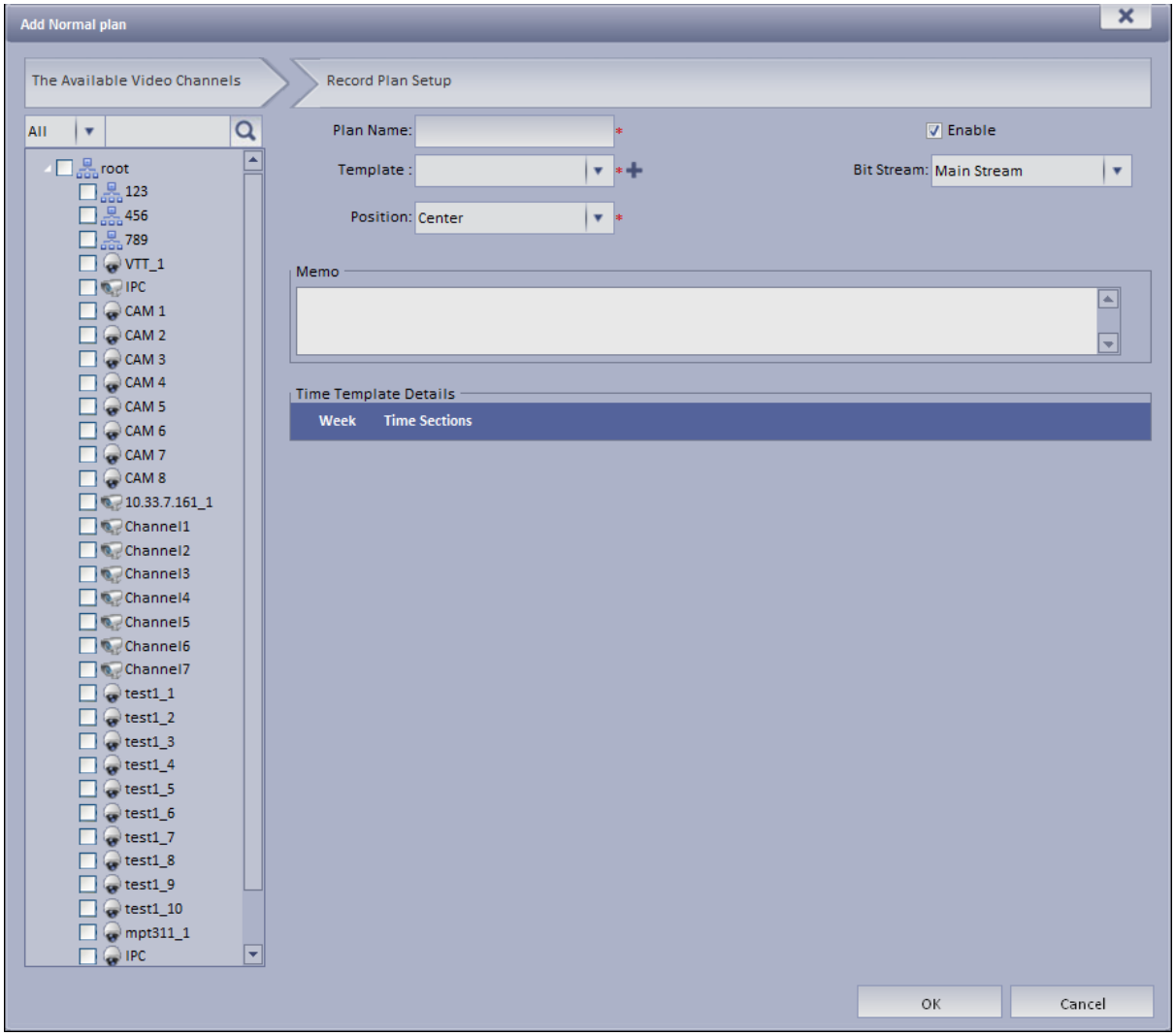


Figure 6-5

Step 3. Select channel on the left Input Plan Name, and select Template, Bit Stream. Check Normal plan. See Figure 6-6.

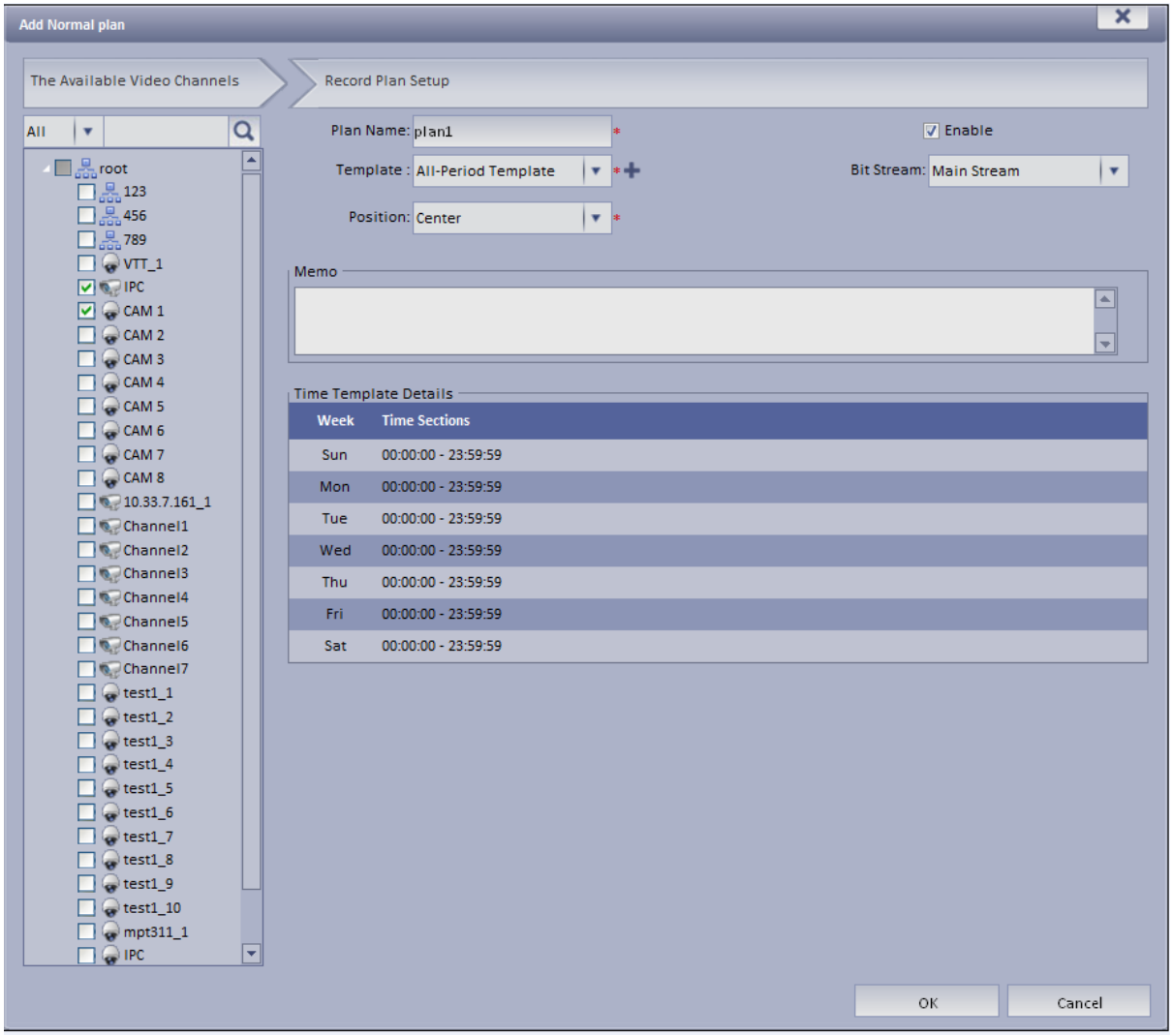


Figure 6-6

Note:

For EVS device front channel, in record plan, for storage position, you can select center (store on center server) or local (store on EVS-carried disk).

Step 4. Click OK. System displays configured normal plan.

6.1.2.2 Add Back Storage Plan

The system supports back up record of the previous 3 days.

Step 1. Click Back Storage Plan tab.

Step 2. Click Add.

Step 3. In device tree on the left, enter plan name, select time template, condition, see Figure 6-7.

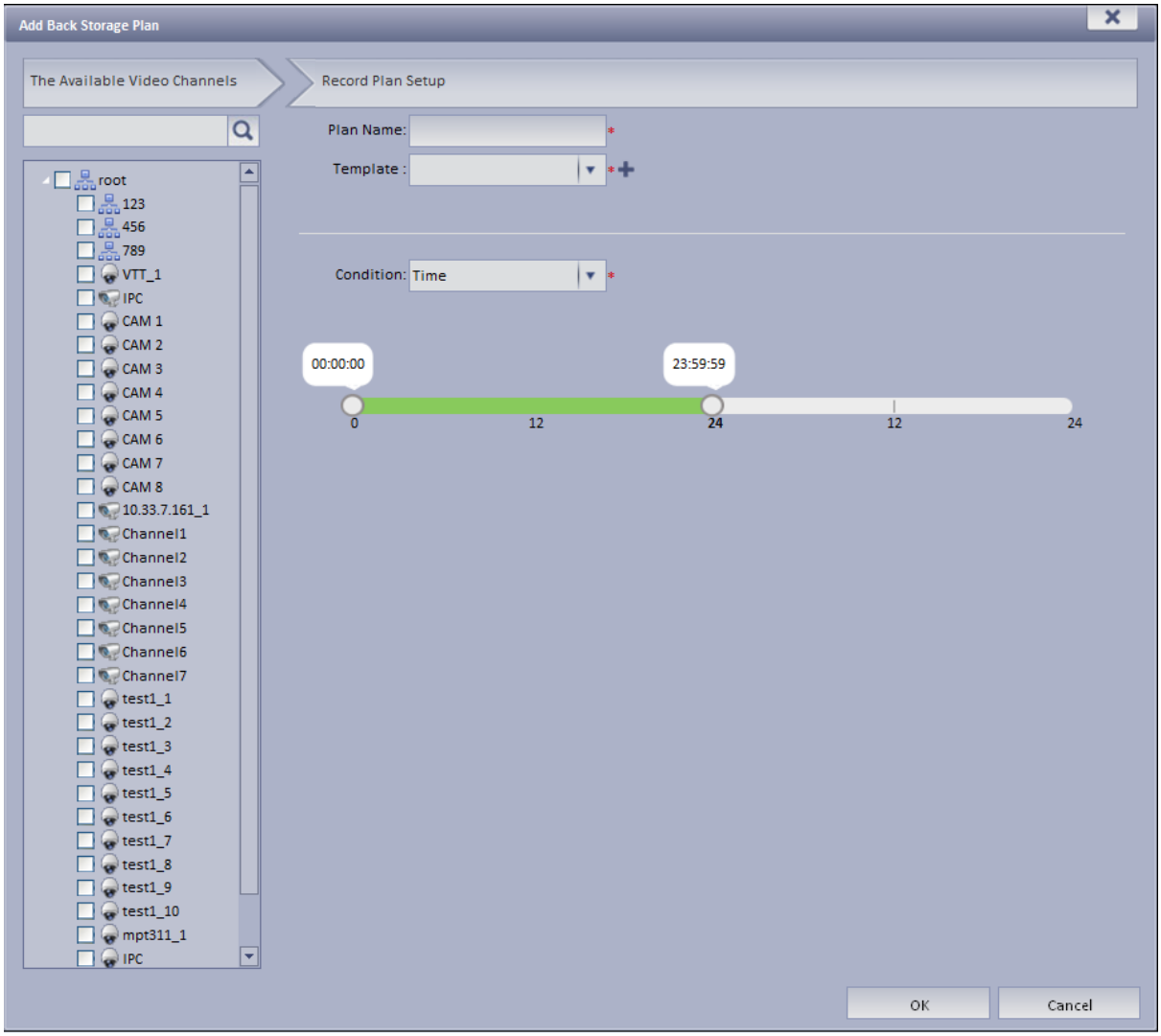


Figure 6-7

Note:

For condition, you can select time, WIFI. If you select time, set back up record time, and when the time is reached, you can back up record. If you select WIDI, when the device connects WIFI, it will auto back up record.

Step 4. Click OK.

6.1.2.3 Disk Quota

Step 1. Click Disk Quota tab.

Step 2. Click  next to Online status server. See Figure 6-8.

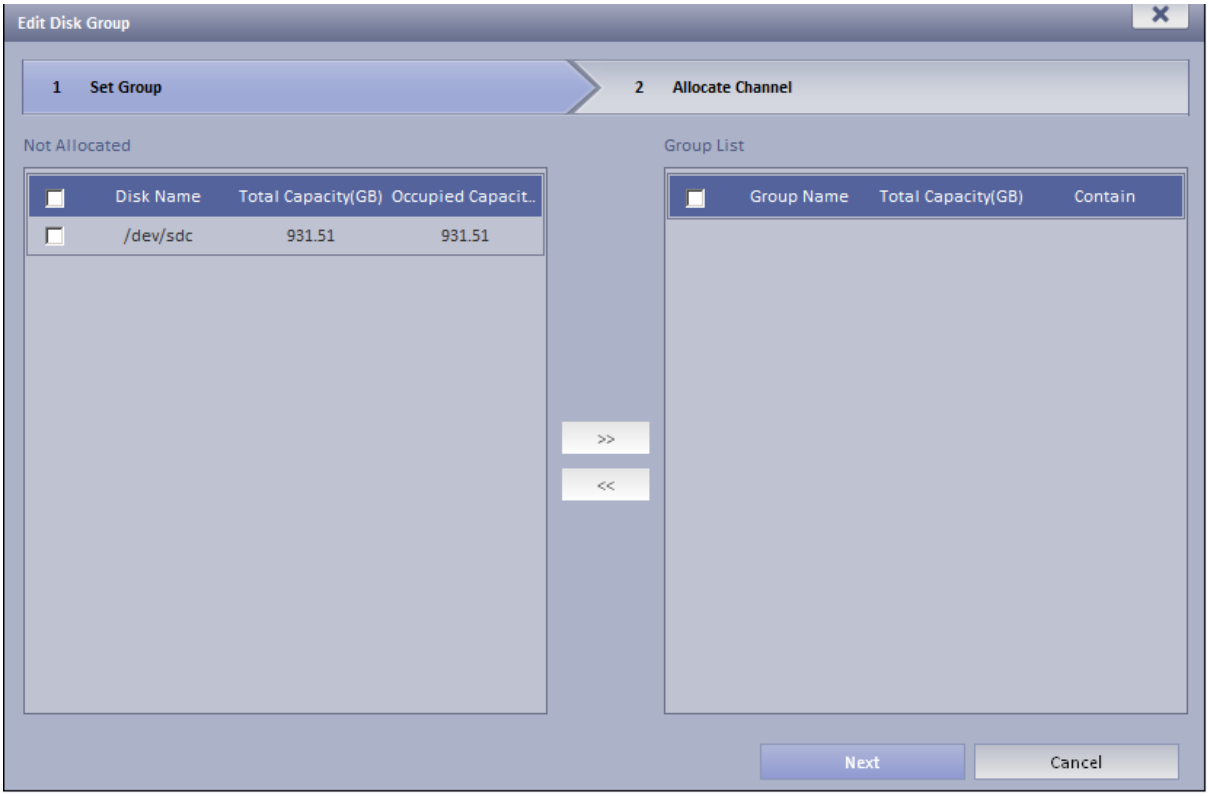


Figure 6-8

Step 3. Select unallocated disk on the left, click >> to add to disk group on the right.

Step 4. Click Next to allocate channel.

Step 5. In device list on the left select channel, click >> to add into disk group on the right. See Figure 6-9.

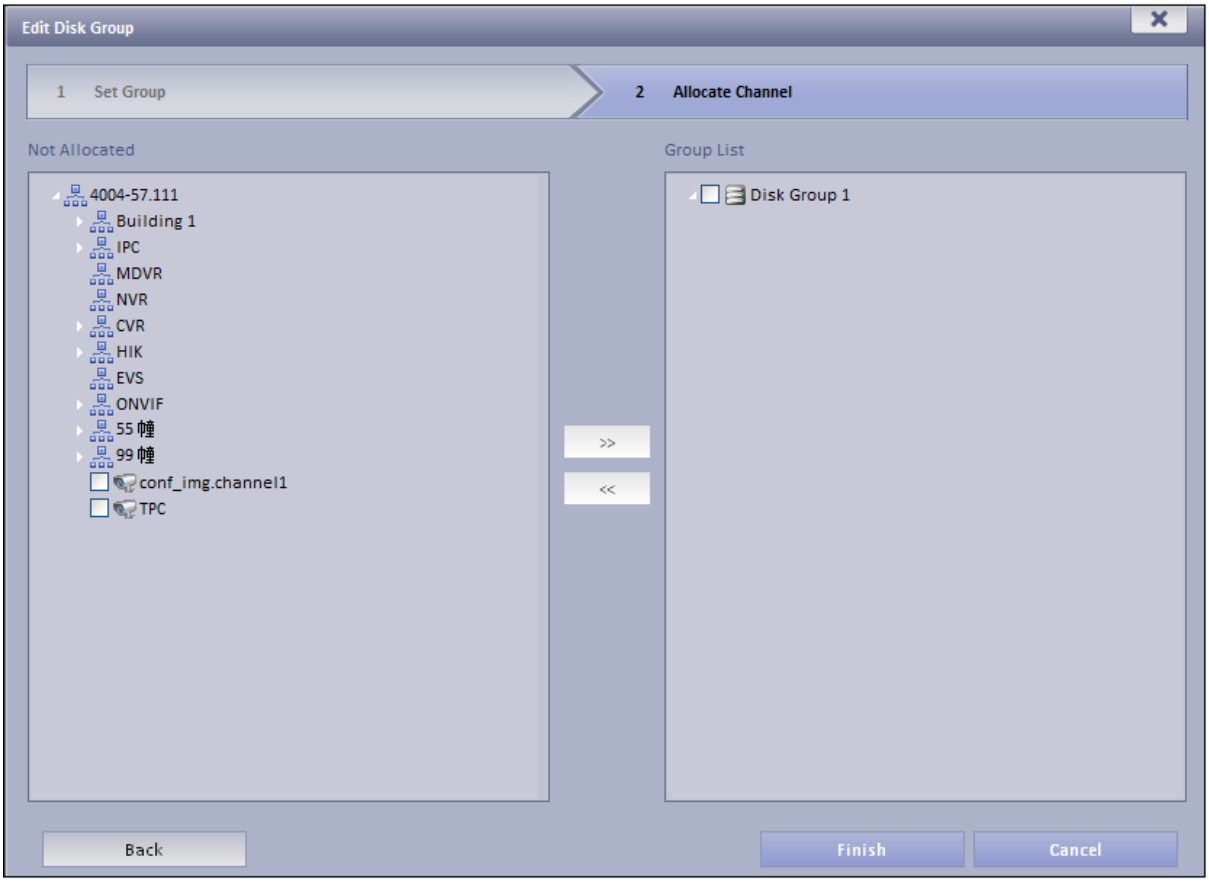
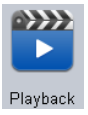


Figure 6-9

Step 6. Click Finish.

6.2 Playback

6.2.1 Playback

Step 1. Open KBiVMS Client. In Basic area, click 

. System displays playback interface.

Step 2. In the upper-right corner, select Device, Center, or Period, and check device channel.

Step 3. Select date, time, record type for search.

Step 4. Click Search. After search is finished, channels with record will be displayed in time progress. See Figure 6-10.

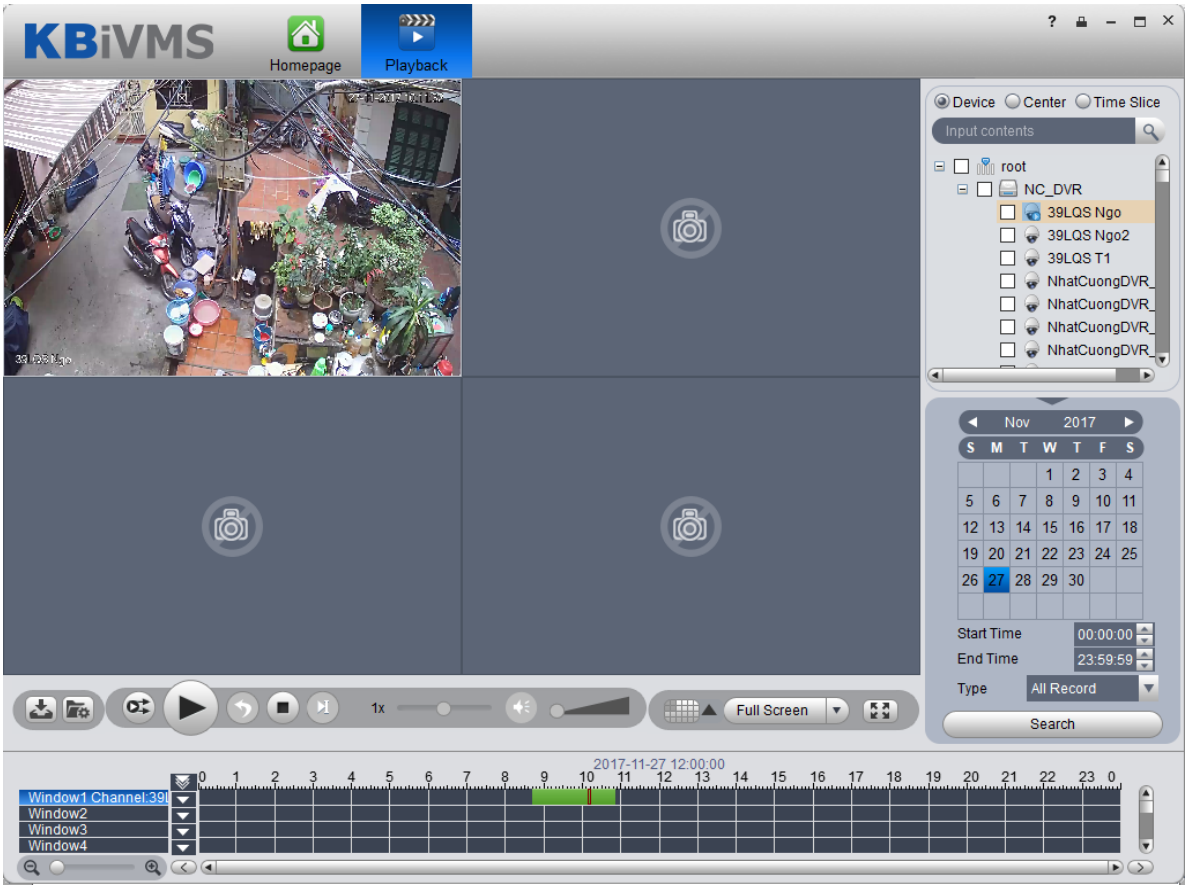


Figure 6-10

Step 5. Select channel to playback, click  to play record. Or, double click time progress bar to playback record of the moment you click.

Step 6. Right click playback window, select “Playback on Wall”. System pops up “TV Wall Channel” box, decode via decoder and output to wall.

Note:

Playback now supports decoders as M60, M70 and NVD.

See Figure 6-11.

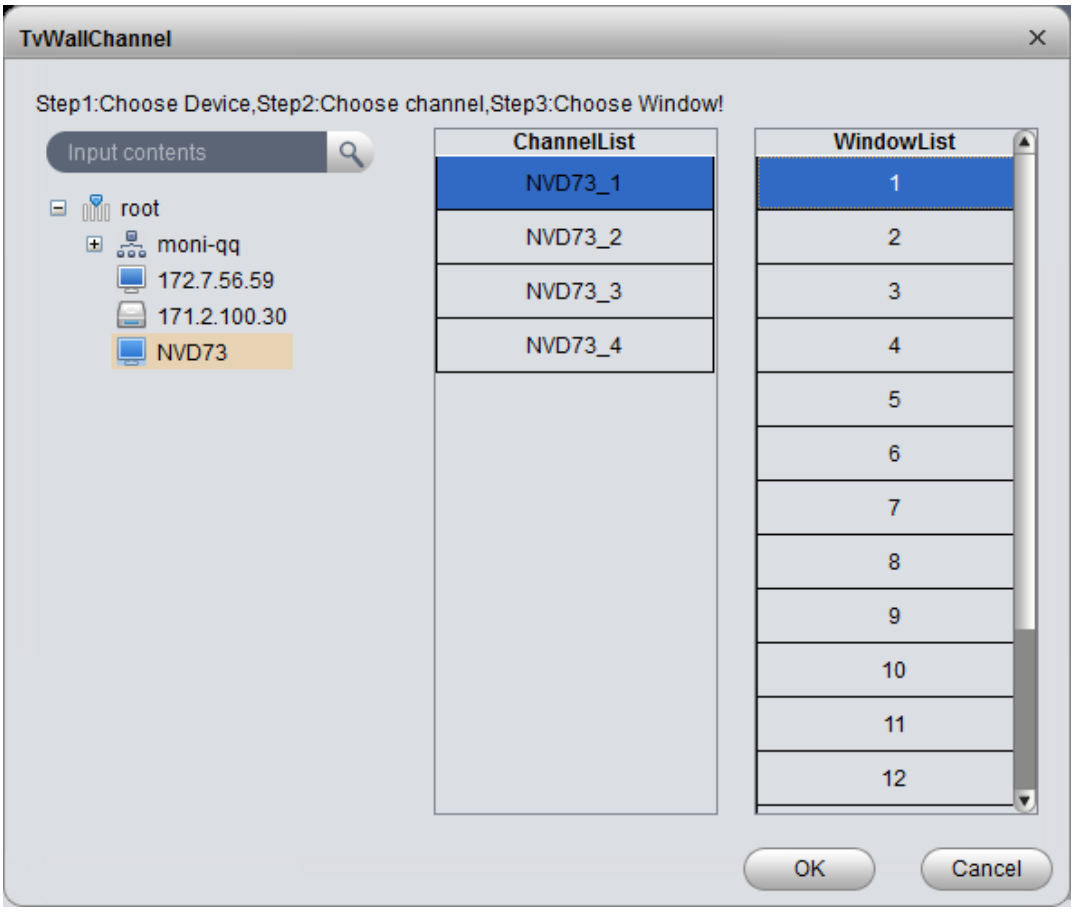


Figure 6-11

6.2.2 **Intelligent Search**

Warning:

Device to playback record must have intelligent search function.

Step 1. In Playback interface, on the right select device channel with intelligent search function, and search for record. See Figure 6-12.

Figure 6-12

Step 2. Click  . See Figure 6-13.

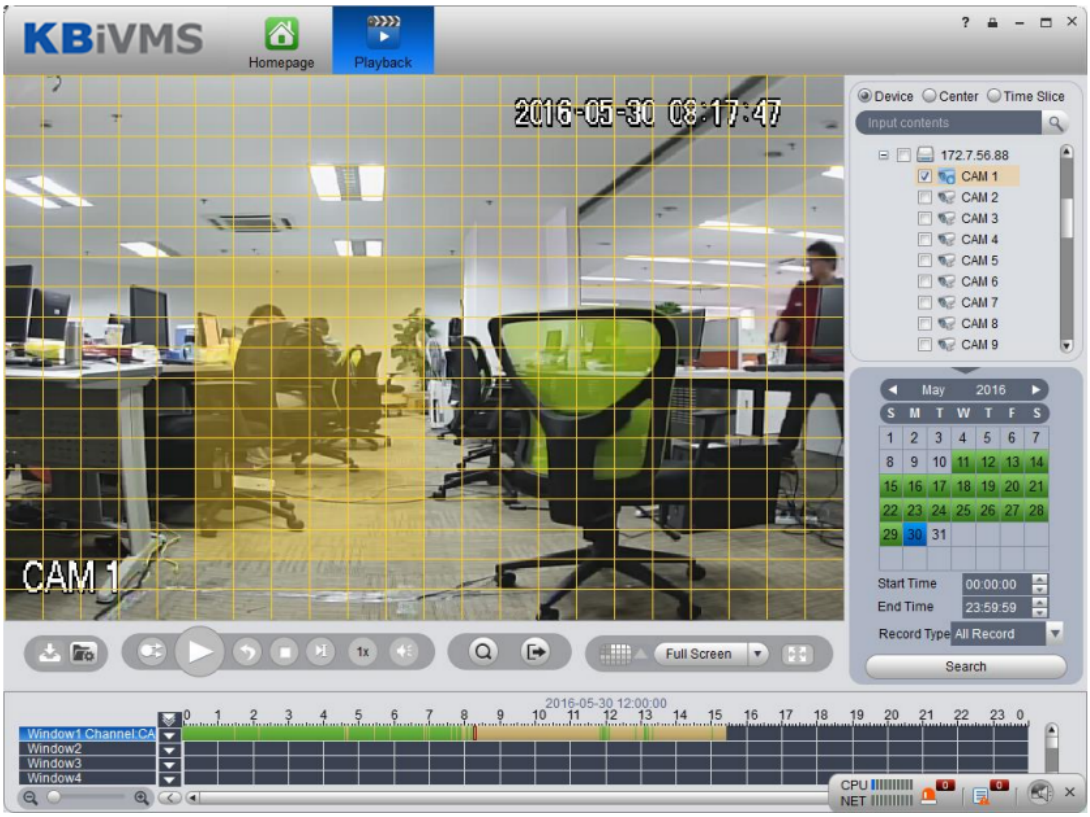


Figure 6-13

Step 3. In the grid draw motion detection area  , and click  .

The system searches motion detection result within the area, and the playback channel is purple, see Figure 6-14.

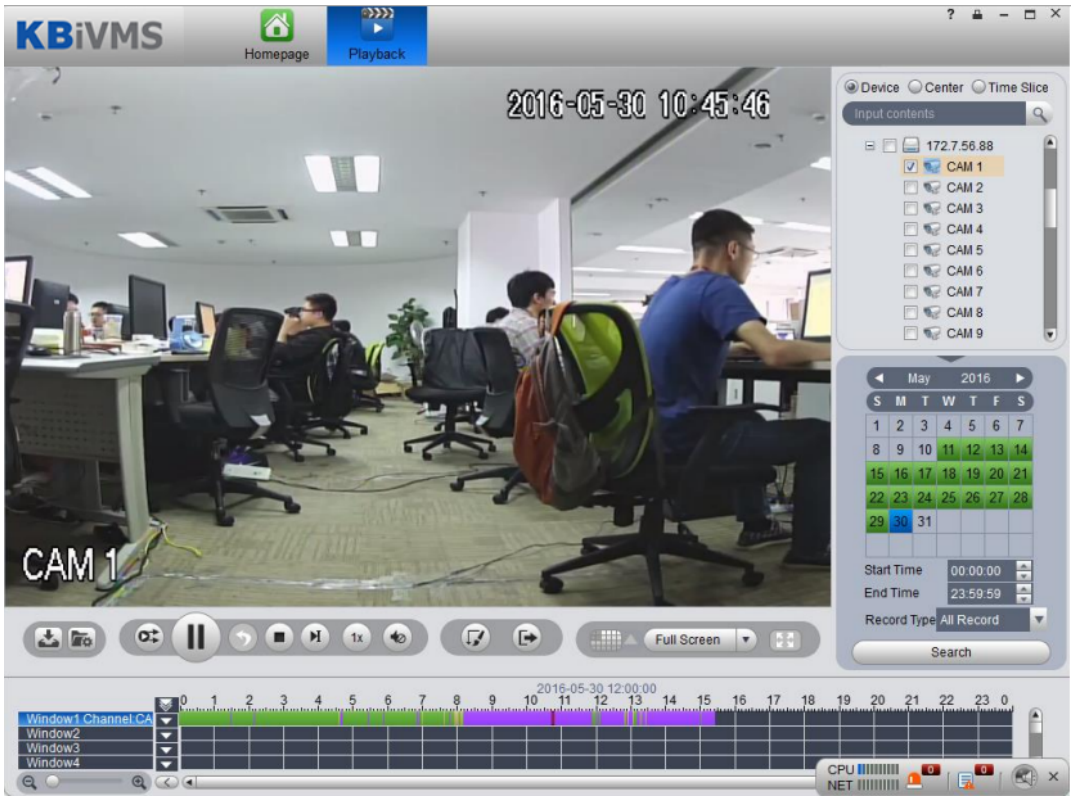


Figure 6-14

6.2.3 **Fisheye Playback Record**

The system supports to playback central record in fisheye device.

Step 1. Click Playback, enter Playback interface.

Step 2. On the right, click fisheye device and set time, click Search.

After videos are searched, double click to open record. Right click and select video mode of fisheye to playback, such as wall mount, see Figure 6-15.

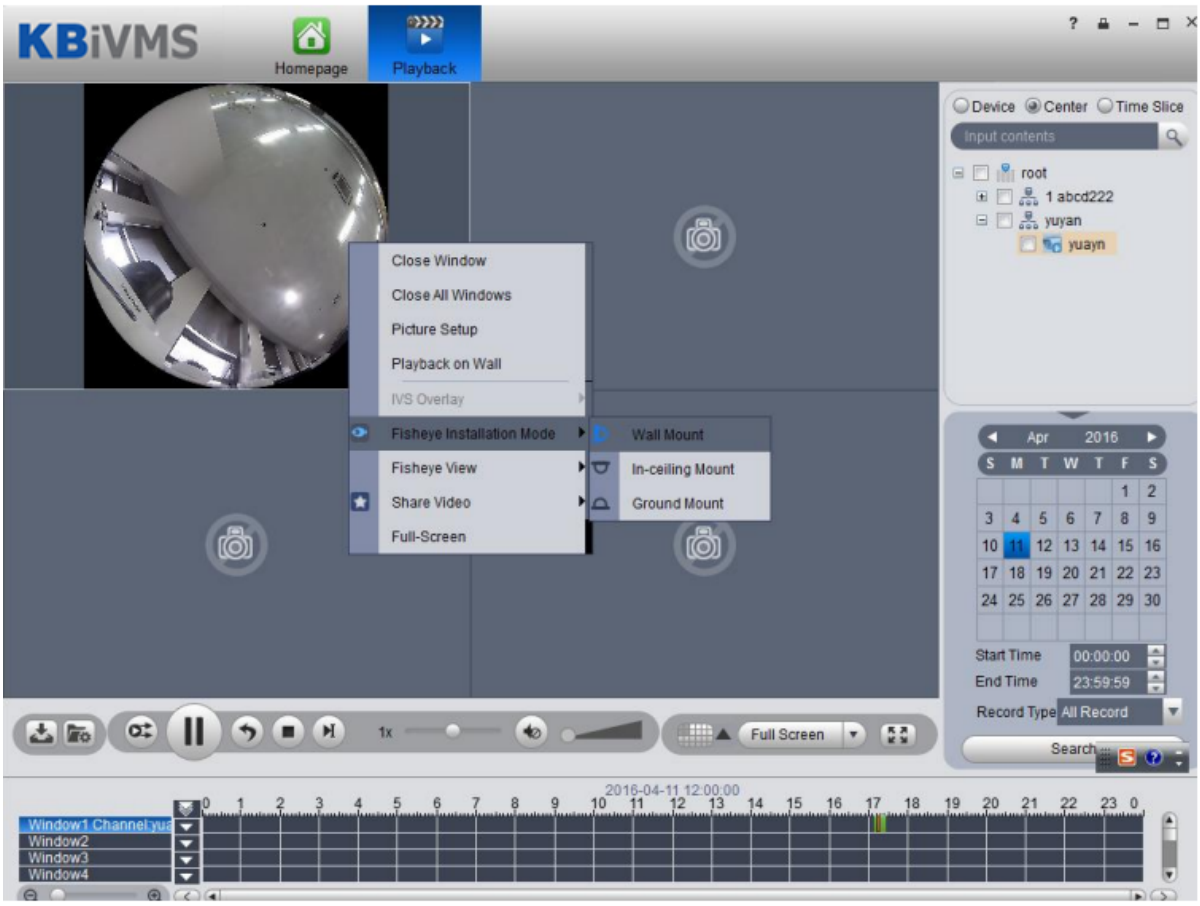


Figure 6-15

Step 3. Select wall mount mode, right click Fisheye View and select split mode, such as 1+2 mode. See Figure 6-16.

Figure 6-16

You also can drag small block on fisheye to rotate video window on the right.

6.2.4 **Playback by Time Slice**

Warning

Time Slice function is for record store in center only, make sure record has been ready.

System Support Center recording will query the video window period by the average number of chips, and displays the corresponding period of the video in each window.

Step 1. In the Playback screen at the top right, select time slice.

Step 2. Select one channel, period for search, click Search.

The system will playback video corresponding period in each window. See Figure 6-17.

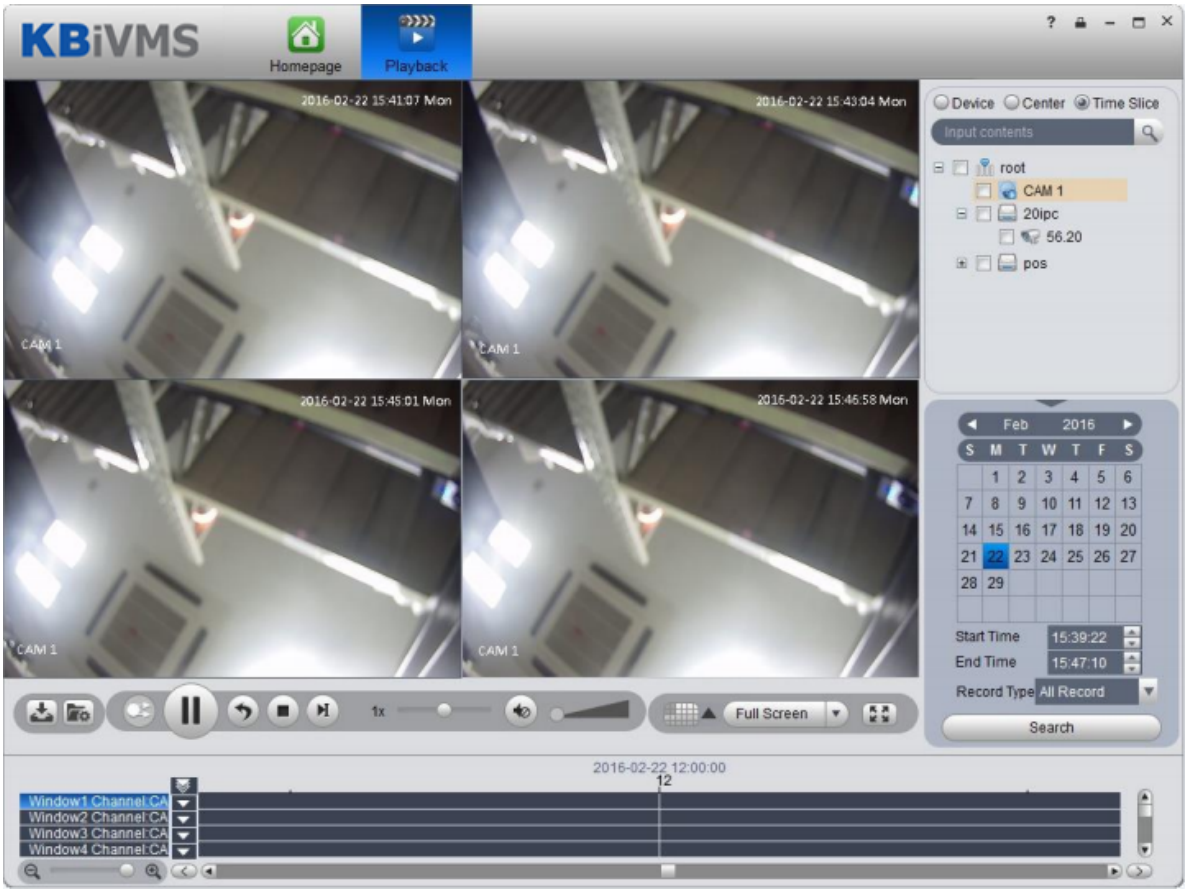


Figure 6-17

6.2.5 **Mark Record**

Via marking record, you can create bookmark in designated record.

To mark record:

Step 1. Click in Playback interface. System pops up a Add Mark box as in Figure 6-18.

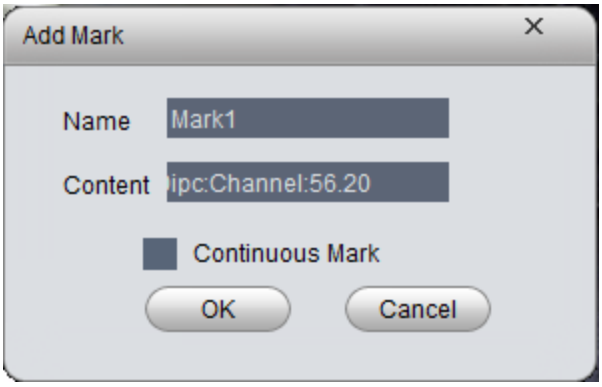


Figure 6-18

Step 2. Input Name and Content, click OK. System pops up box saying mark successfully. Select Continuous Mark to continuously mark current record.

Step 3. Click in playback window. System pops up a Mark Manager box as in .

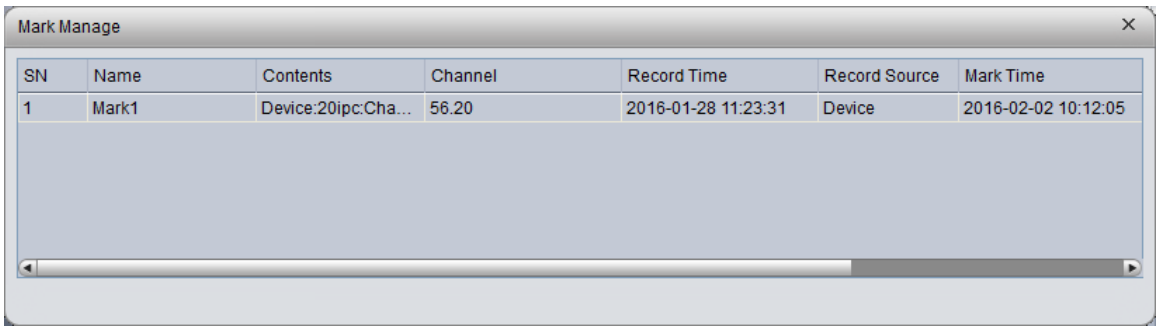


Figure 6-19

Select record, click , , and , you may playback, delete and edit the record. For marked record, it displays in progress bar in playback window, as in Figure 6-20. Click , you can play marked record file.

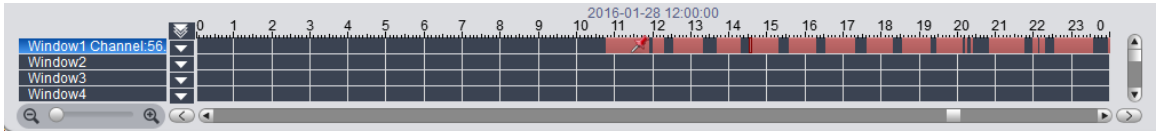


Figure 6-20

KBiVMS Client supports search, playback, edit and delete marked record.

If you have marked record, you can quickly search record with the mark, and you also can playback, edit and delete the record. Please refer to Ch 6.2.3.

To search marked record:

Step 1. In Extension area, click 

. System displays Record Mark interface.

Step 2. In device list, select channel, time, and input mark name.

Step 3. Click Search Mark. System shows search result, see Figure 6-21.

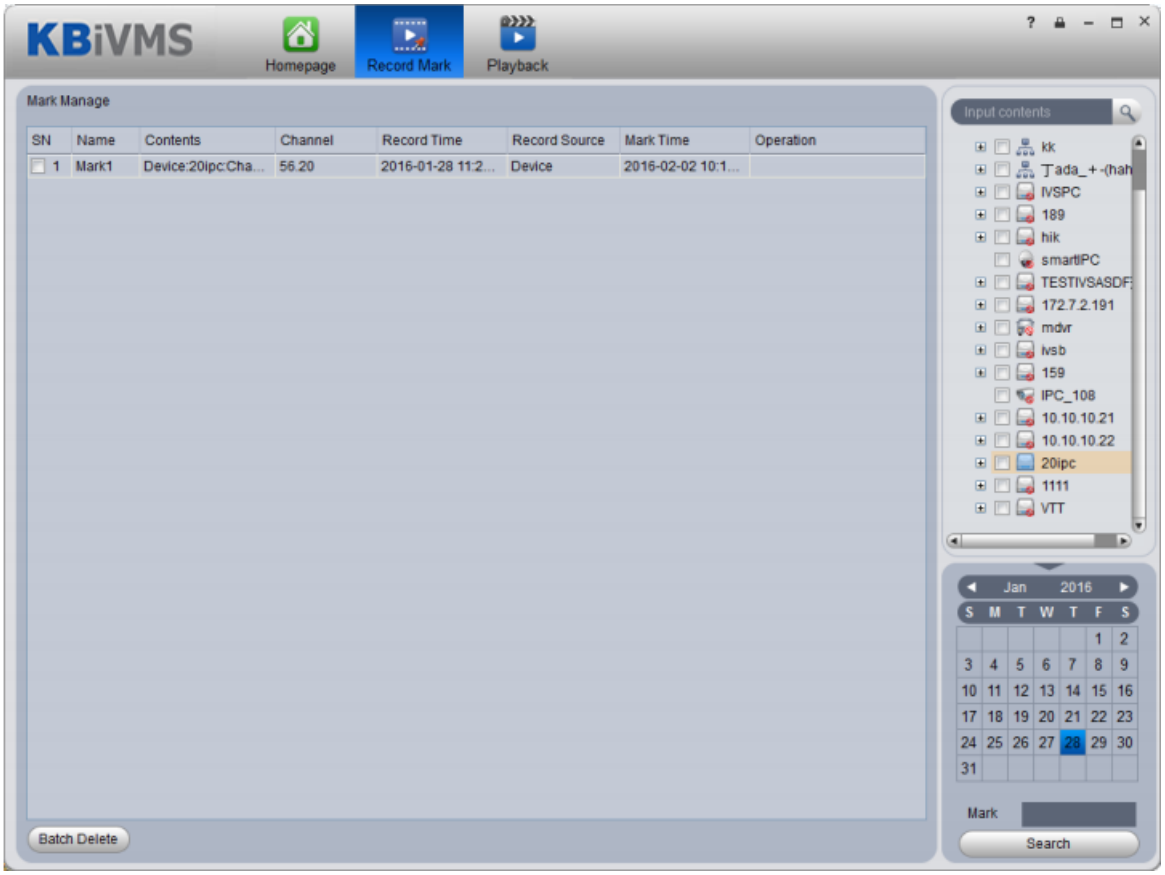


Figure 6-21

Step 4. Check multiple marked records, and click  to delete checked records.

Click  to play record.

Click  to delete record.

Click  to edit.

6.2.6 **Record Lock**

Note:

You can only lock record which is recorded half an hour ago.

Step 1. In time bar in Record Playback window, right click time you want to lock record start at. See Figure 6-22.

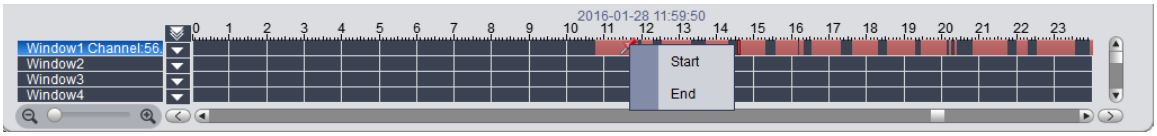


Figure 6-22

Step 2. Fill in record parameter, click Lock.

Step 3. If you search again, you will see blue color in progress bar which is the locked record. See Figure 6-23.

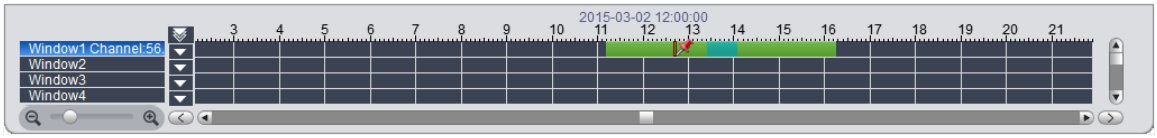


Figure 6-23

Note:

When disk is full, ss will not overwrite locked record. SS is responsible for record storage, playback, download.

All of locked records can be search in Record Lock interface.

Step 1. Click 

in Extension area. System shows Record Lock interface.

Step 2. In device list, select Channel, Start Time, End Time and Enter Lock Reason. Click Search to search lock record. See Figure 6-24.

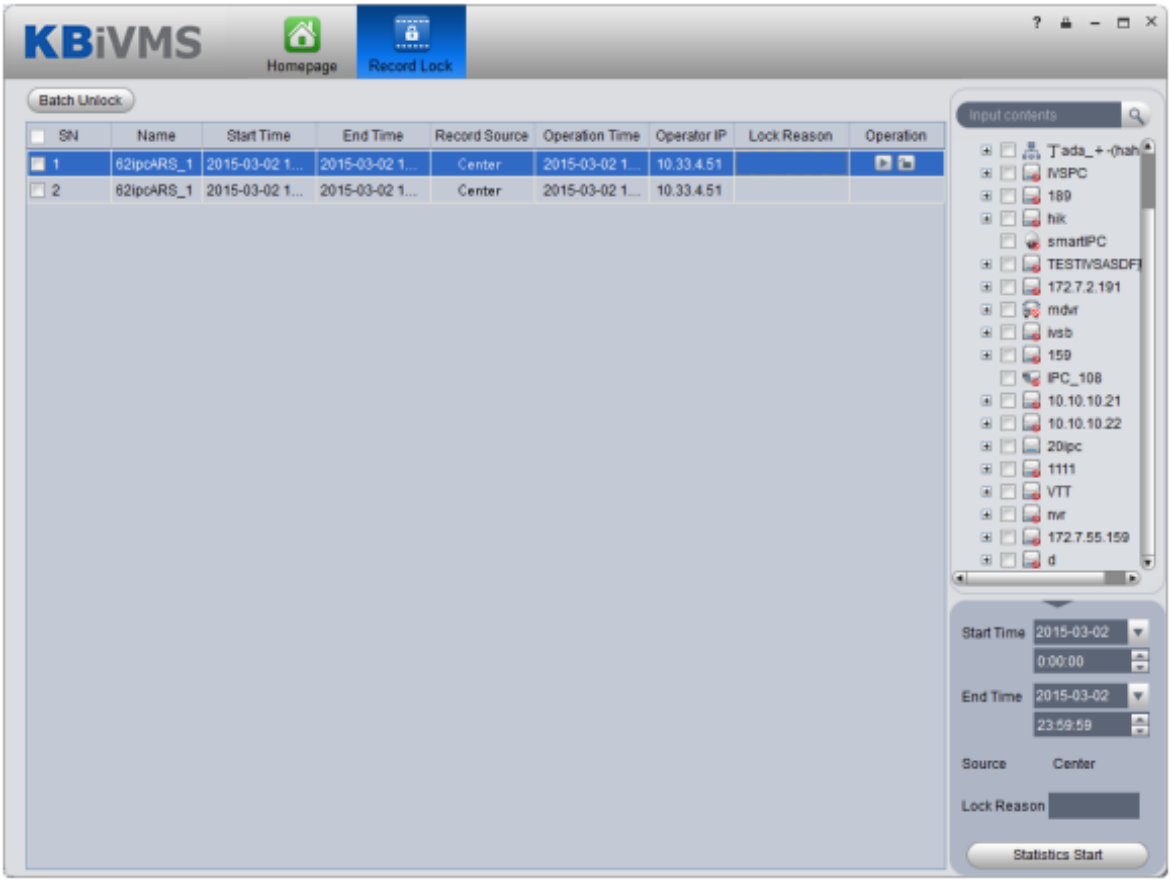


Figure 6-24

Step 3. Select channel, click 

to unlock multiple records at once.

Click  to play record.

Click  to unlock record.

6.2.7 **Download Record**

The system supports the playback of video downloaded and saved to a local PC.

Step 1. Click  above playback window or click  . See Figure 6-25.

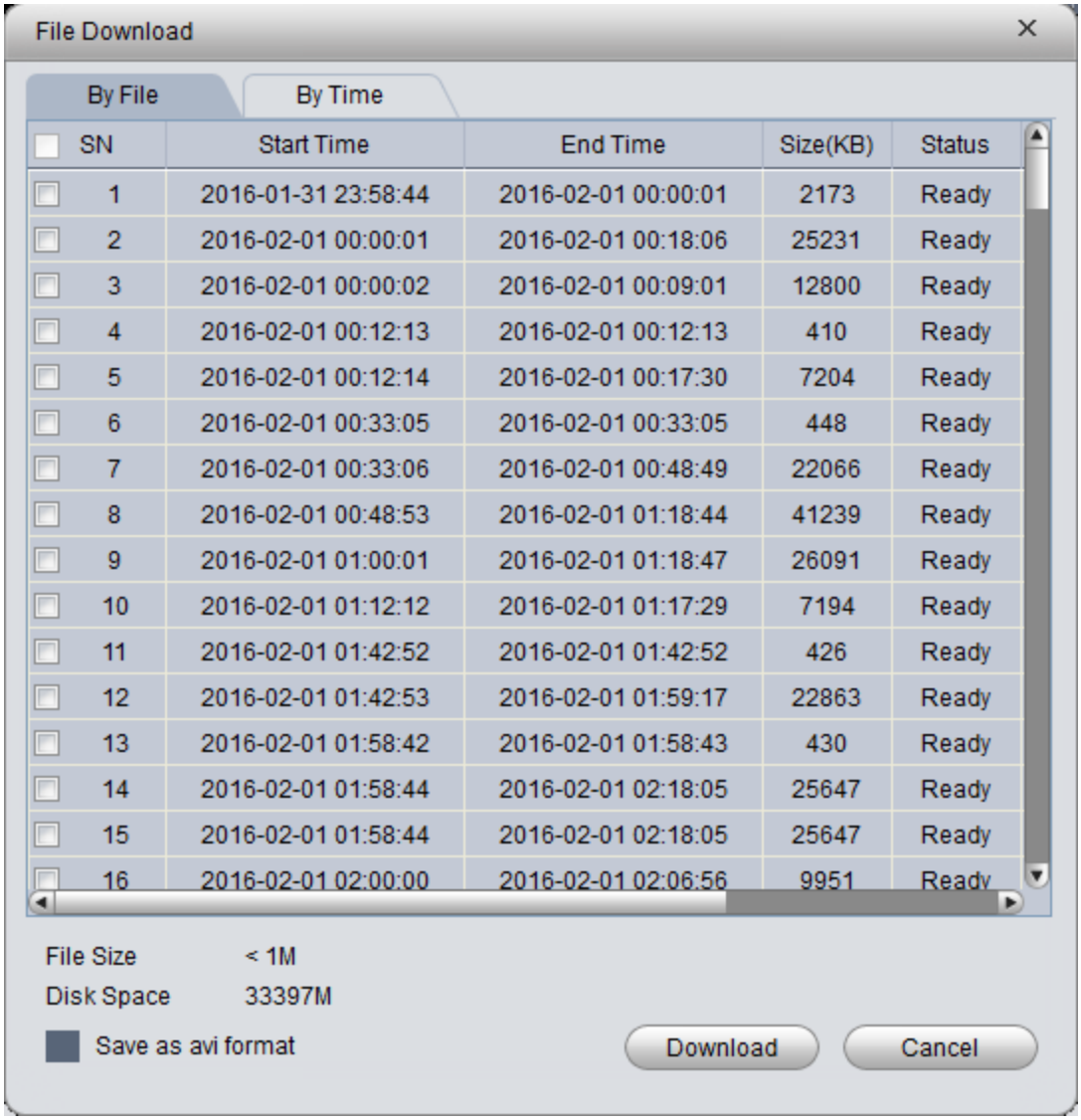


Figure 6-25

Step 2. Check the file to be downloaded, select Download grounds , enter Comments , and click Download.

The system starts downloading the file, Download Status to downloading. You can also click download time tab, select the time period, by time period download video.

Step 3. Click  in Record Playback interface. See Figure 6-26.

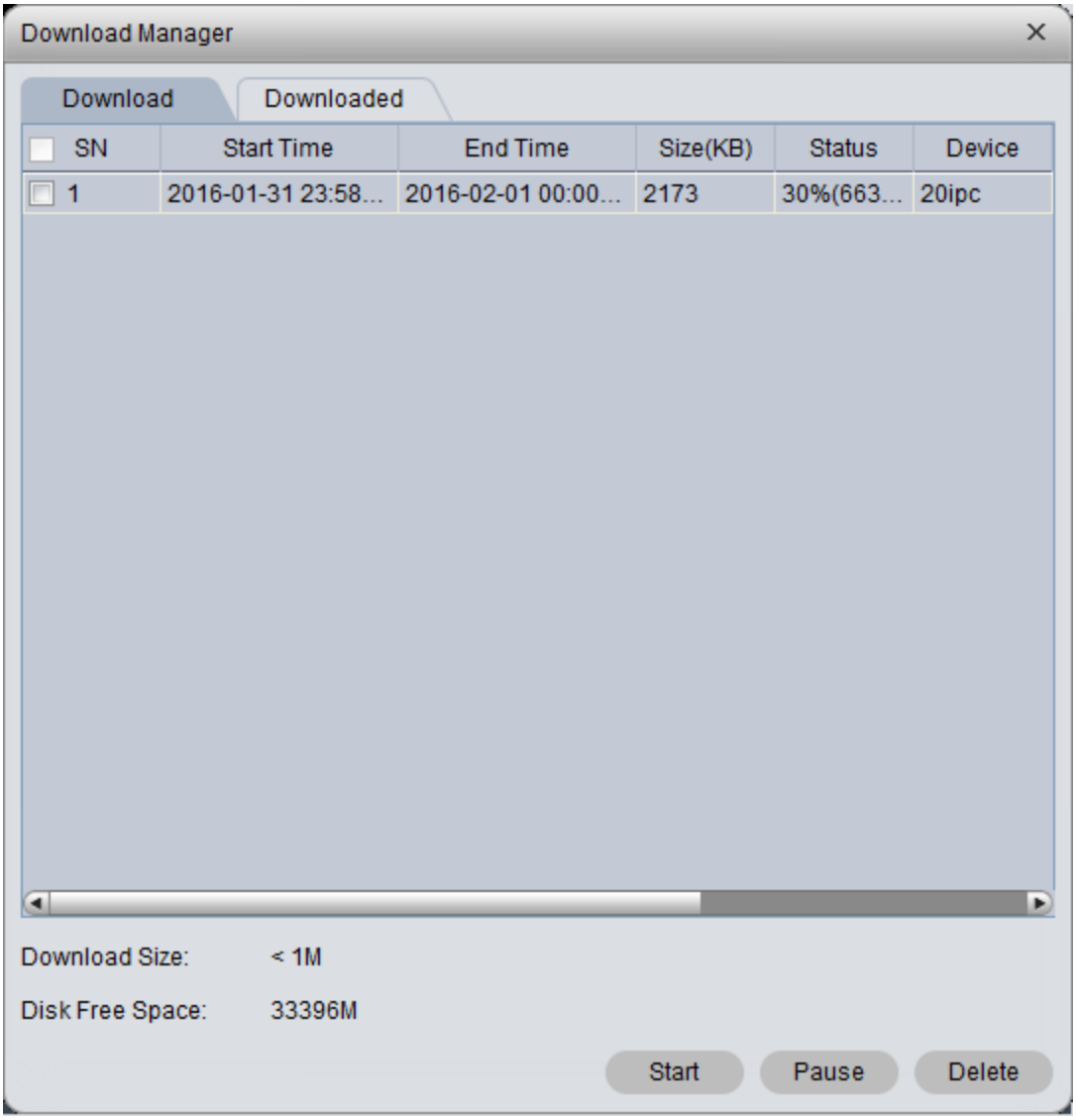


Figure 6-26

You can view the download progress; you can check the video files being downloaded pause download and delete the file being downloaded.

7 E-Map

Before you can use E-map function, you must configure type of map on Server, including raster map, Google, Google offline map, while you must drag video device, ANPR device, alarm device onto map so that you can use E-map function on Client. E-Map supports alarm prompt, video preview and playback.

Note:

- Rater map:
  Show one picture, which is suitable of indoor environment. Place camera at a fixed place, such as parking lot. Server used raster map as default.
- Google:
  Google online map, Client accessing Google map requiring network accessibility of Google Map. Via online Google map, it shows the entire city on map with zooming function.
- Google offline Map
  Google offline map, by distributing map on other server, it allows network accessibility between our Client and Google Map offline server. So you can access Google offline map with the same functions as online map.

7.1 Raster Map

7.1.1 Select Map

Step 1. Select Business>Map.

Step 2. Click config. See Figure 7-1.

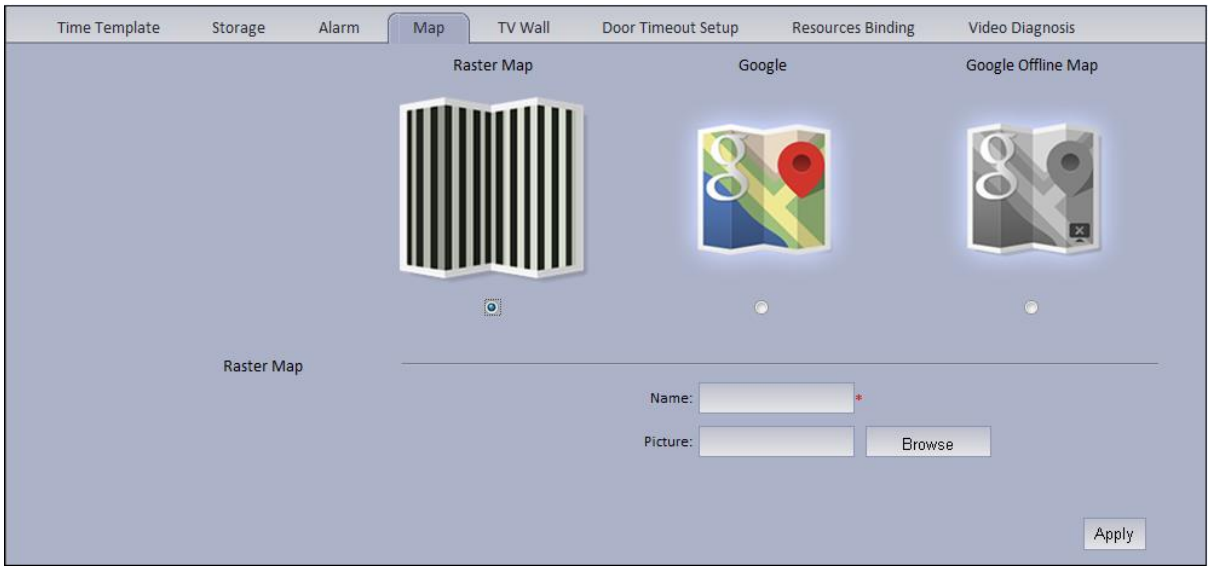


Figure 7-1

Step 3. Select map type to set, click Apply.

7.1.2 KBiVMS Manager Map Config

KBiVMS Manager supports to add video device, access control device, video intercom device and etc.

Step 1. Login KBiVMS Manager.

Step 2. Select Business>Map. See Figure 7-2.

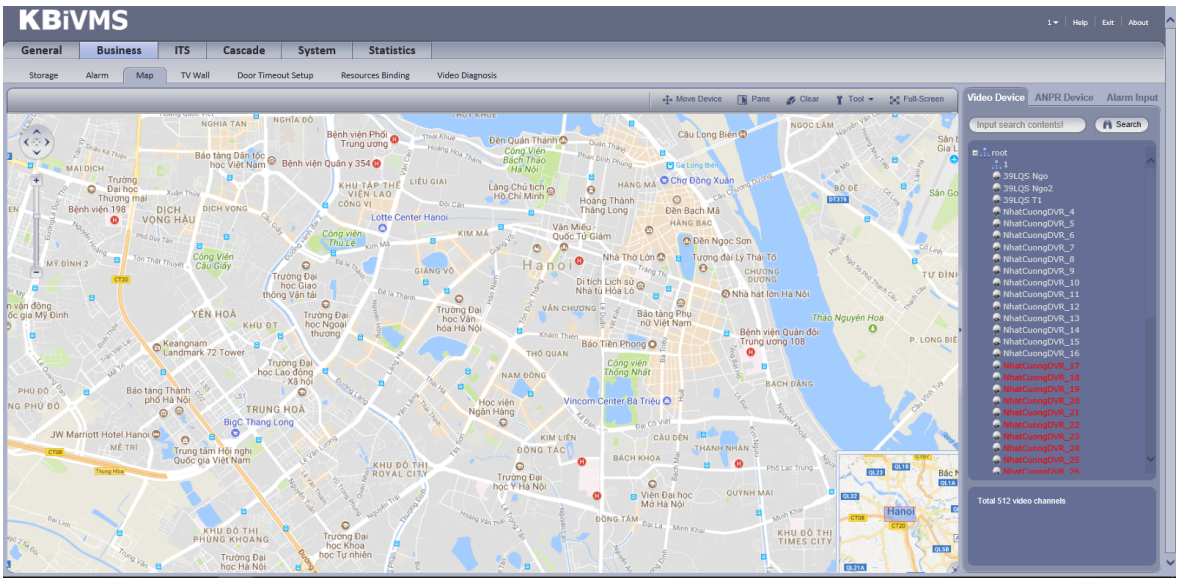


Figure 7-2

Note:

Hot zone: To add a hot zone on map, click Add Hot Zone, then system will auto link to hot zone map.

Step 3. Drag device under Video Input tab on the right onto map. See Figure 7-3.

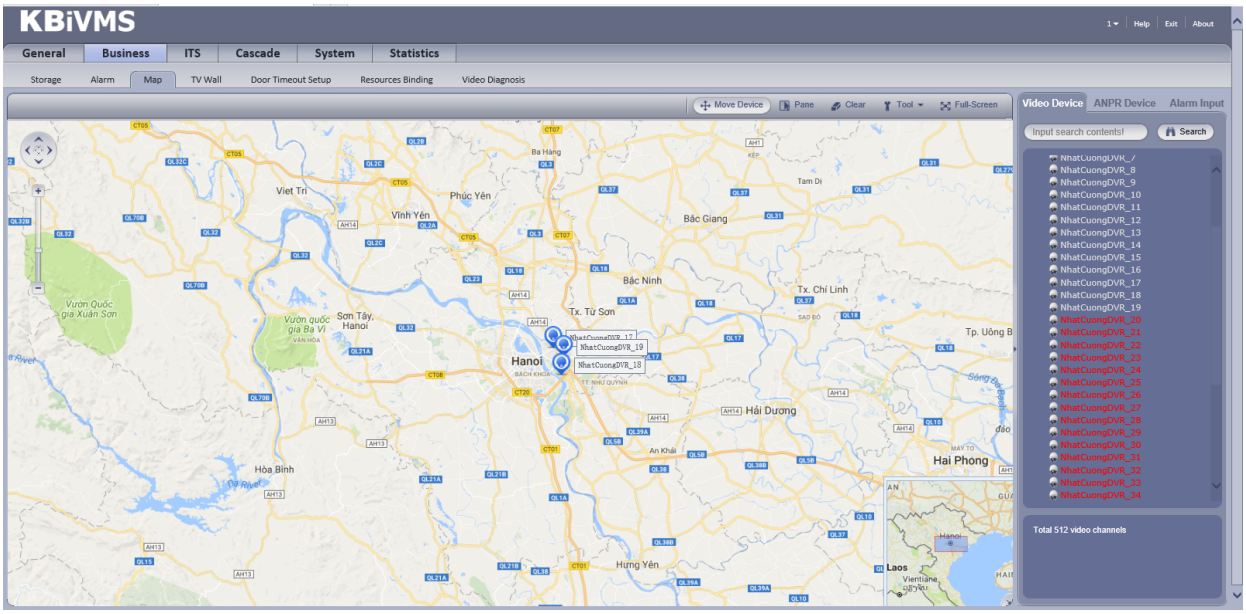


Figure 7-3

Font color in Video Input device list:

- Red: this channel has not configured on map.
- Grey: this channel has been added on map.

Step 4. Drag device under Door Input, Alarm Input and etc. onto the map. Config of map is complete.

7.1.3 KBiVMS Client Map Function

Step 1. Login KBiVMS Client.

Step 2. Click  in Basic Function area. See Figure 7-4.

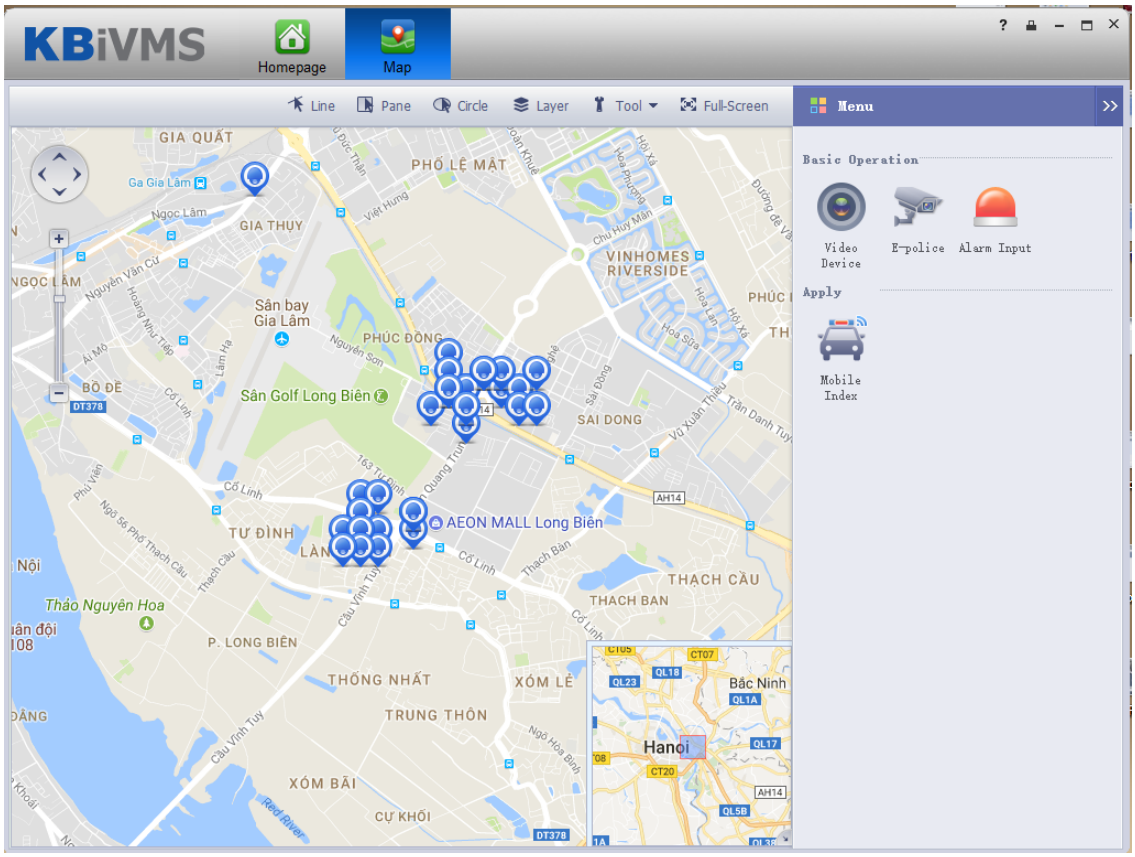


Figure 7-4

Step 3. On the map, pane or circle device you want to select, you can open video, playback and unlock record. See Figure 7-5.

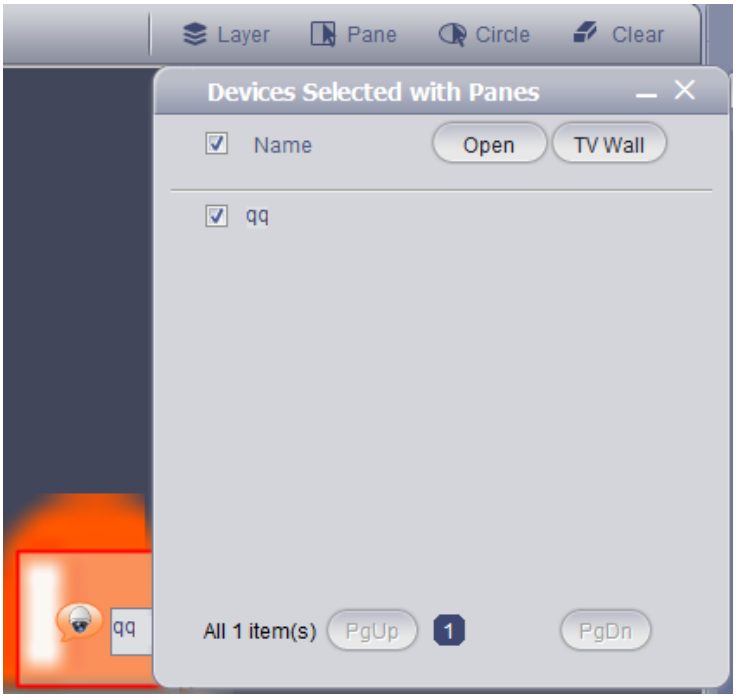


Figure 7-5

Step 4. Client device under Search tab, or directly click device on map.

Device info are shown on map, such as channel name, device no. and channel no.

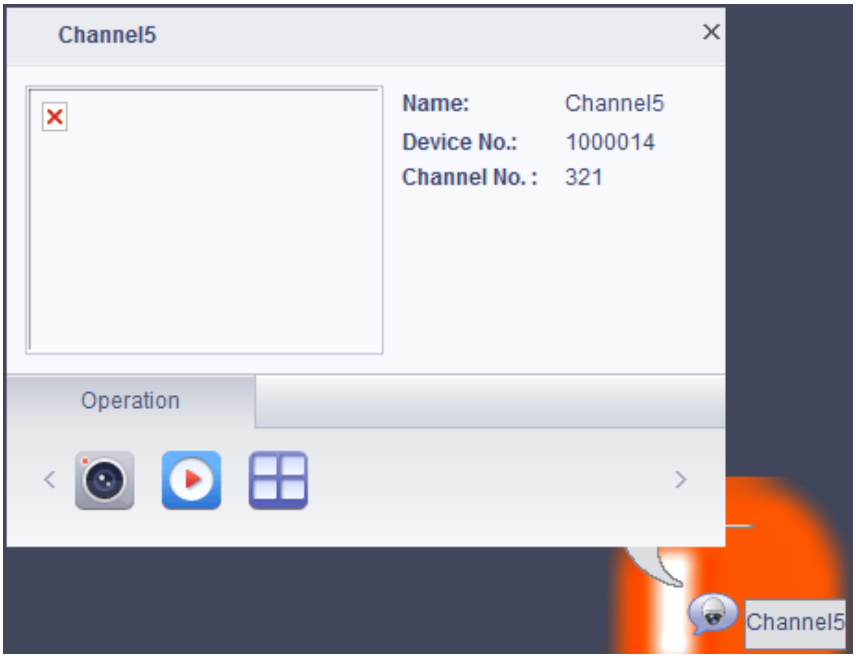


Figure 7-6

Parameter		Note
Device Operation		Open live preview of this channel. When you have live preview, the system supports local record, talk, snapshot and audio.
		Playback.
		Output this channel to video wall.
		Cancel alarm.
		Unlock.
		Call access control device.
		View unlock record.
		Announcement.
Peripheral Search		Search peripheral of this channel for video channel and ANPR channel.

Step 5. Click  , open Video to open live preview, see Figure 7-7.

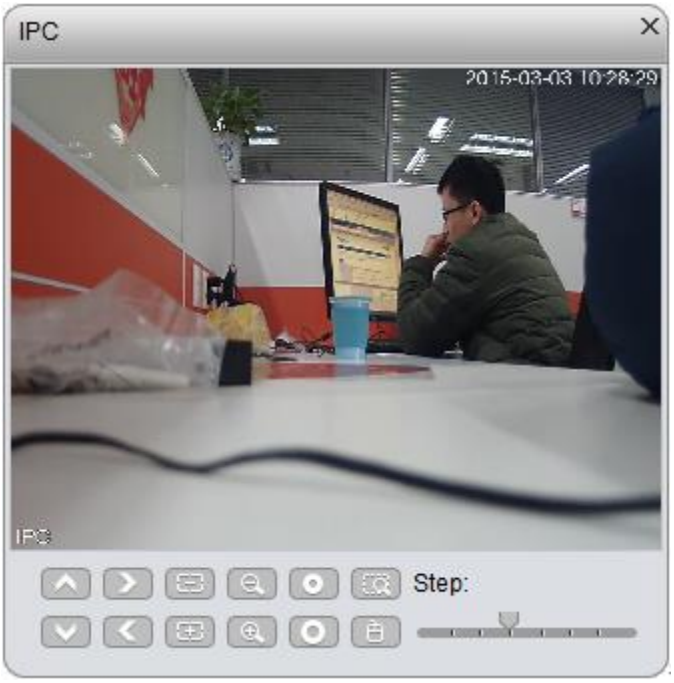


Figure 7-7

Step 6. Click  , configure playback time and storage type. You can search playback record. See Figure 7-8.

Figure 7-8

Step 7. Click  , you can select via Preview window decode and output video to video wall, as well as select TV wall layout to output.

- Select Preview window, see Figure 7-9.

Figure 7-9

The Client supports 4-split, such as select window 1 in live preview, then the first window in Live Preview plays channel video. See Figure 7-10.

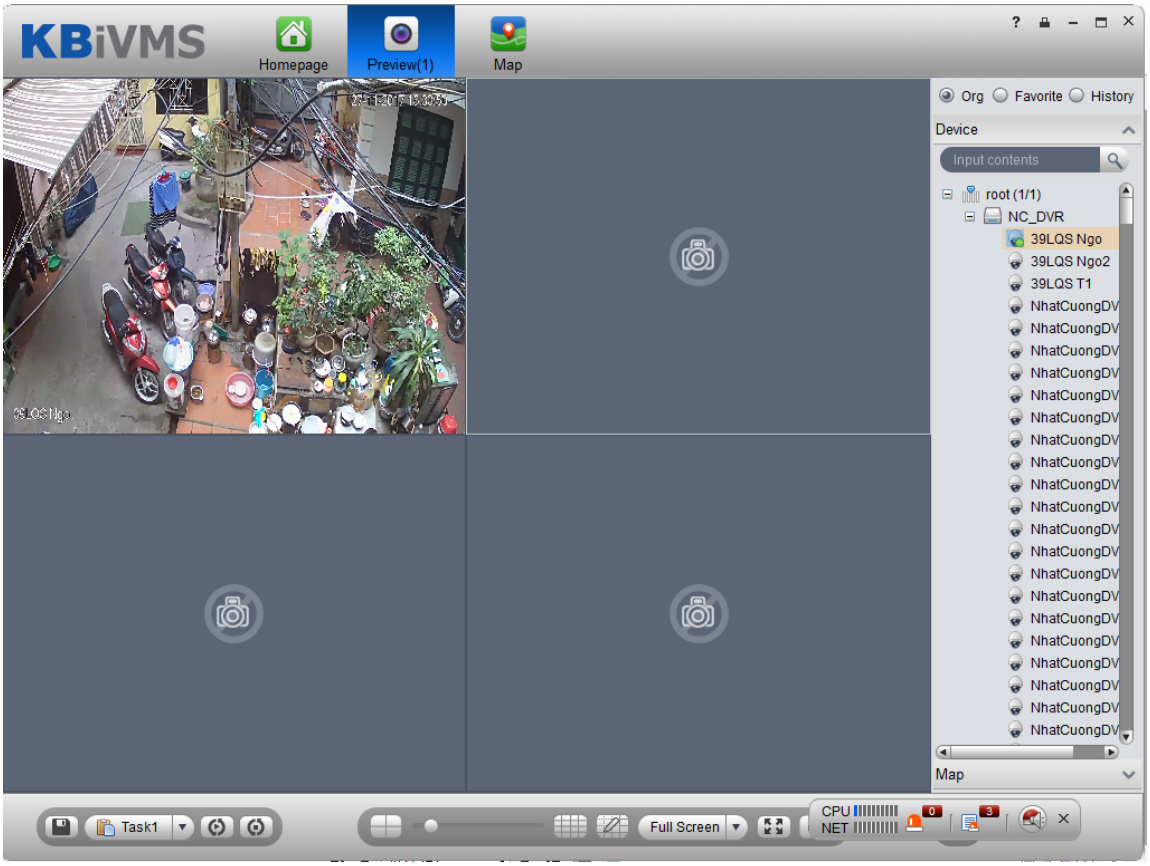


Figure 7-10

➢ Select TV wall task, output to video, see Figure 7-11.

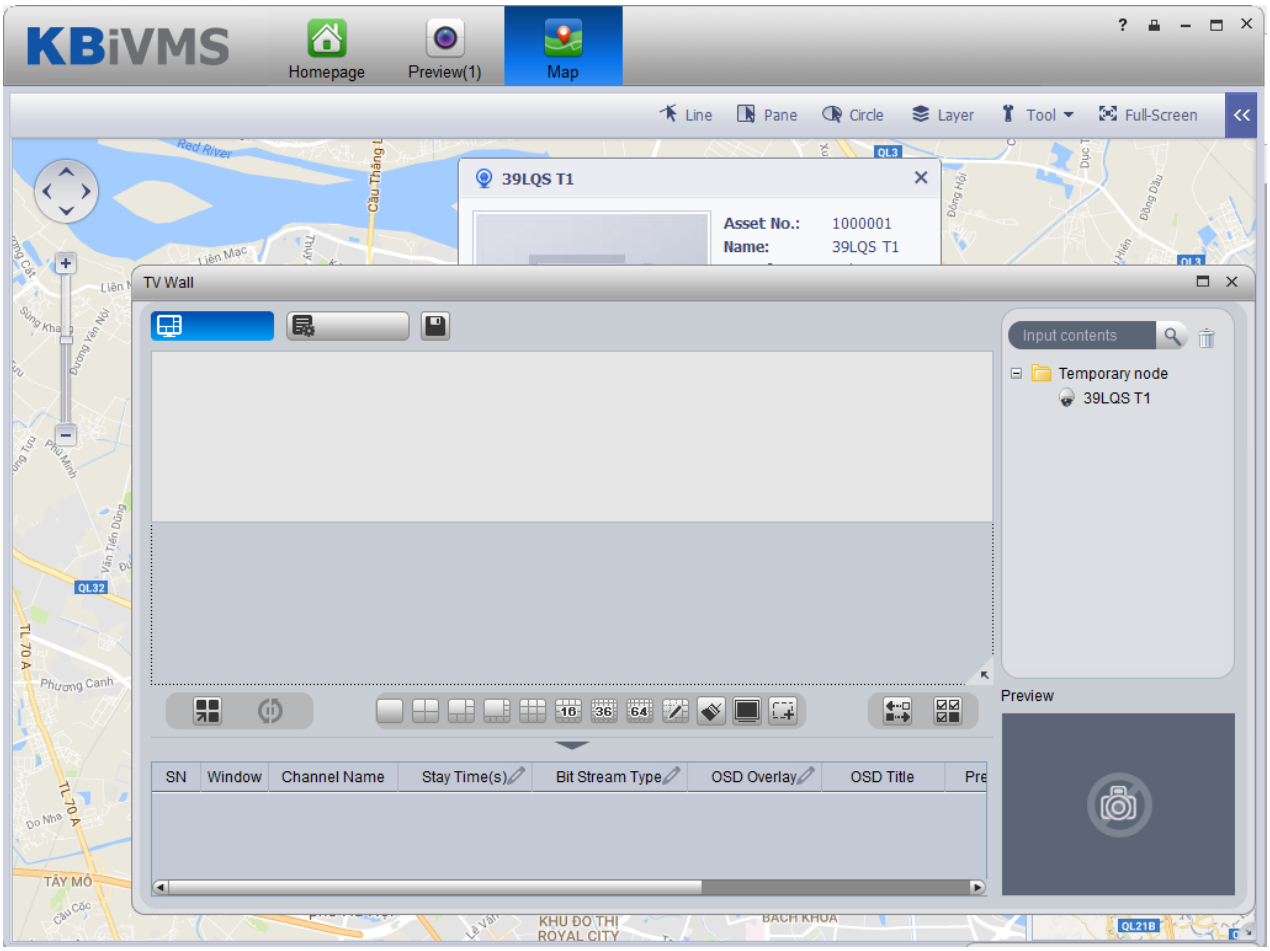


Figure 7-11

7.2 Google, Google Offline Map Config

7.2.1 Select Map

Google and Google offline map have similar configuration steps, so here we make Google online map as an example.

Step 1. Select Map Config.

Step 2. Select Google. See Figure 7-12.

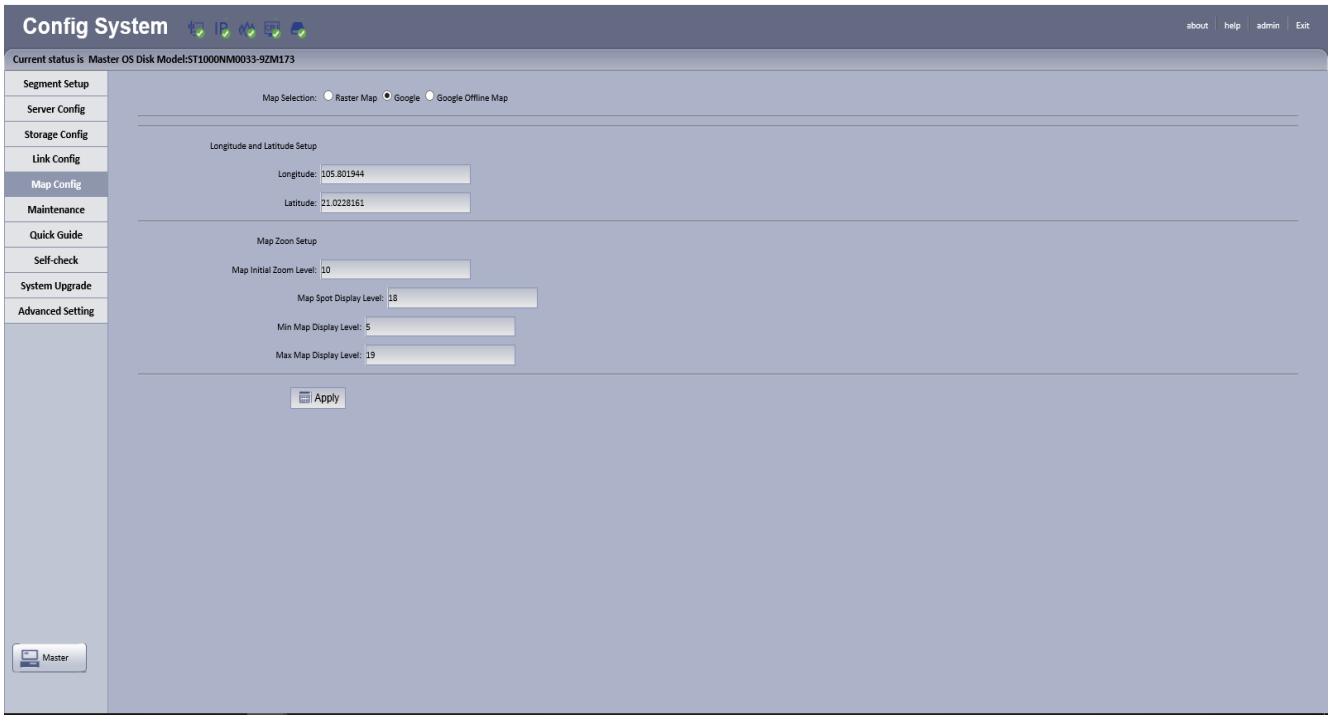


Figure 7-12

Step 3. Input Longtitude and Latitude of the map, click Apply.

7.2.2 KBiVMS Manager Map Config

Step 1. Login KBiVMS Manager.

Step 2. Select Business>Map.

Step 3. Drag device channels under video device, alarm input tabs onto map, see Figure 7-13.

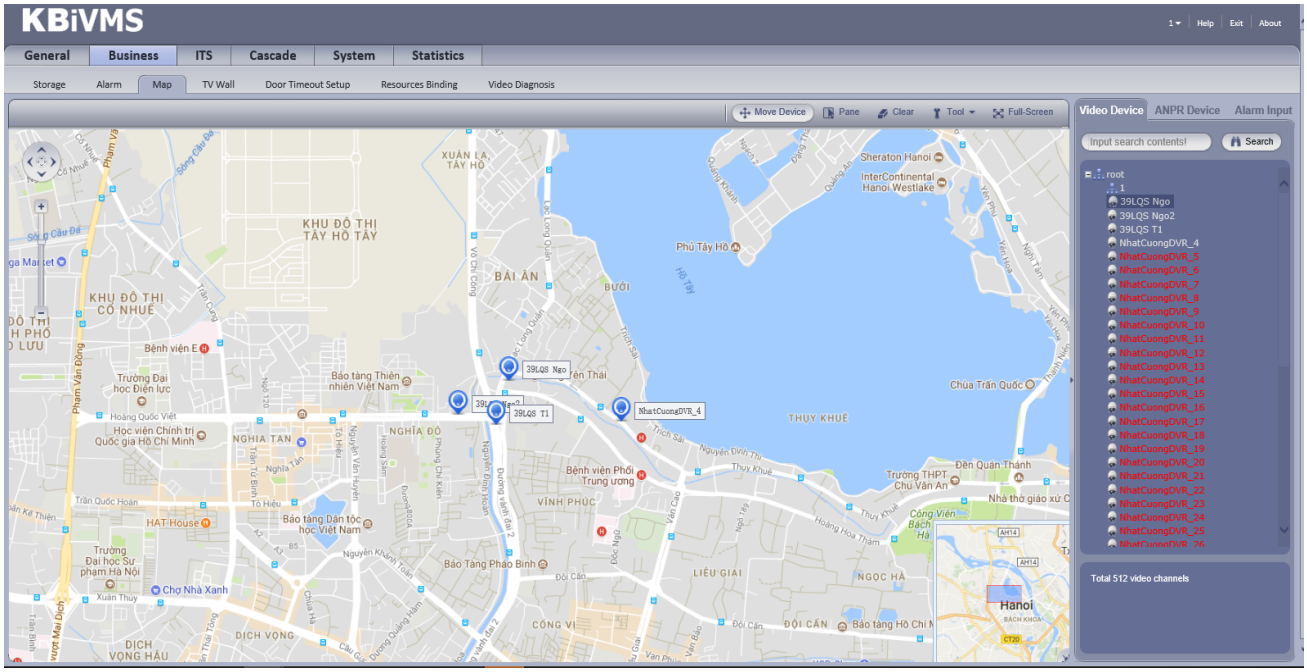


Figure 7-13

Parameter	Note
Move Device	Click to move device on map.
Pane	Select device via pane.
Clear	Clear pane selection on screen.
Tool	Include distance, side measuring, mark and reset. ● Measure distance：measure the actual distance between two points. ● Measure side：measure the actual area of a certain zone on map. ● Mark：mark on map. ● Reset：reset map to initial position.
Full-Screen	Show e-map in full screen. Under full screen mode, click exit full screen at the upper-right corner to exit.
Add Heat Zone	Click Add heat zone. Select position on map and add heat zone map. After entering heat zone, you can continue adding lower heat zone map. On Client map, click heat zone, the system will auto link map to heat zone map.

7.2.3 **KBiVMS Client Using Map Function**

Step 1. Login KBiVMS Client.

Step 2. Click  in Basic Function area. As shown in Figure 7-14, device dragged onto map on Manager are shown.

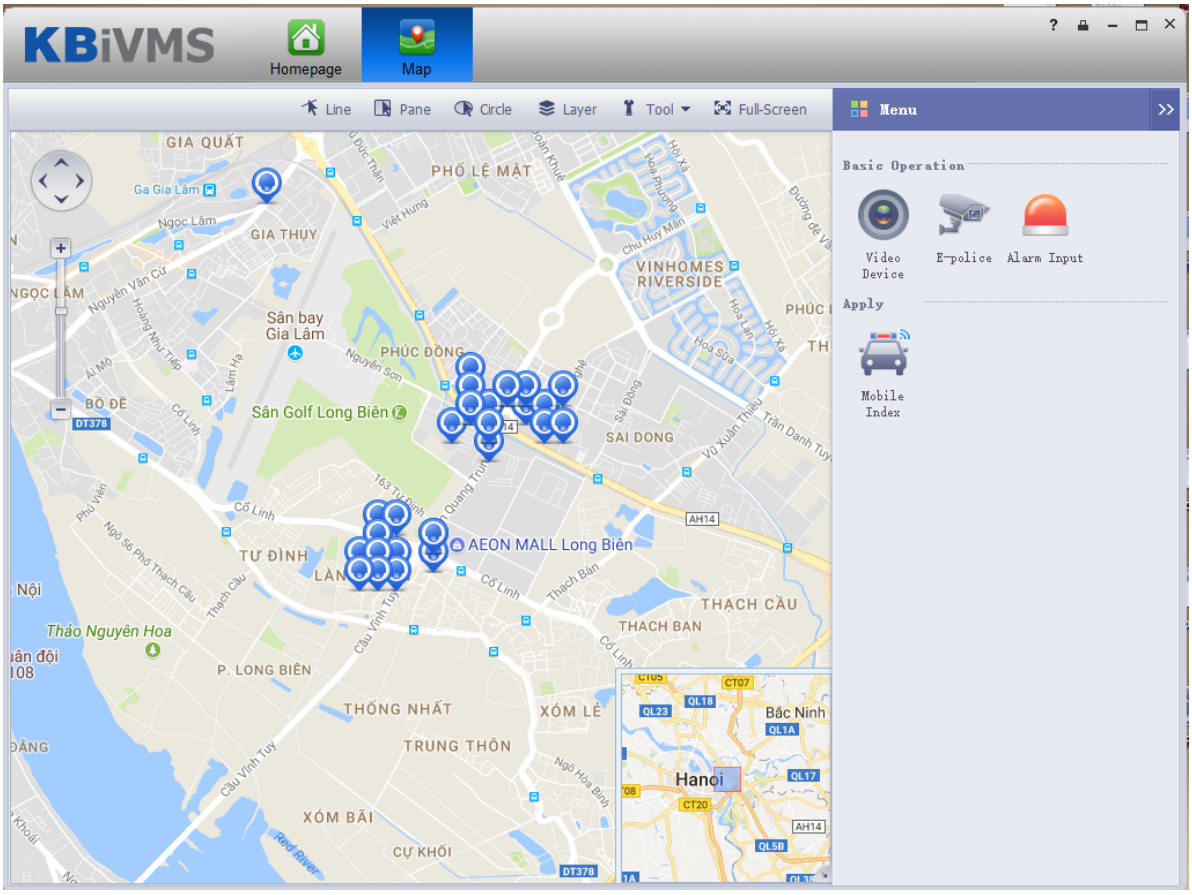


Figure 7-14

Step 3. Click Initial Angle, according to laser dome and thermal imaging device's actual installation adjustment angle. See Figure 7-15.

Note:

If you want to use visible range function, you must add speed dome with visible range function first.

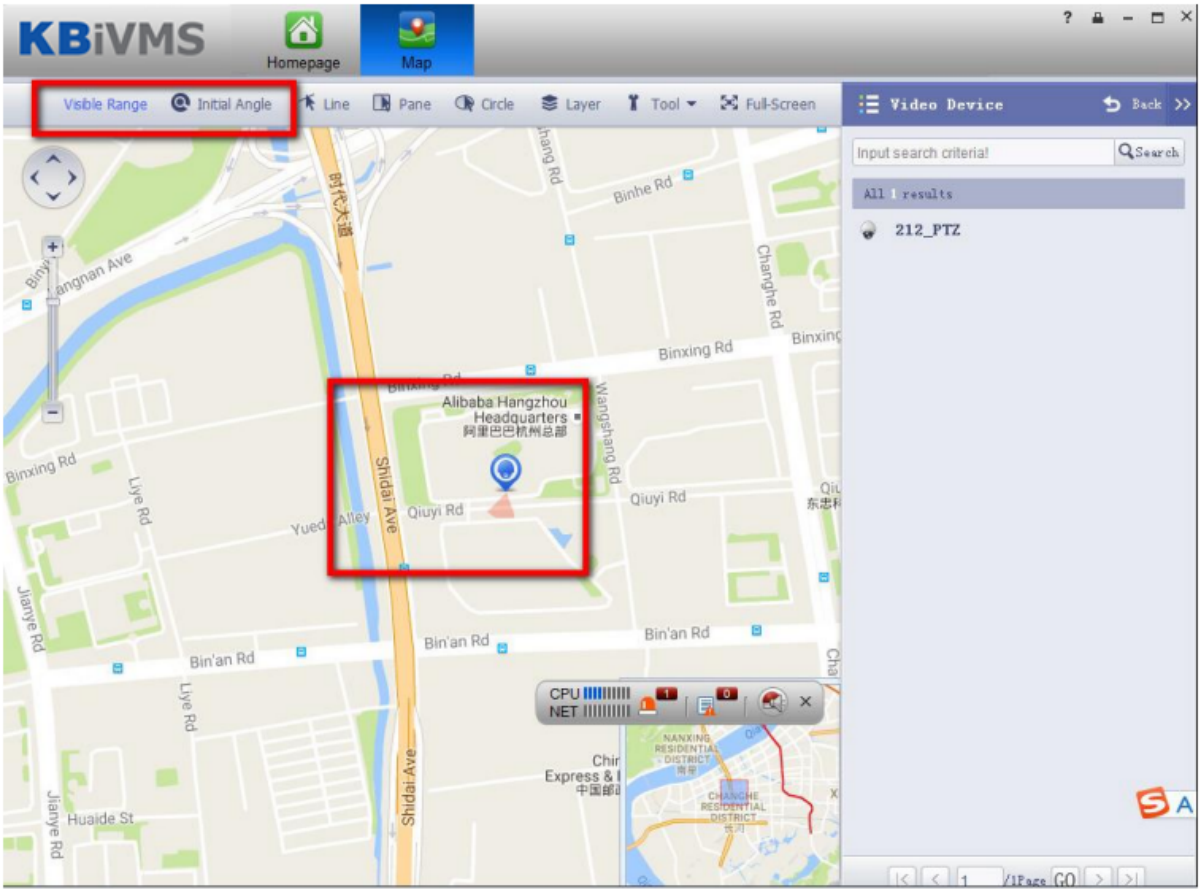


Figure 7-15

Step 4. Click Initial Angle again, this button will be off.

Step 5. Click Visible Range. On map, you can view visible range of laser dome or thermal imaging device, see Figure 7-16.

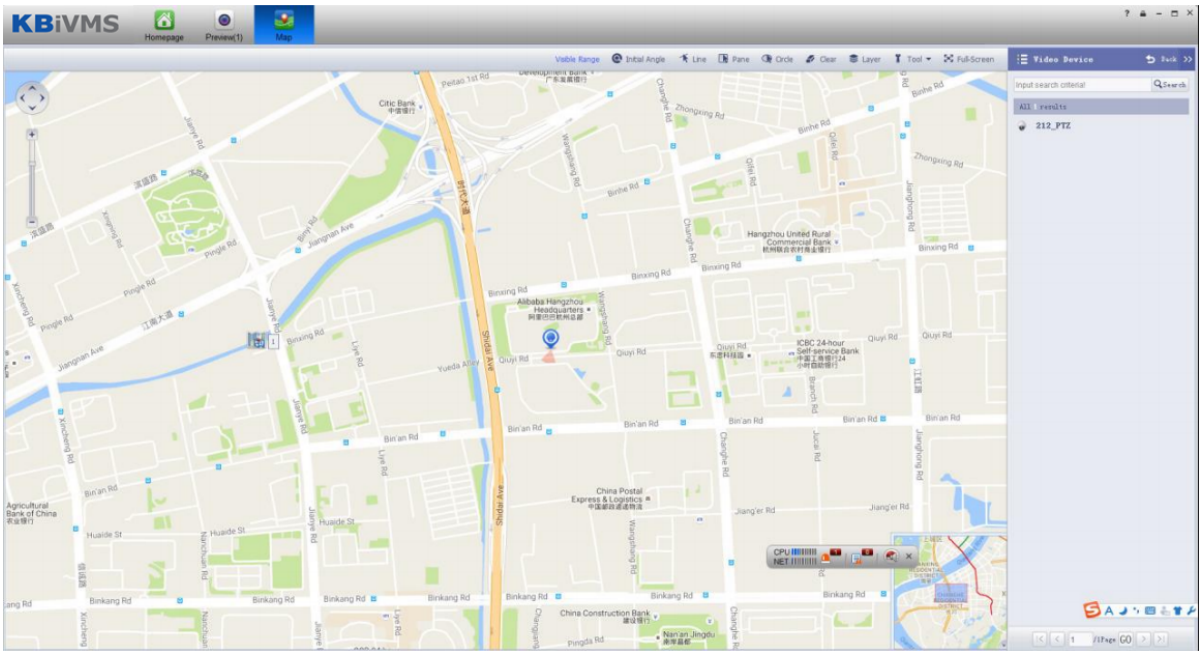


Figure 7-16

Step 6. Open corresponding device live, click PTZ direction button, and device visible range on the corresponding map will rotate. Similar, if you rotate visible range of device on map, the live window will also rotate correspondingly. See Figure 7-17.

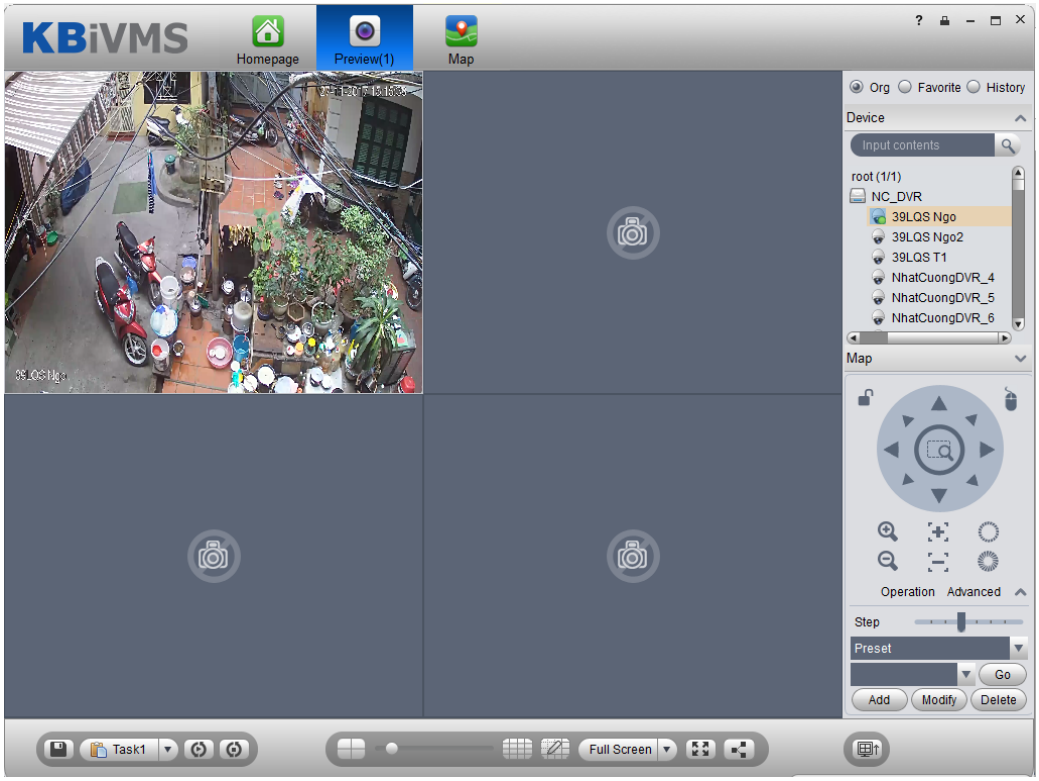


Figure 7-17

Step 7. Click  or  , visible range on corresponding map will also zoom.

Step 8. Click Visible Range again, the button will be off.

Step 9. Click 

on the right. The interface shows surveillance spots in a list with their detailed locations, see Figure 7-18.

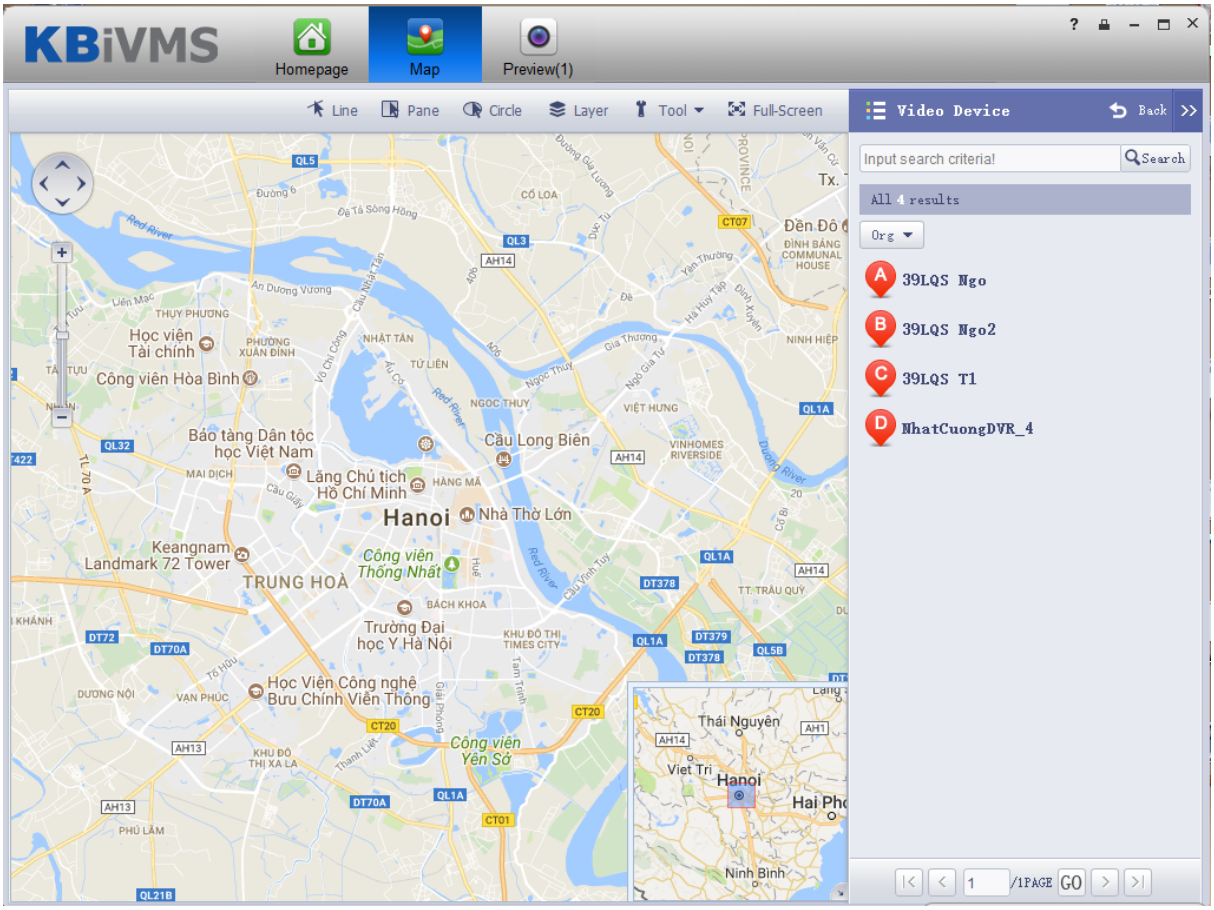


Figure 7-18

Step 10. Click spot, for example: A.

Detailed location is shown on map, such as device no., channel name and etc. See Figure 7-19.

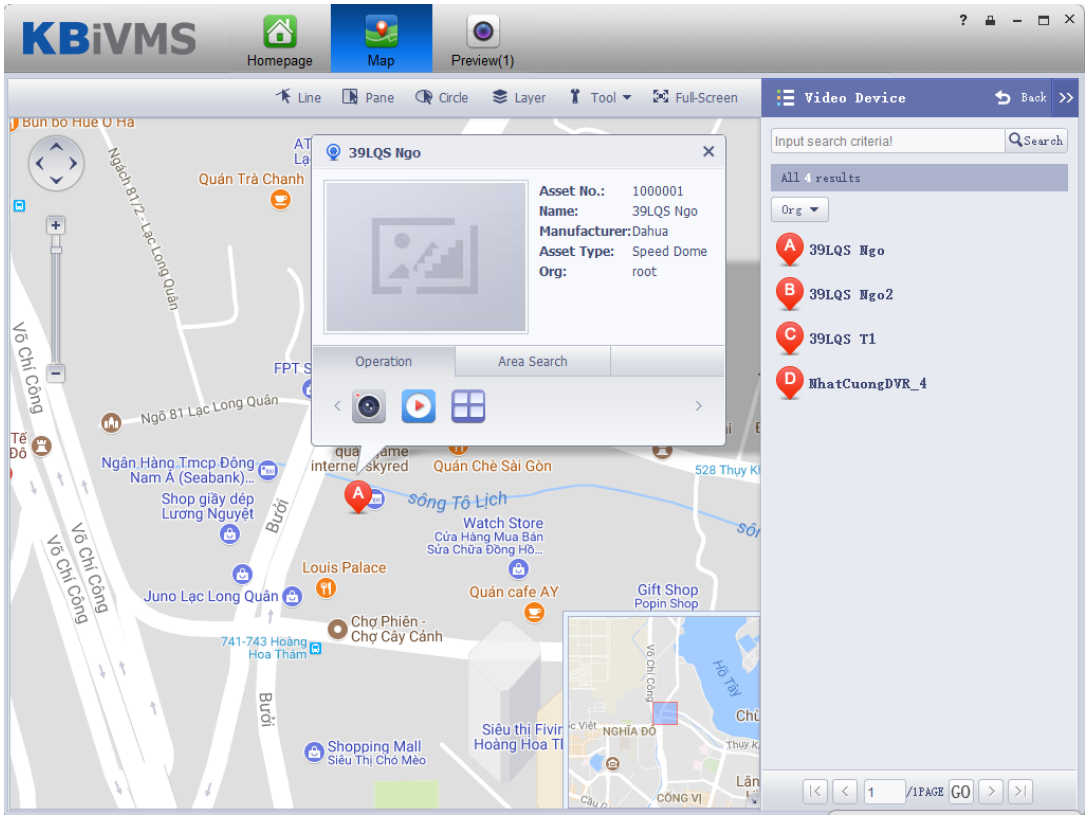


Figure 7-19

Parameter		Note
Device Operation		Open live preview of this channel. When live preview is in progress, the system supports local record, audio intercom, snapshot and ON/OFF audio.
		Playback this channel's record.
		Decode and output this channel to wall.
Area Search		Search for video channel and ANPR e-police within surrounding of this channel.

1. Click in Operation area, to view live preview.
   See Figure 7-20.

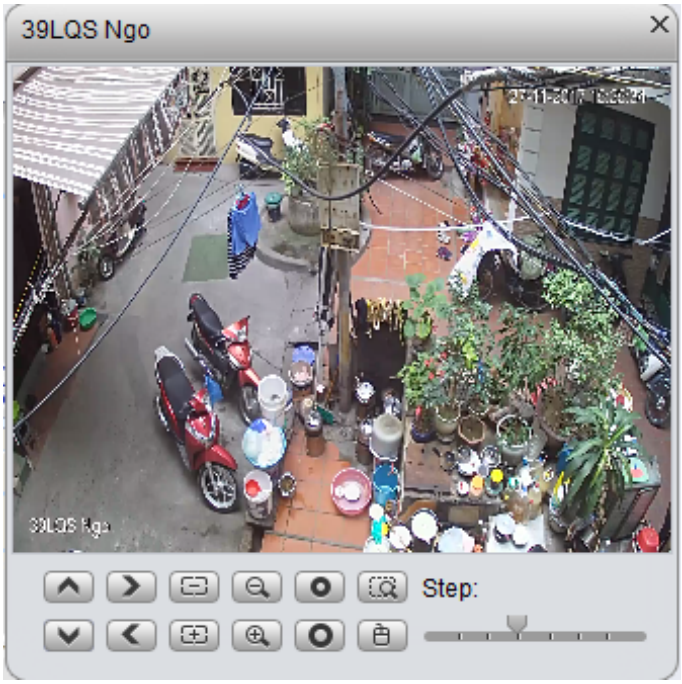


Figure 7-20

2. Click in device operation area, to playback record on device or platform. See Figure 7-21.

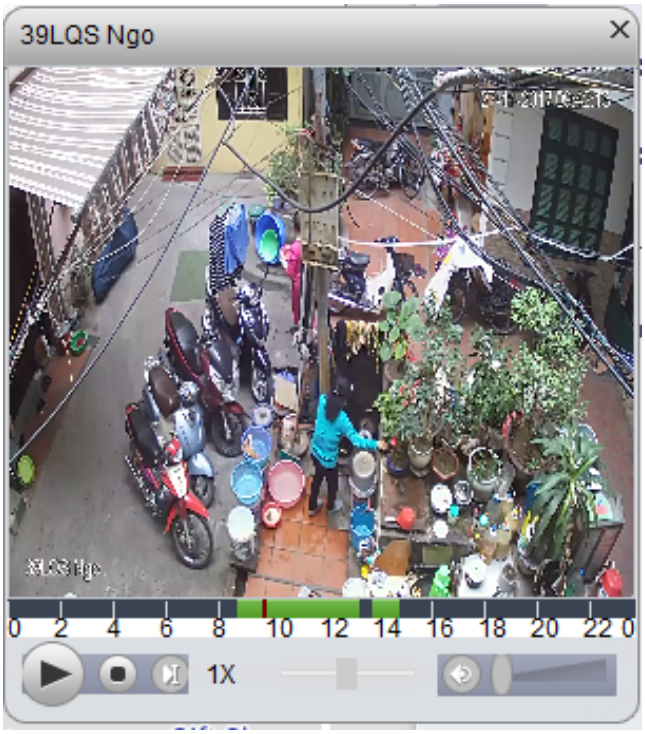


Figure 7-21

3. Click within operation box, to output video to wall.
   See Figure 7-22. Please refer to Ch 10.

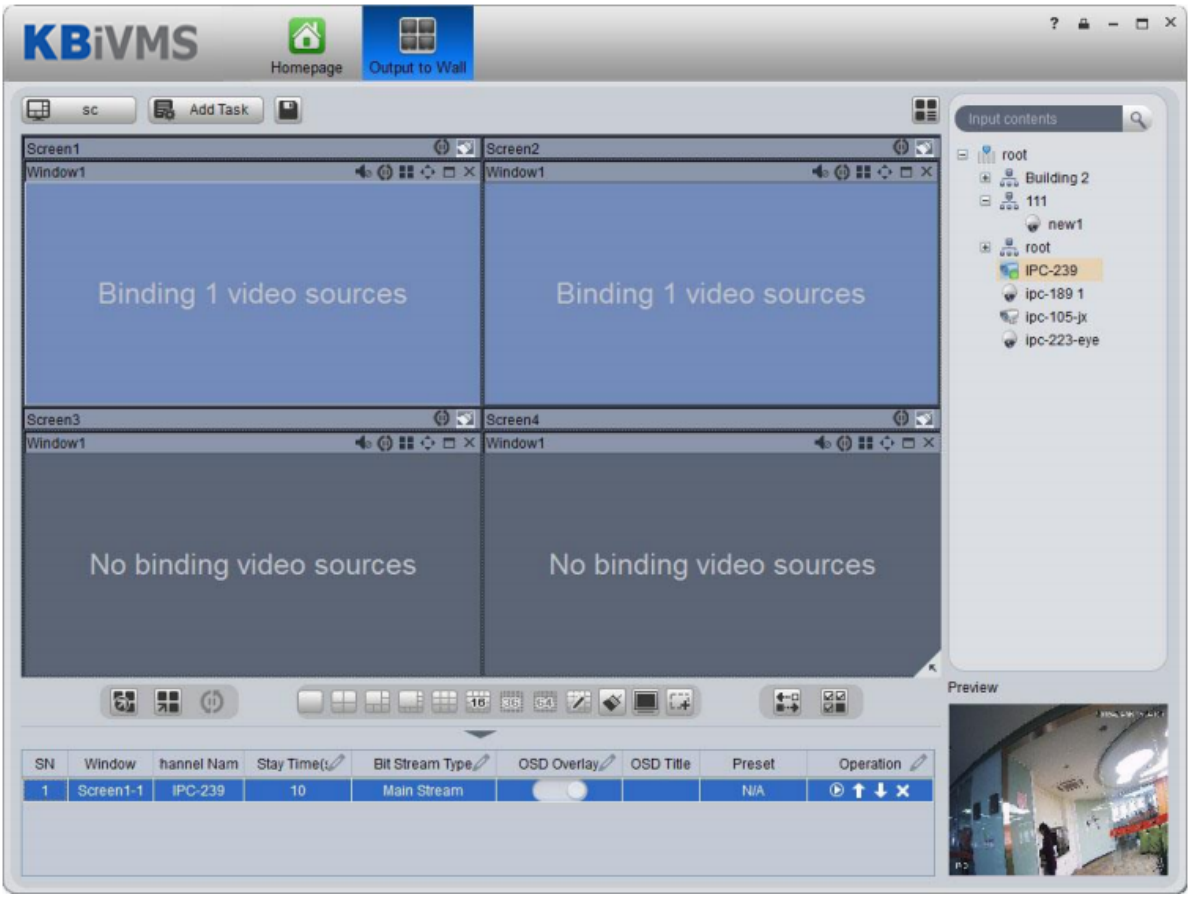


Figure 7-22

8 Alarm

KBiVMS Platform supports alarm function, and you need to set alarm source on device first. Different devices need different alarm type. Here makes NVR an example and introduces web config steps.

8.1 Device-end Config

Step 1. Directly login device web end, or go to KBiVMS Client Manager-end Device interface>NVR device tab, click .

Step 2. Open EVENT tab.

Step 3. Click VIDEO DETECTION.

Video detection includes Motion Detect, Video Loss, Tampering, Video Analytics. For example, make Motion Detect as an example. See Figure 8-1.

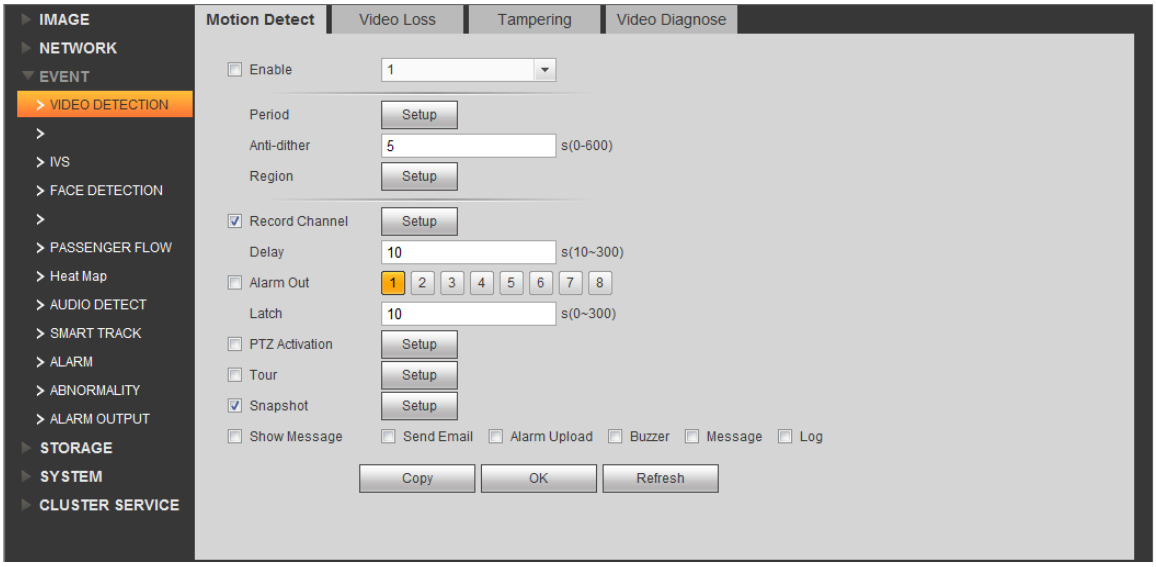


Figure 8-1

Parameter	Note
Enable	
Period	Set monitoring period.
Anti-dither	Set anti-dither time.
Region	Set monitoring zone.
Record Channel	
Delay	Set alarm delay time.
Alarm Out	Select alarm output.
Latch	
PTZ Activation	PTZ activation.
Tour	Select alarm video output.
Snapshot	Set snapshot channel.

Parameter	Note
Show Message	Send Email：send email when alarm occurs. Alarm Upload：report alarm to KBiVMS platform. Here please check, otherwise the platform cannot record alarm. Buzzer：buzzer prompt alarm. Message：send message when alarm occurs. Log：alarm log generated when alarm occurs.

Step 4. Configure parameter info, click OK.

Step 5. According to actual need, you can click FACE DETECTION, AUDIO DETECT, ALARM and other tabs to configure alarm parameter.

Then configure Local Alarm under Alarm tab.

Step 6. Select ALARM>Local Alarm. See Figure 8-2.

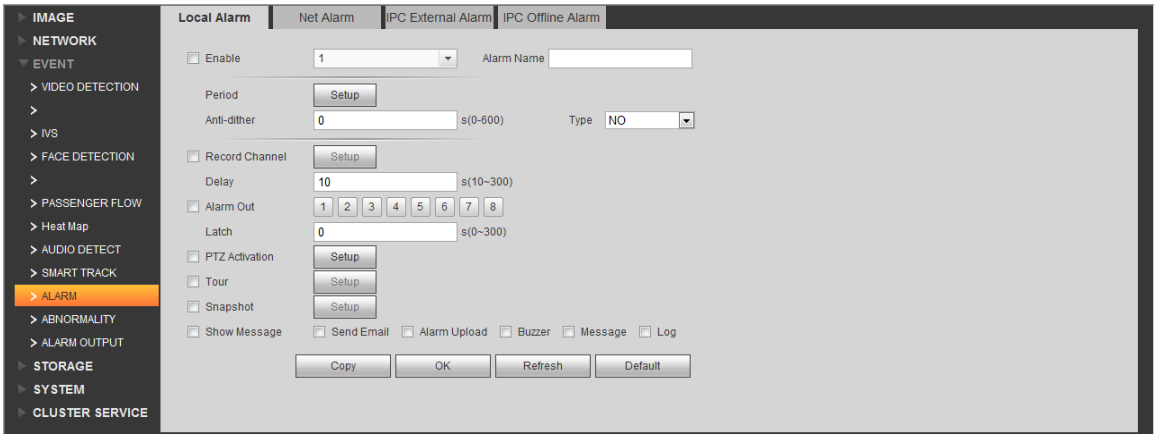


Figure 8-2

Parameter	Note
Period	Set monitoring period.
Delay	Set alarm delay time.
Alarm Out	Select alarm output.
PTZ Activation	PTZ activation.
Tour	Select alarm video output.
Snapshot	Set snapshot channel.
Show Message	Send Email：send email when alarm occurs. Alarm Upload：report alarm to KBiVMS platform. Here please check,otherwise the platform cannot record alarm. Buzzer：buzzer prompt alarm. Message：send message when alarm occurs. Log：alarm log generated when alarm occurs.

Step 7. Configure parameters, click OK.

8.2 Config KBiVMS Manager Alarm Scheme

Manager configured alarm scheme is for the entire platform, not a specific user. Thus all user logged in the platform can receive alarm.

- Contact: user you want to send alarm to.

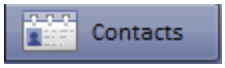
- Link level: link level of alarm.
- Alarm storm: batch config time interval of alarm. For the same device and same type of alarm, when alarm is frequent, set alarm interval may make alarm report at a fixed interval.
- TV wall Alarm Window Setup: set TV wall open window layout.
- Alarm scheme: used to configure alarm scheme template.

8.2.1 Set Contacts

When you add user into contacts and if the setup of Link Level includes email or sms, then system will send email or sms to the new contact.

Step 1. Login KBiVMS Client Manager.

Step 2. Click Business>Alarm tab. System displays Alarm interface.

Step 5. Click 

.

Step 6. Click 

. System pops up a Add Contacts box. See Figure 8-3.

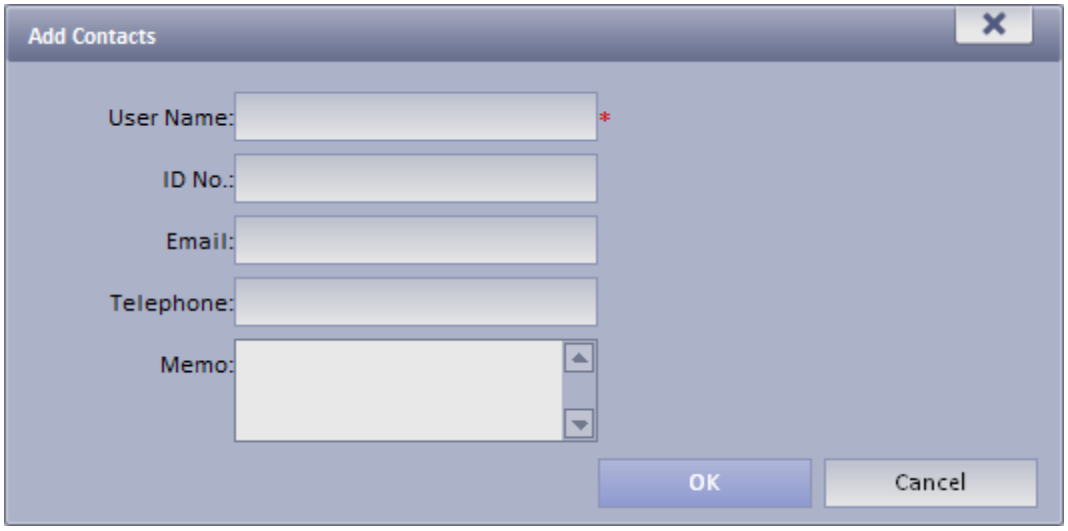


Figure 8-3

Step 7. Input User Name, ID No., Email and Telephone.

Step 8. Click OK.

8.2.2 Set Link Level

You can set Link Level and its corresponding Link Mode as 1 is the highest and 5 is the lowest.

Step 1. Click 

. System pops up an interface as in Figure 8-4.

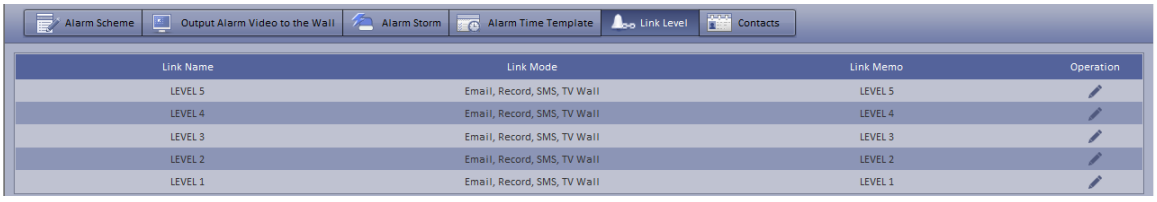


Figure 8-4

Step 9. Click . See Figure 8-5.

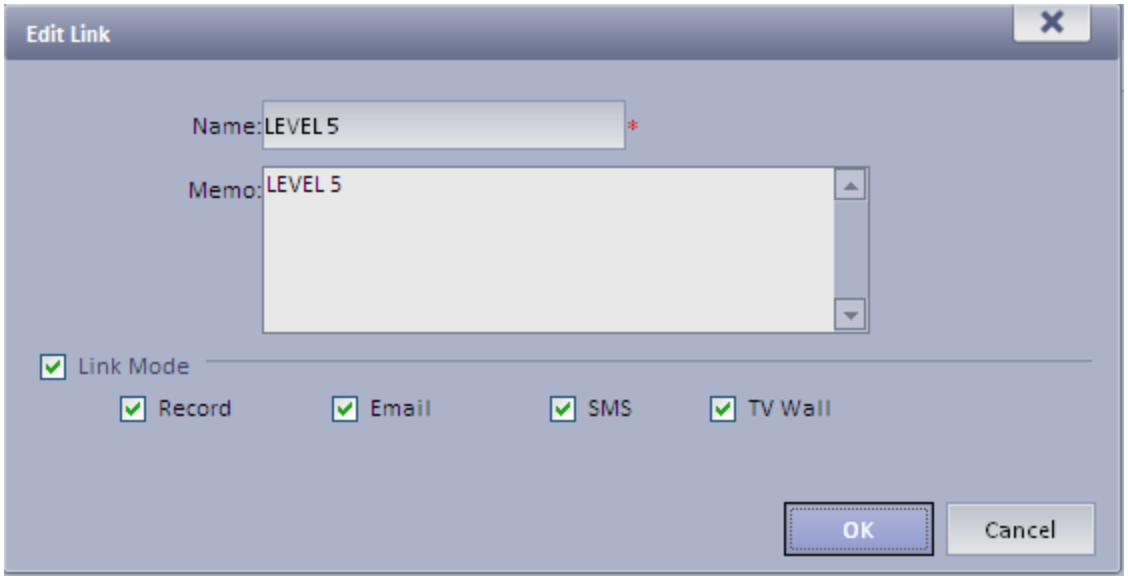


Figure 8-5

Step 10. Set Link Level Name and select Link Mode.

Step 11. Click OK.

8.2.3 Set Alarm Storm

You can set alarm interval and customized alarm storm as batch.

- **Set alarm interval as batch**

Step 1. Click Alarm Storm. System displays Alarm Storm interface.

Step 2. Select one or more alarm storm, and click Alarm Interval Setup. System pops up a box as in Figure 8-6.

Figure 8-6

Step 3. Set Alarm Interval.

Note: The interval cannot be over 86400 seconds.

Step 4. Click OK.

You can click Cancel Alarm Interval Setup to stop alarm interval as batch.

8.2.4 Set Alarm Video on Wall

Note:

You shall configure TV wall before outputting alarm video to the TV wall. Please refer to font color in “0 video input” device list.

- Red: the channel has not configured on map.
- Grey: the channel is added on map.

Step 1. Drag ANPR input, A&C input and alarm input on the right onto map.

Step 2. Complete e-map config.

Configure Alarm Scheme as follows:

Step 1. Click 

.

The system shows added TV wall.

Step 2. Click  . System pops up an Edit Alarm Scheme box.

Step 3. Select a screen, click open window button below, such as  .

See Figure 8-7.

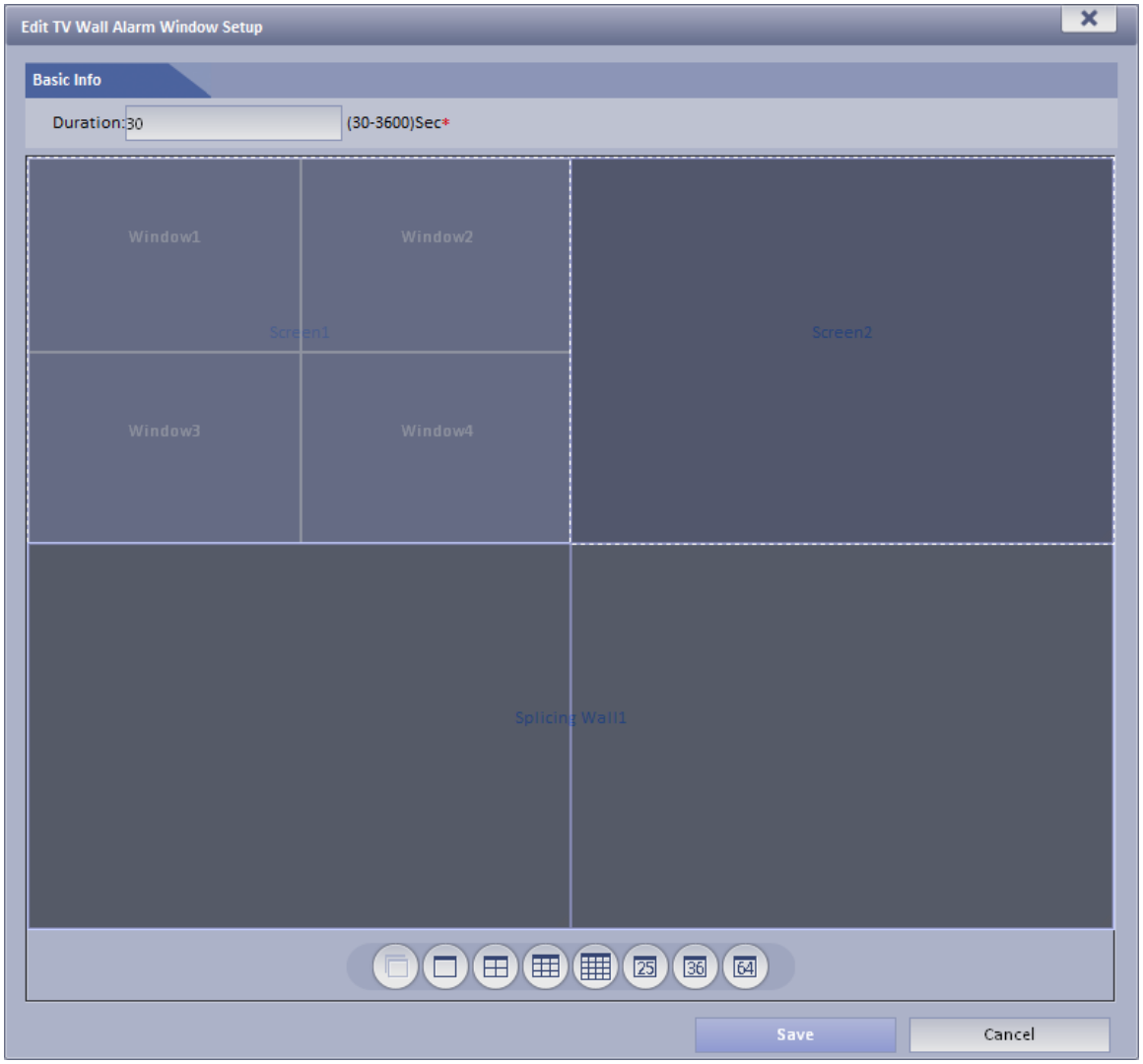
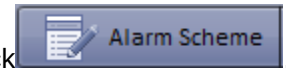


Figure 8-7

Step 4. Click Save.

8.2.5 **Alarm Scheme Config**

Configure Alarm Scheme as follows:

Step 1. Click 

.

Step 2. Click 

. System pops up an Add Alarm Scheme box as in Figure 8-8.

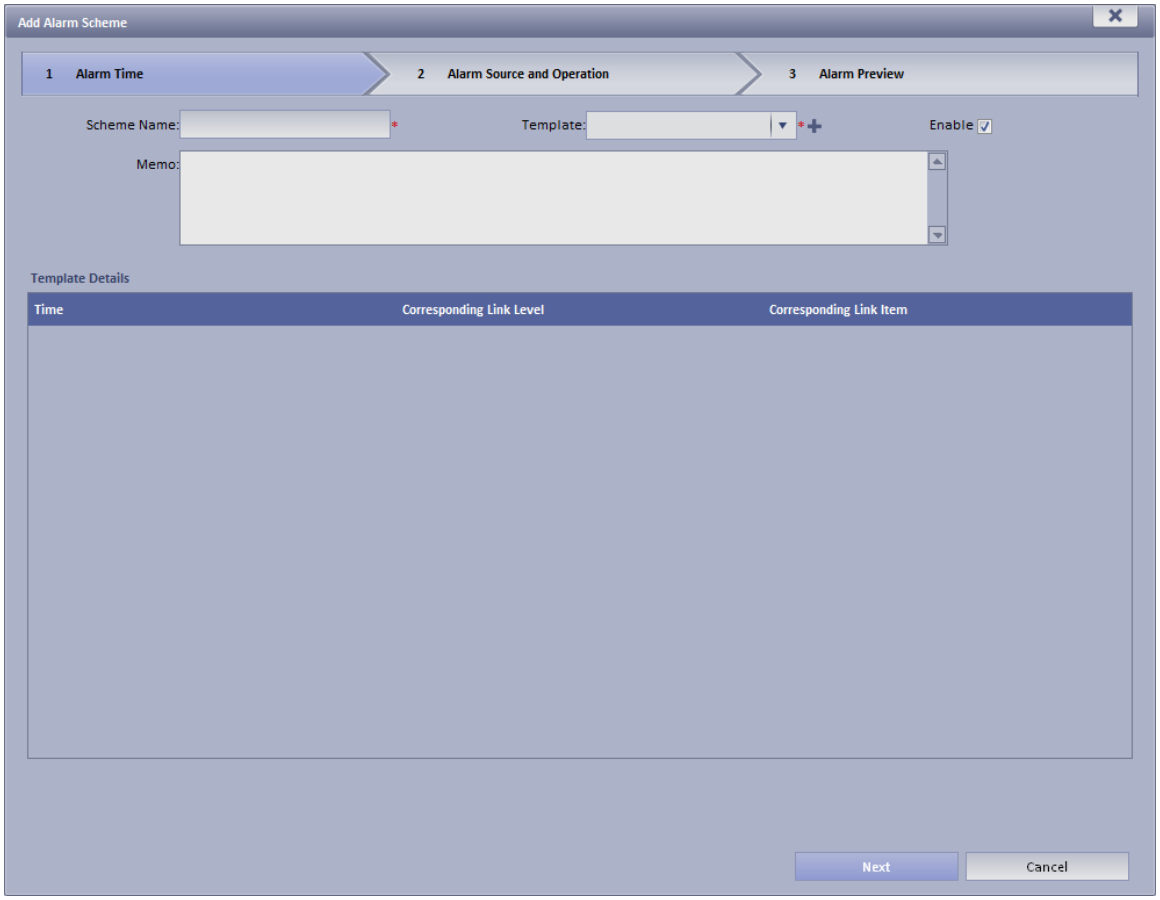


Figure 8-8

Step 3. Input Scheme Name, select template and link level, check Enable.

Step 4. Click Next. System displays Alarm Source and Operation interface.

Step 5. Click 

. System displays Add Alarm Source and Link Operation 1 box, see Figure 8-9.

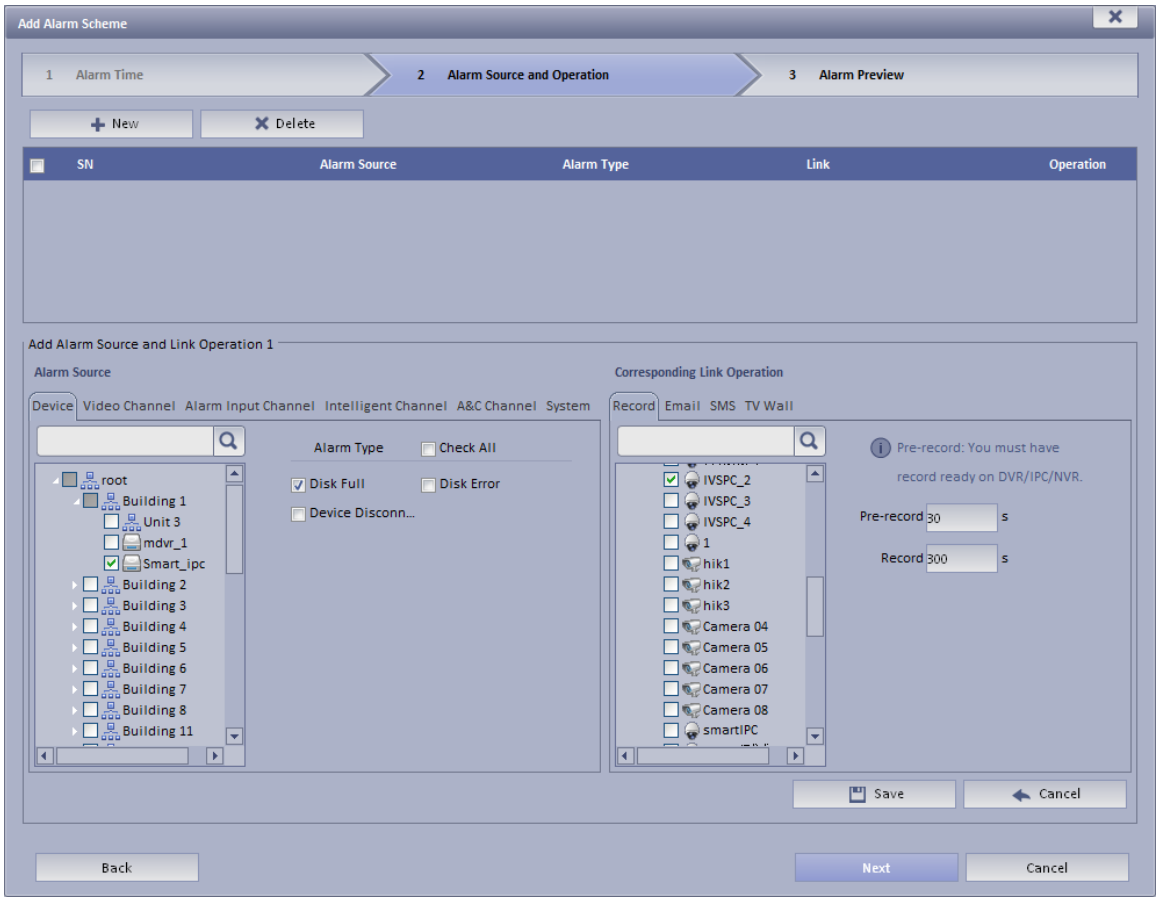


Figure 8-9

Step 6. In Alarm Source area, select alarm source and its link operation. Alarm source includes device, video channel, alarm input channel, intelligent channel, A&C channel and system. Different alarm source corresponds to different alarm type.

Step 7. In Corresponding Link Operation area, select link operation. Link operation includes Record, Mail, SMS, TV Wall and User.

- For link operation, if you select record, you shall select video channel under Record tab, and set record time.

  Note:

  If you need pre-record, then select device record needed.
- For link operation, if you select email and sms, you shall select contacts for both. Users here are users added in Contact. You can click to all alarm contacts.
- When link level is video wall, you must add link video here, and select corresponding TV wall layout window. See Figure 8-10.

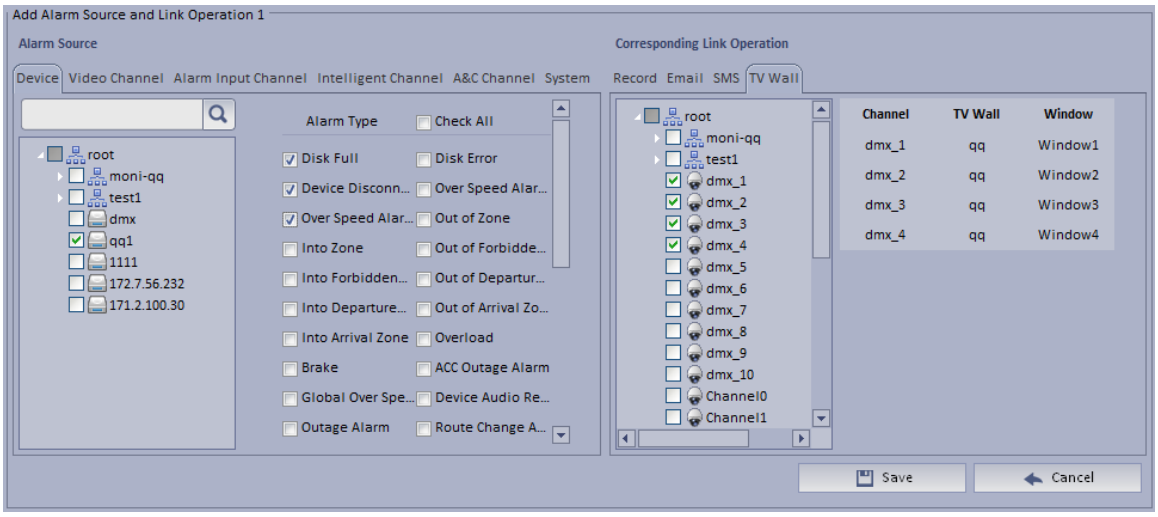


Figure 8-10

- To configure TV wall, please refer to Ch 9.2 and 8.2.4.
- When you select link action user, you shall select user to send, and users here are login user added in User.

Step 8. Click Save. System prompts a message “Successfully save scheme rule!”.

Step 9. Click OK.

Step 10. Click Next. System displays Alarm Preview interface as in Figure 8-11.

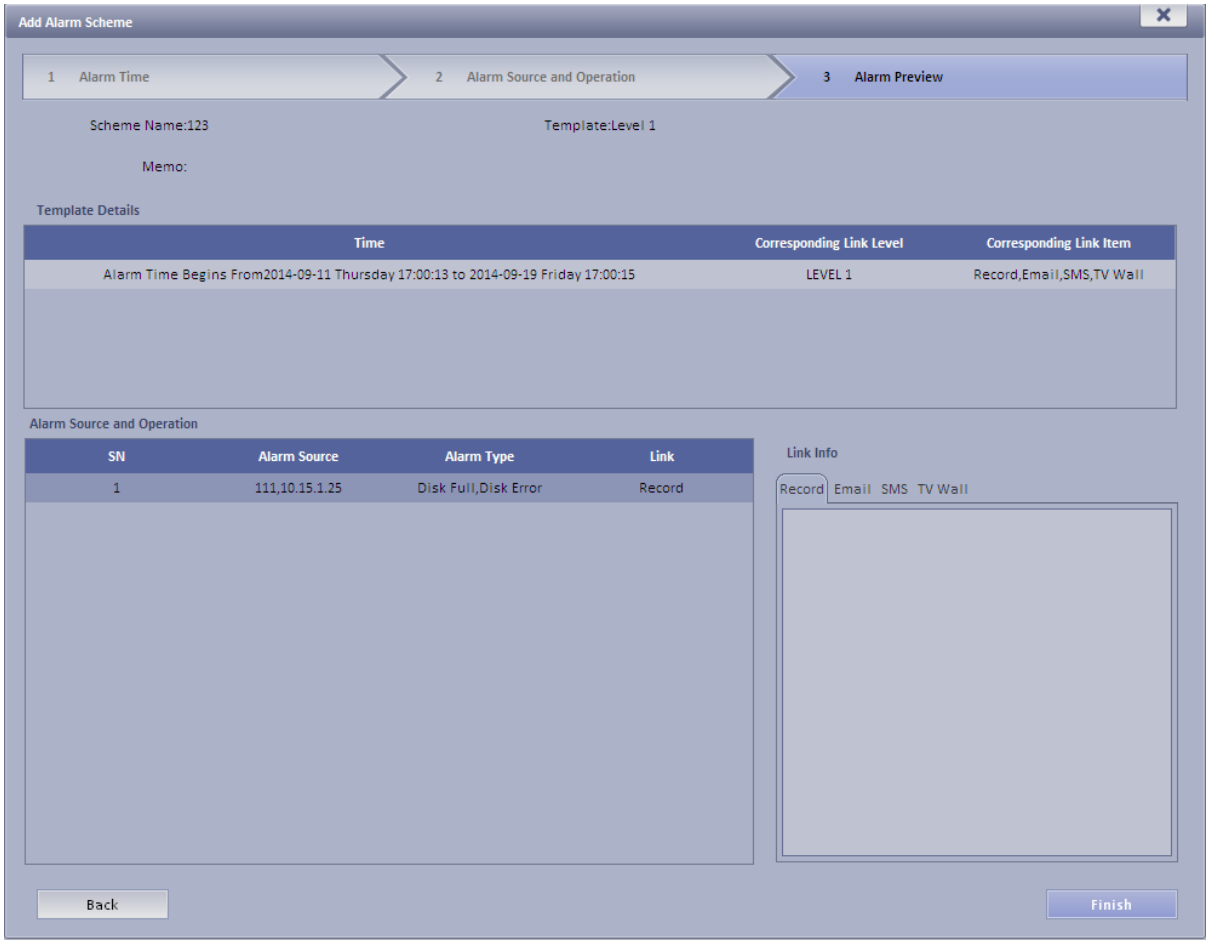


Figure 8-11

Step 11. Click Finish.

When alarm occurs, system performs link operation according to Alarm Scheme settings, and shows alarm info in Statistics>Device>Device Alarm Info.

8.3 KBiVMS Client Alarm Scheme Config

Alarm scheme configured on Client is for user of this Client.

8.3.1 Alarm Scheme Config

You can refer to the following steps to set alarm scheme.

Step 1. Login KBiVMS Client.

Step 2. Click  in Setup Manager area. System displays Alarm Scheme interface as in Figure 8-12.

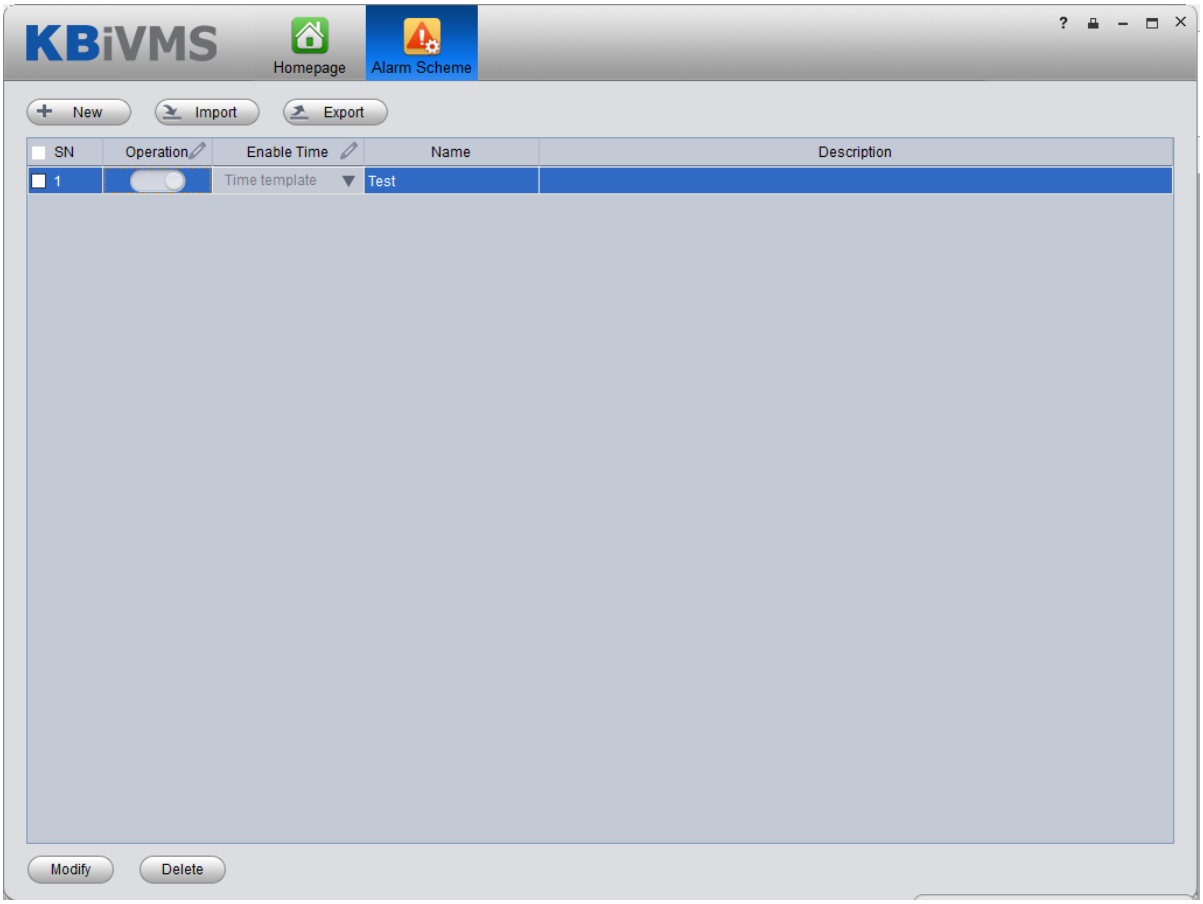


Figure 8-12

Step 3. Set scheme info.

a) Click  . System displays Global interface.

b) Input Scheme Name, Description, Time, Audio and Others as in Figure 8-13.

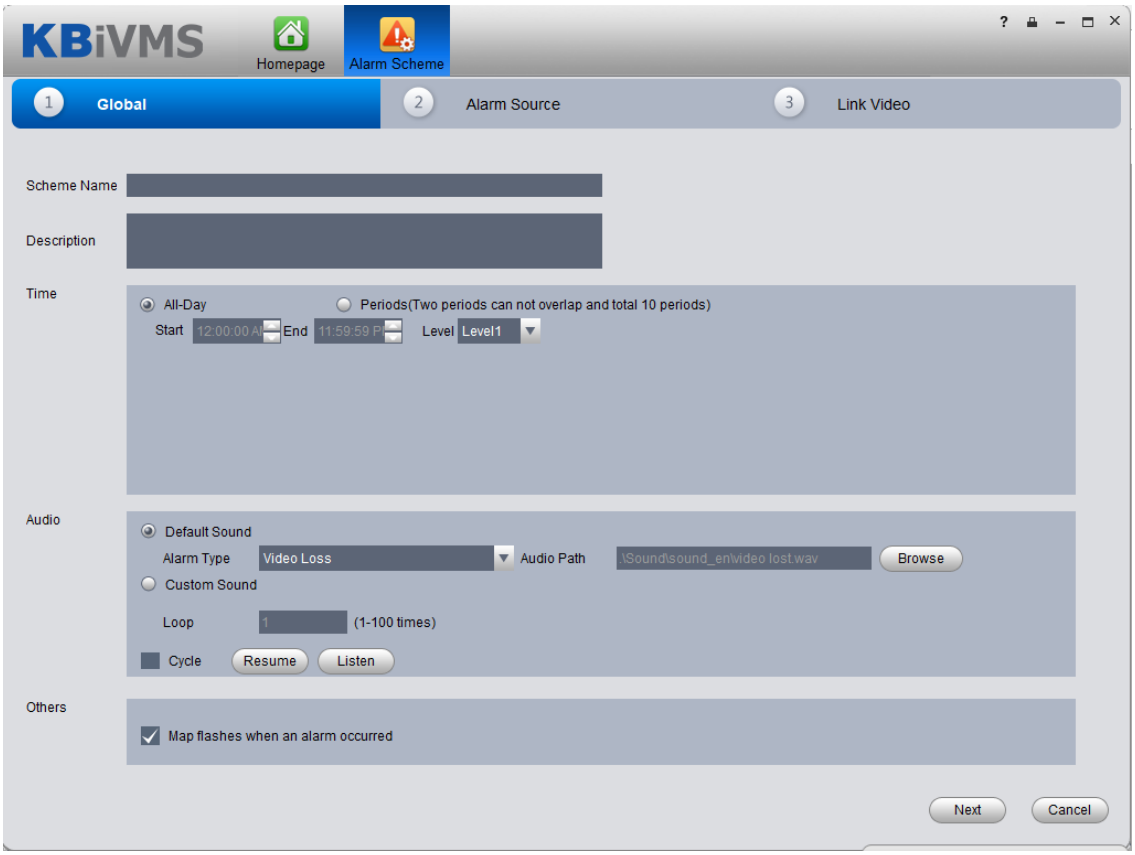


Figure 8-13

Parameter	Note
Time	Set period of arming, and select level. You can select: ● All-Day: All day is arming period. ● Periods: Certain periods in a day are arming period. You can add period via ⊕ and delete period via ⊖. **Note:** **Remaining Time Level represents periods not covered by arming.**
Audio	Set audio of alarm. You can set: ● Alarm Type: Select alarm type to set sound. ● Audio Path: Select path of audio file by click Browse. ● Loop: By selecting this cycle, alarm sound will be looped. ● Listen: You can listen to the selected sound. ● Resume: System can restore default setting of non-customizable alarm type.
Others	If check Map flashed when an alarm occurred, then when alarm occurs, it will flash on E-map.

Step 4. Set Alarm Source.

a) Click 

or Next. System displays Alarm Source interface.

b) Select channel on the left, and in Alarm Type area, select alarm type to be armed.

c) Click . System will add alarm source to list on the right as in Figure 8-14.

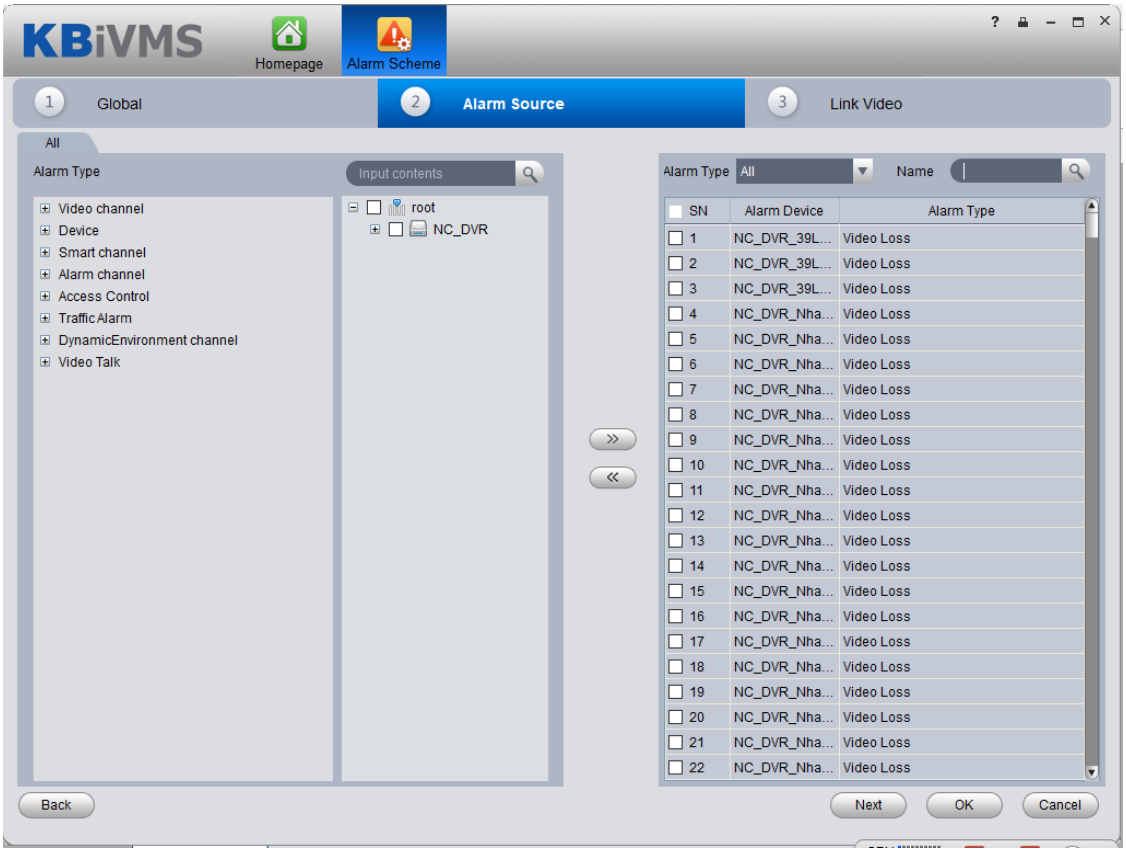


Figure 8-14

Note:

- If you want to delete alarm source, you shall select alarm source on the right, and click to remove.
- For alarm scheme, link video is not required, you can click OK to finish setup.

Step 5. Set Link Video

a) Click 3 Link Video or Next. System displays Link Video interface.

b) Select alarm source on the left.

c) Select video channel under Link Video tab.

d) Click to add selected link video to area on the right as in Figure 8-15.

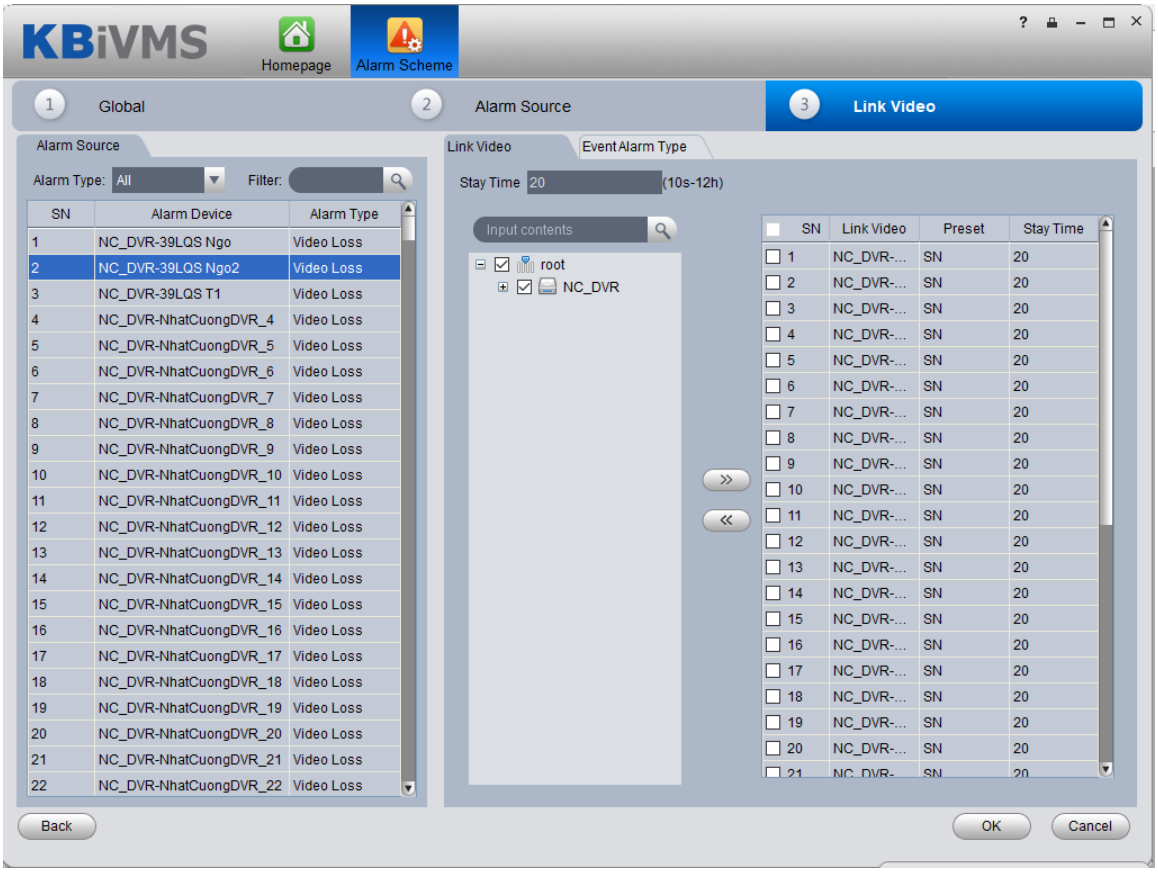


Figure 8-15

Note:

- Double click Stay Time of added link video to edit its value.
- If you want to delete added link video, you can select it and click  .

e) (Optional)Select Display in Preview Interface. See Figure 8-16.

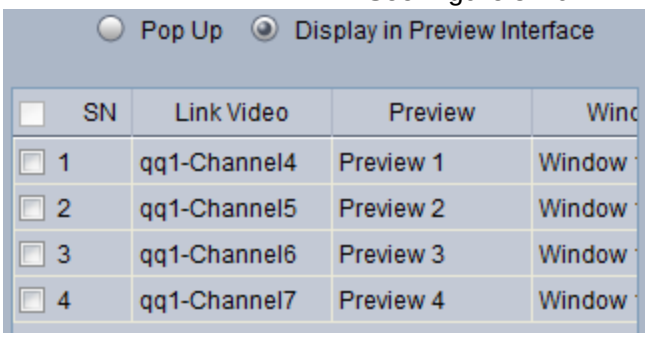


Figure 8-16

f) (Optional) In Preview dropdown list, you can select 4 split, and in Window dropdown list, select link video window.

When alarm occurs, in Live Preview interface, the corresponding window will have red flashing and it will play alarm linked video.

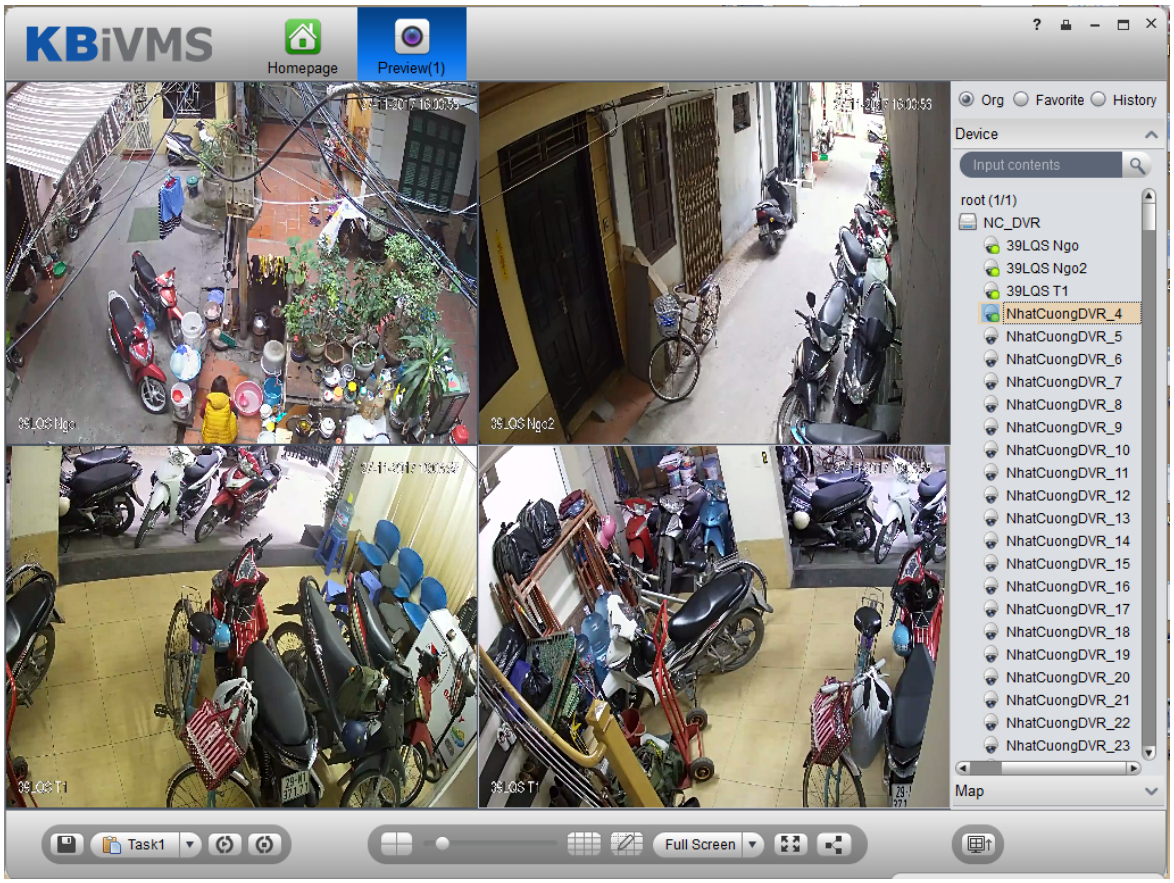


Figure 8-17

g) Select alarm output device under Alarm Output tab.

h) Select whether Auto Enable Output Device or not, input stay time. In device channel list, select channel and click  to add alarm output.

You also can check Auto Enable Output Device and edit stay time for added output items.

i) Click OK. System displays added alarm scheme as in Figure 8-18.

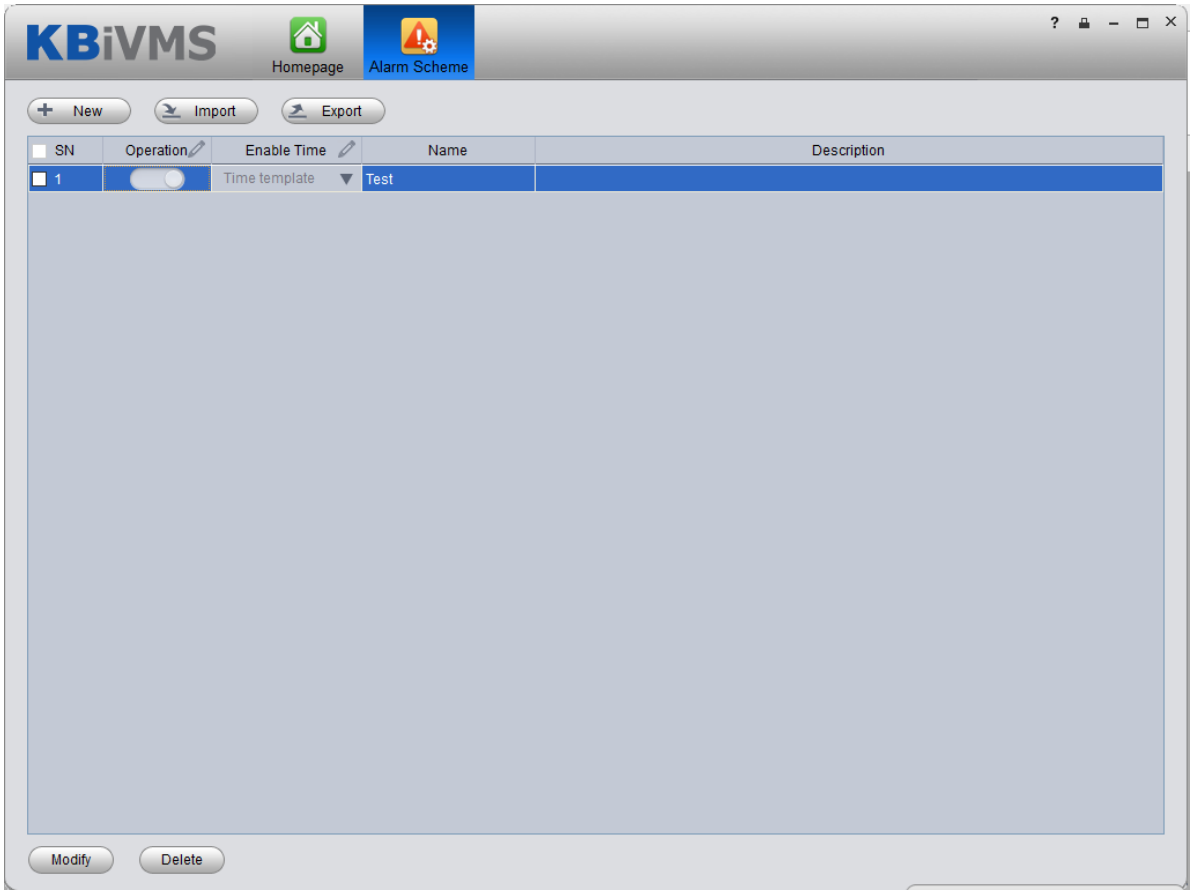


Figure 8-18

- Click  in Operation column to enable alarm scheme.
- When you enable scheme, you need to click ▼ in Enable Time column, select alarm time template, and if alarm occurs within this period, it will alarm. Alarm time template shall be set on KBiVMS Manager Business>Alarm Config, see Ch 8.2.3.

8.3.2 **Alarm Manager**

If alarm scheme is configured, when alarm occurs, Alarm Manager displays corresponding alarm.

Step 1. In homepage, Click  in Basic area. System displays Alarm Manager interface as in Figure 8-19.

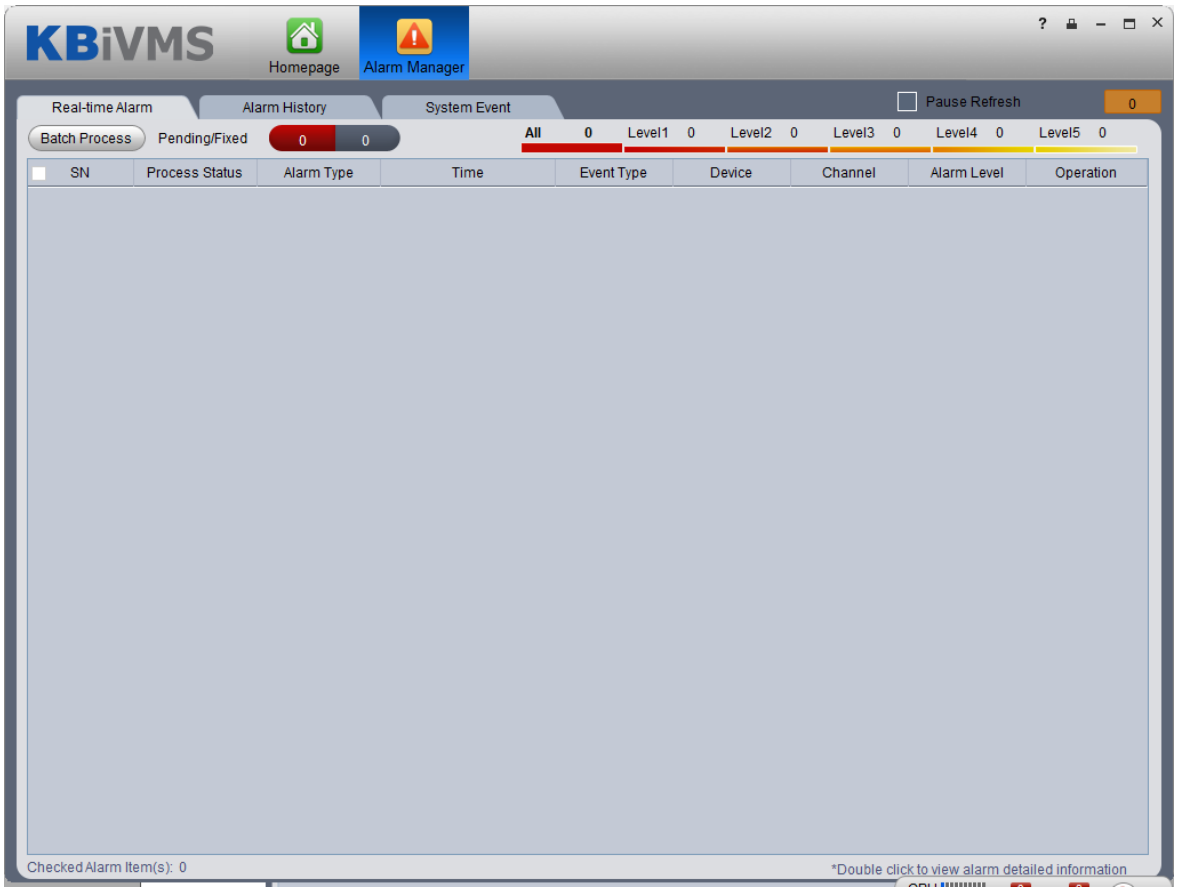


Figure 8-19

Step 2. Select alarm info, double click alarm details.

Step 3. Select process, input Results and click OK.

- You can click  in  to quickly enter Alarm Manager interface.
- Click Alarm List tab, systems displays all alarms by level.
- Click Search List tab, select corresponding channel in list on the right, and select Alarm Type, Start Time and End Time. Click Search to search alarm records meeting above criteria.
- Click System Event tab, system shows all system alarms.

8.4 Thermal Imaging Alarm

8.4.1 Add Thermal Imaging

Step 1. Select Basic Config>Device>Encoder.

Step 2. Click Add, see Figure 8-20.

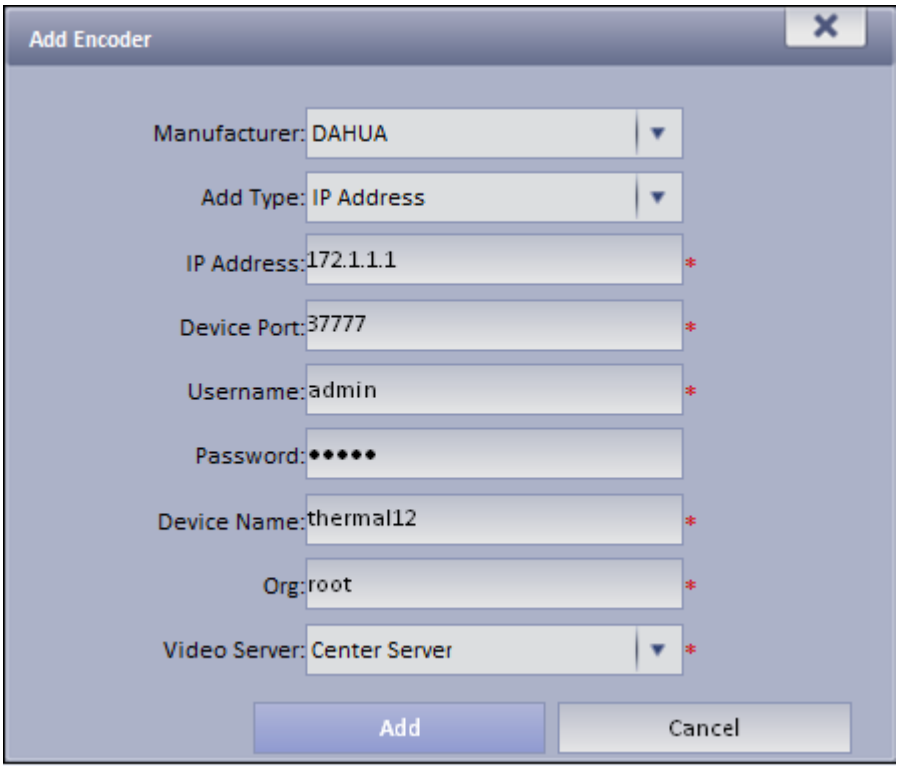


Figure 8-20

Step 3. Config IP address, device name and click Add.

Step 4. In device type dropdown list select" Thermal Camera", config video channel and etc.

Step 5. Click OK.

8.4.2 Thermal Camera Preview on Client

Step 1. Login KBiVMS Client.

Step 2. Click  in Basic function area.

Step 3. Double click thermal device channel, open view, see Figure 8-21.

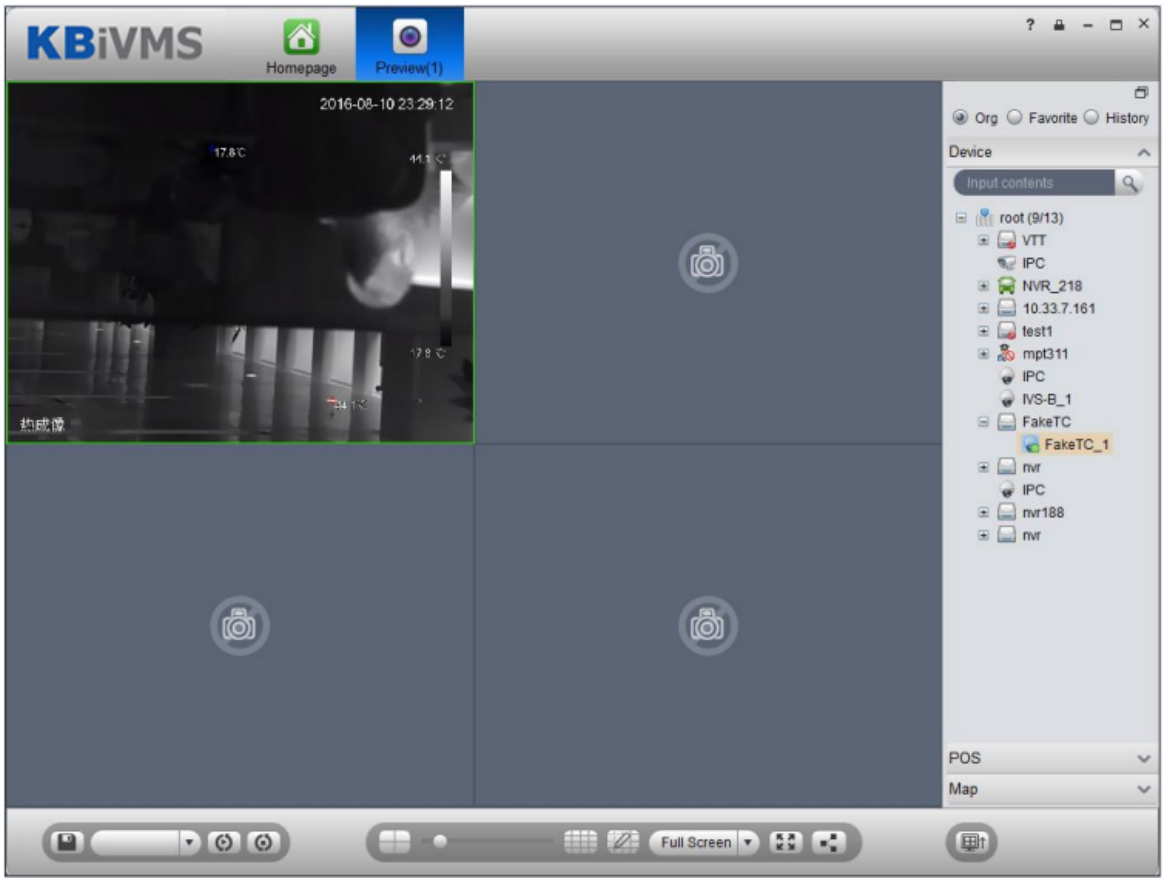


Figure 8-21

8.4.3 **Config Thermal Imaging Alarm on Manager**

Step 1. Select Business>Alarm.

Step 2. For contact, link level, alarm storm, TV wall alarm window and etc, please refer to Ch 8.2.1 -8.2.4.

Step 3. Click Alarm Scheme tab.

Step 4. Click Add. See Figure 8-22.

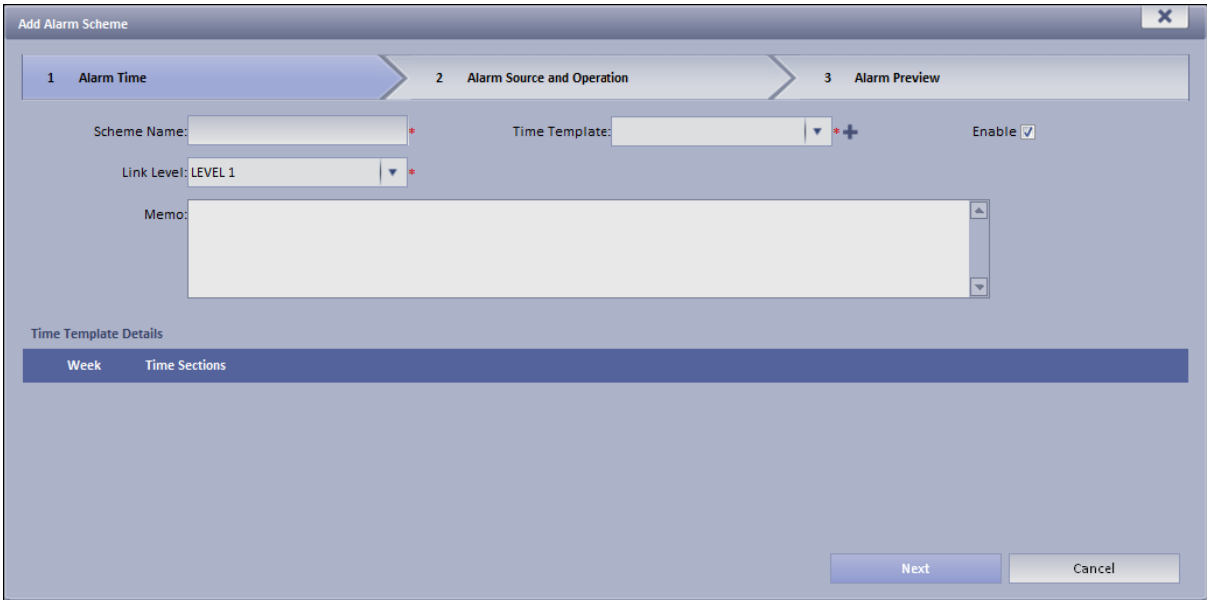


Figure 8-22

Step 5. Enter scheme name, select time template, link level and check Enable.

Step 6. Click Next. System shows alarm source and action setup interface.

Step 7. Click New.

Step 8. In alarm source box, select alarm source, and select fire point alarm, hotspot abnormal alarm and cold spot abnormal alarm. See Figure 8-23.

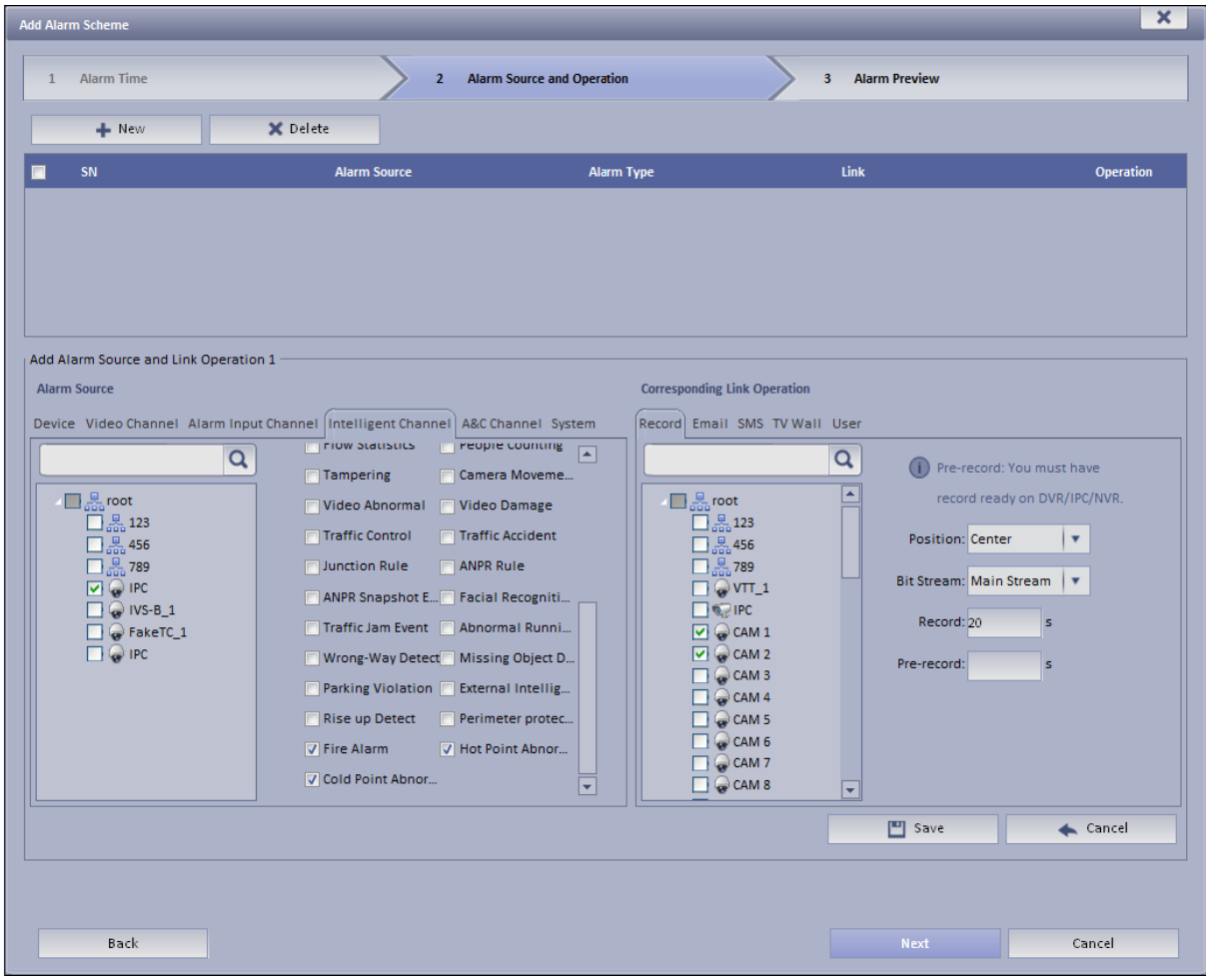


Figure 8-23

Step 9. In corresponding link action area, select link action.

Step 10. Click Save.

Step 11. Click Next.

Step 12. Click Complete.

When alarm occurs, the system links according to set link info in alarm scheme, and shows detailed thermal imaging alarm info in Statistics>Device Statistics> Device Alarm Statistics.

9 TV Wall

KBiVMS Platform supports video wall, and you must add decoder or matrix device on Manager and then configure TV wall before you can configure TV wall task and output to video wall on Client.

9.1 Add Decoder or Matrix Device

Step 1. Login KBiVMS Manager.

Step 2. Select General>Device>Decoder.

Step 3. Click Add. System pops up Add Decoder box, see Figure 9-1.

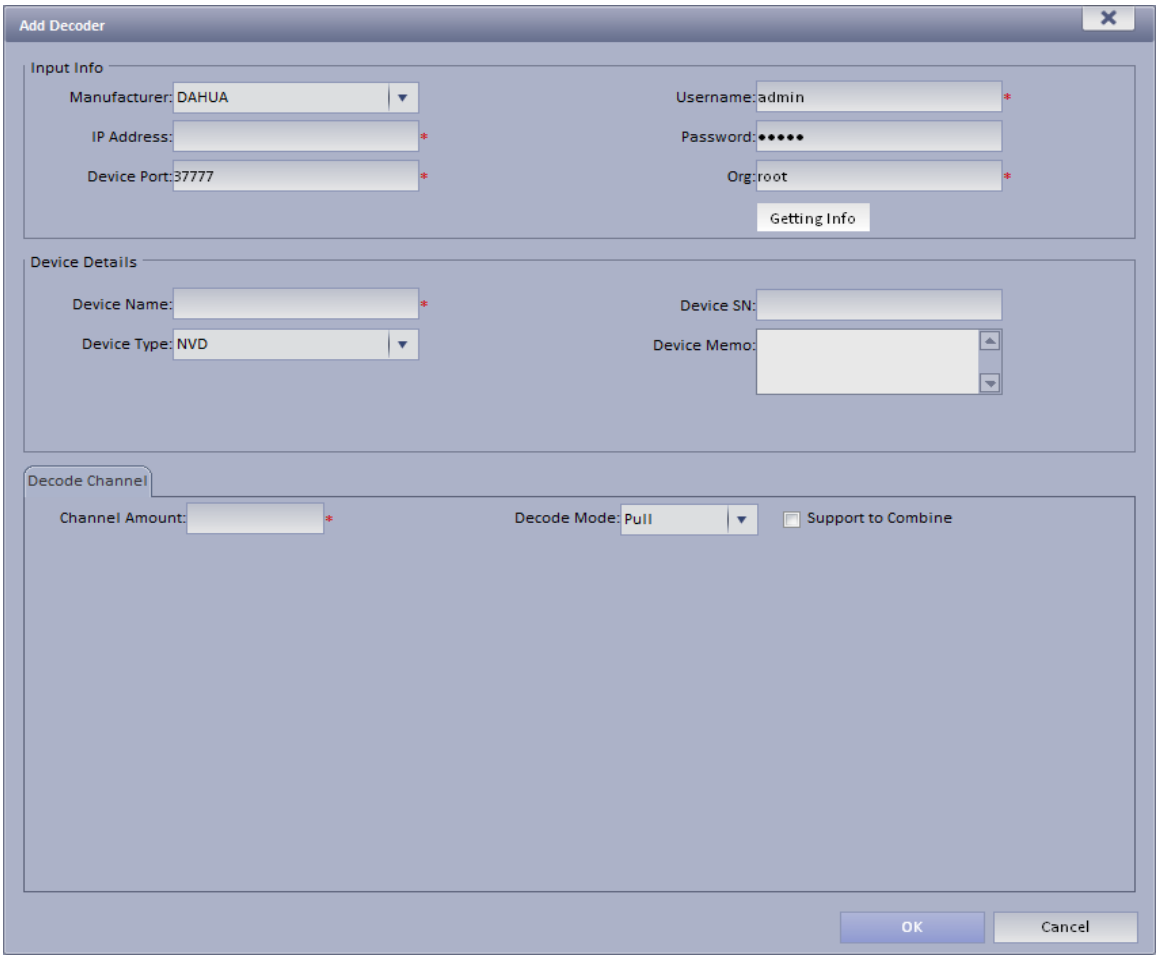


Figure 9-1

Parameter	Note
Device Type	Include NVD, SVDS, UDS.

Decode Mode	Device decoding mode, include pull stream, direct and push stream. ● Pull：decoder gets stream via KBiVMS series server. ● Direct：decoder gets stream directly from device. ● Push：KBiVMS series platform push stream to decoder. It is pull by default. Warning” If you want to output Hikvision device to wall, then you shall add decoder as NVD or add matrix as M60, select pull for decoding mode.
Combine	If decoding supports to combine, check Support to Combine.

9.2 Config TV Wall on KBiVMS Manager

Step 1. Select Business>TV Wall. System shows TV wall config interface.

Step 2. Click 

. System pops up Add TV wall interface, see Figure 9-2.

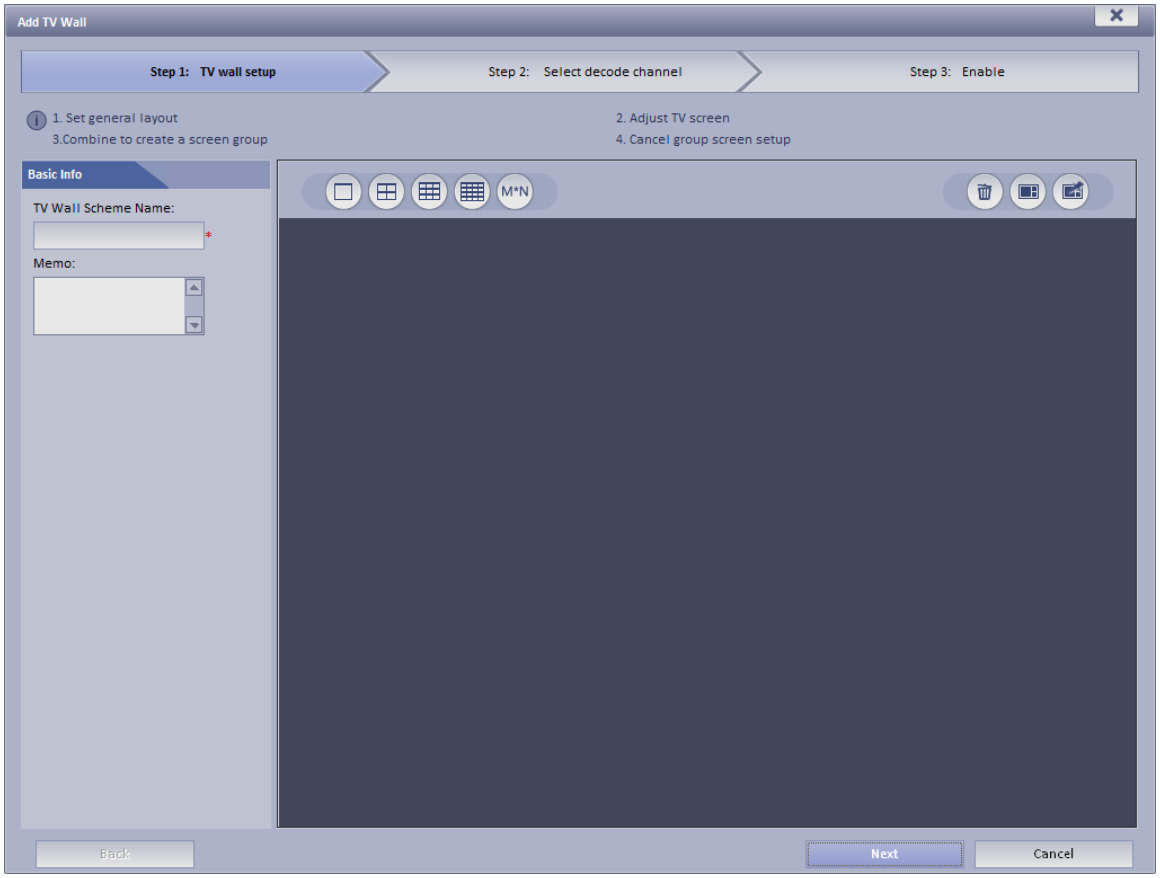


Figure 9-2

Step 3. Enter TV wall scheme name, and click  , select layout to be 1*1, 2*2, 3*3, or 4*4. See Figure 9-3.

You also can click 

to customize TV wall layout.

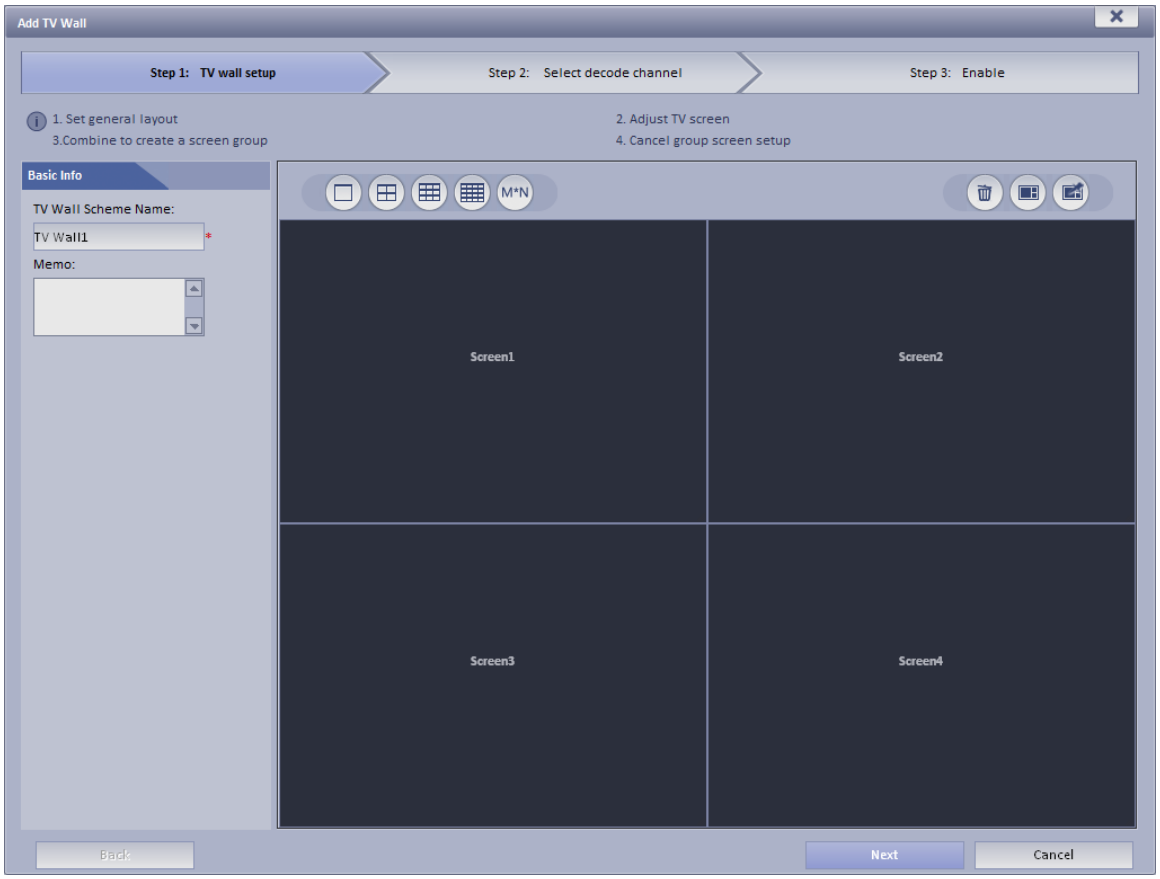


Figure 9-3

Note:

- Press Ctrl and now you can select more than one screen. Click  on the right to combine selected screens. You can cancel combination by clicking on  . Before you combine screens, you must add video wall equipment.
- Double click the screen or right-click and select Properties. In the pop-up box, you can set exact position, size and name of screen.
- Select a screen, and right click to delete or rename the screen.

Step 4. Click Next. System displays Select decode channel interface.

Step 5. In Device Tree, select decoder and drag it to corresponding TV wall. See Figure 9-4.

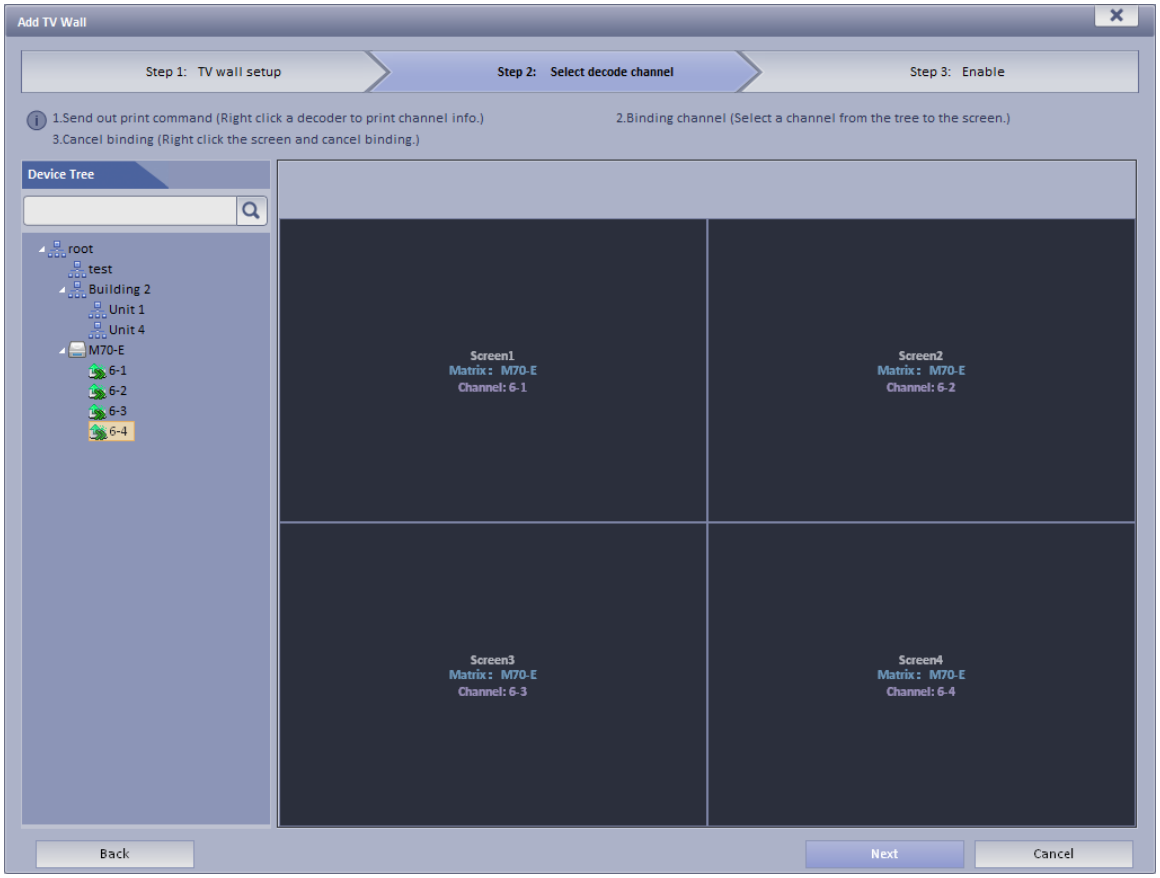


Figure 9-4

Note: Right-click can cancel current binding and rename screen.

Step 6. Click Next. System displays Enable interface.

Step 7. Check Apply Now.

Note: If you do not check Apply Now, then you cannot select this TV wall on Client.

Step 8. Click Finish.

9.3 Config TV Wall Task on KBiVMS Client

Via selecting TV wall schemes and bind video with TV wall to output video to wall.

Step 1. Click 

in Basic area.

System displays TV Wall interface.

Step 2. Click  at the upper-left corner, select TV wall scheme.

Step 3. Drag channel on the right to corresponding screen of TV wall to bind.

See Figure 9-5.

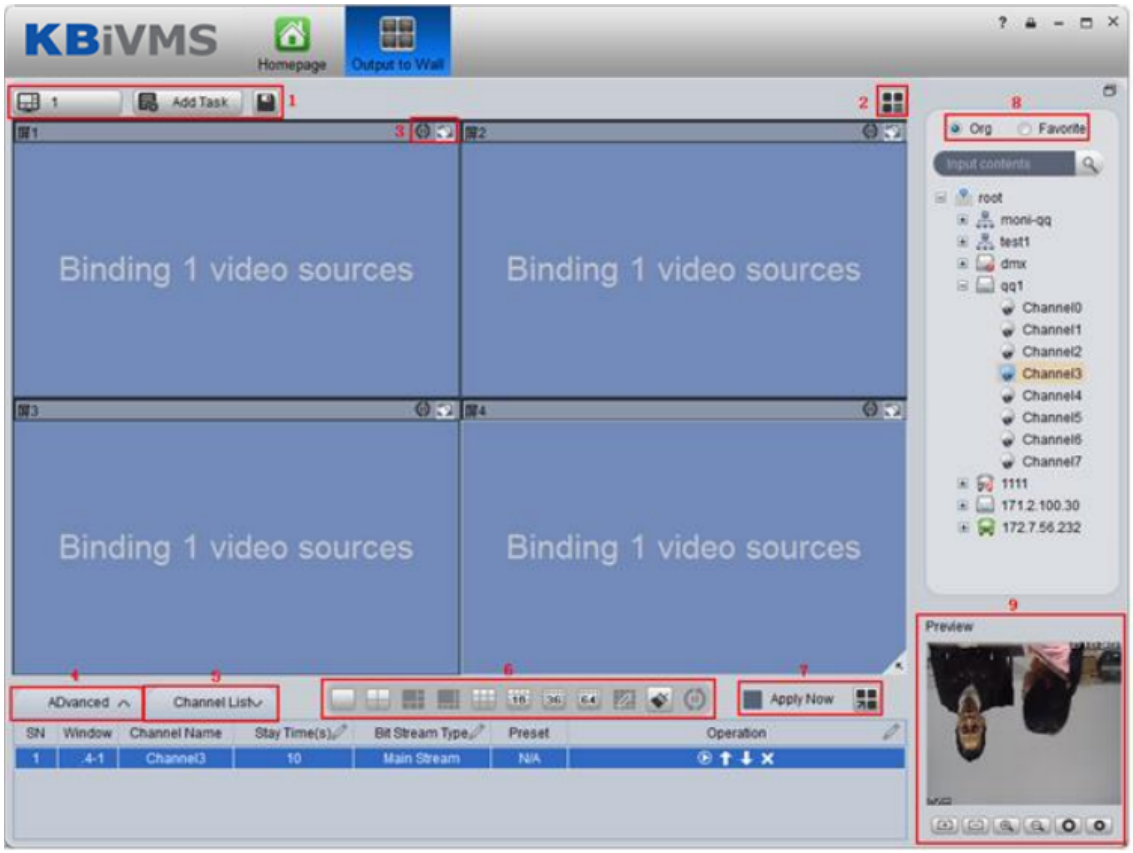
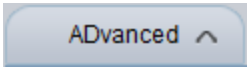
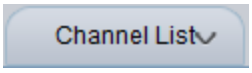


Figure 9-5

No.	Interface	Note
1	TV Wall Scheme	● : click to search all TV wall schemes added on Manager-end. ● : click to search all added TV wall tasks. ● : Save task.
2	TV Wall Plan	● : add schedule plan. ● : add tour plan.
3	Tour, clear	● : enable/disable the window tour. ● : clear.

4	Advanced	Click 

。
● Multiple window：open  ，you can select more than one window or directly select all windows.
● Stream type：main stream, sub stream, three streams, local signal.
● Duration：time interval of window video touring.
●  ：pane
●  ：on/off screen |
| 5 | Operation | Click 

.
Screen, window, channel binding info
● Click  , you can view if it is the channel you want at the lower-right “preview”.
● Click  , to adjust order.
● Click  ，to delete added window signal source. |
| 6 | Output to wall, Tour | ●  ：instant output to wall, when complete this task, system auto output to wall.
●  ：click to output to wall.
●  ：enable/disable tour plan. |

7	Split	●  : screen split, may split 1~64 screens. ●  : customize screen split. ●  : clear. ●  : screen ON/OFF. ●  :
8	Org, Favorite	Select channel from organization or favorite tab. Channel under “Org” tab, right click “Add To Favorite”, to add it into “Favorite” tab. Note: Before you can add it to favorites successfully, you must click  under “Favorite” tab.
9	Video Preview Window	Double click video channel, auto add to window. In channel binding info bat, click  , to preview video.

Step 4. Click  .

Step 5. Input Task Name, click OK.

Step 6. Click  to complete.

You also can customize TV wall plan to output video to wall. Please refer to Ch 4.3.2.

10 Audio Intercom

Via audio talk, you can talk to front-end device and broadcast.

10.1 Audio Talk

Audio talk allows Client to talk to a single front-end device.

Step 1. Click 

in Basic area. System displays broadcast interface, see Figure 10-1.

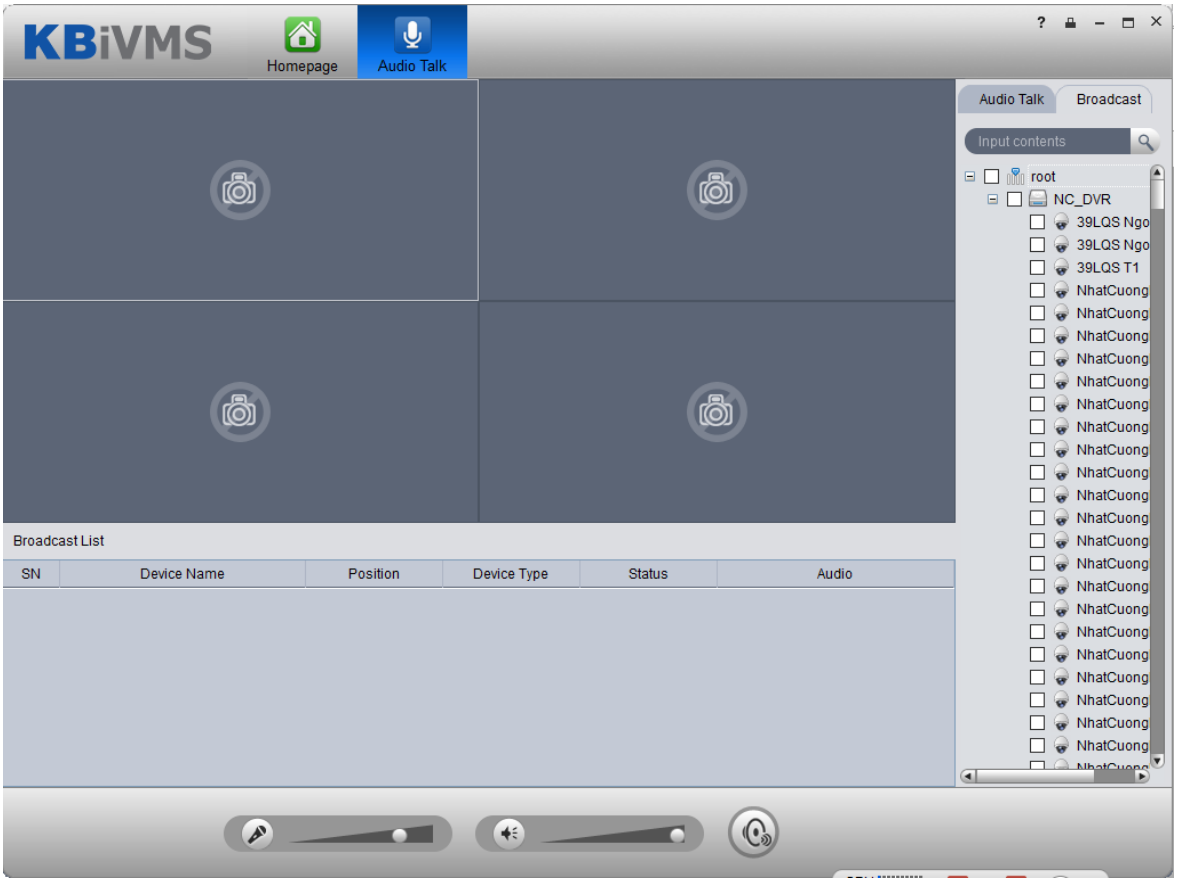


Figure 10-1

Step 2. Click Audio Talk tab in the upper-right. System shows Audio Talk interface.

Step 3. Select a device to talk.

Note:

Audio talk is valid to device only, not to channel.

Step 4. Click  . System shows interface as in Figure 10-2.

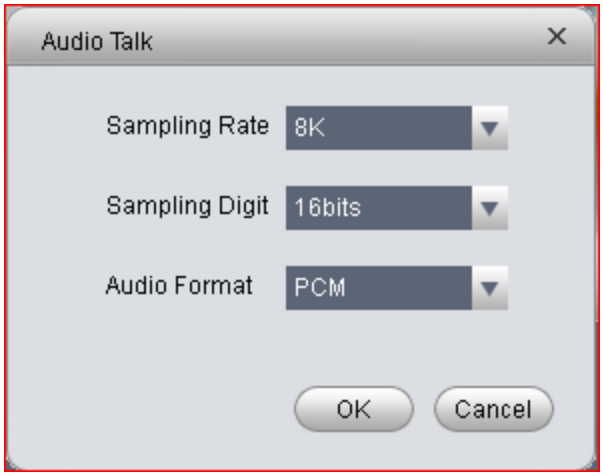


Figure 10-2

Step 5. Set Sampling Rate, Sampling Digit, and Audio Format, click OK. If config match device, system will inform you that audio talk is successfully enabled, see Figure 10-3.

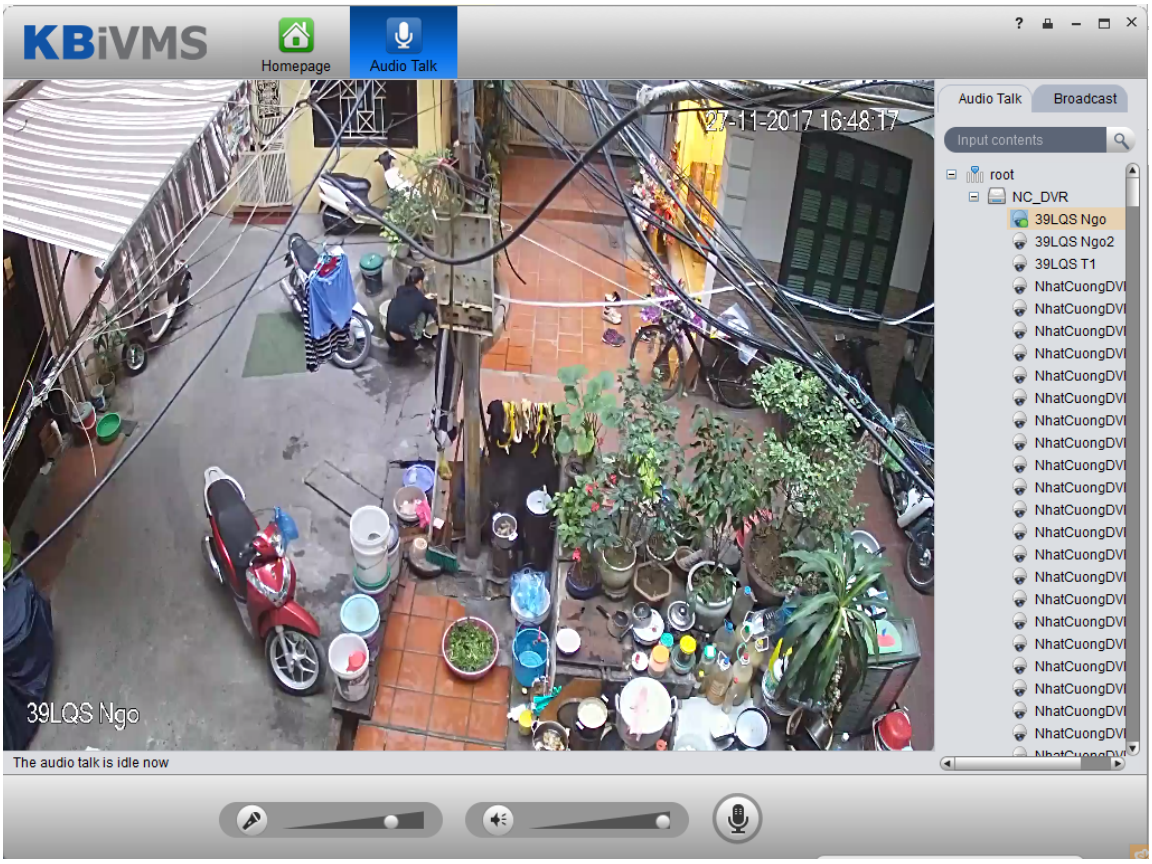


Figure 10-3

If config do not match device, system will inform you that failed to enable audio talk, and show recommended parameter. You can config based on the recommended parameter.

During audio talk, click  to end audio talk.

10.2 **Broadcast**

Broadcast allows the Client to broadcast with multiple front-end devices.

Step 1. Click Broadcast tab in Audio Talk interface. System shows Broadcast interface.

Step 2. Select multiple devices on the right. The selected devices will be displayed in broadcast list.

Step 3. Click  . System displays Broadcast setup interface, see Figure 10-4.

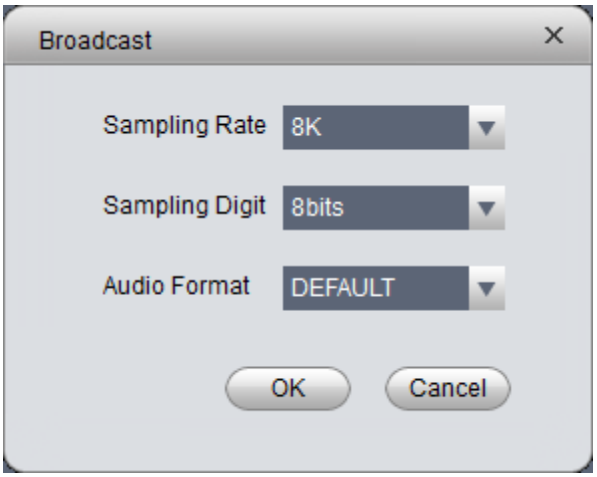


Figure 10-4

Step 4. Set Sampling Rate, Sampling Digit and Audio Format.

Step 5. Click OK.

If config match device, then you enable broadcast successfully and device in list will show enable status, see Figure 10-5.

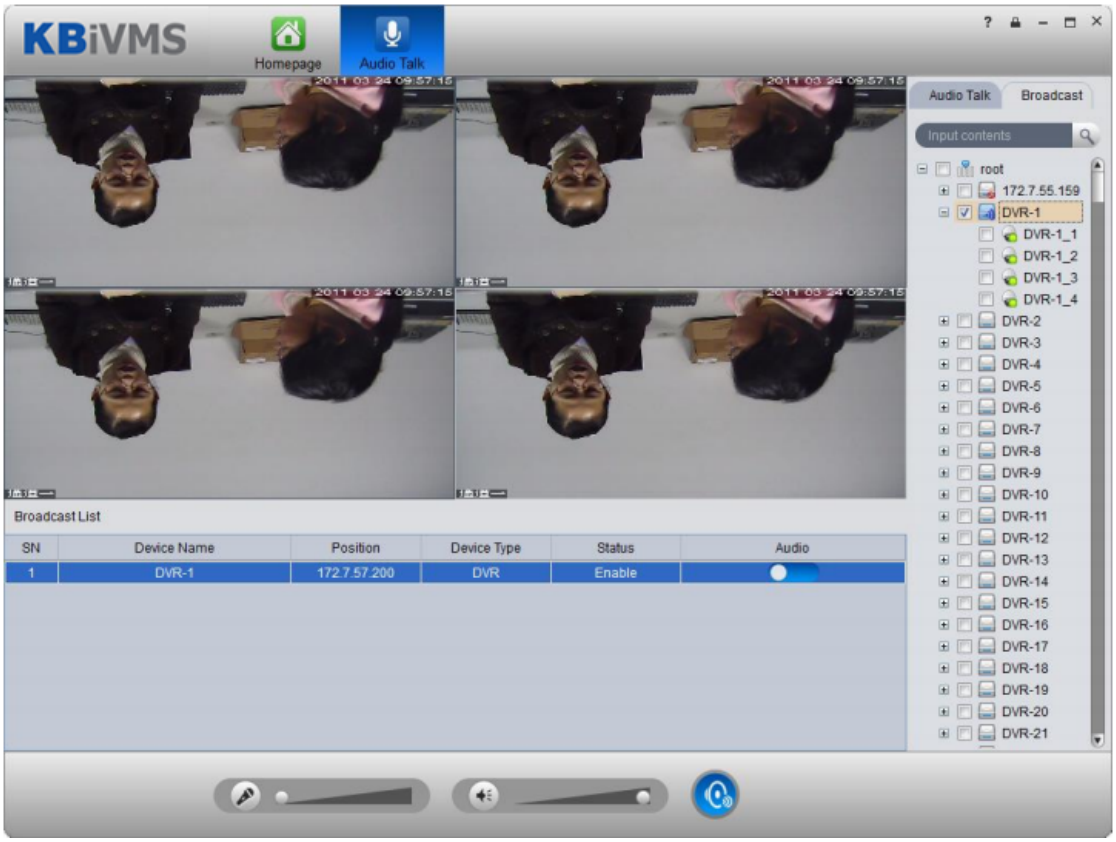


Figure 10-5

During broadcast stats, click  to end broadcast.

11 Video Intercom

Video intercom supports call, remotely unlock, send message, alarm search and etc.

New SIP telephone function allows VDP-G (VTO) to call SIP telephone. When the call is picked up, you can enter VDP-G password to unlock. SIP telephone can also form a group with VDP-Hs (VTH). When VDP-G calls, devices in the same group will respond at the same time, and if one of these device picks up, ring on other devices will stop.

SIP telephone supports to call platform client.

11.1 Config Device

11.1.1 VDP-G Setup

Step 1. Login VDP-G web.

Step 2. Select Network>SIP Server.

Step 3. Configure platform address, port is 5080, see Figure 11-1.

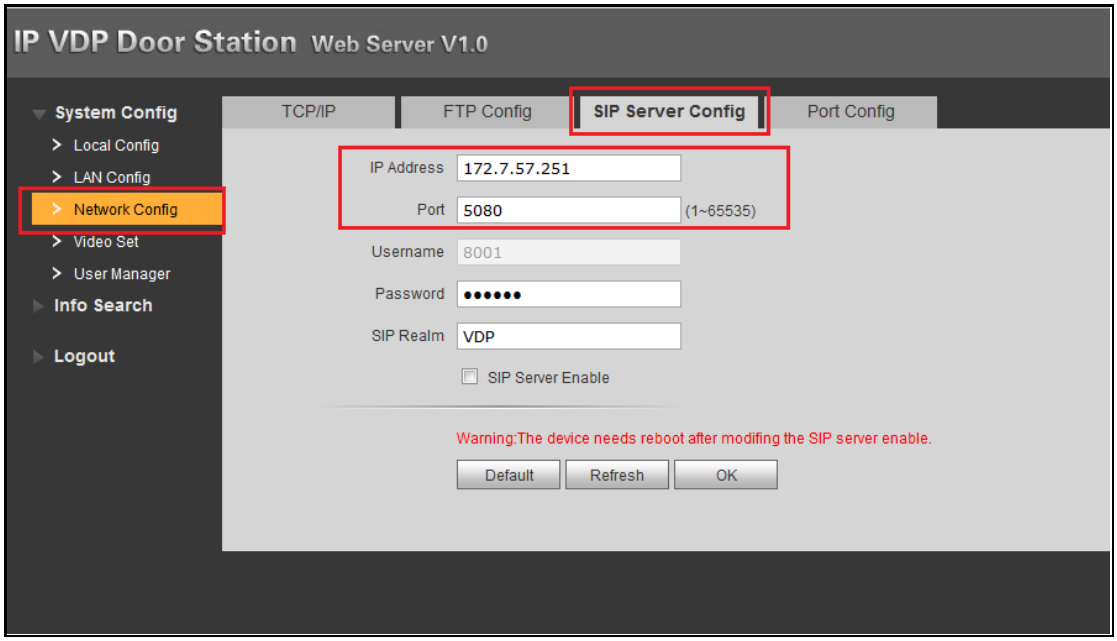


Figure 11-1

Step 4. Select Network Config.

Step 5. Set building/unit no. and call number, see Figure 11-2.

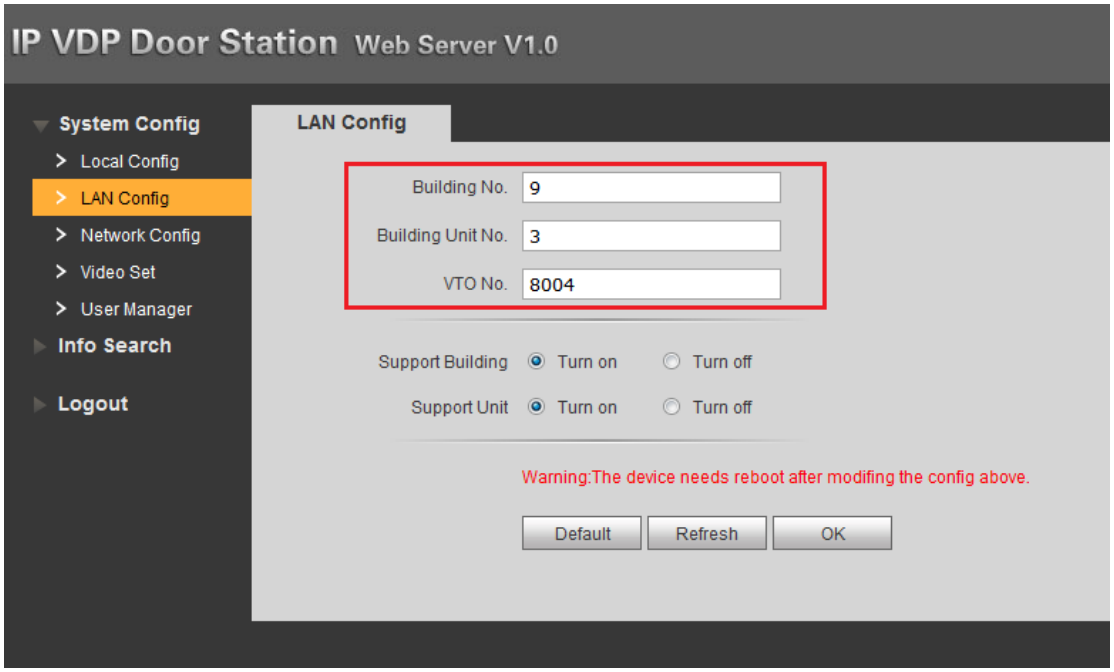


Figure 11-2

Later in the use of VDP-G, if you modify content in red box above, you shall find corresponding VDP-G on platform manager Device interface. Click  , in pop-up window, click Get Info to get latest VDP-G info, and then you can normally use VDP-G function.

Step 6. Select Local Config>A&C Manager.

Step 7. Set unlock password and duress password, check to enable button.

Step 8. Set auto snapshot, select Turn On, and when you swipe card at VDP-G, client will receive the snapshot picture, see Figure 11-3.

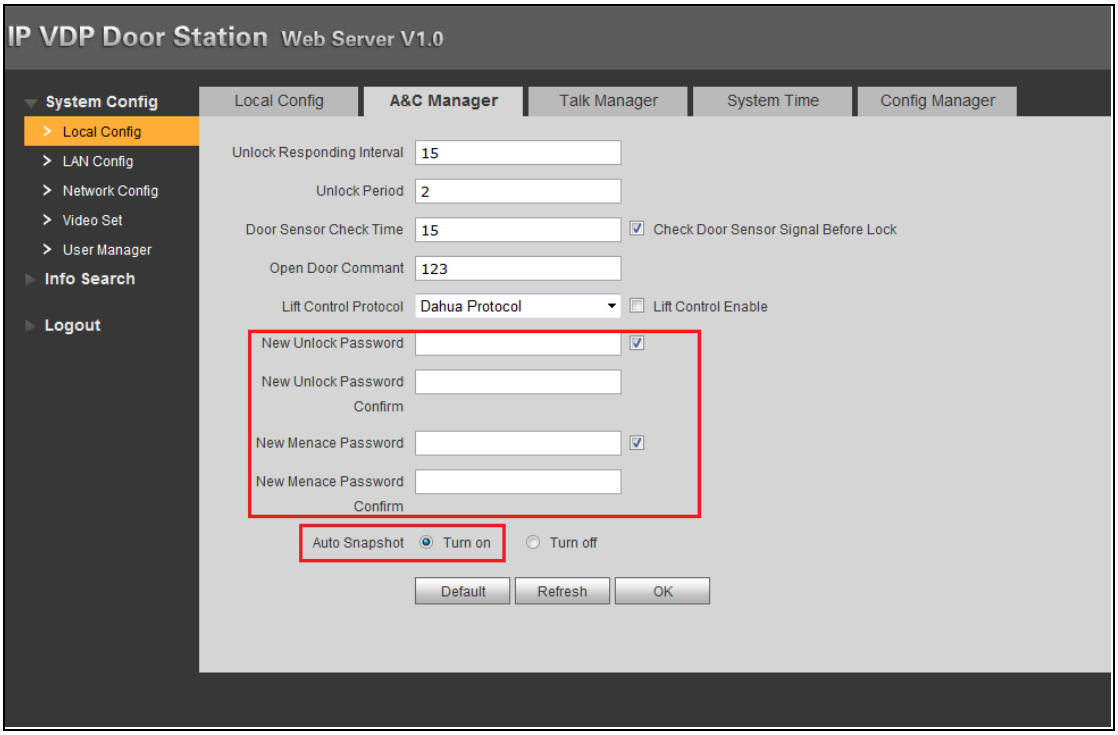


Figure 11-3

If you complete this operation on KBiVMS, you can see device platform connection status on VDP-H device's homepage as online/offline. (Just enter VDP-G IP, config VDP-G name)

11.1.2 **VDP-H Setup**

Step 1. Login VDP-H and go to Settings>Project Settings.

Step 2. In Local Config, config VDP-H room no. and network address, see Figure 11-4. Room no. here is VDP-H no. of added VDP-H.

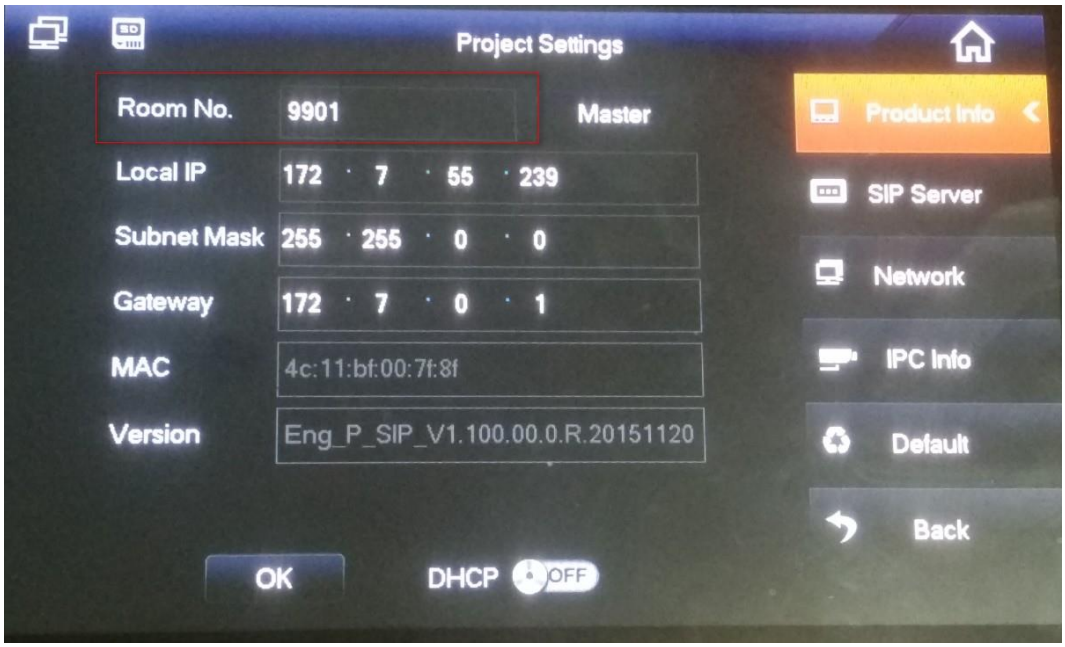


Figure 11-4

Step 3. In SIP server config platform address and port (50800, and enable. You cannot modify other info, see Figure 11-5.

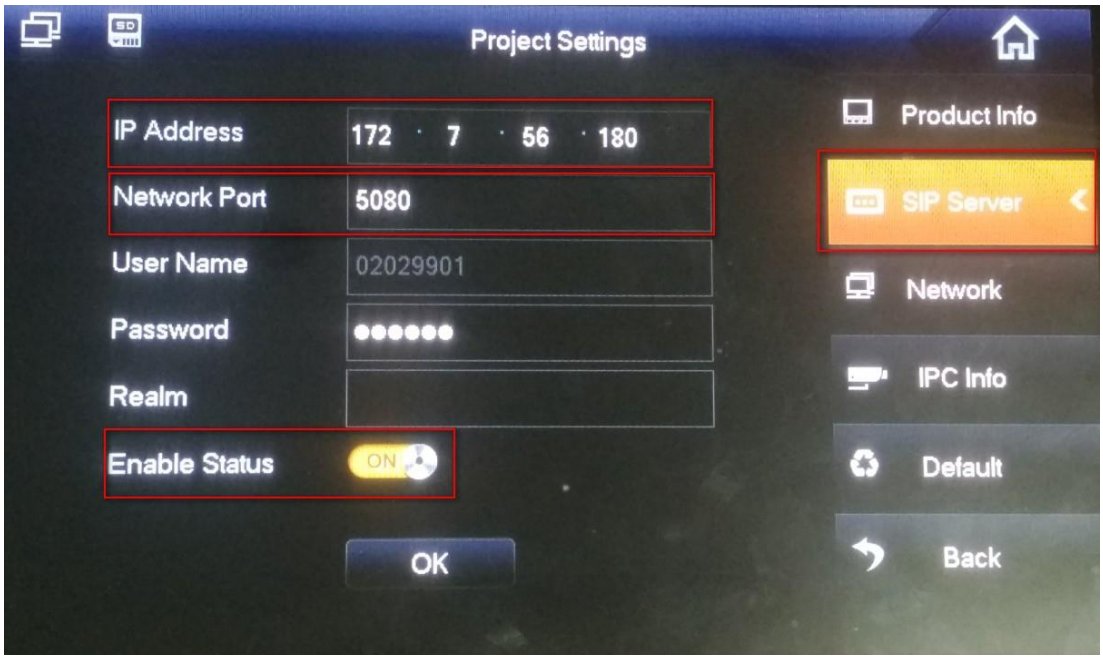


Figure 11-5

Step 4. In Network, configure corresponding VDP-G address, and enable, see Figure 11-6.

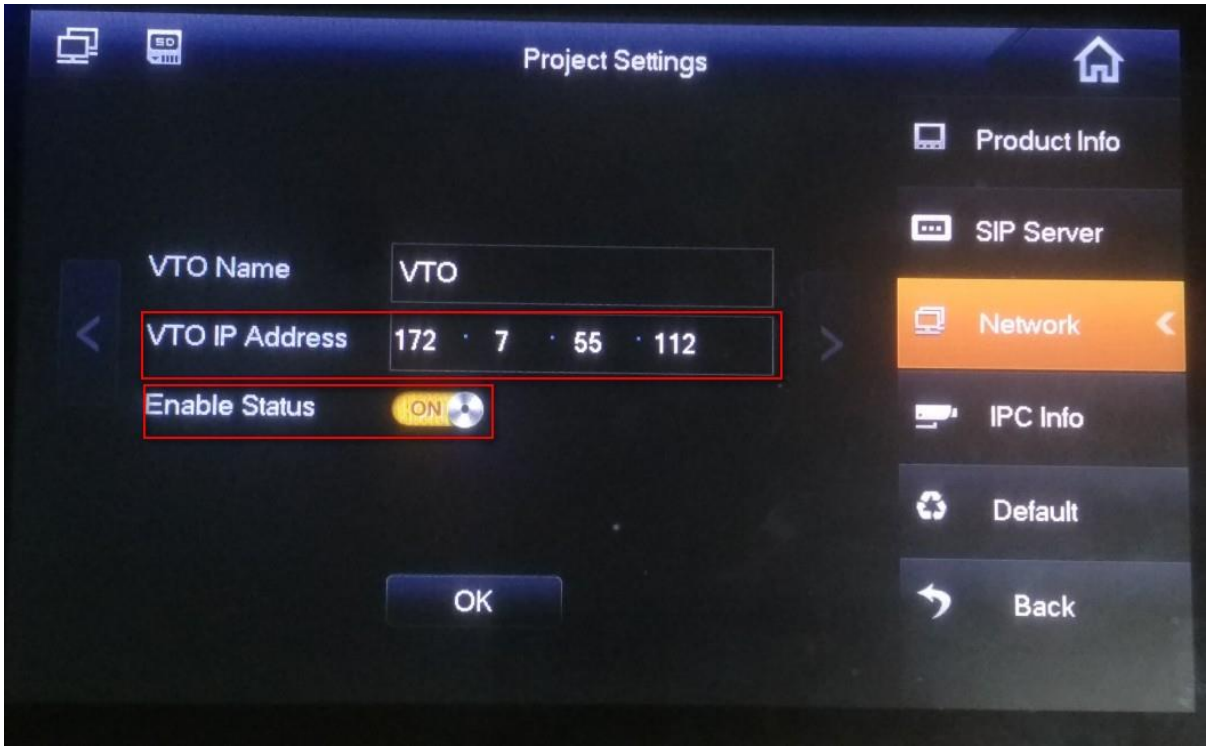


Figure 11-6

Step 5. Set status check. When you complete basic config info, in VTO homepage, view device config stauts. If there is no “X” shown, the config is normal. See Figure 11-7.

Figure 11-7

Note:

The first picture represents VDP-H connection status, and the second picture represents VDP-H registration status on VDP-G. “X” means that registration failed. (After you configure VDP-H, reboot the device, and it will be linked to platform according to VDP-G.)

a) VDP-H zone setup

On VDP-H, click Security>Zone Status, configure zone info of each channel (zone config login

password is 123456.), and you can switch NO/NC status to trigger alarm; in alarm record, you can view alarm record of each zone.

b) VDP-H DND mode

On VDP-H, click User Settings>DND configure DND time, see Figure 11-8.

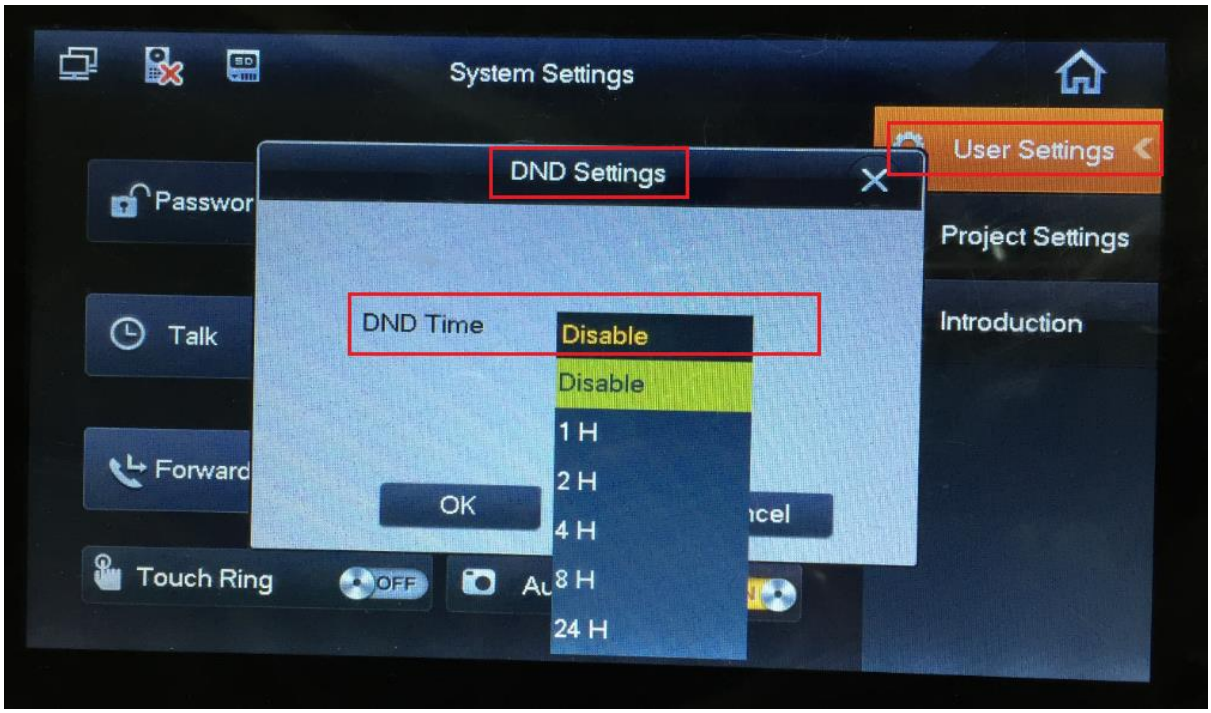


Figure 11-8

Step 6. In Figure 11-8, click Setting.

Step 7. Select User Setting>Talk, see Figure 11-9.

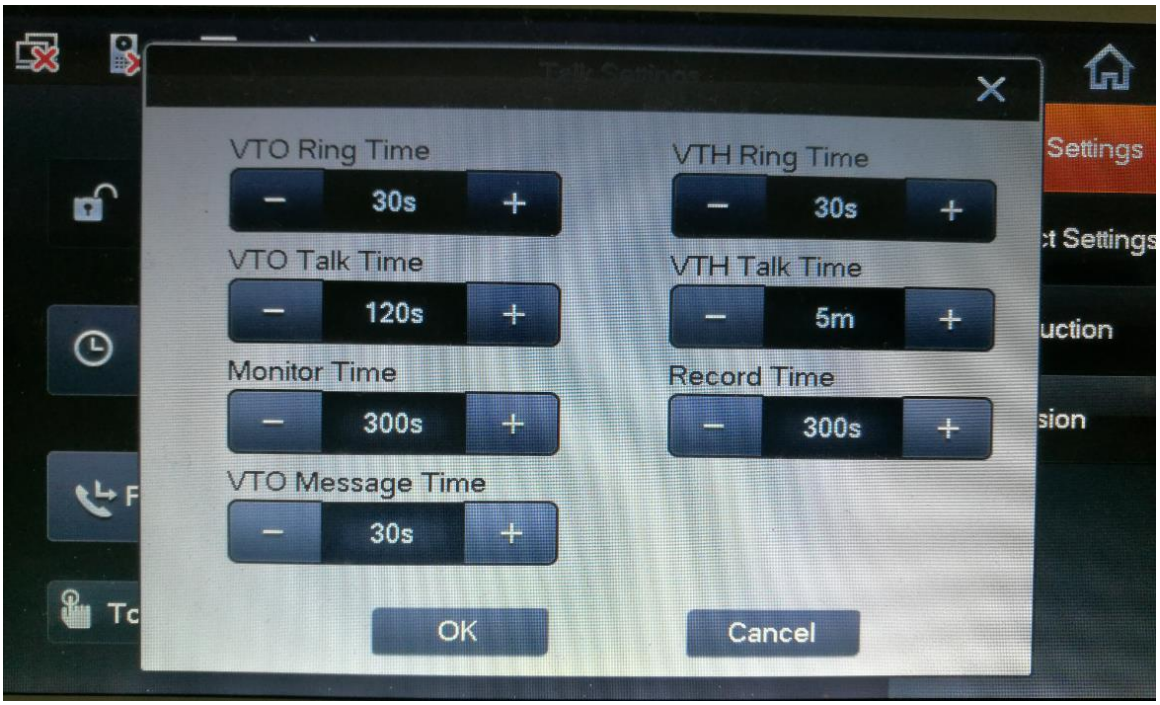


Figure 11-9

Set VDP-G Ring Time, VDP-H Ring Time and VDP-G Message Time to 30s, click OK.

11.1.3 **SIP Telephone Setup**

Step 1. Login SIP Account.

Step 2. Select SIP Account, see Figure 11-10.

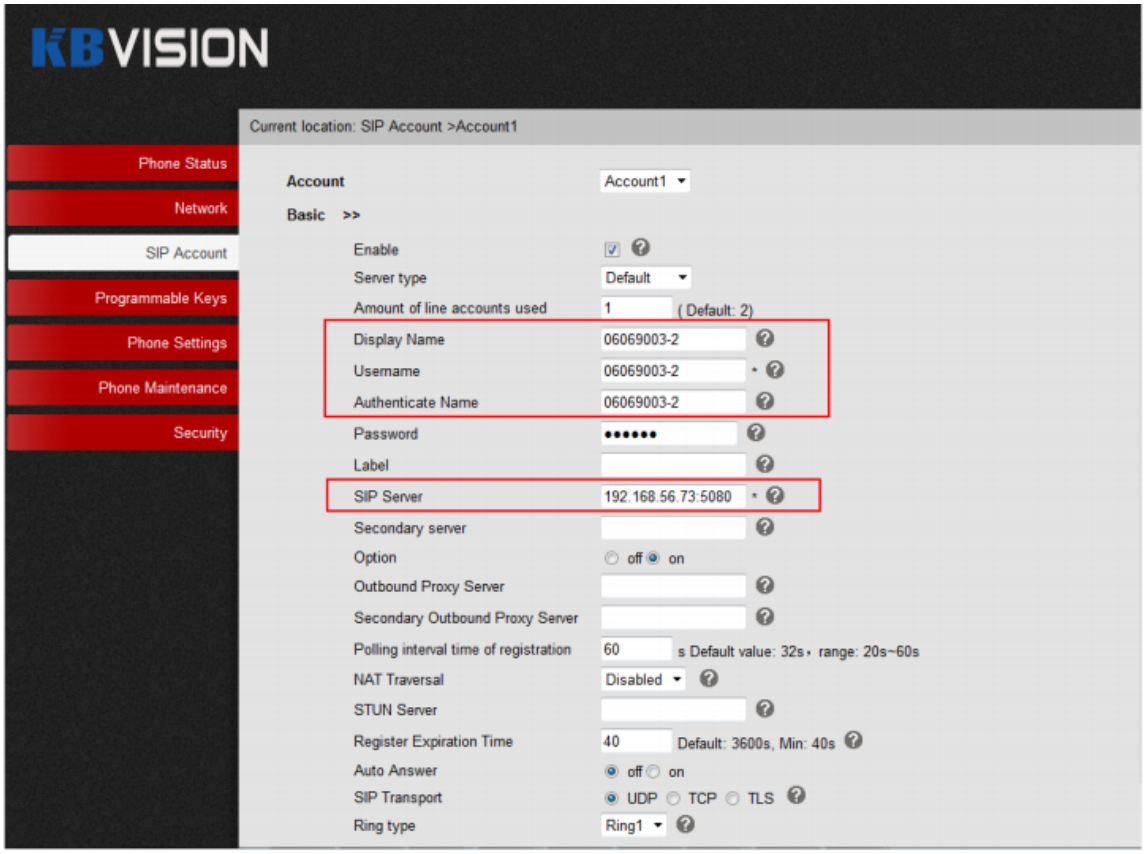


Figure 11-10

Step 3. Enter Display Name, Username, Authenticate Name, matching VDP-H.

Note:

If SIP telephone forms a group with VDP-Hs, number in front of "-" shall match VDP-H, number

following "-" shall be different to differentiate devices.

Step 4. In SIP Server field, enter platform IP.

Step 5. Select Phone Setting>Advanced, see Figure 11-11.

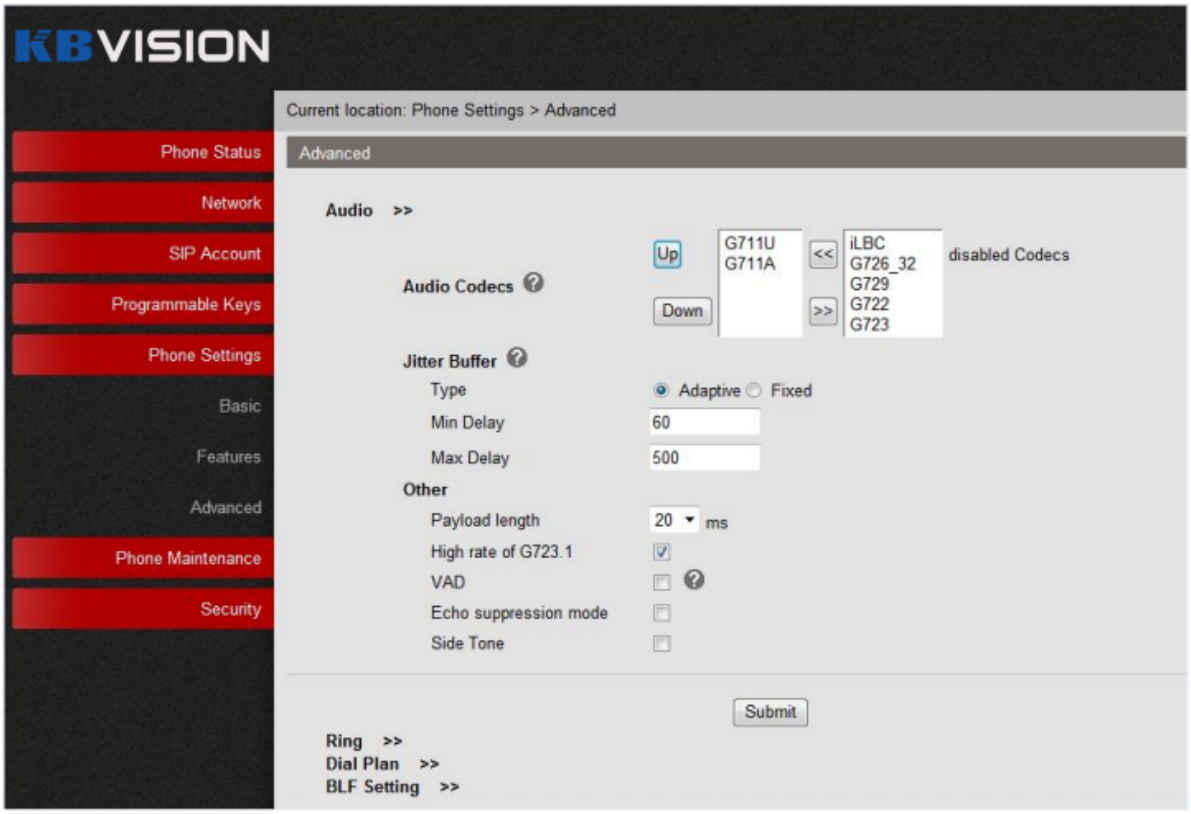


Figure 11-11

Step 6. Click Submit.

11.2 **Add Device on KBiVMS Manager**

Step 1. Login KBiVMS Manager.

Step 2. Select General>Device>Video Talk.

Step 3. Click Add. System pops up Add Video Talk Device box, see Figure 11-12.

Figure 11-12

Step 4. Enter IP address and device name, click Add.

See Figure 11-3.

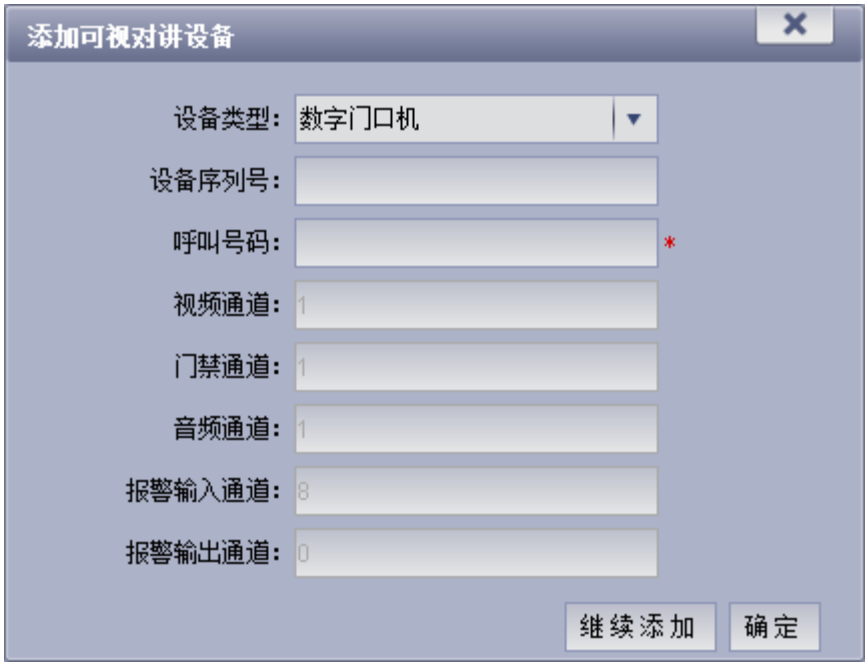


Figure 11-13

Step 5. Configure VDP-G info parameter, and set call and other parameters, click Add. You only need to add VDP-G since VDP-H and SIP Telephone will be auto linked to platform via VDP-G. Or you may select VTS, and platform auto gets call number from the device, click OK.

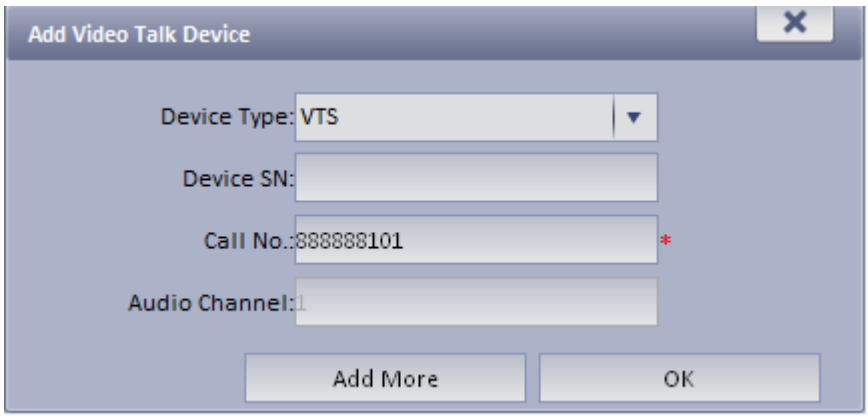


Figure 11-14

11.3 Video Intercom Function on KBiVMS Client

11.3.1 Video Talk

After you have added VDP-G and VDP-H, on KBiVMS Client, go to Video Talk, and see the device tree on the left in the interface. Building no., unit no. reported by each device will auto generate device organization tree.

Step 1. Login KBiVMS Client.

Step 2. Select  in Basic area. System shows Video Talk interface, see Figure 11-15.

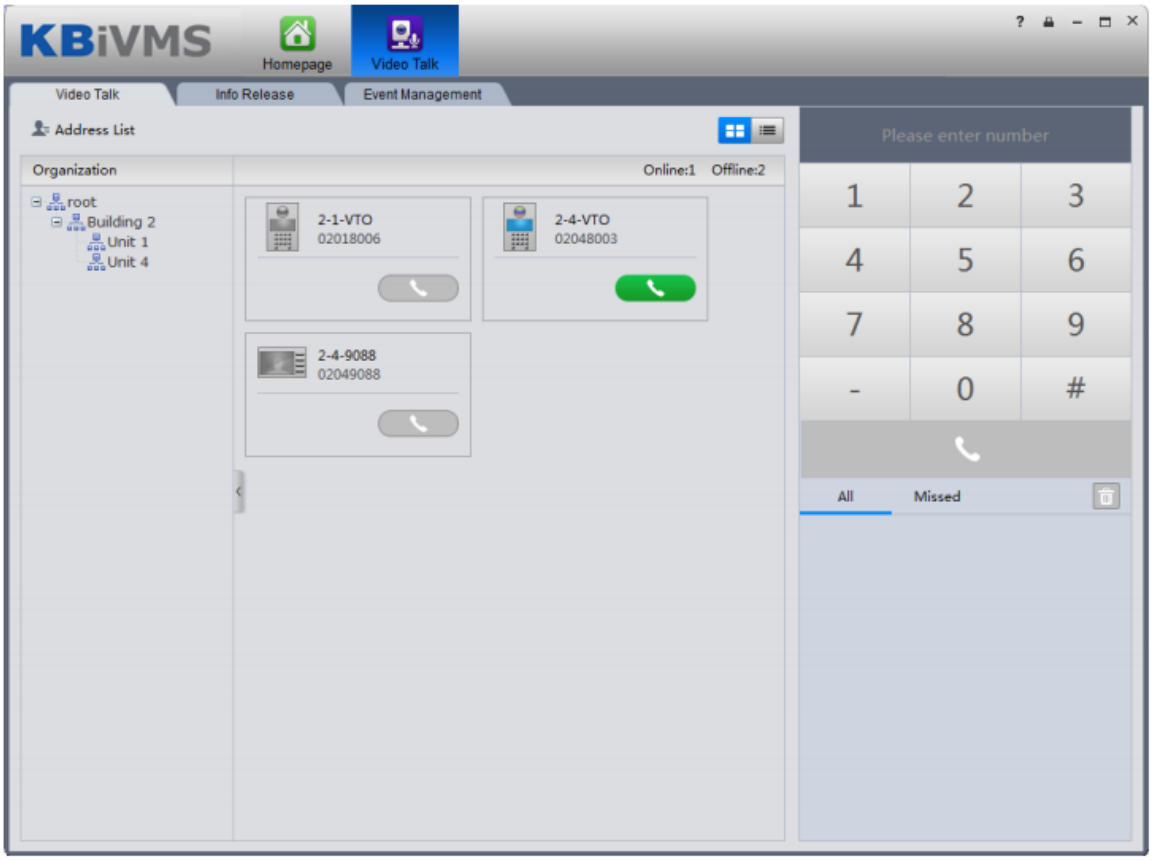


Figure 11-15

According to building no., unit no., and other VDP-Hs reported by the device, it will auto generate contacts.

- If a user wants to call a unit VDP-G via client.

  Click  on VDP-G.

  Call is one-way from clien to VDP-G only.

  System pops up a box, see Figure 11-16.

Figure 11-16

1). Click  .

2). System pops up confirmatio box, click OK.
You can unlock remotely.

3). Click  to stop call.

Call box will not be closed.

- If a user wants to call a specific VDP-H from client.

1). Click  on VDP-H.

Call is bidirectional between client and VDP-H.
System pops up a calling box, see Figure 11-17.

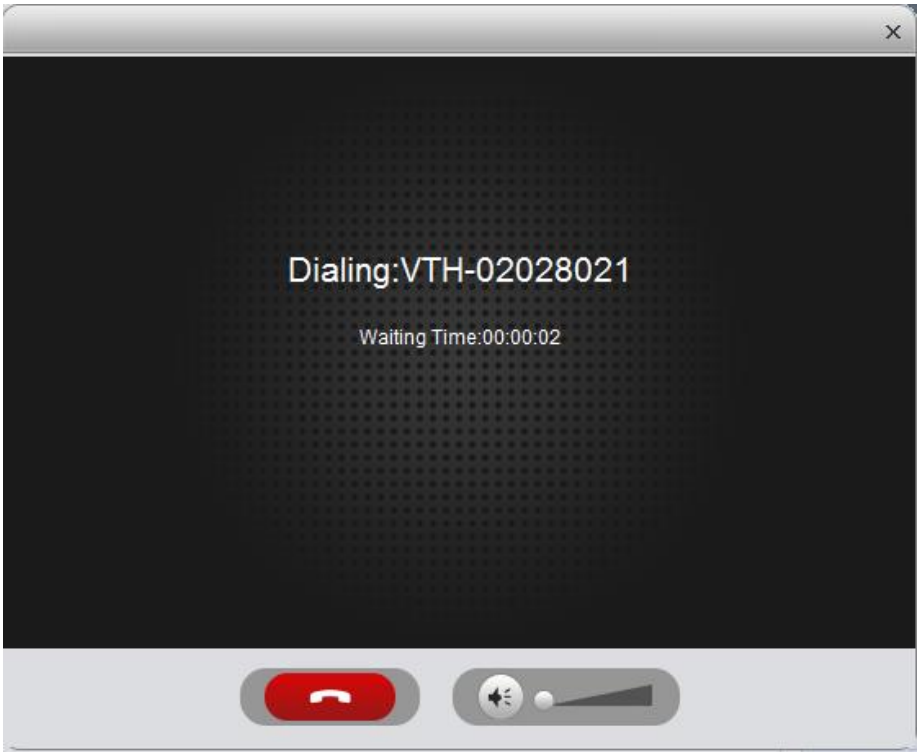


Figure 11-17

2). When VDP-H accepts call, the user can start a bidirectional talk. See Figure 11-18.

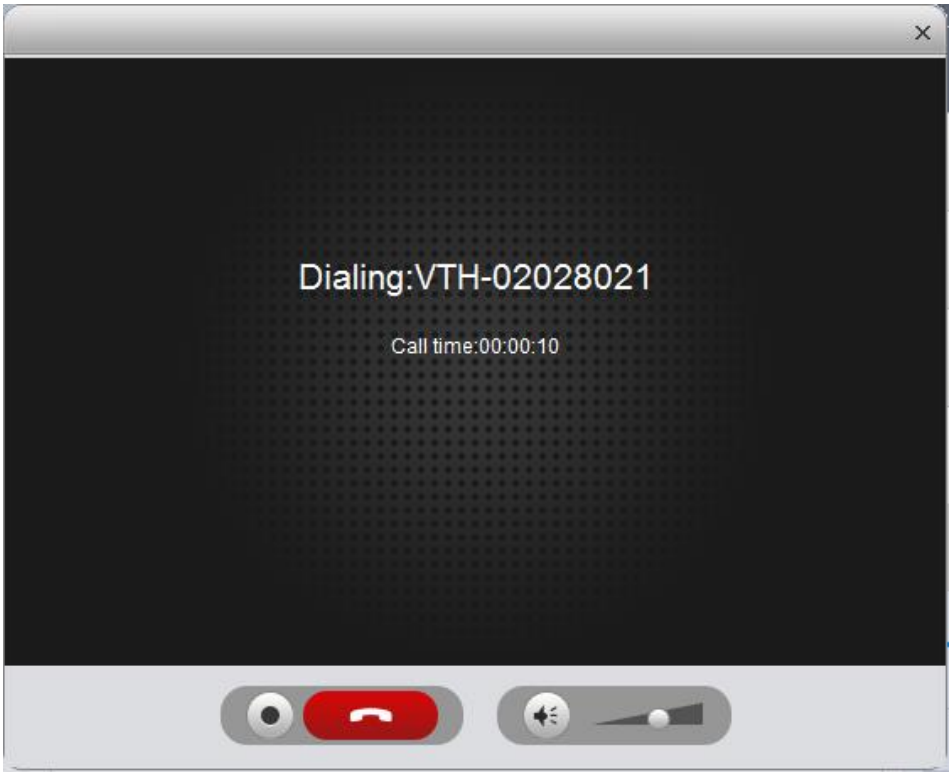


Figure 11-18

1) VDP-H does not accept call in 60s, then client will prompt user and ask if he/she wants to redial. The user may click  again to redial.

2) If the VDP-H being called is busy, client will prompt user to call again later.

- If Client calls SIP phone in certain room of certain unit.

1) Click  on SIP phone card.

See Figure 11-19.

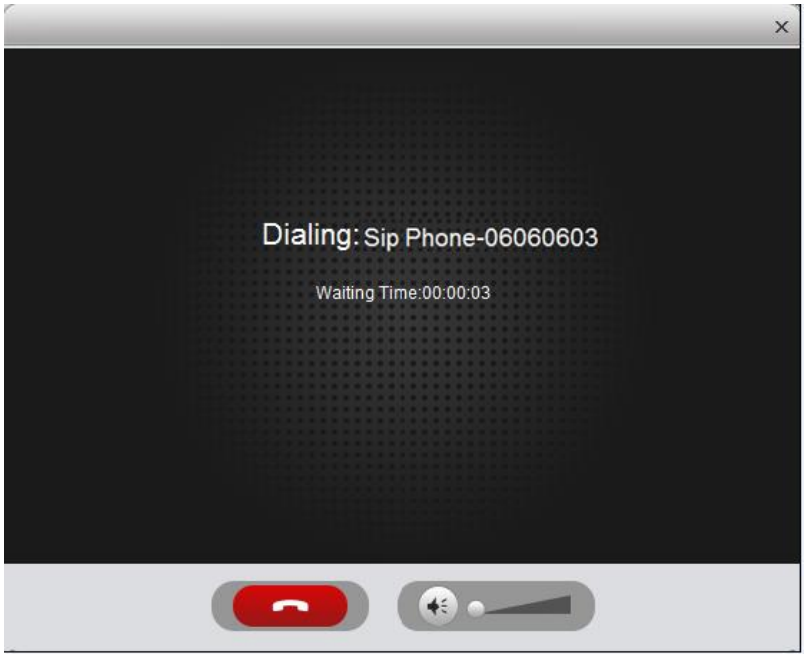


Figure 11-19

2) After SIP phone call is picked up, client can have a bidirectional talk with SIP phone, see Figure 11-20.

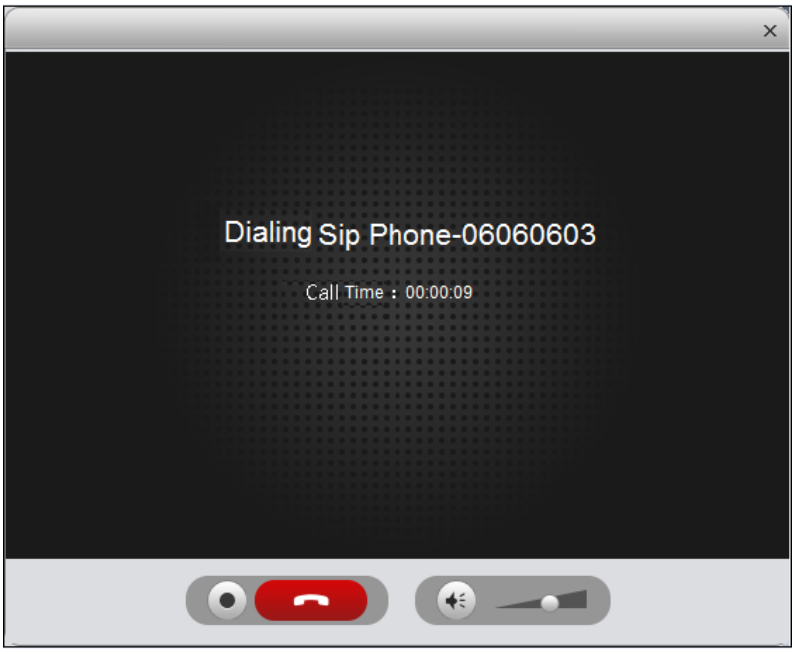


Figure 11-20

- SIP does not accept call in 50s, then client will prompt user and ask if he/she wants to redial. The user may click  again to redial.
- If SIP phone call is busy or hung up directly, client will prompt call busy and ask you to try later.

- If the VDP-G is calling the client.

Client pops up VDP-G calling box, see Figure 11-21.

Figure 11-21

You can click , to accept VDP-G call, and start a bidirectional

Also you can click to unlock.

- If the VDP-H is calling the Client.
  Client pops up VDP-H call box, see Figure 11-22.

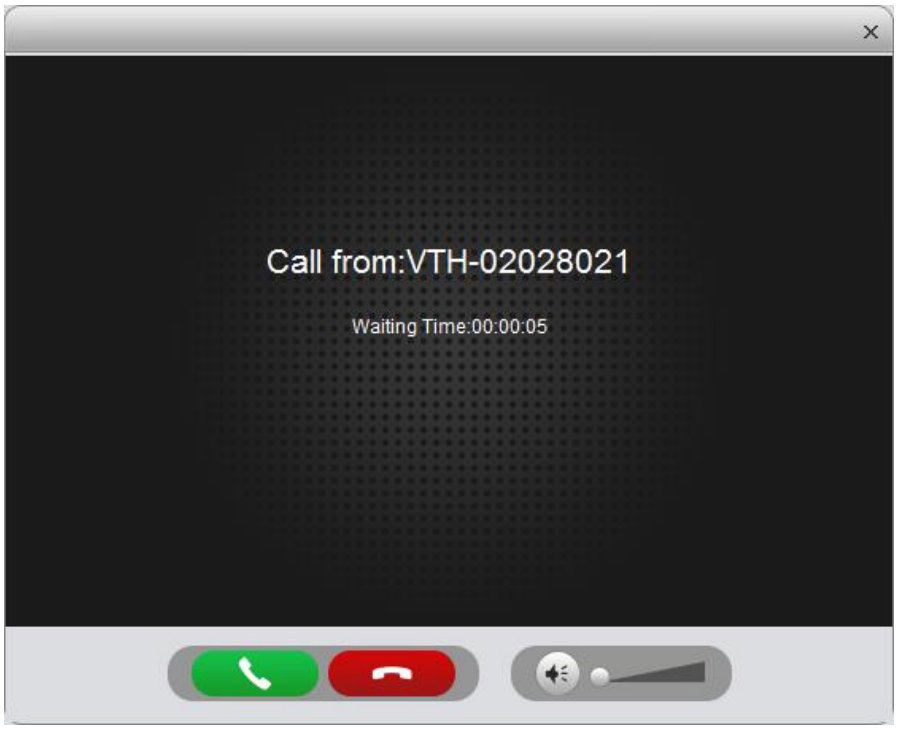


Figure 11-22

You can click to talk with VDP-H.

If there is missing call, you can click missing call shown in red Call Record at the lower-right corner in Talk interface, see Figure 11-23.

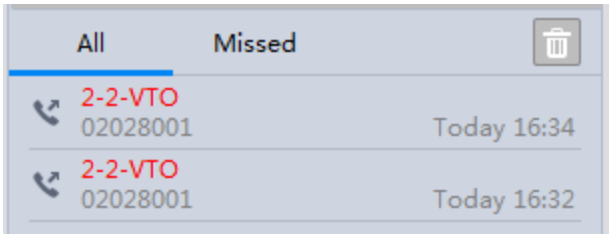
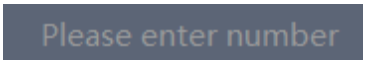


Figure 11-23

Click  , you can call back.

You also can view ALL of call records.

On the right, there are 

, here enter call number to fuzzy search.

In  on the right, you also can directly dial VDP-O to call VDP-H either one-way or bidirectionally.

11.3.2 Send Message

In Message Publish interface, you can add announcement or notice, which can be sent to each VDP-H and users can view them on VDP-H.

11.3.3 Event Search

In Event Search interface, you can search for alarm event and unlock type. You also can learn about time of alarm, device location when alarm occurs, plus alarm status.

12 ANPR Surveillance

12.1 Add ANPR Device

Step 1. Select Basic Config>Device>ANPR Device.

Step 2. Click Add.

See Figure 12-1.

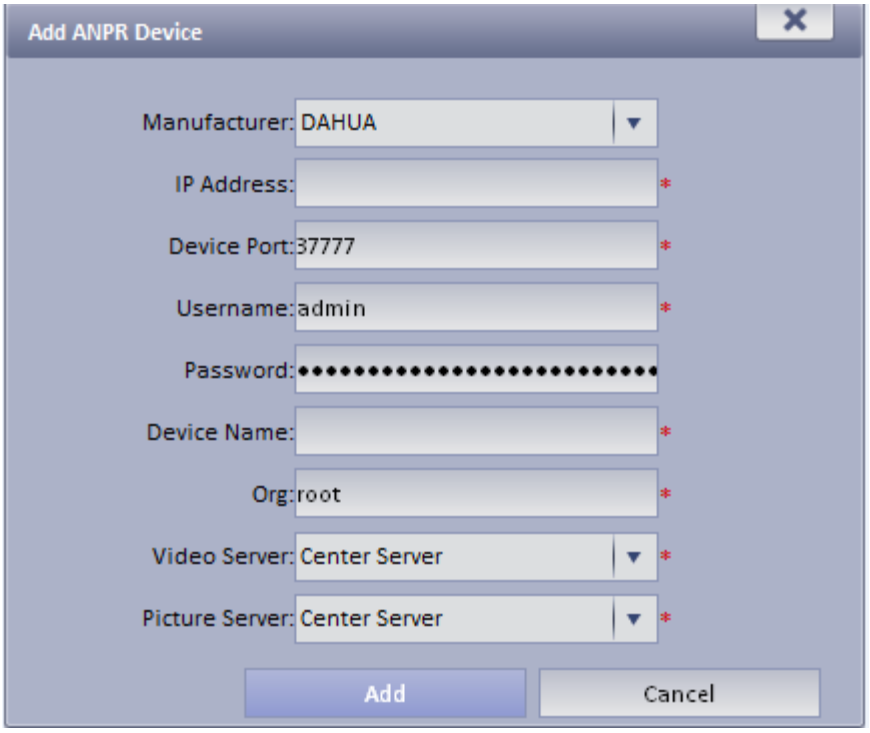


Figure 12-1

Step 3. Set IP address, device name, click Add.

Step 4. In device type dropdown list, select ANPR device.

Step 5. Click OK.

12.2 ANPR Surveillance

ANPR Monitoring is mainly used to show real-time vehicle passing record, and it shows device snapshot time, snapshot location plate info and etc.

Step 1. In Click  in extension function area.

Step 2. In device list, select ANPR device and drag it to video window, you can view snapshot time, plate no., owner and telephone number. See Figure 12-2.

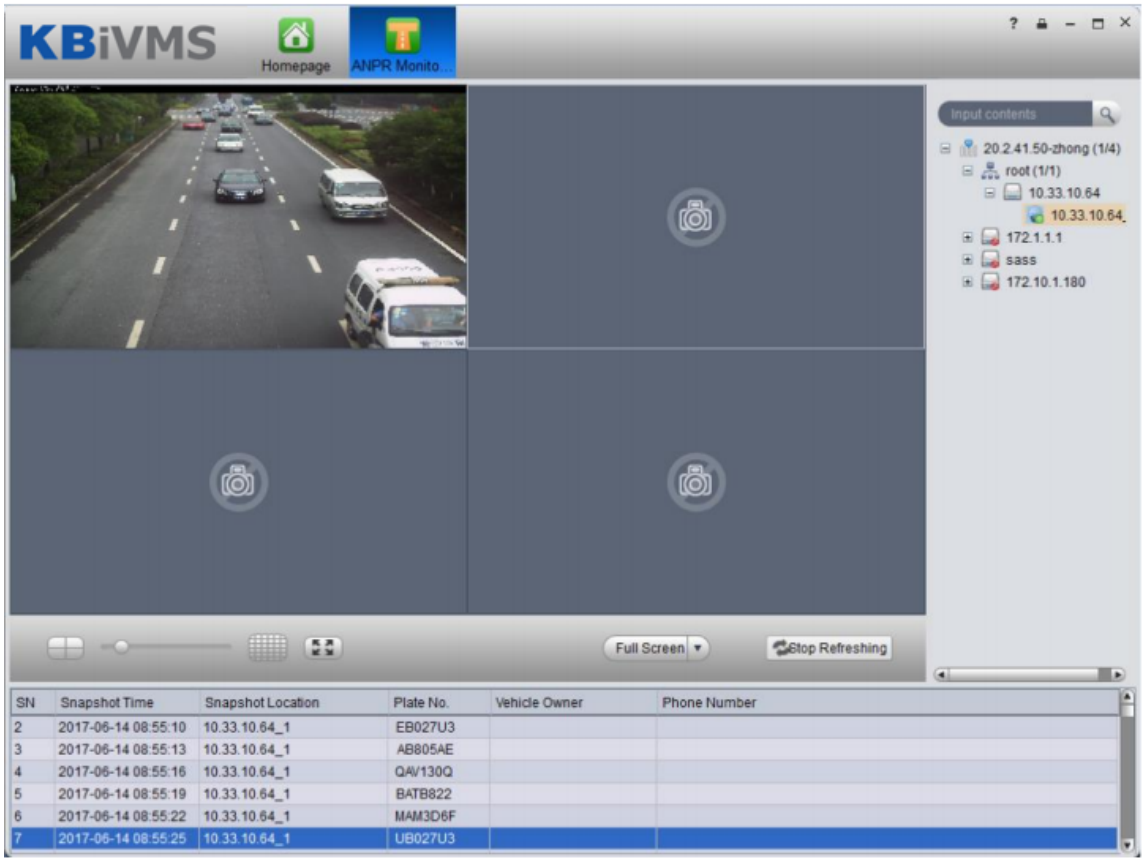


Figure 12-2

Step 3. Double click each snapshot record, see Figure 12-3.

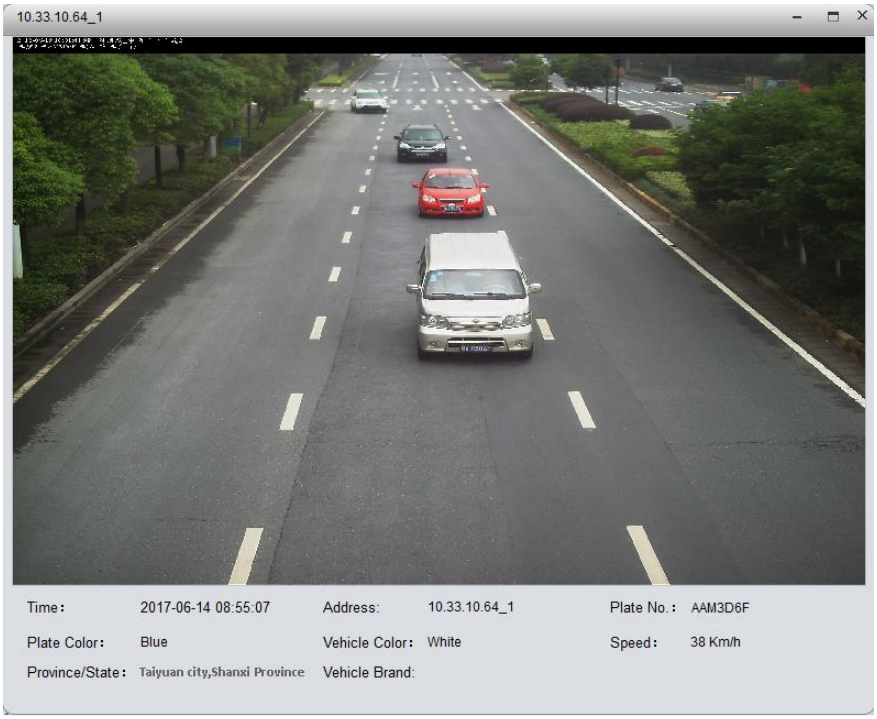


Figure 12-3

13 Vehicle Search

System supports criteria of start time, end time, snapshot location, plate no. and etc. to search history of ANPR monitoring of vehicle.

Step 1. Click  in extension function area.

Step 2. Enter criteria, click Search. See Figure 13-1.

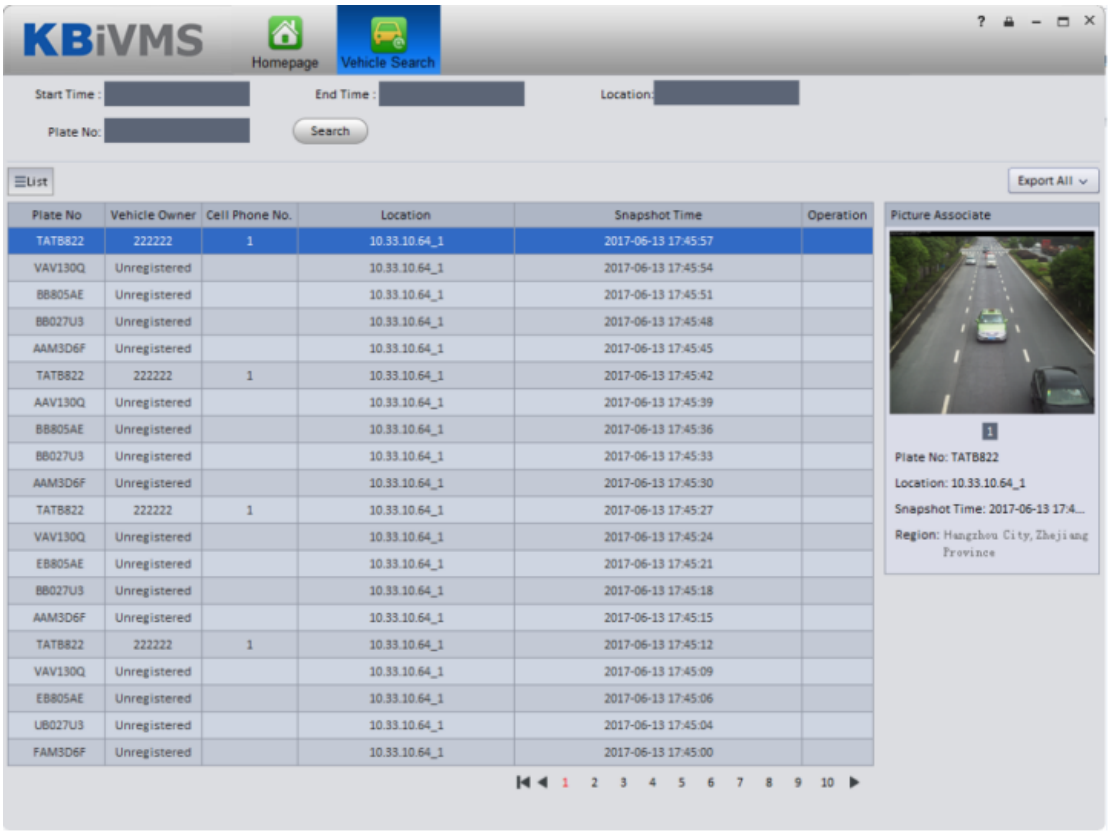


Figure 13-1

Step 3. Double click daily record to open vehicle picture.

14 Mobile

14.1 Add MPT300 Device

14.1.1 MPT300 Device WEB Platform

Step 1. Login device web.

Step 2. Select Platform Settings.

Step 3. Enable platform connection button, fill in device ID, IP address, port and other info, see Figure 14-1.

Figure 14-1

Step 4. Click OK.

14.1.2 Add MPT300 Device on Manager

Step 1. Login Manager-end.

Step 2. Select Device>Encoder.

Step 3. Click Add.

Step 4. Configure parameter info, select auto for method, and register ID shall match device ID. Device type is MPT300, check “Add ITC”. See Figure 14-2.

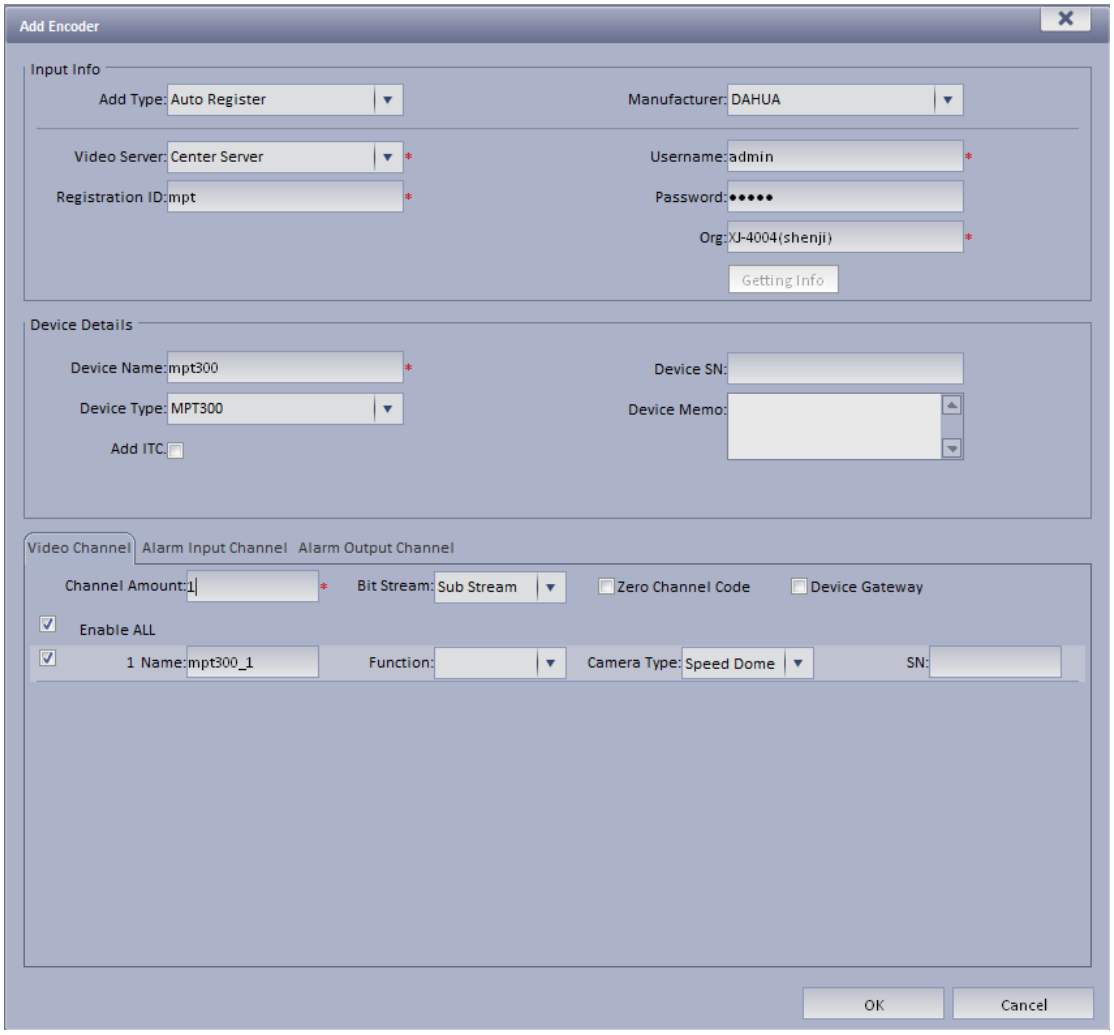


Figure 14-2

Step 5. Click OK. You can view it in Device>ANPR Device.

14.2 Add Mobile Device

14.2.1 Device WEB Setup

Step 1. Login Device WEB.

Step 2. Select Setup>Mobile>Auto Register,

Step 3. Enter Server IP, Port. See Figure 14-3.

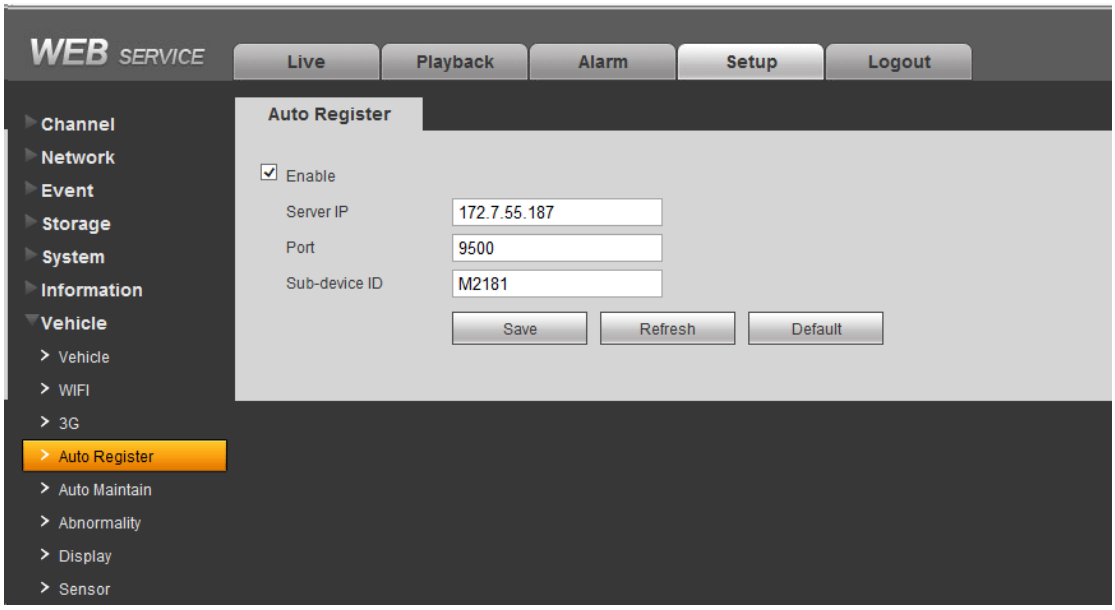


Figure 14-3

Step 4. Click OK.

14.2.2 **Add Mobile Device on Manager**

Step 1. Login KBiVMS Manager.

Step 2. Select General>Device>Encoder.

Step 3. Click Add. System pops up Add Encoder box, see Figure 14-4.

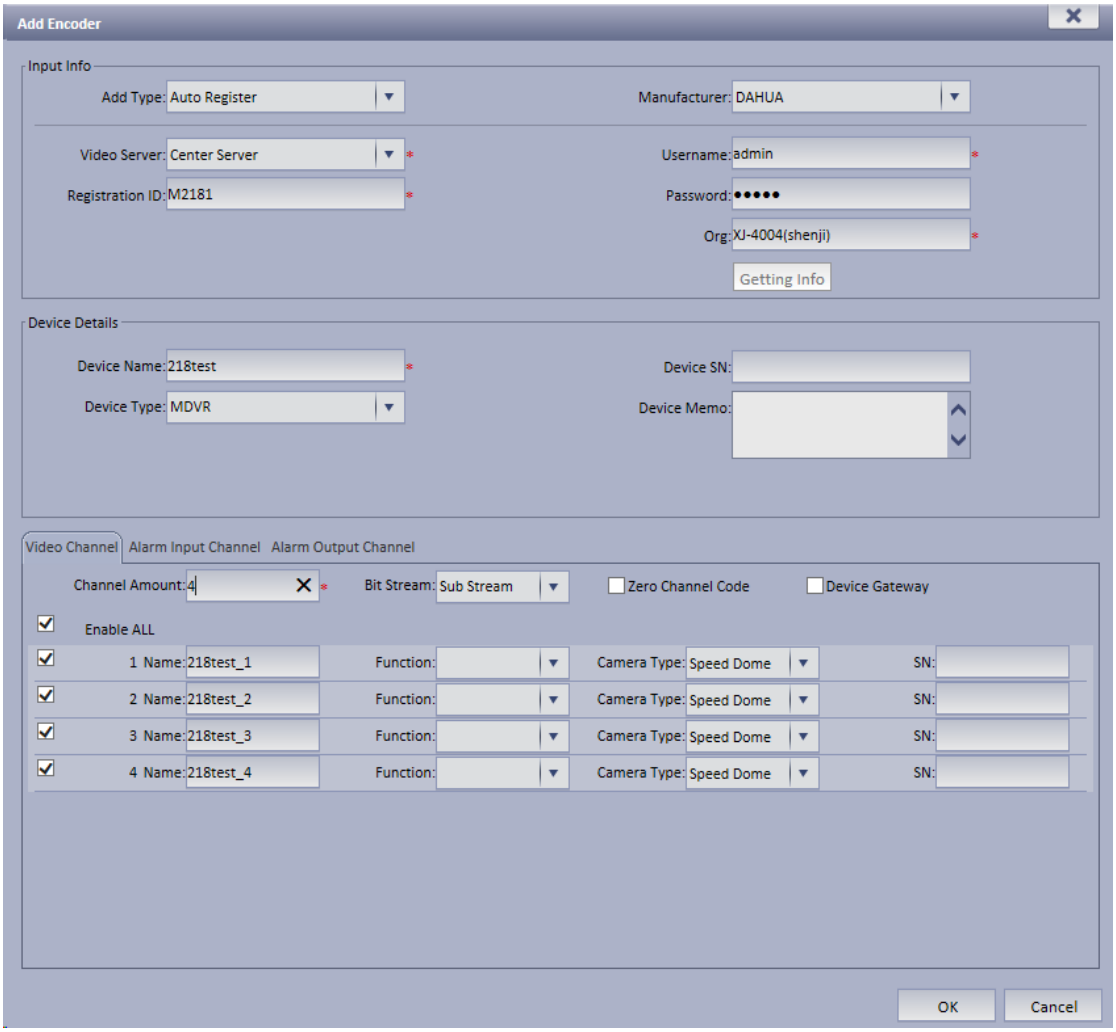


Figure 14-4

Step 4. Set parameter info. For device type, usually users select MDVR.

Step 5. Click OK.

You can search for added device in encoder page as to view device online/offline, and modify or delete device. See Figure 14-5.

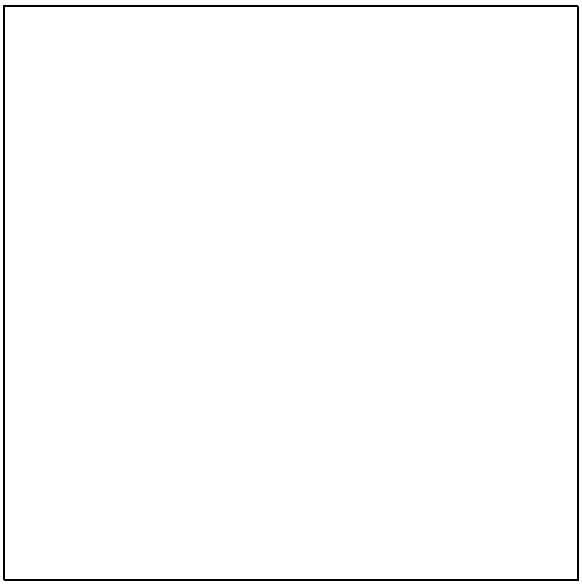


Figure 14-5

Under operation column, there is edit, delete and config icon for existing encoder.

14.3 Mobile Info

14.3.1 Add Driver Information

Step 1. Login KBiVMS Manager-end.

Step 2. Select Mobile>Mobile Info>Driver.

Step 3. Click Add. System pops up Add Driver box, see Figure 14-6.

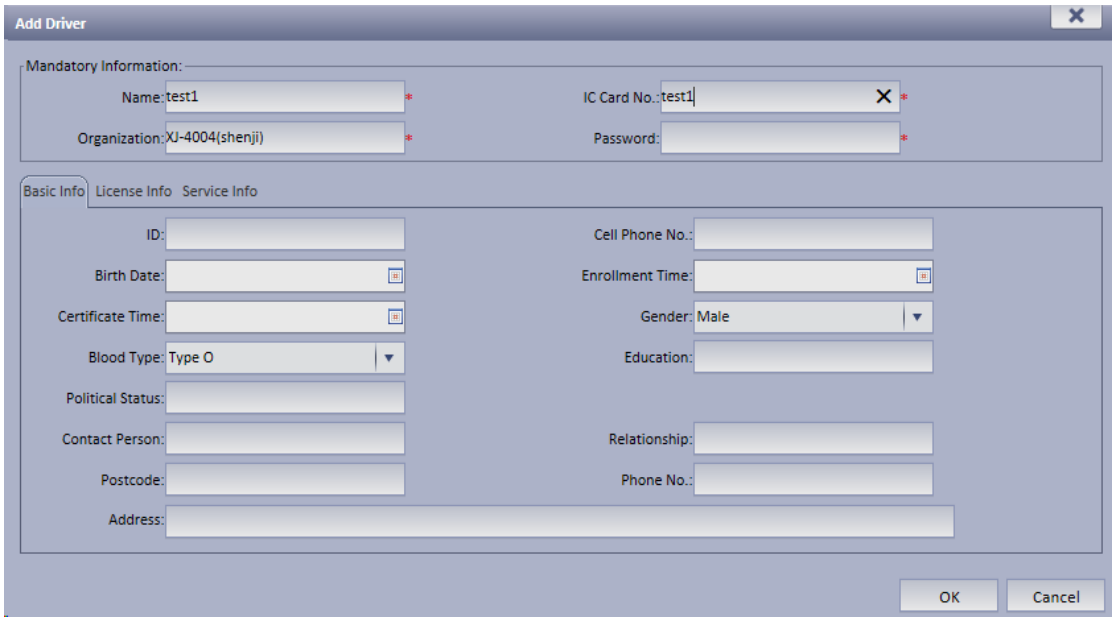


Figure 14-6

Step 4. Enter basic info, click OK.

You can search added driver by keyboard and gender, as well as modify and delete driver. See Figure 14-7.

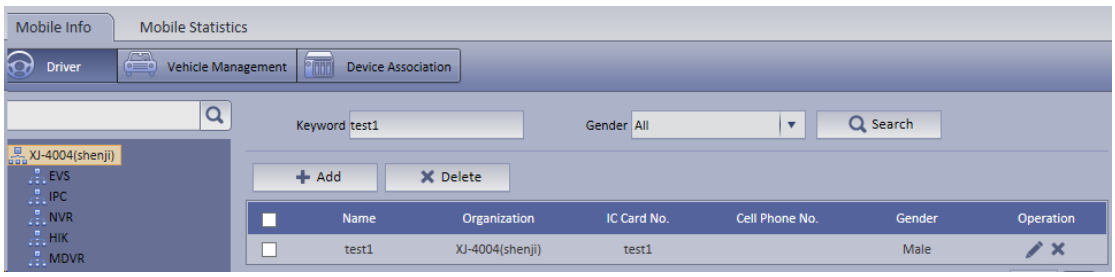


Figure 14-7

14.3.2 Vehicle Management

Step 1. Select Mobile>Mobile Info>Vehicle Management.

Step 2. Click Add. System pops up Add Vehicle box, see Figure 14-8.

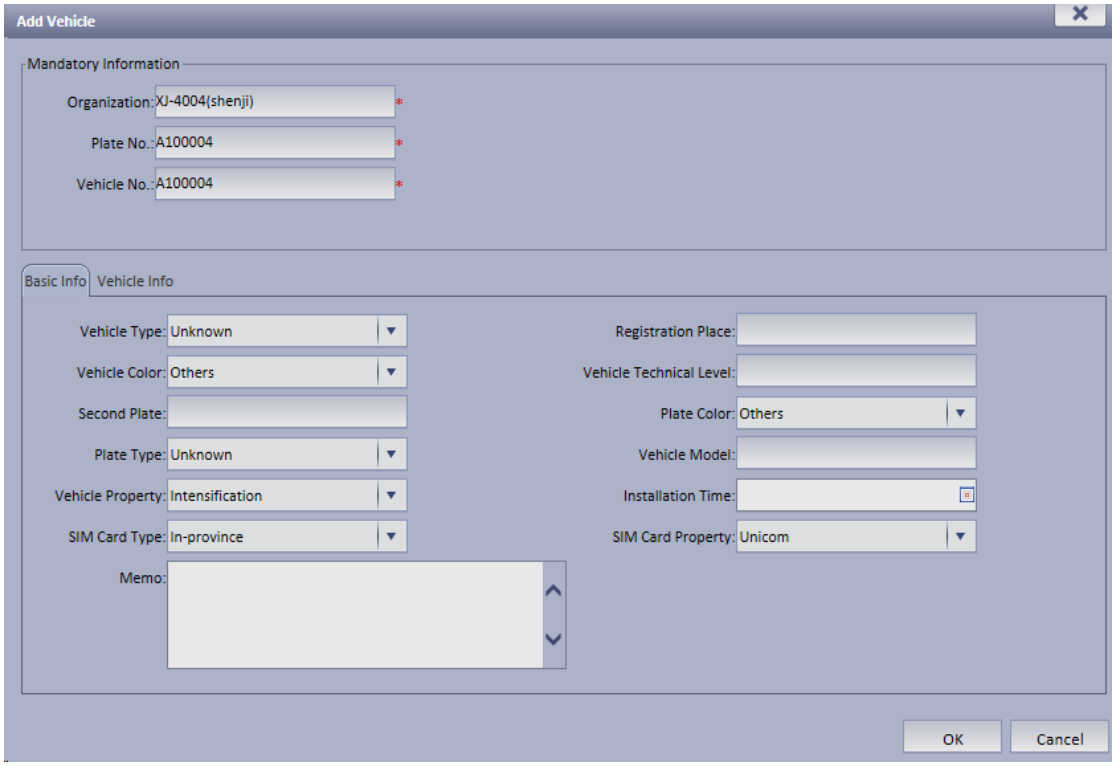


Figure 14-8

Step 3. Enter basic info, click OK. You can searched added vehicle plug modify and delete vehicle. See Figure 14-9.

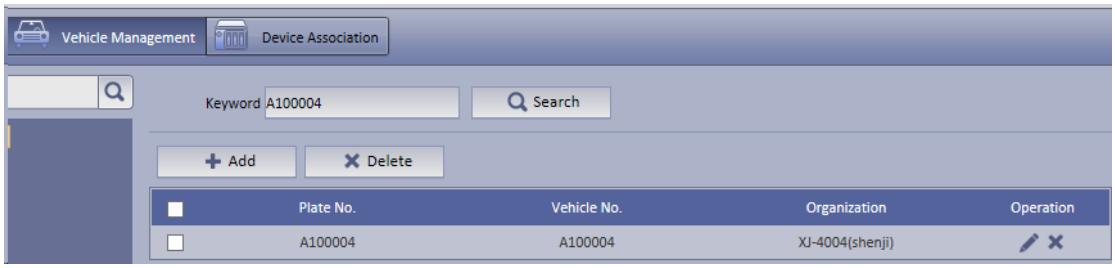


Figure 14-9

14.3.3 **Device Association Management**

You can associate existing MDVR device with existing driver and vehicle.

Step 1. Select Mobile>Mobile Info>Device Association.

Step 2. Select device to associate, click Associate.

Step 3. System pops up Edit Device Association box, see Figure 14-10.

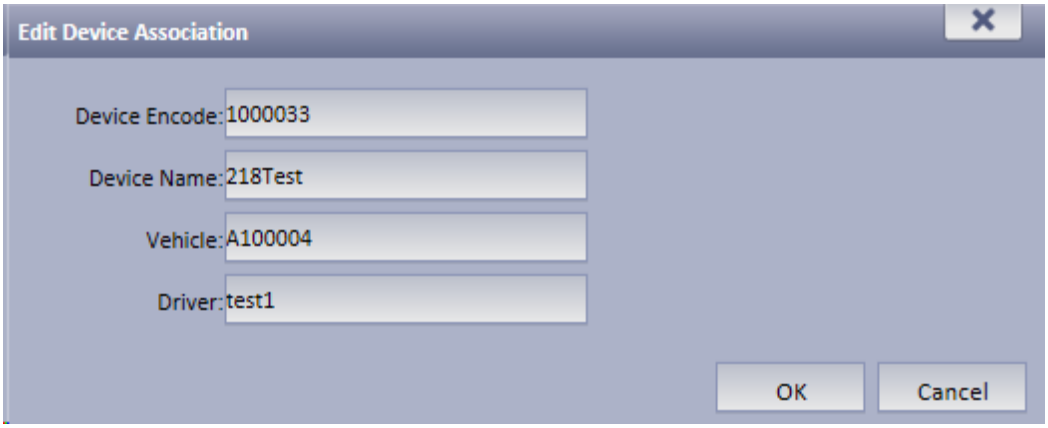


Figure 14-10

Note: You may select vehicle and driver according to you need.

Step 4. After association is complete, click OK to save. Then the device, driver and vehicle are associated.

On Client mobile map, above device you can see the association information same as on Manager-end. See Figure 14-11.

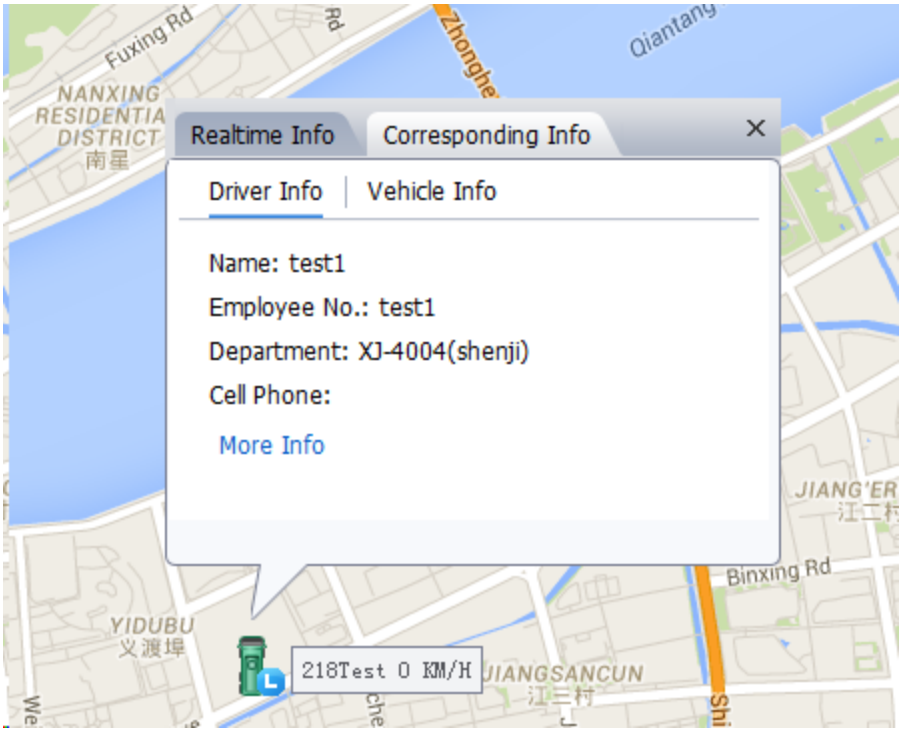


Figure 14-11

The following is vehicle info associated with device.

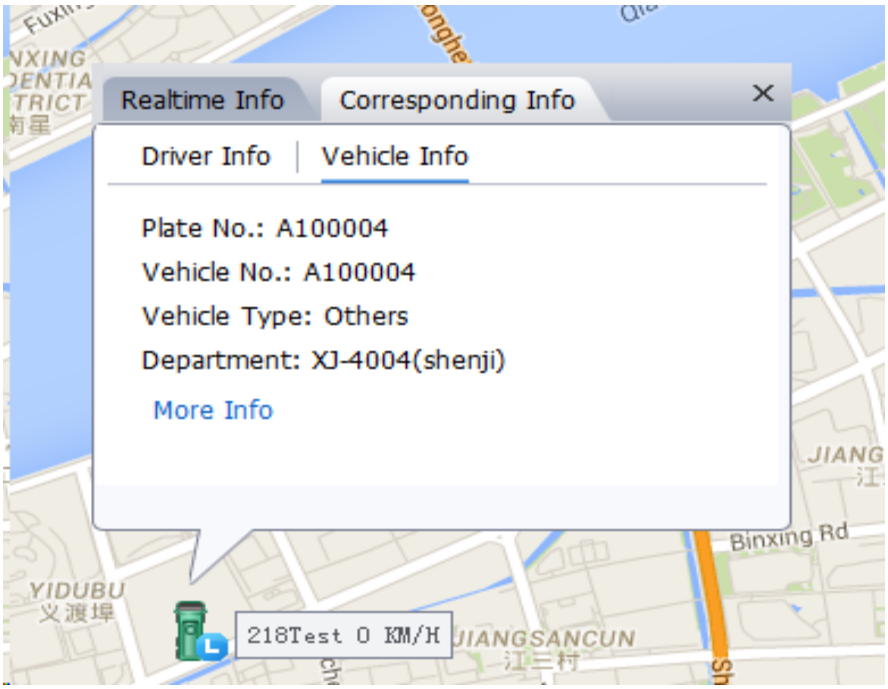


Figure 14-12

14.3.4 **Mobile Statistical Report**

In Mobile Statistics, you can search detailed GPS abnormal report, history GPS report, device status report, overspeed statistics, and area alarm report via different criteria, and export log.

For example, you search for electronic virtual fence, the steps are as follow:

Step 1. Select Mobile>Mobile Statistics> area alarm report.

Step 2. On organization tree, select organization structure you want to search and enter search criteria, click Search.

Step 3. The system displays search result, see Figure 14-13.

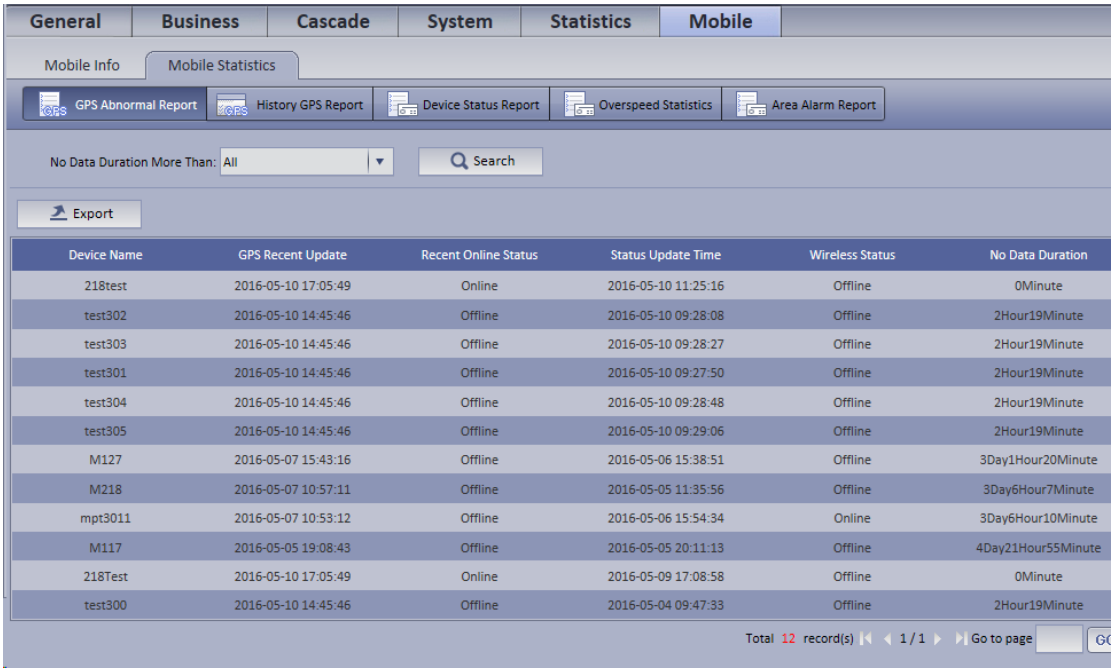


Figure 14-13

Step 4. Click Export, to export search result.

Log	Note
GPS Abnormal Report	Used to record device data during non GPS data duration. You can search for detailed GPS abnormal info via non data duration.
History GPS Report	Used to record device history GPS data. You can search detailed device GPS history data via organization tree node, period, device name and etc.
Device Status Report	Used to record device online or offline status. You can search device status via organization tree node, period and etc.
Overspeed Statistics	Used to record device overspeed status. You can search detailed overspeed info via organization tree node, period and etc.
Area Alarm Report	Used to record alarm condition in electronic virtual fence. You can search for detailed alarm info via organization tree node, period and etc.

14.4 **Violation Query**

According to set time, period, snapshot location, plate and other criteria, you can search for ANPR device snapshot all pictures.

For example, you want to search for all plates with letter “A”:

Step 1. Select ANPR info search.

The system shows General interface.

Step 2. Select by period, enter snapshot date and snapshot period.

Step 3. Check Fuzzy Search, and enter “A” in plate no.

Step 4. Click Search, see Figure 14-14.

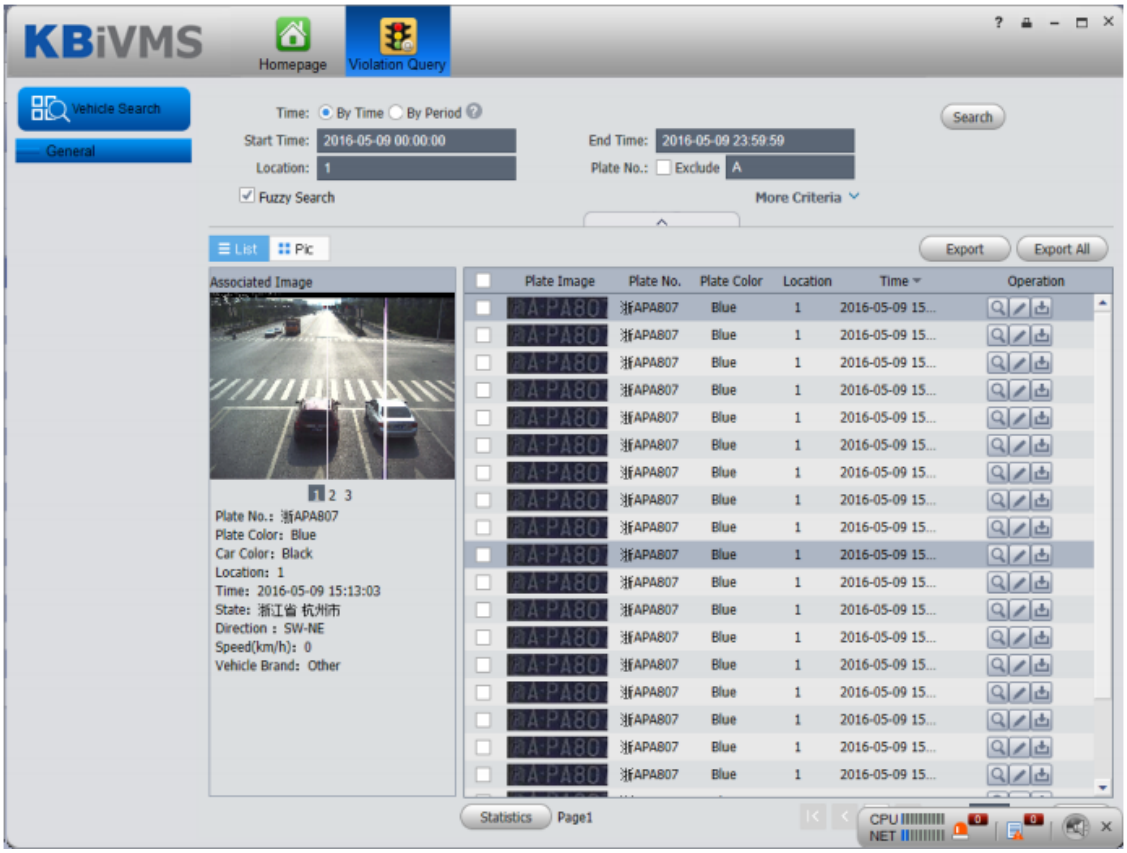


Figure 14-14

Note:

You can use the exclusion function to block certain results.

Step 1.

In step 2 time selection, if you select by time, then you can select start time and end time. The rest steps are the same with by period.

14.5 Mobile Interface

14.5.1 Introduction of Mobile Interface

Mobile interface provides key monitoring, live preview, audio talk, record playback, pattern playback and statistics.

Click  to enter Mobile interface, see Figure 14-15.

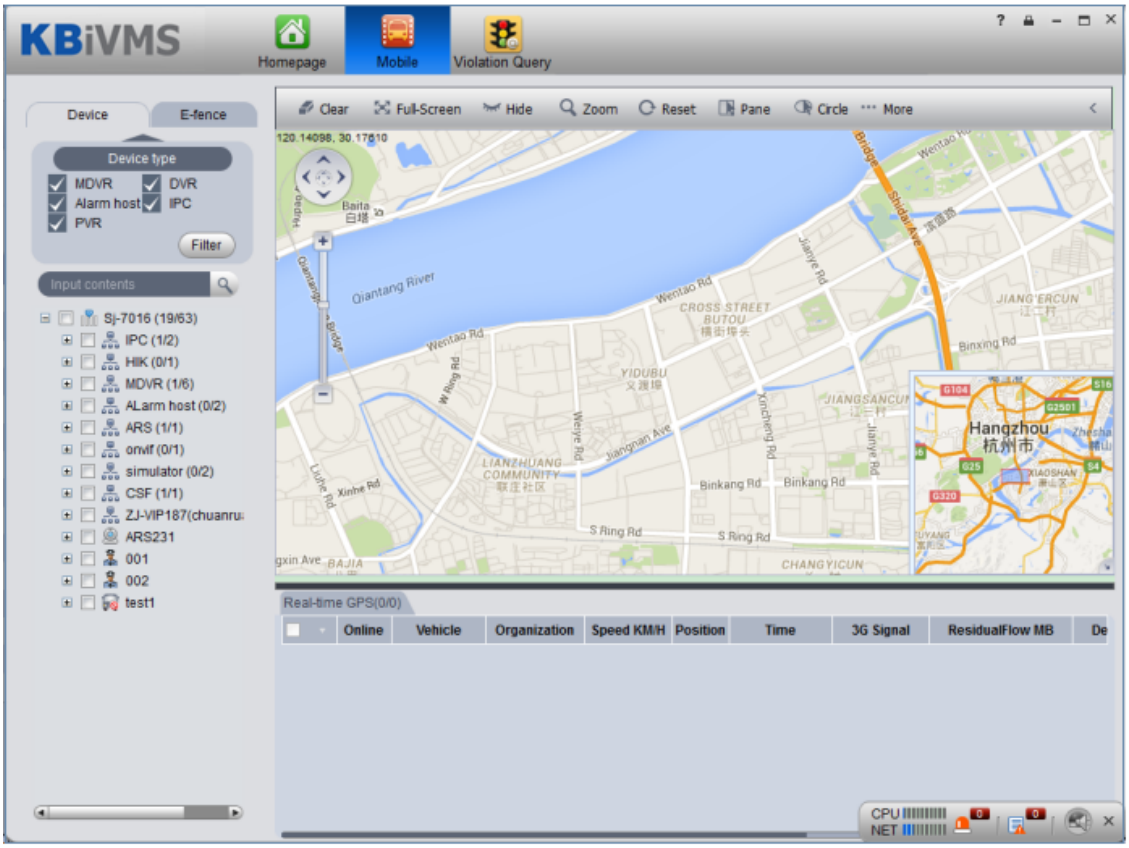


Figure 14-15

Click at the upper-left corner of map, it has four arrows pointing at four directions. You can move the map by clicking this button. Below it there is zoom in/out button.

Functions of mobile interface are shown below.

No.	Interface	Note
1	Map Operation	● Clear screen，clear operation on map. ● Switch, switch city on map. ● Search, search place on map and position it. ● Hide, hide device name shown on map. ● Zoom, right click mouse to zoom map. ● Point, select device by point. ● Line, select device by line. ● Panel, select device by pane. ● Circle, select device by circle. ● Reset, if map has shifted, click reset to restore current position. ● Distance, measure distance between selected points. ● Area, measure area of selected region. ● Mark, mark on map.
2	Device List and Electronic Virtual Fence	● Checked device under “Device ”tab means that the device is subscribed. Detailed info is shown under “Real-time GPS” tab. ● Under “Device Type” tab ,you can check device type to filter. ● Under “Electronic Virtual Fence” tab, you can create speed limit area, driving area and etc. When a vehicle passing Electronic Virtual Fence area is not driving according to the law, the system will alarm. Alarm info will be shown under global overspeed, speed limit, emergenct and other alarm tabs.

No.	Interface	Note
3	Real-time GPS	Real-time GPS may show subscribed device info. Double click device to view live preview. ● Under “Online” tab, see if device is online. ● Under “Vehicle” tab, it shows vehicle info. ● Under “Organization” tab, it shows organization of the vehicle. ● Under “Speed” tab, it shows vehicle speed. ● Under “Position” tab, it shows whether the vehicle is being positioned. ● Under “Time” tab, it shows real-time GPS receiving time. ● Under “3G signal” tab, it shows network intensity. ● Under “Device ID” tab, it shows device ID. ● Under “Position” tab, it shows vehicle current position.

14.5.2 **Right Click Device**

14.5.2.1 Right Click Device

In Mobile interface, right click device under Device tab, you can see Figure 14-16.

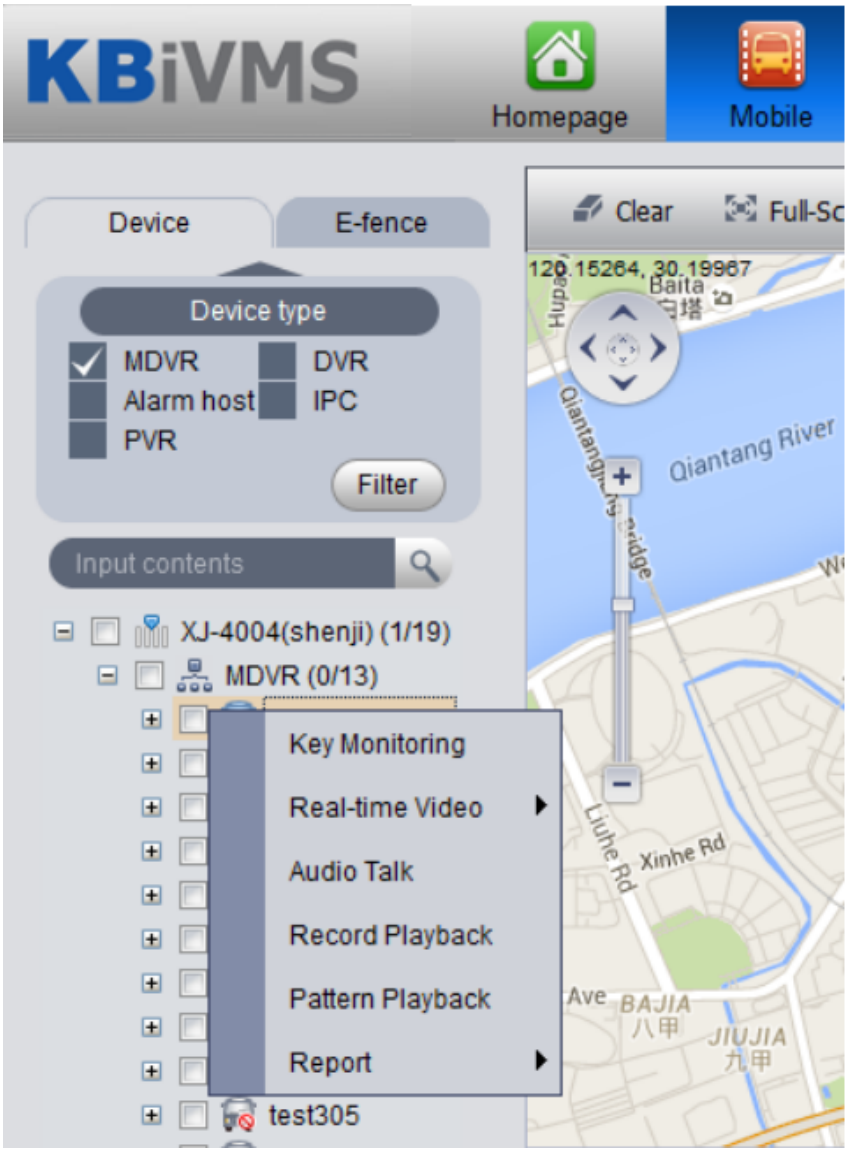


Figure 14-16

14.5.2.2 Key Monitoring

Step 1. Under Device tab, check one device to subscribe it. The interface shows device GPS info plus device real-time info and associated info.

Step 2. Right click the device, select key monitoring, see Figure 14-17.

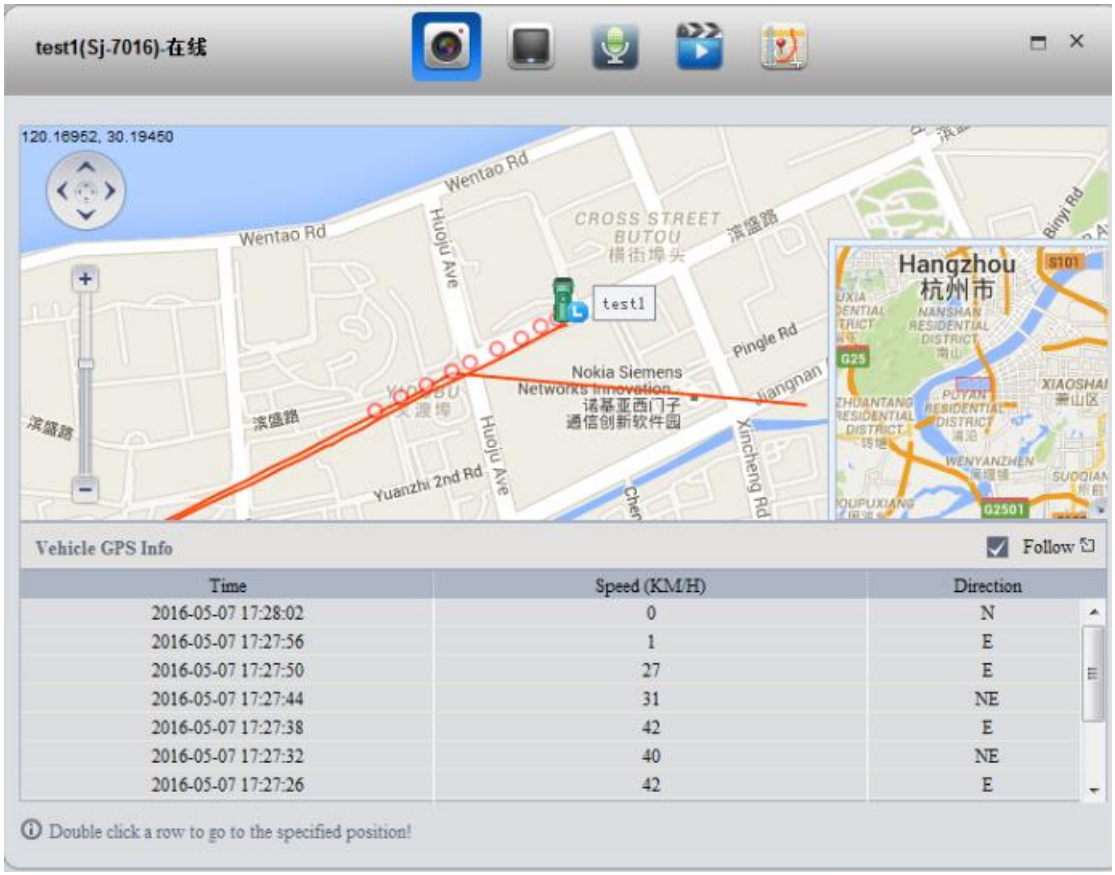


Figure 14-17

Note: The map shows vehicle driving pattern within previous 10 minutes. You can double click any row to position it on map.

14.5.2.3 Live Preview

The system shows 4 live preview channels by default.

In Key Monitoring interface, click  or under Device tab, right click device and select live preview. The system shows live preview video, see Figure 14-18.

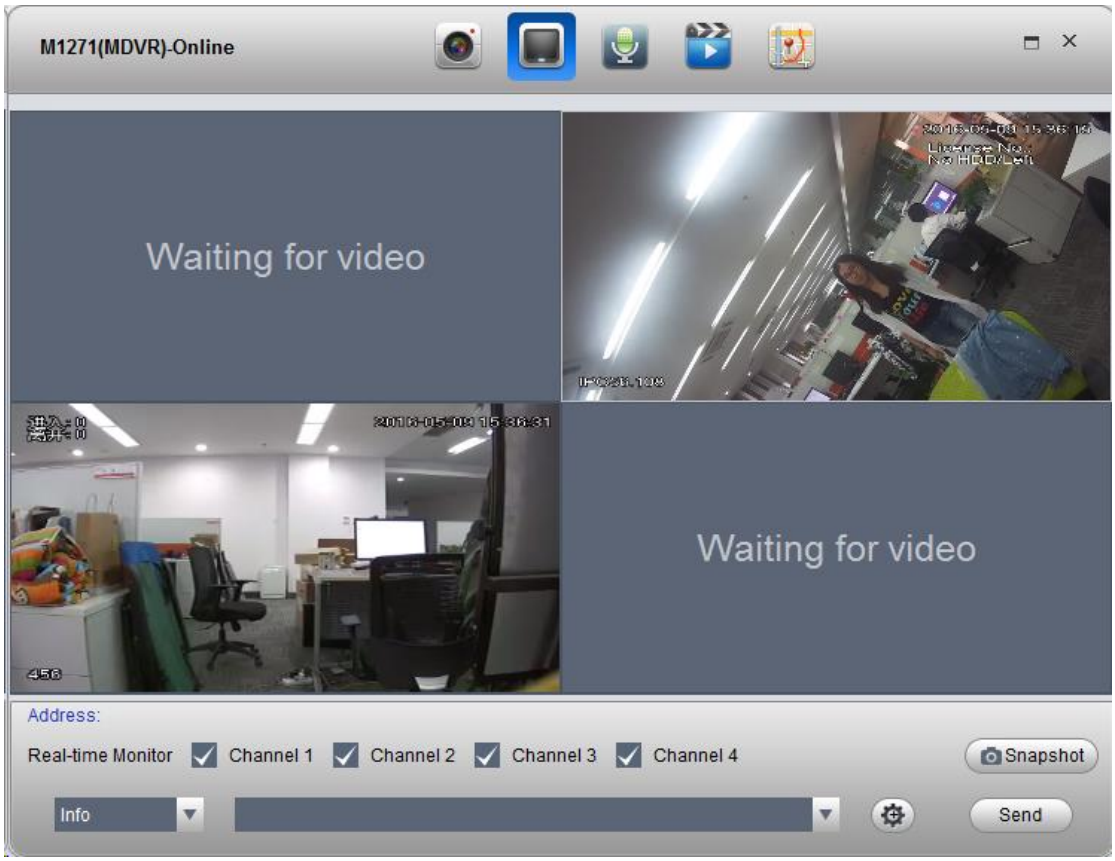


Figure 14-18

No.	Interface	Note
1	Select Channel	● By checking to select channel you want to be shown.
2	Snapshot	● By snapshot, you can snapshot picture from video.
3	Send	● Enter or select one message, send it to mobile device. You can click  to edit message template. You may expand message button to see a ad option which you may also edit to be sent.

Note:

The device currently only has one window for edition of message and ad. After message or ad is sent, it will be shown in video window, see Figure 14-19.

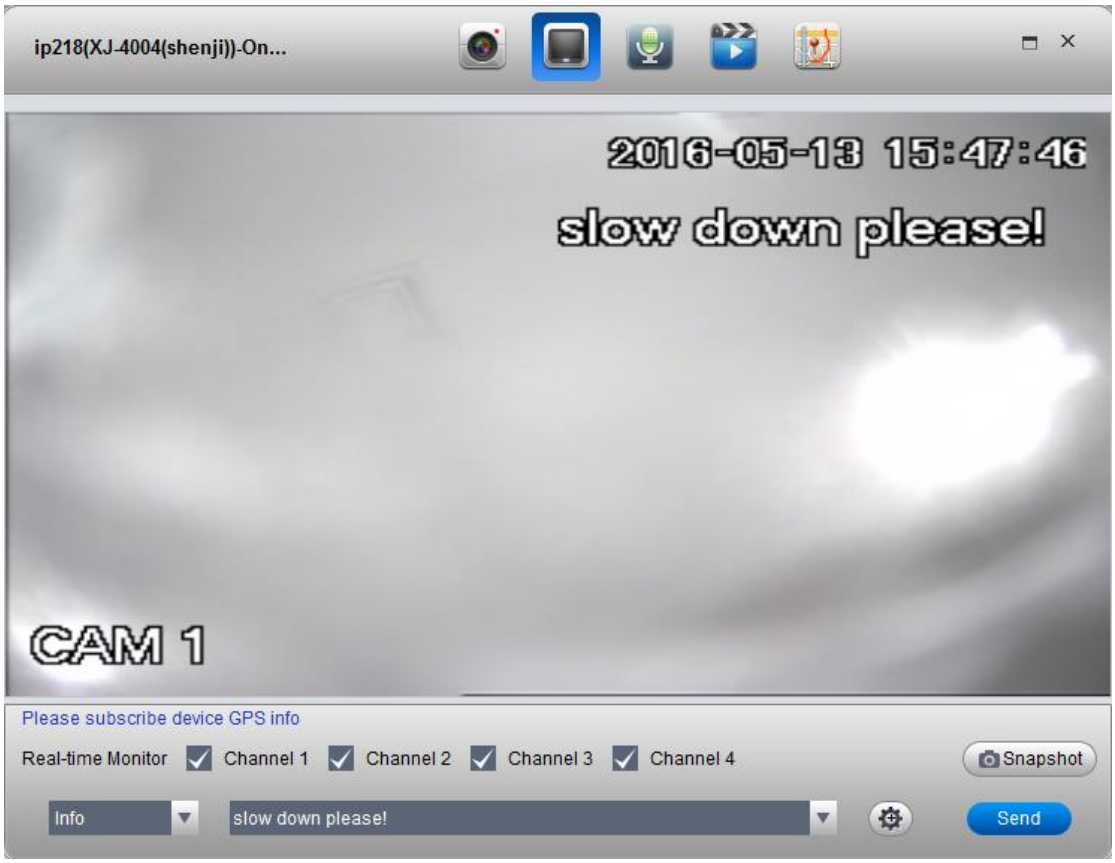


Figure 14-19

14.5.2.4 Audio Talk

You can right click on device to select audio talk function. See Figure 14-20.

Figure 14-20

Note: User can directly talk to device on Client.

You can adjust volume of MIC and earphone on this page.

14.5.2.5 Record Playback

Right click on device to select record playback function, see Figure 14-21.

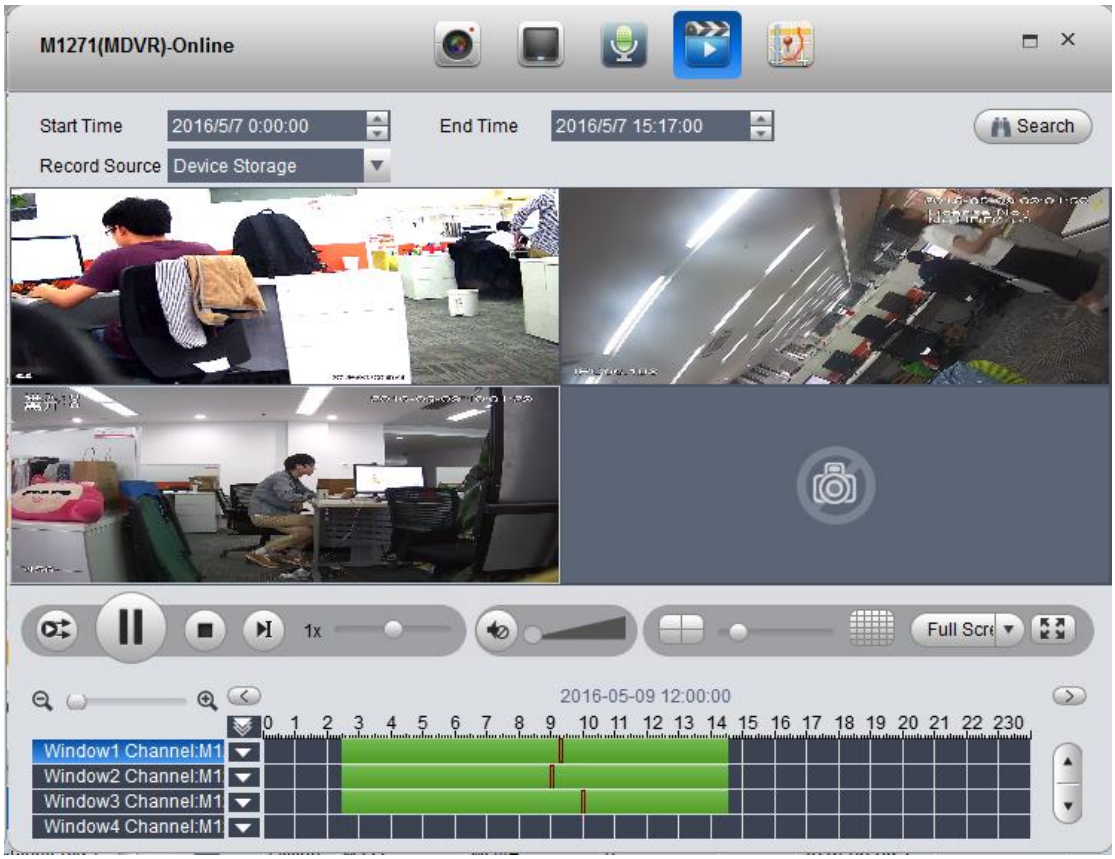


Figure 14-21

Record playback supports search and playback of device record and center record. Click area containing record to position this time point of record.

14.5.2.6 Pattern Playback

Under Device tab, right click device and select pattern playback, you can enter Pattern Playback interface. Select one of GPS, device and platform to search and playback pattern of current device.

- GPS: display current device GPS info and pattern.
- Device, display current device record.
- Platform, display current platform central record (record in record plan).

For example to search GPS, platform steps:

Step 1. Configure start time and end time.

Step 2. Select GPS.

Step 3. Click Search.

See Figure 14-22.

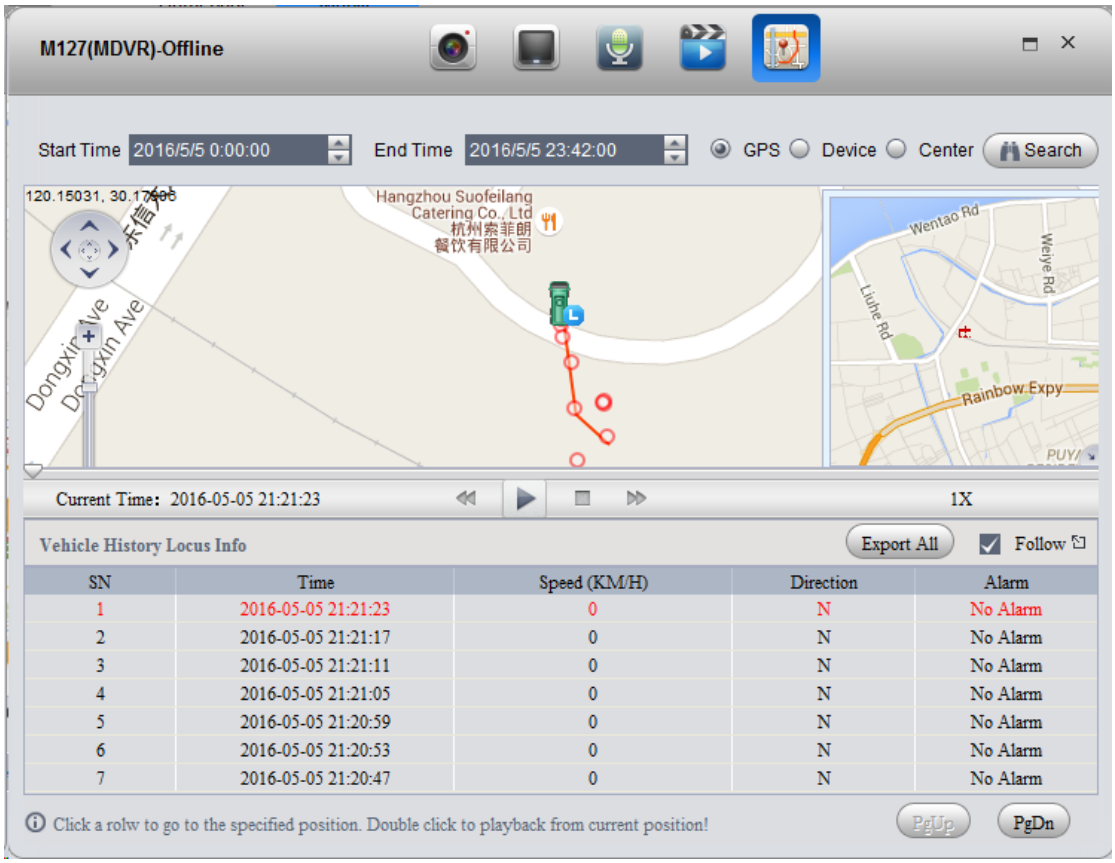


Figure 14-22

14.5.2.7 Statistics

You can search GPS module status report, overspeed report, fence alarm report, history GPS and device offline report.

For example, to search GPS report:

Step 1. Right click device and select report>history GPS.

Step 2. Enter search period.

Step 3. Click Search. See Figure 14-23.

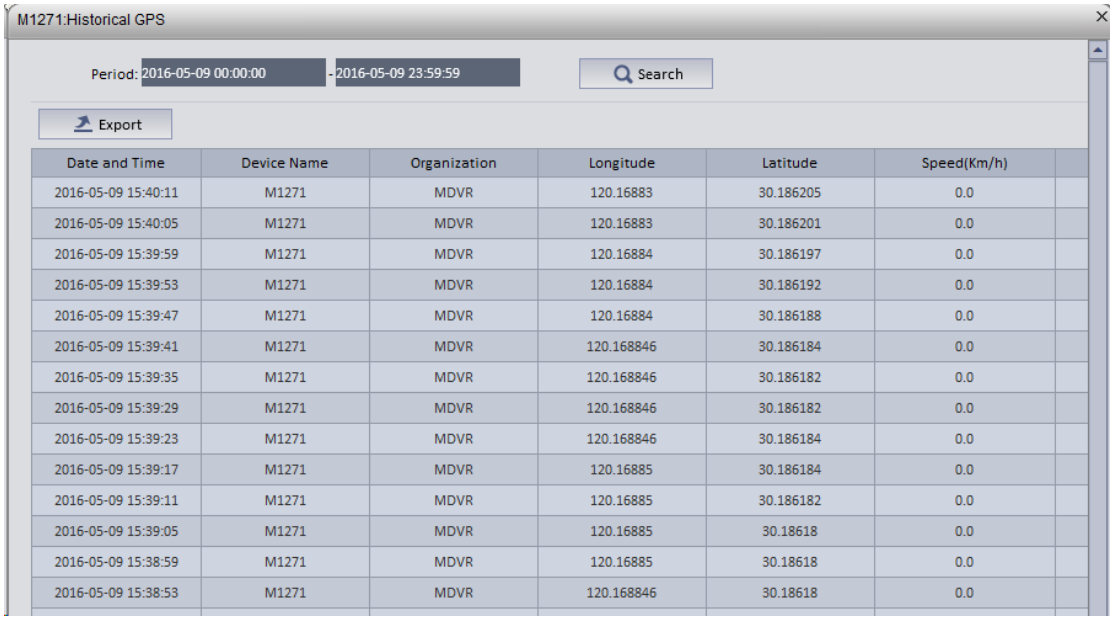


Figure 14-23

You can click Export to export result of search in Excel format to local.

Report	Note
GPS Module Status	Statistics of current device GPS module status info
Overspeed Info	According to Start Time, End Time, Alarm Type, Overspeed and Alarm Interval, make statistics of current device and overspeed info.
Fence Alarm Info	According to Start Time, End Time, Alarm Type and Vehicle, make statistics of current device fence alarm info.
History GPS	Statistics of vehicle history GPS info, including the vehicle longitude, latitude, speed and etc. Click Position to find vehicle on map.
Device Offline Info	Statistics of current device offline status info.

14.5.3 **Icon above Device**

On mobile map, you can see icon above device, see Figure 14-24.

Figure 14-24

You can click these icons or right click device to get corresponding functions:

 =Key monitoring

 =Live preview

 =Recent pattern, not available in right click menu.

 =Audio talk

 =Record playback

=Pattern playback

=Address analysis, not available in right click menu.l

14.5.3.1 Recent Pattern

Recent pattern shows device recent pattern, see Figure 14-25.

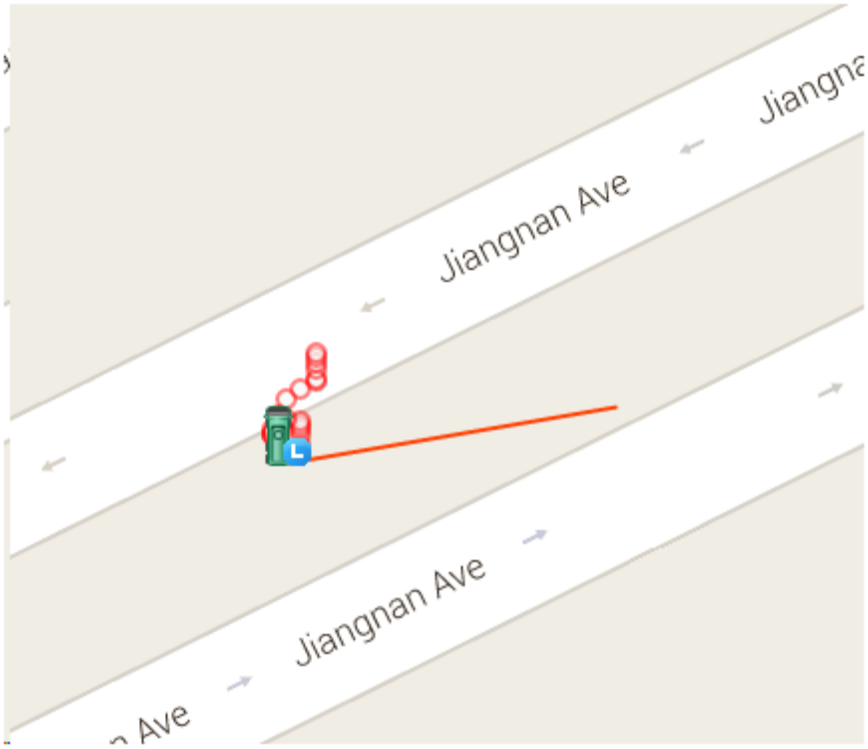


Figure 14-25

Note:

Red line in picture is the recent pattern.

14.5.3.2 Address Analysis

Address analysis button can help you exchange GPS info into real position.

14.5.4 Configure Electronic Virtual Fence

Click Electronic Virtual Fence, see Figure 14-26.

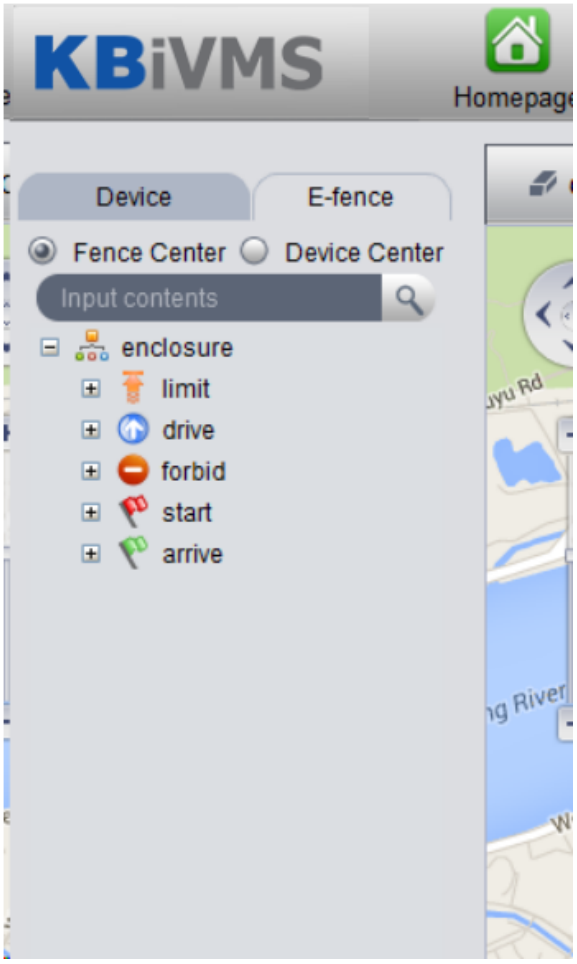


Figure 14-26

Config method of limit, drive, forbid, start, arrive are the same, here uses limit as an example.

Step 1. Click limit, see Figure 14-27.

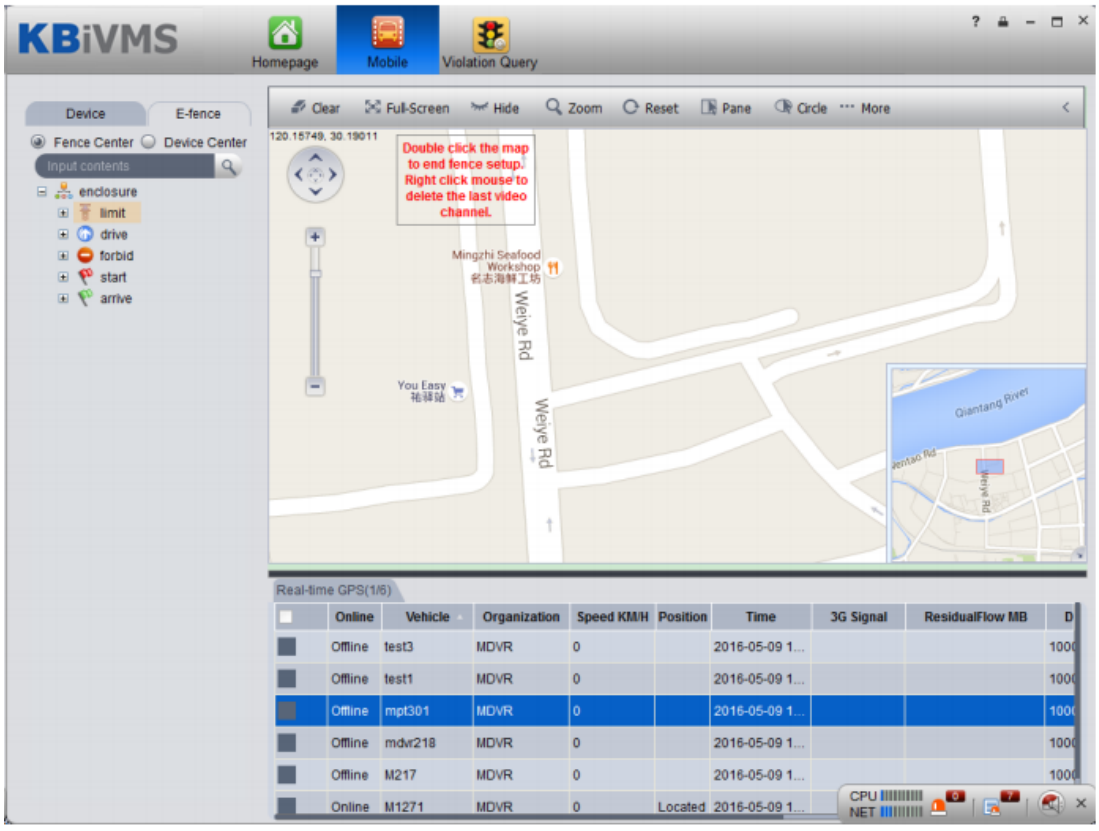


Figure 14-27

Step 2. Click a point on map to add limit area. You can add point progressively. Double click point to end adding. See Figure 14-28.

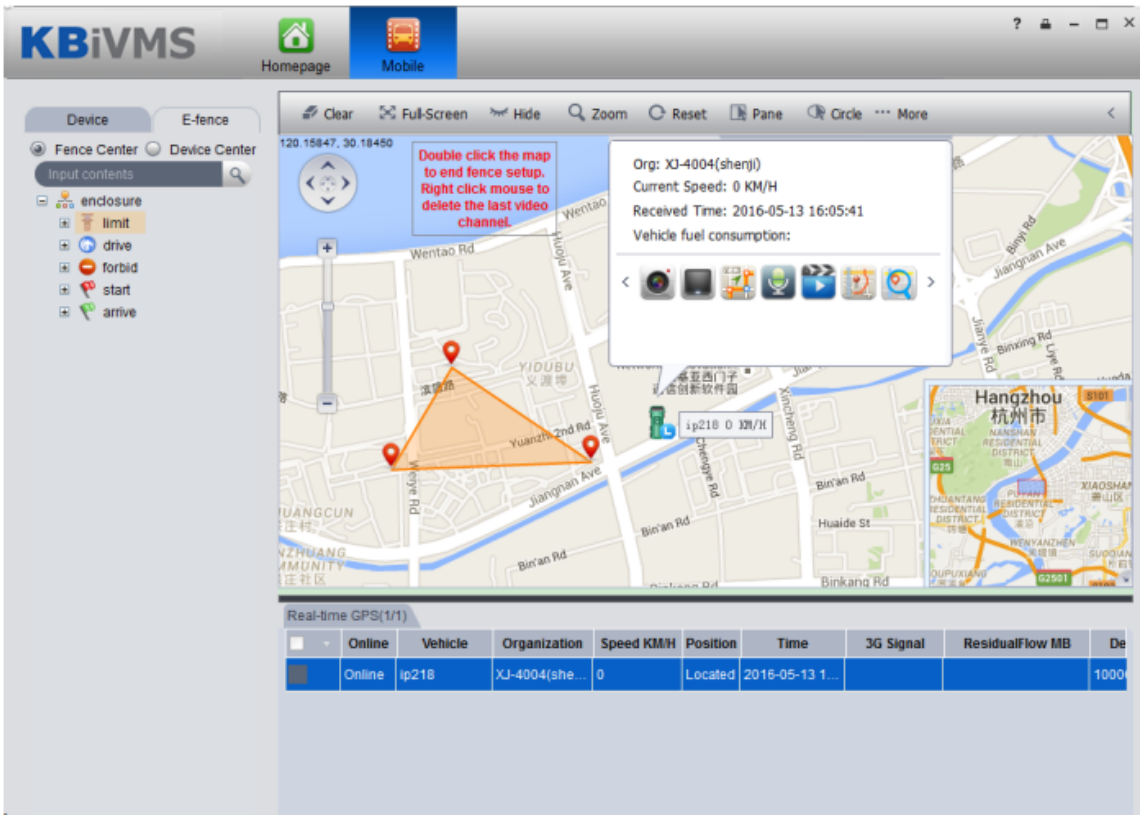


Figure 14-28

Step 3. Double click on red text above, it pops up fence property box, see Figure 14-29.

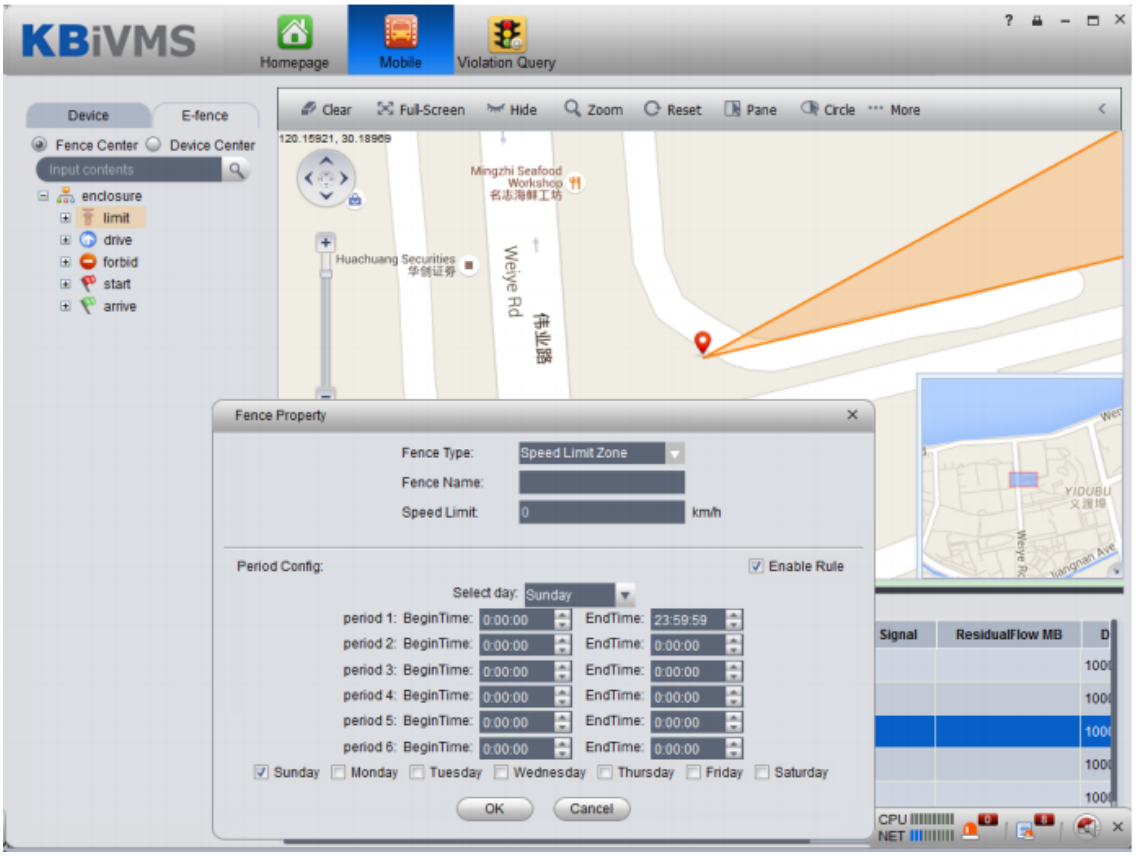


Figure 14-29

Note:

In Fence Property box, you can configure fence type, speed limit and fence name.

When you complete config, click OK. The new limit area will be shown under limit tab of Electronic Virtual Fence.

15 IVS Analysis

The system currently supports people statistical information and heat map.

15.1 Add Smart IPC Device

Before using this statistical function, you must add SmartIPC device on KBiVMS Manager.

Step 1. Login KBiVMS Manager.

Step 2. Select General>Device>Encoder.

Step 3. Click Add. System pops up Add Encoder box.

Step 4. Configure parameter info, select Smart IPC for device type, check People Count box. See Figure 15-1.

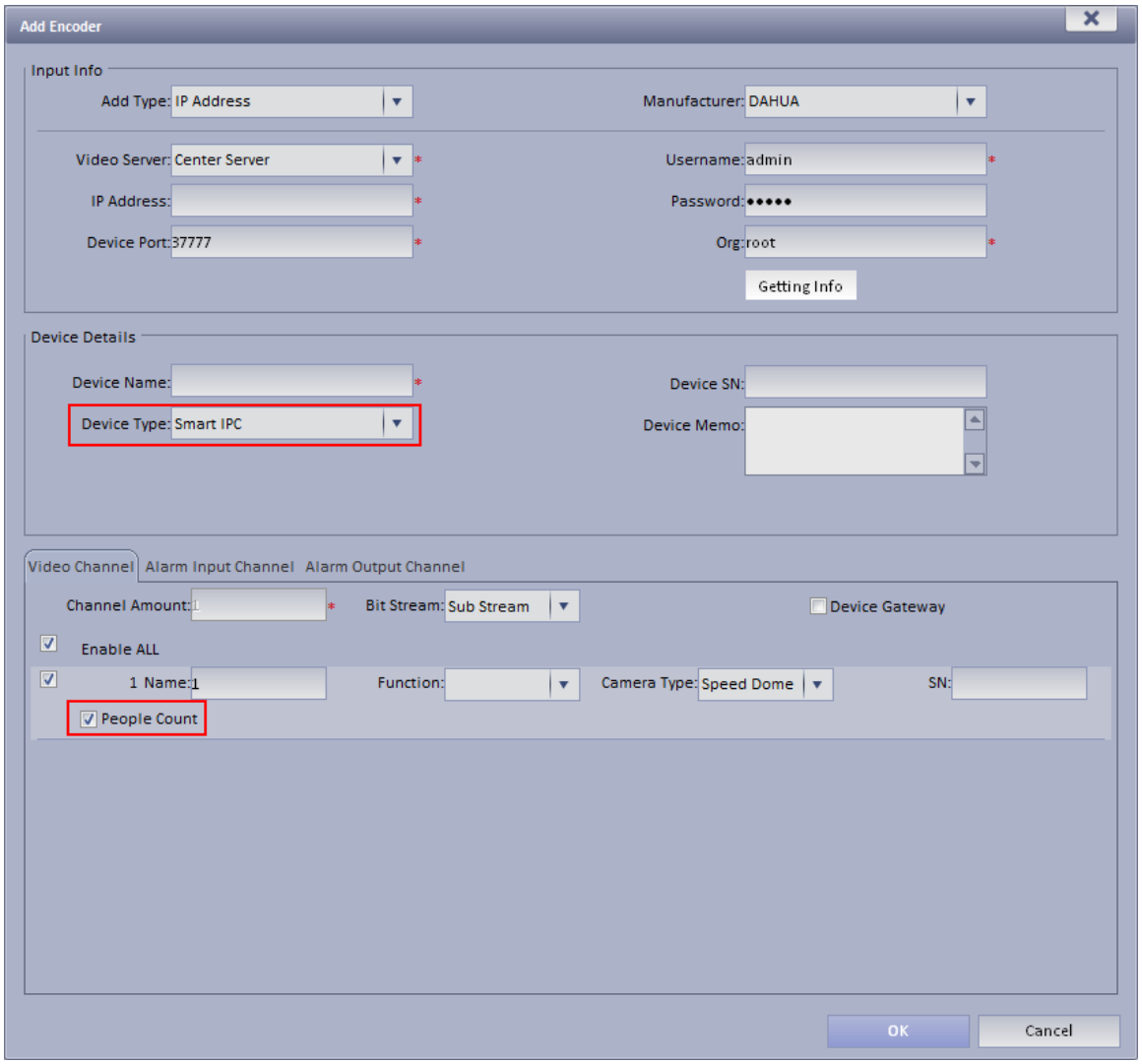


Figure 15-1

Step 5. Click OK.

15.2 People Statistical Report

Step 1. Login KBiVMS Client.

Step 2. Click  in Extension area.

Step 3. On the left, select device channel, configute alarm type, statistical time, click Search. See Figure 15-2.

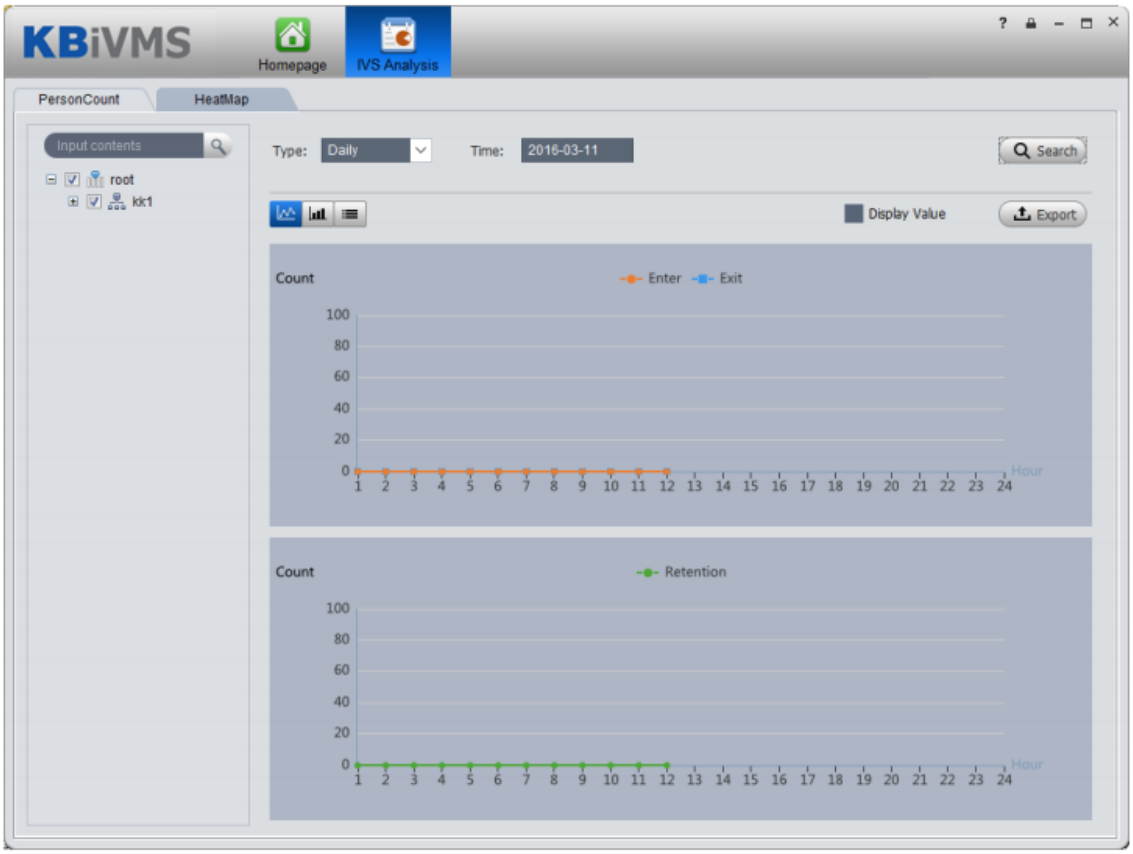


Figure 15-2

Step 4. Click “HeatMap”. See Figure 15-3.

Note:

Device real-time upload heat map data to platform, start from adding device, you can search heat map statistical data, but search is in unit of week. (Interval between start time and end time is up to 7 days).

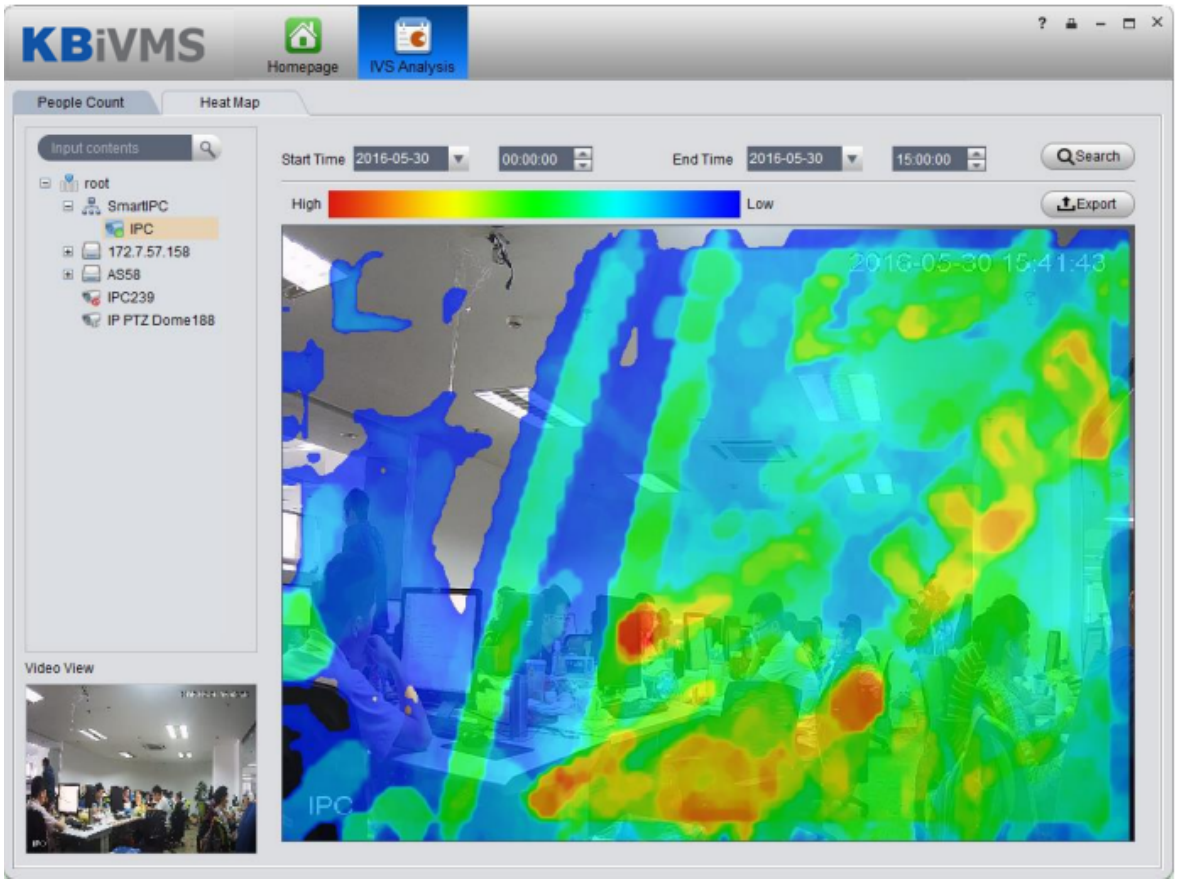

KBiVMS
Homepage
IVS Analysis
People Count
Heat Map
Input contents
root
SmartIPC
IPC
172.7.57.158
AS58
IPC239
IP PTZ Dome188
Video View
Start Time
2016-05-30
00:00:00
End Time
2016-05-30
15:00:00
Search
High
Low
Export
2016-05-30 15:41:43
IPC

Figure 15-3

16 Smart Track

KBiVMS platform client support smart track, which links fisheye camera and general camera, easily monitor each spot.

Note:

Before using smart track function, you must add fisheye device in Basic Config>Device on Manager (after adding device, click , in channel dropdown list select “fisheye (rear calibration) and general speed dome. Please see Ch 5.1.

Step 1. In Extension area click  .

Step 2. Click Add Scheme. See Figure 16-1.

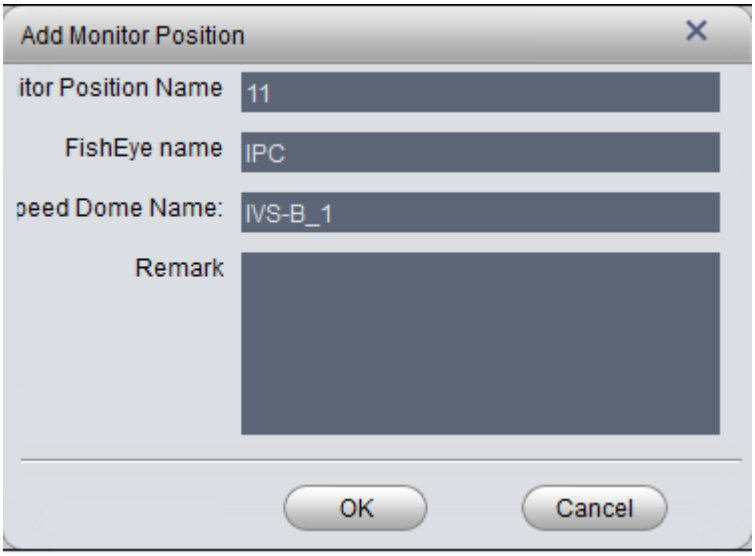


Figure 16-1

Step 3. Configure monitor position name, select fisheye name and speed dome name, click OK. See Figure 16-2.

Figure 16-2

Step 4. Click Add Calib, and select one spot in fisheye video on the left. Then find this spot in general speed dome video on the right, adjust PTZ to center position (green cross in video).

Note:

- Select 3-8 calibration points in fisheye video.
- When you find the calibration points in general video on the right, click  to zoom out PTZ.
- Click  , using 3D positioning, when you click a certain spot in video on the right, it will auto moved to center position.

Step 5. Click save.

Step 6. Follow step 4-5 to add at least three calibration points which shall not be linear.

See Figure 16-3.

Figure 16-3

Step 7. Click OK. See Figure 16-4.

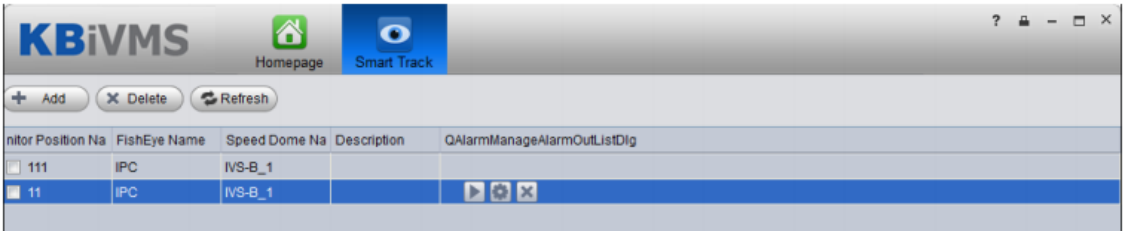


Figure 16-4

Step 8. Click , enter Smart Track interface, see Figure 16-5.

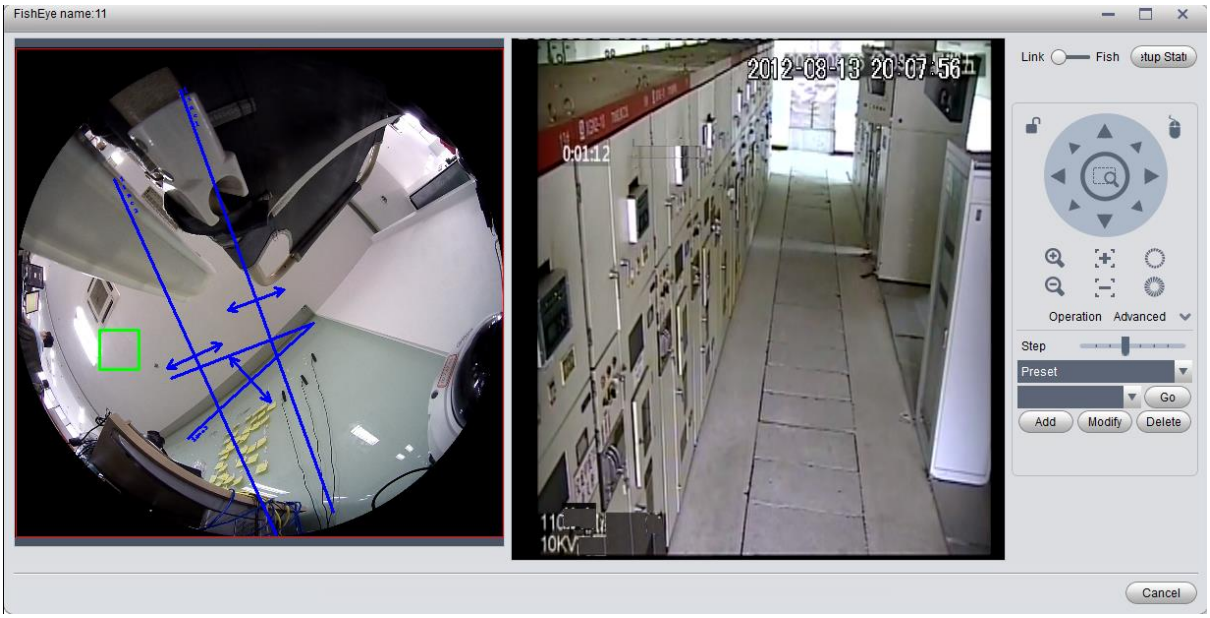


Figure 16-5

Step 9. Click any point on in fisheye video on the left, the general speed dome on the right will auto link to the corresponding position.

Step 10. Click Config Manager at the upper-right corner to shows add calibration point interface.

Step 11. Click Playback at the upper-right corner to return to smart track interface.

17 Access Control

Access control function supports to unlock door, process alarm information and bind video.

17.1 KBiVMS Manager Device

17.1.1 Add A&C Device

Step 1. Login KBiVMS Manager.

Step 2. Select General>Device>Access Control.

Step 3. Click Add. System pops up Add A&C box, see Figure 17-1.

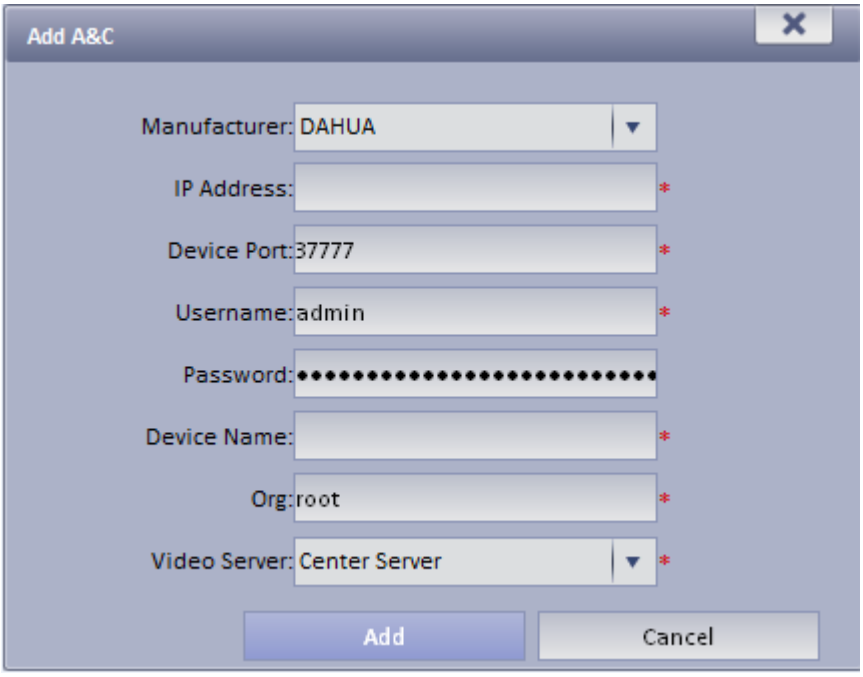


Figure 17-1

Step 4. Enter IP address, device name and etc., click Add.

Figure 17-2

Step 5. Enter A&C channel and etc., click OK.

17.1.2 Unlock Timeout Config

The system supports to configure timeout unlock. If a user unlocks door over this time threshold, then it will link to alarm.

The higher the level, the higher the threshold value will be.

Step 1. Select Business>Unlock Overtime.

Step 2. Enter alarm level name and threshold value, see Figure 17-3.

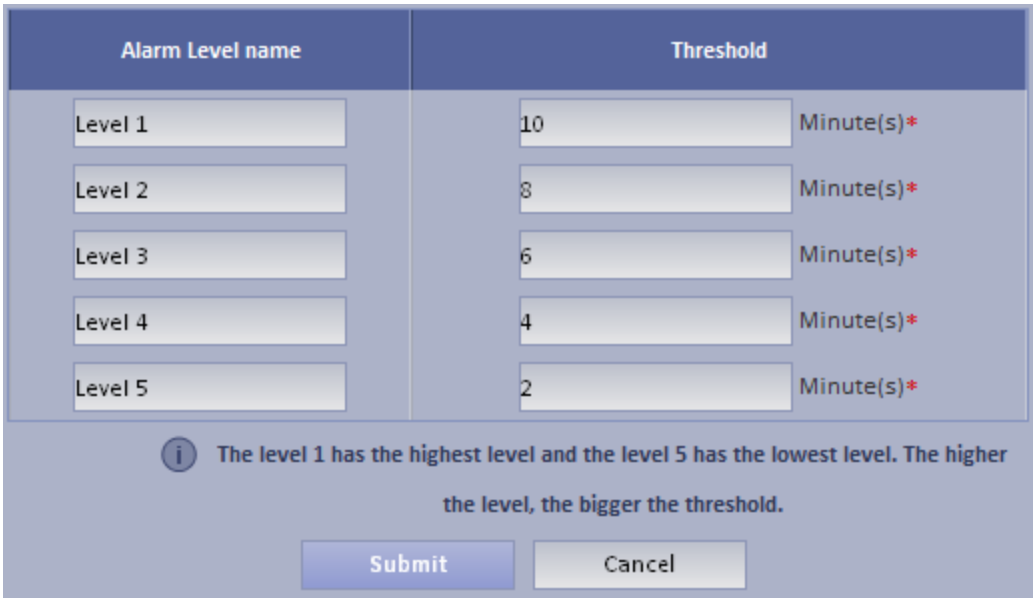


Figure 17-3

Step 3. Click Submit.

17.1.3 **Link Video**

KBiVMS Manager supports to bind video resource to A&C. When A&C has alarm, it will play bound video resource.

Step 1. Select Business>Link Video>A&C.

Step 2. Click 

. See Figure 17-4.

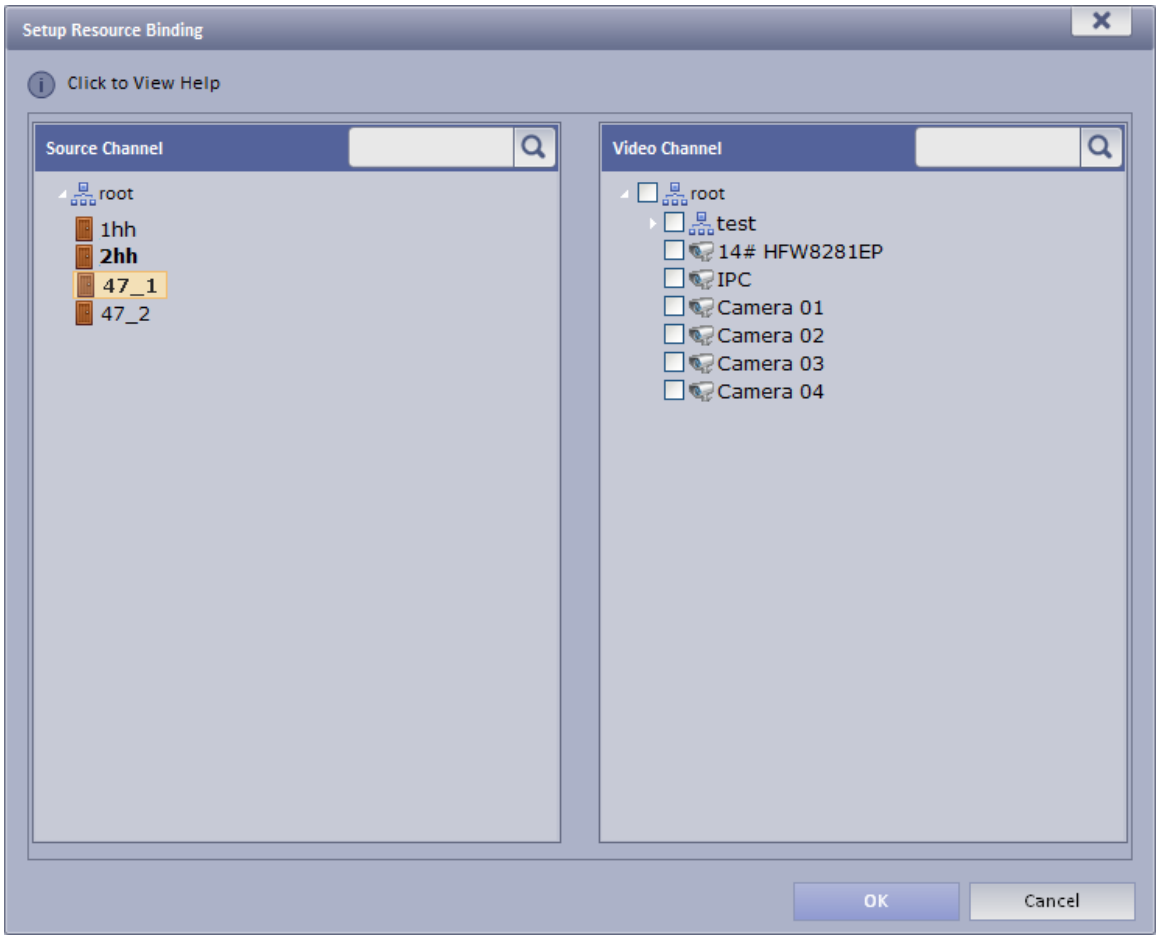


Figure 17-4

Step 3. Select A&C source and linked video channel.

Step 4. Click OK.

17.2 Access Control

17.2.1 Main Control

Step 1. Login KBiVMS Client.

Step 2. Click  in Extension area.

Step 3. In device list on the right, select different A&C devices, so it will show different A&C unlock information, door sensor and overtime alarm.

You can view lock/unlock, door sensor, overtime alarm information in each of the following tab.

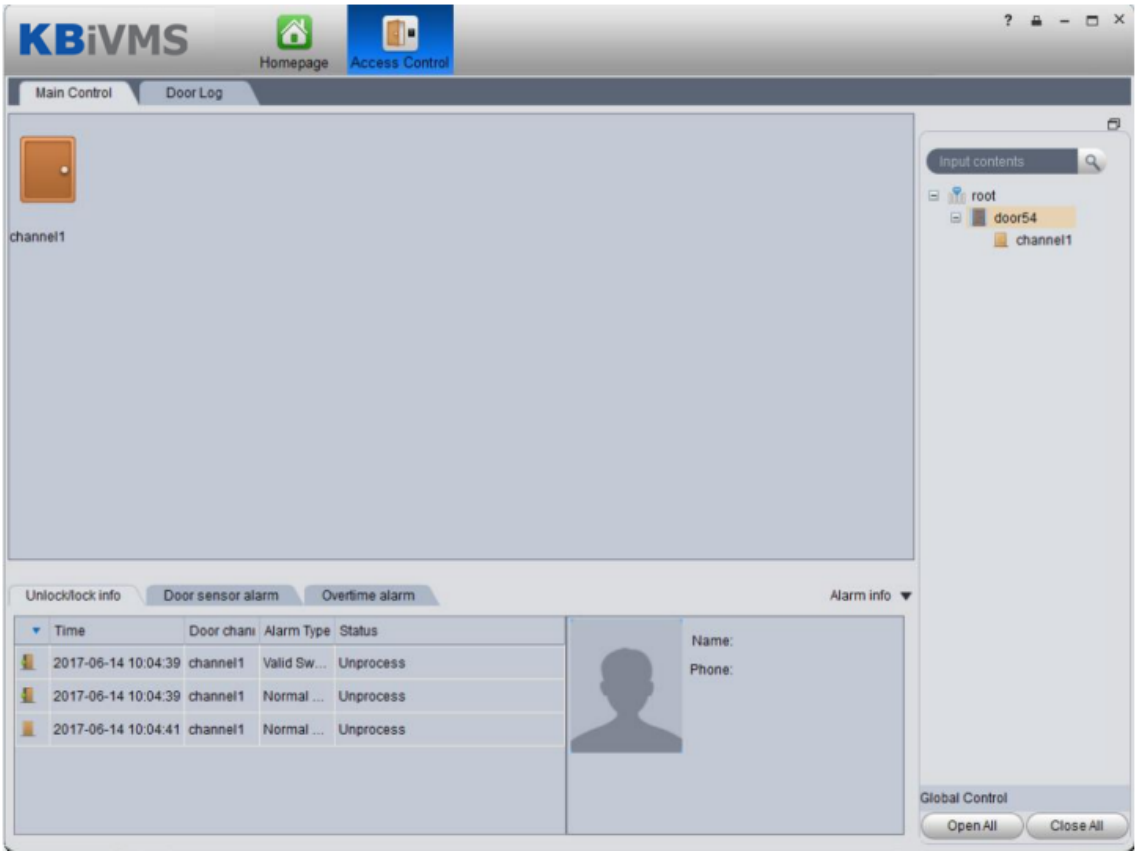


Figure 17-5

You can view unlock unlock info, door sensor alarm, and etc. here.

Step 4. Place mouse on door icon, to show unlock button, such as 

. Click Open Door/Close Door to operate correspondingly.

Step 5. In device tree on the right, right click Unlock, Lock or Door Config, see Figure 17-6.

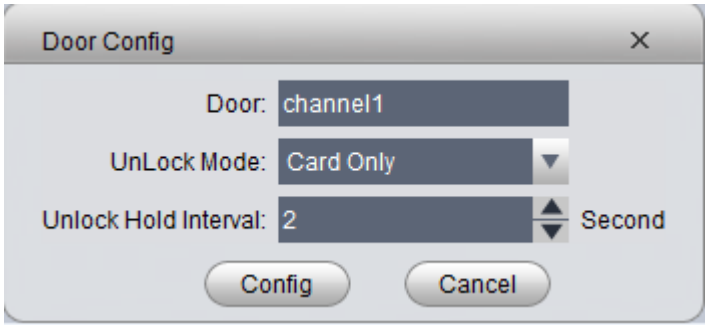


Figure 17-6

Unlock mode includes methods of password, card, password or card.

Step 6. Click Open All, Close All, button to control A&C NO, NC status.

Step 7. Double click alarm record below, you can view alarm details.

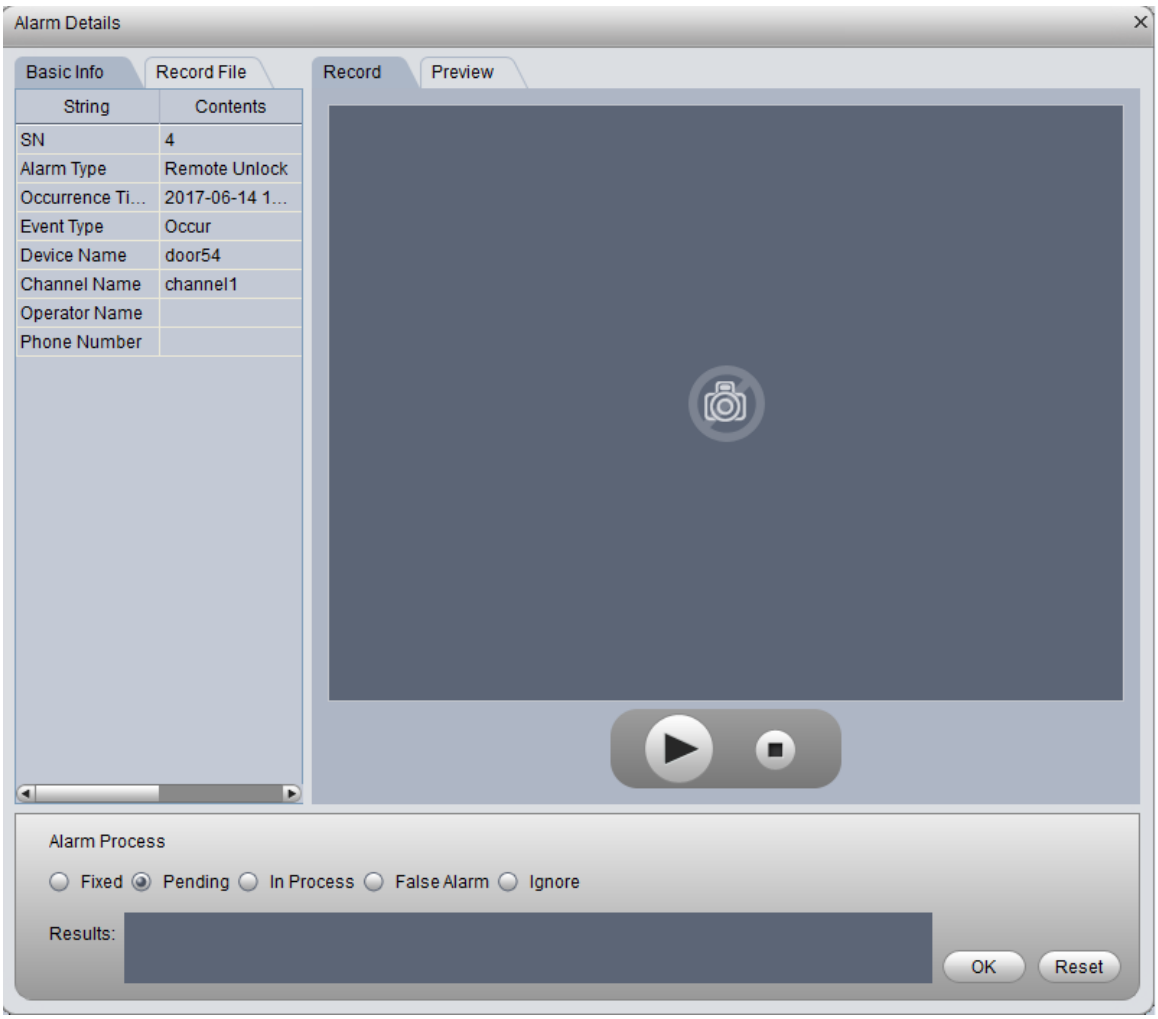


Figure 17-7

17.2.2 **Log**

Step 1. Click Door Log tab in A&C interface.

Step 2. Set search time, select device, event and click Search.

See Figure 17-8.

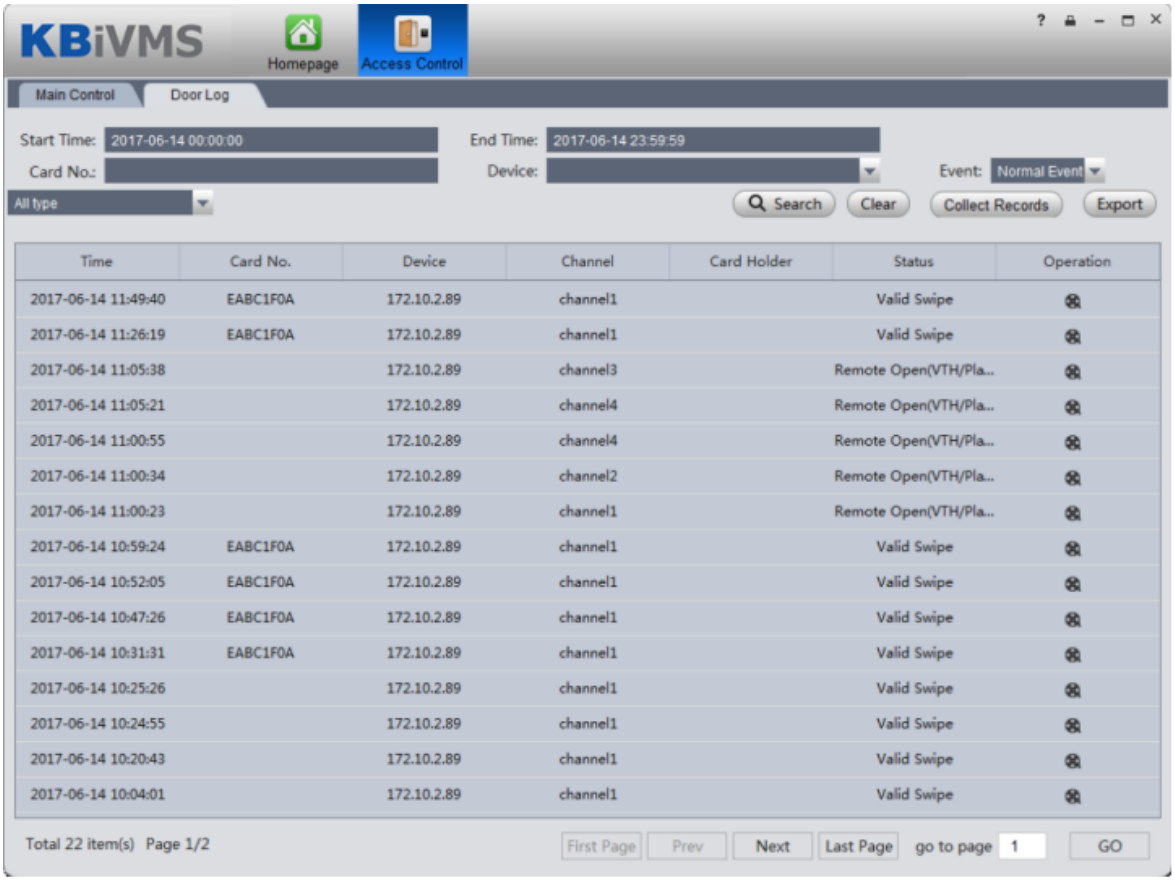


Figure 17-8

Step 3. If you set video link, click , to play record.

If access control device is offline, you can use it as standalone, click Collect Records to sync record during offline period to the platform.

18 Alarm Controller

KBiVMS platform supports to manage alarm controller, and to arm, disarm, bypass alarm controller.

18.1 Add Alarm Controller Device

Step 1. Login KBiVMS Manager.

Step 2. Select General>Device>Alarm Controller.

Step 3. Click Add.

System pops Add Alarm controller box. See Figure 18-1.

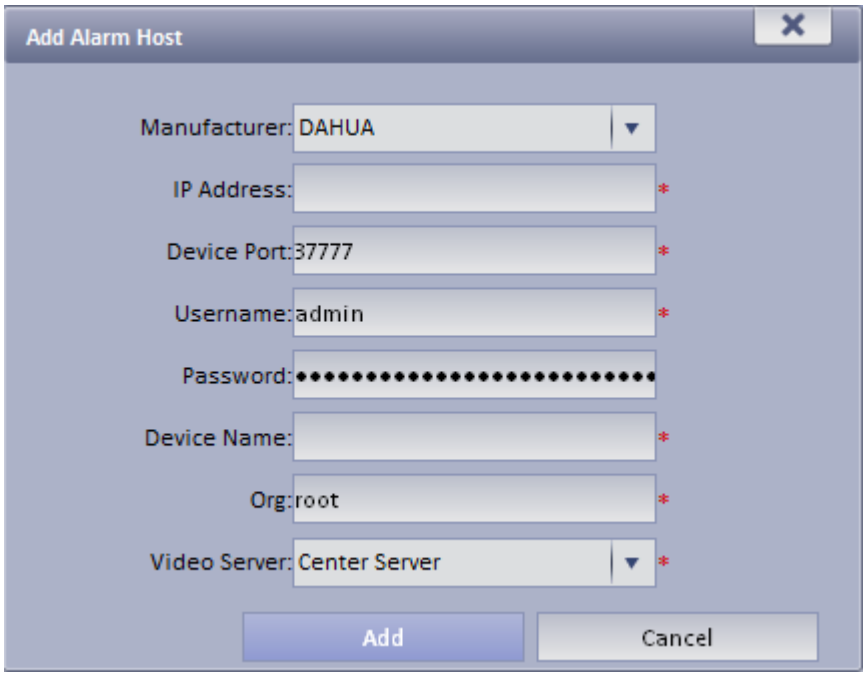


Figure 18-1

Step 4. Enter IP address, device name and etc., click Add. See Figure 18-2.

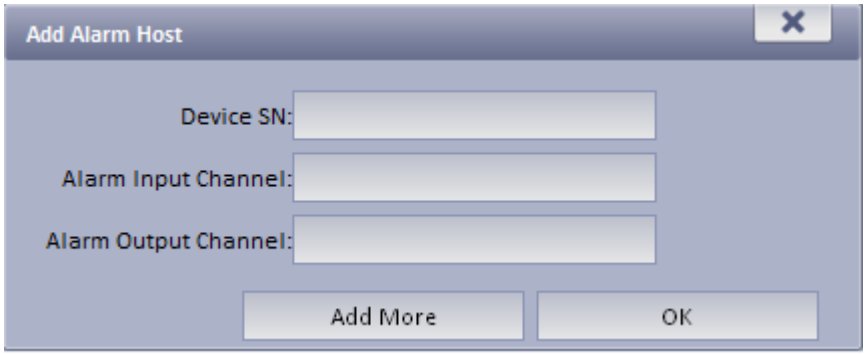


Figure 18-2

Step 5. Enter alarm input channel, alarm output channel, click OK.

Step 6. Refer to Ch 13.1.1 to configure linked video of alarm controller device.

18.2 Alarm Controller

Step 1. Login KBiVMS Client.

Step 2. Click  , system shows Alarm controller interface.

Alarm controller interface shows all added alarm controller device and zone, the shown device status includes online, offline, alarm, bypass, arm and disarm. You can filter device by status.

On the right, select different alarm controllers which lead to different zones. Select root, to show all zones. See Figure 18-3.

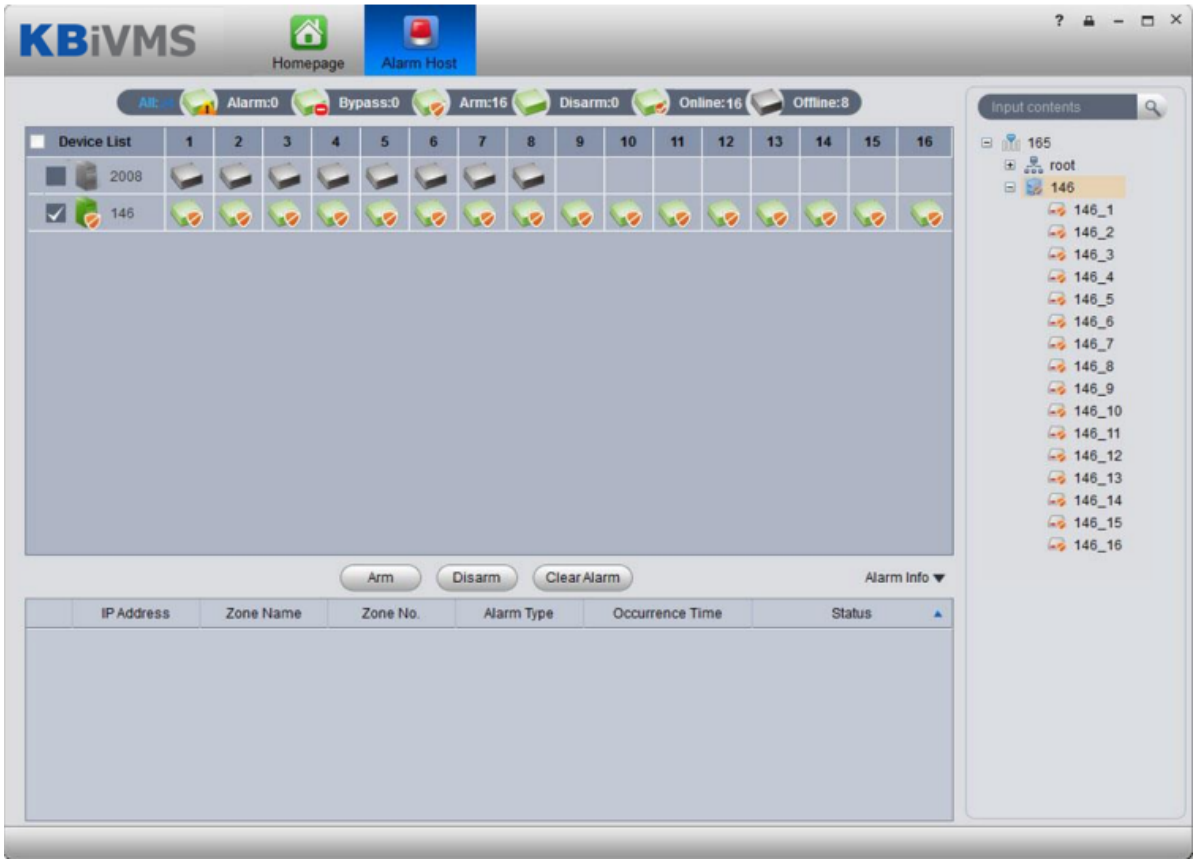


Figure 18-3

You can batch select device and zone to arm and disarm. Double click zone, to view zone details and monitoring video. Double click alarm info, system pops up alarm details page.

You can view current live preview and record video, and process current alarm. Processing status includes processed, pending, in progress, miss-alarmed and ignored. Processes status will be shown in status in alarm info list.

19 Device Config

After you add device in Device interface, you can configure device parameter in Device Config interface.

In homepage, click  or in Device interface, click  of target device to enter Device Config interface. See Figure 19-1.

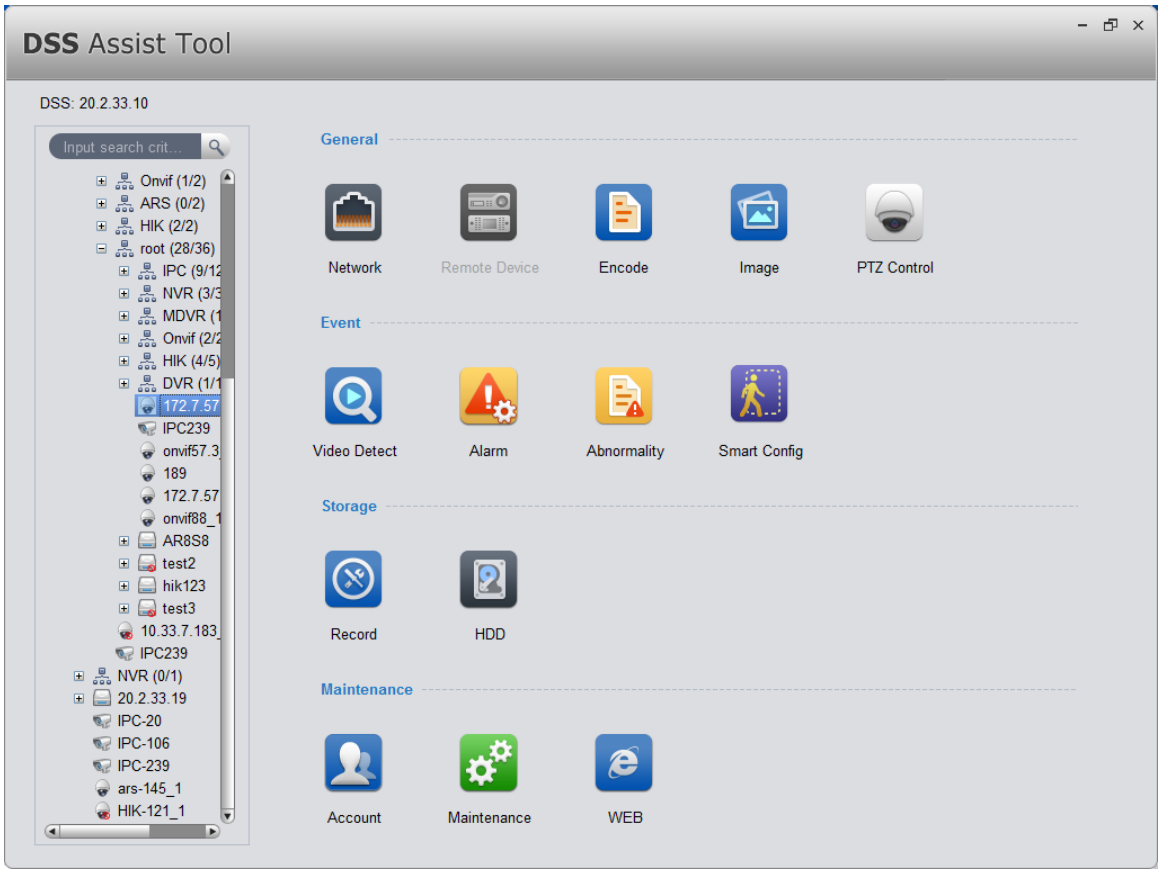


Figure 19-1

19.1 General Setup

19.1.1 Network

You can set network TCP/IP, Connection, PPPoE, DDNS, IP right, SMTP, FTP, multicast, alarm center, ARS, P2P and etc. See Figure 19-2.

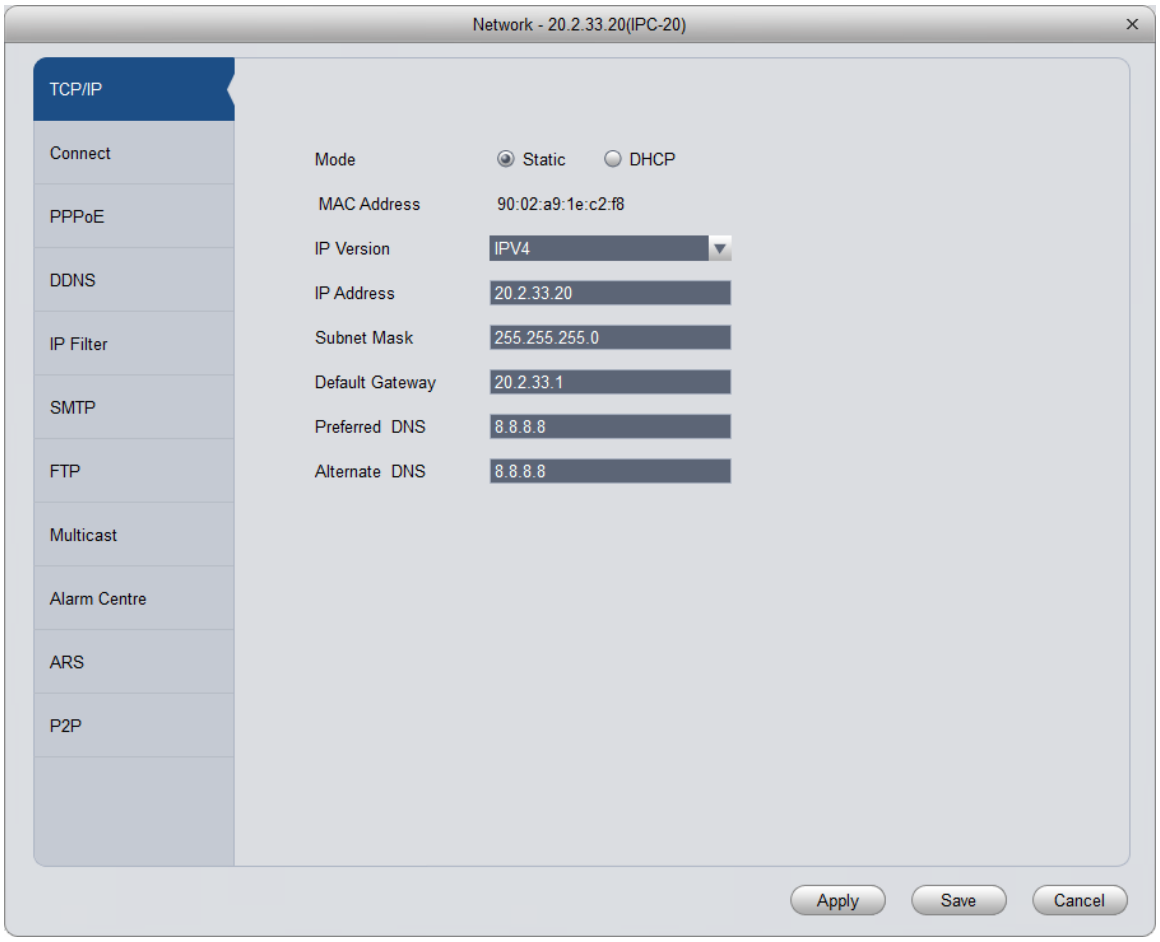


Figure 19-2

19.1.2 **Remote Device**

You can auto search or manually search to add remote device, see Figure 19-3.

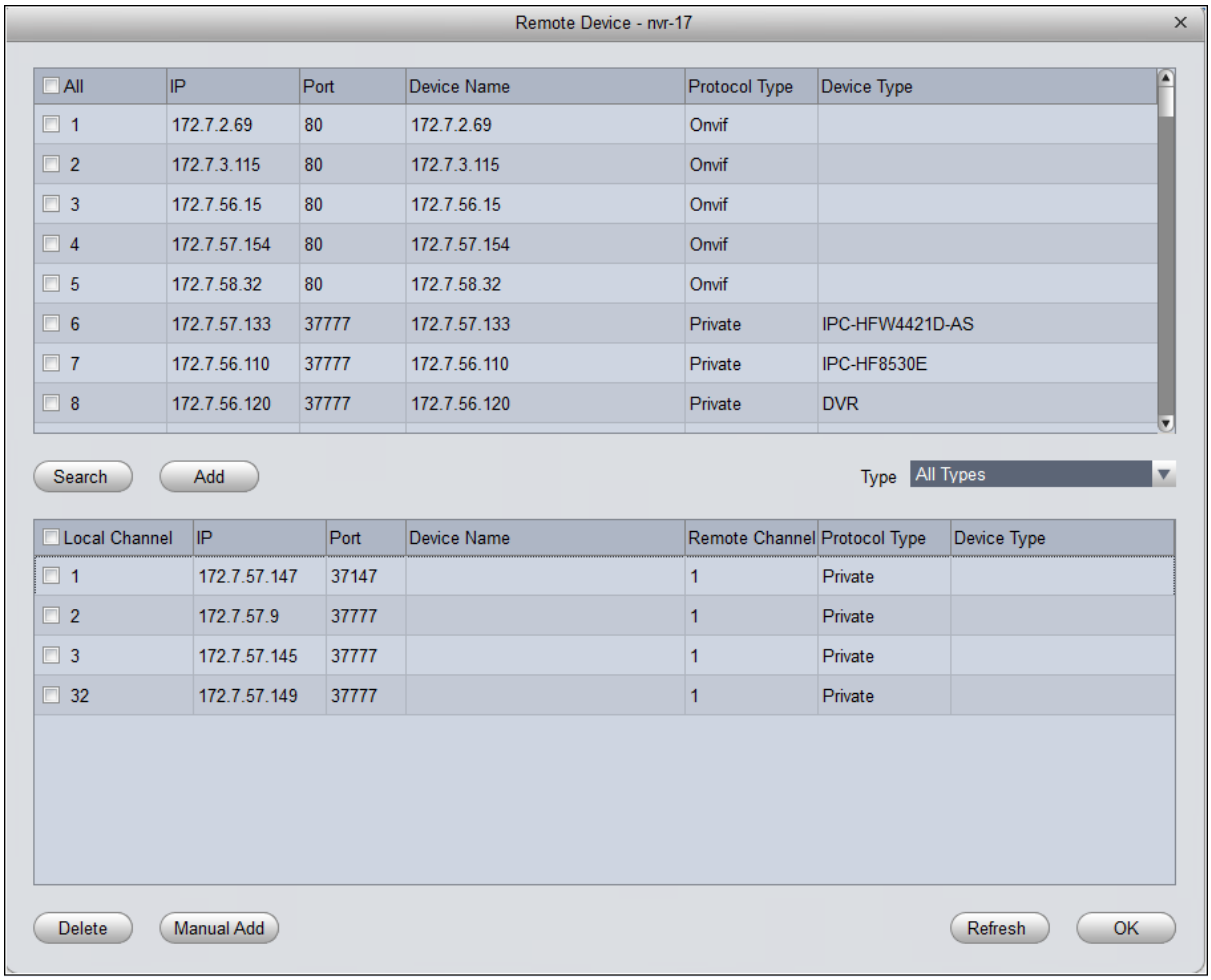


Figure 19-3

Click Device Search, system will show devices that are within the same network segment as this device. For the searched device, click Add to auto add remote device.

Click Manual Add, system pops up add box of remote device, see Figure 19-4. Enter corresponding parameter, and click OK to manually add.

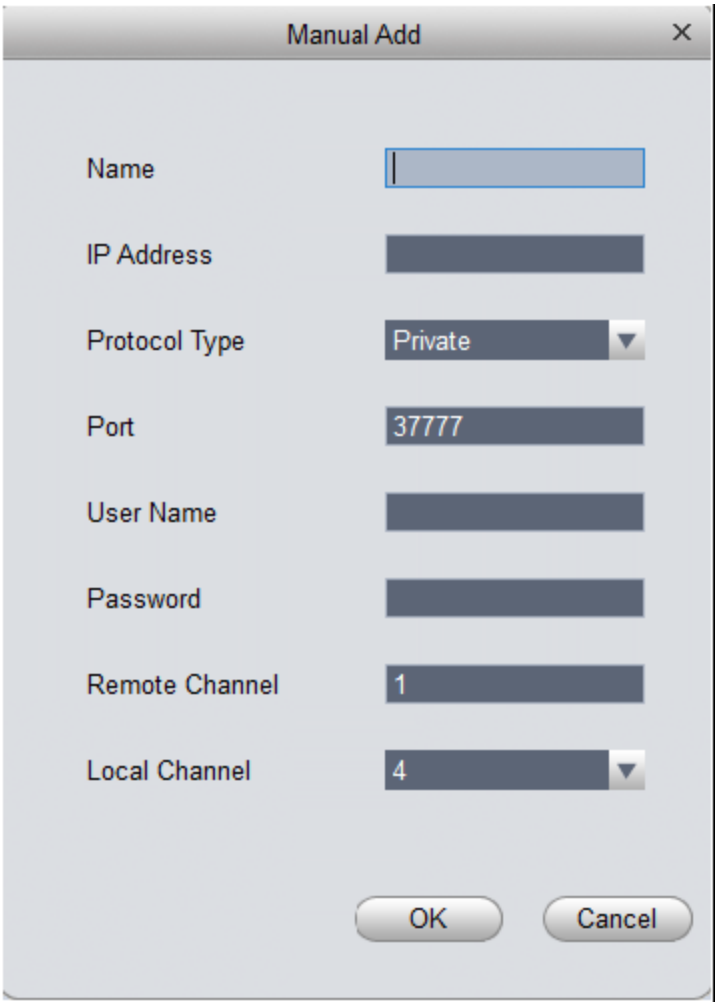


Figure 19-4

19.1.3 **Encode Setup**

You can set device A/V stream, snapshot stream and video overlay.

19.1.3.1 A/V Stream

See Figure 19-5.

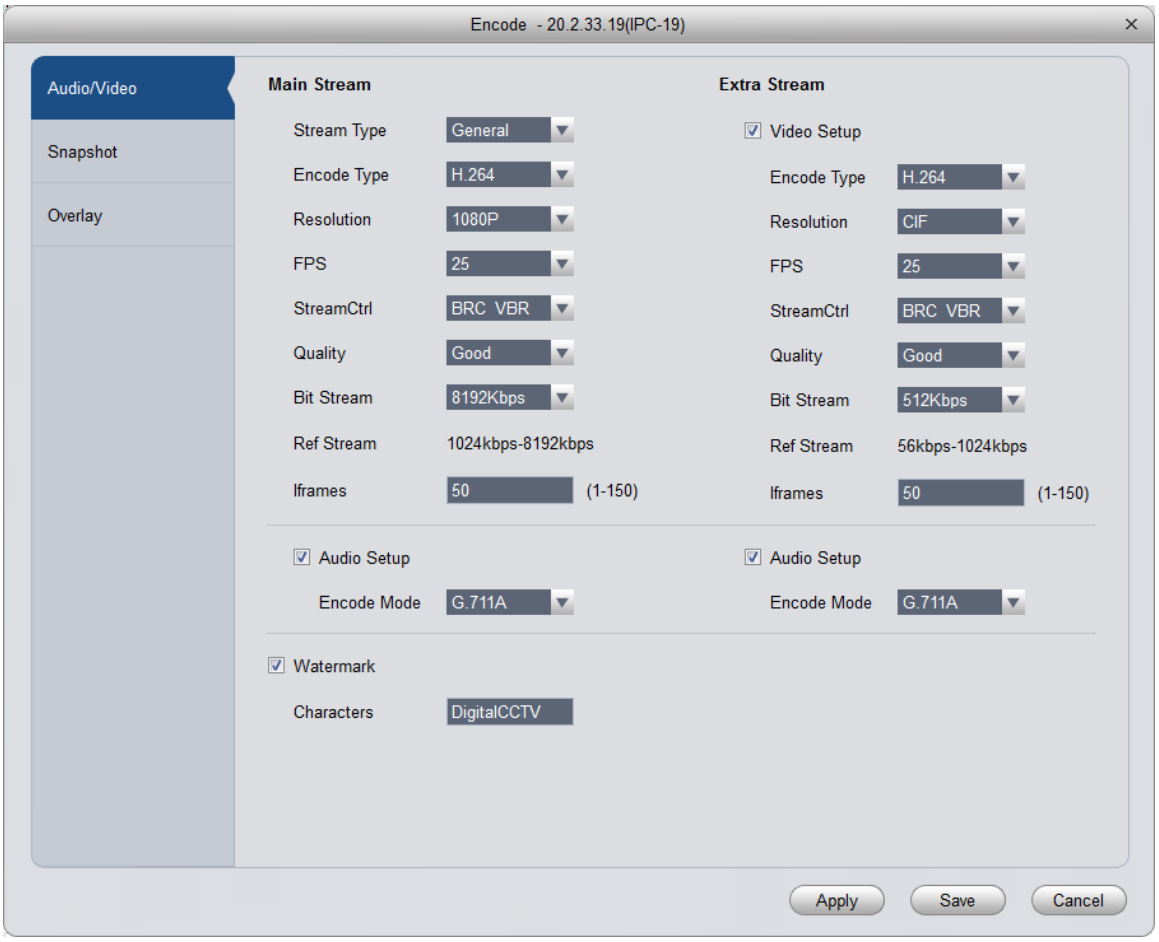


Figure 19-5

Parameter	Note
Stream Type	Include general, motion detection and alarm. Select different steams for different record events.
Encode Type	Auto get audio encode mode from device.
Resolution	Include multiple resolutions, each has different reference streams.
FPS	PAL：1～25 fps, NTSC：1～30 fps.
Stream Control	CBR and VBR.
Bit Stream	Under VBR mode, this value is upper limit; under CBR mode, this value is fixed.
Reference Stream	According to selected encode mode, resolution to dynamicly display stream (range).
I Frames	Time interval between key frames. 。

Parameter	Note
Audio Setup	Select this frame, then enable audio setup.
Encode Mode	Device audio encode method.
Watermark	Select this parameter, then enable watermark function.
Watermark Character	Via watermark character, you can see whether the video has been tampered. Enable option for watermark.

19.1.3.2 Snapshot Stream

See Figure 19-6.

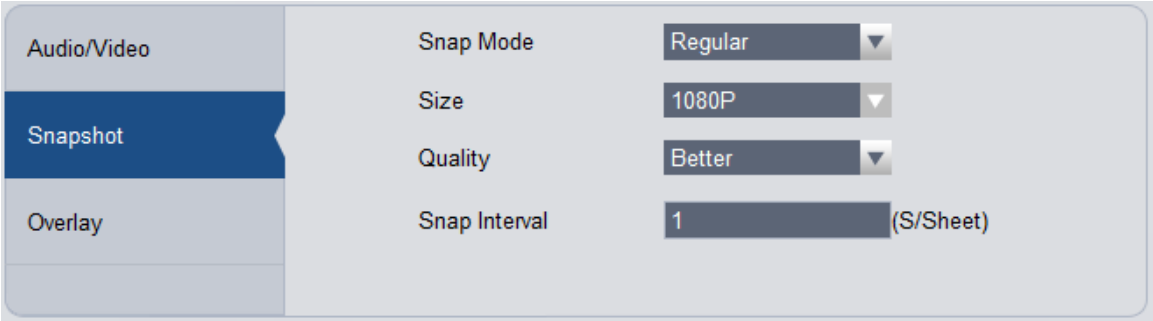


Figure 19-6

Parameter	Note
Snap Mode	Available parameter： ● Regular：in snapshot plan, snapshot within set time range. ● Motion Detect：snapshot when motion is detected. ● Alarm：snapshot when alarms.
Size	Identical with main stream resolution.
Quality	Set quality of snapshot.
Snap Speed	Set frequency of snapshot.

19.1.3.3 Video Overlay

See Figure 19-7.

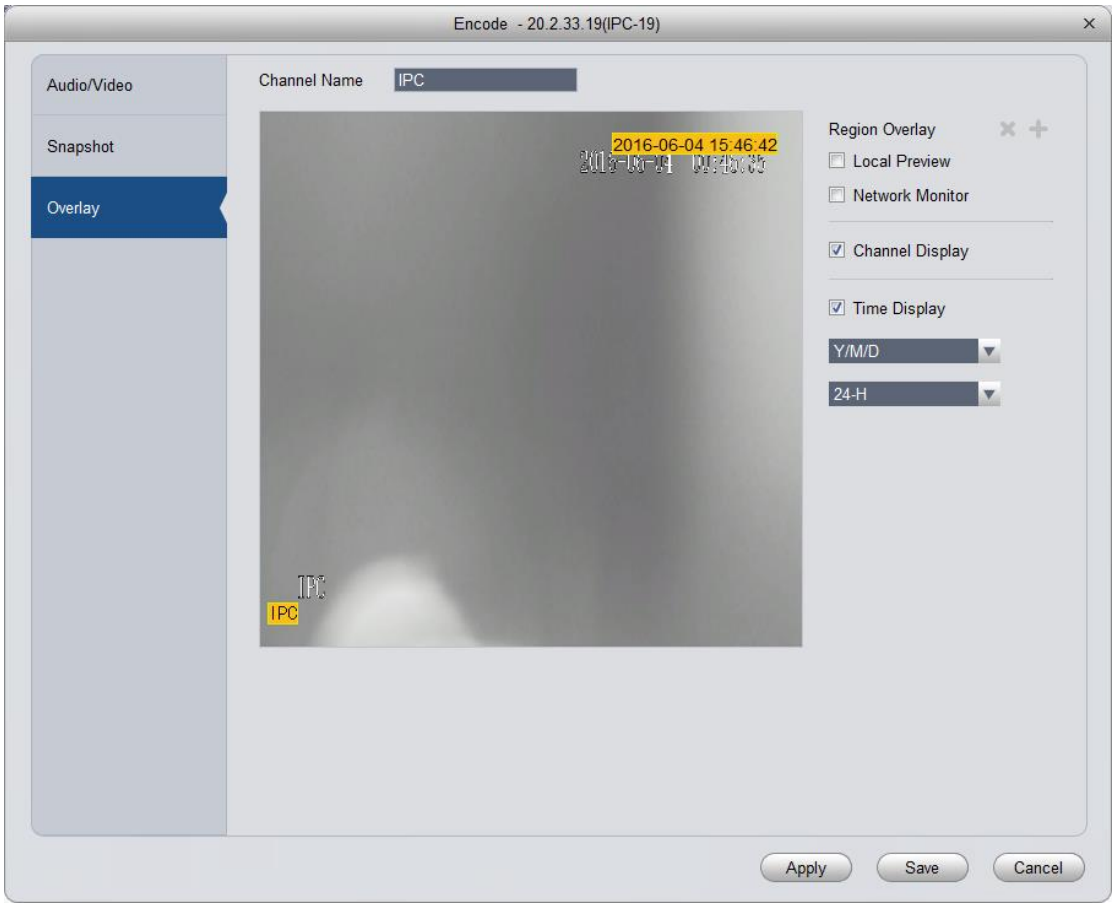


Figure 19-7

Parameter	Note
Channel Name	Set channel name.
Region Overlay	Shield video of specific area in live preview window. Available parameters： • Local preview：shield specific region video in local preview video. • Network monitor：shield specific region video in network monitor. Select “local preview” or “network monitor”, and click ，to configure shielded region.
Channel Display	If you select this parameter, then it will show channel name in video 如 monitor window.
Time Display	If you select this parameter, then it shows time info in video monitor 如 window.

19.1.4 **Image Setup**

You can set video’s color mode, HUE, brightness, contrast and saturation. See Figure 19-8.

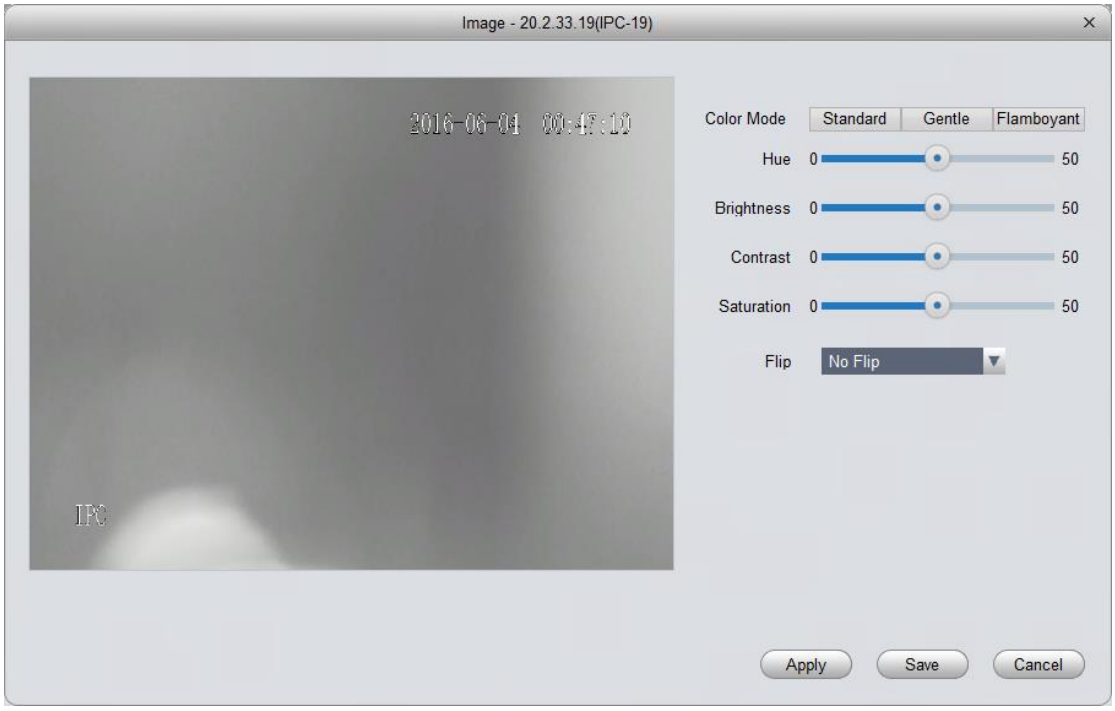


Figure 19-8

Parameter	Note
Color Mode	Set color mode.
HUE	Adjust color HUE.
Brightness	Adjust overall color brightness. The higher the value, the higher the brightness will be. If you increase image brightness, the entire video will be affected including both dark and bright areas.
Contrast	Adjust contrast. The higher the value, the higher the contrast will be.
Saturation	Adjust color depth. The higher the value, the deeper the color will be.
Flip	Viewing angle. You can select among four modes.

19.1.5 **PTZ Config**

See Figure 19-9.

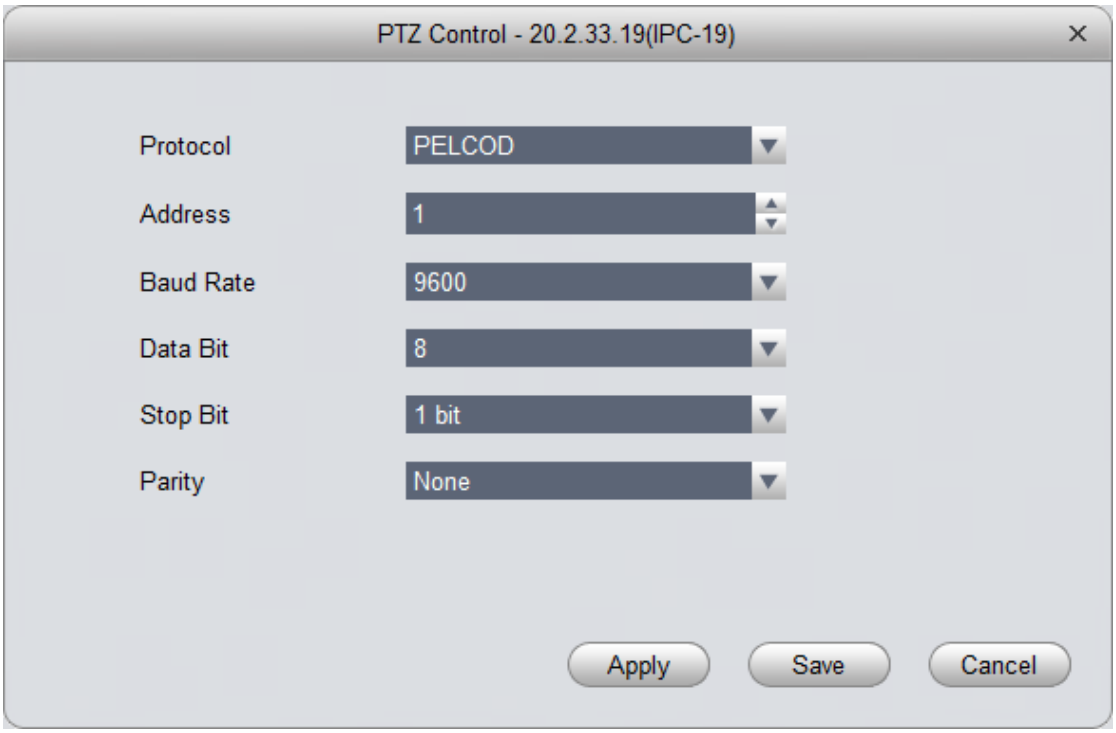


Figure 19-9

Parameter	Note
Protocol	Select protocol of corresponding model, such as PELCOD.
Address	Set speed dome address.
Baud Rate	Select corresponding speed dome's baud rate, and you control corresponding channel PTZ and camera.
Data Bit	Set corresponding data value.
Stop Bit	Set stop bit.
Parity	Select parity.

19.2 **Event**

19.2.1 **Video Detection**

Video detection includes video loss, video tampering and motion detect. While:

- Video loss: when a channel loses video, it will prompts video loss via alarm output, alarm upload, screen prompt, and SMS.
- Video tampering: when someone tampers camera or video is not clear due to light issue, video tamper alarm is ON.

Note:

Enable defocus detect: detect defocus video.

- Motion detection: by analyzing video image, when system detects moving signal which has

reached preset sensitivity, it enables motion detection alarm.

For example see Figure 19-10 as motion detection.

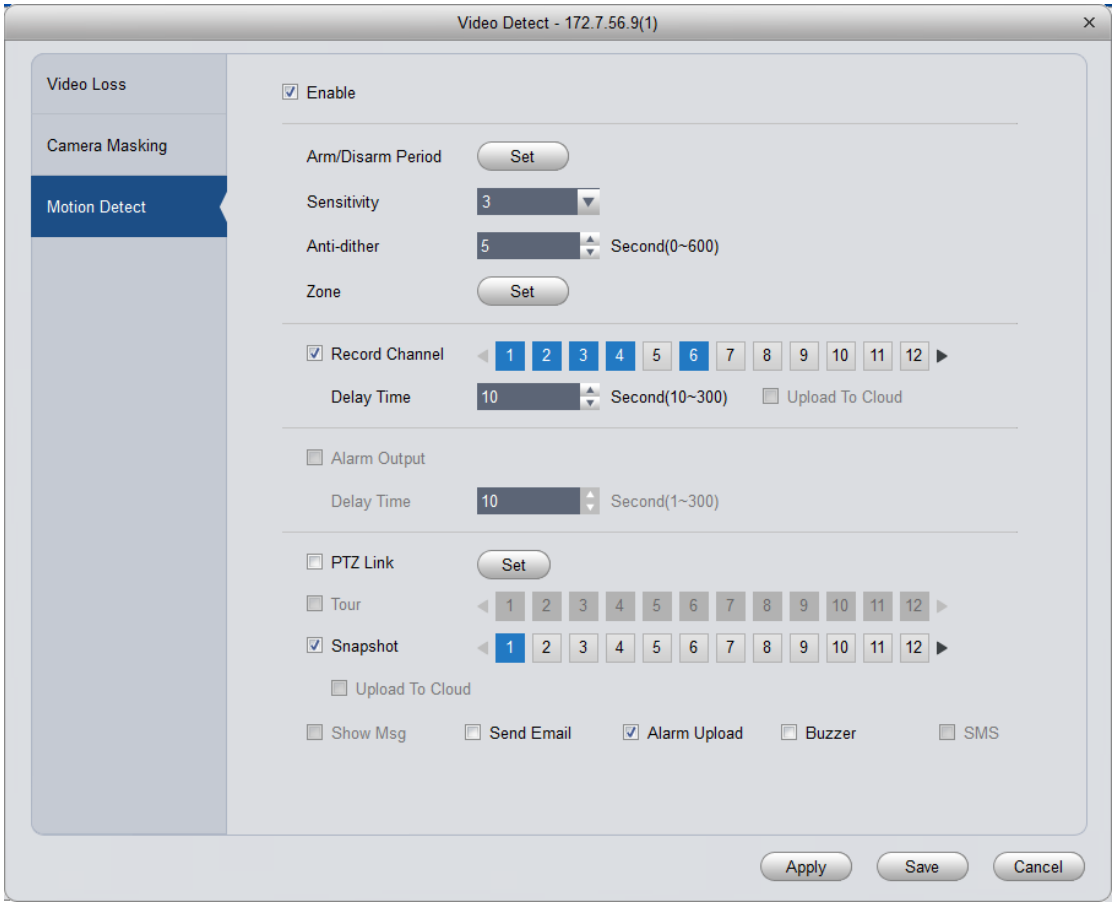


Figure 19-10

Parameter	Note
Enable	If you select this parameter, then you can perform motion detection.
Arm/Disarm Period	Set alarm arm and disarm time. Click setup to pop up arm/disarm period box.
Anti-dither	The anti-dither period only can record one time of motion detection event. Value within 0s～600s.
Zone	• Click Set to enter, blue zone is motion detection zone. (center in figure) • When exit the interface, you must click OK to save motion detect setup.
Record Channel	If you select this parameter, then you can perform motion detection alarm record to this channel. Meantime you must select auto record in Record>Record Control.
Delay Time	When motion detection ends, it will extend for a while before stop.

Parameter	Note
Upload to Cloud	Check, means to upload record to cloud.
Alarm Output	If you select this parameter, then enable alarm link output port, so it can link corresponding alarm output device when alarm occurs.
Output Deploy	After motion detection alarm ends, alarm extends for a while before stop.
PTZ Link	When motion detection occurs, link PTZ, such as rotate to point X. PTZ config event type includes: preset, point tour and pattern.
Tour	If you select this parameter, then enable tour channel function.
Snapshot	If you select this parameter, then config motion detection snapshot function for this channel.
Screen Prompt	If you select this parameter, then when alarm occurs, screen has prompt.
Send EMAIL	If you select this parameter, then when alarm occurs, send mail to user.
Alarm Upload	If you select this parameter, then when alarm occurs, upload alarm.
Buzzer	If you select this parameter, then when alarm occurs, buzzer.
SMS	If you select this parameter, then when alarm occurs, send SMS to user.

19.2.2 **Alarm Setup**

See Figure 19-11.

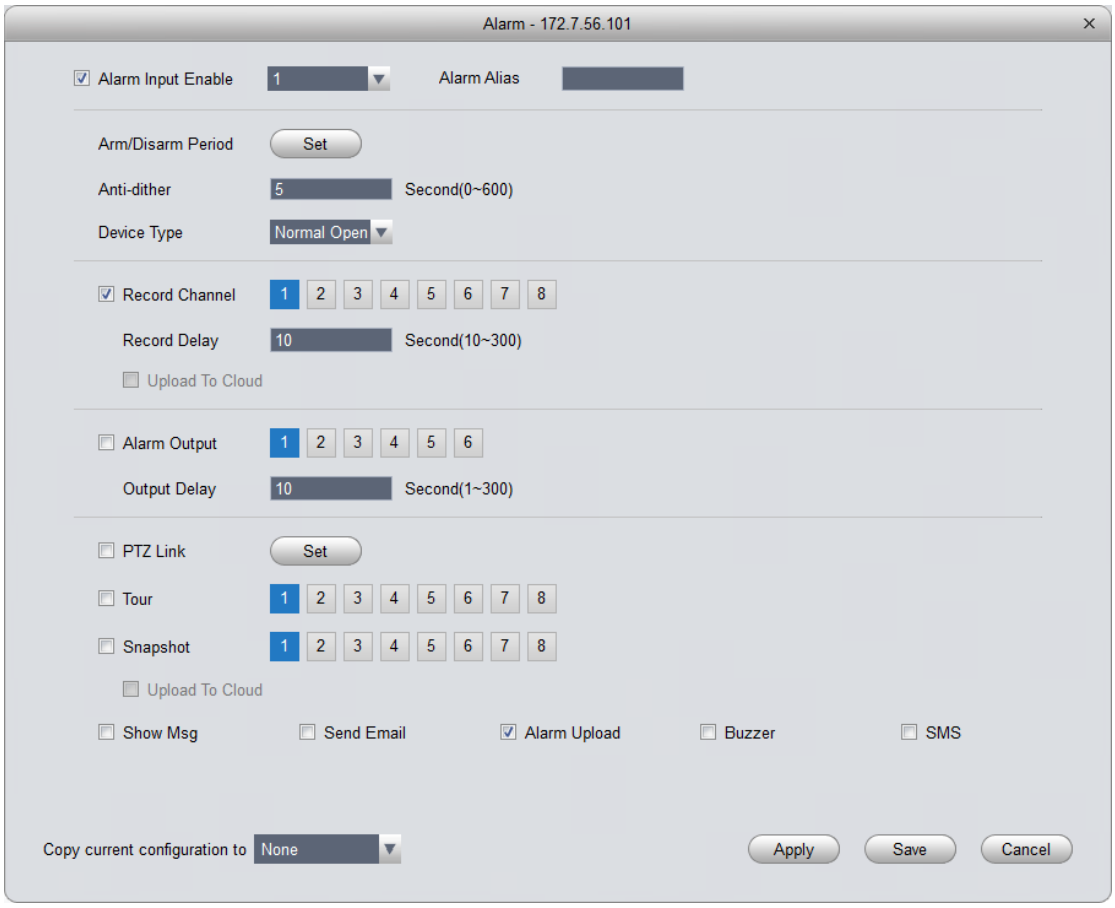


Figure 19-11

Parameter	Note
Alarm Input Enable	If you select this parameter, then it will link to alarm.
Arm/Disarm Period	Set alarm arm and disarm time. Click setup to pop up arm/disarm period box.
Anti-dither	The anti-dither period only can record one time of motion detection event. Value within 0s～600s.
Device Type	Set to NO or NC.
Record Channel	If you select this parameter, then you can perform motion detection alarm record to this channel. Meantime you must select auto record in Record>Record Control.
Record Delay	When alarm link ends, it will extend for a while before stop.
Upload to Cloud	Check, means to upload record to cloud.

Parameter	Note
Alarm Output	If you select this parameter, then enable alarm link output port, so it can link corresponding alarm output device when alarm occurs.
Output Delay	After motion detection alarm ends, alarm extends for a while before stop.
PTZ Link	When alarm link occurs, link PTZ, such as rotate to point X. PTZ config event type includes: preset, point tour and pattern.
Tour	If you select this parameter, then enable tour channel function.
Snapshot	If you select this parameter, then config alarm link snapshot function for this channel.
Video Matrix	If you select this parameter, then enable matrix.
Show Message	If you select this parameter, then when alarm occurs, screen shows message.
Send EMAIL	If you select this parameter, then when alarm occurs, send mail to user.
Alarm Upload	If you select this parameter, then when alarm occurs, upload alarm.
Buzzer	If you select this parameter, then when alarm occurs, buzzer.
SMS	If you select this parameter, then when alarm occurs, send SMS to user.

19.2.3 **Abnormality**

When an abnormality (i.s. no storage device, capacity warning, storage device error, offline) occurs, by enabling alarm output function, select alarm output channel, set corresponding alarm format, create alarm to notify user. For example no storage device is in Figure 19-12.

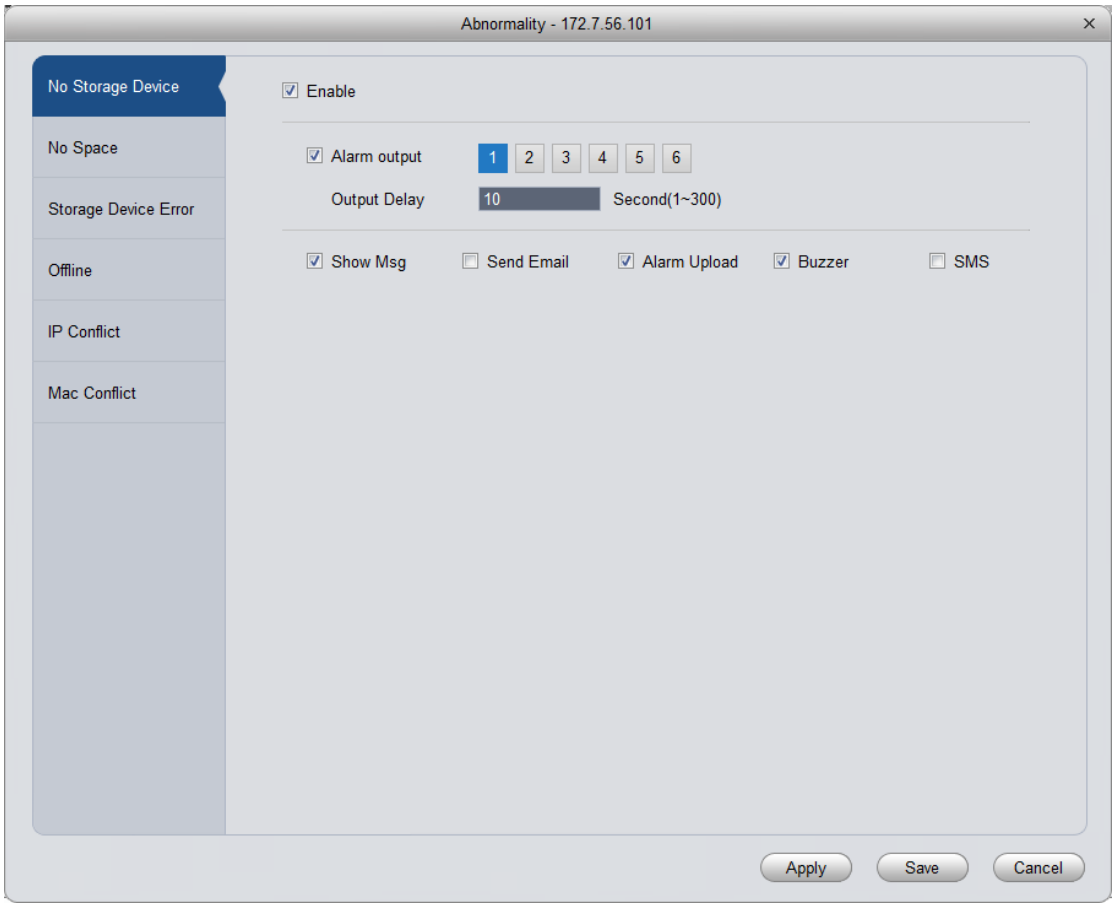


Figure 19-12

19.2.4 **Intelligent Config**

KBiVMS supports to add SmartIPC and you may configure added intelligent device, including audio detection config and face detection fig. After config is finished, you can to go Live preview, see Ch 5.

See Figure 19-13.

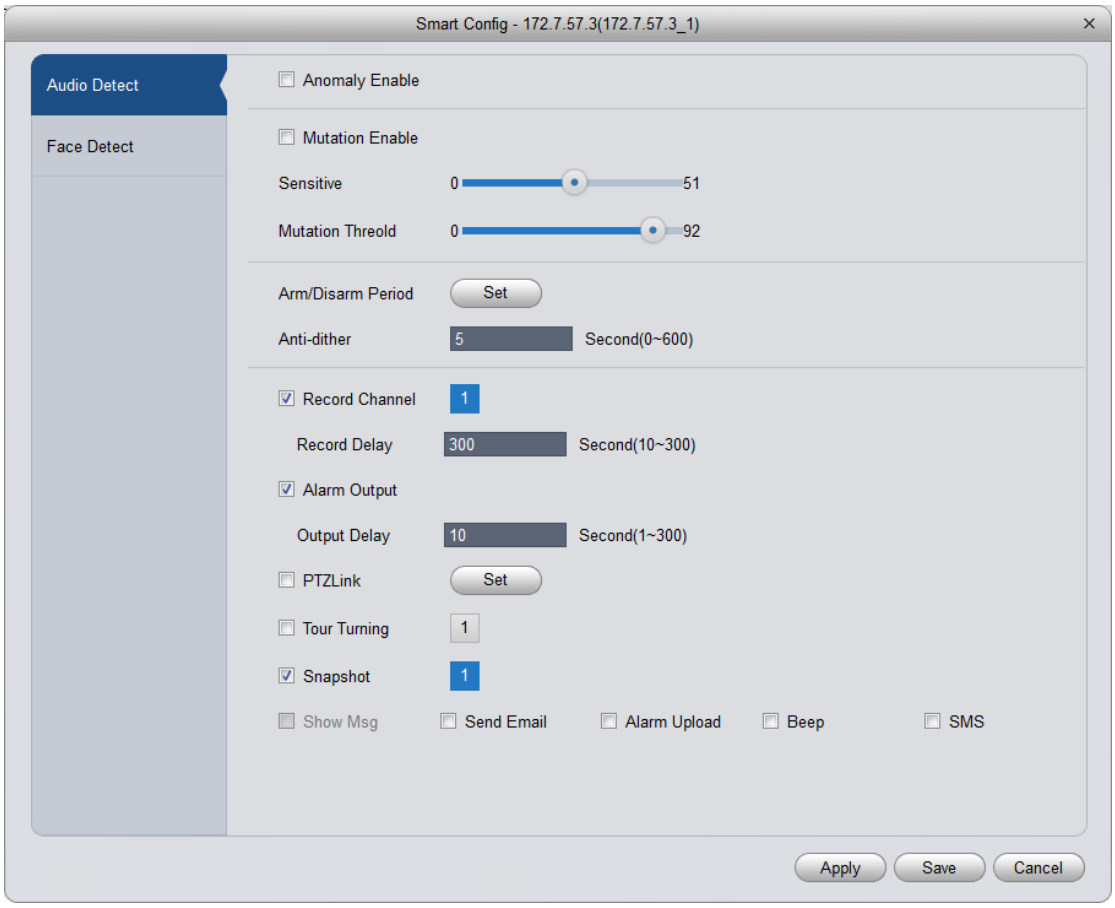


Figure 19-13

Parameter	Note
Anomaly Enable	If you select this parameter, then enable audio detection alarm.
Mutation Enable	You can set sensitivity and threshold. If you select this parameter, enable mutation. sensitivity： 1-100 level adjustable, the smaller the value, then the more input sound volume change needs to exceed continuous environmental volume for being judged as audio abnormality. User shall test and adjust according to actual environment. Mutation threshold：1-100 level adjustable, used to set filter environment sound intensity. If environmental noise is higher, then you shall set this value higher. User shall test and adjust according to actual environment.
Arm/Disarm Period	Set alarm arm and disarm time. Click “setup” to pop up “Arm/Disarm Period” box.
Anti-dither	Within one anti-dither period, it only records one time motion detection event. Value within 0s～100s.

Parameter	Note
Record Channel	If you select this parameter, then you can perform motion detection alarm record to this channel. Meantime you must select auto record in Record>Record Control.
Record Delay	When alarm link ends, it will extend for a while before stop.
Alarm Output	If you select this parameter, then enable alarm link output port, so it can link corresponding alarm output device when alarm occurs.
Output Delay	When alarm link ends, alarm extend for a while before stop.
Snapshot	If you select this parameter, then config motion detection snapshot for the channel.
Send EMAIL	If you select this parameter, then when alarm occurs, send mail to user.
Alarm Upload	If you select this parameter, then when alarm occurs, upload alarm.
Buzzer	If you select this parameter, then when alarm occurs, buzzer.
SMS	If you select this parameter, then when alarm occurs, send SMS to user.

For face detection config, see Figure 19-14.

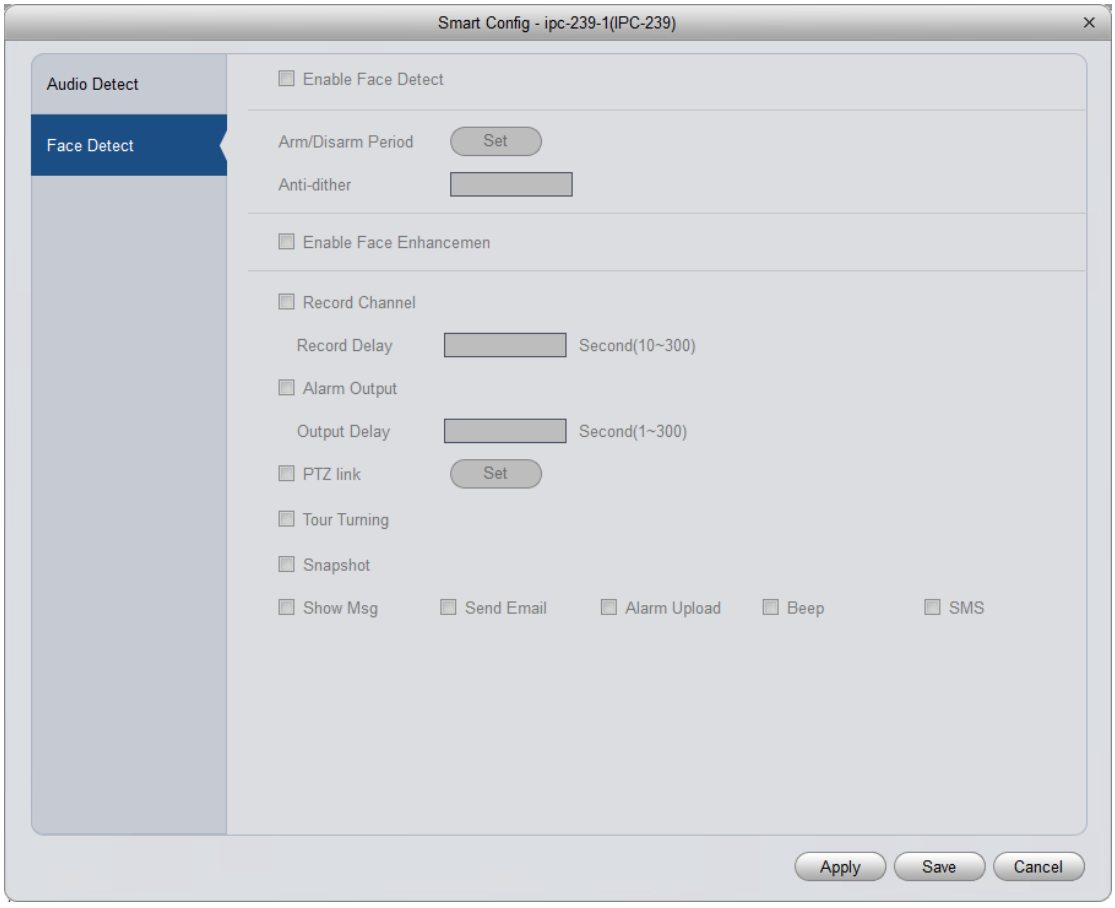


Figure 19-14

Parameter	Note
Enable Face Detect	If you select this parameter, then alarm links.
Arm/Disarm Period	Set alarm arm/disarm period. Click Set to pop up arm/disarm box.
Enable Face Enhancement	If you select this parameter, then enable face detection.
Record Channel	If you select this parameter, then you can perform motion detection alarm record to this channel. Meantime you must select auto record in Record>Record Control.
Record Delay	When alarm link ends, it will extend for a while before stop.
Alarm Output	If you select this parameter, then enable alarm link output port, so it can link corresponding alarm output device when alarm occurs.
Output Delay	When alarm link ends, alarm extends for a while before stop.
Snapshot	If you select this parameter, then config motion detection snapshot for the channel.
Send EMAIL	If you select this parameter, then when alarm occurs, send mail to user.
Alarm Upload	If you select this parameter, then when alarm occurs, upload alarm.
Buzzer	If you select this parameter, then when alarm occurs, buzzer.
SMS	If you select this parameter, then when alarm occurs, send SMS to user.

19.3 **Record/Storage**

19.3.1 **Record Setup**

Record setup has schedule and record control.

- Schedule: system records at set time period.
- Record control: select record mode.

19.3.1.1 Schedule

You can set corresponding record time, and record during the set period. Example is as below:

Step 1. Select Storage>Record. See record setup interface.

Step 2. Select Schedule. See Figure 19-15.

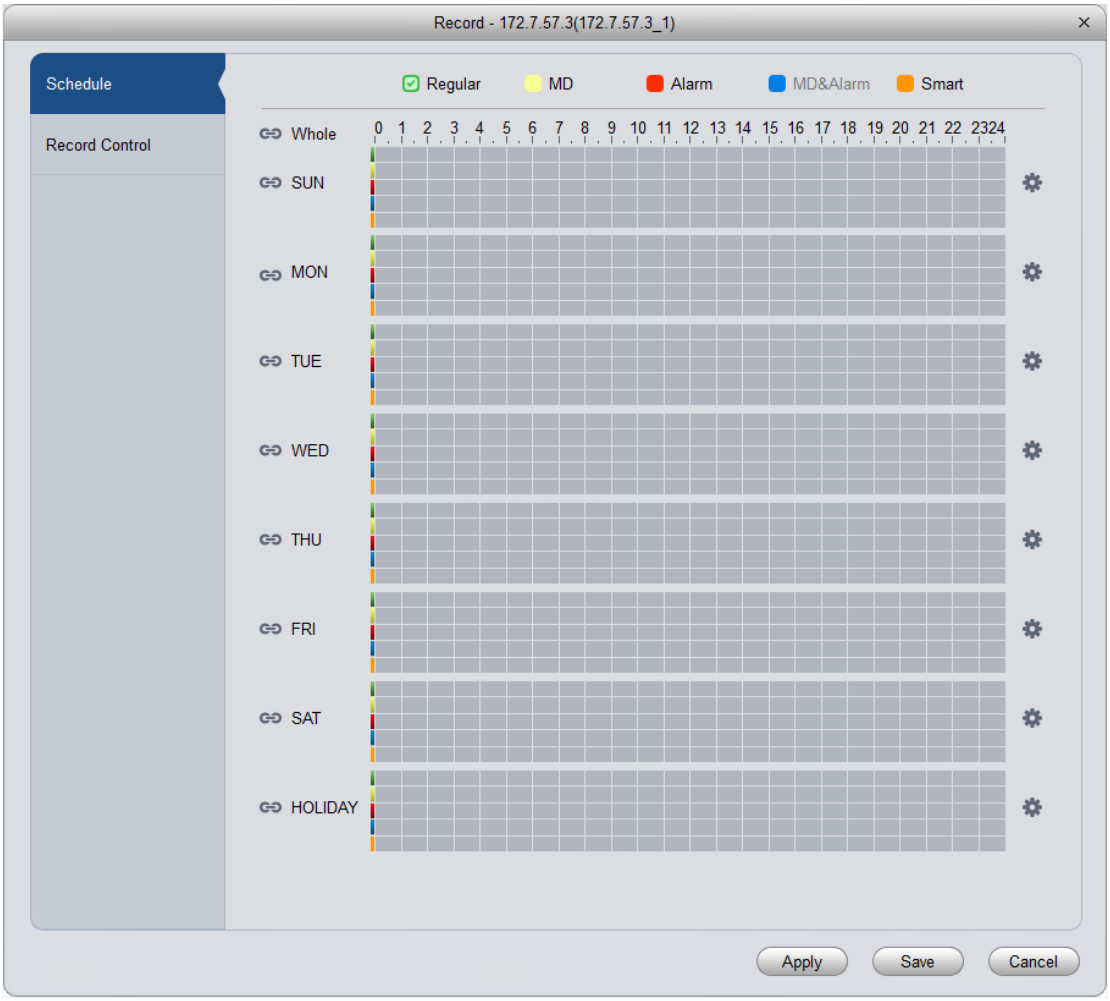


Figure 19-15

Step 3. Click . See Figure 19-16.

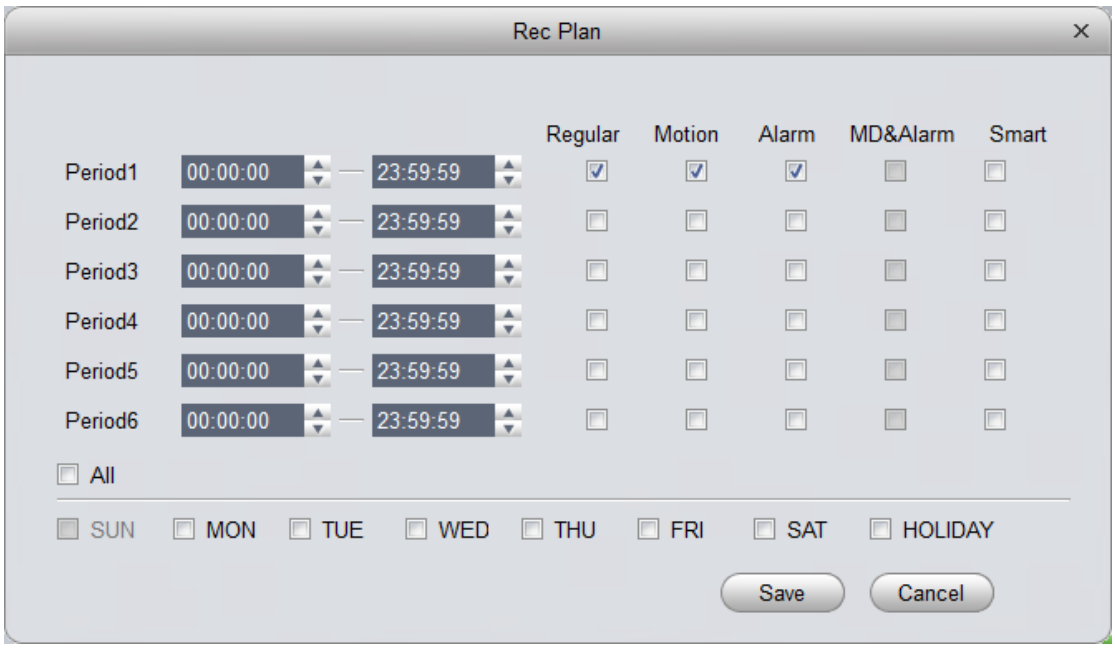


Figure 19-16

Step 4. Set period you want to record, select record type, and click OK.

See Figure 19-17.

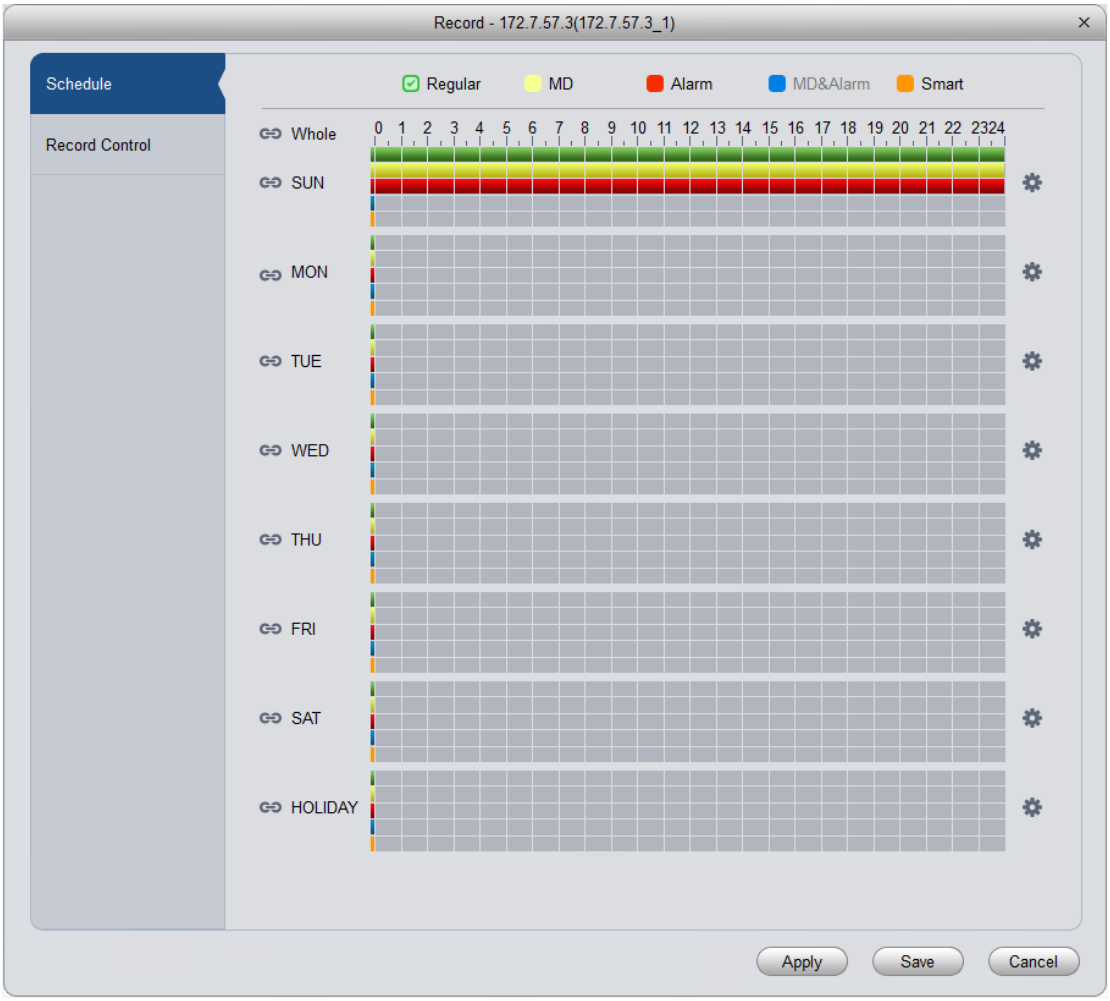


Figure 19-17

Note:

- Green: normal record.
- Yellow: motion detection triggered record.
- Red: alarm triggered record.
- Blue: motion detection and alarm record.
- Orange: intelligent alarm record.

You can click Apply to copy current config to other channels.

19.3.1.2 Record Control

You can select record mode, see Figure 19-18.

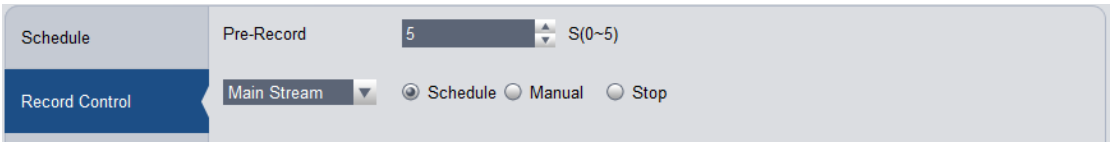


Figure 19-18

Parameter	Note
Pre-record	During certain period of time, records are stored in memory. For example, pre-record is 4 seconds, then record in the first 4 seconds are stored in memory and records start from the 5th second are stored locally.
Main Stream	Set main stream record mode. Available modes are auto, manual and OFF.
Sub Stream	Set sub stream record mode. Available modes are auto, manual and OFF.

19.3.2 Disk Management

You can manage local storage and remote storage.

Local Storage

Store data in local SD card or disk, meantime you can view healthy condition of disk, see Figure 19-19.

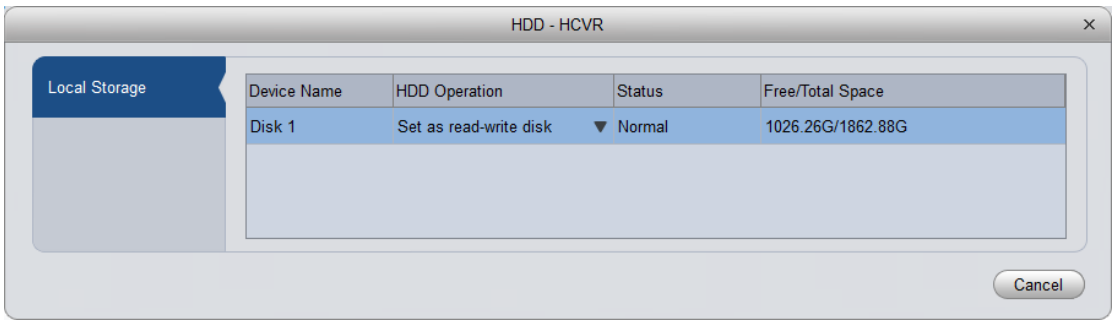


Figure 19-19

19.4 System Maintenance

19.4.1 User Management

You can add, modify, delete user group and use. System default user groups include admin and user.

Default users are admin, 888888, and 666666.

To add user:

Step 1. Select Maintenance>Account. It shows User interface.

Step 2. Select group and click Add.

System pops up Add Group box, see Figure 19-20.

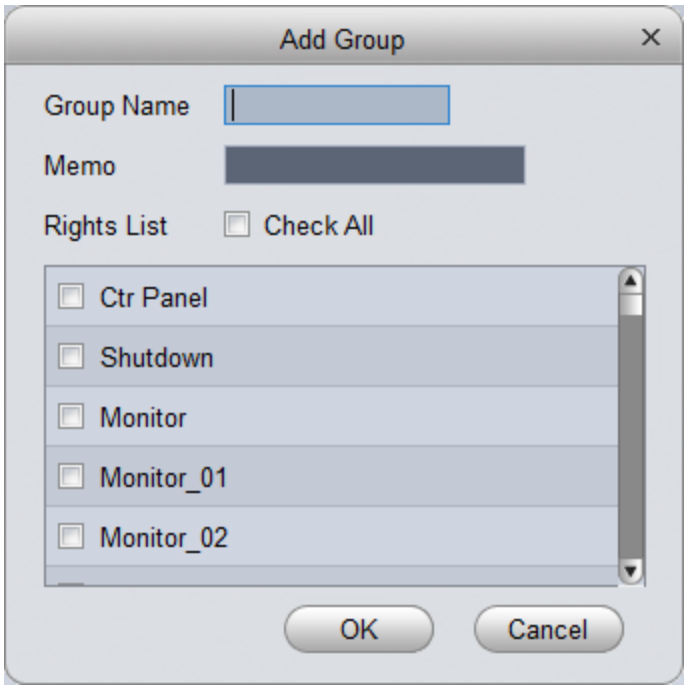


Figure 19-20

Step 3. Enter user group name, select corresponding right, and click OK.

Step 4. Select user, and click Add. See Figure 19-21.

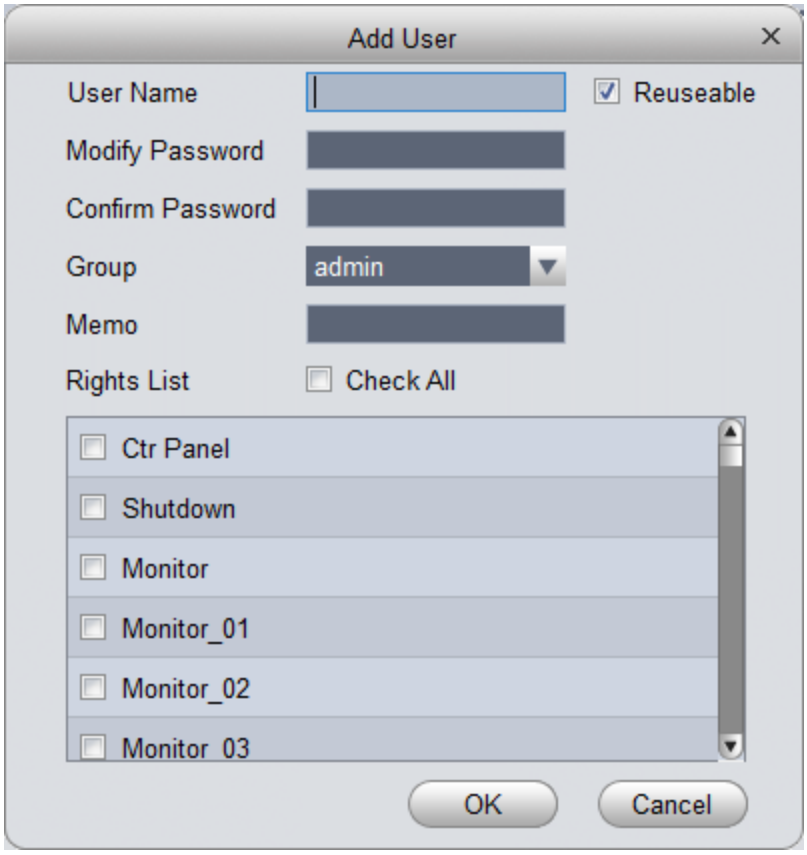


Figure 19-21

Step 5. Enter corresponding parameter, select right and click OK.

Note:

Username and password in access controller are fixed, which are “123456”.

19.4.2 System Maintenance

19.4.2.1 Local Setup

See Figure 19-22.

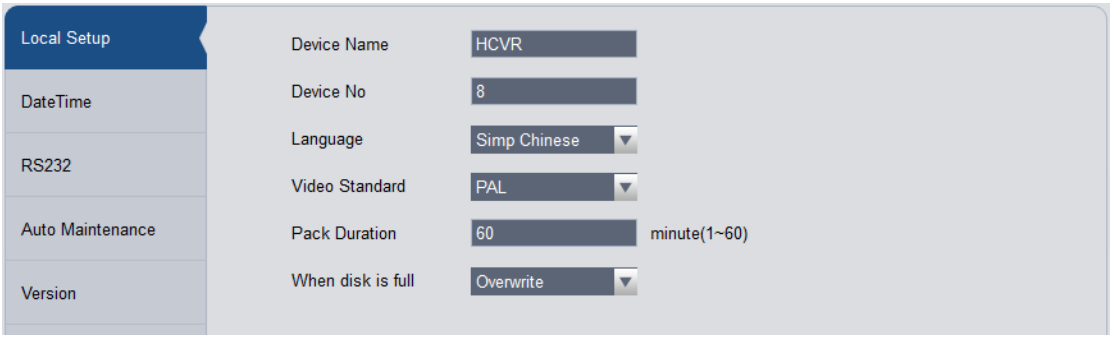


Figure 19-22

Parameter	Note
Device Name	Set device name.
Device No.	Device no. in remote control app. Used to in scene when one remote control controls multiple devices. Only when you press address button on remote control and enter remote control address and device no. are the same with corresponding device before you can operate.
Language	Show device system language.
Video Standard	Show video standard of device.
Pack Duration	Set pack duration of each record file. Default is 60 minutes.
When disk is full	Available parameters: ● Stop, current work disk is overwriting, or current disk is just full, it stops record. ● Overwrite, when current disk is full, it will overwrite the earliest record file.

19.4.2.2 Time Setup

See Figure 19-23.

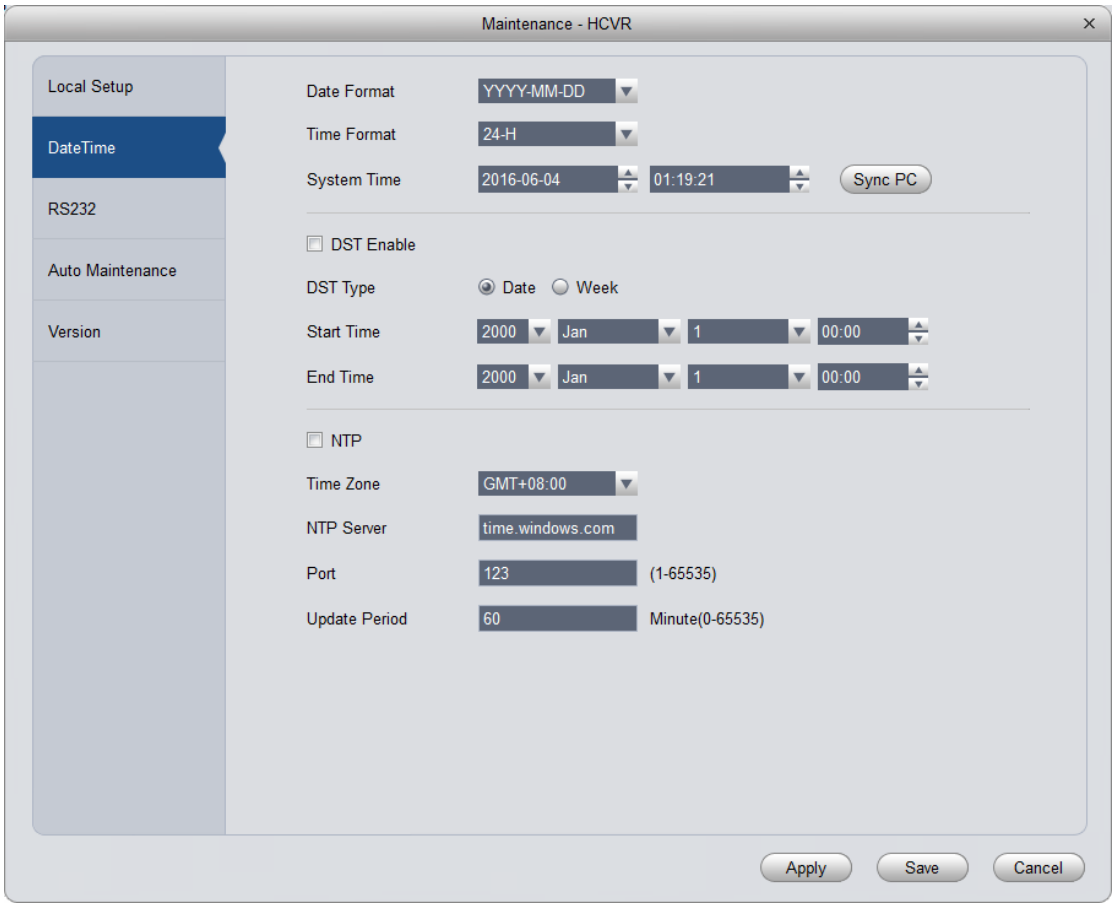


Figure 19-23

Parameter	Note
Date Format	Select date display format.
Time Format	Select corresponding time format.
System Time	Set system time of current device.
Sync PC	Push SmartPSS PC time to device.
DST	DST time.
NTP Server	By setting NTP server, system auto sync time according to server.

19.4.2.3 Serial Setup

You can set serial information, see Figure 19-24.

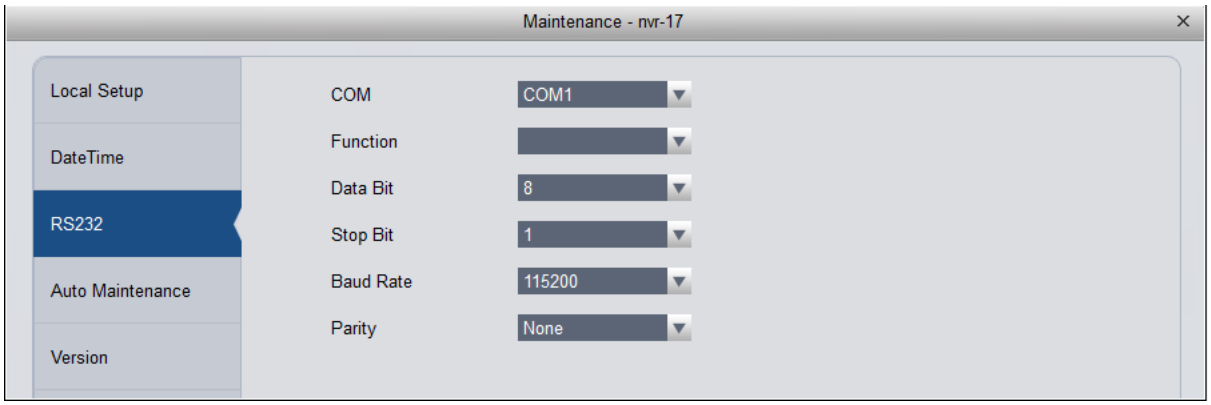


Figure 19-24

Parameter	Note
COM	Select COM.
Function	Select corresponding serial control protocol, serial function control protocol have: ● General, use COM and mini terminal software to upgrade and debug. ● Control keyboard, via COM use professional keyboard to contol device. ● Transparent COM, use to connect PC, and send data. ● Protocol COM, when card no. overlaps, you need to set to this COM. ● Network keyboard, via Ethernet port use professional keyboard to contol device.
Data Bit	Default is “8”.
Stop Bit	Default is “1”.
Baud Rate	Select corresponding baud rate length, default is “115200”.
Parity	Default is “no parity”.

19.4.2.4 Auto Maintenance

You can self set auto reboot system or auto delete file. Auto reboot system can set scheduled reboot. Auto delete file can customize day to delete file, see Figure 19-25.

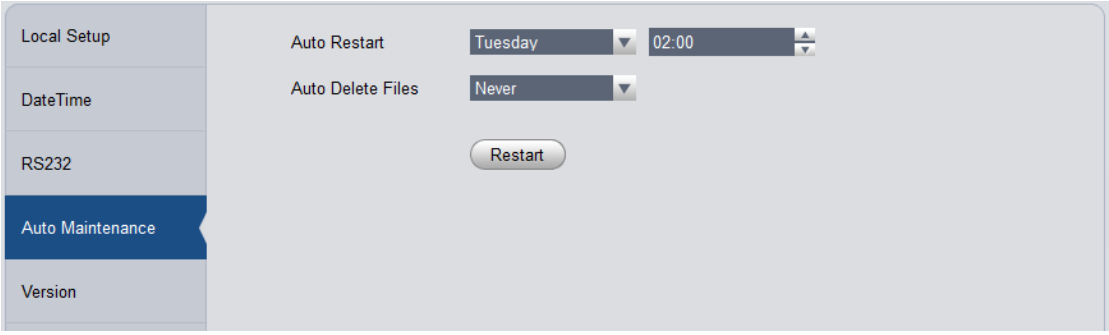


Figure 19-25

19.4.2.5 Version

View current device software version and SN.

19.4.2.6 Firmware Upgrade

Upgrade device program.

19.4.3 **Link to WEB**

You can link device WEB.

20 Statistics

20.1 Statistics

KBiVMS Manager supports search of server statistics, device statistics, management statistics, operation statistics and user statistics. The detailed steps are skipped here.

Overview

KBiVMS Manager supports real-time statistics of server and device online status, and supports search for alarm history and channel real-time analytics of server and device.

Step 1. Open Statistics>Overview interface. See Figure 20-1.

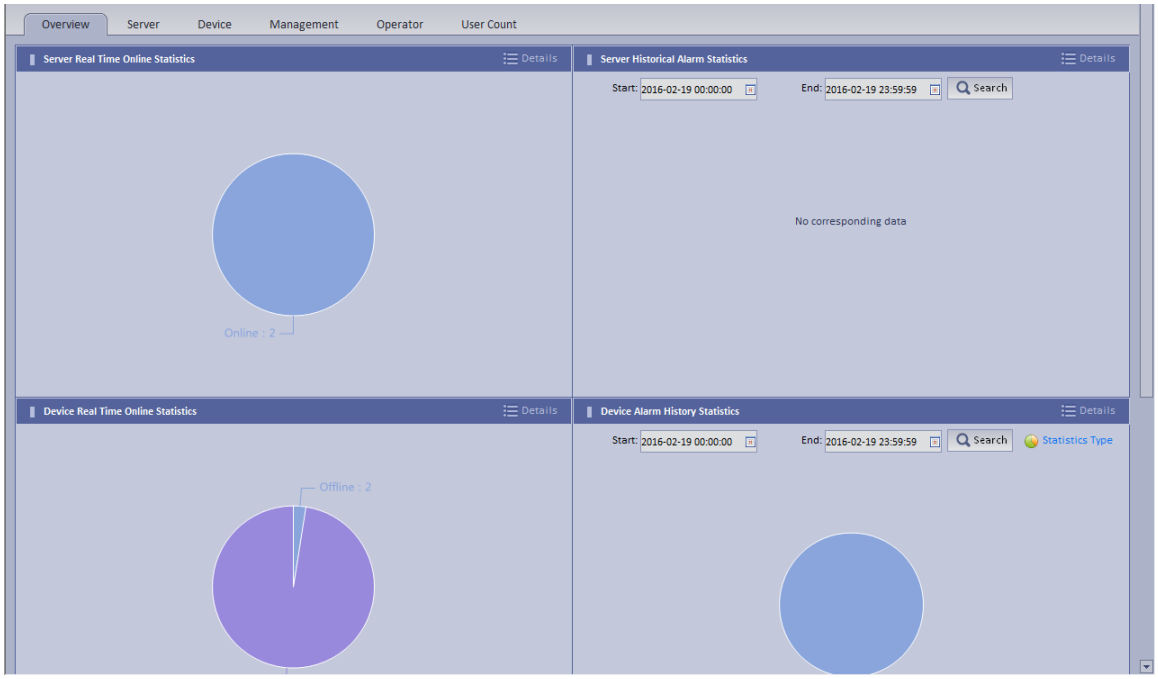


Figure 20-1

Step 2. Click Details next to Device Real Time Online Statistics or graph below to enter corresponding Statistics>Device>Device Online Statistics tab to view device real time online alarm info.

See Figure 20-2.

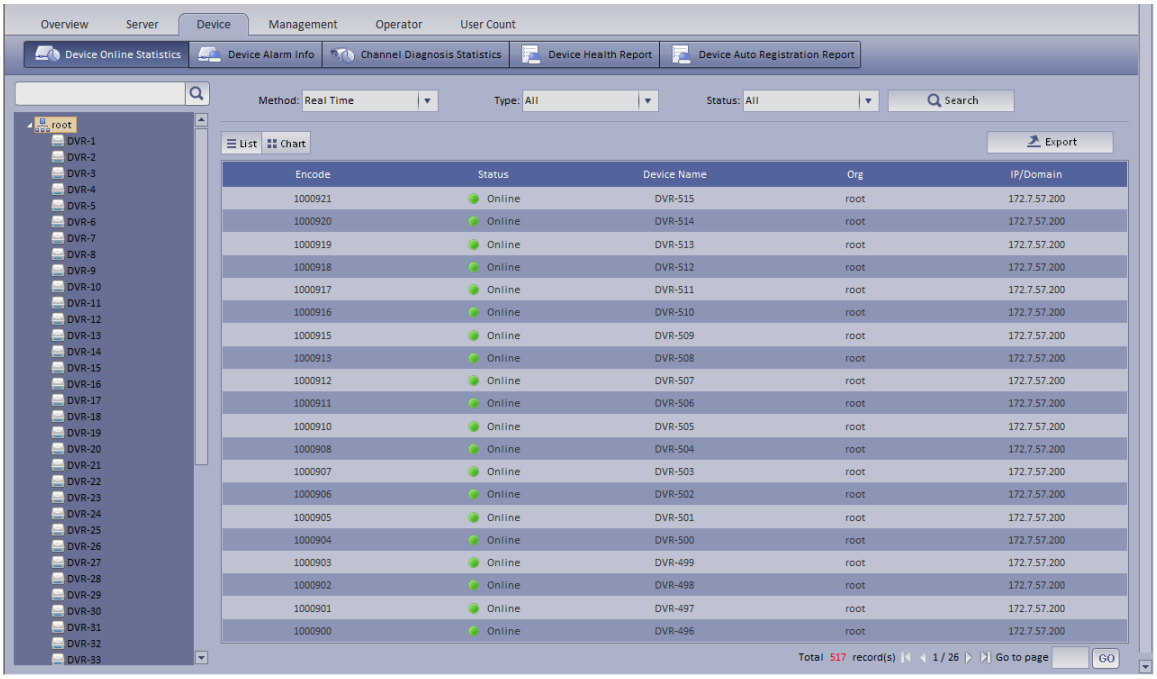


Figure 20-2

Step 3. Click Statistics Type on the bottom in Overview interface. You will see Figure 20-3.

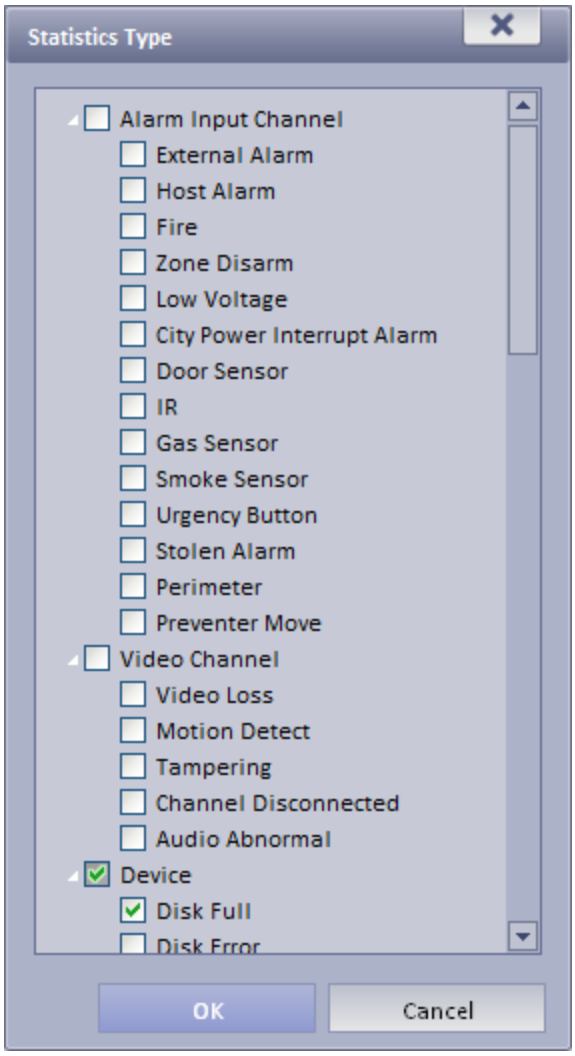


Figure 20-3

Step 4. Check designated type and click OK.

Step 5. Enter start time and end time. Click Search to search corresponding type info.

20.2 **Server Management**

KBiVMS Manager provides server management. Server management has center unit and distribution unit.

- Center
  - ➢ Dual hot spare not added

Step 1. Open General>Server>Center Unit. You can see operation status of center unit host. See Figure 20-4.

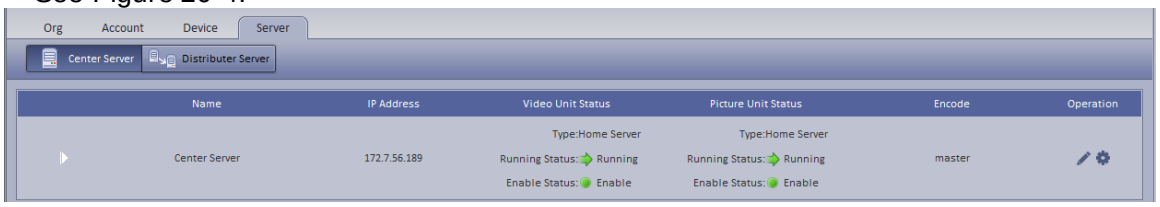


Figure 20-4

Step 2. Click , you can view name, server type, IP and status of center unit, video unit and picture unit in main server center unit. See Figure 20-5.

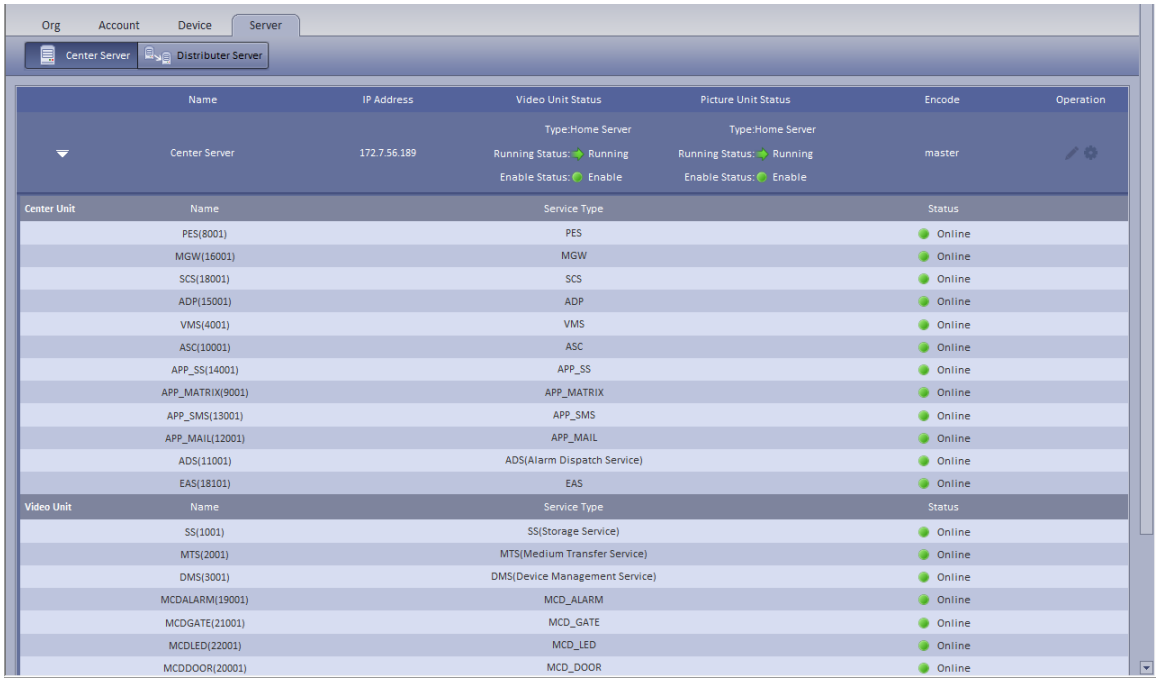


Figure 20-5

- ➢ Dual hot spare added

  Click open General>Server Config>Center Unit interface, you can view center unit and spare operation status of center unit. See Figure 20-6.

Figure 20-6

- Distribution unit

  Step 1. Open General>Server>Distribution Unit interface, you can view operation status of master/slave mode server. See Figure 20-7.

Figure 20-7

Step 2. Click  or  , you can edit or delete distribution unit.

Click  , you can enter initalization interface.

Step 3. Click  , you can view video server name, server type and IP status. See Figure 20-8.

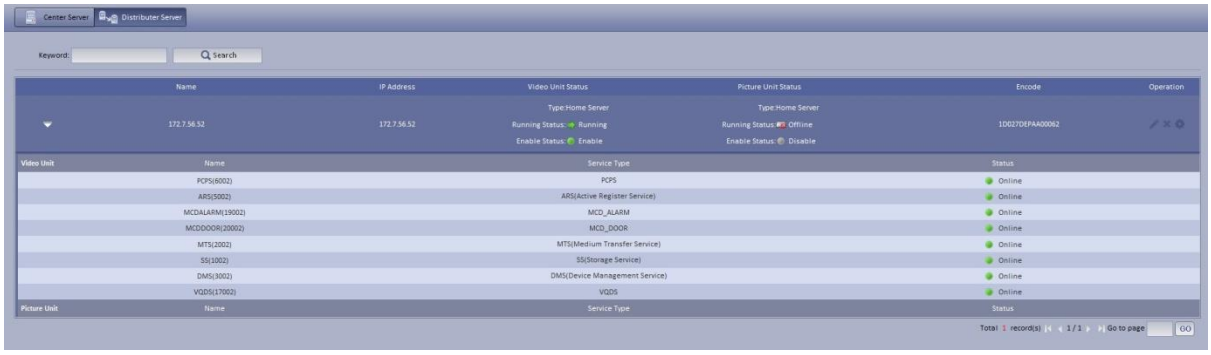


Figure 20-8

20.3 **Video Quality Analytics**

KBiVMS platform supports video quality analytics, first please set video analytics, analytics task, analytics scheme on Manager, and then you can view result of analytics on Client.

Step 1. Login KBiVMS Manager.

Step 2. Select Business>Video Analytics.

- Analytics item config: used to config video analytics.
- Task config: used to config video analytics task.
- Scheme config: used to config video analytics scheme template.

20.3.1 **Config Analytics Item**

Step 1. Select Video Analytics>Video Analytics.

Step 2. Click 

. System pops up Add Analytics Item Config box.

Step 3. Configure name and select analytics item, see Figure 20-9.

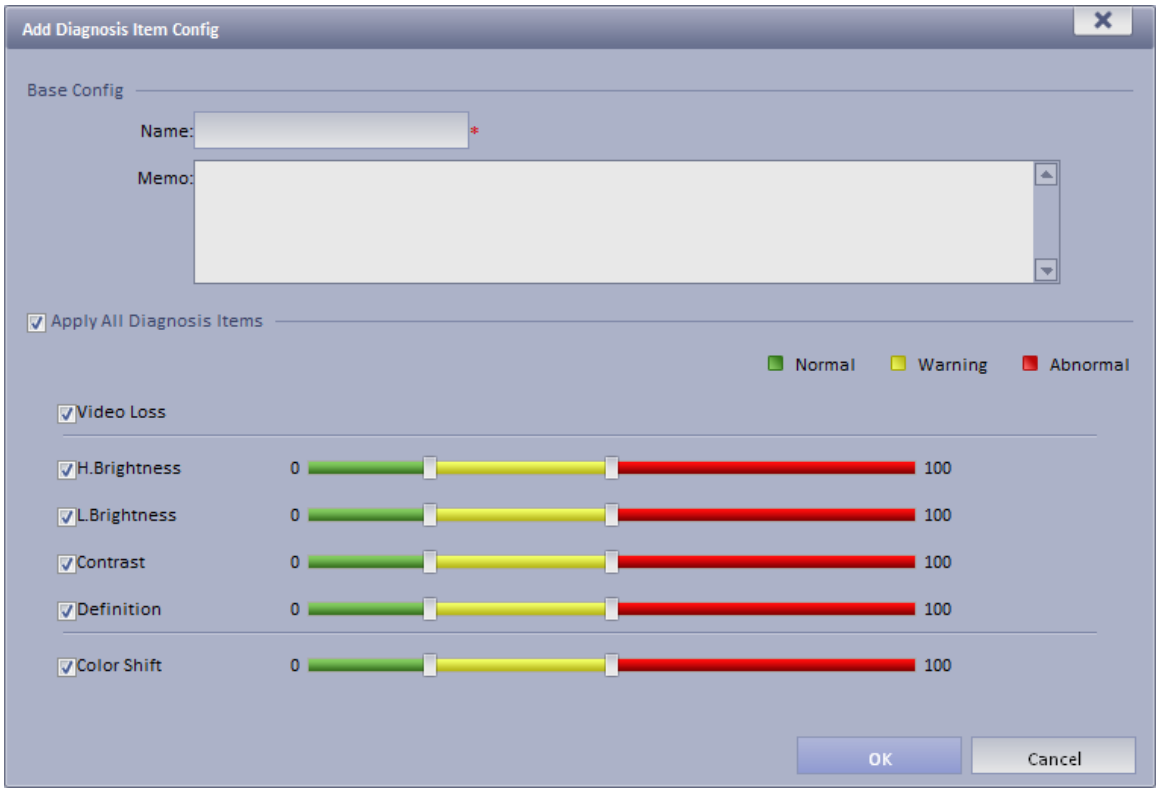


Figure 20-9

Step 4. Click OK. The added analytics item is shown in Analytics Config interface. You can modify and delete existing analytics item.

20.3.2 **Configure Analytics Task**

Step 1. Select Video Analytics Config>Task Config.

Step 2. Click 

. System pops up Add Task Config box, see Figure 20-10.

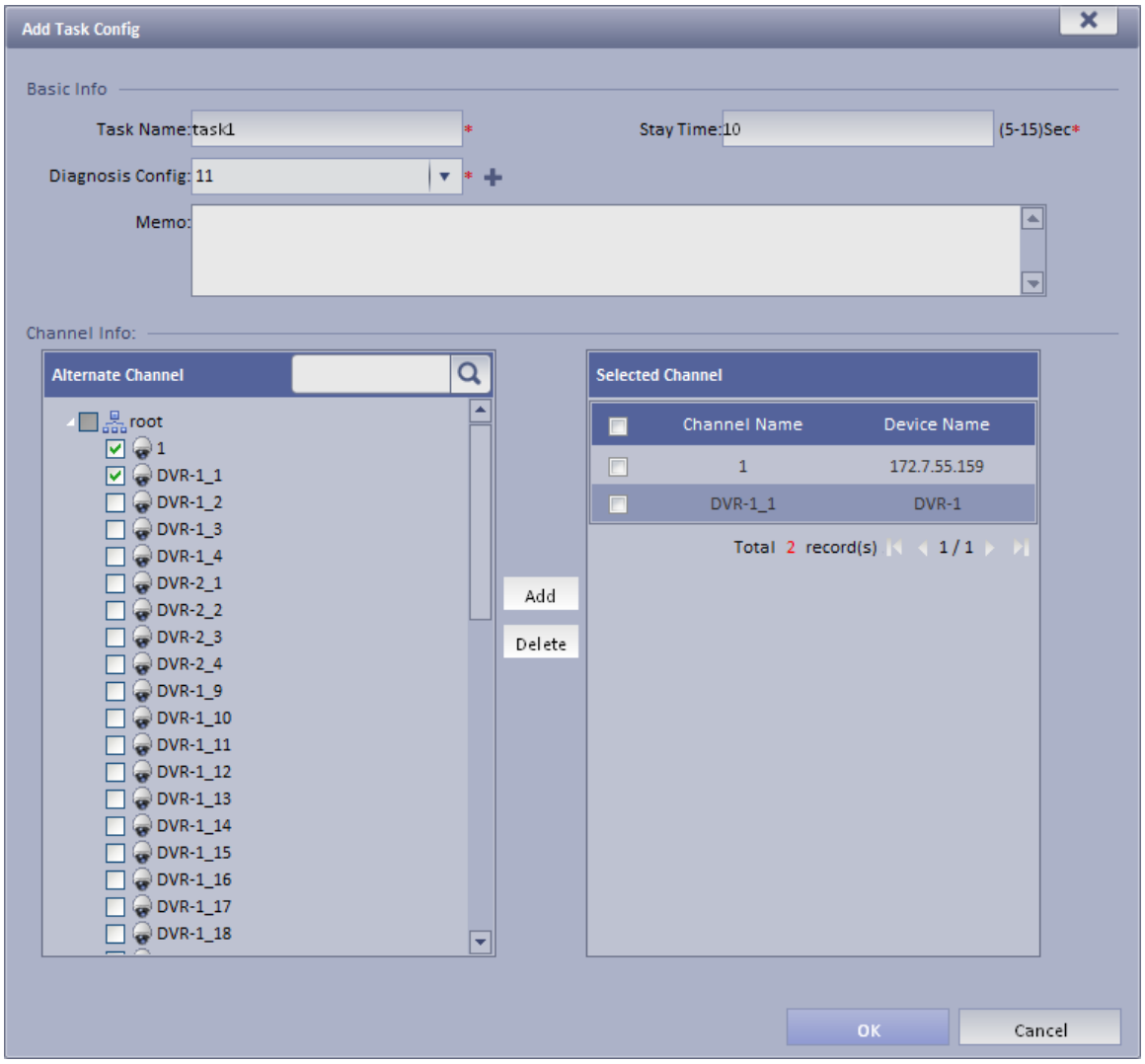


Figure 20-10

Step 3. Configure task name, single channel analytics overtime, analytics item config and etc.

Note:

Single channel analytics overtime: analytics of each channel required time.

Step 4. Check alternate channel, and click Add to add channel below selected channel.

Step 5. Click OK.

Configured task is shown in task config list. You can view, modify and delete added task.

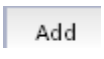
20.3.3 Config Analytics Scheme

Step 1. Select Video Analytics Config>Scheme Config.

Step 2. Click 

. System pops up Add Scheme Config box.

Step 3. Configure scheme name and check Enable.

Step 4. Under alternate task box, select alternate task, and click 

to add task to selected task.

Note:

The system supports multiple task.

Step 5. Configure task's start time, see Figure 20-11.

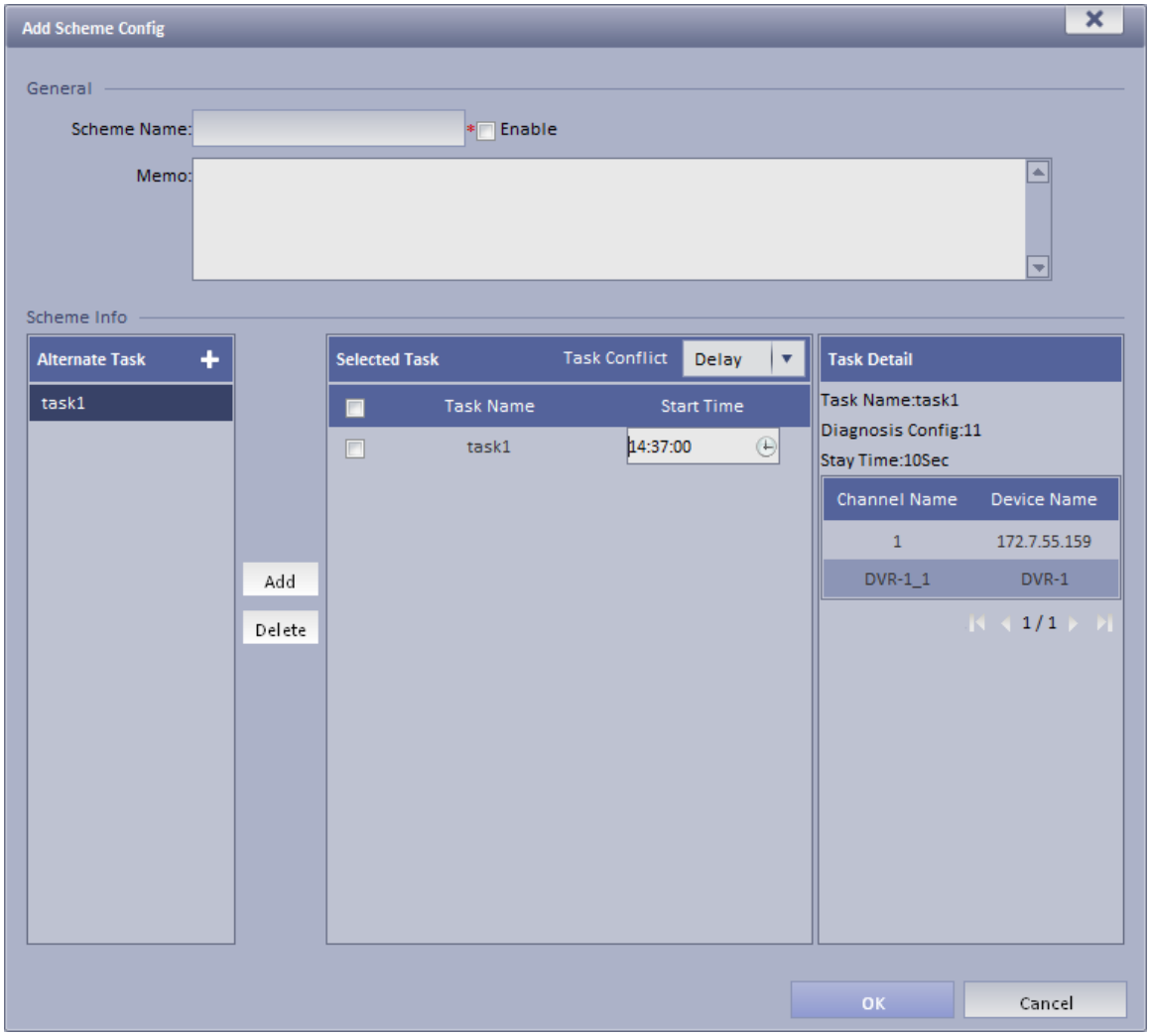


Figure 20-11

Step 6. Click OK. Configured scheme will be shown under scheme config list, you can modify and delete added scheme.

20.3.4 View Video Diagnosis Result

Step 1. Login KBiVMS Client.

Step 2. Click  in Extension area. System shows Video Analytics>Abnormal Analytics interface, see Figure 20-12.

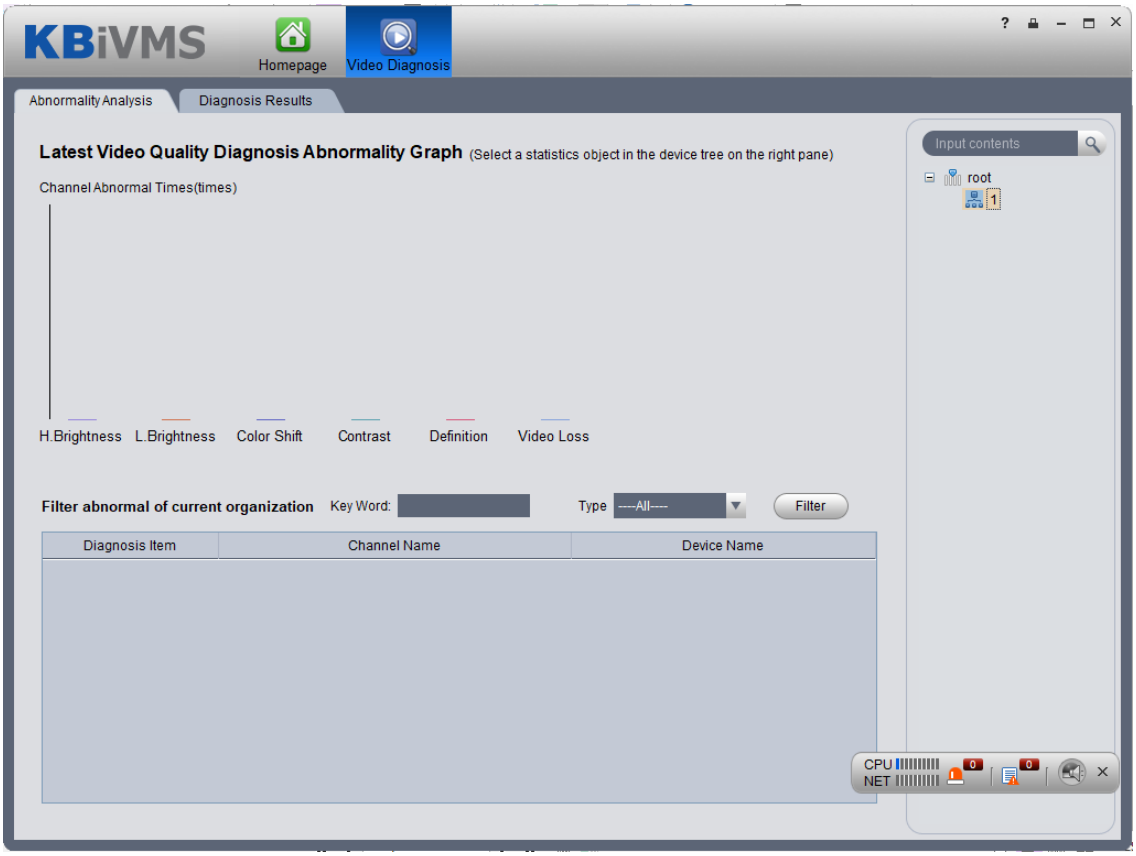


Figure 20-12

Step 3. Click Diagnosis Result tab, you can view all video analytics content.

See Figure 20-13.

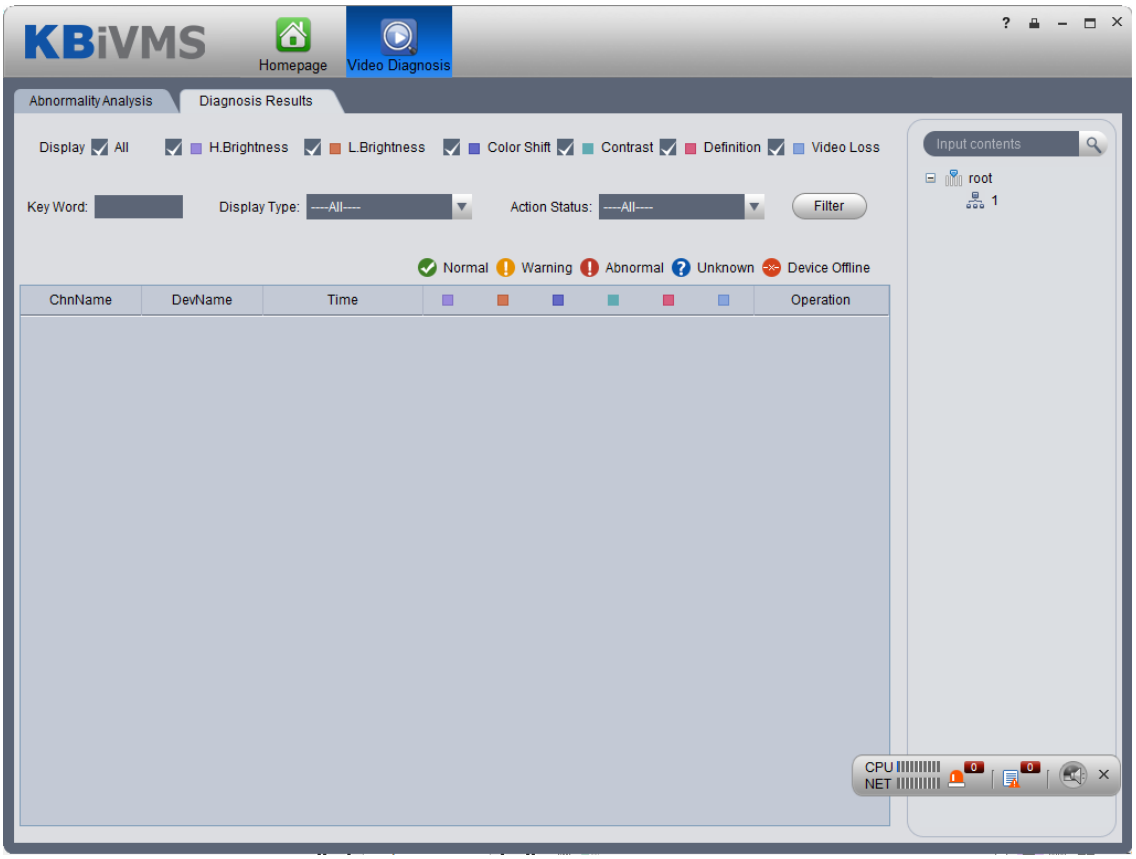


Figure 20-13

- Click  : view channel analytics history.
- Click  : view channel live preview.
- Click  : palyback channel record.

21 All-in-one Card

All-in-one management allow you to add and delete user/card, and authorize user.

Two methods to add cardholder:

- Add one: add one user.

  Step 1. Click All-in-one tab.

  Step 2. Click Add.

  Step 3. Set user ID, cardholder, department, mobile phone and etc. and upload user photo, see Figure 21-1.

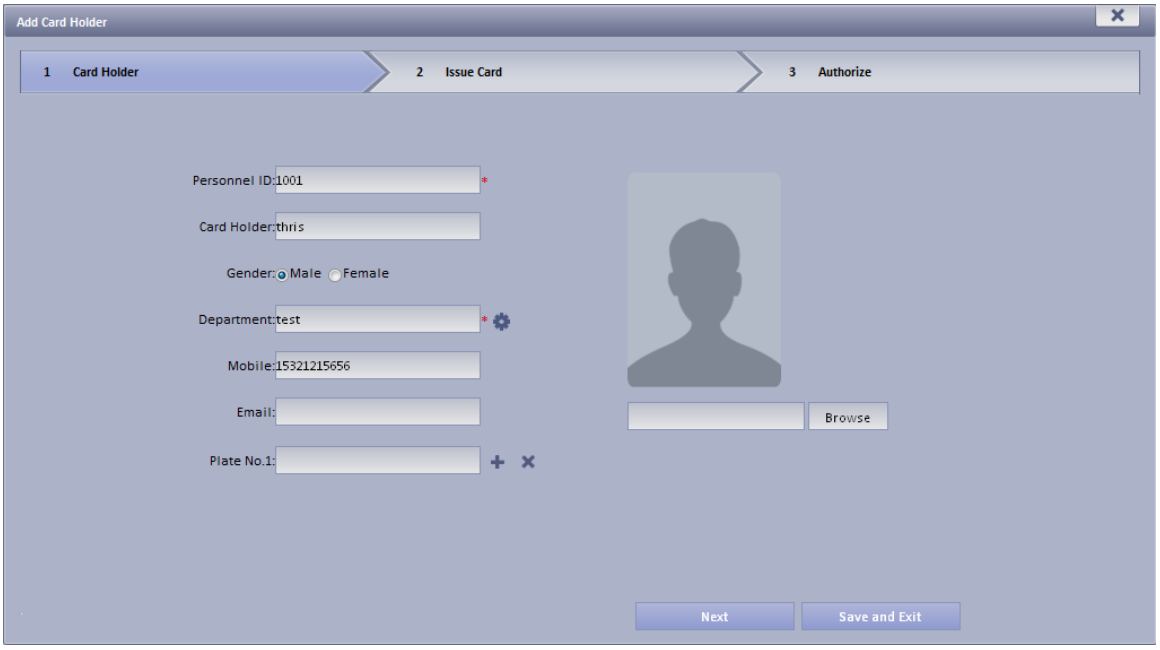


Figure 21-1

Note:

When you upload user image, please Internet Explorer 10 and lower, auto pop up control unit. Install the control unit, then you can upload image, otherwise you will fail. Or, please add this IP address to trusted site list.

Step 4. Click Next, see Figure 21-2.

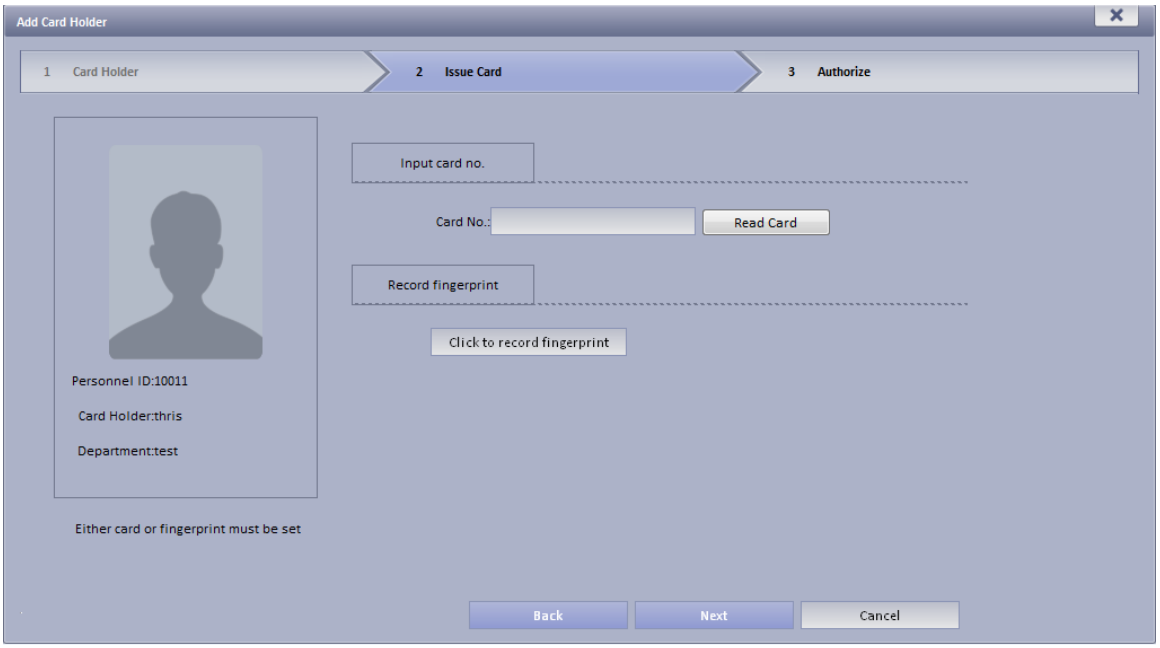


Figure 21-2

Step 5. Read card or record fingerprint.

Note:

- At least one of card no. or fingerprint must be entered.
- Card no. shall be read via card reader, or manual input.
- Recording fingerprint shall be repeated for three times to record identical fingerprint. One fingerprint is recorded at once. You may delete old fingerprint and record again.

Step 6. Click Next.

Step 7. Check Video Talk, A&C, or ANPR Device right, see Figure 21-3.

Figure 21-3

Step 8. Click Finish.

Wait about a few minutes for info send to device. In new cardholder list, click in

Operation column, you can view status. If it is , then sending is abnormal, please authorize again.

- Batch Add: Add more than one user at once, suitable for condition of many users, can be anonymous.

Step 1. In All-in-one card tab, click Batch Add.

Step 2. Set room no., department, quantity and etc. Card Holder is optional, see Figure 21-4.

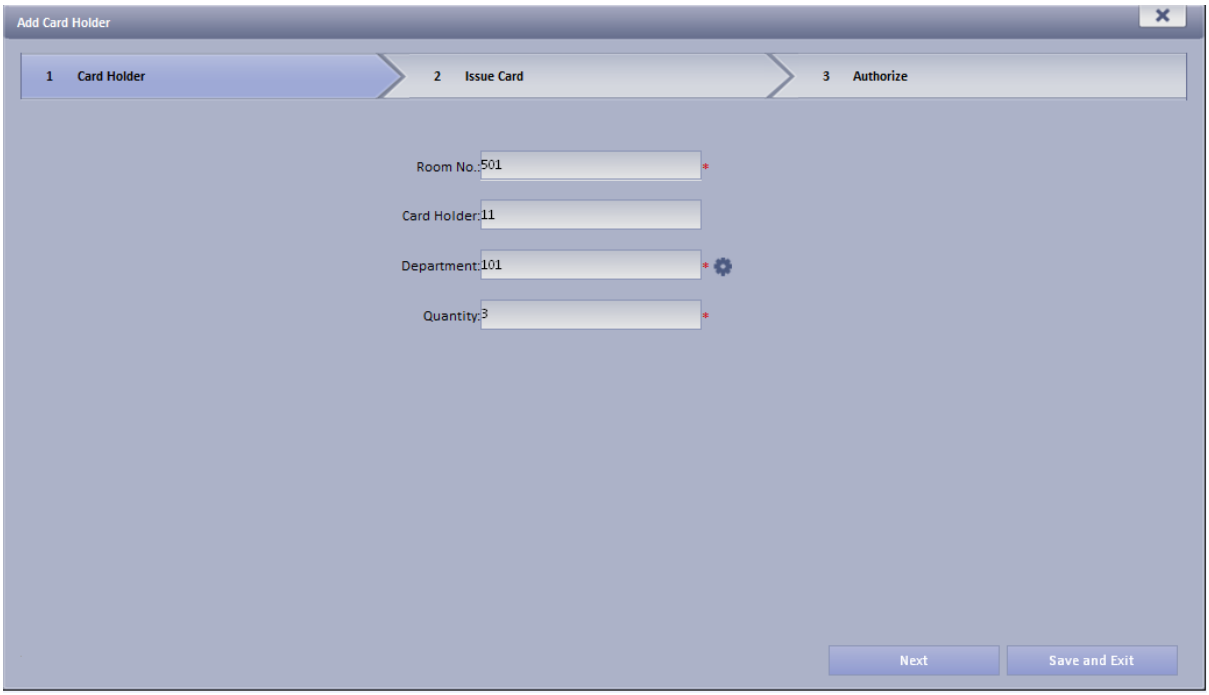


Figure 21-4

Step 3. Click Next.

Step 4. Progressively record card no. according to card holder sequence, click OK. As well as press Read Card button to record no. progressively.

Step 5. Once you complete record one user, click Confirm next to card no. See Figure 21-5.

Figure 21-5

Step 6. Click Next, see Figure 21-6.

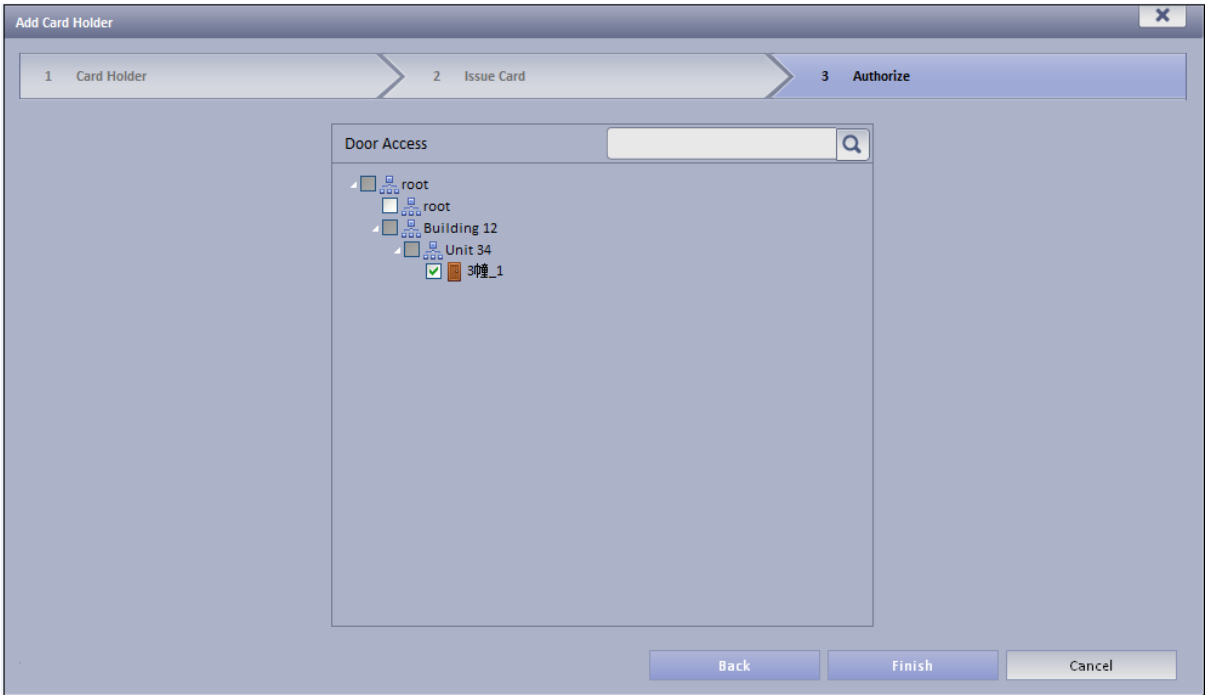


Figure 21-6

Step 7. Check access control right, click Finish.

Wait a few minutes to send info to device, and confirm whether successfully sent on card holder list. Repeat Step 8.

See Figure 21-7.

Figure 21-7

- Issue Card: check unbound user to authorize access control to user.

1. Check unbound user, click Issue Card. See Figure 21-8.

Figure 21-8

2. Progressively record card no. according to card holder sequence, click OK. As well as press Read Card button to record no. progressively.
3. Click Next. See Figure 21-9.

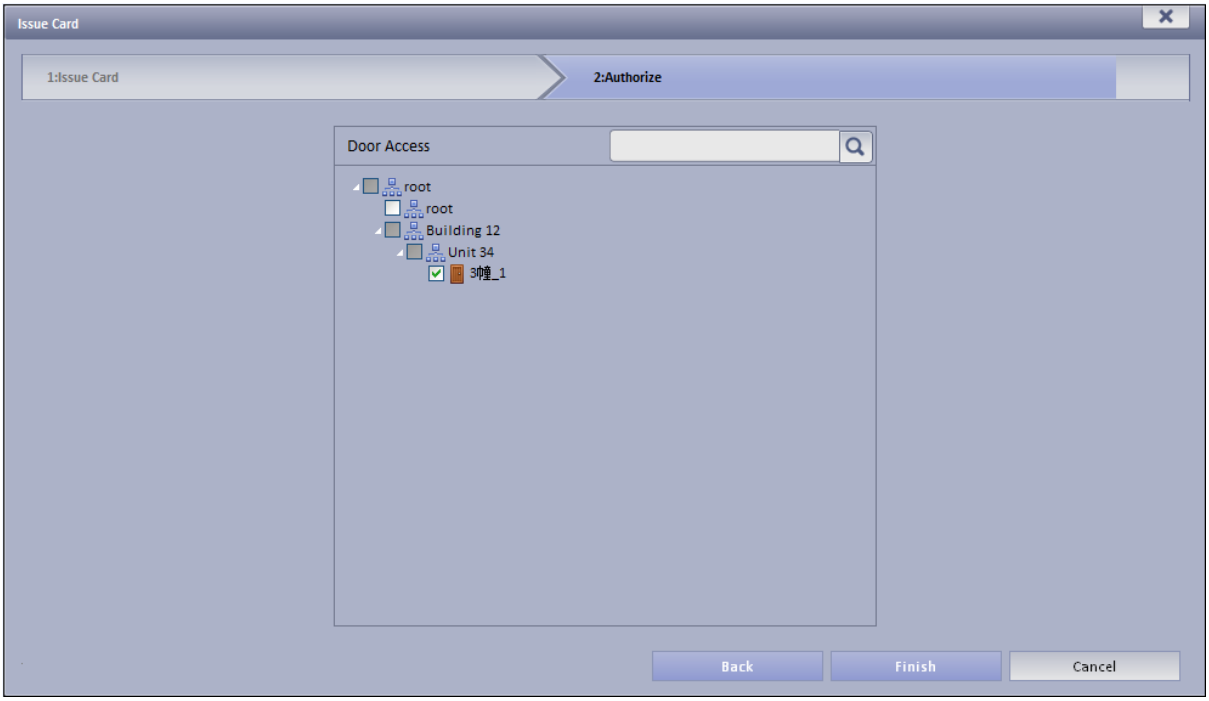


Figure 21-9

4. Check door access right, click Finish.

Wait a few minutes to send info to device, and confirm whether successfully sent on card holder list. Repeat Step 8.

- Download Control :Drive fingerprint device and card reader OCX control. After control unit is installed, insert card reader and fingerprint device into USB port to enable.
- : view authorization info. If it is : authorization error, need to authorize again.
- : manage user entrance/exit info, system supports re-record fingerprint or modify access control right.

1. Click . See Figure 21-10.

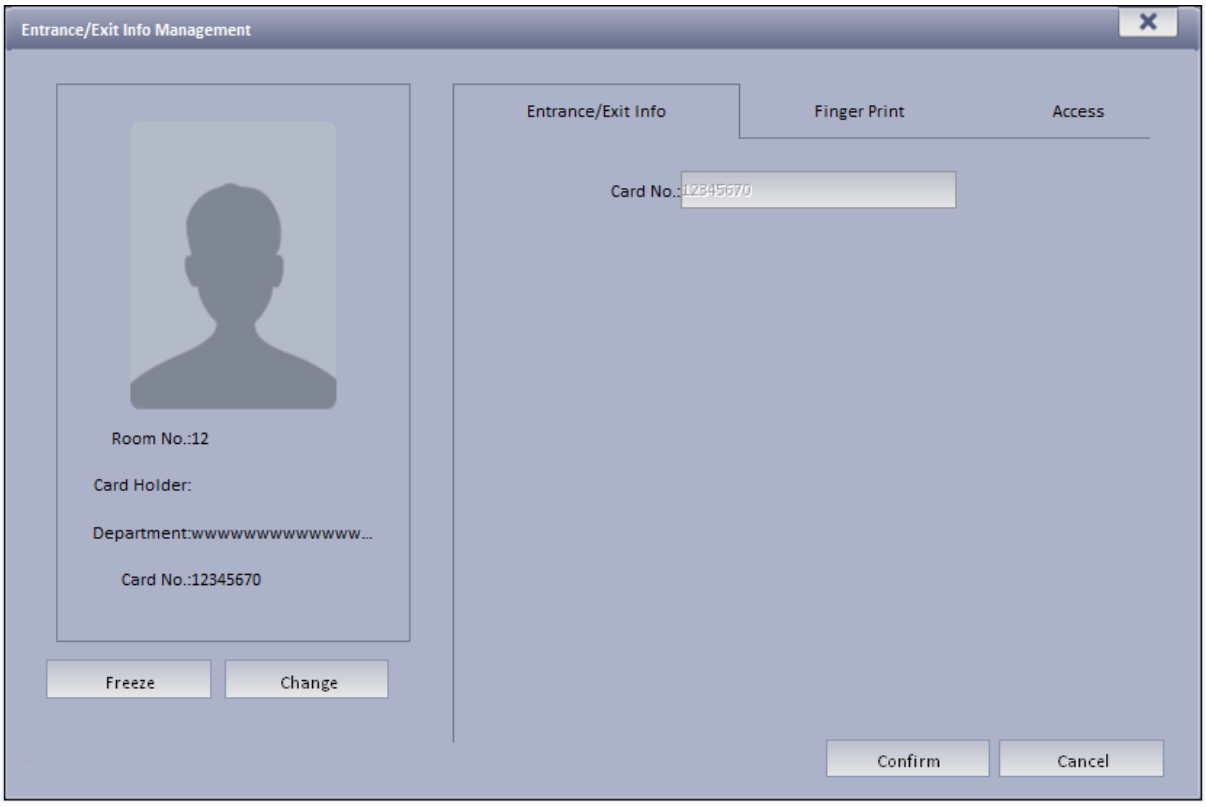


Figure 21-10

2. Click Freeze, to freeze lost card.
3. Click Change to change card.
4. Click Fingerprint tab, re-record fingerprint for user.
5. Click Right tab, check access control to re-allocate video talk, a&c, and ANPR device right.
6. Click OK.

22 Other KBiVMS Manager Operations

22.1 Device Security

KBiVMS Manager supports to initialize device or modify IP.

Step 1. Select Basic Config>Device>Device Security.

Step 2. Click Initialization tab.

Step 3. Check one or more devices to initialize, click Initialization.

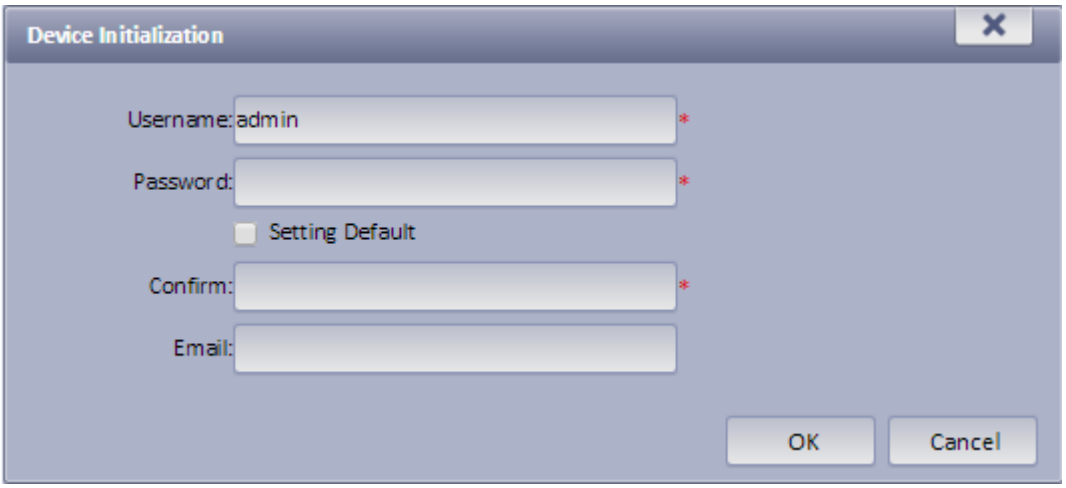


Figure 22-1

Step 4. Enter device password, confirm password, click OK. See Figure 22-2.

Figure 22-2

Step 5. Click Change IP tab, see Figure 22-3.

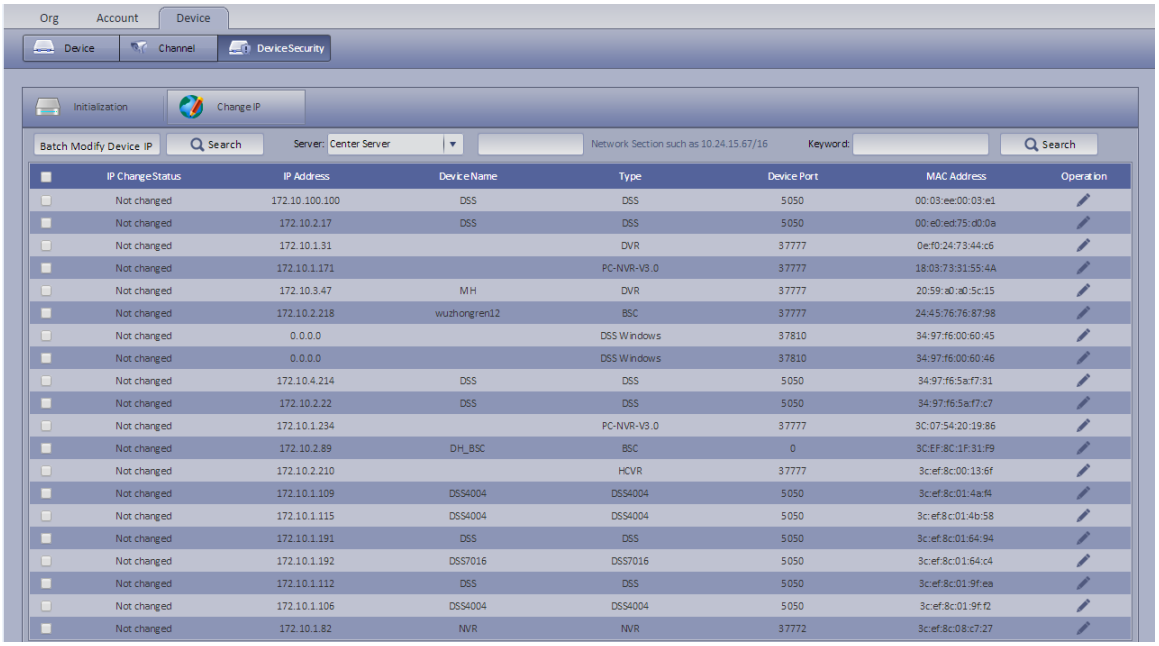


Figure 22-3

Step 6. Click  next to each item, or check multiple items and click Batch Modify Device IP. See Figure 22-4.

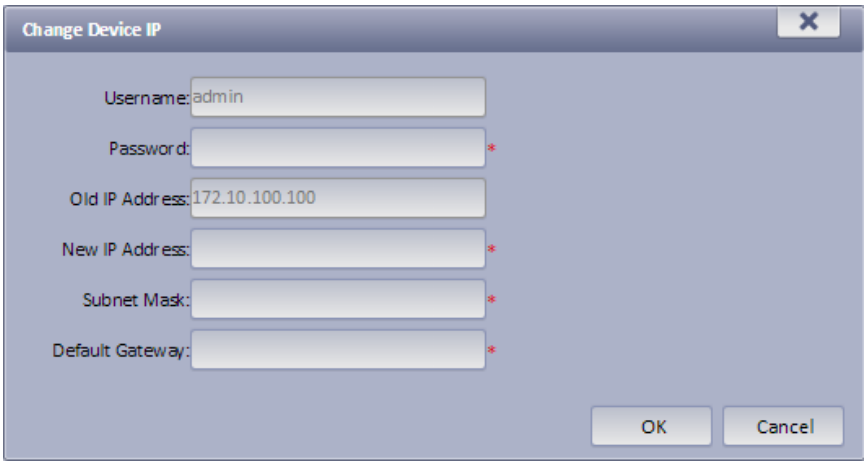


Figure 22-4

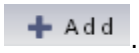
Step 7. Enter password, new IP address, subnet mask and etc., click OK.

22.2 **Cascade**

KBiVMS Manager supports cascading configuration. You can set Domain, Domain Service of other zones. After cascading, you can manager lower organization and device.

Before configuring cascading, you must obtain the IP address and port where lower-level CMS server is installed, and IP address and port where WEB server is installed.

Step 1. Select Cascade>Domain. System displays Domain interface.

Step 2. Click  . System pops up Add Domain box, see Figure 22-5.

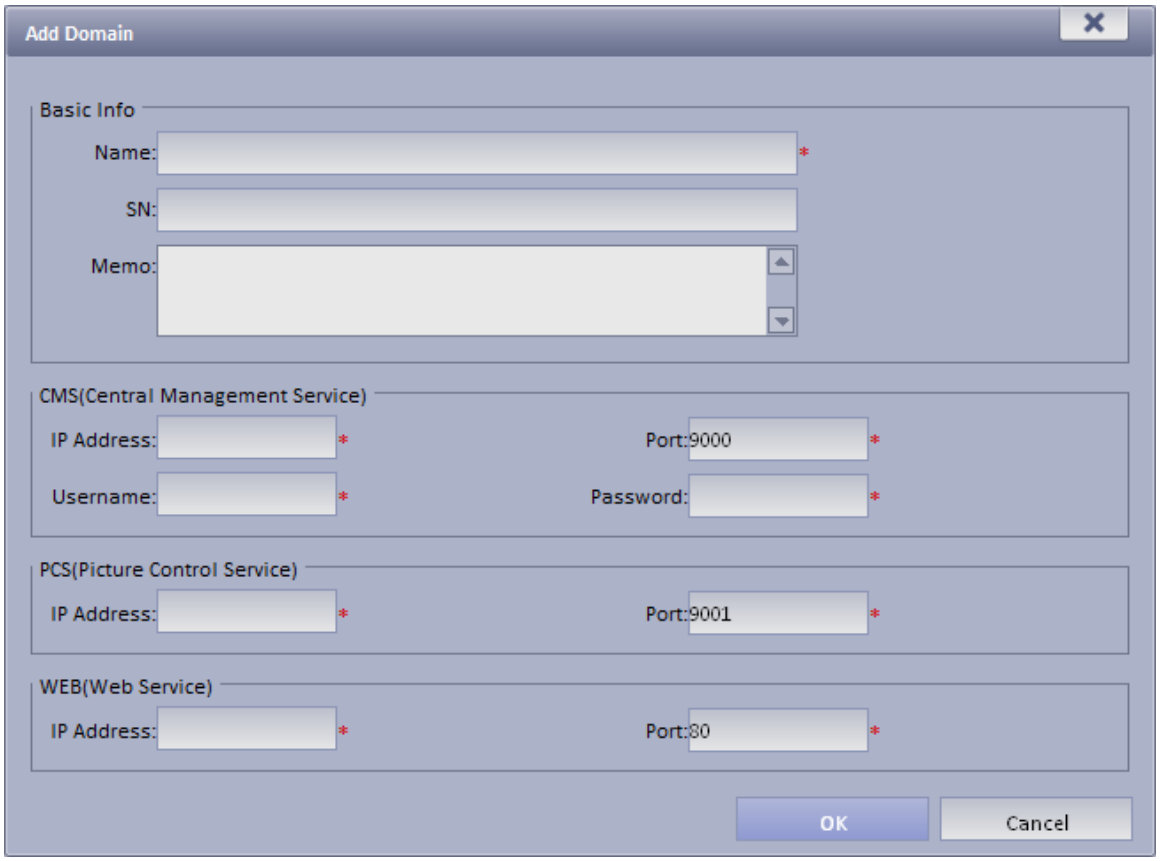


Figure 22-5

Step 3. Input Name, CMS IP address, CMS port, CMS username, CMS password, WEB IP address, WEB port.

Step 4. Click OK. After configuration, select General>Org. Here you can view added domain or device info. You can select Cascade>Domain Service to view online status of domain.

22.3 System Config

22.3.1 Upload

KBiVMS supports uploading file to CMS.

Step 1. Select System>Upload. System displays Upload interface.

Step 2. Click 

. System pops up Upload File box, see Figure 22-6.

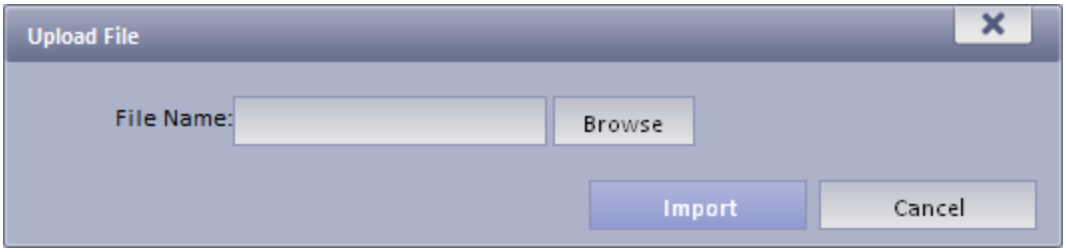


Figure 22-6

Step 3. Click Browse to select file to upload.

Step 4. Click Import to upload selected file.

22.3.2 **Backup and Restore**

KBiVMS supports config info backup to local PC, and restoration of the backup file. Note:

Only system user can backup and restore.

22.3.2.1 System Backup

System backup detailed step:

Step 1. Select System>Backup Restore, see Figure 22-7.

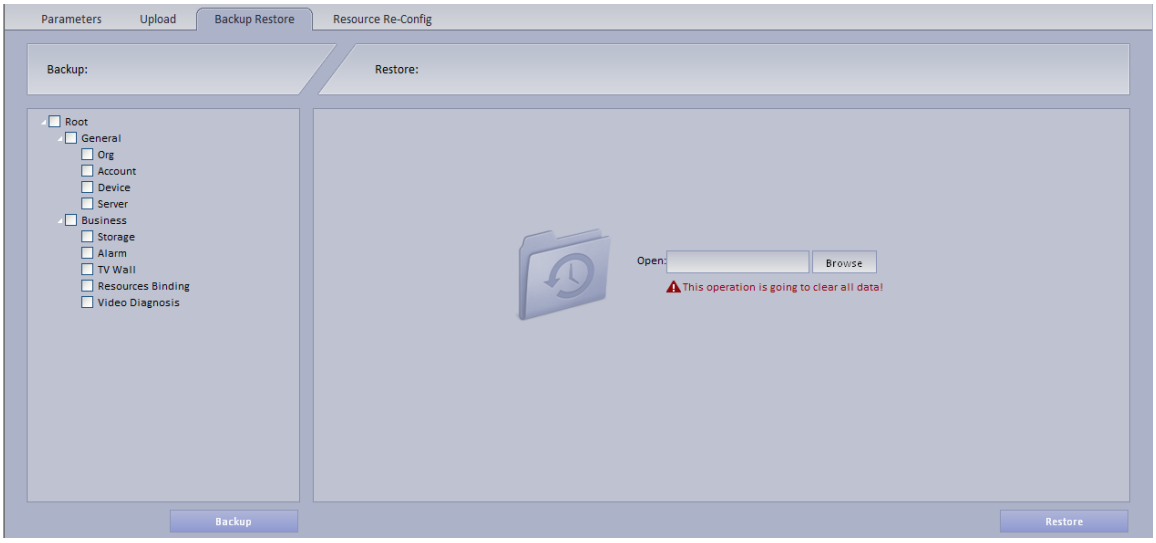


Figure 22-7

Step 2. Check info to backup. For example, Org, Account.

Step 3. Click on Backup.

Step 4. Click on Save, system pops up Save as box.

Step 5. Select storage path and click on Save. System prompt when downloading is complete.

Step 6. Click on Close.

22.3.2.2 Restore

You can select backup file to restore system.

Step 1. Select System>Backup Restore.

Step 2. Click on Browse in Restore area.

Step 3. Select backup file.

Step 4. Click on Restore.

Step 5. Input password user “system”.

Step 6. Click on OK.

Step 7. System will restore, and system need to be rebooted.

22.3.3 **Resource Re-Config**

You can re-configure KBiVMS server resource and parameter. 22.3.3.1 Video Server

Step 1. Select System>Resource Re-Config.

Step 2. Click Video Server.

Step 3. Drag device on the left into server. See Figure 22-8.

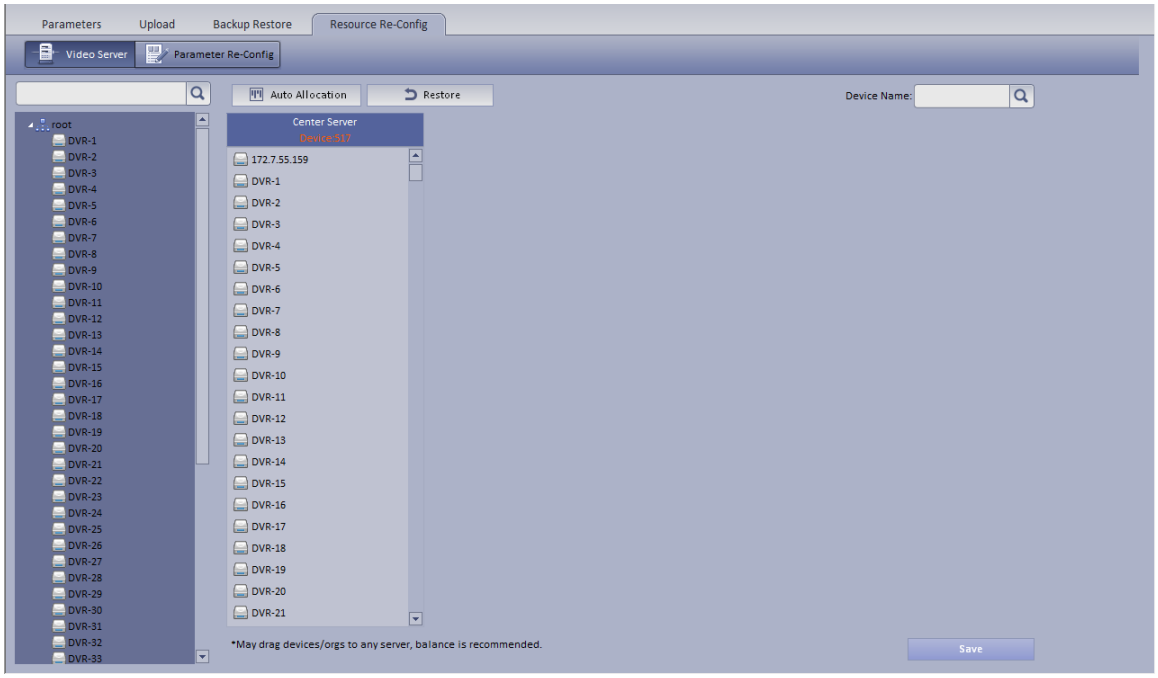


Figure 22-8

- Auto Allocation: You can select one device, and click Auto Allocation so system will automatically allocate device to one server.
- Restore: You can restore previous operation.
- :Enter device name, click Search to search device.

22.3.3.2 Parameter Re-Config

You can modify device username, password and organization together.

Step 1. Select System Config>Resource Re-Config.

Step 2. Click Parameter Re-Config.

Step 3. In device list on the left, check device.

You can select more than one device at the same time, and all of checked device will be shown in the area at device to be batch modified.

Step 4. Check Modify username password, to batch modify device username and password.

Step 5. Check Re-config organization to batch modify device organization.

Step 6. Click Save.

23 WEB Client

KBiVMS supports B/S format client. Via login WEB Manager, you can set local config, preview, playback, TV wall and E-map.

23.1 Login WEB

To log in WEB:

Step 1. In Internet Explorer, input IP address of Server, and press Enter. System shows login interface as in Figure 23-1.

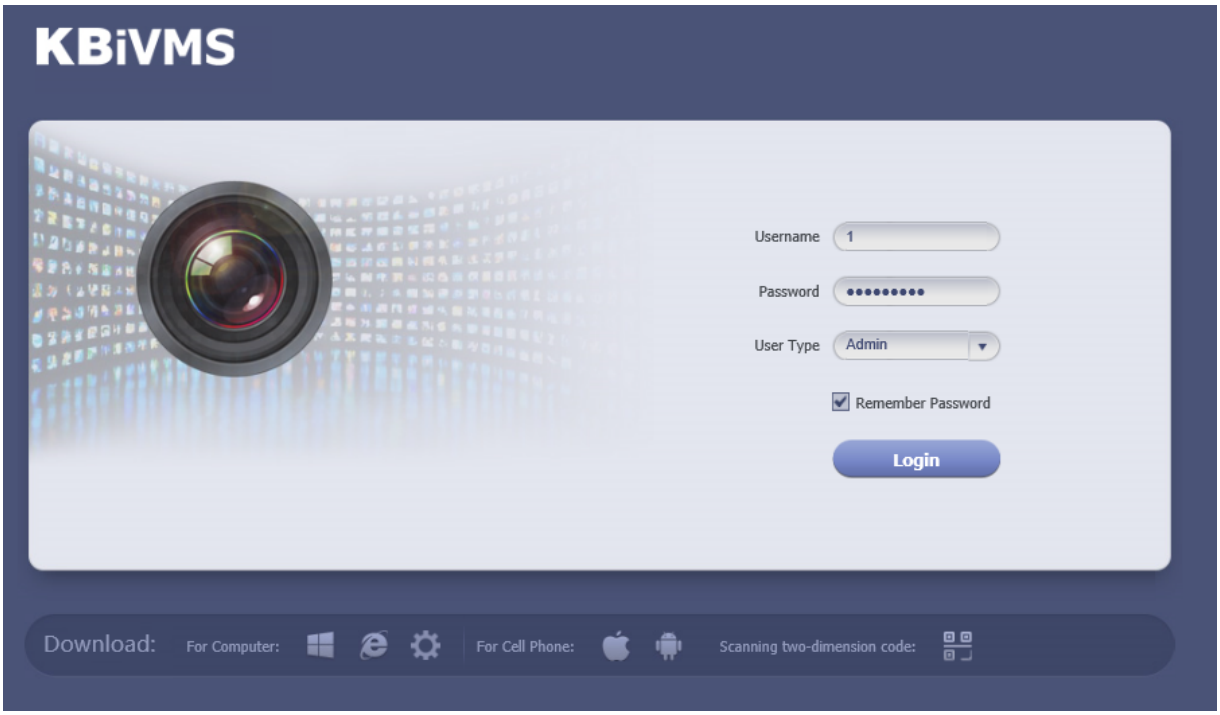


Figure 23-1

Step 2. Click , system prompts to download Plugin.exe.

Step 3. Download and install Plugin.exe.

Step 4. In Internet Explorer, input IP address of the Server, and press Enter.

Step 5. In login interface, input username and password. Select user type as Operator.

Step 6. Click Login. See Figure 23-2.

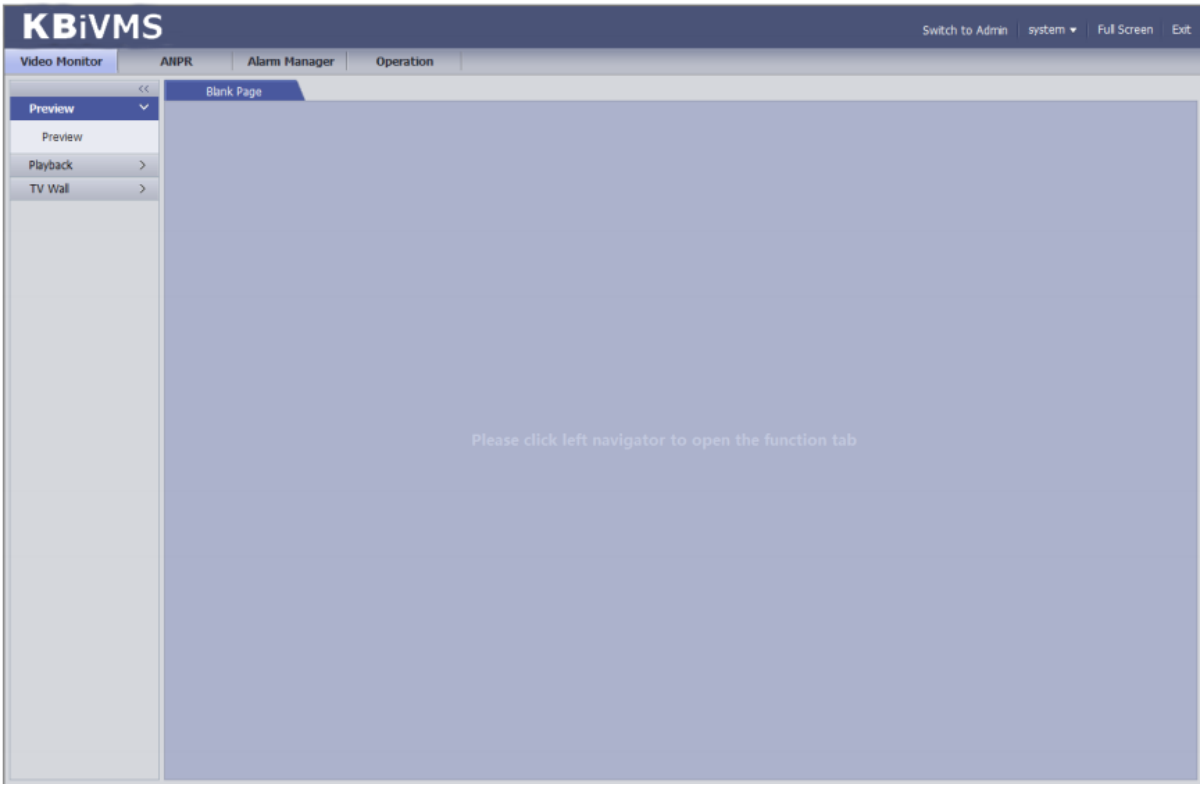


Figure 23-2

23.2 Setup

Please refer to Ch 2.2.3.

23.3 Video Monitor

23.3.1 Preview

Please refer to Ch 5.

23.3.2 Playback

Please refer to Ch 6.

23.3.3 TV Wall

Please refer to Ch 9.

23.4 Map

Please refer to Ch 7.

Note:

- **This manual is for reference only. Slight difference may be found in the user interface.**
- **All the designs and software here are subject to change without prior written notice.**
- **All trademarks and registered trademarks are the properties of their respective owners.**
- **If there is any uncertainty or controversy, please refer to the final explanation of us.**
- **Please visit our website or contact your local service engineer for more information.**