OPTIVIEW
VMX

USER MANUAL

Foreword

General

This user's manual (hereinafter referred to be the Manual) introduces the functions and operations of the OPTIVIEW VMX general surveillance management center (hereinafter referred to be the Device or the System) and client operations.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠ **DANGER**	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ **WARNING**	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ **CAUTION**	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
Note	Provides additional information as the emphasis and supplement to the text.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures including but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

Revision History

Version	Software Version	Revision Content	Release Time
V1.0.4	1.000.0000003.1	● Added intelligent analysis configuration instructions	August 2019

Version	Software Version	Revision Content	Release Time
V1.0.3	1.000.0000003	● Added alarm controller, entrance, smart track, visitor management and POS. ● Optimized attendance management, personnel management and access control. Optimized user's manual description and outline structure. ● Deleted FTP. ● Added electronic focus function introduction.	May 2019
V1.0.2	1.000.0000002	● Added modules of Attendance and Flow Analysis. ● Added generating track in the module of Face Recognition.	October 2018

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

Foreword ... II
1 Overview ... 1
1.1 Product Positioning ... 1
1.2 Highlights ... 1
2 Installation and Deployment ... 2
2.1 Preparations ... 2
2.1.1 Server Configuration Requirement ... 2
2.1.2 Configuring Server IP Address ... 2
2.1.3 Configuring Server System Time ... 5
2.2 Installing Program (Update) ... 7
2.3 Service Management ... 9
2.3.1 Logging in System Config Tool ... 9
2.3.2 Modifying Service Port ... 11
2.3.3 WAN and LAN Mapping ... 12
2.4 Installing Client ... 14
2.4.1 Installing Client ... 14
2.4.2 Initialization Configurations ... 18
2.4.3 Logging in to Client ... 20
2.5 Importing License ... 23
2.5.1 License Introduction ... 23
2.5.2 Applying for License ... 24
2.5.3 Loading License ... 26
3 Operation Guide ... 28
3.1 Installing Client ... 28
3.2 Basic Configuration ... 28
3.2.1 System Setting ... 28
3.2.2 Managing Device ... 36
3.2.3 Adding User ... 54
3.2.4 Setting Alarm Event ... 57
3.2.5 Setting Record Plan ... 67
3.2.6 Configuring Emap ... 68
3.3 Local Config ... 76
3.3.1 Setting Basic Parameter ... 77
3.3.2 Setting Real-time Video Parameter ... 78
3.3.3 Setting Record Playback ... 79
3.3.4 Setting Snapshot ... 80
3.3.5 Setting Recording Parameter ... 81
3.3.6 Setting Alarm Parameter ... 81
3.3.7 Setting Video Wall ... 82
3.3.8 Setting Shortcut Key ... 83
3.4 Live View ... 84

3.4.1 Entering Live View Interface ... 84
3.4.2 Enabling Live View ... 86
3.4.3 Enabling Tour View ... 90
3.4.4 Setting PTZ ... 90
3.4.5 Electronic Focus ... 96
3.4.6 View ... 98
3.4.7 Favorites ... 100
3.4.8 Region of Interest (RoI) ... 103
3.5 Device Configuration ... 104
3.5.1 Configuring Camera Properties ... 104
3.5.2 Video ... 114
3.5.3 Audio ... 120
3.6 Configuring Intelligent Analysis ... 122
3.6.1 Intelligent Analysis Configuration Interface ... 122
3.6.2 IVS ... 124
3.6.3 Face Detection ... 146
3.6.4 People Counting ... 153
3.6.5 Heatmap ... 160
3.7 Fisheye-PTZ Smart Track ... 165
3.7.1 Adding Device ... 165
3.7.2 Adding Smart Track Configuration ... 166
3.7.3 Enabling Smark Track Function ... 168
3.8 Bullet-PTZ Smart Track ... 168
3.8.1 Preparations ... 169
3.8.2 Applying Smart Track ... 169
3.9 Record ... 175
3.9.1 Record Playback ... 175
3.9.2 POS Record Playback ... 187
3.10 Event Center ... 187
3.10.1 Setting Alarm Parameters ... 187
3.10.2 Searching and Processing Real-Time Alarm ... 189
3.10.3 Searching and Processing History Alarm ... 191
3.11 Video Wall ... 192
3.11.1 Adding Encoder ... 193
3.11.2 Entering Video Wall Interface ... 193
3.11.3 Adding Video Wall ... 195
3.11.4 Adding Task ... 198
3.11.5 Setting Video Wall Plan ... 199
3.11.6 Applying Video Wall ... 206
3.12 POS ... 210
3.12.1 Adding Encoder ... 210
3.12.2 Modifying POS End Mark ... 211
3.12.3 Live View ... 212
3.12.4 Record Playback ... 214
3.13 Face Recognition ... 216
3.13.1 Adding Encoder ... 217
3.13.2 Setting Picture Storage Disk ... 217

3.13.3 Setting Record Plan ... 218
3.13.4 Managing Face Database ... 218
3.13.5 Setting Alarm Event ... 228
3.13.6 Face Recognition Application ... 228
3.14 ANPR ... 244
3.14.1 Adding ANPR ... 244
3.14.2 Setting Picture Storage Disk ... 244
3.14.3 Setting Record Plan ... 244
3.14.4 Plate Recognition Application ... 245
3.15 Flow Analysis ... 249
3.15.1 Adding Encoder ... 250
3.15.2 Flow Analysis Application ... 250
3.16 Personnel Management ... 253
3.16.1 Adding Department ... 254
3.16.2 Adding Personnel ... 255
3.16.3 Editing Personnel ... 269
3.16.4 Importing/Exporting Personnel ... 274
3.16.5 Batch Issue Card ... 277
3.16.6 Personnel Extraction ... 280
3.16.7 Generating Path ... 281
3.17 Access Control ... 282
3.17.1 Adding Access Control ... 283
3.17.2 Personnel Management ... 287
3.17.3 Managing Time Template ... 287
3.17.4 Setting Access Level ... 291
3.17.5 Advanced Function ... 293
3.17.6 Setting Record Plan ... 312
3.17.7 Configuring Super Password ... 312
3.17.8 Access Control Application ... 313
3.17.9 Searching Access Control Log ... 321
3.17.10 AC Device Maintenance ... 325
3.18 Visitor Management ... 327
3.18.1 Adding AC Device ... 327
3.18.2 Visitor Appointment ... 327
3.18.3 Visit Registration ... 329
3.18.4 End Visit Registration ... 333
3.18.5 Searching Visit Record ... 334
3.19 Video Intercom ... 336
3.19.1 Adding Video Intercom Device ... 336
3.19.2 Personnel Management ... 337
3.19.3 Configuring Building/Unit ... 337
3.19.4 Synchronizing Contacts ... 337
3.19.5 Call Management ... 339
3.19.6 Video Intercom Application ... 344
3.20 Attendance Management ... 352
3.20.1 Adding Attendance Device ... 353
3.20.2 Personnel Management ... 354

3.20.3 Setting Attendance Terminal....354
3.20.4 Setting Statistics Rule.... 355
3.20.5 Setting Attendance Period.... 356
3.20.6 Setting Holiday.... 361
3.20.7 Setting Attendance Shift.... 363
3.20.8 Shift Management.... 365
3.20.9 Viewing Attendance Report.... 369
3.21 Entrance.... 372
3.21.1 Adding Device.... 373
3.21.2 Setting Picture Storage Disk.... 381
3.21.3 Setting Alarm Event.... 381
3.21.4 Configuring Parking Lot.... 382
3.21.5 Vehicle Management.... 387
3.21.6 Entrance Application.... 390
3.22 Alarm Host.... 399
3.22.1 Adding Alarm Host.... 399
3.22.2 Entering Alarm Controller Interface.... 401
3.22.3 Updating Alarm Controller Status.... 403
3.22.4 Alarm Controller Application.... 403
4 Maintenance Guide.... 409
4.1 Backup and Restore.... 409
4.1.1 Backup.... 409
4.1.2 Restore....411
4.2 Update.... 413
4.3 Log.... 415
4.4 Password Maintenance.... 416
4.4.1 Changing Password.... 416
4.4.2 Resetting Password.... 417
Appendix 1 Service Module Introduction.... 420
Appendix 2 Shortcut Key List.... 422
Appendix 3 Deleting Videos on Central Server.... 423
Appendix 4 Cybersecurity Recommendations.... 424

1 Overview

1.1 Product Positioning

Optiview VMX is an important surveillance platform product in Optiview Surveillance (Optiview Video Management Software), design for medium-small project. Optiview VMX supports simple, reliable, open and more features which bring user with HD, smart, safe experience. By extending to 512 channels via License, it needs to integrate access control and VDP device organizations in order to provide solutions. Optiview VMX is widely used for residence, supermarket, factory, casino and other scenarios.

1.2 Highlights

- GPU decoding.
- Vector graph design, perfect support over 4K display.
- Both administrator and operator use the client with powerful control experience.
- Export device list from Optiview VMS, and import device list on Optiview VMX. No need to add device again when switching from Optiview VMS to Optiview VMX.
- Within LAN, auto search device in different network segment and show device list. One-click to add management. Save deployment time effectively.
- Mobile phone APP. Realize access anytime when you are not there.
- Auto and manual backup of database. Quickly recover when system error occurs.
- Lock record, permanent storage of important record footage, without being overwritten.

2 Installation and Deployment

2.1 Preparations

2.1.1 Server Configuration Requirement

Please refer to Table 2-1 for the requirements of server config.

Table 2-1 Server configuration requirement

OPTIVIEW VMX Server Configuration Requirement	
Recommended config	CPU: Intel® Xeon® CPU E3-1220 v5 @3.00GHz RAM: 18 GB Network adapter: 1Gps installation directory space: Over 500 GB
Minimum config	CPU: i3-2120 RAM: 8 GB Network adapter: 1Gps OPTIVIEW VMX installation directory space: Over 200 GB
System	Support Win10 and later systems. 🕮 The manual takes Windows Server 2012 R2 as an example to introduce how to configure server IP address and system time.

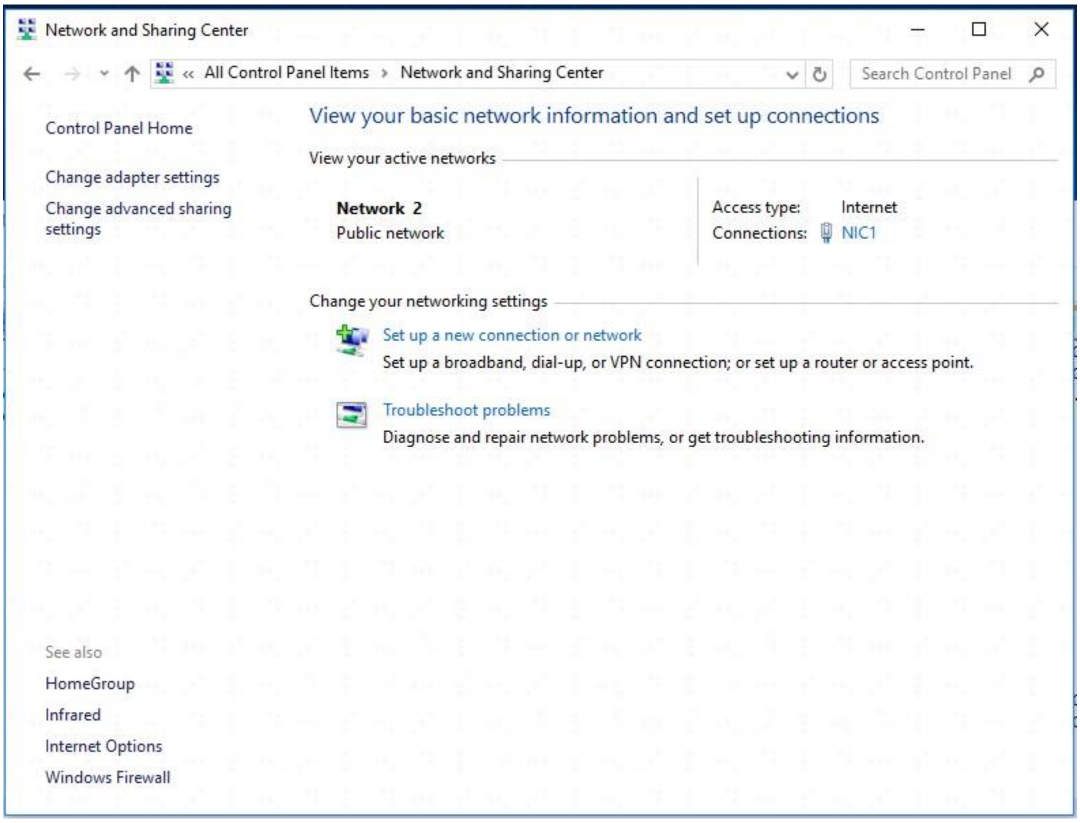
2.1.2 Configuring Server IP Address

Server IP address is platform IP address, modify server IP address and make sure the platform is well connected with other devices in the networking.

Step 1 Connect server to mouse, keyboard and monitor, connect to network cable, power on and start the server.

Step 2 Select ⊞ **> Control Panel > Network and Internet > Network and Sharing**.
The **Network and Sharing** is displayed. See Figure 2-1.

Figure 2-1 Network and sharing center


Network and Sharing Center
All Control Panel Items > Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Infrared
Internet Options
Windows Firewall

View your basic network information and set up connections

View your active networks

Network 2
Public network

Access type: Internet
Connections: NIC1

Change your networking settings

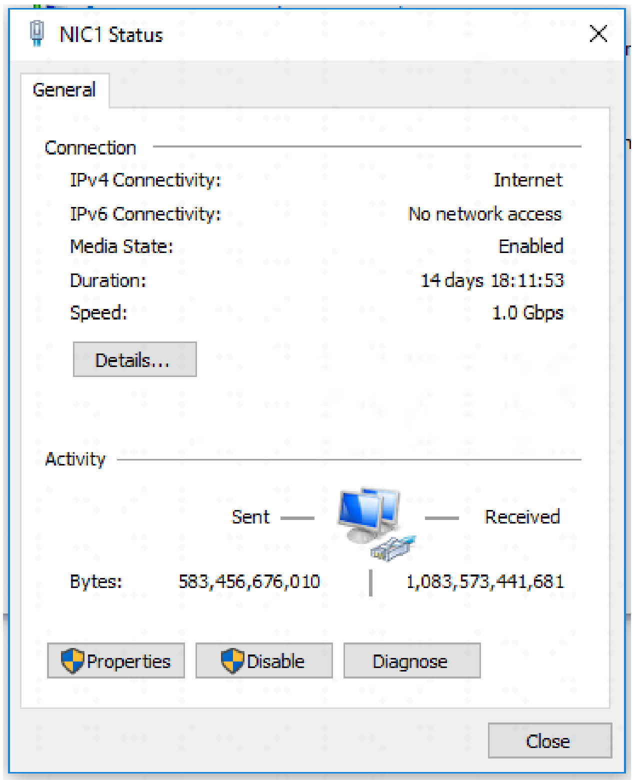
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Step 3 Click **Ethernet0**.

The **Ethernet0 Status** interface is displayed. See Figure 2-2.

Figure 2-2 Ethernet0


NIC1 Status
General
Details...
Properties
Disable
Diagnose
Close

Connection

IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 14 days 18:11:53
Speed: 1.0 Gbps

Activity

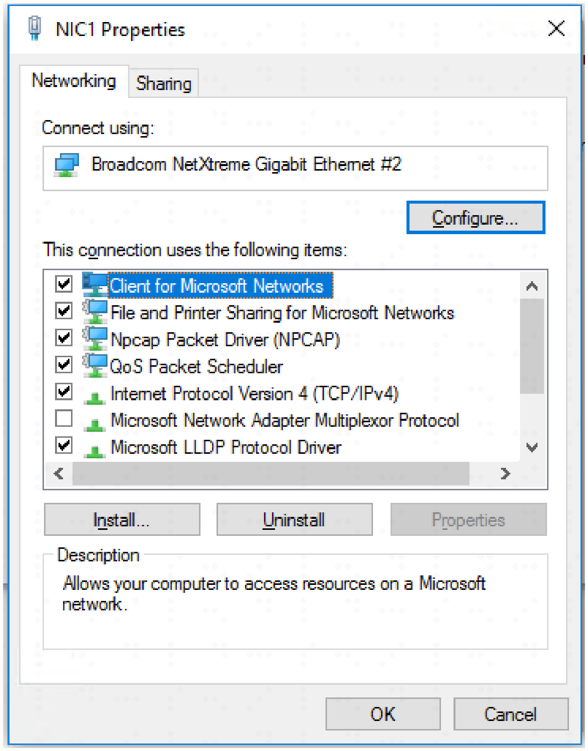
Sent — Received

Bytes: 583,456,676,010 | 1,083,573,441,681

Step 4 Click **Properties**.

The system displays network configuration info. See Figure 2-3.

Figure 2-3 Ethernet0 properties



NIC1 Properties

Connect using:

Broadcom NetXtreme Gigabit Ethernet #2

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Npcap Packet Driver (NPCAP)
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

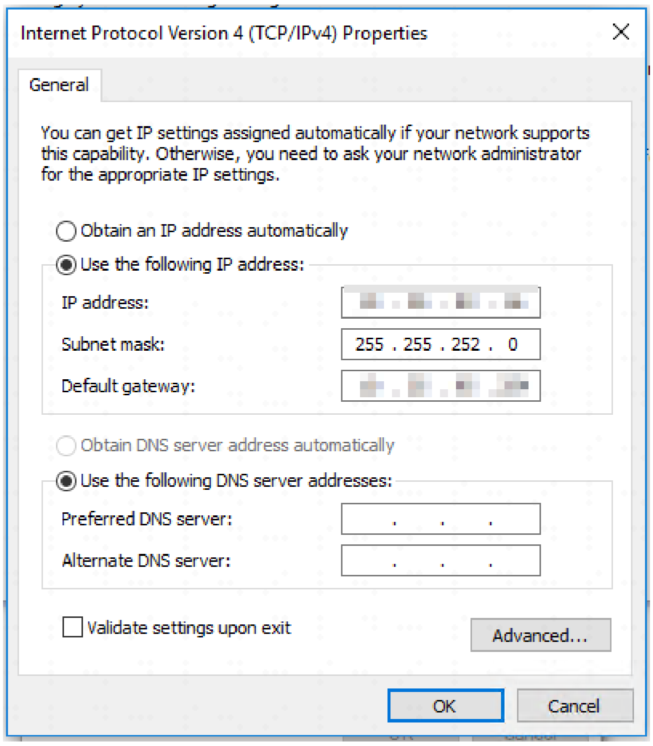
Description

Allows your computer to access resources on a Microsoft network.

Step 5 Double-click IPv6 or IPv4 according to network environment. The chapter takes IPv4 as an example.

The system displays **Internet Protocol Version 4 (TCP/IPv4)** properties. See Figure 2-4.

Figure 2-4 TCP/IPv4 properties



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: [redacted]
Subnet mask: 255 . 255 . 252 . 0
Default gateway: [redacted]

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

Step 6 Select **Use Following IP Address(S)**; configure IP address info according to plan, and then click **OK**.

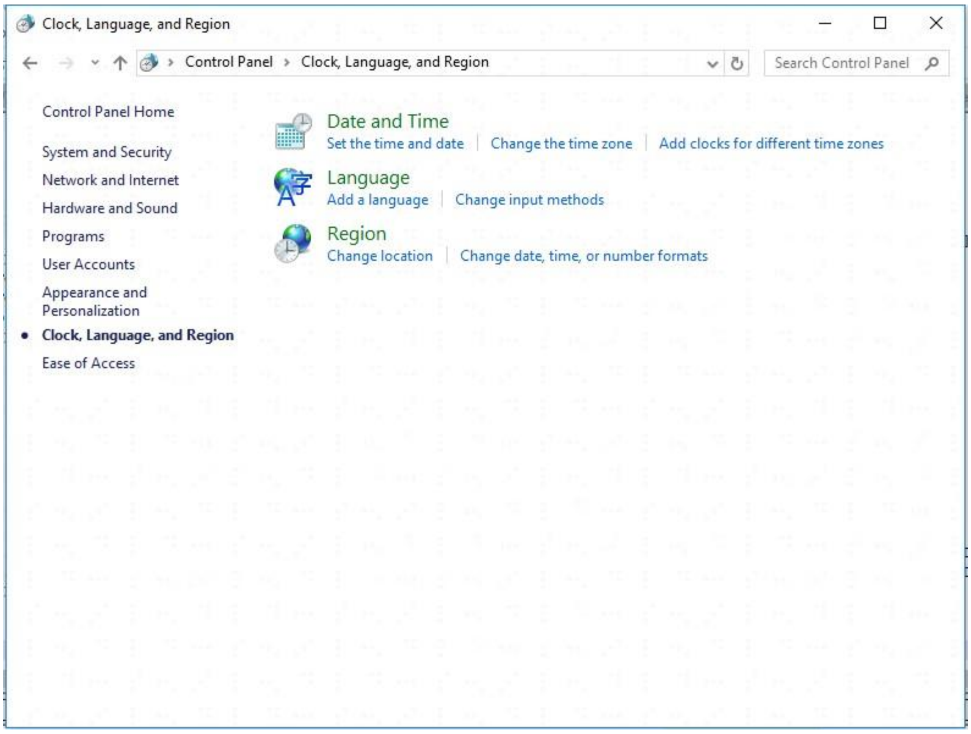
2.1.3 Configuring Server System Time

Modify server system time; make sure the server License is within expiry date and system time is in accordance with other devices in networking to avoid log and video loss.

Step 1 Select **> Control Panel > Clock, Language and Region**.

The **Clock, Language and Region** interface is displayed. See Figure 2-5.

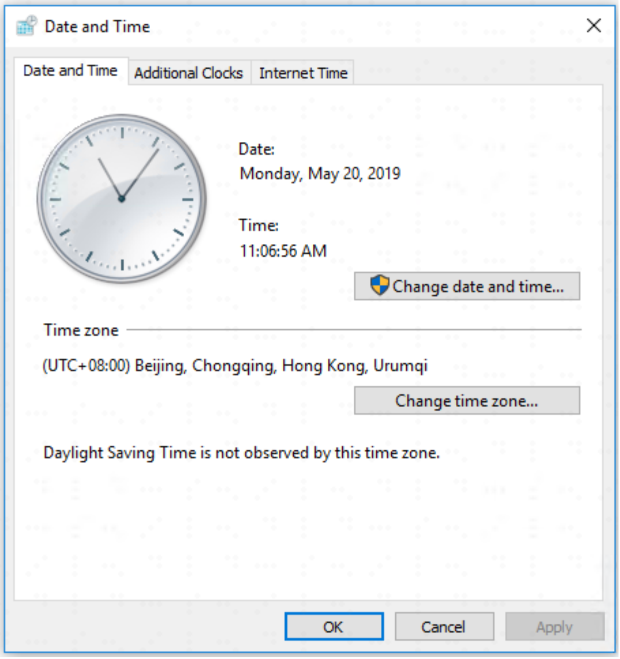
Figure 2-5 Clock, language and region


Clock, Language, and Region
Control Panel > Clock, Language, and Region
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Date and Time
Set the time and date | Change the time zone | Add clocks for different time zones
Language
Add a language | Change input methods
Region
Change location | Change date, time, or number formats

Step 2 Click **Date and Time**.

The **Date and Time** interface is displayed. See Figure 2-6.

Figure 2-6 Date and time


Date and Time
Date and Time
Additional Clocks
Internet Time
Change date and time...
Change time zone...
OK
Cancel
Apply

Date:
Monday, May 20, 2019

Time:
11:06:56 AM

Time zone
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Daylight Saving Time is not observed by this time zone.

Step 3 Set date and time.

1) Click **Change date and time**…

The date and time setting interface is displayed. See Figure 2-7.

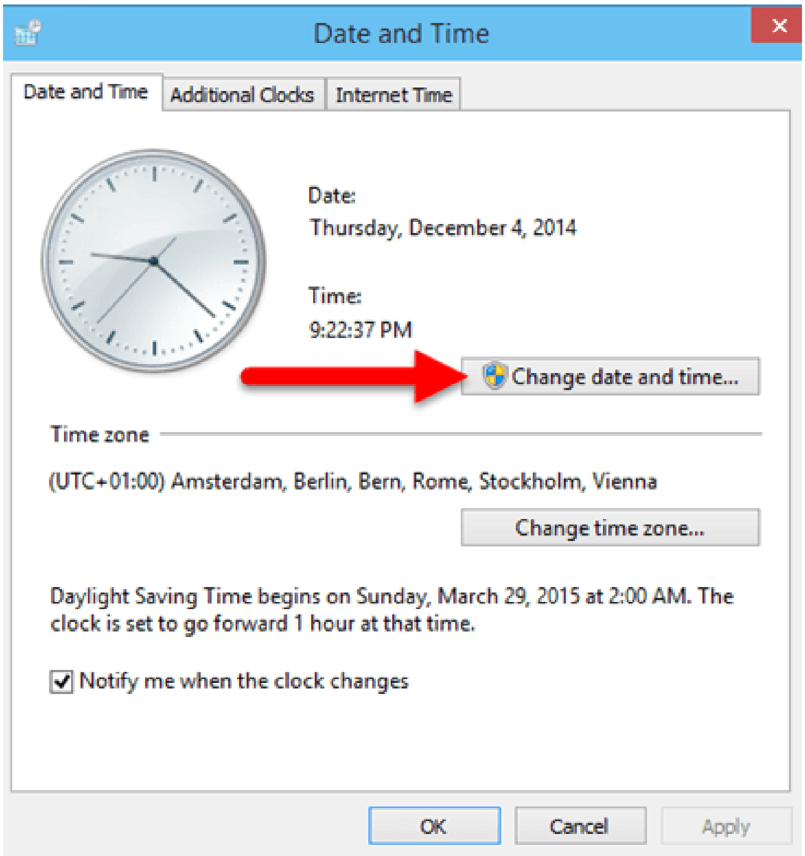

Date and Time
Date and Time
Additional Clocks
Internet Time
Date:
Thursday, December 4, 2014
Time:
9:22:37 PM
Change date and time...
Time zone
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Change time zone...
Daylight Saving Time begins on Sunday, March 29, 2015 at 2:00 AM. The clock is set to go forward 1 hour at that time.
☑ Notify me when the clock changes
OK
Cancel
Apply

Figure 2-7 Date and time setting

2) Select date, set time, click **OK**.

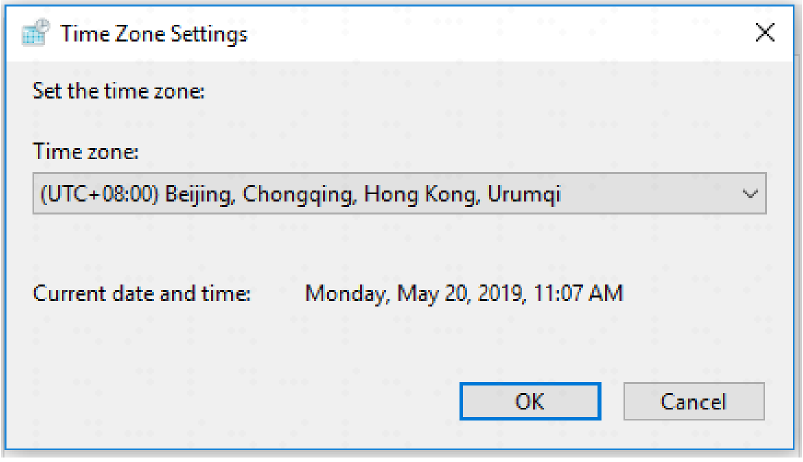
If you want to modify the calendar's date format or first day of week, click Change Calendar Setting to modify.

Step 4 Setting time zone.

1) Click **Change Time Zone (Z)**…

The **Time Zone Setting** interface is displayed. See Figure 2-8.

Figure 2-8 Time zone setting


Time Zone Settings
Set the time zone:
Time zone:
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Current date and time:
Monday, May 20, 2019, 11:07 AM
OK
Cancel

2) Select your time zone, and click **OK**.

Step 5 Click **OK**.

Server system time setting is completed.

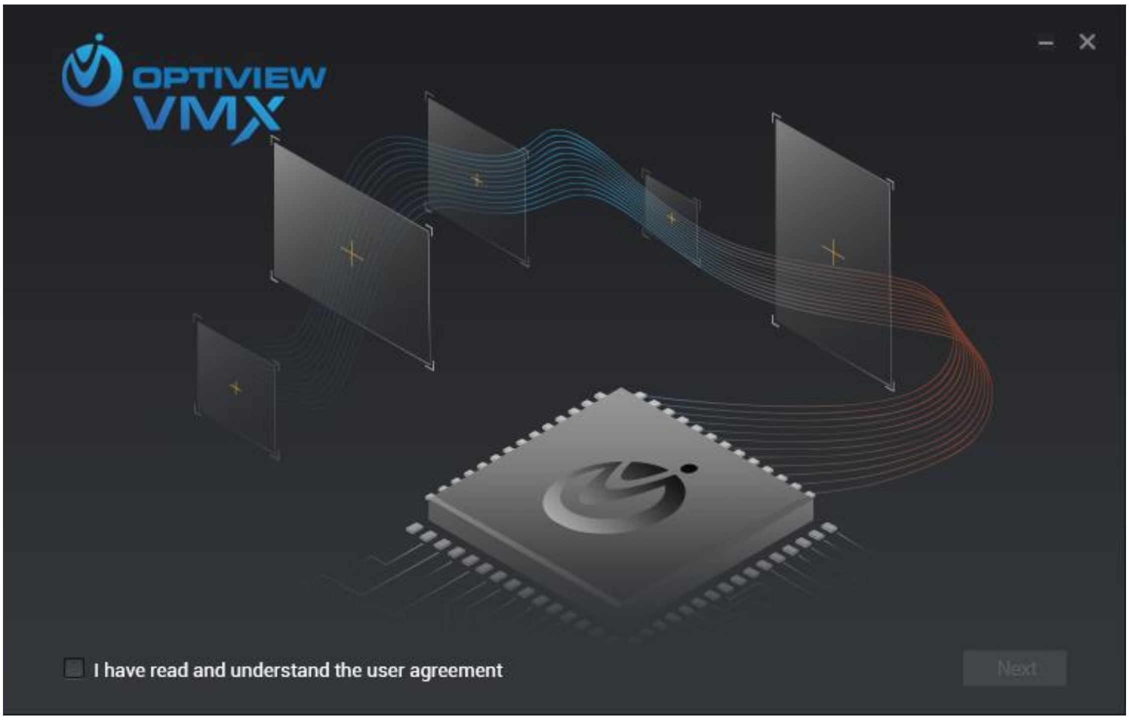
2.2 Installing Program (Update)

- Make sure you have acquired program before update, otherwise please contact technical support for update program.
- Program name includes version number and date, please check before installation.

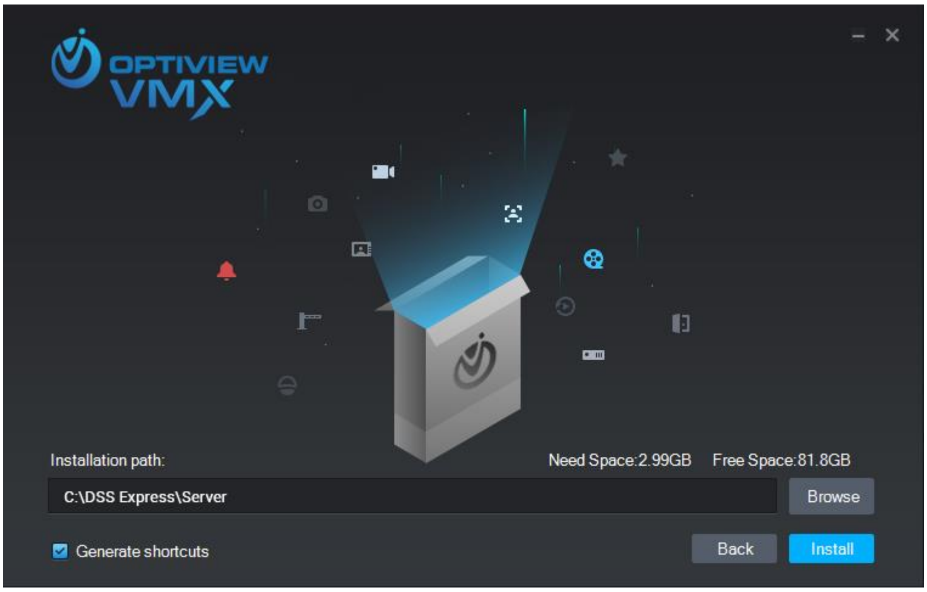
Step 1 Double-click installer.

The agreement interface is displayed. See Figure 2-9.

Figure 2-9 Agreement confirm


OPTIVIEW
VMX
☐ I have read and understand the user agreement
Next

Step 2 Select I have read and agree the OPTIVIEW VMX agreement, click Next. The installation path interface is displayed. See Figure 2-10



Installation path: C:\DSS Express\Server

Need Space:2.99GB Free Space:81.8GB

☑ Generate shortcuts

Figure 2-10 Select installation path

Step 3 Click **Browse** and select installation path, click **Install**.

The system displays installation progress, the whole installation needs 5-10 minutes. See Figure 2-11 after installation is completed. The server starts automatically after installation.

- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** beomes gray, and installation cannot be implemented.
- Do not select **Generate Shortcuts** if it is not necessary.
- If port conflict exists, the system will prompt conflicted port during installation. Open Optiview VMX Server and modify port after installation is completed. See 2.3.2 Modifying Service Port for more details.

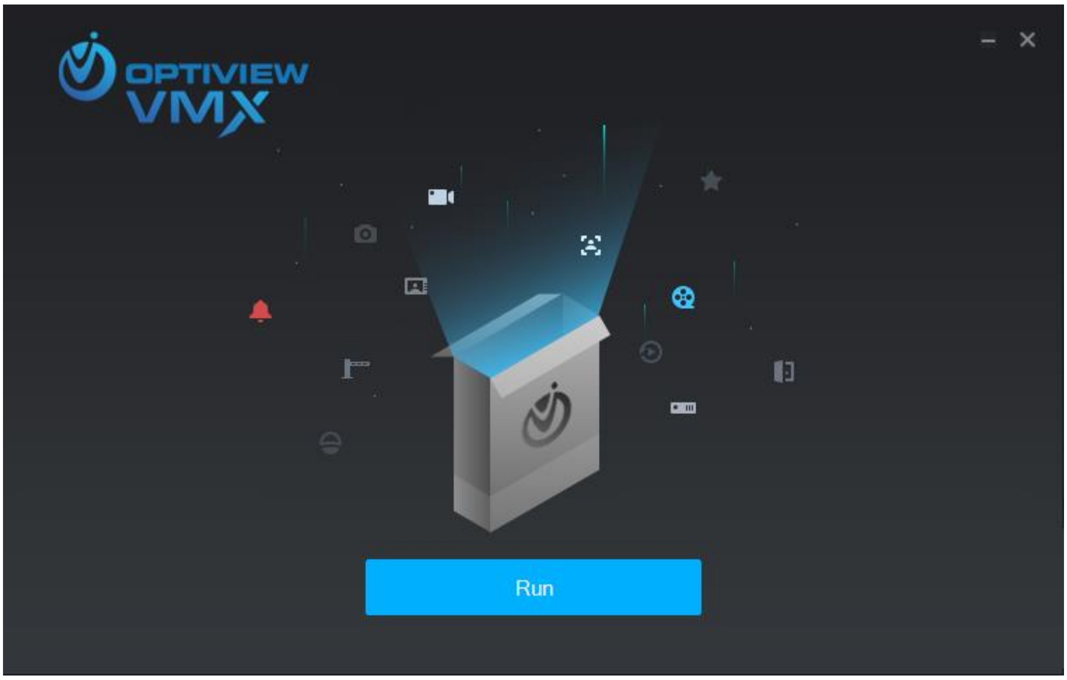


Figure 2-11 Installation completed

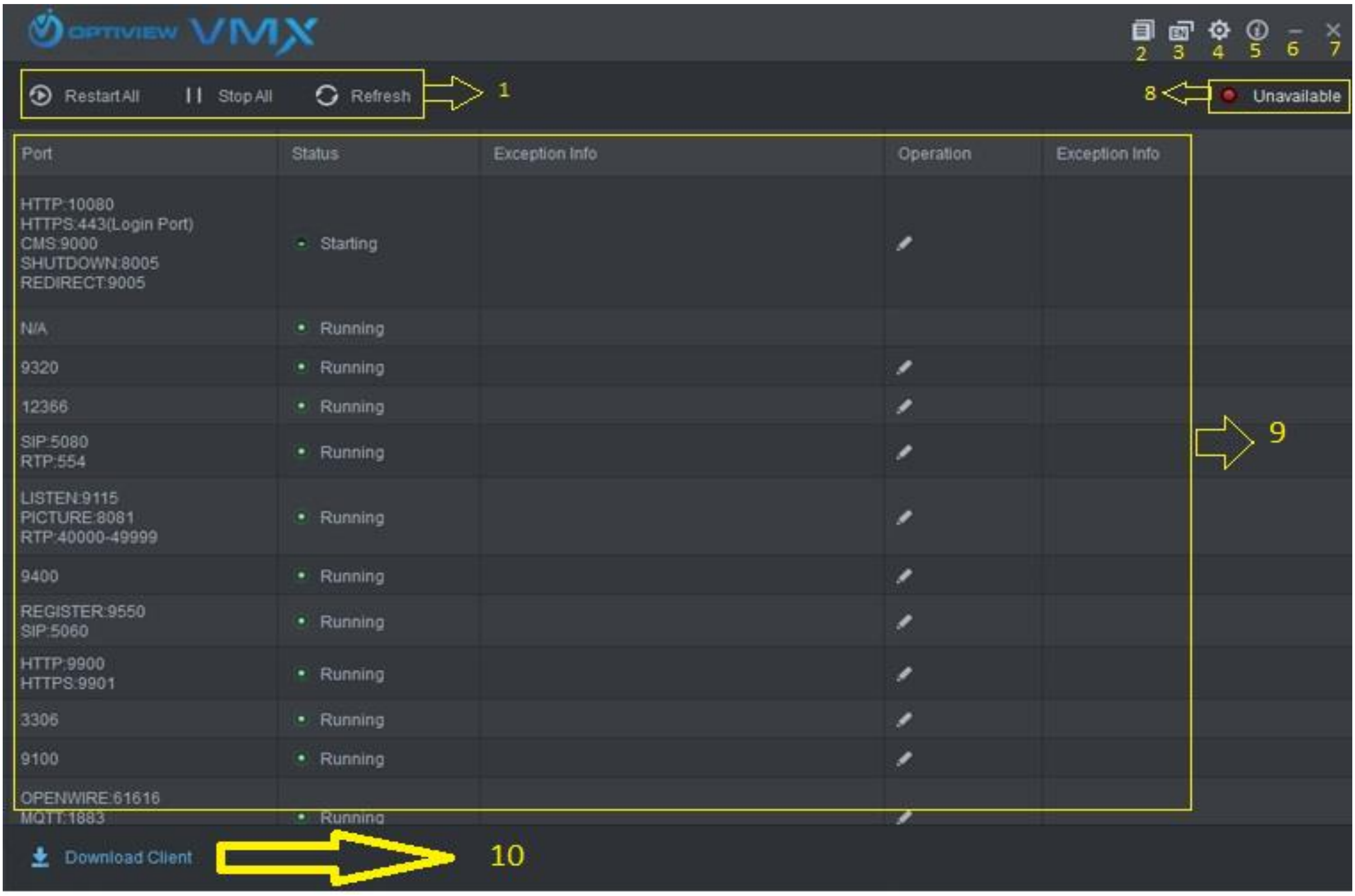
2.3 Service Management

You can modify service port, stop service and start service. If both device and platform are in two different network segments, the platform supports configuring network mapping, make sure the platform can be accessed by two different network segments.

2.3.1 Logging in System Config Tool

Introduce login method and interface of server system config tool.

Double-click on the server desktop, or click **Run** on the interface after program installation is completed. The system displays the interface of system config tool. See Figure 2-12. For interface description, see Table 2-2.



Port	Status	Exception Info	Operation	Exception Info
HTTP:10080 HTTPS:443(Login Port) CMS:9000 SHUTDOWN:8005 REDIRECT:9005	Starting		✎	
N/A	Running			
9320	Running		✎	
12366	Running		✎	
SIP:5080 RTP:554	Running		✎	
LISTEN:9115 PICTURE:8081 RTP:40000-49999	Running		✎	
9400	Running		✎	
REGISTER:9550 SIP:5060	Running		✎	
HTTP:9900 HTTPS:9901	Running		✎	
3306	Running		✎	
9100	Running		✎	
OPENWIRE:61616 MQTT:1883	Running		✎	

Figure 2-12 System config

Table 2-2 Module introduction

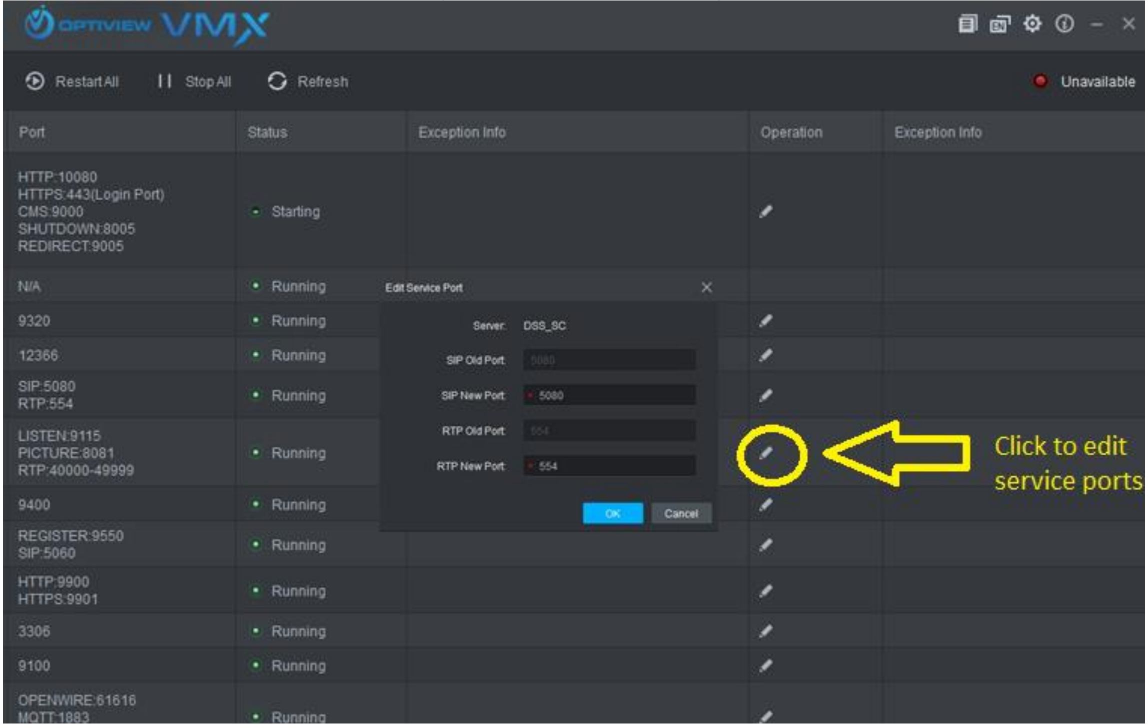
No.	Function	Description
1	Service Management	Service management, support following three types of operation. ● Click Restart All and restart all services. ● Click Stop All and stop all services. ● Click Refresh and refresh all services.
2	Language	Click the icon to switch language, the language takes effect after the server restarts.
3	Setting	Set CMS IP as server IP address. If device and platform exist in two different network segments, then you need to configure mapping address as IP address of the other network segment, make sure both segments can access platform.
4	About	Click the icon and view software version and release date.
5	Minimize	Click the icon and minimize config tool interface.
6	Close	Close config tool.

No.	Function	Description
7	Service Status	Include following service status. ● ● Starting, service is being started. ● ● Unavailable, service is abnormal. ● ● Stopping, service is being stopped. ● ● Running, all services are running normally. ● ● Stopped, all services are stopped.
8	Server Display	Display each service and service status. Click ✎ and you can modify server port, after that the system automatically restarts services.
9	Download Client	Click the icon and jump to WEB interface, then you can download client installation program.

2.3.2 Modifying Service Port

Step 1 On the interface of system config tool, click ✎ of the target server whose port you want to modify. The system displays the interface of Edit Service Port. See Figure 2-13.

Figure 2-13 Edit service port



Port	Status	Exception Info	Operation	Exception Info
HTTP:10080 HTTPS:443(Login Port) CMS:9000 SHUTDOWN:8005 REDIRECT:9005	Starting		✎	
N/A	Running			
9320	Running		✎	
12366	Running		✎	
SIP:5080 RTP:554	Running		✎	
LISTEN:9115 PICTURE:8081 RTP:40000-49999	Running		✎	
9400	Running		✎	
REGISTER:9550 SIP:5060	Running		✎	
HTTP:9900 HTTPS:9901	Running		✎	
3306	Running		✎	
9100	Running		✎	
OPENWIRE:61616 MQTT:1883	Running		✎	

Server: DSS_SC
SIP Old Port: 5080
SIP New Port: 5080
RTP Old Port: 554
RTP New Port: 554

Click to edit service ports

Step 2 Modify service port, click **OK**.

The system automatically restarts services after modified successfully.

- Default port of “OPTIVIEW VMX_PTS” service is “8081”, which is often occupied. You are recommended to modify the port.
- The system prompts when the port is occupied; please modify port according to prompt.

2.3.3 WAN and LAN Mapping

If both device and platform are in two different network segments, the platform supports configuring network mapping, and make sure two network segments can access platform.

2.3.3.1 Configuring Mapping Rule

Access platform according to the mapping rule formulated in advance. Mapping rule configuration method differs depending on different products; refer to corresponding user manual for more details. For the ports needed to be opened and its description, refer to "Appendix 1 Service Module Introduction" for more details.

DMZ mapping is recommended if router is used in networking. If environment is not allowed, then port mapping is available.

If port is occupied by other mapping, for example, port 80 is occupied, then you need to modify it as 81, you need to modify port first, then add mapping rule on the router. For more details, please refer to "2.3.2 Modifying Service Port."

WAN and LAN port of the server is not distinguished by system, port configuration options are unified and WAN/LAN ports are consistent. (Server port does not distinguish WAN or LAN, both belongs to the same port number.)

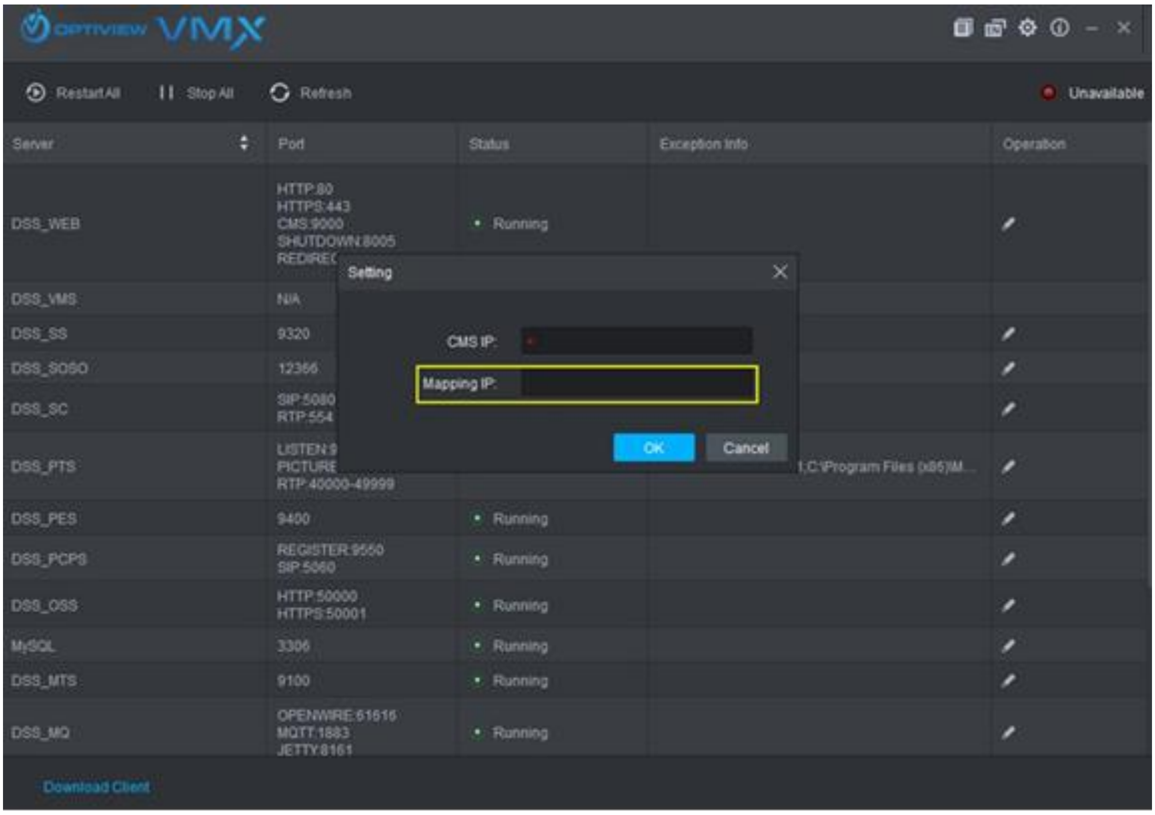
2.3.3.2 Configuring Mapping IP

If device and platform are in two different segments, the platform supports configuring network mapping and realizing access to different segments.

Step 1 On the interface of system config tool, click ⚙ on the upper right corner.

The system displays **Config** interface. See Figure 2-14.

Figure 2-14 Config

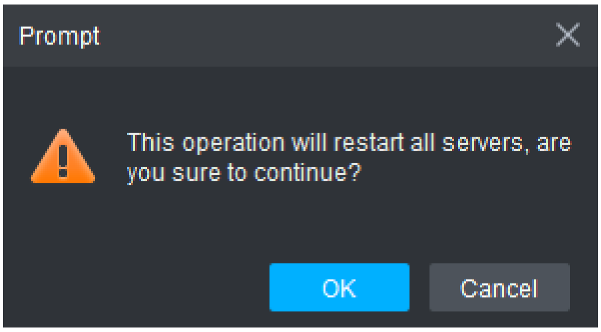


Server	Port	Status	Exception Info	Operation
DSS_WEB	HTTP:80 HTTPS:443 CMS:9000 SHUTDOWN:8005 REDIREC	● Running		✎
DSS_VMS	N/A			
DSS_SS	9320			✎
DSS_SOSO	12366			✎
DSS_SC	SIP:5080 RTP:554			✎
DSS_PTS	LISTEN:9 PICTURE RTP:40000-49999		1;C:\Program Files (x86)\M...	✎
DSS_PES	9400	● Running		✎
DSS_PCPS	REGISTER:9550 SIP:5060	● Running		✎
DSS_OSS	HTTP:50000 HTTPS:50001	● Running		✎
MySQL	3306	● Running		✎
DSS_MTS	9100	● Running		✎
DSS_MQ	OPENWIRE:61616 MQTT:1883 JETTY:8161	● Running		✎

Step 2 Set **Mapping IP** as IP address of the other segment, and then click **OK**.

The system pops up **Prompt** dialog box. See Figure 2-15.

Figure 2-15 Prompt



This operation will restart all servers, are you sure to continue?

Step 3 Click **OK** and system restarts services.

2.4 Installing Client

2.4.1 Installing Client

You can manage and operate platform by client, client includes PC client and mobile APP.

2.4.1.1 PC Client

2.4.1.1.1 PC Configuration Requirement

For configuration requirement of PC where OPTIVIEW VMX Client is installed, see Table 2-3.

Table 2-3 Configuration requirement

PC Configuration Requirement	
Recommended Config	CPU: i5-6500 Basic frequency: 3.20GHz Memory: 8GB Graphic card: Intel® HD Graphics 530 Network adapter: 1Gbps OPTIVIEW VMX client installation directory space: 100GB
Min Config	CPU: i3-2120 Memory: 4GB Graphic card: Intel（R）Sandbridge Desktop Gra Network adapter: 1Gbps OPTIVIEW VMX installation directory space: 50GB

2.4.1.1.2 Download and Install

Step 1 Enter server IP address into browser, click **Enter**.
The system displays the interface of downloading client. See Figure 2-16.

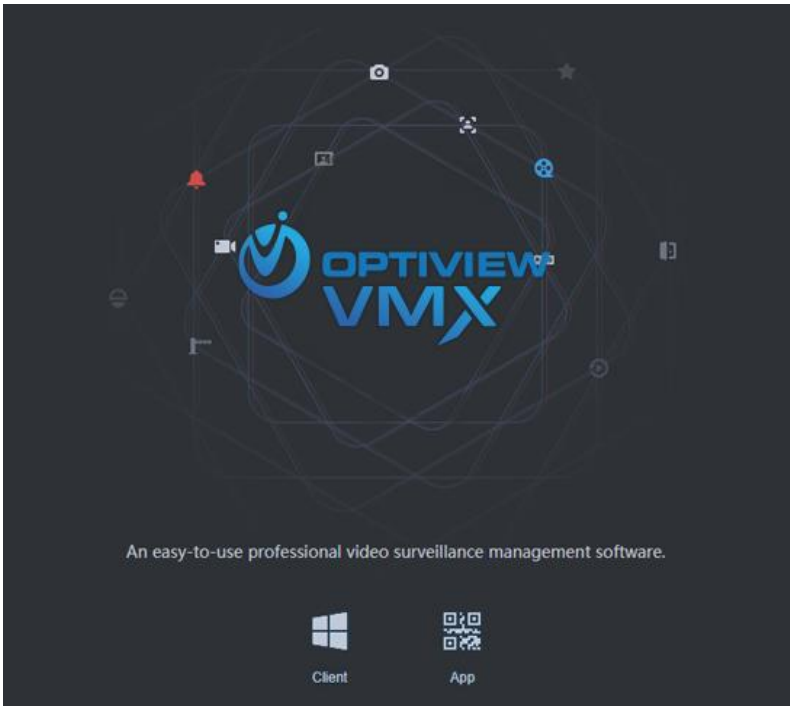

OPTIVIEW VMX
An easy-to-use professional video surveillance management software.
Client
App

Figure 2-16 Download client

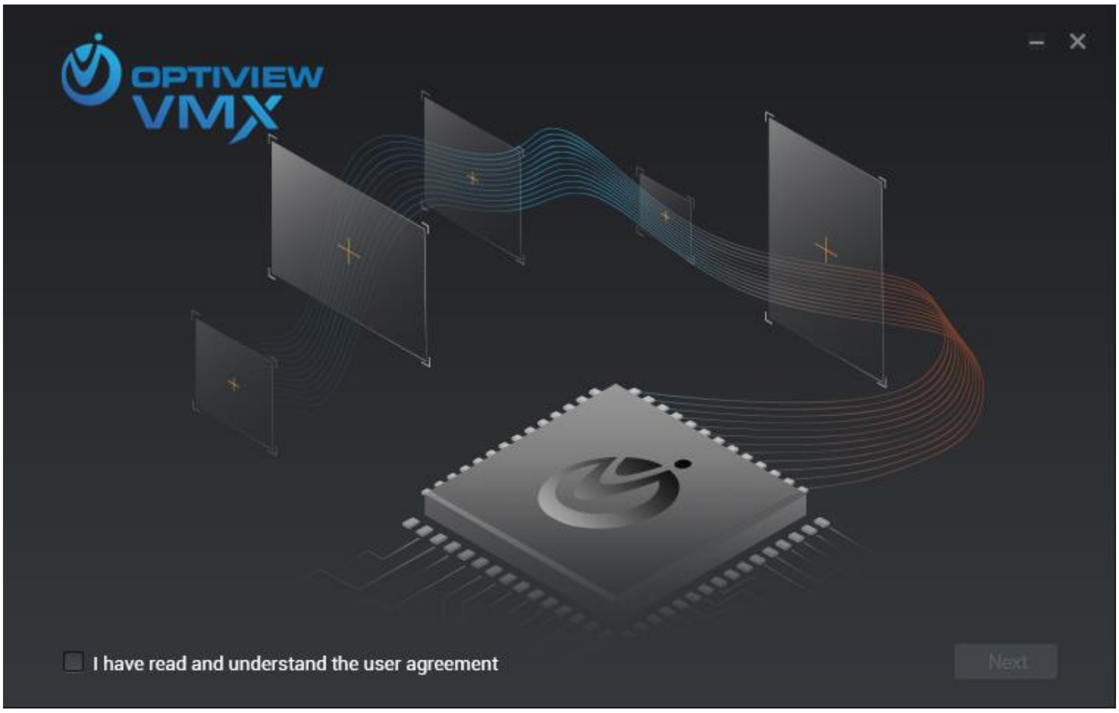
Step 2 Double-click ⊞, run or download client according to interface prompt. For more download details, see Table 2-4.

Table 2-4 Download operation

Operation	Description
Run	Download temporary file, you can install after it is checked.
Save	Download installation package to IE default path.
Save as	Download installation package to designated path.
Save and Run	Download installation package to IE default path, and you can install after it is checked.

Step 3 Click **Run**, or Double-click client installation program under the save directory.

The system displays agreement interface. See Figure 2-17.



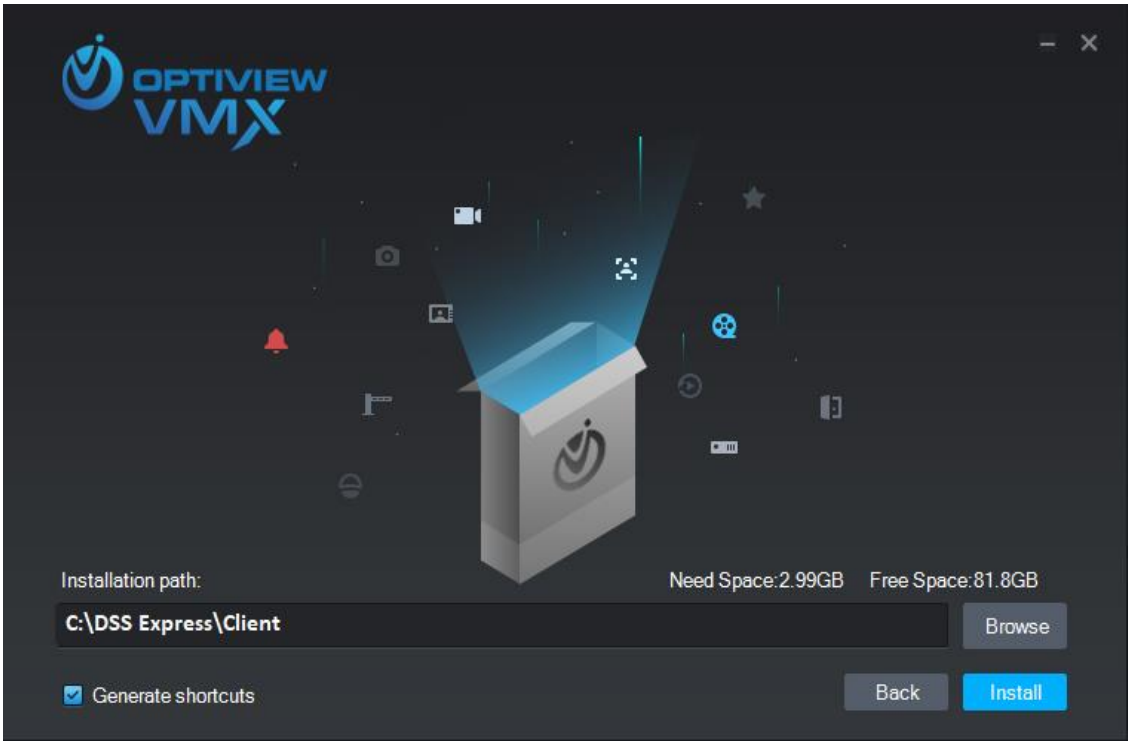
☐ I have read and understand the user agreement

Figure 2-17 Confirm agreement

Step 4 Select I have read and agree the OPTIVIEW VMX agreement, click **Next**.

The system displays the interface of installation path, See Figure 2-18.

Figure 2-18 Select installation path



Installation path: C:\DSS Express\Client

Need Space:2.99GB Free Space:81.8GB

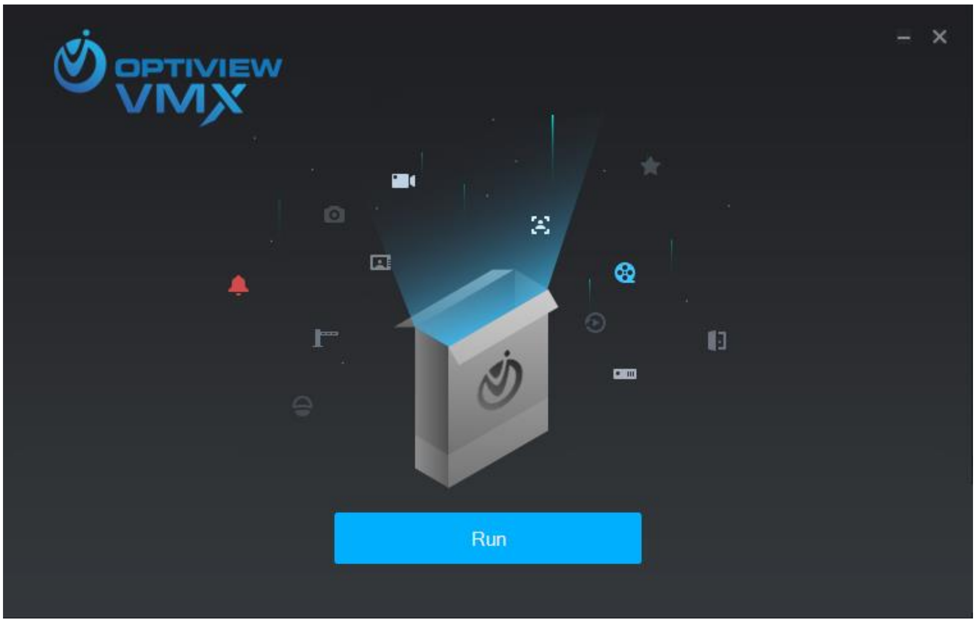
☑ Generate shortcuts

Step 5 Click **Browse** and select installation path, click **Install**.

The system displays installation progress, the installation takes about 2-3 minutes. The interface is shown in Figure 2-19 after installation is completed.

- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** beomes gray, and installation cannot be implemented.
- Do not select Generate Shortcuts if it is not necessary.

Figure 2-19 Installation completed



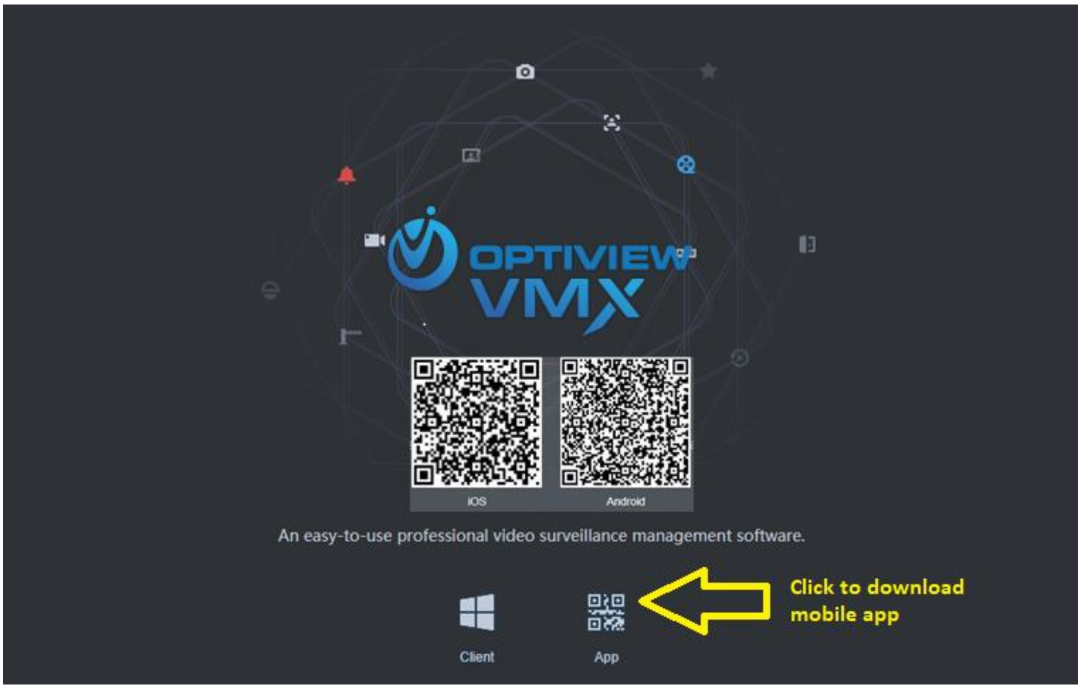
2.4.1.2 Mobile Phone APP

Currently mobile APP can be installed on IOS or Android.

This manual only introduces how to install mobile phone APP, for more operation details, please refer to APP help document.

Step 1 Enter server IP address into browser, click **Enter**.

The system displays the interface of downloading client. See Figure 2-20.



An easy-to-use professional video surveillance management software.

Click to download mobile app

Figure 2-20 Mobile APP QR code

Step 2 Move the mouse to App, use mobile phone to scan corresponding QR code, then acquire and install APP according to prompt.

2.4.2 Initialization Configurations

You need to initialize server if you log in for the first time. Modify password, set security questions for system user. You can find password by answering questions when you forget password.

Step 1 Double-click on server desktop, or click Run on the interface after program is installed. The system displays client login interface. See Figure 2-21.

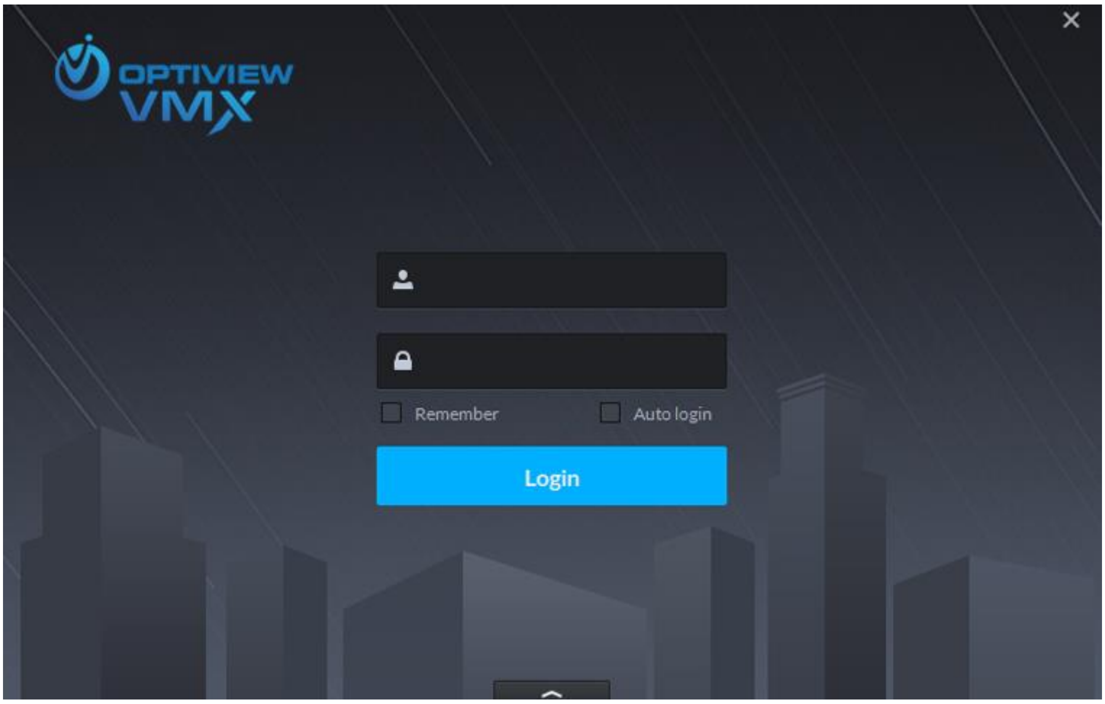

OPTIVIEW
VMX
☐ Remember
☐ Auto login
Login

Figure 2-21 Client login interface

Step 2 Enter username and password.

The default username and password is system, 123456 respectively.

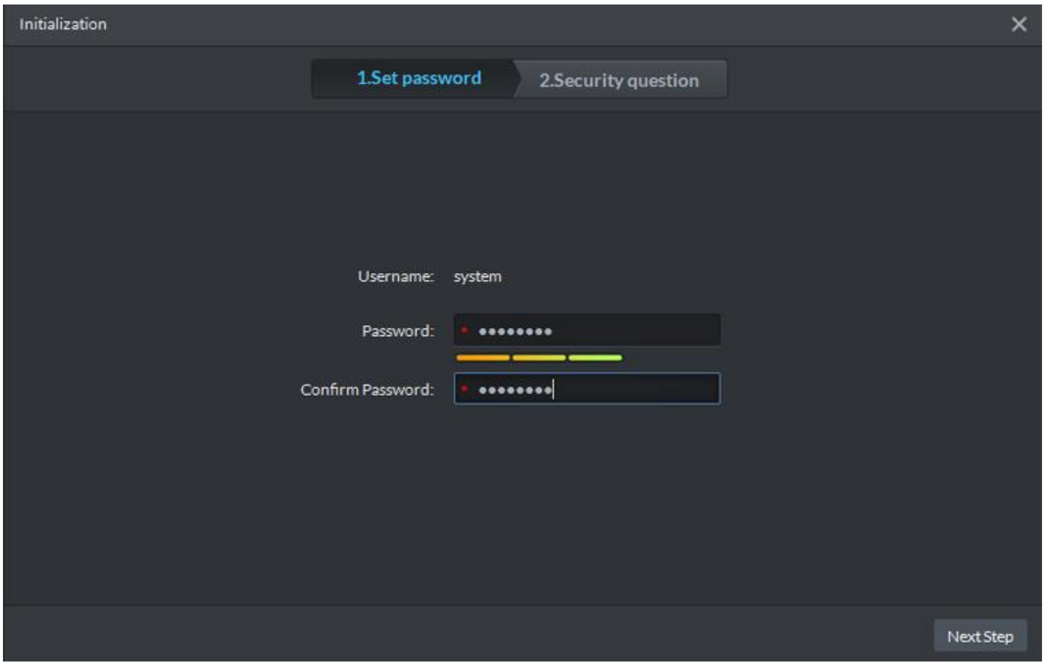
Step 3 Click ︿, enter server IP address and HTTPS port number.

HTTPS port number is 441 by default.

Step 4 Click **Login**.

The system displays the interface of **Set Password**. See Figure 2-22.

Figure 2-22 Set password


Initialization
1.Set password
2.Security question
Next Step

Username: system

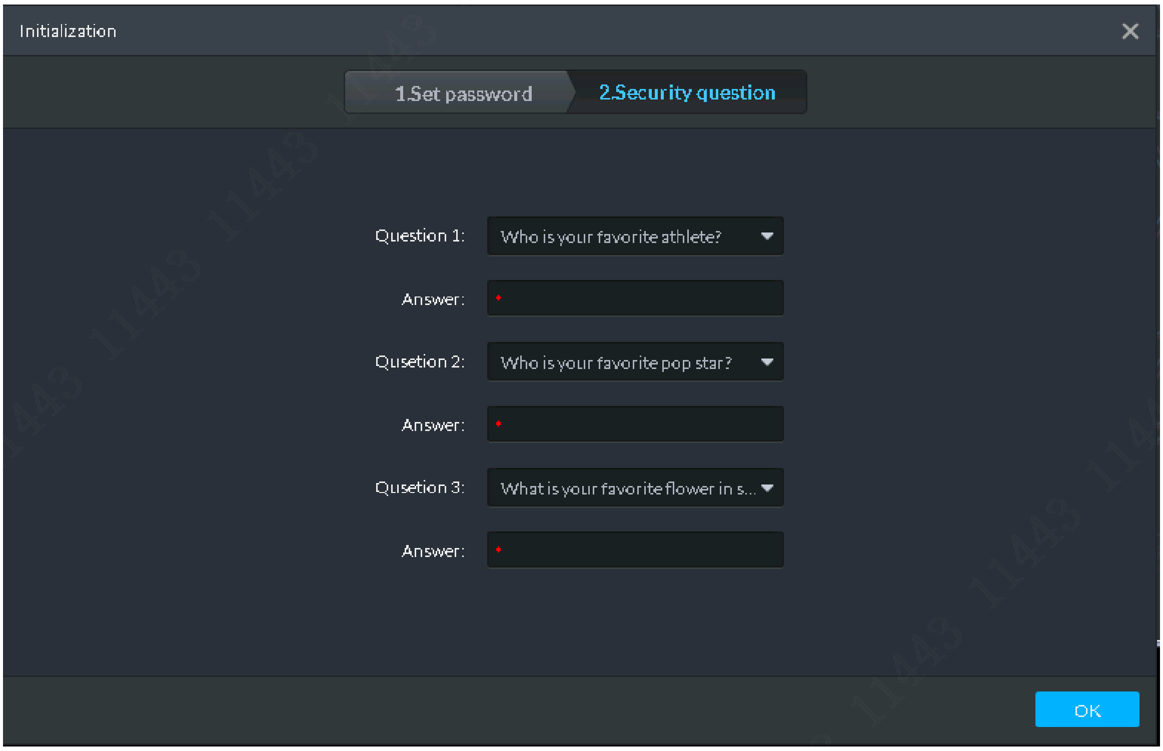
Password: •••••••••

Confirm Password: •••••••••

Step 5 Enter new password, click **Next**.

The system displays the **Security Question** interface. See Figure 2-23.

Figure 2-23 Security question


Initialization

1.Set password

2.Security question

Question 1: Who is your favorite athlete?

Answer:

Qusetion 2: Who is your favorite pop star?

Answer:

Qusetion 3: What is your favorite flower in s...

Answer:

OK

Step 6 Select question, set answer, then click **OK**.

The system displays **Homepage** interface by default.

2.4.3 Logging in to Client

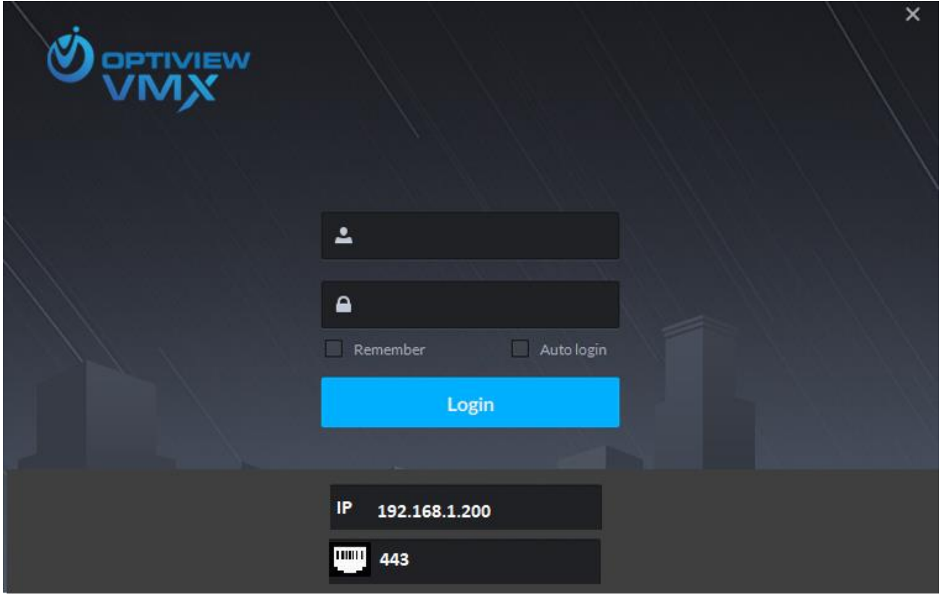
You can configure and manage the system remotely by using the client.

Step 7 Double-click the shortcut icon on the server desktop, or click **Run** on the program interface after the program installation is completed.

The client login interface is displayed.

See Figure 2-24.

Figure 2-24 Client login interface



IP 192.168.1.200

443

Step 8 Click , enter the IP address of your Optiview VMX platform, and the corresponding username and password, and then click **Login**.

The **Homepage** interface is displayed. See Figure 2-25. For homepage description, see Table 2-5.

- If you need to switch server IP address, click , enter server IP address and HTTPS port number. HTTPS port is 443 by default.
- If you select **Remember**, you do not need to enter the username and password again when logging in next time.
- If you select **Auto login**, the system will skip the login interface and directly open the homepage of the client when logging in next time.

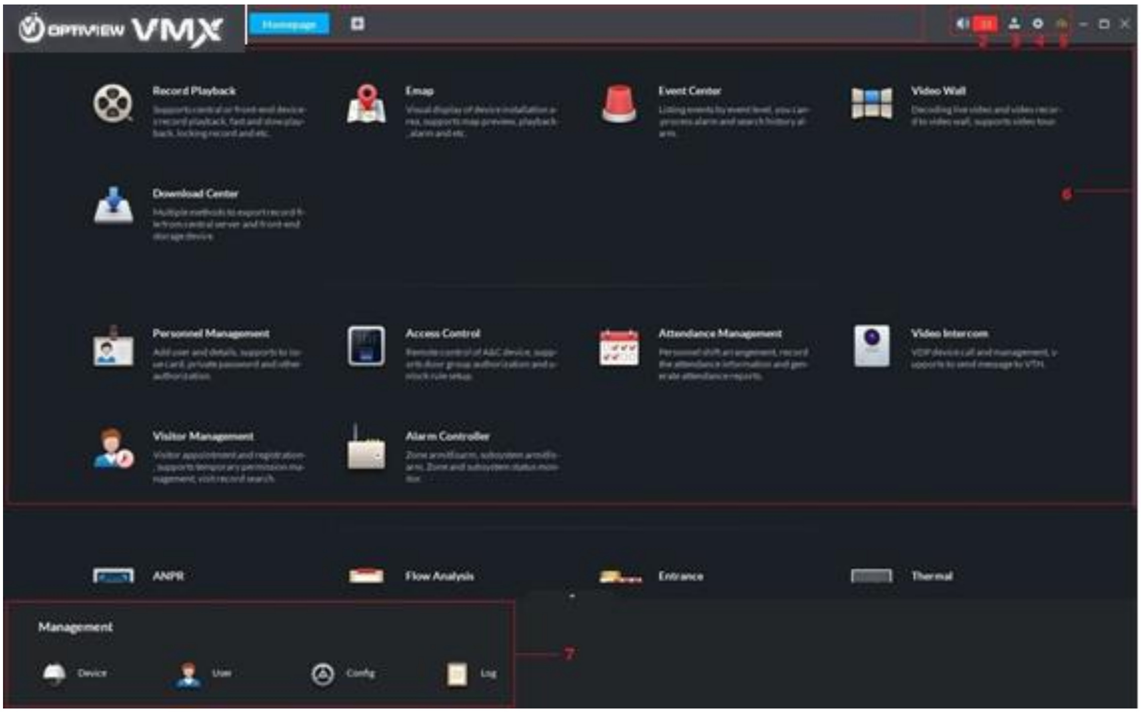

OPTIVIEW VMX
Homepage
2
3
4
5
Record Playback
Emap
Event Center
Video Wall
Download Center
6
Personnel Management
Access Control
Attendance Management
Video Intercom
Visitor Management
Alarm Controller
ANPR
Flow Analysis
Entrance
Thermal
Management
Device
User
Config
Log
7

Figure 2-25 Client homepage

Table 2-5 Client homepage description

No.	Name	Description
1	Function Tab	Display all opened tabs. Click ⊞ and you can select the module you want to open. **Homepage** tab and ⊞ are displayed by default.
2	Alarm	● 🔊: Alarm tone switch, the tone is on by default, click the icon and change to 🔇, tone is off. ● 0: Alarm quantity, when the number is not zero, you can click and jump to **Event Center** interface, and view alarm info.
3	User Info	Click the icon and select corresponding functions, you can modify password, lock client, view help and sign out. Supported operations are shown as follows: ● View login username and service IP address. ● Select **Change Password** and you can modify user password. ● Select Lock Client, and you can lock client and client is not allowed to operate. If you want to operate, click anywhere on client and enter password to unlock. ● Click **Help** to open user manual. ● Select About and view client version info and release date. ● Select **Sign Out** to log out, the system jumps to client login interface.

No.	Name	Description
4	Config	Click the icon and you can make settings, such as basic setting, video setting, video playback, snapshot setting, record, alarm and shortcut button.
5	System Status	Click the icon and you can view the status of server network, CPU and memory.
6	Function	Display live view, video playback, map, event center, video wall, download center, user management, access control and plate recognition. You can click corresponding function to enter.
7	Management	Display device management, user management, configuration management and log management. Click to enter corresponding management page. Click ▼ and you can hide the section.

2.5 Importing License

License includes free version and paid version. The free license is imported by platform by default. If you want higher performance, please purchase license of paid version immediately.

2.5.1 License Introduction

For the functions supported by free version, see Table 2-6. For the restricted functions, see Table 2-7.

Table 2-6 License version description

Module	Free Version	Paid version
Video	64 channels	512 channels
POS	2 channels	50 channels
Access Control	64 IP, 64 doors	200 IP, 1024 doors
Video Intercom	128 IP	1024 IP
Alarm Host	1 IP	100 IP
ANPR	2 channels	32 channels
Face Recognition	2 channels	64 channels
Client	1	100 simultaneous login
Mobile APP	1	100 simultaneous login
Attendance Terminal	4 channels	512 channels
OPTIVIEW VMX Mobile for VDP	10	5000 register

Table 2-7 Restricted functions of paid version

Function Module	Sub Function
Login	Multi-client login
Device	Onvif > 8 channels
Storage Management	Network disk 📖

Function Module	Sub Function
	IPSAN storage.
Video	Enable remote record
	Continuous snapshot
	ROI
	Alarm output control
	Switch playback
	Smart track (fisheye+PTZ)
	Playback on video wall
Event Management	Link video wall
	Event forwarding
	Send email 📖 Send email actively when dealing with event.
	Temporary disarm
	Alarm processing
Video Wall	Video wall tour
E map	Multi-layer map 📖 Hot zone application (only single layer map can be used)
	Visible range 📖 Restrict custom visible range.
Personnel Management	Issue cards in batch
	Import and export personnel in batch
	Access control track
Face Recognition	Face track

2.5.2 Applying for License

Step 1 Acquire license request file.

1) Click **Config** on the client homepage.

The system displays the **Config** interface. See Figure 2-26.

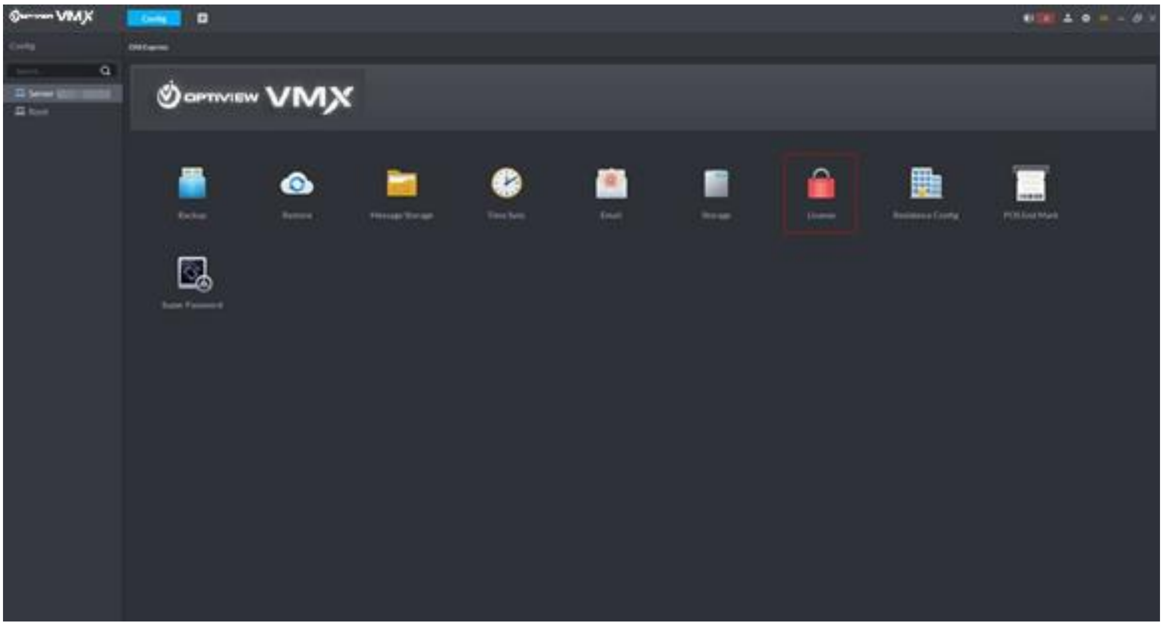
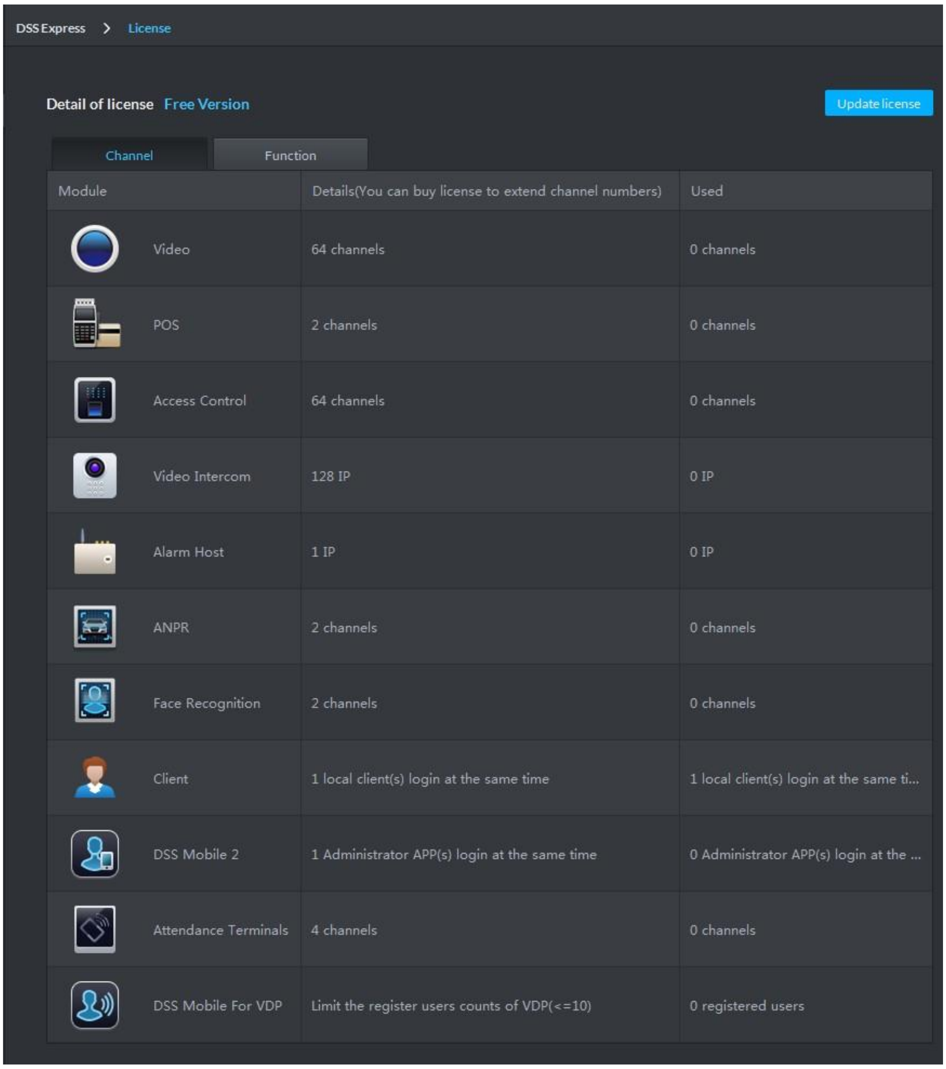


Figure 2-26 Config

2) Click **License**.

The system displays **License** interface. See Figure 2-27.

Figure 2-27 Export license request file



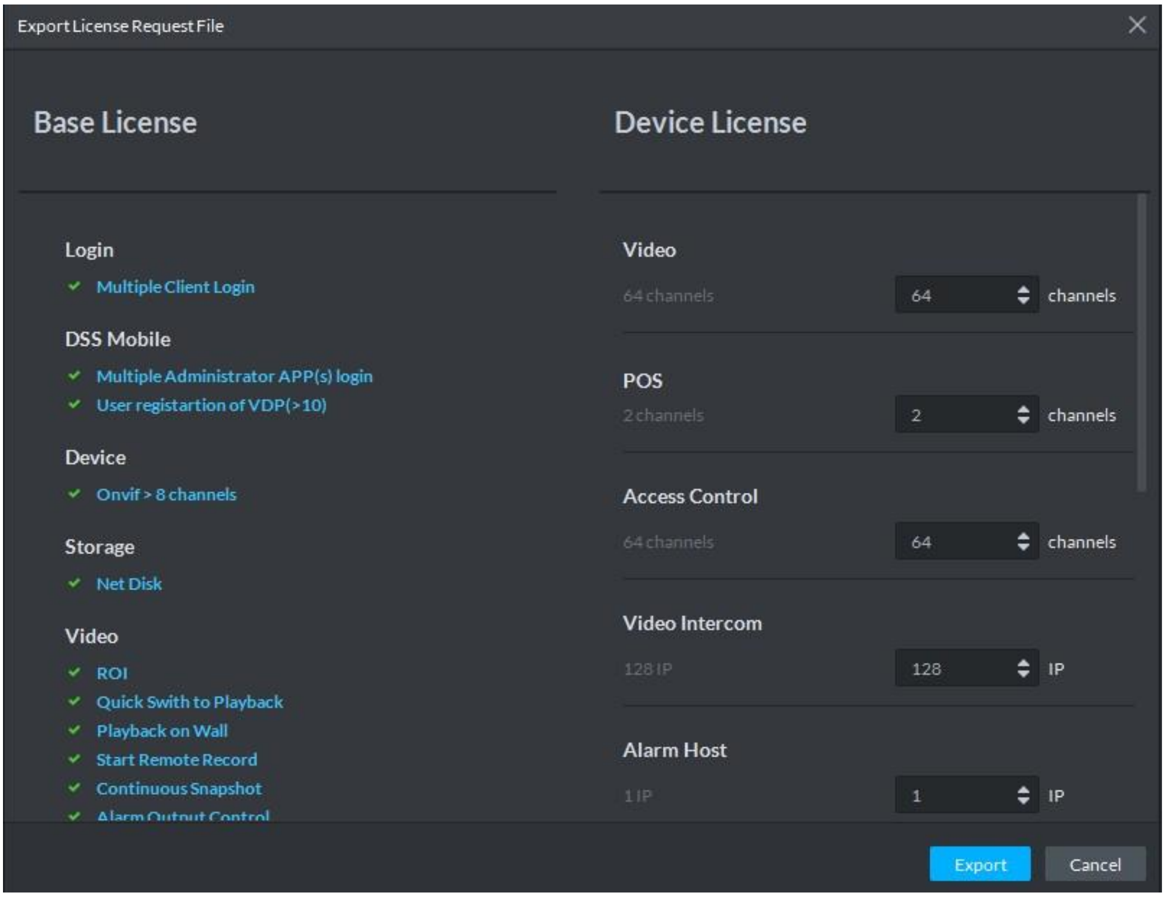
Detail of license Free Version

Module	Details(You can buy license to extend channel numbers)	Used
Video	64 channels	0 channels
POS	2 channels	0 channels
Access Control	64 channels	0 channels
Video Intercom	128 IP	0 IP
Alarm Host	1 IP	0 IP
ANPR	2 channels	0 channels
Face Recognition	2 channels	0 channels
Client	1 local client(s) login at the same time	1 local client(s) login at the same ti...
DSS Mobile 2	1 Administrator APP(s) login at the same time	0 Administrator APP(s) login at the ...
Attendance Terminals	4 channels	0 channels
DSS Mobile For VDP	Limit the register users counts of VDP(<=10)	0 registered users

3) Click **Export**.

The system displays the interface of **Export License Request File**, See Figure 2-28.

Figure 2-28 Export license request file



Base License

Login
- ✓ Multiple Client Login

DSS Mobile
- ✓ Multiple Administrator APP(s) login
- ✓ User registartion of VDP(>10)

Device
- ✓ Onvif > 8 channels

Storage
- ✓ Net Disk

Video
- ✓ ROI
- ✓ Quick Swith to Playback
- ✓ Playback on Wall
- ✓ Start Remote Record
- ✓ Continuous Snapshot
- ✓ Alarm Output Control

Device License

Video		
64 channels	64	channels
POS		
2 channels	2	channels
Access Control		
64 channels	64	channels
Video Intercom		
128 IP	128	IP
Alarm Host		
1 IP	1	IP

4) Enter channel and IP quantity according to actual situation, and then click **Export**. License request file is saved in the Optiview VMX client installation path in the form of .zip

Step 2 Send license request file to sales.

Sales make and return License file according to license request file.

2.5.3 Loading License

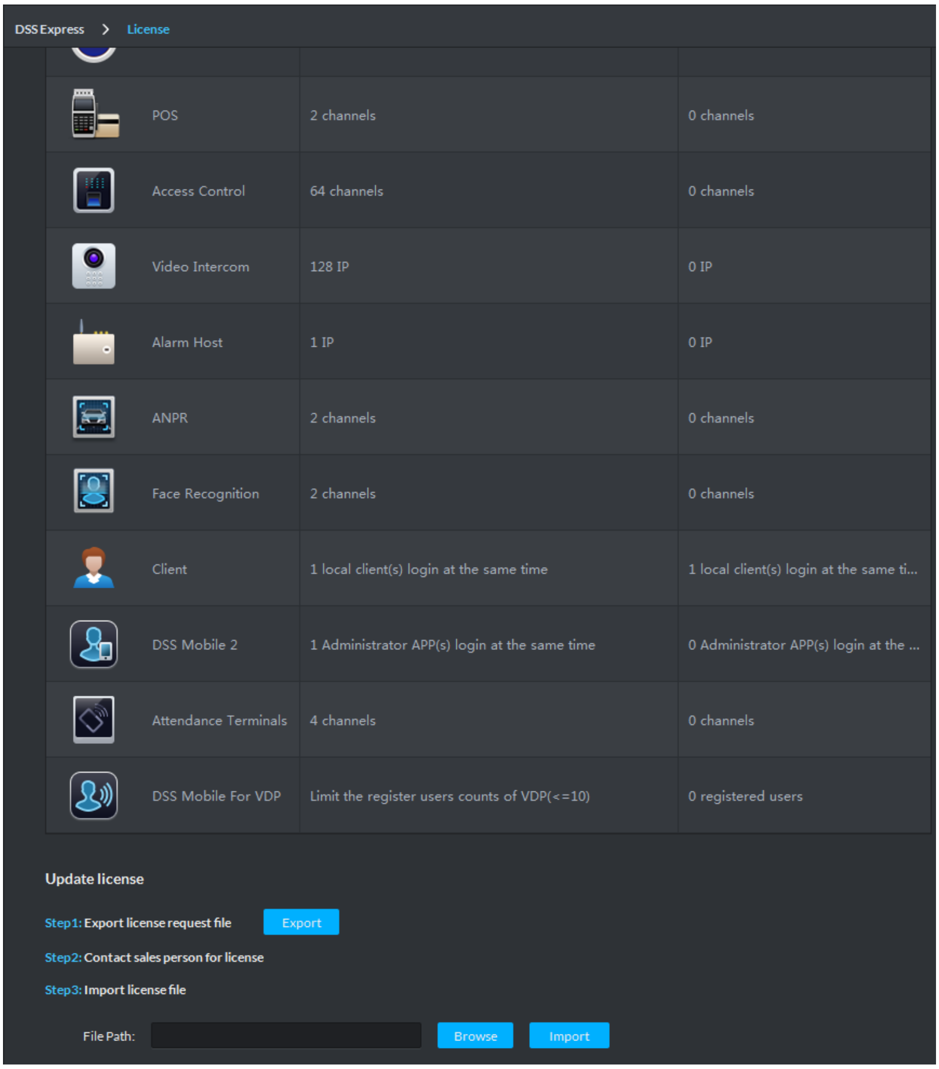
Step 1 On the client homepage, select **Config > License**.

The system displays the interface of **License**.

Step 2 Click Update License.

The system moves to the license update section, see Figure 2-29.

Figure 2-29 Update license


DSS Express > License

POS	2 channels	0 channels
Access Control	64 channels	0 channels
Video Intercom	128 IP	0 IP
Alarm Host	1 IP	0 IP
ANPR	2 channels	0 channels
Face Recognition	2 channels	0 channels
Client	1 local client(s) login at the same time	1 local client(s) login at the same ti...
DSS Mobile 2	1 Administrator APP(s) login at the same time	0 Administrator APP(s) login at the ...
Attendance Terminals	4 channels	0 channels
DSS Mobile For VDP	Limit the register users counts of VDP(<=10)	0 registered users

Update license

Step1: Export license request file

Step2: Contact sales person for license

Step3: Import license file

File Path:

Step 3 Click **Browse**, select License file you want to upload according to system prompt.

Step 4 Click Import.

Step 5 System loads License, after that the system prompts license info is changed and the program restarts.

Log in client again, enter license configuration interface, and make sure the License is the same as applied.

3 Operation Guide

3.1 Installing Client

After installing and logging in client, you can configure and manage server remotely. For detailed operation, see “2.4 Installing Client.”

3.2 Basic Configuration

After installation and deployment is completed, you need to configure basic information including add device, configure message storage, time sync, email, storage space, user and record plan.

3.2.1 System Setting

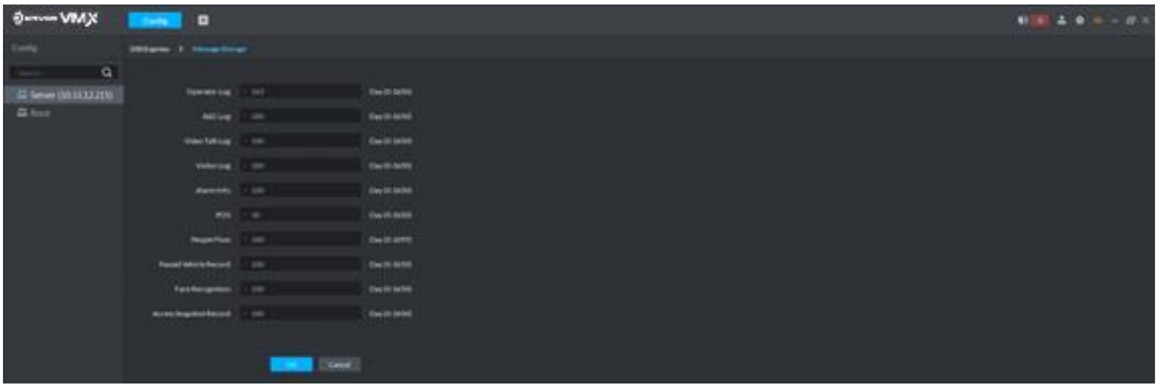
3.2.1.1 Setting Message Storage

You can set storage duration of operator log, A&C log, video talk log, alarm info, passed vehicle record, face recognition and picture storage. System deletes information when exceeding duration threshold.

Step 1 Enter the configuration interface of **Message Storage**.

1) On the client homepage, click **Config**.
   The system displays **Config** interface.
2) Click **Message Storag**e.
   The system displays **Message Storage** interface. See Figure 3-1.

Figure 3-1 Message storage



Step 2 Set storage duration log.

Step 3 Click **OK**.
The configuration is saved and takes effect.

3.2.1.2 Time Sync

Time sync means synchronizing the time between server and PC where client is located, server and accessed encoder or access control. The system time of server is considered as standard time after sync. The platform supports two methods of time sync which are auto and manual.

3.2.1.2.1 Auto Time Sync

The system automatically starts time sync within designated period and time.

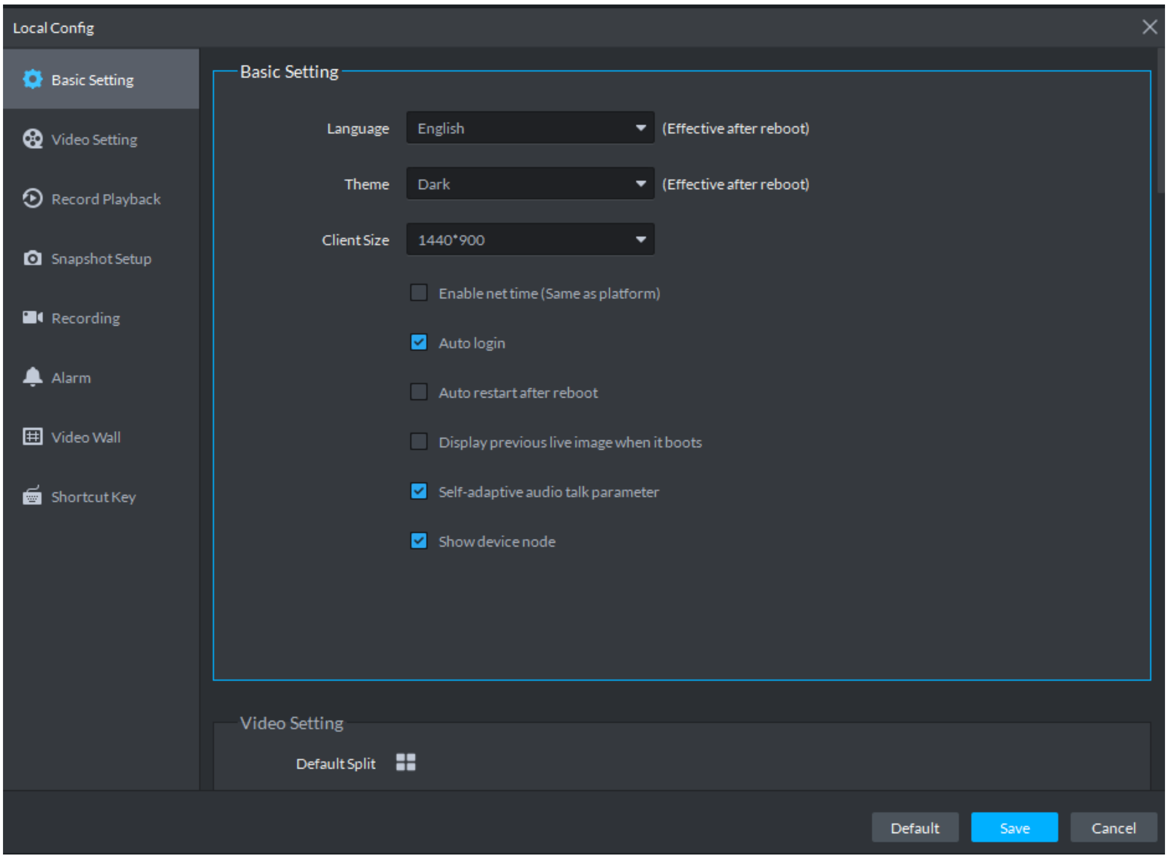
Step 1 Enable time sync on **Local Config** of client.(Optional)

Synchronize time between server and PC where client is located, the item is required to be configured. Skip the step if you only need to synchronize time of server and accessed device.

1) Click ⚙ on the upper right corner of client interface.

The system displays the interface of **Local Config**. See Figure 3-2.

Figure 3-2 Local config



Local Config

Basic Setting

Language: English (Effective after reboot)

Theme: Dark (Effective after reboot)

Client Size: 1440*900

☐ Enable net time (Same as platform)

☑ Auto login

☐ Auto restart after reboot

☐ Display previous live image when it boots

☑ Self-adaptive audio talk parameter

☑ Show device node

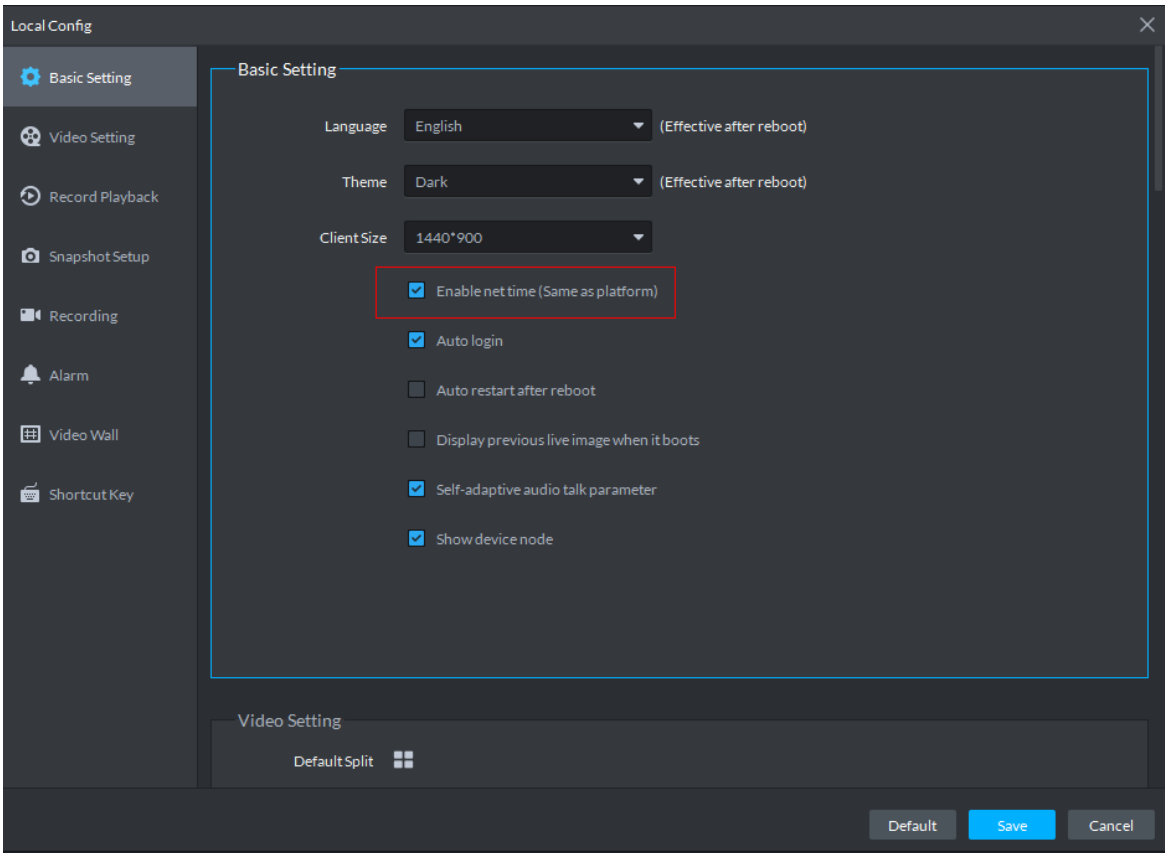
Video Setting

Default Split

2) Click the tab of **Basic Config**.

The system displays **Basic Config** interface. See Figure 3-3.

Figure 3-3 Enable net time


Local Config
Basic Setting
Video Setting
Record Playback
Snapshot Setup
Recording
Alarm
Video Wall
Shortcut Key
Default
Save
Cancel

Basic Setting

Language: English (Effective after reboot)

Theme: Dark (Effective after reboot)

Client Size: 1440*900

☑ Enable net time (Same as platform)

☑ Auto login

☐ Auto restart after reboot

☐ Display previous live image when it boots

☑ Self-adaptive audio talk parameter

☑ Show device node

Video Setting

Default Split

3) Select **Enable net time (Same as platform)**, click **Save**.

Enable net time on client of local config, the client immediately makes a net time request to server and complete time sync.

Step 2 Enter **Time Sync** configuration interface.

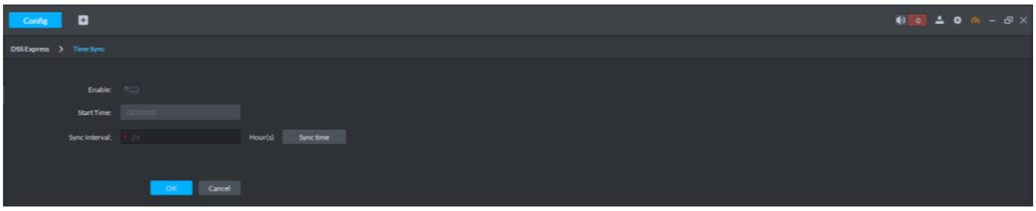
1) On client homepage, click **Config**.

The system displays **Config** interface.

2) Click **Time Sync**.

The system displays the interface of **Time Sync**. See Figure 3-4.

Figure 3-4 Time sync


Config
DSS Express
Time Sync
Sync time
OK
Cancel

Enable: ○

Start Time: 00:00:00

Sync Interval: * 24 Hour(s)

Step 3 Click ○ next to **Enable**, and enable auto time sync.

The icon becomes ● and auto time sync is enabled.

Step 4 Set start time and sync interval, click **OK**.

Set start time of each period, synchronize time between server and PC client, and synchronize time between server and accessed device.

3.2.1.2.2 Manual Time Sync

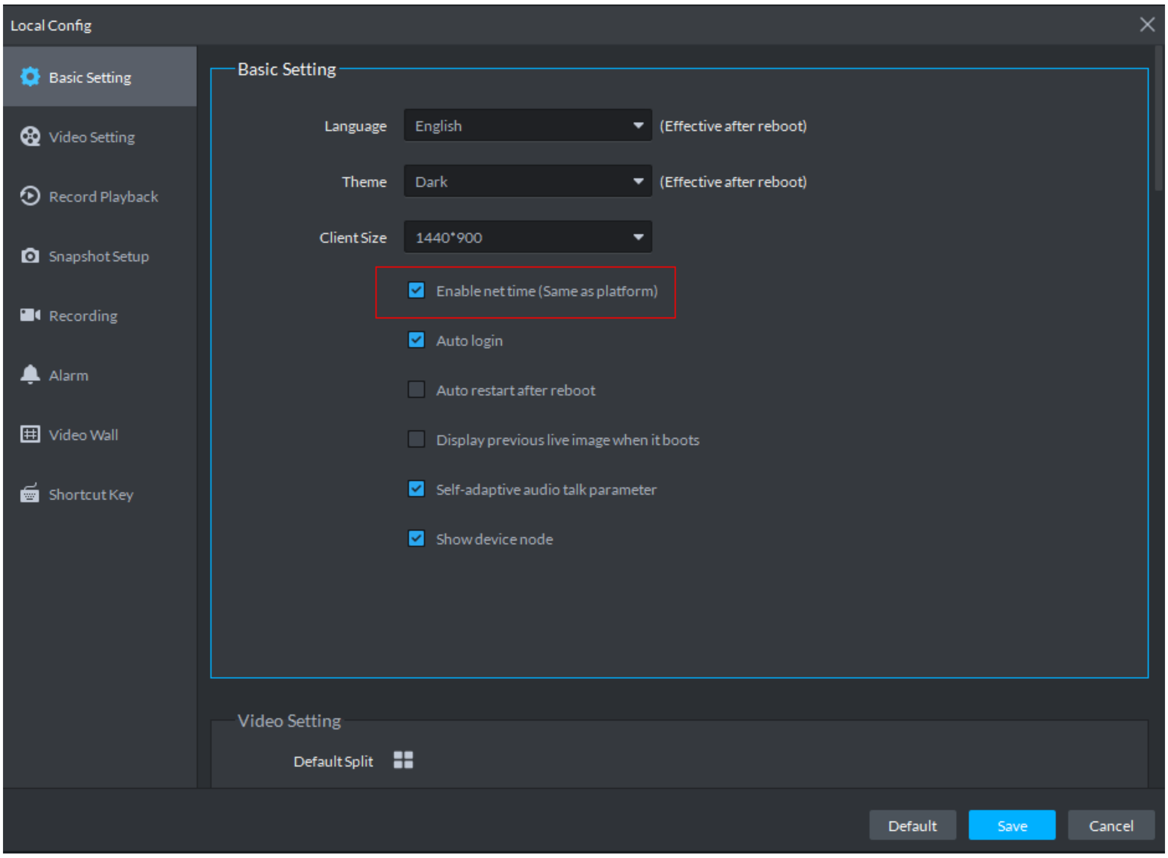
Start time sync request manually, and the system responds to request immediately.

Step 1 Enable time sync on **Local Config** of client.(Optional)

Synchronize time between server and PC client, the item is required to be configured. Skip the step if you only need to synchronize time of server and accessed device.

1) Click ⚙ on upper right corner of client interface.
   The system displays the interface of **Local Config**.
2) Click the tab of Basic Setting.
   The system displays the interface of **Basic Setting**. See Figure 3-5.

Figure 3-5 Enable client time sync



Basic Setting

Language: English (Effective after reboot)

Theme: Dark (Effective after reboot)

Client Size: 1440*900

☑ Enable net time (Same as platform)

☑ Auto login

☐ Auto restart after reboot

☐ Display previous live image when it boots

☑ Self-adaptive audio talk parameter

☑ Show device node

Default Split

3) Select **Enable net time (Same as platform)**, click **Save**.

Enable net time on client of local config, the client immediately makes a net time request to server and complete time sync.

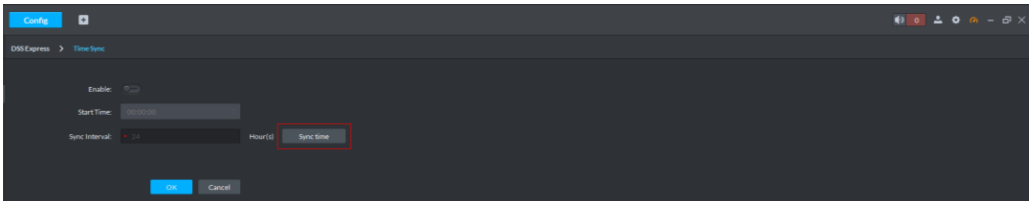
Step 2 Enter configuration interface of **Time Sync**.

1) On client homepage, click **Config**.
   The system displays **Config** interface.
2) Click Time Sync.
   The system displays the interface of Time Sync. See Figure 3-4.

Step 3 Click **Sync Time**, see Figure 3-6.

The system immediately synchronizes time between server and accessed device, server and PC client.

Figure 3-6 Sync time



Enable:
Start Time: 00:00:00
Sync Interval: * 24 Hour(s)

3.2.1.3 Setting Email

Set email address info, you can send email via designated email address when necessary. For example, after alarm linkage email is enabled, when alarm event occurs, the system automatically sends email to inform user.

Step 1 Enter the configuration interface of **Mail Server**.

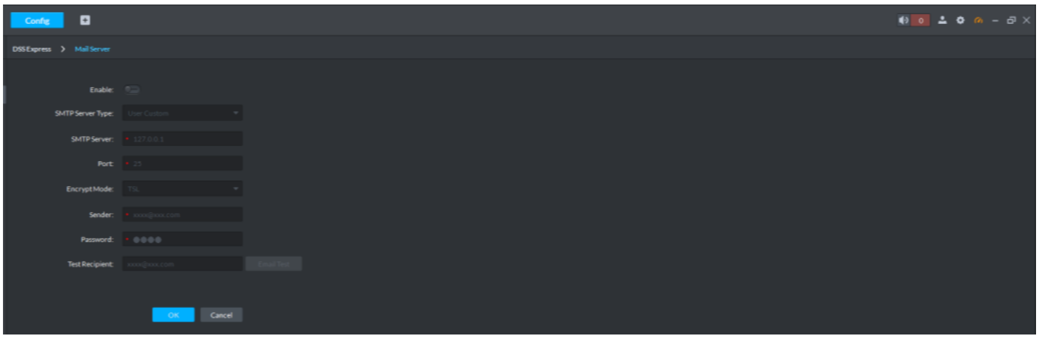
1) Click **Config** on the client homepage.

   The system displays **Config** interface.

2) Click **Email**.

   The system displays **Mail Server** interface. See Figure 3-7.

Figure 3-7 Email server



Enable:
SMTP Server Type: User Custom
SMTP Server: * 127.0.0.1
Port: * 25
Encrypt Mode: TSL
Sender: * xxxx@xxx.com
Password: * ●●●●
Test Recipient: xxxx@xxx.com

Step 2 Click ○, and enable email.

The icon becomes ● and the function is enabled.

Step 3 Select SMTP server type, set email address info, and click **OK**.

📖

TSL encryption method is highly recommended.

3.2.1.4 Setting Storage Space

Configure local storage space or connect network storage device, used to store pictures and videos.

3.2.1.4.1 Setting Local Storage Disk

The system automatically detects storage space of all the disks in the system, and creates exclusive space for platform, used to store videos, general pictures and ANPR pictures.

Step 1 Enter configuration interface of **Storage Manager**.

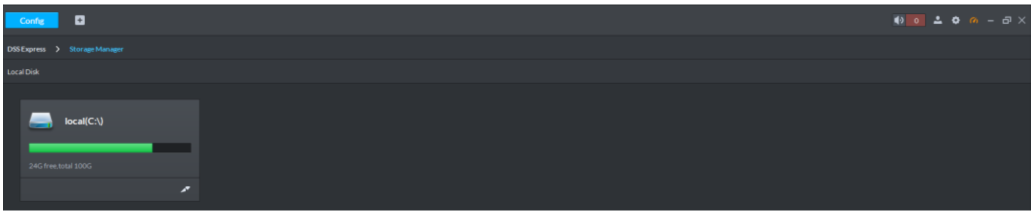
1) Click **Config** on the client homepage.

   The system displays the interface of **Config**.

2) Click **Storage**.

The system displays **Storage Manager** Interface; the system automatically detects disk info of server (Disk info of non PC client). See Figure 3-8.

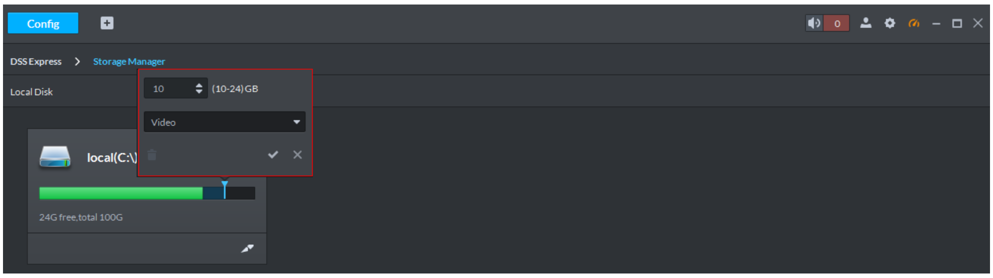
Figure 3-8 Storage manager


Config
DSS Express
Storage Manager
Local Disk
local(C:\)
24G free,total 100G

Step 2 Click .

The system pops out the dialog of setting storage space size and type. See Figure 3-9.

Figure 3-9 Create storage space


Config
DSS Express
Storage Manager
Local Disk
10
(10-24)GB
Video
local(C:\)
24G free,total 100G

Step 3 Set storage space size, select storage space type and click ✓.

Platform exclusive storage space is created on the disk, see Figure 3-10. The exclusive storage space is displayed in the red box.

- The minimum storage space is 10GB.
- Storage space type includes video, general picture and ANPR picture. Video disk is used to store video, ANPR picture disk is used to store ANPR snapshot, general picture is used to store all snapshots except ANPR pictures.
- One local disk can divide general pictures for once top, but it can also modify storage space of general pictures.
- If you want to delete the storage space, you can click the storage segment, and delete exclusive space setting according to system prompt. See Figure 3-11.

Figure 3-10 Disk status change

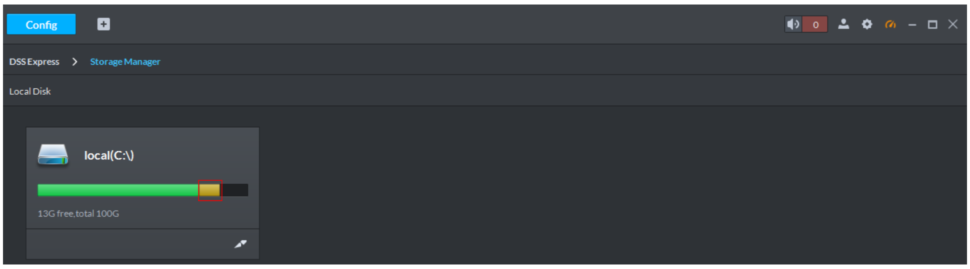
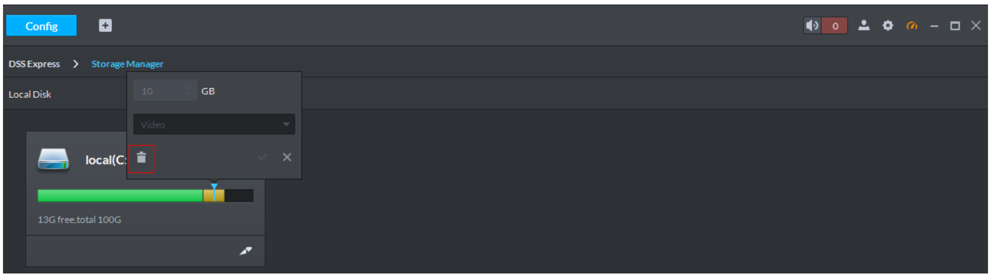

Config
DSS Express
Storage Manager
Local Disk
local(C:\)
13G free,total 100G

Figure 3-11 Delete exclusive storage space


Config
0
DSS Express
Storage Manager
Local Disk
10
GB
Video
local(C:
13G free,total 100G

3.2.1.4.1 Setting Network Disk

If network storage device exists in networking, you can create platform’s exclusive storage space on network storage device, used to store video and ANPR pictures.

- Storage server is required to be deployed.
- One user volume of current network disk can only be used by one server at the same time.
- User volume needs to be formatted if you want to add network disk.

Step 1 Enter the configuration interface of **Storage Manager**.

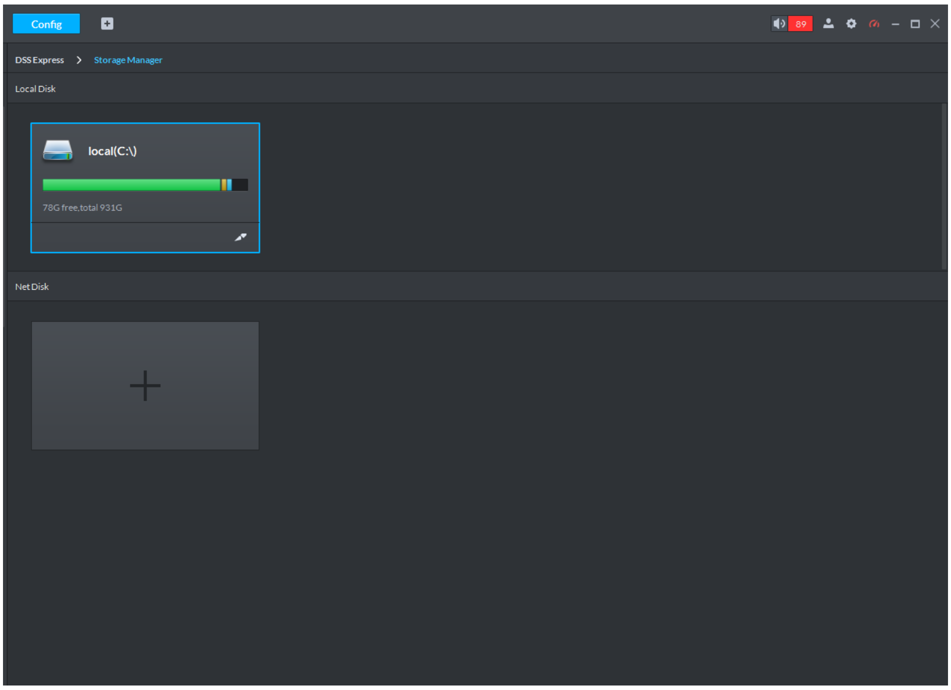
1) Click **Config** on the client homepage.

   The system displays the **Config** interface.

2) Click **Storage**.

   The system displays **Storage Manager** interface. See Figure 3-12.

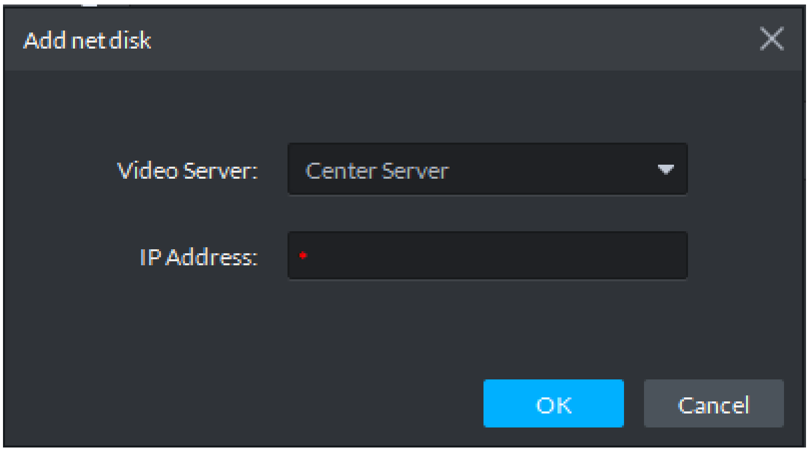
Figure 3-12 Storage manager


Config
89
DSS Express
Storage Manager
Local Disk
local(C:\)
78G free,total 931G
Net Disk
+

Step 2 Click +.

The system pops out the interface of **Add Network Disk**. See Figure 3-13.

Figure 3-13 Fill in IP


Add net disk

Video Server: Center Server

IP Address: *

Step 3 Enter IP address of network storage device, click **OK**.

See Figure 3-14 for the adding result, green means remaining space, red means used space which can be overwritten.

If network disk is not formatted, please format it according to system prompt. The operations of adding network disk are shown as follows.

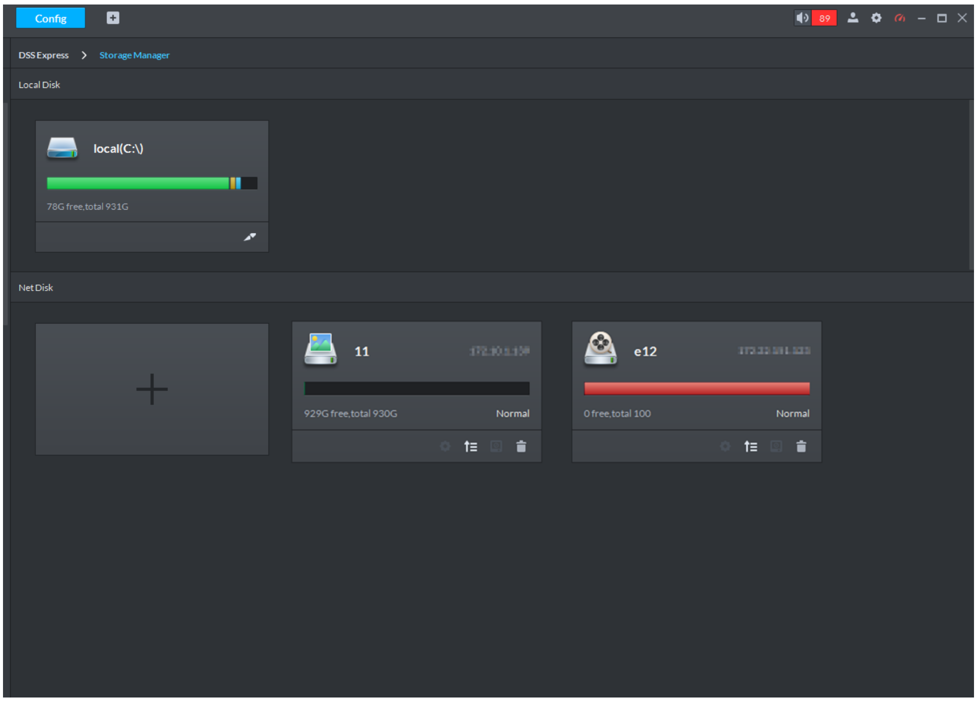
- Click ⚙ and modify storage space type of disk, including video and ANPR picture.

  Video disk is used to store video, ANPR picture disk is used to store ANPR snapshot. If you need to store ANPR device snapshot, storage space type must be set as ANPR picture.

- Click ⇡☰ and take the network disk used by other devices. Please make sure other device has stopped recording or snapshot before being taken, otherwise it will cause video or picture loss.

- Click 🗑 and delete network disk. Please make sure recording or snapshot has stopped before being deleted, otherwise it will cause video or picture loss.

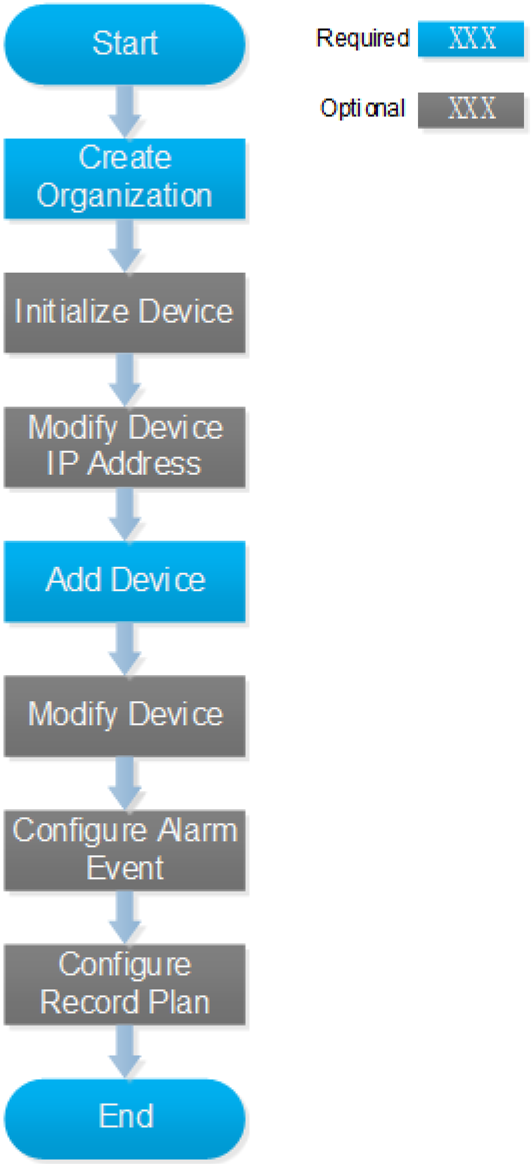
Figure 3-14 Network disk


Config
89
DSS Express
Storage Manager
Local Disk
local(C:\)
78G free,total 931G
Net Disk
+
11
[redacted]
929G free,total 930G
Normal
e12
[redacted]
0 free,total 100
Normal

3.2.2 Managing Device

After device is added on the server, you can operate device remotely by server. The flow of device management is shown in Figure 3-15.

Figure 3-15 Device management flow


Start
Create Organization
Initialize Device
Modify Device IP Address
Add Device
Modify Device
Configure Alarm Event
Configure Record Plan
End
Required XXX
Optional XXX

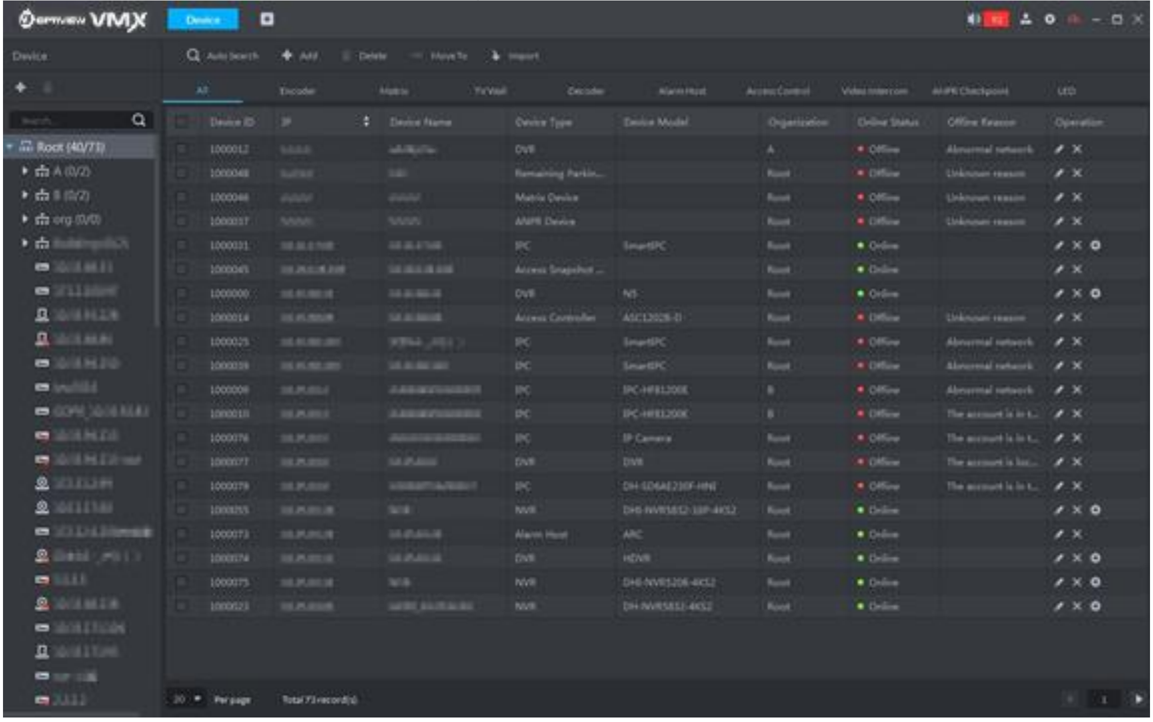
3.2.2.1 Creating Organization

Create organization and realize device management by organizations. **Root Node** organization already exists by default, if no organization is created, then all the added devices belong to the root node.

Step 1 Click **Device** on the client homepage.

The system displays the **Device** interface. See Figure 3-16. The device is online if online status is green, device is offline if online status is red.

Figure 3-16 Device


Device
Auto Search
Add
Delete
Move To
Import
All
Encoder
Matrix
TV Wall
Decoder
Alarm Host
Access Control
Video Intercom
ANPR Checkpoint
LED
Device ID
IP
Device Name
Device Type
Device Model
Organization
Online Status
Offline Reason
Operation
Root (40/73)
Per page

Step 2 Select organization, click + or right-click organization, select Create Organization.

The system displays the interface of **Create Organization**. See Figure 3-17.

Figure 3-17 Create organization

Step 3 Enter organization name, click **OK**.

The system displays info of added organization. See Figure 3-18.

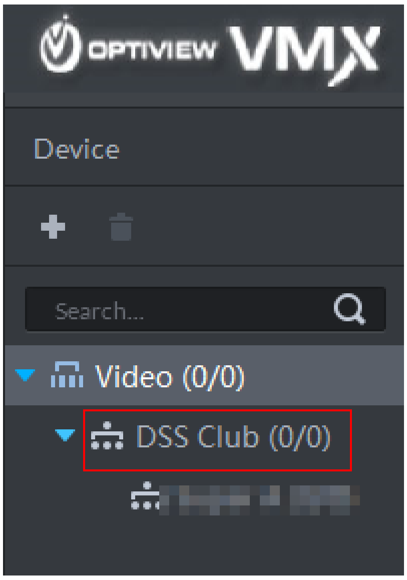

OPTIVIEW VMX
Device
Search...
Video (0/0)
DSS Club (0/0)

Figure 3-18 Organization list

More operations of organization are shown as follows:

- Root node supports creating subordinate organization; Set display type means setting device display by name or IP; Set sort means setting sort mode of all devices and organizations under root node, including ascending, descending and default order. See Figure 3-19.

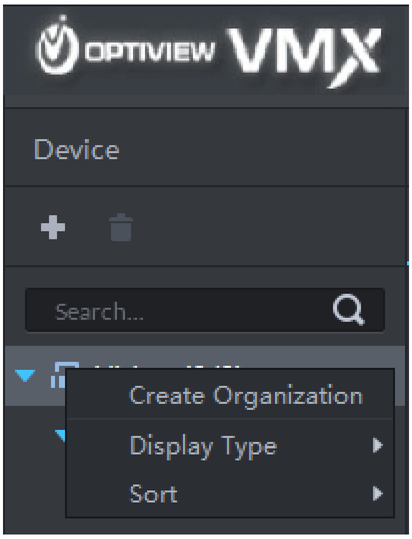

OPTIVIEW VMX
Device
Search...
Create Organization
Display Type
Sort

Figure 3-19 Root node operation

- Child node organization supports creating subordinate child node organization; delete and rename organization. See Figure 3-20.

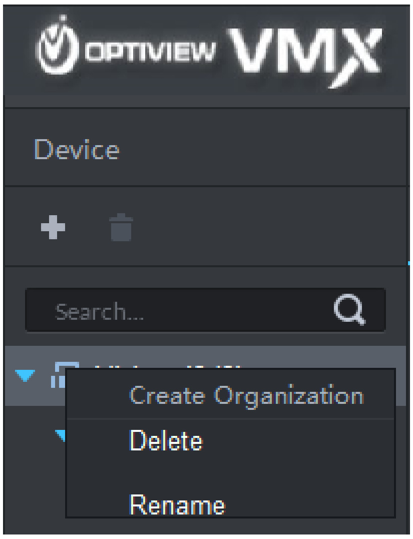

OPTIVIEW VMX
Device
Search...
Create Organization
Delete
Rename

Figure 3-20 Child node organization

3.2.2.2 Initializing Device

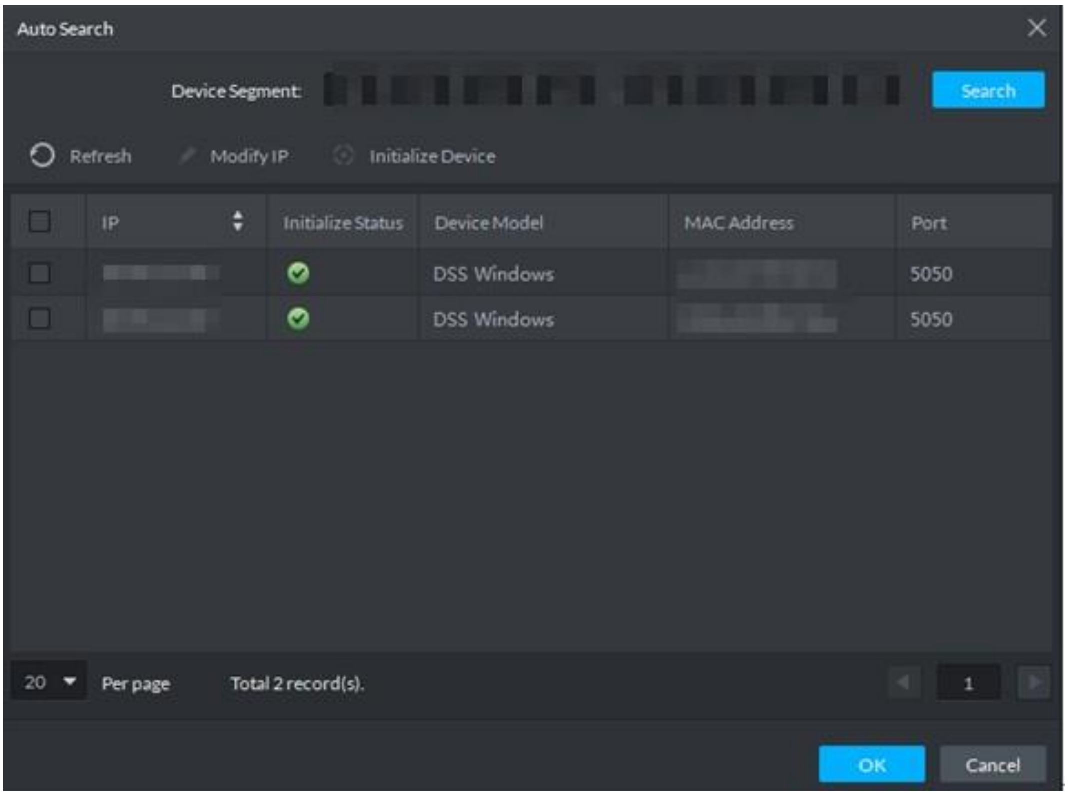
The device is required to configure admin account password and security questions after being delivered out of factory; otherwise, it cannot be used normally. The platform supports initializing device remotely.

Step 1 Click **Device** on the client homepage.
The system displays the **Device** interface.

Step 2 Click Auto Search.
The system displays the **Auto Search** interface.

Step 3 Enter start IP and end IP, click **Search**.
The system displays search results.

Figure 3-21 Search result


Auto Search
Search
Refresh
Modify IP
Initialize Device
20
Per page
Total 2 record(s).
1
OK
Cancel

Device Segment: [redacted]

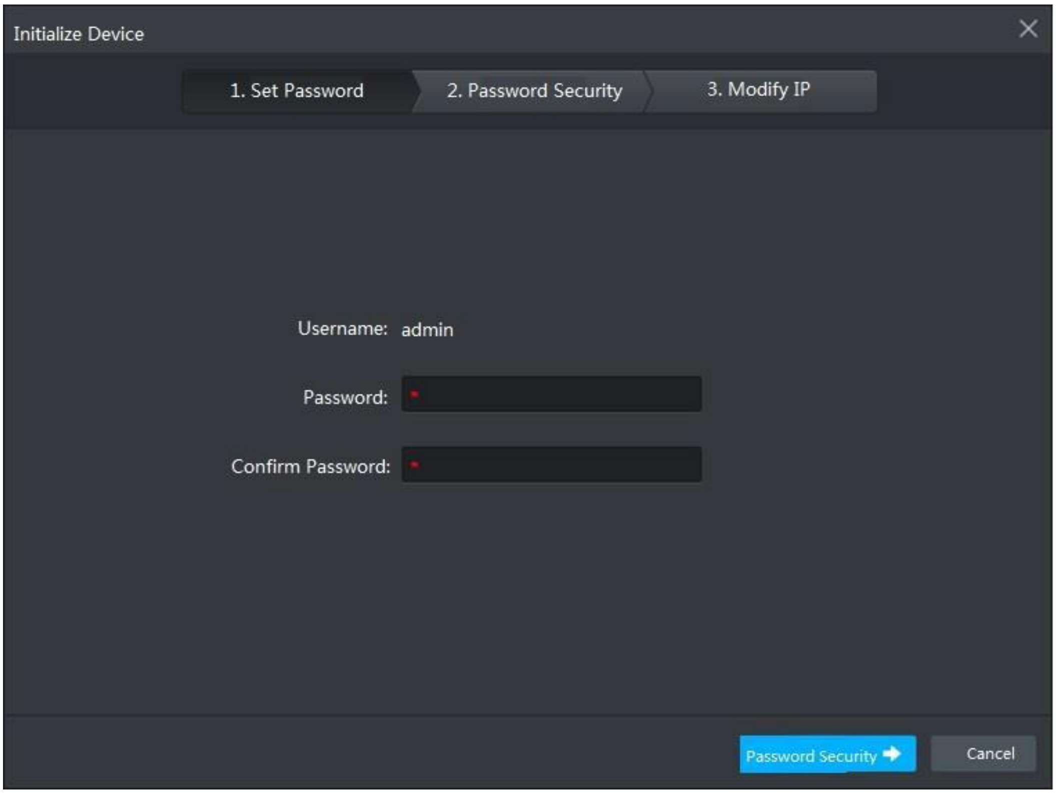
☐	IP	Initialize Status	Device Model	MAC Address	Port
☐	[redacted]	✓	DSS Windows	[redacted]	5050
☐	[redacted]	✓	DSS Windows	[redacted]	5050

Step 4 Select uninitialized device, click **Initialize Device**.

The system displays **Set Password**. See Figure 3-22.

Several devices can be initialized together.

Figure 3-22 Set password


Initialize Device
1. Set Password
2. Password Security
3. Modify IP
Password Security
Cancel

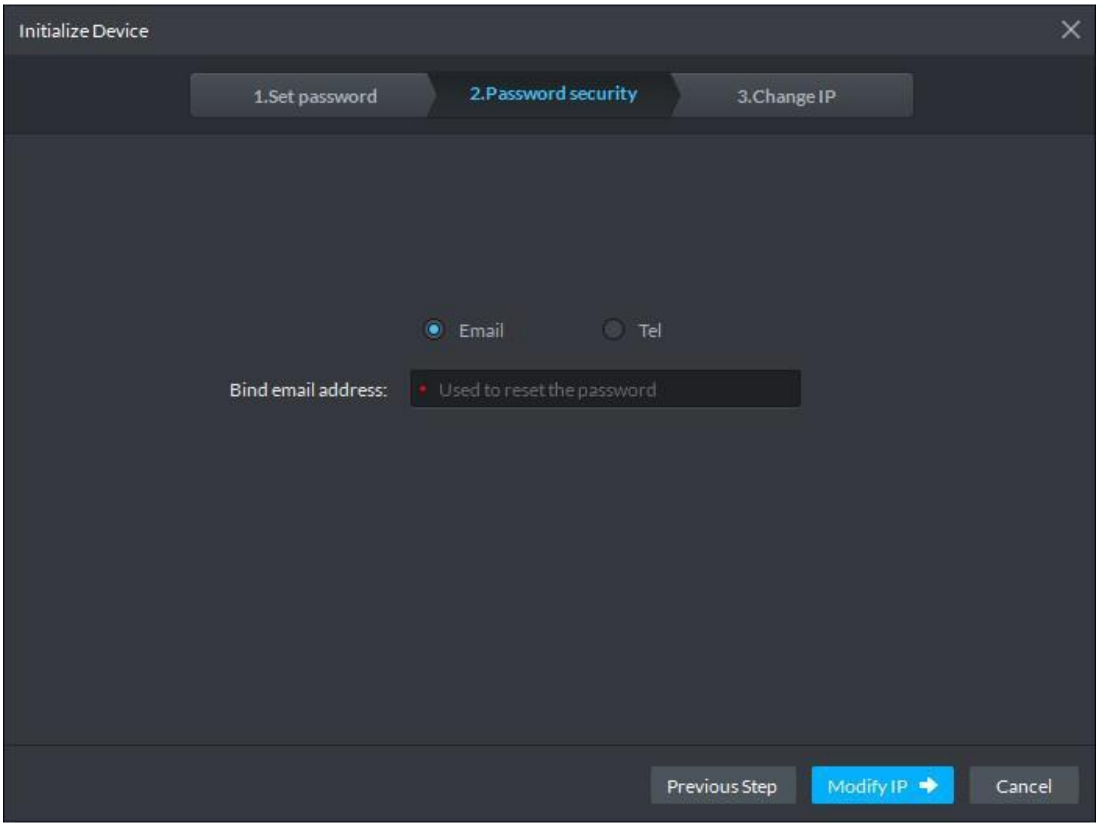
Username: admin

Password:

Confirm Password:

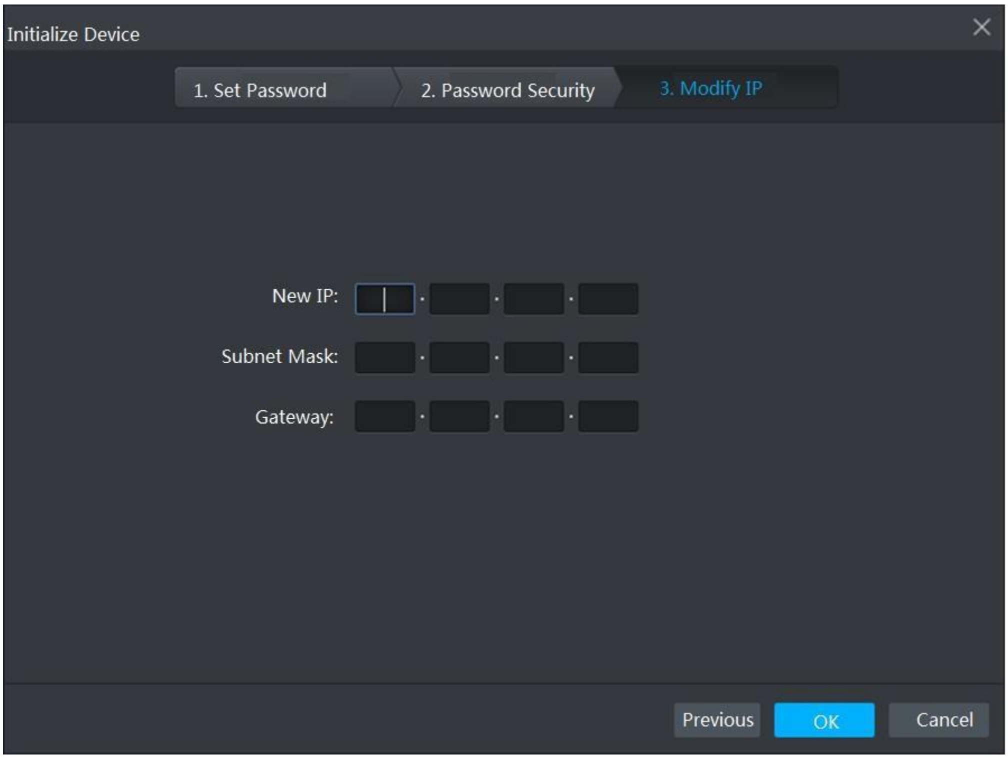
Step 5 Enter password, click **Password Security**. See Figure 3-23.

Figure 3-23 Password security


Initialize Device
1.Set password
2.Password security
3.Change IP
Email
Tel
Bind email address:
Used to reset the password
Previous Step
Modify IP
Cancel

Step 6 Select email or phone, enter corresponding email address or phone number, click **Modify IP**. The system displays **Modify IP** interface. See Figure 3-24.

Figure 3-24 Modify IP


Initialize Device
1. Set Password
2. Password Security
3. Modify IP
New IP:
Subnet Mask:
Gateway:
Previous
OK
Cancel

Step 7 Enter new IP address, subnet mask and gateway, click **OK**.

3.2.2.3 Modifying Device IP Address

You can modify device IP address on the auto search interface.

Step 1 Click **Device** on the client homepage.

The system displays **Device** interface.

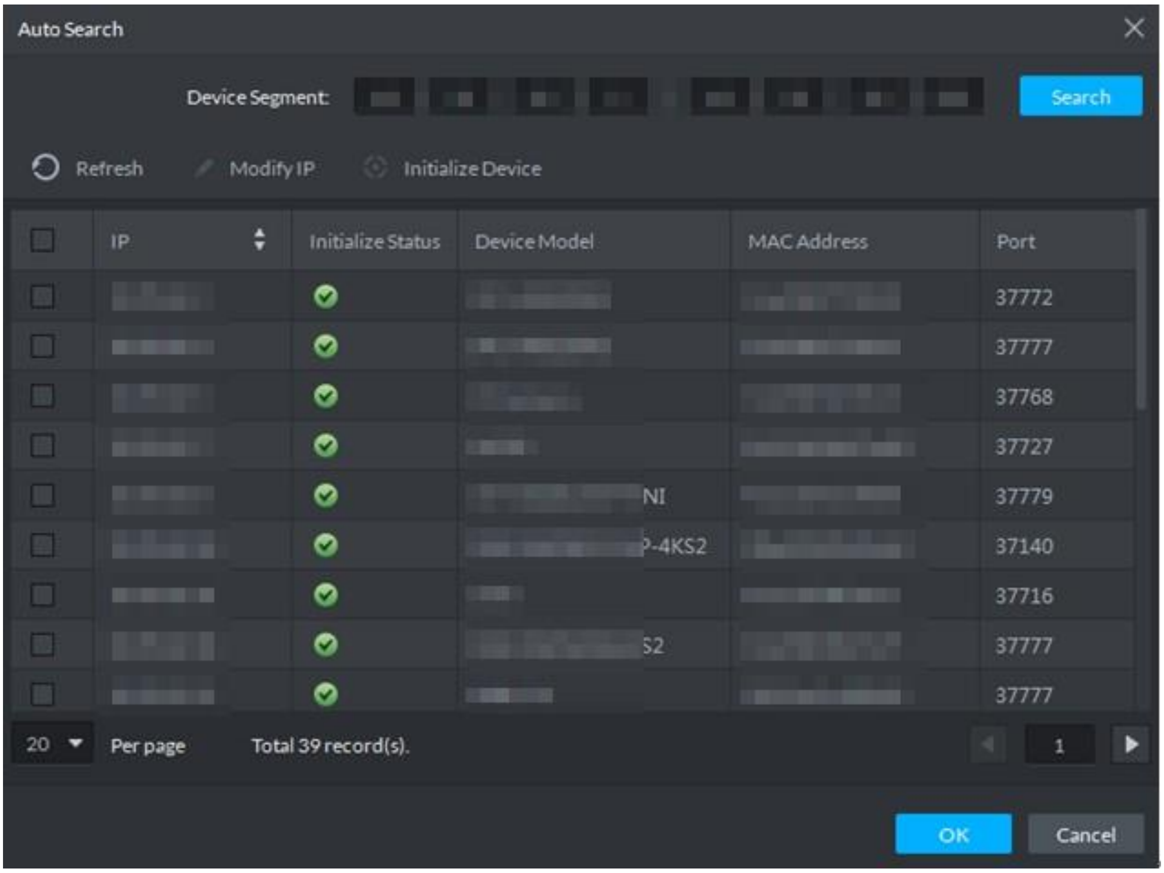
Step 2 Click Auto Search.

The system displays **Auto Search** interface.

Step 3 Enter start IP and end IP, click **Search**.

The system displays search result. See Figure 3-25.

Figure 3-25 Search result



Device Segment: [redacted] - [redacted]

☐	IP	Initialize Status	Device Model	MAC Address	Port
☐	[redacted]	✓	[redacted]	[redacted]	37772
☐	[redacted]	✓	[redacted]	[redacted]	37777
☐	[redacted]	✓	[redacted]	[redacted]	37768
☐	[redacted]	✓	[redacted]	[redacted]	37727
☐	[redacted]	✓	[redacted]	[redacted]	37779
☐	[redacted]	✓	[redacted]	[redacted]	37140
☐	[redacted]	✓	[redacted]	[redacted]	37716
☐	[redacted]	✓	[redacted]	[redacted]	37777
☐	[redacted]	✓	[redacted]	[redacted]	37777

20 Per page Total 39 record(s). 1

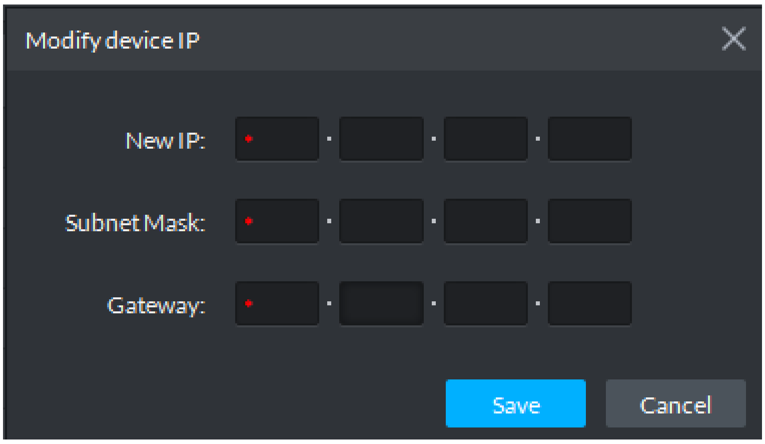
Step 4 Select device whose IP address needs to be modified, click **Modify IP**.

The system displays the interface of **Modify Device IP**.

Step 5 Modify device IP, click **OK**.

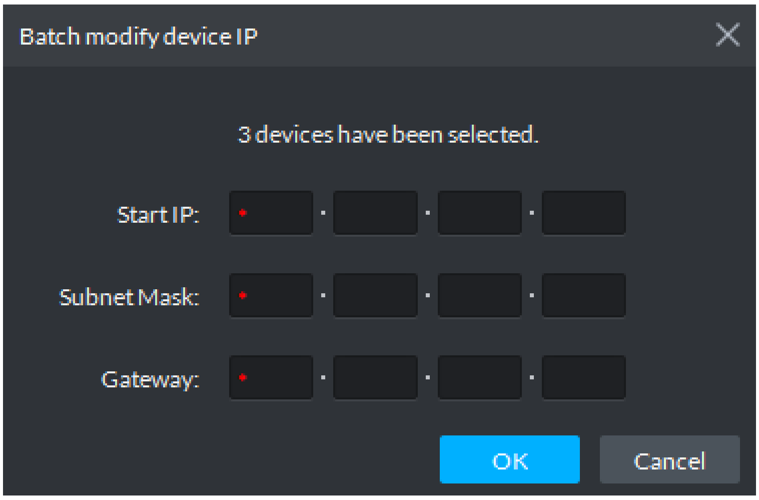
- When you select one device, the system pops out the **Modify Device IP** dialog box. See Figure 3-26.

Figure 3-26 Singly modify device IP


Modify device IP
New IP:
Subnet Mask:
Gateway:
Save
Cancel

- When you select several devices, the system pops out the dialog box of **Batch Modify Device IP**. See Figure 3-27.

Figure 3-27 Batch modify device IP


Batch modify device IP
Start IP:
Subnet Mask:
Gateway:
OK
Cancel

3 devices have been selected.

Step 6 Set new IP address or start IP, subnet mask and gateway.

Modify in batches, IP address increases by 1 sequentially.

Step 7 Click **Save** or **OK**.

3.2.2.4 Adding Device

You can add access control, encoder, decoder, video wall, ANPR and matrix, after that you can manage and configure device remotely on client.

⚠

If users want to use the newly added device, enter **User** interface, edit user to make him have permission to use the device, otherwise, the device cannot be used.

3.2.2.4.1 Searching and Adding Device

Add several devices, and devices are in the same network segment, login username is the same as password. The system can search all the devices covered by server network.

Step 1 Click **Device** on the client homepage.

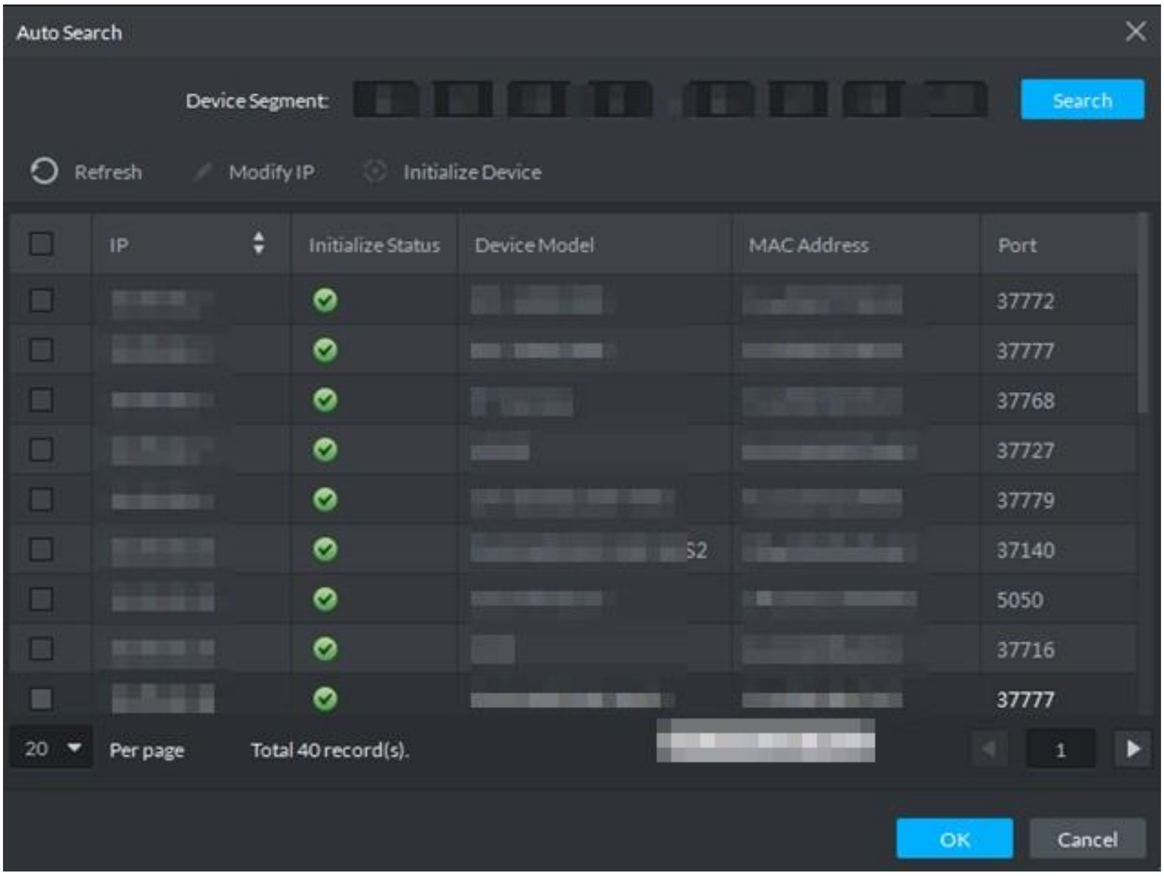
The system displays the **Device** interface.

Step 2 Click Auto Search.

The system displays the interface of **Auto Search**. See Figure 3-28. The system searches the device with the same segment as server by default.

- Click **Refresh** to refresh device info.
- Select device, click Modify IP and modify device IP address. For details, see 3.2.2.3 Modifying Device IP Address.
- Select uninitialized device, click Initialize Device and initialize device. For details, see 3.2.2.2 Initializing Device.

Figure 3-28 Auto search device



Device Segment: [redacted]

☐	IP	Initialize Status	Device Model	MAC Address	Port
☐	[redacted]	✓	[redacted]	[redacted]	37772
☐	[redacted]	✓	[redacted]	[redacted]	37777
☐	[redacted]	✓	[redacted]	[redacted]	37768
☐	[redacted]	✓	[redacted]	[redacted]	37727
☐	[redacted]	✓	[redacted]	[redacted]	37779
☐	[redacted]	✓	[redacted]	[redacted]	37140
☐	[redacted]	✓	[redacted]	[redacted]	5050
☐	[redacted]	✓	[redacted]	[redacted]	37716
☐	[redacted]	✓	[redacted]	[redacted]	37777

20 Per page Total 40 record(s). [redacted] 1

Step 3 Enter searched start IP and end IP, click **Search**.

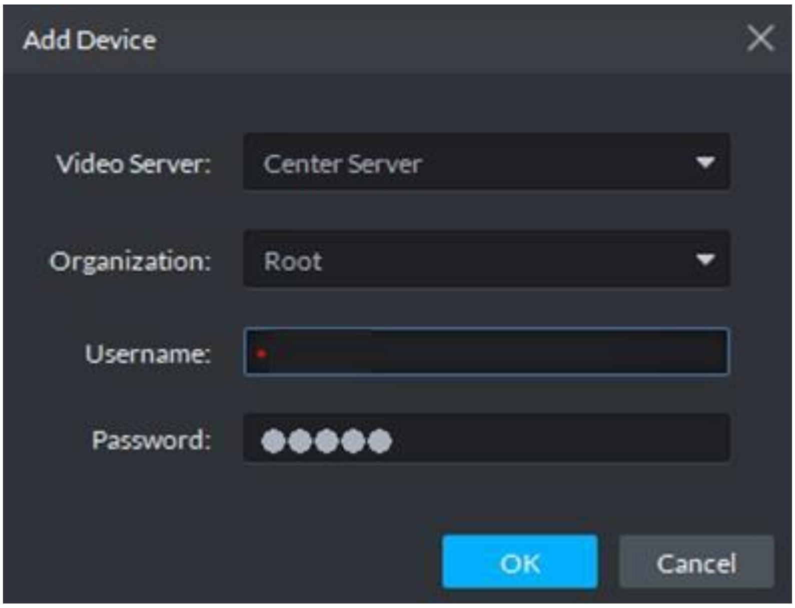
The system displays search results.

Step 4 Select the device to be added, click **OK**.

The system displays the interface of **Add Device**. See Figure 3-29.

Figure 3-29 Add Device

Step 5



Enter login username and password, click **OK**.

📖

- The added device username is required to be the same as password when adding several devices.
- After device is added, the system continues to stay on the **Auto Search** interface, click **Cancel** or ✕ to exit interface.
- After device is added, the platform logs in device automatically, the device is displayed as online after logging in successfully. If offline, please make sure if login username and password are correct, click ✎ to modify username and password.

3.2.2.4.2 Adding Device Manually

Add single device, or the username and password of the added device are different, or the added device is not in the same segment.

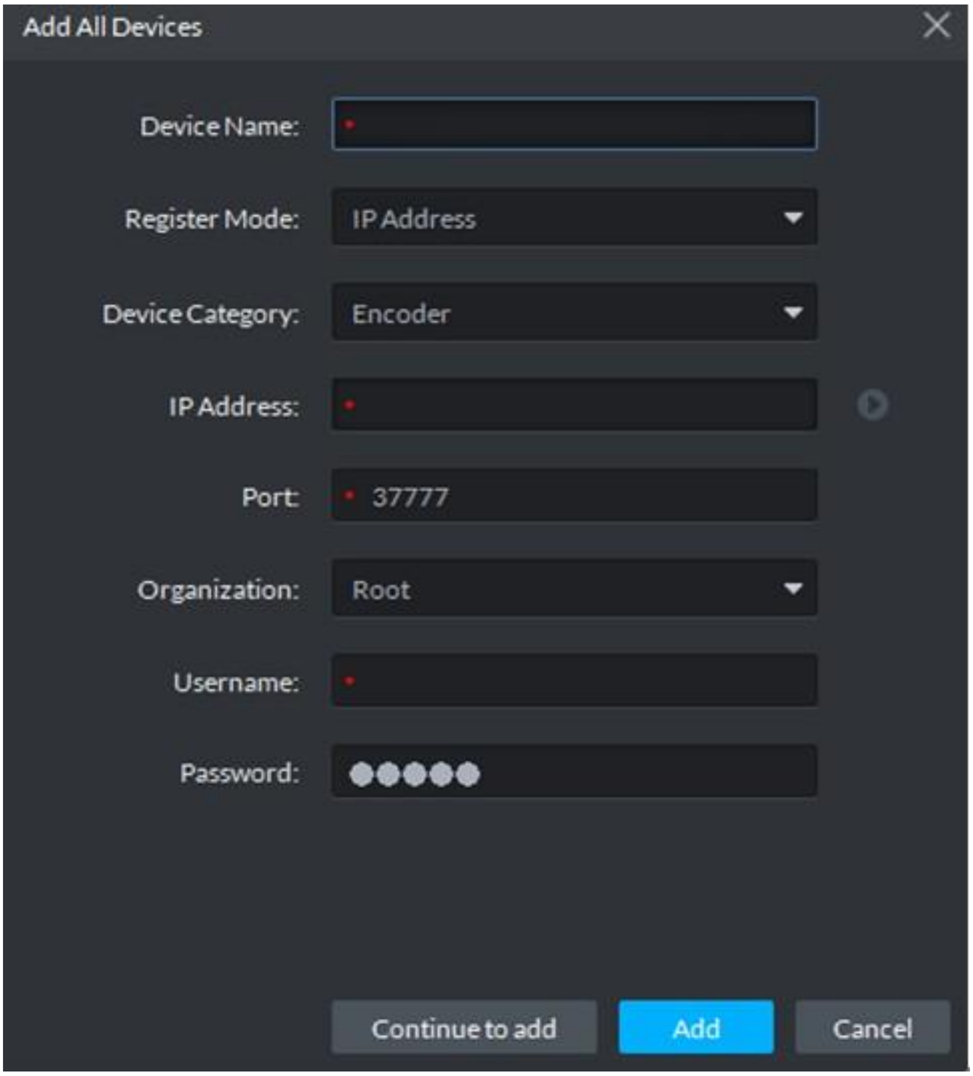
Step 1 Click **Device** on the client homepage.

The system displays the **Device** interface.

Step 2 Click **Add**.

The system displays the interface of **Add All Devices**, see Figure 3-30.

Figure 3-30 Manually add device


Add All Devices
Device Name:
Register Mode:
IP Address
Device Category:
Encoder
IP Address:
Port:
37777
Organization:
Root
Username:
Password:
Continue to add
Add
Cancel

Step 3 Set parameters, for more details, refer to Table 3-1.

- The item with * is required to be filled in. You need to set different parameters if different device are connected.
- Add encoder, set correct parameters, and click ▶ to view device video.

Table 3-1 Parameter description

Parameter	**Description**
Device Category	Select according to the type of added device, currently support adding access control, encoder, decoder, video wall, ANPR, matrix, LED, alarm host and video intercom.

Parameter	Description
Register Mode	Support registration by following method: ● IP address Add device to platform by adding device IP. ● Serial number (Device with P2P function) If device supports P2P function, then you can add device to platform by adding device serial number. ● Onvif If device enables Onvif protocol, then you can add device to platform by Onvif protocol. Generally it can be used when adding third-party device.
Port	TCP protocol communication provides service port, and keeps it in accordance with added device.
Organization	Select organization node of added device.
IP Address	When register by IP address or Onvif mode, set the IP address of added device.
SN	When register by serial number mode, set the serial number of added device.
Username	Enter login username and password of added device.
Password	
Decode mode	Select according to the decode mode of added device: ● Pull Decoder extracts stream from platform by url address, the decode mode of device is pull. ● Direct Decoder extracts stream directly from encoder, the decode mode is direct for device, under this mode; you need to add decoder IP address when trusted list is added by device. ● Push VMS pushes stream directly to decoder, currently only support NVD without combination screen, the mode is not supported by matrix, video wall or NVD under combination mode.
Support Combination	Select when added device supports combination.
Picture Server	Select storage location of picture reported by ANPR.
LED Type	Support added LED including general screen and free parking screen, select corresponding device type according to the accessed device.

Step 4 Click **Add**.

Click **Continue to add** if necessary, then you can add more devices.

3.2.2.4.3 Importing Device

If there is device list exported by Optiview VMS, or video intercom template already exists and its information is complete, or device is already added by easy4ip account. You can quickly add device to platform by importing existing file or account.

Import Local File

Import device list exported by Optiview VMS, or video intercom template file, and add device to the platform quickly.

Please contact technical support for video intercom template.

Step 1 Click **Device** on the client homepage.

The system displays **Device** interface.

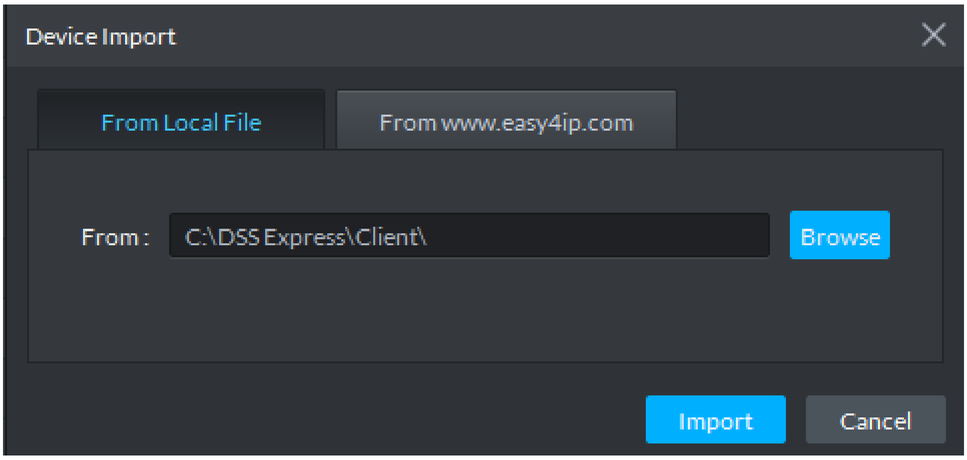
Step 2 Click **Import**.

The system displays **Device Import** interface.

Step 3 Click From Local File tab.

The system displays the interface of **From Local File**. See Figure 3-31.

Figure 3-31 Import from local file



Device Import
From Local File
From www.easy4ip.com
From :
C:\DSS Express\Client\
Browse
Import
Cancel

Step 4 Click **Browse**, select device info file and click **Import**.

The system shows import results.

Import easy4ip Device Info

Import device info added on easy4ip account, and then device is added to the platform.

Step 1 Click Device on the client homepage.

The system displays Device interface.

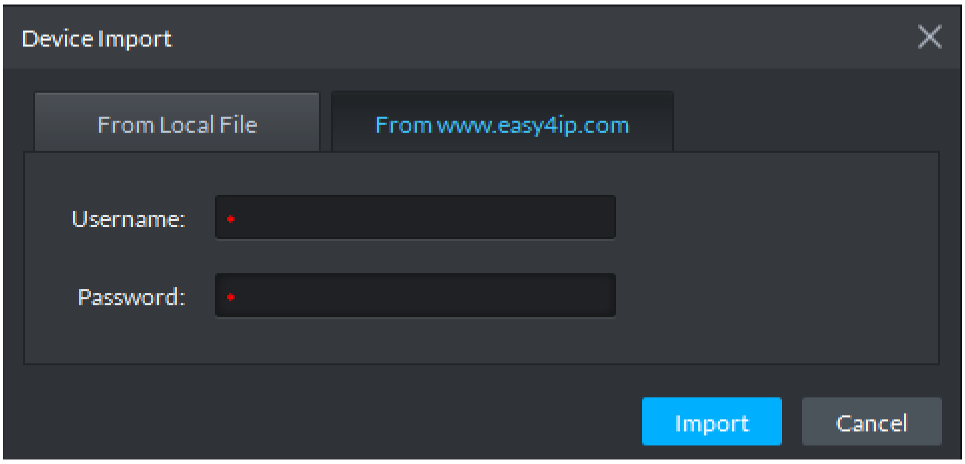
Step 2 Click **Import**.

The system displays **Device Import** interface.

Step 3 Click the tab **From www.easy4ip.com**

The system displays the **From www.easy4ip.com** interface. See Figure 3-32.

Figure 3-32 Import from www.easy4ip.com



Device Import
From Local File
From www.easy4ip.com
Username:
Password:
Import
Cancel

Step 4 Enter username and password, click **Import**.

The system shows import result.

3.2.2.5 Editing Device

3.2.2.5.1 Modifying Device Info

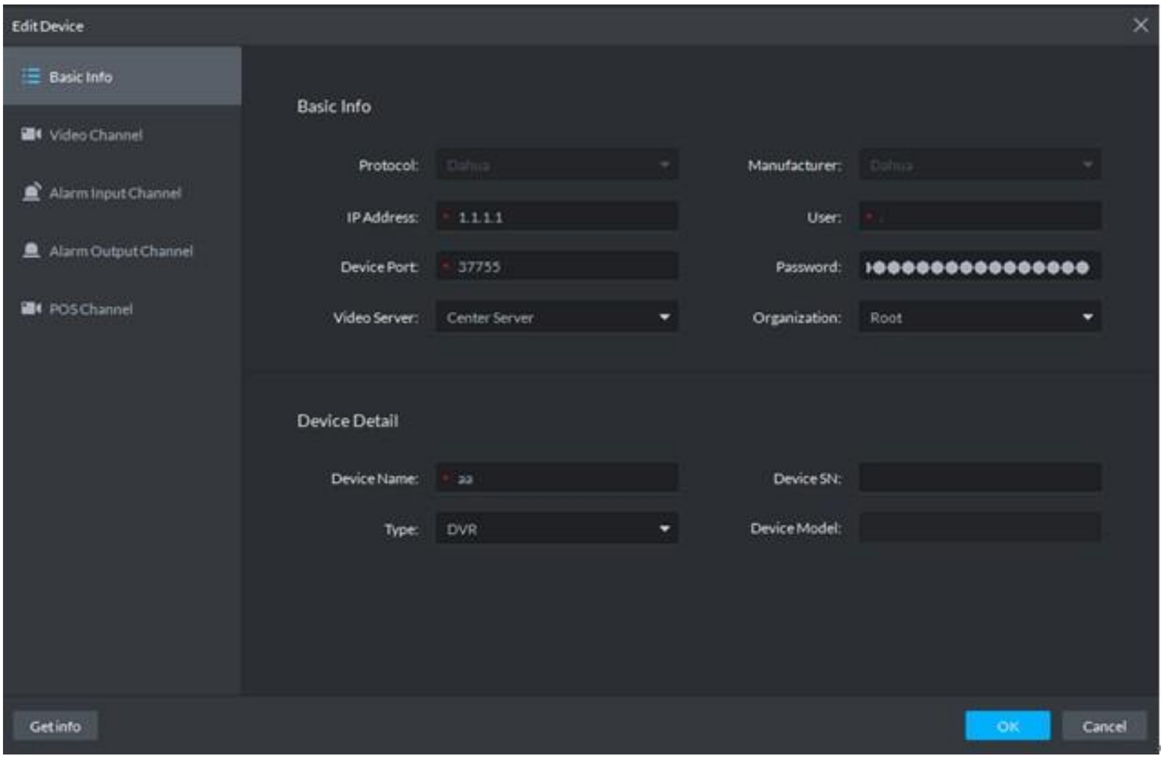
Modify device info in the device list, including username, password and some basic info, video channel info, alarm input and output channel. The chapter takes NVR as an example to describe. There are two modification methods shown below.

- Please modify device according to the following method if you want to modify info except device IP address, port number, user and password.

Step 1 Click **Device** on the client homepage.
The system displays **Device** interface.

Step 2 Click ✎ next to device list.
The system displays **Edit Device** interface. See Figure 3-33.

Figure 3-33 Edit device



Protocol: Dahua
Manufacturer: Dahua
IP Address: 1.1.1.1
User:
Device Port: 37755
Password: ●●●●●●●●●●●●●●●●
Video Server: Center Server
Organization: Root
Device Name: aa
Device SN:
Type: DVR
Device Model:

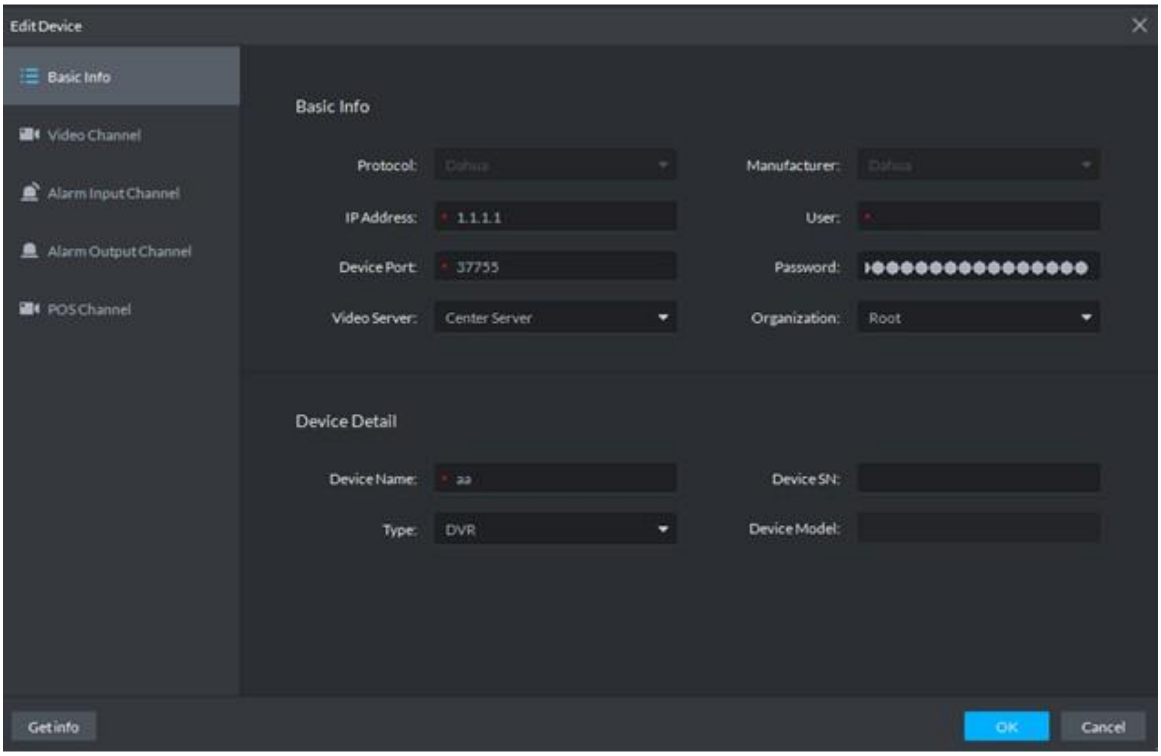
Step 3 Select corresponding tab, click **Get Info** on the lower left corner of the interface, sync device info.

- Please modify device according to the following method if you want to modify device IP address, port number, user and password.

Step 1 Click **Device** on the client homepage.
The system displays the **Device** interface.

Step 2 Click ✎ next to the device list.
The system displays **Edit Device** interface, see Figure 3-34.

Figure 3-34 Modify device basic info


Edit Device
Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
Get info
OK
Cancel

Basic Info

Protocol: Dahua
Manufacturer: Dahua
IP Address: * 1.1.1.1
User: *
Device Port: * 37755
Password: ●●●●●●●●●●●●●●●●
Video Server: Center Server
Organization: Root

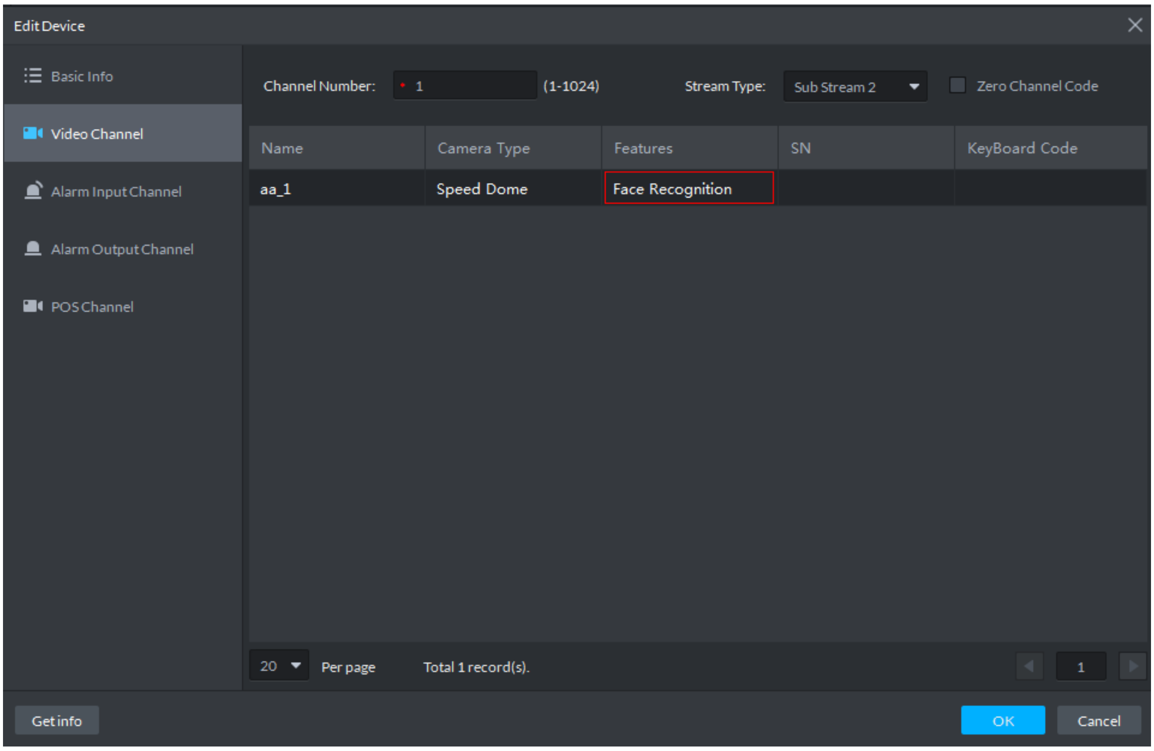
Device Detail

Device Name: * aa
Device SN:
Type: DVR
Device Model:

Step 3 Click **Basic Info** tab, modify device IP address, username, password, device port, organization, device name and type.

Step 4 Click **Video Channel** tab, modify channel number and stream type, and see Figure 3-35. You need to enable corresponding intelligent function if the added device owns intelligent functions. For example, the added camera is face recognition camera, the camera is required to detect face, and then you need to set **Features** as **Face Recognition**.

Figure 3-35 Video channel


Edit Device
Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
Get info
OK
Cancel

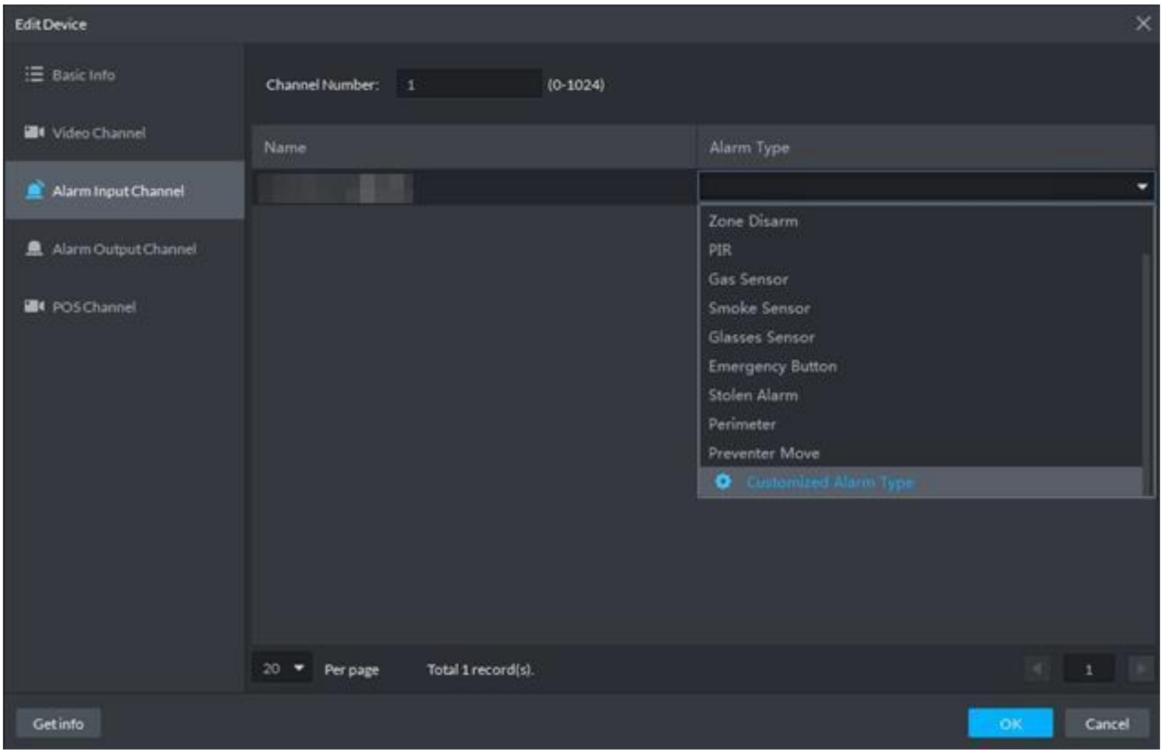
Channel Number: * 1 (1-1024)
Stream Type: Sub Stream 2
☐ Zero Channel Code

Name	Camera Type	Features	SN	KeyBoard Code
aa_1	Speed Dome	Face Recognition		

20 Per page Total 1 record(s). 1

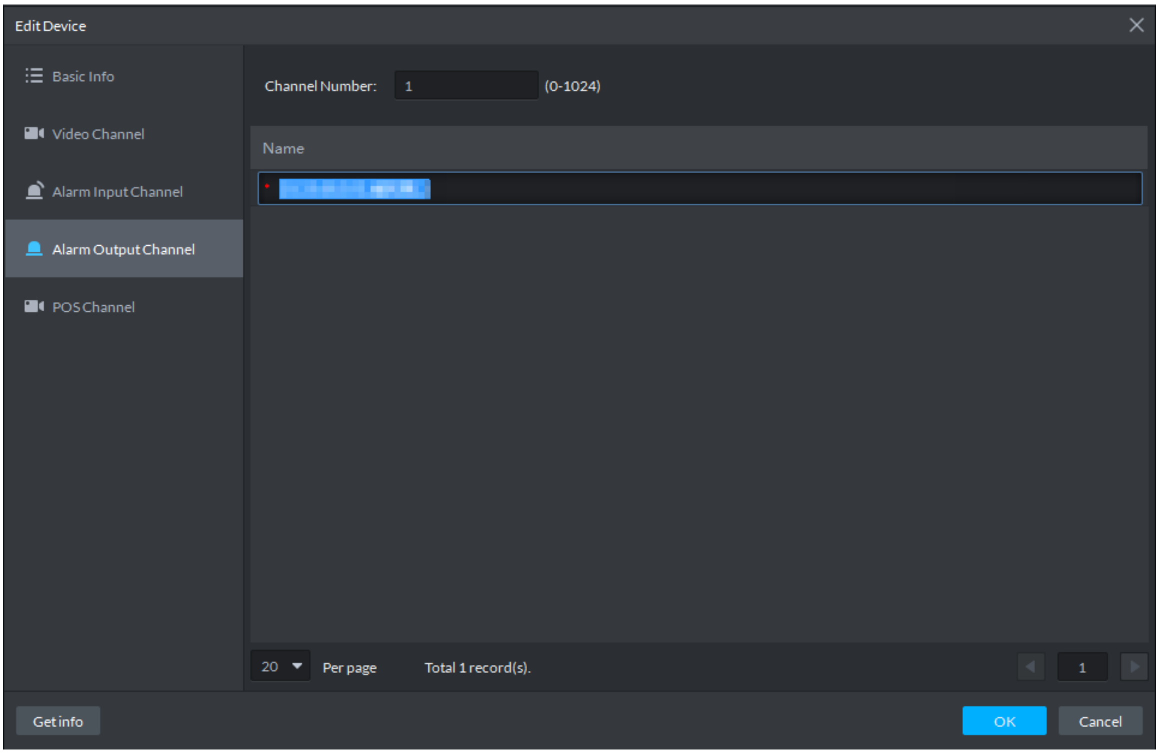
Step 5 Click **Alarm Input Channel** tab and modify alarm input channel number, see Figure 3-36. Alarm type supports custom. Select **Customized Alarm Type** from the drop-down box of **Alarm Type**, set needed alarm type, used to quickly identify alarm. After config, on the event configuration interface, you can configure corresponding alarm event for corresponding alarm input.

Figure 3-36 Alarm input channel


Edit Device
Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
Channel Number:
1
(0-1024)
Name
Alarm Type
Zone Disarm
PIR
Gas Sensor
Smoke Sensor
Glasses Sensor
Emergency Button
Stolen Alarm
Perimeter
Preventer Move
Customized Alarm Type
20
Per page
Total 1 record(s).
1
Get info
OK
Cancel

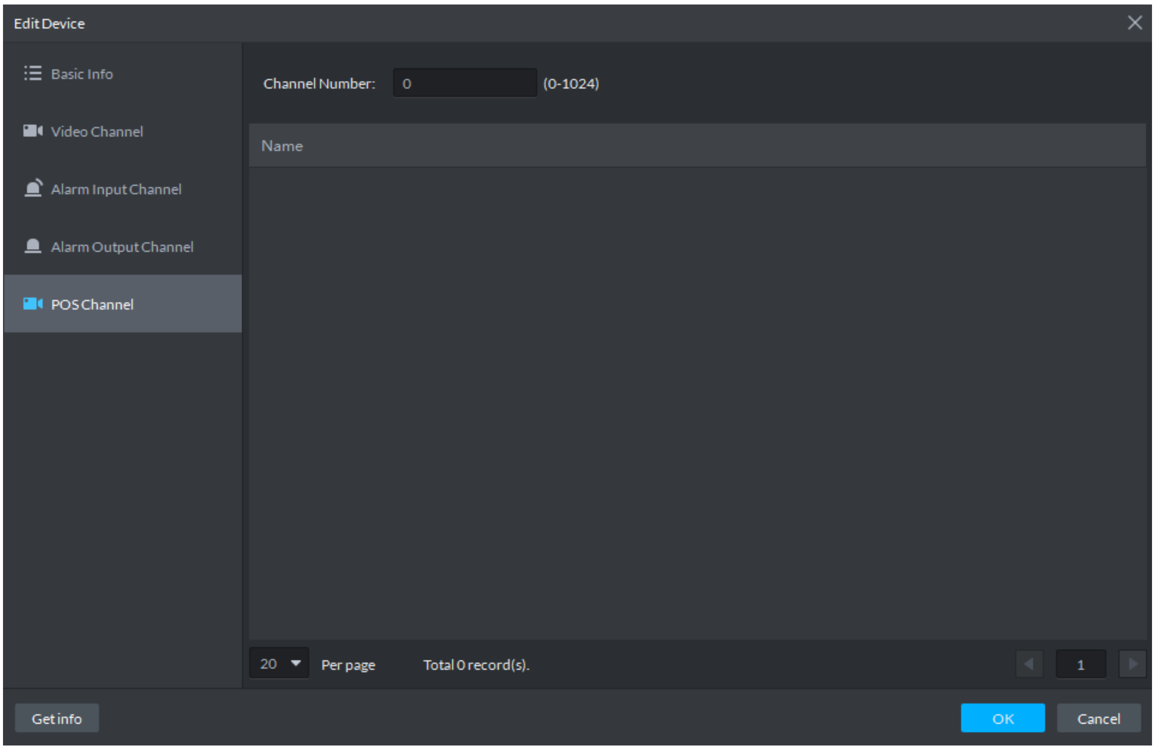
Step 6 Click **Alarm Output Channel** tab, modify device alarm output channel number, Double-click to modify corresponding channel name, see Figure 3-37.

Figure 3-37 Alarm output channel


Edit Device
Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
Channel Number:
1
(0-1024)
Name
20
Per page
Total 1 record(s).
1
Get info
OK
Cancel

Step 7 Click **POS Channel** tab, modify device POS channel number, Double-click and modify corresponding channel name, see Figure 3-38.

Figure 3-38 POS channel


Edit Device
Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
Name
Per page
Get info
OK
Cancel

Channel Number: 0 (0-1024)

20 Per page Total 0 record(s). 1

Step 8 Click **OK**.

3.2.2.5.2 Modifying Device's Organization

You can move device from one organization to another.

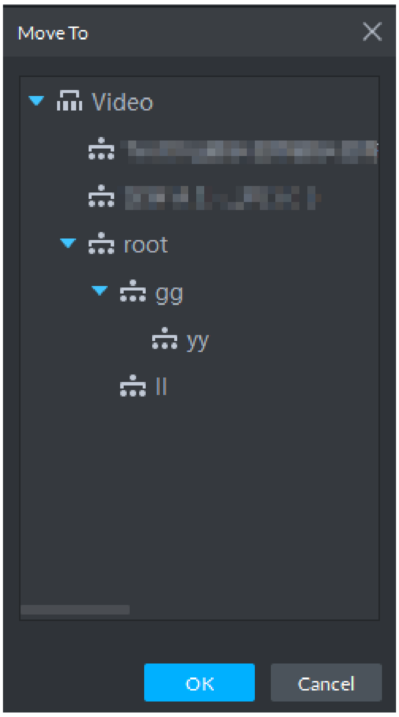
Step 1 Click **Device** on the client homepage.

The system displays **Device** interface.

Step 2 Select the device to be moved, click **Move To**.

The system displays **Move To** interface, see Figure 3-39.

Figure 3-39 Move device



Step 3 Select the organization node you want to move to, click **OK**.

3.2.3 Adding User

3.2.3.1 Adding Basic User

Create users with different permissions for platform and make sure the platform is safe. The platform provides three types of user, including administrator, advanced user and general user, different users have different permissions. Each type of user can adjust permission within certain permission range.

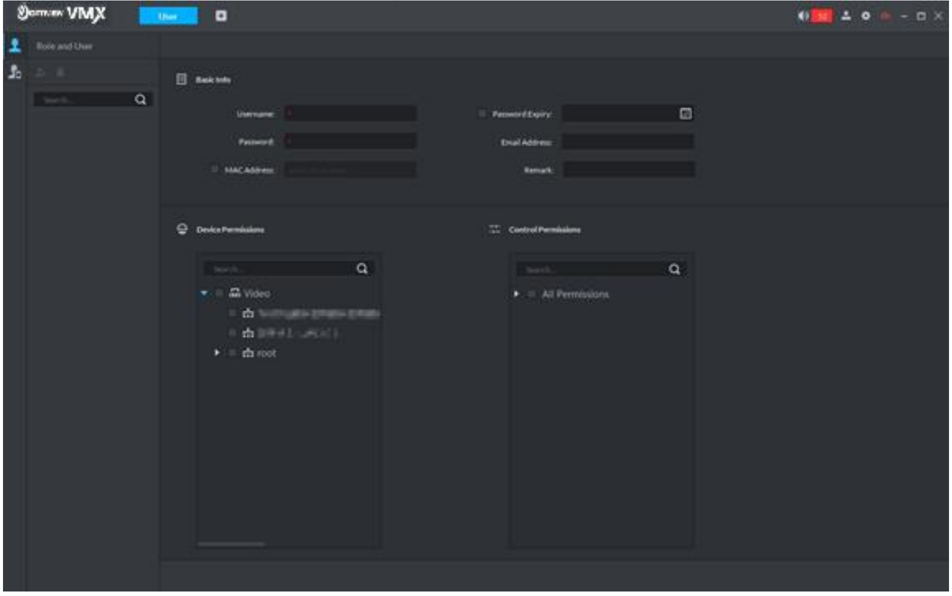
- Administrator: Owns all control permissions.
- Advanced user: Owns all permissions except system config.
- General user: Owns other permissions except device management, user management, system config, configuration management, video wall config, emap config, log management.

Added user can be deleted but the platform’s system cannot.

Step 1 Click **User** on the client homepage.

The system displays **User** interface, see Figure 3-40.

Figure 3-40 User


VMX
User
Role and User
Basic Info
Username:
Password:
MAC Address:
Password Expiry:
Email Address:
Remark:
Device Permissions
Control Permissions
Search...
Video
root
All Permissions

Step 2 Click .

The system displays **User** interface.

Step 3 Select user type from the left list, click .

The system displays **Add User** interface. See Figure 3-41.

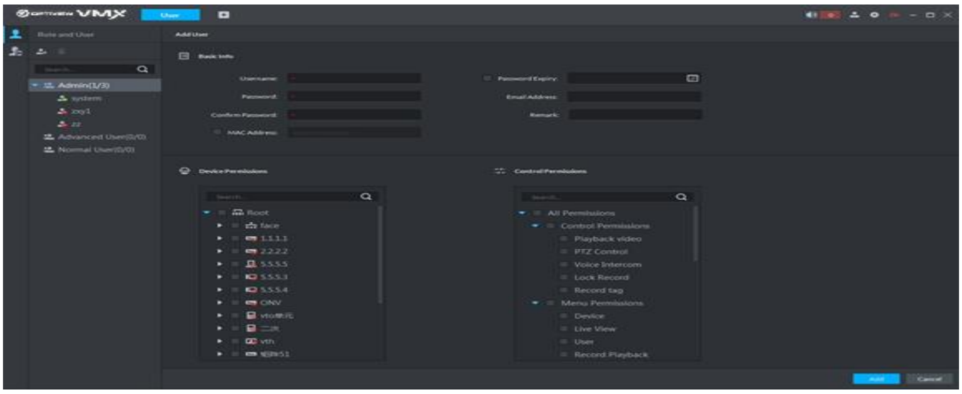

VMX
User
Role and User
Add User
Admin(1/3)
system
zxy1
zz
Advanced User(0/0)
Normal User(0/0)
Basic Info
Username:
Password:
Confirm Password:
MAC Address:
Password Expiry:
Email Address:
Remark:
Device Permissions
Control Permissions
Search...
Root
face
1.1.1.1
2.2.2.2
5.5.5.5
5.5.5.3
5.5.5.4
ONV
vto
vth
All Permissions
Control Permissions
Playback video
PTZ Control
Voice Intercom
Lock Record
Record tag
Menu Permissions
Device
Live View
User
Record Playback
Add
Cancel

Figure 3-41 Add user

Step 4 Set user info, select device and permission that can be used by user, click **Add**.

3.2.3.2 Managing APP User

You can view APP user info, freeze user, modify login password and delete user.

📖

APP user can register by scanning QR code on the device, for more details, refer to APP user manual.

Click 👤 on the **User** interface. The system displays APP User interface, and shows info of all registered APP users. See Figure 3-42. For operation details, see Table 3-2.

Figure 3-42 Enter APP user interface

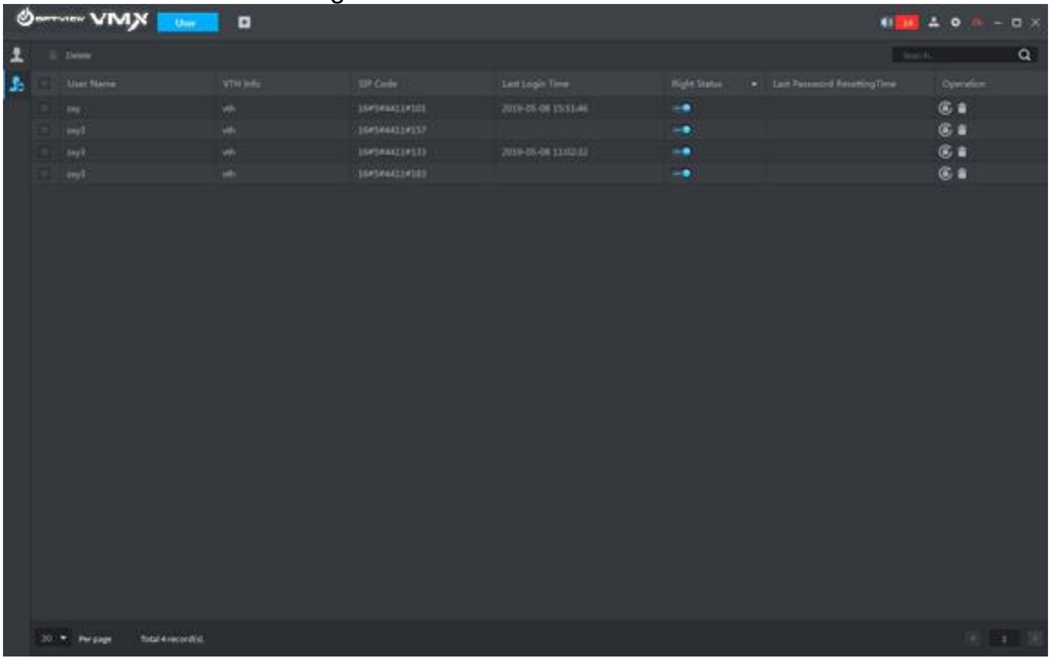

VMX
User
Delete
User Name
VTH Info
SIP Code
Last Login Time
Right Status
Last Password ResettingTime
Operation
Per page

Table 3-2 Operation description

Operation	Description
Freeze APP User	After APP user is freezed, APP user cannot log in within 600s. ON means normal, OFF means freeze, both can be mutually switched. 📖 The account can also be freezed if password attempts exceed 5 by APP user.
Modify APP User Login Password	Click 🔑 and enter new password the interface of **Reset Password**, click **OK**. 📖 Password length is 8~16 characters, must include number and letter. 👁 means showin password; 🙈 means enabling password protection and hiding password. Click icon to switch mutually.

Operation	Description
Delete APP User	Click ✖ next to APP user or select APP user, you can select several users, click **Delete** and delete users according to prompt on interface.

3.2.4 Setting Alarm Event

Device reports all alarm messages. Alarm messages can be responded only when the platform configures corresponding alarm linkage scheme. Linkage actions are shown as follows when responding to alarm.

- Link camera

  Play video of designated channel on client, or record upon designated channel, or take snapshot upon designated channel.

  To play video of designated channel on client, you need to enable Open camera video on client when triggering alarm, and also select **Open Alarm Associated Video** on Local **Config** interface at client.
- Link PTZ

  PTZ moves to designated preset.
- Alarm output

  Output alarm signal on the designated alarm output channel. It responds to alarm if alarm output port is connected to alarm device.
- Link Video Wall

  Display video channel onto video wall by sequence.
- Email

  Send email to inform designated personnel of alarm.
- Link Access Control

  Lock or unlock designated access control channel.

Alarm event types are different due to different device types, but the event parameters are the same. This chapter takes disk full alarm as an example to make introduction.

- Each alarm type needs to be configured independently.
- Linkage item is independent, you can link several items.

Step 1 Click **Config** on the client homepage.

The system displays **Config** interface.

Step 2 Select device or device channel from left device tree, click **Event Config**. See Figure 3-43.

The system displays **Event** interface, see Figure 3-44.

Select root node on the left device tree, device event configuration is displayed on the right. If no config, click No event config, click to config. or ▤ and enter configuration interface.

Figure 3-43 Config

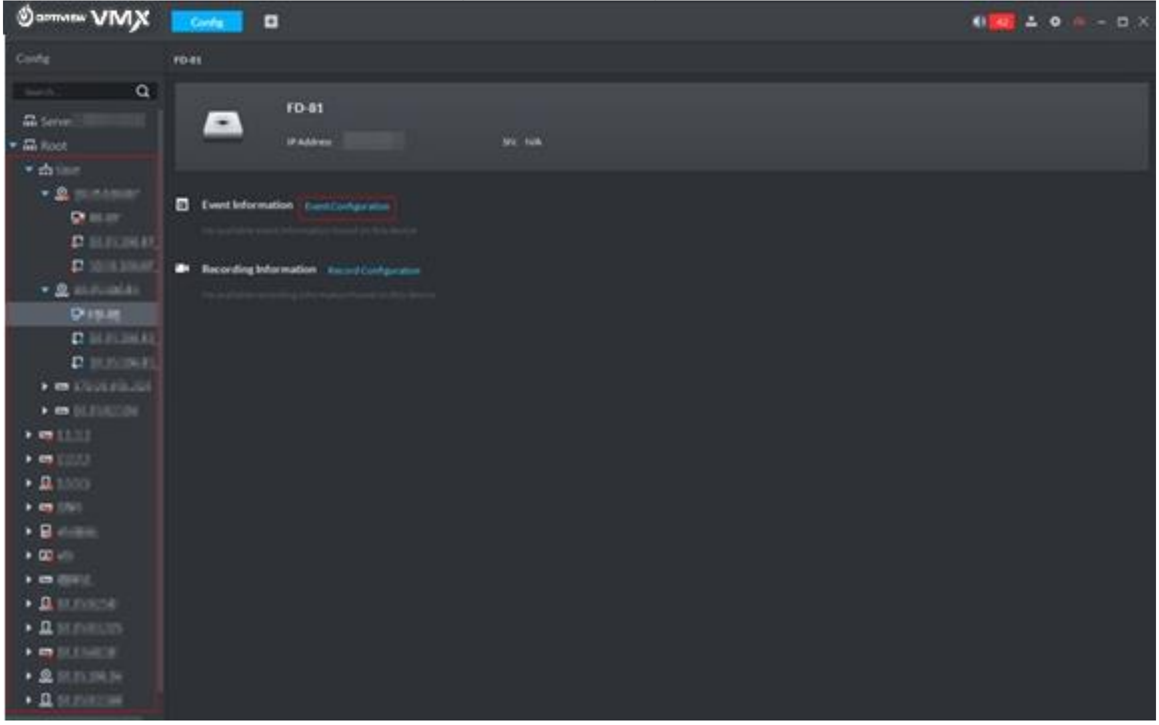
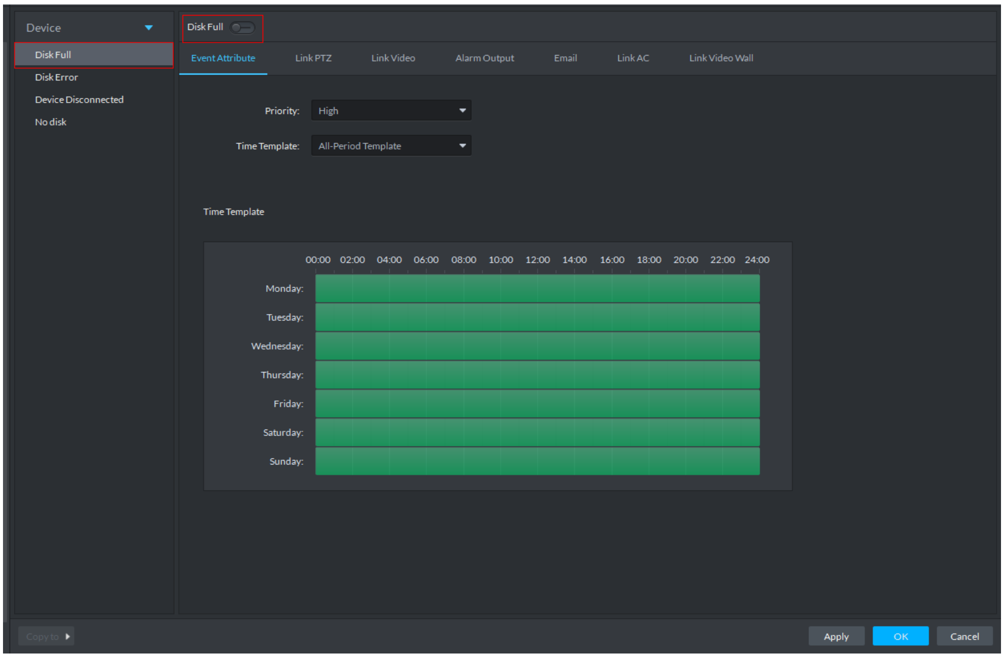

VMX
Config
Config
FD-81
Server
Root
FD-81
IP Address
Event Information
Event Configuration
Recording Information
Record Configuration

Figure 3-44 Event


Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Time Template
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
24:00
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:
Copy to
Apply
OK
Cancel

Priority: High

Time Template: All-Period Template

Step 3 Select alarm event type as disk full, and then click ○.

Icon is switched to ●, enable disk full. At this moment, ✓ is displayed next to the alarm event type on the left.

Step 4 Set event attribute

Include setting alarm event priority and effective period of event.

- Set Event Attribute

1) Click **Event Attribute** tab.

The system displays **Event Attribute** interface, see Figure 3-44.

2) Select priority.

Priority is only used to recognize alarm message.

3) Select time template, you need to configure again if default time template fails to meet requirement. For details, see **Set Time Template**.

After selected, the time info set by time template is displayed below.

- Set Time Template

Default time templates include all-period template, week day template and weekend template. If the default template fails to meet requirement, please add new template according to the following steps.

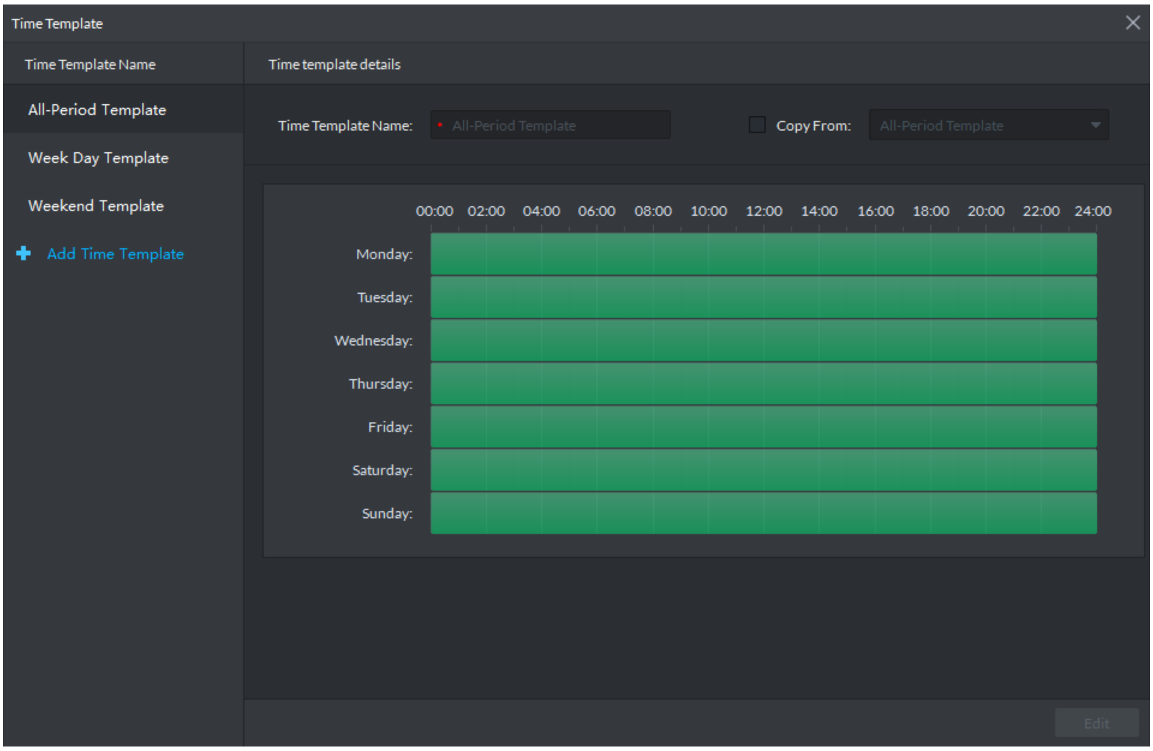
1) Click **Event Attribute** tab.

The system displays **Event Attribute** interface, see Figure 3-44.

2) Click **Time Template** and select **Manage Time Template**.

The system displays **Time Template** interface. See Figure 3-45.

Figure 3-45 Time template


Time Template
Time Template Name
All-Period Template
Week Day Template
Weekend Template
Add Time Template
Time template details
Time Template Name:
All-Period Template
Copy From:
All-Period Template
00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:
Edit

3) Click **Add Time Template.**

The system displays **Time Template Details** interface. See Figure 3-46.

Figure 3-46 Add time template

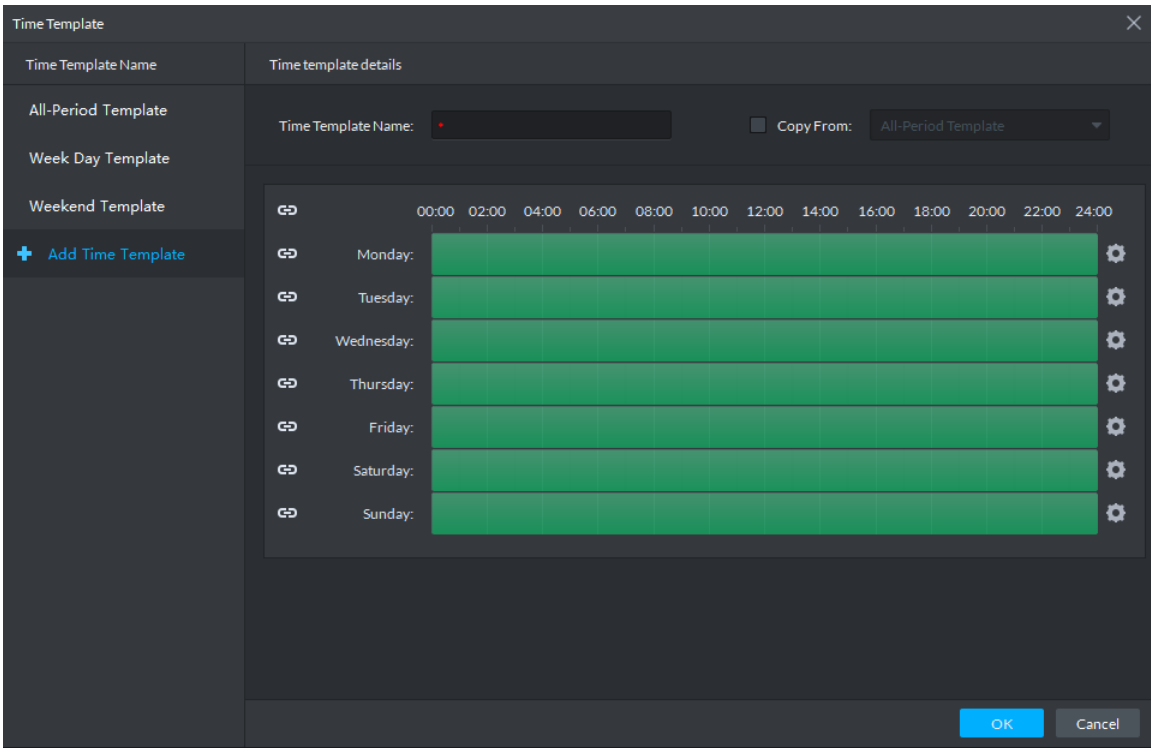
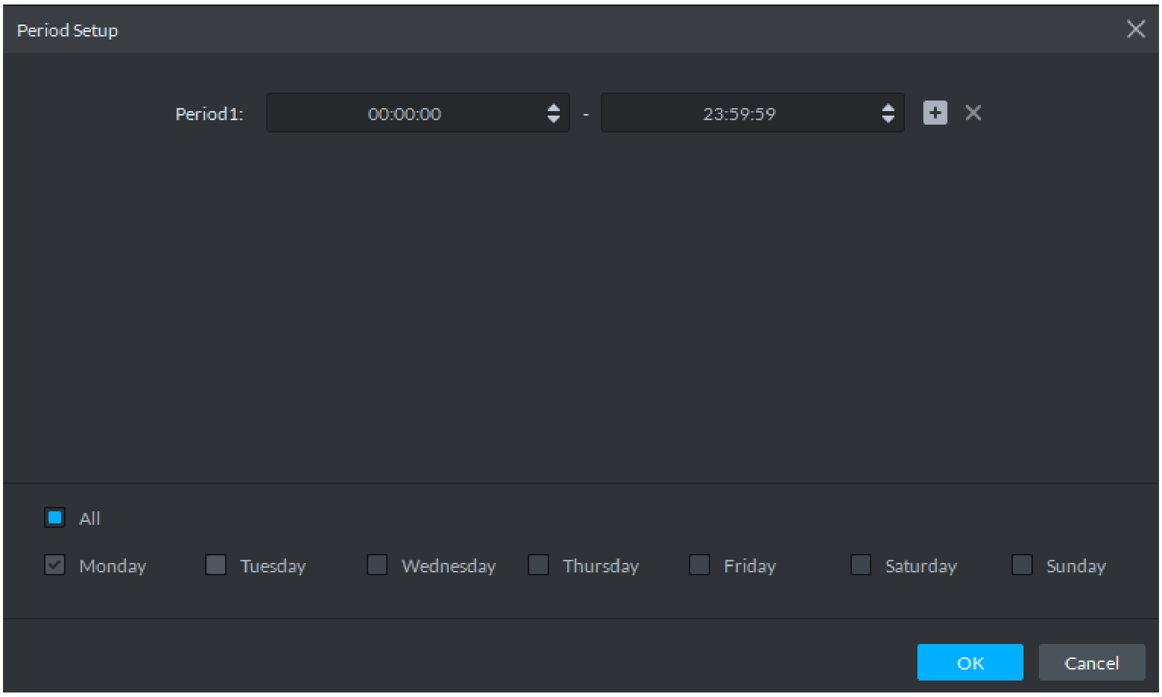

Time Template
Time Template Name
All-Period Template
Week Day Template
Weekend Template
Add Time Template
Time template details
Time Template Name:
Copy From:
All-Period Template
00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:
OK
Cancel

Figure 3-47 Period setting

4) Enter time template name, and set time by three following methods.
   - ◇ Select **Copy**, select existed default template, and copy time directly from default template.
   - ◇ Use mouse and drag time line, if time is set, then eraser is displayed, and erase the time of location where you drag; if time is not set, then pen is displayed, and add time of dragged location.
   - ◇ Click ⚙, set period and week, click ⊞ and add several periods, click ✕ to delete time. Click **OK** after setting is completed, save and return to the interface of Time Template Details. See Figure 3-48.

Figure 3-48 Period setup


Period Setup
OK
Cancel

Period1: 00:00:00 - 23:59:59

☑ All

☑ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

5) Click **OK** and time template is created.

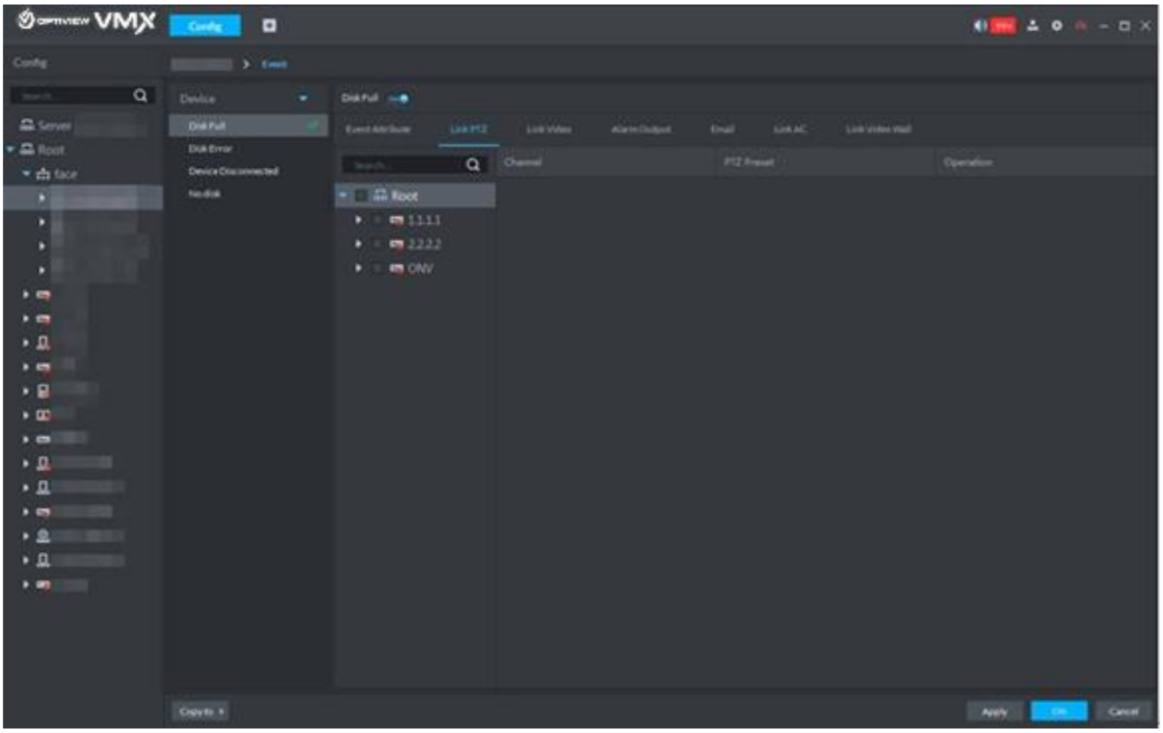
Step 5 Link PTZ.

When alarm event occurs, the linked PTZ moves to preset and realize monitoring.

1) Click **Link PTZ** tab.

The system displays **Link PTZ** interface, see Figure 3-49.

Figure 3-49 Link PTZ


OPTIVIEW VMX
Config
Config
Event
Search
Server
Root
face
Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Search
Root
1.1.1.1
2.2.2.2
ONV
Channel
PTZ Preset
Operation
Copy to
Apply
OK
Cancel

2) Select PTZ device from device tree.

3) Click drop-down box and select PTZ preset.

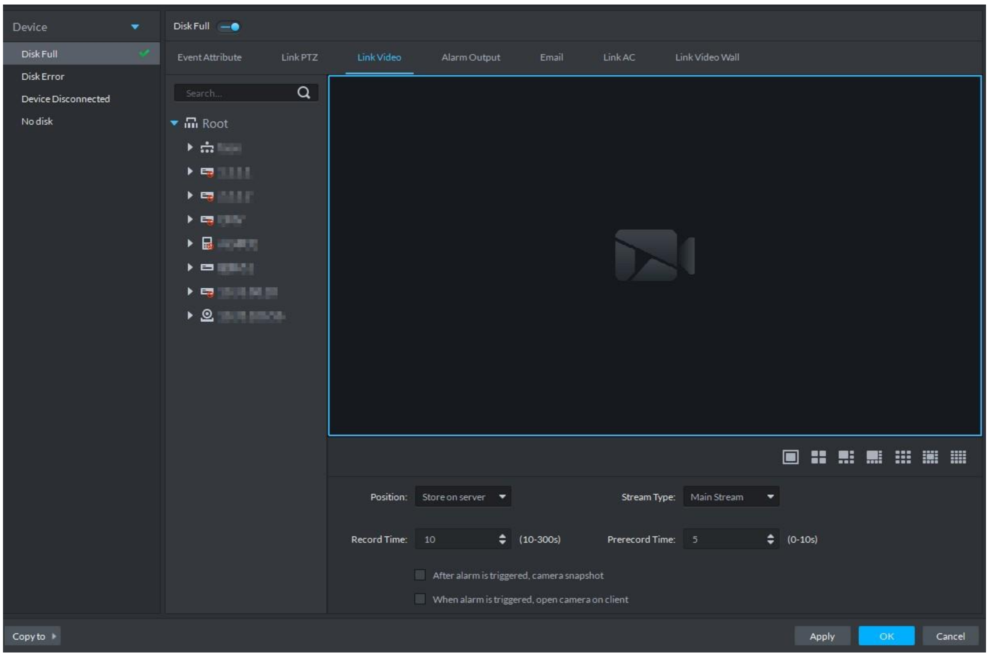
Step 6 Link Video.

When alarm event occurs, link associated device to record, capture and pop out video.

1) Click **Link Video** tab.

The system displays **Link Video** interface. See Figure 3-50.

Figure 3-50 Link video


Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Search...
Root
Copy to
Apply
OK
Cancel

Position: Store on server

Stream Type: Main Stream

Record Time: 10 (10-300s)

Prerecord Time: 5 (0-10s)

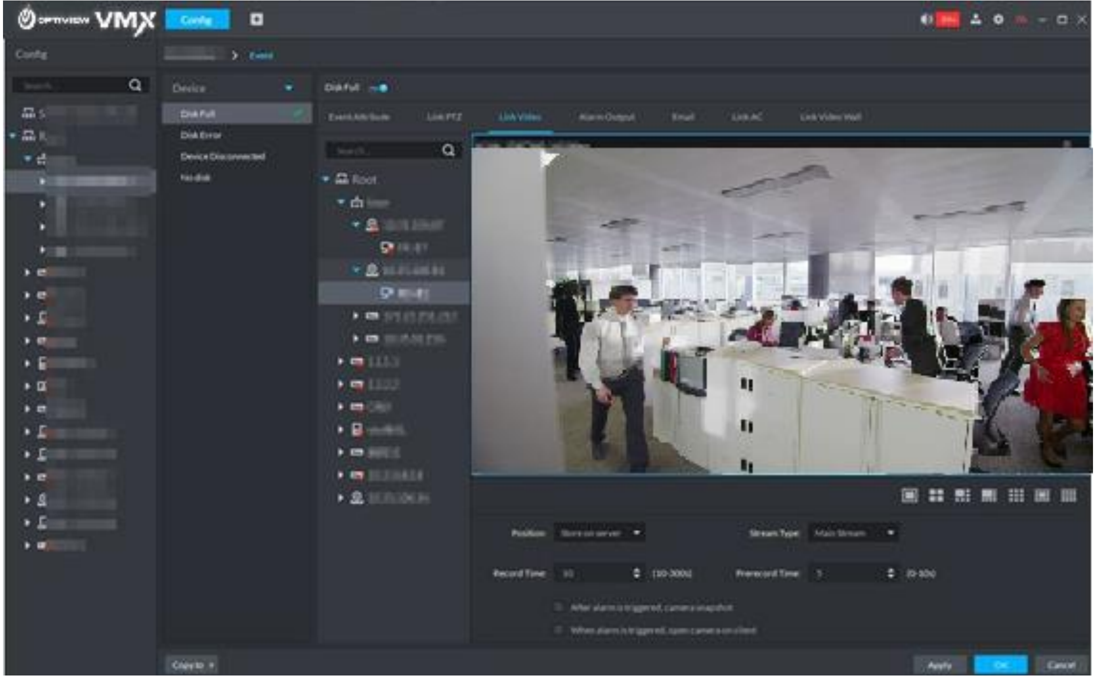
☐ After alarm is triggered, camera snapshot

☐ When alarm is triggered, open camera on client

2) Select window, drag the linked device to the window, and see Figure 3-51.

- Click icon under the window, you can select number of windows.
- After channel is dragged into window, click ▶ and display real-time video, click 🗑 to delete channel. If video is already played, please move the mouse to window, and click ✕.

Figure 3-51 Bind device channel


VMX
Config
Event
Device
Disk Full
Disk Error
Device Disconnected
No disk
Link Video
Root
Copy to
Apply
OK
Cancel

3) Set linked parameters, for more details, see Table 3-3.

Table 3-3 Link video parameter

Parameter	Description
Storage Position	Set storage position of videos and snapshots, support store on server, store on device or not record.
Stream Type	Select video stream of channel, support main stream, sub stream 1 and sub stream 2.
Record Time	Set time of linking record after alarm event is triggered.
Prerecord Time	Set prerecord time before linking record.
After alarm is triggered, camera snapshot	Link corresponding camera snapshot after alarm event is triggered.
When alarm is triggered, open camera on client	After alarm output is triggered, you can open camera’s real-time video on client.

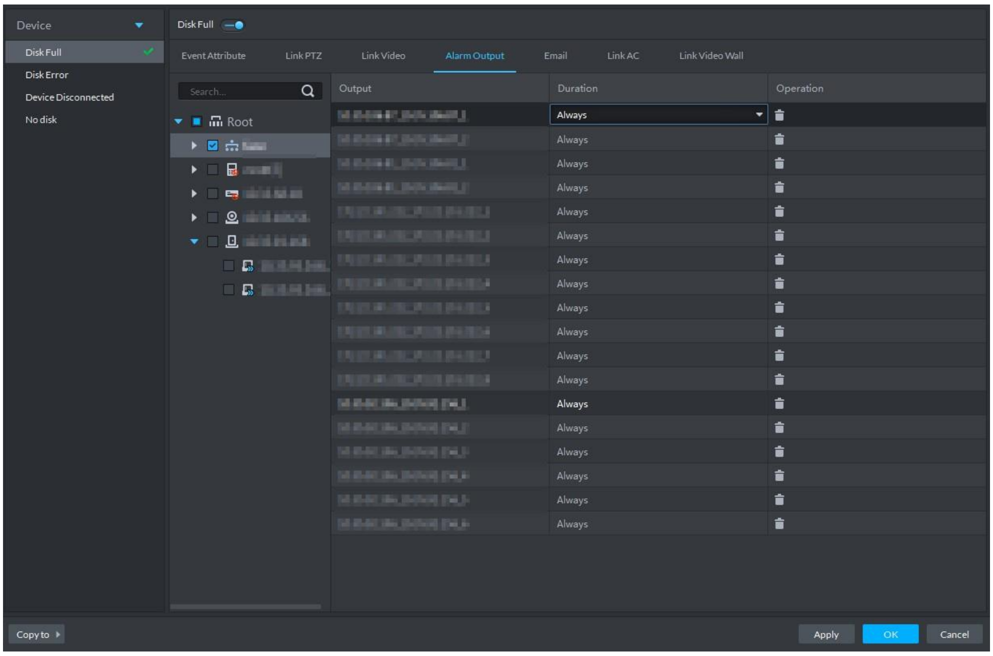
Step 7 Link Alarm Output.

Link external alarm output device and output alarm info when alarm event occurs.

1) Click **Alarm Output** tab.

The system displays **Alarm Output** interface, see Figure 3-52.

Figure 3-52 Alarm output


Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Search...
Root
Output
Duration
Operation
Always
Copy to
Apply
OK
Cancel

2) Select alarm output device.

3) Click the drop-down box of Duration on the right list, select alarm duration.

Click 🗑 in the list, or not select device, and then you can delete alarm output device.

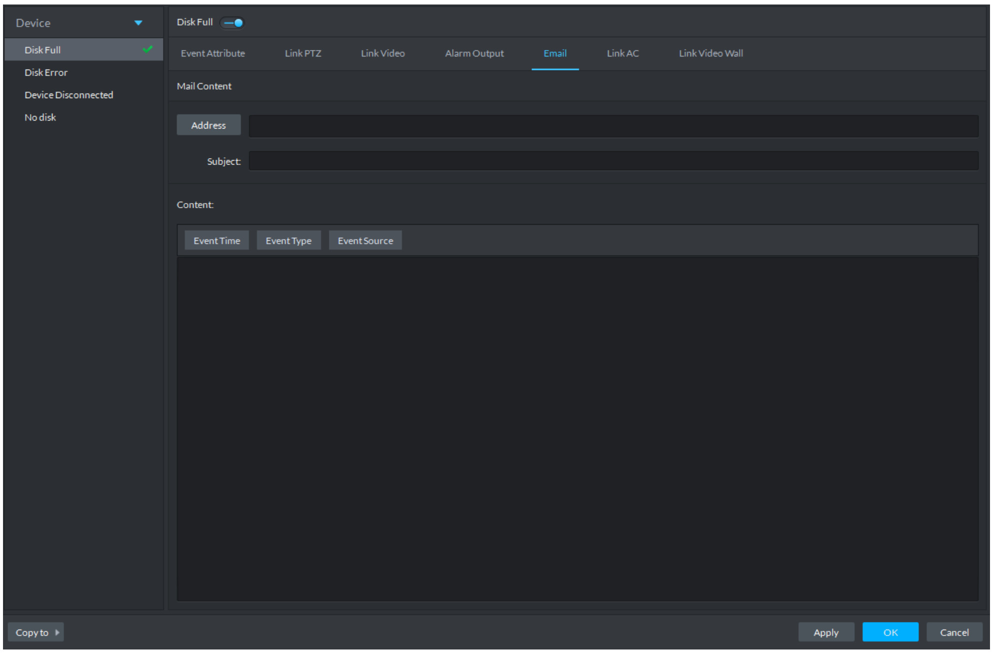
Step 8 Link Email.

When alarm event occurs, you can send email to remind user to deal with alarm event.

1) Click **Email**.

The system displays the **Email** interface, see Figure 3-53.

Figure 3-53 Email


Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Mail Content
Address
Subject:
Content:
Event Time
Event Type
Event Source
Copy to
Apply
OK
Cancel

2) Enter email address of the receiver into the address bar, or click **Address**, select email address of the receiver.

If you click Address and select receiver's email address, you need to make sure the email address of added user is already set; otherwise it cannot be displayed in the list.

3) Enter email subject.

4) Click the item and set email content, or enter email content directly. For example, select **Event Time**, then the email content sent to receiver will have event time.

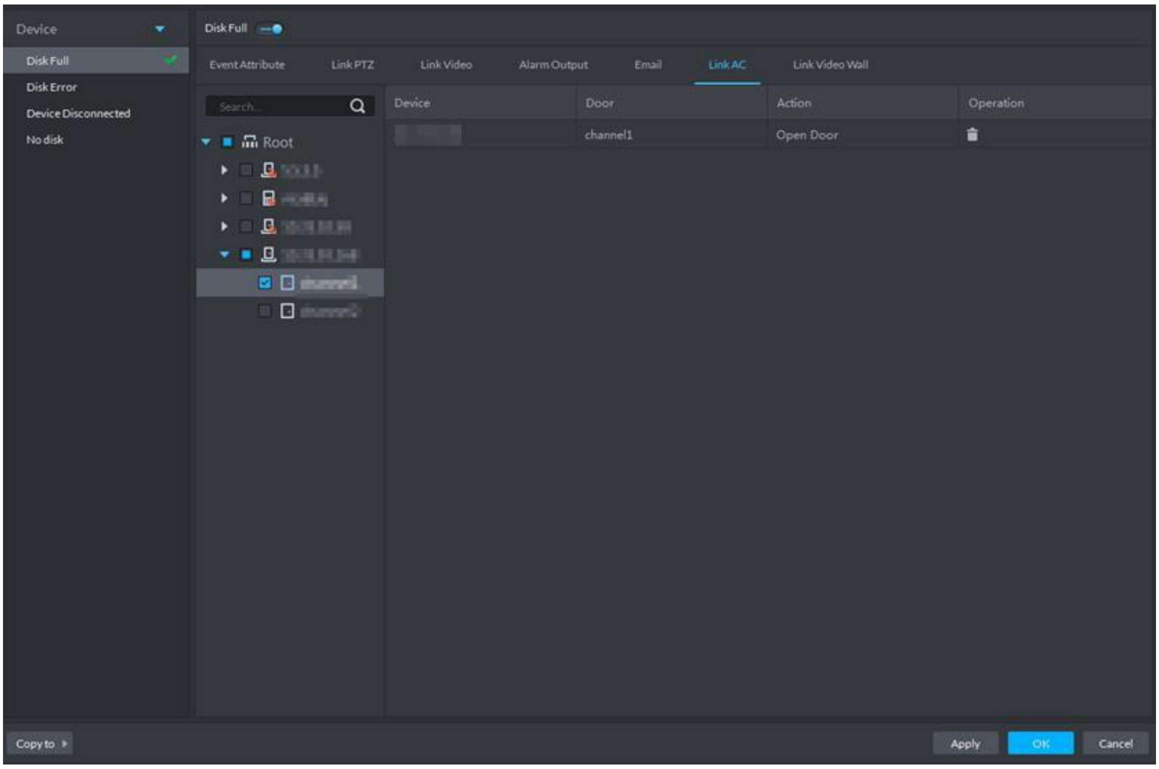
Step 9 Link Access Control

When alarm event occurs, it links several access control channels to close or open, each channel's status can be set independently.

1) Click **Link AC** tab.

The system displays **Link AC** interface, see Figure 3-54.

Figure 3-54 Link AC


Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Search...
Root
Copy to
Apply
OK
Cancel

Device	Door	Action	Operation
[redacted]	channel1	Open Door	🗑

2) Select channel of access control.

3) Select linkage action of the access control channel in the right list.

Support four types of action, open door, close door, always open and always close.

- ◇ Open door: Link to open door when alarm event is triggered.
- ◇ Close door: Link to close door when alarm event is triggered.
- ◇ Always open: Linked door is always open when alarm event is triggered.
- ◇ Always close: Linked door is always close when alarm event is triggered.

Click 🗑 in the list, or not select device, then you can delete access control channel.

Step 10 Link Video Wall.

When alarm event occurs, display video channel onto the video wall by sequence.

Please configure video wall before linking video wall setting. If video wall is not configured, enter Link Video Wall interface, the platform jumps to video wall configuration interface.

1) Click **Link Video Wall** tab.

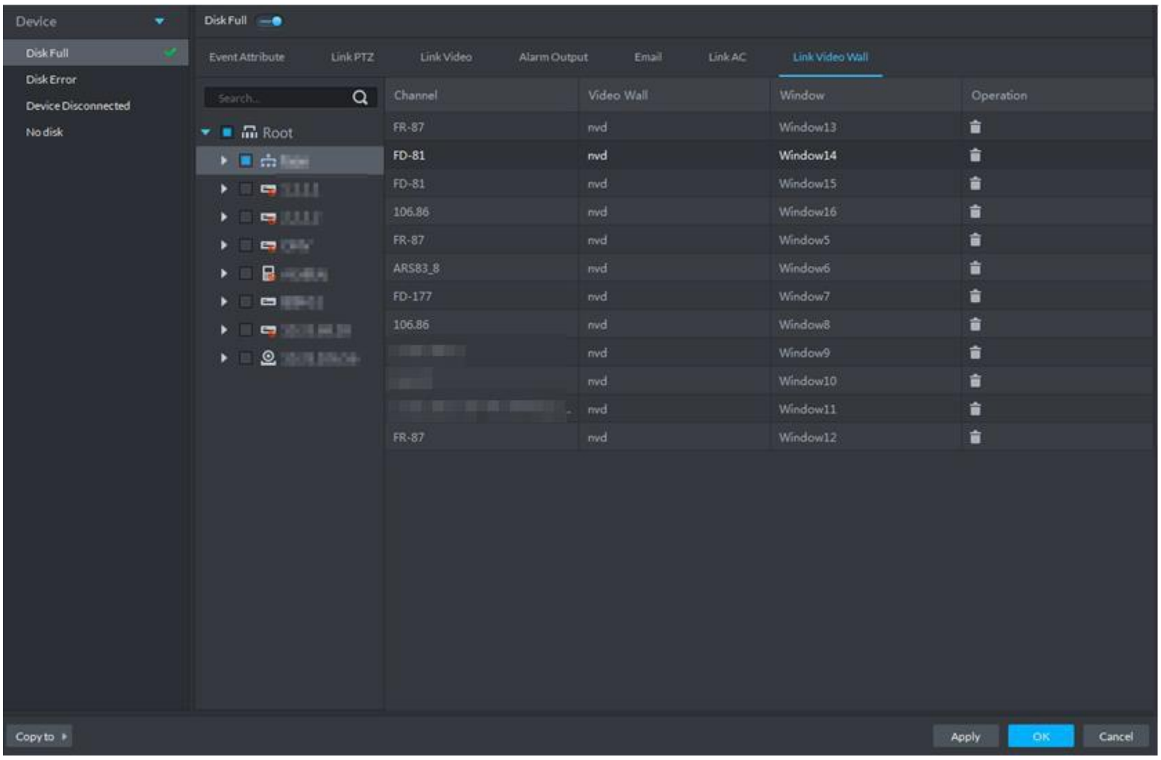
The system displays **Link Video Wall** interface.

2) Select video wall channel from the middle device list.

The system displays info of linking video wall, see Figure 3-55.

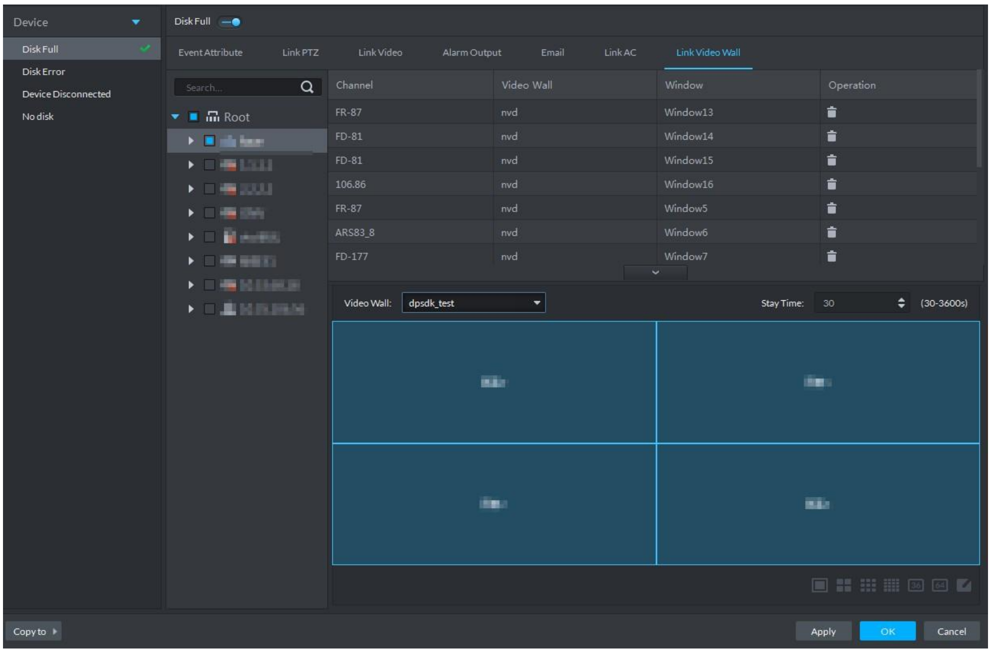
If video wall window is not configured, click **OK** on the prompt box, configure window on the video wall configuration interface, and see Figure 3-55.

Figure 3-55 Link video wall


Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Search...
Root
Copy to
Apply
OK
Cancel

Channel	Video Wall	Window	Operation
FR-87	nvd	Window13	🗑
FD-81	nvd	Window14	🗑
FD-81	nvd	Window15	🗑
106.86	nvd	Window16	🗑
FR-87	nvd	Window5	🗑
ARS83_8	nvd	Window6	🗑
FD-177	nvd	Window7	🗑
106.86	nvd	Window8	🗑
	nvd	Window9	🗑
	nvd	Window10	🗑
	nvd	Window11	🗑
FR-87	nvd	Window12	🗑

Figure 3-56 Configure video wall window.


Device
Disk Full
Disk Error
Device Disconnected
No disk
Disk Full
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Search...
Root
Copy to
Apply
OK
Cancel

Channel	Video Wall	Window	Operation
FR-87	nvd	Window13	🗑
FD-81	nvd	Window14	🗑
FD-81	nvd	Window15	🗑
106.86	nvd	Window16	🗑
FR-87	nvd	Window5	🗑
ARS83_8	nvd	Window6	🗑
FD-177	nvd	Window7	🗑

Video Wall: dpsdk_test

Stay Time: 30 (30-3600s)

3) Select **Video Wall** and **Window**, click **OK**.

If you want to configure new window, select New Window from the drop-down box, see Figure 3-55.

Step 11 Click **OK** and complete setting.

3.2.5 Setting Record Plan

If the device is equipped with video channel, it supports configuring different stream record plans (such as main stream, sub stream), and configure storage position of video (platform server or device).

For storage space config, refer to 3.2.1.4 Setting Storage Space. Following risks may exist if not configured.

- Record disk is not configured, system may fail to store record file.
- Local storage disk does not divide general picture disk, causing intelligent alarm event and linkage snapshot cannot be stored, snapshots are not displayed.

Step 1 Click **Config** on the client homepage.

The system displays **Config** interface.

Step 2 From the device tree on the left, select device channel, click **Record Configuration**, see Figure 3-57.

The system displays **Record** interface, see Figure 3-58.

Figure 3-57 Enter record configuration interface

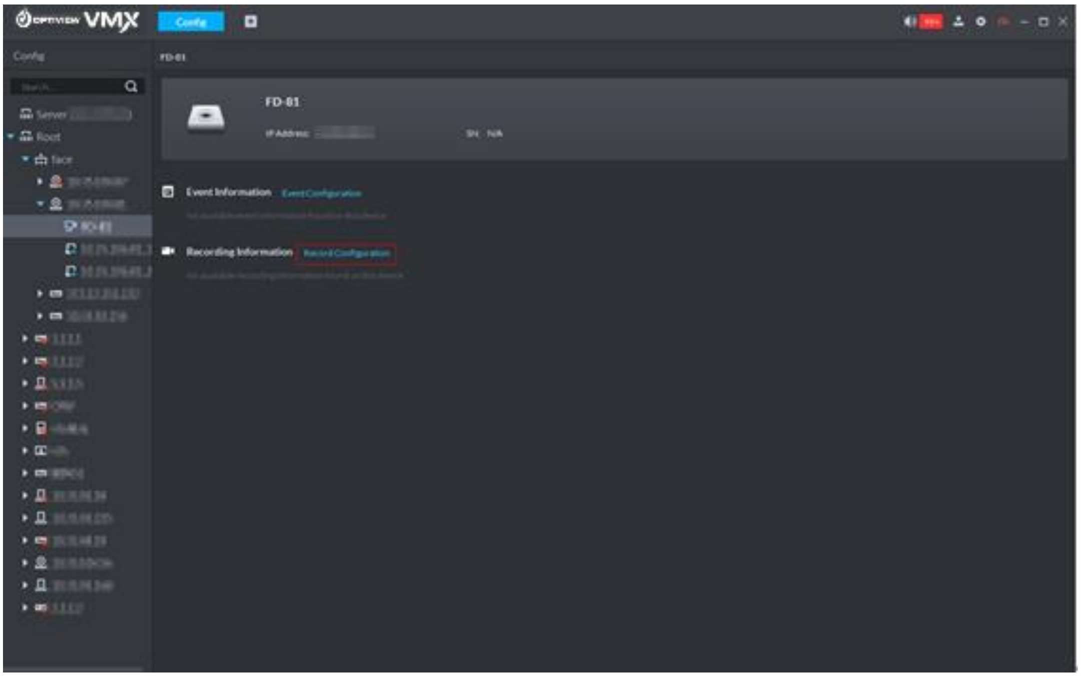
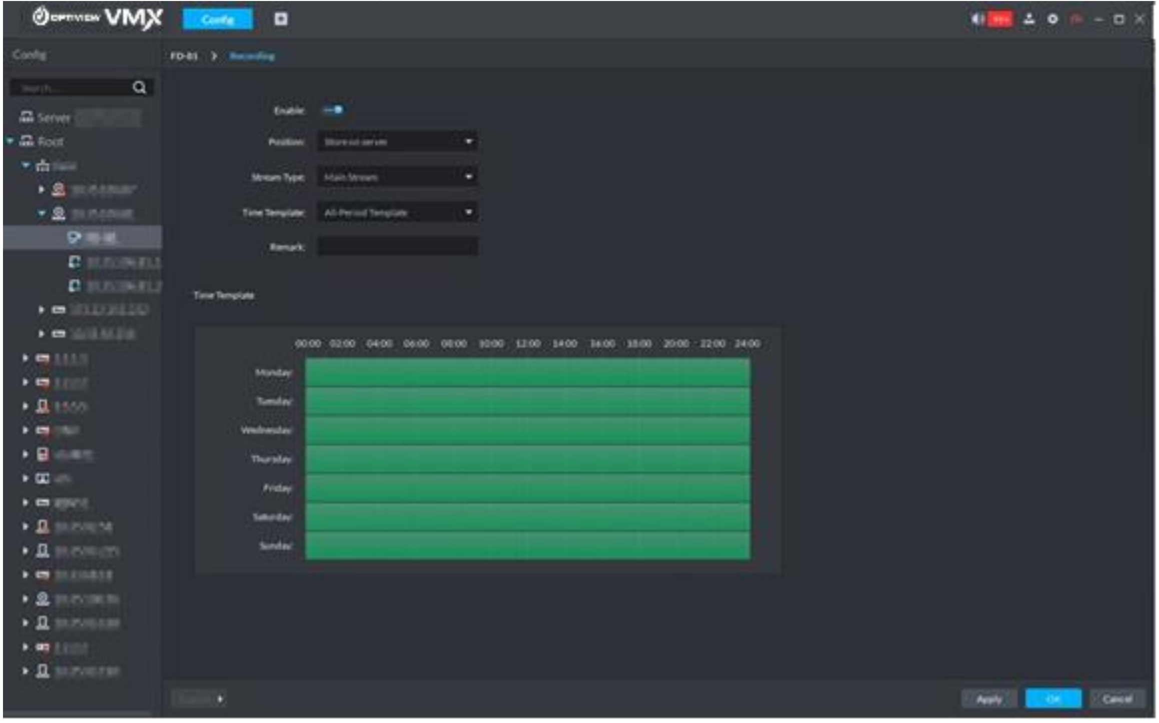

VMX
Config
Config
FD-01
Server
Root
face
FD-01
IP Address:
SN: N/A
Event Information
Event Configuration
Recording Information
Record Configuration

Figure 3-58 Record



Enable: ●

Position: Store on server

Stream Type: Main Stream

Time Template: All-Period Template

Remark:

VMX
Config
FD-01
Recording
Server
Root
Time Template
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
24:00
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Apply
OK
Cancel

Step 3 Click ○.

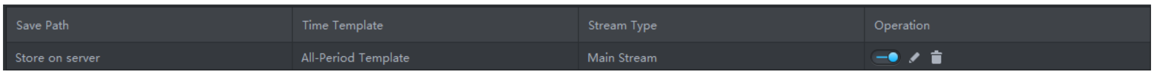
The icon is switched to ●, enable record plan.

Step 4 Select Position, Stream Type and Time Template.

The default time template is provided by system, if requirement is not met, then you can cteate new template. For details, you can refer to **Configure Time Template**.

Step 5 Click **OK**, complete record plan config, and see Figure 3-59.

Figure 3-59 Record info



Save Path	Time Template	Stream Type	Operation
Store on server	All-Period Template	Main Stream	● ✎ 🗑

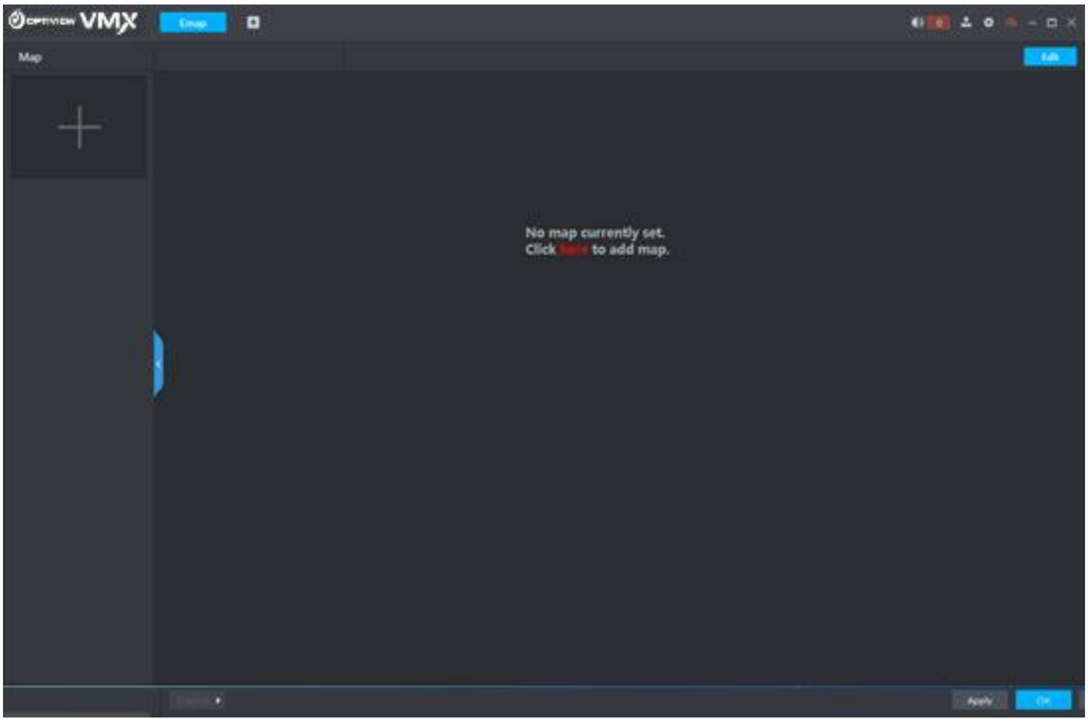
3.2.6 Configuring Emap

The platform supports to import raster map. Import raster map means importing a map picture on the platform. You can add device on the map and link device to map, you can view device and alarm on the map directly. Meanwhile, the track function of different modules (such as personnel management and face recognition) can call map and generate movement track.

3.2.6.1 Adding Map

Step 1 Click **Emap** on the client homepage.

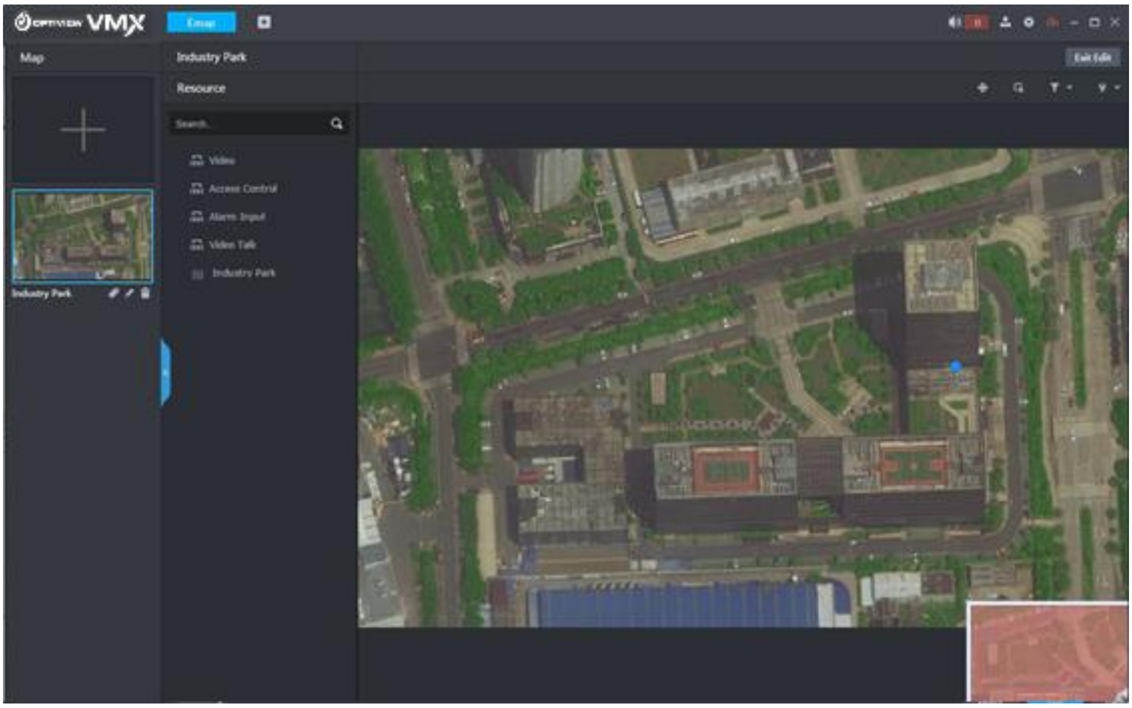
The system displays **Emap** interface, see Figure 3-60 and Figure 3-61.


VMX
Emap
Map
Edit
Apply
OK

No map currently set.
Click here to add map.

Figure 3-60 Emap-first use

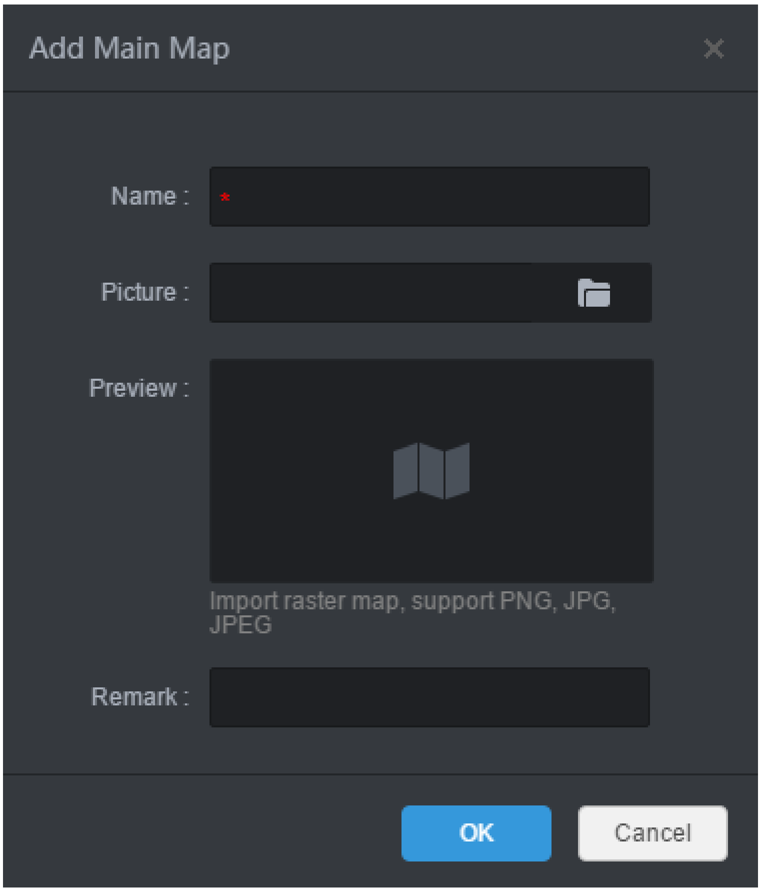
Figure 3-61 Emap-non first use


VMX
Emap
Map
Industry Park
Exit Edit
Resource
Search...
Video
Access Control
Alarm Input
Video Talk
Industry Park
Industry Park

Step 2 Add main map.

1) Click Here for the first use, click + on the left if not use for the first time.
The system displays Add Main Map interface, see Figure 3-62.

Figure 3-62 Add main map


Add Main Map
×
Name :
*
Picture :
Preview :
Import raster map, support PNG, JPG, JPEG
Remark :
OK
Cancel

2) Enter **Name** and **Remark**, click 🗀 and select picture.

After the picture is selected, selected pictures are displayed on the **Live View** area.

🕮

Picture supports raster map, supports PNG, JPG and JPEG.

3) Click **OK**.

The map is imported to platform. See Figure 3-63.

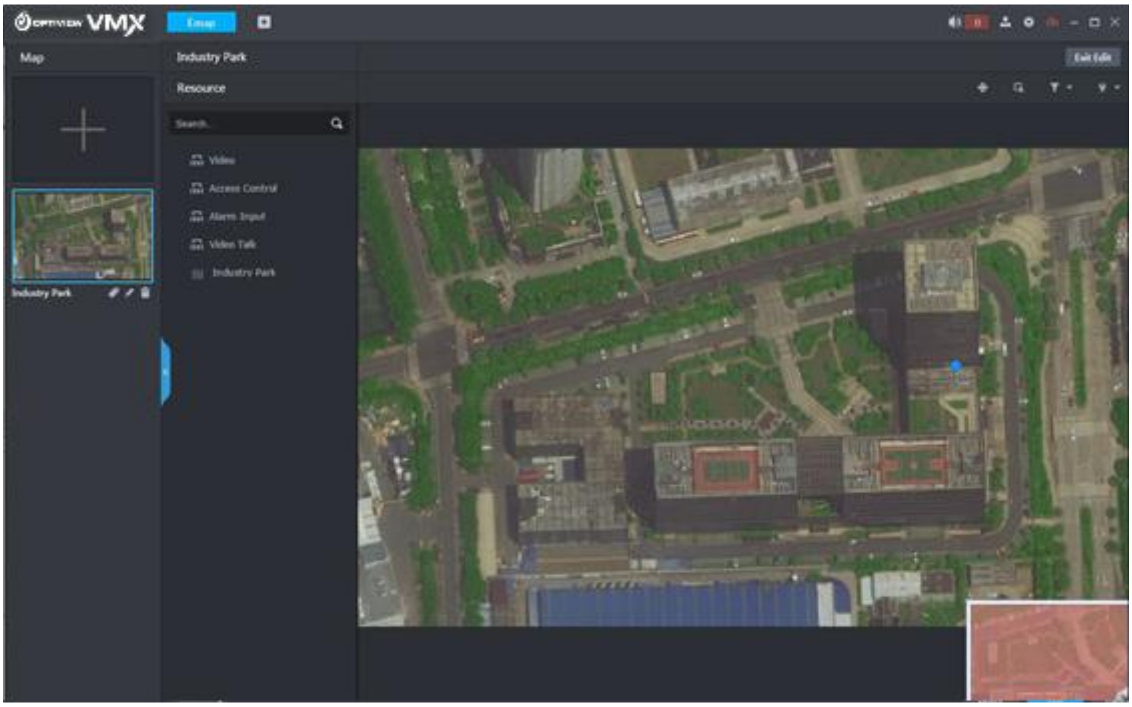
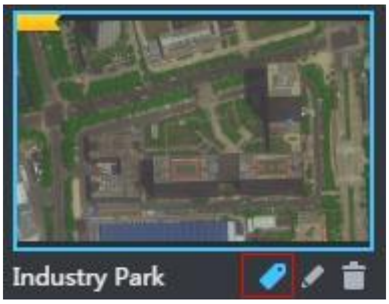

VMX
Emap
Map
Industry Park
Resource
Exit Edit
Search...
Video
Access Control
Alarm Input
Video Talk
Industry Park
Industry Park

Figure 3-63 Added map

4) Click 🏷 under the map, set it as main map, yellow mark is displayed on the left upper corner, see Figure 3-64.

   When several maps are added at the same time, the main map is displayed.

Figure 3-64 Set main map


Industry Park

Step 3 Add hot zone in the map list.

The map can be configured with several layers, you can add lower level map to the existed map, and manage by levels.

1) Click map in the list, open the map, and see Figure 3-65.

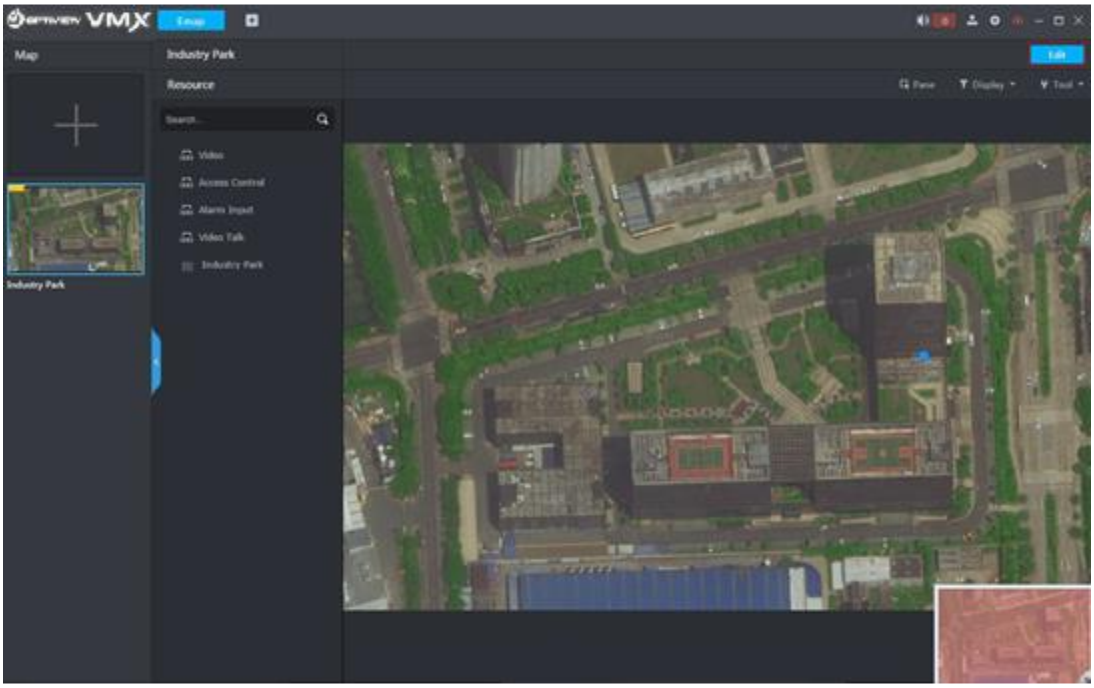

VMX
Emap
Map
Industry Park
Resource
Edit
Pane
Display
Tool
Search...
Video
Access Control
Alarm Input
Video Talk
Industry Park
Industry Park

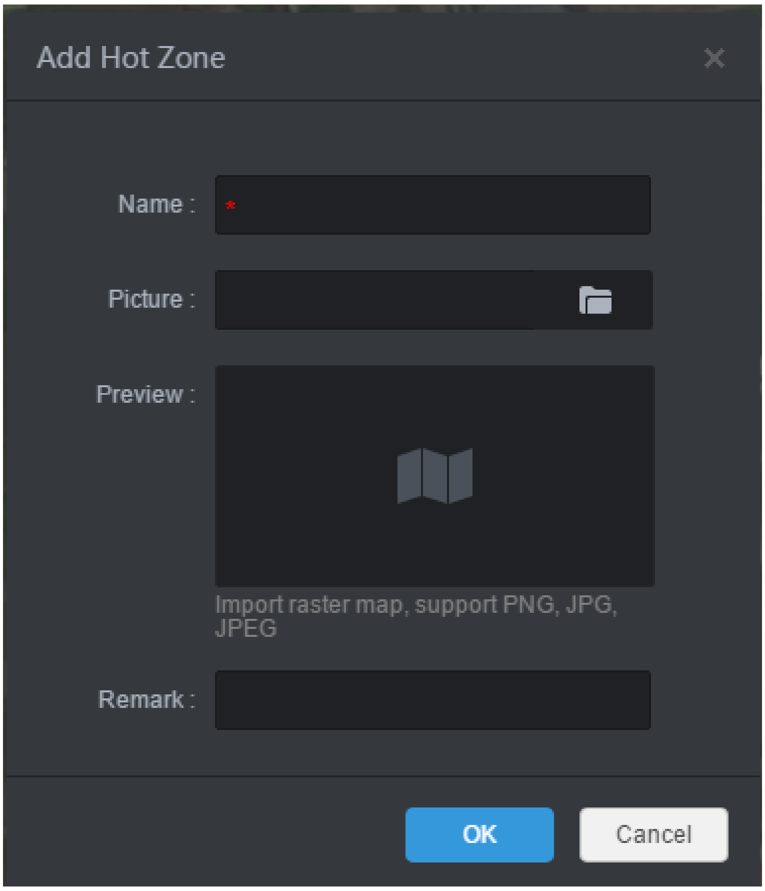
Figure 3-65 Open map

2) Open map, click **Edit** on the upper right corner, and then you can edit the map.

3) Click , the mouse becomes map icon, select location on the map and click **Add**.

The system displays **Add Hot Zone** interface, see Figure 3-66.

Figure 3-66 Add hot zone


Add Hot Zone
Name :
*
Picture :
Preview :
Import raster map, support PNG, JPG, JPEG
Remark :
OK
Cancel

4) Enter **Name** and **Remark**, click and select picture.

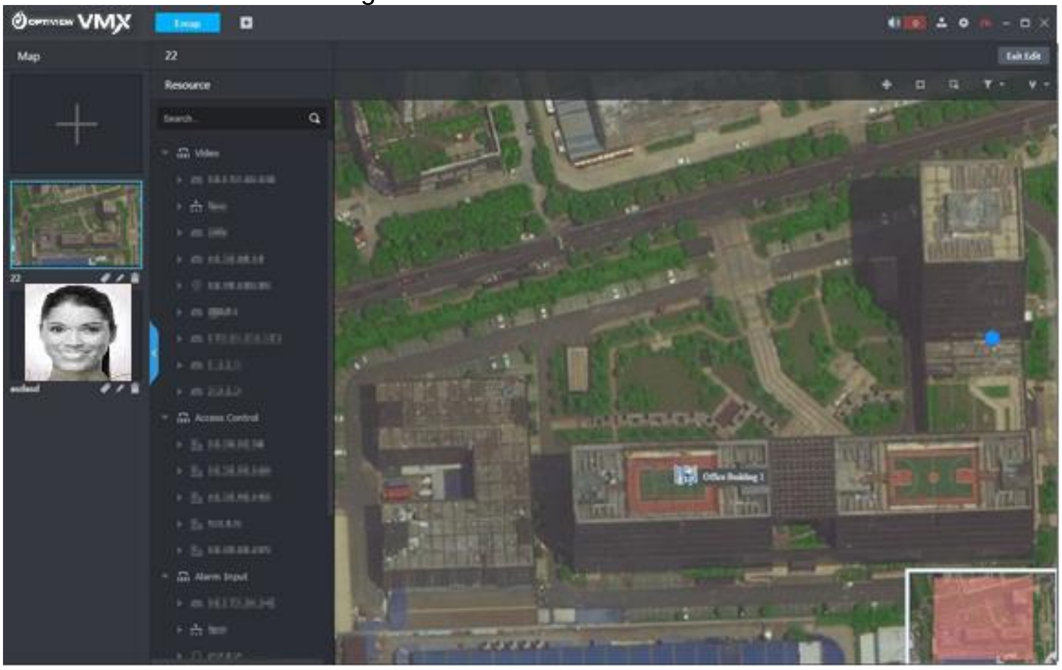
- The format of imported raster map supports PNG, JPG and JPEG.
- After adding the picture, it is displayed on the live view area.

5) Click **OK**.

Hot zone is added, see Figure 3-67. Left list displays map levels, right map displays hot zone icon.

- After the hot zone is added, click hot zone on the left or hot zone icon on the right, then you can open hot zone for display.
- You can continue to add lower-level hot zone according to the operation above.

Figure 3-67 Hot zone added

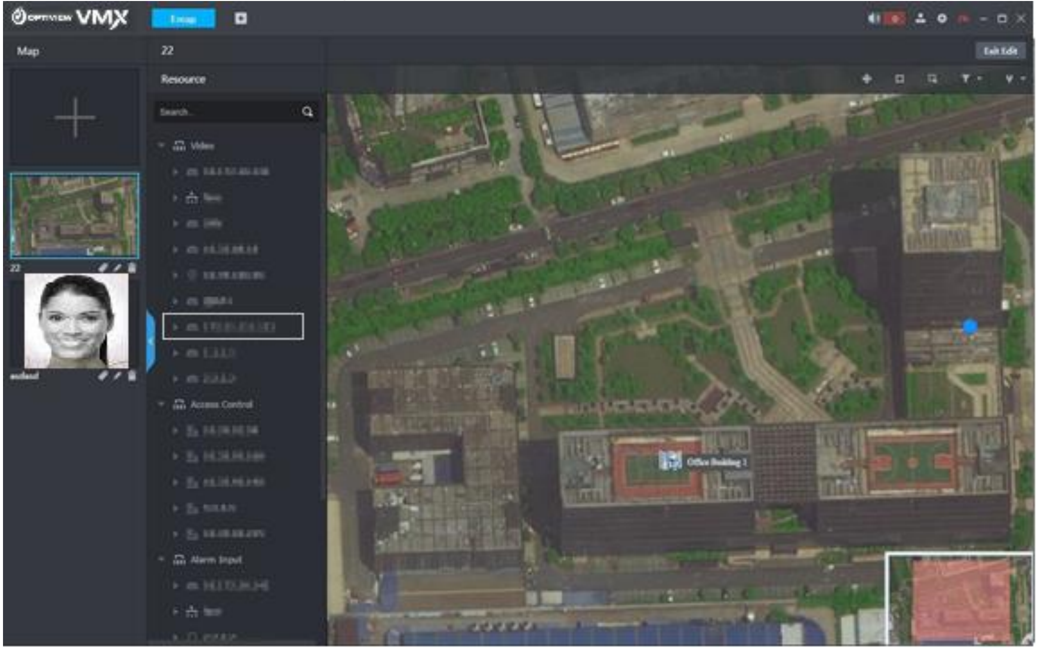


Step 4 Drag device channel onto the map for display.

According to actual requirement, add video channel, access control channel or alarm channel to the map, and device is linked to map, then you can see device and alarm on the map directly. Meanwhile, the track functions of different modules (such as personnel management and face recognition) can call map, and generate movement track.

1) Click the map in the list, and open the map, see Figure 3-65.
2) Click **Edit** on the upper right corner.
   The map can be edited.
3) Select device channel from the resource list in the middle, drag to the proper location on the map, see Figure 3-68.

Figure 3-68 Add device channel


VMX
Emap
Map
22
Resource
Search...
Video
Access Control
Alarm Input
Exit Edit
Office Building 1

4) Click **Exit Edit** on the upper right corner.

3.2.6.2 Viewing Map

Step 1 Click **Emap** on the client homepage.

The system displays Emap interface.

Step 2 Click map in the list.

The system opens map, see Figure 3-69. For interface description, see Table 3-4.

Figure 3-69 Map

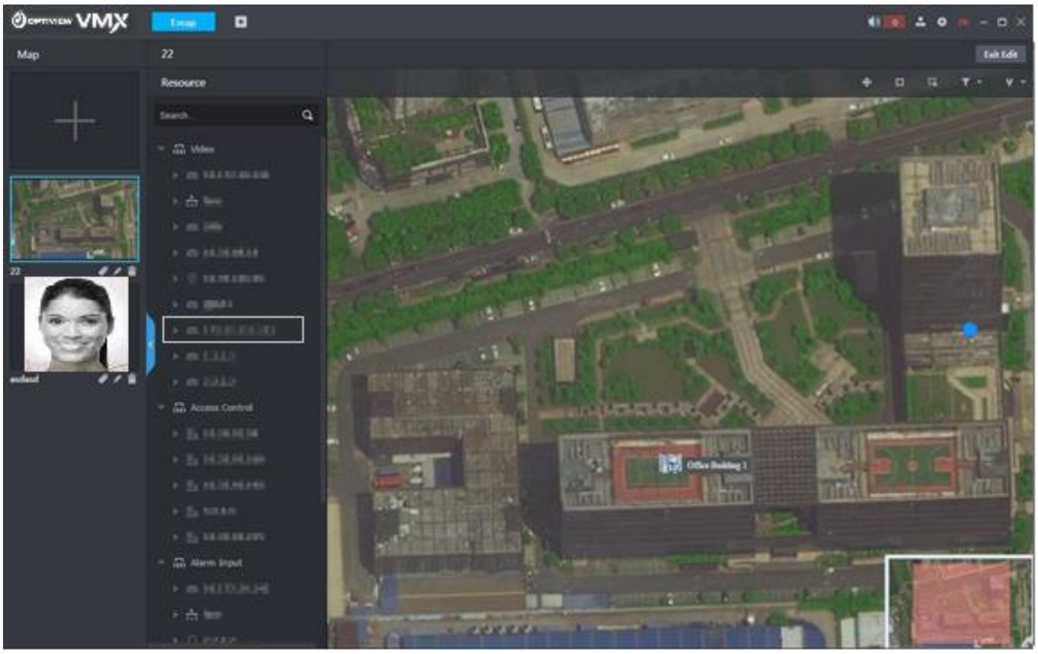

VMX
Emap
Map
22
Resource
Search...
Video
Access Control
Alarm Input
Exit Edit
Office Building 1

Table 3-4 Interface function description

Icon	Function	Description
	Select device	Click the icon and it becomes blue, select an area on the map and it displays the device list within the area. Select device, click corresponding icon, and then you can view video, playback video and delete the device.
	Display device	Filter by device type, only the kept device type is displayed on the map.
	Mark or reset	Include mark and reset. ● Mark: Mark on the map. ● Reset: Restore the map to default position.

Following operations are supported on the map:

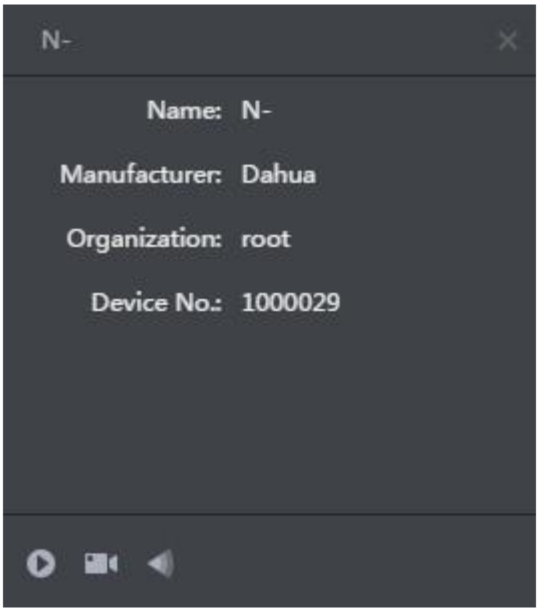
- View channels on map

  Double-click channel from the left device tree, and then you can view the channel position on the map.
  - ◇ Roll the mouse on the map and you can zoom in or out map.
  - ◇ If the picture is too big to be completely displayed, you can drag the red module on the lower right corner to display by mouse.
- View channel details

  Click the channel on the map, the system displays device number, name, manufacturer and organization, see Figure 3-70.

  Different devices may have different channel details and operations.

Figure 3-70 Channel info



N-

Name: N-

Manufacturer: Dahua

Organization: root

Device No.: 1000029

- View channel video

  Click and open channel video.
- View playback

  Click and realize video playback.
- View visible range

Click ◀ and view visible range.

- Edit map

  Click **Edit** on the upper right corner, the map can be edited, see Figure 3-71. For operations, see

Figure 3-71 Edit map

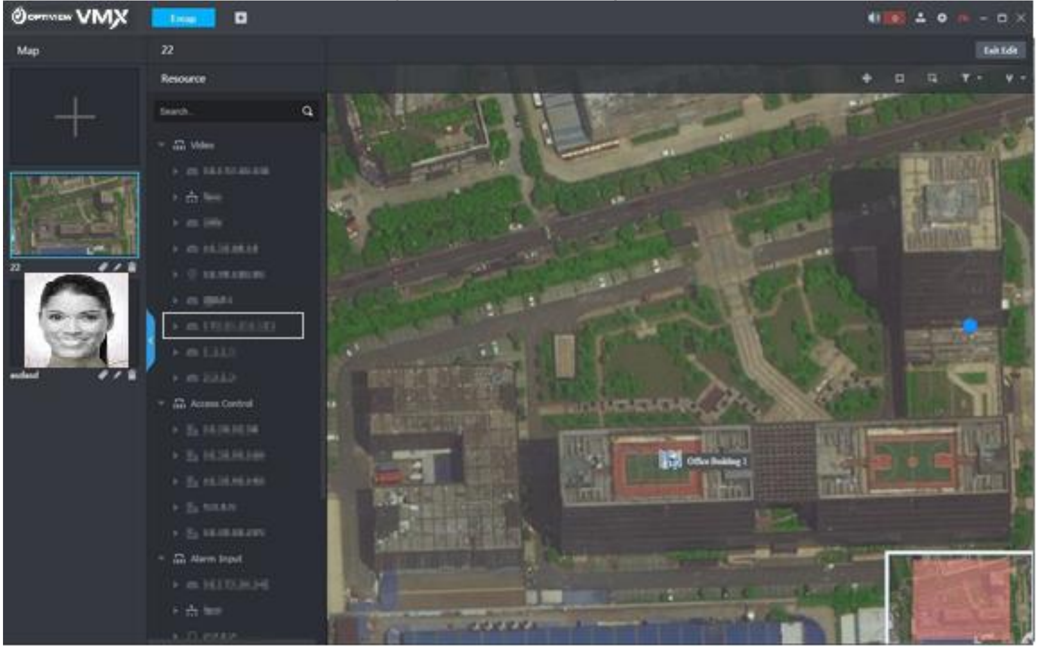


Table 3-5 Operation description

Icon	Function	Description
✥	Move device	Click the icon and it becomes blue, you can drag the device on map and change its position. Click again to exit move status
▢	Add hot zone	Refer to “3.2.6.1 Adding Map.”
⬚	Select device	Click the icon and it becomes blue, select an area on the map and it will display device list within the area. Select device, click corresponding icon, and then you can playback video and delete the device.
▼ ▾	Display device	Filter by device type, only kept device type is displayed on the map.
▾	Mark or reset	Include mark and reset. ● Mark: Mark on the map. ● Reset: Restore the map to default position.

3.3 Local Config

Set client local config, including basic setting, video setting, playback setting, snapshot setting, record setting, alarm and shortcut key. All the settings only take effect to client.

If you want to restore default config, click **Default** and restart client according to system prompt.

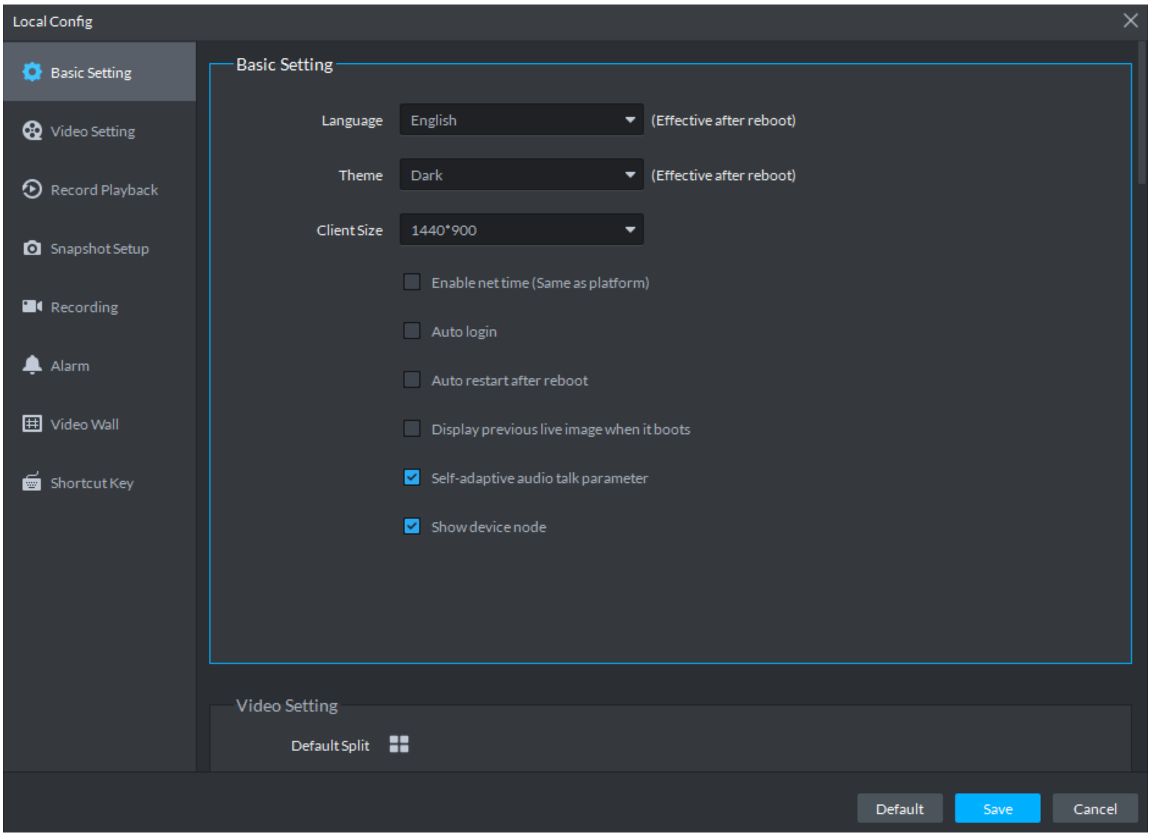
3.3.1 Setting Basic Parameter

Set client language, client size and sync time.

Step 1 Click ⚙ on the upper right corner on client interface.

The system displays **Local Config** interface, see Figure 3-72

Figure 3-72 Local config


Local Config
Basic Setting
Video Setting
Record Playback
Snapshot Setup
Recording
Alarm
Video Wall
Shortcut Key
Default
Save
Cancel

Basic Setting

Language: English (Effective after reboot)

Theme: Dark (Effective after reboot)

Client Size: 1440*900

☐ Enable net time (Same as platform)

☐ Auto login

☐ Auto restart after reboot

☐ Display previous live image when it boots

☑ Self-adaptive audio talk parameter

☑ Show device node

Video Setting

Default Split

Step 2 Click **Basic Setting** tab, set basic parameters, and see Figure 3-72. For parameter description, see Table 3-6.

Table 3-6 Basic parameter description

Parameters	Description
Language	Modify the language displayed on client; reboot the client to make it valid after setting.
Theme	Theme color includes dark and white. Reboot the client to make it valid after setting.
Client size	Select client proper resolution according to PC display screen.

Parameters	Description
Enable net time	If enabled, the client starts to synchronize network time with the server, and make the client time in accordance with that of server. The client will make following response when server requires net time. ● If the parameter is selected, then client will respond to net time when server makes request. ● If the parameter is not selected, then client will not respond when server makes request.
Auto login	● For login this time, Remember Password is selected on the Login interface, after selecting Auto Login, exit client and log in again, the system logs in automatically. ● For login this time, Remember Password is not selected on the Login interface, after selecting Auto Login, exit client and log in again, Remember Password and Auto Login are selected by default on login interface, but still need to enter password authentication login.
Auto restart after reboot	● For login this time, Remember Password is selected on the Login interface, after selecting Auto restart after reboot, start PC again, and the system logs in client automatically. ● For login this time, Remember Password is not selected on the Login interface, after selecting Auto restart after reboot, start PC again, the system displays client login interface.
Displayprevious live Image when it boots	If enabled, system displays the last live video automatically after rebooting the client.
Self-adaptive audio talk parameter	If enabled, the systems adapt to sampling frequency, sampling bit, and audio format to the device automatically during audio talk.
Show device node	Device tree displays device and channel info under device, otherwise it only displays channel.

Step 3 Click **Save**.

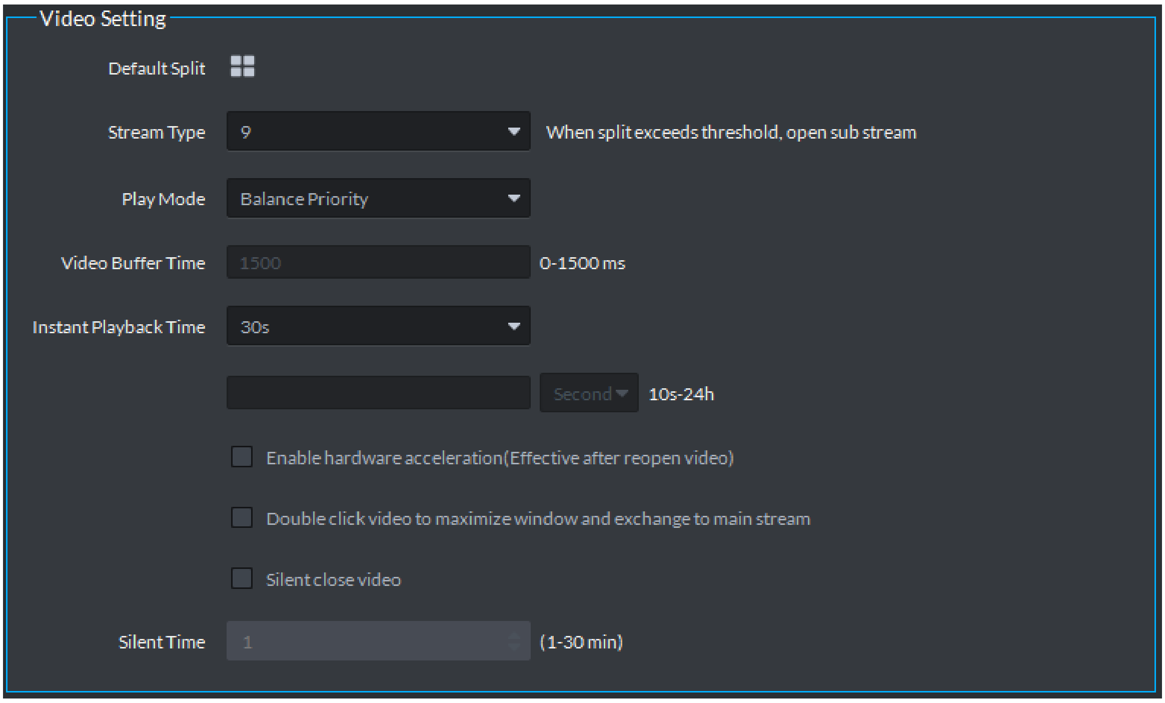
3.3.2 Setting Real-time Video Parameter

Set video window split mode, stream type, play mode and instant playback time.

Step 1 Click ⚙ on the upper right corner of client interface.
The system displays **Local Config** interface.

Step 2 Click **Video Setting** tab, set parameters, and see Figure 3-73. For parameter details, see Table 3-7.

Figure 3-73 Video setting



Video Setting

Default Split

Stream Type: 9 — When split exceeds threshold, open sub stream

Play Mode: Balance Priority

Video Buffer Time: 1500 — 0-1500 ms

Instant Playback Time: 30s

Second — 10s-24h

☐ Enable hardware acceleration(Effective after reopen video)

☐ Double click video to maximize window and exchange to main stream

☐ Silent close video

Silent Time: 1 — (1-30 min)

Table 3-7 Video setting parameter description

Parameter	Description
Default Split	Set split mode of the video window.
Stream type	Defines bit stream type for video transmission. With main bit stream as default, the auxiliary bit stream will be used when number of window splits is greater than the value selected here.
Play Mode	Play mode to be selected as required, including Real Time Priority, Fluency Priority, Balance Priority, as well as user-defined modes.
Video buffer time	Set video buffer time. It is only valid when play mode is customized.
Instant playback time	Select instant playback time and then click Instant playback on the Live view interface, you can view the record of current period.
Enable hardware acceleration	Check the box to enable the function. Use hardware module to enhance acceleration features.
Double-click video to maximize window and exchange to main stream	Check the box to enable the function.
Silent close video	After being enabled, if the time of no operation for the Live interface exceeds the set value, the system will close Live automatically.

Step 3 Click **Save**.

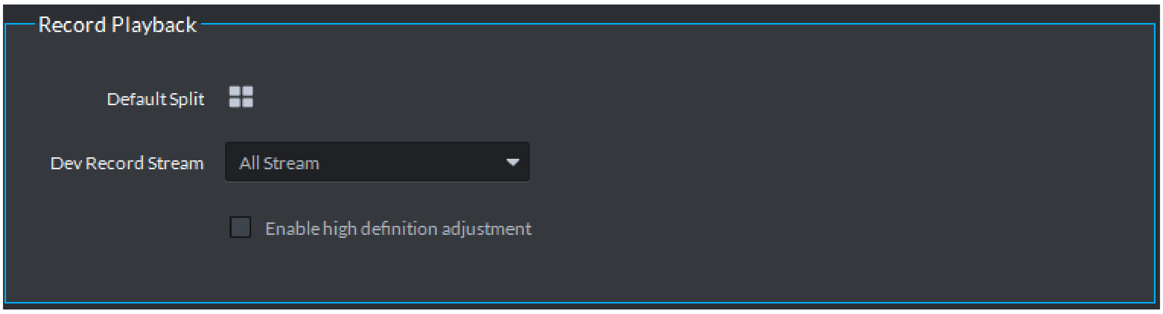
3.3.3 Setting Record Playback

Set video window split mode and record stream type.

Step 1 Click ⚙ on upper right corner of client interface.
The system displays **Local Config** interface.

Step 2 Click **Record Playback** tab, set parameters, and see Figure 3-74. For details, refer to Table 3-8.

Figure 3-74 Record playback



Record Playback

Default Split

Dev Record Stream: All Stream

☐ Enable high definition adjustment

Table 3-8 Record playback parameter description

Parameters	Description
Default Split	Set default split mode of the playback window.
Device record stream	Select record playback bit stream.
Enable high definition adjustment	Check the box to enable the function. In high definition, big bit stream playback mode, system reserves I frames only to guarantee video fluency and reduce high decoding pressure.

Step 3 Click **Save**.

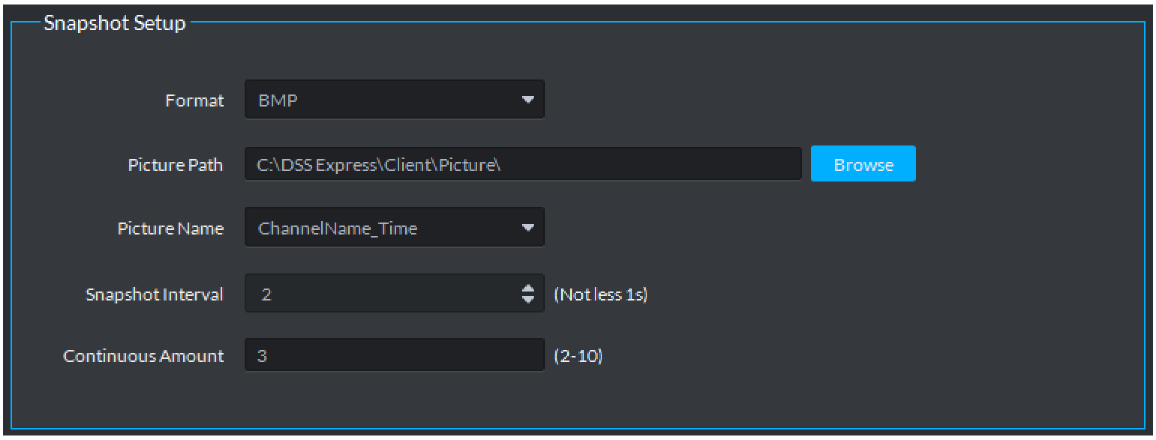
3.3.4 Setting Snapshot

Set snapshot save format, path and naming rule.

Step 1 Click ⚙ on upper right corner of client interface.
The system displays **Local Config** interface.

Step 2 Click **Snapshot Setup** tab, set snapshot format and save path, see Figure 3-75. For parameter details, see Table 3-9.

Figure 3-75 Snapshot setting



Snapshot Setup

Format: BMP

Picture Path: C:\DSS Express\Client\Picture\

Picture Name: ChannelName_Time

Snapshot Interval: 2 (Not less 1s)

Continuous Amount: 3 (2-10)

Table 3-9 Snapshot setting parameter description

Parameter	Description
Format	Set snapshot image format.

Parameter	Description
Picture path	Set snapshot storage path. The default path: C:\OPTIVIEW VMX \Client\Picture\.
Picture name	Select picture name rule.
Snapshot interval	Set snapshot interval. System snapshot once after the specified period.
Continuous amount	Snapshot amount at each time.

Step 3 Click **Save**.

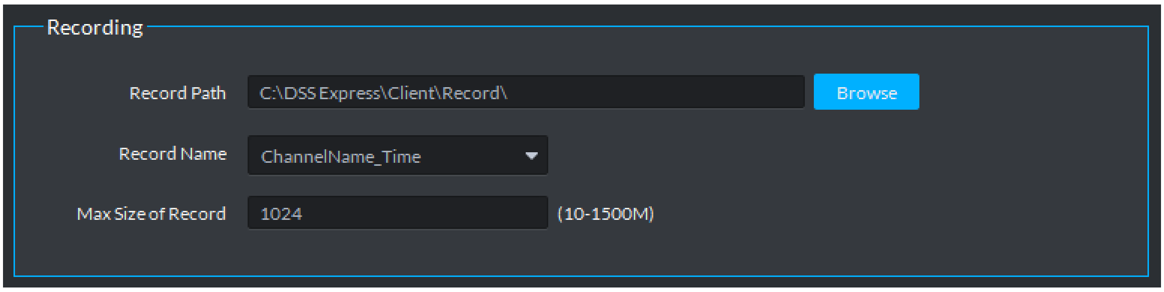
3.3.5 Setting Recording Parameter

Set record path and record name of record file when recording on client.

Step 1 Click ⚙ on upper right corner of client interface.
The system displays **Local Config** interface.

Step 2 Click **Recording** tab, set record path and save path, see Figure 3-76. For parameter details, see Table 3-10.

Figure 3-76 Recording



Recording

Record Path: C:\DSS Express\Client\Record\

Record Name: ChannelName_Time

Max Size of Record: 1024 (10-1500M)

Table 3-10 Recording parameter description

Parameters	Description
Record path	Set record storage path. The default path: C:\OPTIVIEW VMX \Client\Record\.
Record name	Set record file name rule.
Max. record size	Set record file size.

Step 3 Click **Save**.

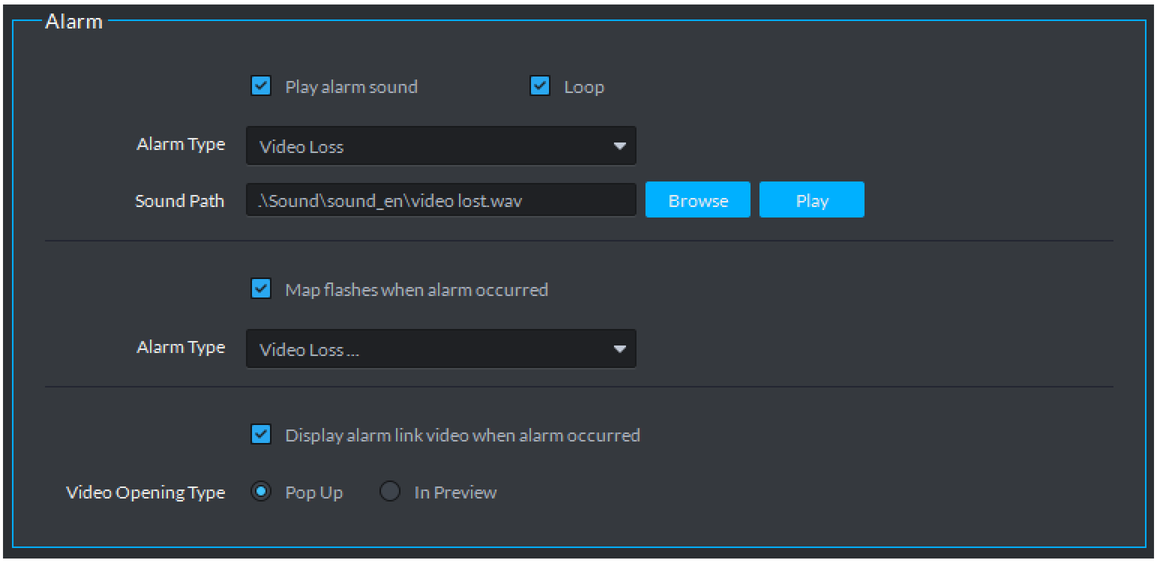
3.3.6 Setting Alarm Parameter

Set alarm type, sound path and video opening type.

Step 1 Click ⚙ on upper right corner of client interface.
The system displays **Local Config** interface.

Step 2 Click **Alarm** tab, set client alarm type, see Figure 3-77.

Figure 3-77 Alarm



Alarm

☑ Play alarm sound ☑ Loop

Alarm Type: Video Loss

Sound Path: .\Sound\sound_en\video lost.wav

☑ Map flashes when alarm occurred

Alarm Type: Video Loss ...

☑ Display alarm link video when alarm occurred

Video Opening Type: ● Pop Up ○ In Preview

Table 3-11 Alarm parameter description

Parameter	Description
Play alarm sound	Check the box, system generates a sound when an alarm occurs.
Loop	Check the box; system plays alarm sound repeatedly when an alarm occurs. 📖 This item is only valid when Play alarm sound function is enabled.
Alarm Type	Set alarm type. System can play sound when corresponding alarm occurs. 📖 This item is only valid when Play alarm sound function is enabled.
Sound Path	Select alarm audio file path.
Map flashes when alarm occurred	Check the box and then select alarm type. When the corresponding alarm occurs, the device on the emap can flash.
Display alarm link video when alarm occurred	Check the box, system automatically opens linkage video when an alarm occurs.
Video opening type	System automatically opens linkage video when an alarm occurs. You can view on the pop-up window or on the **Live View** interface.

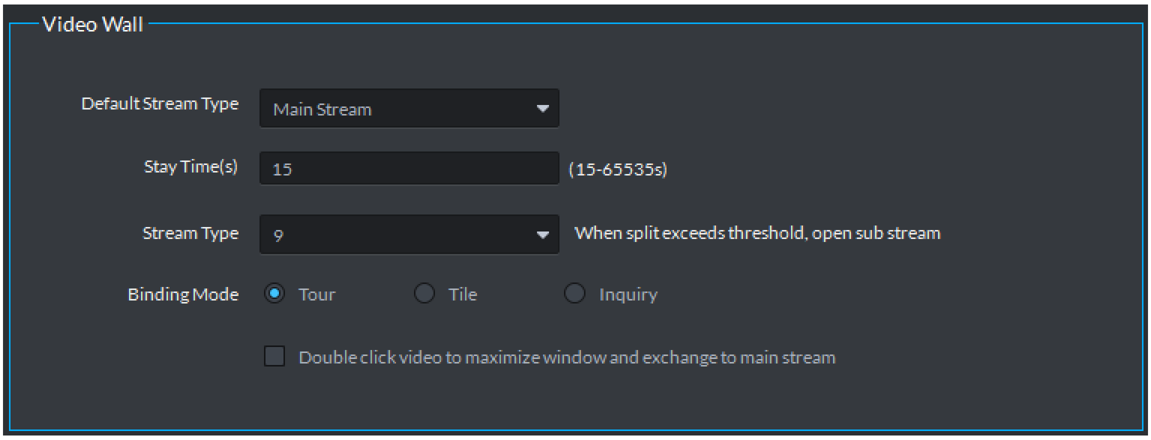
Step 3 Click **Save**.

3.3.7 Setting Video Wall

Set default stream type and stay time when linking video wall.

Click **Video Wall** and set parameters, see Figure 3-78. For parameter details, see Table 3-12.

Figure 3-78 Video wall


Video Wall

Default Stream Type: Main Stream

Stay Time(s): 15 (15-65535s)

Stream Type: 9 When split exceeds threshold, open sub stream

Binding Mode: ● Tour ○ Tile ○ Inquiry

☐ Double click video to maximize window and exchange to main stream

Table 3-12 Video wall parameter description

Parameter	Description
Stream type	When split exceeds threshold, open sub stream.
Binding mode	● Tour: Device nodes are displayed on 1 window by tour. ● Tile: Device nodes are displayed on windows of current screen by tile. ● Inquiry: When dragging the device nodes to the window, the systems prompts whether tour or tile.
Double-click video to maximize window and exchange to main stream	Double-click the video screen to maximize the window, and the stream change to main stream.

3.3.8 Setting Shortcut Key

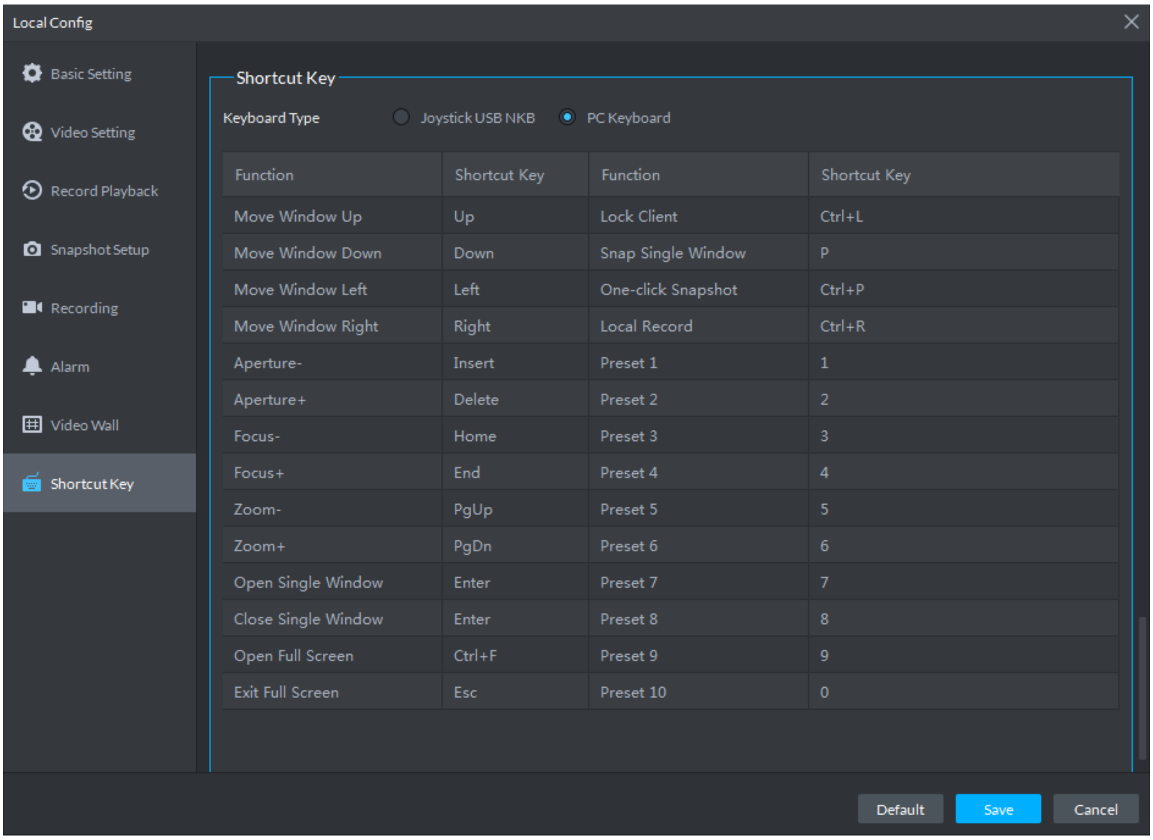
Set client shortcut key and control client quickly.

Step 1 Click ⚙ on upper right corner of client interface.

The system displays **Local Config** interface.

Step 2 Click **Shortcut Key** tab, check PC keyboard or shortcut key of USB keyboard, see Figure 3-79.

Figure 3-79 Shortcut key


Local Config
Basic Setting
Video Setting
Record Playback
Snapshot Setup
Recording
Alarm
Video Wall
Shortcut Key
Default
Save
Cancel

Shortcut Key

Keyboard Type ○ Joystick USB NKB ● PC Keyboard

Function	Shortcut Key	Function	Shortcut Key
Move Window Up	Up	Lock Client	Ctrl+L
Move Window Down	Down	Snap Single Window	P
Move Window Left	Left	One-click Snapshot	Ctrl+P
Move Window Right	Right	Local Record	Ctrl+R
Aperture-	Insert	Preset 1	1
Aperture+	Delete	Preset 2	2
Focus-	Home	Preset 3	3
Focus+	End	Preset 4	4
Zoom-	PgUp	Preset 5	5
Zoom+	PgDn	Preset 6	6
Open Single Window	Enter	Preset 7	7
Close Single Window	Enter	Preset 8	8
Open Full Screen	Ctrl+F	Preset 9	9
Exit Full Screen	Esc	Preset 10	0

Step 3 Click **Save**.

3.4 Live View

You can check video of online channel. If the device is equipped with PTZ function, then you can operate PTZ on platform.

3.4.1 Entering Live View Interface

On client homepage, click **Live View**. The system displays **Live View** interface, see Figure 3-80. For interface description, see Table 3-13.

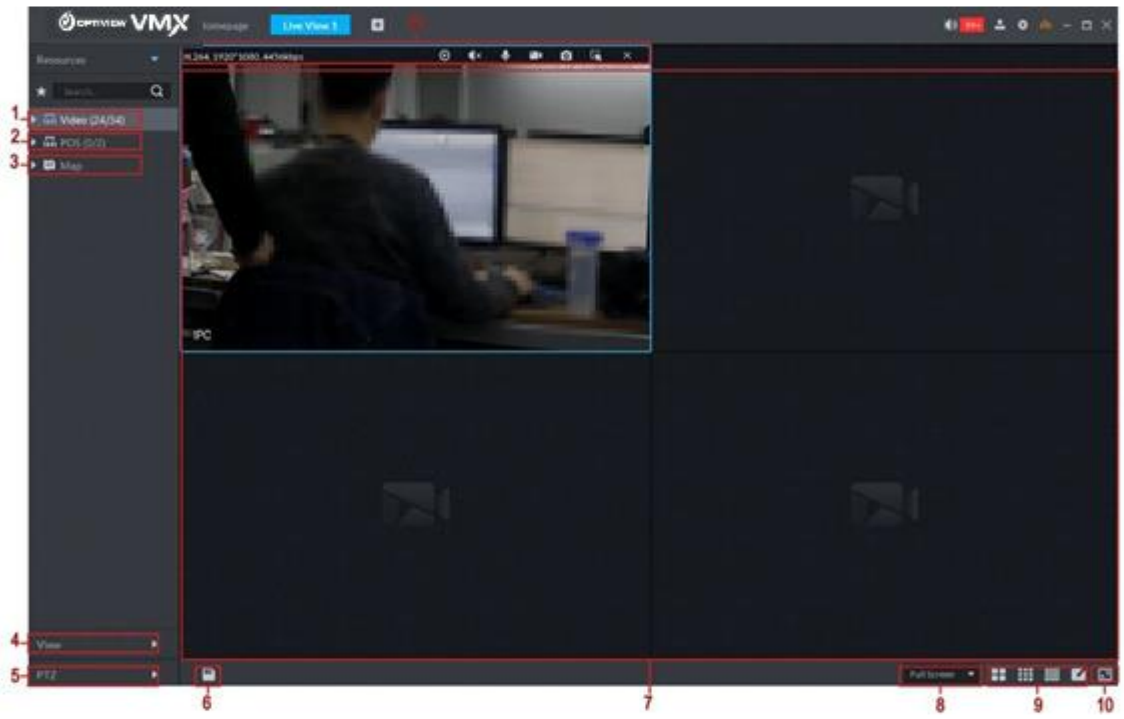


Figure 3-80 Live view

Table 3-13 Live view interface description

No.	Parameter	Description
1	Resources	● Click ★ and enter favorite. ● You can search device or channel in Search... according to device name or channel name. ● Display device list. If you enable **Show Device Node** in **Local Config > Basic Setting**, then the device tree displays device and its channels, or you can disable it and display all the device channels.
2	POS	You can open POS and related video channels from live window.
3	Map	Display added map, Double-click to open map, select device and support live view and cancel alarm.
4	View	Display created view list.
5	PTZ / Electronic Focus	For detailed operation of PTZ, refer to "3.4.4 Setting PTZ." For detailed operation of electronic focus, see "3.4.5 Electronic Focus."
6	Save View	Record live video window split and window play. Save as live view plan for quick call. For detailed operation, see "3.4.5 Electronic Focus."
7	Video Play Window	Display live view image. Move the mouse to the video window which is being displayed; scroll the mouse to zoom in or out video. Right-click and refer to "3.4.2 Enabling Live View."

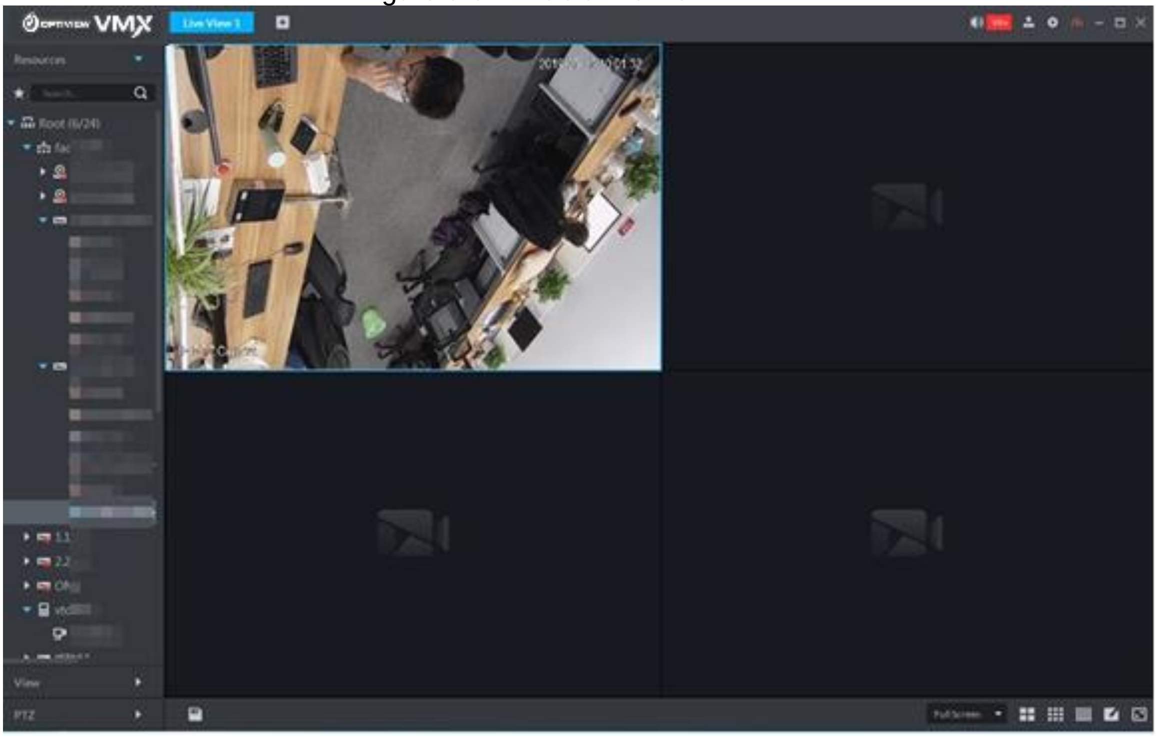
No.	Parameter	Description
8	Display Mode	Select height and width ratio of video window, you can play video by actual ratio or full window.
9	Image Split Mode	Used to set image split mode, support 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 and 64, or click ✎ and customize split mode.
10	Full Screen	Switch video window to **Full Screen** mode. If you want to exit **Full Screen**, you can press Esc button or right-click and select **Exit Full Screen**.
11	Stream and Shortcut	Display encode format, stream and shortcut operation. For detailed operation, see “3.4.2 Enabling Live View.”

3.4.2 Enabling Live View

Select channel or device from device list on the **Live View** interface, Double-click or drag to video window. The system plays real-time video, see Figure 3-81.

- If number of window splits is less than number of device online channels, then you can select online channel by window splits in sequence.
- If number of window splits is more than number of device online channels, then channel video is displayed on window in sequence.
- You need to close tour and then display live view.

Figure 3-81 Enable live view



Related operations of live view are shown as follows:

- Move the mouse to video window, shortcut operation menu is displayed on upper right corner of the window, see Figure 3-82. For detailed description, see Table 3-14.

Figure 3-82 Shortcut menu

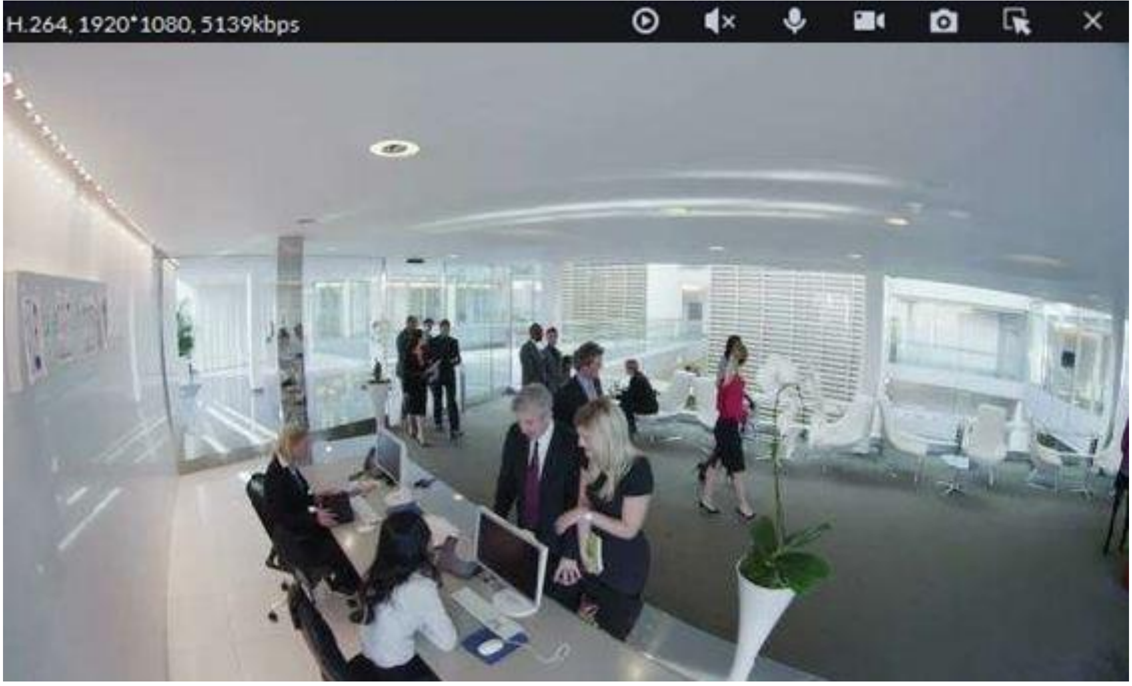


Table 3-14 Shortcut menu description

Icon	Name	Description
⏵	Instant playback	Open/close instant playback. Go to **Local config>General** to set instant playback time. Make sure there is a record on the platform or the device.
🔇	Audio	Open/close audio.
🎤	Audio talk	Open/close bidirectional talk.
📹	Local record	Click it, system begins record local file and you can view the record time at the top left. Click again, system stops record and save the file on the PC.
📷	Snapshot	Click to snapshot once.
⬚	Zoom	Zoom in, and it supports mouse wheel zooming after zooming in the image.
☒	Close	Click to close video.

- Right-click live view window, display menu shown in Figure 3-83. For operation description, see Table 3-15.

  🕮

  Different devices display different menu by right-click, the actual interface shall prevail.

Figure 3-83 Right-click menu

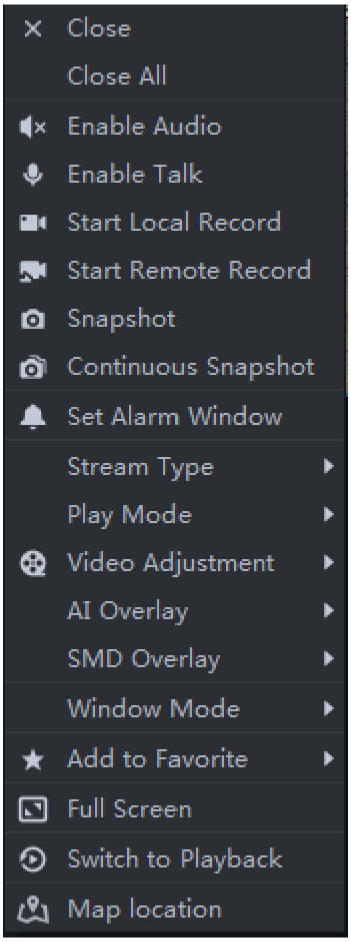

Close
Close All
Enable Audio
Enable Talk
Start Local Record
Start Remote Record
Snapshot
Continuous Snapshot
Set Alarm Window
Stream Type
Play Mode
Video Adjustment
AI Overlay
SMD Overlay
Window Mode
Add to Favorite
Full Screen
Switch to Playback
Map location

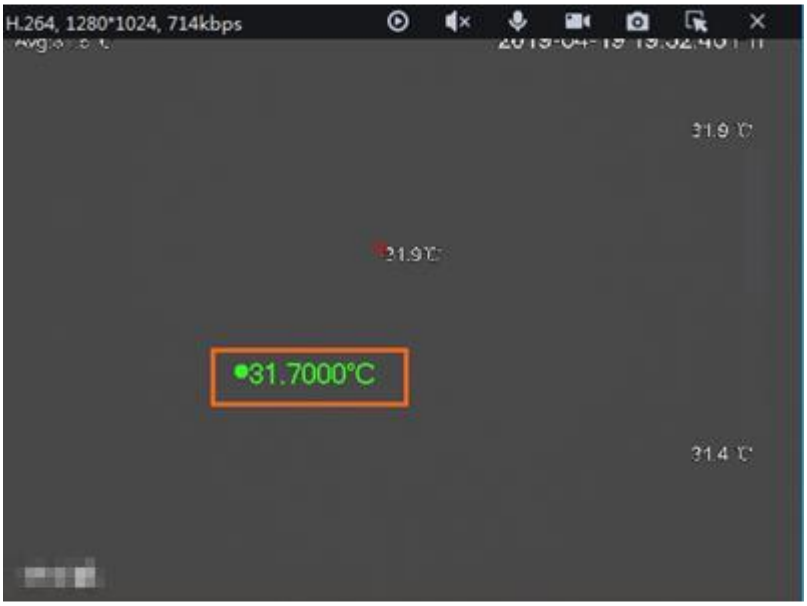
Table 3-15 Right-click menu description

Parameters	Description
Close	Close active video window.
Close All	Close all video windows.
Enable Audio	Same as 🔇, to enable or disable camera audio.
Enable Talk	Same as 🎤, to enable or disable audio talk of corresponding device. Check **Self-adaptive Audio Talk Parameters** from **Local Config > General**; when audio talk is on, it will automatically adapt to various parameters without showing a pop-up box.
Start Local Record	Same as 📹, to record audio/video of the active video window and save them in local PC.
Start remote record	Click to start remote record. The item becomes **Stop** remote record. Click **Stop** remote record, system stops record. If the platform has configured video storage HDD, the record file is saved on the platform server.
Snapshot	Same as 📷, to save image of the active video window as picture (one picture for each snapshot).
Continuous Snapshot	To save image of the active video window as picture (three snapshots each time by default).
Set Alarm Window	Turn on/off alarm output.

Parameters	Description
Stream Type	Switch among **Main** stream, **Sub** stream and **Third** stream. If selecting **Sub** stream or **Third** stream, you need to check enable Sub Stream and enable Third Stream in the Bit Stream dropdown list when adding encoder from the Manager.
Play Mode	Switch between the modes of Real Time Priority, Fluency Priority, Balance Priority and custom defined mode.
Video Adjustment	Perform video adjustment and video enhancement.
AI Overlay	The client does not show overlay lines over live video bu default. When needed, you can click **AI Overlay** and enable **Rule Overlay** and **Target Box Overlay**, and then the live video shows overlay lines if the AI detection rules are enabled on the device. This configuration is only effective to the current selected channel.
SMD Overlay	Enable **SMD Overlay** to show target frame over live video. When SMD is enabled on the device, you can enable **SMD Overlay** for the device channel, and then the live video will display dynamic target frames. This configuration is only effective to the current selected channel.
Installation mode	For fisheye camera only. The installation mode has three types:ceiling mount, wall mount and ground mount. Select corresponding installation mode according to the actual situation, the real-time video can automatically dewarp according to the installation mode.
Fisheye view mode	For fisheye camera only. When changing the video stream, the fisheye view mode keeps the configuration before the stream is changed. It refers to current video display mode (system supports original video mode by default.). System supports following display modes according to different installation mode. ● Ceiling mount: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. ● Wall mount: 1P, 1P+3, 1P+4, 1P+8. ● Ground mount: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8.
Split mode	Support standard mode, 1+3 mode, 1+5 mode.
Alarm output control	It control alarm input/output.
Add To Favorites	You can add the active channel or all channels into Favorite.
Full Screen	Switch the video window to full screen mode. To exit full screen, Double-click video window, or right-click to select exit full screen.
Switch to Playback	You can switch between live view interface and playback interface quickly, without going back to homepage first.
Map location	After enabling map location, a map that centers on the device will be displayed.

- If you view thermal channel, move the mouse and lay it any position of the image, and then the platform displays real-time temperature of the position, see Figure 3-84.

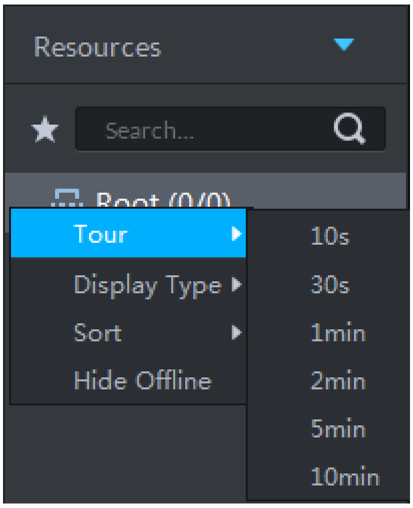
Figure 3-84 Spot temperature measurement


H.264, 1280*1024, 714kbps
31.9 ℃
21.9℃
31.7000℃
31.4 ℃

3.4.3 Enabling Tour View

Right-click device or organization in the device list on **Live View** interface, select Tour and set duration. See Figure 3-85. The system plays video image of all online channels in loop, click or right-click window to stop. Select **Stop Tour** if you want to.

Figure 3-85 Tour interface

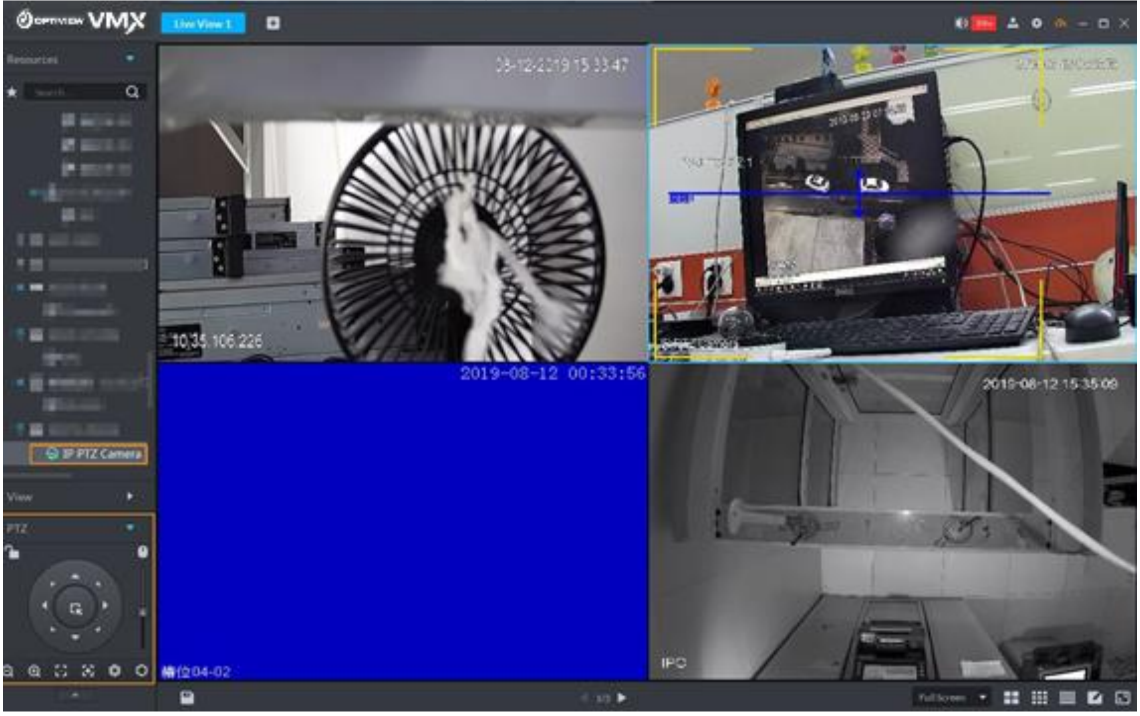

Resources
Search...
Root (0/0)
Tour
Display Type
Sort
Hide Offline
10s
30s
1min
2min
5min
10min

3.4.4 Setting PTZ

3.4.4.1 PTZ Operation Interface

Step 1 On **Live View** interface, open video from the PTZ camera, you can see PTZ operation interface on the left. See Figure 3-86.

Figure 3-86 Live view


VMX
Live View 1
Resources
IP PTZ Camera
View
PTZ
10.35.106.226
2019-08-12 00:33:56
2019-08-12 15:35:09
IPC
Full Screen

Step 2 Click at the bottom of the interface to operate. See Figure 3-87.

Figure 3-87 PTZ

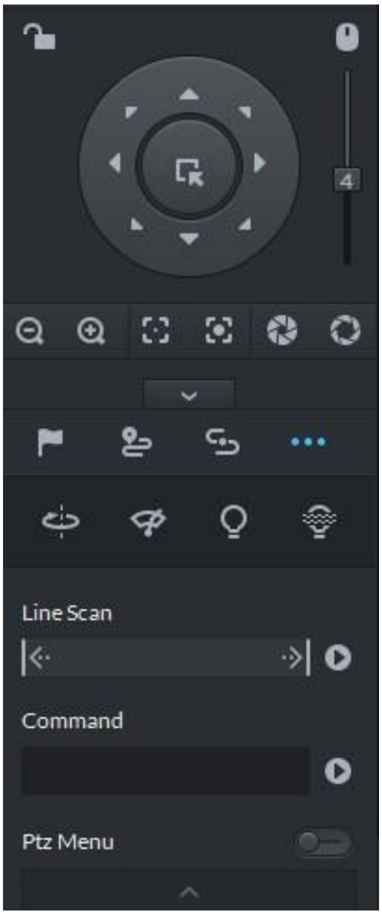

4
Line Scan
Command
Ptz Menu

Table 3-16 PTZ operation description

Parameters	Description
🔓	Click 🔓 to lock the current PTZ. Locked status shows as 🔒. Control over PTZ varies depending on user level. ● When user of low level locks PTZ, user of high level can unlock and enable the PTZ by clicking 🔒. ● When user of high level locks PTZ, user of low level can't unlock the PTZ, unless PTZ automatically unlock itself. ● Users of the same level can unlock PTZ locked by each other. 📖 Default time for automatically unlocking PTZ is 30s.
🖱	● Control speed dome with mouse.
Direction Key	● Set rotation direction of PTZ, eight directions are available in total: up, down, left, right, upper left, upper right, lower left and lower right.
⬚	● 3D Location and Partially Zoom In (for Speed Dome PTZ), to zoom in or zoom out the selected area. 📖 This function can be controlled with mouse only.
4	From top to the bottom to adjust rotation speed of PTZ, to set the step size chosen from 1 to 8.
⊖ ⊕	● Zoom, to control zoom operation of speed dome.
⛶ ⛶	● Focus, to adjust focus.
◎ ◎	● Aperture, to adjust brightness.
⚑, ⇆, ↻, •••	Set preset, tour, pattern, scan, rotation, wiper, light, IR light function, etc. Refer to 3.4.4.2 PTZ Settings for more information.

3.4.4.2 PTZ Settings

3.4.4.2.1 Configuring Preset

By adding preset, you can rotate the camera to the specified position.

Step 1 Click direction key of the PTZ to rotate the camera to the needed place.

Step 2 Click ⚑.

Step 3 Place mouse over 1 and click ✎.

Step 4 Input preset point SN, and click ☑.

Adding preset point completed.

To the right of

, click , then camera will be rotated to the related position.

3.4.4.2.2 Configuring Tour

Set Tour to enable camera to go back and forth among different presets.

To enable tour, at least 2 preset points are required.

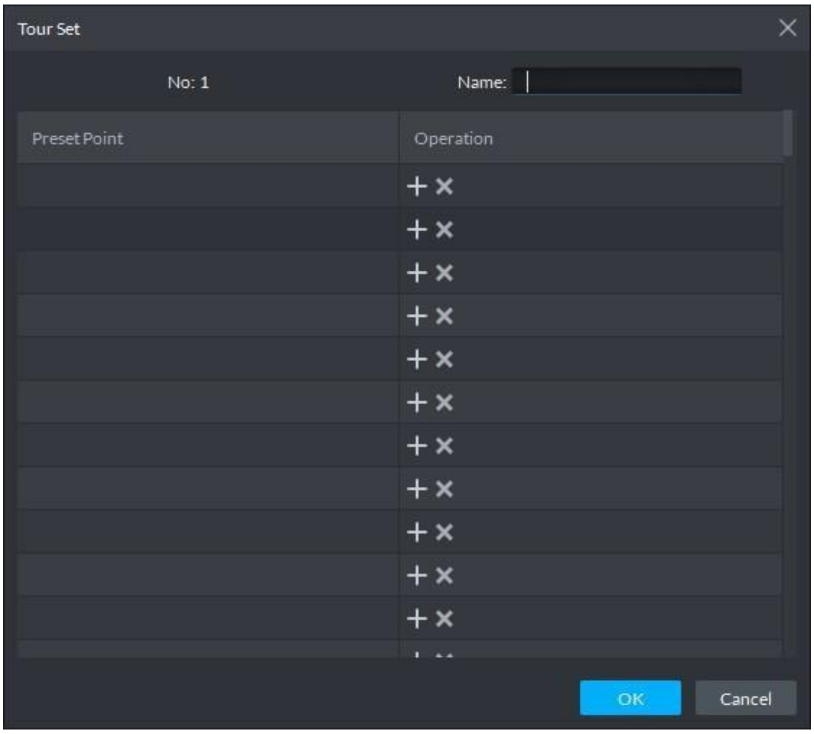
Step 1 Click .

Step 2 Place mouse over 1 and click .
New tour dialogue box pops up.

Step 3 Input name, and click Operation bar .

Choose preset points from the dropdown list on the left. See Figure 3-88.

Figure 3-88 Add preset



Step 4 Click **OK**.
System prompts Tour Saved Successfully.

Step 5 Click **OK**.

To start tour, place mouse over 1 and click , then camera goes back and forth among the presets of Tour 1.

3.4.4.2.3 Configuring Pattern

Pattern is equivalent to a record process.

Step 1 Click .

Step 2 Place mouse over 1 and click , then operate 8 buttons of PTZ to set pattern.

Step 3 Click to complete pattern setup.

Step 4 Click ▶, and the camera will rotate following the pattern settings.

3.4.4.2.4 Configuring Scan

Step 1 Click •••.

Step 2 Click PTZ button, and rotate PTZ toward left to a position, then click |←··· to set left boundary.

Step 3 Continue to rotate PTZ toward right to a position, and click ···→| to set right boundary.

Step 4 Click ▶ to start scan, then PTZ will rotate back and forth within the two boundaries.

3.4.4.2.5 Enable/Disable Pan

Click •••, and then click , PTZ rotate at 360°by specified speed. Click to stop camera rotation.

3.4.4.2.6 Enable/Disable wiper

It is to use RS485 command to control the connected peripheral device wiper on/off. Make sure the connected peripheral device supports wiper function.

Click •••, and then click , it is to enable wiper. After enabling wiper, click to disable.

3.4.4.2.7 Enable/Disable light

It is to use RS485 command to control the connected peripheral device light on/off. Make sure the connected peripheral device supports light function.

Click •••, and then click , it is to enable light. After enabling light, click to disable.

3.4.4.2.8 Enable/Disable IR light

Click •••, and then click , it is to enable IR light. After enabling IR light, click to disable.

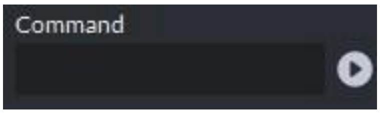
3.4.4.2.9 Configuring custom commands

Different devices support different customized commands. Contact the manufacture for detailed information.

Step 1 Click ⋯.

Step 2 Input command on the customized command interface. See Figure 3-89.

Figure 3-89 Command



Step 3 Click ▶ to display the function of the customized command.

3.4.4.2.10 PTZ Menu

Step 1 Click ⋯.

The PTZ menu is shown as in Figure 3-90.

Figure 3-90 Menu

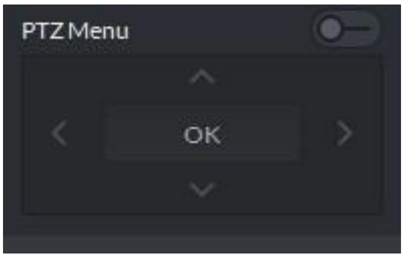


Table 3-17 PTZ menu parameter description

Parameters	Description
∧/∨	Up/down button. Move the cursor to the corresponding item.
</>	Left/right. Move the cursor to set parameters.
○─	Click ○─ to enable PTZ menu function. System displays main menu on the monitor window.
─●	Click ─● to close PTZ menu function.
OK	It is the confirm button. It has the following functions. ● If the main menu has the sub-menu, click **OK** to enter the sub-menu. ● Move the cursor to Back and then click **OK** to go to go back to the previous menu. ● Move the cursor to Exit and then click **OK** to exit the menu.

Step 2 Click **OK**.

The monitor window displays main menu. See Figure 3-91.

Figure 3-91 Display main menu interface

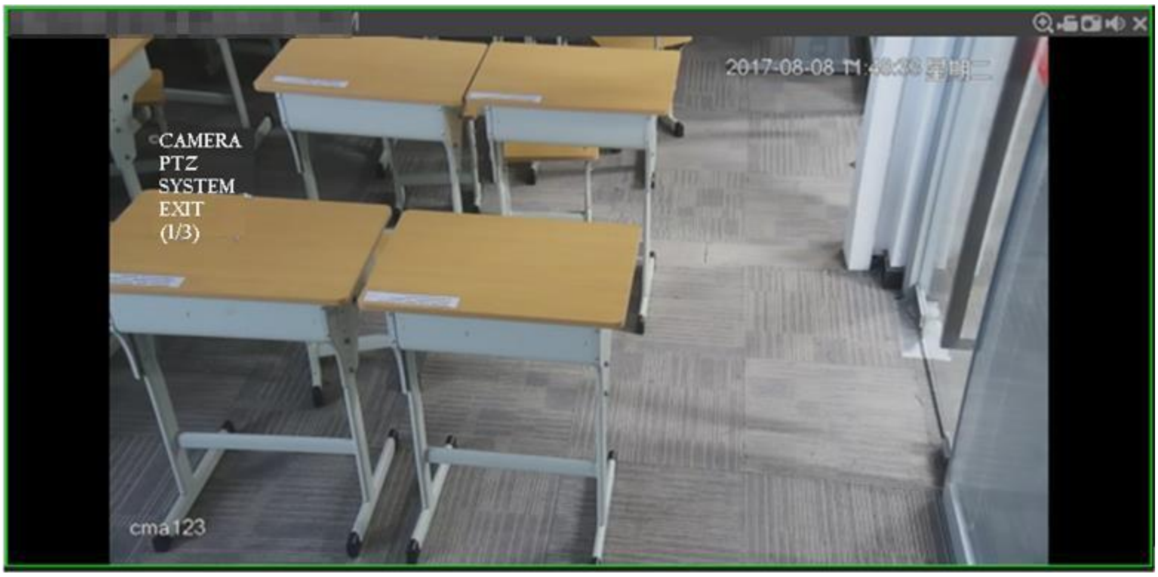


Table 3-18 Main menu parameter description

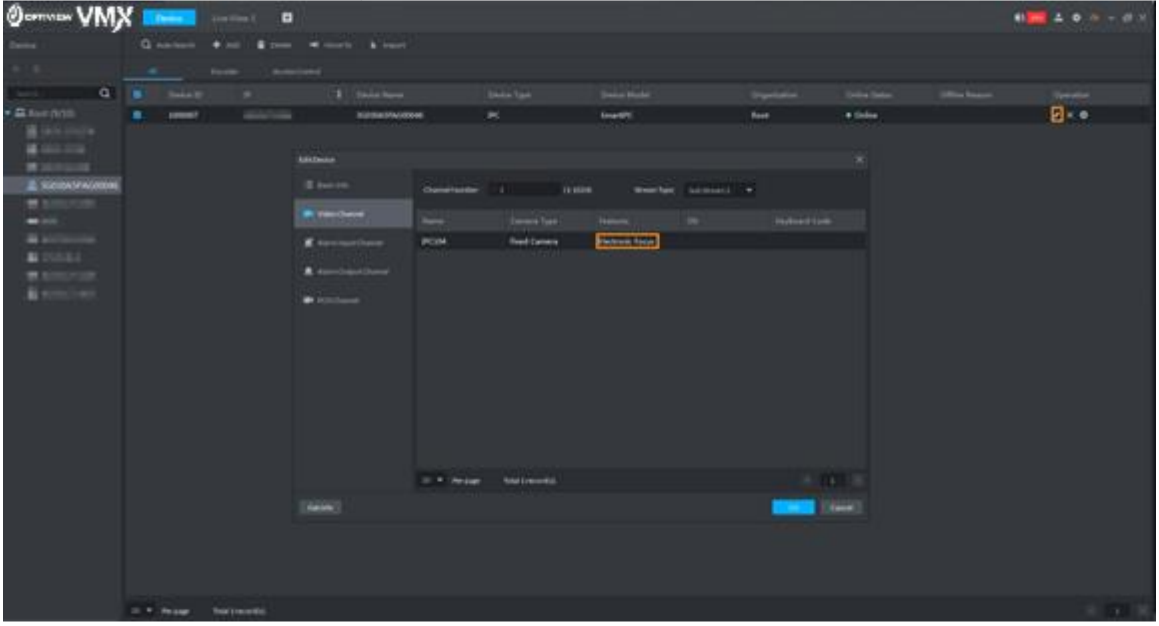
Parameters	Description
Camera	Move the cursor to Camera and then click **OK** to enter camera settings sub-menu interface. Set camera parameters.It includes picture, exposure, backlight, day/night mode, focus and zoom, defog, default, etc.
PTZ	Move the cursor to PTZ and then click **OK** to enter PTZ sub-menu interface. Set PTZ functions. It includes preset, tour, scan, pattern, rotation, PTZ restart, etc.
System	Move the cursor to System and then click **OK** to enter system sub-menu interface. Set PTZ simulator, restore camera default settings, video camera software version and PTZ version.
Return	Move the cursor to the **Return** and then click **OK**, and go back to the previous menu.
Exit	Move the cursor to the **Exit** and then click **OK**, and exit PTZ menu.

3.4.5 Electronic Focus

If a channel supports electronic focus, you can enable electronic focus for it on the platform to adjust video definition and size.

- If a channel does not support electronic focus, or if you did not modify the **Features** of the channel to **Electronic Focus**, this function will be unavailable for this channel on the platform.
- To modify channel **Features** to **Electronic Focus**, see Figure 3-92.

Figure 3-92 Set channel features



The **Electronic Focus** operation panel is displayed on the **Live View** interface if the selected channel supports this function. See Figure 3-93. For details, see Table 3-19.

The interface might vary according to the lens types of cameras. Lens types include embedded zoom lens and external CS electronic lens. The following figure is for reference only and the actual interface shall prevail.

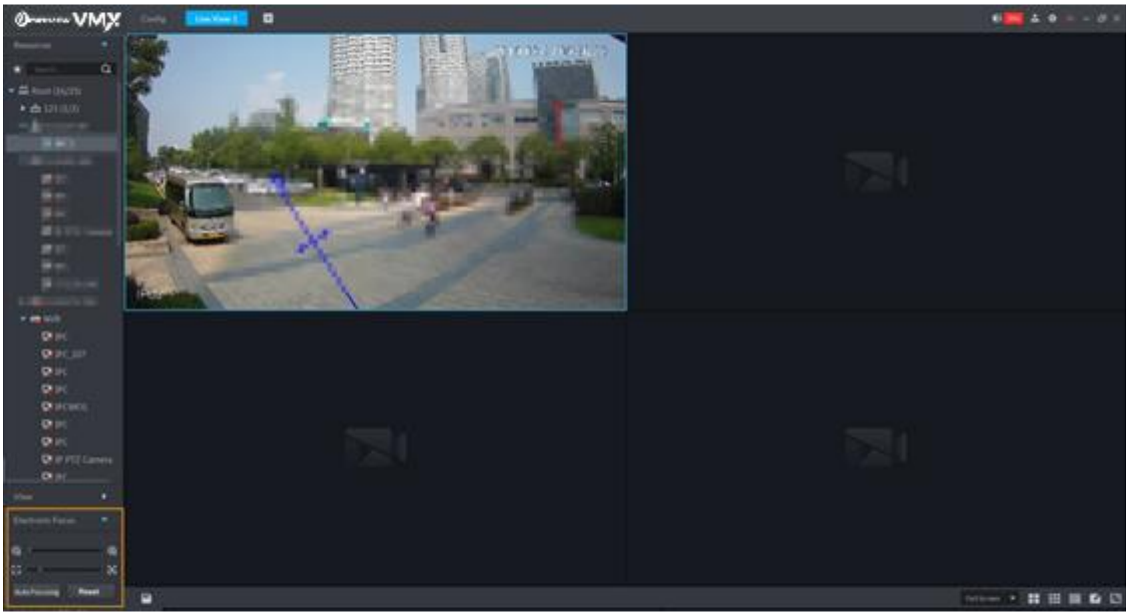


Figure 3-93 Live View

Table 3-19 Parameters description

Parameters	Description
Zoom +/- (for embedded zoom lens)	Zoom in/out. Click or click and hold or , or drag the slider to the left or right to zoom in/out.
Focus +/-	Adjust camera focus to achieve the best video definition. Click or click and hold or , or drag the slider to the left or right to adjust focus.
Auto Focusing (for embedded zoom lens)	Adjust image definition automatically. Other focusing operations are unavailable during auto focusing.
ABF (auto back focusing, for external CS electronic lens)	
Reset	When image definition is imperfect, or after many times of zooming or focusing operations, you can click **Reset** to reset the lens, so as to eliminate lens deviation.

3.4.6 View

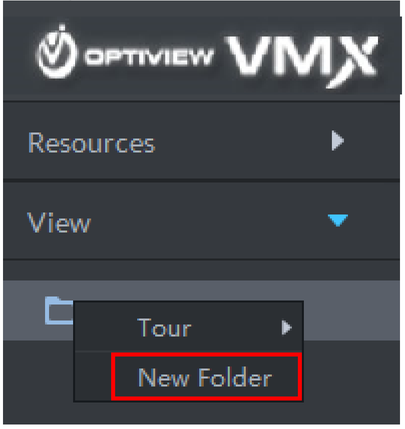
3.4.6.1 Creating View

Created views are categorized into different groups, convenient for management and call. Group includes three levels, first-level root node, second-level grouping and third-level view.

Step 1 Create group.

1) Click **View** tab on the **Live View** interface.
2) Right-click **View**, select **New Folder**, and see Figure 3-94.
   The system displays **New Folder** interface.

Figure 3-94 New folder


OPTIVIEW VMX
Resources
View
Tour
New Folder

3) Enter folder name, click **OK**.

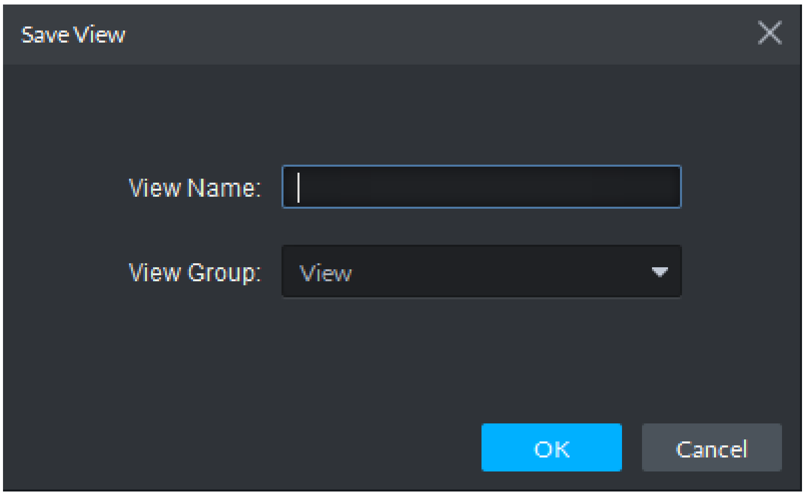
All new groups are displayed under view.

Step 2 Create view.

1) On **Live View** interface, click 💾 according to your needs.

The system displays **Save View** interface, see Figure 3-95.

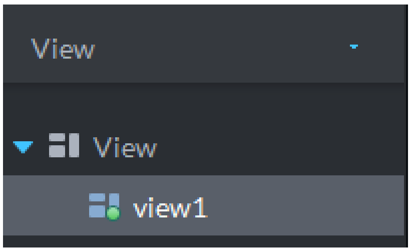
Figure 3-95 Save view


Save View
View Name:
View Group:
View
OK
Cancel

2) Enter **View Name**, select **View Group** and click **OK**.

New view is created under view group, see Figure 3-96.

Figure 3-96 Generate view


View
View
view1

3.4.6.2 View

- Live view

  Select view from the list on **Live View** interface, Double-click or drag to video window, the system starts to play live video.

- Tour
  On **Live View** interface, right-click view group or root node, select **Tour** and tour period, see
  Figure 3-97. The system tours according to view group or root node; see Figure 3-98. Click to stop tour.

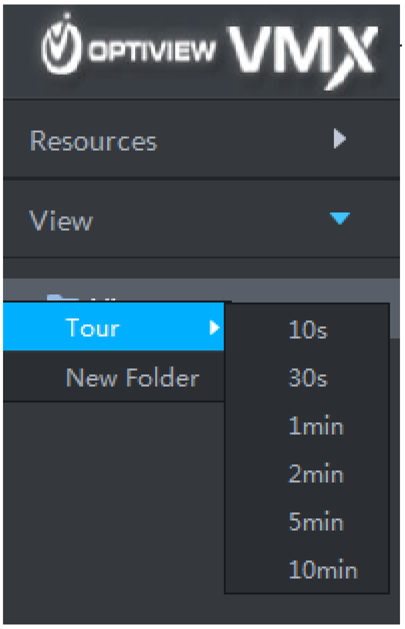
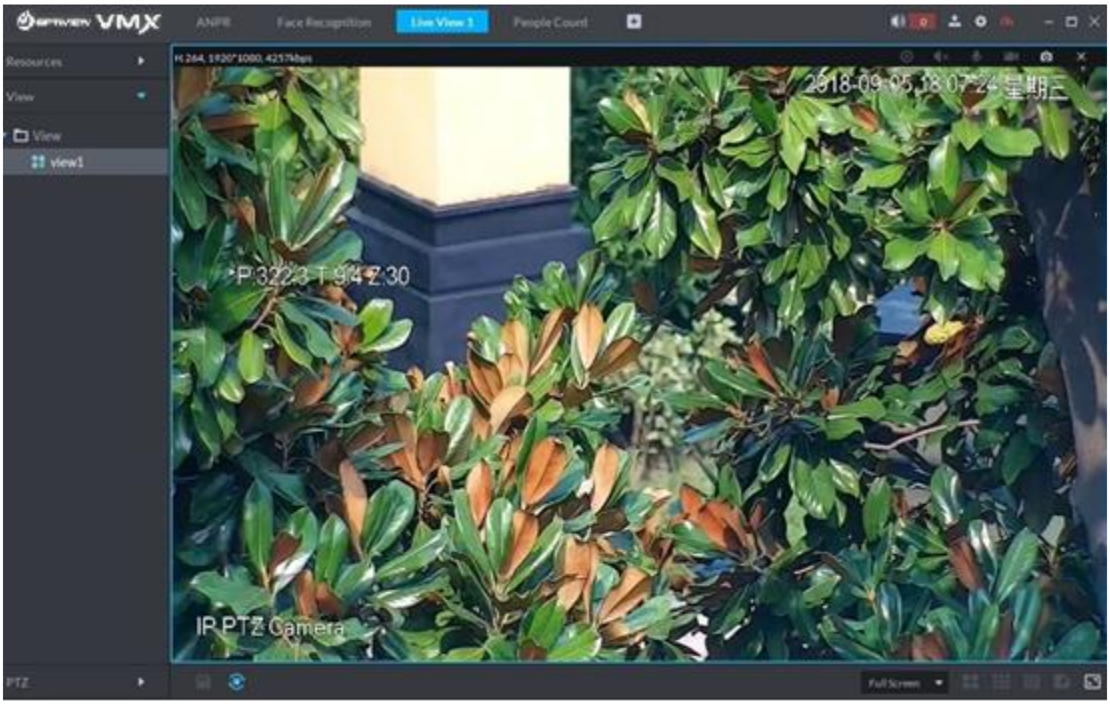

OPTIVIEW VMX
Resources
View
Tour
New Folder
10s
30s
1min
2min
5min
10min

Figure 3-97 Entering video tour interface

Figure 3-98 View tour


OPTIVIEW VMX
ANPR
Face Recognition
Live View 1
People Count
Resources
View
View
view1
PTZ
2018-09-05 18:07:24 星期三
P:322.3 T:94 Z:30
IP PTZ Camera
Full Screen

3.4.7 Favorites

Add frequently used channels to favorites, and realize quick search and call.

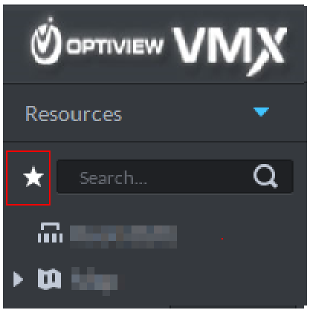
3.4.7.1 Creating Favorites

Step 1 Create favorites.

1) On **Live View** interface, click ★, see Figure 3-99.

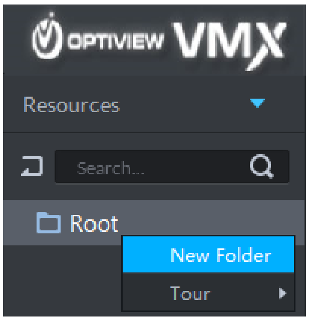
The system displays favorites list.

Figure 3-99 Enter favorites list


OPTIVIEW VMX
Resources
Search...

2) Right-click root node or created favorites, select **New Folder**, see Figure 3-100. The system displays **Create Folder** interface.

Figure 3-100 Favorites list


OPTIVIEW VMX
Resources
Search...
Root
New Folder
Tour

3) Enter folder name, click **OK**. Selected root node or favorites generates lower-level favorites.

4) Click ⮐.

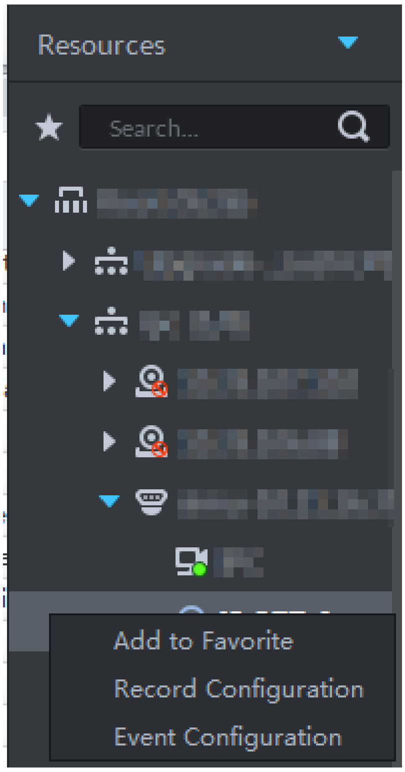
The system returns to device list.

Favorite channel.

- In the device list on **Live View** interface, right-click channel, select **Add to Favorites**, and add the channel to favorite according to system prompt. See Figure 3-101.

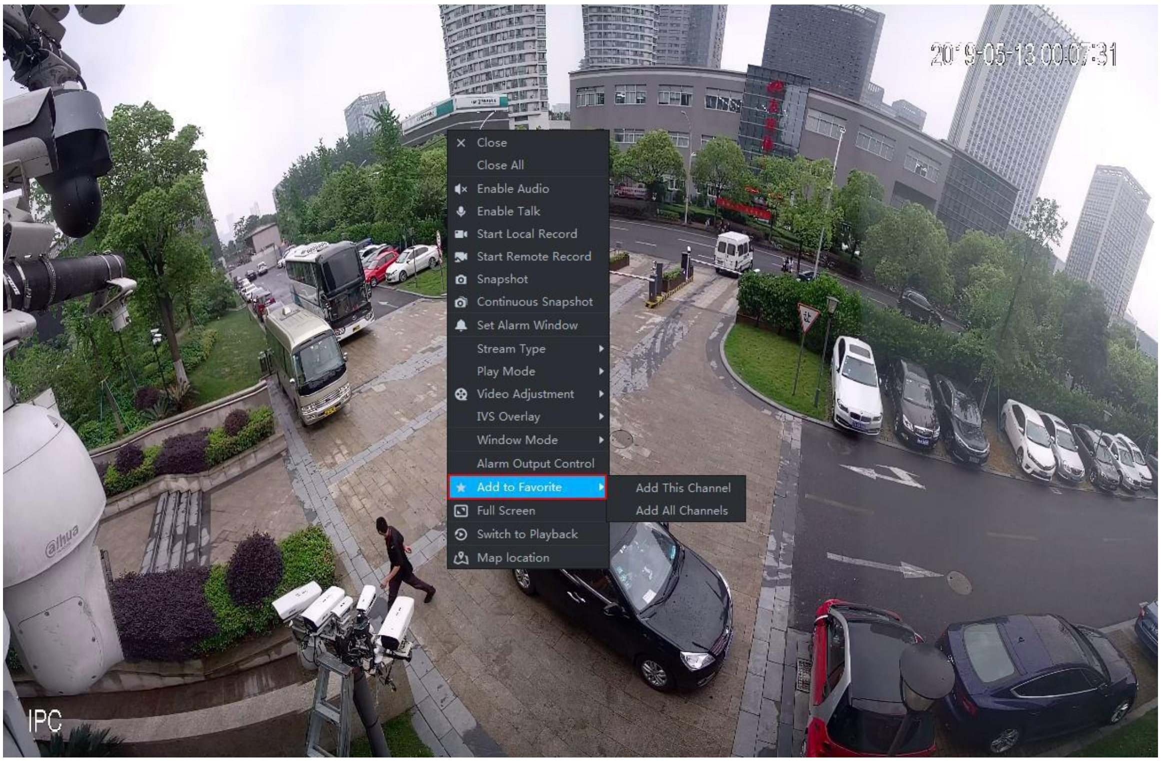
Step 2

Figure 3-101 Favorite channel (1)


Resources
Search...
IPC
Add to Favorite
Record Configuration
Event Configuration

- On **Live View** interface, right-click the window with live view, and select **Add to favorite**, add it to favorite according to system prompt, see Figure 3-102.

Figure 3-102 Favorite channel (2)


Close
Close All
Enable Audio
Enable Talk
Start Local Record
Start Remote Record
Snapshot
Continuous Snapshot
Set Alarm Window
Stream Type
Play Mode
Video Adjustment
IVS Overlay
Window Mode
Alarm Output Control
Add to Favorite
Full Screen
Switch to Playback
Map location
Add This Channel
Add All Channels
IPC

3.4.7.2 Viewing Favorites

- Live view

On **Live View** interface, click , open favorite list, select favorite or channel,

Double-click or drag to video window and the system starts to play live video.

- Tour

On **Live View** interface, click , open favorite list, right-click root node or favorite, select **Tour** and tour period. The system plays root node or all channels under favorite in loop. Click to stop tour.

3.4.8 Region of Interest (RoI)

A window can be divided into 4 or 6 regions during live view, one area is used to play live video and other regions are used to zoom in regional image.

On **Live View** interface, right-click the window under live view, select **Split Mode**, and see Figure 3-103. The system displays split image. For example, select 1+3 mode. See Figure 3-104.

Figure 3-103 Split mode

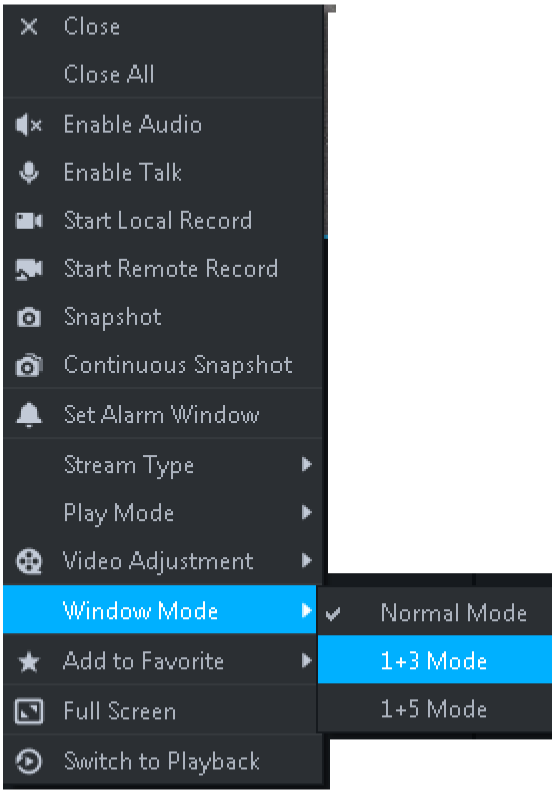
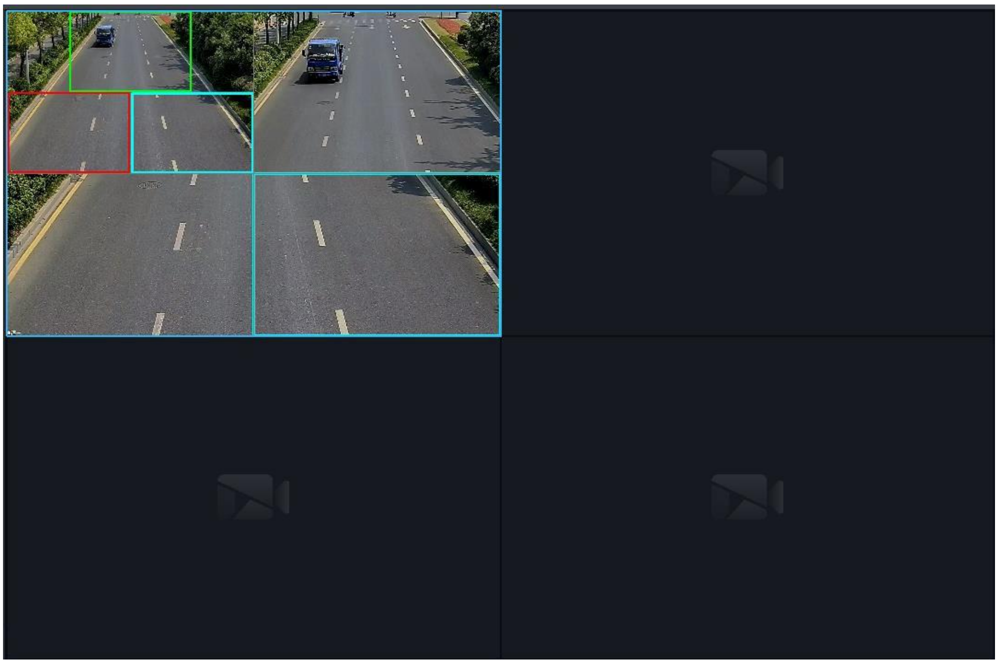

Close
Close All
Enable Audio
Enable Talk
Start Local Record
Start Remote Record
Snapshot
Continuous Snapshot
Set Alarm Window
Stream Type
Play Mode
Video Adjustment
Window Mode
Add to Favorite
Full Screen
Switch to Playback
Normal Mode
1+3 Mode
1+5 Mode

Figure 3-104 1+3 mode



3.5 Device Configuration

Configure the camera properties, video stream, snapshot, video overlay, and audio parameters for the device channel on the platform. Only support configuring the channels added by IP in Private protocols.

Device configuration differs by the capacities of the devices depending on model number.

3.5.1 Configuring Camera Properties

Support configuring the property files in the modes of **Daytime**, **Night**, and **Regular**. The system switches between different modes based on the preset time to ensure image quality collected by the camera.

3.5.1.1 Configuring Property Files

Step 1 On the **Live View** interface, right-click the video device and select **Device Config**. See Figure 3-105.

The **Device Config** interface is displayed. See Figure 3-106.

- Only PTZ cameras and speed domes support PTZ control function.
- Click **More configuration** to open the web configuration interface for the device.

Figure 3-105 Entering device configuration

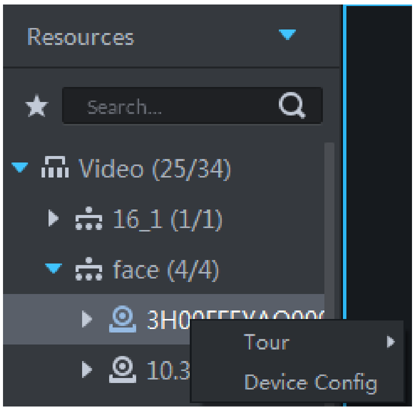
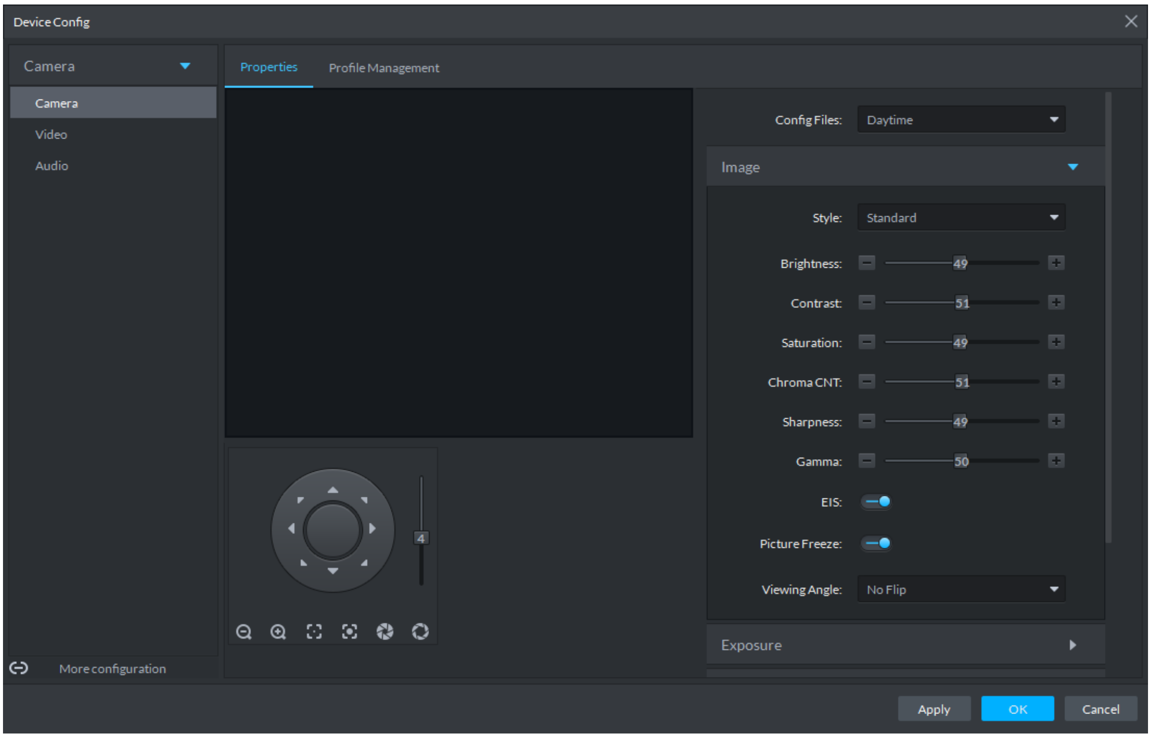

Resources
Search...
Video (25/34)
16_1 (1/1)
face (4/4)
3H00FFFYAQ00
10.3
Tour
Device Config

Figure 3-106 Device configuration


Device Config
Camera
Camera
Video
Audio
Properties
Profile Management
Image
Exposure
More configuration
Apply
OK
Cancel

Config Files: Daytime

Style: Standard

Brightness: 49

Contrast: 51

Saturation: 49

Chroma CNT: 51

Sharpness: 49

Gamma: 50

EIS:

Picture Freeze:

Viewing Angle: No Flip

Step 2 Select **Camera > Camera > Properties > Image**.

The **Properties** interface is displayed. See Figure 3-106.

Step 3 Select **Profile Management**.

Step 4 Click **Image**. See Figure 3-106. For details of the parameters, see Table 3-20.

Table 3-20 Image parameter description

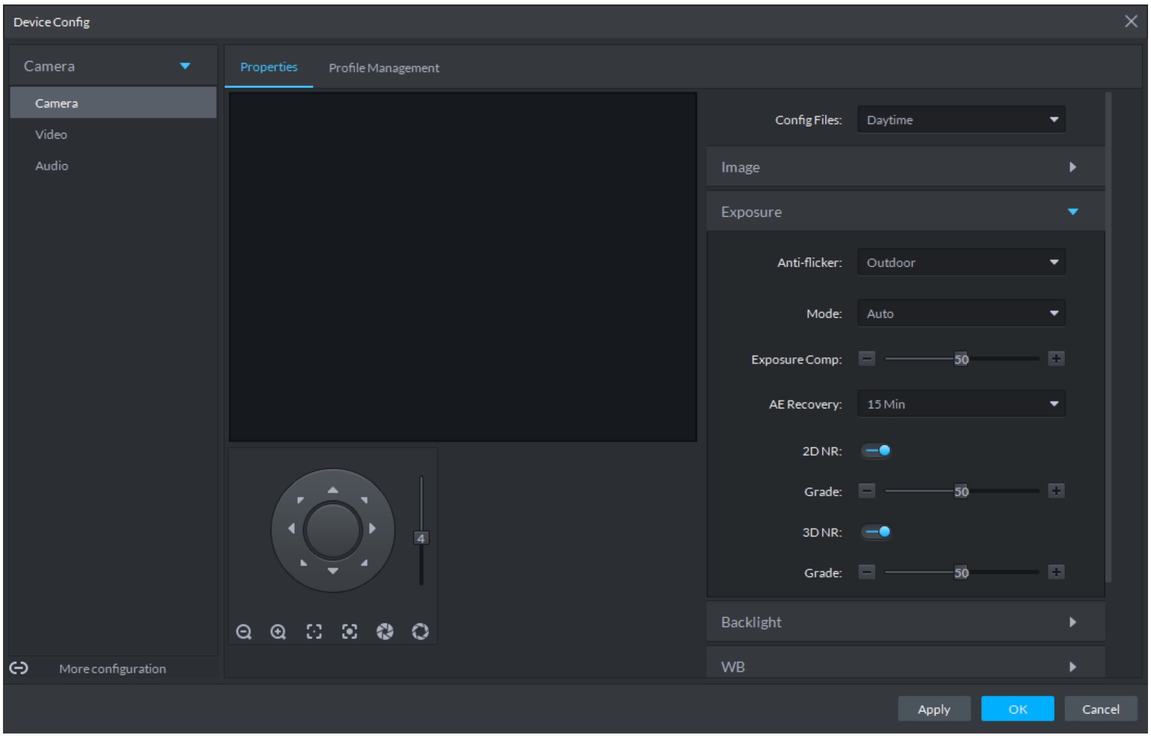
Parameter	Description
Style	You can set the image style to be **Standard**, **Gentle**, or **Flamboyant**.
Brightness	You can adjust the overall image brightness through linear tuning. The higher the value, the brighter the image and vice versa. If this value is set too high, images tend to lo**OK** blurred.
Contrast	Adjusts the contrast of the images. The higher the value, the bigger the contrast between the bright and dark portions of an image. If the contrast value is set too high, the dark portions of an image might become too dark, and the bright portions might be over-exposed. If the contrast value is set too low, images tend to lo**OK** blurred.

Parameter	Description
Saturation	Adjusts color shade. The higher the value, the deeper the color and vice versa. The saturation value does not affect the overall brightness of the images.
Sharpness	Adjusts the edge sharpness of images. The higher the value, the sharper the image edges. Setting this value too high might easily result in noises in images.
Gamma	Changes image brightness by non-linear tuning to expand the dynamic display range of images. The higher the value, the brighter the image and vice versa.

Step 5 Click **Exposure** to set up relevant parameters. See Figure 3-107. For details of the parameters, see Table 3-21.

If the device that supports real wide dynamic (WDR) has enabled WDR, long exposure is not available.

Figure 3-107 Exposure



Config Files: Daytime

Anti-flicker: Outdoor

Mode: Auto

Exposure Comp: 50

AE Recovery: 15 Min

2D NR:

Grade: 50

3D NR:

Grade: 50

Table 3-21 Exposure parameter description

Parameter	Description
Anti-flicker	You can select from these three modes: **50Hz**, **60Hz**, or **Outdoor**. ● 50Hz: With the 50Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not generate horizontal stripes. ● 60Hz: With the 60Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not yield horizontal stripes. ● Outdoor: In an outdoor scenario, you can switch the exposure modes to achieve your target effect.

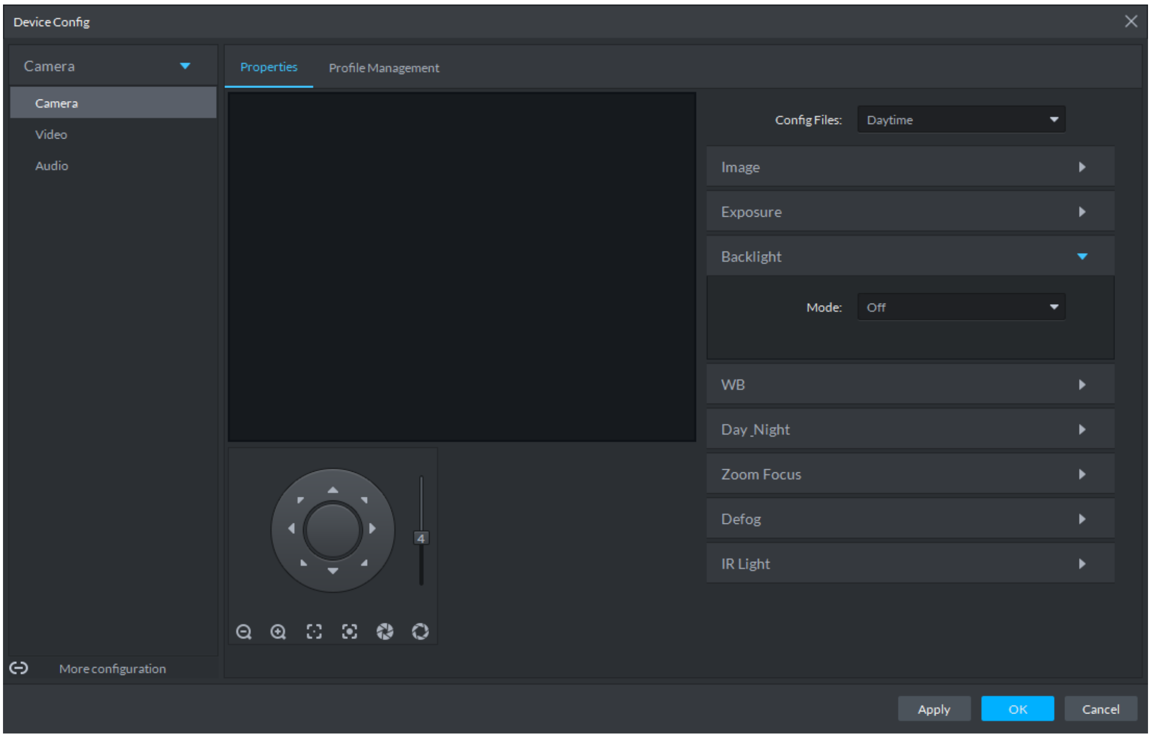
Parameter	Description
Mode	The following options are available for the different exposure modes of the camera: 📖 ● If the **Anti-flicker** is set to **Outdoor**, you can set the **Mode** to **Gain Priority** or **Shutter Priority**. ● Different devices have different exposure modes. The actual interfaces shall prevail. ● Auto: Auto tuning of the image brightness based on the actual environment. ● Gain Priority: Within the normal exposure range, the device adjusts itself automatically first in the preset range of gains according to the brightness of the scenes. If the image has not achieved the target brightness when the gains hit the upper limit or lower limit, the device adjusts the shutter automatically to achieve the best brightness. The Gain Priority mode also allows for adjusting the gains by setting up a gain range. ● Shutter Priority: Within the normal exposure range, the device adjusts itself automatically first in the preset range of shutter values as per the brightness of the scenes. If the image has not achieved the target brightness when the shutter value hits the upper limit or lower limit, the device adjusts the gains automatically to achieve the best brightness. ● Aperture Priority: The aperture is fixed at a preset value before the device adjusts the shutter value automatically. If the image has not achieved the target brightness when the shutter value hits the upper limit or lower limit, the device adjusts the gains automatically to achieve the best brightness. ● Manual: You can set up the gains and shutter values manually to adjust image brightness.
3D NR	Reduces the noises of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video.
Grade	When 3D NR is On, you can set up this parameter. The higher the grade, the better the noise reduction effect is.

Step 6 Click **Backlight** to set up relevant parameters. See Figure 3-108. For details of the parameters, see Table 3-22.

The Backlight mode offers **Backlight Correction**, **Wide Dynamic**, and **Glare Inhibition** features.

- Turning on **Backlight Correction** avoids silhouettes of relatively dark portions in pictures taken in a backlight environment.
- Turning on **Wide Dynamic** inhibits too bright portions and makes too dark portions brighter, presenting a clear picture overall.
- Turning on **Glare Inhibition** partially weakens strong light. This feature is useful in a toll gate, and the exit and entrance of a parking lot. Under extreme lighting conditions such as deep darkness, this feature can help capture the details of the faces and license plates.

Figure 3-108 Backlight


Device Config
Camera
Camera
Video
Audio
Properties
Profile Management
Image
Exposure
Backlight
WB
Day Night
Zoom Focus
Defog
IR Light
4
More configuration
Apply
OK
Cancel

Config Files: Daytime

Mode: Off

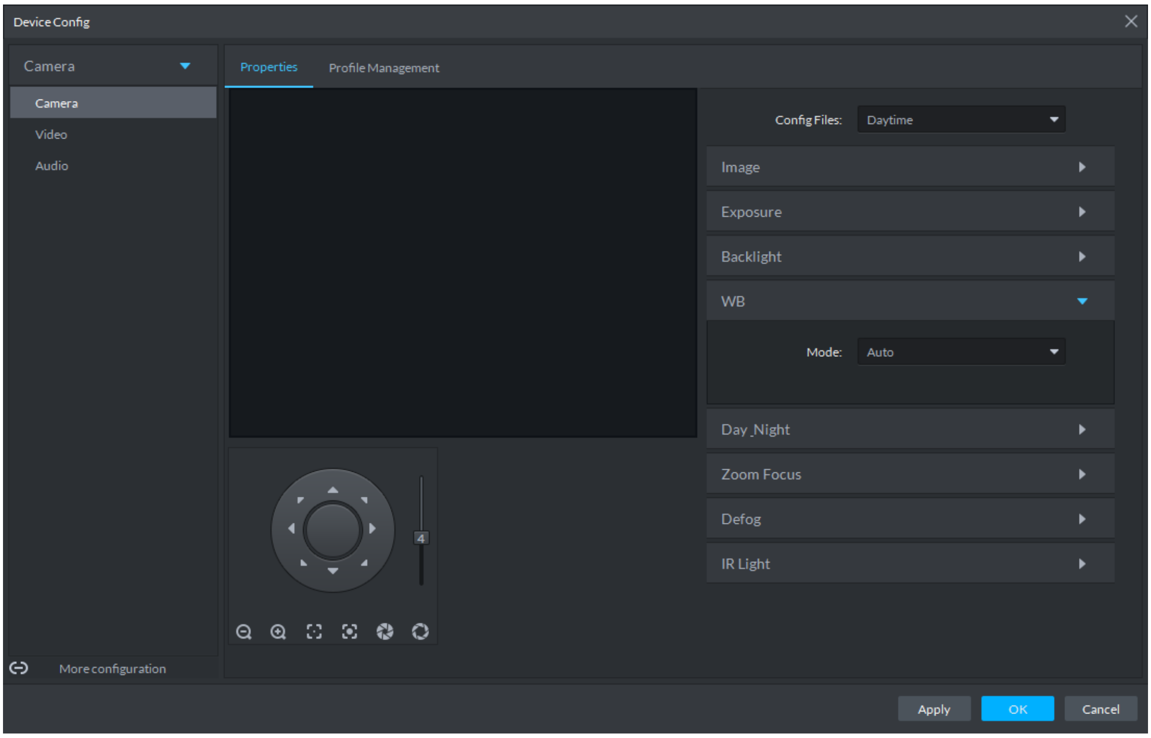
Table 3-22 Backlight mode description

Backlight mode	**Description**
SSA	The system adjusts image brightness automatically based on the environmental lighting conditions to show image details clearly.
Backlight Correction	You can select Default mode or Custom mode. ● When selecting the **Default** mode, the system adjusts exposure automatically to adapt to the environment and make the images taken in the darkest regions clear. ● When selecting the **Custom** mode and setting up a custom region, the system exposes the selected custom region to give the images taken in this region proper brightness.
Wide Dynamic	To adapt to the environmental lighting conditions, the system reduces the brightness in bright regions and increases the brightness in dark regions. This ensures clear display of objects in both bright and dark regions. 📖 The camera might lose seconds of video recordings when switching to **Wide Dynamic** mode.
Glare Inhibition	The system inhibits the brightness in bright regions and reduces the size of the halo, to make the entire image less bright.

Step 7 Click **WB** to set up relevant parameters. See Figure 3-109. For details of the parameters, see Table 3-23.

The WB feature makes the colors of the images more accurate. In WB mode, white objects in the images appear white in various lighting conditions.

Figure 3-109 WB


Device Config
Camera
Camera
Video
Audio
More configuration
Properties
Profile Management
Image
Exposure
Backlight
WB
Day Night
Zoom Focus
Defog
IR Light
4
Apply
OK
Cancel

Config Files: Daytime

Mode: Auto

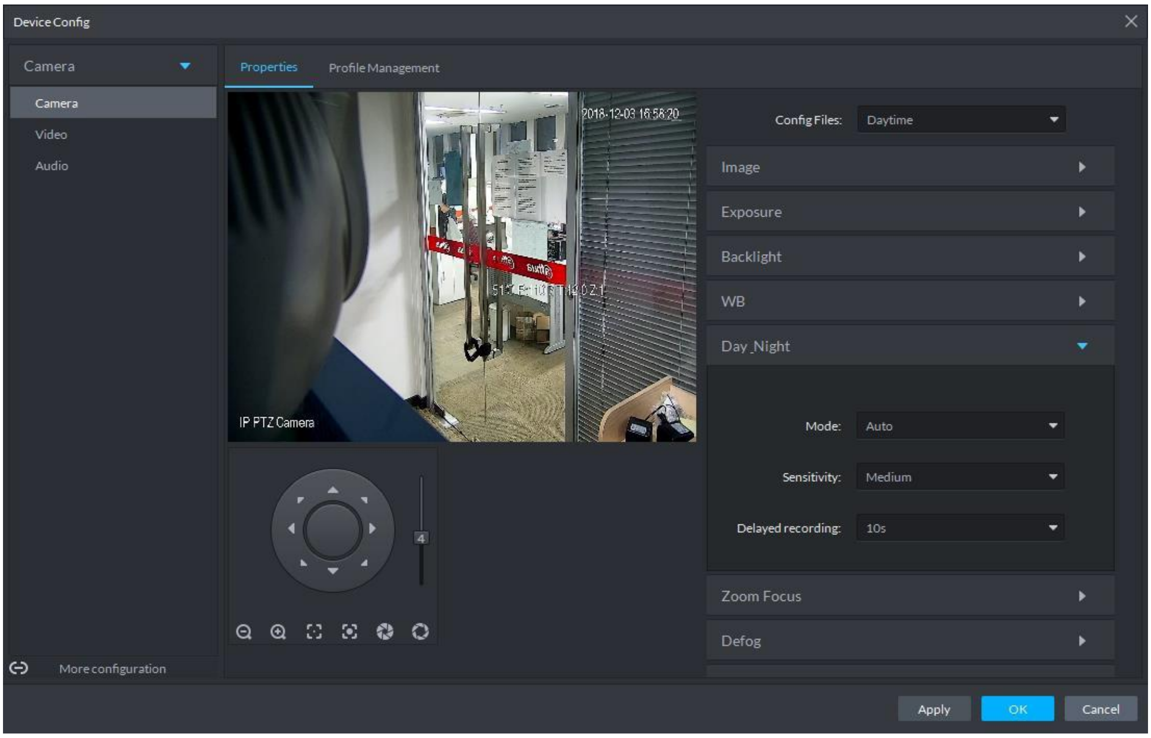
Table 3-23 WB mode description

WB mode	Description
Auto	The system automatically WB corrects different color temperatures to ensure normal display of image colors.
Natural Light	The system automatically WB corrects the scenes without manmade lighting to ensure normal display of image colors.
Street Lamp	The system automatically WB corrects the outdoor scenes at night to ensure normal display of image colors.
Outdoor	The system automatically WB corrects most outdoor scenes with natural lighting and manmade lighting to ensure normal display of image colors.
Manual	You can set up the red gains and blue gains manually for the system to correct different color temperatures in the environment accordingly.
Regional Custom	You can set up custom regions and the system WB corrects different color temperatures to ensure normal display of image colors.

Step 8 Click **Day & Night** to set up relevant parameters. See Figure 3-110. For details of the parameters, see Table 3-24.

You can set up the display mode of images. The system can switch between the Colored mode and the Black&White mode to adapt to the environment.

Figure 3-110 Day/Night


Device Config
Camera
Camera
Video
Audio
More configuration
Properties
Profile Management
IP PTZ Camera
2018-12-03 16:58:20
Image
Exposure
Backlight
WB
Day Night
Zoom Focus
Defog
Apply
OK
Cancel

Config Files: Daytime

Mode: Auto

Sensitivity: Medium

Delayed recording: 10s

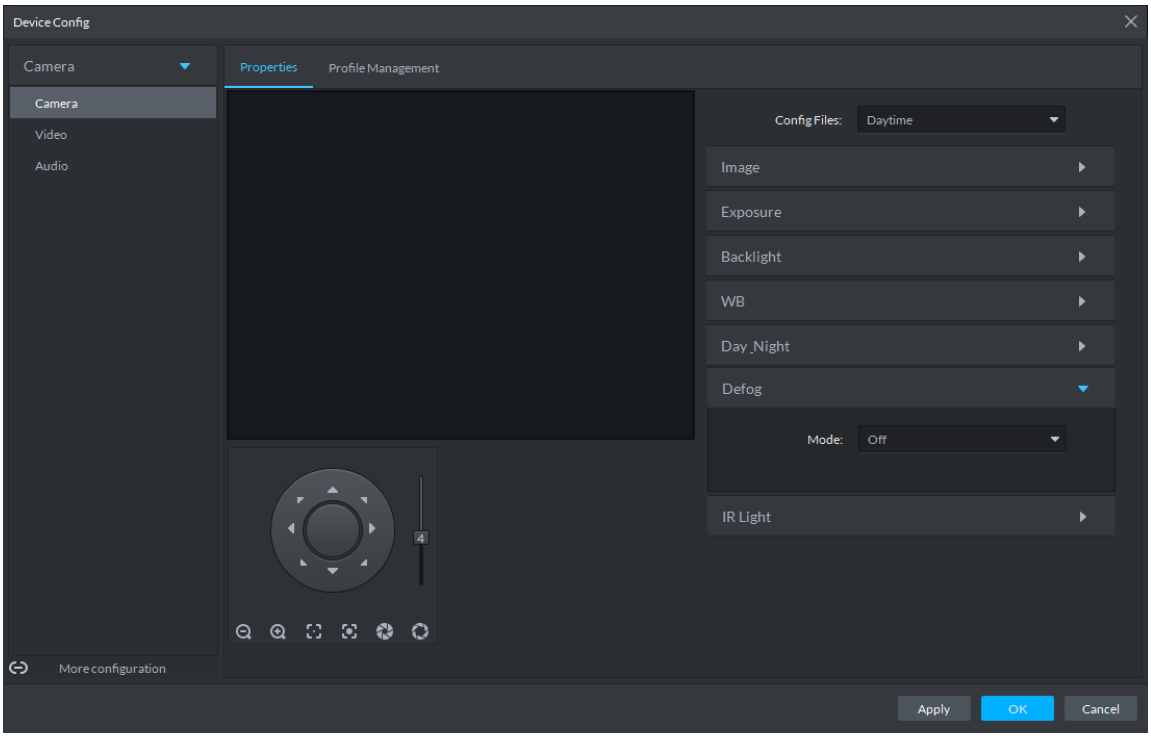
Table 3-24 Day/night mode parameter description

Parameter	Description
Mode	You can set up the image display of the camera to the Colored mode or the Black&White mode, including the following options: The **Day & Night** settings are independent of the **Config Files** settings. ● Colored: The camera displays colored images. ● Auto: The camera automatically selects to display colored or black&white images based on the environmental brightness. ● Black&White: The camera displays black&white images.
Sensitivity	You can set up this parameter when the **Day & Night** mode is set to **Auto**. Defines the sensitivity of the camera in switching between the Colored mode and the Black&White mode.
Delayed recording	You can set up this parameter when the **Day & Night** mode is set to **Auto**. Defines the delay of the camera in switching between the Colored mode and the Black&White mode. The lower the delay, the faster the switch between the Colored mode and the Black&White mode.

Step 9 Click **Defog** to set up relevant parameters. See Figure 3-111. For details of the parameters, see Table 3-25.

Image quality drops when the camera is placed in the foggy or hazy environment. You can turn on Defog to make the images clearer.

Figure 3-111 Defog


Device Config
Camera
Camera
Video
Audio
More configuration
Properties
Profile Management
Image
Exposure
Backlight
WB
Day Night
Defog
IR Light
Apply
OK
Cancel

Config Files: Daytime

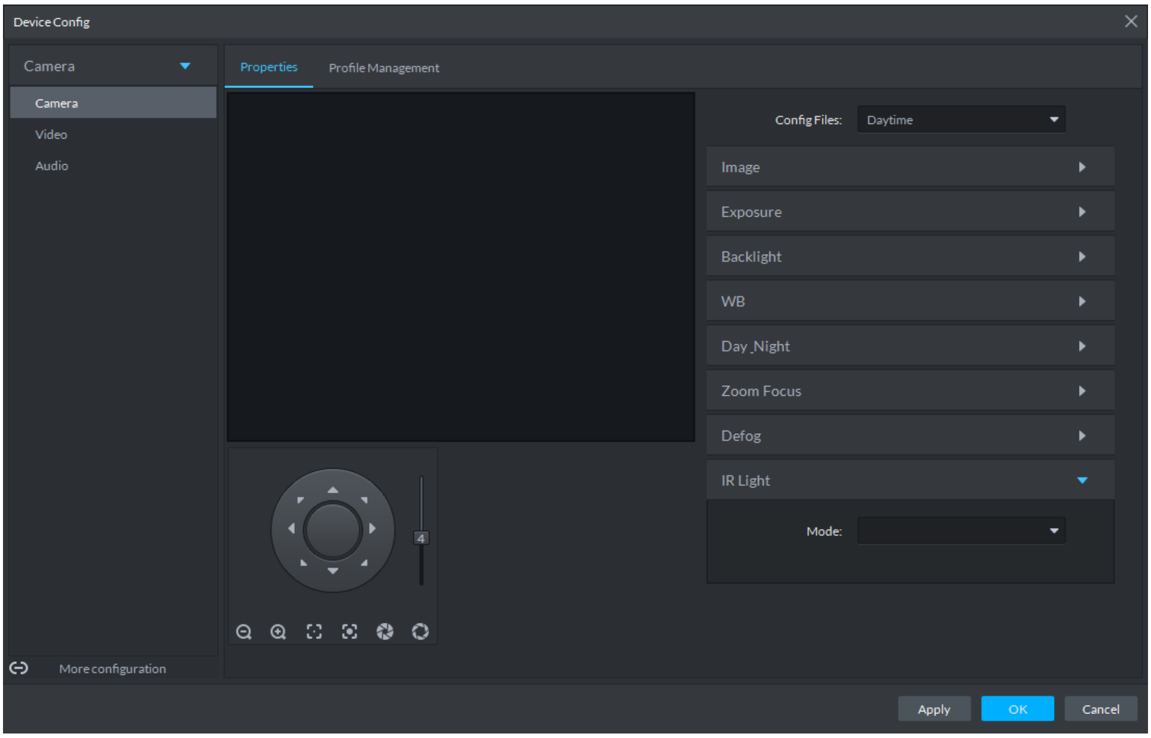
Mode: Off

Table 3-25 Defog mode description

Defog mode	Description
Manual	You can set up the defog intensity and the atmospheric light intensity manually. The system adjusts the image quality according to such settings. The atmospheric light intensity mode can be set to Auto or Manual for light intensity adjustment.
Auto	The system adjusts the image quality automatically to adapt to the surrounding conditions.
Off	Defog disabled.

Step 10 Click **IR Light** to set up relevant parameters. See Figure 3-112. For details of the parameters, see Table 3-26.

Figure 3-112 IR light


Device Config
Camera
Camera
Video
Audio
More configuration
Properties
Profile Management
Image
Exposure
Backlight
WB
Day Night
Zoom Focus
Defog
IR Light
Apply
OK
Cancel

Config Files: Daytime

Mode:

Table 3-26 IR light mode description

IR Light mode	Description
Manual	You can set up the IR Light brightness manually.
SmartIR	The system adjusts the brightness of the light to adapt to the surrounding conditions.
ZoomPrio	The system adjusts the IR Light automatically to adapt to the brightness changes in the environment. ● When the scene darkens, the system opens the near light first. If the required brightness still cannot be achieved when the near light runs at full power, the system turns on the far light. ● When the scene becomes brighter, the system reduces the brightness of the far light all the way until it is turned off, before adjusting the brightness of the near light. ● When the lens focus is adjusted to a certain wide end, the system keeps the far light off to avoid over-exposure at the near end, You can also set up lighting correction manually to fine tune the brightness of the IR Light.
Off	IR Light disabled.

Step 11 Click **OK**.

3.5.1.2 Applying Configuration Files

The system monitors the objects in different time periods based on the preset configuration files modes.

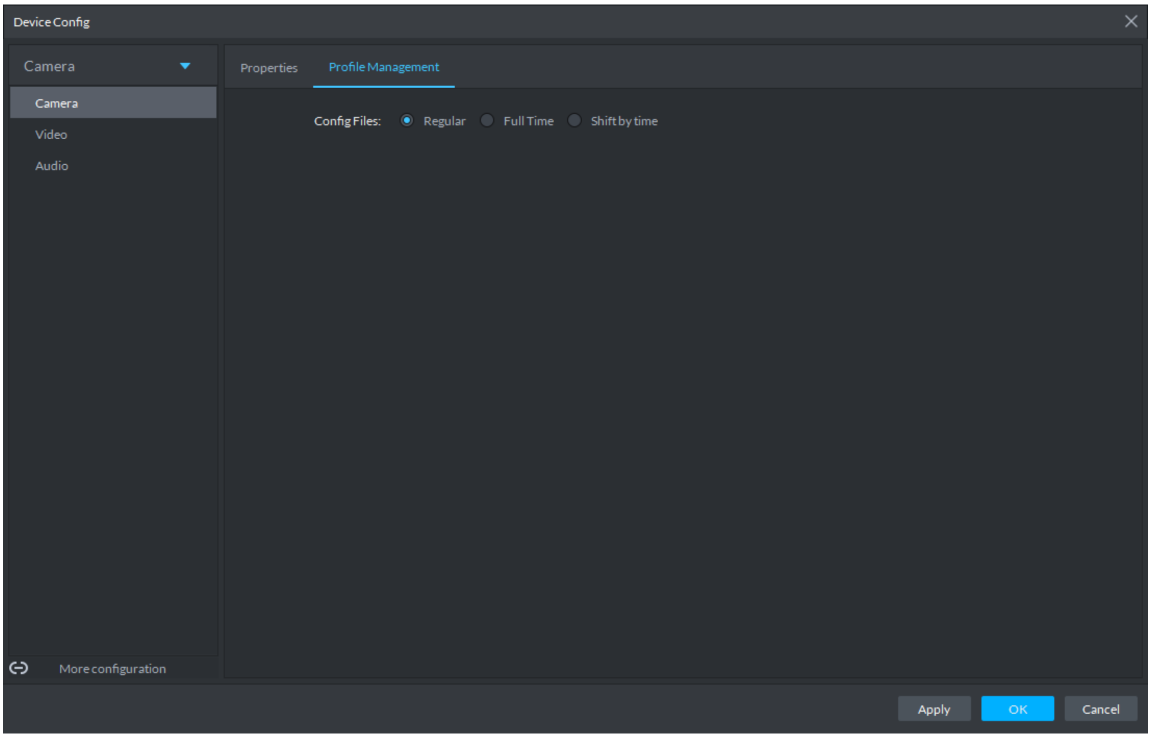
Step 1 Select **Camera > Camera > Profile Management**.

The **Profile Management** interface is displayed.

Step 2 Setting up configuration files.

- When **Config Files** is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 3-113 Regular

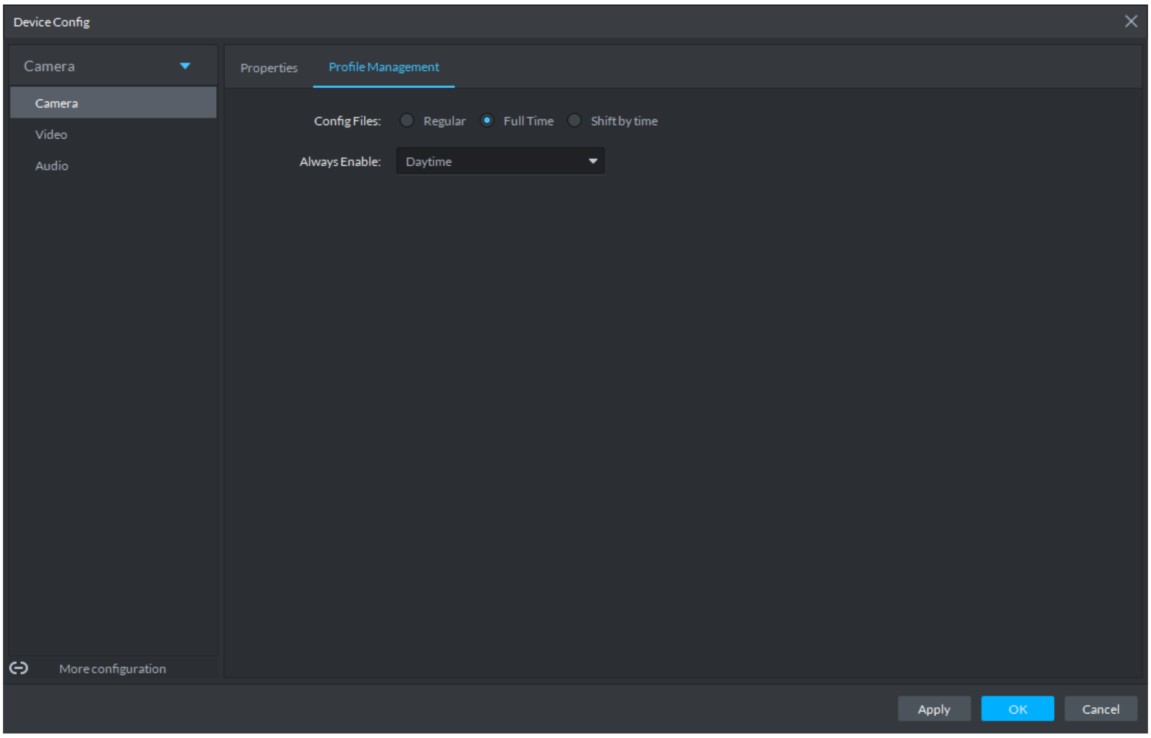


Device Config
Camera
Camera
Video
Audio
More configuration
Properties
Profile Management
Apply
OK
Cancel

Config Files: ● Regular ○ Full Time ○ Shift by time

- When **Config Files** is set to **Full Time**, you can set **Always Enable** to **Daytime** or **Night**. The system monitors the objects as per the **Always Enable** configurations.

Figure 3-114 Full time



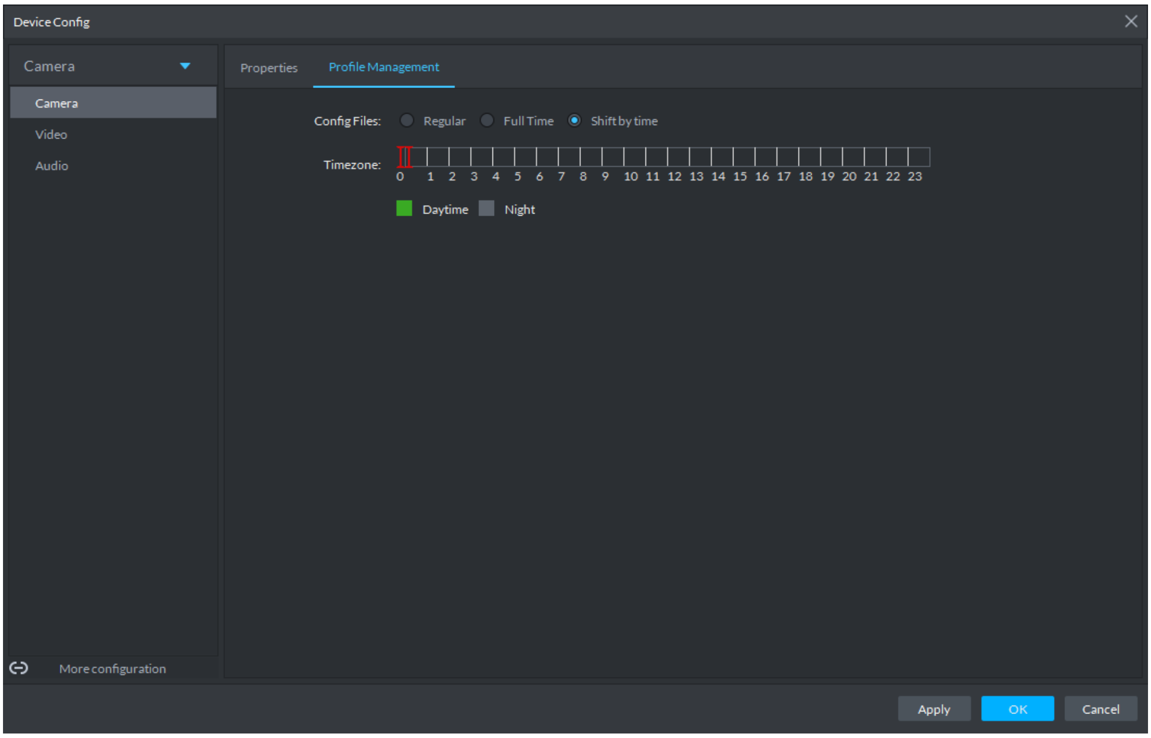
Device Config
Camera
Camera
Video
Audio
More configuration
Properties
Profile Management
Apply
OK
Cancel

Config Files: ○ Regular ● Full Time ○ Shift by time

Always Enable: Daytime

- When **Config Files** is set to **Shift by time**, you can drag the slider to set a period of time as daytime or night. For example, you can set 8:00–18:00 as daytime, 0:00–8:00 and 18:00–24:00 as night. The system monitors the objects in different time periods as per corresponding configurations.

Figure 3-115 Shift by time


Device Config
Camera
Camera
Video
Audio
More configuration
Properties
Profile Management
Config Files:
○ Regular
○ Full Time
● Shift by time
Timezone:
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
🟩 Daytime
▨ Night
Apply
OK
Cancel

Step 3 Click **OK** to save the configurations.

3.5.2 Video

You can set some video parameters, including Video Stream, Snapshot Stream, Overlay, ROI, Save Path, and Video Encryption.

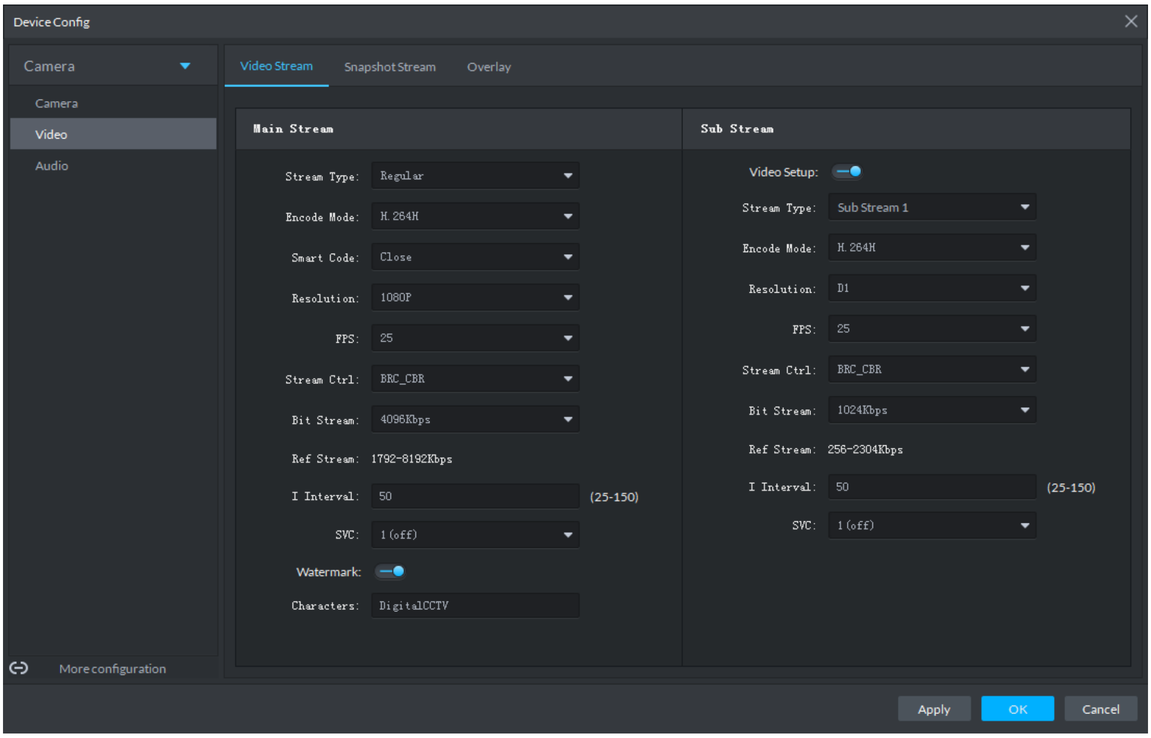
3.5.2.1 Video Stream

You can set up some video stream parameters, including Stream Type, Encode Mode, Resolution, FPS, Stream Ctrl, Bit Stream, I Interval, SVC, Watermark, and more.

Step 1 On the **Device Config** interface, select **Camera > Video > Video Stream**.

The **Video Stream** interface is displayed. See Figure 3-116.

Figure 3-116 Video stream



Main Stream

Stream Type: Regular
Encode Mode: H.264H
Smart Code: Close
Resolution: 1080P
FPS: 25
Stream Ctrl: BRC_CBR
Bit Stream: 4096Kbps
Ref Stream: 1792-8192Kbps
I Interval: 50 (25-150)
SVC: 1 (off)
Watermark: ●
Characters: DigitalCCTV

Sub Stream

Video Setup: ●
Stream Type: Sub Stream 1
Encode Mode: H.264H
Resolution: D1
FPS: 25
Stream Ctrl: BRC_CBR
Bit Stream: 1024Kbps
Ref Stream: 256-2304Kbps
I Interval: 50 (25-150)
SVC: 1 (off)

Step 2 To configure the details, see Table 3-27.

The default values of streams might vary in different devices. The actual interfaces shall prevail.

Table 3-27 Video stream parameter description

Parameter	Description
Video Setup	Indicates whether to set up the Sub Stream parameters.
Encode Mode	The following video encoding modes are available: ● H.264: Main Profile. ● H.264H: High Profile. ● H.265: Main Profile.
Smart Code	Turning on Smart Code helps compress the images more and reduce the storage space. When Smart Code is on, the device does not support sub stream 2, ROI, IVS event detection. The actual screens shall prevail.
Resolution	The resolution of the videos. Different devices might have different max resolutions. The actual interfaces shall prevail.
FPS	The number of frames per second in a video. The higher the FPS, the more distinct and smooth the images.
Stream Ctrl	The following video stream control modes are available: ● BRC_CBR: The bit stream changes slightly around the preset value. ● BRC_VBR: The bit stream changes according to the monitored scenes. When the **Encode Mode** is set to **MJPEG**, BRC_CBR remains the only option for stream control.

Parameter	Description
Image Quality	This parameter can be set only when **Stream Ctrl** is set to BRC_VBR. Video image quality is divided into six grades: Best, Better, Good, Bad, Worse and Worst.
Bit Stream	This parameter can be set only when **Stream Ctrl** is set to **BRC_CBR**. You can select the proper stream value from the dropdown list based on actual scenarios.
Ref Stream	The system will recommend an optimal range of stream values to users based on the resolution and FPS set up by them.
I Interval	Refers to the number of P frames between two I frames. The range of I Interval changes with FPS. It is recommended to set the I Interval to be two times as the FPS value.
SVC	FPS is subject to layered encoding. SVC is a scalable video encoding method on time domain. The default value is 1, that is non-layered encoding.
Watermark	Turn on **Watermark** to enable this feature. You can verify the watermark characters to check whether the video has been tempered or not.
Characters	Characters for watermark verification. The default value is DigitalCCTV.

Step 3 Click **OK** to save the configurations.

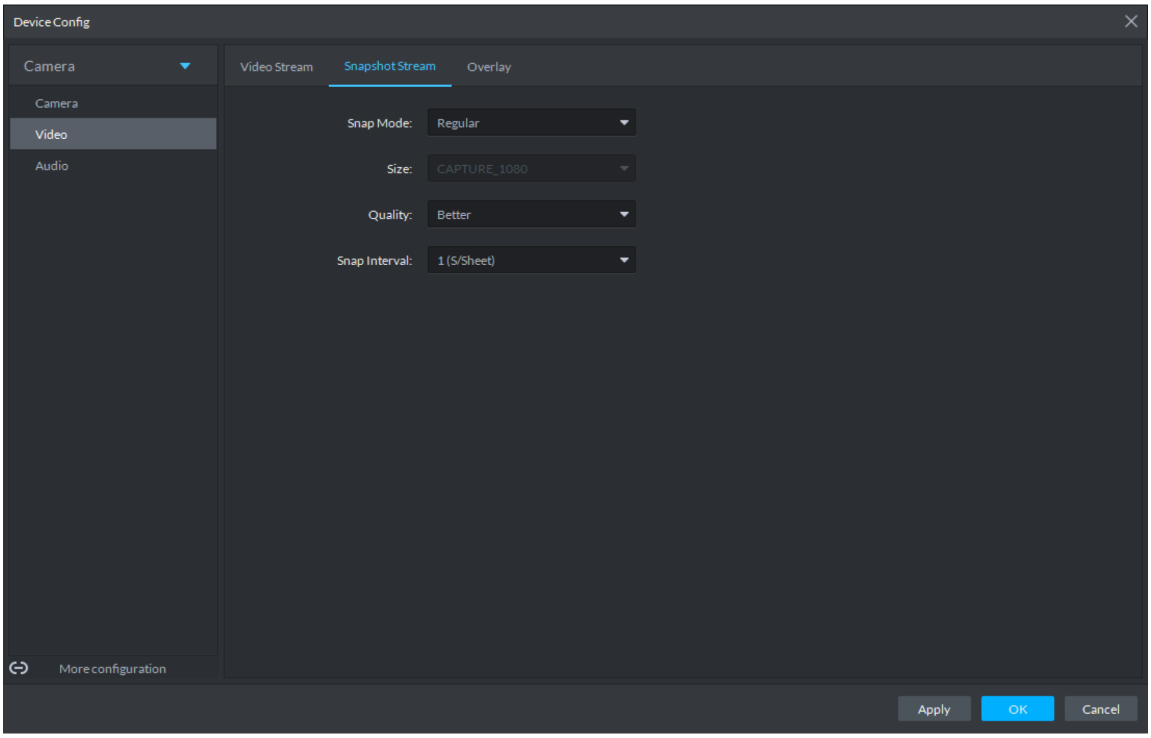
3.5.2.2 Snapshot Stream

You can set up some stream parameters for snapshots, including Snap Mode, Size, Quality, and Snap Interval.

Step 1 On the **Device Config** interface, select **Camera > Video > Snapshot Stream**.

The **Snapshot Stream** interface is displayed. See Figure 3-117.

Figure 3-117 Snapshot stream



Snap Mode: Regular

Size: CAPTURE_1080

Quality: Better

Snap Interval: 1 (S/Sheet)

Step 2 To set up Snapshot Stream, see Table 3-28 for the details of various parameters.

Table 3-28 Snapshot stream parameter description

Parameter	Description
Snap Mode	It includes **Regular** and **Trigger**. ● **Regular** refers to capturing pictures within the time range set up in a time table. ● **Trigger** refers to capturing pictures when video detection, audio detection, IVS events, or alarms are triggered, provided that video detection, audio detection, and corresponding snapshot functions are turned on.
Size	Same as the resolution in Main Stream.
Quality	Set up image quality. It is divided into six grades: Best, Better, Good, Bad, Worse and Worst.
Snap Interval	Sets up the frequency of snapshots. Select Custom to manually set up the frequency of snapshots.

Step 3 Click **OK** to save the configurations.

3.5.2.3 Overlay

You can set up video overlay, including Tampering/Privacy Mask, Channel Title, Period Title, Geographic Position, OSD Overlay, Font, and Picture Overlay.

Step 1 **On the Device Config interface**, select **Camera > Video > Overlay**.

The **Overlay** interface is displayed.

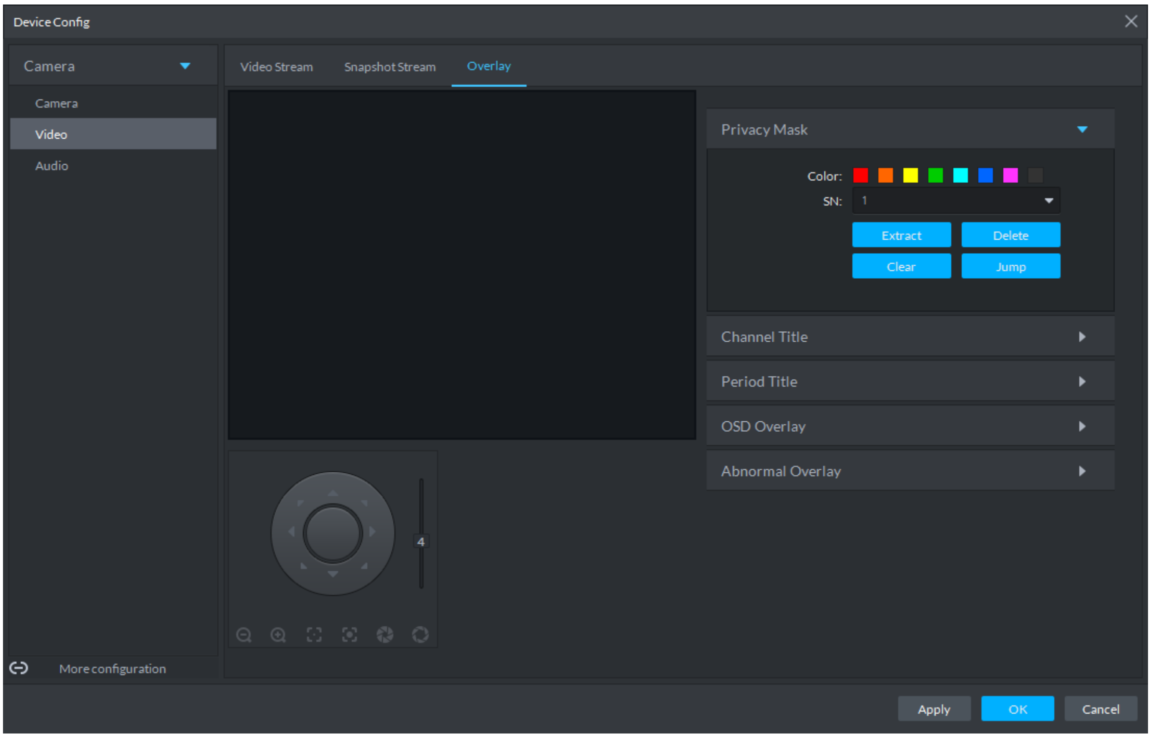
Step 2 (Optional) Set up **Privacy Mask**.

Masking is useful in case that privacy protection is needed for some parts of the video images.

5) Click the **Privacy Mask** tab.

The **Privacy Mask** interface is displayed. See Figure 3-118.

Figure 3-118 Privacy mask


Device Config
Camera
Camera
Video
Audio
More configuration
Video Stream
Snapshot Stream
Overlay
Privacy Mask
Color:
SN:
1
Extract
Delete
Clear
Jump
Channel Title
Period Title
OSD Overlay
Abnormal Overlay
4
Apply
OK
Cancel

6) Select **Enable** and drag a box to the target area for privacy protection.

- You can draw up to four boxes.
- Click **Clear** to delete all boxes; to delete a box, select it and click **Delete**, or right-click and delete the box you want.

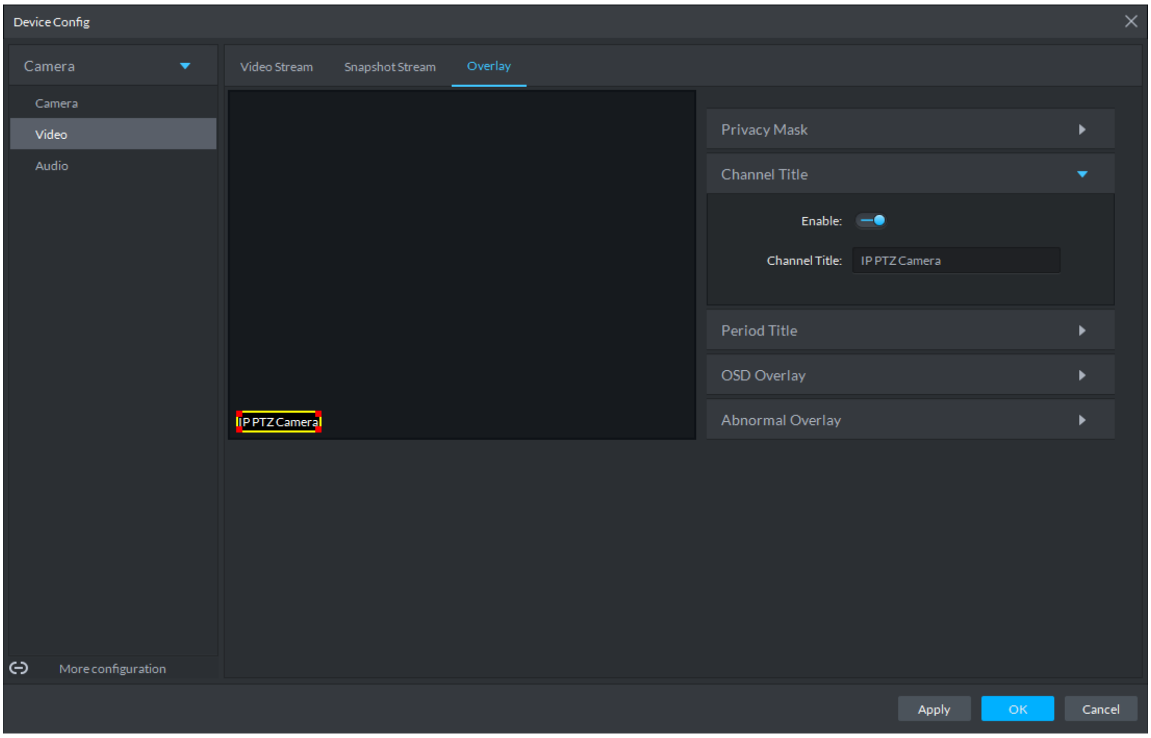
Step 3 (Optional) Set up Channel Title.

You can set up the Channel Title if it must be displayed in video images.

1) Click the **Channel Title** tab.

The **Channel Title** interface is displayed. See Figure 3-119.

Figure 3-119 Channel title


Device Config
Camera
Camera
Video
Audio
More configuration
Video Stream
Snapshot Stream
Overlay
IP PTZ Camera
Privacy Mask
Channel Title
Period Title
OSD Overlay
Abnormal Overlay
Apply
OK
Cancel

Enable: (on)

Channel Title: IP PTZ Camera

2) Select **Enable** and set up the Channel Title, which is then displayed in the video images.

In the video image, the channel title box can be moved to a proper position.

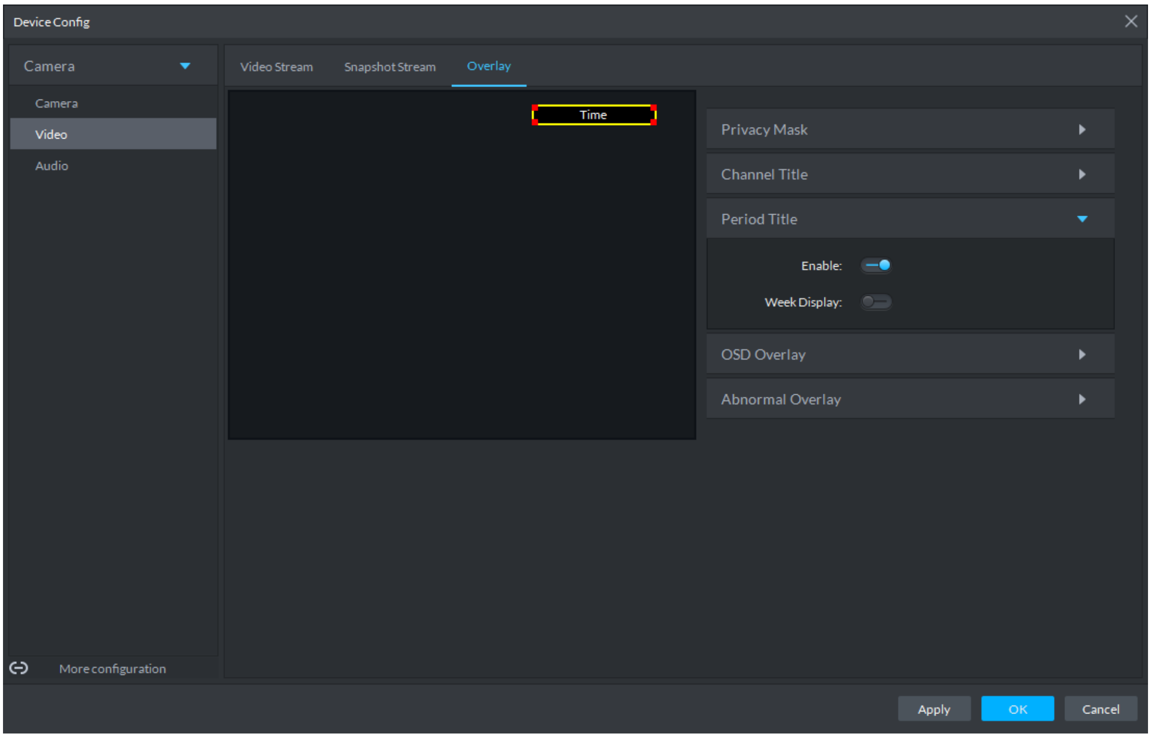
Step 4 (Optional) Set up Period Title.

You can set up the Period Title if it must be displayed in video images.

1) Click the **Period Title** tab.

The **Period Title** interface is displayed. See Figure 3-120.

Figure 3-120 Period title


Device Config
Camera
Camera
Video
Audio
More configuration
Video Stream
Snapshot Stream
Overlay
Time
Privacy Mask
Channel Title
Period Title
Enable:
Week Display:
OSD Overlay
Abnormal Overlay
Apply
OK
Cancel

2) Select **Enable** and the time information is displayed in the video images.

3) Select **Week Display** and the week information displays in video images.

📖

In the video image, the period title box can be moved to a proper position.

Step 5 Click **OK** to save the configurations.

3.5.3 Audio

You can set some audio parameters such as Encode Mode, Sampling frequency, Audio input type, Noise filtering.

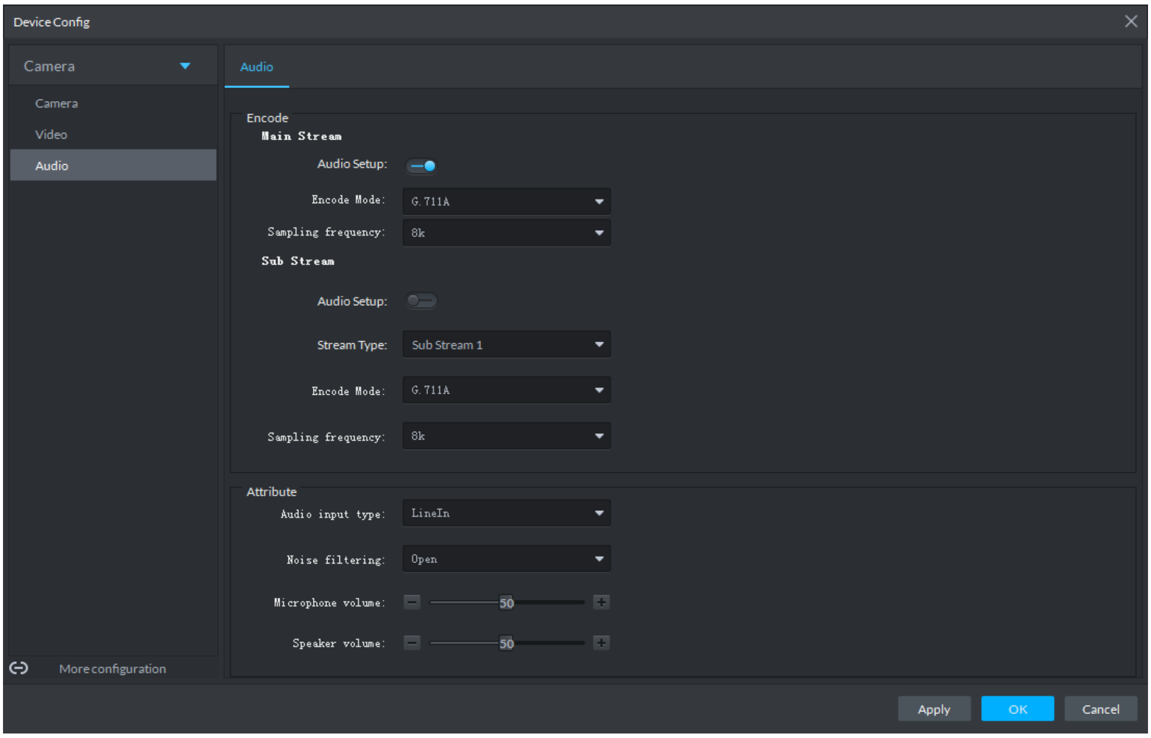
📖

Some devices do not support audio functions.

Step 1 On the **Device Config** interface, select **Camera > Audio**.

The **Audio** interface is displayed. See Figure 3-121.

Figure 3-121 Audio



Encode

Main Stream

Audio Setup:

Encode Mode: G.711A

Sampling frequency: 8k

Sub Stream

Audio Setup:

Stream Type: Sub Stream 1

Encode Mode: G.711A

Sampling frequency: 8k

Attribute

Audio input type: LineIn

Noise filtering: Open

Microphone volume: 50

Speaker volume: 50

Step 2 To set up audio parameters, see Table 3-29 for details.

Table 3-29 Audio parameter description

Parameter	Description
Enable	Audio cannot be enabled unless video has been enabled. After selecting Enable in **Main Stream** or **Sub Stream** sections, the network transmits a mixed flow of videos and audios. Otherwise, the transmitted flow only contains video images.
Encode Mode	The encoding modes of audios include G.711A, G.711Mu, AAC, and G.726. The preset audio encode mode applies both to audio call and video call
Sampling frequency	Available audio sampling frequencies include 8K, 16K, 32K, 48K, and 64K.
Audio input type	The following types of audios connected to devices are available: ● LineIn: The device must connect to external audio devices. ● Mic: The device does not need external audio devices.
Noise filtering	After enabling noise filtering, the system automatically filters out the noises in the environment.
Microphone volume	Adjust the microphone volume. 📖 This function is available on select models.
Speaker volume	Adjust the speaker volume. 📖 This function is available on select models.

Step 3 Click **OK** to save the configurations.

3.6 Configuring Intelligent Analysis

Configure intelligent analysis rules on the client to realize intelligent analysis business. Intelligent analysis types supported: IVS, people counting, face detection and heatmap. The rule configuration interface might vary according to the function capability of the different devices. The actual interface shall prevail.

📖

The platform only supports configuring intelligent analysis rules for IPC channels.

3.6.1 Intelligent Analysis Configuration Interface

The following two methods are supported to go to the intelligent analysis configuration interface.

- Right-click an IPC channel on the **Live View** interface, and then select **Intelligent Analyse**. See Figure 3-122.

  The **IVS Setting** interface is displayed. See Figure 3-123.

Figure 3-122 Go to intelligent analysis interface

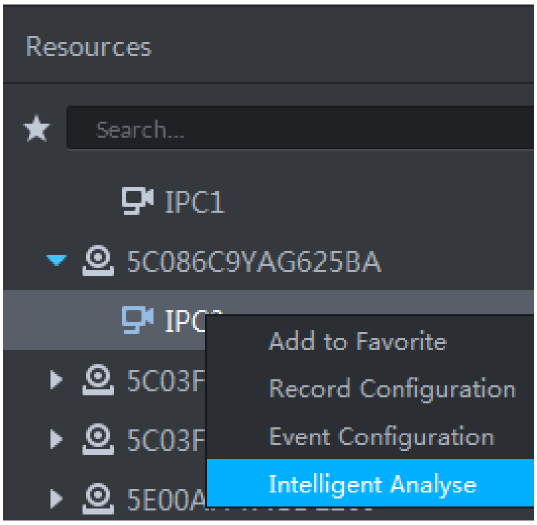
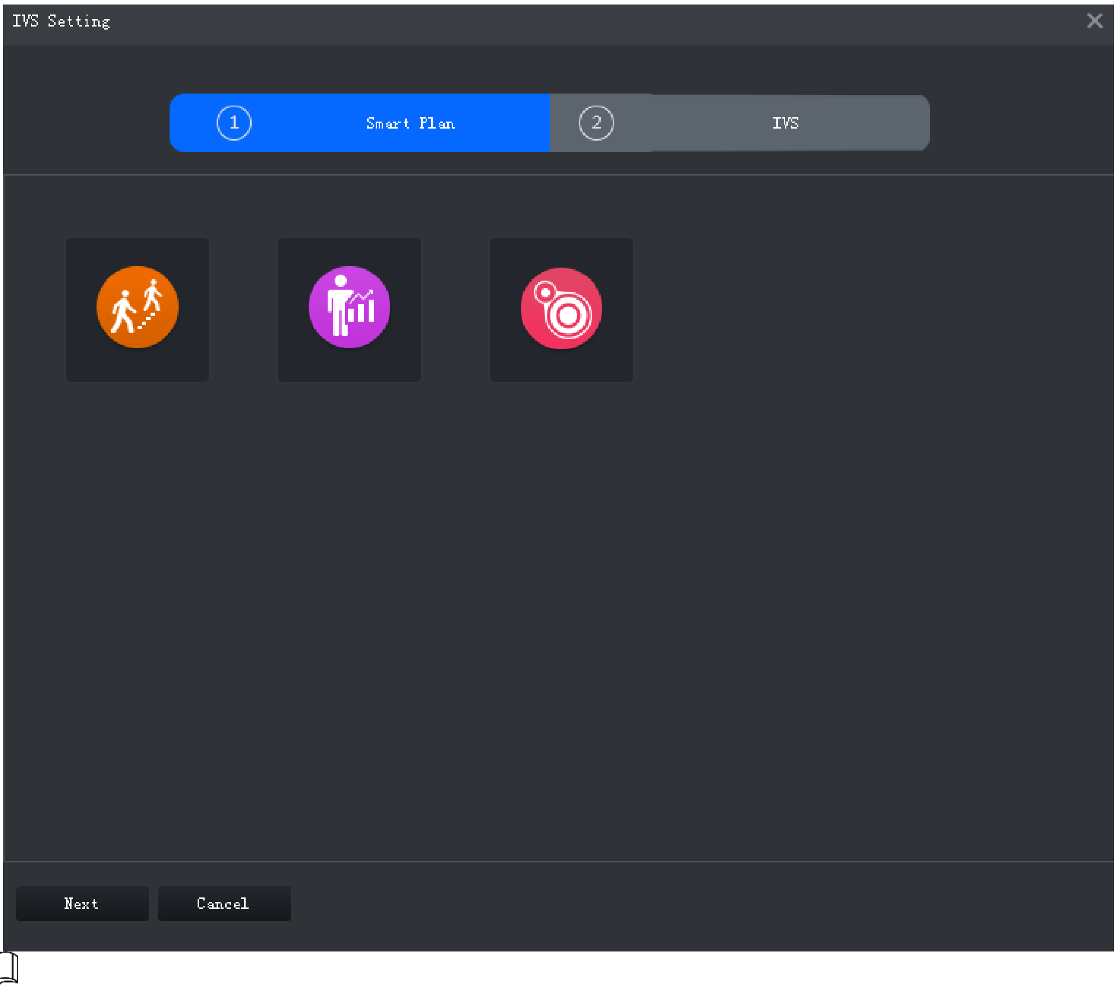

Resources
Search...
IPC1
5C086C9YAG625BA
IPC
5C03F
5C03F
5E00A
Add to Favorite
Record Configuration
Event Configuration
Intelligent Analyse

Figure 3-123 IVS setting interface


IVS Setting
1
Smart Plan
2
IVS
Next
Cancel

The interface might vary according to the smart function capability of the different devices. The actual interface shall prevail.

- Select an IPC channel in the device list on the **Config** interface, and then click . See Figure 3-124.

  The interface of **IVS Setting** is displayed. See Figure 3-123.

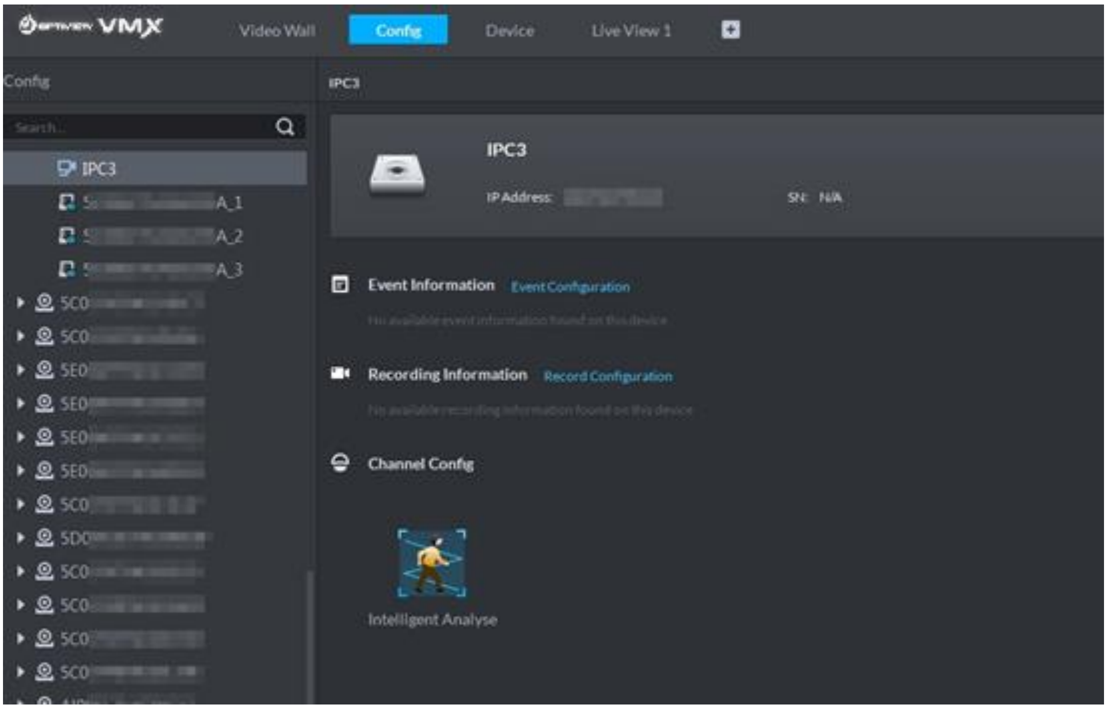

VMX
Video Wall
Config
Device
Live View 1
Config
IPC3
Search...
IPC3
IPC3
IP Address:
SN: N/A
Event Information
Event Configuration
No available event information found on this device
Recording Information
Record Configuration
No available recording information found on this device
Channel Config
Intelligent Analyse

Figure 3-124 Go to intelligent analysis interface

3.6.2 IVS

IVS includes tripwire analysis, intrusion detection, abandoned object, loitering detection, fast moving, crowd gathering, missing object and parking detection. The actual camera capability shall prevail. With IVS configured, when a target is detected, the system will trigger an event as you have set and display it on the platform.

See requirements as follows when configuring:

- The total target ratio does not exceed 10% of the screen.
- The size of the target in the picture is not less than 10 pixels × 10 pixels, the target size of the abandoned object is not less than 15 pixels × 15 pixels (CIF image); the target height and width is not more than 1/3 of the picture height and the recommended target height is 10% of the picture height.
- The difference between the brightness value of the target and the background is not less than 10 gray levels.
- At least ensure that the target appears continuously for more than 2 seconds in the field of view, the moving distance exceeds the target's own width, and is not less than 15 pixels (CIF image).
- Minimize the complexity of the monitoring and analysis scenario when conditions permit. It is not recommended to use the smart analysis function in scenarios with dense targets and frequent light changes.
- Try to avoid areas such as glass, ground reflection and water surface; try to avoid branches, shadows and mosquito interference areas; try to avoid backlit scenes and avoid direct light.

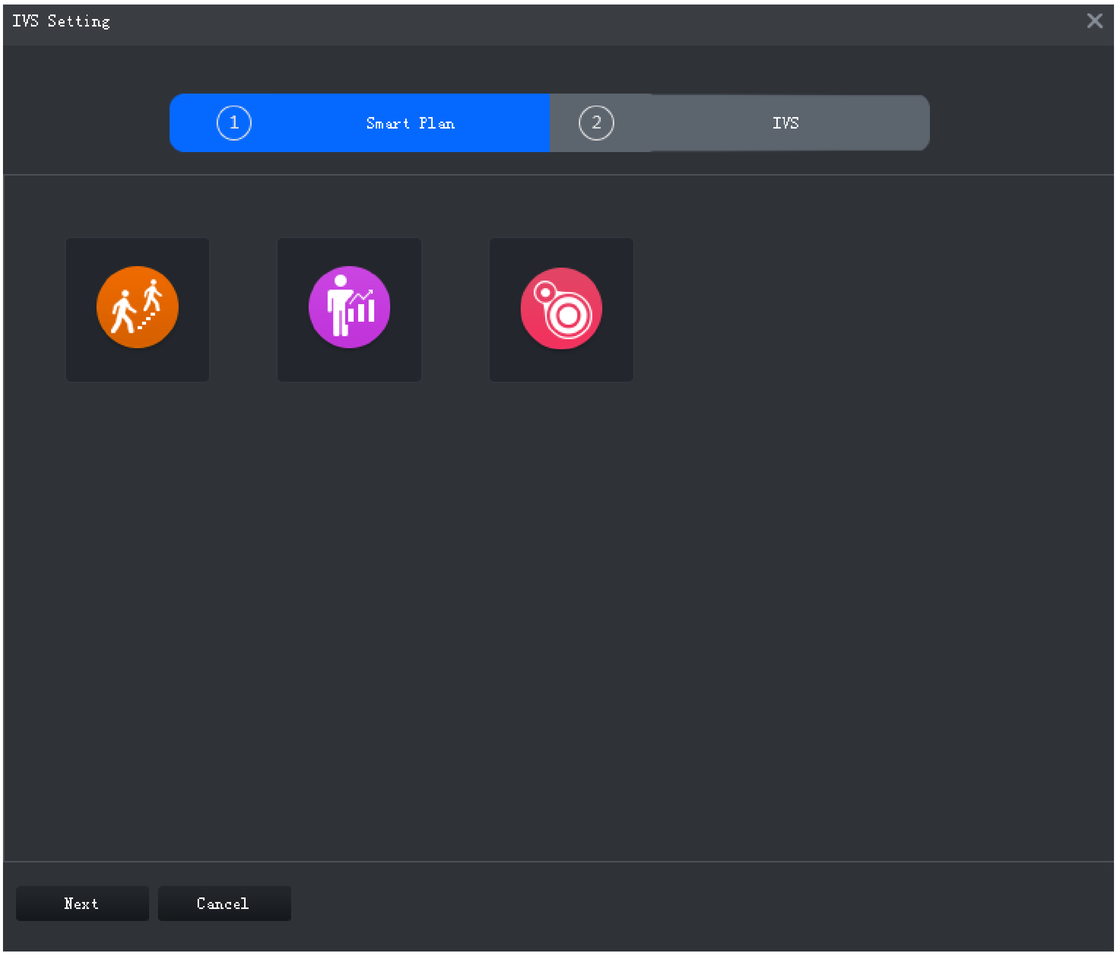
3.6.2.1 Enabling IVS Smart Plan

Step 1 Go to the **Intelligent Analyse** interface.

Step 2 Click on the smart plan interface to enable IVS smart plan. See Figure 3-125.

When the icon is displayed in the white frame, it means the smart plan is selected. If another smart plan has been selected, click that smart plan icon to deselect it and then click to select IVS.

Figure 3-125 Enable IVS smart plan



Step 3 Click **Next**.

The **IVS Setting** interface is displayed.

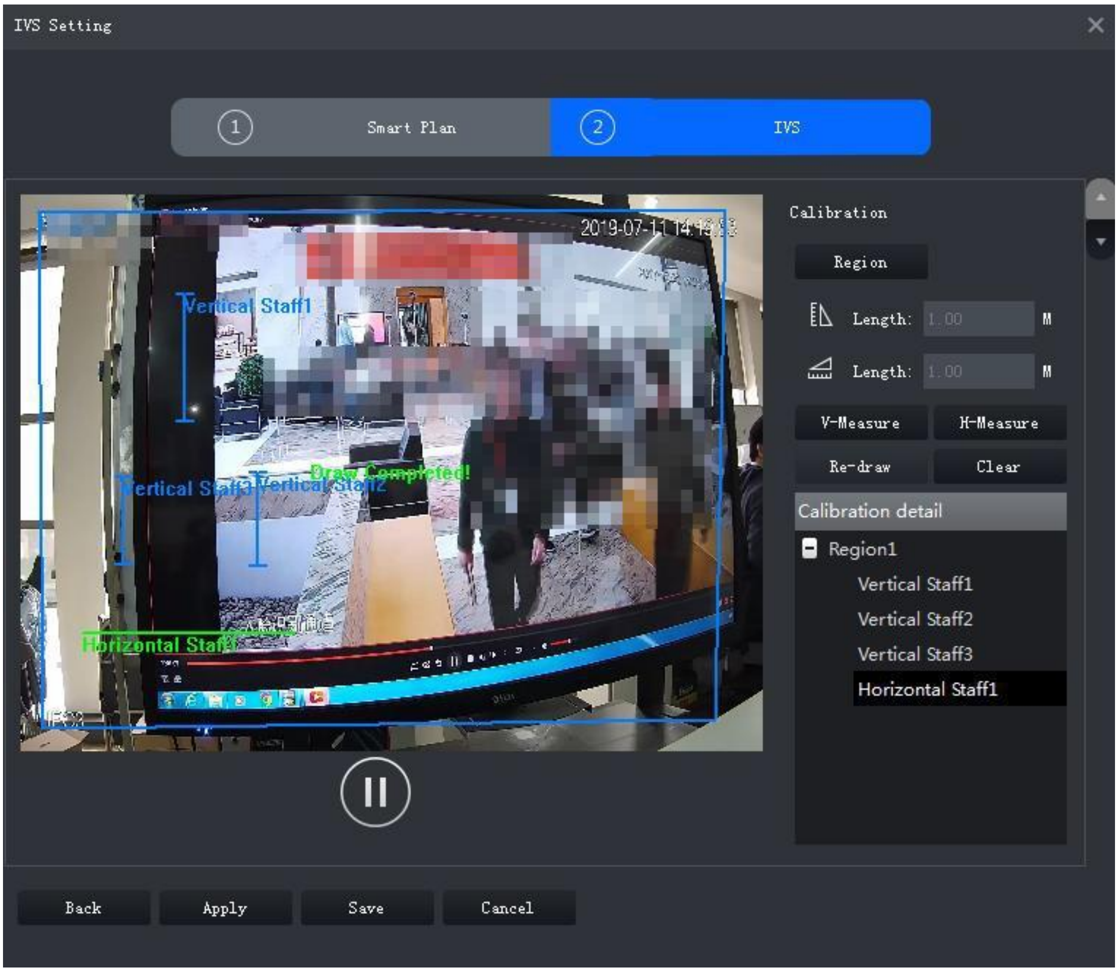
3.6.2.2 Calibrating Depth of Field

After setting one horizontal gauge and three vertical gauge and the actual geographical distances of each gauge, the system can estimate the internal parameters (internal geometrical features and optical properties) and external parameters (the network camera position and direction on the actual environment) of network camera, so as to work out the relation between the two-dimensional image and three dimensional objects in the current surveillance environment.

Step 1 After selecting the smart plan in the **Smart Plan** interface, click **Next**.

The interface of **Calibration** is displayed, See Figure 3-126.

Figure 3-126 Calibrating depth of field


IVS Setting
1
Smart Plan
2
IVS
2019-07-11 14:14:23
Vertical Staff1
Vertical Staff3
Vertical Staff2
Draw Completed!
Horizontal Staff1
Calibration
Region
Length: 1.00 M
Length: 1.00 M
V-Measure
H-Measure
Re-draw
Clear
Calibration detail
Region1
Vertical Staff1
Vertical Staff2
Vertical Staff3
Horizontal Staff1
Back
Apply
Save
Cancel

Step 2 Click **Region** and draw calibration zone on the video. Right-click to finish.

Step 3 Set length value of the vertical gauge. Click and then draw a vertical gauge in the calibration area. Click to finish.

Draw another three vertical gauges in the calibration area.

Step 4 Set length value of horizontal gauge. Click and then draw a horizontal gauge in the calibration area. Click to finish.

- To modify the gauge, you can select it and click **Re-draw**. You can also select the calibration are and click **Re-draw** to draw new calibration areas and gauges.
- To delete a gauge, select it and click **Delete**. To delete a calibration area and the gauges in it, select the area and click **Delete**.

Step 5 Click **Apply** to save.

Step 6 (Optional)Vertical/horizontal measuring

Do the following steps to measure distance.

- Click **V-Measure** and draw vertical line in the calibration area. The measuring result will be displayed.
- Click **H-Measure** and draw horizontal line in the calibration area. The measuring result will be displayed.

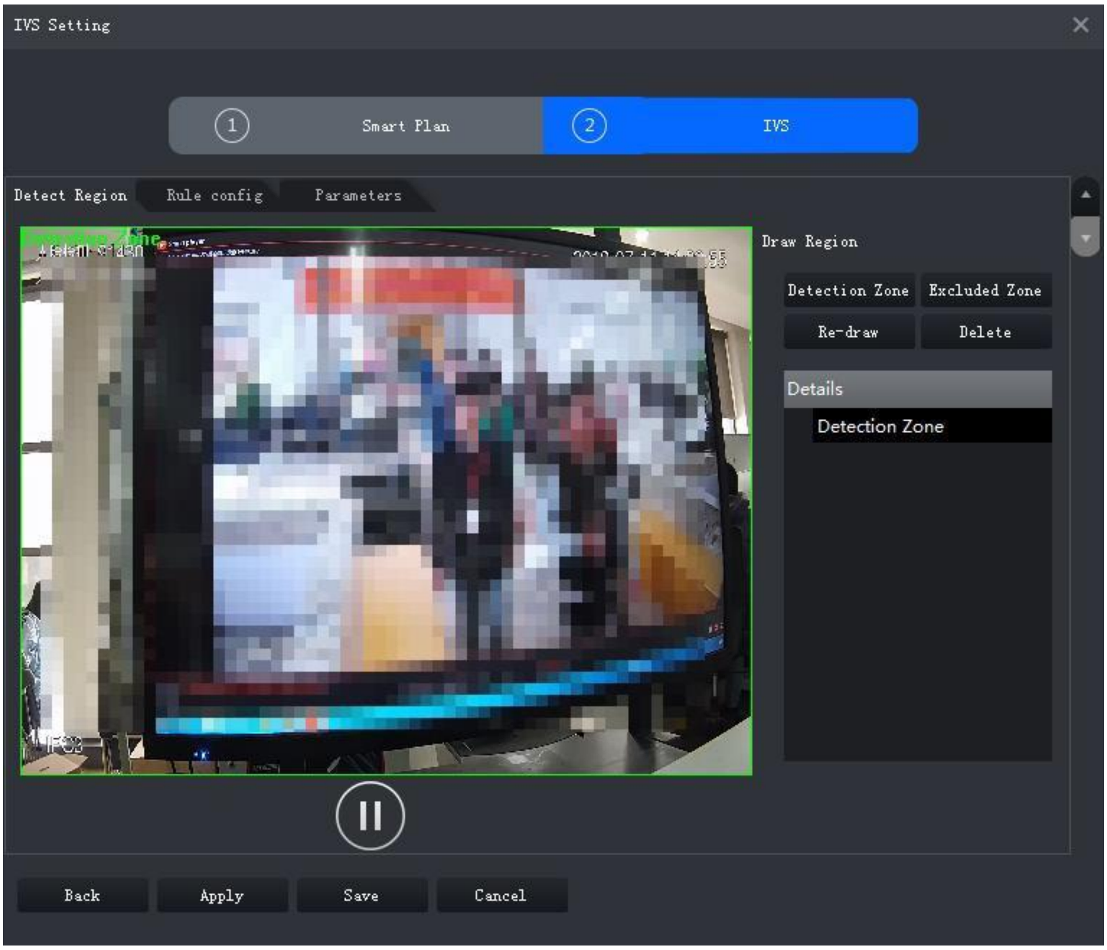
3.6.2.3 Configuring Detection Region

Configure the detection zone of IVS.

Step 1 Click ▾.

The interface of **Detect Region** is displayed. See Figure 3-127.

Figure 3-127 Detection region


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Rule config
Parameters
Draw Region
Detection Zone
Excluded Zone
Re-draw
Delete
Details
Detection Zone
Back
Apply
Save
Cancel

Step 2 Click **Detection Zone**, and then draw the frame of the detection zone on the video and right-click to finish.

Step 3 Click **Excluded Zone**, and then draw the frame of the zone on the video and right-click to finish.

🕮

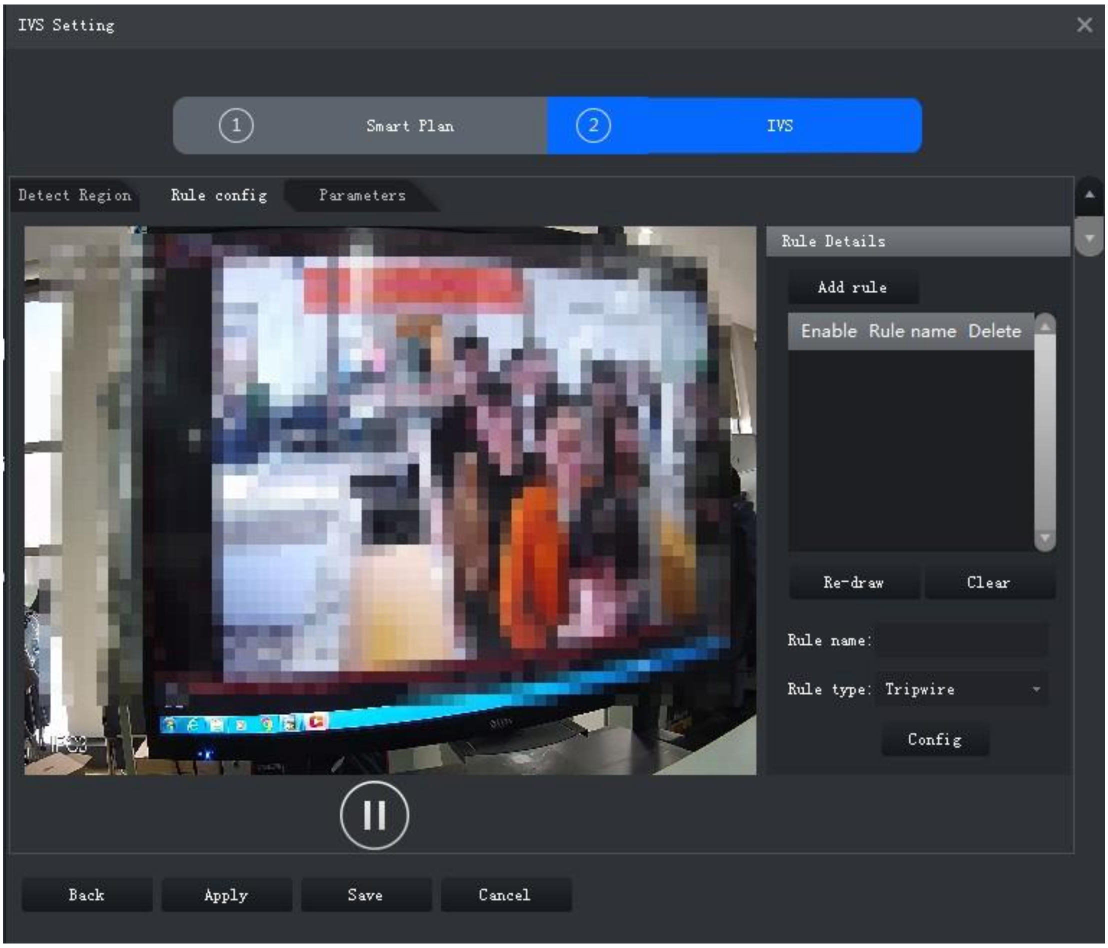
- Select the excluded zone and click **Re-draw** to draw a new excluded zone; select the detection zone and click **Re-draw** to draw a new detection zone and a new excluded zone.
- Select the excluded zone and click **Delete** to delete the excluded zone; select the detection zone and click **Delete** to delete the detection zone and excluded zone.

3.6.2.4 Configuring IVS Rule

Configure arming schedules and alarm linkages of IVS type including tripwire and intrusion.

Click **Rule config**. The interface of **Rule config** is displayed. SeeFigure 3-128.

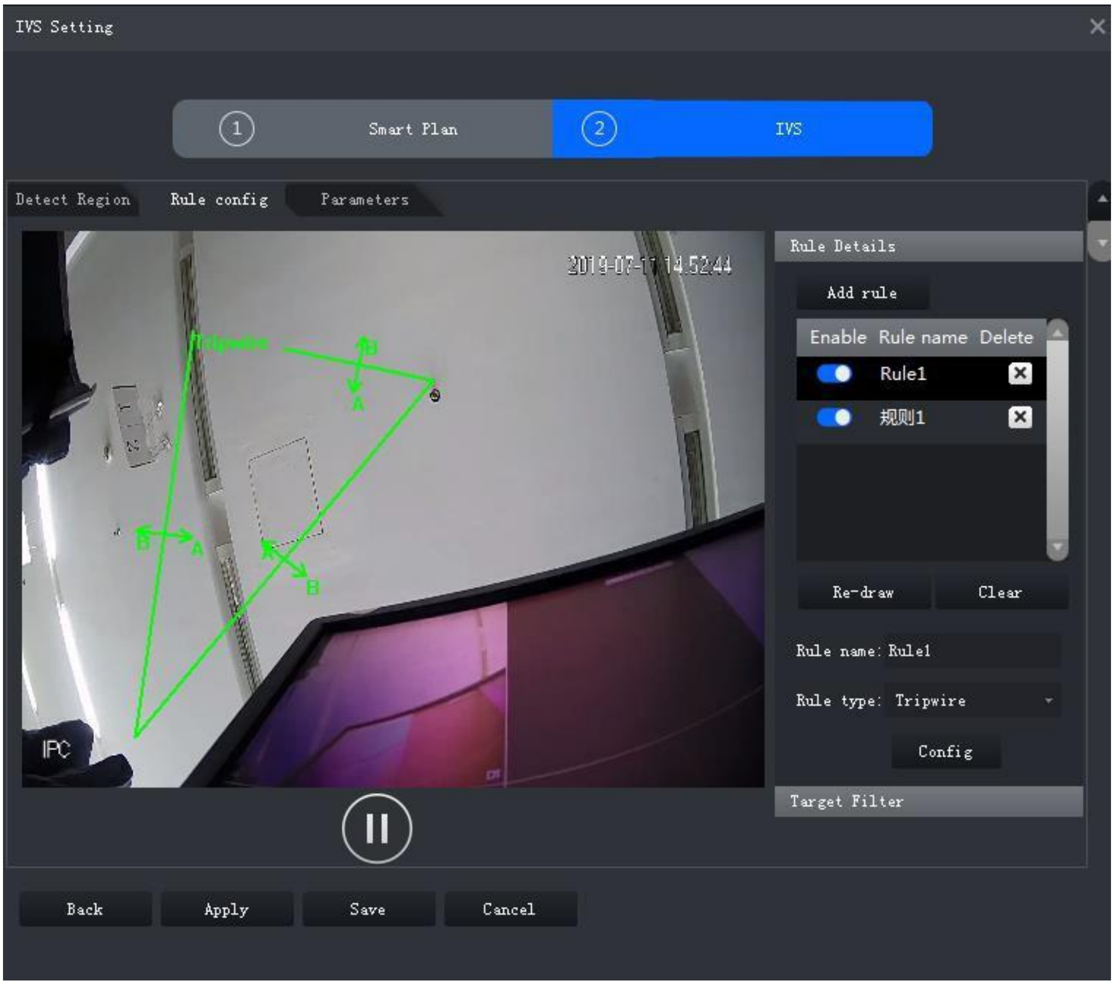
Figure 3-128 Rule configuration interface


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Rule config
Parameters
Rule Details
Add rule
Enable
Rule name
Delete
Re-draw
Clear
Rule name:
Rule type:
Tripwire
Config
Back
Apply
Save
Cancel

3.6.2.4.2 Tripwire

When a target is detected crossing a line, an alarm will be triggered immediately.

Figure 3-129 Tripwire


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Rule config
Parameters
2019-07-11 14:52:44
Tripwire
A
B
IPC
Rule Details
Add rule
Re-draw
Clear
Config
Target Filter
Back
Apply
Save
Cancel

Enable	Rule name	Delete
●	Rule1	☒
●	规则1	☒

Rule name: Rule1

Rule type: Tripwire

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. ● indicates rule is enabled.

2) Modify **Rule name**.

3) Select **Tripwire** in the dropdown list of **Rule type**.

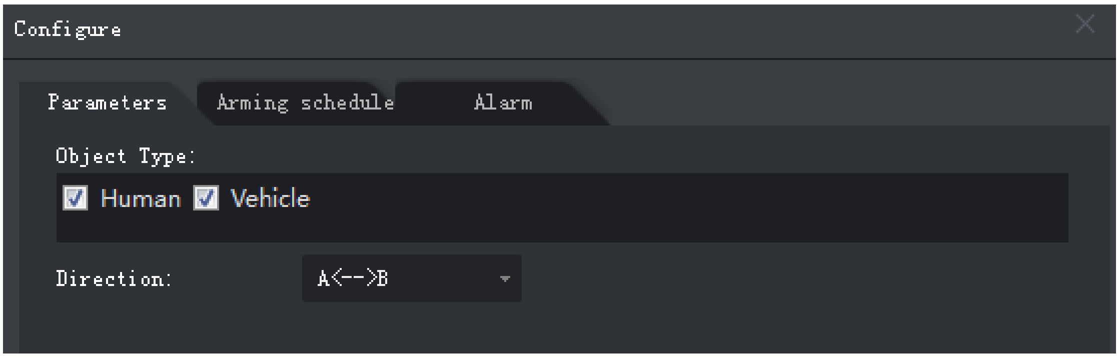
Step 3 Draw a line on the video and right-click to finish.

Select an existing tripwire line and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage.

1) Click **Config** and set parameters. See Figure 3-130. See Table 3-30 for details.

Figure 3-130 Set parameters



Object Type:

☑ Human ☑ Vehicle

Direction: A<-->B

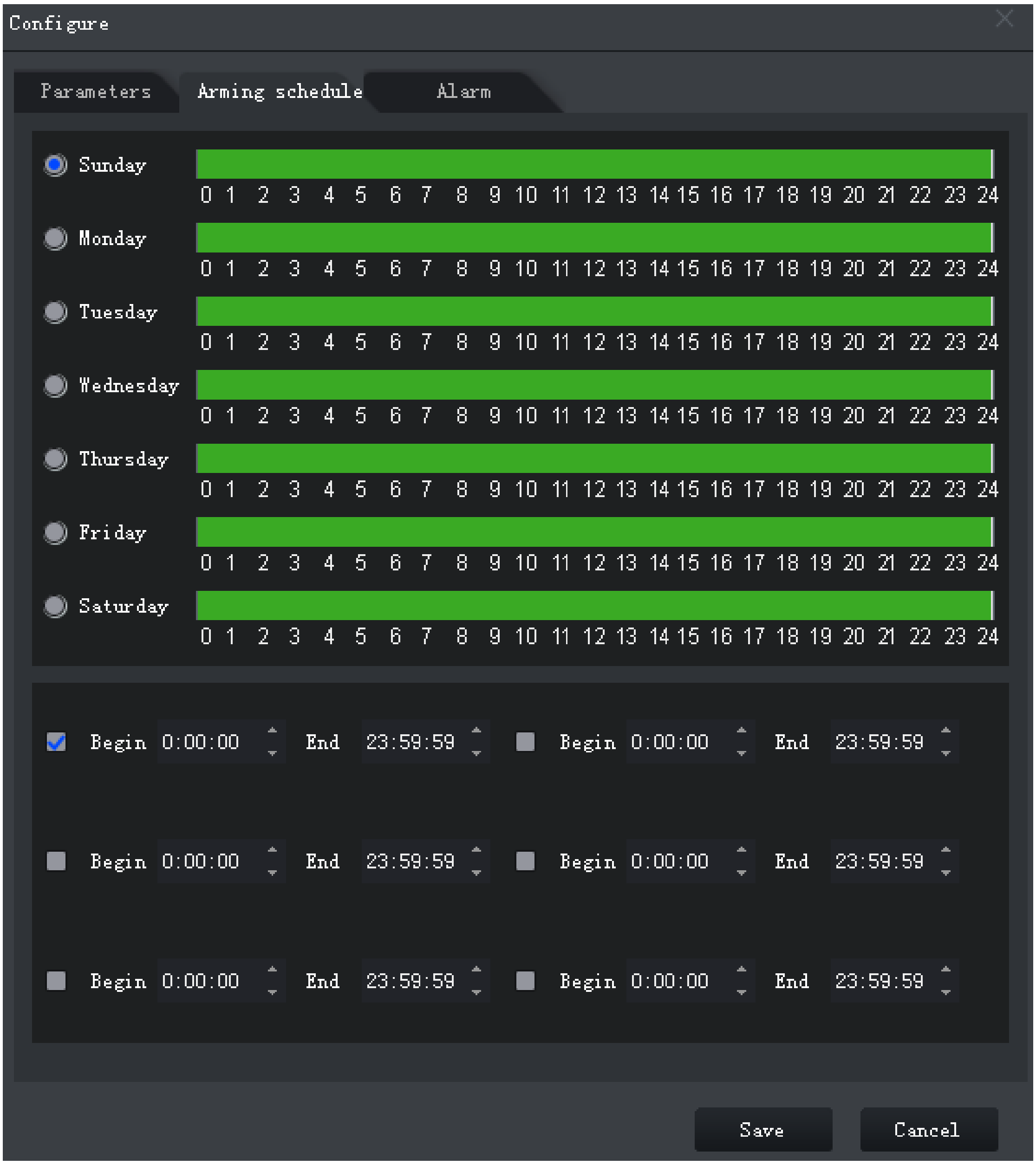
Table 3-30 Parameters

Parameter	Description
Object type	Only human or vehicle can trigger alarm.
Direction	When the target is moving in the rule direction, it is an intrusion. Directions include A→B, B→A and A↔B.

2) Click **Arming schedule**, select day and hours and then set the start time and end time. See Figure 3-131.

The default arming schedule is 24 hours per day.

Figure 3-131 Arming schedule

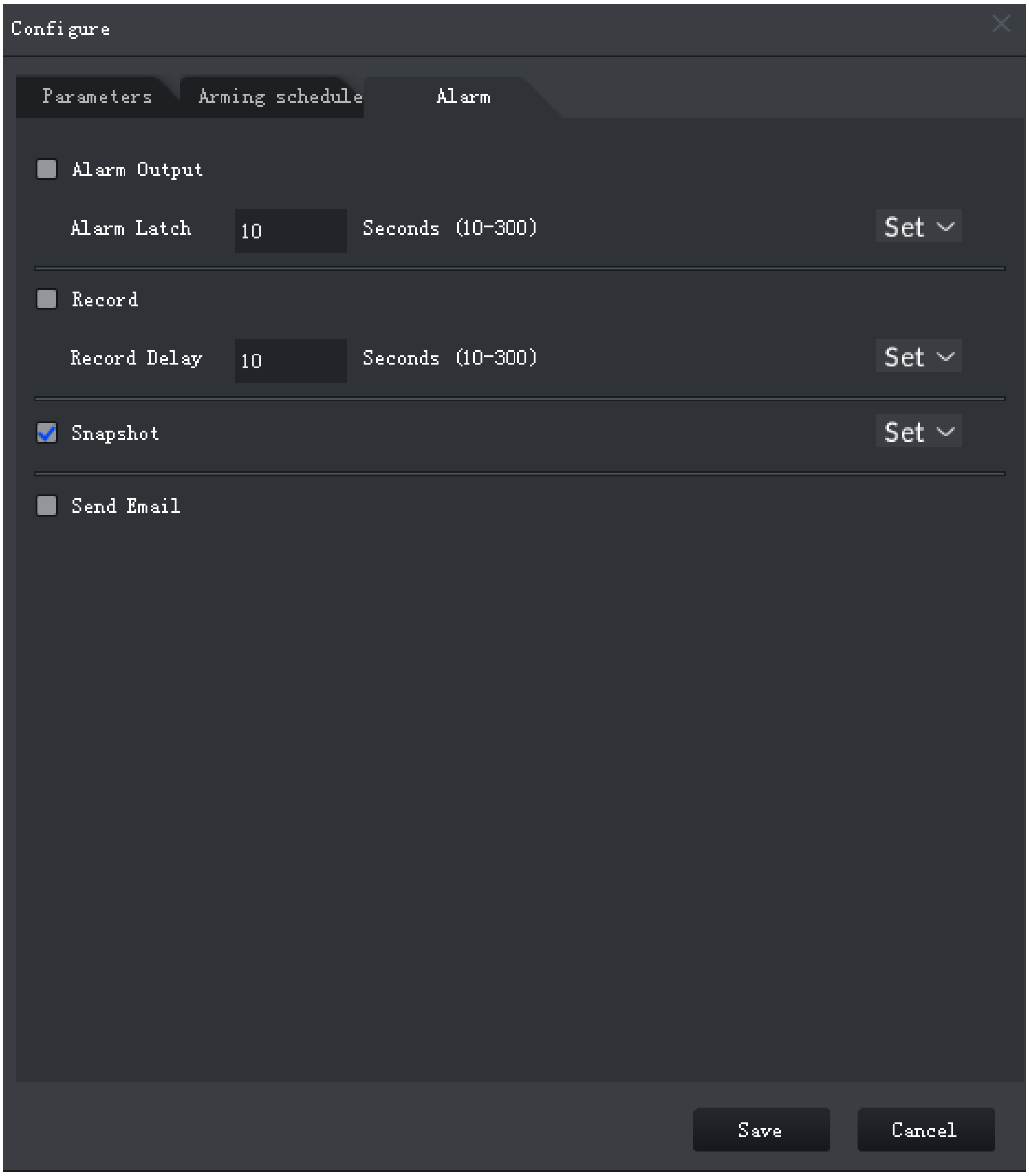

Configure
Parameters
Arming schedule
Alarm
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Save
Cancel

● Sunday
○ Monday
○ Tuesday
○ Wednesday
○ Thursday
○ Friday
○ Saturday

☑ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59
☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59
☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

3) Click **Alarm**, and then set linkage actions. See Figure 3-132. See Table 3-31 for details.

Figure 3-132 Alarm linkage



☐ Alarm Output

Alarm Latch: 10 Seconds (10-300)

☐ Record

Record Delay: 10 Seconds (10-300)

☑ Snapshot

☐ Send Email

Configure
Parameters
Arming schedule
Alarm
Set
Set
Set
Save
Cancel

Table 3-31 Parameters

Parameter	Description	
Alarm output	Connect alarm output devices to the alarm output interfaces. When an alarm is triggered, the system will send the alarm to the alarm output device.	Click **Set** next to **Alarm Latch** and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the alarm event ends.	

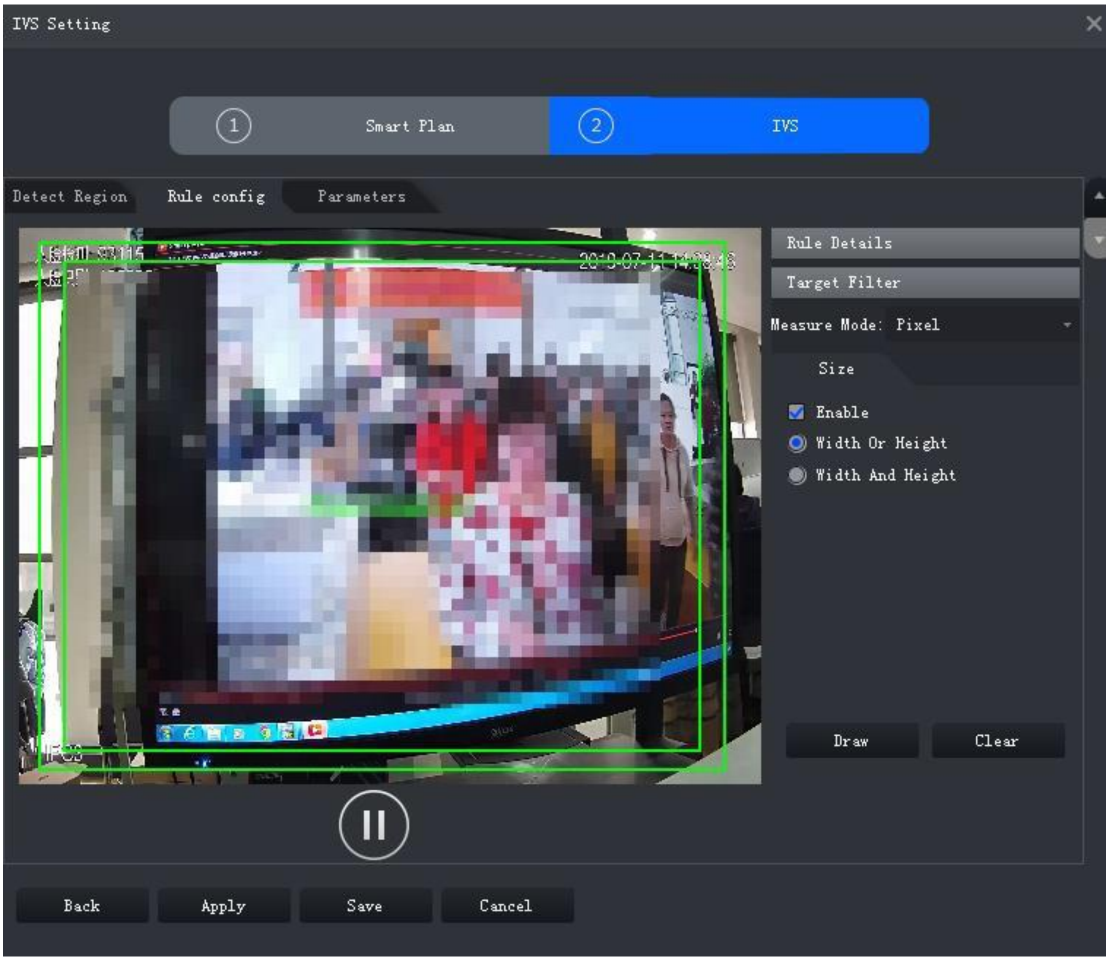
Parameter	Description	
Record	When an alarm happens, it will trigger video recording immediately. 📖 It requires the device to have recording schedules already. See device manual for detailed instruction.	Click **Set** next to **Record** and select an alarm output channel.
Record delay	Video recording delays stopping for a while after the alarm event ends.	
snapshot	The system will take snapshots automatically when an alarm happens. 📖 It requires the device to have snapshot schedules already. See device manual for detailed instruction.	Click **Set** next to **Snapshot** to select the snapshot channel.
Send email	The system will send an email to the related mail address when an alarm happens. 📖 It requires the device to have email configured already. See device manual for detailed instruction.	

4) Click **Save**.

Step 5 Draw target-filtering frame. See Figure 3-133

The filtering frame is used to filter targets that are too big or too small. When the target size is within the preset value, it can trigger alarm.

Figure 3-133 Target filtering


IVS Setting
1 Smart Plan
2 IVS
Detect Region
Rule config
Parameters
Rule Details
Target Filter
Measure Mode: Pixel
Size
☑ Enable
● Width Or Height
○ Width And Height
Draw
Clear
Back
Apply
Save
Cancel

1) Click **Target Filter**.
2) Select **Enable**.
3) Select a filtering method, **Width or Height** or **Width and Height**. Select filtering frame and drag the frame corners to adjust the size.

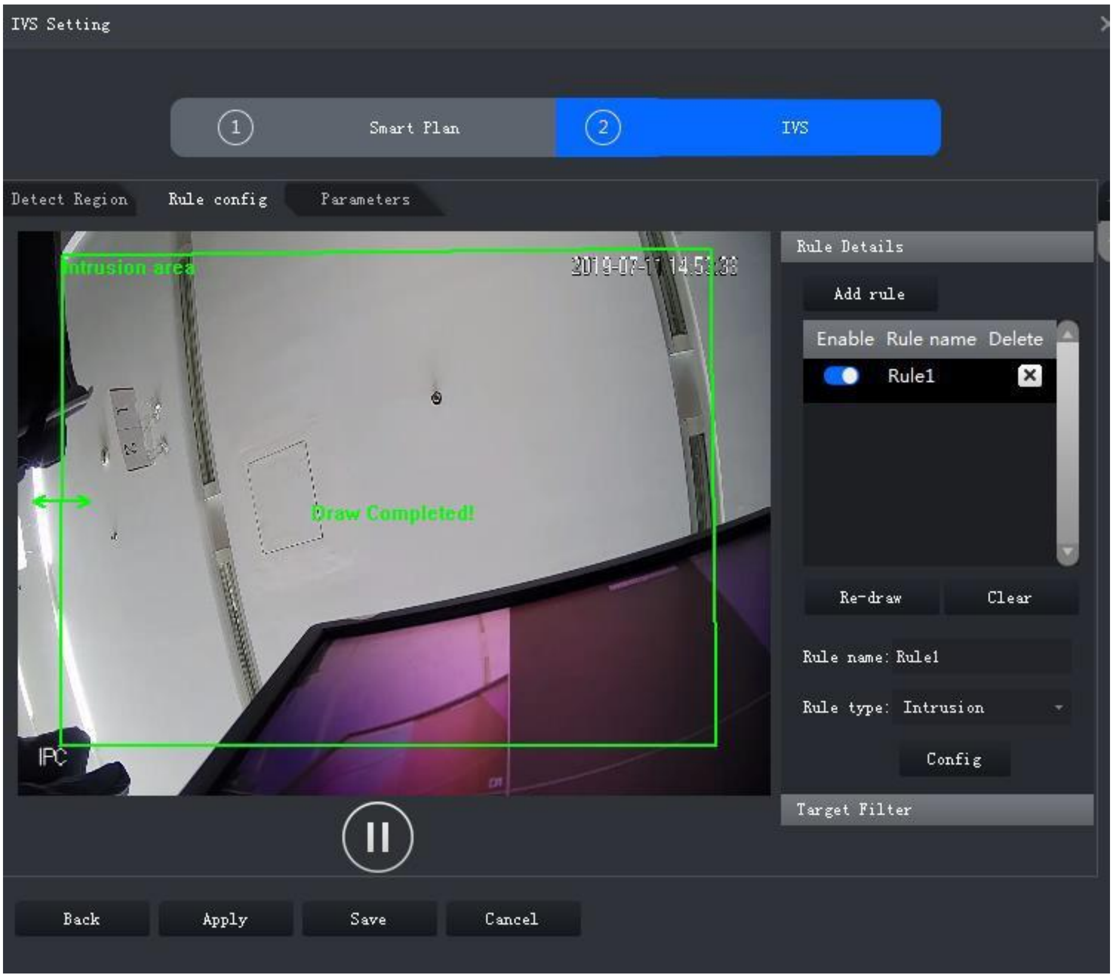
Select filtering frame, and click **Clear** to delete it.

Step 6 Click **Apply**.

3.6.2.4.3 Intrusion

When a target is detected entering or leaving an area, an alarm will be triggered.

Figure 3-134 Intrusion


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Rule config
Parameters
Intrusion area
2019-07-17 14:53:33
Draw Completed!
IPC
Rule Details
Add rule
Enable
Rule name
Delete
Rule1
Re-draw
Clear
Config
Target Filter
Back
Apply
Save
Cancel

Rule name: Rule1

Rule type: Intrusion

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. indicates rule is enabled.

2) Modify **Rule name**.

3) Select **Intrusion** in the dropdown list of **Rule type**.

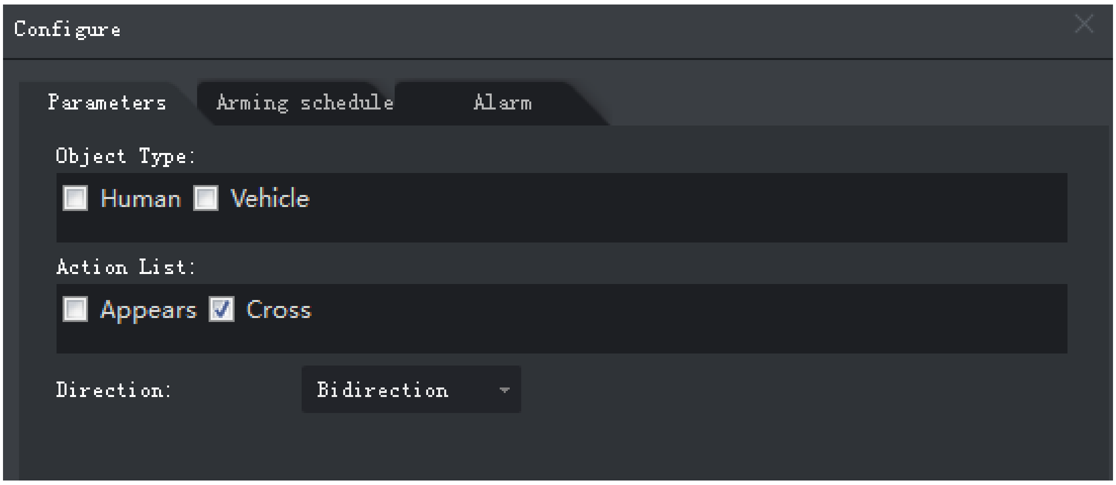
Step 3 Draw a detection zone on the video and right-click to finish.

Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.6.2.4.2 Tripwire."

Set intrusion detection parameters. See Figure 3-135. For details, see Table 3-32.

Figure 3-135 Set parameters



Object Type:

☐ Human ☐ Vehicle

Action List:

☐ Appears ☑ Cross

Direction: Bidirection

Table 3-32 Parameters

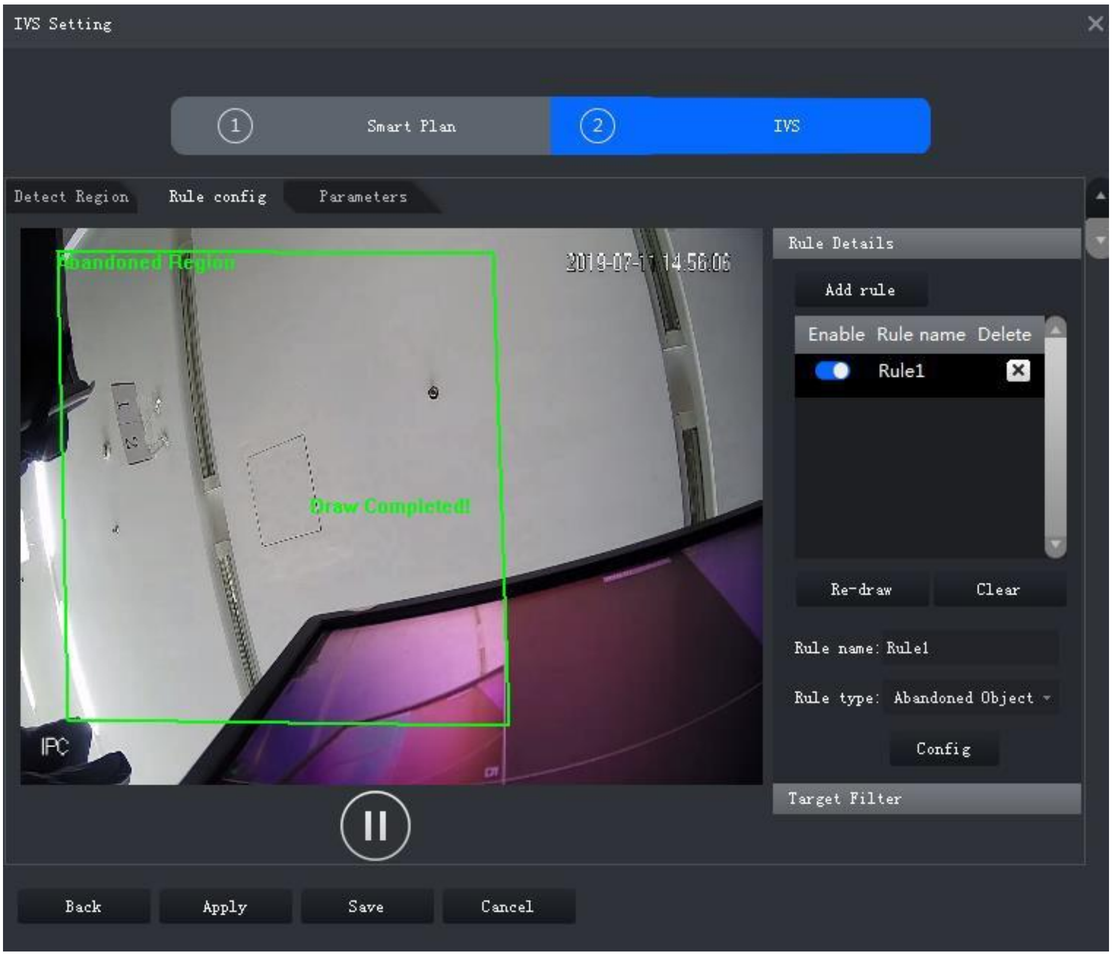
Parameter	Description
Object type	Only human or vehicle can trigger alarm.
Target actions	Appear and cross
Direction	When a crossing-zone action is selected, **Direction** setting will be effective. Direction includes entering zone, leaving zone and two-way.

Step 5 Click **Apply**.

3.6.2.4.4 Abandoned Object

When an object appears and stays in the detection area for a time period, system will trigger an alarm.

Figure 3-136 Abandoned Object


IVS Setting
1 Smart Plan
2 IVS
Detect Region
Rule config
Parameters
Abandoned Region
2019-07-17 14:56:06
Draw Completed!
IPC
Rule Details
Add rule
Enable
Rule name
Delete
Re-draw
Clear
Config
Target Filter
Back
Apply
Save
Cancel

Rule1

Rule name: Rule1

Rule type: Abandoned Object

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. indicates rule is enabled.
2) Modify **Rule name**.
3) Select **Abandoned Object** in the dropdown list of **Rule type**.

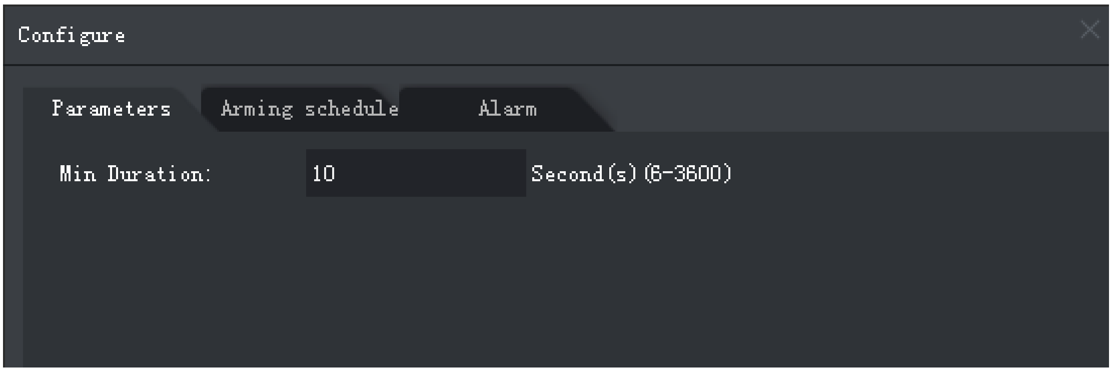
Step 3 Draw a detection zone on the video and right-click to finish.

Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.6.2.4.2 Tripwire."

Set parameters. See Figure 3-137. For details, see Table 3-33.

Figure 3-137 Set parameters


Configure
Parameters
Arming schedule
Alarm

Min Duration: 10 Second(s) (6-3600)

Table 3-33 Parameters

Parameter	Description
Minimum duration	The minimum time period between appearing and alarm triggering.

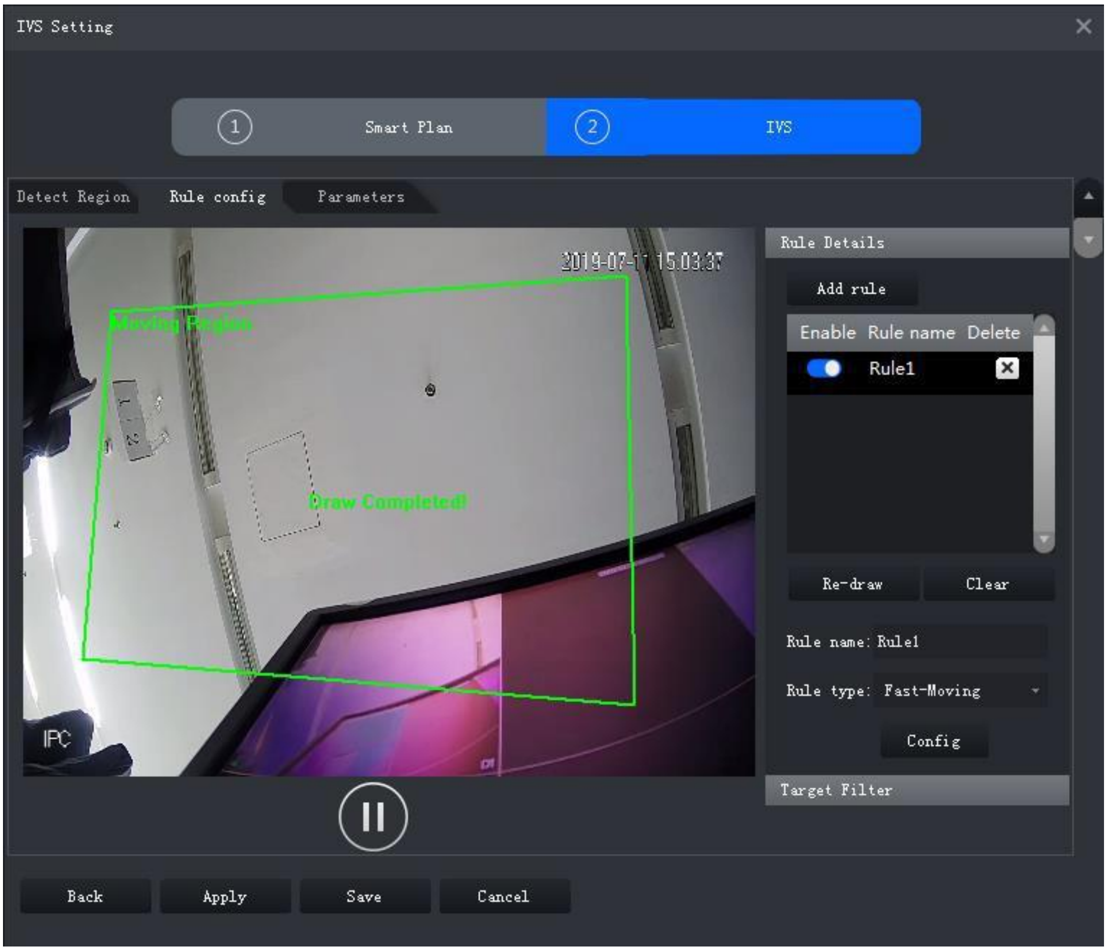
Step 5 Click **Apply**.

3.6.2.4.5 Fast Moving

When a target appears and its moving speed is or exceeds the preset value for the preset time period, system will trigger an alarm.

To ensure the accuracy of fast moving detection, make sure you have completed the calibration configuration. See "3.6.2.2 Calibrating Depth of Field for details."

Figure 3-138 Fast moving


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Rule config
Parameters
2019-07-17 15:03:37
Moving Region
Draw Completed!
IPC
Rule Details
Add rule
Enable Rule name Delete
Rule1
Re-draw
Clear
Config
Target Filter
Back
Apply
Save
Cancel

Rule name: Rule1

Rule type: Fast-Moving

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. ● indicates rule is enabled.

2) Modify **Rule name**.

3) Select **Fast-Moving** in the dropdown list of **Rule type**.

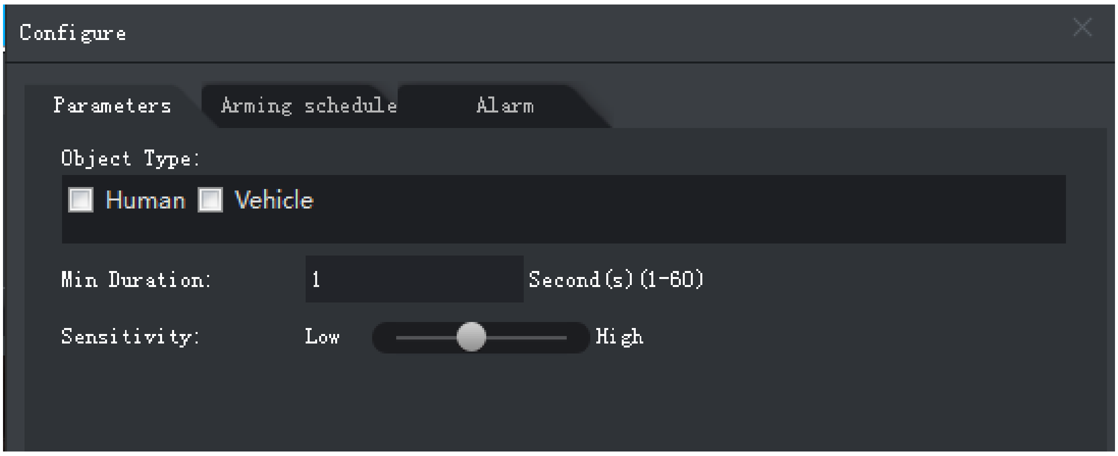
Step 3 Draw a detection zone on the video and right-click to finish.

Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.6.2.4.2 Tripwire."

See Figure 3-139 for fast moving parameters. For details, see Table 3-34.

Figure 3-139 Set parameters



Object Type:

☐ Human ☐ Vehicle

Min Duration: 1 Second(s)(1-60)

Sensitivity: Low High

Table 3-34 Parameters

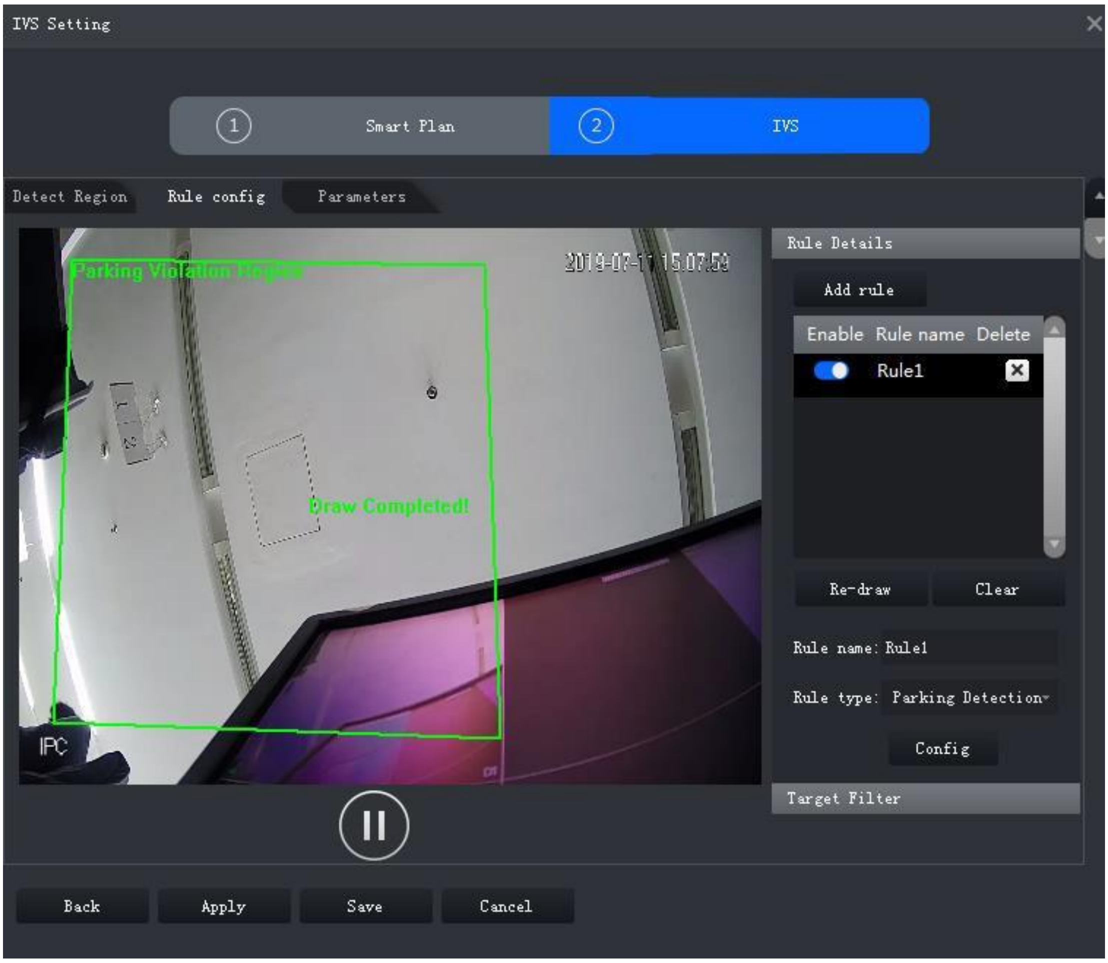
Parameter	Description
Object type	Only human or vehicle can trigger alarm.
Minimum duration	The minimum duration of fast moving in the detection zone.
Sensitivity	It is recommended to keep the default value.

Step 5 Click **Apply**.

3.6.2.4.6 Parking Detection

When a vehicle is detected parking in an area, an alarm will be triggered.

Figure 3-140 Parking detection


IVS Setting
1 Smart Plan
2 IVS
Detect Region
Rule config
Parameters
Parking Violation Region
2019-07-11 15:07:59
Draw Completed!
IPC
Rule Details
Add rule
Enable
Rule name
Delete
Re-draw
Clear
Config
Target Filter
Back
Apply
Save
Cancel

Rule1

Rule name: Rule1

Rule type: Parking Detection

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. ● indicates rule is enabled.
2) Modify **Rule name**.
3) Select **Parking Detection** in the dropdown list of **Rule type**.

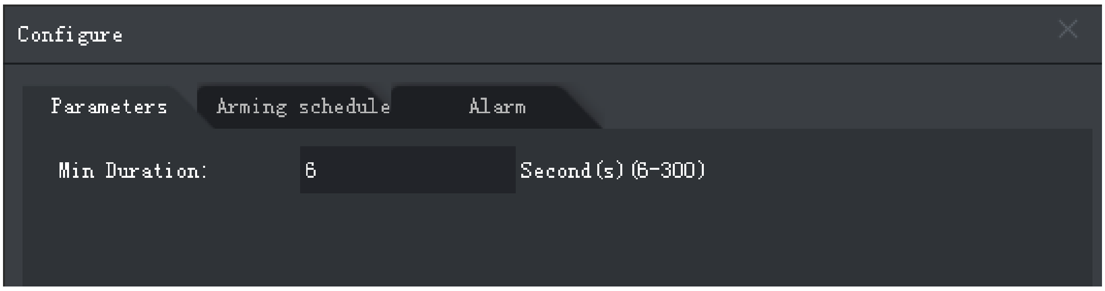
Step 3 Draw a detection zone on the video and right-click to finish.

Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.6.2.4.2 Tripwire."

Set parameters. See Figure 3-141. For details, see Table 3-35.

Figure 3-141 Set parameters


Configure
Parameters
Arming schedule
Alarm

Min Duration: 6 Second(s) (6-300)

Table 3-35 Parameters

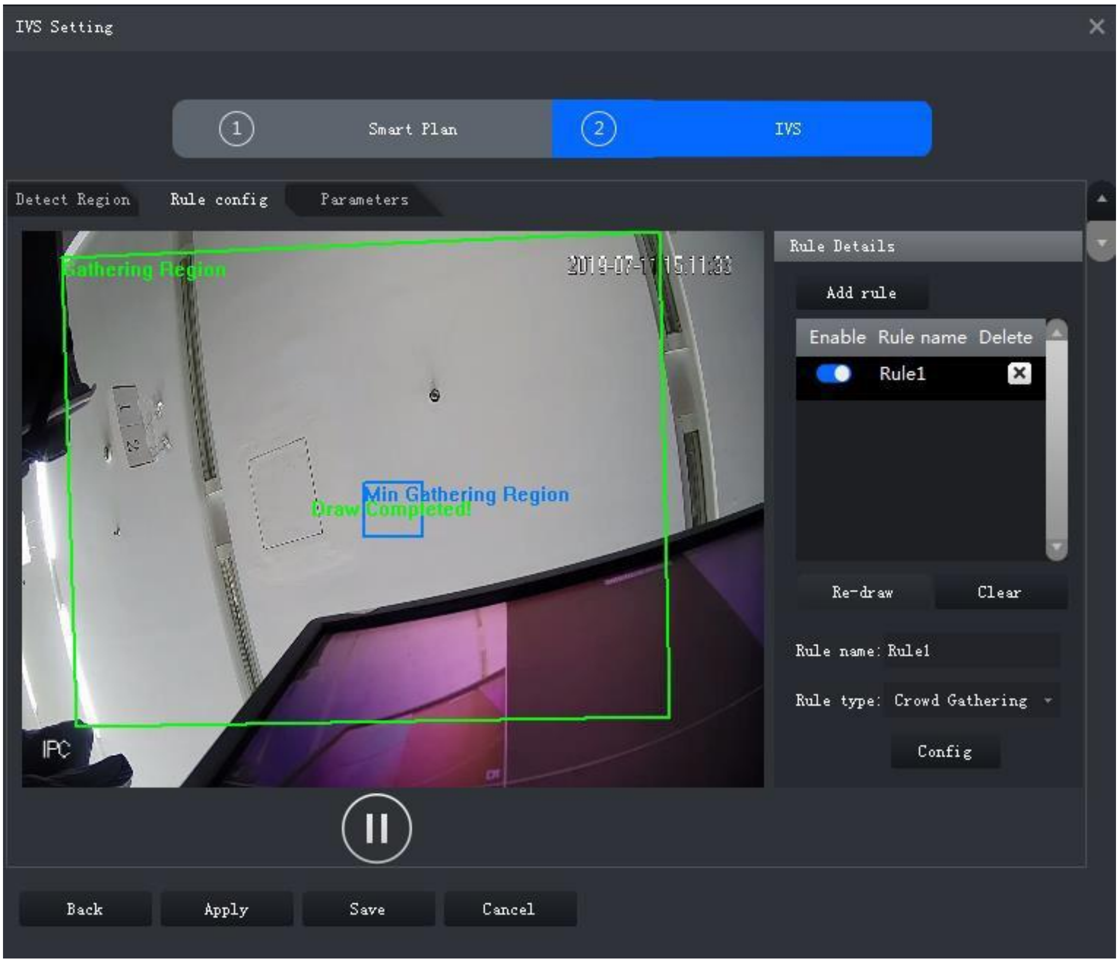
Parameter	Description
Minimum duration	The minimum time duration from parking to alarm triggering.

Step 5 Click **Apply**.

3.6.2.4.7 Crowd Gathering

When the people crowd size in the detection zone exceeds the preset value, system will trigger an alarm.

Figure 3-142 Crowd gathering


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Rule config
Parameters
Gathering Region
2019-07-17 15:11:33
Min Gathering Region
Draw Completed!
IPC
Rule Details
Add rule
Enable
Rule name
Delete
Rule1
Re-draw
Clear
Config
Back
Apply
Save
Cancel

Rule name: Rule1

Rule type: Crowd Gathering

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. ● indicates rule is enabled.

2) Modify **Rule name**.

3) Select **Crowd Gathering** in the dropdown list of **Rule type**.

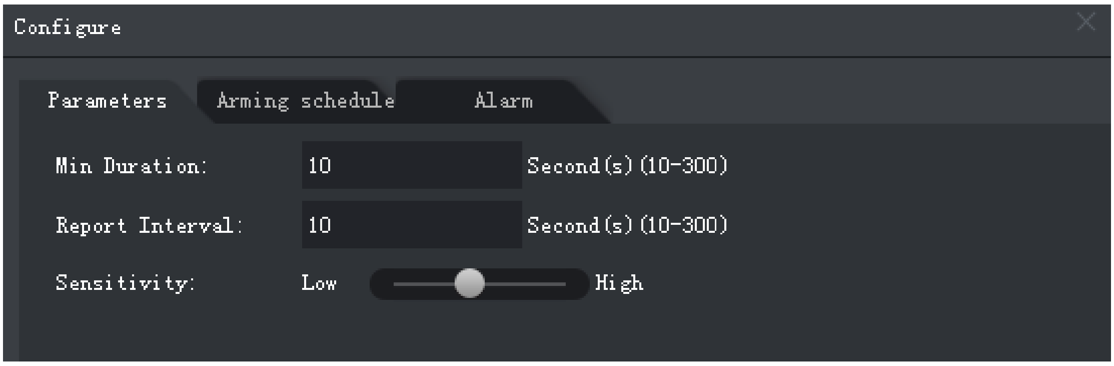
Step 3 Draw a detection zone on the video and right-click to finish. Click the **Min Gathering Region** and drag the zone corners to adjust the size.

Select an existing zone or the minimum gathering region and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.6.2.4.2 Tripwire."

Set parameters. See Figure 3-143. For details, see Table 3-36.

Figure 3-143 Set parameters



Min Duration: 10 Second(s)(10-300)

Report Interval: 10 Second(s)(10-300)

Sensitivity: Low High

Table 3-36 Parameters

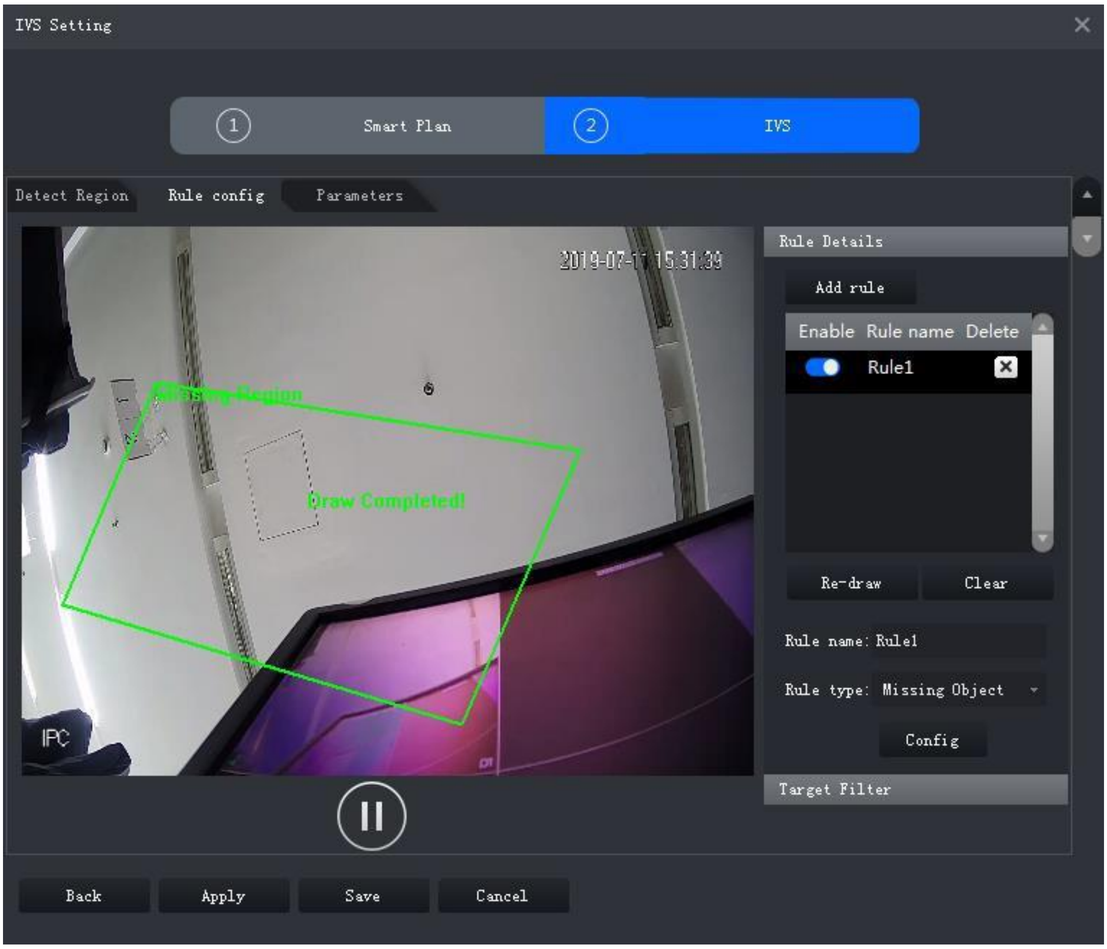
Parameter	Description
Minimum duration	The minimum duration from the time crowd gathering being detected to alarm triggering
Report interval	If the event still exists after the first alarm, system will trigger more alarms by the preset alarm interval.
Sensitivity	It is recommended to keep the default value.

Step 5 Click **Apply**.

3.6.2.4.8 Missing Object

If an object has been moved out of the detection zone and not put back anymore for a certain time period, system will trigger an alarm.

Figure 3-144 Missing object


IVS Setting
1 Smart Plan
2 IVS
Detect Region
Rule config
Parameters
2019-07-11 15:31:39
Missing Region
Draw Completed!
IPC
Rule Details
Add rule
Enable
Rule name
Delete
Re-draw
Clear
Config
Target Filter
Back
Apply
Save
Cancel

Rule1

Rule name: Rule1

Rule type: Missing Object

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. ● indicates rule is enabled.

2) Modify **Rule name**.

3) Select **Missing Object** in the dropdown list of **Rule type**.

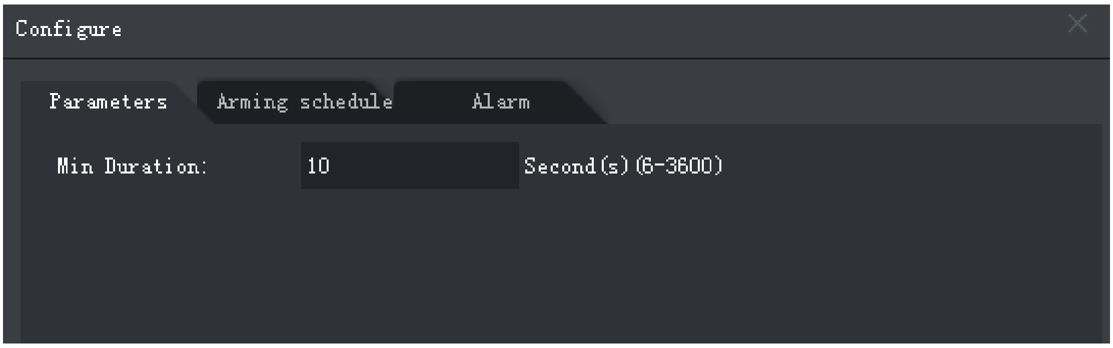
Step 3 Draw a detection zone on the video and right-click to finish.

Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See 3.6.2.4.2Tripwire.

Set parameters. See Figure 3-145. For details, see Table 3-37.

Figure 3-145 Set parameters


Configure
Parameters
Arming schedule
Alarm

Min Duration: 10 Second(s)(6-3600)

Table 3-37 Parameters

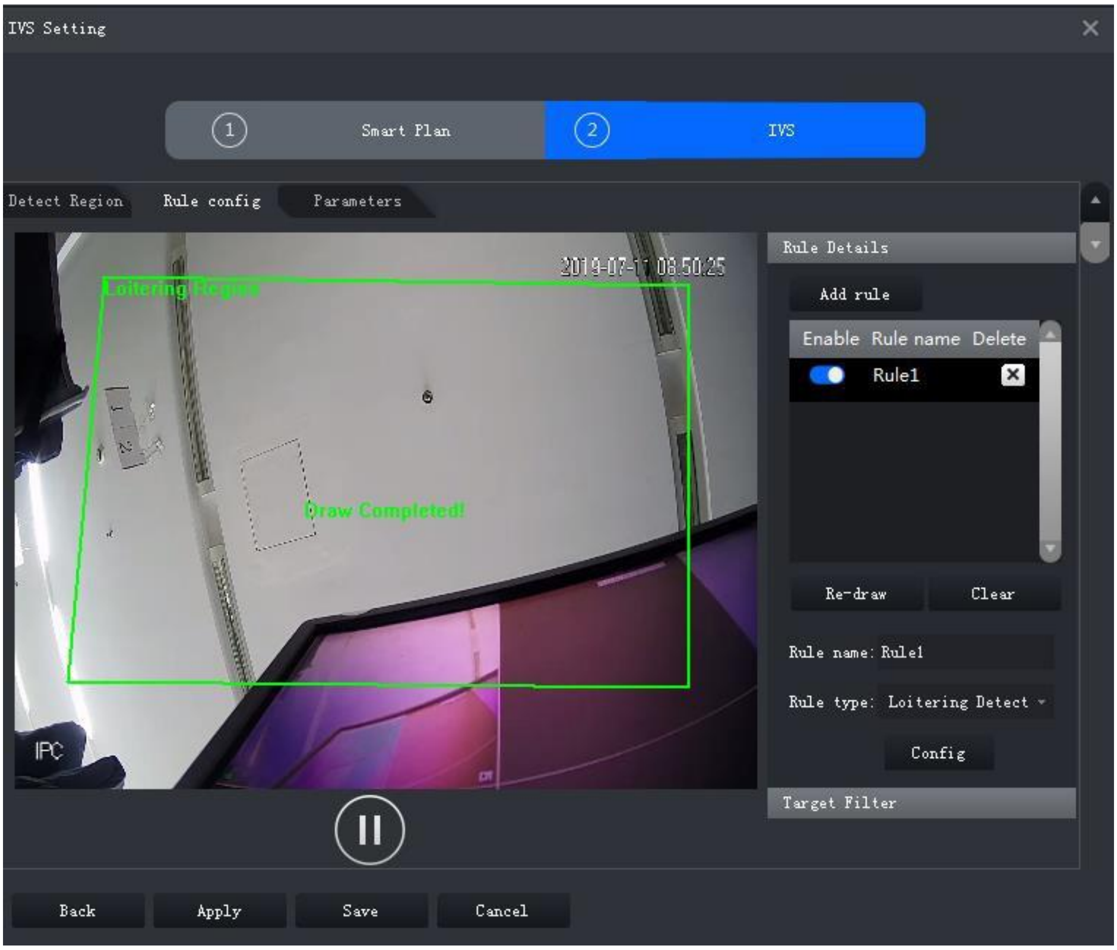
Parameter	Description
Minimum duration	The minimum time duration from object disappearing to alarm triggering.

Step 5 Click **Apply**.

3.6.2.4.9 Loitering Detection

When a target stays in the detection zone after appearing for a certain time period, an alarm will be triggered.

Figure 3-146 Loitering detection


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Rule config
Parameters
2019-07-11 08:50:25
Loitering Region
Draw Completed!
IPC
Rule Details
Add rule
Enable
Rule name
Delete
Rule1
Re-draw
Clear
Config
Target Filter
Back
Apply
Save
Cancel

Rule name: Rule1

Rule type: Loitering Detect

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. ● indicates rule is enabled.

2) Modify **Rule name**.

3) Select **Loitering Detect** in the dropdown list of **Rule type**.

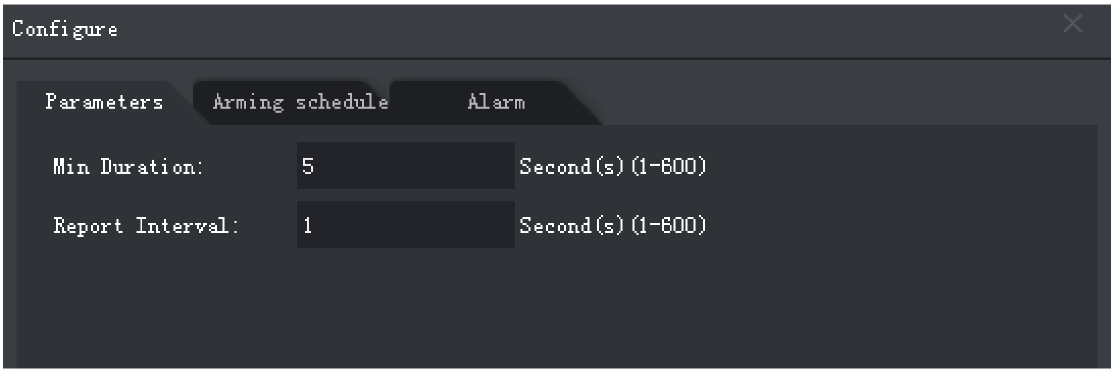
Step 3 Draw a detection zone on the video and right-click to finish.

Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See 3.6.2.4.2 Tripwire.

Set parameters. See Figure 3-147. For details, see Table 3-38.

Figure 3-147 Set parameters



Min Duration: 5 Second(s)(1-600)

Report Interval: 1 Second(s)(1-600)

Table 3-38 Parameters

Parameter	Description
Minimum duration	The minimum time duration from target appearing to alarm triggering.
Report interval	If the event still exists after the first alarm, system will trigger more alarms by the preset alarm interval.

Step 5 Click **Apply**.

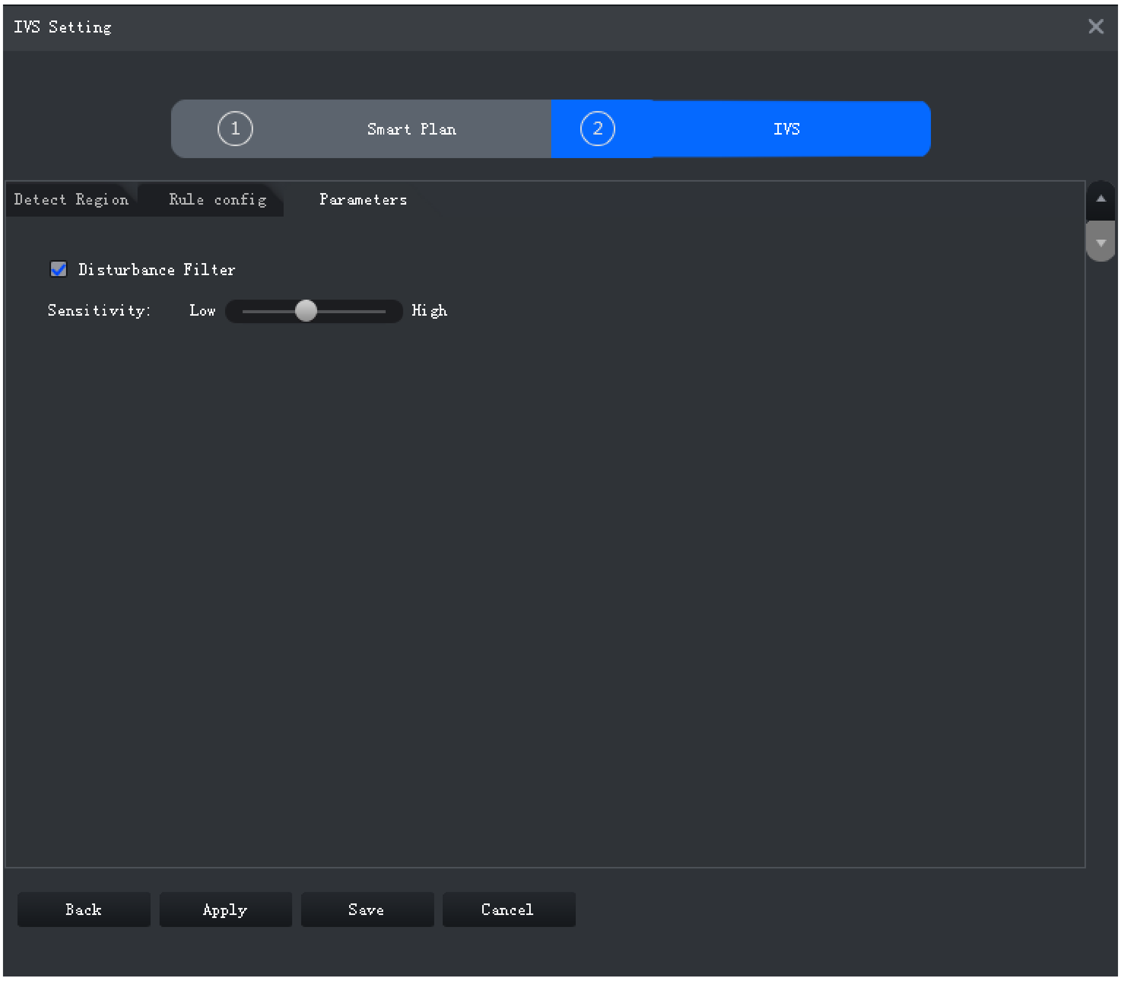
3.6.2.5 Setting Parameters

Set common parameters for the IVS, including disturbance filter and sensitivity.

Step 1 Click **Parameters** after configuring rules in the **Rule config** interface.

The interface of **Parameters** is displayed. See Figure 3-148.

Figure 3-148 Parameters



☑ Disturbance Filter

Sensitivity: Low ● High

Step 2 See Table 3-39 for details.

Table 3-39 Parameters

Parameter	Description
Disturbance filter	Filter false targets including waving plants and water waves. This function may cause target omissions as some parts of a true target may be judged as false factors.
Sensitivity	Control detection sensitivity. The smaller the value is, the lower the false detection rate will be and the higher omission rate will happen. The bigger the value is, the higher false detection rate will be and the lower the omission rate will happen.

Step 3 Click **Save**.

3.6.3 Face Detection

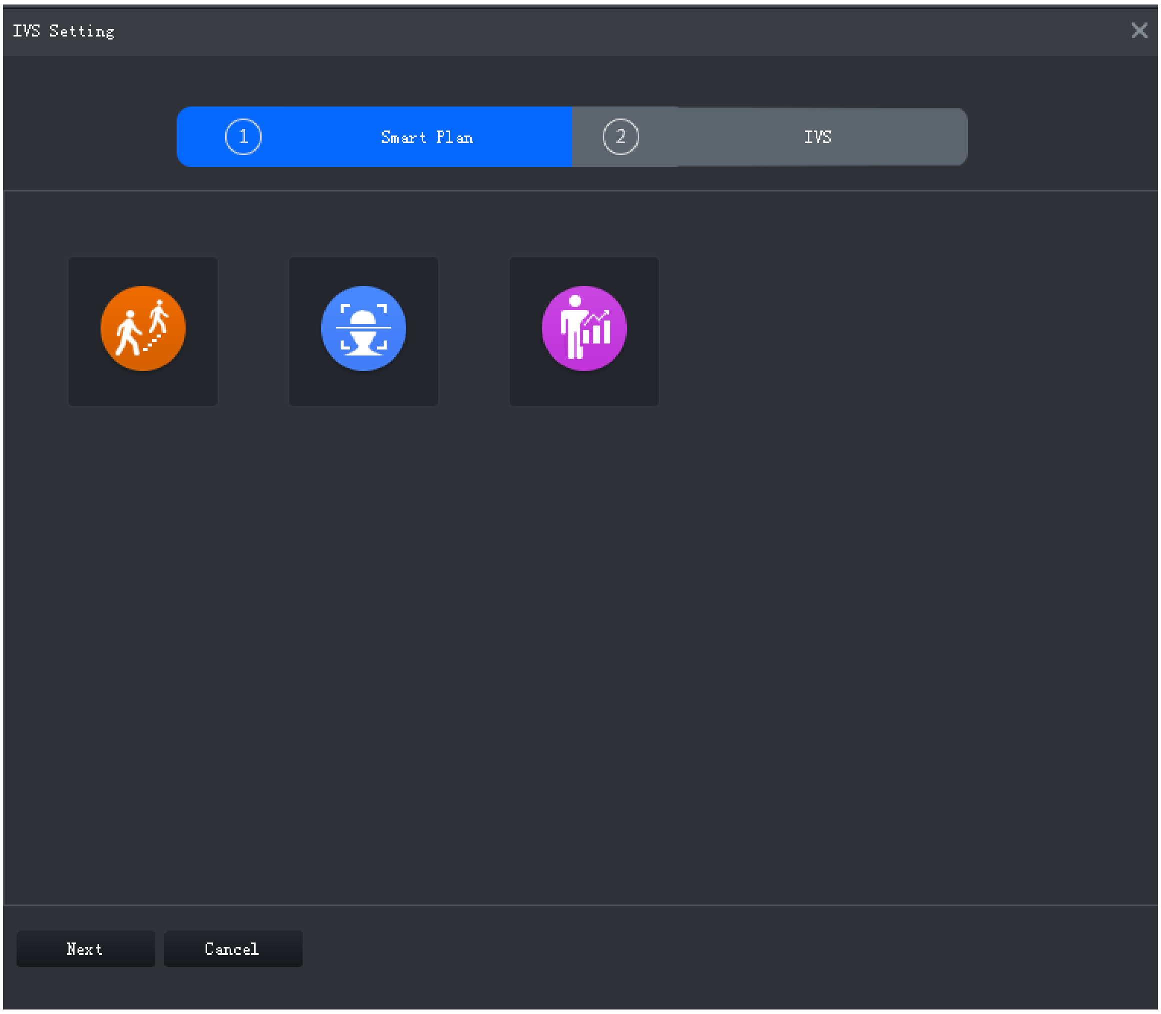
This function supports detecting human targets in the defined zone. It supports capturing and recognizing human face, and extracting face features including gender, age, expression and glasses.

3.6.3.1 Enabling Face Detection

Step 1 Go to the **Intelligent Analyse** interface.

Step 2 Click in the smart plan interface to select face detection. See Figure 3-149. When the icon is displayed in the white frame, it means the smart plan is selected. If another smart plan, which is conflicting with face detection, is selected already, click that smart plan icon to deselect it and then click to select face detection.

Figure 3-149 Smart plan



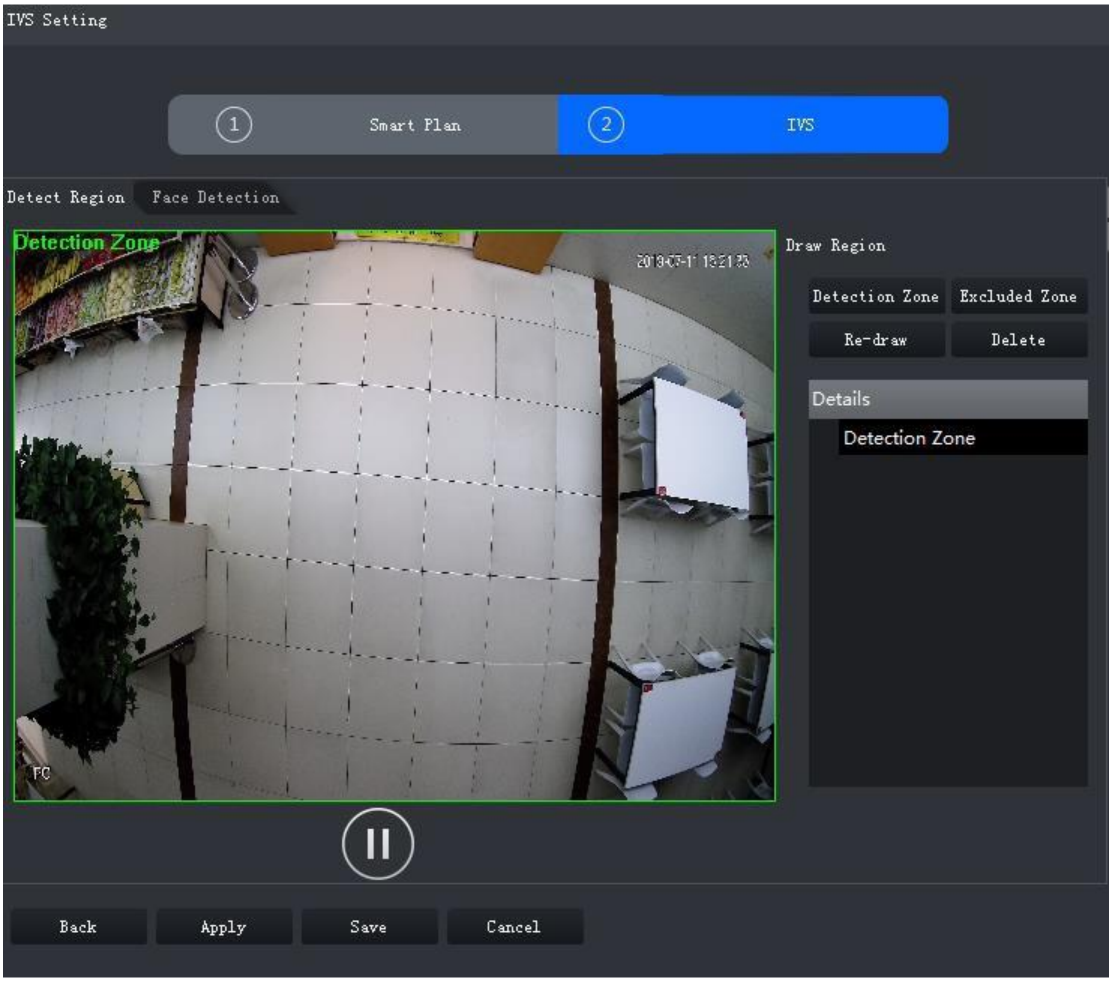
Step 3 Click **Next.**

The **IVS Setting** interface is displayed.

3.6.3.2 Configuring Detection Region

Configure the detection region.

Figure 3-150 Detection region


IVS Setting
1
Smart Plan
2
IVS
Detect Region
Face Detection
Detection Zone
Draw Region
Detection Zone
Excluded Zone
Re-draw
Delete
Details
Detection Zone
Back
Apply
Save
Cancel

Step 1 Click **Detect Region** tab in the interface of IVS.

The interface of **Detect Region** is displayed.

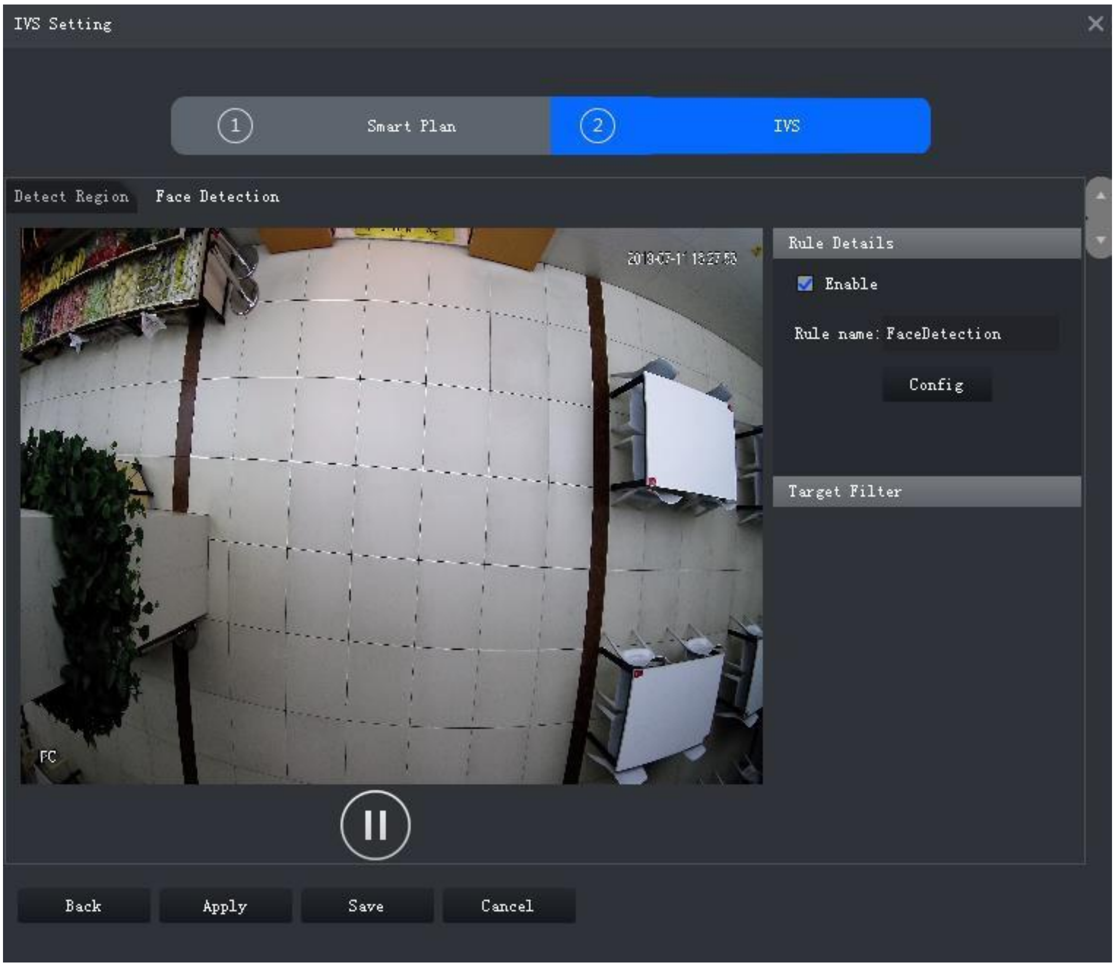
Step 2 Click **Detection Zone** and then draw the frame of the detection region on the video and right-click to finish.

Step 3 Click **Excluded Zone** and then draw the frame of the zone on the video and right-click to finish.

- Select the excluded zone and click **Re-draw** to draw a new excluded zone; select detection region and click **Re-draw** to draw a new detection region and a new excluded zone.
- Select the excluded zone and click **Delete** to delete the excluded zone; select detection region and click **Delete** to delete the detection region and excluded zone.

3.6.3.3 Configuring Face Detection Rule

Figure 3-151 Face detection


IVS Setting
1 Smart Plan
2 IVS
Detect Region
Face Detection
Rule Details
☑ Enable
Rule name: FaceDetection
Config
Target Filter
Back
Apply
Save
Cancel

Step 1 Select the check box of **Enable** to enable face detection.

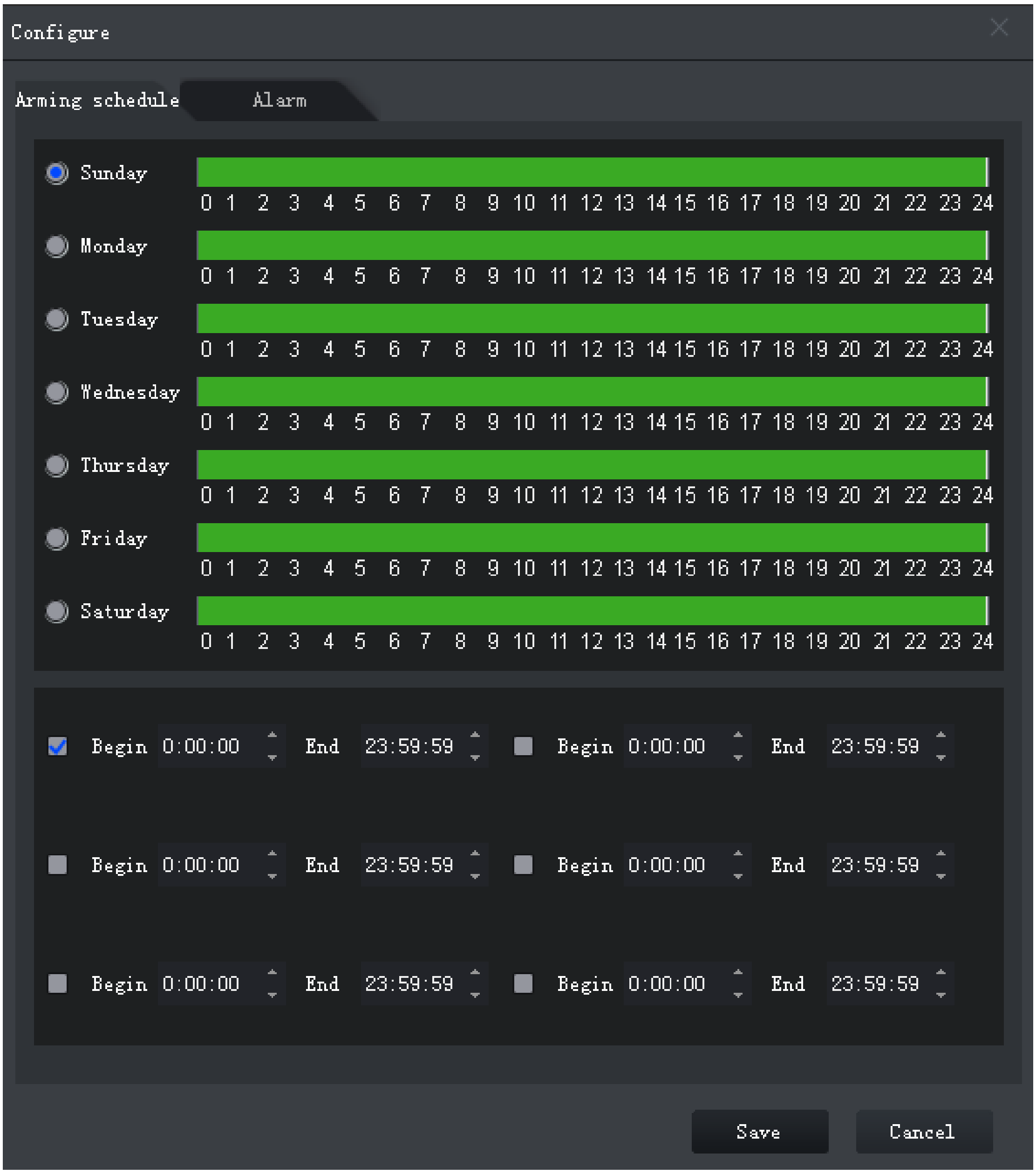
Step 2 Modify Rule name.

Step 3 Configuring arming schedule and alarm linkage.

1) Click **Config**.

   The system displays the interface of **Configure**. See Figure 3-152.

Figure 3-152 Configure


Configure
Arming schedule
Alarm
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Save
Cancel

● Sunday
○ Monday
○ Tuesday
○ Wednesday
○ Thursday
○ Friday
○ Saturday

☑ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

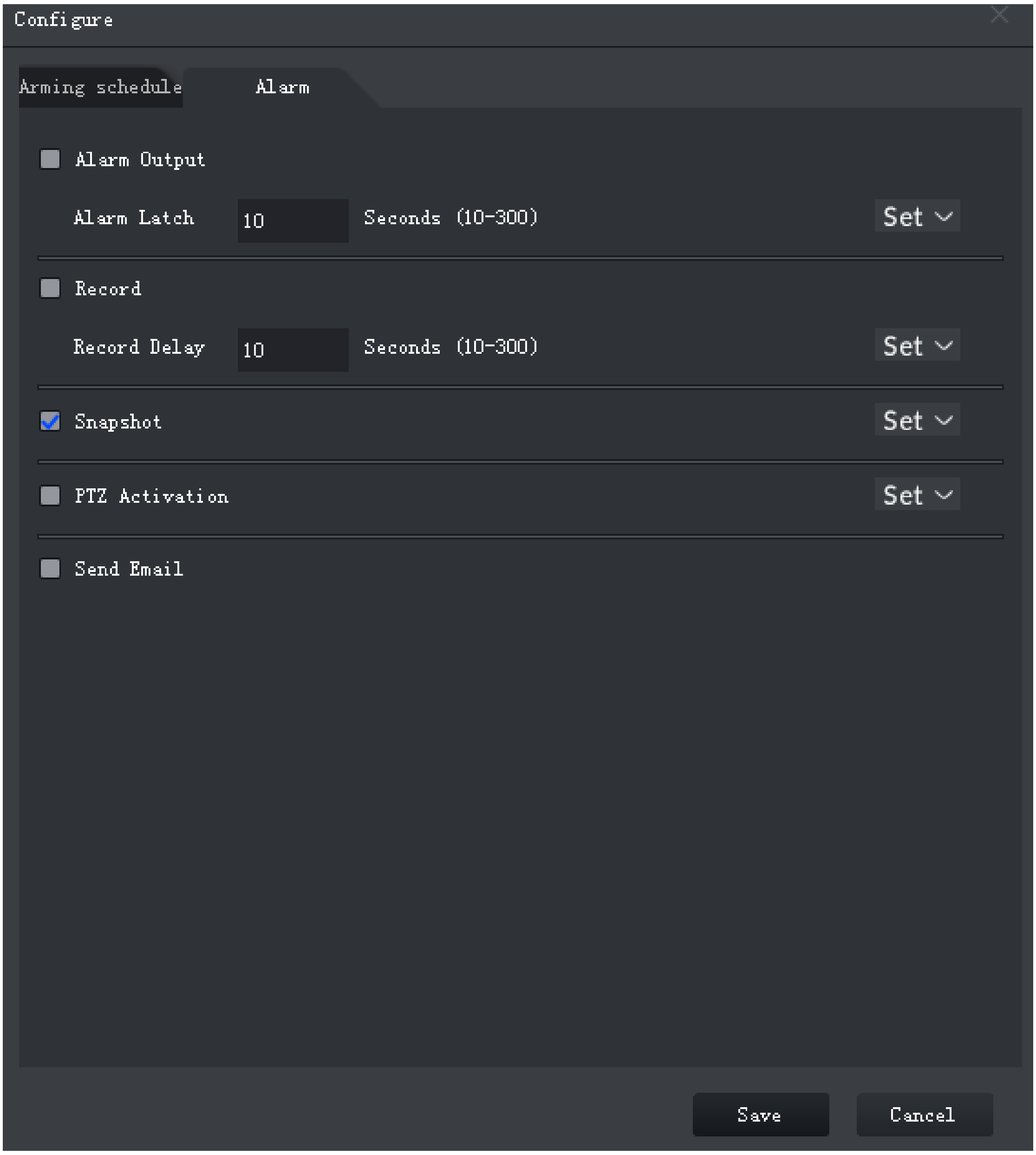
☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

2) Click **Arming schedule**, select day and hours and then set the start time and end time.

The default arming schedule is 24 hours per day.

3) Click **Alarm** to set linkage actions. See Figure 3-153. See Table 3-40 for details.

Figure 3-153 Alarm



☐ Alarm Output

Alarm Latch 10 Seconds (10-300)

☐ Record

Record Delay 10 Seconds (10-300)

☑ Snapshot

☐ PTZ Activation

☐ Send Email

Table 3-40 Parameters

Parameter	**Description**	
Alarm output	Connect alarm output devices to the alarm output interfaces. When an alarm is triggered, the system will send the alarm to the alarm output device.	Click **Set** next to **Alarm Latch** and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the the alarm event ends.	
Record	When an alarm happens, it will trigger auto video recording immediately. To get video records, set the recording schedule in adavance. See device manual for detailed instruction.	Click **Set** next to **Record** to select the recording channel.

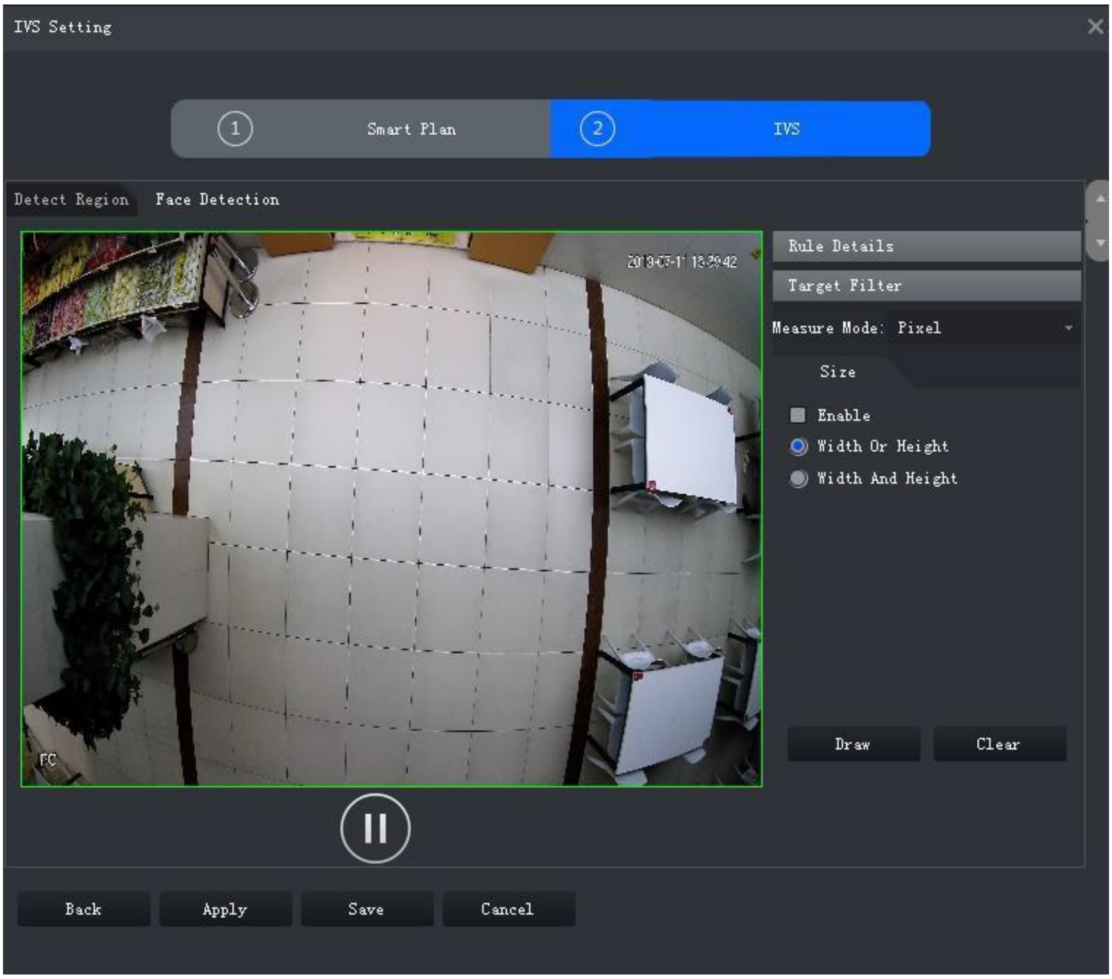
Parameter	Description	
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	The system will take snapshots automatically when an alarm happens. It requires the device to have snapshot schedules already. See device manual for detailed instruction.	Click **Set** next to **Snapshot** to select the snapshot channel.
Send email	The system will send an email to the related mail address when an alarm happens. It requires the device to have email configured already. See device manual for detailed instruction.	None

4) Click **Save**.

Step 4 Draw target-filtering frame. See Figure 3-154

The filtering frame is used to filter targets that are too big or too small. When the target size is within the setting value, it can trigger alarm.

Figure 3-154 Target filtering


IVS Setting
1 Smart Plan
2 IVS
Detect Region
Face Detection
2019-07-11 15:29:42
FC
Rule Details
Target Filter
Size
Draw
Clear
Back
Apply
Save
Cancel

Measure Mode: Pixel

☐ Enable

● Width Or Height

○ Width And Height

5) Select **Enable**.

6) Select a filtering method.

Two filtering methods:

- ◇ **Width or Height** means the target will be kept when either width or height meets the requirement.

- ◇ **Width and Height** means the target will be kept only when both width and height meet the requirement.

7) Click **Draw** and draw a filtering frame on the video.

Select filtering frame and drag the four angles adjust the size.

Select filtering frame, and click **Clear** to delete it.

Step 5 Click **Save**.

3.6.4 People Counting

Count the number of people entry and exit.

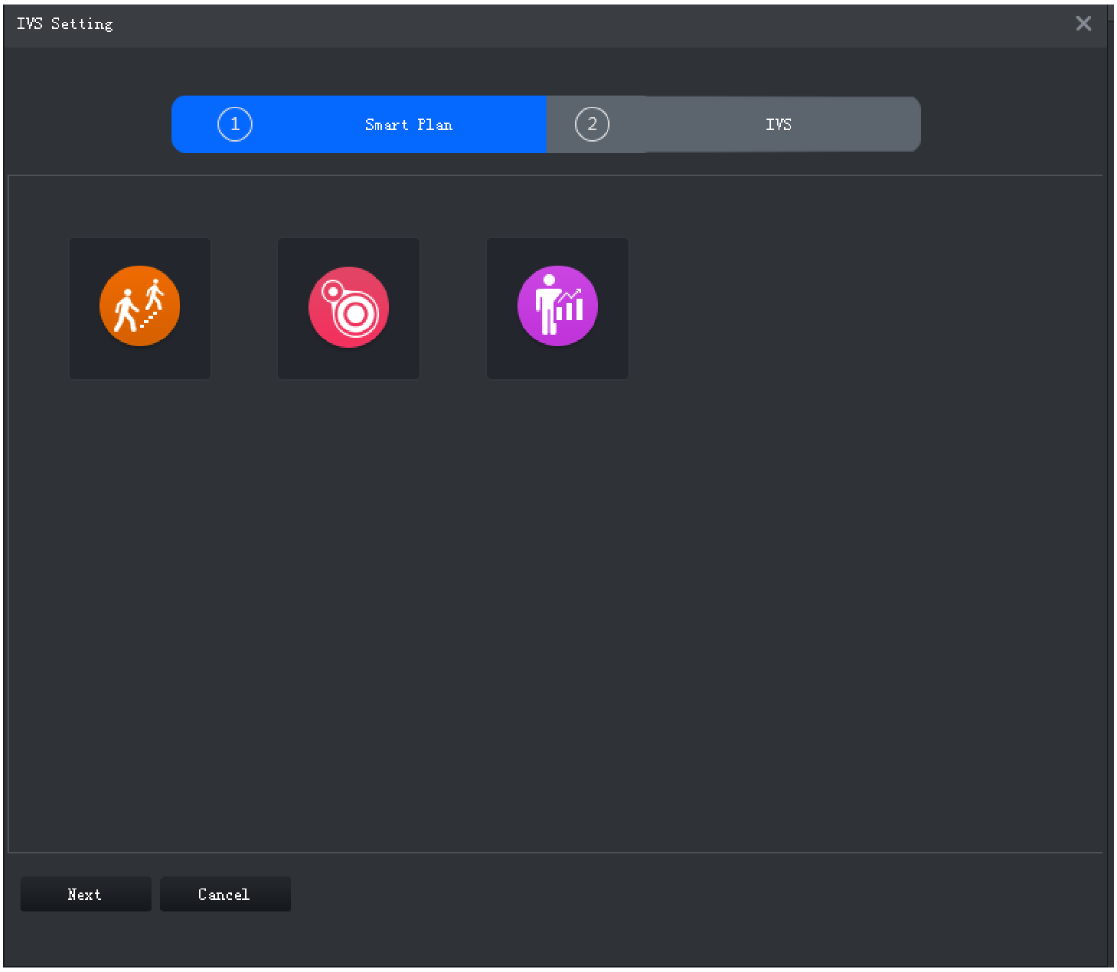
3.6.4.1 Enable People Counting

Step 1 Go into the **Intelligent Analyse** interface.

Step 2 Click to select people counting.

When the icon is displayed in the white frame, it means the smart plan is selected. If another smart plan, which is conflicting with people counting, is selected already, click that smart plan icon to deselect it and then click to select people counting.

Figure 3-155 Smart plan

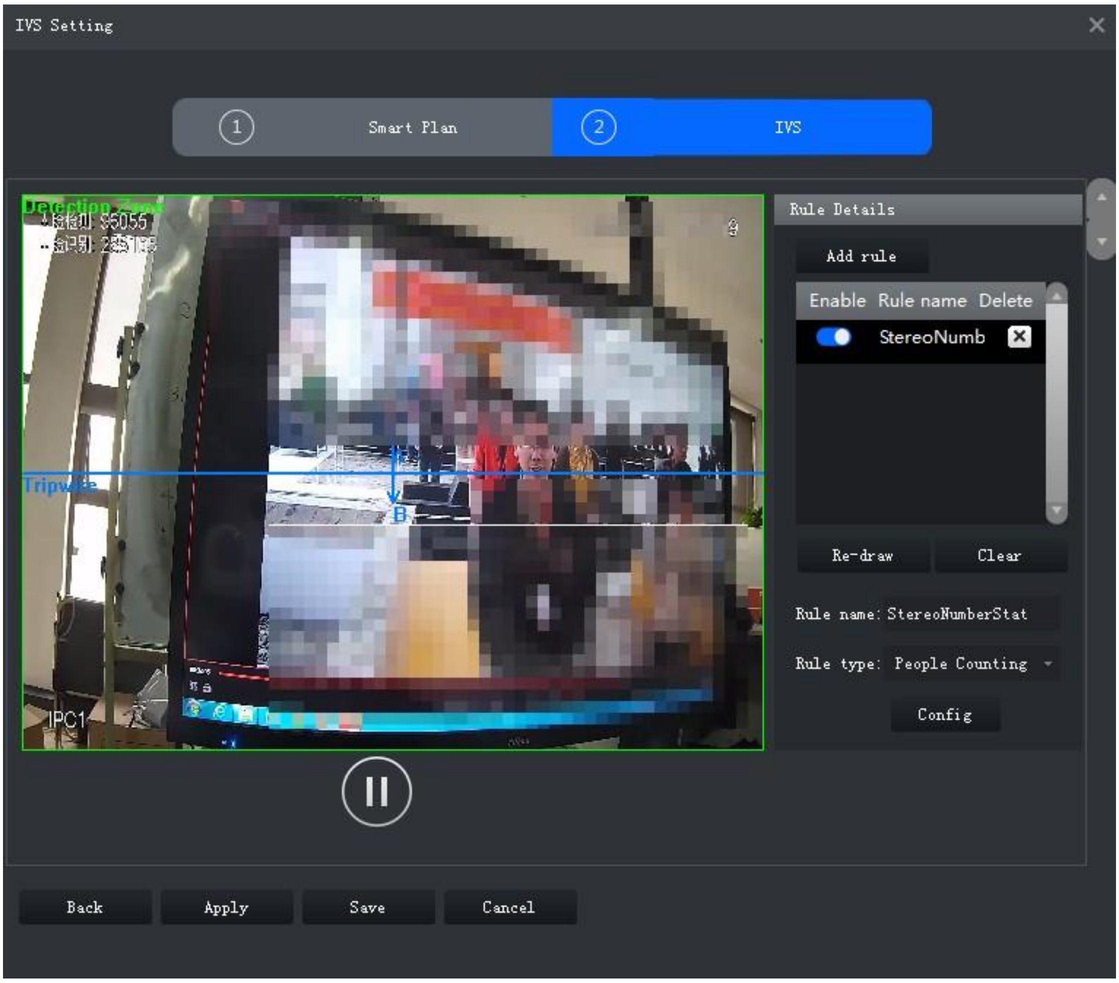

IVS Setting
1
Smart Plan
2
IVS
Next
Cancel

Step 3 Click **Next**.

The **IVS Setting** interface is displayed.

3.6.4.2 Configuring People Counting Rule

Figure 3-156 People counting


IVS Setting
1
Smart Plan
2
IVS
Detection Zone
Tripwire
B
IPC1
Rule Details
Add rule
Enable
Rule name
Delete
StereoNumb
Re-draw
Clear
Config
Back
Apply
Save
Cancel

Rule name: StereoNumberStat

Rule type: People Counting

Step 1 Click Add rule.

Step 2 Enable rule and modify the name and type.

1) Enable rule. ● indicates rule is enabled.
2) Modify **Rule name**.
3) Select rule type in the dropdown list of **Rule type**.
   - ◇ **People Counting**: System detects the number of people entry and exit in the detection zone. When the number of entry/exit/stay exceeds the preset value, system will trigger an alarm.
   - ◇ **ManNumDetection**: system detects people number and the duration of stay inside the detection zone. When the people number or duration of stay exceeds the preset value, system will trigger an alarm.

Step 3 Select the default zone or line on the video and click **Clear** to delete it or **Re-draw** to draw a new one.

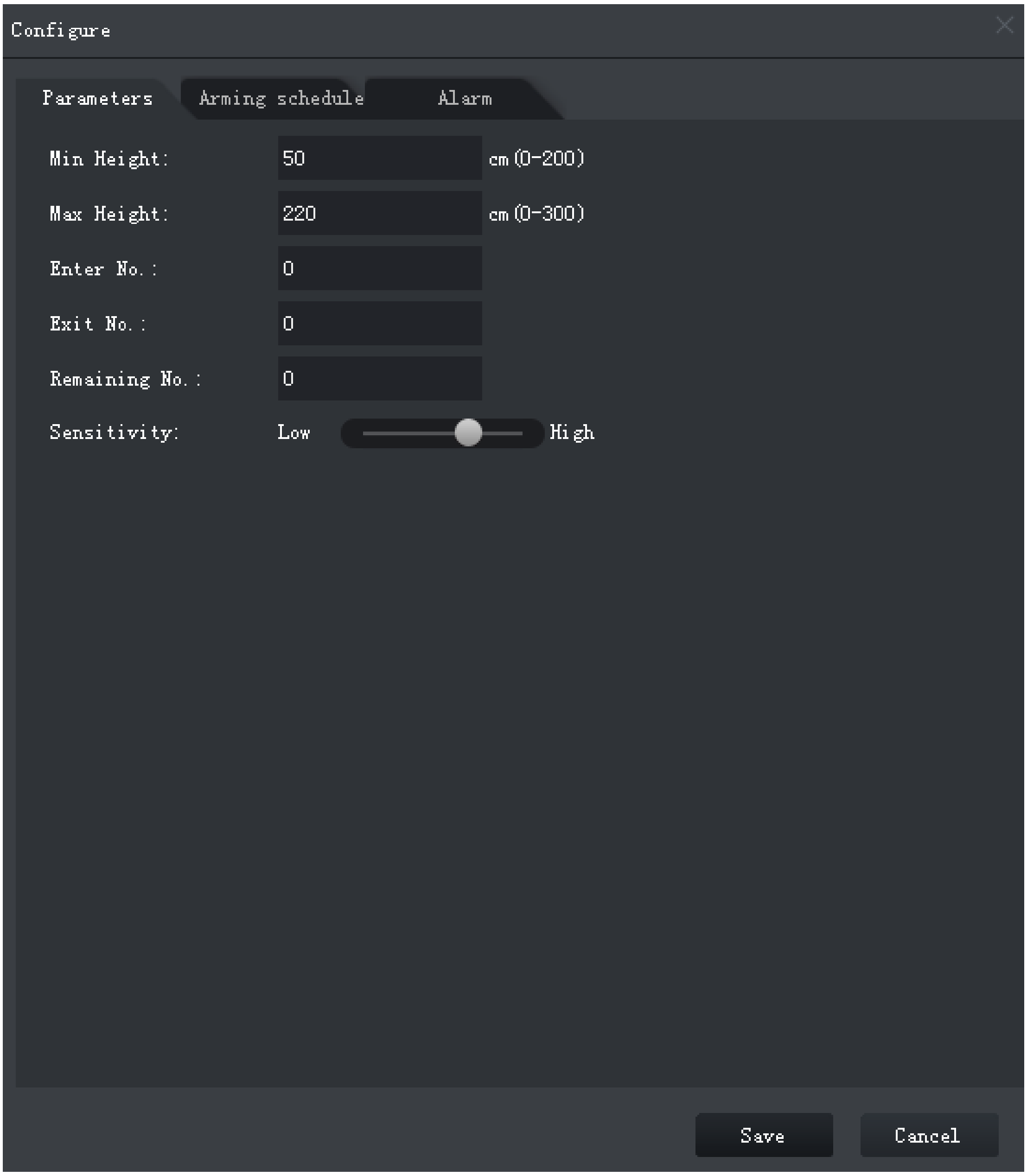
People counting requires to draw a detection zone and a line while **ManNumDetection** requires only a detection zone.

When drawing the line from left to right, the direction is A to B, and then people flow from A to B is entry number and B to A is exit number. When drawing the line from right to left, the direction is B to A, and then people flow from B to A is entry number and A to B is exit number.

Step 4 Set parameters, arming schedule and alarm linkage.

1) Click **Config** and set parameters. See Figure 3-158. See Table 3-41 for details.

Figure 3-157 Set parameters（People counting）



Min Height: 50 cm (0-200)

Max Height: 220 cm (0-300)

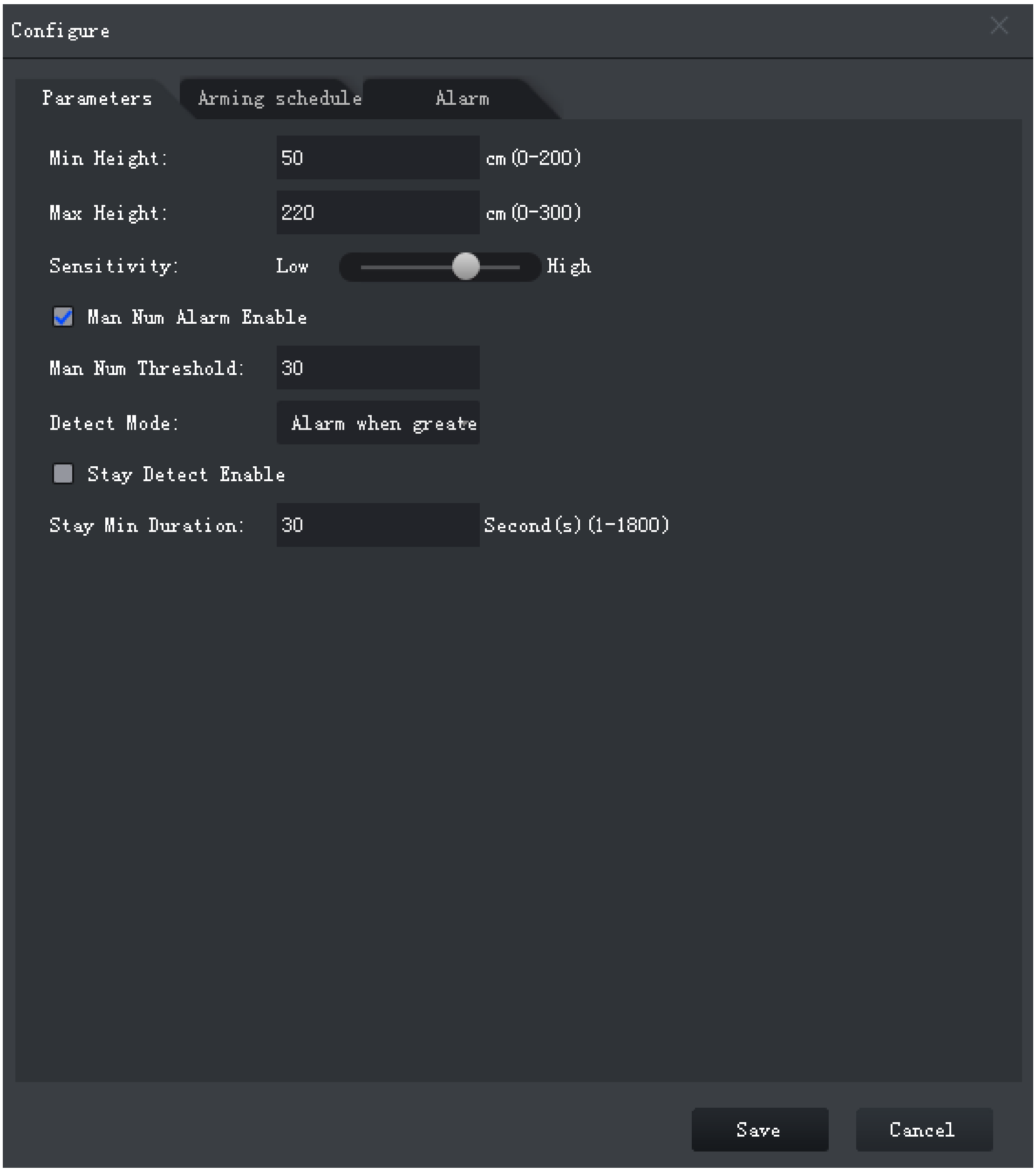
Enter No.: 0

Exit No.: 0

Remaining No.: 0

Sensitivity: Low High

Figure 3-158 Set parameters (ManNumDetection)



Min Height: 50 cm (0-200)

Max Height: 220 cm (0-300)

Sensitivity: Low High

☑ Man Num Alarm Enable

Man Num Threshold: 30

Detect Mode: Alarm when greate

☐ Stay Detect Enable

Stay Min Duration: 30 Second(s)(1-1800)

Table 3-41 Parameters

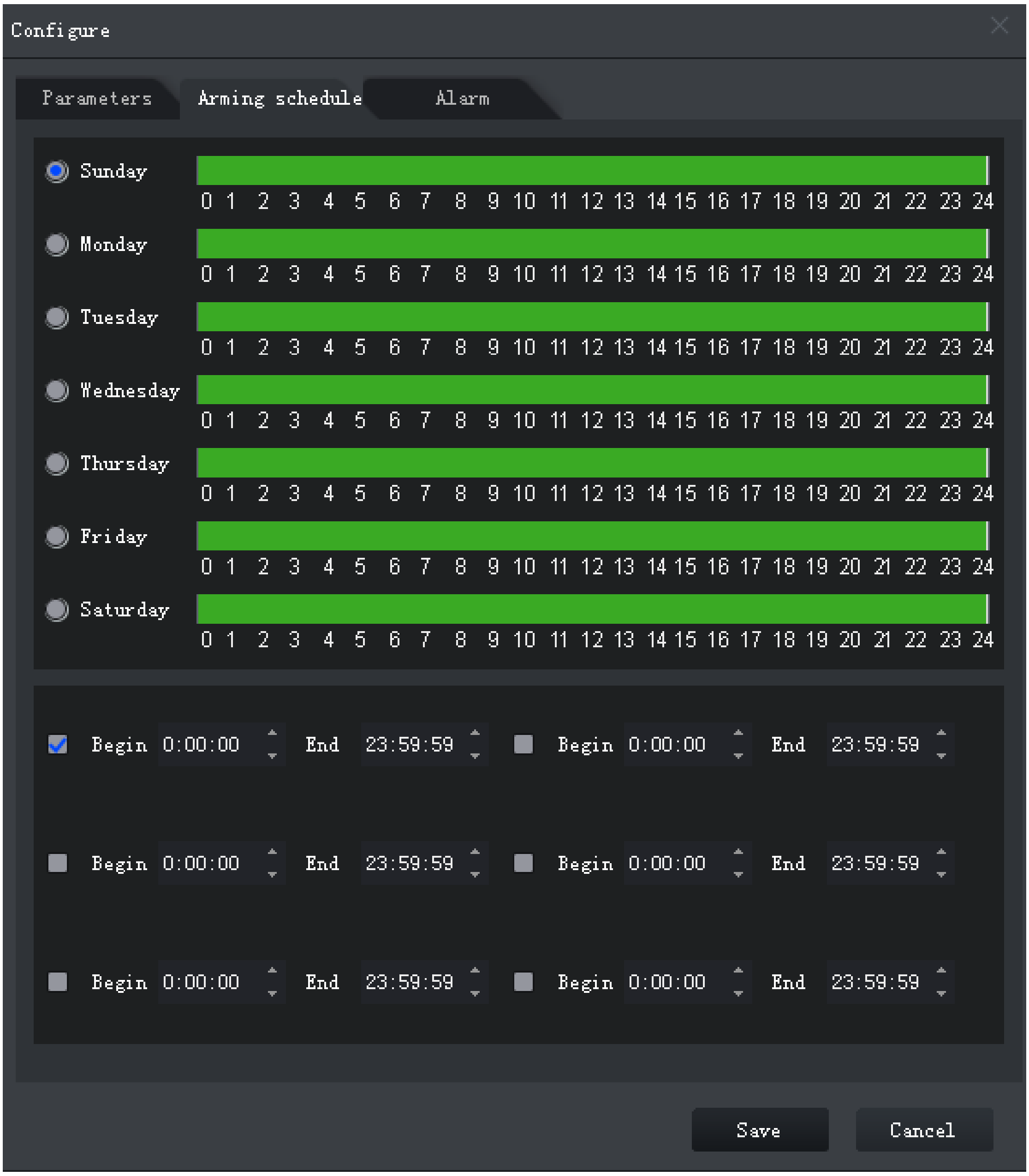
Parameter	Description
Min Height	When the target height is between the minimum height and maximum height, system will trigger the statistics rule.
Max Height	
Man Num Alarm Enable	When the people number in the zone reaches, exceeds or is smaller than the preset value, system will trigger an alarm.
Man Num Threshold	
Detect Mode	
Stay Detect Enable	When the people stay time in the zone is exceeds the preset value, system will trigger an alarm.
Stay Min Duration	

Parameter	Description
Enter No.	When the entry number exceeds the preset value, system will trigger an alarm.
Exit No.	When the exit number exceeds the preset value, system will trigger an alarm.
Remaining No.	When the remaining people number exceeds the preset value, system will trigger an alarm.
Sensitivity	It is recommended to keep the default value.

2) Click **Arming schedule**, select day and hours and then set the start time and end time. See Figure 3-159

The default arming schedule is 24 hours per day.

Figure 3-159 Arming schedule


Configure
Parameters
Arming schedule
Alarm
● Sunday
○ Monday
○ Tuesday
○ Wednesday
○ Thursday
○ Friday
○ Saturday
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Save
Cancel

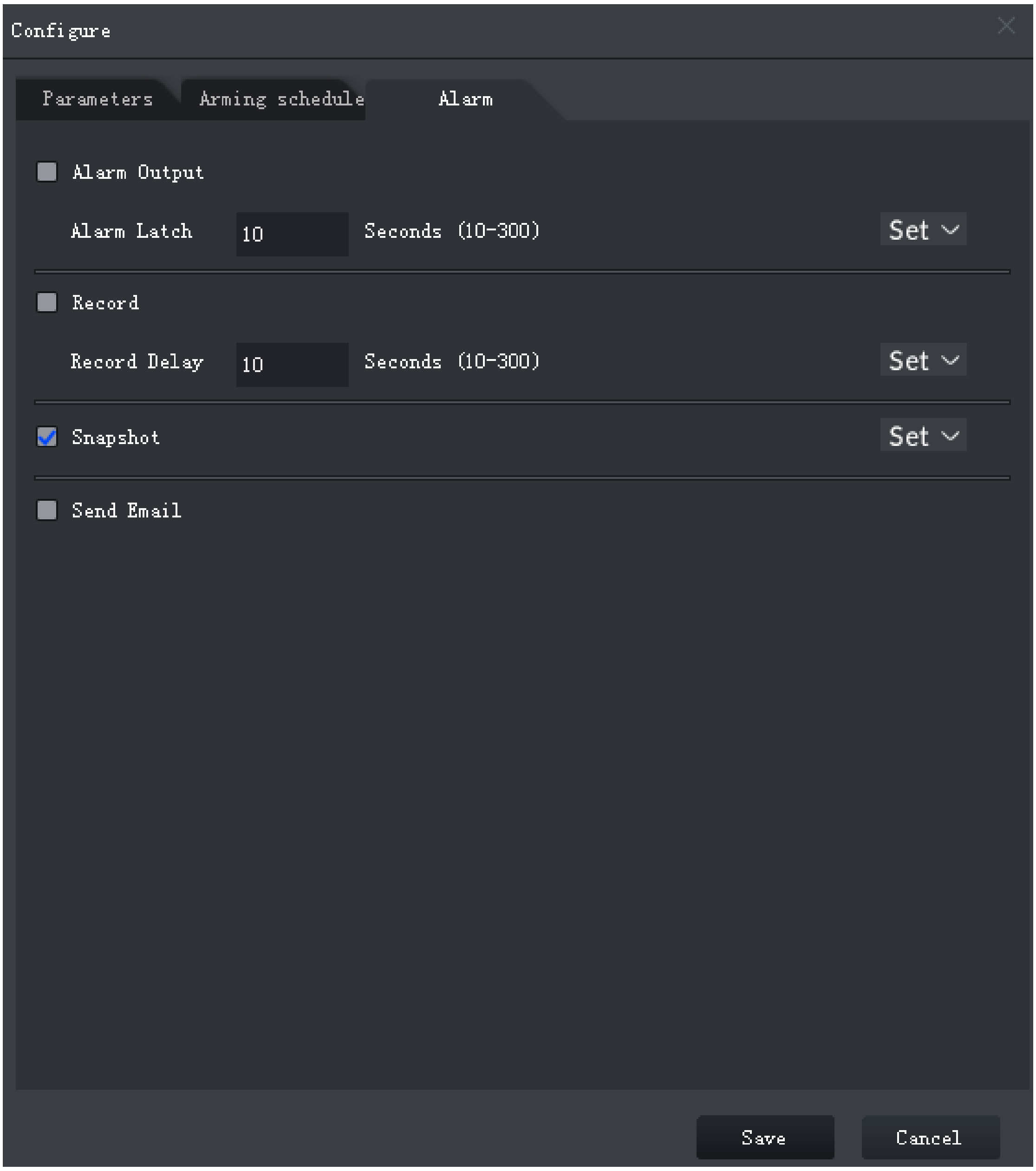
☑ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

3) Click **Alarm** to set linkage actions. See Figure 3-160. See Table 3-42 for details.

Figure 3-160 Alarm


Configure
Parameters
Arming schedule
Alarm
Set
Set
Set
Save
Cancel

☐ Alarm Output

Alarm Latch 10 Seconds (10-300)

☐ Record

Record Delay 10 Seconds (10-300)

☑ Snapshot

☐ Send Email

Table 3-42 Parameters

Parameter	Description	
Alarm output	Connect alarm output devices to the alarm output interfaces. When an alarm is triggered, the system will send the alarm to the alarm output device.	Click **Set** next to **Alarm Latch** and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the the alarm event ends.	

Parameter	Description	
Record	When an alarm happens, it will trigger auto video recording immediately. 📖 It requires the device to have recording schedules already. See device manual for detailed instruction.	Click **Set** next to **Record** to select the recording channel.
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	The system will take snapshots automatically when an alarm happens. 📖 It requires the device to have snapshot schedules already.See device manual for detailed instruction.	Click **Set** next to **Snapshot** to select the snapshot channel.
Send email	The system will send an email to the related mail address when an alarm happens. 📖 It requires the device to have email configured already. See device manual for detailed instruction.	

4) Click **Save**.

Step 5 Click **Save**.

3.6.5 Heatmap

Detect the accumulated people density in a specific zone and display the result in different colors which range from blue to red. Blue indicates low density and red means high density.

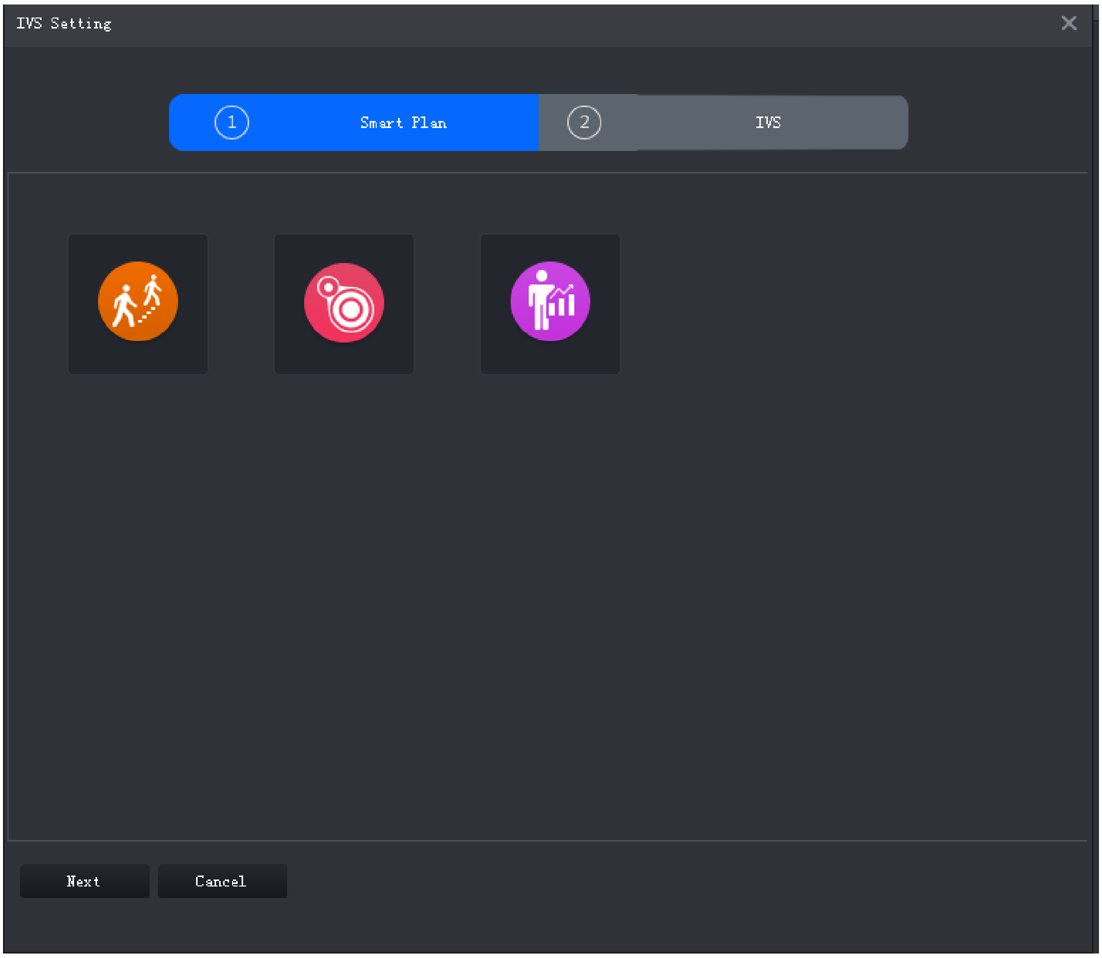
3.6.5.1 Enabling Heatmap

Step 1 Go to the **Intelligent Analyse** interface.

Step 2 Click ◎ to select heatmap.

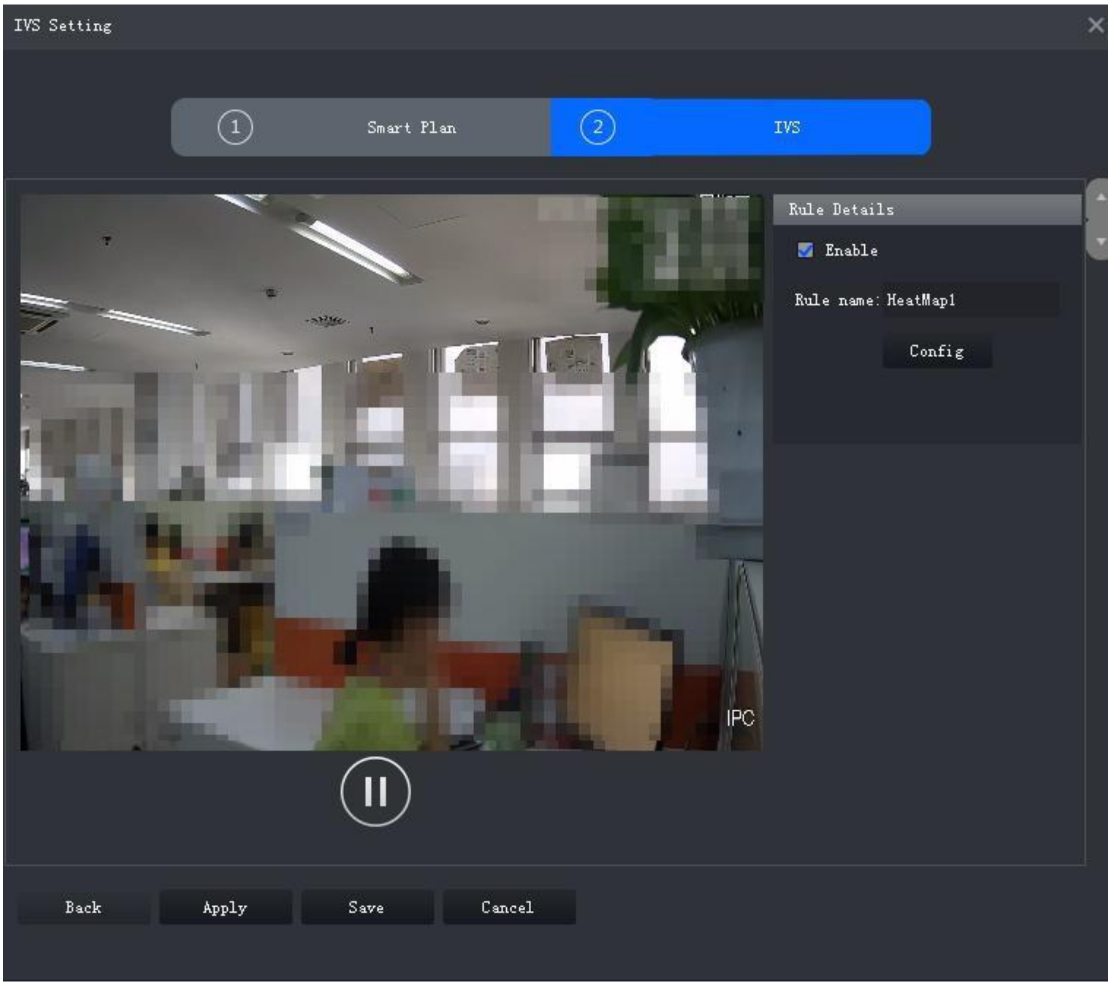
When the icon is displayed in the white frame, it means it is selected. If another smart plan, which is conflicting with Heatmap, is selected already, click that smart plan icon to deselect it and then click ◎ to select heatmap.

Figure 3-161 Smart plan


IVS Setting
1
Smart Plan
2
IVS
Next
Cancel

3.6.5.2 Configuring Heatmap Rule

Figure 3-162 Heatmap


IVS Setting
① Smart Plan
② IVS
Rule Details
☑ Enable
Rule name: HeatMap1
Config
IPC
Back
Apply
Save
Cancel

Step 1 Select the check box of **Enable** to enable heatmap.

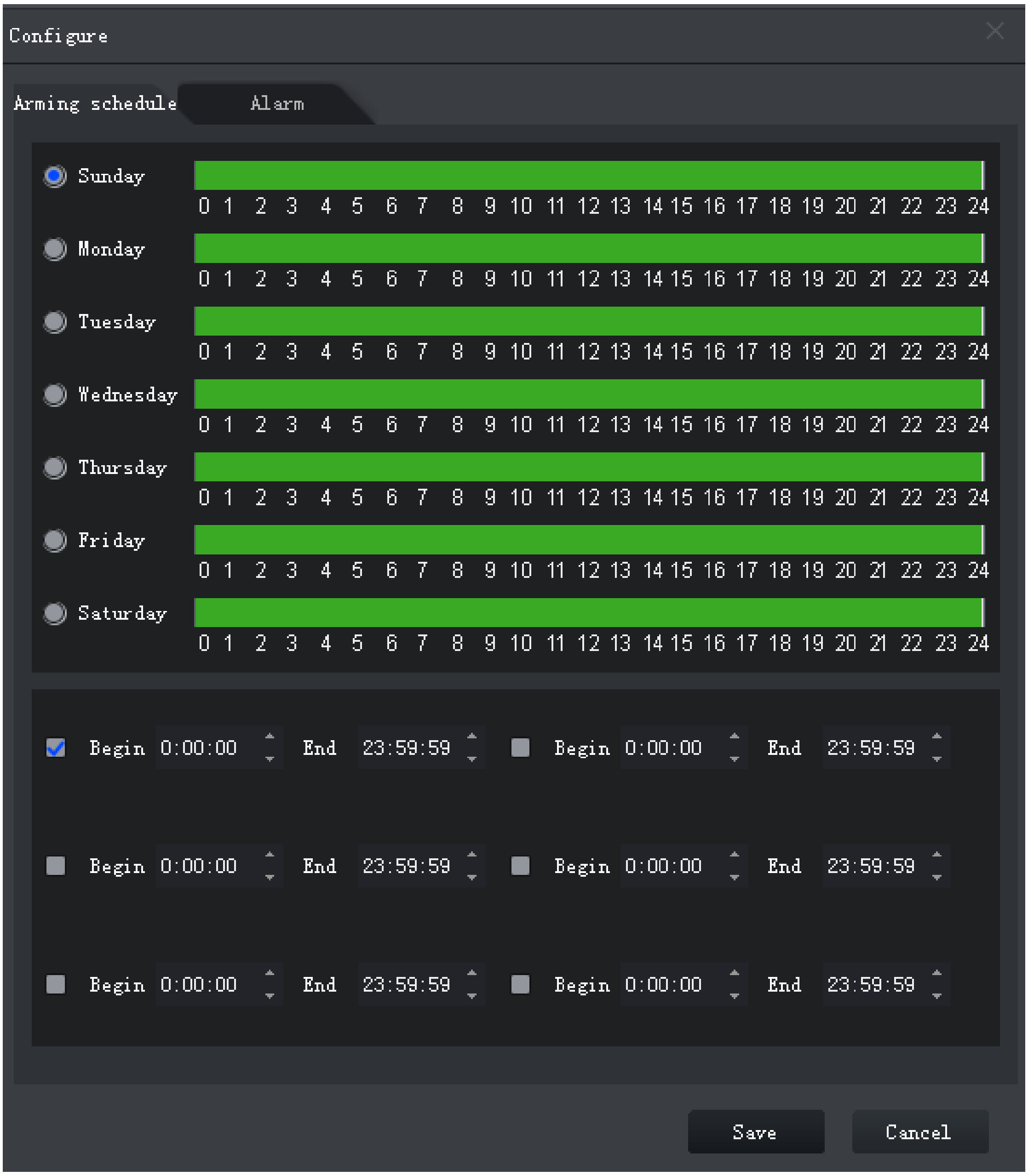
Step 2 Modify Rule name.

Step 3 Configuring arming schedule and alarm linkage.

1) Click **Config**.

The interface of **Configure** is displayed. See Figure 3-163.

Figure 3-163 Configure


Configure
Arming schedule
Alarm
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Save
Cancel

● Sunday
○ Monday
○ Tuesday
○ Wednesday
○ Thursday
○ Friday
○ Saturday

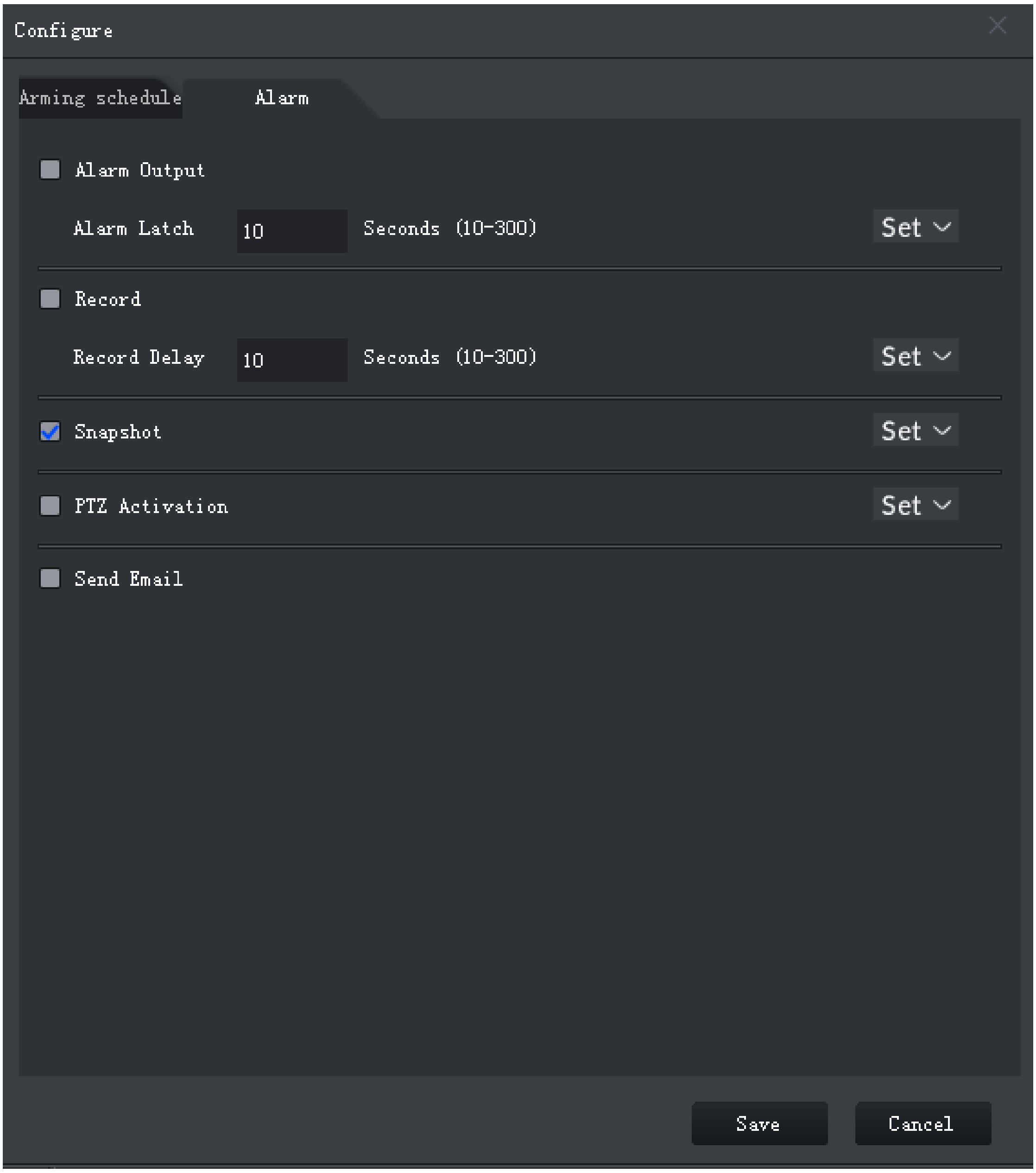
☑ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59
☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59
☐ Begin 0:00:00 End 23:59:59 ☐ Begin 0:00:00 End 23:59:59

2) Click **Arming schedule**, select day and hours, and then set the start time and end time.

The default arming schedule is 24 hours per day.

3) Click **Alarm** to set linkage actions. See Figure 3-164. See Table 3-43 for details.

Figure 3-164 Alarm


Configure
Arming schedule
Alarm
Set
Set
Set
Set
Save
Cancel

☐ Alarm Output

Alarm Latch 10 Seconds (10-300)

☐ Record

Record Delay 10 Seconds (10-300)

☑ Snapshot

☐ PTZ Activation

☐ Send Email

Table 3-43 Parameters

Parameter	Description	
Alarm output	Connect alarm output devices to the alarm output interfaces. When an alarm is triggered, the system will send the alarm to the alarm output device.	Click Set next to **Alarm Latch** and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the the alarm event ends.	

Parameter	Description	
Record	When an alarm happens, it will trigger auto video recording immediately. 📖 It requires the device to have recording schedules already. See device manual for detailed instruction.	Click **Set** next to **Record** to select the recording channel.
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	The system will take snapshots automatically when an alarm happens. 📖 It requires the device to have snapshot schedules already.See device manual for detailed instruction.	Click **Set** next to **Snapshot** to select the snapshot channel.
Send email	The system will send an email to the related mail address when an alarm happens. 📖 It requires the device to have email configured already. See device manual for detailed instruction.	None

4) Click **Save.**

Step 4 Click **Save**.

3.7 Fisheye-PTZ Smart Track

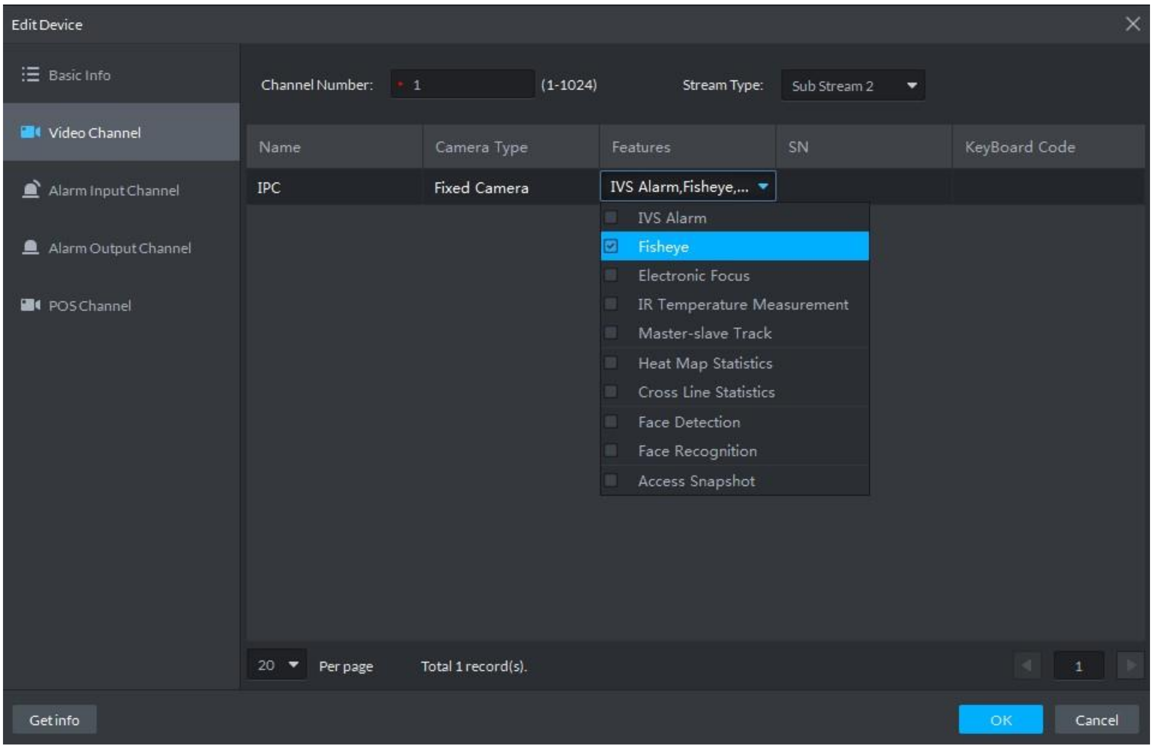
OPTIVIEW VMX Client supports smart track which links fisheye speed dome to general speed dome to better control each monitoring position.

3.7.1 Adding Device

Step 1 Add fisheye and speed dome. For more details, see "3.2.2.4 Adding Device."

Step 2 On the **Edit Device** interface, click ✎ next to the fisheye device, and then you can modify the device features as **Fisheye**. See Figure 3-165.

Figure 3-165 Fisheye device



Channel Number: 1 (1-1024)

Stream Type: Sub Stream 2

Name	Camera Type	Features	SN	KeyBoard Code
IPC	Fixed Camera	IVS Alarm,Fisheye,...		

20 Per page Total 1 record(s).

Edit Device
Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
☐ IVS Alarm
☑ Fisheye
☐ Electronic Focus
☐ IR Temperature Measurement
☐ Master-slave Track
☐ Heat Map Statistics
☐ Cross Line Statistics
☐ Face Detection
☐ Face Recognition
☐ Access Snapshot
1
Get info
OK
Cancel

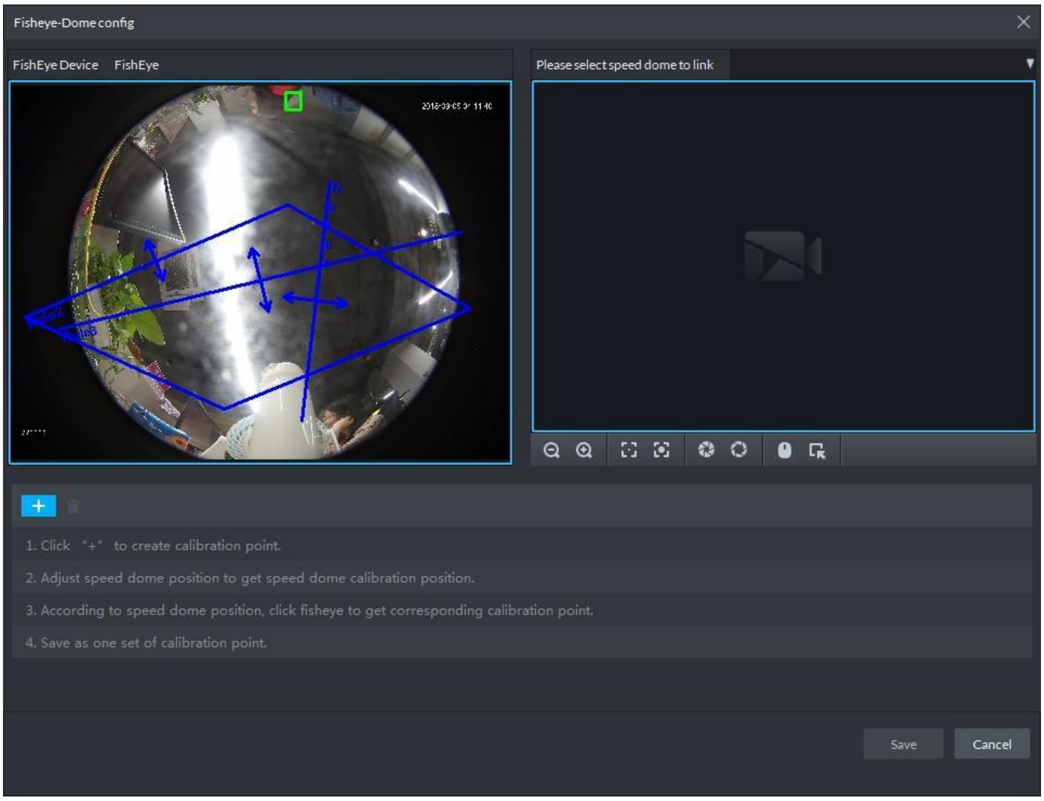
3.7.2 Adding Smart Track Configuration

Step 1 Select the fisheye device on the device tree and then right-click to select smart track.

If it is not the first time to use smart track function, select the fisheye device and then right-click to select smart track config.

The smart track interface is displayed. See Figure 3-166.

Figure 3-166 Smart track config


Fisheye-Dome config
FishEye Device
FishEye
Please select speed dome to link
Save
Cancel

1. Click "+" to create calibration point.

2. Adjust speed dome position to get speed dome calibration position.

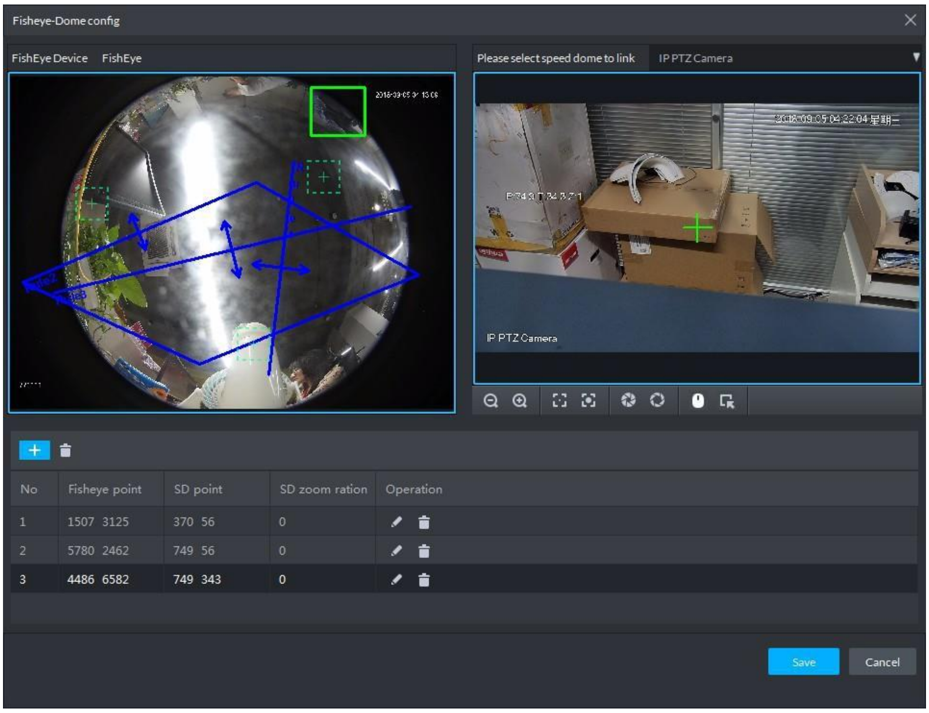
3. According to speed dome position, click fisheye to get corresponding calibration point.

4. Save as one set of calibration point.

Step 2 Click ▼ and then select a PTZ camera.

Step 3 Click + and then move the ⊞ of the fisheye on the right to select a position. Click 🖱 on the general PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image). See Figure 3-167.

Figure 3-167 Configure calibration point


Fisheye-Dome config
FishEye Device
FishEye
Please select speed dome to link
IP PTZ Camera
IP PTZ Camera
Save
Cancel

No	Fisheye point	SD point	SD zoom ration	Operation
1	1507 3125	370 56	0	✎ 🗑
2	5780 2462	749 56	0	✎ 🗑
3	4486 6582	749 343	0	✎ 🗑

- Select 3-8 mark points on fisheye camera.
- When you find mark point on the left side of general PTZ camera, click to zoom out PTZ.
- Click to 3D position, and when you click a certain point on the left side of PTZ camera, it will automatically move to the center.

Step 4 Click ✓ to save the calibration point.

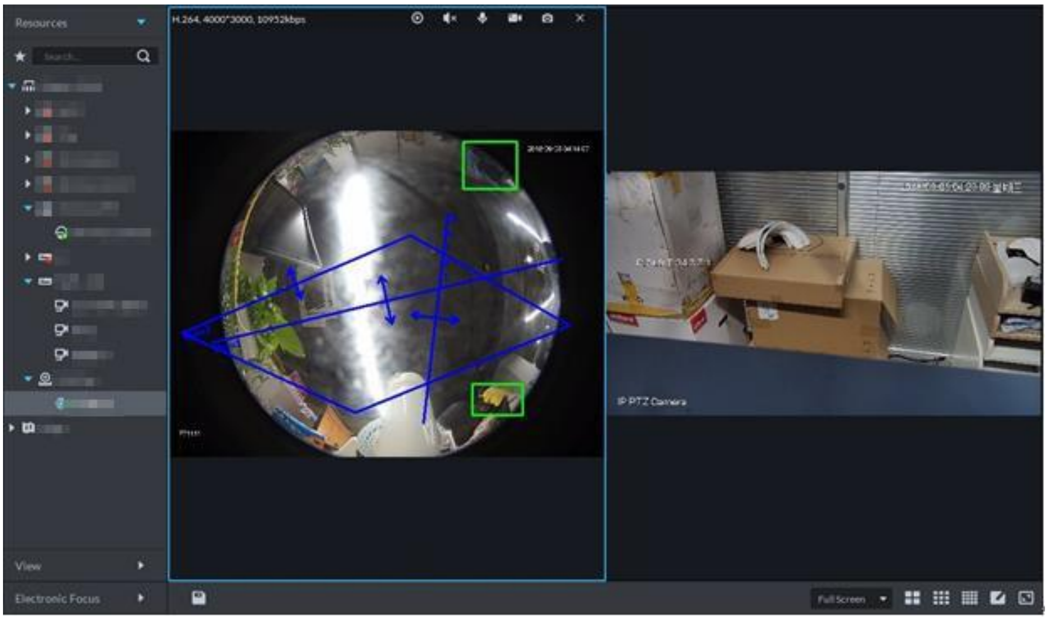
Refer to above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 5 Click **Save**.

3.7.3 Enabling Smark Track Function

Step 1 Select the fisheye device on the device tree and then right-click to select **Smart Track**. See Figure 3-168.

Figure 3-168 Smart track



Step 2 Click any point on the left of fisheye, general PTZ camera on the right will auto link to corresponding position

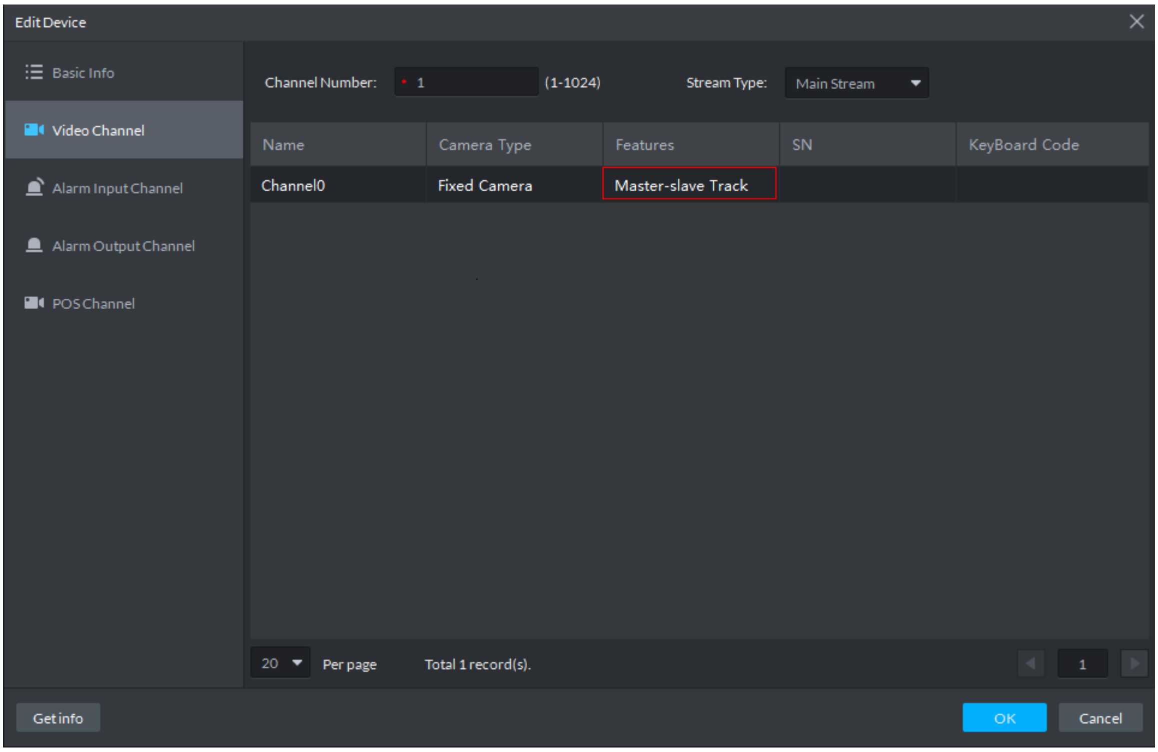
3.8 Bullet-PTZ Smart Track

Support smart track which links bullet with PTZ camera, and it is good for panoramic monitoring and details tracking. Currently smart track supports bullet PTZ all-in-one camera and panoramic+PTZ camera etc. Besides, it also supports individual bullet and PTZ camera which have been bound and calibrated.

3.8.1 Preparations

- Before implementing smart track (bullet + PTZ camera), it needs to add bullet and PTZ camera from **Device** on Web interface. For detailed steps, refer to **3.2.2.4 Adding Device**
- Click ✎ after adding bullet, and select **Master Slave Track**. Tracking function can be realized after configuring master slave track.

Figure 3-169 Master slave track



Channel Number: 1 (1-1024)

Stream Type: Main Stream

Name	Camera Type	Features	SN	KeyBoard Code
Channel0	Fixed Camera	Master-slave Track		

20 Per page Total 1 record(s). 1

- It needs to calibrate bullet and PTZ camera by config tool in advance if you want to add individual bullet and PTZ camera. For detailed operations, refer to config tool user manual.

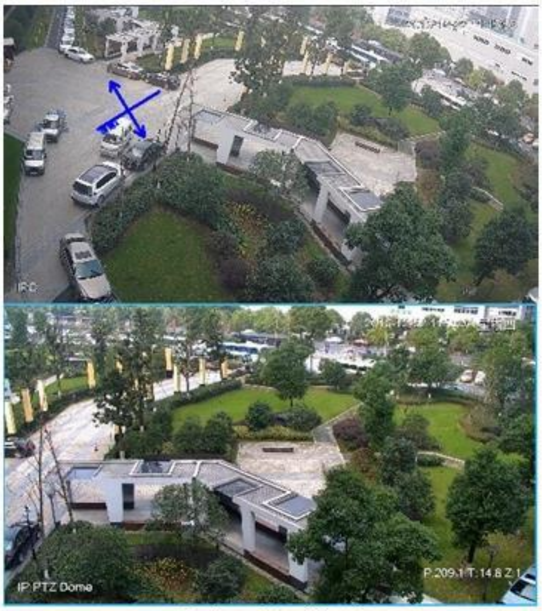
3.8.2 Applying Smart Track

Smart track application includes manual positioning, 3D positioning, manual tracking, auto tracking and preset return.

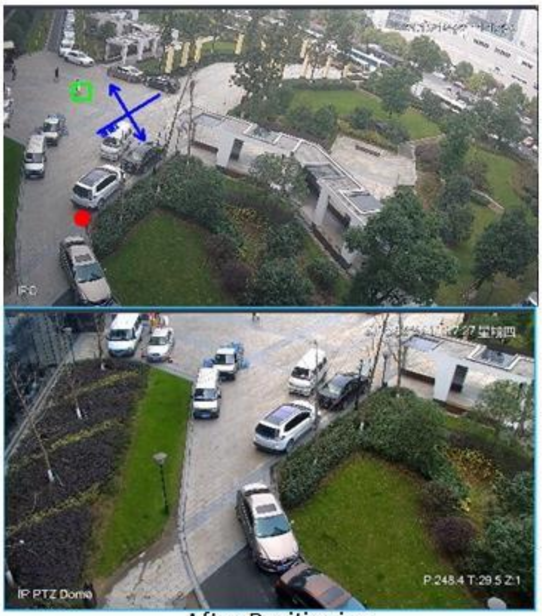
3.8.2.1 Manual Positioning

Click any position on the bullet image, and the PTZ will position the image to the area designated by bullet due to smart track. See Figure 3-170. Click the red spot on the bullet image, and the PTZ central point will move to the corresponding location automatically.

Figure 3-170 Manual positioning


IPC
IP PTZ Dome
P:209.1 T:14.8 Z:1

Before Positioning


IPC
IP PTZ Dome
P:248.4 T:29.5 Z:1

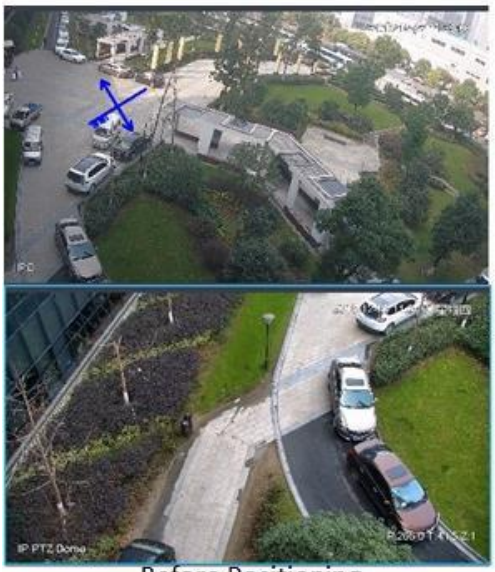
After Positioning

3.8.2.2 3D Positioning

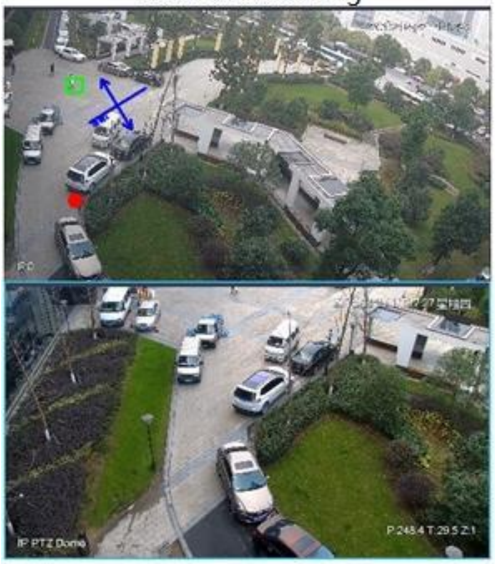
Select an area on the bullet image, and the PTZ camera will position the image to the corresponding area, meanwhile zoom in or out.

- Draw rectangular box from upper left to lower right, zoom in after being positioned by PTZ camera. See Figure 3-171.
- Draw rectangular box from lower right to upper left; zoom out after being positioned by PTZ camera. See Figure 3-172.

Figure 3-171 3D positioning (Zoom in after positioning)

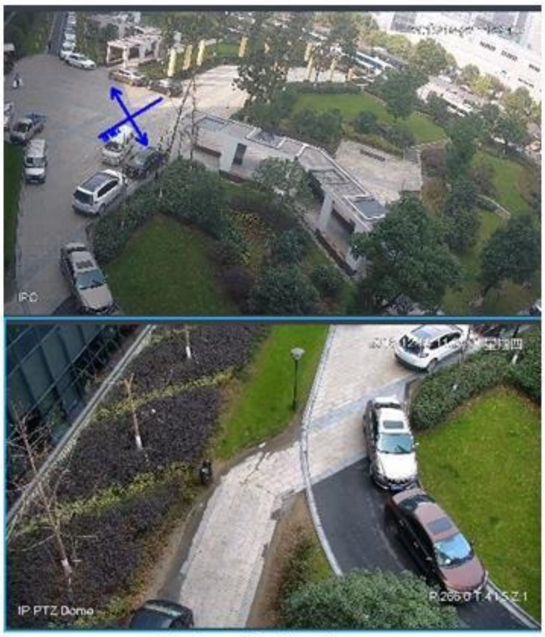

IPC
IP PTZ Dome

Before Positioning

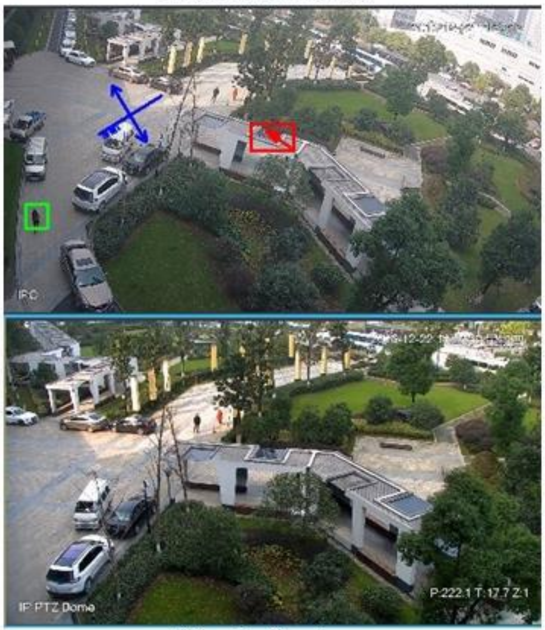

IPC
IP PTZ Dome
P:248.4 T:29.5 Z:1

After Positioning

Figure 3-172 3D positioning (Zoom out after positioning)



Before Positioning



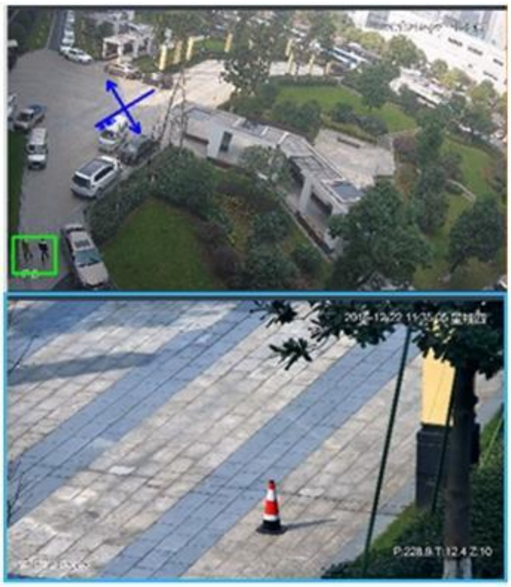
After Positioning

3.8.2.3 Manual Track

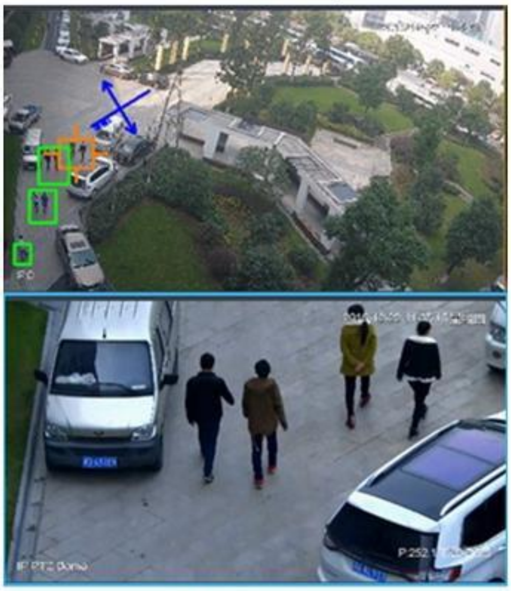
- Bullet PTZ all-in-one camera, panoramic+PTZ camera and individual bullet have been configured with smart rules. For detailed operation, refer to device user manual.
- IVS Overlay is required to be selected on the bullet image, enable target box overlay. Target box will be displayed only when there is moving target appears in the image.
- Manual track priority is higher than auto track.

Click moving target box (valid inside the box as well) in the bullet monitoring image, and the color of target box changes, PTZ camera will track the selected target.

Figure 3-173 Manual track



Before Tracking



After Tracking

3.8.2.4 Auto Track

After auto track is enabled, when there is target triggering IVS rule in the bullet image, then PTZ camera will automatically track the target that triggers IVS rule. If there are more than two tracking targets in the image, then it will select tracking target according to trigger time.

- Bullet PTZ all-in-one camera, panoramic+PTZ camera and individual bullet have been configured with smart rules. For detailed operation, refer to device user manual.
- IVS Overlay is required to be selected on the bullet image, enable target box overlay. Target box will be displayed only when there is moving target appears in the image.
- Manual track priority is higher than auto track.

In the device list on **Live** interface, select individual bullet, bullet PTZ all-in-one camera or panoramic+PTZ camera, right-click and select Auto **Track** > **On** and eenable auto track. When there is moving target in the image, then PTZ camera will track the target automatically. See Figure 3-174 and Figure 3-175.

Figure 3-174 Auto track

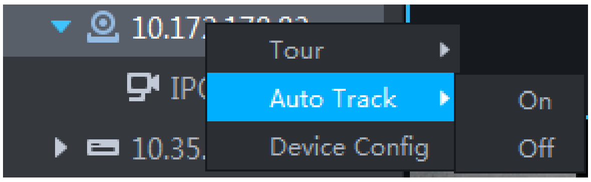
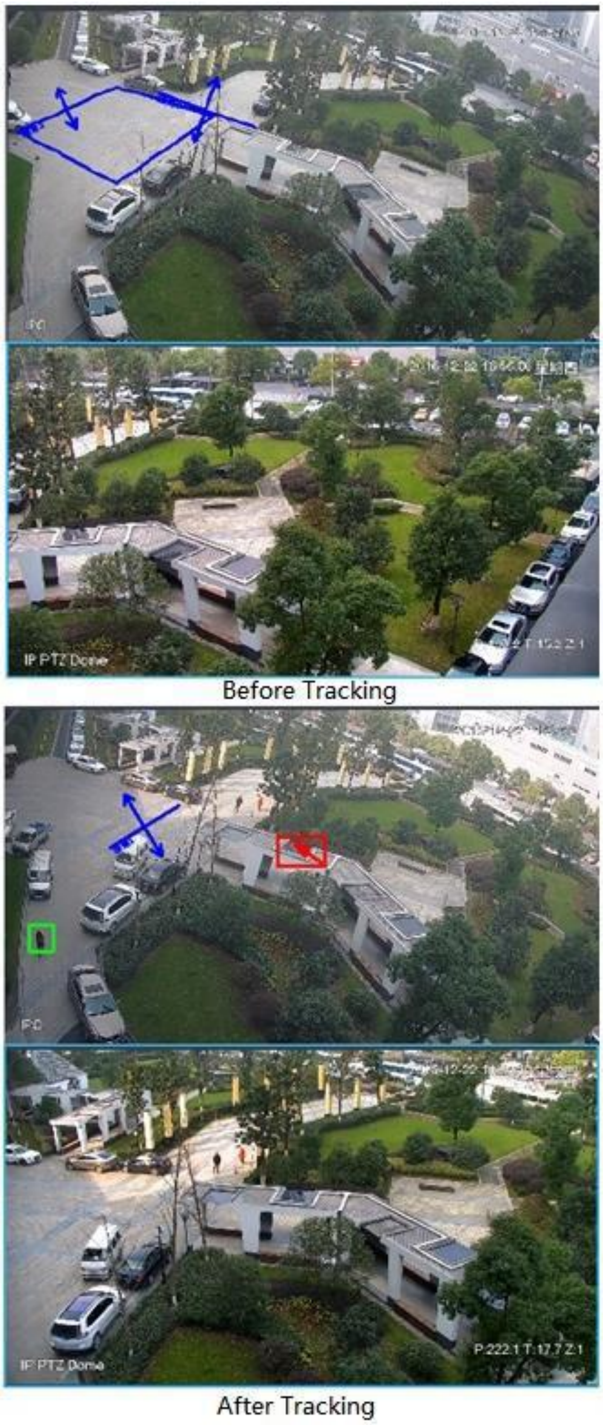

10.17
IPC
10.35.
Tour
Auto Track
Device Config
On
Off

Figure 3-175 Auto track


IPC
IP PTZ Dome
Before Tracking
IPC
IP PTZ Dome
After Tracking

3.8.2.5 Preset Return

Enable preset return when idle during calibration, in any status, when there is no target triggering track within the specific period on the bullet image, then PTZ image will return to the designated preset.

3.9 Record

View videos recorded on device or server, you can download video and save to local.

3.9.1 Record Playback

If neither device nor platform is configured with record plan, then you can search no video. If you want to configure platform record plan, refer to **3.2.5 Setting Record Plan** for more details.

3.9.1.1 Entering Record Playback Interface

On client homepage, click **Record Playback**. The system displays **Record Playback** interface, See Figure 3-176. For interface description, see Table 3-44.

Figure 3-176

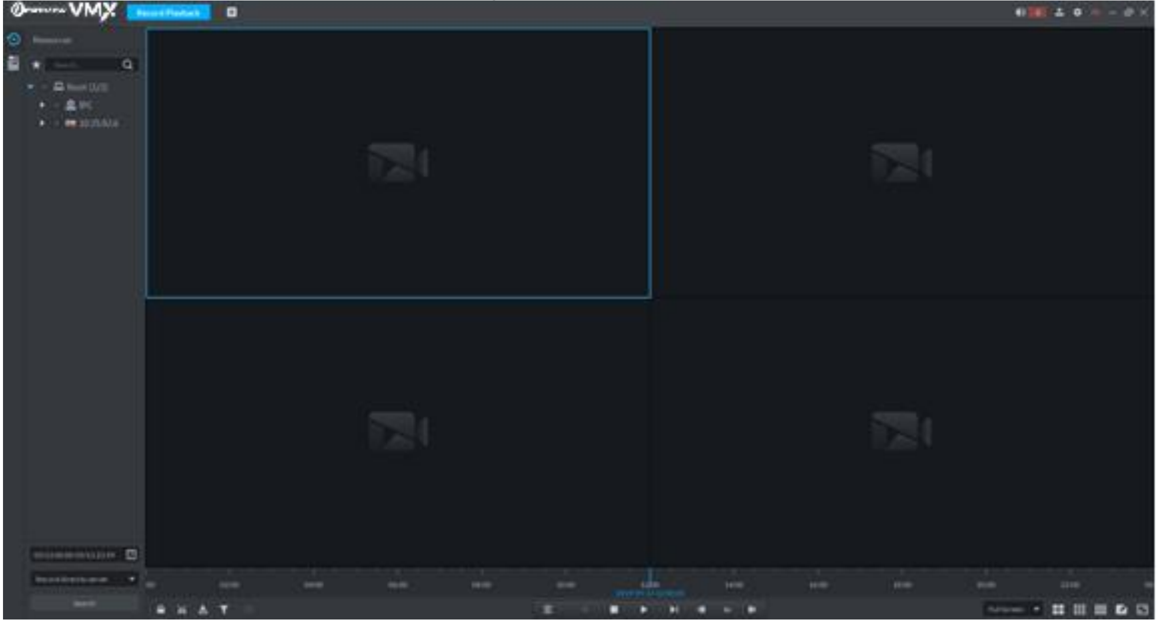


Table 3-44 Record playback icon description

Icon	Description
🔒	Lock the video stored on server within some period of designated channel. Locked video will not be overwritten when disk is full.
✂	Cut video
⬇	Download video
▼	Filter video according to record type.

Icon	Description
	Make dynamic detection analysis over some area of the record image, it only replays the video with dynamic image in the detection area.
	Playback record files of the same period from different channels on selected windows.
■ ‖	Stop/pause playback
⏮/	Frame by frame playback/frame by frame backward.
⏪ 1x ⏩	Fast/slow playback. Max. supports 64X or 1/64X.
10:00 12:00 14:00 16:00 2018-07-18 12:16:09	During playback, you can drag time progress bar to play back record at the specific time.

3.9.1.2 Playback Video

Step 1 In the device tree on **Record Playback** interface, select channel, time and record storage position, click **Search**.

When selecting time, the date with blue spot means record file exists on this date.

Step 2 Select window with video, and then click ▶.

The corresponding window plays video of the channel, see Figure 3-177. For operation description, see Table 3-45.

Figure 3-177 Playback video

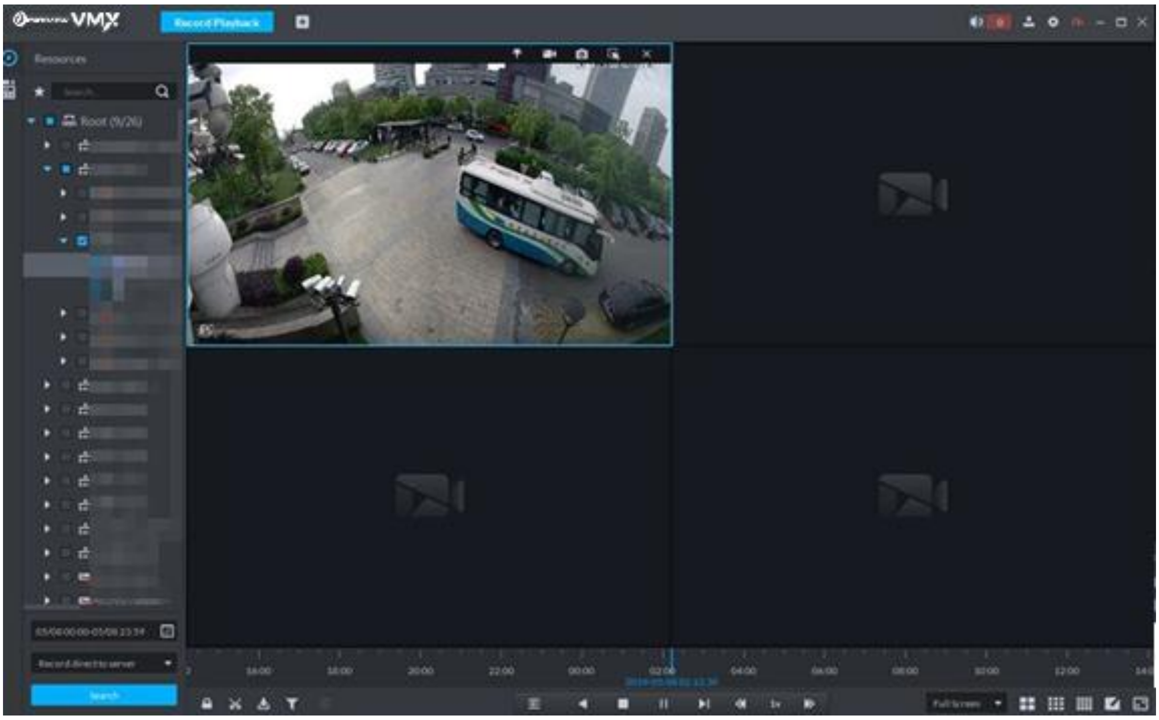


Table 3-45 Shortcut menu description

Icon	Icon Name	Description
	Record Tagging	Mark the record if you are interested in, convenient for future search. For detailed operations, see “3.9.1.4 Tagging Record.”

Icon	Icon Name	Description
📹	Local Record	Click the icon and system begins to record audio and video of current video window, recording duration is displayed on the upper left corner of the window; click the icon again, stop record and store to local PC. The default save path is “C:\Optiview VMX\Client\Record\”. If you want to modify save path, refer to “3.3.5 Setting Recording Parameter.”
📷	Snapshot	Save the image in the form of snapshot (one snapshot for once). Default save path is “C:\Optiview VMX\Client\Picture\”. If you need to modify save path, refer to “3.3.4 Setting Snapshot.”
🔍	Zoom in	Select and zoom in regionally, you can scroll the mouse to zoom in or out.
☒	Close	Click the icon to close video.

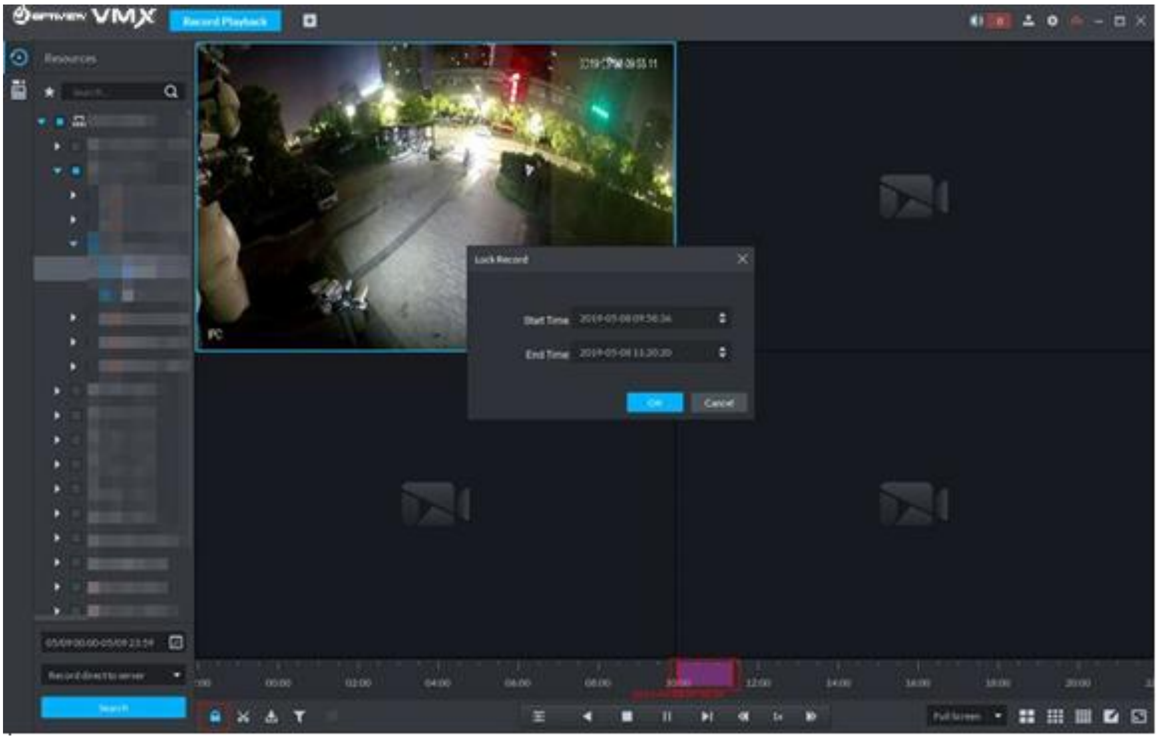
3.9.1.3 Locking Record

Lock the video stored on the server within some period of specific channel. The locked video will not be overwritten when disk is full.

Step 1 On **Record Playback** interface, set search condition and search videos.

Step 2 Click 🔒 at the bottom of the **Record Playback** interface (make sure the window has the record). The system pops out **Lock Record** interface. See Figure 3-178.

Figure 3-178 Select lock time



Step 3 Confirm time, click **OK**.

3.9.1.4 Tagging Record

Tag the video that you are interested in, convenient for future search.

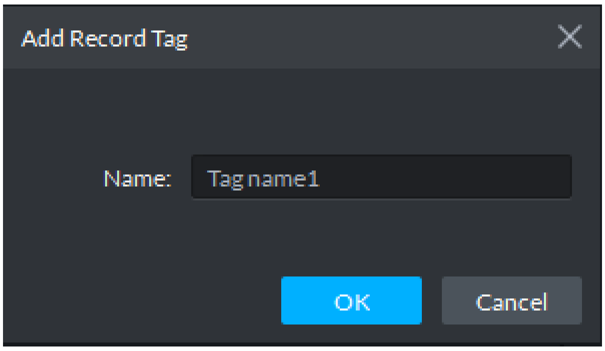
Step 1 On Record Playback interface, set search condition and search video.

Step 2 Select video, click ▶ and play video.

Step 3 Move the mouse to the window with video, click 📌 on top of the window.

The system pops out Add Record Tag interface. See Add record tag.

Figure 3-179 Add record tag



Add Record Tag

Name: Tag name1

Step 4 Enter **Name**, click **OK**.

3.9.1.5 Record Type Filter

Filter video according to record type, record type includes schedule record; alarm record and motion detect record.

Step 1 On **Record Playback** interface, click ▼. See Figure 3-180.

The system displays the interface of **Record Type Filter**. See Figure 3-181.

Figure 3-180 Record type filter

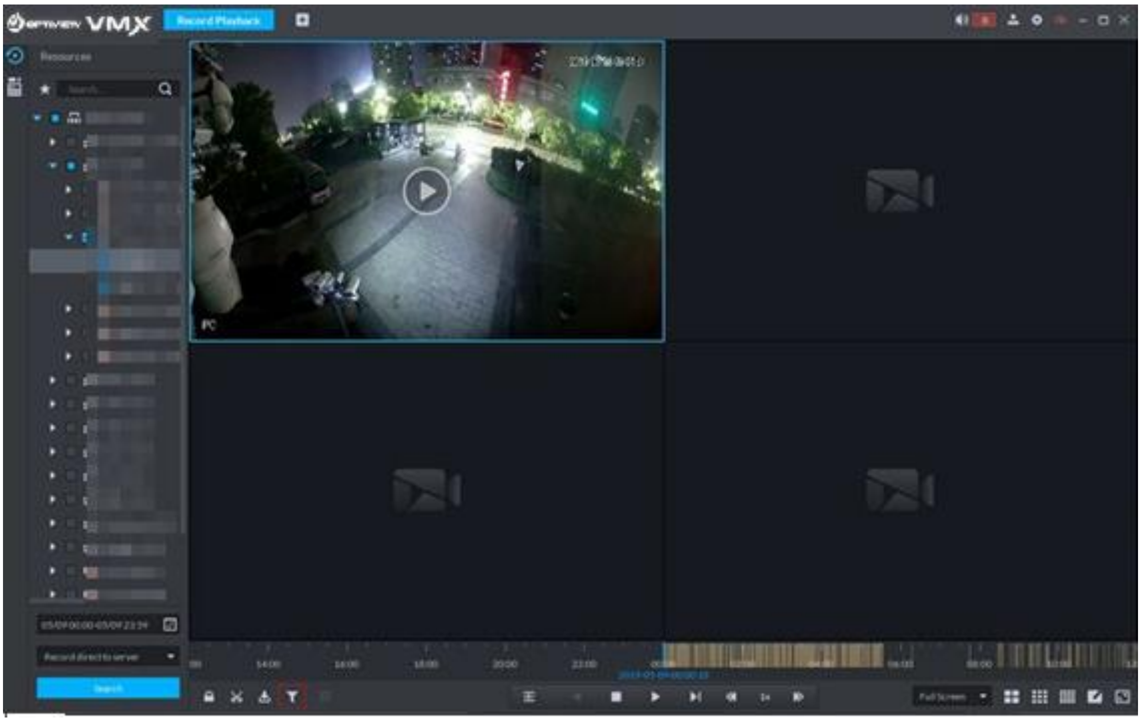
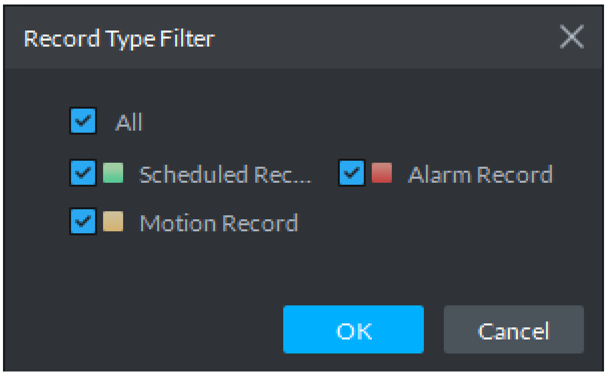


Figure 3-181 Record filter


Record Type Filter

☑ All

☑ 🟩 Scheduled Rec... ☑ 🟥 Alarm Record

☑ 🟨 Motion Record

Step 2 Select a record type (or types) and then click **OK**.

The system only displays the video of selected type.

3.9.1.6 Clip Record

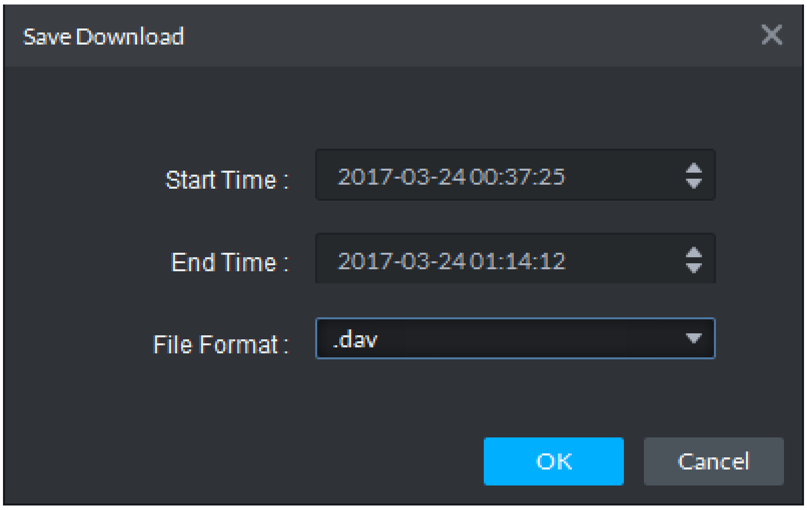
Step 1 On **Record Playback** interface, set search condition and search videos.

Step 2 Click ✂ at the bottom of the **Record Playback** interface (make sure there is record in the window).

Step 3 During the timeline, click to start clip and then drag the mouse, click to stop clip.

The **Save Download** interface is displayed. See Figure 3-182.

Figure 3-182 Save download


Save Download

Start Time : 2017-03-24 00:37:25

End Time : 2017-03-24 01:14:12

File Format : .dav

Step 4 Set file format and then click **OK**.

3.9.1.7 Smart Search

It makes dynamic detection analysis over some area and only replays the video with dynamic image with the detection area. The added front device is required to support smart search, otherwise the search result will be null.

Step 1 Point your mouse to 🔍 on the interface of **Record Playback**, and then select a type. See Figure 3-183.

Click 🔍. The system displays the interface of smart search. See Figure 3-184. 22×18 squares are displayed in the window.

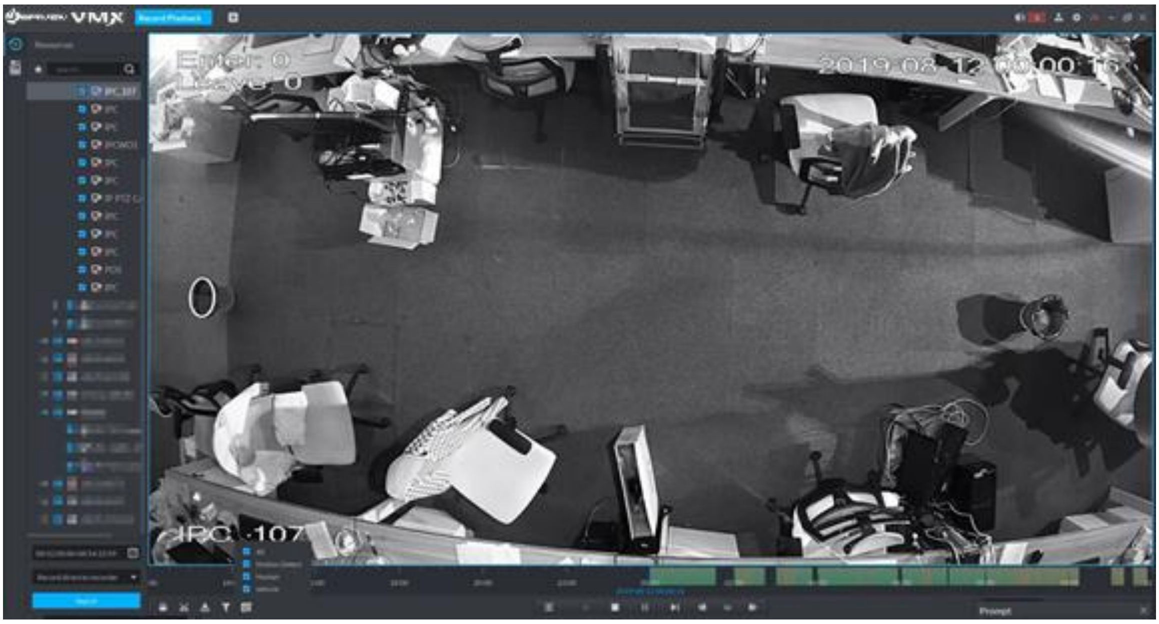
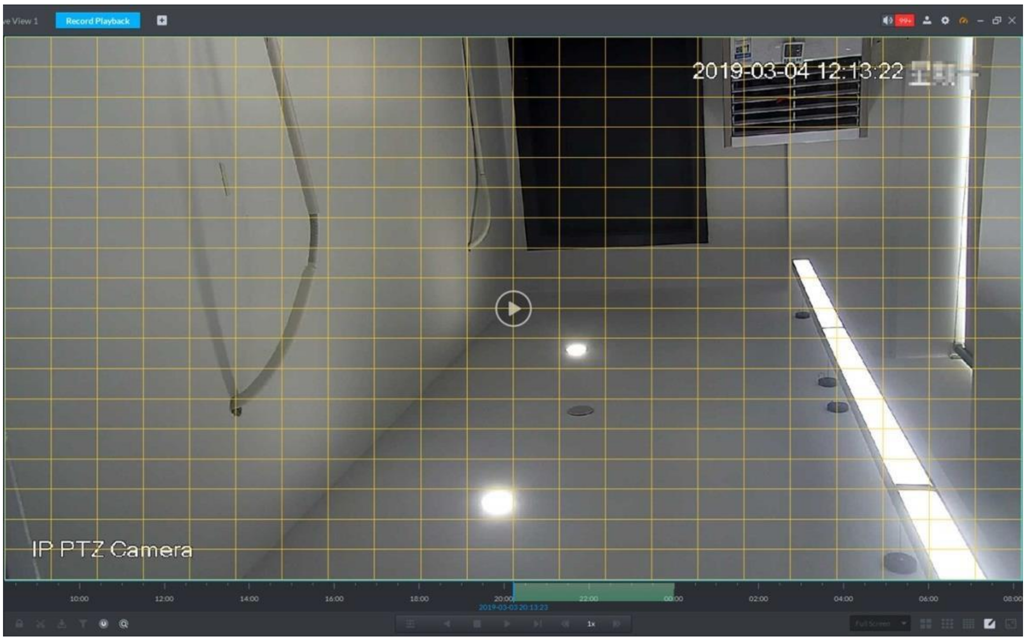

VMX
Record Playback
Enter: 0
Leave: 0
2019-08-12 00:00:16
IPC_107
Prompt

Figure 3-183 Enable smart search

Figure 3-184 Smart search


Record Playback
2019-03-04 12:13:22
IP PTZ Camera
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00

Step 2 Click the squares to select detection areas. You can select several areas.

- Select detection area; move the mouse to image, press mouse left button and drag the mouse to select square.
- For selected area, click again or select square to cancel it.

Step 3 Click and start smart search analysis.

- If there is search result, the time progress bar will become purple and display dynamic frame.
- If there is no search result, or selected playback device fails to support smart search, then it will prompt that smart search result is null.

Click and you can reselect detection area.

Step 4 Click the play button on the image or control bar.

The system only replays search result, which is the purple display frame on the time progress bar.

Step 5 Click ⏻ and exit smart search.

3.9.1.8 Downloading Record

The system supports downloading the record in the server or the device to local.

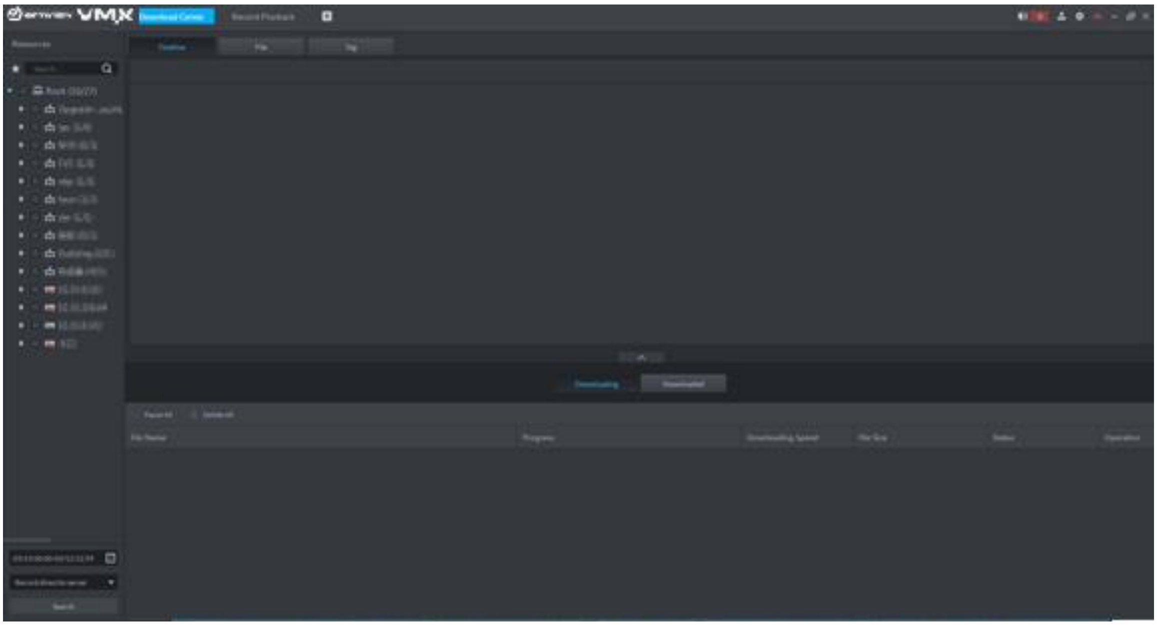
3.9.1.8.1 Timeline

Download video of some period for record file.

Step 1 On **Record Playback** interface, click ⤓, or click **Download Center** on the client homepage.

The system displays **Download Center** interface, see Figure 3-185.

Figure 3-185 Download center



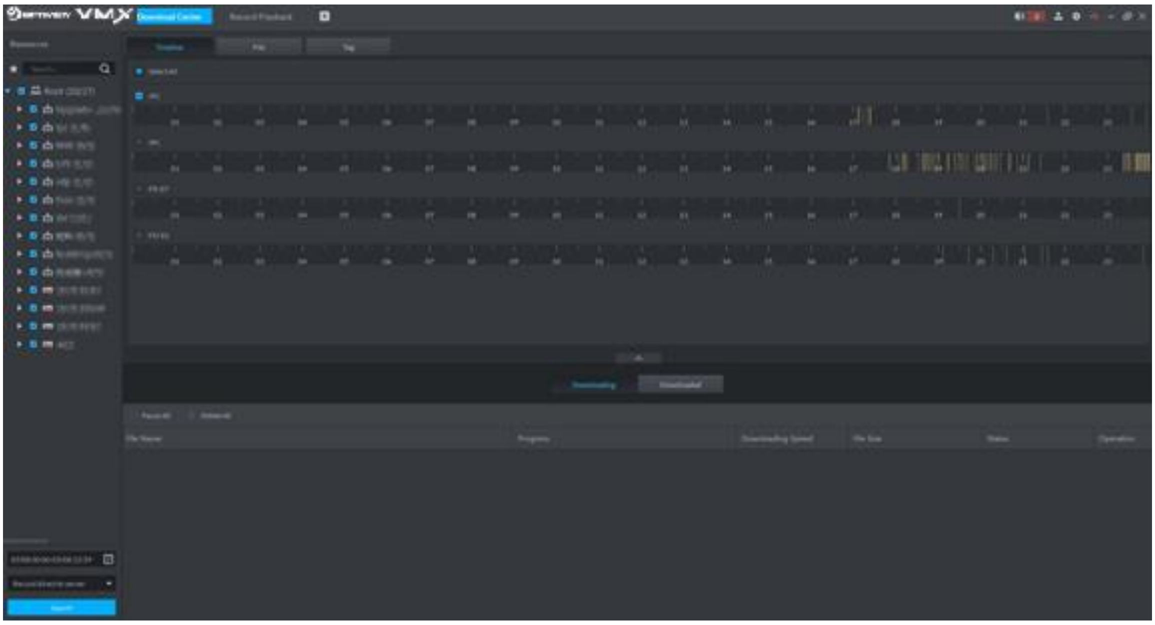
Step 2 Set search condition, click **Search**.

The system displays search results.

Step 3 Click **Timeline** tab.

The system displays search results in the form of timeline, see Figure 3-186.

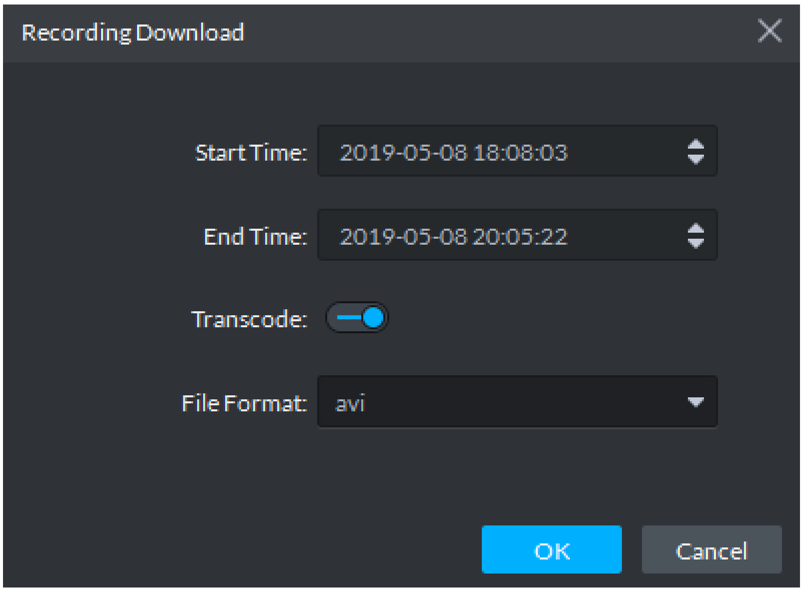
Figure 3-186 Record search result



Step 4 Move the mouse to timeline, select start time and end time.

The system displays **Recording Download** interface, see Figure 3-187.

Figure 3-187



Recording Download

Start Time: 2019-05-08 18:08:03

End Time: 2019-05-08 20:05:22

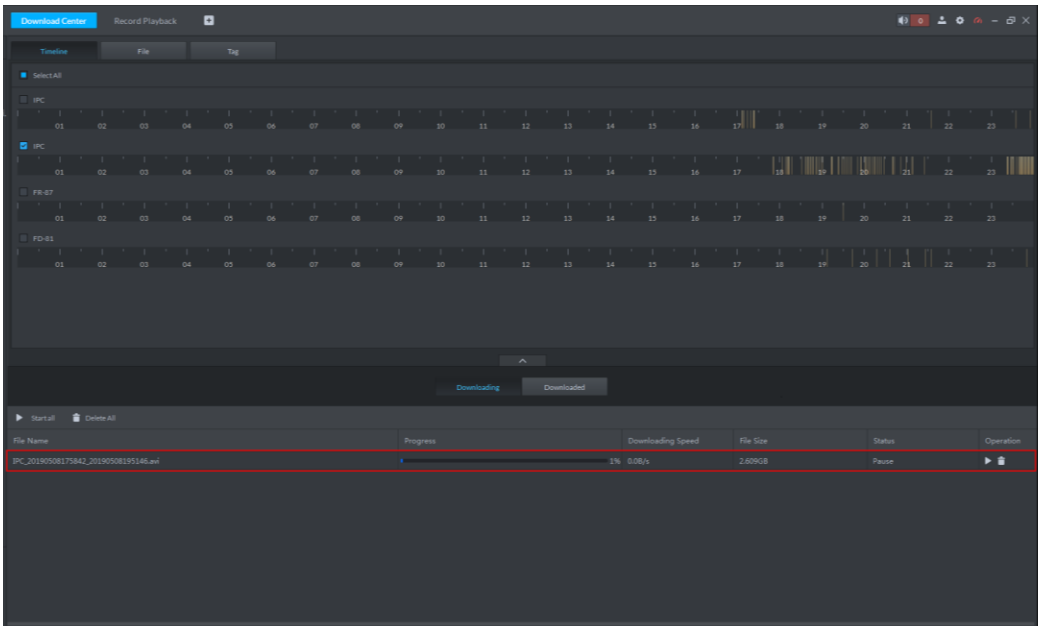
Transcode:

File Format: avi

Step 5 Confirm recording time, select file format, including dav, avi, mp4, flv and asf. Click **OK**.

The system displays download progress, see Figure 3-188. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 3-188 Download progress


Download Center
Record Playback
Timeline
File
Tag
Select All
IPC
IPC
FR-87
FD-81
Downloading
Downloaded
Start all
Delete All

File Name	Progress	Downloading Speed	File Size	Status	Operation
IPC_20190508175842_20190508195146.avi	1%	0.0B/s	2.609GB	Pause	▶

3.9.1.8.2 File

Within search period, the system automatically generates a record file after half an hour.

If hour or half an hour exists within search time, then the first file list starts from record time to the first hour or half an hour. For example, if video starts from 4:15, then the time of first record file is 4:15-4:30.

Step 1 On **Record Playback** interface, click , or click **Download Center** on the client homepage.

The system displays **Download Center** interface.

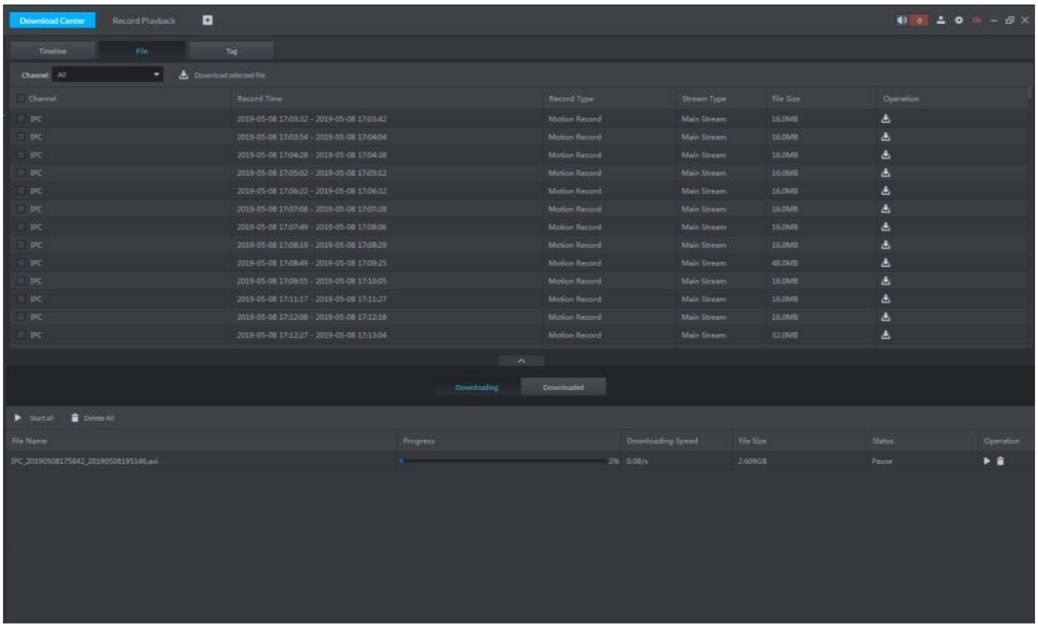
Step 2 Set search condition, click **Search**.

The system displays search result.

Step 3 Click **File** tab.

The system displays searched result in the form of file list, see Figure 3-189.

Figure 3-189 Record search result



Channel: All

☐ Channel	Record Time	Record Type	Stream Type	File Size	Operation
☐ IPC	2019-05-08 17:03:32 - 2019-05-08 17:03:42	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:03:54 - 2019-05-08 17:04:04	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:04:28 - 2019-05-08 17:04:38	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:05:02 - 2019-05-08 17:05:12	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:06:22 - 2019-05-08 17:06:32	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:07:08 - 2019-05-08 17:07:28	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:07:49 - 2019-05-08 17:08:06	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:08:19 - 2019-05-08 17:08:29	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:08:49 - 2019-05-08 17:09:25	Motion Record	Main Stream	48.0MB	⬇
☐ IPC	2019-05-08 17:09:55 - 2019-05-08 17:10:05	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:11:17 - 2019-05-08 17:11:27	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:12:08 - 2019-05-08 17:12:18	Motion Record	Main Stream	16.0MB	⬇
☐ IPC	2019-05-08 17:12:27 - 2019-05-08 17:13:04	Motion Record	Main Stream	32.0MB	⬇

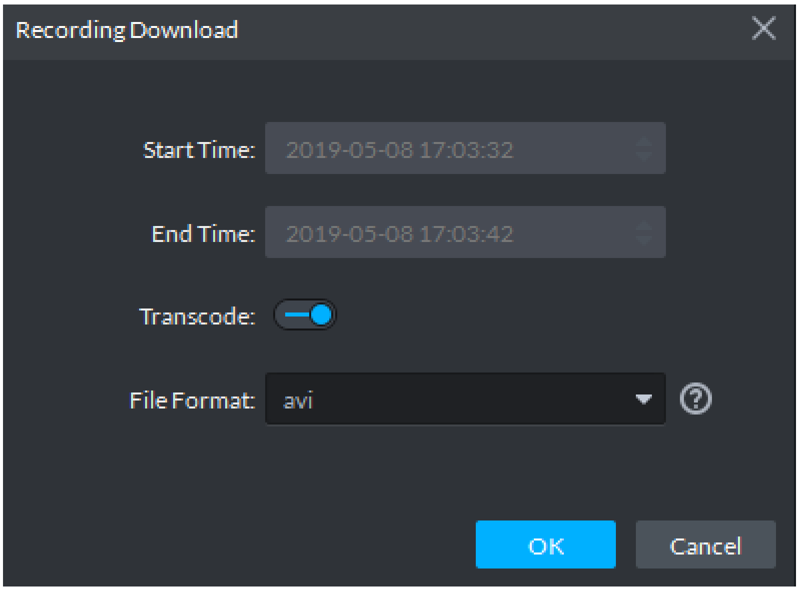
File Name	Progress	Downloading Speed	File Size	Status	Operation
IPC_20190508175842_20190508195146.avi	2%	0.0B/s	2.609GB	Pause	▶ 🗑

Step 4 Click ⬇ in the back of file list.

The system displays **Recording Download** interface, see Figure 3-190.

Select several file lists, click ⬇ on top of the interface, then you can download in batched and saved in .dav by default.

Figure 3-190 Recording download



Start Time: 2019-05-08 17:03:32

End Time: 2019-05-08 17:03:42

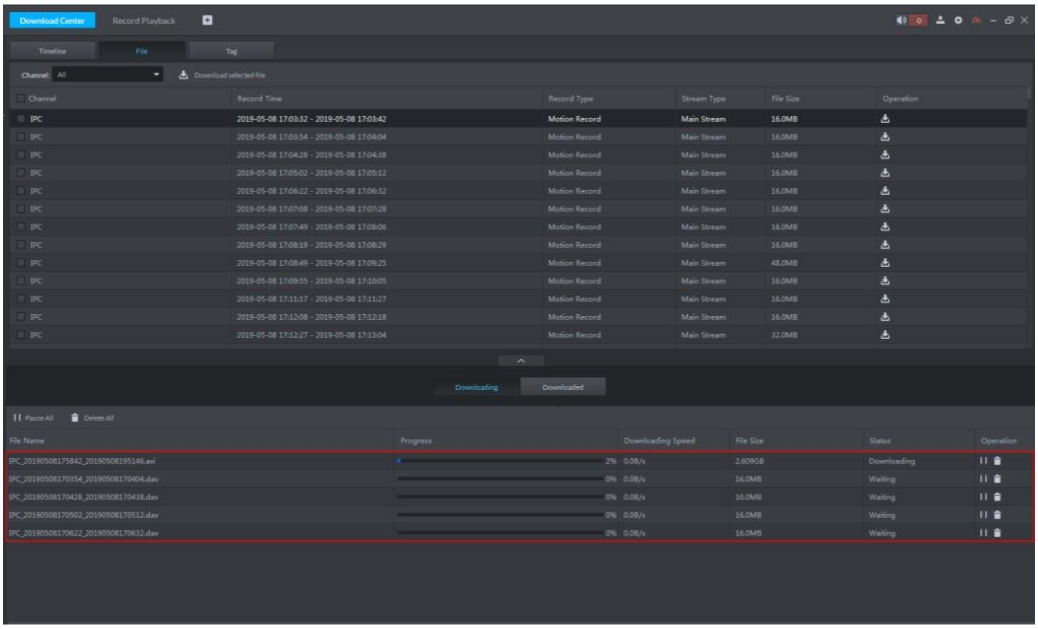
Transcode: ●

File Format: avi

Step 5 Select file format, including dav, avi, mp4, flv and asf, click **OK**.

The system displays download progress, see Figure 3-191. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 3-191 Download progress



Channel: All

Channel	Record Time	Record Type	Stream Type	File Size	Operation
IPC	2019-05-08 17:03:32 - 2019-05-08 17:03:42	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:03:54 - 2019-05-08 17:04:04	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:04:28 - 2019-05-08 17:04:38	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:05:02 - 2019-05-08 17:05:12	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:06:22 - 2019-05-08 17:06:32	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:07:08 - 2019-05-08 17:07:28	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:07:49 - 2019-05-08 17:08:06	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:08:19 - 2019-05-08 17:08:29	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:08:49 - 2019-05-08 17:09:25	Motion Record	Main Stream	48.0MB	
IPC	2019-05-08 17:09:55 - 2019-05-08 17:10:05	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:11:17 - 2019-05-08 17:11:27	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:12:08 - 2019-05-08 17:12:18	Motion Record	Main Stream	16.0MB	
IPC	2019-05-08 17:12:27 - 2019-05-08 17:13:04	Motion Record	Main Stream	32.0MB	

File Name	Progress	Downloading Speed	File Size	Status	Operation
IPC_20190508175842_20190508195146.avi	2%	0.0B/s	2.609GB	Downloading	
IPC_20190508170354_20190508170404.dav	0%	0.0B/s	16.0MB	Waiting	
IPC_20190508170428_20190508170438.dav	0%	0.0B/s	16.0MB	Waiting	
IPC_20190508170502_20190508170512.dav	0%	0.0B/s	16.0MB	Waiting	
IPC_20190508170622_20190508170632.dav	0%	0.0B/s	16.0MB	Waiting	

3.9.1.8.3 Tag

If record is tagged, then the system supports downloading video within some period before and after tag time.

Step 1 On **Record Playback** interface, click , or click **Download Center** on client homepage.

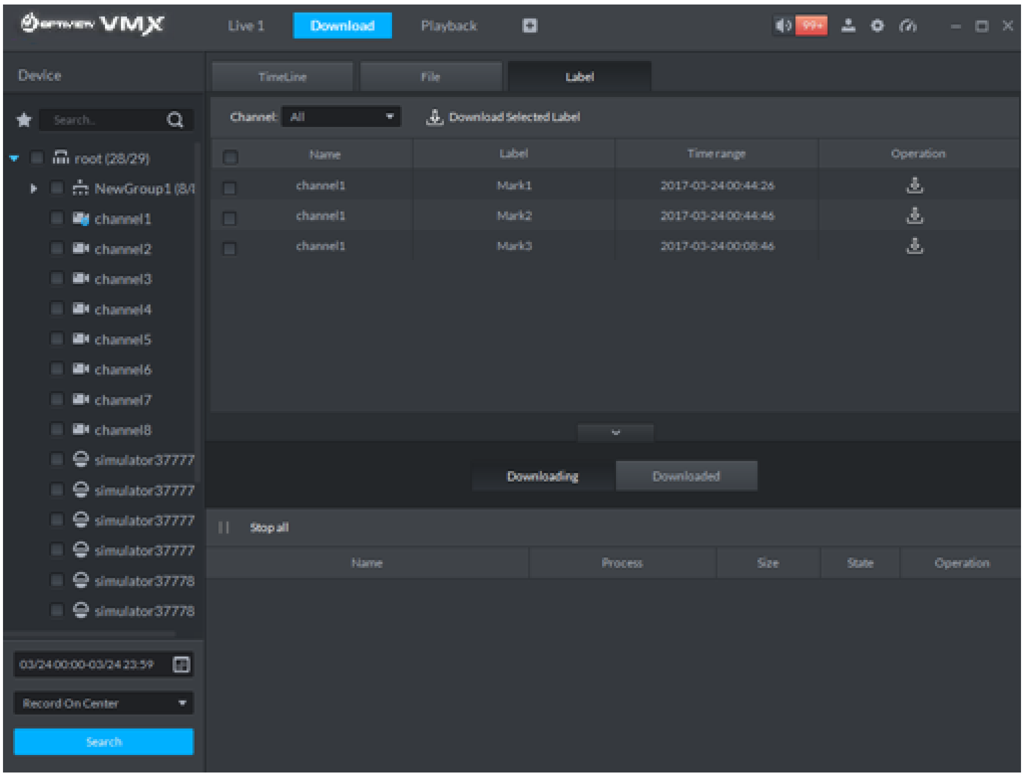
The system displays **Download Center** interface.

Step 2 Set search condition, click **Search**.

The system displays searched results.

Step 3 Click **Tag** tab.

The system displays tag file result, see Figure 3-192.



VMX
Live 1
Download
Playback
Device
Search...
root (28/29)
NewGroup1 (8/
channel1
channel2
channel3
channel4
channel5
channel6
channel7
channel8
simulator37777
simulator37777
simulator37777
simulator37777
simulator37778
simulator37778
03/24 00:00-03/24 23:59
Record On Center
Search
TimeLine
File
Label
Download Selected Label
Downloading
Downloaded
Stop all
Name
Process
Size
State
Operation

Channel: All

☐	Name	Label	Time range	Operation
☐	channel1	Mark1	2017-03-24 00:44:26	
☐	channel1	Mark2	2017-03-24 00:44:46	
☐	channel1	Mark3	2017-03-24 00:08:46	

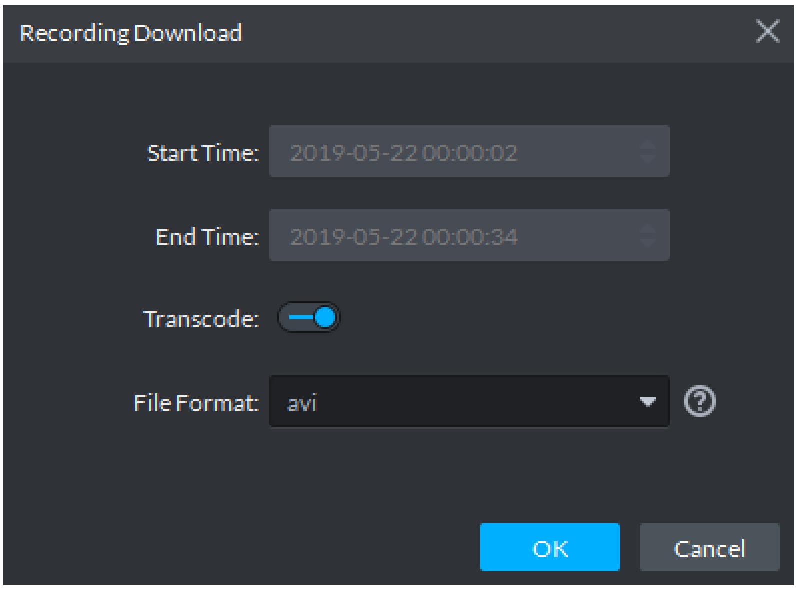
Figure 3-192 Record search result

Step 4 Click in the back of tag list.

The system displays Recording Download interface, see Figure 3-193.

Select several file lists, click on top of interface, supports download in batches.

Figure 3-193 Recording download



Recording Download
OK
Cancel

Start Time: 2019-05-22 00:00:02

End Time: 2019-05-22 00:00:34

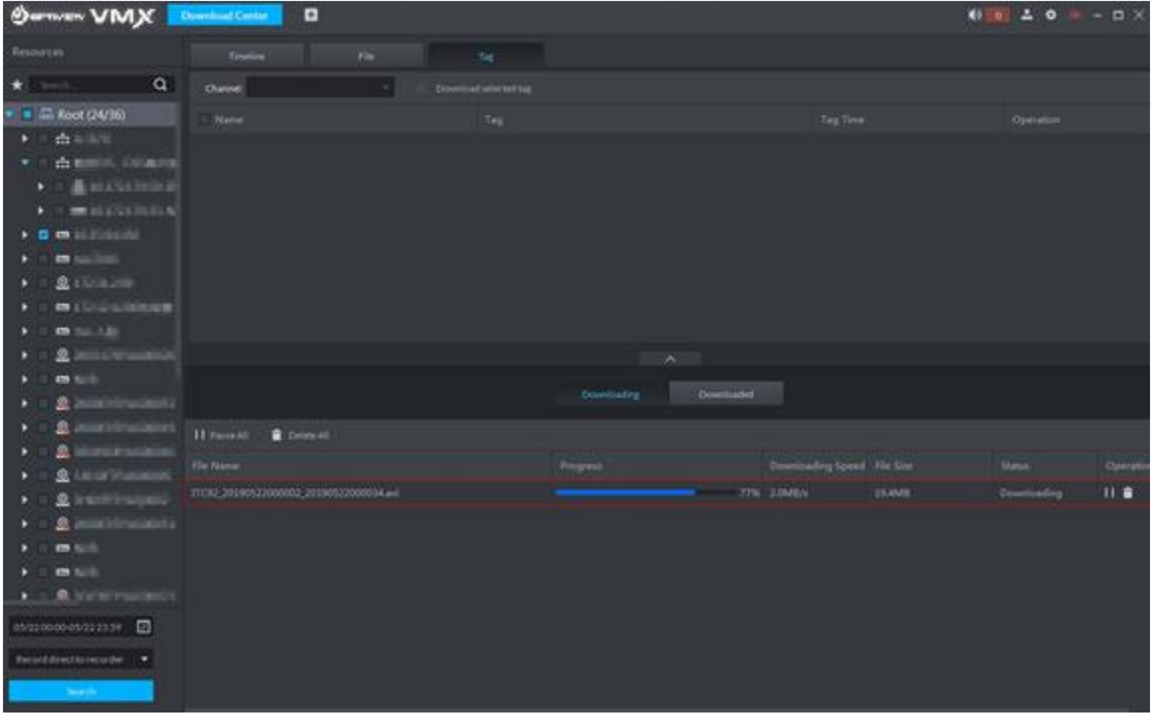
Transcode: ●

File Format: avi

Step 5 Select file format, including dav, avi, mp4, flv and asf, click **OK**.

The system displays download progress, see Figure 3-191. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 3-194 Download progress


Download Center
Resources
Root (24/36)
Timeline
File
Tag
Channel
Name
Tag
Tag Time
Operation
Downloading
Downloaded
Pause All
Delete All
File Name
Progress
Downloading Speed
File Size
Status
Operation
Search

3.9.2 POS Record Playback

Search POS receipt, check related video record. Search the video half an hour before and half an hour after POS receipt is printed, play the video 30s before the receipt is printed. For more details, refer to **3.12 POS**.

3.10 Event Center

Device reports all alarm messages, client reponds to alarm message only when corresponding alarm event is enabled. You can view and deal with corresponding alarm message on client.

For detailed operation of alarm event config, see **3.2.4 Setting Alarm Event**

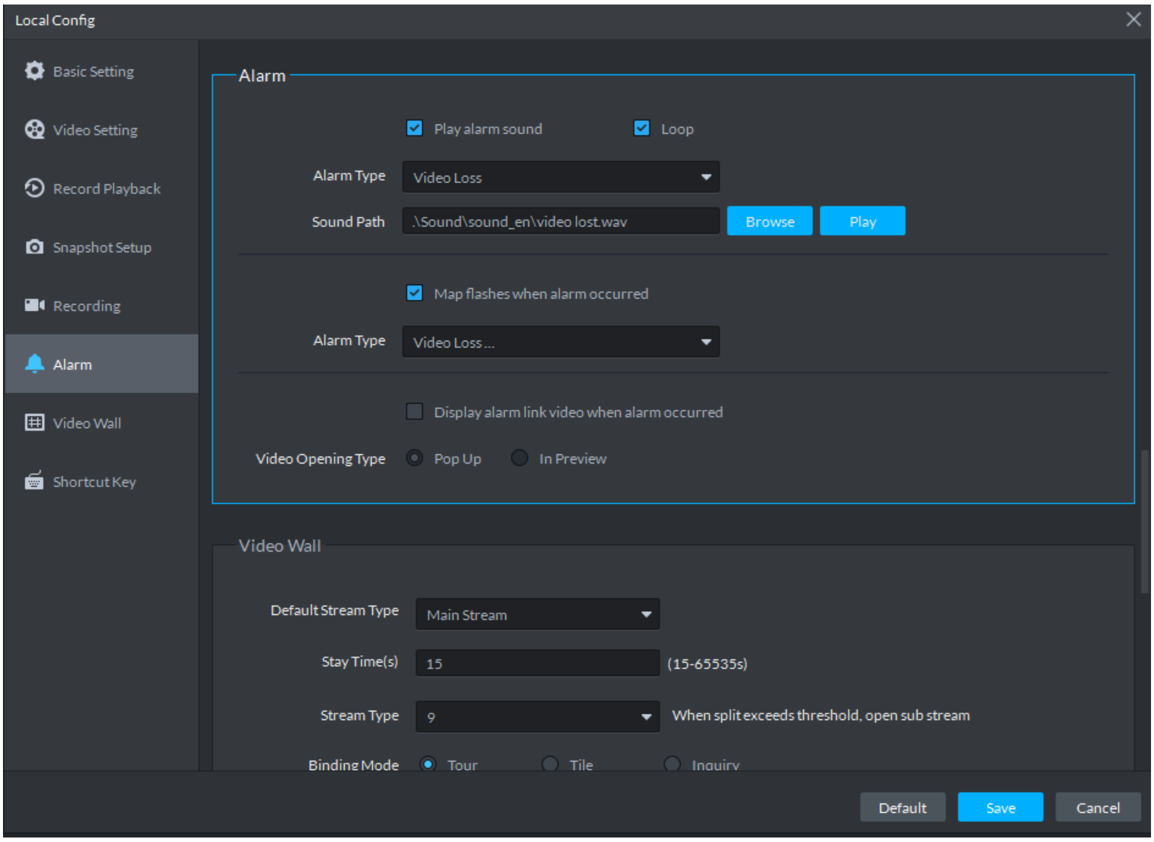
3.10.1 Setting Alarm Parameters

Configure alarm display mode on client, including alarm tone, whether flash alarm on map. Please skip the chapter if configuration is already done in **Local Config**.

Step 1 Click ⚙ at the top right corner on client interface.
The system displays **Local Config** interface.

Step 2 Click **Alarm** tab.
The system displays **Alarm** interface, see Figure 3-195.

Figure 3-195 Alarm


Local Config
Basic Setting
Video Setting
Record Playback
Snapshot Setup
Recording
Alarm
Video Wall
Shortcut Key
Alarm
Browse
Play
Video Wall
Default
Save
Cancel

☑ Play alarm sound ☑ Loop

Alarm Type: Video Loss

Sound Path: .\Sound\sound_en\video lost.wav

☑ Map flashes when alarm occurred

Alarm Type: Video Loss ...

☐ Display alarm link video when alarm occurred

Video Opening Type: ● Pop Up ○ In Preview

Default Stream Type: Main Stream

Stay Time(s): 15 (15-65535s)

Stream Type: 9 When split exceeds threshold, open sub stream

Binding Mode: ● Tour ○ Tile ○ Inquiry

Step 3 Set alarm parameters and then click **Save**. Refer to Table 3-46 for detailed information.

Table 3-46 Alarm parameter description

Parameters	Description
Play alarm sound	Check the box, system generates a sound when an alarm occurs.
Loop	Check the box; system plays alarm sound repeatedly when an alarm occurs. This item is only valid when Play alarm sound function is enabled.
Alarm type	Set alarm type. System can play sound when corresponding alarm occurs. This item is only valid when Play alarm sound function is enabled.
Sound path	It is to select alarm audio file path.
Map flashes when alarm occurred	Check the box and then select alarm type. When the corresponding alarm occurs, the device on the emap can flash.
Display alarm link video when alarm occurred	Check the box, system automatically opens linkage video when an alarm occurs.
Display type	System automatically opens linkage video when an alarm occurs. You can view on the pop-up window or on the live view interface.

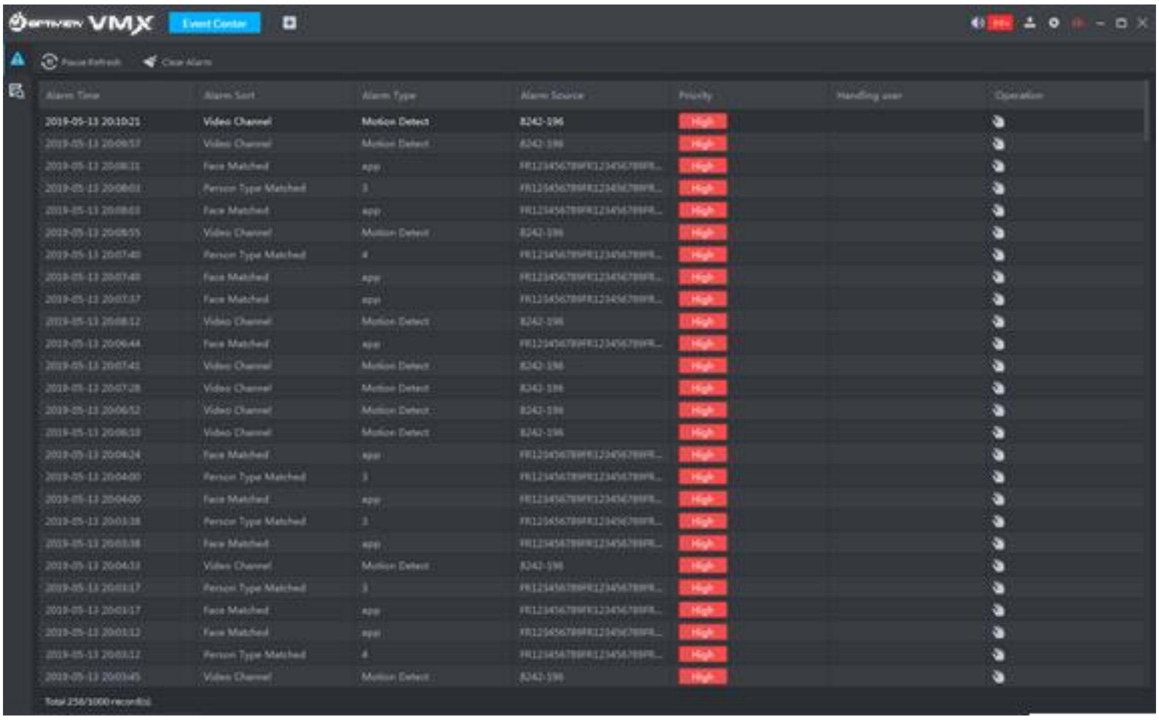
3.10.2 Searching and Processing Real-Time Alarm

After alarm is reported to client, users can claim alarm, view and confirm alarm, process alarm and register processed alarm. If alarm is claimed by user A, then other users cannot see the alarm record in real-time alarm. They can view the alarm details in histort alarm, but cannot deal with it. Client displays max 1000 real-time alarm messages.

Step 1 If alarm quantity is not zero on upper right corner of client, click the number, such as 1, or click **Event Center** on client homepage.

The system displays **Event Center** interface, see Figure 3-196.

Figure 3-196 Event center

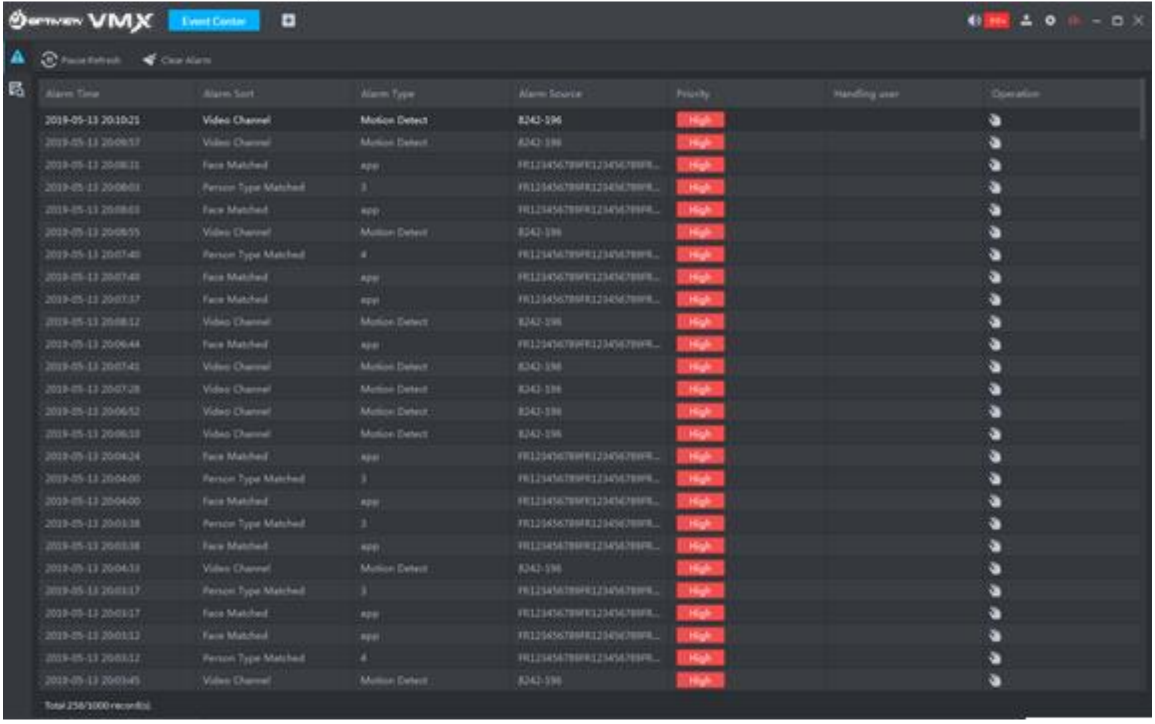


VMX
Event Center
Force Refresh
Clear Alarm
Alarm Time
Alarm Sort
Alarm Type
Alarm Source
Priority
Handling user
Operation

Step 2 Click ⚠.

The system displays **Real-time Alarm** interface, see Figure 3-197.

Figure 3-197 Real-time alarm


VMX
Event Center
Pause Refresh
Clear Alarm
Alarm Time
Alarm Sort
Alarm Type
Alarm Source
Priority
Handling user
Operation
High

- System refreshes to display real-time alarm by default. Click Pause Refresh to pause refresh, click Refresh to continue refresh.
- Click Clear Alarm and delete all alarms on real-time alarm interface, but not the data on server, you can still find it in history alarm.

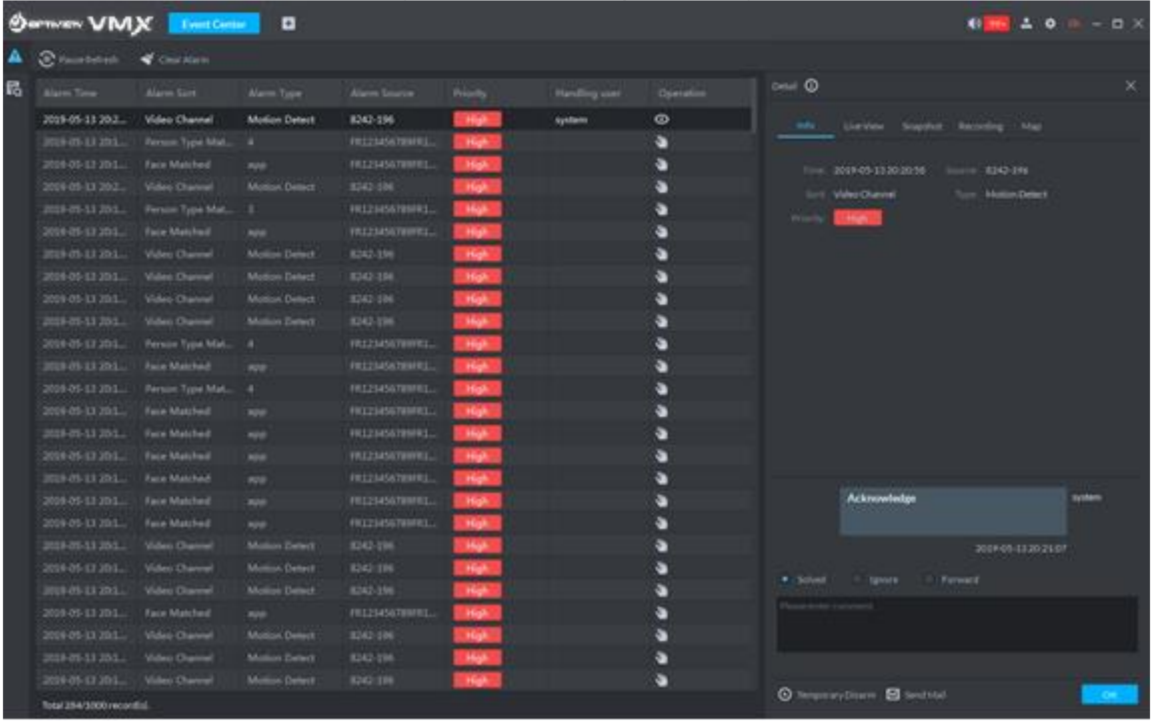
Step 3 Click of corresponding alarm.

The icon becomes , current login user claimed alarm, and then user name is displayed in the **User** column.

Step 4 Click .

The system displays alarm processing interface, see Figure 3-198.

Figure 3-198 Alarm processing


Event Center
Pause Refresh
Clear Alarm
Alarm Time
Alarm Sort
Alarm Type
Alarm Source
Priority
Handling user
Operation
Detail
Info
Live View
Snapshot
Recording
Map
Acknowledge
Solved
Ignore
Forward
Temporary Disarm
Send Mail
OK

Step 5 Click **Info**, **Live View**, **Snapshot**, **Recording** and **Map** on the right of interface, and view related information of the alarm.

Step 6 Process alarm.

- Select processing result and enter comment.
  Forward the alarm event to other users to process.
- Temporary disarm means receiving no alarm events during specific period.
- Send email, send email and inform related personnel of alarm event.

Step 7 Click **OK**.

3.10.3 Searching and Processing History Alarm

Step 1 If alarm quantity is not zero on upper right corner of client, click the number, such as 1, or click **Event Center** on client homepage.

The system displays **Event Center** interface,

Step 2 Click .

The system displays **History Alarm** interface, see Figure 3-199.

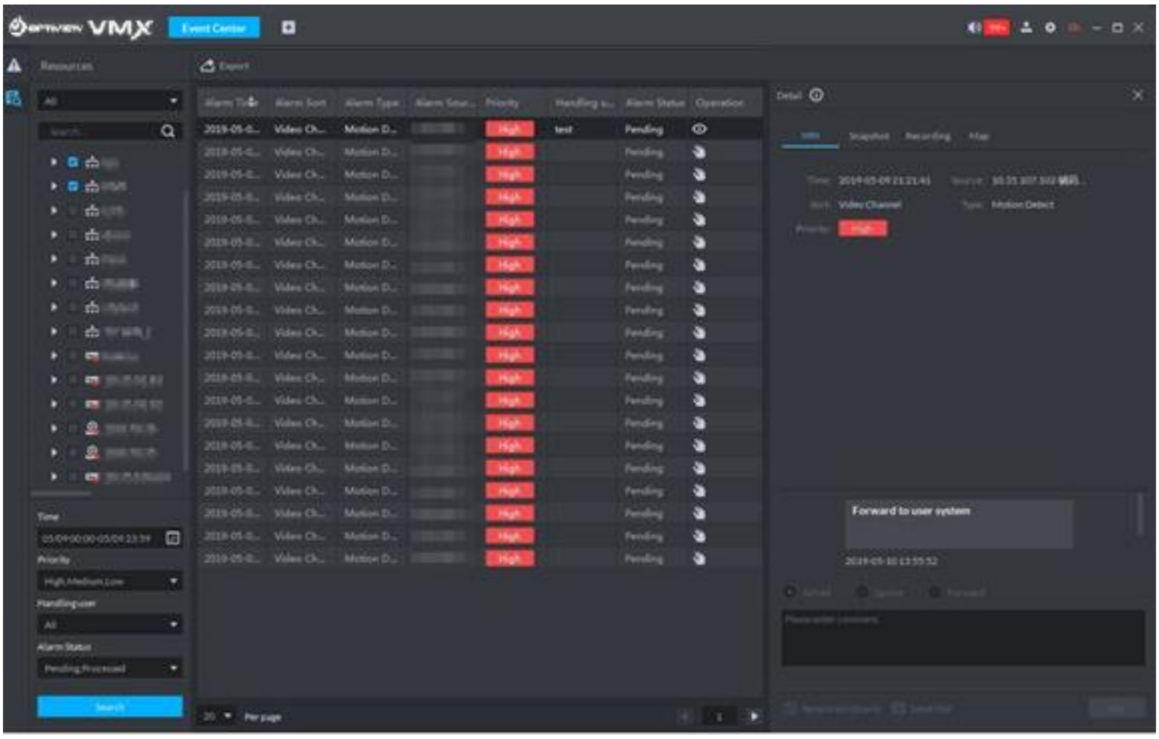

VMX
Event Center
Resources
Export
Alarm Time
Alarm Sort
Alarm Type
Alarm Sour...
Priority
Handling u...
Alarm Status
Operation
Detail
Forward to user system
Time
Priority
Handling user
Alarm Status
Search
Per page

Figure 3-199 Select alarm type

Step 3 Set search condition, click Search.

The system displays result. You can only search alarm within one month.

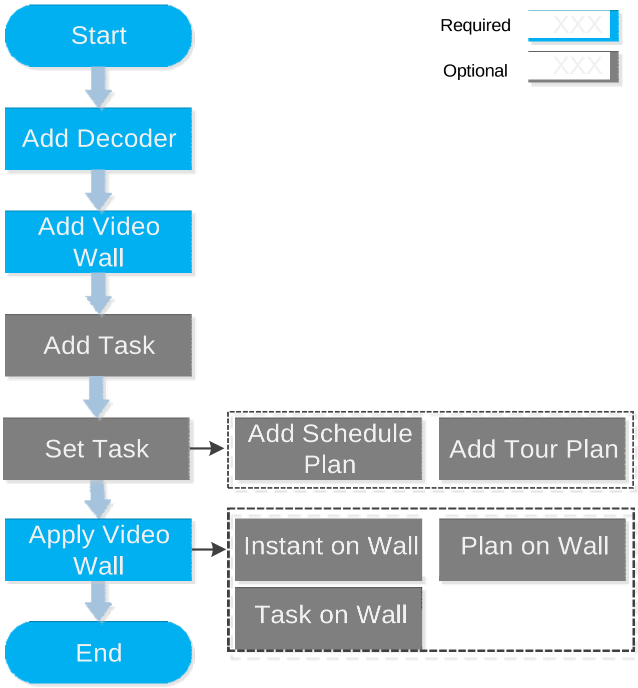
Step 4 View and process alarm. For operations, refer to 3.10.2 Searching and Processing Real-Time Alarm.

Step 5 Click **Export**, export alarm record, saved to local in the form of .xls.

3.11 Video Wall

Decoder decodes video source, output image and display on video wall. The operation flow of video wall is shown in Figure 3-200.Video wall flow

Figure 3-200 Video wall flow


Start
Required
Optional
Add Decoder
Add Video Wall
Add Task
Set Task
Add Schedule Plan
Add Tour Plan
Apply Video Wall
Instant on Wall
Plan on Wall
Task on Wall
End

3.11.1 Adding Encoder

Add decoding devices; currently support decoder, matrix and video wall. For details, see **3.2.2.4 Adding Device**

3.11.2 Entering Video Wall Interface

On client homepage, click **Video Wal**l. The system displays **Video Wall** interface. See Figure 3-201. For interface description, see Table 3-47.

Figure 3-201 Video wall

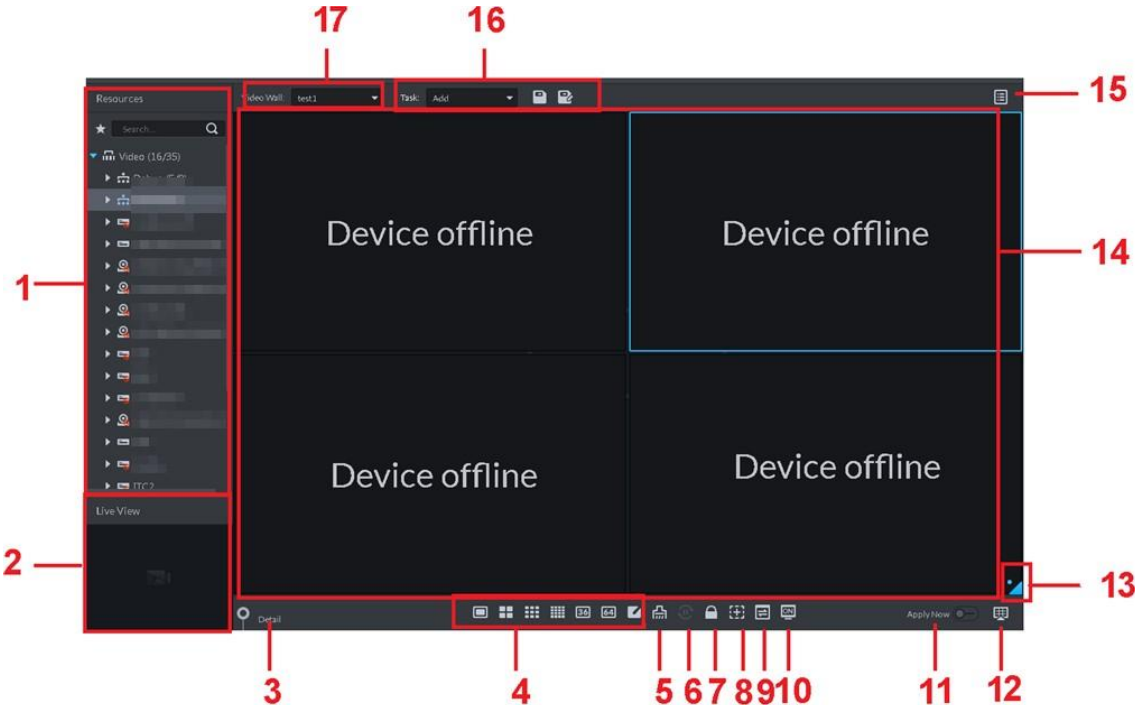

17
16
15
14
13
1
2
3
4
5
6
7
8
9
10
11
12
Resources
Search...
Video (16/35)
Live View
Video Wall
test1
Task:
Add
Device offline
Device offline
Device offline
Device offline
Detail
Apply Now

Table 3-47 Interface description

No.	Name	Function
1	Device tree	From **Local Config> General**, if you enable **Show device node**, device tree displays all channels of current device. If you cancel the box, system display all channels of all device. Click ★ to view the channels on the favorites folder. Search is supported by input device name or channel name in Search.. 🔍 here.
2	Live View	View channel video.
3	Detailed information	● Click to view the screen, window, and channel bound information. ● Click ▶ to view the video at the bottom left pane. It is to check current channel is what you want or not. ● Click ↑ ↓ to adjust sequence. ● Click 🗑 to delete the video channel that adds to current window. ● Click **Stay** time column or click ✎, modify signal interval on current channel when tour. ● Click Stream column or ✎, modify video bit stream.
4	Window split	Set window split mode.

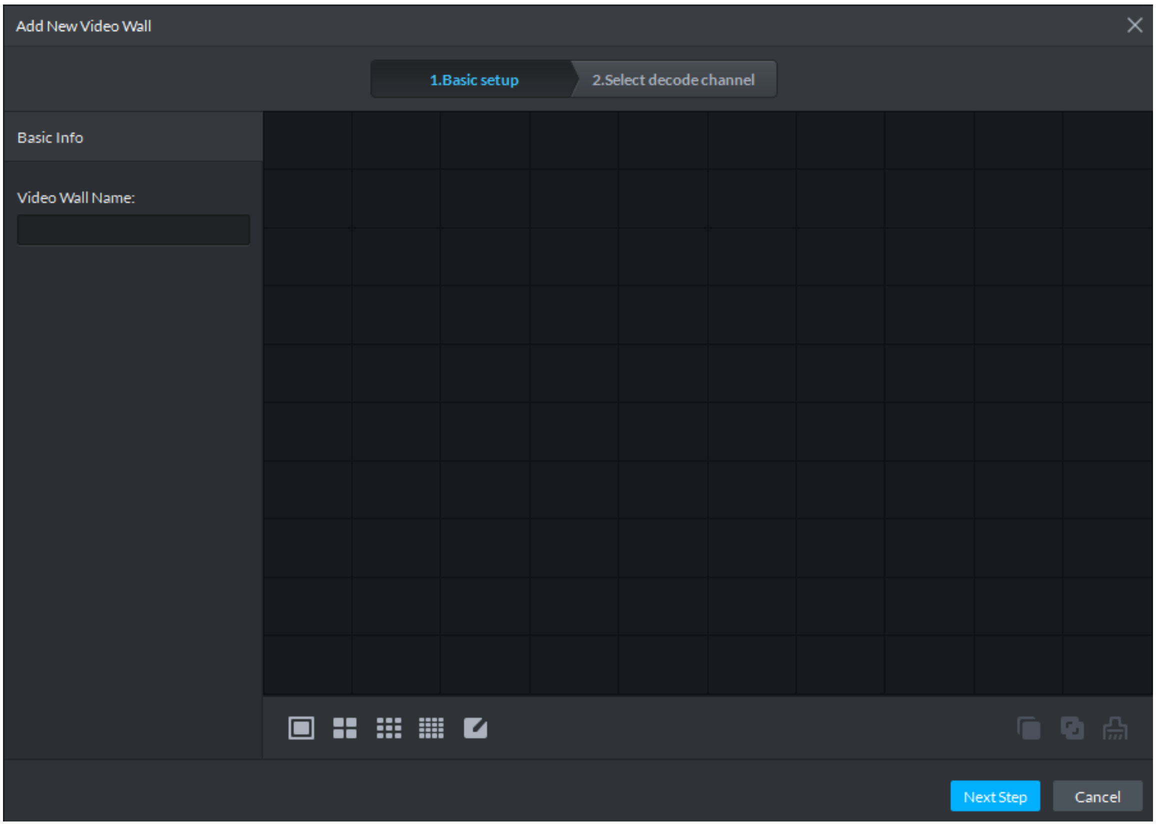
No.	Name	Function
5	Clear	Clear information on all screens.
6	Start/stop all tours	Start or stop all tours.
7	Lock window	Click to lock the window. You cannot operate on the locked window.
8	Add box	You can click to add a box, and click again to cancel box.
9	Back display	View current layout
10	Screen On/Off	In Screen On mode, the system will automatically display the video after configuring the tasks.
9	Apply now	If you enable the function, system automatically outputs the video to the wall after you set the task.
10	Decode to wall	Click to manually output the video to the wall.
11	Eagle eye	View current video wall layout
12	Video wall	Video wall area.
13	Video wall task	Set schedule task and tour task. Refer to “3.11.5 Setting Video Wall Plan for detailed information.”
14	Task management pane	Add, save delete task.
15	Video wall selection	Select a video wall to configure.

3.11.3 Adding Video Wall

Create video wall, and bind decoding channel to screen.

Step 1 On **Video Wall** interface, click drop-down box and select **Add New Video Wall**.
The system displays **Add New Video Wall** interface, see Figure 3-202.

Figure 3-202 Add new video wall


Add New Video Wall
1.Basic setup
2.Select decode channel
Basic Info
Video Wall Name:
Next Step
Cancel

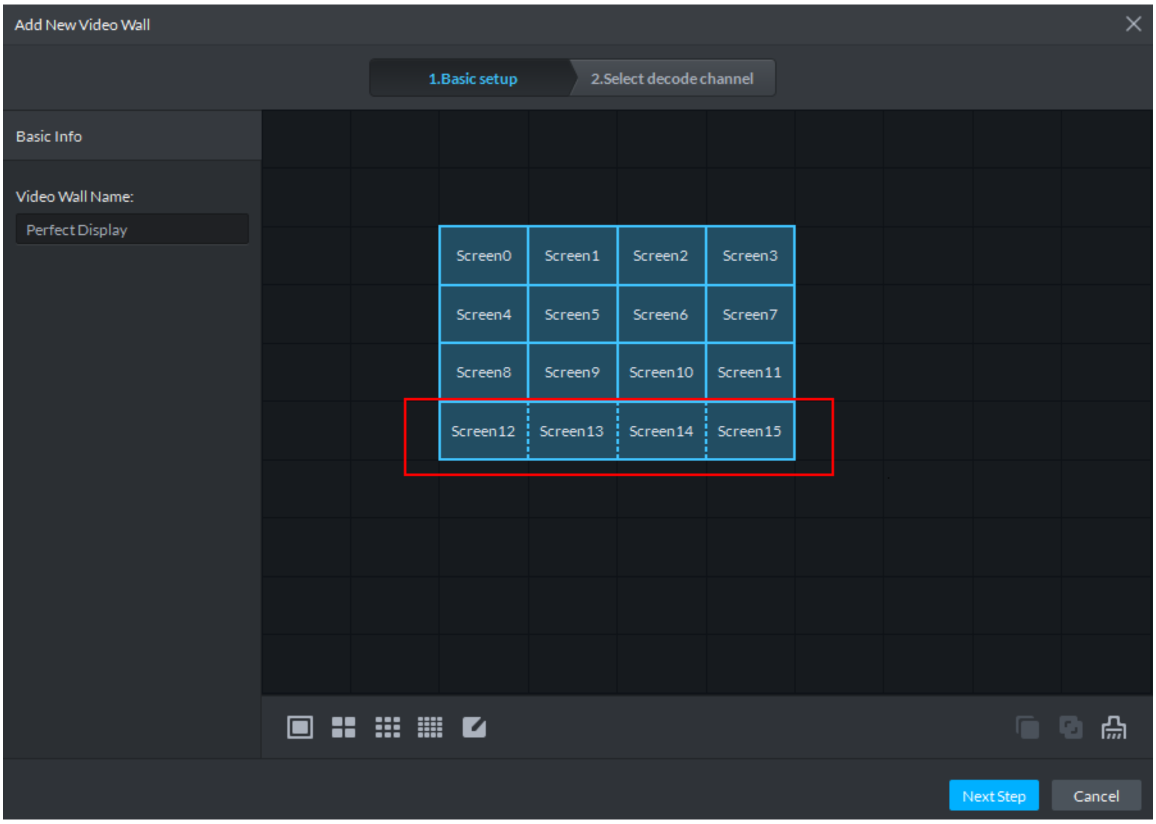
Step 2 Enter **Video Wall Name**, select screen quantity icon on the bottom, and click add anywhere on the screen.

- You can add 1 window, 4 windows, 9 windows and 16 windows, click ✎ to customize window.
- If the added window is not right, you can click to delete and add again.

Step 3 (Optional) Press **Shift** button, select several screens, click and combine the screens, see Figure 3-203.

- Please skip the step if combination screen is not needed.
- Select combination screen, click to cancel.

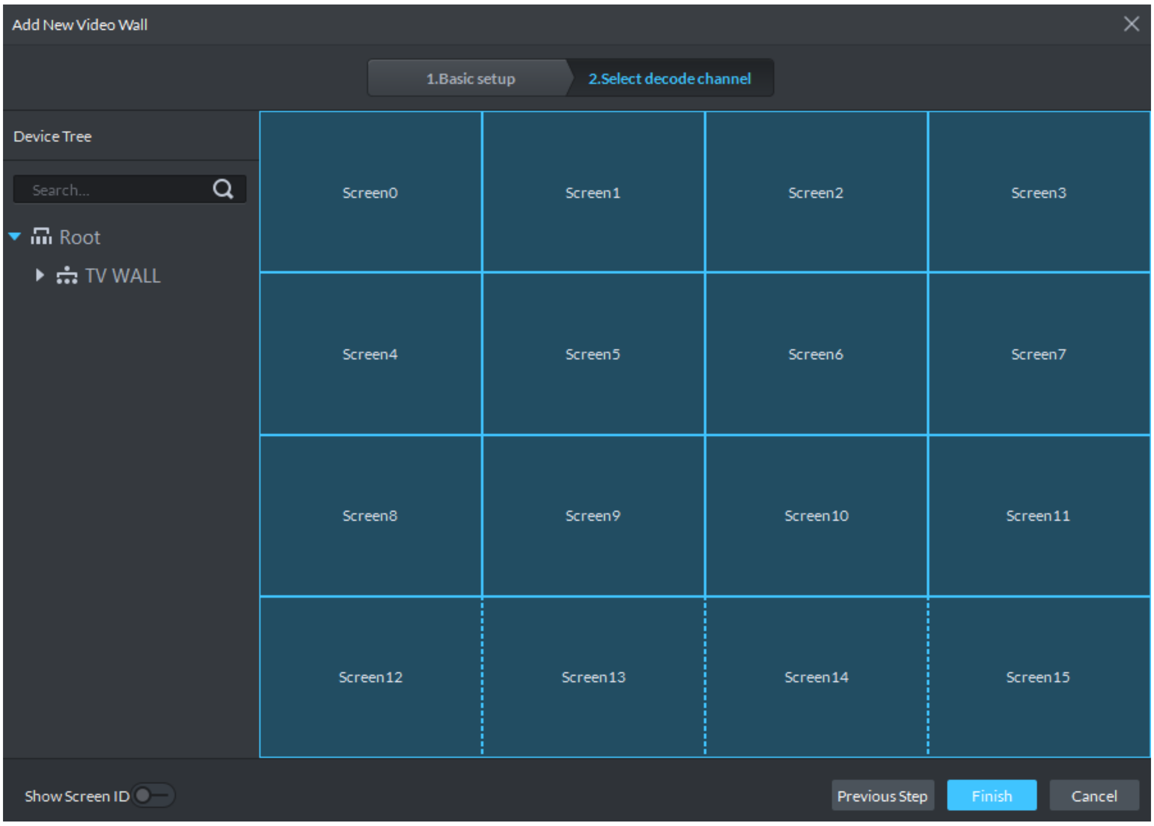
Figure 3-203 Combination Screen


Add New Video Wall
1.Basic setup
2.Select decode channel
Basic Info
Video Wall Name:
Perfect Display
Screen0
Screen1
Screen2
Screen3
Screen4
Screen5
Screen6
Screen7
Screen8
Screen9
Screen10
Screen11
Screen12
Screen13
Screen14
Screen15
Next Step
Cancel

Step 4 Click Next Step.

The system displays **Select Decode Channel**, see Figure 3-204.

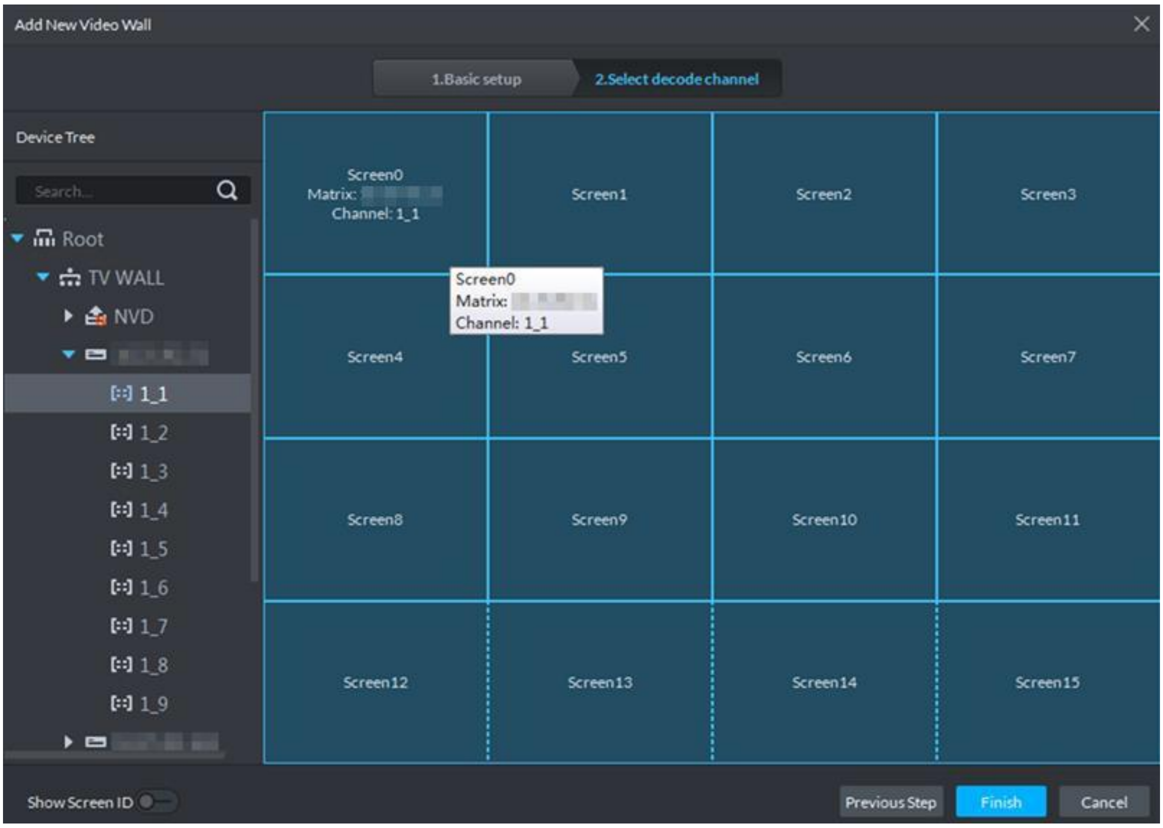
Figure 3-204 Bind decode channel


Add New Video Wall
1.Basic setup
2.Select decode channel
Device Tree
Search...
Root
TV WALL
Screen0
Screen1
Screen2
Screen3
Screen4
Screen5
Screen6
Screen7
Screen8
Screen9
Screen10
Screen11
Screen12
Screen13
Screen14
Screen15
Show Screen ID
Previous Step
Finish
Cancel

Step 5 Drag the decode channel on the left to each screen on the right for binding, see Figure 3-205.

- Each screen in combination screen must bind with decode channel.
- One video wall can bind several channels of decode device.

Figure 3-205 Binding result



Add New Video Wall
1.Basic setup
2.Select decode channel
Device Tree
Search...
Root
TV WALL
NVD
1_1
1_2
1_3
1_4
1_5
1_6
1_7
1_8
1_9
Screen1
Screen2
Screen3
Screen4
Screen5
Screen6
Screen7
Screen8
Screen9
Screen10
Screen11
Screen12
Screen13
Screen14
Screen15
Show Screen ID
Previous Step
Finish
Cancel

Screen0
Matrix: [redacted]
Channel: 1_1

Step 6 Click **OK** and video wall is added.

3.11.4 Adding Task

Save the task plan and next time you can directly call task and realize quick display on wall.

Step 1 Select **Add** from the **Task** box.

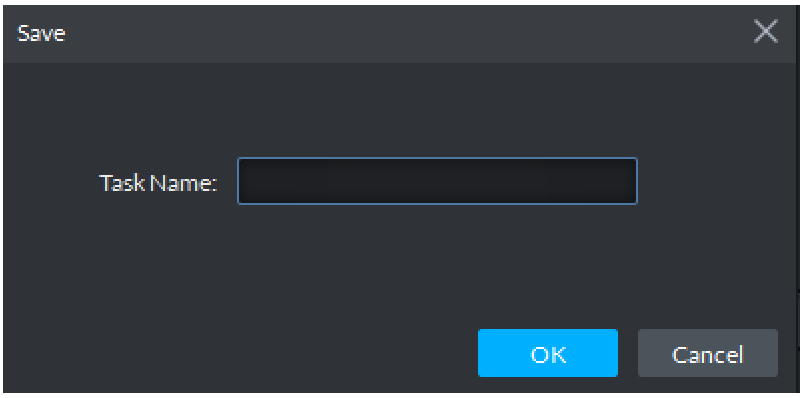
Step 2 Drag the video channel on the left to the screen on the right.

Step 3 Click .

The system displays **Save** interface, see Figure 3-206.

If you select created task from task box, then drag video channel for binding, clic and save as other task. The saved task displays on wall automatically.

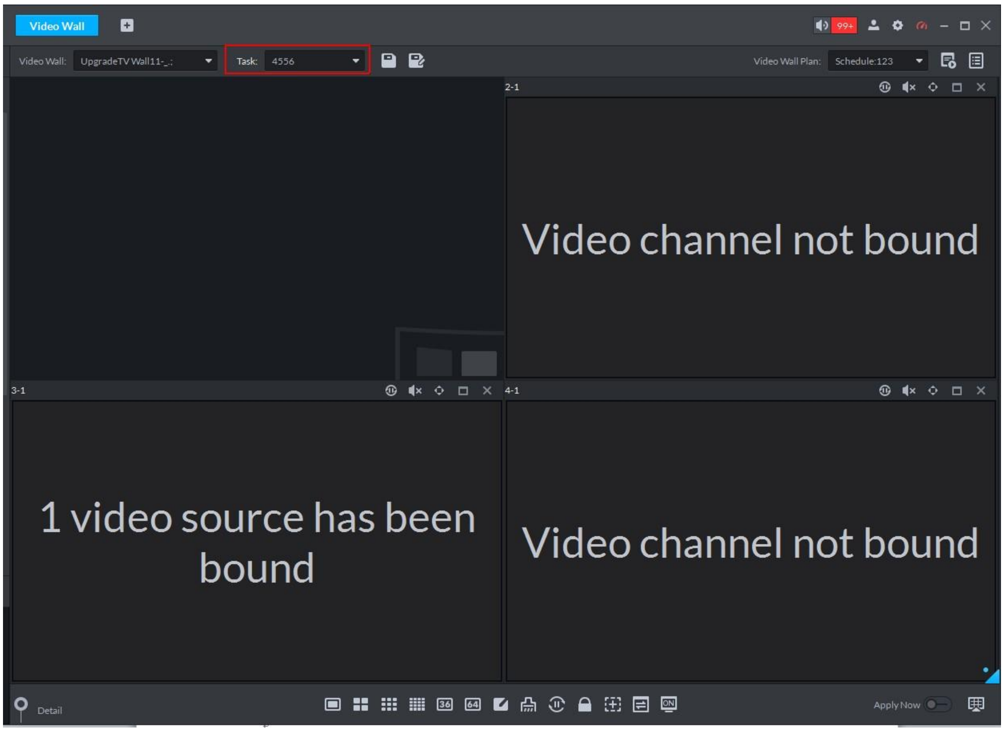
Figure 3-206 Save task



Step 4 Enter task name, click **OK** and save.

- After task is displayed on wall, and bound video channel is modified, then you need to click to display on wall manually.
- Click / and you can stop tour or start tour.

Figure 3-207 Task display on wall


Video Wall: UpgradeTV Wall11-_:

Task: 4556

Video Wall Plan: Schedule:123

2-1 Video channel not bound

3-1 1 video source has been bound

4-1 Video channel not bound

3.11.5 Setting Video Wall Plan

3.11.5.1 Adding Scheduel Plan

If task is configured, you can set task start time, end time and duration of each task, form plan and realize by schedule. If the set task occupies less than 1 day, then you can set remaining time to implement other tasks.

The task is required to be configured. For detailed operations, see **3.11.4 Adding Task**.

Step 1 On **Video Wall** interface, click ☰ on upper right corner.

The system displays interface of video wall plan, see Figure 3-208.Video wall plan

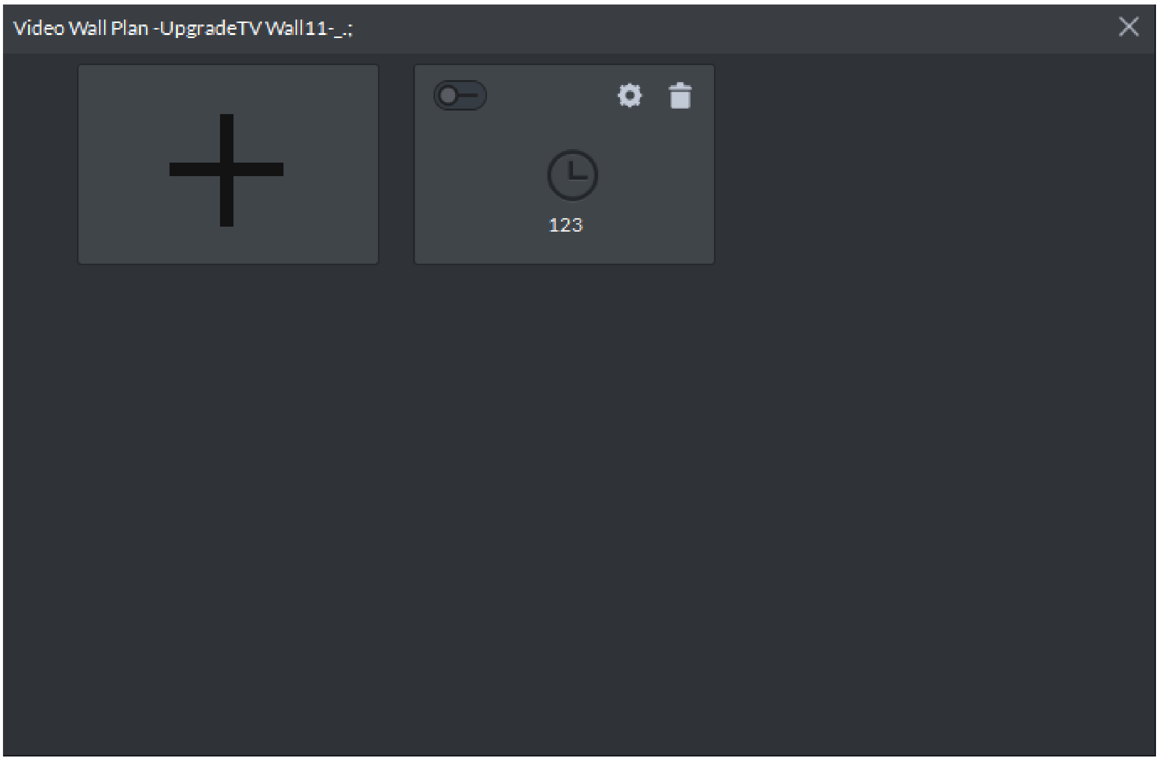


Figure 3-208 Video wall plan

Step 2 Move the mouse to “+”, select **Schedule**, see Figure 3-209.

The system displays Schedule Plan interface, see Figure 3-210.

Figure 3-209 Plan type

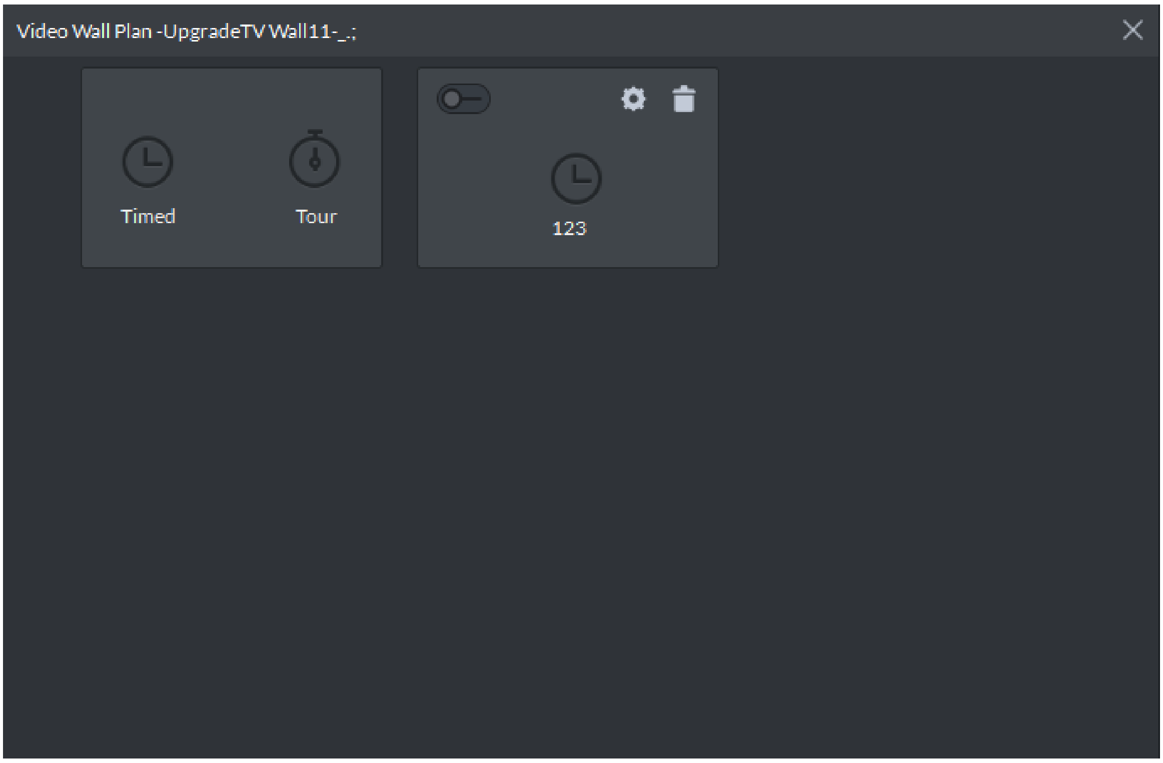
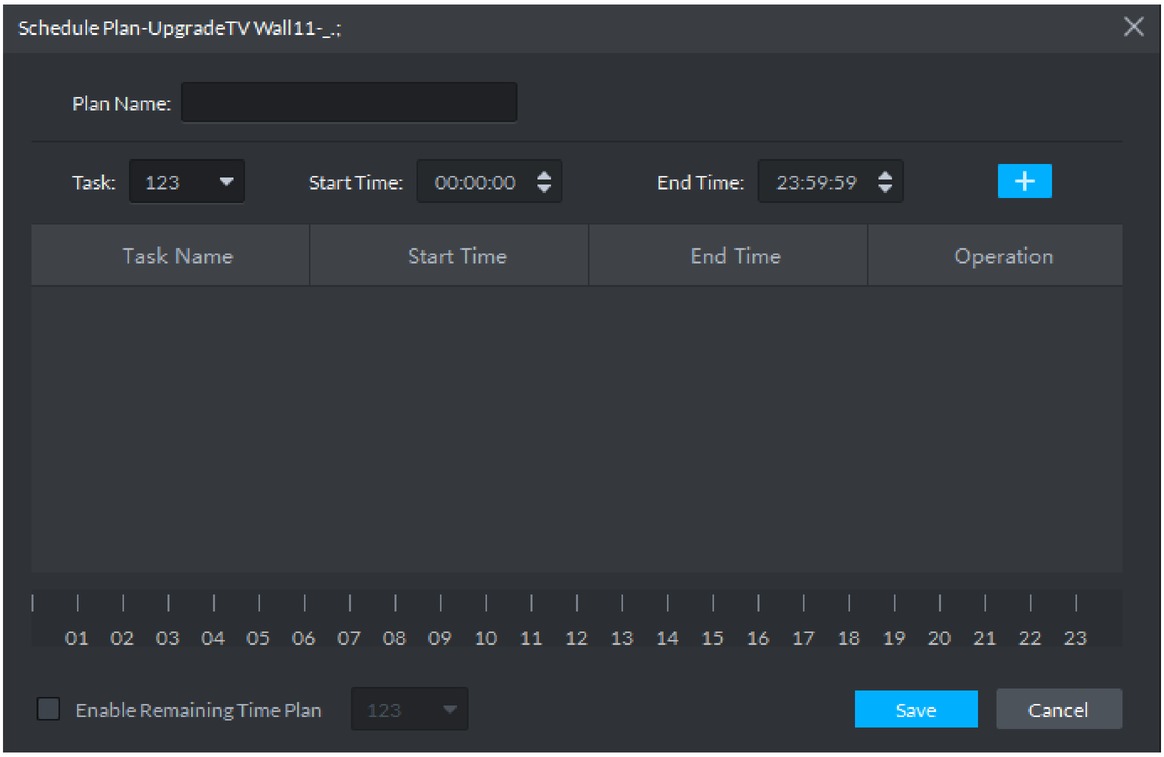

Video Wall Plan -UpgradeTV Wall11-_;
Timed
Tour
123

Figure 3-210 Add schedule plan


Schedule Plan-UpgradeTV Wall11-_;
Plan Name:
Task:
123
Start Time:
00:00:00
End Time:
23:59:59
+
Task Name
Start Time
End Time
Operation
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
☐ Enable Remaining Time Plan
123
Save
Cancel

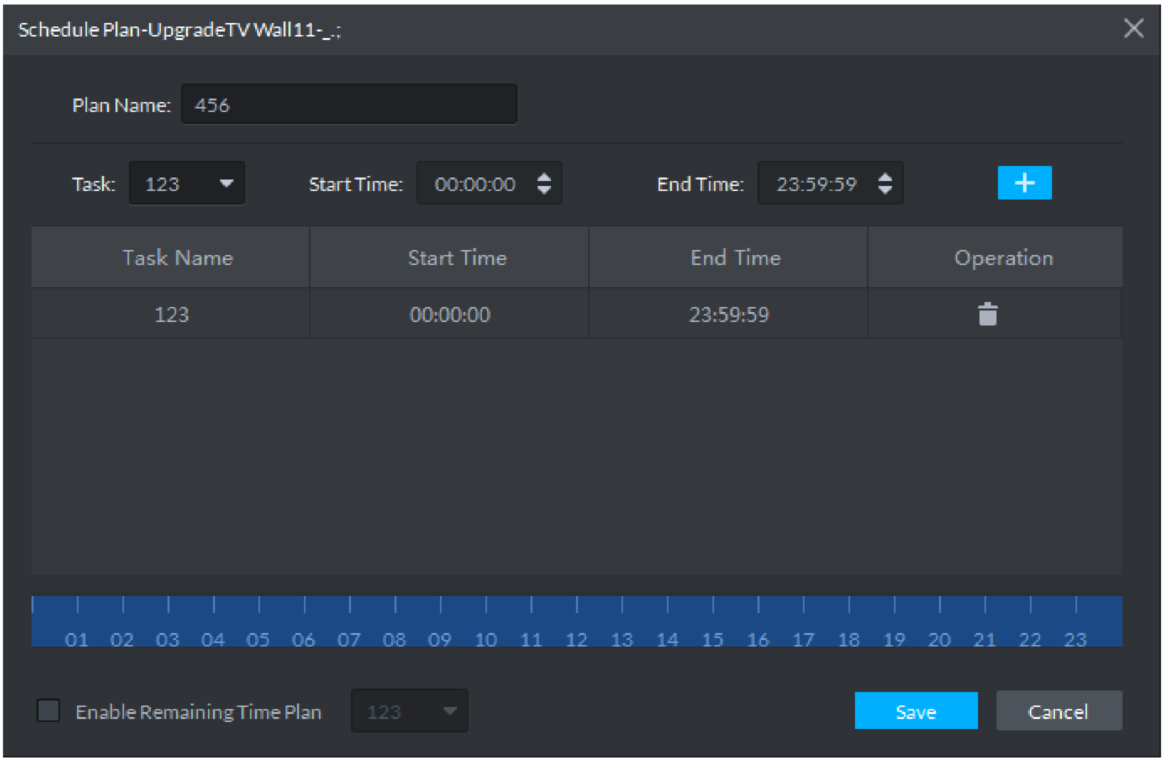
Step 3 Enter plan name.

Step 4 Select task, enter start time and end time, click "+", add to list.

Repeat the operation and you can add several tasks. But the start time and end time cannot be repeated. See Figure 3-211.

If task is added and it occupies less than 1 day, then you can select **Enable Remaining Time Plan**, and select tour plan of remaining time.

Figure 3-211 Added task



Schedule Plan-UpgradeTV Wall11-_:

Plan Name: 456

Task: 123 Start Time: 00:00:00 End Time: 23:59:59

Task Name	Start Time	End Time	Operation
123	00:00:00	23:59:59	🗑

☐ Enable Remaining Time Plan 123

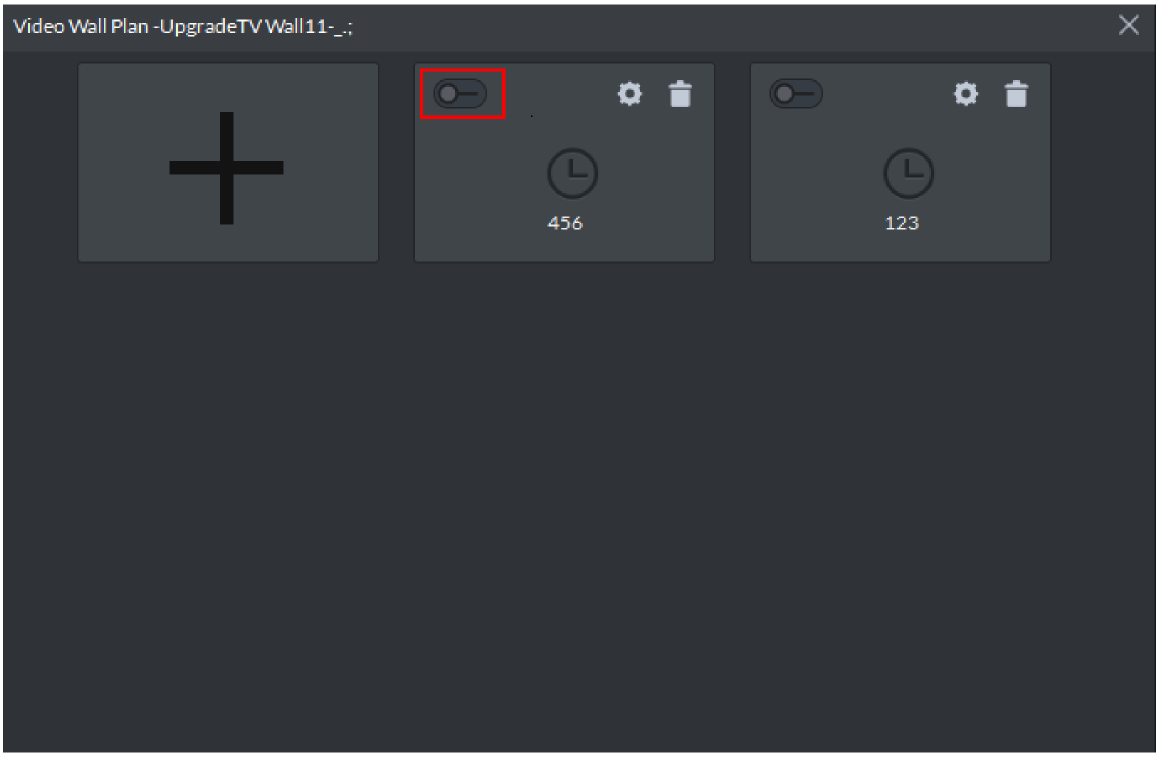
+
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
Save
Cancel

Step 5 Click **Save** to add.

Step 6 In the plan list, click ⊖ and realize schedule plan, see Figure 3-212.

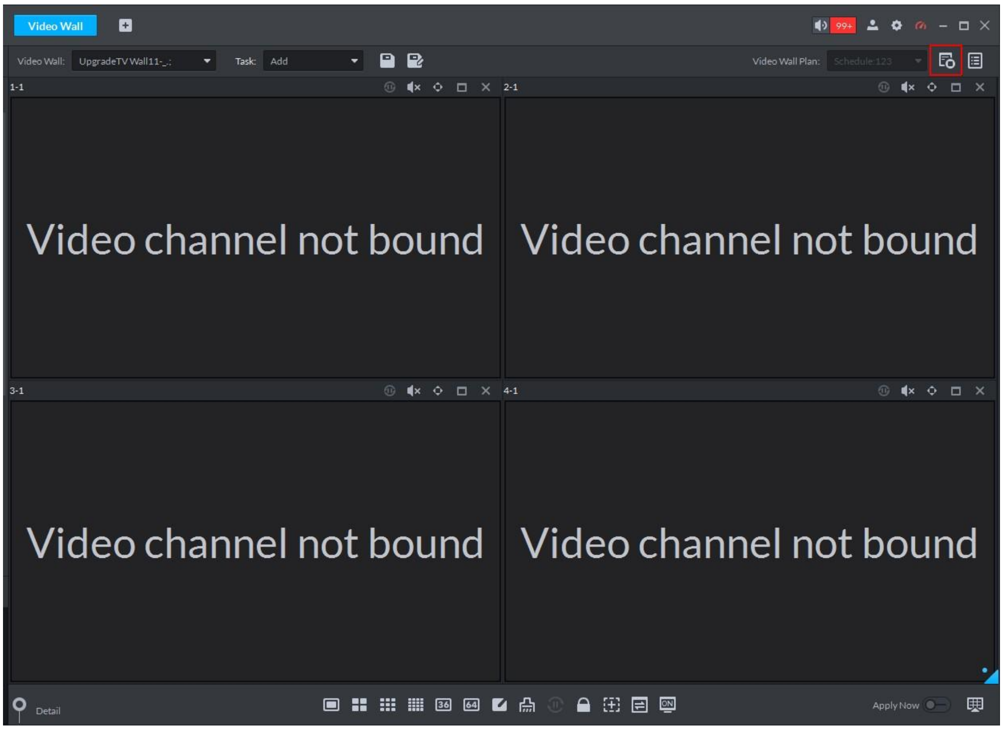
- Several plans cannot be displayed on wall at the same time; the previous plan is closed when you open another plan.
- Click ⚙ and modify plan.
- Click 🗑 and delete plan.

Figure 3-212 Enable schedule plan


Video Wall Plan -UpgradeTV Wall11-_;
456
123

If you want to stop plan, click , see Figure 3-213. The icon is switched to , click again to display on wall; If you want to switch other plans, you can enable other plan in the list.

Figure 3-213 Stop/Start plan


Video Wall
Video Wall:
UpgradeTV Wall11-_;
Task:
Add
Video Wall Plan:
Schedule:123
1-1
2-1
3-1
4-1
Video channel not bound
Video channel not bound
Video channel not bound
Video channel not bound
Detail
Apply Now

3.11.5.2 Adding Tour Plan

If the plan is configured, you can set sequence of several tasks and stay duration of each task. Display on wall in a cycle.

The task is required to be configured. For details, refer to **3.11.4 Adding Task**.

Step 1 On Video Wall interface, click ☰ on upper right corner, the system displays plan management interface, see Figure 3-214.

Step 2 Move the mouse to "+", select **Tour**, see Figure 3-214.

The system displays **Tour Plan** interface, see Figure 3-215.

Figure 3-214 Plan type

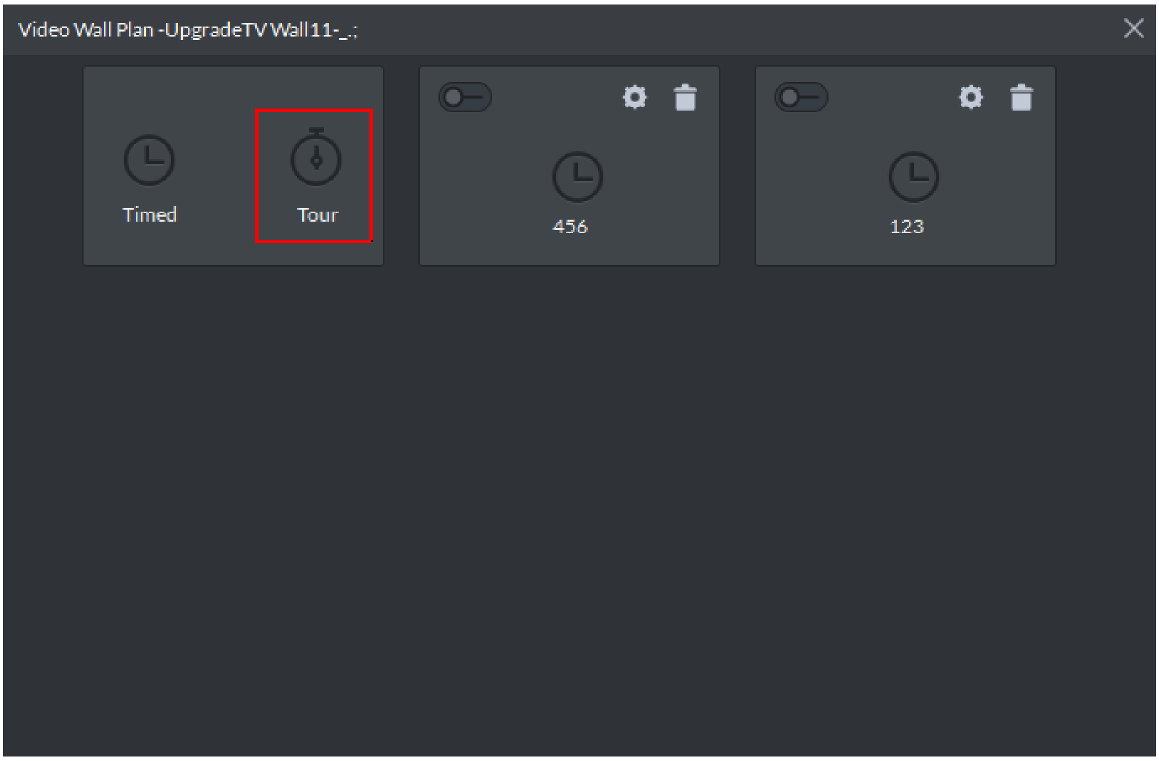
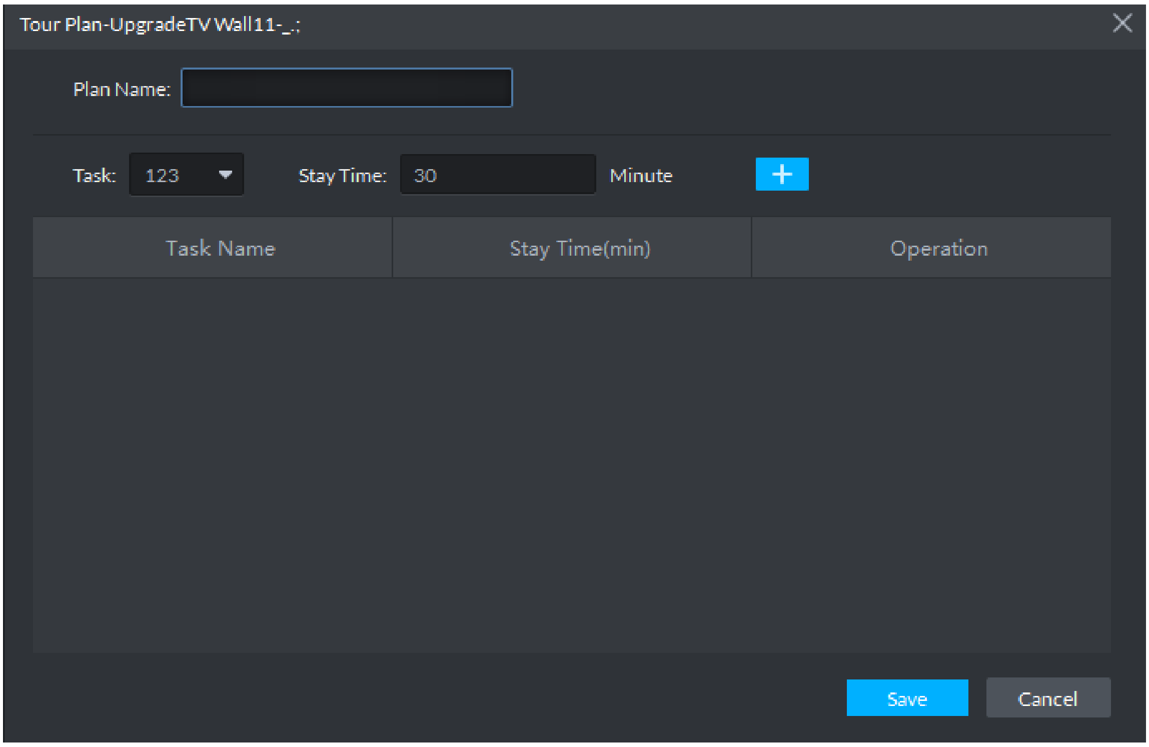

Video Wall Plan -UpgradeTV Wall11-_;
Timed
Tour
456
123

Figure 3-215 Add tour plan


Tour Plan-UpgradeTV Wall11-_;
Plan Name:
Task:
123
Stay Time:
30
Minute
+
Task Name
Stay Time(min)
Operation
Save
Cancel

Step 3 Enter plan name.

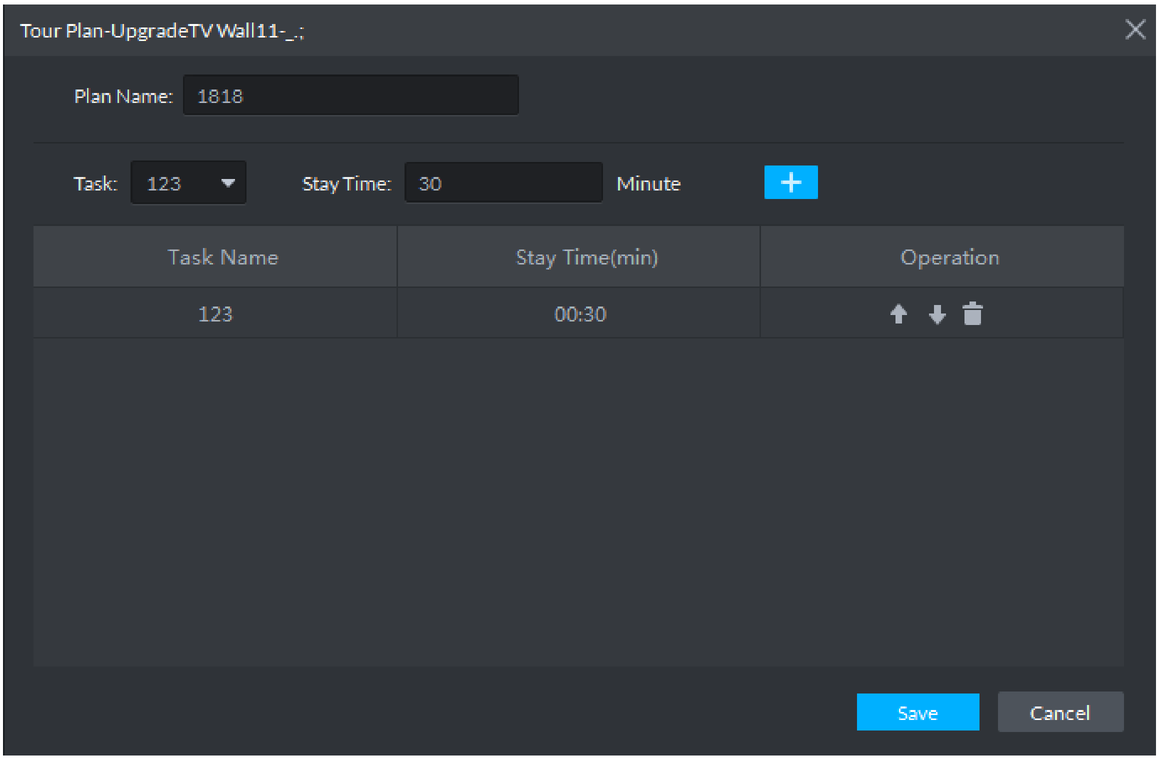
Step 4 Select task, enter stay time, click "+", add to list.

Repeat the operation and you can add several tasks, see Figure 3-216.

📖

Click ⬆ ⬇ and adjust the display sequence of taks.

Figure 3-216 Added task



Plan Name: 1818

Task: 123 Stay Time: 30 Minute

Task Name	Stay Time(min)	Operation
123	00:30	⬆ ⬇ 🗑

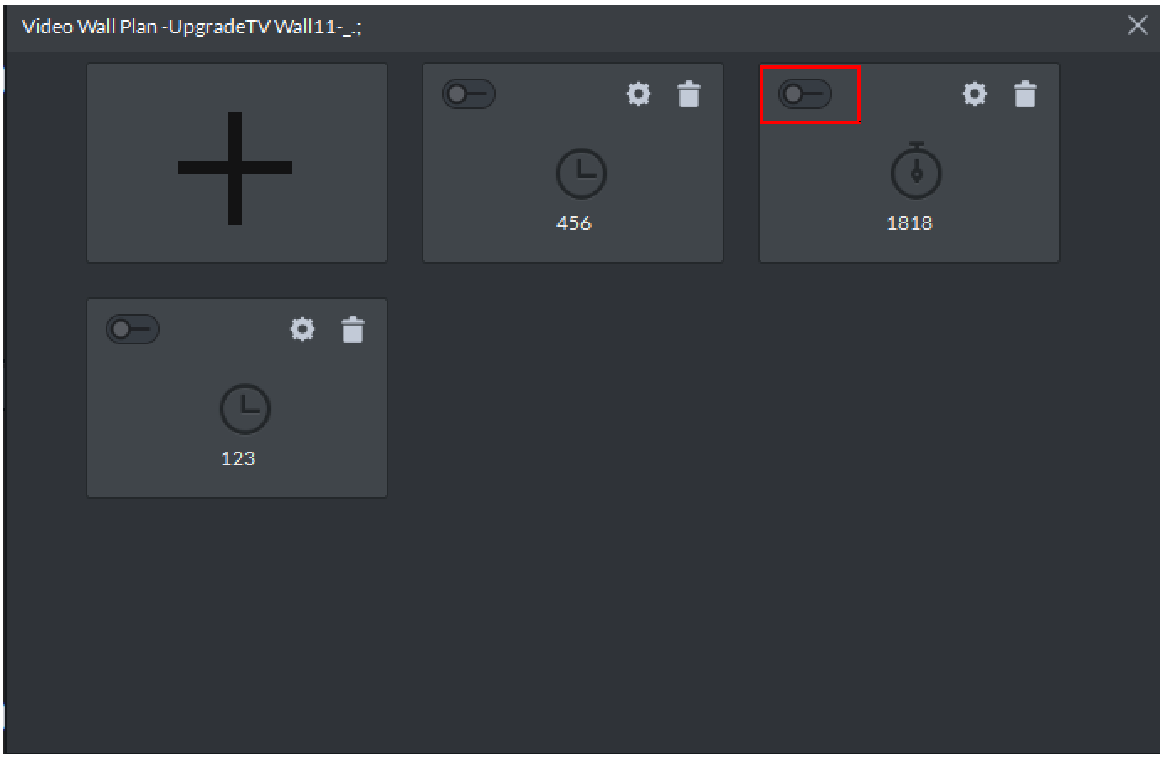
Step 5 Click **Save**, and plan is added.

Step 6 In plan list, click ⊸ and enable tour plan, see Figure 3-217.

📖

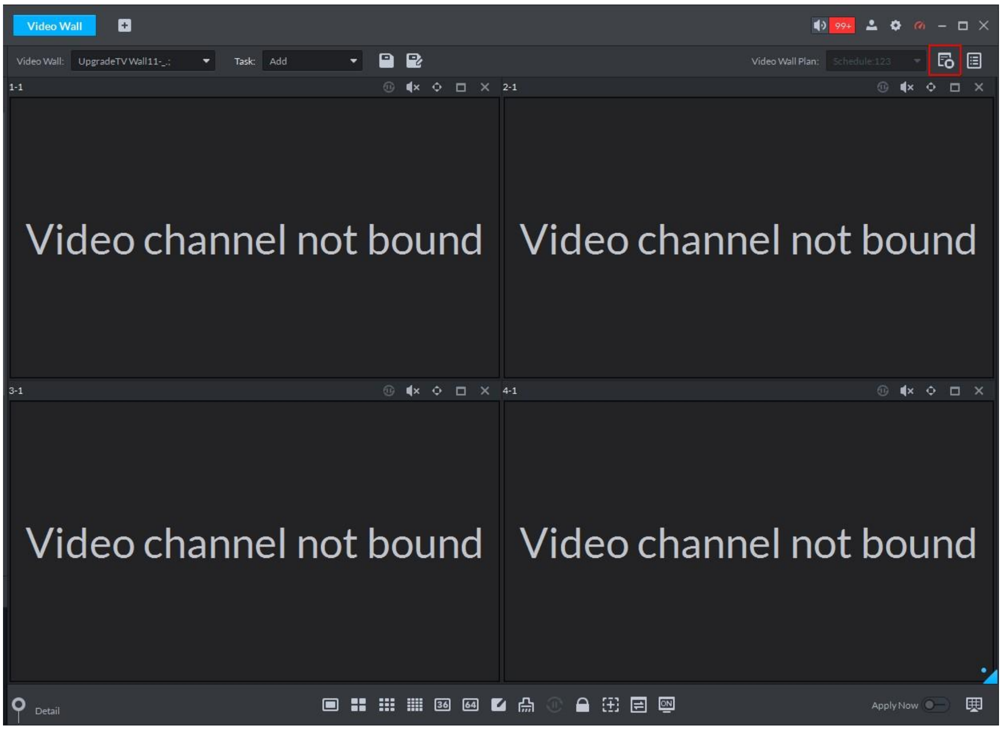
- Several plans cannot be displayed on wall at the same time; the previous plan is closed when you open another plan.
- Click ⚙ and modify plan.
- Click 🗑 and delete plan.

Figure 3-217 Enable tour plan


Video Wall Plan -UpgradeTV Wall11-_:
456
1818
123

If you want to stop plan, click , see Figure 3-218. The icon is switched to , click again to display on wall; If you want to switch other plans, you can enable other plan in the list.

Figure 3-218 Stop/Start plan


Video Wall
Video Wall:
UpgradeTV Wall11-_:
Task:
Add
Video Wall Plan:
Schedule123
1-1
2-1
Video channel not bound
Video channel not bound
3-1
4-1
Video channel not bound
Video channel not bound
Detail
Apply Now

3.11.6 Applying Video Wall

Encoding device is required to be connected to video wall, otherwise it cannot be displayed on wall.

3.11.6.1 Apply Now

Drag video channel to screen and display on wall directly.

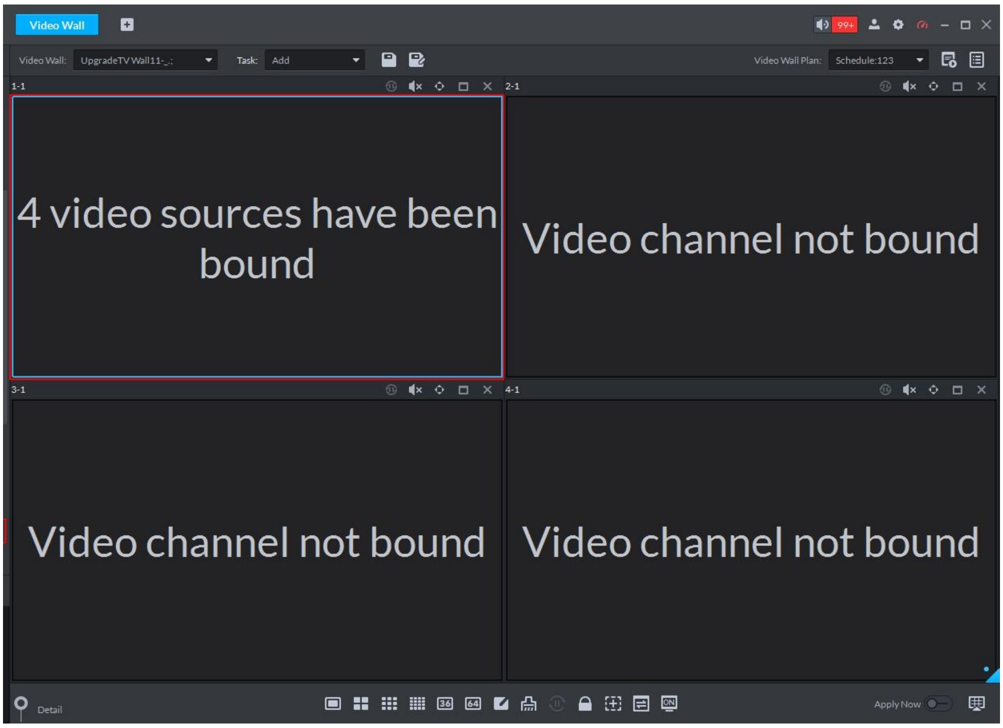
Step 1 Select video wall from the box.

Step 2 Click Apply Now on lower right corner, and enable the function of displaying on wall instantly.

Step 3 Drag left video channel to right screen for binding, see Figure 3-219.

If you select fisheye channel display on wall, right-click to select fisheye mounting mode and realize fisheye dewarping, see Figure 3-220.

Figure 3-219 Bind video channel



Video Wall: UpgradeTV Wall11-_.:

Task: Add

Video Wall Plan: Schedule:123

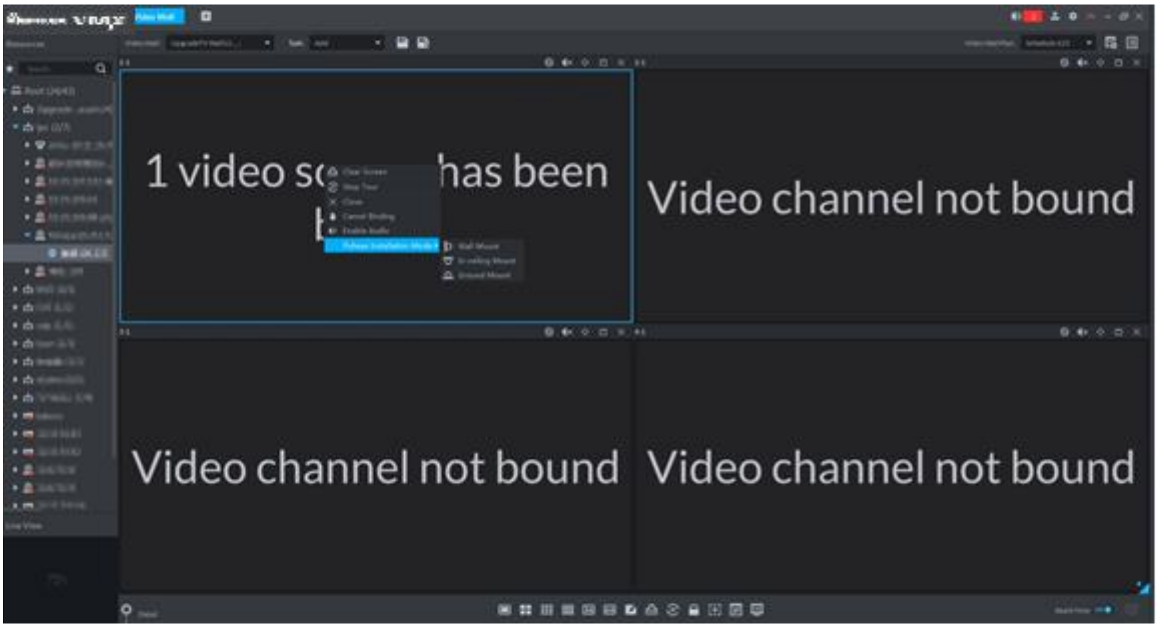
4 video sources have been bound

Video channel not bound

Video channel not bound

Video channel not bound

Figure 3-220 Fisheye dewarp


1 video s has been

Video channel not bound

Video channel not bound

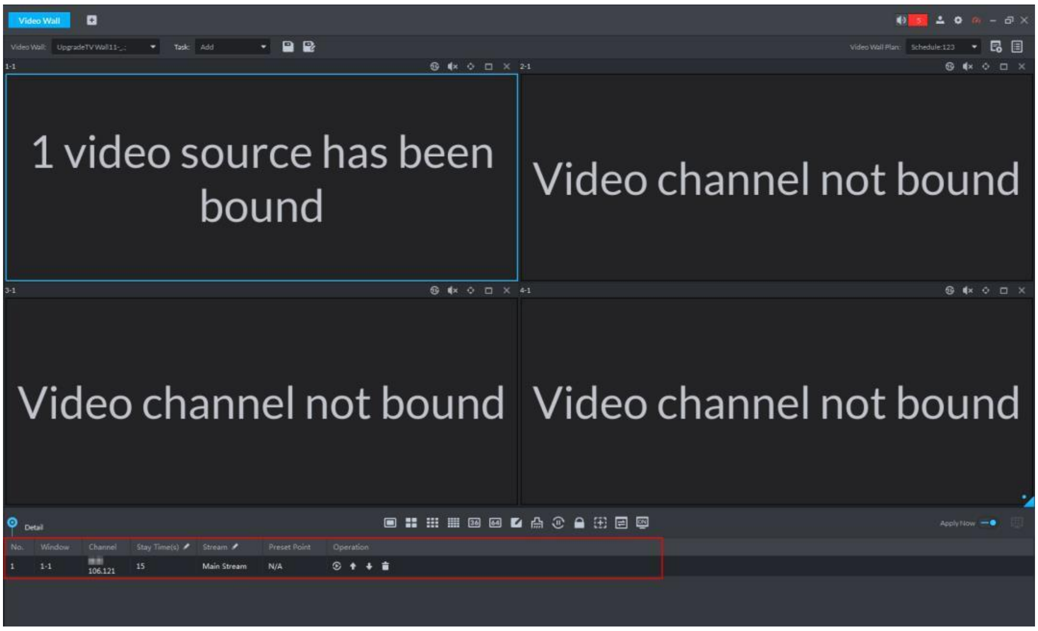
Video channel not bound

Step 4 Select screen, click **Detail** on the bottom.

System displays setting interface of channel, see Figure 3-221. View the bound video channel info, meanwhile you can set stay time, stream type, preset and operation of each video channel.

- Click ⊙ and open the channel’s real-time video on lower left corner.
- When binding several video sources; click ⬆/ ⬇, adjust display sequence.
- Click 🗑 and delete video source.

Figure 3-221 Set video channel parameter



1 video source has been bound

Video channel not bound

Video channel not bound

Video channel not bound

No.	Window	Channel	Stay Time(s)	Stream	Preset Point	Operation
1	1-1	[redacted] 106.121	15	Main Stream	N/A	⊙ ⬆ ⬇ 🗑

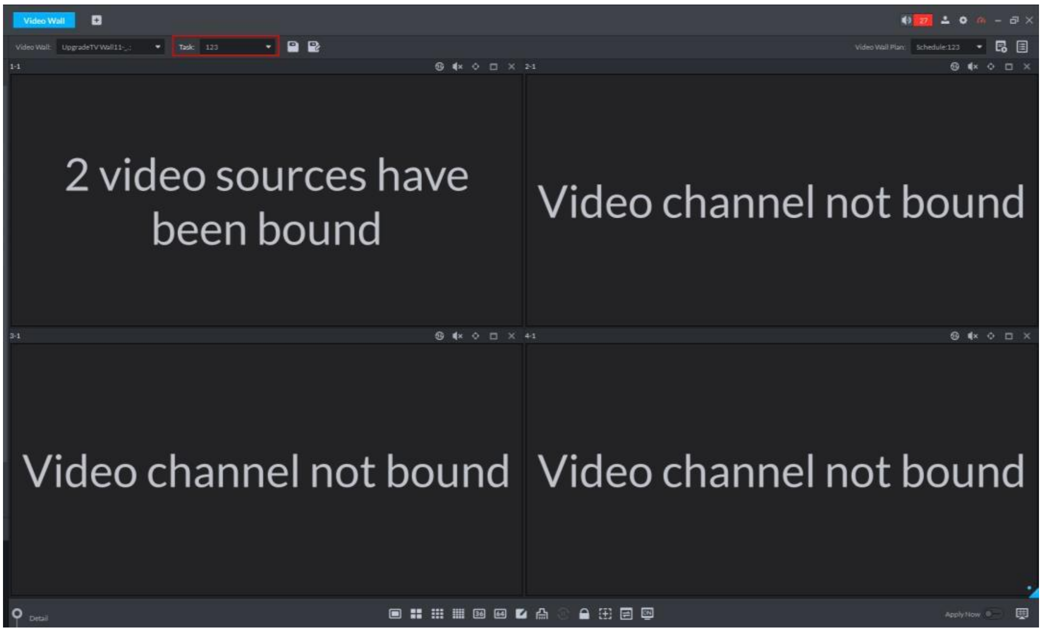
3.11.6.2 Task Displayed on Wall

Call configured task plan and realize quick display on wall.

The task is required to be configured, for detailed configuration operation, see **3.11.4 Adding Task**

Select task from the box, task is automatically displayed on wall. See Figure 3-222.

Figure 3-222 Task displayed on wall



2 video sources have been bound

Video channel not bound

Video channel not bound

Video channel not bound

Support following operations after displayed on wall.

- After task is displayed on wall, if bound video channel is modified, then you need to click on lower right corner and display on wall manually.
- Task displayed on wall, click / on the bottom, then you can stop or start tour.
- Select screen, click **Detail** on the bottom. You can view info of bound video channel; meanwhile you can set stay time, stream type, preset and operation for each video channel.
  - ◇ Click , open real-time video of the channel on lower left corner.
  - ◇ When binding several video sources, click / , and adjust display sequence of video source.
  - ◇ Click and delete video source.

3.11.6.3 Plan Displayed on Wall

According to the timed plan and tour plan that have been set, display on wall automatically with specific period. For details of configuration plan, refer to "3.11.5 Setting Video Wall Plan."

3.12 POS

If NVR with POS channel is added on Web, then you can view related video and playback of POS channel on client.

3.12.1 Adding Encoder

Platform needs to connect to NVR with POS channel, and then POS function is realized.

Step 1 Add NVR with POS channel. For detailed operation, refer to 3.2.2.4 Adding Device

Step 2 On **Bind Resource** interface, bind POS channel as video channel.

After video channel is bound, you can view related channel video in live view, during record playback, you can play the video before and after POS receipt is generated, and then bind video of video channel.

- The added NVR binds at least one POS channel.
- The panoramic camera is required to be added to platform before binding resources.

1) On client homepage, click **Config**.

   The system displays **Config** interface.

2) In left device tree, select POS channel, click **Bind Resource**, and see Figure 3-223.

   The system displays **Bind Resource** interface, see Figure 3-224.

Figure 3-223 Enter bind resource interface

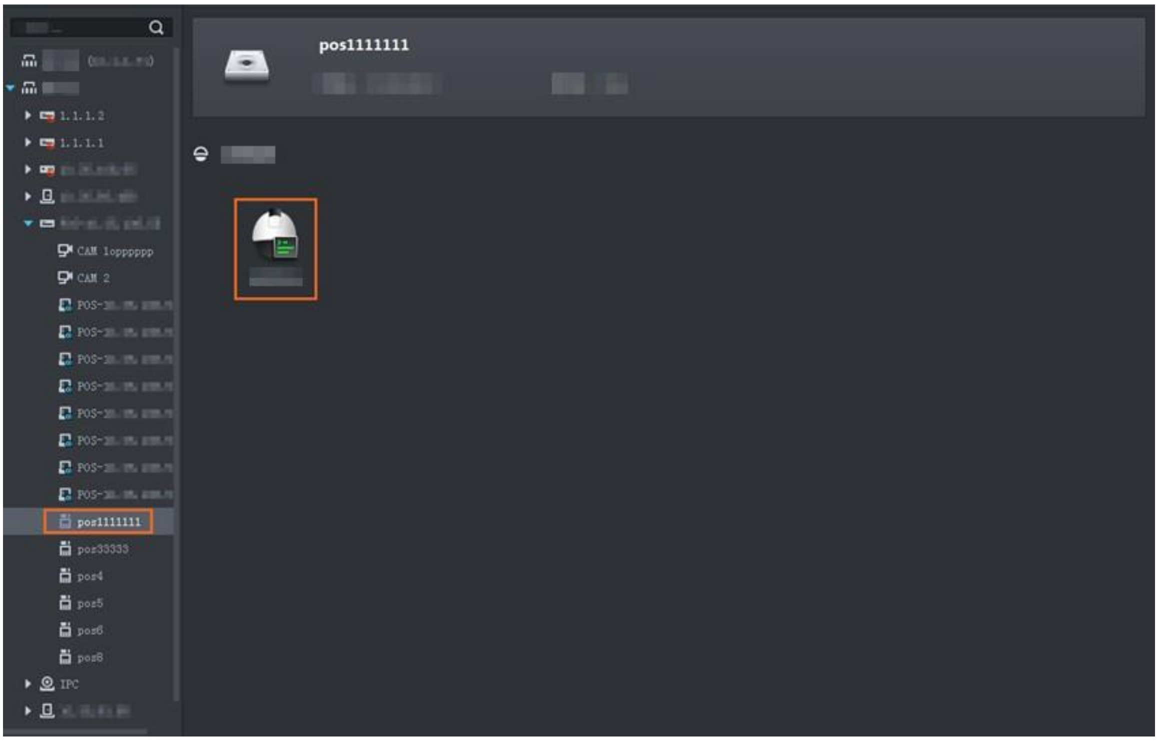
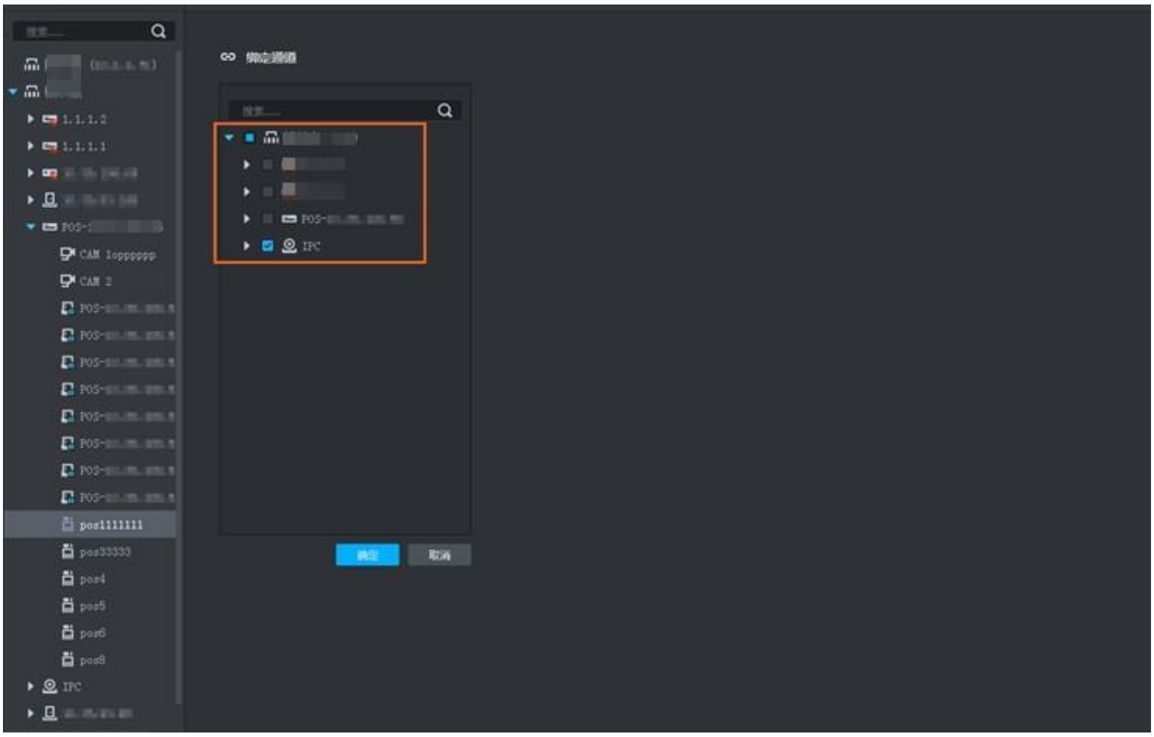

pos1111111
1.1.1.2
1.1.1.1
CAM 1oppppp
CAM 2
POS-
POS-
POS-
POS-
POS-
POS-
POS-
POS-
pos1111111
pos33333
pos4
pos5
pos6
pos8
IPC

Figure 3-224 Bind resource


CAM 1oppppp
CAM 2
pos1111111
pos33333
pos4
pos5
pos6
pos8
IPC
POS-
IPC

3) Select bound video channel, click **OK**.

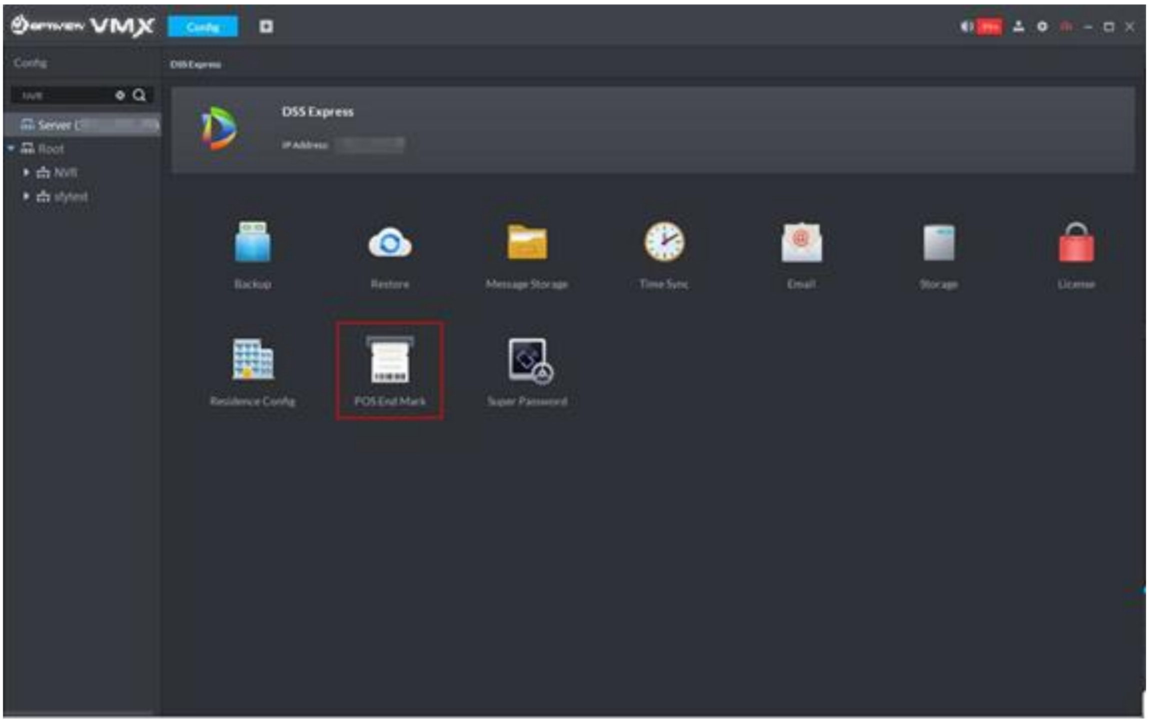
3.12.2 Modifying POS End Mark

POS end mark is the mark printed on the bottom of the POS receipt, mark that POS receipt is completely printed. The default end mark is “Thank You!”, refer to the chapter if you want to modify.

Step 1 Click **Config** on client homepage.

The system displays **Config** interface, see Figure 3-225.

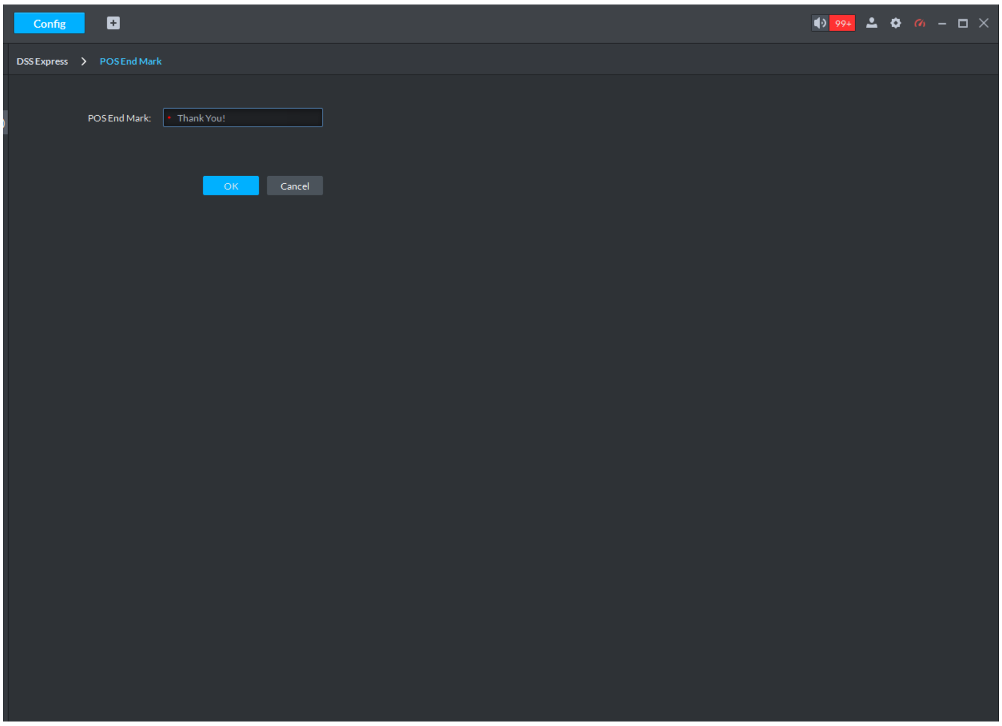
Figure 3-225 Config interface


VMX
Config
Config
DSS Express
Server
Root
NVR
DSS Express
IP Address
Backup
Restore
Message Storage
Time Sync
Email
Storage
License
Residence Config
POS End Mark
Super Password

Step 2 Click POS End Mark.

The system displays **POS End Mark** interface, see

Figure 3-226 POS End Mark



POS End Mark: * Thank You!

Step 3 Modify end mark, clock **OK**.

3.12.3 Live View

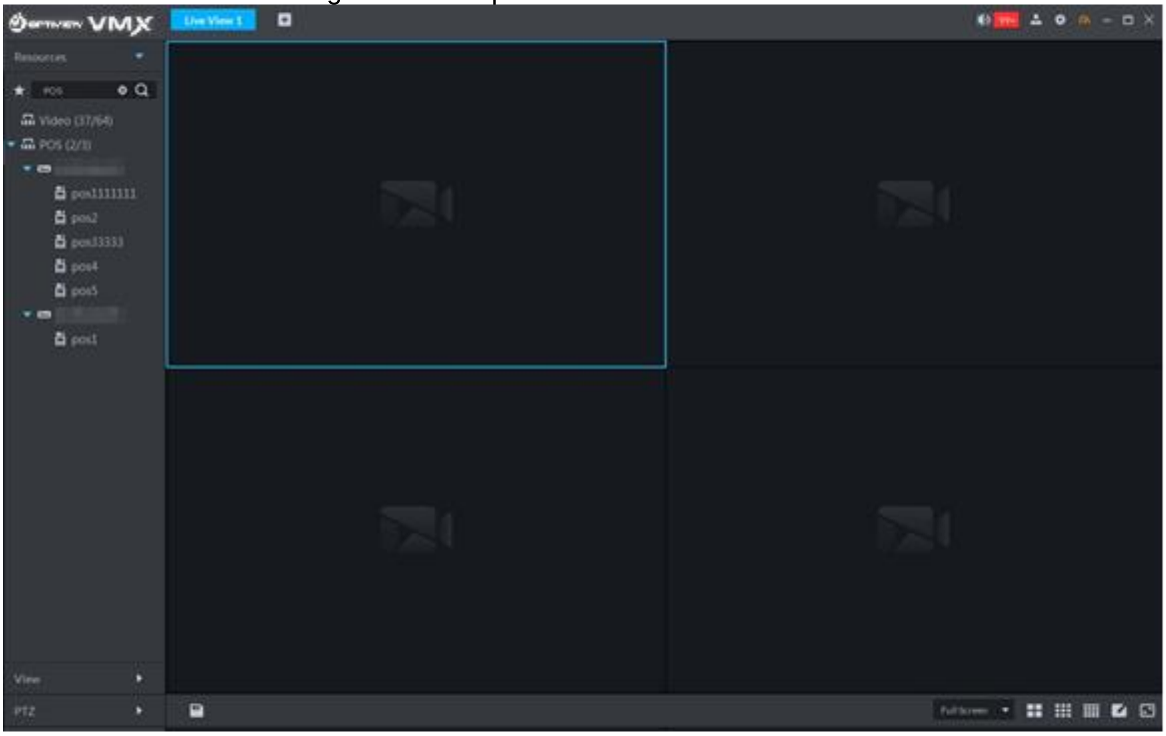
View real-time video and POS info of video channel linked to POS channel.

In this chapter, it introduces how to enable settings of live view and POS format. For more details, refer to 3.4 Live View.

Step 1 Click **Live View** on the client homepage.

The interface of **Live View** is displayed. See Figure 3-227.

Figure 3-227 Open live view interface


VMX
Live View 1
Resources
POS
Video (37/64)
POS (2/3)
pos1111111
pos2
pos33333
pos4
pos5
pos1
View
PTZ
Full Screen

Step 2 Click ▶ next to POS on the left of interface.

The system displays POS channel info.

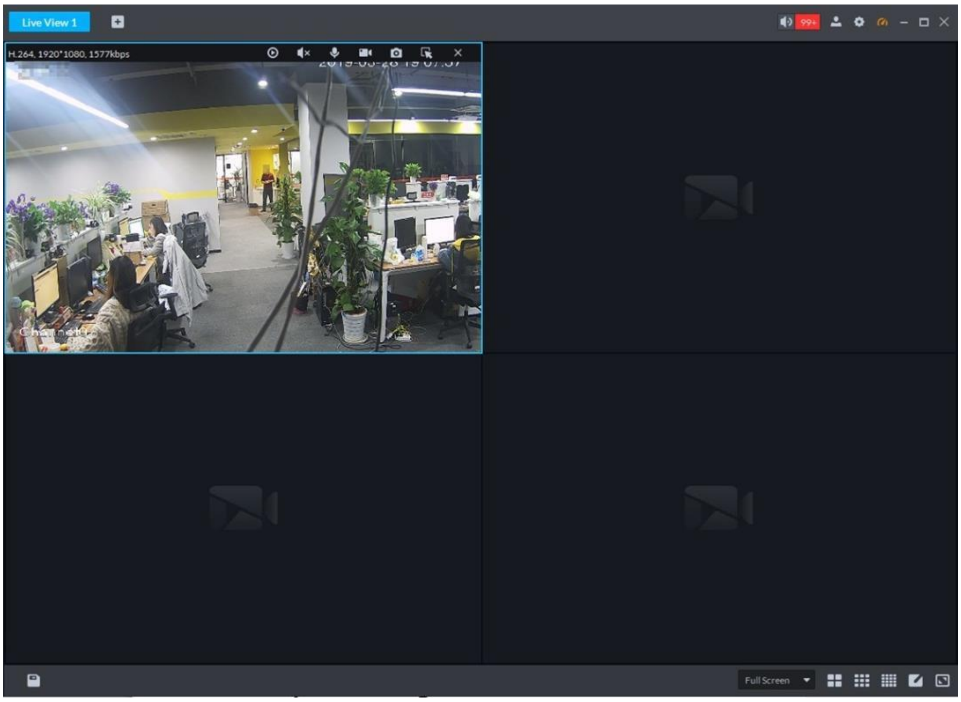
Step 3 View real-time channel video linked by POS.

Support following methods to view.

- Select channel in the POS channel list, Double-click or drag to window.
- Double-click device in the POS channel list, open all the channels of the device.

Corresponding video and POS info of linked channel are displayed. See Figure 3-228.

Figure 3-228 Start live view


Live View 1
H.264, 1920*1080, 1577kbps
Full Screen

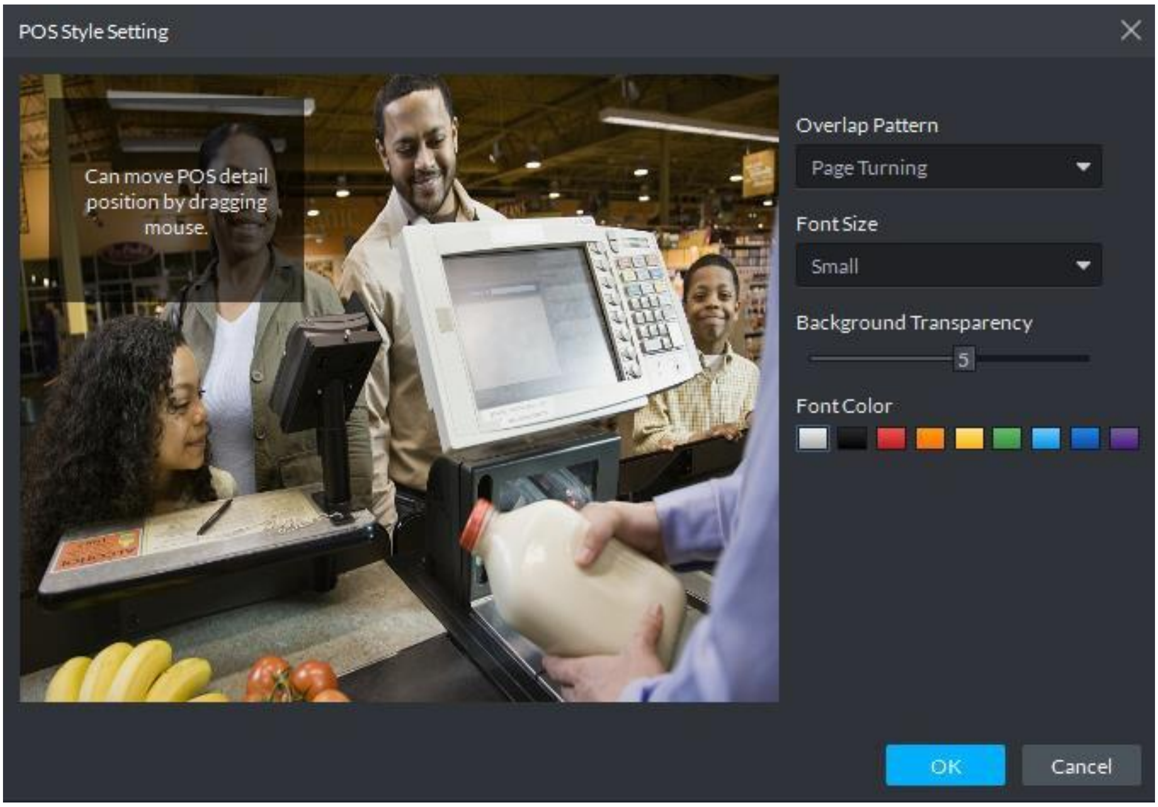
Step 4 Set POS format.

POS overlay info of all windows will be valid after setting POS style.

- Right-click and select Set POS Style on the live interface.

  The interface of **POS Style Setting** is displayed. See Figure 3-229.

Figure 3-229 POS style setting



POS Style Setting
Can move POS detail position by dragging mouse.
Overlap Pattern
Page Turning
Font Size
Small
Background Transparency
5
Font Color
OK
Cancel

1. Set **Overlap Pattern**, **Font Size**, **Background Transparency** and **Font Color**.
2. Move the mouse to POS info overlay area, press mouse left button and move it to adjust POS info overlay position.
3. Click **OK** and save config.

3.12.4 Record Playback

Search POS receipt, view related video of receipt. You can search the video half an hour before and half an hour after the time when POS receipt is printed, and you can start to play video 30s before the time when POS receipt is printed.

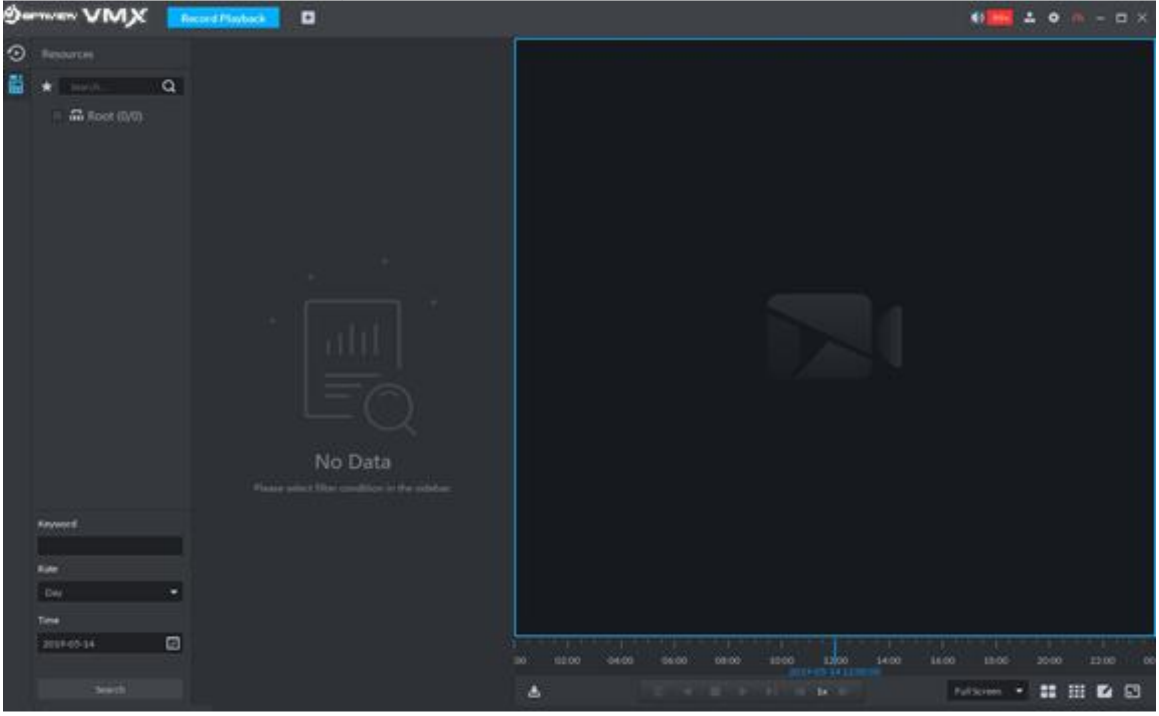
This chapter introduces how to replay related video of POS receipt. For more operation details, refer to **3.9.1 Record Playback**.

Step 1 Click ＋ and select **Record Playback** on the interface of **Homepage**.

Step 2 Click .

The interface of **POS Search** is displayed. See Figure 3-230.

Figure 3-230 POS search

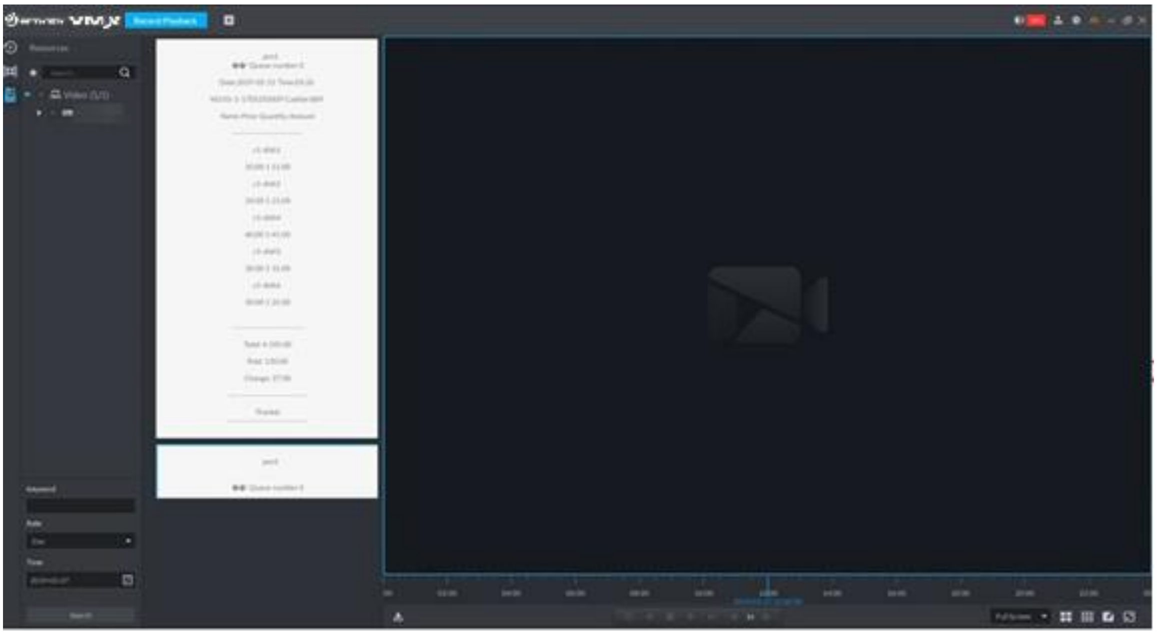

VMX
Record Playback
Resources
Search...
Root (0/0)
No Data
Please select filter condition in the sidebar
Keyword
Rule
Day
Time
2019-05-14
Search
Full Screen

Step 3 Select channel from the device tree.

Step 4 Enter **Keyword**, select **Date** and **Time**, click **Search**.

The search result is displayed. See Figure 3-231

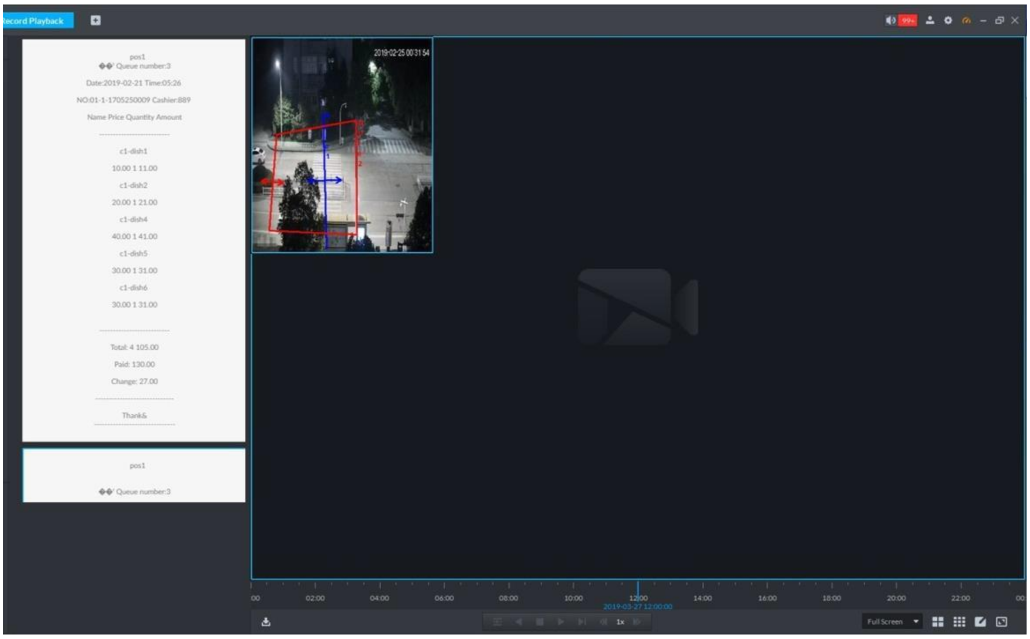
Figure 3-231 POS search result


VMX
Record Playback
Resources
Keyword
Rule
Time
Search

Step 5 Double-click the POS info of related video that needs to be replayed.

The window will play related video of POS. See Figure 3-232.

Figure 3-232 Playback video


ecord Playback
2019-02-25 00:31:54
00
02:00
04:00
06:00
08:00
10:00
12:00
2019-03-27 12:00:00
14:00
16:00
18:00
20:00
22:00
00
1x
Full Screen

pos1
◆◆' Queue number:3

Date:2019-02-21 Time:05:26

NO:01-1-1705250009 Cashier:889

Name Price Quantity Amount

----

c1-dish1

10.00 1 11.00

c1-dish2

20.00 1 21.00

c1-dish4

40.00 1 41.00

c1-dish5

30.00 1 31.00

c1-dish6

30.00 1 31.00

Total: 4 105.00

Paid: 130.00

Change: 27.00

Thank&

----

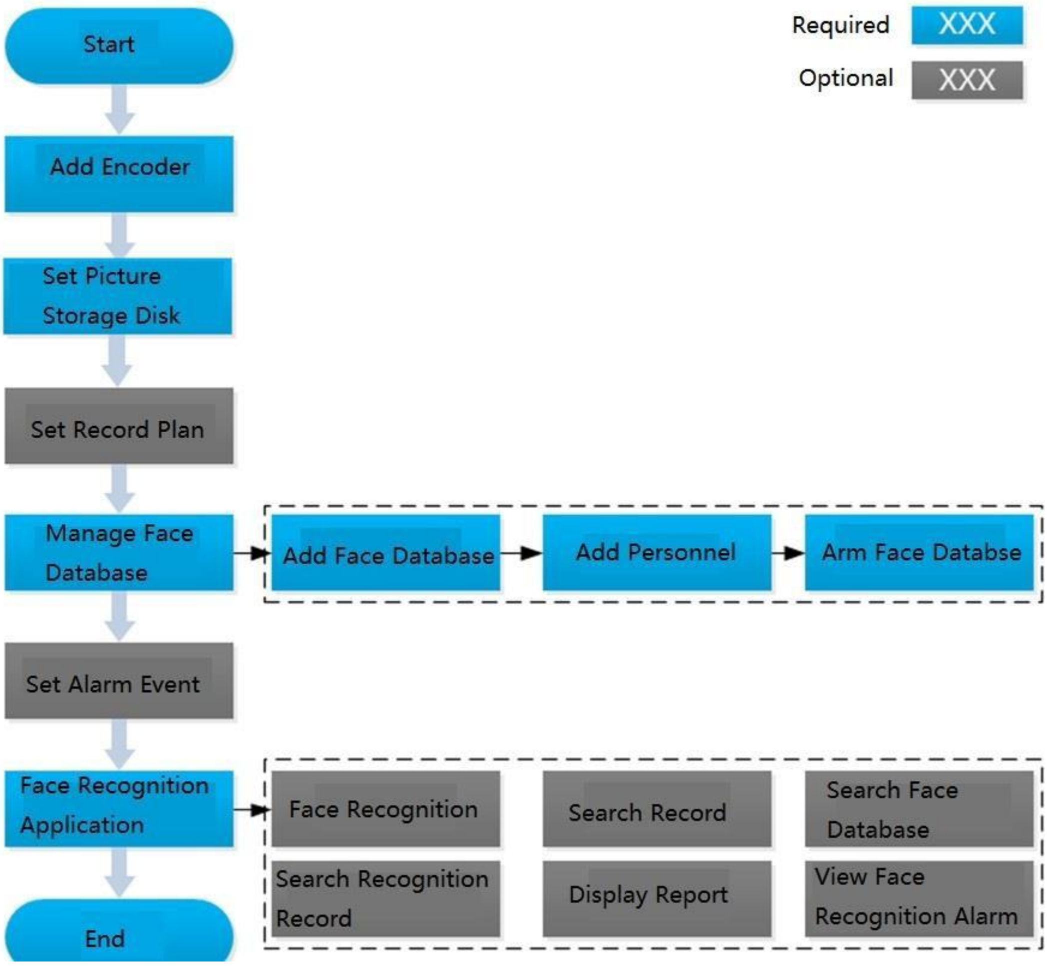
pos1

◆◆' Queue number:3

3.13 Face Recognition

After face recognition device is added to platform, platform displays face recognition results. The operation of face recognition is shown in Figure 3-233.

Figure 3-233 Face recognition flow


Required
XXX
Optional
XXX
Start
Add Encoder
Set Picture Storage Disk
Set Record Plan
Manage Face Database
Add Face Database
Add Personnel
Arm Face Databse
Set Alarm Event
Face Recognition Application
Face Recognition
Search Record
Search Face Database
Search Recognition Record
Display Report
View Face Recognition Alarm
End

3.13.1 Adding Encoder

Face recognition function can be realized only when the platform is connected to face recognition device. Intelligent devices include face recognition camera, NVR and IVSS that support face recognition function.

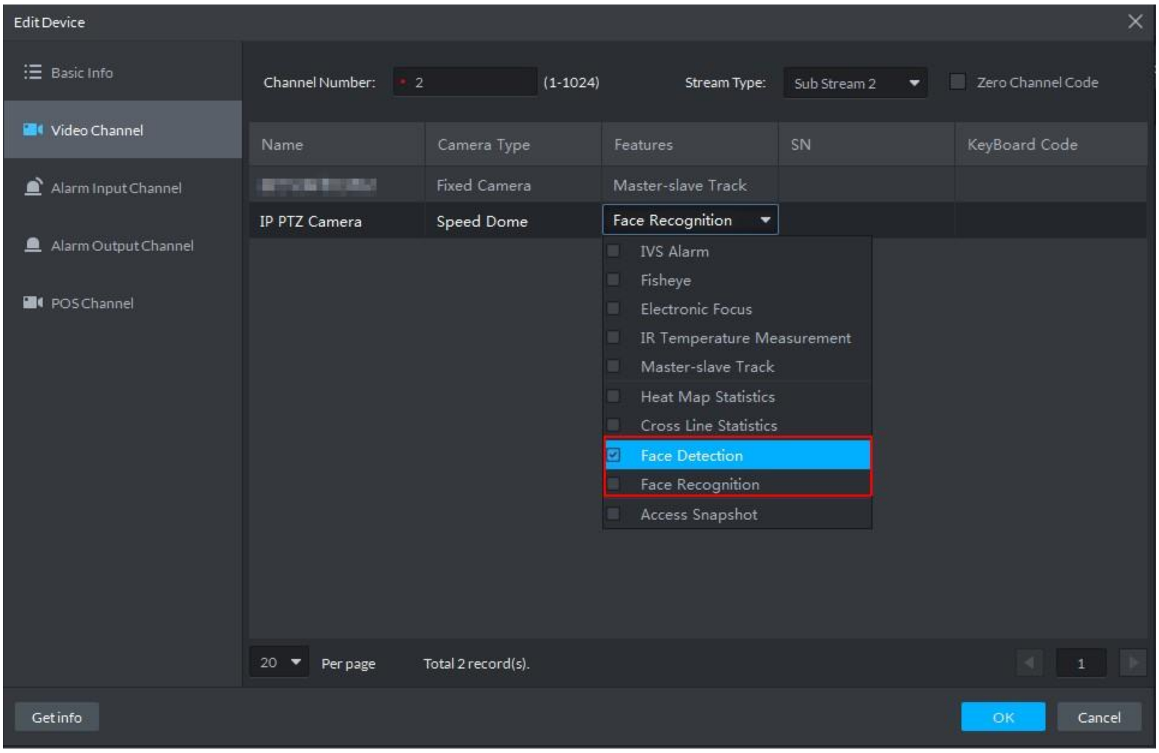
- Platform only displays face recognition results reported by device. Please make sure the added device is equipped with face recognition function, and the function is already enabled. Please refer to user manual for more details.
- If the intelligent device is IVSS or NVR, please make sure camera is added to IVSS or NVR. Please refer to device user manual for more details.

Step 1 Add face recognition camera, NVR or IVSS. For detailed operations, refer to 3.2.2.4 Adding Device.

Step 2 Modify device channel features. On Device interface, click ✏ next to device, modify device channel **Features**, see Figure 3-234.

- If face detection is realized by camera, then select **Face Detection** from **Features** of device channel.
- If face recognition is realized by camera, then select **Face Recognition** from **Features** of device channel.

Figure 3-234 Modify feature



Edit Device

Channel Number: 2 (1-1024)

Stream Type: Sub Stream 2

☐ Zero Channel Code

Name	Camera Type	Features	SN	KeyBoard Code
[redacted]	Fixed Camera	Master-slave Track		
IP PTZ Camera	Speed Dome	Face Recognition		

20 Per page Total 2 record(s).

Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
☐ IVS Alarm
☐ Fisheye
☐ Electronic Focus
☐ IR Temperature Measurement
☐ Master-slave Track
☐ Heat Map Statistics
☐ Cross Line Statistics
☑ Face Detection
☐ Face Recognition
☐ Access Snapshot
1
Get info
OK
Cancel

3.13.2 Setting Picture Storage Disk

Configure local storage disk, you have to reserve a general picture disk to store snapshots, otherwise snapshots cannot be stored and displayed. For detailed operations, refer to **3.2.1.4 Setting Storage Space**.

3.13.3 Setting Record Plan

After record storage plan is configured, the video before and after face detection snapshot is stored, the platform can playback video 10s before and after snapshot. If you want to set record storage plan, refer to **3.2.5 Setting Record Plan**.

3.13.4 Managing Face Database

Face database management includes following functions.

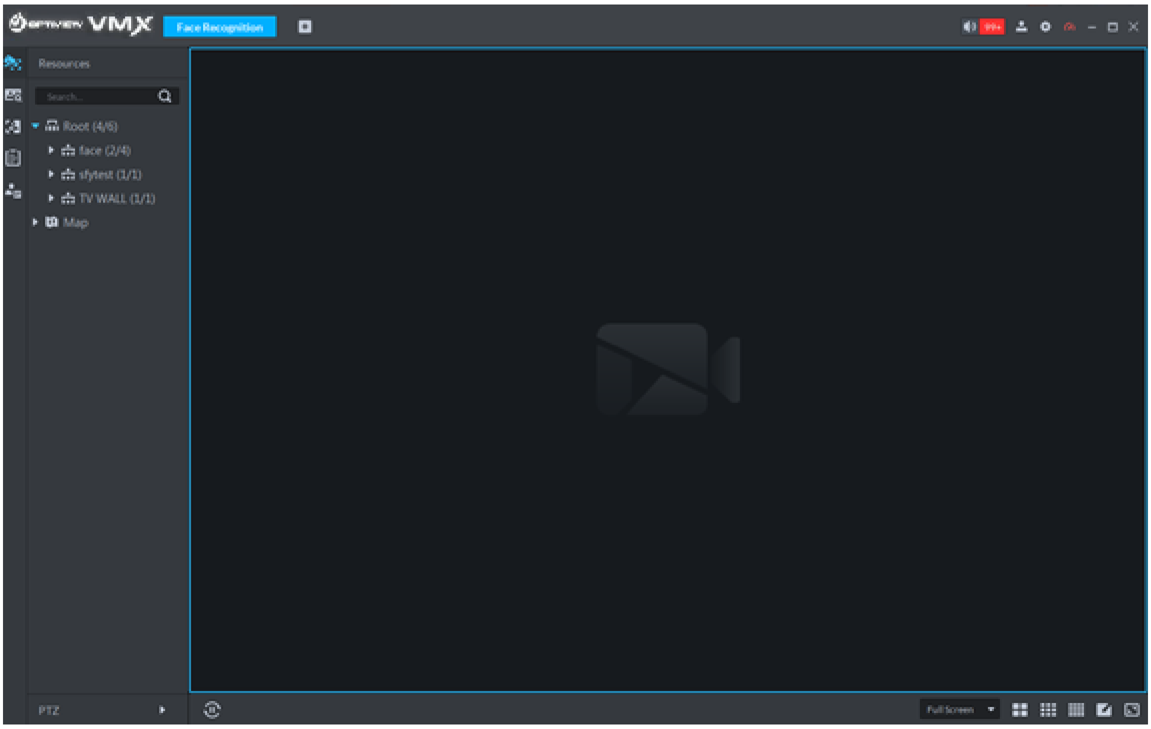
- Add face database, used to store personnel info, convenient for unified deployment over personnel in database. Meanwhile, you can edit and delete face database.
- Add personnel, you can add personnel into face database. Meanwhile, you can edit and delete personnel.
- Arm face database. After database is armed, face recognition device (such as FR camera, NVR and IVSS) compares snapshot with picture in database, if the similarity is ≧ threshold, then face recognition device (such as FR camera, NVR and IVSS) makes judgment that two pictures show the same person, and then report comparison record to the platform.

3.13.4.1 Adding Face Database

Step 1 On client homepage, click **Face Recognition**.

The system displays **Face Recognition** interface, see Figure 3-235.

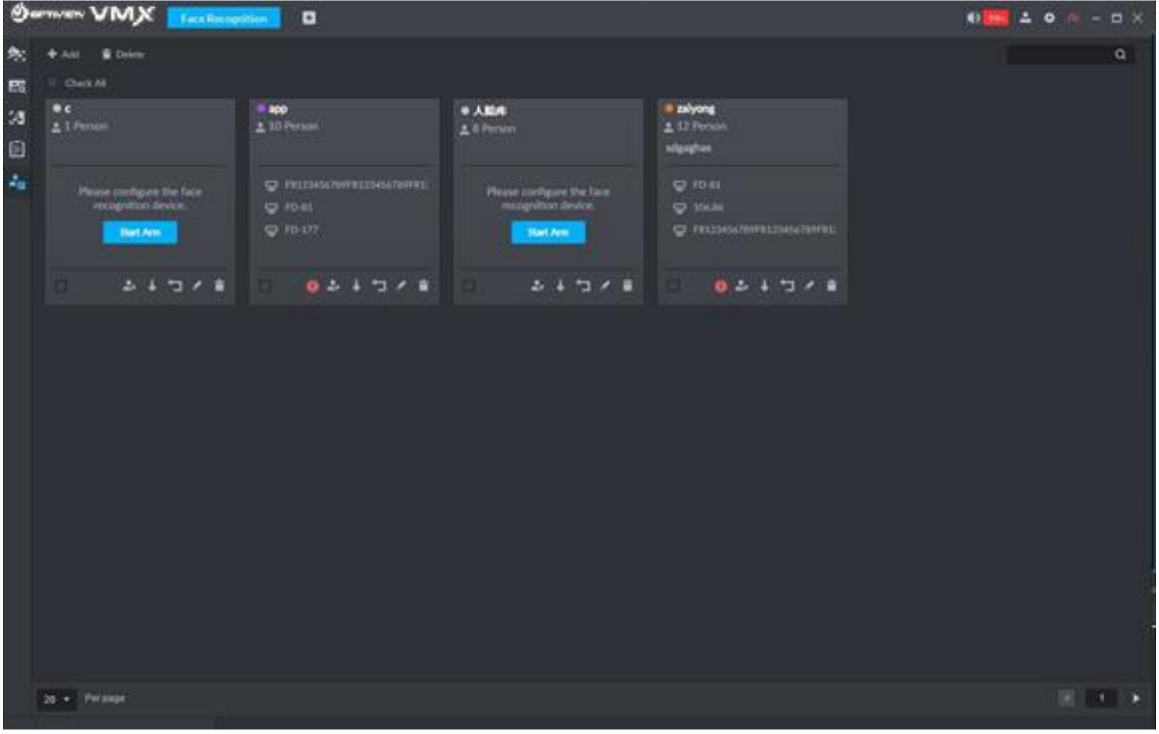
Figure 3-235 Face recognition



Step 2 Click .

The system displays **Face Database** interface, see Figure 3-236.

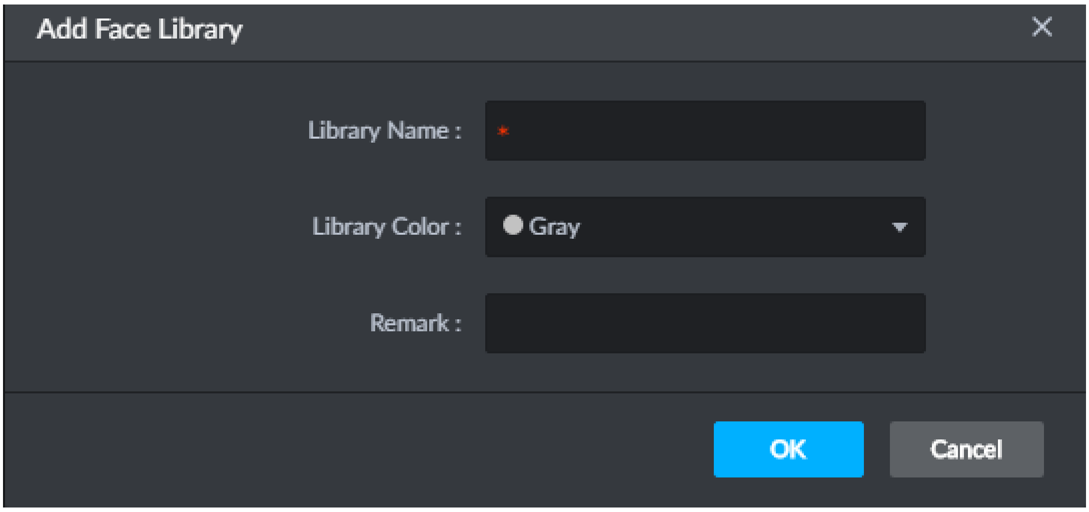
Figure 3-236 Face database management


VMX
Face Recognition
Add
Delete
Check All
Please configure the face recognition device.
Start Arm
Per page

Step 3 Click Add.

The system displays **Add face library** interface, see Figure 3-237.

Figure 3-237 Add face library

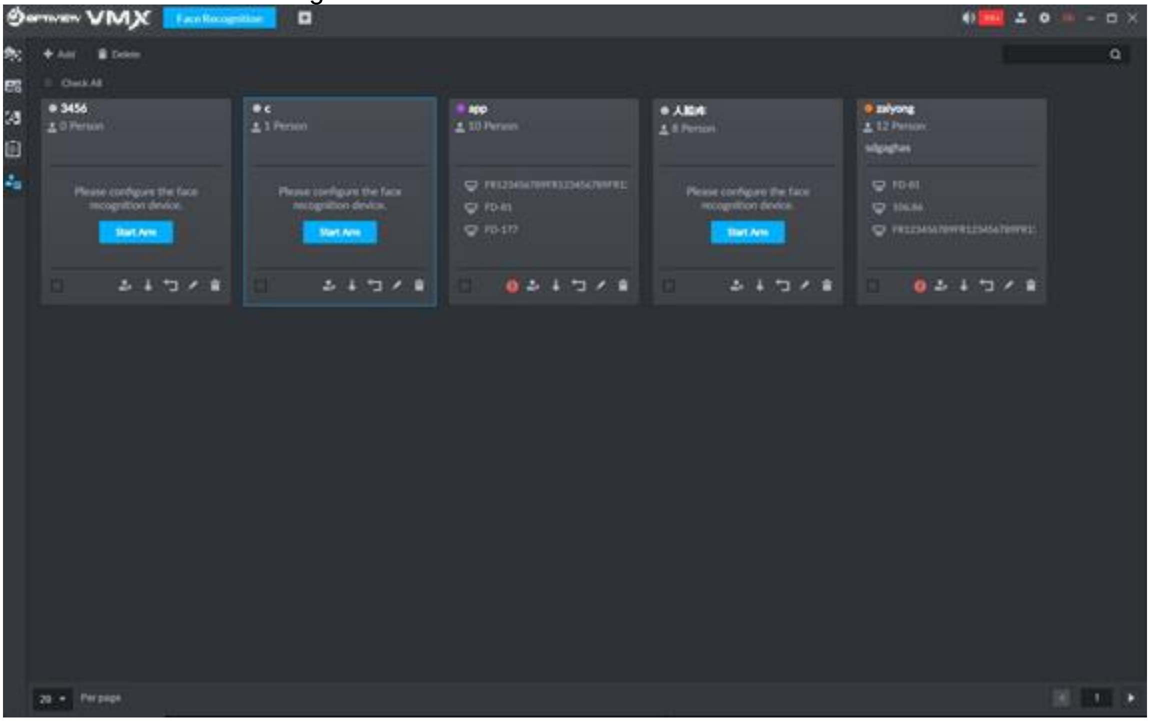

Add Face Library
Library Name :
Remark :
OK
Cancel

Library Color : Gray

Step 4 Set face database info, click **OK**.

Library color is identified, the system displays new face database info, see Figure 3-238.

Figure 3-238 Added face database


VMX
Face Recognition
Add
Delete
Check All
3456
0 Person
Please configure the face recognition device.
Start Arm
c
1 Person
Please configure the face recognition device.
Start Arm
app
10 Person
FD-81
FD-177
8 Person
Please configure the face recognition device.
Start Arm
zaiyong
12 Person
FD-81
20 Per page
1

3.13.4.2 Adding Personnel

The platform can add personnel info to face database singly or in batches, you can also register captured personnel into face database.

3.13.4.2.1 Adding Personnel Singly

Step 1 On **Face Database** interface, click on face database or click face database, see Figure 3-239.

The system displays interface of adding personnel, see Figure 3-240.

Figure 3-239 Enter add interface

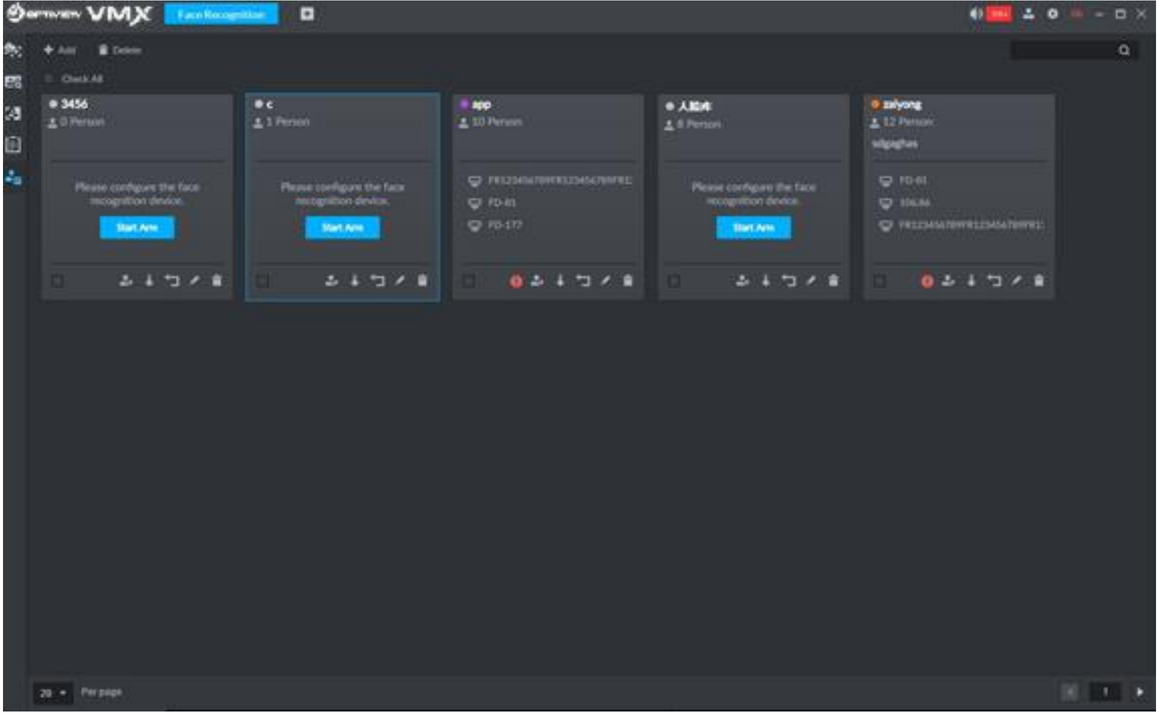
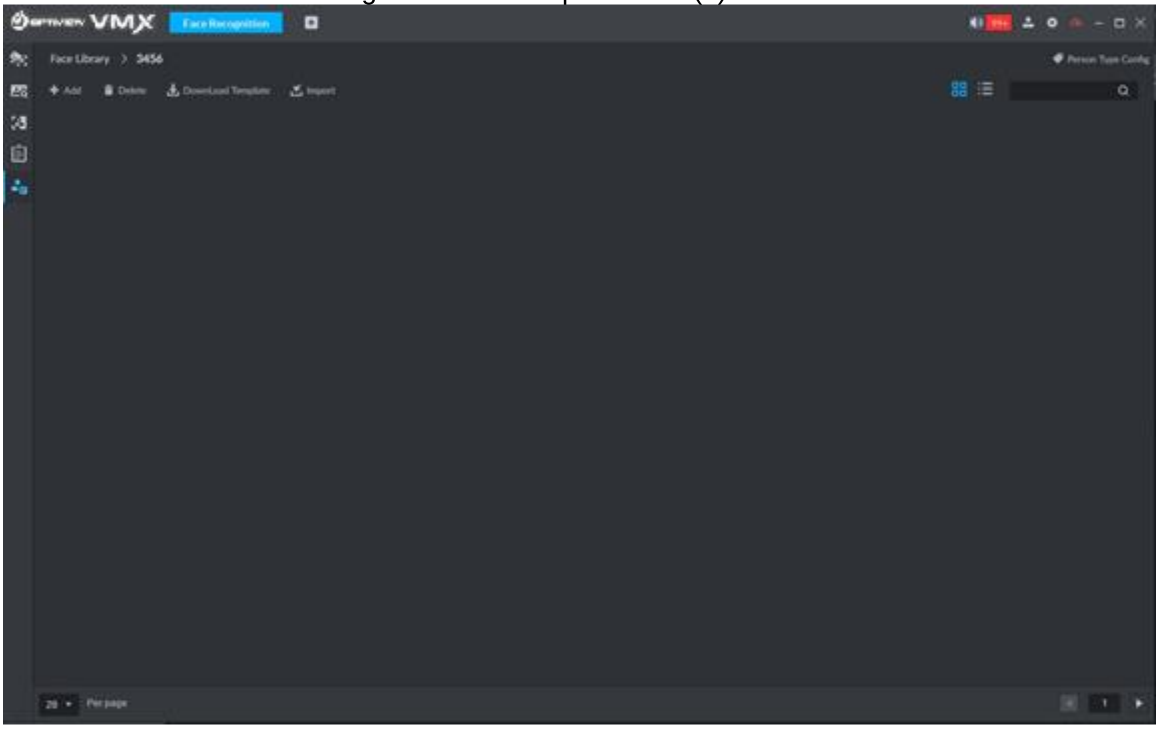

Face Recognition
Add
Delete
Check All
3456
0 Person
Please configure the face recognition device.
Start Arm
c
1 Person
app
10 Person
FD-81
FD-177
8 Person
12 Person
20
Per page
1

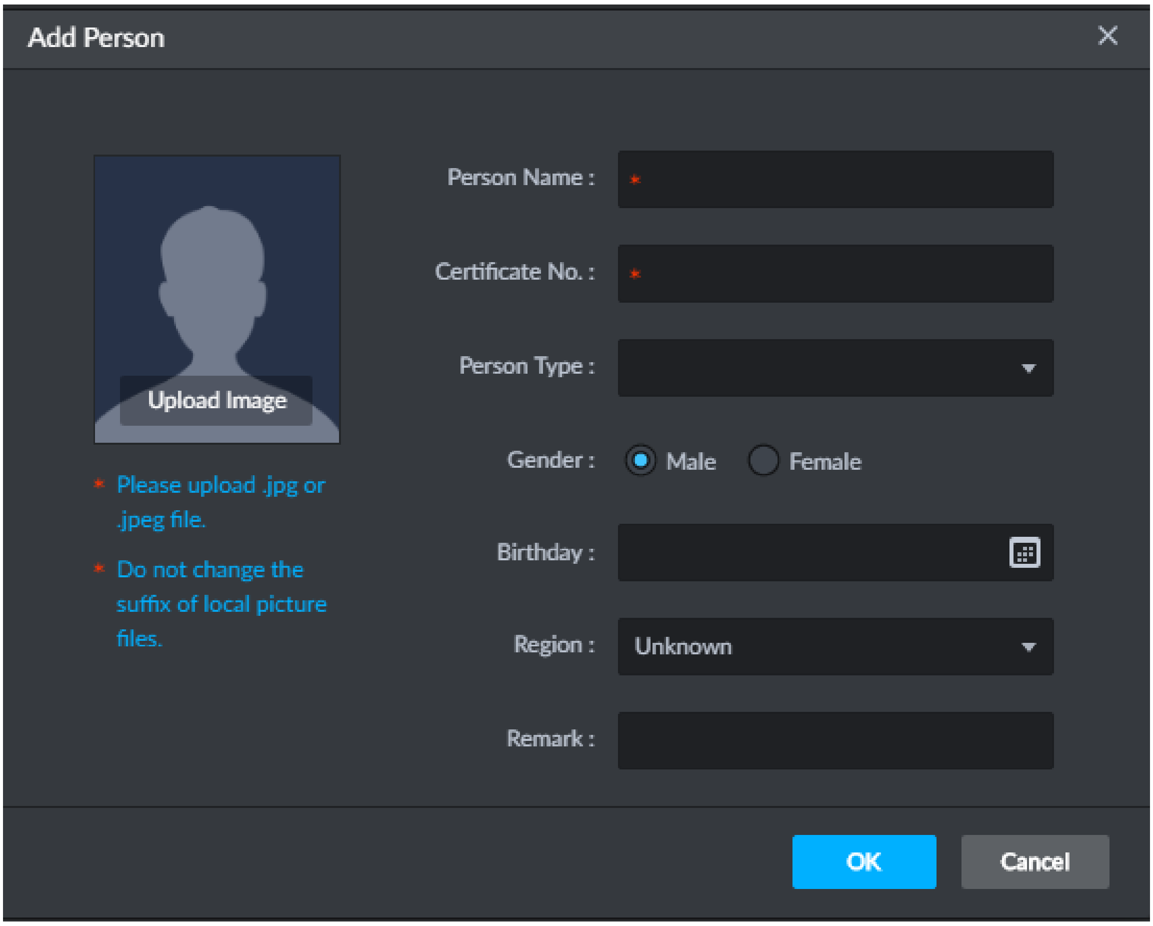
Figure 3-240 Add personnel (1)


Face Recognition
Face Library
3456
Add
Delete
Download Template
Import
Person Type Config
20
Per page
1

Step 2 Click **Add**.

The system displays **Add Person** interface, see Figure 3-241.

Figure 3-241



* Please upload .jpg or .jpeg file.

* Do not change the suffix of local picture files.

Person Name : *

Certificate No. : *

Person Type :

Gender : ● Male ○ Female

Birthday :

Region : Unknown

Remark :

Step 3 Click drop-down box of **Person Type**, select **Add Person Type**, and configure person type according to prompt on interface.

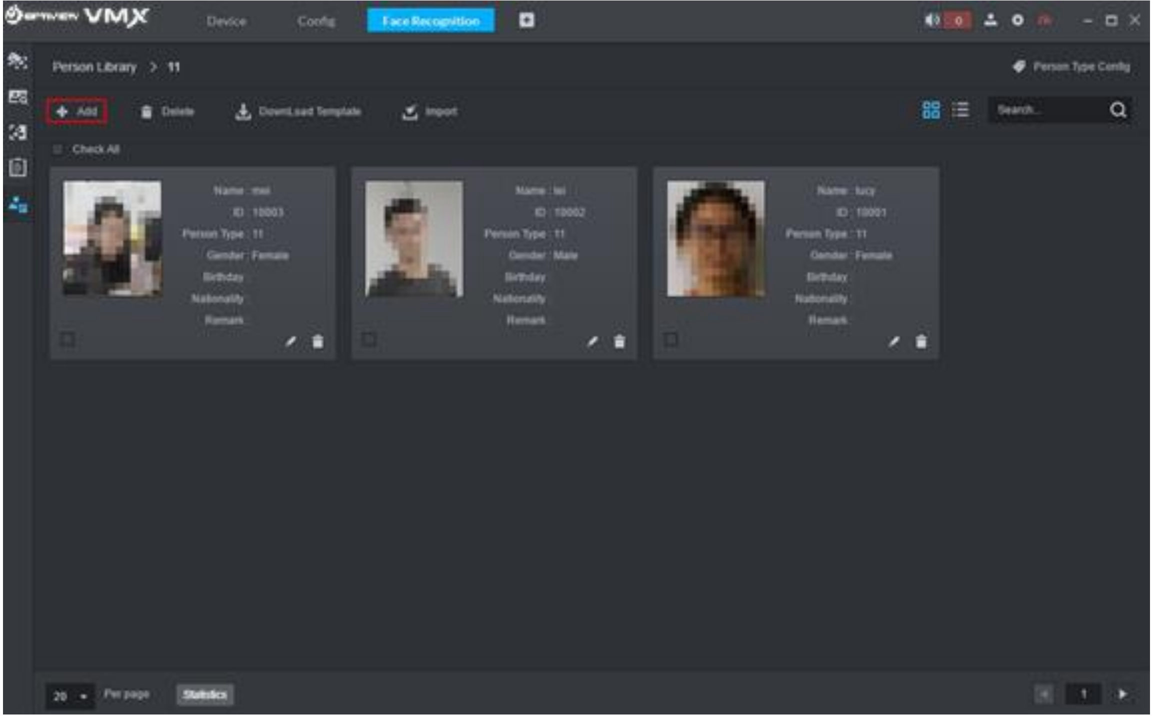
Person type is considered as person property to distinguish person.

Click Person Type Config on upper right corner of Figure 3-240, and you can configure person type as well.

Step 4 Upload person picture (You are required to clip the picture before upload), fill in person info, click **OK**.

The system displays info of added person, see Figure 3-242.

Figure 3-242 Add



Name : mei
ID : 10003
Person Type : 11
Gender : Female
Birthday
Nationality
Remark

Name : lei
ID : 10002
Person Type : 11
Gender : Male
Birthday
Nationality
Remark

Name : lucy
ID : 10001
Person Type : 11
Gender : Female
Birthday
Nationality
Remark

3.13.4.2.2 Importing Personnel

Step 1 On **Face Database** interface, click or the face database, see Figure 3-239.

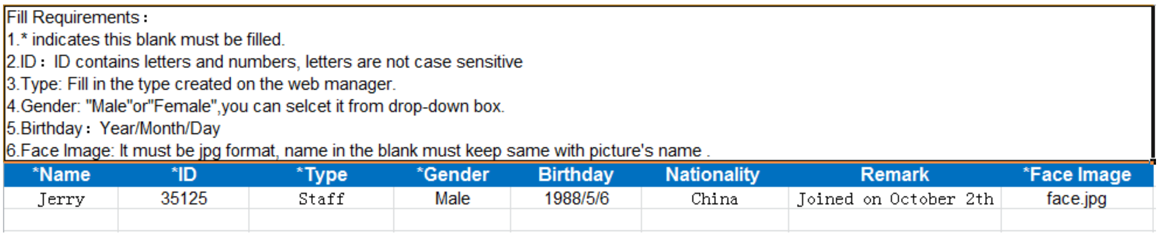
The system displays interface of adding person, see Figure 3-240.

Step 2 Click **Download Template**, save template according to system prompt.

Step 3 Make upload file.

1) Edit personnel info excel table, Picture info is required to be in accordance with picture file name, see Figure 3-243.

Figure 3-243



Fill Requirements：
1.* indicates this blank must be filled.
2.ID： ID contains letters and numbers, letters are not case sensitive
3.Type: Fill in the type created on the web manager.
4.Gender: "Male"or"Female",you can selcet it from drop-down box.
5.Birthday： Year/Month/Day
6.Face Image: It must be jpg format, name in the blank must keep same with picture's name .

*Name	*ID	*Type	*Gender	Birthday	Nationality	Remark	*Face Image
Jerry	35125	Staff	Male	1988/5/6	China	Joined on October 2th	face.jpg

2) Compress personnel picture and info excel tables into zip/rar/7z.

Step 4 Click **Import**, and upload compression package according to interface prompt.

The system displays import progress and result.

3.13.4.2.3 Captured Person Register Library

Step 1 Enter person register interface.

Support following methods to enter register interface.

- On **Face Recognition** interface, Double-click person snapshot, see Figure 3-244. Enter person detail interface, see Figure 3-245. Click and enter register interface.

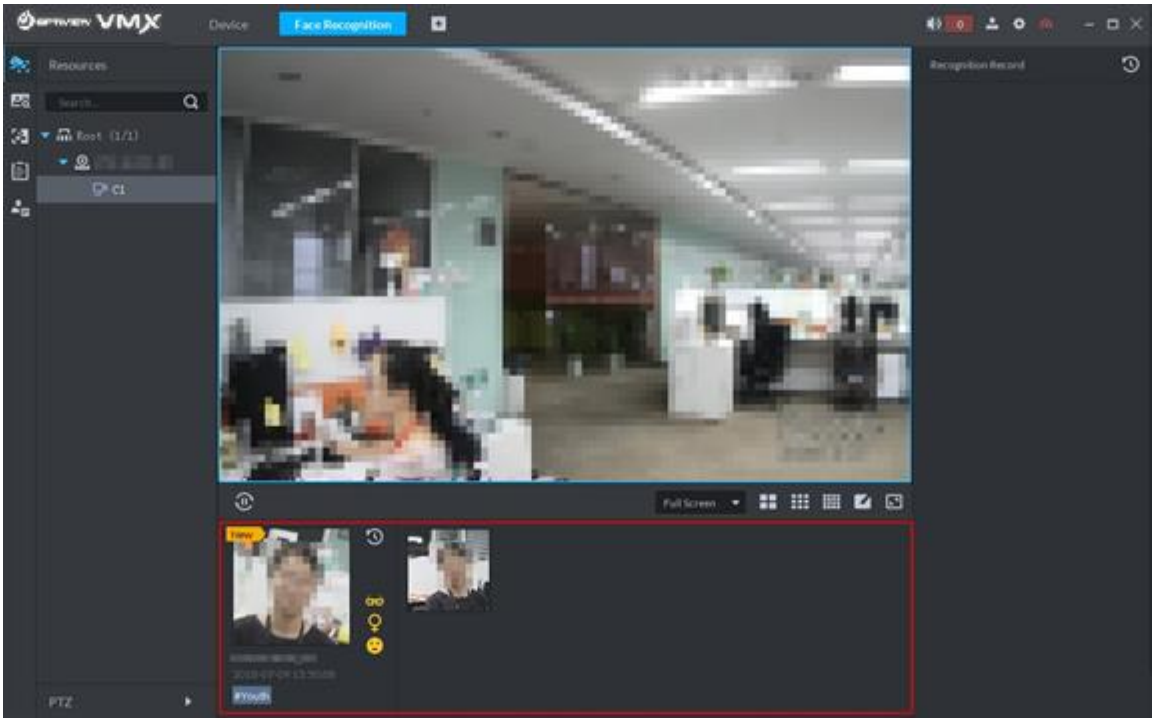
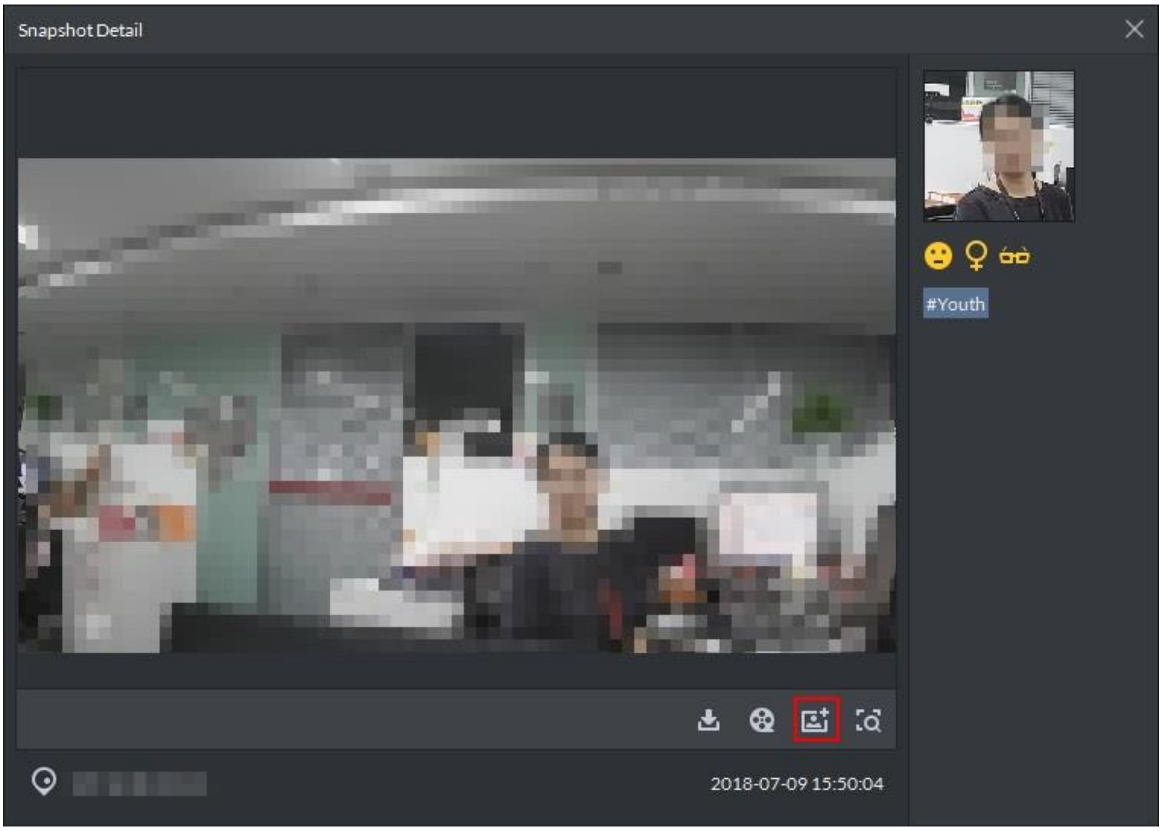

VMX
Device
Face Recognition
Resources
Root (1/1)
C1
Full Screen
Recognition Record
New
#Youth
PTZ

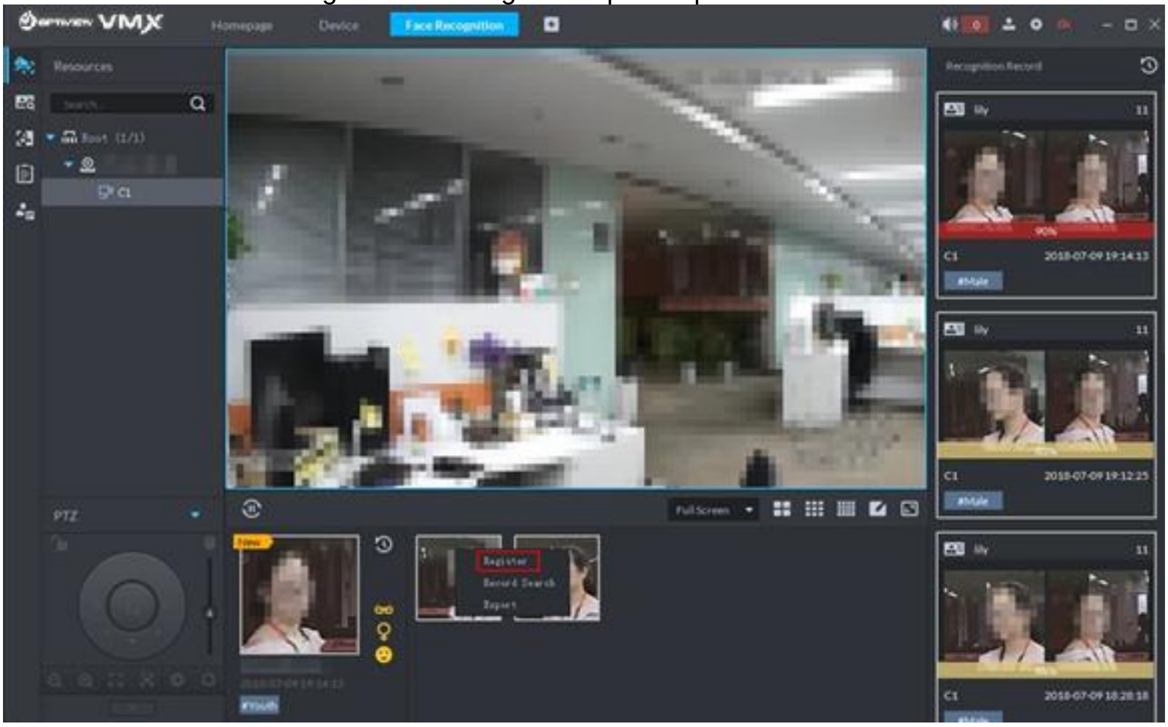
Figure 3-244 Double-click snapshot

Figure 3-245 Person detail


Snapshot Detail
#Youth
2018-07-09 15:50:04

- On **Face Recognition** interface, move mouse to person snapshot, right-click and select **Rgister**, and enter register interface. See Figure 3-246.

Figure 3-246 Register captured person


VMX
Homepage
Device
Face Recognition
Resources
Search...
Root (1/1)
C1
PTZ
Full Screen
Recognition Record
lily
C1
2018-07-09 19:14:13
#Male
lily
C1
2018-07-09 19:12:25
#Male
lily
C1
2018-07-09 18:28:18
New
Register
Record Search
Export
#Youth

- On record search interface, click and enter register interface, see Figure 3-247. Or Double-click searched result, enter person detail, click and enter register interface.

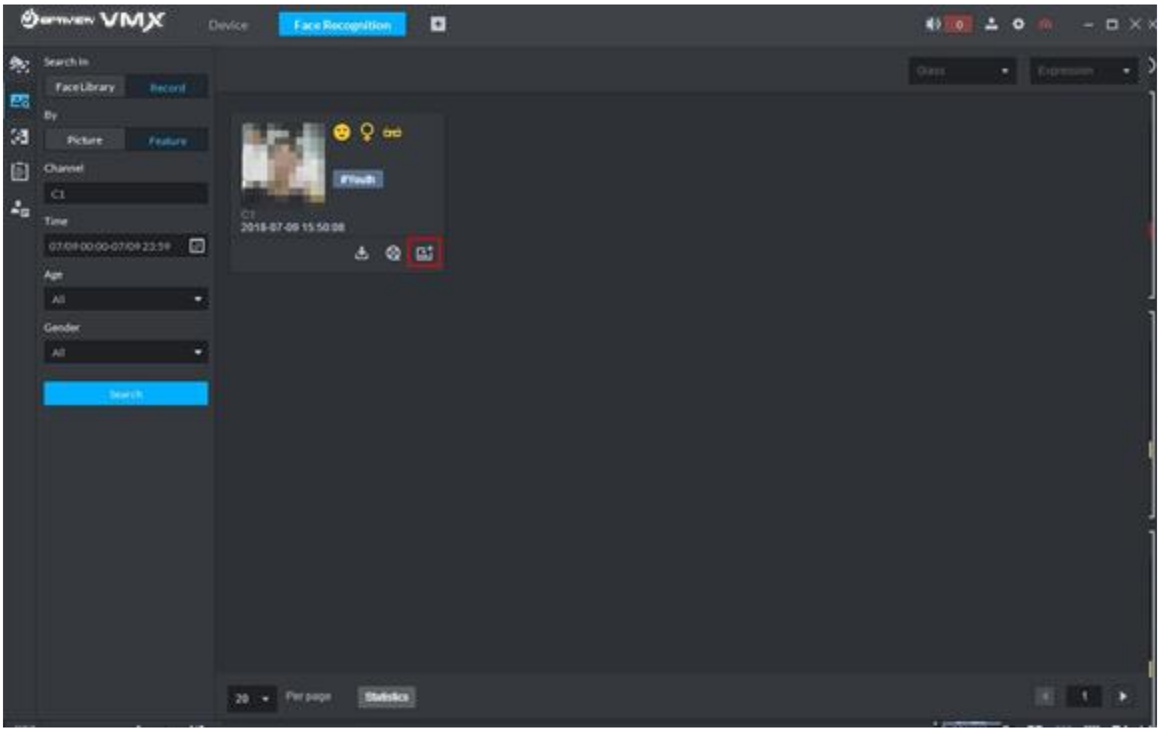
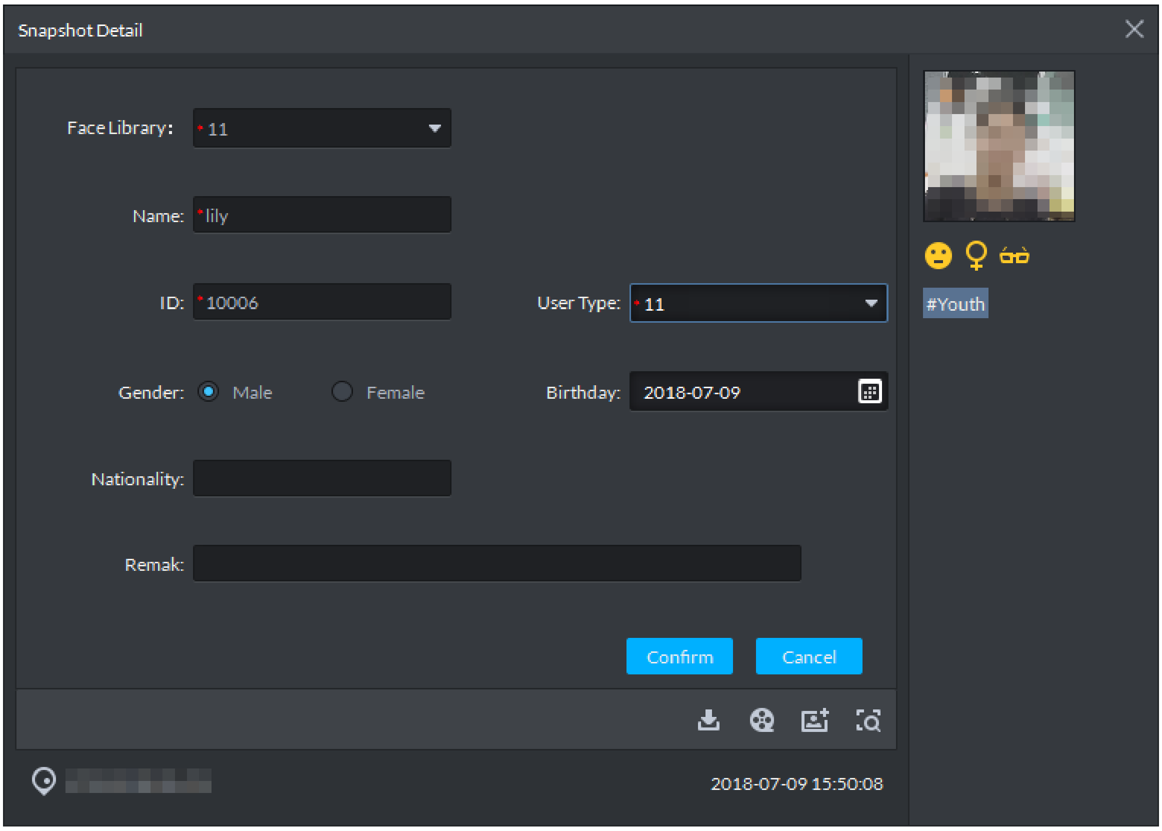

VMX
Device
Face Recognition
Search in
Face Library
Record
By
Picture
Feature
Channel
C1
Time
07/09 00:00-07/09 23:59
Age
All
Gender
All
Search
Glass
Expression
#Youth
C1
2018-07-09 15:50:08
20
Per page
Statistics
1

Figure 3-247 Record search

Step 2 Select face database you want to add, enter person info. Click **OK**, see Figure 3-248.

Figure 3-248 Register person



Snapshot Detail

Face Library: 11

Name: lily

ID: 10006

User Type: 11

Gender: ● Male ○ Female

Birthday: 2018-07-09

Nationality:

Remak:

[redacted] 2018-07-09 15:50:08

3.13.4.3 Arming Face Database

Step 1 On **Face Recognition** interface, click .

The system displays **Face Database** interface.

Step 2 Click **Start Arm** or ⬇ on the face database, see Figure 3-249.

The system displays **Face Config** interface, see Figure 3-250.

- Start Arm button only displays after face databased is created. After armed, the button will no longer display on the interface.
- Click ↩ and cancel arm.

Figure 3-249 Arm button

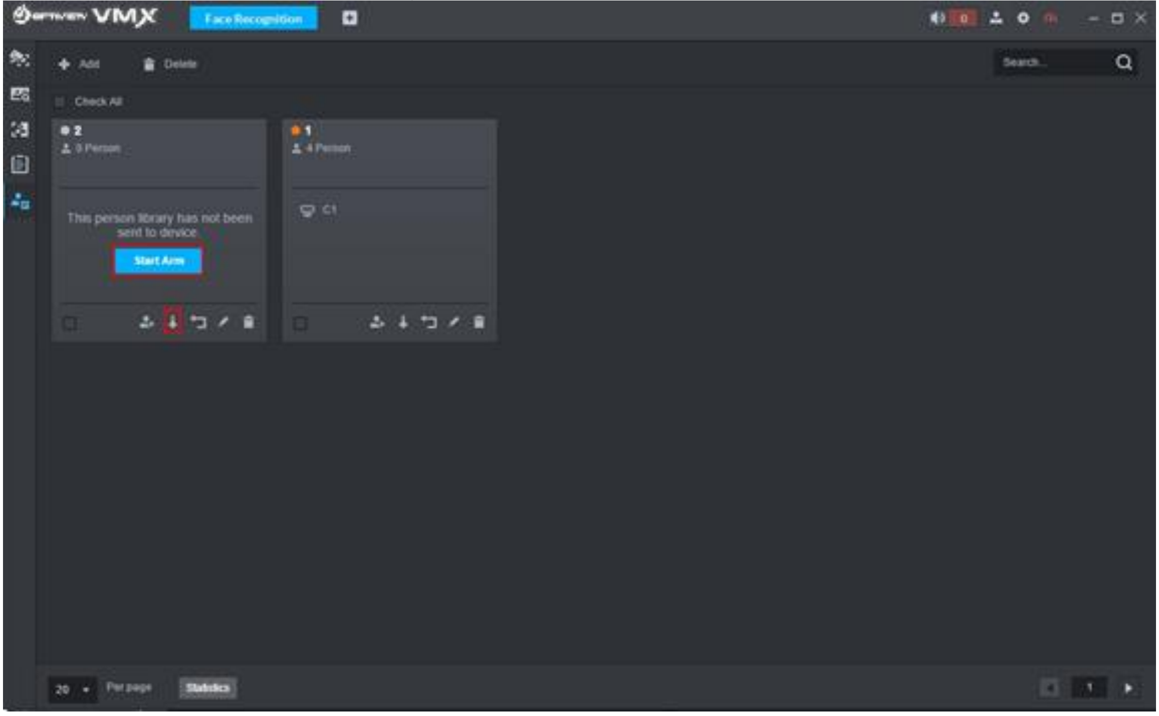
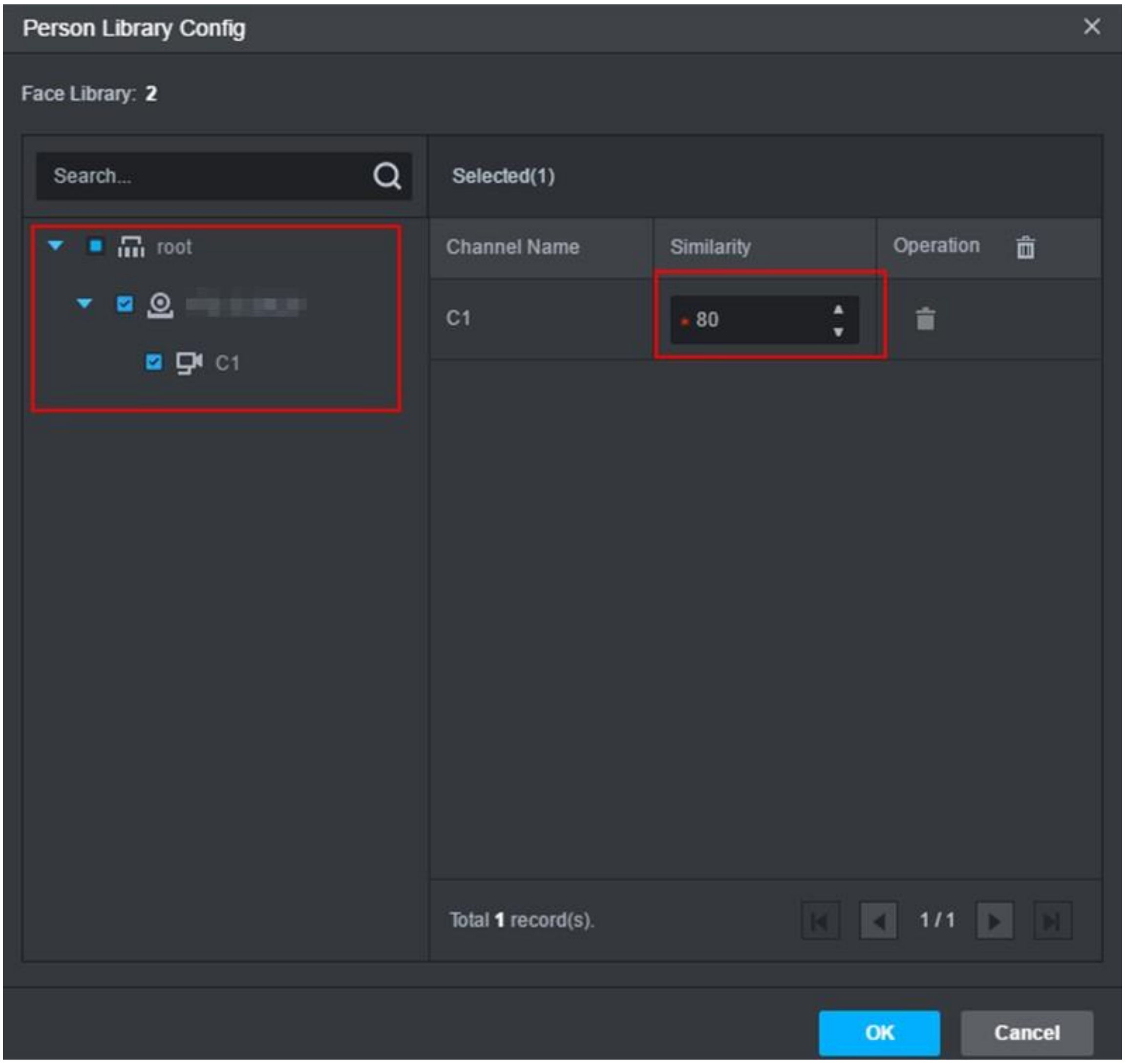

Face Recognition
Add
Delete
Search...
Check All
2
0 Person
This person library has not been sent to device
Start Arm
1
4 Person
C1
20
Per page
Statistics
1

Figure 3-250 Arm config


Person Library Config
Search...
root
C1
Selected(1)
Total 1 record(s).
1 / 1
OK
Cancel

Face Library: 2

Channel Name	Similarity	Operation
C1	80	

Step 3 Select the channel you want to arm (multiple choice supported), set similarity, and click **OK**.

Recognition record is reported when similarity is e supported)

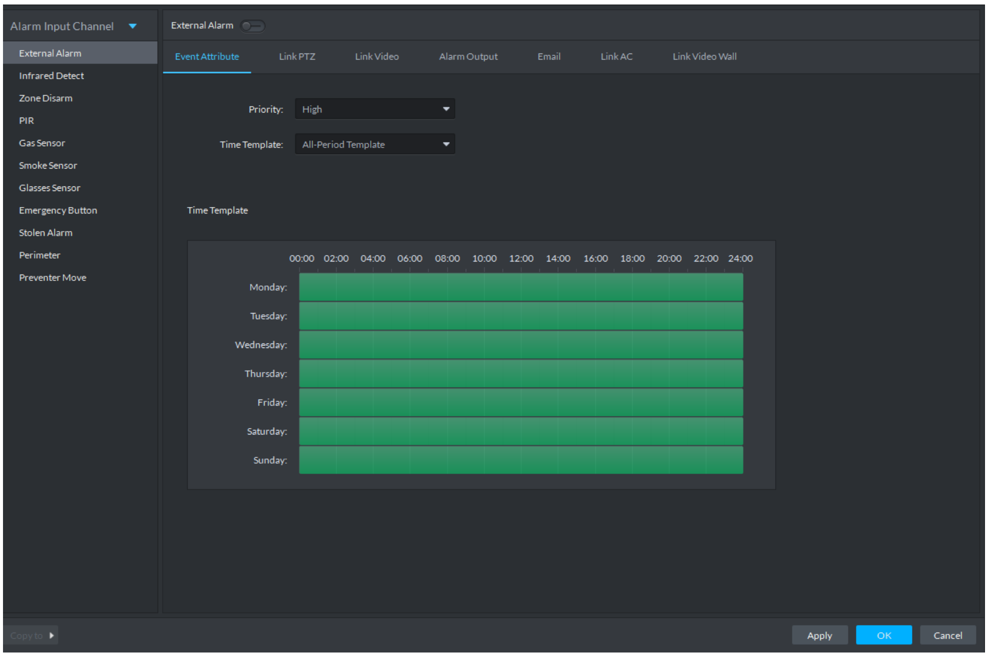
3.13.5 Setting Alarm Event

This chapter only introduces related alarm about face recognition, for more alarm event setting, see **3.2.4 Setting Alarm Event**. Face recognition alarms include following types.

- Person type alarm, alarm is triggered when target person type is recognized. Person type is set when adding person.
- Face recognition alarm, alarm is triggered when face database is recognized. The classification under face recognition alarm is face database name.

Set alarm event, see Figure 3-251.

Figure 3-251 Face recognition alarm event



Priority: High

Time Template: All-Period Template

Alarm Input Channel
External Alarm
Infrared Detect
Zone Disarm
PIR
Gas Sensor
Smoke Sensor
Glasses Sensor
Emergency Button
Stolen Alarm
Perimeter
Preventer Move
External Alarm
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Time Template
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
24:00
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:
Copy to
Apply
OK
Cancel

3.13.6 Face Recognition Application

Application of face recognition business client includes:

- Live View

  Supports live video, person snapshot and recognition record. Meantime it supports view of corresponding panorama and link video of person snapshot, download link video, sign up snapshot person and etc.
- Snapshot Search

  Via feature info or person picture, search matched person in face library or snapshot record.
- Recognition Search

  Via set feature info, search matched recognition record in recognition record.
- Report

  For a certain channel, according to snapshot time, snapshot person age, create a report of snapshot person.

Face snapshot storage info

- Snapshot is stored in server installation path "..\WEBCLIENT\webclient\apache-tomcat\webapps\upload\face". Pictures are stored for 30 days by default, if you want to modify storage days, refer to 3.2.1.1 Setting Message Storage
- Take 2 snapshots a time, one face snapshot and the other panoramic picture. In general the picture size is 100KB.
- Snapshots are stored for 30 days by default. If you want to modify details, refer to 3.2.1.1 Setting Message Storage

3.13.6.1 Face Recognition

When setting storage space, local storage disk must reserve a general picture disk; otherwise, snapshot cannot be seen.

3.13.6.1.1 Live View

View and recognize video, capture face and recognize face info.

Step 1 On Face Recognition interface, click .

The system displays **Face Recognition** interface.

Step 2 Enable real-time monitoring, enable real-time monitoring interface, and see Figure 3-252.

- Select monitoring window, Double-click channel on the left and enable live monitoring.
- Drag channel on the left to monitoring window.

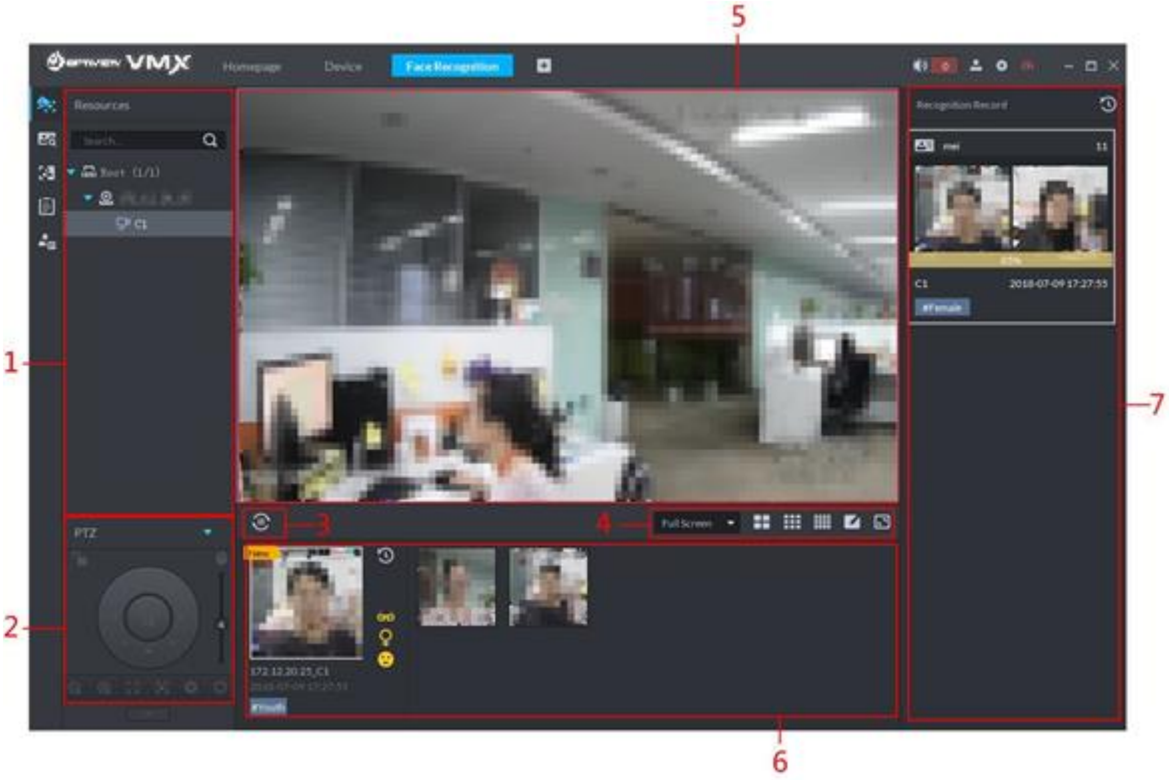


Figure 3-252 Live view

Table 3-48 Live video interface description

No.	Name	Description
1	Device Tree	Display device and device channel info. Right-click root node, support display type. You can set display by name and IP. Support ranking, by ascending and descending and default sequence. Support to hide and show offline node. Right-click device, select tour，support to set all channel tour view of this device. After you enter touring, if you want to stop touring, then you can right-click in live view video, select “Stop Touring”, to end tour. Right-click channel to enter Record Configuration and Event Configuration.
2	PTZ	Speed dome adjust. If you want to expand PTZ operation zone, click ▼ behind PTZ to hide PTZ area. When PTZ area is hidden, click ▶ behind PTZ to expand PTZ zrea.
3	Pause Refresh/Start Refresh	▶，page shows this icon，snapshot area does not refresh face snapshot. Click this icon, live refresh face snapshot. ⏸，page shows this icon. Snapshot display area shows refresh of face snapshot. Click this icon, refresh face snapshot.

No.	Name		Description
4	全屏 ▾	Picture Display Scale	Support full screen and original scale.
	▦ ▦ ▦ ✎	Window Switch Number	Support switch display of window quantity, and customized setup.
	⤡	Full Screen	Show full screen.
5	Monitor Window		● Multiple window/single window switch Multiple window display mode, Double-click window, switch to single display mode and Double-click again to return to multiple window display mode. ● Full screen mode Right-click window to select to enter full screen mode. If it is already in full screen mode, right-click to exit full screen. ● Exit tour. ● If it is in touring mode, to stop touring, you can right-click in the live view window and select "Stop Tour".
6	Person Snapshot Record Display Area		Show snapshot face snapshot. Move mouse to person snapshot and right-click the snapshot, you can: ● If this person is only snapshot but not recognized ◇ Select "sign up", add person to library following prompt. ◇ Select "record search", go to snapshot search page and search picture by picture. In snapshot history record, search all snapshots of this person. ◇ Select"Export", save person snapshot to client locally. Path is default path: ..\OPTIVIEW VMX \Client\Picture\Face\Export\Capture. ● If this person is recognized ◇ Select "Recognition Record Search", go to search page, and in snapshot history record search all recognition records of this person. ◇ Select"Export", save person snapshot and pictures this person in library all to client locally. Path is default path: ..\OPTIVIEW VMX Client\Picture\Face\Export\Recognize。 Double-click person snapshot, to view person details, including snapshot person cutout and panorama.

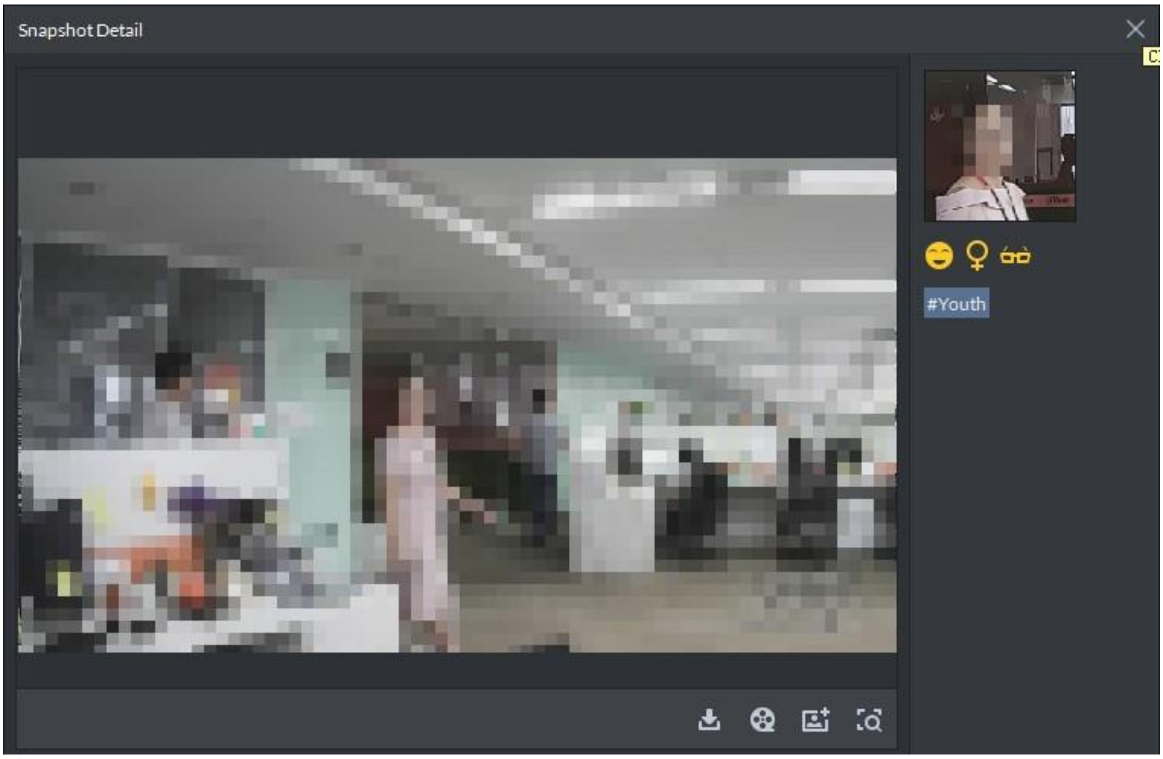
No.	Name	Description
7	Recognition Record Display Area	Show recognition record. ● Move mouse to person snapshot, and right-click support to: ◇ Select“Recognition Record Search”， go to recognition search page, and in snapshot history record, search all recognition records of this person. ◇ Select“Export”,and save person snapshot and snapshot of this person already uploaded to library all to client locally, default path is ..\Optiview VMX\Client\Picture\Face\Export\Recognize。 ● Double-click recognition record，you can view person cutout, panorama, used to person picture and info in face library. ● Click 🕘 at the upper right corner, go to recognition search page.

3.13.6.1.2 Viewing and Processing Snapshot Detail

- View snapshot detail

  In the area of person snapshot record, Double-click person snapshot to view face cutout and panoramic picture, see Figure 3-253.

Figure 3-253 Snapshot detail

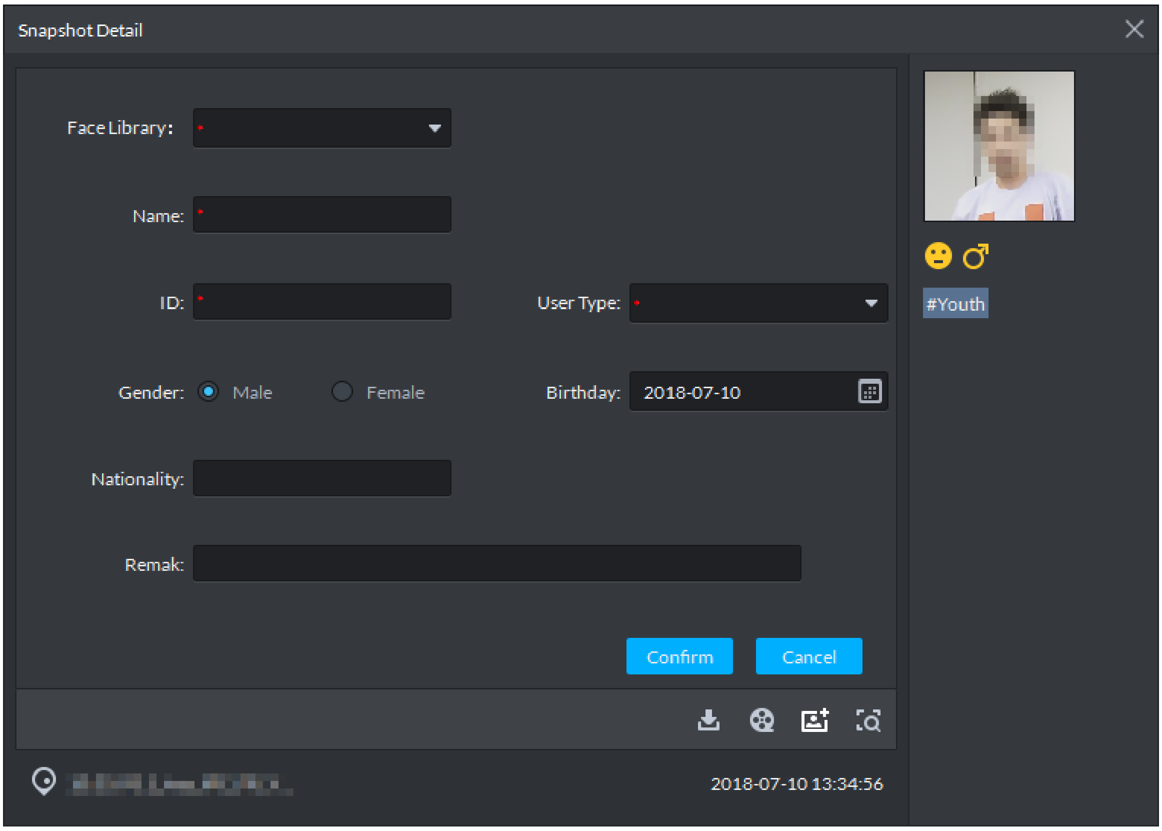


- Register captured person

Step 1 On snapshot detail window, click 🖼.

The system displays **Snapshot Detail** interface, see Figure 3-254.

Figure 3-254 Snapshot detail



Face Library: *

Name: *

ID: *

User Type: *

Gender: ● Male ○ Female

Birthday: 2018-07-10

Nationality:

Remak:

[redacted] 2018-07-10 13:34:56

Step 2 Configure person info, click **OK**.

- View video

  On the snapshot detail window, click 🎞 and enter record playback interface. If corresponding video exists in central server or device, then playback video, otherwise, system promps no record file. Video source priority is central server > device.
- Download video

  On snapshot detail window, click ⭳ and enter download center, download video according to requirement. For details, refer to **3.9.1.8 Downloading Record**.
- Search record

  On snapshot detail window, click 🔍 to enter record search page, search picture by picture. See Figure 3-255. Set search time and channel, click **Search** to search result. See Figure 3-256.

Figure 3-255

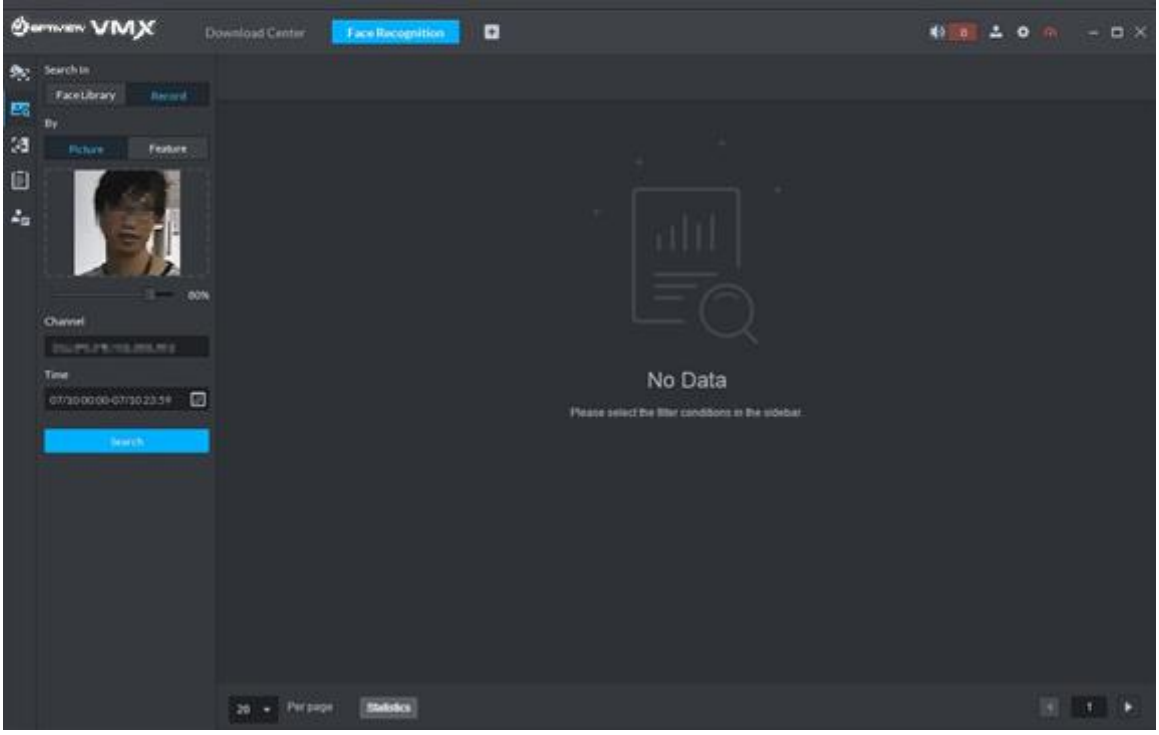
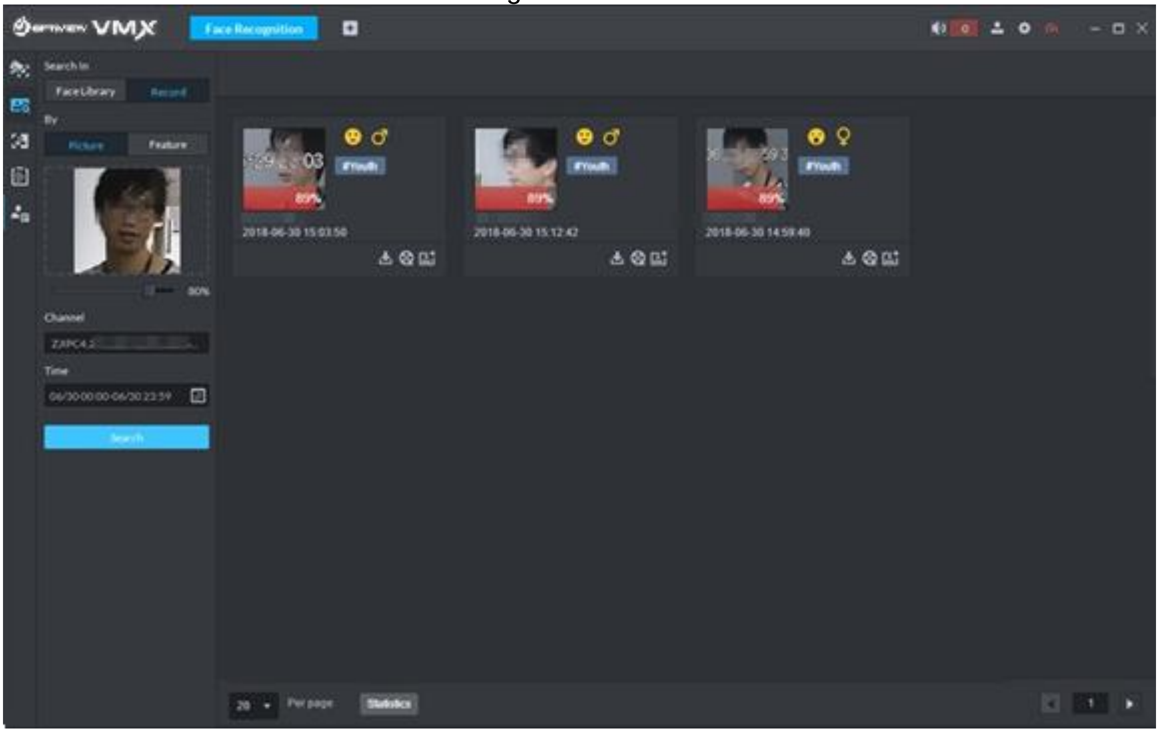

VMX
Download Center
Face Recognition
Search In
Face Library
Record
By
Picture
Feature
80%
Channel
Time
07/30 00:00-07/30 23:59
Search
No Data
Please select the filter conditions in the sidebar
20
Per page
Statistics
1

Figure 3-256

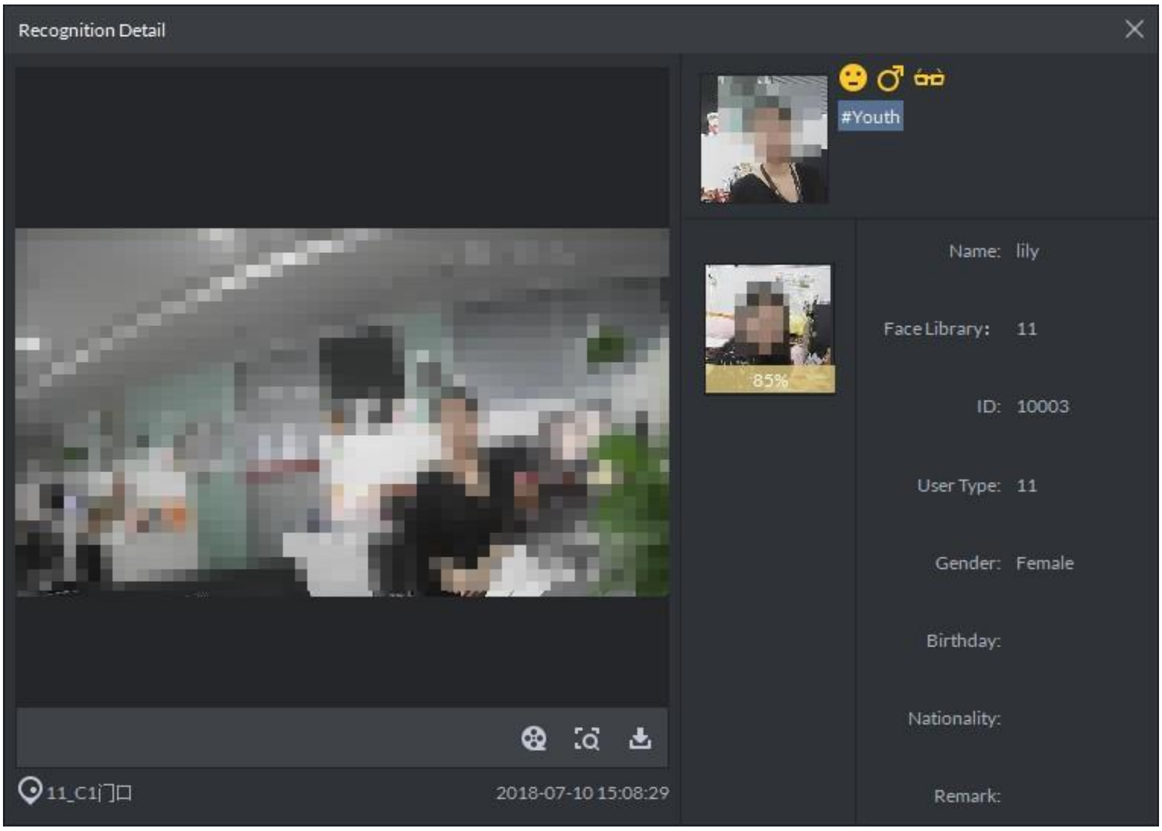

VMX
Face Recognition
Search In
Face Library
Record
By
Picture
Feature
80%
Channel
Time
06/30 00:00-06/30 23:59
Search
#Youth
89%
2018-06-30 15:03:56
#Youth
89%
2018-06-30 15:12:42
#Youth
89%
2018-06-30 14:59:40
20
Per page
Statistics
1

3.13.6.1.3 Viewing and Processing Recognition Record Detail

- View recognition detail

  In recognition record display area, double-click a piece of recognition record to view the details including face snapshot, scene picture, the corresponding registered face picture and person information. See Figure 3-257.

Figure 3-257 Recognitiond detail



Name: lily

Face Library: 11

ID: 10003

User Type: 11

Gender: Female

Birthday:

Nationality:

Remark:

11_C1门口

2018-07-10 15:08:29

- View video

On the snapshot detail window, click and enter record playback interface. If corresponding video exists in central server or device, then playback video, otherwise, system promps no record file. Video source priority is central server > device.

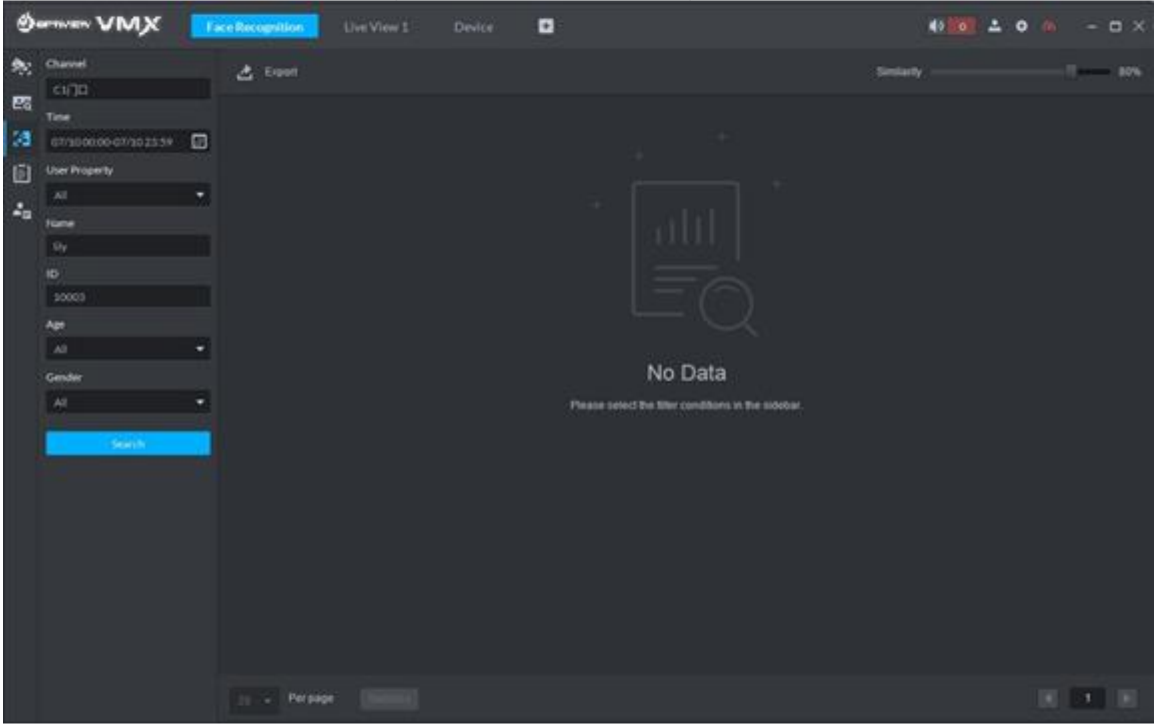
- Download video

On snapshot detail window, click and enter download center, download video according to requirement. For details, refer to **3.9.1.8 Downloading Record**.

- Search record

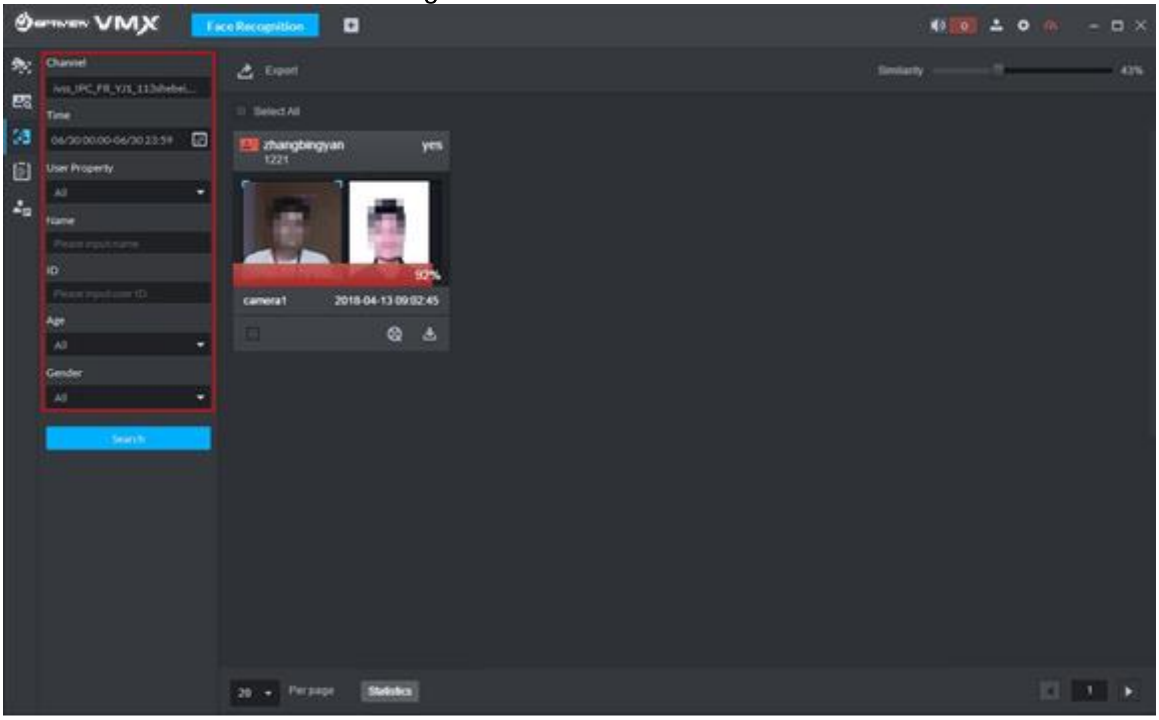
On snapshot detail window, click to enter record search page, search picture by picture. See Figure 3-258. Set search time and channel, click **Search** to search result. See Figure 3-259.

Figure 3-258 Search recognition


VMX
Face Recognition
Live View 1
Device
Channel
Time
User Property
Name
ID
Age
Gender
Search
Export
Similarity
80%
No Data
Please select the filter conditions in the sidebar.
Per page
1

Time: 07/10 00:00-07/10 23:59
User Property: All
ID: 10003
Age: All
Gender: All

Figure 3-259 Search result


VMX
Face Recognition
Channel
Time
User Property
Name
Please input name
ID
Please input user ID
Age
Gender
Search
Export
Similarity
43%
Select All
zhangbingyan
1221
yes
92%
camera1
2018-04-13 09:02:45
20
Per page
Statistics
1

Time: 06/30 00:00-06/30 23:59
User Property: All
Age: All
Gender: All

3.13.6.2 Searching Person

You can search qualified person by features or pictures. The supported search methods are shown as follows.

- Set feature info, search person who conforms to conditions in face database.
- Import picture, search person whose similarity conforms to threshold in face database.

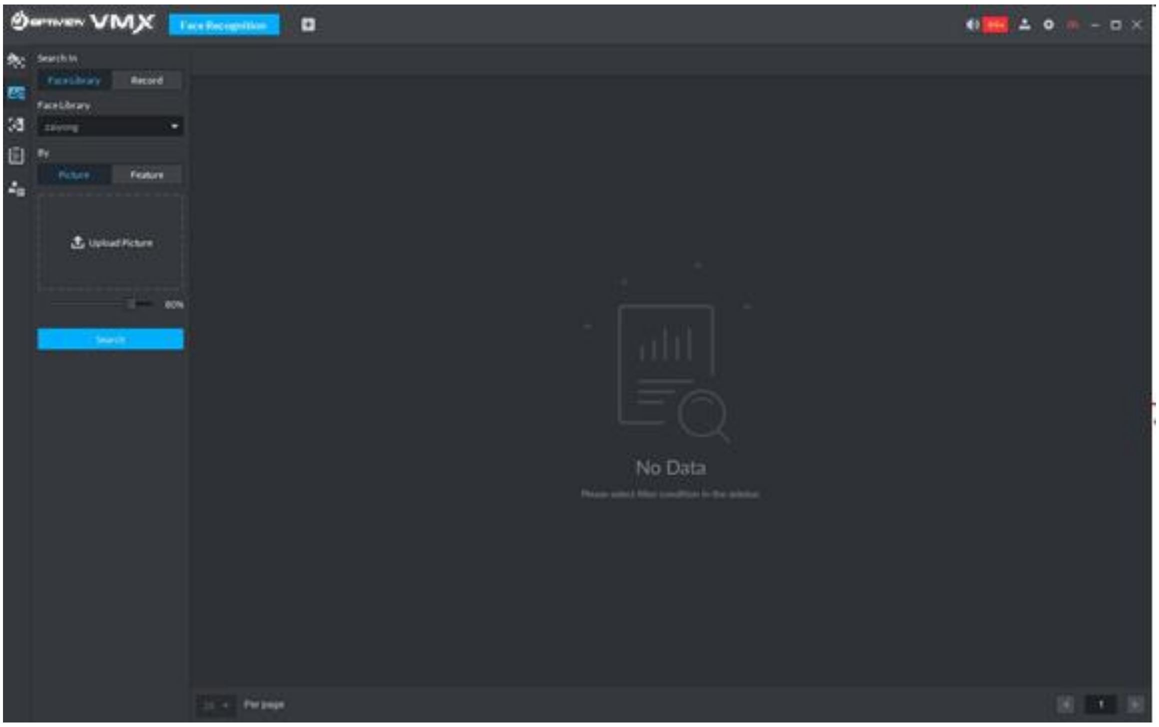
- Set feature info, search person who conforms to conditions in face database. You can view and search person movement track on map.
- Import picture and search person whose similarity conforms to threshold in snapshot record. You can view and search person movement track on map.

- If the device does not support search by picture, then the platform cannot search by picture either. If not supported by device, the platform prompts that channel not supported when selecting channel.
- In this chapter, it takes search by importing picture as an example to introduce operation. You can refer to the operation in this chapter for other search operations.

Step 1 On Face Recognition interface, click .

The system displays **Face Search** interface, see Figure 3-260.

Figure 3-260 Face search



Step 2 Select **Record** and **Picture**; click **Upload Picture**; set similarity; click **Search**.

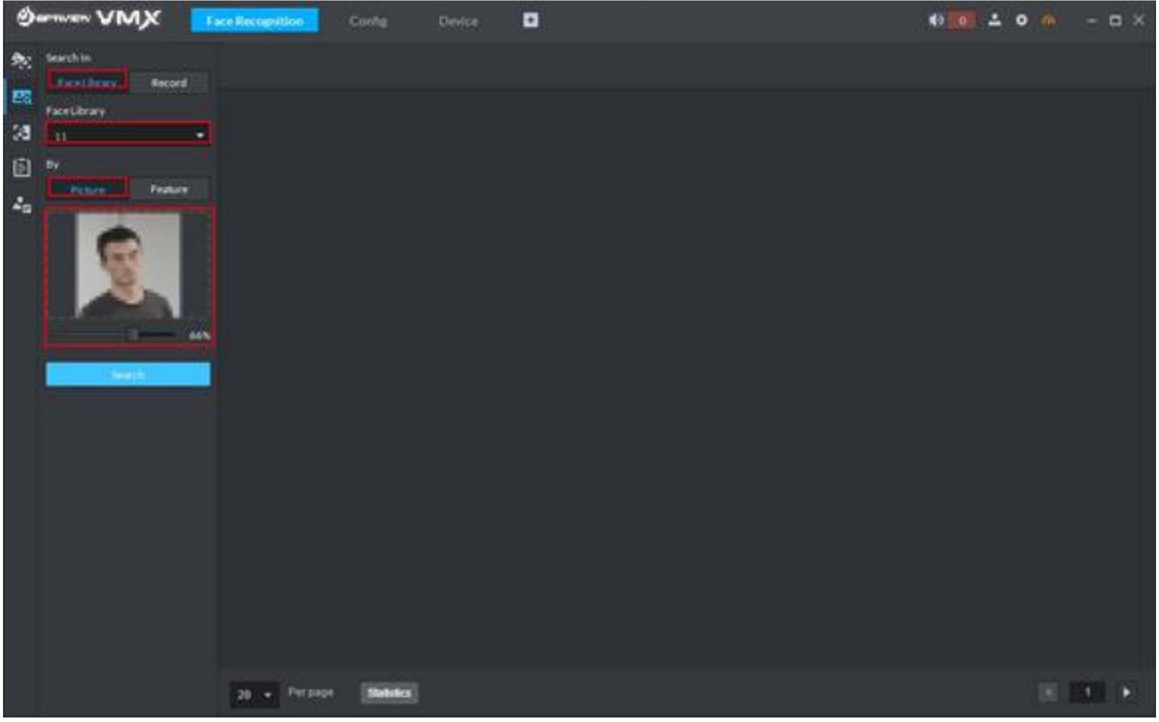
You need to set search condition during operation.

- Select **Face Library** and you can search from the face library, select **Record** and you can search from snapshot records.
- Select **Picture** and you can search by picture, you are required to upload picture and set similarity; select **Feature** and you can search by feature info.

Searched result is shown in Figure 3-261.

Similarity is not displayed if you search by feature.

Figure 3-261 Search by picture


VMX
Face Recognition
Config
Device
Search in
Face Library
Record
Face Library
11
By
Picture
Feature
66%
Search
20
Per page
Statistics
1

The supported operation of search result is similar.

The following are the operations of snapshot record search results, if it is the face database search result, then only support click , skip to recognition search interface, and search the recognition record of the person.

- Search detail

  Double-click to view detail.
- Download video

  On snapshot detail window, click and enter download center, download video according to requirement. For details, refer to **3.9.1.8 Downloading Record**.
- View video

  On the snapshot detail window, click and enter record playback interface. If corresponding video exists in central server or device, then playback video, otherwise, system promps no record file. Video source priority is central server > device.
- Register captured person to face database

  Click and display window of registered person.
- View track on map

  View track, you are required to drag device to map for display in advance. For more details, see 3.2.6 Configuring Emap.

  Click **Generate Track**, and display track map, see Figure 3-262.

Figure 3-262 Generate track

◇ Double-click the device on the map, and it will display all the snapshot records of the device, the device record is marked by blue in the left snapshot record list. See Figure 3-263.

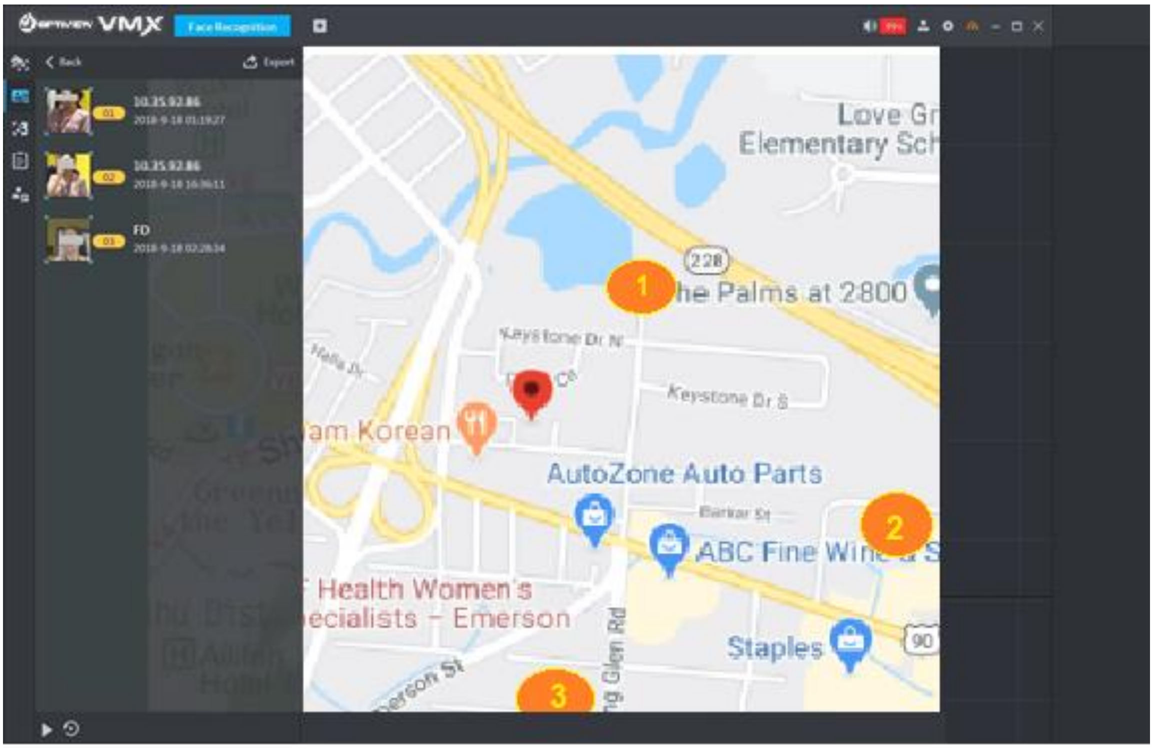

VMX
Face Recognition
Back
Export
01
10.35.92.86
2018-9-18 01:19:27
02
10.35.92.86
2018-9-18 16:36:11
03
FD
2018-9-18 02:28:34
1
2
3
Love Gr
Elementary Sch
228
he Palms at 2800
Keystone Dr N
Keystone Dr S
am Korean
AutoZone Auto Parts
ABC Fine Win
Health Women's
ecialists – Emerson
Staples
90

Figure 3-263 View detail

◇ Click ▶ to play movement trajectory; click ❚❚ to pause movement track; click ⟲ to play again.

◇ Click 📹 to playback video in the left snapshot record list.

◇ Playback video calls the stored video on the face recognition device; there will be no playback video if the device fails to store relevant video.

◇ Export trackcture.

◇ Click **Export**, press left mouse button on the map, and drag the mouse the select region. See Figure 3-264.

◇ Save it in the local as the form of picture according to the interface prompt.

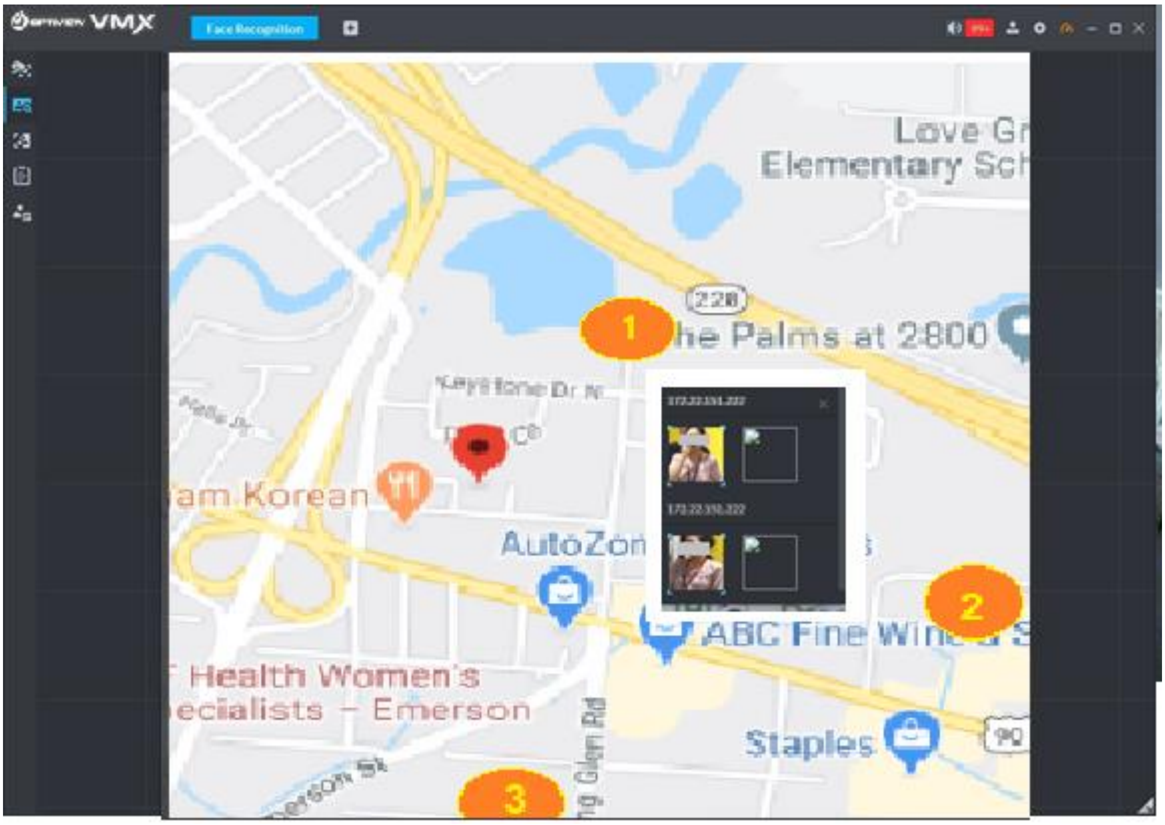

VMX
Face Recognition
Love Gr
Elementary Sch
228
1
he Palms at 2800
Keystone Dr N
am Korean
AutoZon
2
ABC Fine Win
Health Women's
ecialists – Emerson
Staples
90
3
ng Glen Rd

Figure 3-264 Export track

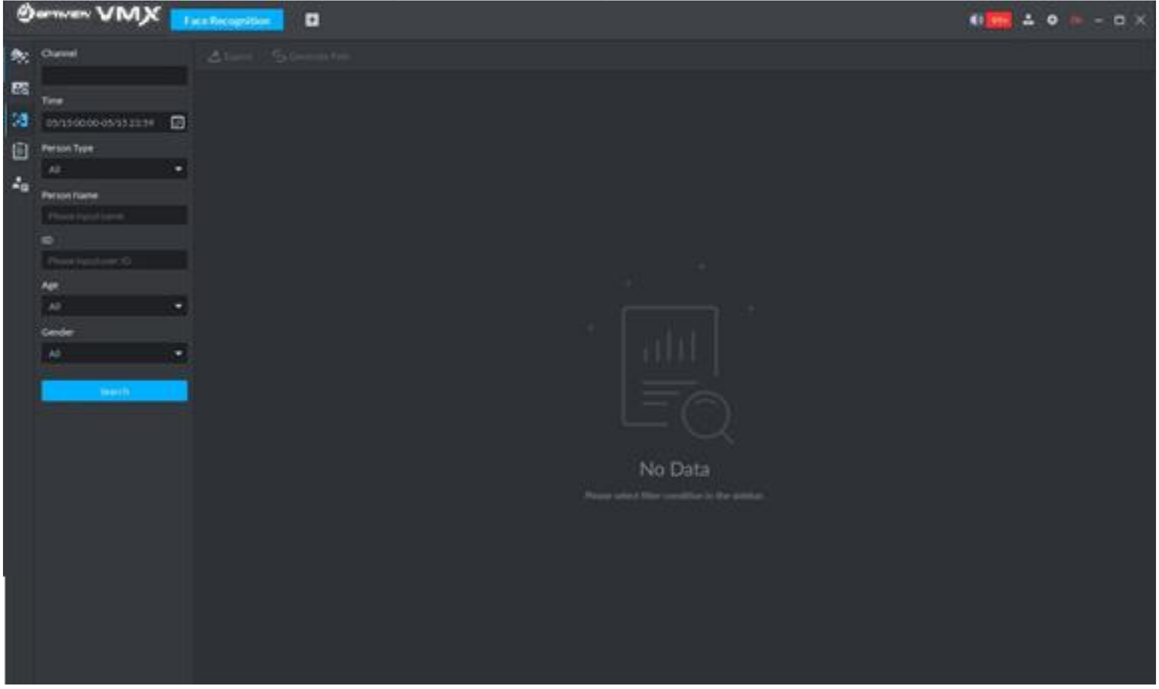
3.13.6.3 Searching Recognition Record

You can search qualified record from recognition record.

Step 1 On **Face Recognition** interface, click .

The system displays **Recognition Search** interface, see Figure 3-265.

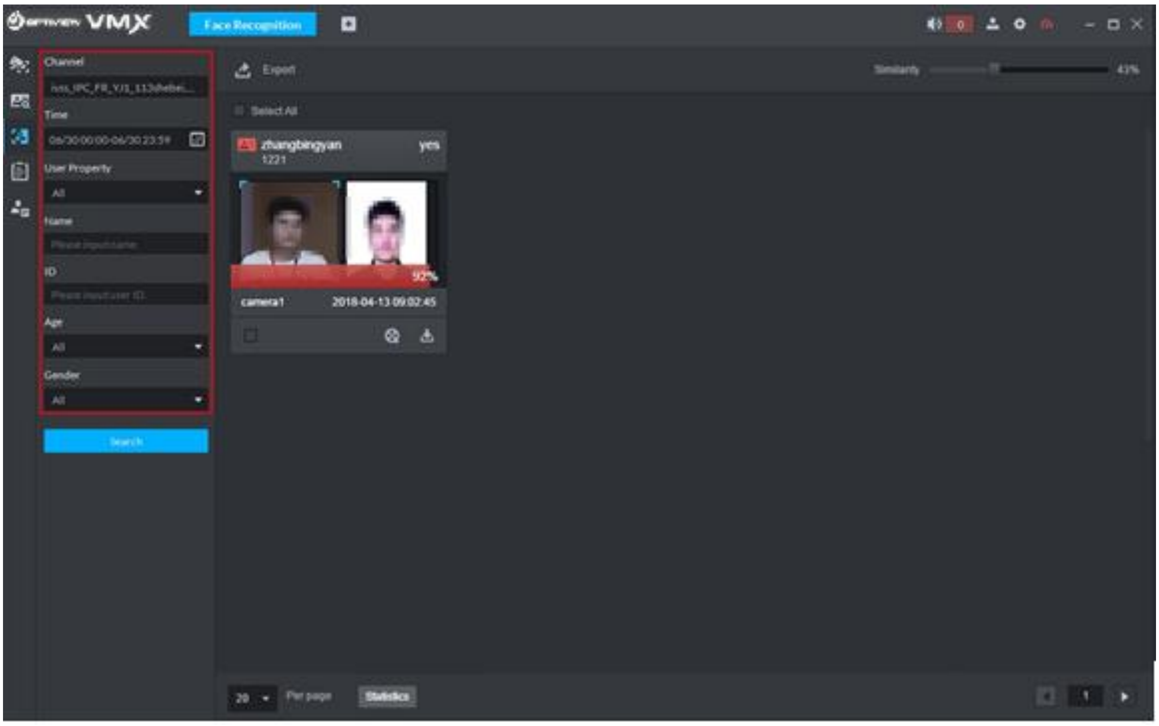
Figure 3-265 Recognition search


VMX
Face Recognition
Channel
Time
05/15 00:00:00-05/15 23:59
Person Type
All
Person Name
ID
Age
All
Gender
All
Search
Export
Generate File
No Data

Step 2 Set search condition, click **Search**.

The system displays search result, see Figure 3-266.

Figure 3-266


VMX
Face Recognition
Export
Similarity
43%
Channel
Time
06/30 00:00:00-06/30 23:59
User Property
All
Name
ID
Age
All
Gender
All
Search
Select All
zhangbingyan
1221
yes
92%
camera1
2018-04-13 09:02:45
20
Per page
Statistics
1

3.13.6.4 Showing Report

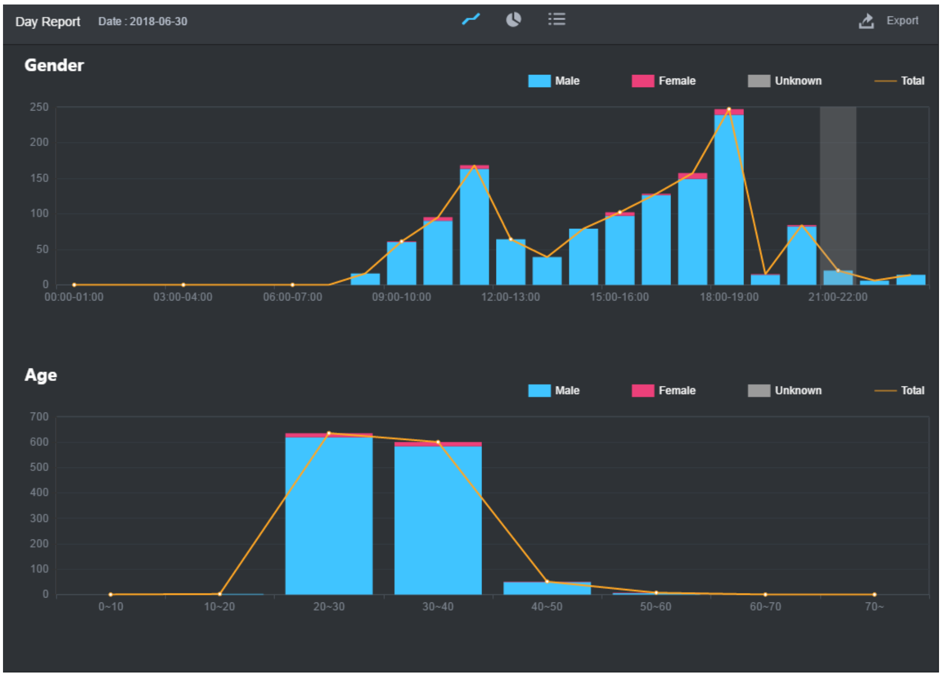
Step 1 On **Face Recognition** interface, click 📋.

The system displays **Report** interface.

Step 2 Select channel of data report you want to view (multiple choice), select data period (day, week, and month), and click **Search** to create a report of the selected period.

- Line chart is shown in Figure 3-267.

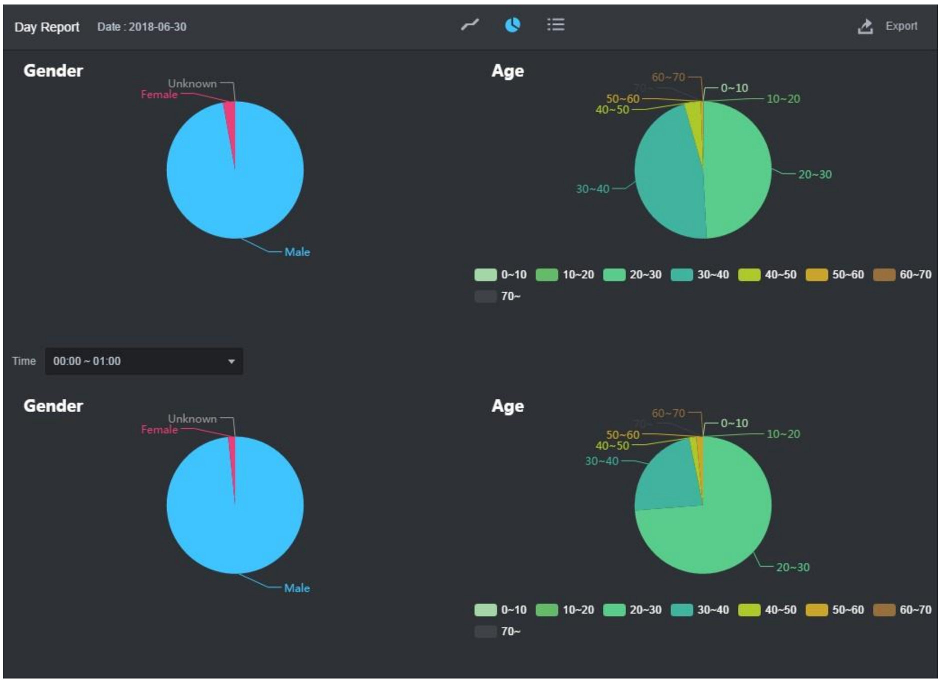
Figure 3-267 Face report line chart



Day Report
Date : 2018-06-30
Export
Gender
Male
Female
Unknown
Total
250
200
150
100
50
0
00:00-01:00
03:00-04:00
06:00-07:00
09:00-10:00
12:00-13:00
15:00-16:00
18:00-19:00
21:00-22:00
Age
Male
Female
Unknown
Total
700
600
500
400
300
200
100
0
0~10
10~20
20~30
30~40
40~50
50~60
60~70
70~

- Pie chart is shown in Figure 3-268.

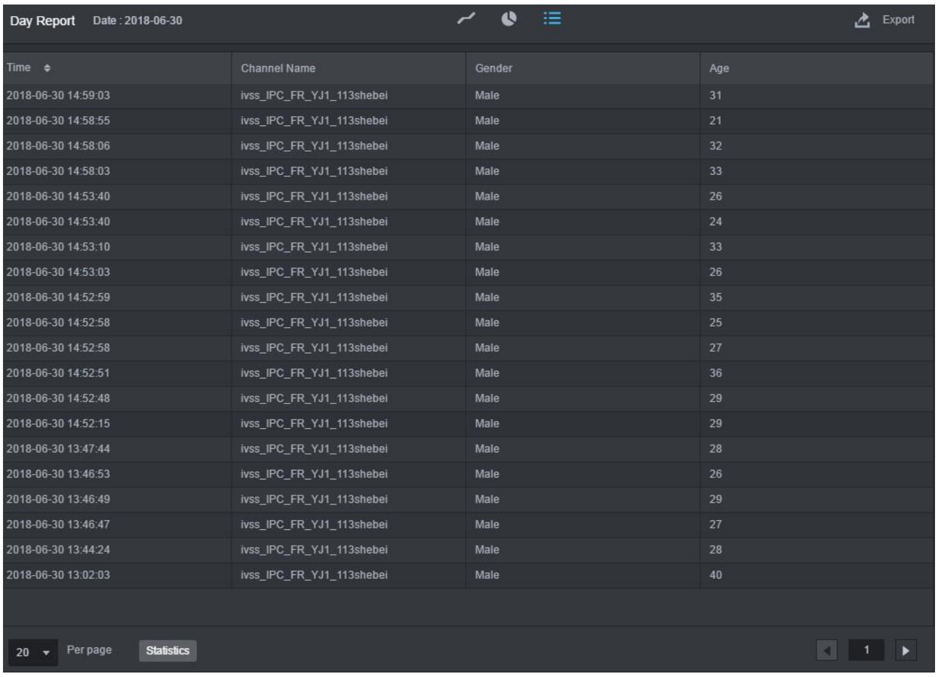
Figure 3-268 Face report pie chart



Day Report
Date : 2018-06-30
Export
Gender
Unknown
Female
Male
Age
60~70
0~10
10~20
50~60
40~50
30~40
20~30
0~10
10~20
20~30
30~40
40~50
50~60
60~70
70~
Time
00:00 ~ 01:00
Gender
Unknown
Female
Male
Age
60~70
0~10
10~20
50~60
40~50
30~40
20~30
0~10
10~20
20~30
30~40
40~50
50~60
60~70
70~

- List is shown in Figure 3-269.

Figure 3-269 List display



Time	Channel Name	Gender	Age
2018-06-30 14:59:03	ivss_IPC_FR_YJ1_113shebei	Male	31
2018-06-30 14:58:55	ivss_IPC_FR_YJ1_113shebei	Male	21
2018-06-30 14:58:06	ivss_IPC_FR_YJ1_113shebei	Male	32
2018-06-30 14:58:03	ivss_IPC_FR_YJ1_113shebei	Male	33
2018-06-30 14:53:40	ivss_IPC_FR_YJ1_113shebei	Male	26
2018-06-30 14:53:40	ivss_IPC_FR_YJ1_113shebei	Male	24
2018-06-30 14:53:10	ivss_IPC_FR_YJ1_113shebei	Male	33
2018-06-30 14:53:03	ivss_IPC_FR_YJ1_113shebei	Male	26
2018-06-30 14:52:59	ivss_IPC_FR_YJ1_113shebei	Male	35
2018-06-30 14:52:58	ivss_IPC_FR_YJ1_113shebei	Male	25
2018-06-30 14:52:58	ivss_IPC_FR_YJ1_113shebei	Male	27
2018-06-30 14:52:51	ivss_IPC_FR_YJ1_113shebei	Male	36
2018-06-30 14:52:48	ivss_IPC_FR_YJ1_113shebei	Male	29
2018-06-30 14:52:15	ivss_IPC_FR_YJ1_113shebei	Male	29
2018-06-30 13:47:44	ivss_IPC_FR_YJ1_113shebei	Male	28
2018-06-30 13:46:53	ivss_IPC_FR_YJ1_113shebei	Male	26
2018-06-30 13:46:49	ivss_IPC_FR_YJ1_113shebei	Male	29
2018-06-30 13:46:47	ivss_IPC_FR_YJ1_113shebei	Male	27
2018-06-30 13:44:24	ivss_IPC_FR_YJ1_113shebei	Male	28
2018-06-30 13:02:03	ivss_IPC_FR_YJ1_113shebei	Male	40

3.13.6.5 Viewing Face Recognition Alarm

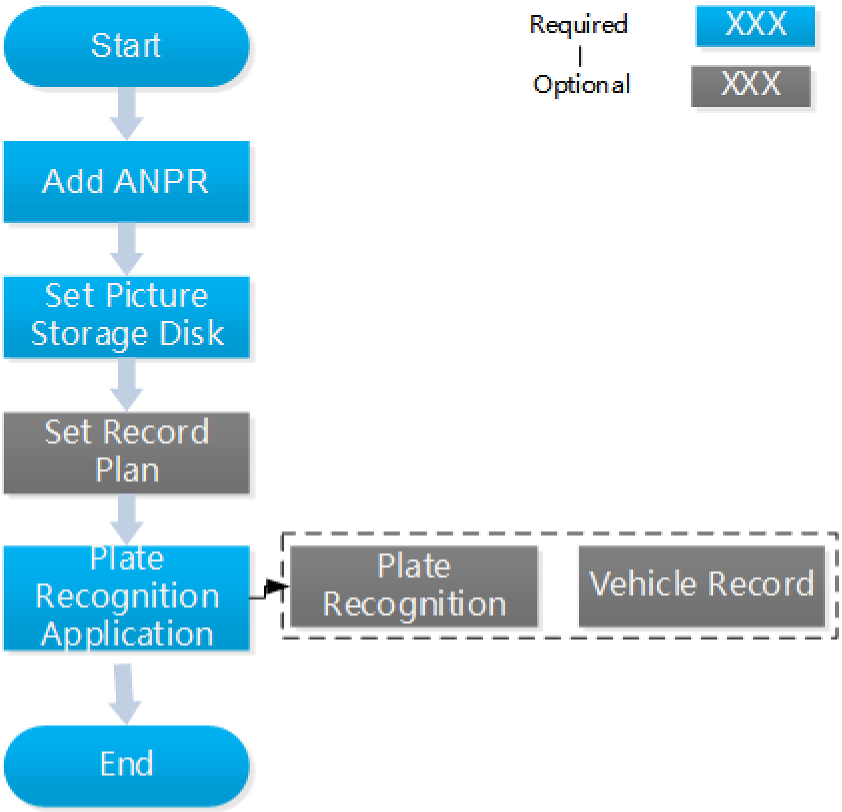
View and process face recognition alarm event in event center, see Figure 3-270. For more details, see **3.10 Event Center**.

Figure 3-270 List display

3.14 ANPR

After ANPR is added to platform, the platform can receive plate recognition result reported by ANPR. The plate recognition operation flow is shown in Figure 3-271.

Figure 3-271 Plate recognition flow


Required
Optional
XXX
XXX
Start
Add ANPR
Set Picture Storage Disk
Set Record Plan
Plate Recognition Application
Plate Recognition
Vehicle Record
End

3.14.1 Adding ANPR

Add ANPR; see **3.2.2.4 Adding Device** for more details.

3.14.2 Setting Picture Storage Disk

Configure local storage disk, you have to reserve a ANPR picture disk to store ANPR snapshot, otherwise, snapshot cannot be stored, and snapshots are not displayed. For more details, see **3.2.1.4 Setting Storage Space**

3.14.3 Setting Record Plan

Only when record storage plan is configured, then video before and after snapshot can be stored, the platform can playback video 10 seconds before and after ANPR snapshot. If you need to set record storage plan, see **3.2.5 Setting Record Plan**.

3.14.4 Plate Recognition Application

3.14.4.1 Plate Recognition

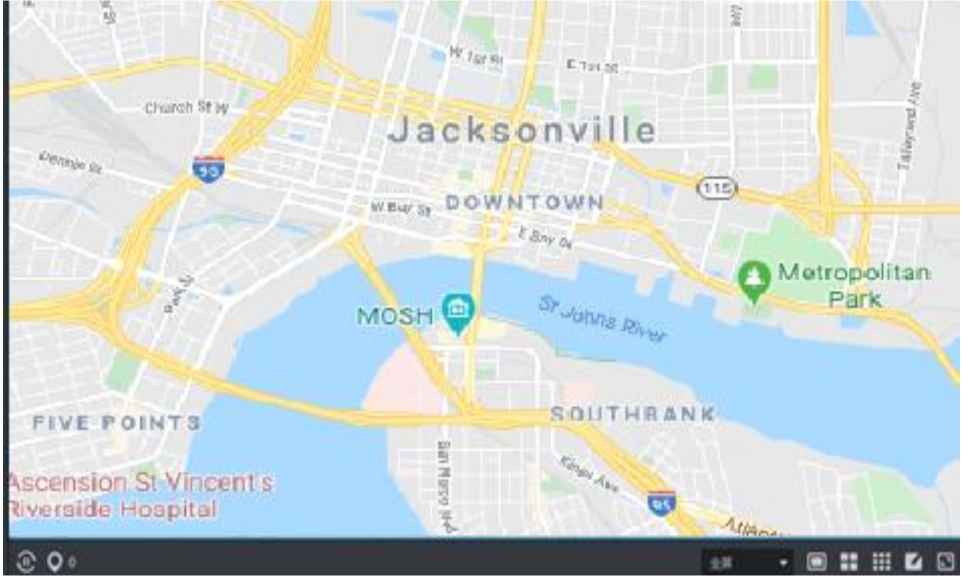
Step 1 On client homepage, click **ANPR**.

The system displays **ANPR** interface.

Step 2 Click .

The system displays **ANPR** interface. The emap is displayed with single window by default; you can switch number of windows. See Figure 3-272.

Figure 3-272 Plate recognition

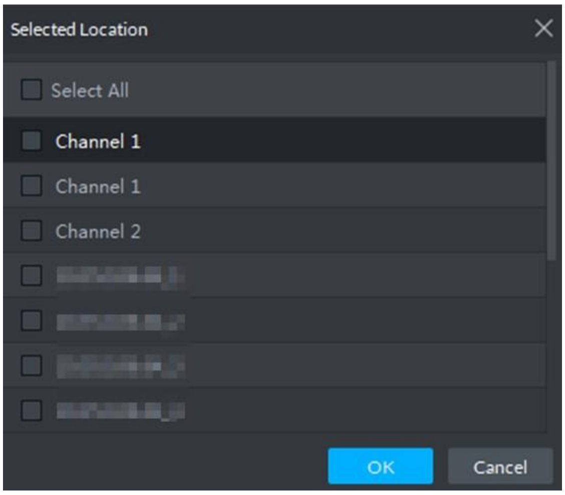

Church St W
Jacksonville
DOWNTOWN
W Bay St
E Bay St
115
Metropolitan
Park
MOSH
St Johns River
FIVE POINTS
SOUTHBANK
scension St Vincent's
iverside Hospital
San Marco Blvd
Kings Ave
95
Talleyrand Ave

Click .

The system displays **Selected Location** interface, see Figure 3-273.

Step 3

Figure 3-273 Select ANPR channel



Selected Location

☐ Select All

☐ Channel 1

☐ Channel 1

☐ Channel 2

☐ [redacted]

☐ [redacted]

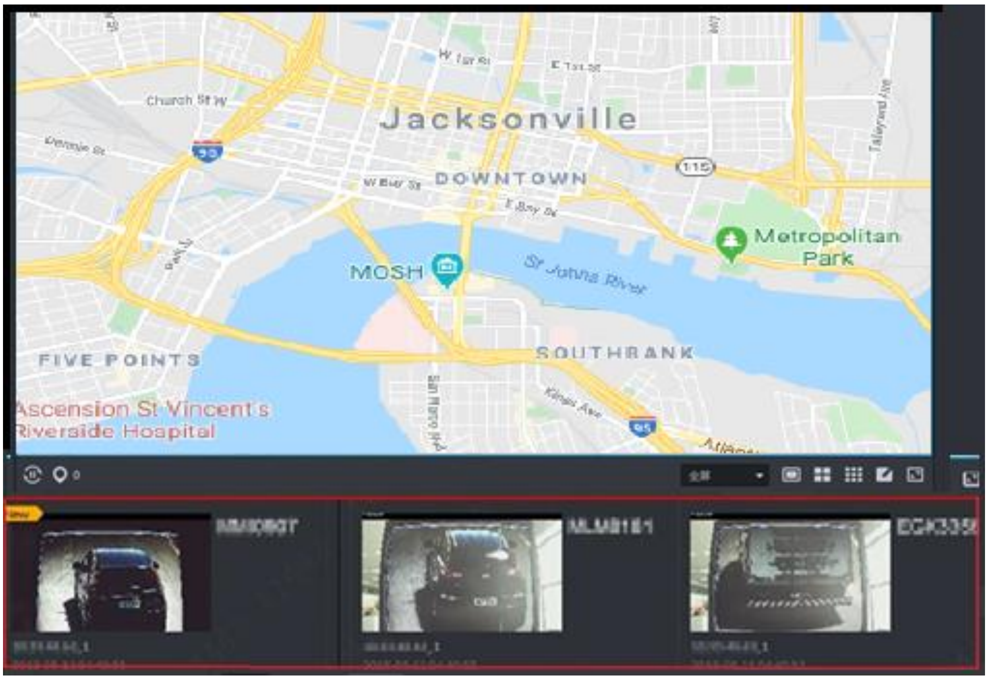
☐ [redacted]

☐ [redacted]

Step 4 Select ANPR device and then click **OK**.

System displays the selected channel amount and the latest passing vehicle image on the rolling pane. See Figure 3-274.

Figure 3-274 Plate recognition result


Jacksonville
DOWNTOWN
Metropolitan Park
MOSH
St Johns River
FIVE POINTS
SOUTHBANK
Ascension St Vincent's Riverside Hospital
Church St W
W 1st St
E 1st St
W Bay St
E Bay St

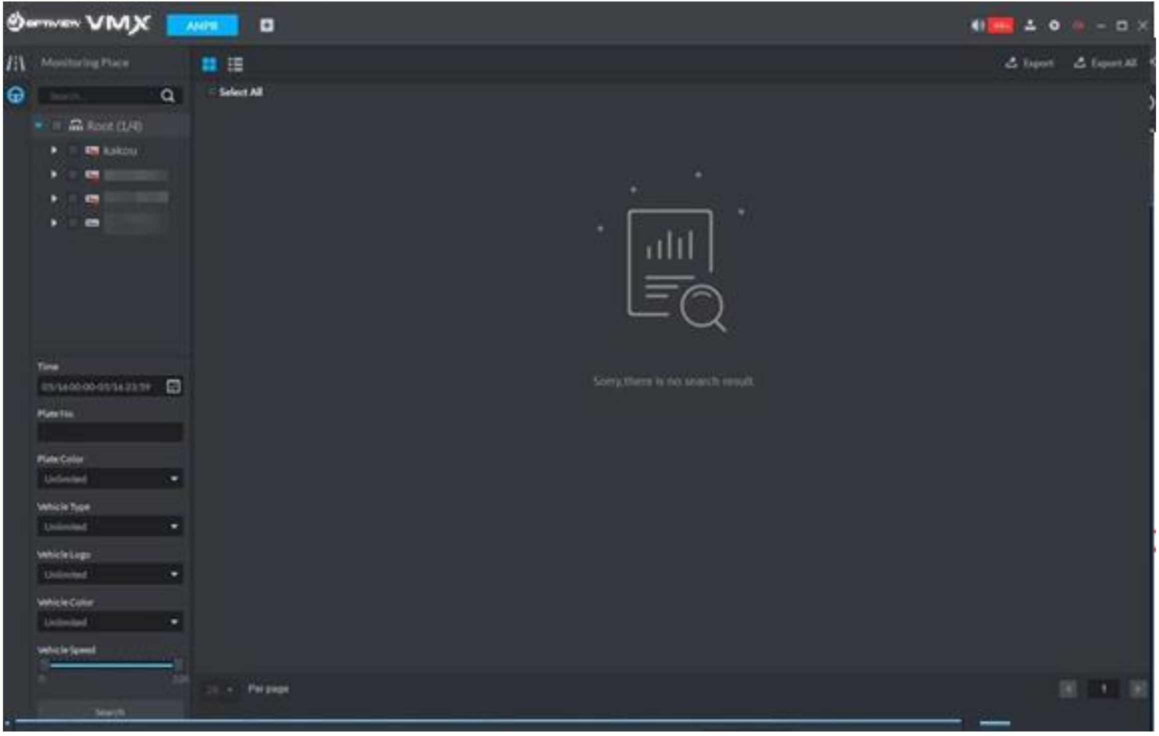
Step 5 Double-click the image to view image details. It includes plate number, snapshot time, ANPR channel name, vehicle logo, vehicle color.

3.14.4.2 Vehicle Record

Step 1 On ANPR interface, click .

The system displays **Vehicle Record** interface, see Figure 3-275.

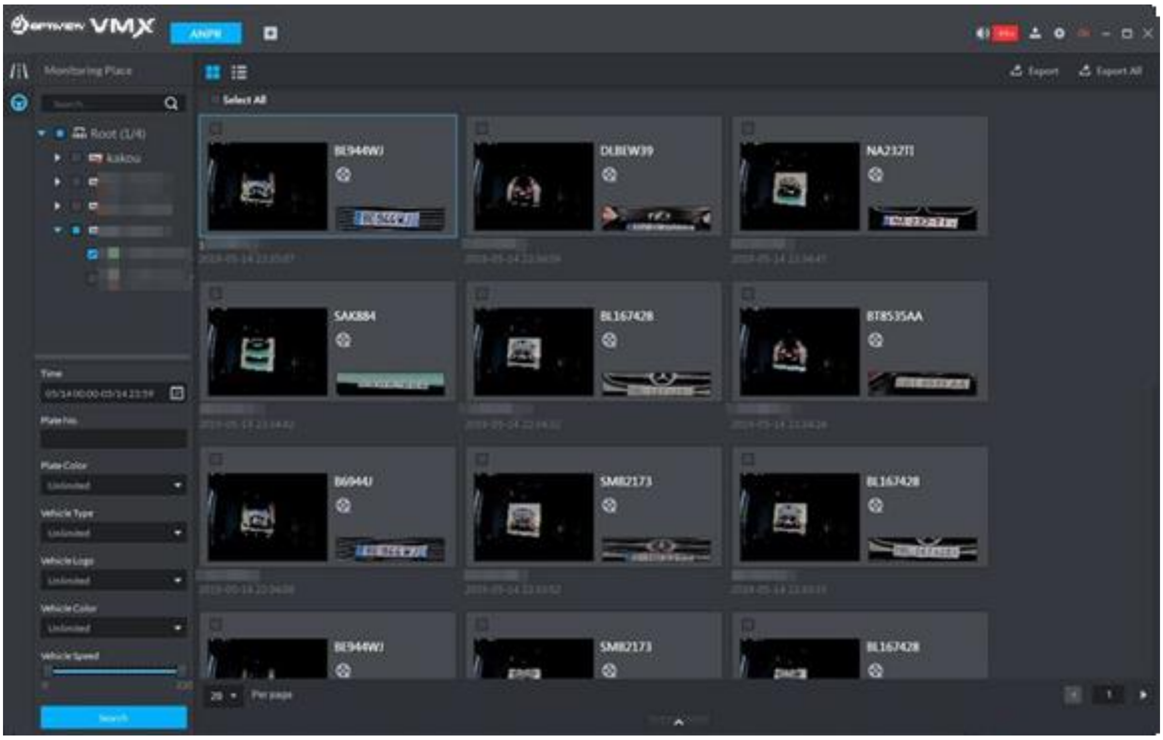
Figure 3-275 Vehicle record


VMX
ANPR
Monitoring Place
Export
Export All
Select All
Root (1/4)
kakou
Sorry, there is no search result.
Time
Plate No.
Plate Color
Unlimited
Vehicle Type
Unlimited
Vehicle Logo
Unlimited
Vehicle Color
Unlimited
Vehicle Speed
Per page
Search

Step 2 Select video channel and set search conditions. Click **Search**.

System displays search result. See Figure 3-276.

Figure 3-276 Passed vehicle search result


VMX
ANPR
Monitoring Place
Export
Export All
Select All
Root (1/4)
kakou
BE944WJ
DLBEW39
NA232TI
SAK884
BL167428
BT8535AA
B6944J
SMB2173
BL167428
BE944WJ
SMB2173
BL167428
Time
Plate No.
Plate Color
Unlimited
Vehicle Type
Unlimited
Vehicle Logo
Unlimited
Vehicle Color
Unlimited
Vehicle Speed
20
Per page
Search

For the passed vehicle, you can view its detailed information, record and running track. Refer to the operations listed below.

- Click View mode (⊞) or list mode (☰), it is to select different display mode.

- Select a snapshot image and then click ⌃ or Double-click the image, system displays detailed information. See Figure 3-277. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 3-278.

Figure 3-277 Vehicle details

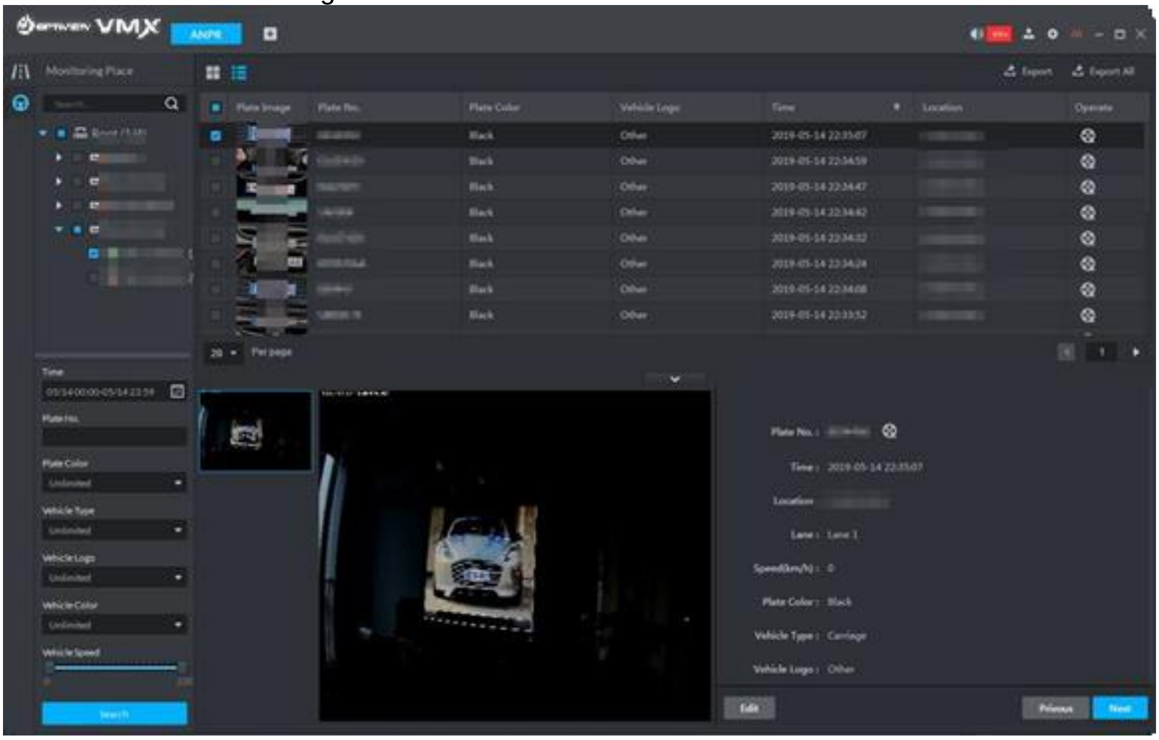
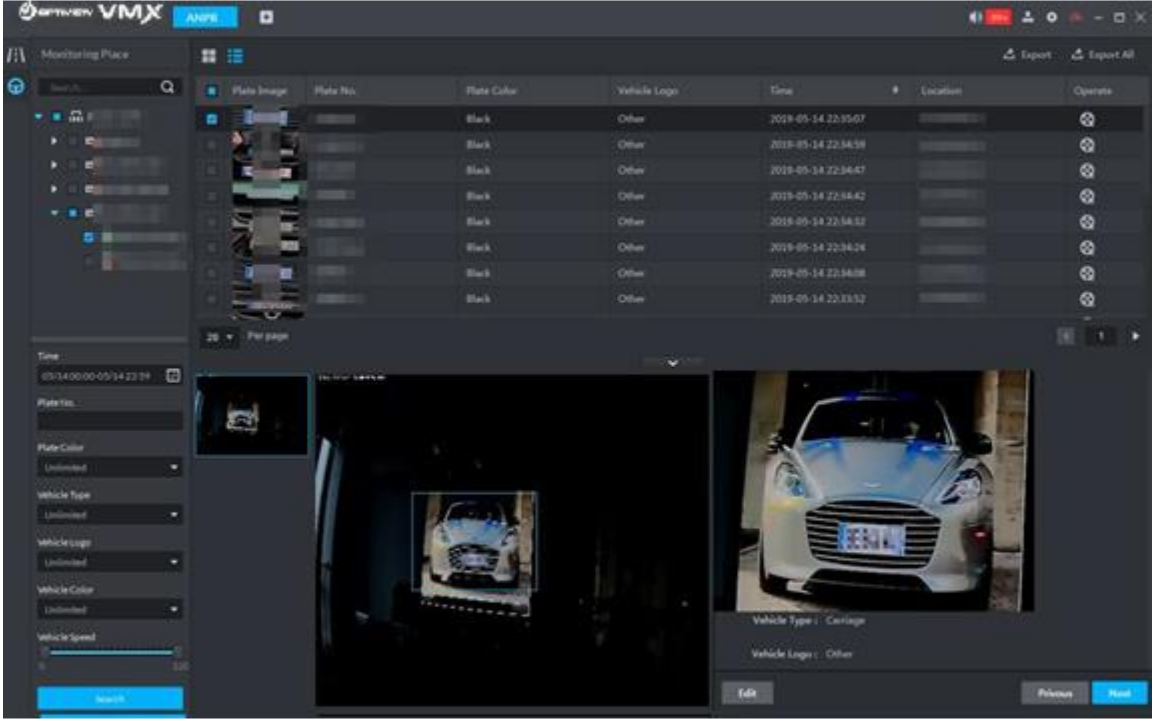
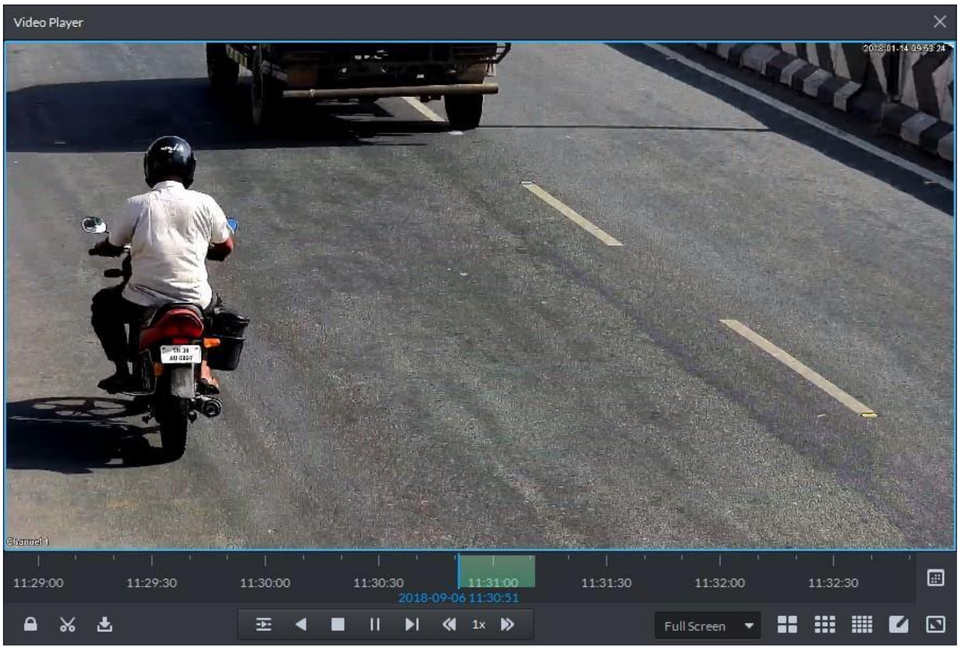

VMX
ANPR
Monitoring Place
Export
Export All
Plate Image
Plate No.
Plate Color
Vehicle Logo
Time
Location
Operate
Per page
Time
Plate No.
Plate Color
Vehicle Type
Vehicle Logo
Vehicle Color
Vehicle Speed
Search
Plate No.:
Time: 2019-05-14 22:35:07
Location
Lane: Lane 1
Speed(km/h): 0
Plate Color: Black
Vehicle Type: Carriage
Vehicle Logo: Other
Edit
Previous
Next

Figure 3-278 Regional zoom


VMX
ANPR
Monitoring Place
Export
Export All
Plate Image
Plate No.
Plate Color
Vehicle Logo
Time
Location
Operate
Per page
Time
Plate No.
Plate Color
Vehicle Type
Vehicle Logo
Vehicle Color
Vehicle Speed
Search
Vehicle Type: Carriage
Vehicle Logo: Other
Edit
Previous
Next

- Click ▶ to playback the 15-second video before and after the vehicle passed time. See Figure 3-279. The video file is total 30 seconds. Display the 15-second video before and after the vehicle passed.

Figure 3-279 Playback video

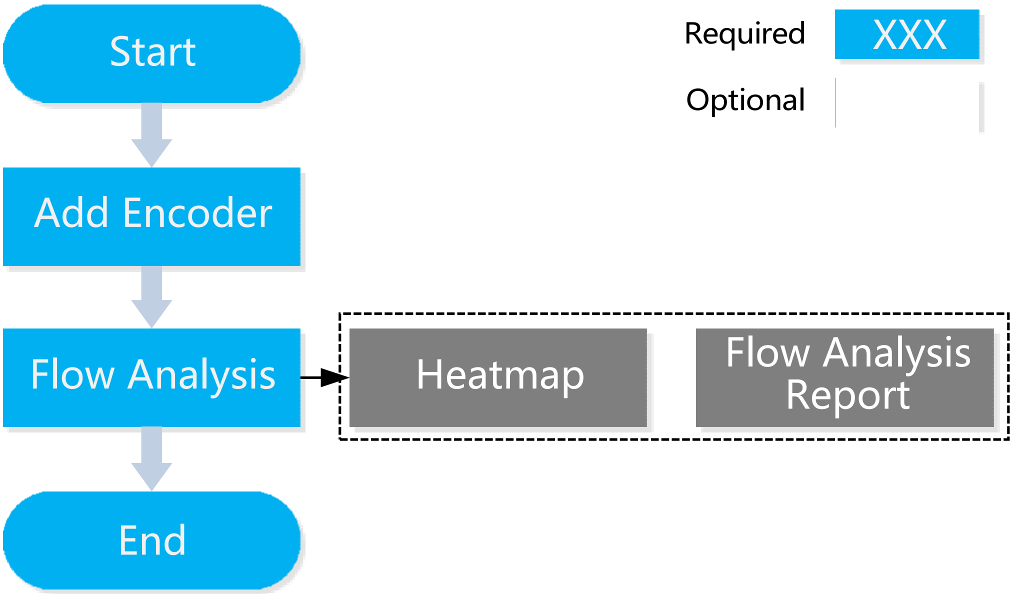

Video Player
Channel 1
11:29:00
11:29:30
11:30:00
11:30:30
11:31:00
11:31:30
11:32:00
11:32:30
2018-09-06 11:30:51
1x
Full Screen

- Click to view the vehicle running track.
- Export: Select the passed vehicle information and then click **Export** and export selected passed vehicle. Click **Export All**, and export all searched passed vehicle information.

3.15 Flow Analysis

After adding steoreo vision flow analysis camera to platform, the platform supports searching flow analysis report and heat map. The operation of flow analysis is shown in Figure 3-280.

Figure 3-280 Flow analysis


Start
Add Encoder
Flow Analysis
Heatmap
Flow Analysis Report
End
Required
XXX
Optional

3.15.1 Adding Encoder

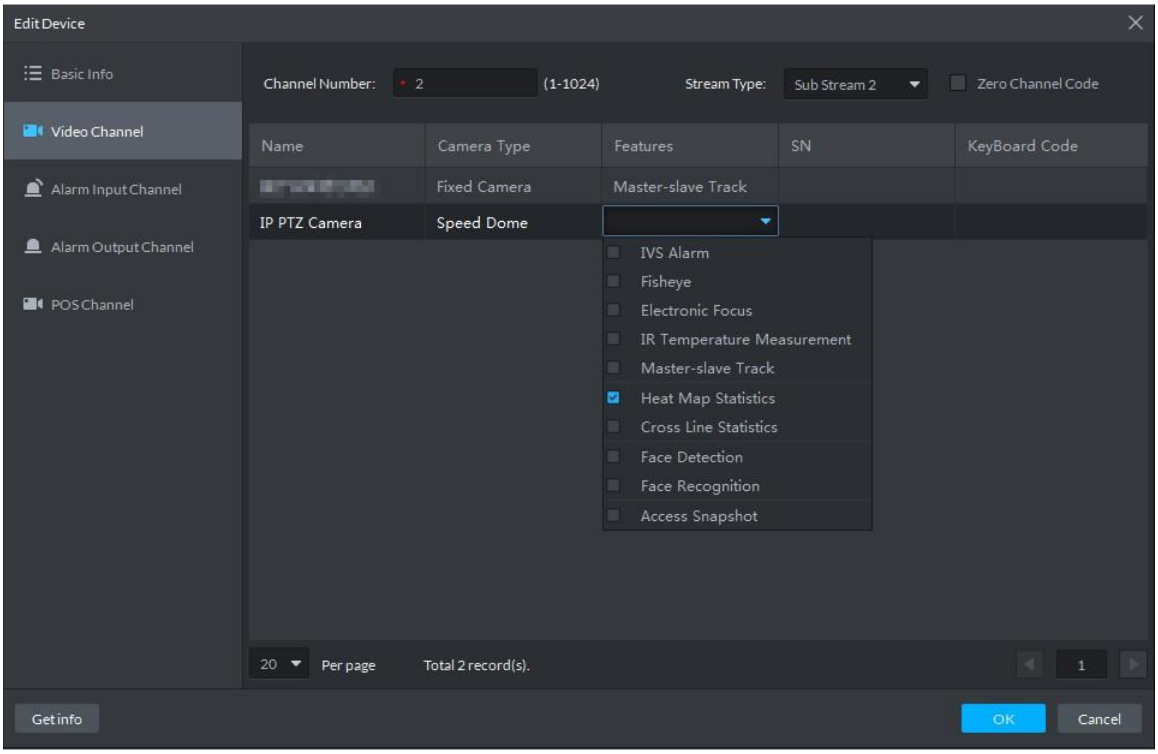
⚠

The platform only displays results reported by camera. Please make sure the added steoreo vision camera already enables people counting function. For detailed operation, please refer to device user manual.

Step 1 Add steoreo vision camera. For detailed operation, see 3.2.2.4 Adding Device.

Step 2 Modify device feature. On **Device** interface, click ✎ and modify device **Features** as **Heatmap Statistics**. See Figure 3-281.

Figure 3-281 Modify feature



Edit Device

Channel Number: * 2 (1-1024)

Stream Type: Sub Stream 2

☐ Zero Channel Code

Name	Camera Type	Features	SN	KeyBoard Code
[redacted]	Fixed Camera	Master-slave Track		
IP PTZ Camera	Speed Dome			

- ☐ IVS Alarm
- ☐ Fisheye
- ☐ Electronic Focus
- ☐ IR Temperature Measurement
- ☐ Master-slave Track
- ☑ Heat Map Statistics
- ☐ Cross Line Statistics
- ☐ Face Detection
- ☐ Face Recognition
- ☐ Access Snapshot

20 Per page Total 2 record(s). 1

3.15.2 Flow Analysis Application

3.15.2.1 Heatmap

Present distribution of moving objects according to color.

📖

The device uploads heatmap statistics data to platform. You can view the uploaded statistics data.

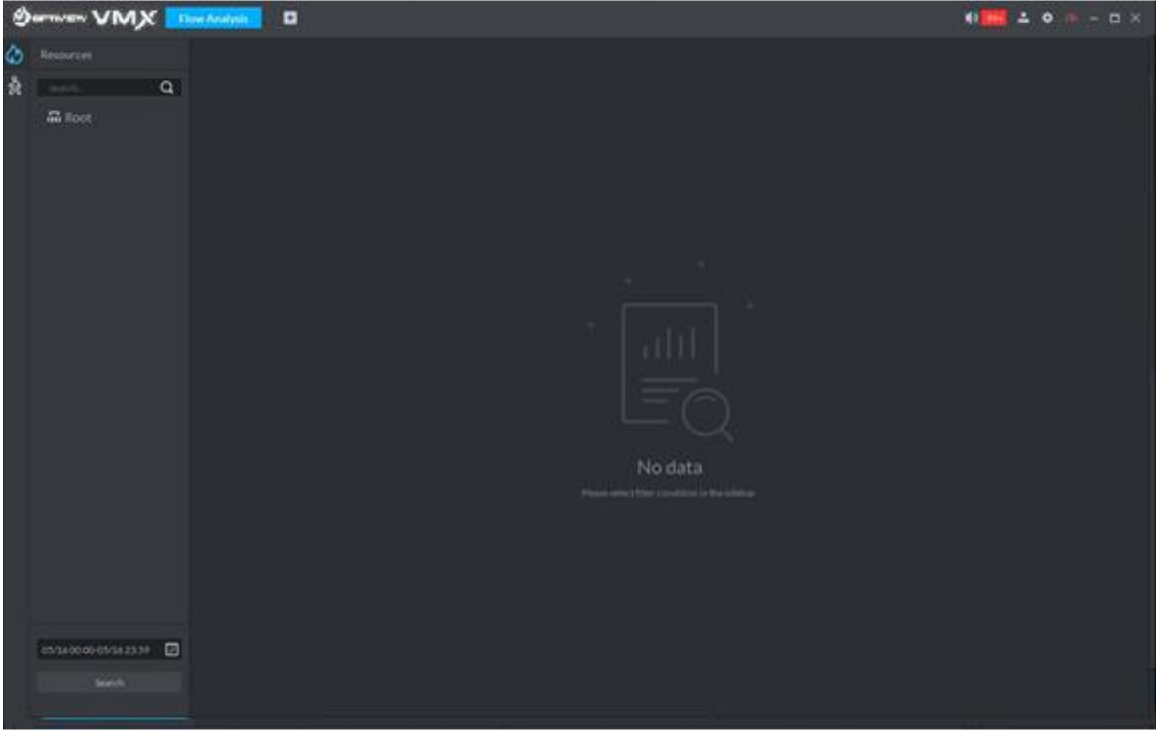
Step 1 On client homepage, click **Flow Analysis**.

The system displays **Flow Analysis** interface.

Step 2 Click 🔥.

The system displays **Heatmap** interface, see Figure 3-282.

Figure 3-282 Heatmap

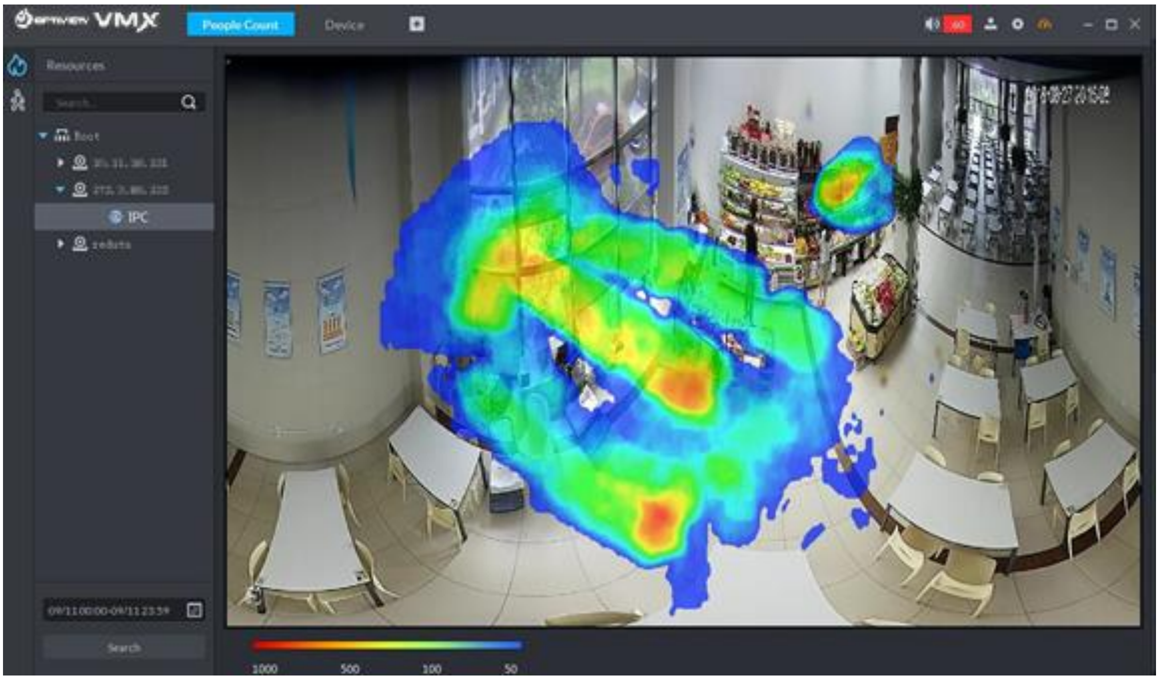

VMX
Flow Analysis
Resources
Root
No data
Search

N

Step 3 Select the channel that displays heatmap, select time and click **Search**.

The system displays heatmap, see Figure 3-283.

Figure 3-283 Heatmap search result


VMX
People Count
Device
Resources
Root
IPC
Search
1000
500
100
50

Step 4 Click Export on upper right corner of the interface, save heatmap picture to local in bmp according to prompt on interface.

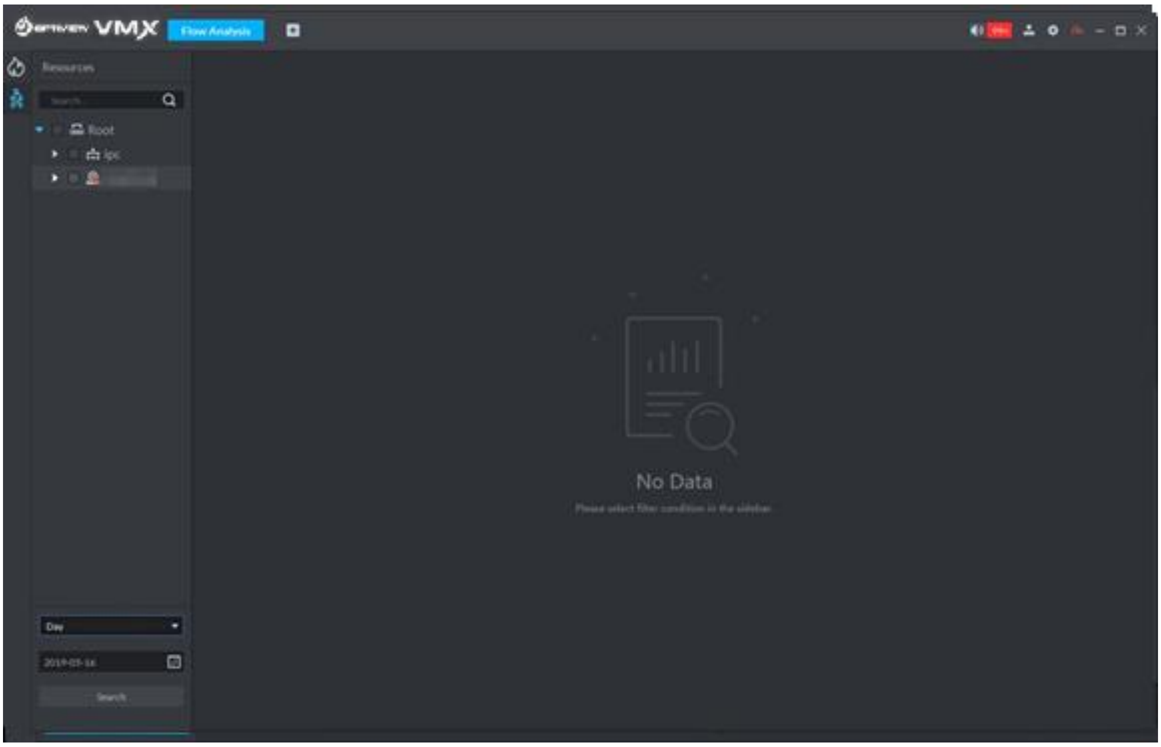
3.15.2.2 Flow Analysis Report

Search in and out people number, and form data report. Support searching stay people number if it is day report.

Step 1 On **Flow Analysis** interface, click .

The system displays **Flow Analysis** interface, see Figure 3-284.

Figure 3-284 Flow analysis


VMX
Flow Analysis
Resources
Search
Root
ipc
No Data
Day
Search

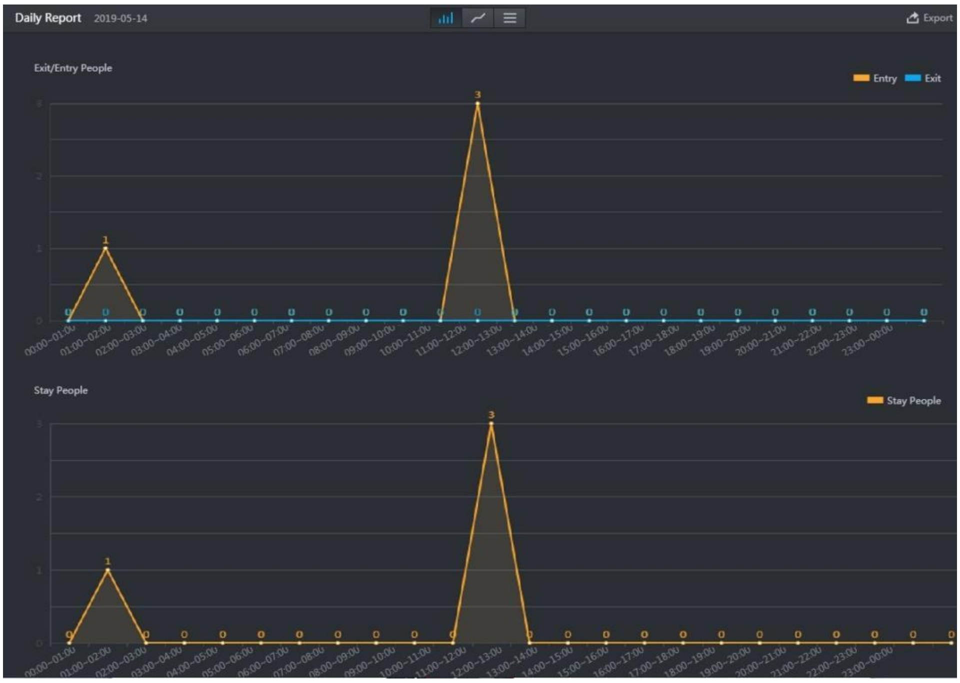
Step 2 Select device channel, search period and statistics time, and click **Search**.

The system generates report, see Figure 3-285.

Report includes bar chart, line chart and list, click on top of interface and switch display mode.

Statistics about stay people number is not implemented if search period is week, month or year.

Figure 3-285 Search result

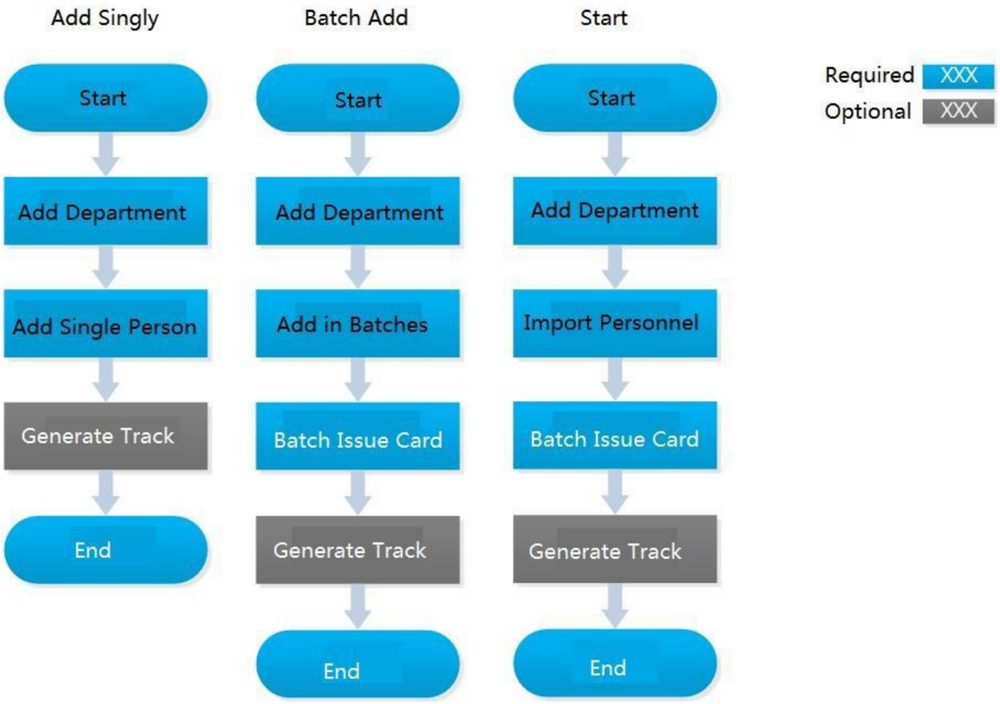

Daily Report 2019-05-14
Export
Exit/Entry People
Entry
Exit
Stay People
Stay People

Step 3 Click **Export** on upper right corner of interface, save report to local in pdf according to prompt on interface.

3.16 Personnel Management

Personnel refer to the people responsible for access control management. They have the authorization to unlock doors with password, fingerprint, card, or face recognition. Operation flow is shown in Figure 3-286.

Figure 3-286 Personnel management flow


Add Singly
Start
Add Department
Add Single Person
Generate Track
End
Batch Add
Start
Add Department
Add in Batches
Batch Issue Card
Generate Track
End
Start
Start
Add Department
Import Personnel
Batch Issue Card
Generate Track
End
Required XXX
Optional XXX

3.16.1 Adding Department

Adding department is to manage personnel in the added departments.

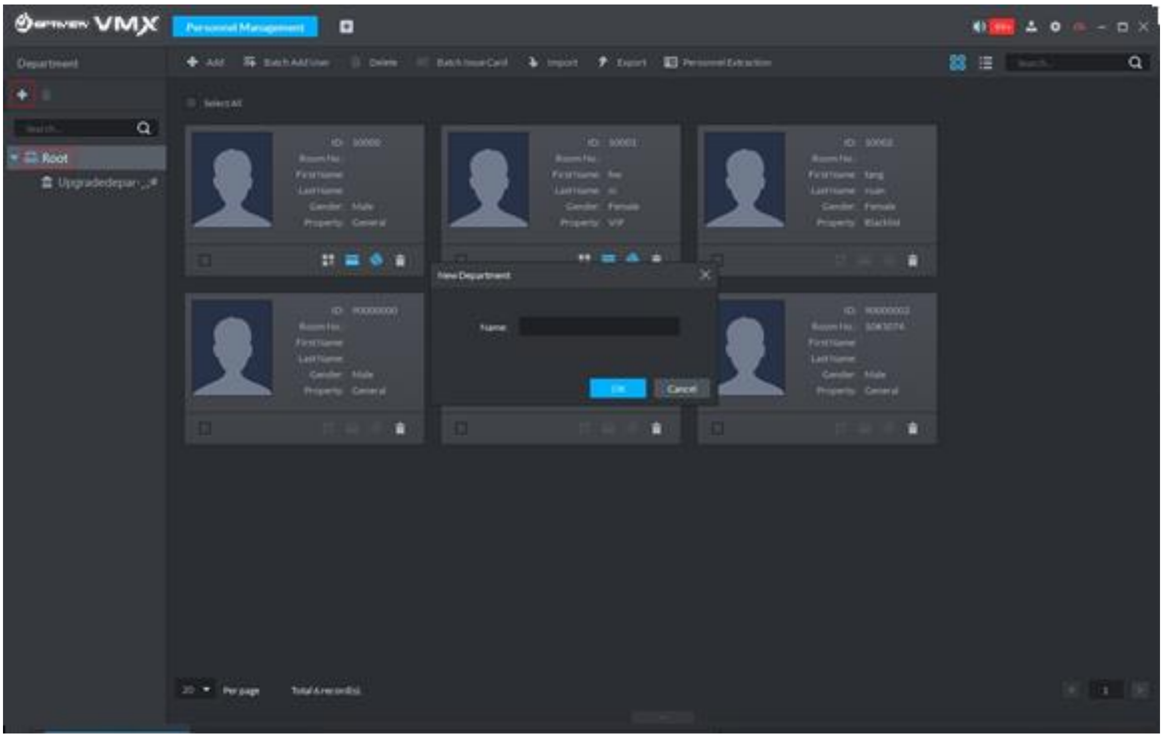
Step 1 Click . On the **Homepage** interface, select **Personnel Management**.

The **Personnel Management** interface is displayed.

Step 2 Select a node from the department list on the left side, and click **Add**.

The **New Department** interface is displayed. See Figure 3-287. The new department is directly under the selected node.

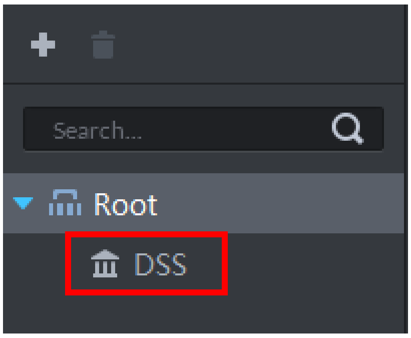
Figure 3-287 New department



Step 3 Input the department name and click **OK**.

The newly added department is displayed. See Figure 3-288.

Figure 3-288



You can delete or rename a newly added department.

- To delete a department, select it, click , and follow the instructions on the interface. You cannot delete a department with personnel.
- To rename a department, right-click it and select **Rename** to modify the name.

3.16.2 Adding Personnel

Add personnel and authorize them to unlock doors. When adding personnel, system uploads the collected personnel information to the server for proper protection.

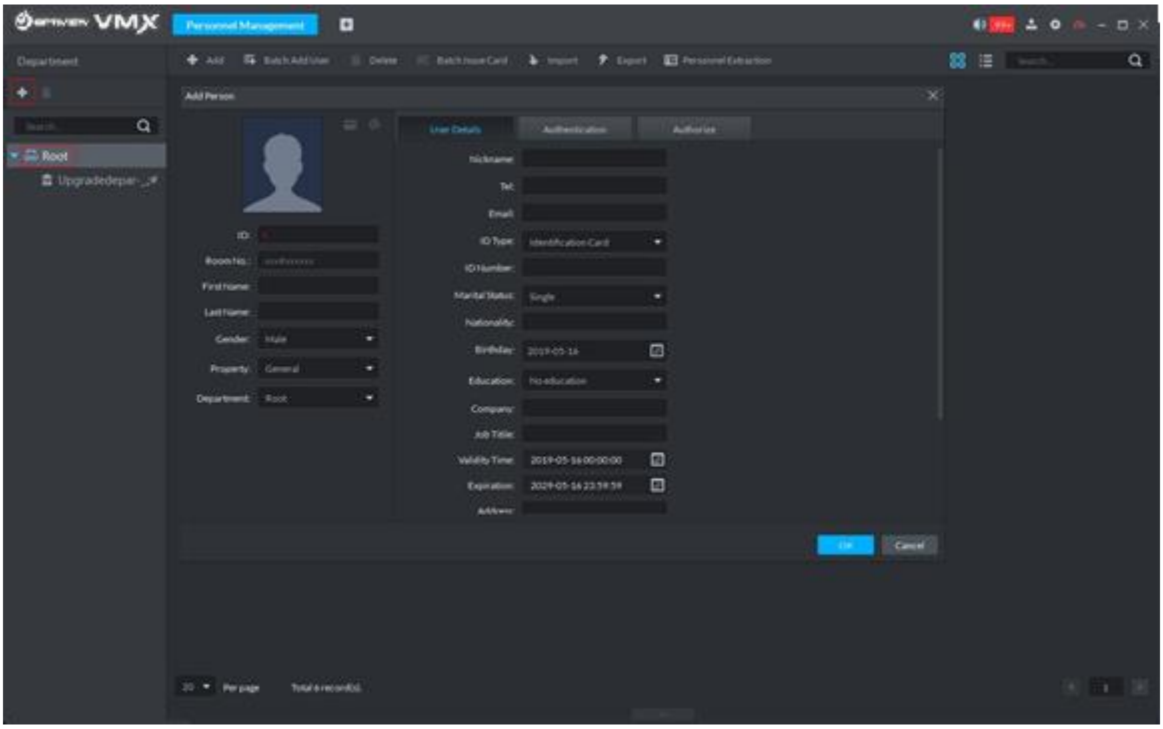
- The ID of added personnel should be in accordance with personnel ID of attendance device, otherwise, attendance data cannot be synchronized.
- If you want to read or import fingerprint or card from fingerprint collector, reader, please make sure fingerprint collector or reader is connected.
- IR face feature code needs to add personnel, enter edit status and read from IR face access control.

3.16.2.1 Adding Person Singly

Step 1 On the **Personnel Management** interface, click **Add**.

The **Add Person** interface is displayed. See Figure 3-289.

Figure 3-289 Add personnel


VMX
Personnel Management
Department
Root
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Personnel Extraction
Add Person
User Details
Authentication
Authorize
OK
Cancel
Per page

ID:
Room No.:
First Name:
Last Name:
Gender: Male
Property: General
Department: Root
Nickname:
Tel:
Email:
ID Type: Identification Card
ID Number:
Marital Status: Single
Nationality:
Birthday: 2019-05-16
Education: No education
Company:
Job Title:
Validity Time: 2019-05-16 00:00:00
Expiration: 2029-05-16 23:59:59
Address:

Step 2 Configure personnel details.

1) Move the mouse to the picture section, click **Upload**. Follow the instructions on the interface to upload a picture. If the PC comes with a camera, click **Snapshot** to take a face snapshot and upload it.
2) Fill in personnel information as necessary. For parameter details, see Table 3-49.

Table 3-49 Personnel detail description

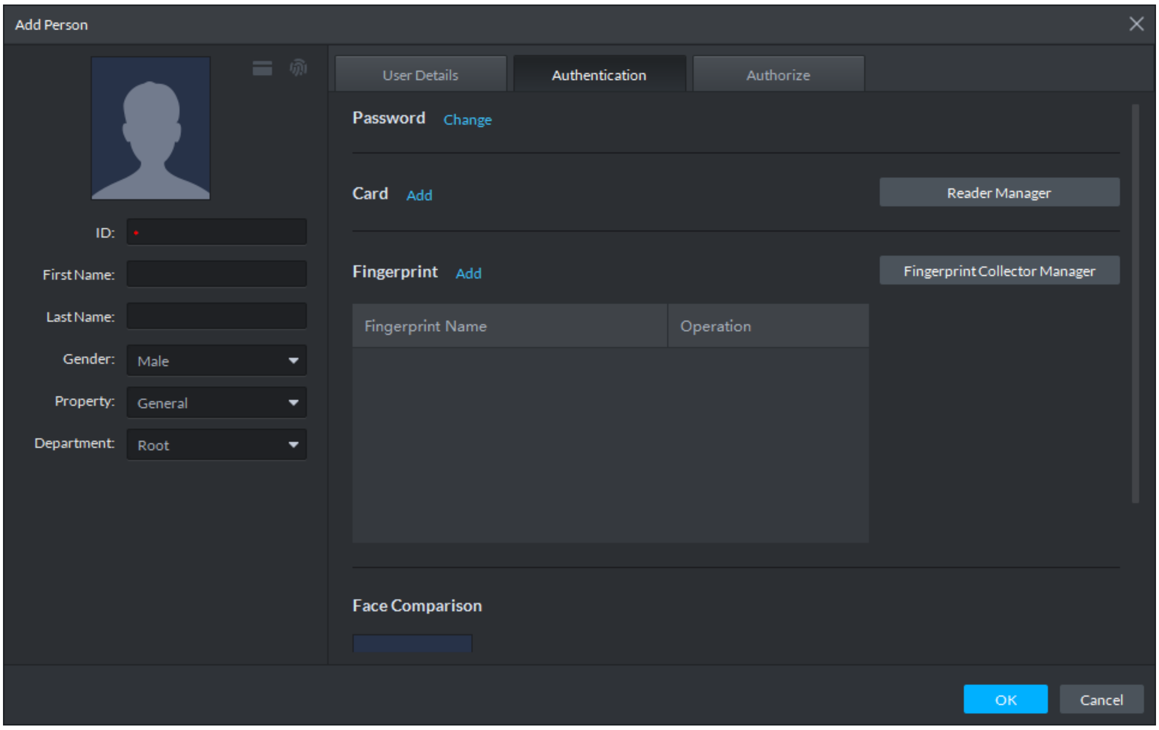
Parameter	Description
ID	Required, used to recognize personnel, each ID number is unique.

Parameter	Description
Property	Set person as different types. 📖 If the person is the first card unlock, then person property is set as **General**.
Householder	If the added personnel belong to the same household, then you can set one person as householder, you can issue contacts and householder info under video intercom.
Admin	Personnel divided into general and admin. Admin has the permission to operate device interface. The parameter takes effect only when personnel info issued to 2nd generation access control.

Step 3 Click the **Authentication** tab.

The **Authentication** interface is displayed. See Figure 3-290.

Figure 3-290 Authentication

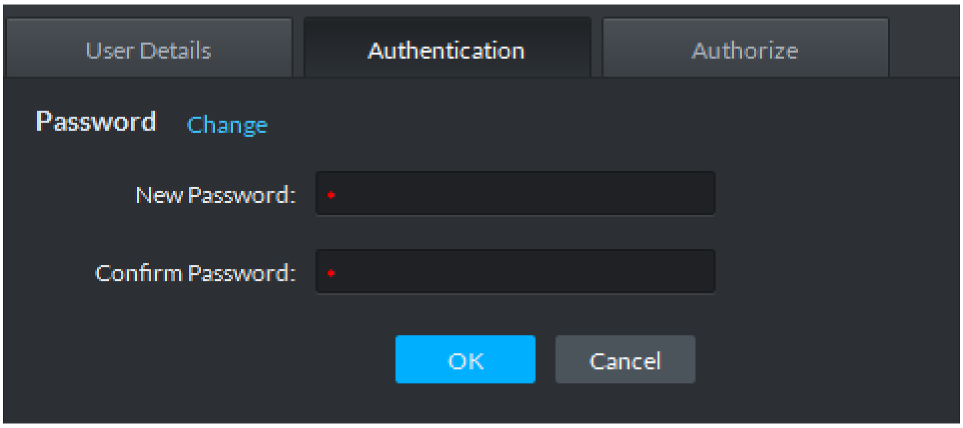

Add Person
User Details
Authentication
Authorize
Password
Change
Card
Add
Reader Manager
Fingerprint
Add
Fingerprint Collector Manager
Fingerprint Name
Operation
Face Comparison
ID:
First Name:
Last Name:
Gender:
Male
Property:
General
Department:
Root
OK
Cancel

Step 4 Set a password.

1) Click **Change**.

The system displays password setting. See Figure 3-291.

Figure 3-291 Set password


User Details
Authentication
Authorize
Password
Change
New Password:
Confirm Password:
OK
Cancel

2) Enter a password, and click **OK** to save the password settings.

Step 5 Issue cards to personnel.

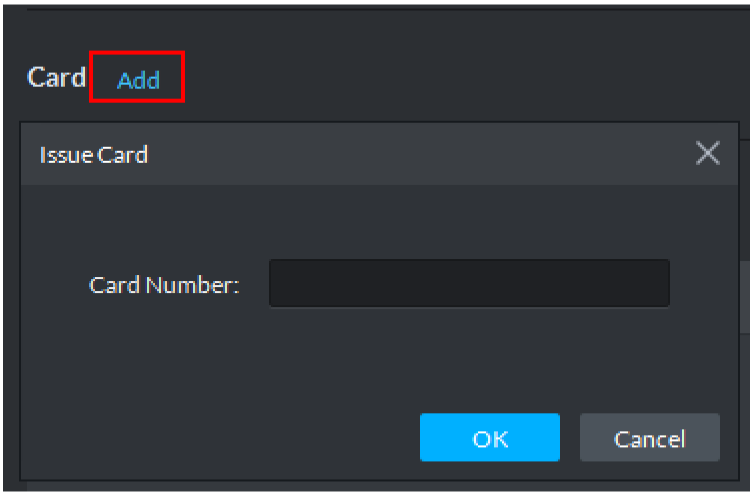
The system supports issuing card by entering card No. manully and card reader.

- Issue card by entering card No. manully

1) Click **Add** next to **Card**.

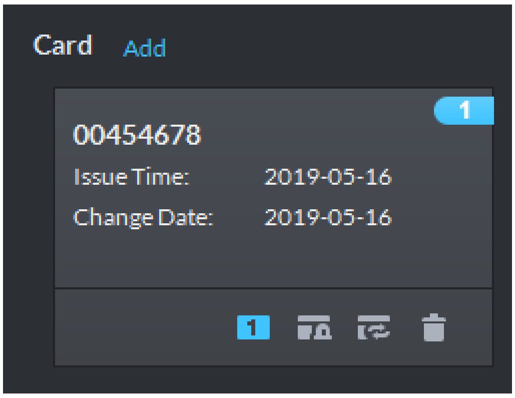
The **Issue Card** interface is displayed. See Figure 3-292.

Figure 3-292 Add card



2) Enter personnel card number and click **OK** to save the card added. See Figure 3-293. For more details, refer to Table 3-50.

Figure 3-293 Card added



00454678

Issue Time: 2019-05-16

Change Date: 2019-05-16

Table 3-50 Card operation

Icon	Description
1	If a person has several cards, only the main card can be issued to 1st generation access control device. The first added card is considered as main card by default. Click the icon and it becomes 1, and then 1 is displayed on upper right corner of the interface, which means that the card is set as main card. Click 1 to cancel main card setting.

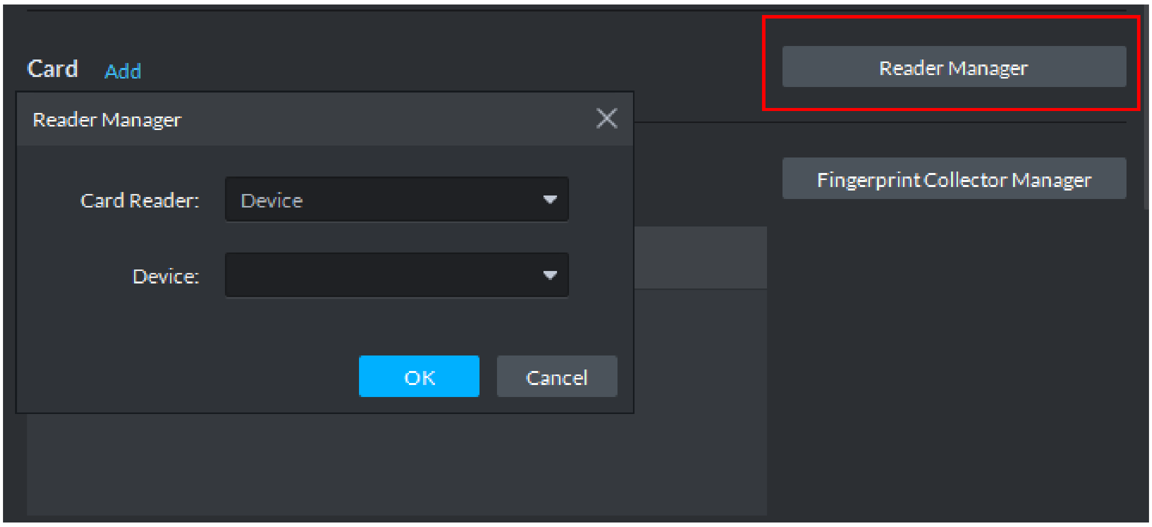
Icon	Description
	Set the card as duress card, after that use the card to unlock, then duress alarm is generated. After clicking the icon, it becomes , is displayed on upper right corner of the interface, which means that the card is set as duress card. Click to cancel duress card setting.
	Card cannot be used if it is damaged, so you can change a new card.
	Delete card info, after that the card has no unlock permission.

- Issue card by card reader.

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 3-294.

Figure 3-294 Reader manager



Card Reader: Device

Device:

2) Select from **Card Reader** or **Device**, and click **OK**.

3) Swipe the card on the card reader or device.

Complete issuing cards.

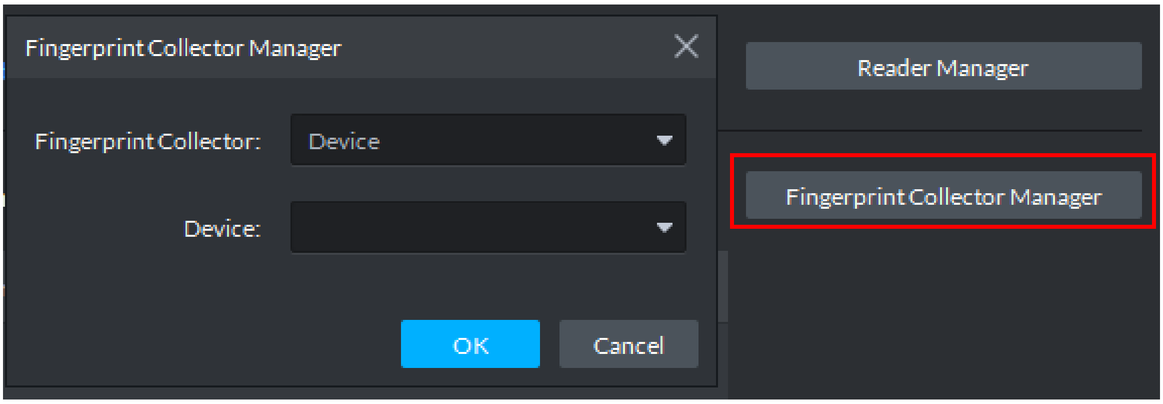
Step 6 Collect fingerprint.

When the system is connected to access control, unlocks by fingerprint, you need to collect personnel fingerprint. Each person can collect max 10 fingerprints.

1) Click **Fingerprint Collector Manager**.

The **Fingerprint Collector Manager** interface is displayed. See Figure 3-295.

Figure 3-295 Fingerprint collector manager

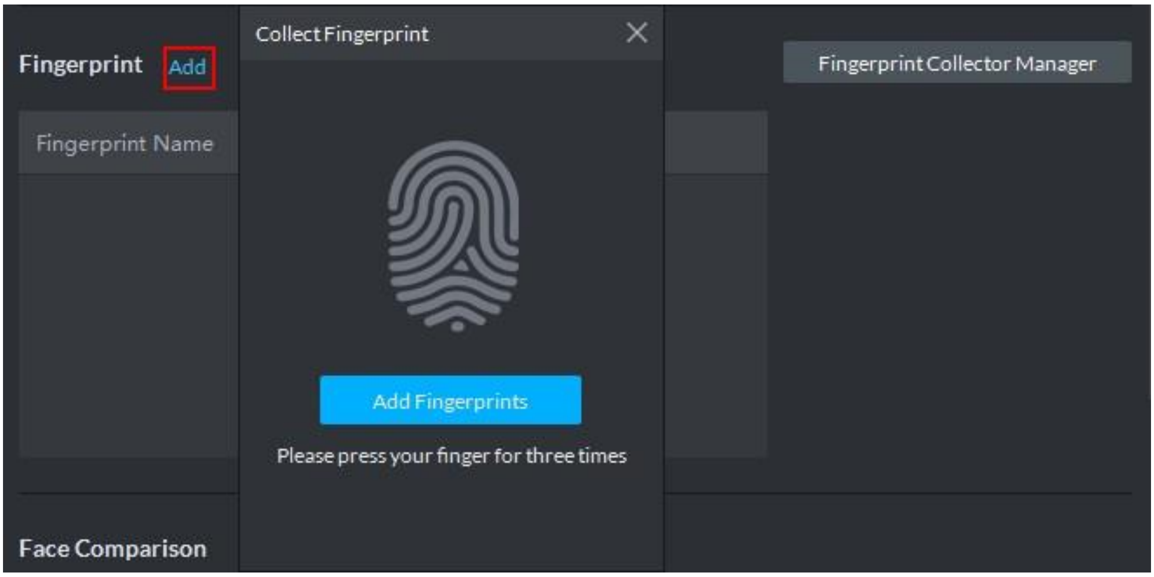

Fingerprint Collector Manager
Fingerprint Collector:
Device
Device:
OK
Cancel
Reader Manager
Fingerprint Collector Manager

2) Select from **Fingerprint Collector** and click **OK**.

3) Click **Add**.

The **Collect Fingerprint** interface is displayed. See Figure 3-296.

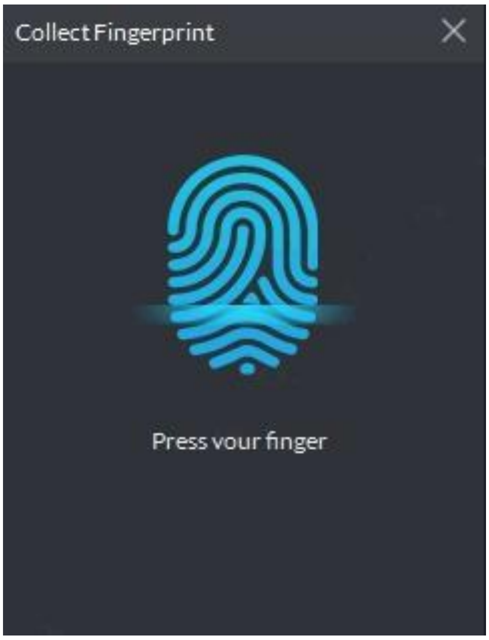
Figure 3-296 Collect fingerprint


Fingerprint
Add
Fingerprint Name
Face Comparison
Collect Fingerprint
Add Fingerprints
Please press your finger for three times
Fingerprint Collector Manager

4) Click **Add Fingerprints**.

The **Collect Fingerprint** interface is displayed. See Figure 3-297.

Figure 3-297 Collect fingerprint


Collect Fingerprint
Press your finger

5) Records fingerprint on the reader by raising and then laying down the finger upon hearing the beep sound. Repeat this for three times. See Figure 3-298. Fingerprint collection is completed, see Figure 3-299. For more details, see Table 3-51.

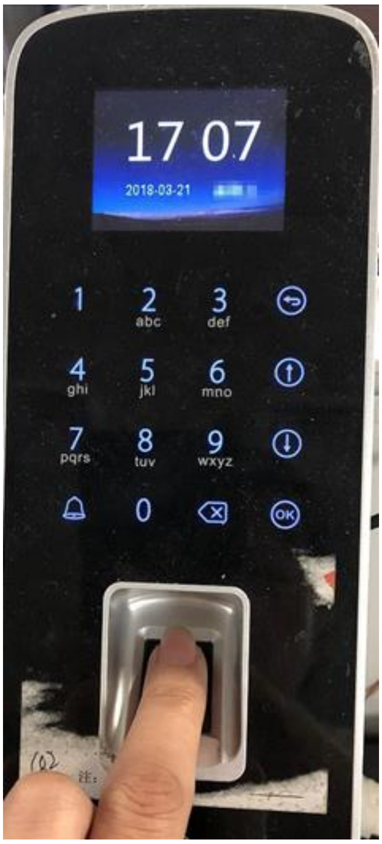
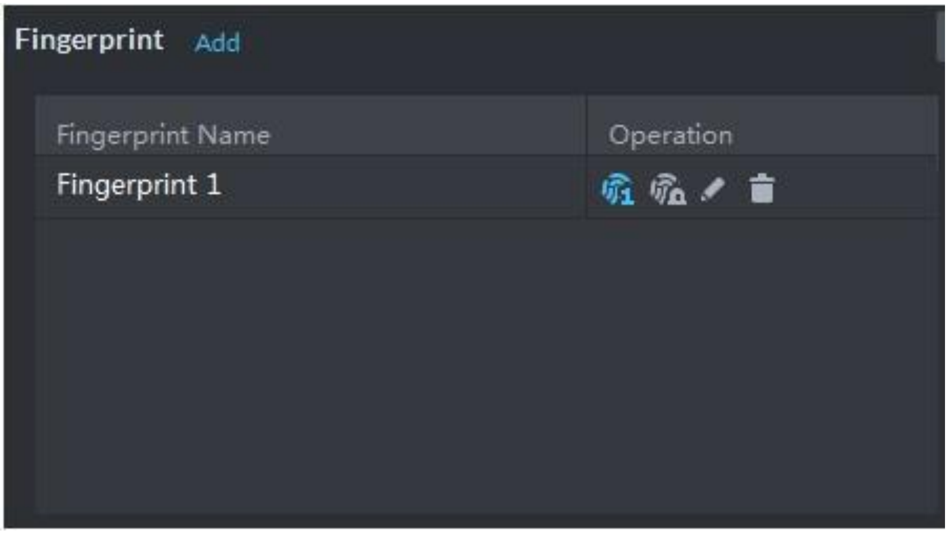

17 07
2018-03-21
1
2 abc
3 def
4 ghi
5 jkl
6 mno
7 pqrs
8 tuv
9 wxyz
0
OK

Figure 3-298 Collecting fingerprint

Figure 3-299 Fingerprint collection completed



Fingerprint Add

Fingerprint Name	Operation
Fingerprint 1	

Table 3-51 Fingerprint operation

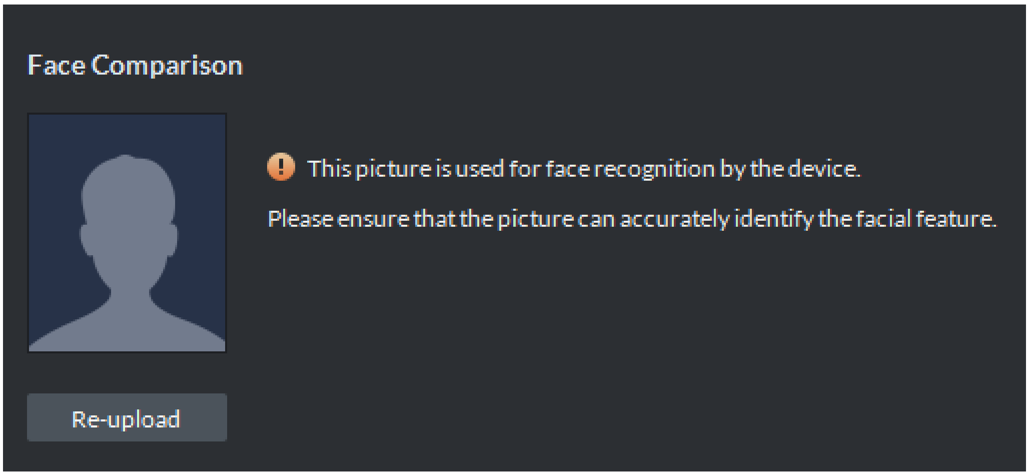
Icon	Description
	If more than 3 fingerprints are imported, then only then main fingerprint can be issued to access control device. The latest three fingerprints are considered as main fingerprint by default. One person cam set max three main fingerprints. After clicking the icon, it becomes , which means that the fingerprint is set as main fingerprint. Click and cancel main fingerprint setting.
	Set fingerprint as duress fingerprint, after that you can unlock the door by the fingerprint and generate duress alarm. Click the icon, it becomes , which means the fingerprint is set as duress fingerprint. Click and cancel duress fingerprint setting.
✎	Modify fingerprint name.
🗑	Delete fingerprint, after that the fingerprint has no permission to unlock door.

Step 7 Upload pictures for face recognition.

Click Add, and select picture to upload according to system prompt. See Figure 3-300.

- If the picture is wrong, or need to be replaced. Click Re-upload and upload new picture.
- Move the mouse to uploaded picture, 🗑 shows up on the picture, click the icon and delete the uploaded picture.

Figure 3-300 Face picture upload



Face Comparison

This picture is used for face recognition by the device.

Please ensure that the picture can accurately identify the facial feature.

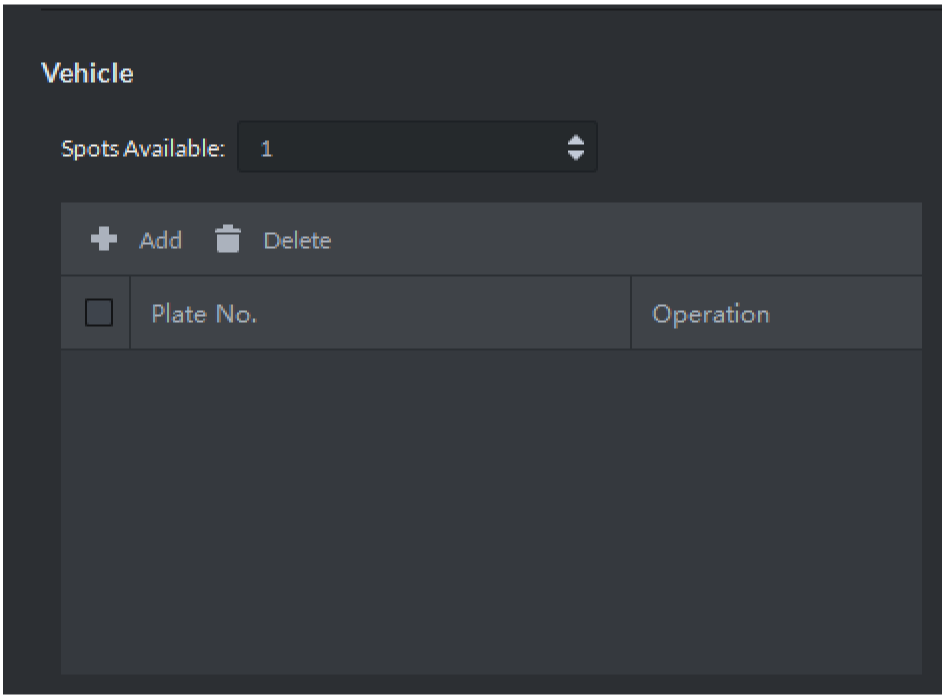
Step 8 Add vehicle info.

Added vehicle info is synced to entrance module, used as recognition info for vehicle entrance and exit.

Set the available spots for personnel, click **Add**, set plate No. and see Figure 3-301. If the person has several cars, then you need to add vehicle plate No. one by one.

If the number of added vehicles is more than available spots, then the number of entered vehicles cannot exceed the number of available spots which has been set.

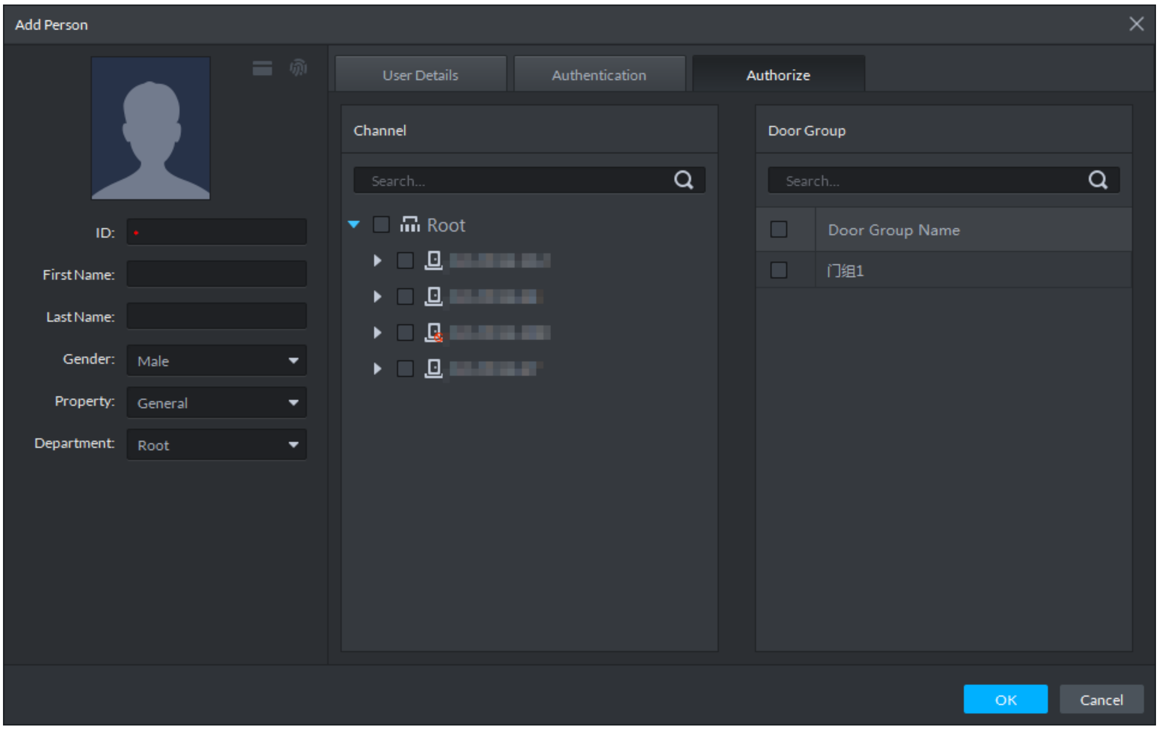
Figure 3-301 Add vehicle info


Vehicle
Add
Delete
Plate No.
Operation

Spots Available: 1

Step 9 Click **Authorize** and select the channels to which the authorized users can have access. See Figure 3-302.

Figure 3-302 Authorize


Add Person
User Details
Authentication
Authorize
Channel
Search...
Root
Door Group
Search...
Door Group Name
门组1
OK
Cancel

ID:
First Name:
Last Name:
Gender: Male
Property: General
Department: Root

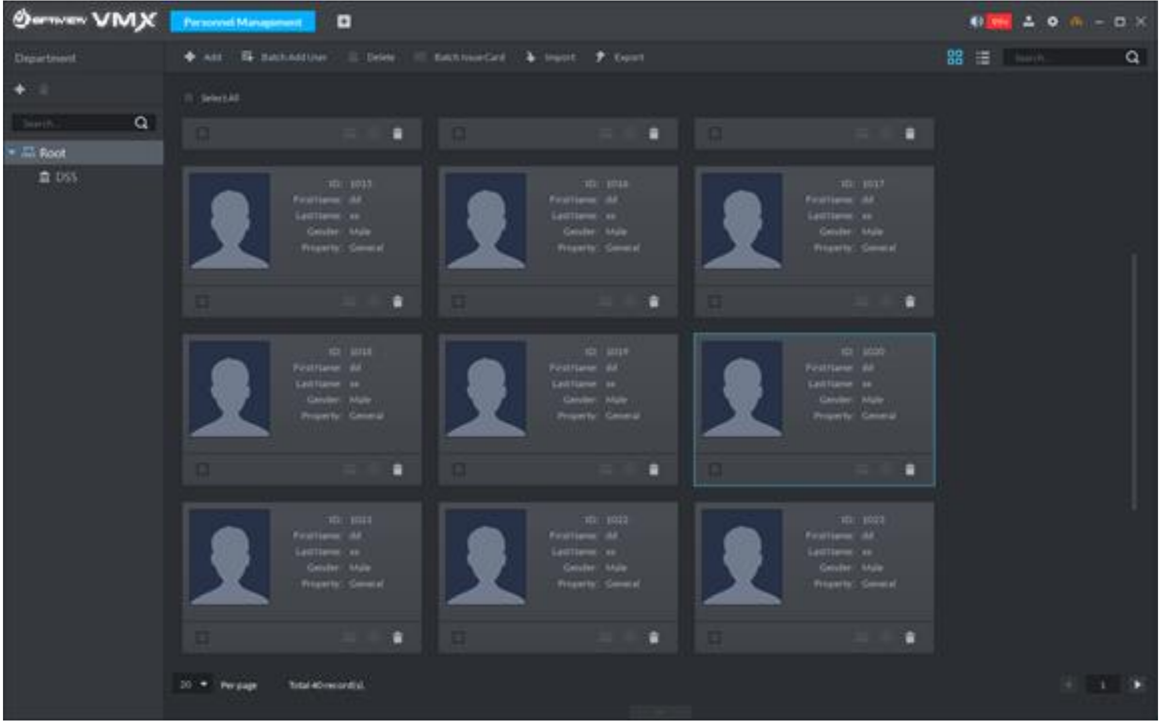
Step 10 Click **OK**.

For the information of the added personnel, see Figure 3-303. If there are authorized fingerprint and card, the corresponding icon displays in blue.

- Double-click personnel information, or select a person and click ^ to go to the interface for editing personnel information. The system supports modifying personnel information.

- Select a person, click **Delete**, and follow the instructions on the interface to delete the selected personnel. Click **Select All** to quickly delete all personnel on the current page.

Figure 3-303 Personnel list


VMX
Personnel Management
Department
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Select All
Root
DSS
Per page
Total 40 record(s).

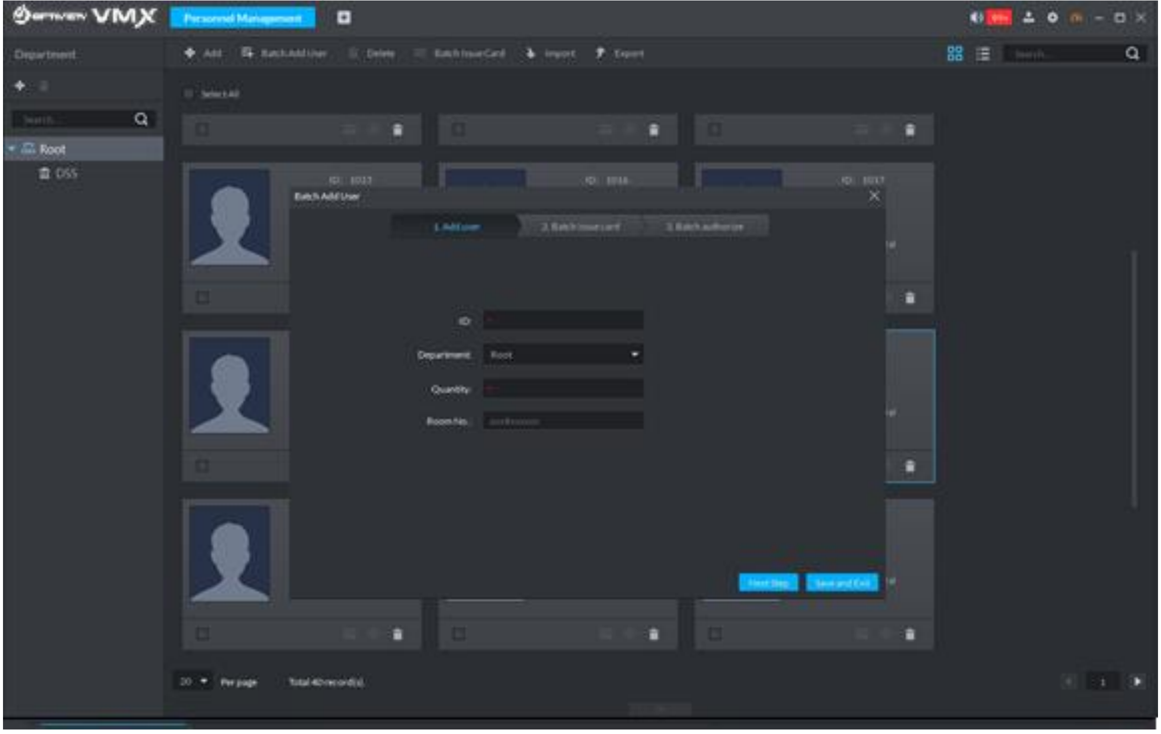
3.16.2.2 Batch Add

If multiple persons are added in one time, you can authorize them by issuing cards only. You cannot authorize password and fingerprint. If necessary, you can edit personnel authorization separately.

Step 1 On the Personnel Management interface, click Batch Add User.

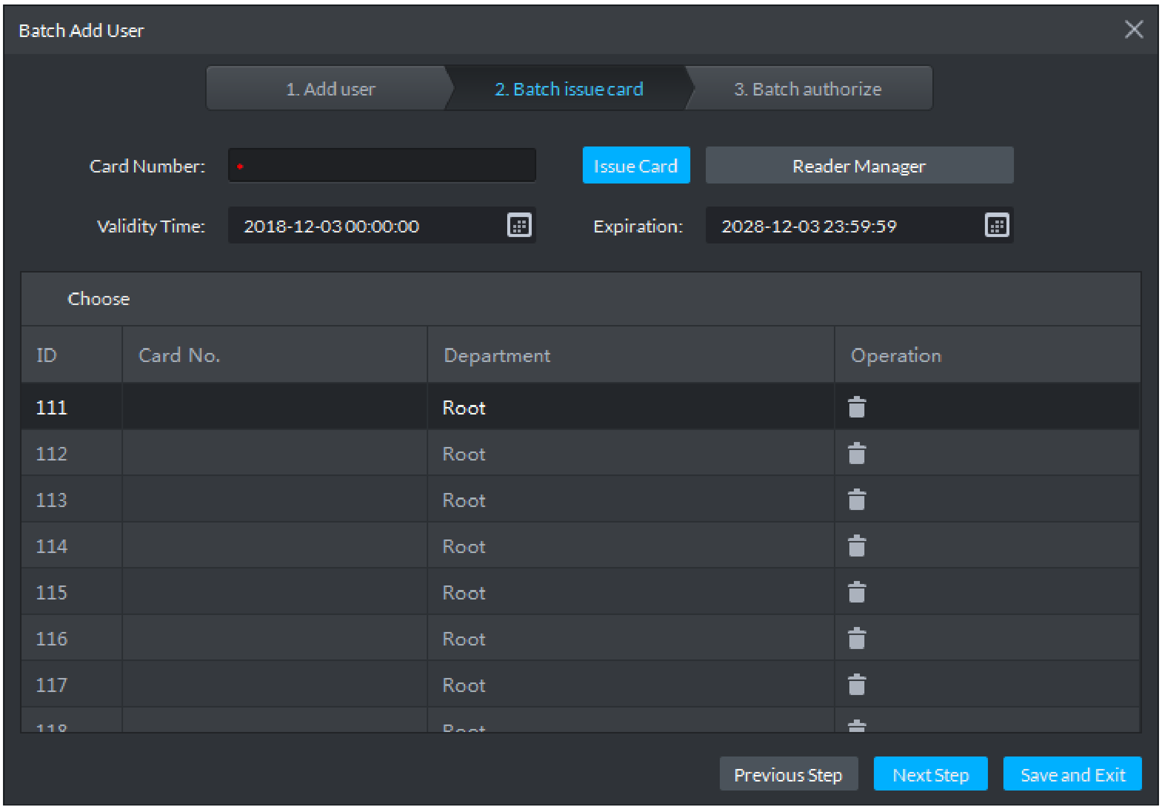
The **Batch Add User** interface is displayed. See Figure 3-304.

Figure 3-304 Batch add user


VMX
Personnel Management
Department
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Root
DSS
Select All
Batch Add User
1. Add user
2. Batch issue card
3. Batch authorize
ID:
Department:
Root
Quantity:
Room No.:
Next Step
Save and Exit
Per page
Total 40 record(s)

Step 2 Enter the starting ID and user quantity, select their departments, and click **Next Step**. The **Batch issue card** interface is displayed. See Figure 3-305.

Figure 3-305 Add batch info


Batch Add User
1. Add user
2. Batch issue card
3. Batch authorize
Issue Card
Reader Manager
Choose
Previous Step
Next Step
Save and Exit

Card Number:

Validity Time: 2018-12-03 00:00:00

Expiration: 2028-12-03 23:59:59

ID	Card No.	Department	Operation
111		Root	🗑
112		Root	🗑
113		Root	🗑
114		Root	🗑
115		Root	🗑
116		Root	🗑
117		Root	🗑

Step 3 Issue cards to personnel.

The device supports issuing card by entering card No. manually and card reader.

- Issue card by entering card No. manually

1) Select a person, input the card number, and set up the validity time and expiry

time.

2) Click **Issue Card**.

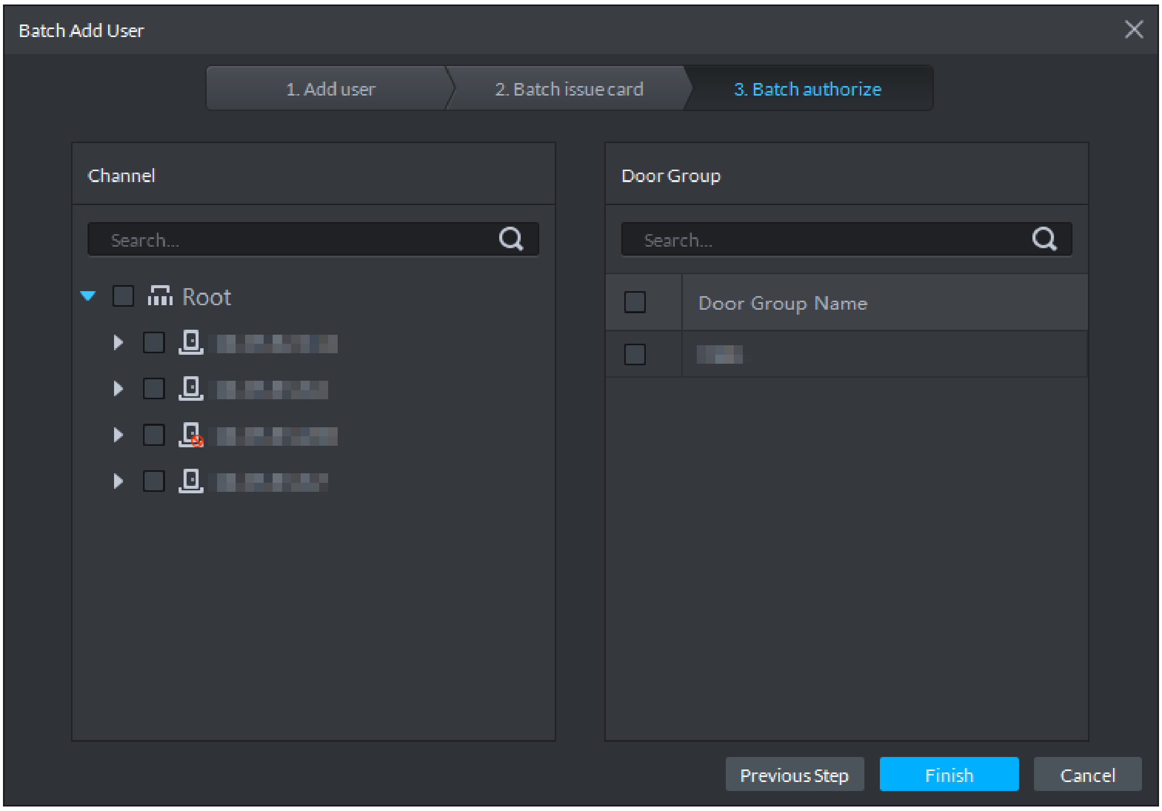
Complete issuing card to the selected personnel and the interface shows the personnel card number.

3) Repeat the steps until all personnel get their cards.

4) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 3-306.

Figure 3-306 Batch authorize

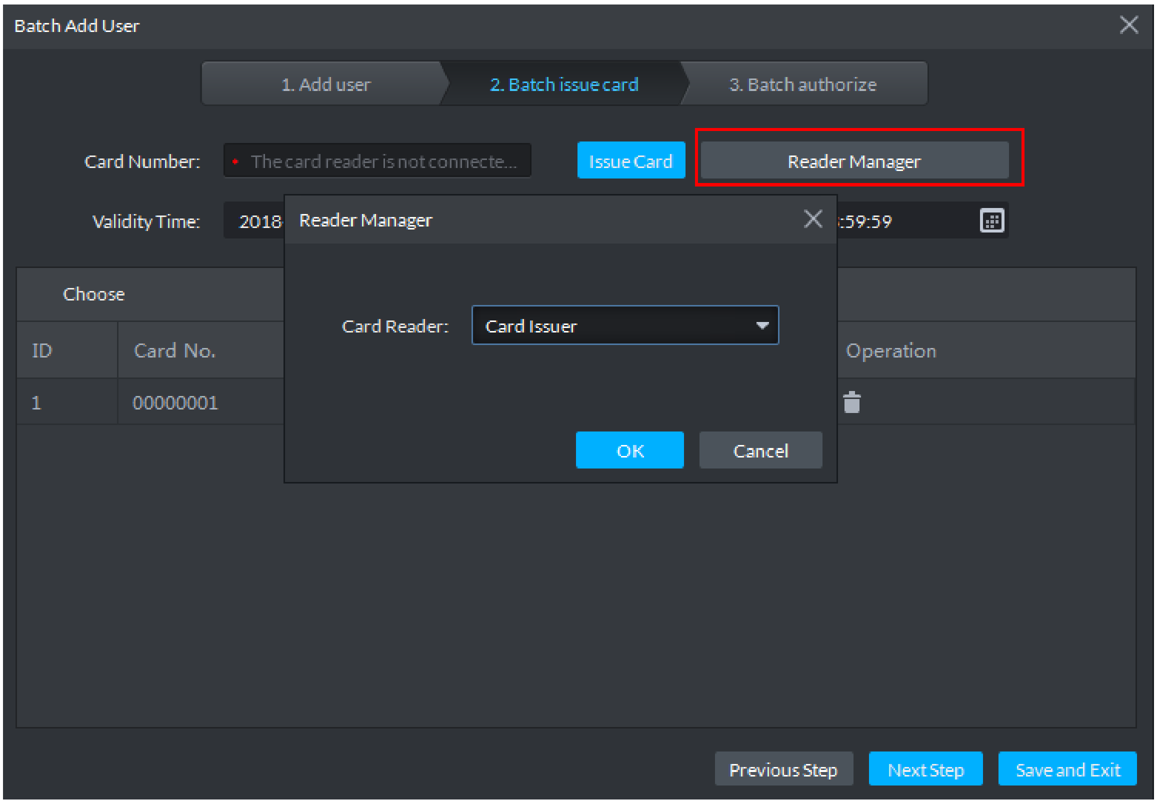

Batch Add User
1. Add user
2. Batch issue card
3. Batch authorize
Channel
Search...
Root
Door Group
Search...
Door Group Name
Previous Step
Finish
Cancel

- Issue card by card reader

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 3-307.

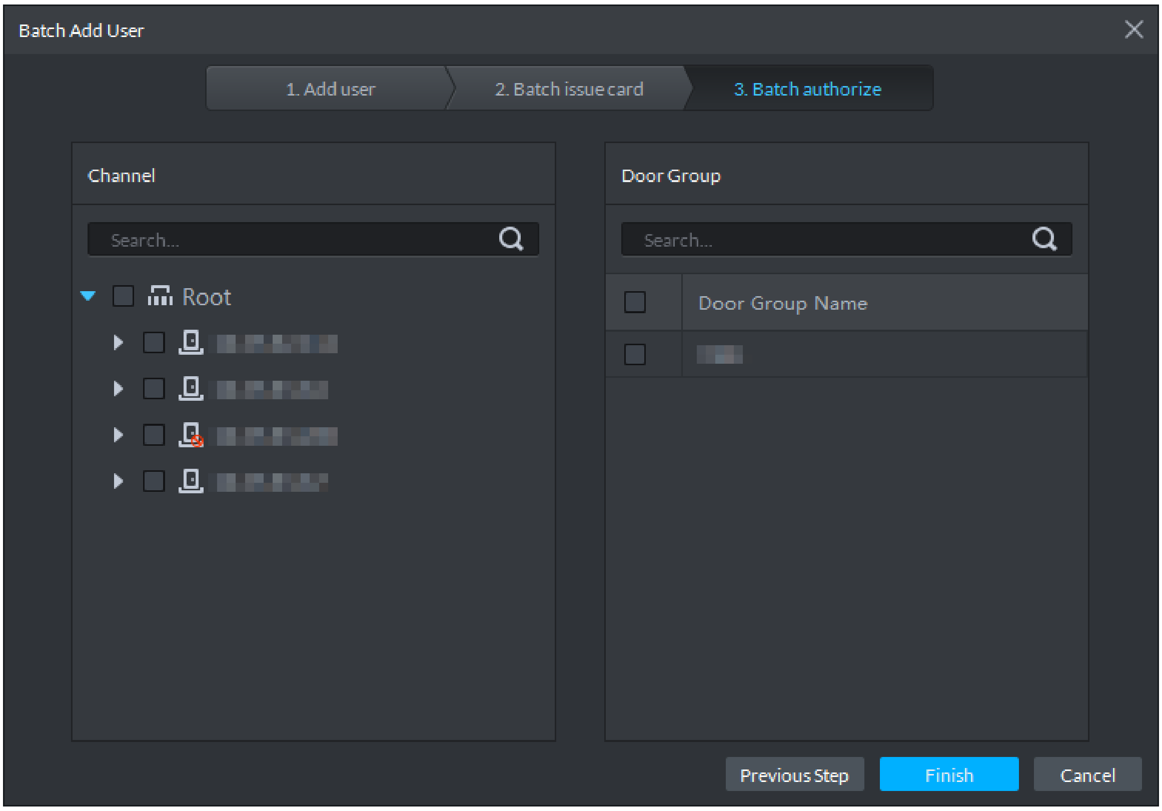
Figure 3-307 Reader manager


Batch Add User
1. Add user
2. Batch issue card
3. Batch authorize
Card Number:
The card reader is not connecte...
Issue Card
Reader Manager
Validity Time:
2018
:59:59
Reader Manager
Card Reader:
Card Issuer
OK
Cancel
Choose
ID
Card No.
Operation
1
00000001
Previous Step
Next Step
Save and Exit

2) Select from **Card Reader** or **Device**, and click **OK**.
3) Swipe the card on the card reader or device.
4) Select a person, set up the validity time and expiry time, and click **Issue Card**.
5) Repeat the steps until all personnel get their cards.
6) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 3-308.

Figure 3-308 Batch authorize

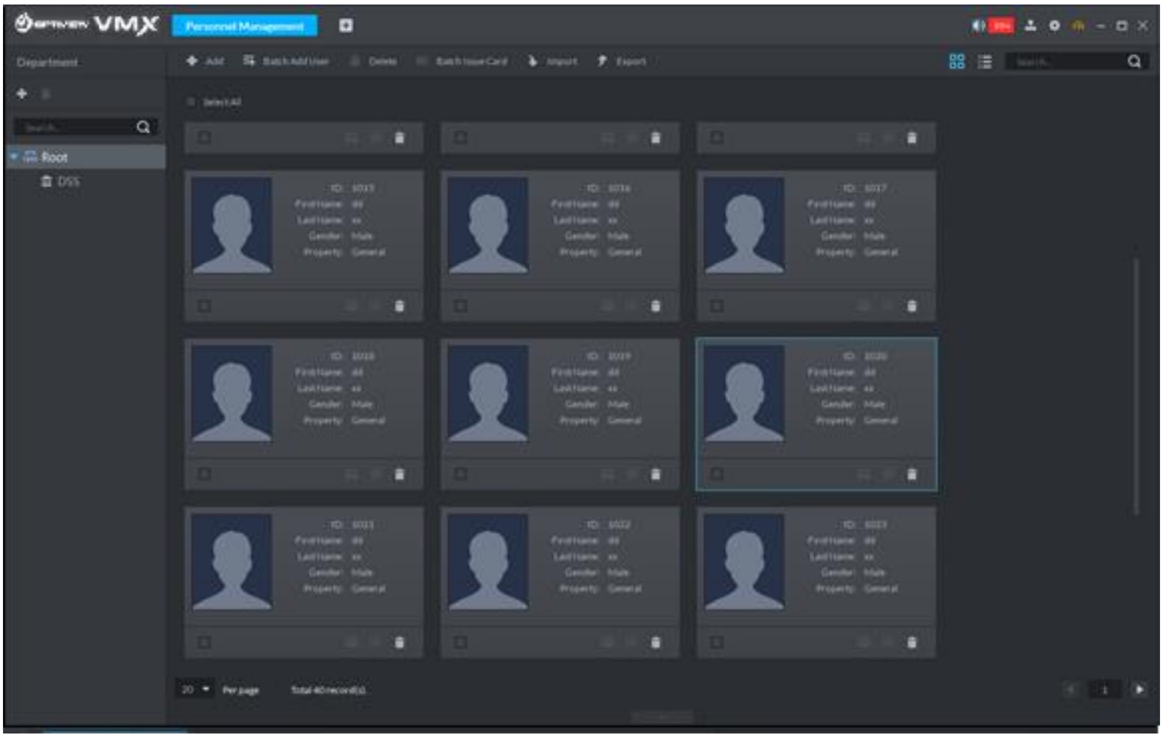

Batch Add User
1. Add user
2. Batch issue card
3. Batch authorize
Channel
Search...
Root
Door Group
Search...
Door Group Name
Previous Step
Finish
Cancel

Step 4 Select the access control channels or door groups to which the personnel have access, and click **Finish**.

The interface displays info of added personnel. See Figure 3-309.

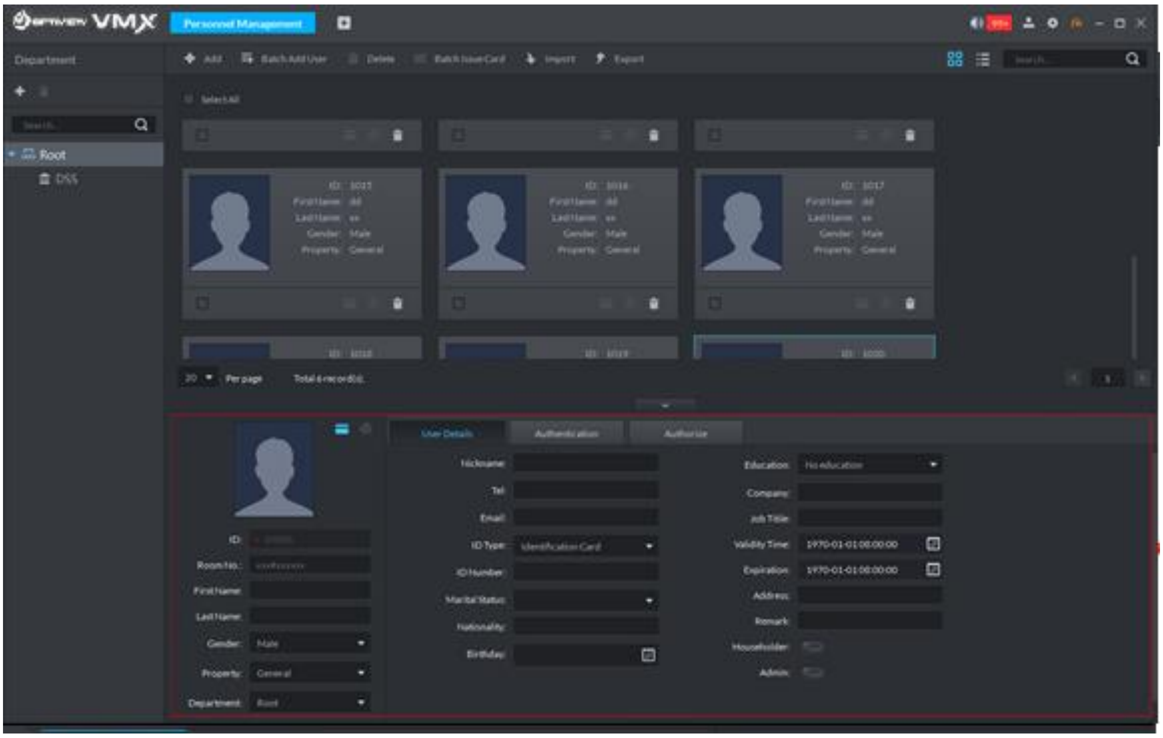
Door group is introduced in access control, for more details, see Access Control.

Figure 3-309 Batch add user


VMX
Personnel Management
Department
Root
DSS
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Select All
Per page

Step 5 Double-click a person, or select a person and click to go to the screen for editing personnel information, where you can modify the personnel information. See Figure 3-310. Modification takes effect immediately.

Figure 3-310 Edit personnel


VMX
Personnel Management
Department
Root
DSS
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Select All
Per page
User Details
Authentication
Authorize
Nickname
Tel
Email
ID Type
Identification Card
ID Number
Marital Status
Nationality
Birthday
Education
No education
Company
Job Title
Validity Time
Expiration
Address
Remark
Householder
Admin
ID
Room No.
First Name
Last Name
Gender
Male
Property
General
Department
Root

3.16.3 Editing Personnel

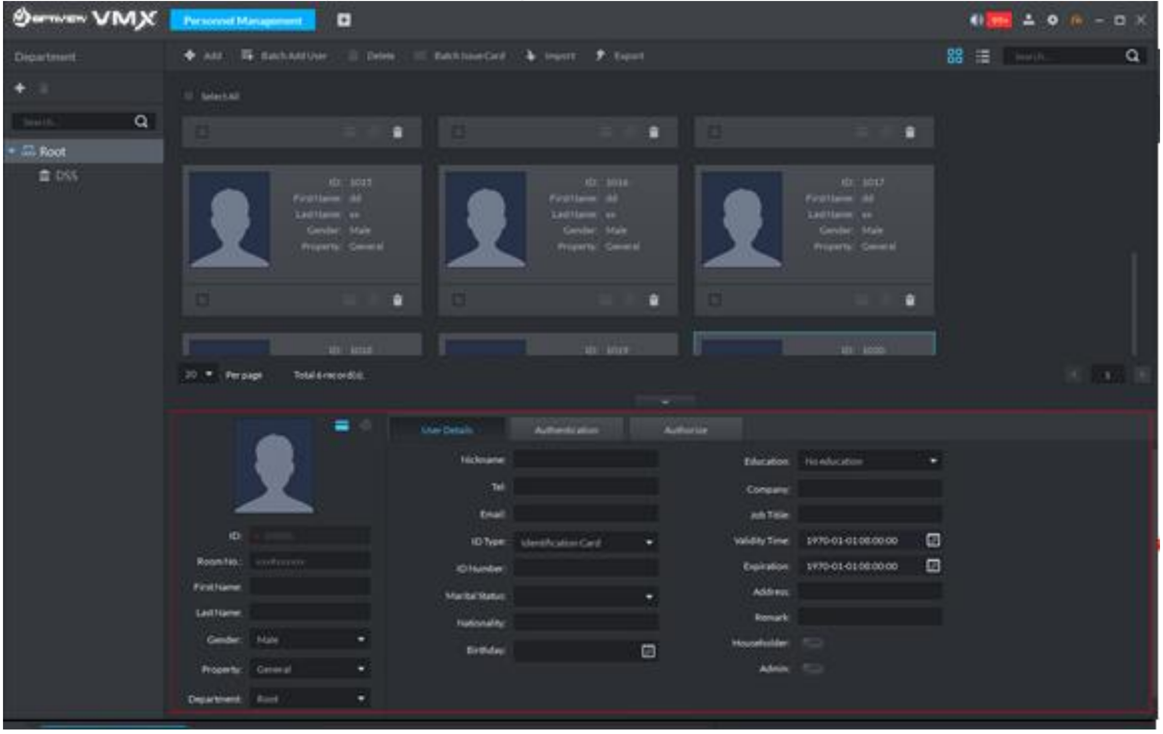
You can modify information of added person like user details, authentication and authorize except ID.

- If system adopts IR face attendance, you have to edit personnel and extract face feature code of person with same ID from IR face attendance device.
- If you want to read or import fingerprint, card or face feature from fingerprint collector, reader or IR face access control, please make sure the device is connected.

Step 1 On **Personnel Management** interface, double-click person, or select the person and click .

The interface of **Editing Personnel Info** is displayed. See Figure 3-311.

Figure 3-311 Edit personnel


VMX
Personnel Management
Department
Root
DSS
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Select All
Per page
User Details
Authentication
Authorize
Nickname
Tel
Email
ID Type
ID Number
Marital Status
Nationality
Birthday
Education
Company
Job Title
Validity Time
Expiration
Address
Remark
Householder
Admin
ID
Room No.
First Name
Last Name
Gender
Property
Department

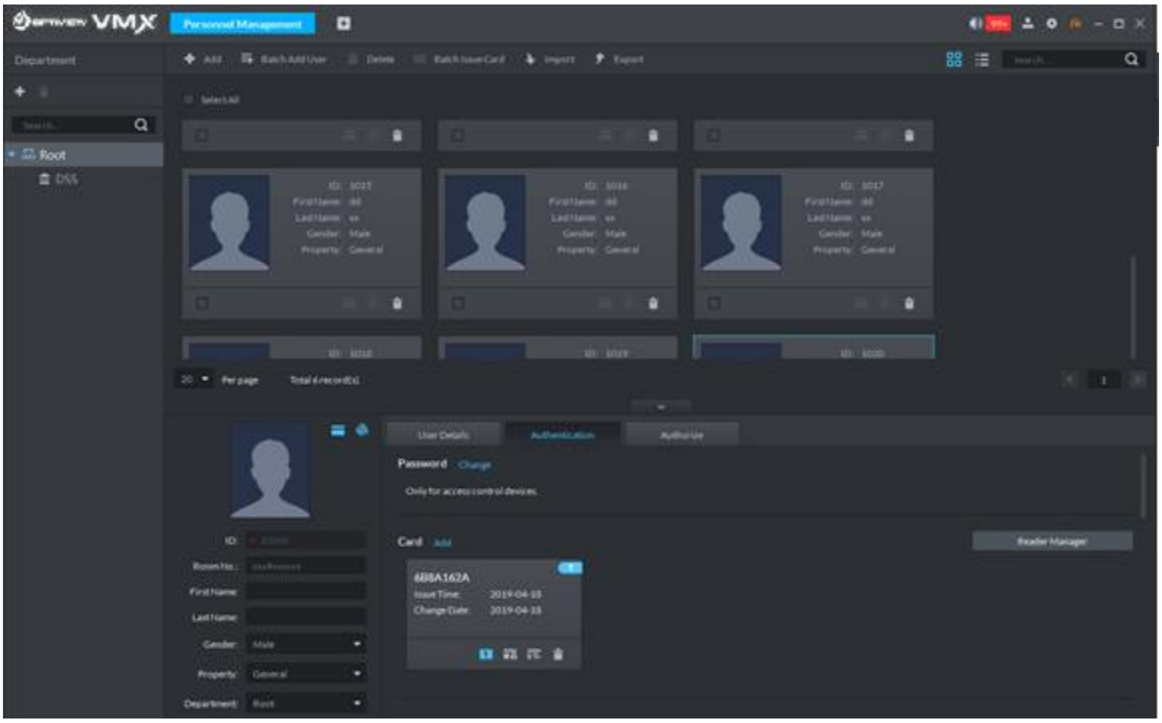
Step 2 Modify personnel info and details except ID.

If the person is the first card unlock, then you need to set person property as **General**.

Step 3 Click Authentication tab.

The system displays **Authentication** interface, see Figure 3-312.

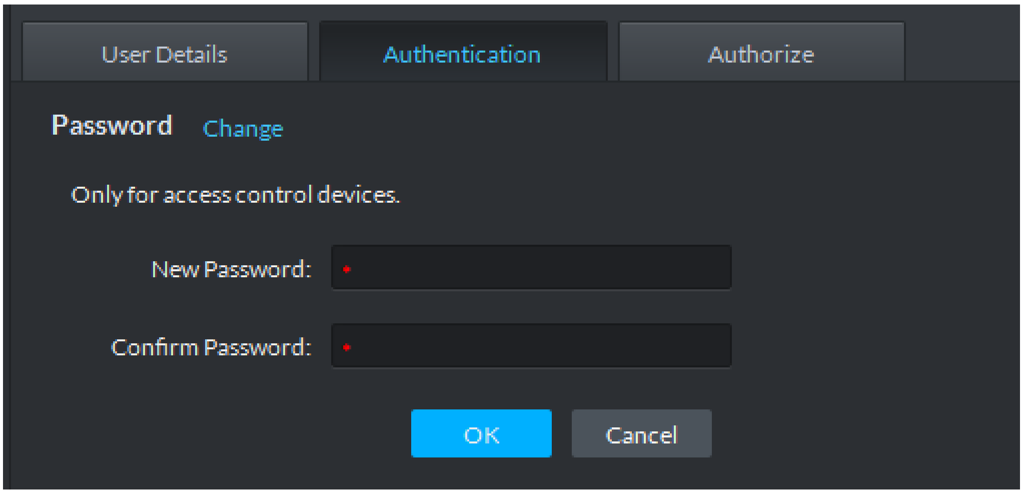
Figure 3-312 Authentication


VMX
Personnel Management
Department
Root
DSS
User Details
Authentication
Authorize
Password
Change
Only for access control devices.
Card
Add
Reader Manager
6B8A162A
Issue Time
Change Date

Step 4 Click **Change**, you can set new password according to prompt, click **OK**. See Figure 3-313.

When the system is connected to access control, use password to unlock door, you need to set password.

Figure 3-313 Set password

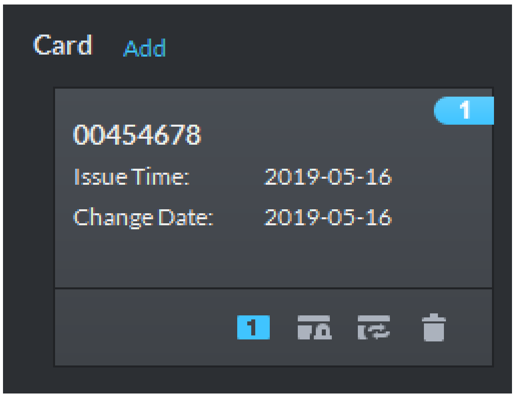


Only for access control devices.

Step 5 Manage card info.

After door card is added, and you can modify card. For more details, see Figure 3-314 and Table 3-52.

Figure 3-314 Add card



00454678

Issue Time: 2019-05-16

Change Date: 2019-05-16

Table 3-52 Card operation

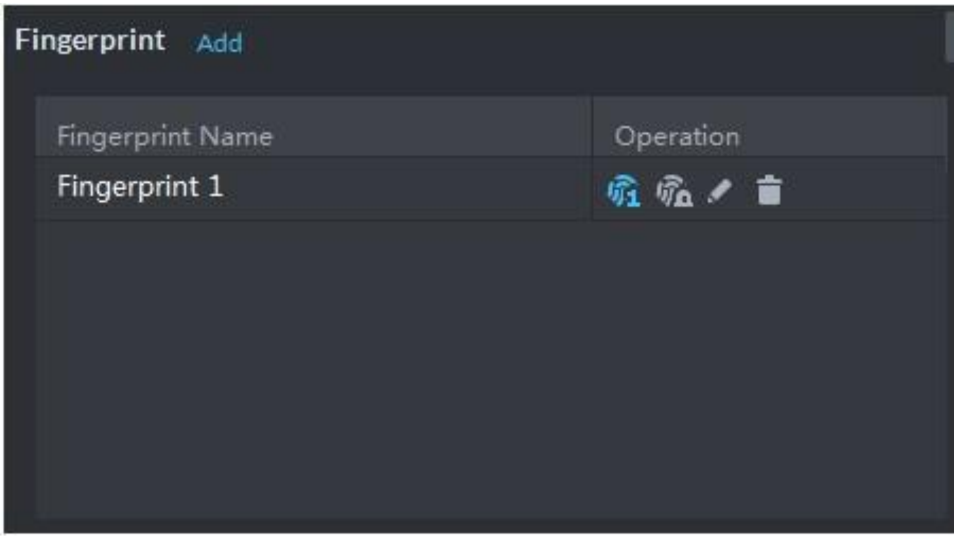
Icon	Description
1	If a person has several cards, only the main card can be issued to 1st generation access control device. The first added card is considered as main card by default. Click the icon and it becomes 1, and then 1 is displayed on upper right corner of the interface, which means that the card is set as main card. Click 1 to cancel main card setting.
▣	Set the card as duress card, after that use the card to unlock, then duress alarm is generated. After clicking the icon, it becomes ▣, ▣ is displayed on upper right corner of the interface, which means that the card is set as duress card. Click ▣ to cancel duress card setting.
⇄	Card cannot be used if it is damaged, so you can change a new card.

Icon	Description
🗑	Delete card info, after that the card has no unlock permission.

Step 6 Manage fingerprint.

Personnel fingerprint is collected, and you can modify status and name. For more details, see Figure 3-315.

Figure 3-315 Fingerprint collected



Fingerprint Add

Fingerprint Name	Operation
Fingerprint 1	✎ 🗑

Table 3-53 Fingerprint operation

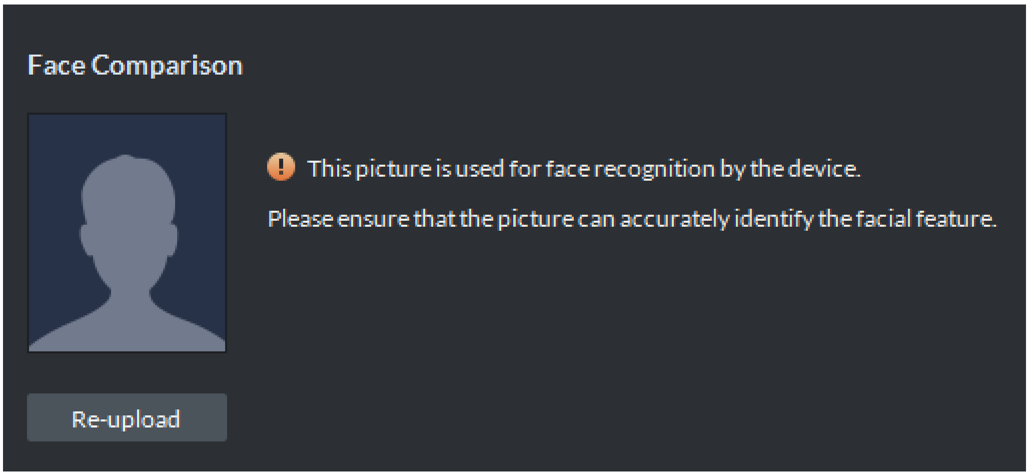
Icon	Description
	If more than 3 fingerprints are imported, then only then main fingerprint can be issued to access control device. The latest three fingerprints are considered as main fingerprint by default. One person can set max three main fingerprints. After clicking the icon, it becomes , which means that the fingerprint is set as main fingerprint. Click and cancel main fingerprint setting.
	Set fingerprint as duress fingerprint, after that you can unlock the door by the fingerprint and generate duress alarm. Click the icon, it becomes , which means the fingerprint is set as duress fingerprint. Click and cancel duress fingerprint setting.
✎	Modify fingerprint name.
🗑	Delete fingerprint, after that the fingerprint has no permission to unlock door.

Step 7 Update face recognition picture.

Click **Re-upload** and upload new face picture according to system prompt.

Move the mouse to uploaded picture, 🗑 shows up on the picture, click the icon and delete the uploaded picture.

Figure 3-316 Upload face picture



Face Comparison

This picture is used for face recognition by the device.

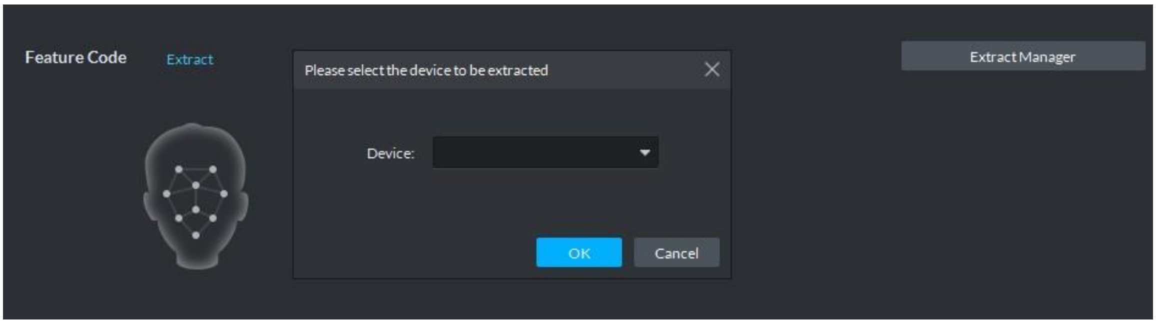
Please ensure that the picture can accurately identify the facial feature.

Step 8 Extract IR face feature code.

1) Click **Extract Manager**.

The system displays the interface of **Please select the device to be extracted,** see Figure 3-317.

Figure 3-317 Extract IR face feature code



Feature Code
Extract
Please select the device to be extracted
Device:
OK
Cancel
Extract Manager

2) Select IR face device, click **OK**.

3) Click **Extract**.

The system extracts IR face feature code from device, and prompts that extracted successfully.

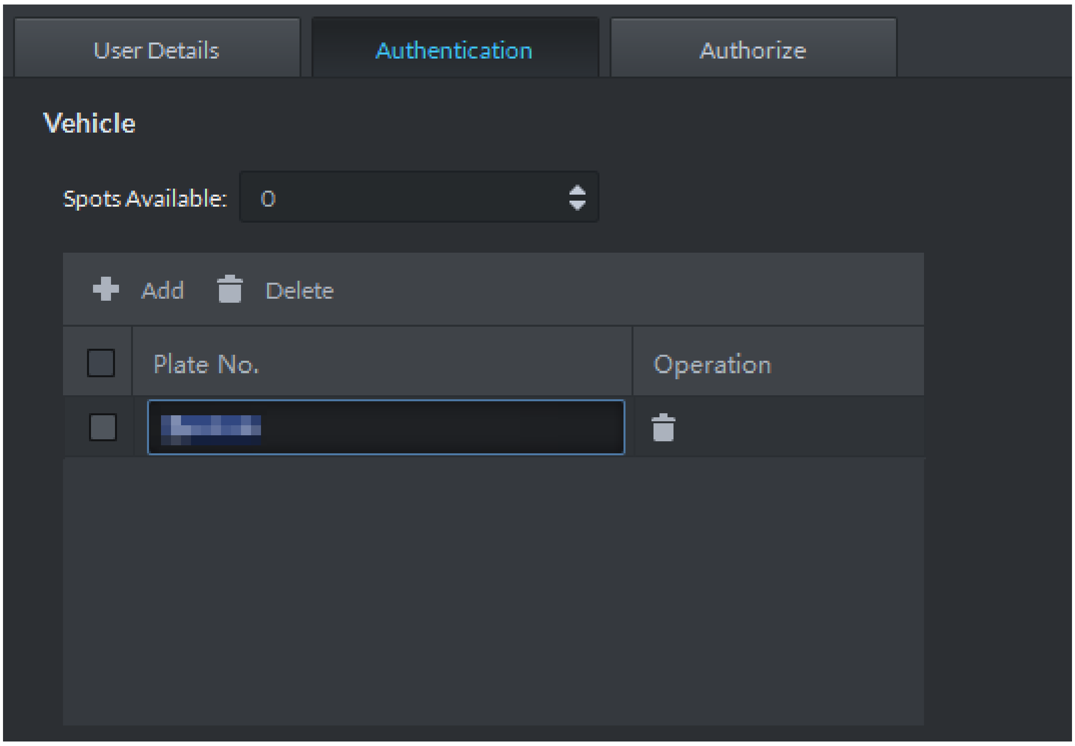
The IR face feature code is extracted; click **Re-extract** to update IR face feature code.

Step 9 Modify available spots and plate number.

Click **Spots Available**, modify spots, click **Plate No.** and modify plate No.

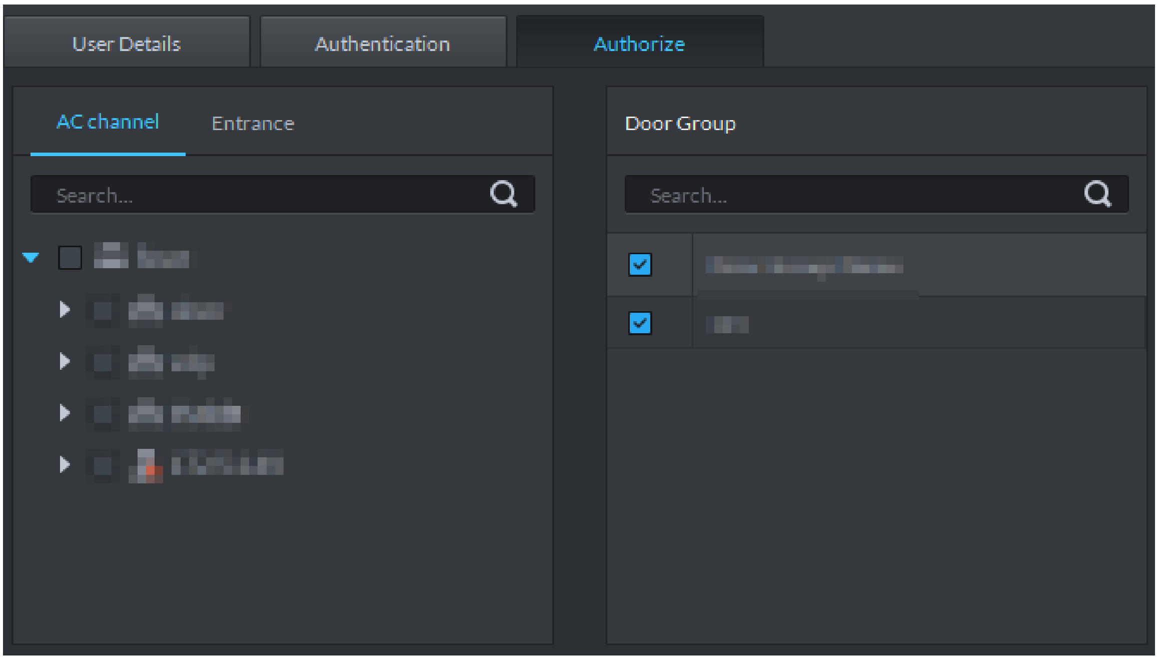
Click 🗑 next to plate, or select plate and click 🗑 to delete plate.

Figure 3-318 Add vehicle


User Details
Authentication
Authorize
Vehicle
Spots Available:
0
Add
Delete
Plate No.
Operation

Step 10 Click **Authorize**, modify access control and entrance is open to personnel. See Figure 3-319.

Figure 3-319 Authorize


User Details
Authentication
Authorize
AC channel
Entrance
Search...
Door Group
Search...

Step 11 Click **OK** and confirm modification.

3.16.4 Importing/Exporting Personnel

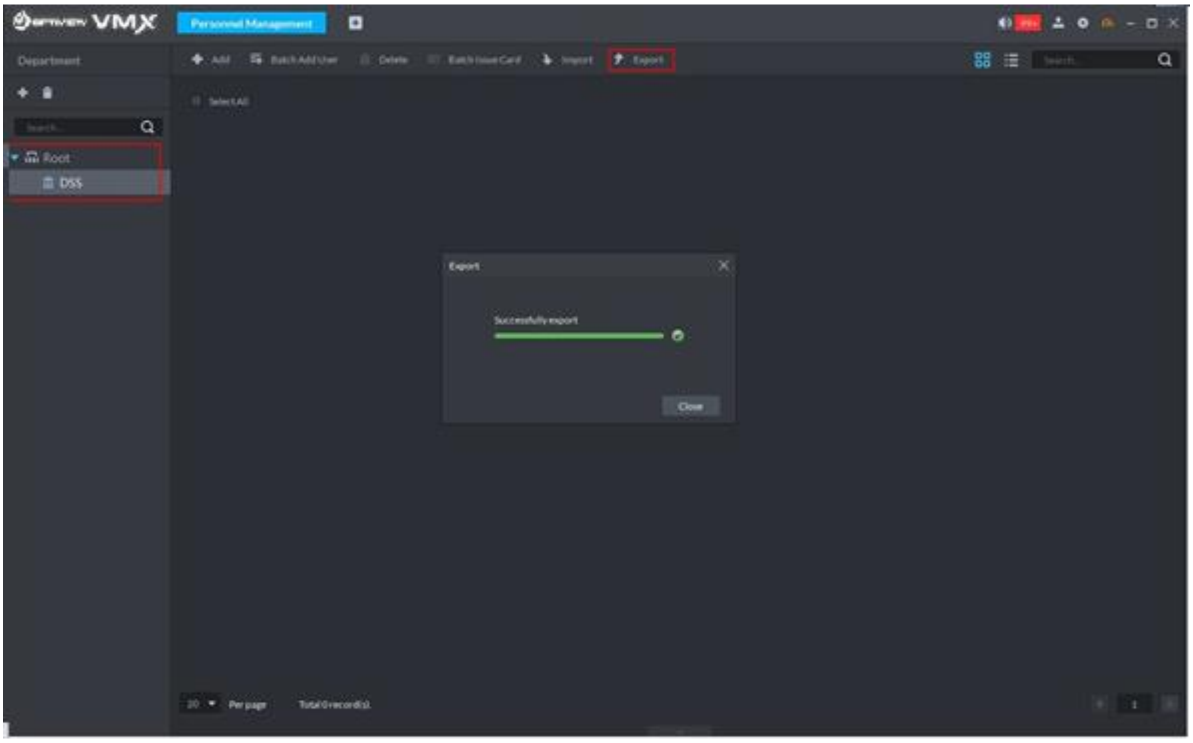
3.16.4.1 Exporting Personnel

Back up personnel data to restore damaged data or complete personnel configuration on the platform when there is a need for quick import of the personnel information.

Step 1 On the left side of the **Personnel Management** interface, select an organization, click **Export**, and follow the instructions on the interface to save the exported information to a local disk.

The system displays the progress of the export. See Figure 3-320.

Figure 3-320 Export personnel


VMX
Personnel Management
Department
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Search...
Select All
Root
DSS
Export
Successfully export
Close
20
Per page
Total 0 record(s)
1

Step 2 Select save path, click **Save**.

The system pops up **Export** dialog box, displays export progress.

Step 3 Click **Close** to close dialog box.

3.16.4.2 Importing Personnel

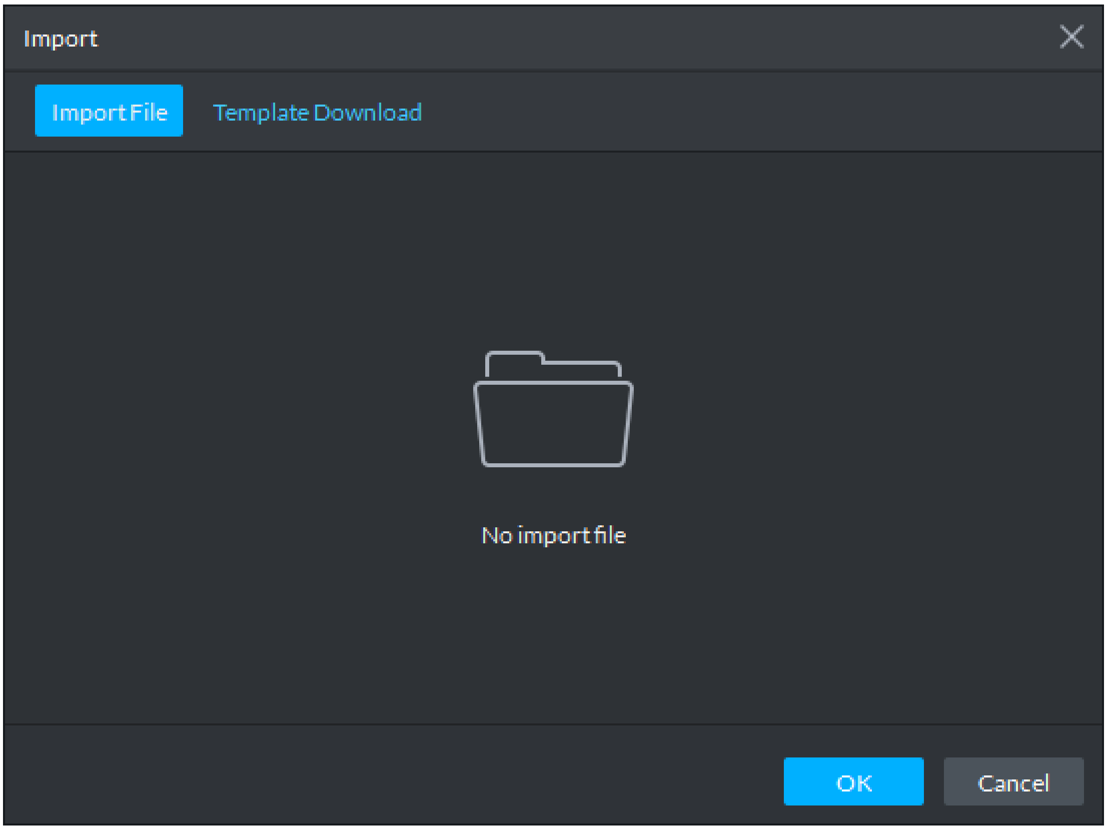
Edit the template or import information of existing personnel to quickly add them. You can import a file in .xls no larger than 1 M.

You can import personnel info exported from Optiview VMS.

Step 1 On the **Personnel Managemen**t interface, click **Import**.

The **Import** interface is displayed. See Figure 3-321.

Figure 3-321 Import



Step 2 Import personnel information files.

1) Click **Import**, and follow the instructions on the interface to select the files.

   If there is no personnel information file, click **Template Download** and follow the instructions on the interface to create personnel information.

2) Click **OK**.

   Complete the import of personnel information.

The following might occur during an import:

- The system prompts that the imported personnel already exist on the platform.
- Personnel ID duplicate in the imported file. If the same ID does not exist, the system accepts it as a new ID; if it already exists, the system gives a prompt.
- The system prompts that the imported personnel information is improperly filled, such as field length exceeding the limit on the client, and timeout resulting in a failure to upload to the database.
- Abnormal default values. The rules are: Gender (male), property (common staff), department (root node), ID type (Identification Card), marital status (null) and education (No education). The valid period starts from now and ends in 2028 by default.
- A person does not exist. If the department does not exist, a new department is created under the root node; if the department exists, the person is created under the department; department information matches by name.
- Cannot read the contents with a parsing error reported directly.

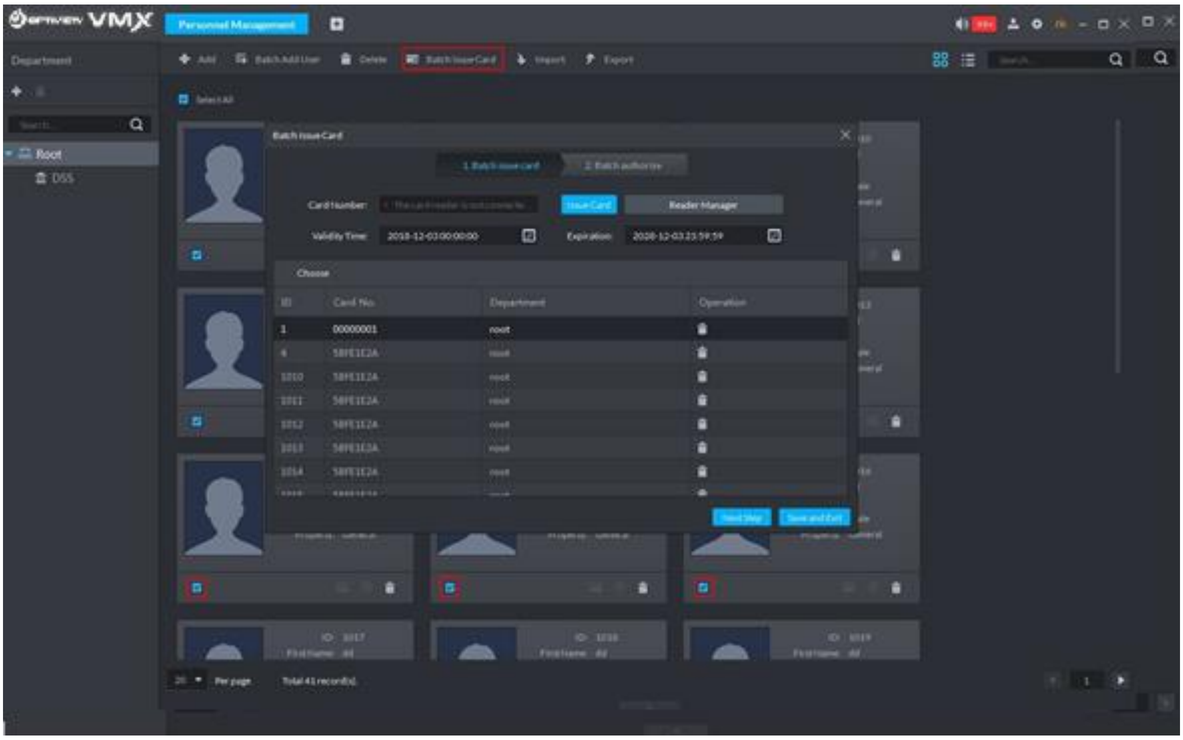
3.16.5 Batch Issue Card

Supports batch issuing cards to personnel to complete access control authorization.

Step 1 On the **Personnel Management** interface, select the personnel to issue card to, and click **Batch Issue Card**.

The **Batch issue card** interface is displayed. See Figure 3-322.

Figure 3-322 Batch issue card


VMX
Personnel Management
Department
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Select All
Root
DSS
Batch Issue Card
1. Batch issue card
2. Batch authorize
Card Number:
Issue Card
Reader Manager
Validity Time:
Expiration:
Choose
Next Step
Save and Exit
Per page
Total 41 record(s)

ID	Card No.	Department	Operation
1	00000001	root	
4	58FE1E2A	root	
1010	58FE1E2A	root	
1011	58FE1E2A	root	
1012	58FE1E2A	root	
1013	58FE1E2A	root	
1014	58FE1E2A	root	

Step 2 Issue cards to personnel.

You can issue card by entering card No. manually or card reader.

- Issue card by entering card No. manually

1) Select a person, enter the card number, and set up the validity time and expiry time.

2) Click **Issue Card**.

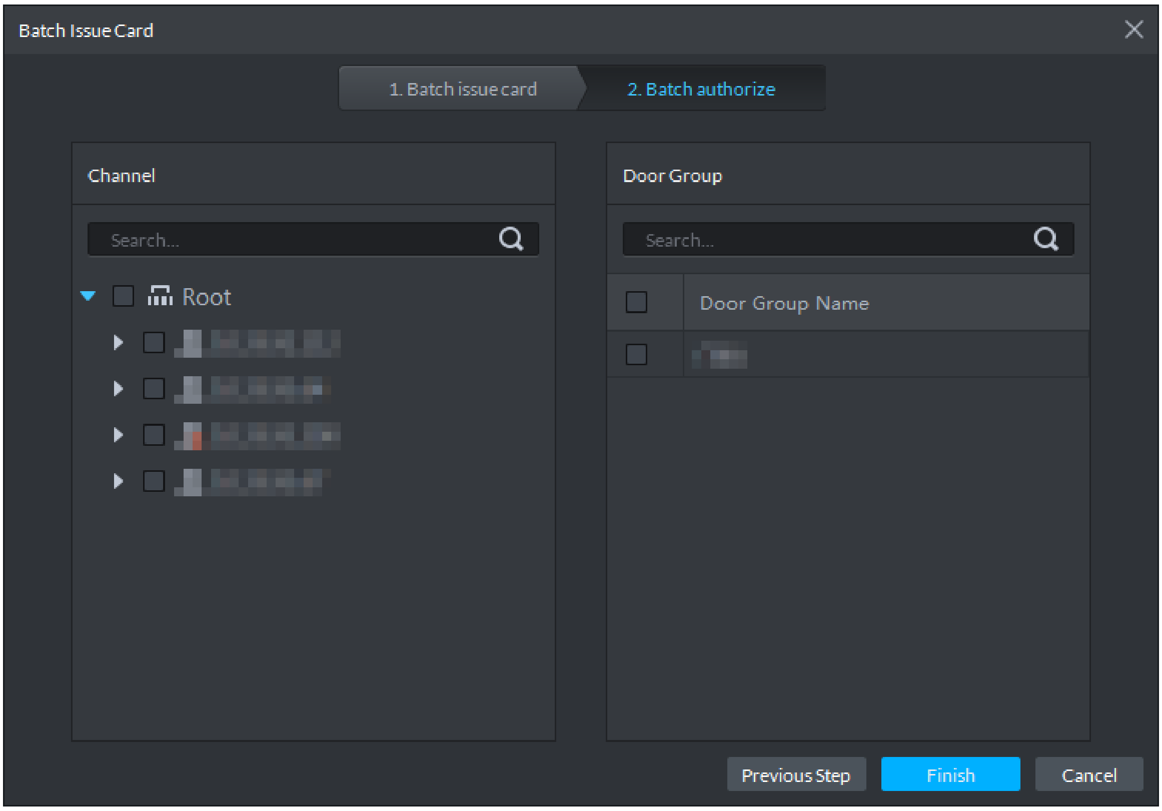
Complete issuing card to the selected personnel and the interface shows the personnel card number.

3) Repeat the steps until all personnel get their cards.

4) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 3-323.

Figure 3-323 Batch authorize

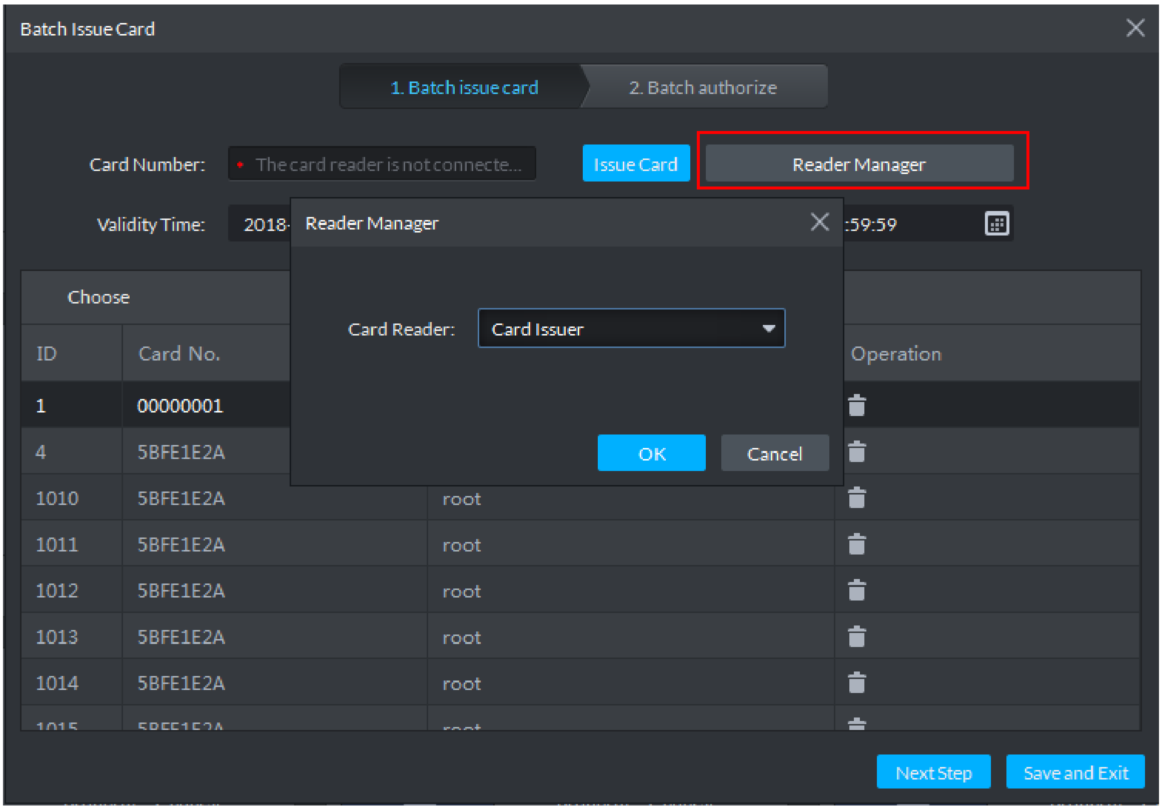

Batch Issue Card
1. Batch issue card
2. Batch authorize
Channel
Search...
Root
Door Group
Search...
Door Group Name
Previous Step
Finish
Cancel

- Issue card by card reader

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 3-324.

Figure 3-324 Reader manager


Batch Issue Card
1. Batch issue card
2. Batch authorize
Issue Card
Reader Manager
Choose
Reader Manager
OK
Cancel
Next Step
Save and Exit

Card Number: The card reader is not connecte...

Validity Time: 2018- ... :59:59

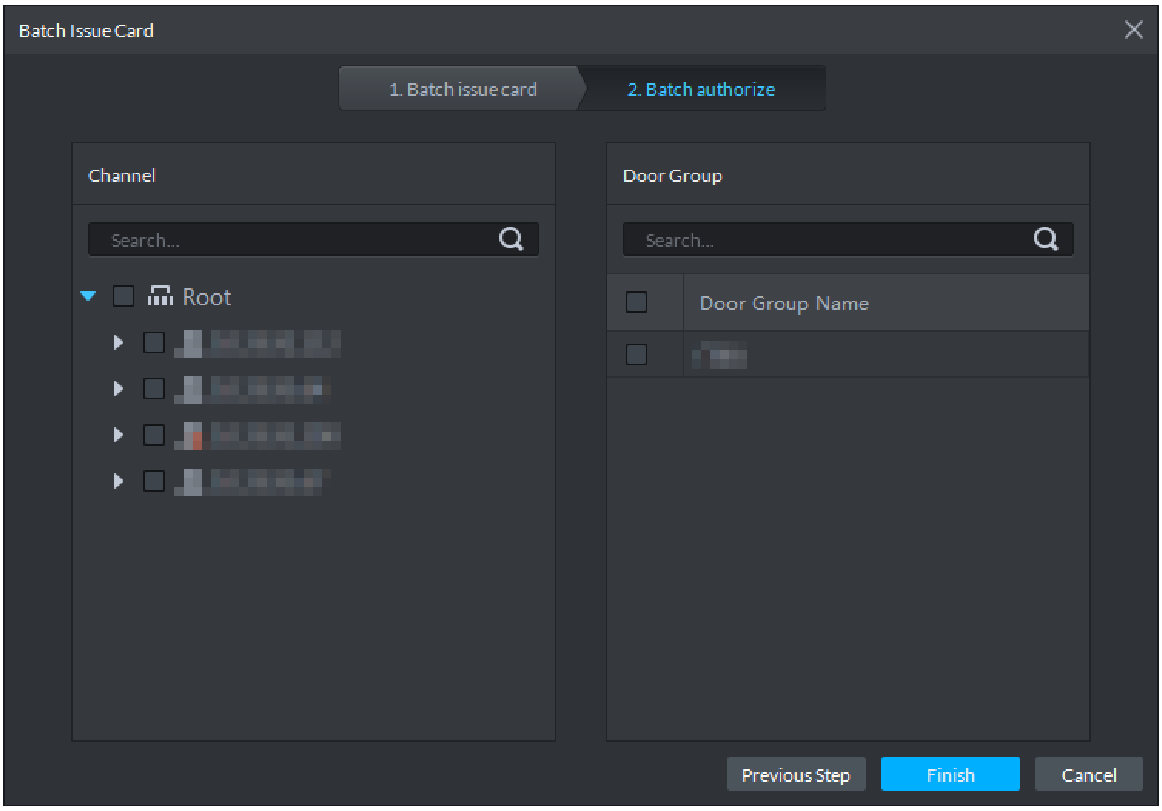
Card Reader: Card Issuer

ID	Card No.		Operation
1	00000001		
4	5BFE1E2A		
1010	5BFE1E2A	root	
1011	5BFE1E2A	root	
1012	5BFE1E2A	root	
1013	5BFE1E2A	root	
1014	5BFE1E2A	root	

2) Select from **Card Reader** or **Device**, and click **OK.**

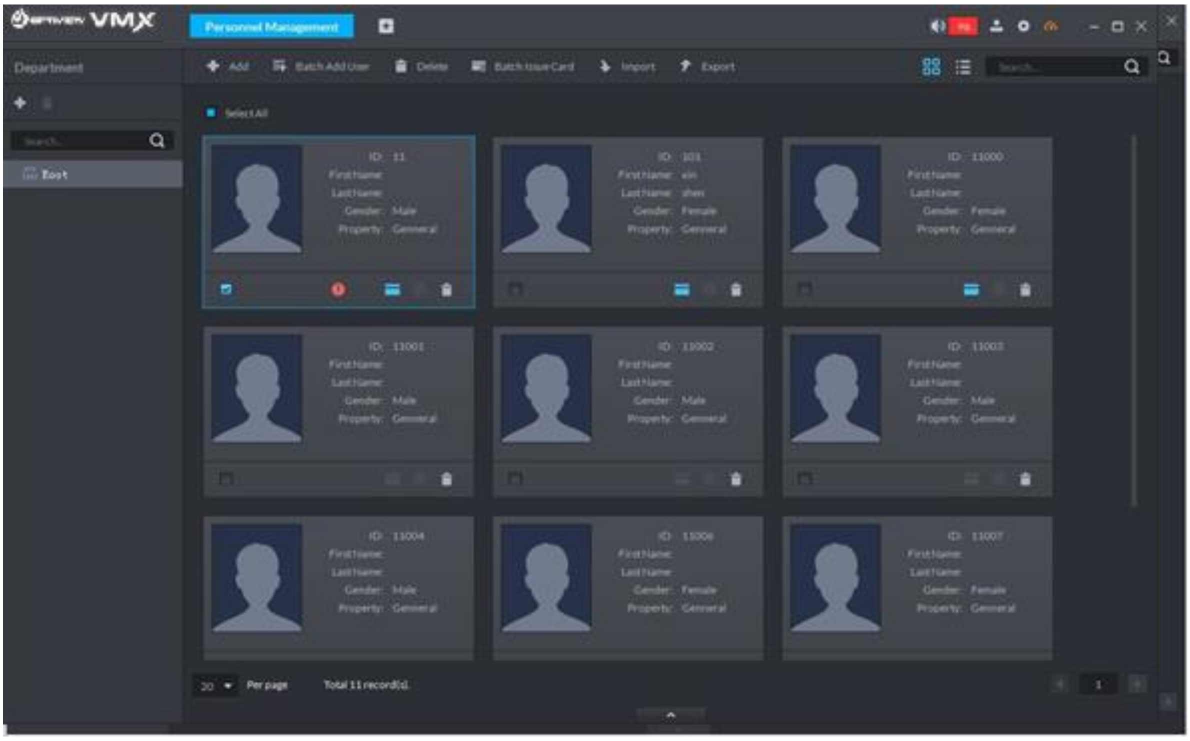
3) Swipe the card on the card reader or device.
4) Select a person, set up the validity time and expiry time, and click **Issue Card**.
5) Repeat the steps until all personnel get their cards.
6) Click **Next Step**.
   The **Batch authorize** interface is displayed. See Figure 3-325.

Figure 3-325 Batch authorize


Batch Issue Card
1. Batch issue card
2. Batch authorize
Channel
Search...
Root
Door Group
Search...
Door Group Name
Previous Step
Finish
Cancel

Step 3 Select the access control channels or door groups to which the personnel have access, and click **Finish**.

The interface displays the card issuing results. See Figure 3-326. The card icon changes into blue, as ▬ and it means that you have issued a card to the person.


VMX
Personnel Management
Department
Search...
Root
Add
Batch Add User
Delete
Batch Issue Card
Import
Export
Search...
Select All
20
Per page
Total 11 record(s)
1

ID: 11
First Name:
Last Name:
Gender: Male
Property: General

ID: 101
First Name: xin
Last Name: shen
Gender: Female
Property: General

ID: 11000
First Name:
Last Name:
Gender: Female
Property: General

ID: 11001
First Name:
Last Name:
Gender: Male
Property: General

ID: 11002
First Name:
Last Name:
Gender: Male
Property: General

ID: 11003
First Name:
Last Name:
Gender: Male
Property: General

ID: 11004
First Name:
Last Name:
Gender: Male
Property: General

ID: 11006
First Name:
Last Name:
Gender: Female
Property: General

ID: 11007
First Name:
Last Name:
Gender: Female
Property: General

Figure 3-326 Issue card result

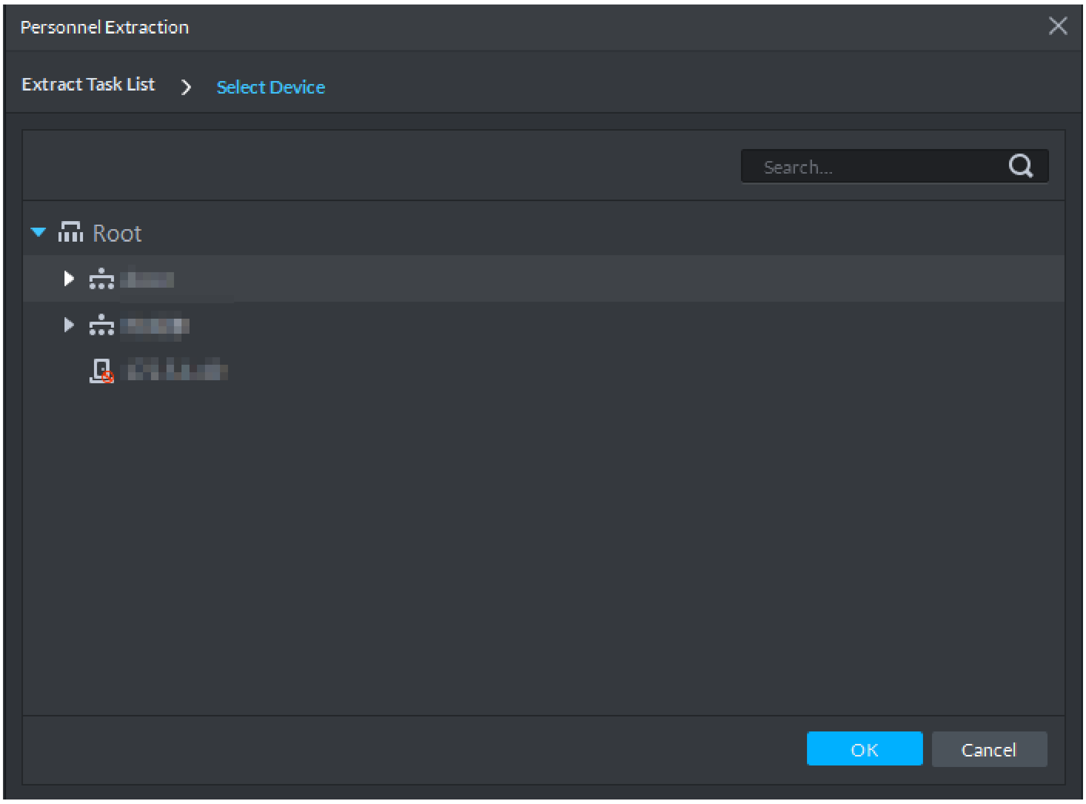
3.16.6 Personnel Extraction

Extract personnel info from access control, and sync it to platform.

Step 1 On Personnel Management interface, click Personnel Extraction.

The system displays **Personnel Extraction** interface, see Figure 3-327.

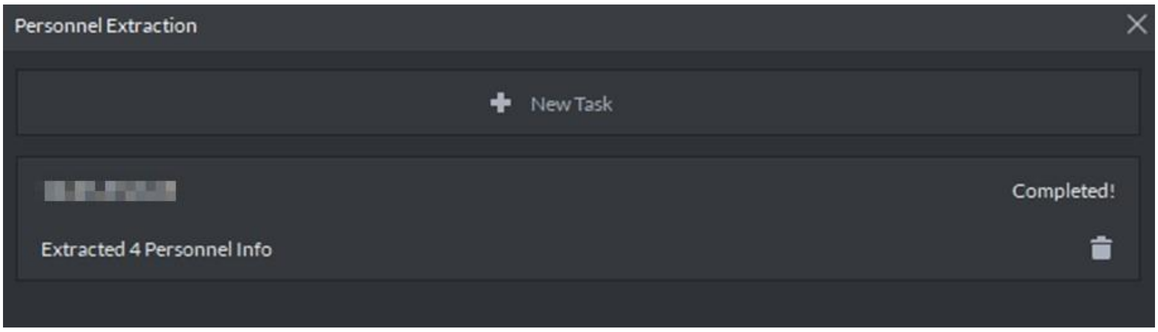
Figure 3-327 Personnel extraction


Personnel Extraction
Extract Task List
Select Device
Search...
Root
[redacted]
[redacted]
[redacted]
OK
Cancel

Step 2 Select access control device, click **OK**.

The system displays extraction result, see Figure 3-328.

Figure 3-328 Extraction result



[redacted]

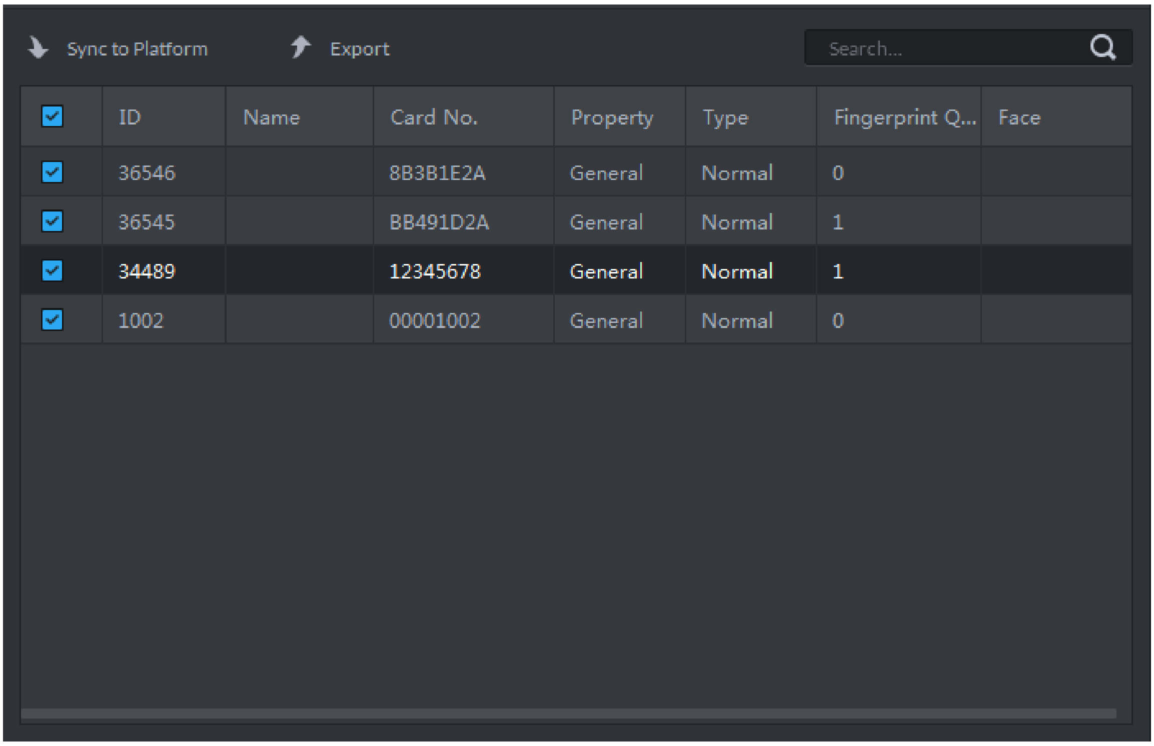
Completed!

Extracted 4 Personnel Info

Step 3 Double-click record.

The system displays info of extracted personnel, see Figure 3-328.

Figure 3-329 Extracted personnel detail



☑	ID	Name	Card No.	Property	Type	Fingerprint Q...	Face
☑	36546		8B3B1E2A	General	Normal	0	
☑	36545		BB491D2A	General	Normal	1	
☑	34489		12345678	General	Normal	1	
☑	1002		00001002	General	Normal	0	

Step 4 Select personnel, click **Sync to platform**.

Select personnel and add to list.

Select personnel, click **Export** and save personnel info to local PC.

3.16.7 Generating Path

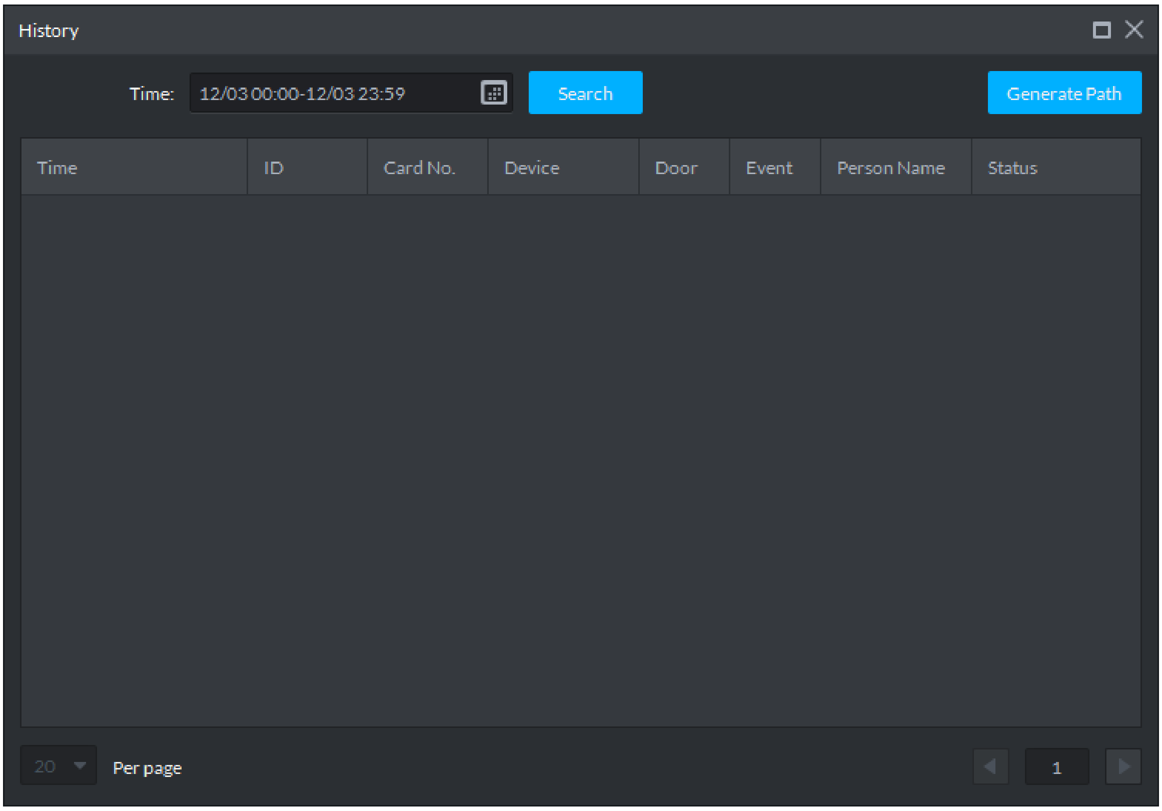
You can check all door unlocking records by personnel and generate a path.

To view the generated path, you have to drag the access control device to the map for display first. See 3.2.6 Configuring Emap for detailed steps.

Step 1 On **Personnel Management** interface, click ▭ or ◉ of the person.

Step 2 The **History** interface is displayed. See Figure 3-330.

Figure 3-330 Personnel history record


History
Time:
12/03 00:00-12/03 23:59
Search
Generate Path
Time
ID
Card No.
Device
Door
Event
Person Name
Status
20
Per page
1

Step 3 Set up time for the search and click **Search**.
The system displays the search results.

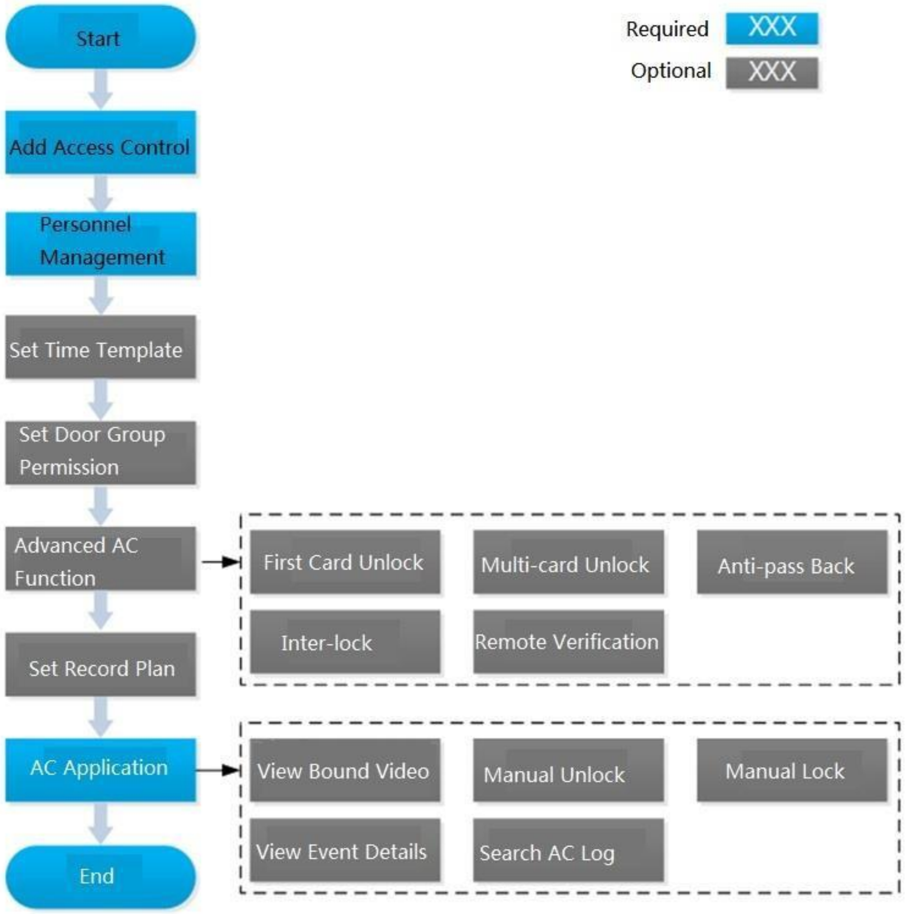
Step 4 Click Generate Path.
The system displays the map interface to show the activity path of the person.

Step 5 Click **Export**, and drag the mouse on the interface to select a region. Follow the instructions on the interface to save the path as a picture to a local disk.

3.17 Access Control

After adding access control devices on Pro, you can control the door locking/unlocking on platform, view videos and events related to the access control channel, and configure advanced access control functions, such as First Card Unlock and Multi-card Unlock. For operation flow, see Figure 3-331.

Figure 3-331 AC management flow


Required XXX
Optional XXX
Start
Add Access Control
Personnel Management
Set Time Template
Set Door Group Permission
Advanced AC Function
First Card Unlock
Multi-card Unlock
Anti-pass Back
Inter-lock
Remote Verification
Set Record Plan
AC Application
View Bound Video
Manual Unlock
Manual Lock
View Event Details
Search AC Log
End

3.17.1 Adding Access Control

Step 1 Add access control device. For more details, see 3.2.2.4 Adding Device.

Support access control devices including general AC device, AC integrated controller, 2nd generation AC, face AC and IR face AC. Set **Device Category** as **Access Control** when adding.

Step 2 Bind resources.

If panoramic camera is installed in the scene, it supports binding AC channel and panoramic camera. You can view real-time video image of panoramic camera on console. When alarm is triggered, you can view video of bound panoramic camera.

📖

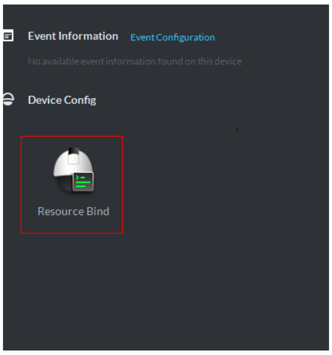
The panoramic camera is required to be added to platform before binding resources.

1) On client homepage, click **Config.**

   The system displays **Config** interface.

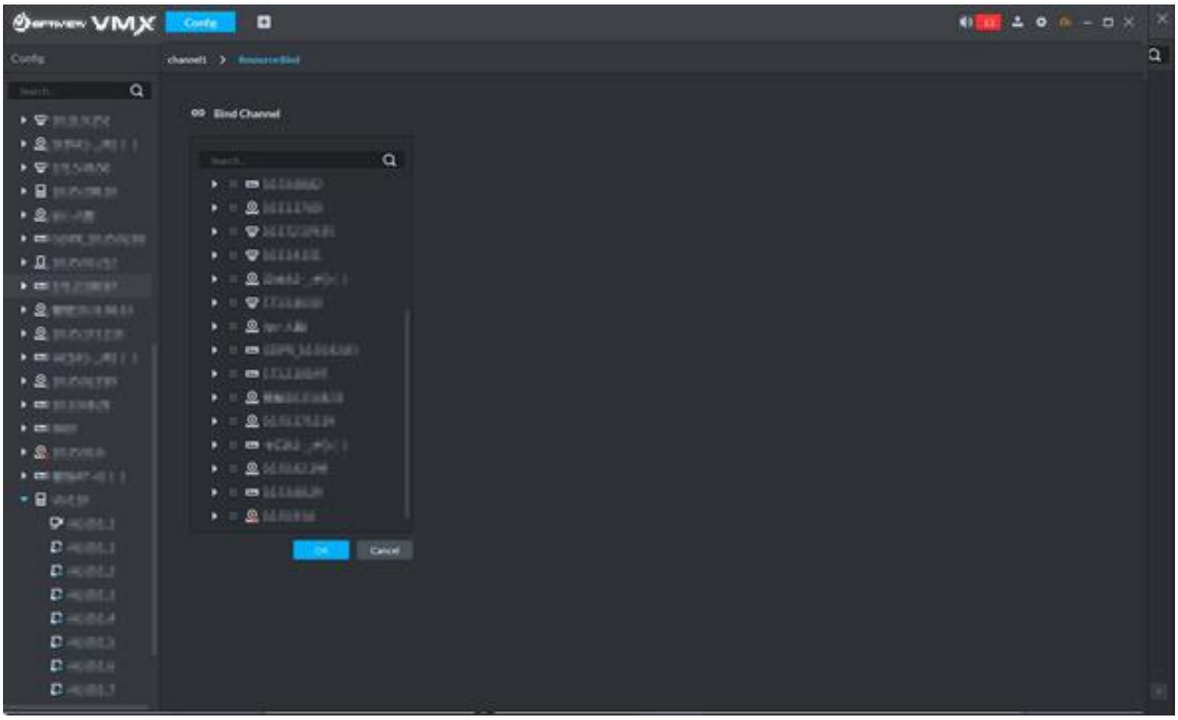
2) In the left device tree, select AC channel, click **Resource Bind**, and see Figure 3-332. The system displays **Resource Bind** interface, see Figure 3-333.

Figure 3-332 Enter resource bind interface


Event Information
Event Configuration
Device Config
Resource Bind

No available event information found on this device

Figure 3-333 Resource bind


Config
Config
Search...
channel1
Resource Bind
Bind Channel
Search...
OK
Cancel

3) Select bound video channel, click **OK**.

Step 3 Configure door info.

You can configure door status, NC and NO period, alarm enable and unlock length.

1) On client homepage, click **Config**.

The system displays **Config** interface.

2) In left device tree, select AC channel, click **Door Configuration**, and see Figure 3-334.

The system displays **Door Config** interface, see Figure 3-335.

For the console on access control interface, right-click **AC Channel**, select **AC Channel Config** and enter **Door Config** interface.

Figure 3-334 Enter config interface

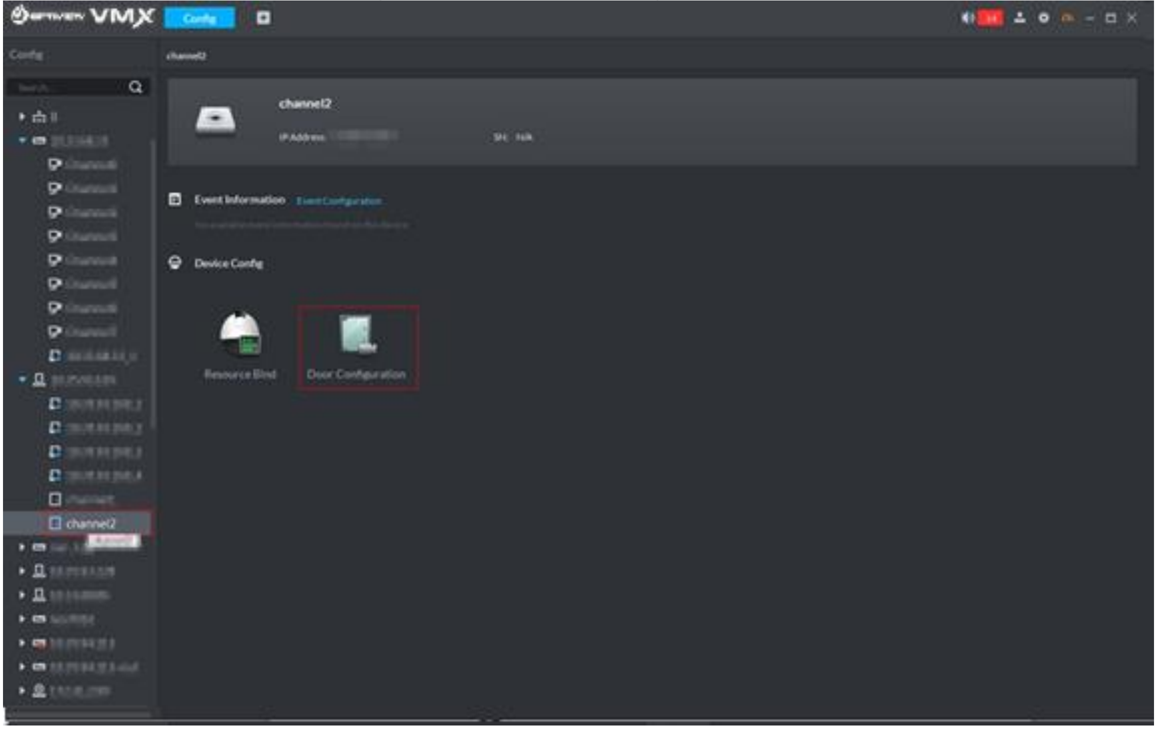
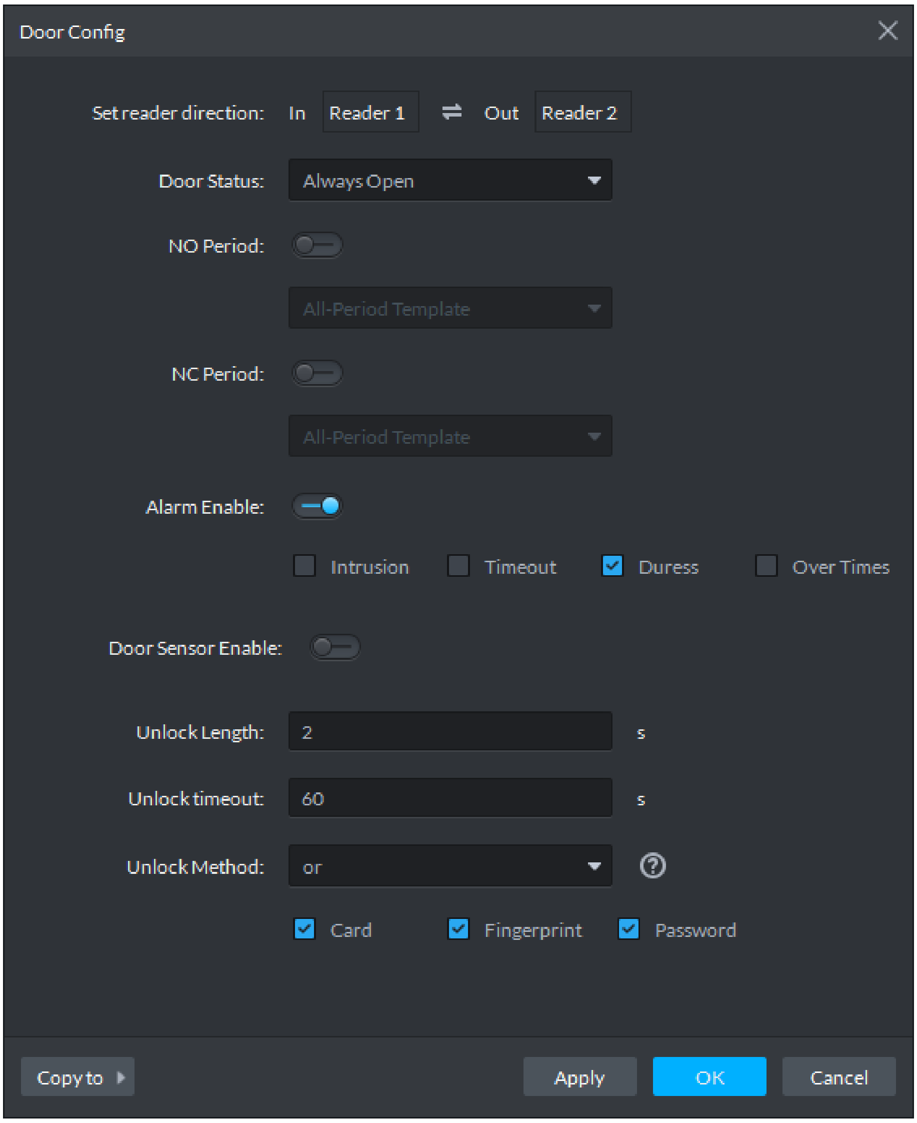

VMX
Config
Config
channel2
channel2
IP Address:
SN: N/A
Event Information
Event Configuration
Device Config
Resource Bind
Door Configuration
channel2

Figure 3-335 Door config



Door Config

Set reader direction: In Reader 1 ⇄ Out Reader 2

Door Status: Always Open

NO Period: ○

All-Period Template

NC Period: ○

All-Period Template

Alarm Enable: ●

☐ Intrusion ☐ Timeout ☑ Duress ☐ Over Times

Door Sensor Enable: ○

Unlock Length: 2 s

Unlock timeout: 60 s

Unlock Method: or

☑ Card ☑ Fingerprint ☑ Password

3) Configure door information and click **OK**. For details of the parameters, see Table 3-54.

The interface might be different for different access control devices connected. The actual interfaces shall prevail.

Table 3-54 Door configuration description

Parameter	Description
Set reader direction	Indicates the in/out reader based on the wiring of ACS.
Door Status	Sets the access control status to **Normal**, **Always Open**, or **Always Close**.
NO Period	If enabled, you can set up a period during which the door is always open.
NC Period	If enabled, you can set up a period during which the door is always close.

Parameter	Description
Alarm Enable	● If the door is opened not as intended, the door sensor is enabled and triggers an intrusion alarm. ● Entry with the duress card, duress password, or duress fingerprint triggers a duress alarm. ● Unlock duration exceeding the **Unlock timeout** triggers a timeout alarm. ● Swiping an illegal card for more than five times triggers a malicious alarm.
Door Sensor Enable	Enables the door sensor. The intrusion alarm and timeout alarm take effect only when door sensor is enabled.
Unlock Length	Sets up the duration of door unlocking. The door is automatically locked when the duration is over.
Unlock timeout	Unlock duration exceeding the **Unlock timeout** triggers a timeout alarm.
Unlock Method	You can use any one of the methods: card, fingerprint, face, and password, or any of their combinations to unlock the door.
Inter-door Lock	There can only be one door open in a door group at the same time. When one door is open, the others will keep locked until that door closes. See “3.13.5.4 Inter-door Lock” for details.
Malicious Alarm	Swiping an unauthorized card for five times continuously within 50s triggers a malicious alarm. In the next 50s, every swipe of the card triggers a same alarm.

3.17.2 Personnel Management

If you want to add personnel, see 3.16 **Personnel Management.** When adding personnel, you need to add information such as card, fingerprint and face comparison according to requirement, and enable access control permission.

3.17.3 Managing Time Template

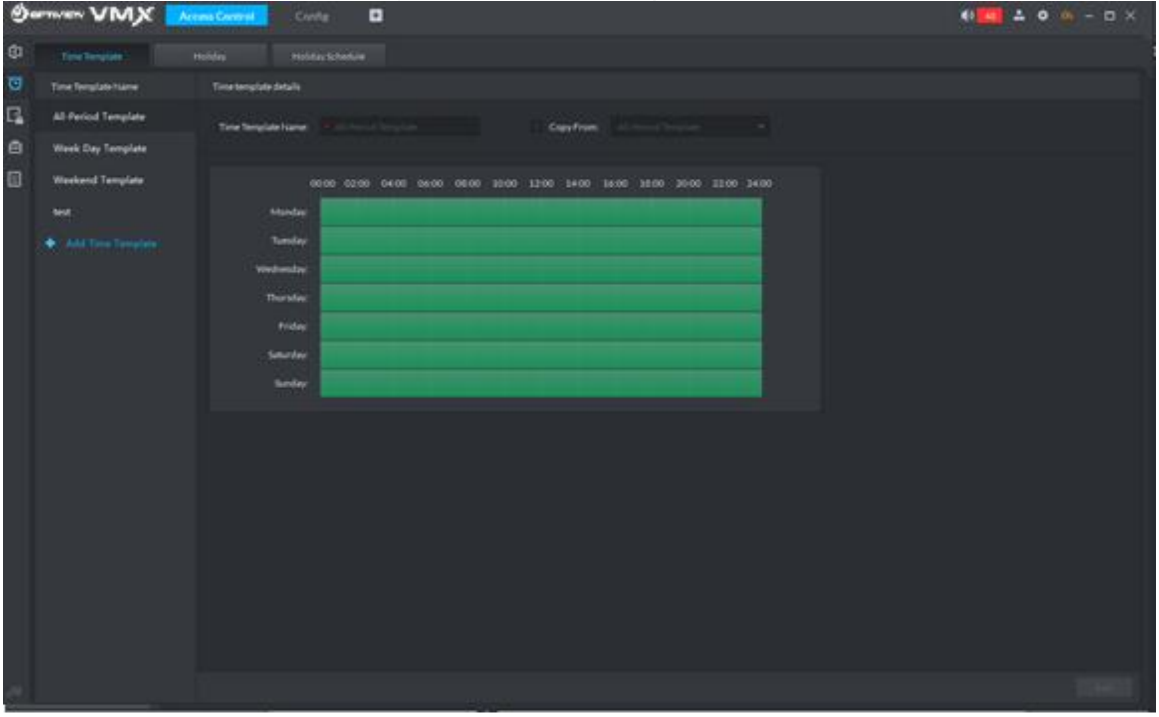
3.17.3.1 Setting Time Template

Default time template includes all-period template, week day template and weekend template. If default template fails to meet requirement, then set time template and you can adopt different unlock modes at different time.

Step 1 On client homepage, click **Access Control**.
The system displays **Access Control** interface.

Step 2 Click 🕒 and the system displays **Time Template** interface, see Figure 3-336.

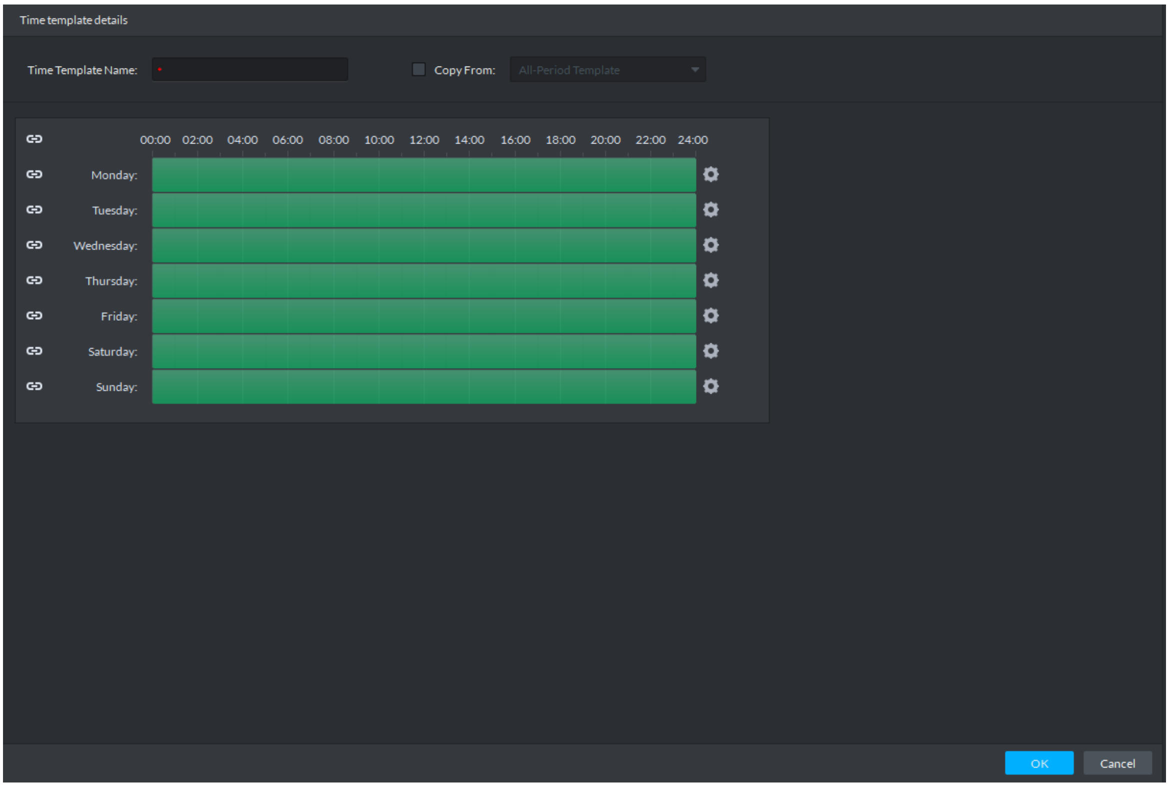
Figure 3-336 Time template


VMX
Access Control
Config
Time Template
Holiday
Holiday Schedule
Time Template Name
All-Period Template
Week Day Template
Weekend Template
test
Add Time Template
Time template details
Time Template Name:
All-Period Template
Copy From:
00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:

Step 3 Click Add Time Template.

The **Time template details** interface is displayed. See Figure 3-337.

Figure 3-337 Add time template


Time template details
Time Template Name:
Copy From:
All-Period Template
00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:
OK
Cancel

Step 4 Set up **Time Template Name** and the required time period, and click **OK**.

Select **Copy From** and the copied template, and you can use the time periods of the copied template. In this way, you can quickly configure the time periods by modifying the ones of the copied template.

Methods to set up the time period:

- Method I: Press and hold the left button of the mouse. Over the time periods not selected, the mouse displays as a pen, and you can drag the mouse on the setting interface to select a time period. Over the selected time periods, the mouse displays as an eraser, and you can erase selected time periods with it.

  Click the icons in front of multiple week numbers one by one and the icons change to . In this way, you can configure the time periods corresponding to the week numbers. You can quickly select all the week numbers by clicking on the top.

- Method II: Click ⚙ and set up the time periods in the popup interface. You can set up six time periods at most.

Step 5 The new time template is displayed in the left list.

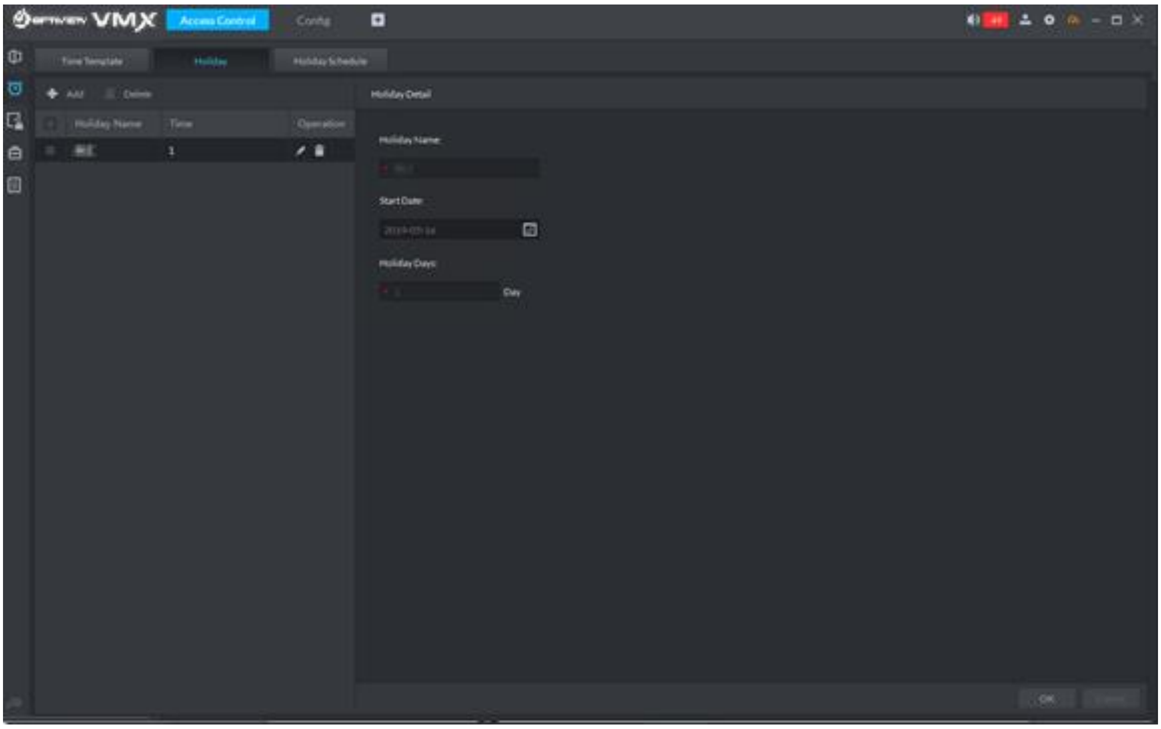
3.17.3.2 Setting Holiday

Set holiday according to actual situation, used to configure holiday plan, and you can unlock according to holiday plan.

Step 1 On **Access Control** interface, click and select **Holiday**.

The system displays **Holiday** interface, see Figure 3-338.

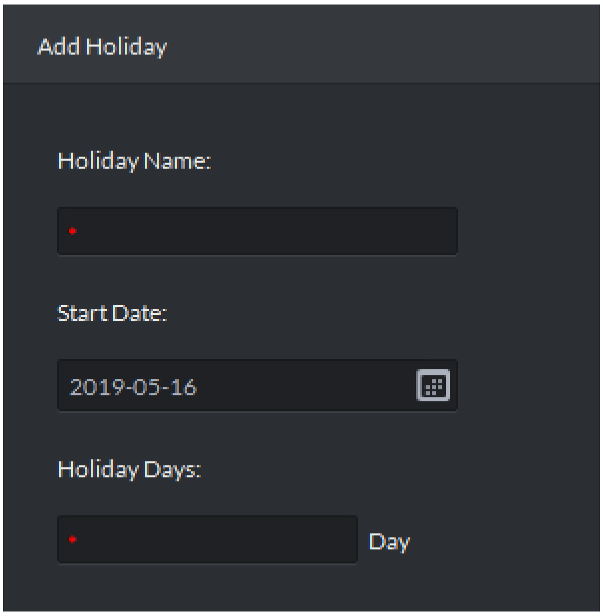
Figure 3-338 Holiday


VMX
Access Control
Config
Time Template
Holiday
Holiday Schedule
Add
Delete
Holiday Name
Time
Operation
1
Holiday Detail
Holiday Name:
Start Date:
Holiday Days:
Day
OK
Cancel

Step 2 Click **Add**.

The system displays holiday configuration interface, see Figure 3-339.

Figure 3-339 Add holiday



Add Holiday

Holiday Name:

Start Date:

2019-05-16

Holiday Days:

Day

Step 3 Set holiday info, click **OK**.

3.17.3.3 Setting Holiday Schedule

Door group can unlock according to the holiday schedule that is set.

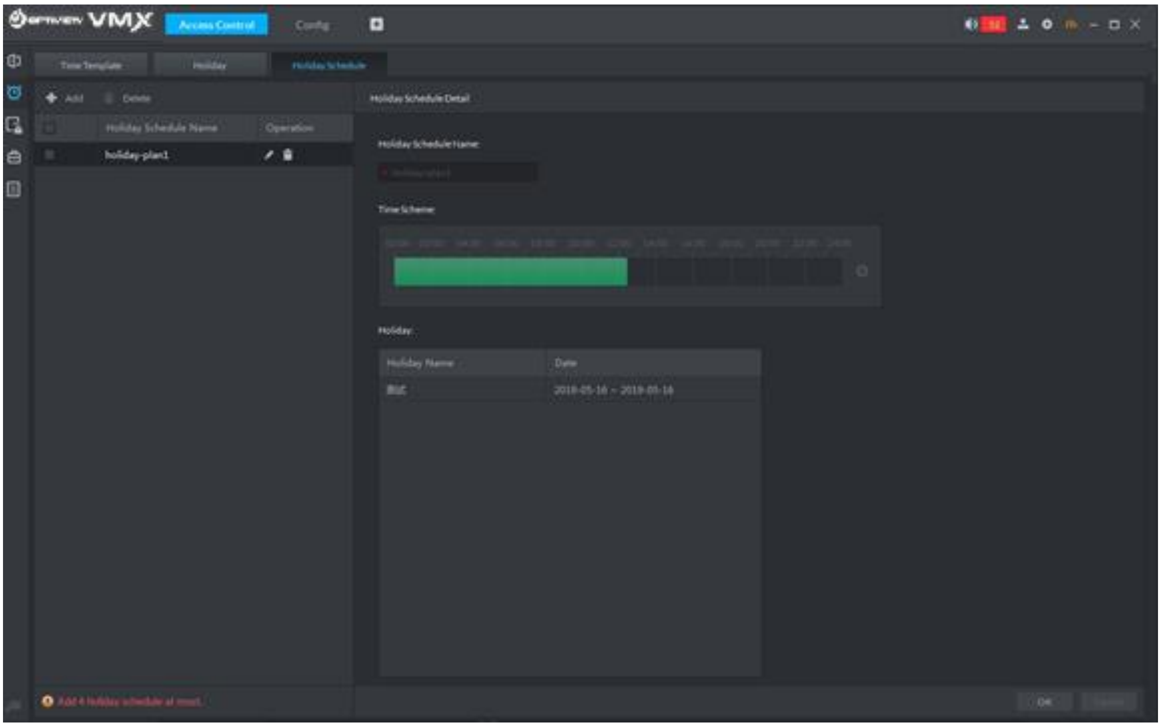
Step 1 On **Access Control** interface, click ⏰ and select **Holiday Schedule**.

The system displays **Holiday Schedule** interface.

Step 2 Click **Add**.

The system displays interface of add holiday schedule, see Figure 3-340.

Figure 3-340 Add holiday schedule



VMX
Access Control
Config
Time Template
Holiday
Holiday Schedule
Add
Delete
Holiday Schedule Name
Operation
holiday-plan1
Holiday Schedule Detail
Holiday Schedule Name:
Time Scheme:
Holiday:
Holiday Name
Date
OK

Add 4 holiday schedule at most.

Step 3 Set holiday schedule parameters, click **OK** and complete config.

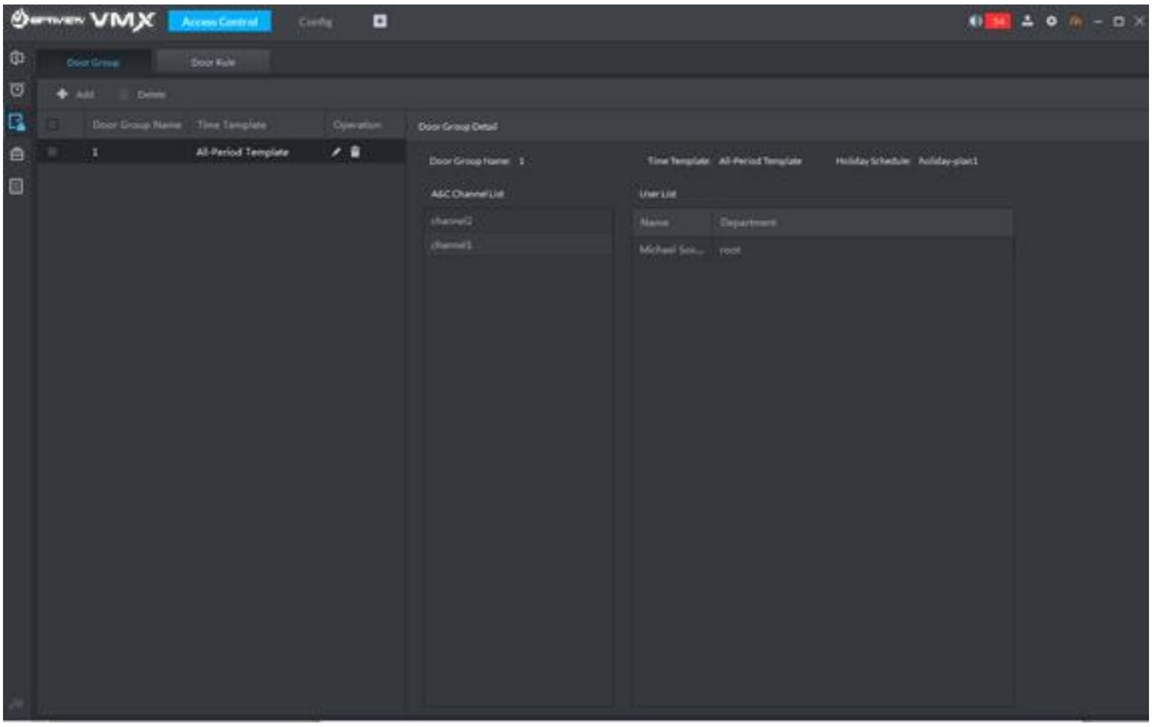
3.17.4 Setting Access Level

If you manage the doors by groups, you can quickly grant users with the authorizations to unlock the doors in a specific group.

Step 1 On the **Access Control** interface, click .

The **Access Level** interface is displayed. See Figure 3-341.

Figure 3-341 Access level



Door Group Name	Time Template	Operation
1	All-Period Template	

Door Group Name: 1

Time Template: All-Period Template

Holiday Schedule: holiday-plan1

A&C Channel List

channel2

channel1

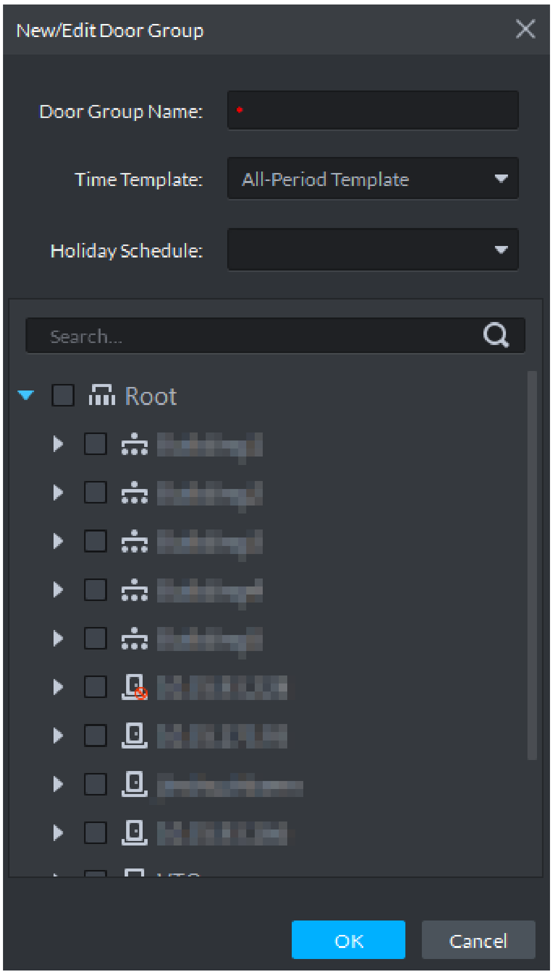
User List

Name	Department
Michael Sco...	root

Step 2 Create door groups.

1) Click the **Door Group** tab.
   The **Door Group** interface is displayed.
2) Click **Add**.
   The **New/Edit Door Group** interface is displayed. See Figure 3-342.

Figure 3-342 New/Edit door group


New/Edit Door Group
Door Group Name:
Time Template:
All-Period Template
Holiday Schedule:
Search...
Root
OK
Cancel

3) Enter **Door Group Name**, select **Time Template** and an access control channel, and click **OK**.

   After selecting the time template and access control channel, you can only use the time periods of the selected time template and the selected access control channel when granting authorizations to users. The interface displays the information of the newly created door groups.

Step 3 Authorize users.

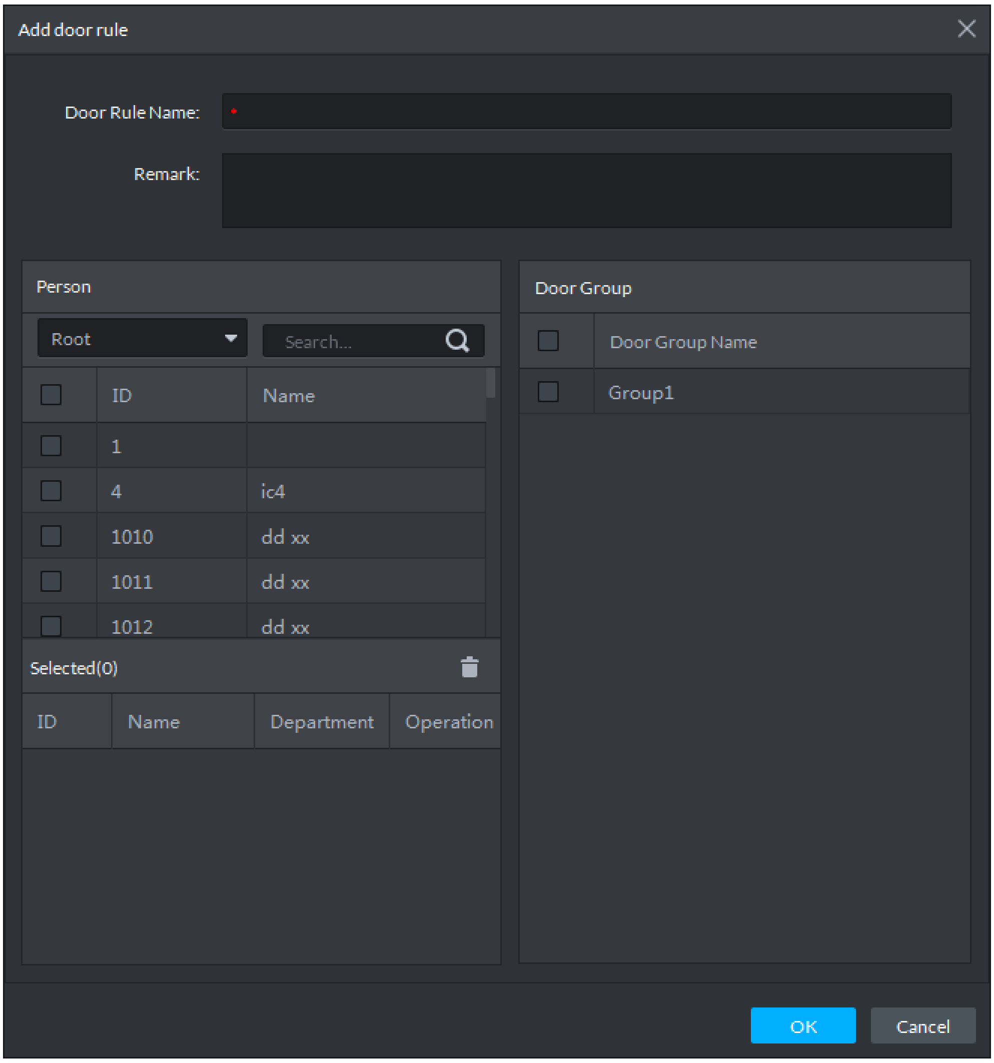
1) Click the **Door Rule** tab.

   The **Door Rule** interface is displayed.

2) Click **Add**.

   The **Add door rule** interface is displayed. See Figure 3-343.

Figure 3-343 Add door rule


Add door rule
Door Rule Name:
Remark:
Person
Root
Search...
ID
Name
1
4
ic4
1010
dd xx
1011
dd xx
1012
dd xx
Selected(0)
ID
Name
Department
Operation
Door Group
Door Group Name
Group1
OK
Cancel

3) Enter **Door Rule Name**, select **Person** and **Door Group**, and click **OK**. The interface displays the authorization information.

3.17.5 Advanced Function

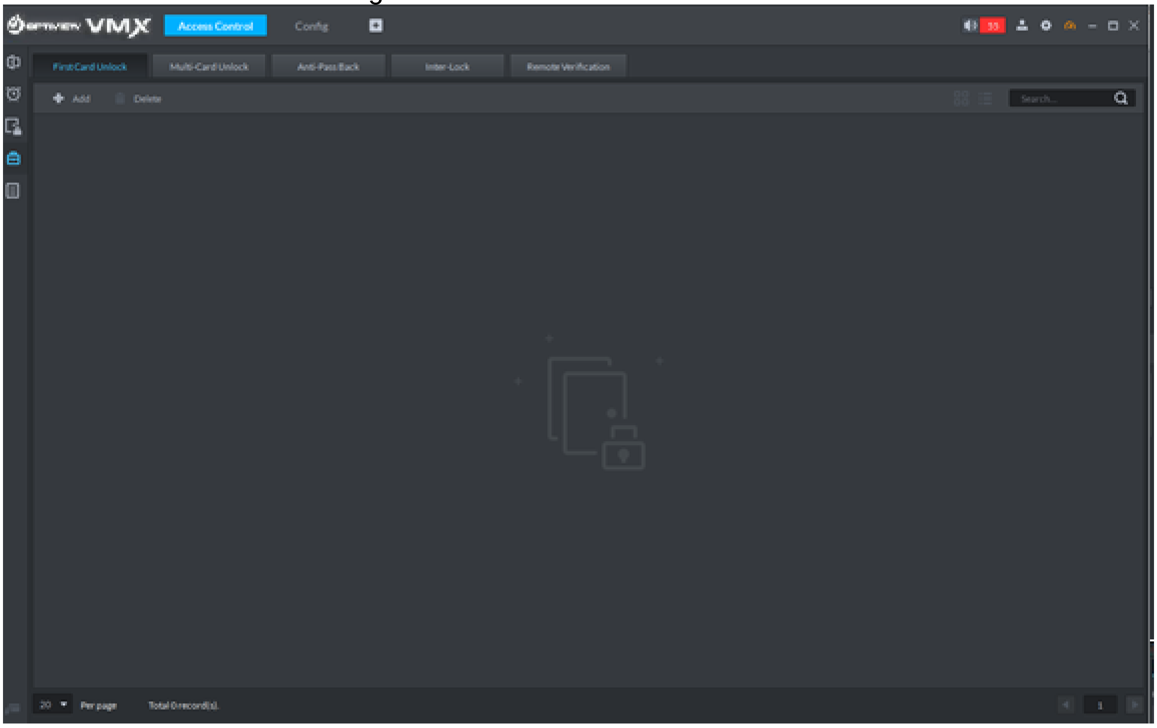
3.17.5.1 First Card Unlock

Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. You can set up multiple first cards. Only after any one of the users swipes the first card can other users without first cards unlock the door with their cards.

Step 1 On the **Access Control** interface, click 🗄 and select **First Card Unlock**

The **First Card Unlock** interface is displayed. See Figure 3-344.

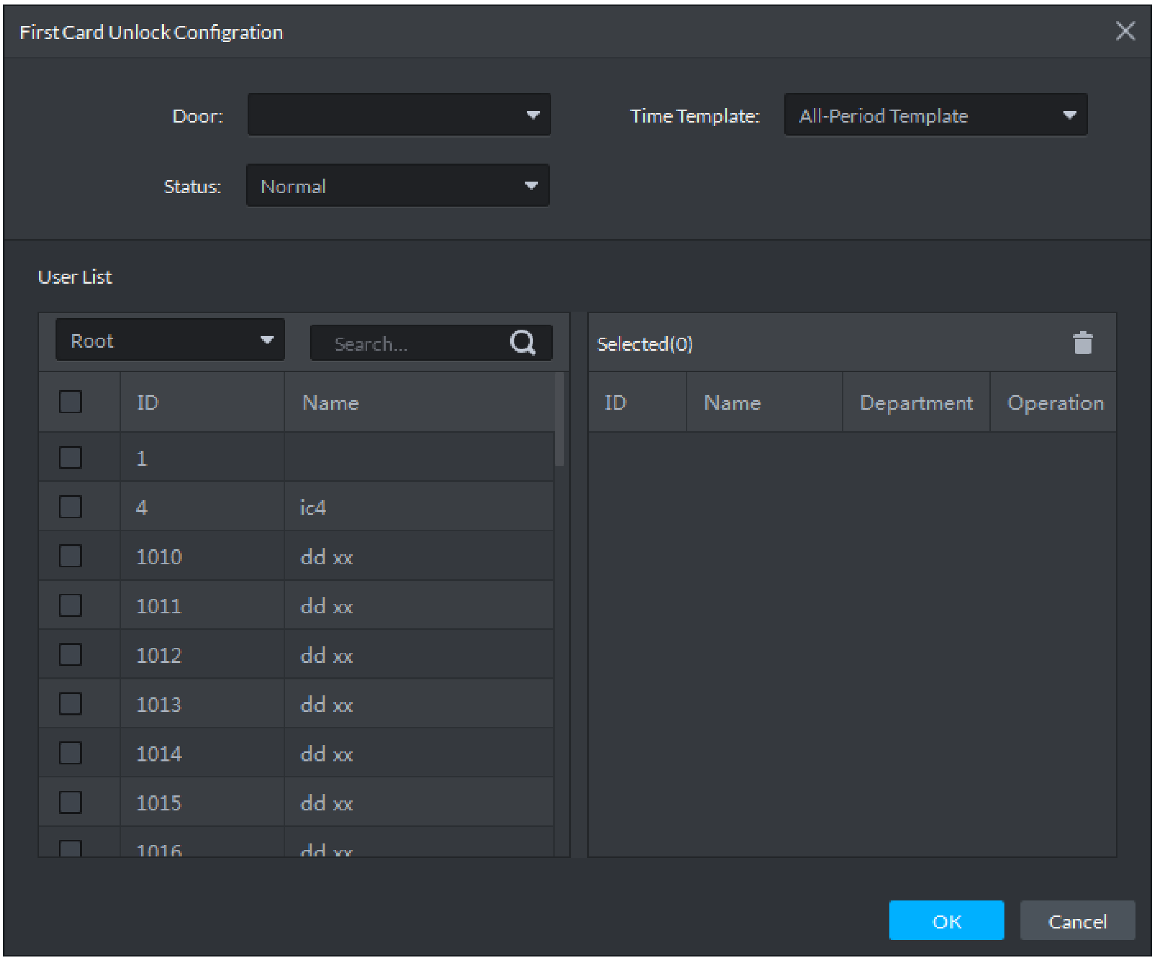
Figure 3-344 First card unlock


VMX
Access Control
Config
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Search...
20
Per page
Total 0 record(s).
1

Step 2 Click **Add**.

The **First Card Unlock Configuration** interface is displayed. See Figure 3-345.

Figure 3-345 First card unlock config


First Card Unlock Configration

Door:

Time Template: All-Period Template

Status: Normal

User List

Root
Search...
Selected(0)
OK
Cancel

☐	ID	Name
☐	1	
☐	4	ic4
☐	1010	dd xx
☐	1011	dd xx
☐	1012	dd xx
☐	1013	dd xx
☐	1014	dd xx
☐	1015	dd xx
☐	1016	dd xx

ID	Name	Department	Operation

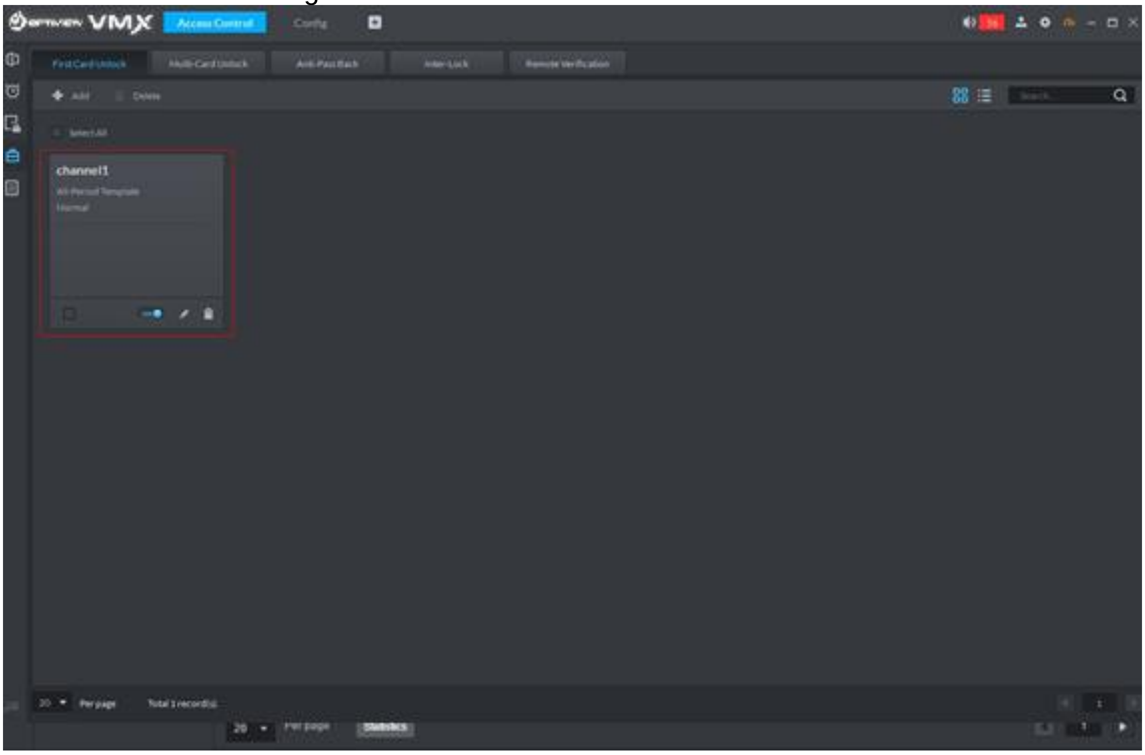
Step 3 Configure the **First Card Unlock** parameters and click **OK**. For details of the parameters, see Table 3-55.

The system displays the **First Card Unlock** information. See Figure 3-346. First Card Unlock is enabled by default.

Table 3-55 First card unlock parameter description

Parameter	Description
Door	You can select the target access control channel to configure the first card unlock.
Time Template	**First Card Unlock** is valid in the time period of the selected time template.
Status	After **First Card Unlock** is enabled, the door is in either the Normal mode or Always Open mode.
User	You can select the user to hold the first card. Supports selecting a number of users to hold first cards. Any one of them swiping the first card means first card unlock is done.

Figure 3-346 First card info list


VMX
Access Control
Config
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Select All
channel1
All-Period Template
Normal
20
Per page
Total 1 record(s)

Step 4 Click .

The icon changing into indicates **First Card Unlock** is enabled.

3.17.5.2 Multi-Card Unlock

In this mode, multiple groups of users have to swipe cards for an access control channel in an established sequence to unlock the door.

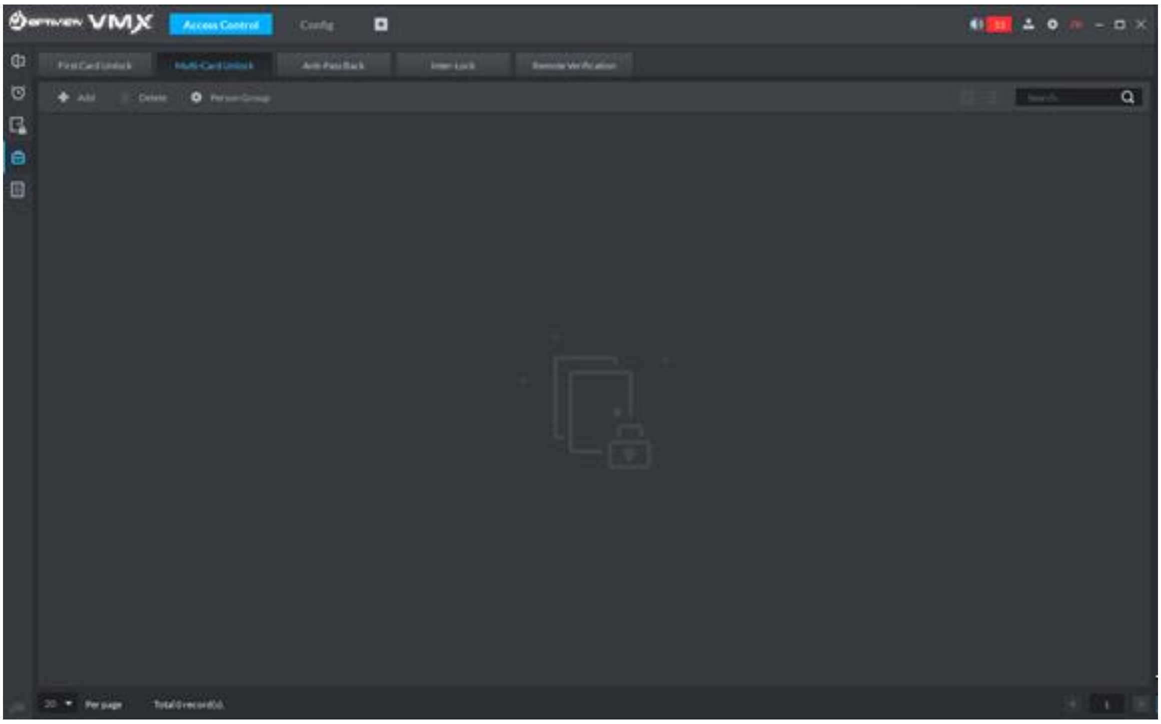
- One group can have up to 64 users.
- With Multi-Card Unlock enabled for an access control channel, it supports up to four groups of users being on site at the same time for verification. The total number of users

can be 64 at most, with up to five valid users.

Step 1 On the Access Control interface, click and select **Multi-card Unlock**.

The **Multi-Card Unlock** interface is displayed. See Figure 3-347.

Figure 3-347 Multi-card unlock

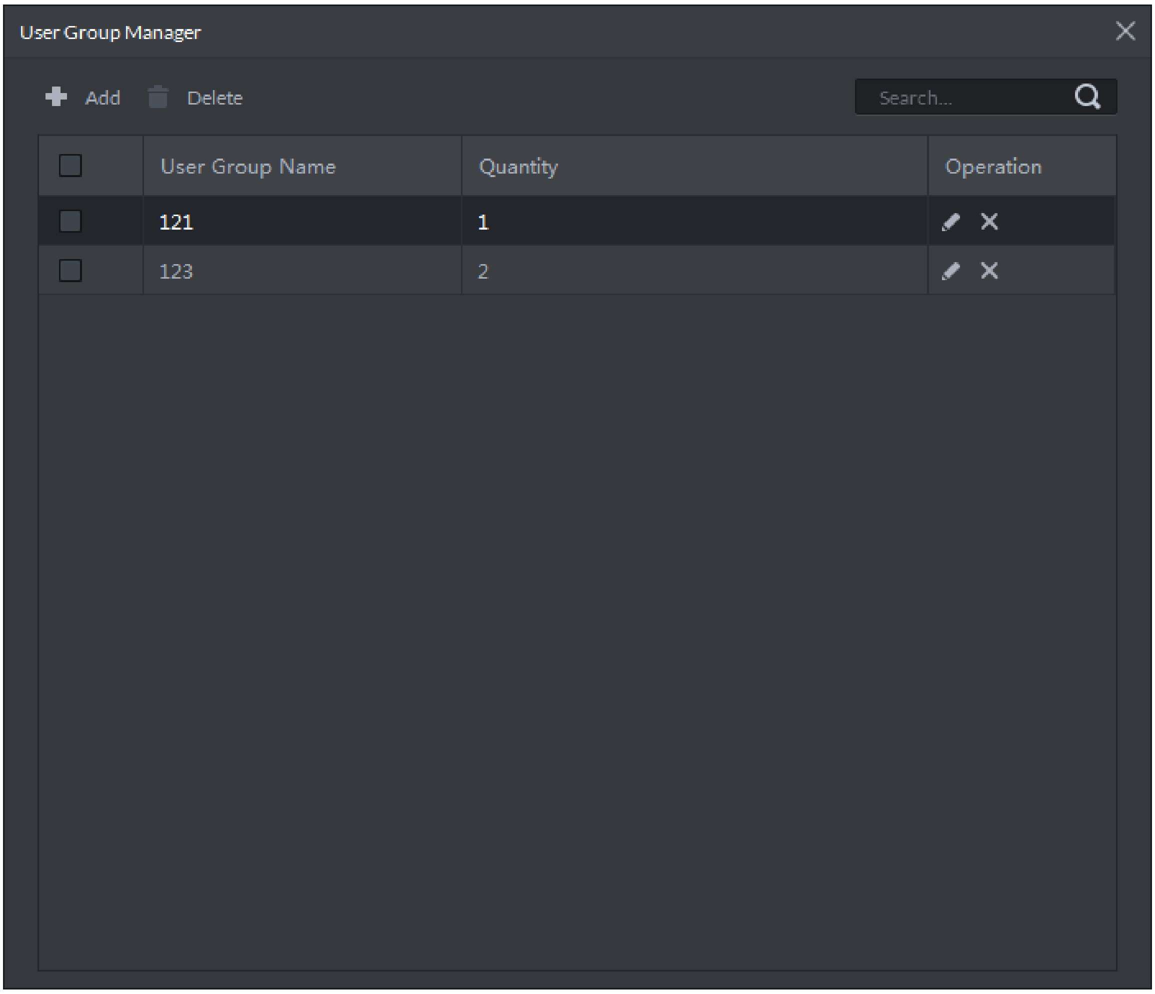

VMX
Access Control
Config
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Person Group
Search
20
Per page
Total 0 record(s).
1

Step 2 Add user group.

1) Click **Person Group**.

The **User Group Manager** interface is displayed. See Figure 3-348.

Figure 3-348 User group manager

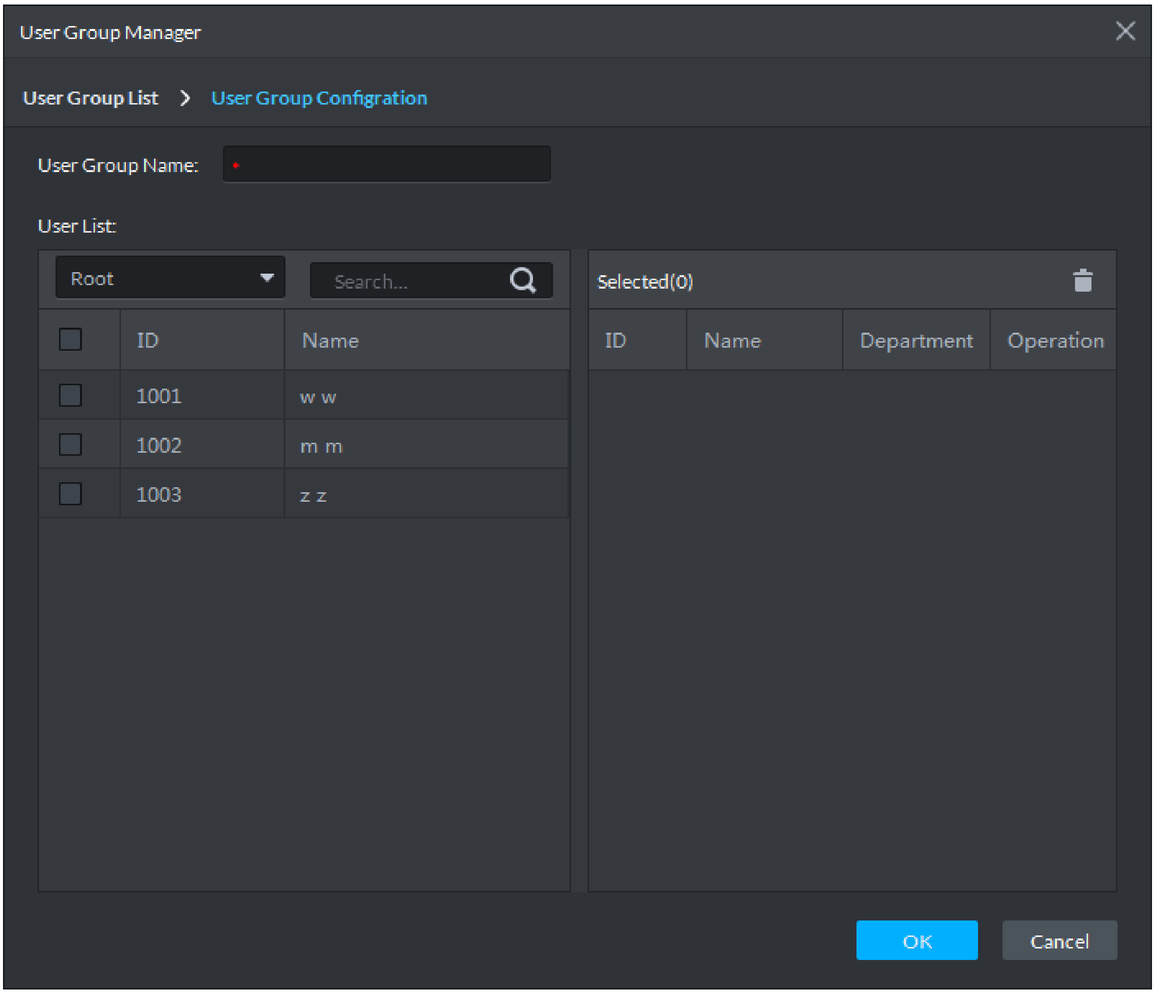

User Group Manager
Add
Delete
Search...

☐	User Group Name	Quantity	Operation
☐	121	1	✎ ✕
☐	123	2	✎ ✕

2) Click **Add**.

The **User Group Manager** interface is displayed. See Figure 3-349.

Figure 3-349 User group config


User Group Manager
User Group List
User Group Configration
User Group Name:
User List:
Root
Search...
Selected(0)
OK
Cancel

☐	ID	Name
☐	1001	w w
☐	1002	m m
☐	1003	z z

ID	Name	Department	Operation

3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 64 users.

   The system displays the user group information.

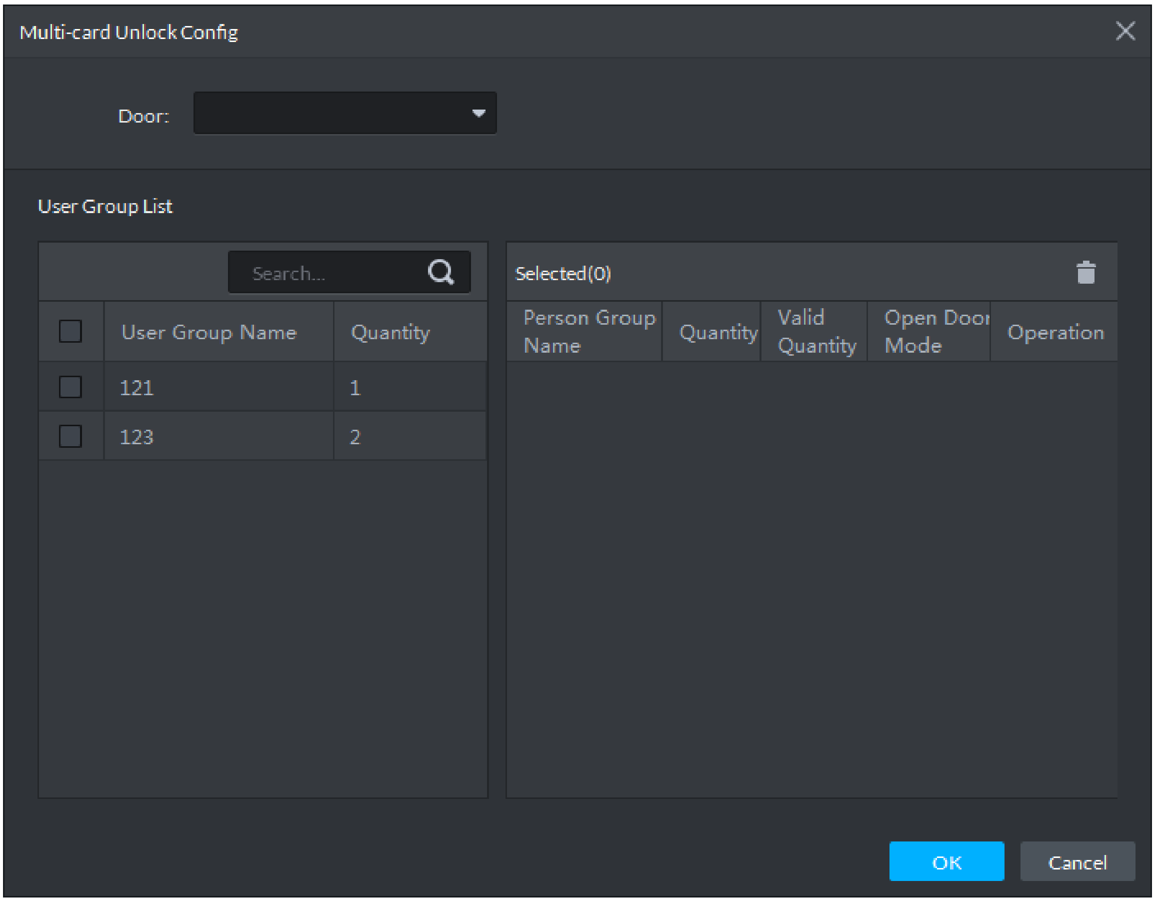
4) Click ☒ in the upper right corner of the **User Group Manager** interface.

Step 3 Configure **Multi-Card Unlock**.

1) Click **Add**.

   The **Multi-card Unlock Config** interface is displayed. See Figure 3-350.

Figure 3-350 Configure user group


Multi-card Unlock Config
Door:
User Group List
Search...
Selected(0)
OK
Cancel

☐	User Group Name	Quantity
☐	121	1
☐	123	2

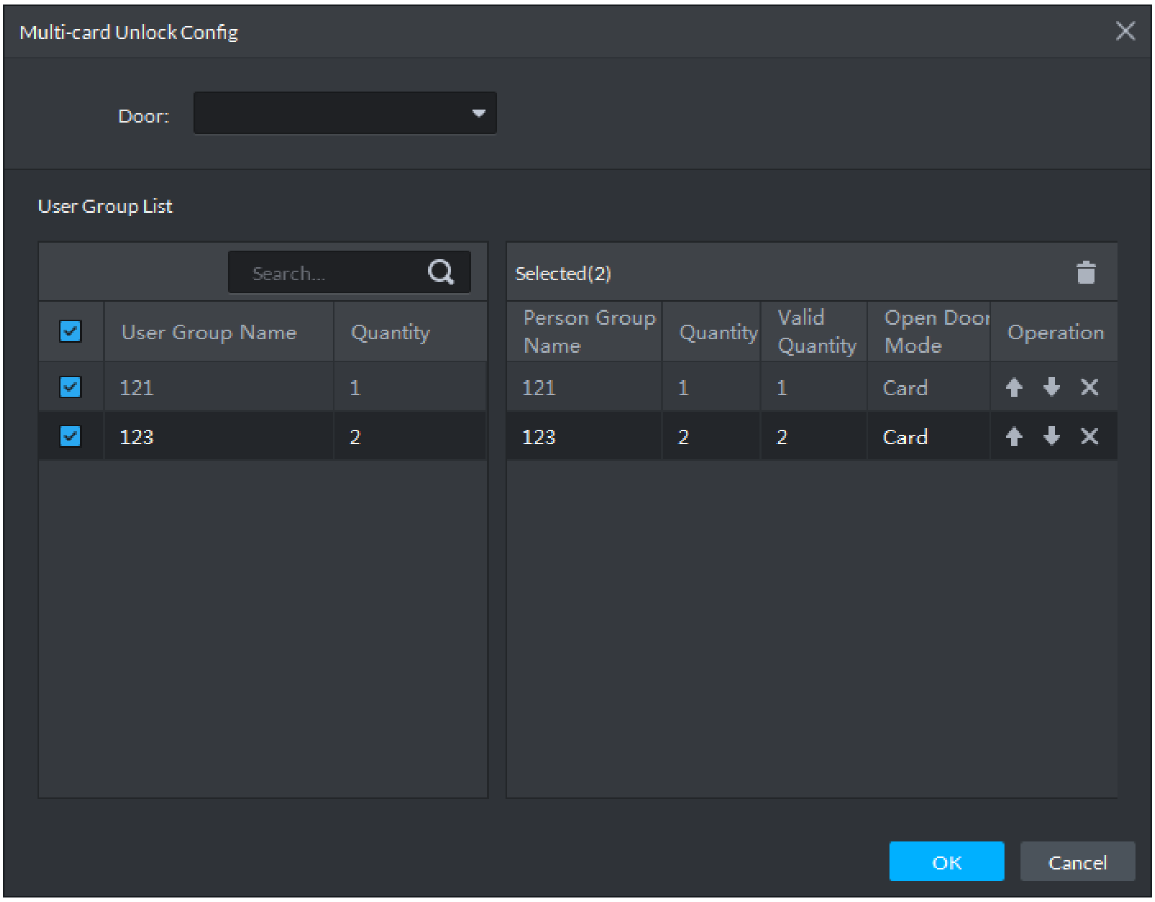
Person Group Name	Quantity	Valid Quantity	Open Door Mode	Operation

2) Select the door to set up Multi-Card Unlock.

3) Select the user group. You can select up to four groups.

The system displays the user group information. See Figure 3-351.

Figure 3-351 Select user group


Multi-card Unlock Config
Door:
User Group List
Search...
Selected(2)
OK
Cancel

☑	User Group Name	Quantity
☑	121	1
☑	123	2

Person Group Name	Quantity	Valid Quantity	Open Door Mode	Operation
121	1	1	Card	⬆ ⬇ ✕
123	2	2	Card	⬆ ⬇ ✕

4) Fill in the **Valid Quantity** for each group to be on site and the **Open Door Mode**.

Click ⬆ or ⬇ to adjust the user sequence for each group to unlock the door.

The valid quantity refers to the number of users in each group that must be on site to swipe their cards.

5) Click **OK**.

The system displays the Multi-Card Unlock information. See Figure 3-352.

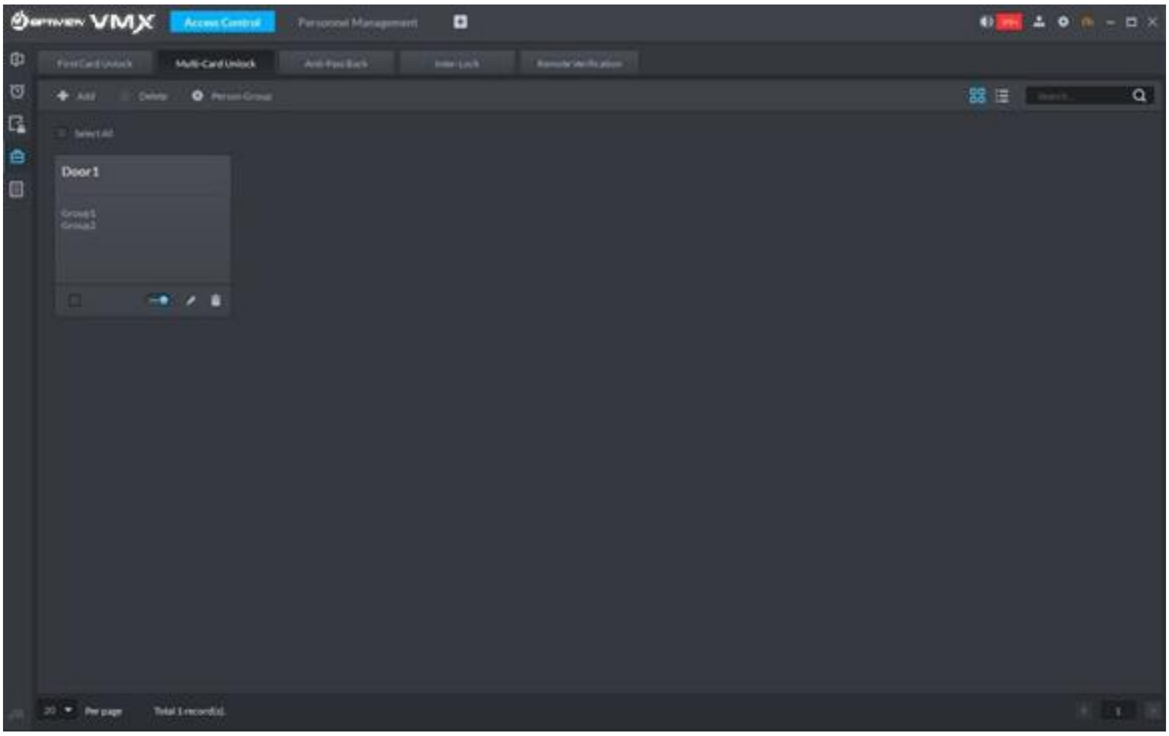

VMX
Access Control
Personnel Management
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Person Group
Select All
Door 1
Group1
Group2
20
Per page
Total 1 record(s).
1

Figure 3-352 Multi-card unlock

Step 4 Click.

The icon changing into indicates Multi-Card Unlock is enabled.

3.17.5.3 Anti-Pass Back

The Anti-Pass Back feature refers to that a user entering through a door group by verification must exit from the same door group by verification. One entry swipe must have a matching exit swipe. A non-verified user following a verified one to enter cannot pass the verification when taking exit; a non-verified user following a verified one to exit cannot pass verification when taking entry again. The door cannot be unlocked by swiping cards until the reset period on the A&C Central Controller expires.

Step 1 On the **Access Control** interface, click and select **Anti-pass Back**

The **Anti-Pass Back** interface is displayed. See Figure 3-353.

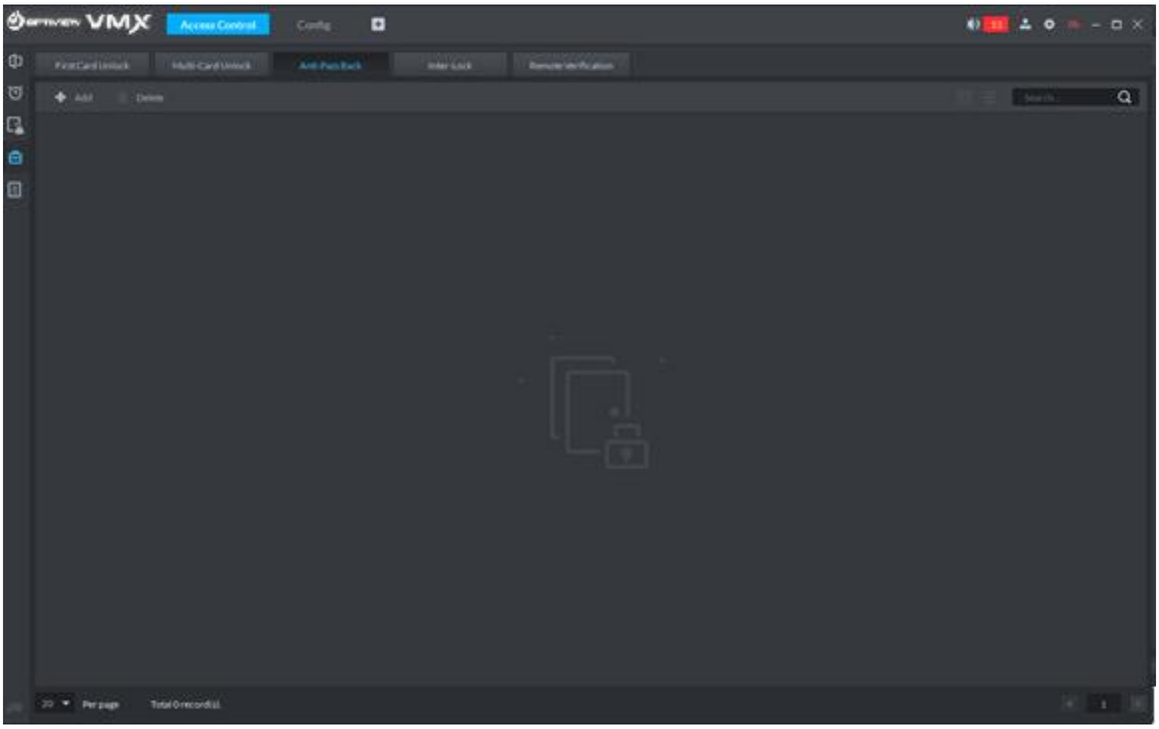
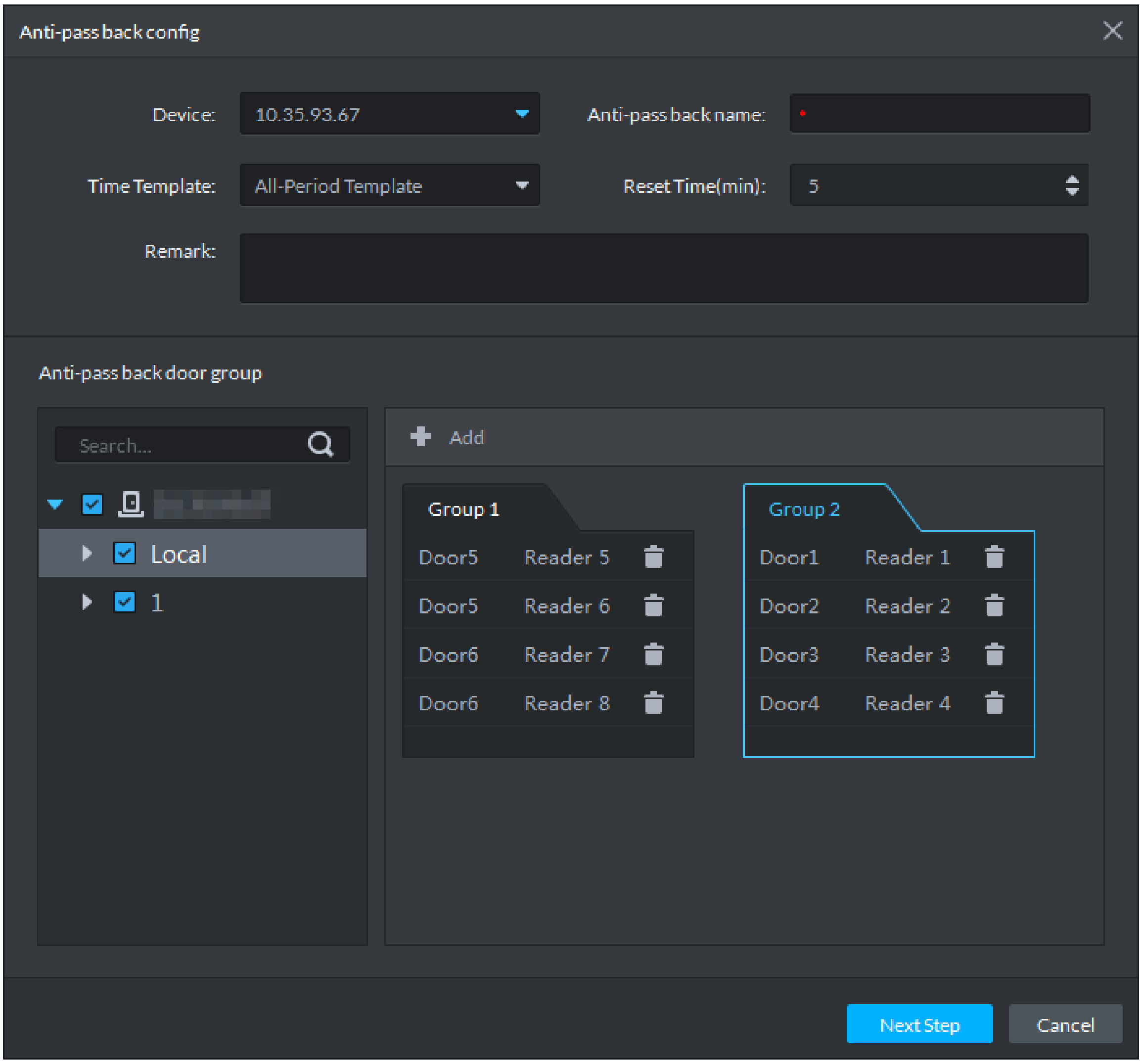

VMX
Access Control
Config
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Search...
20
Per page
Total 0 record(s)

Figure 3-353 Anti-pass back

Step 2 Click **Add**.

The **Anti-pass back config** interface is displayed. See Figure 3-354.

Figure 3-354 Anti-pass back config



Device: 10.35.93.67

Anti-pass back name:

Time Template: All-Period Template

Reset Time(min): 5

Remark:

Group 1

Door5	Reader 5
Door5	Reader 6
Door6	Reader 7
Door6	Reader 8

Group 2

Door1	Reader 1
Door2	Reader 2
Door3	Reader 3
Door4	Reader 4

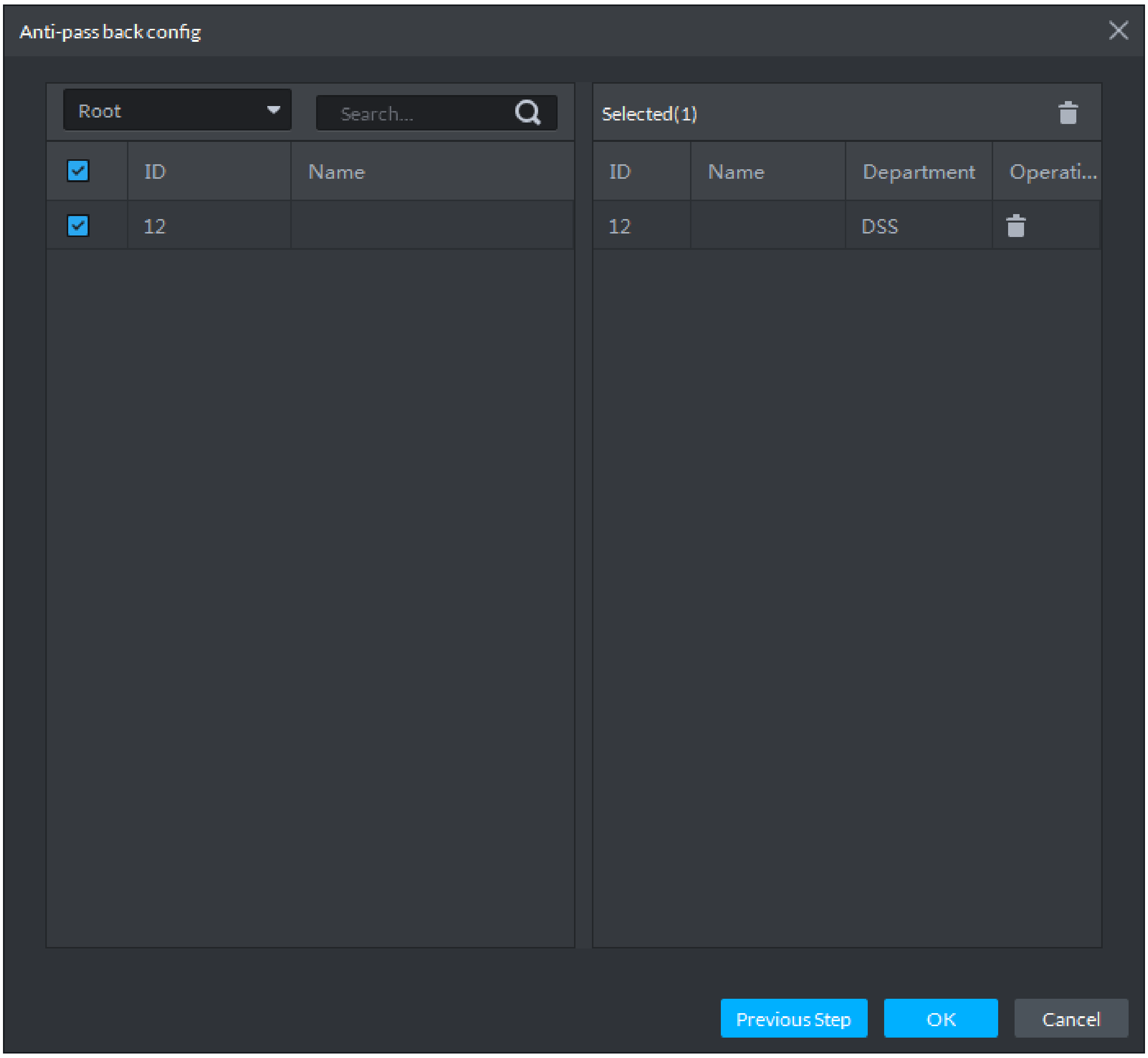
Step 3 Configure the anti-pass back parameters and click **Next Step**. For details of the parameters, see Table 3-56.

The system displays the user selection information. See Figure 3-355.

Table 3-56

Parameter	Description	
Device	You can select the device to configure the anti-pass back rules.	
Anti-pass back name	You can customize the name of an anti-pass back rule.	
Reset Time(min)	The access card becomes invalid if an anti-pass back rule is violated. The reset time is the invalidity duration.	🕮 When the selected device is a multi-door controller, you must set up these parameters.
Time Template	You can select the time periods to implement the anti-pass back rules.	
Remark	Note info.	
Group X 🕮 X is a number.	The group sequence here is the sequence for swiping cards. You can add up to 16 readers for each group. Each group can swipe cards on any of the readers.	

Figure 3-355 Select user


Anti-pass back config
Root
Search...
Selected(1)
Previous Step
OK
Cancel

☑	ID	Name
☑	12	

ID	Name	Department	Operati...
12		DSS	🗑

Step 4 Select users and click **OK**.

The system displays the anti-pass back information. See Figure 3-356.

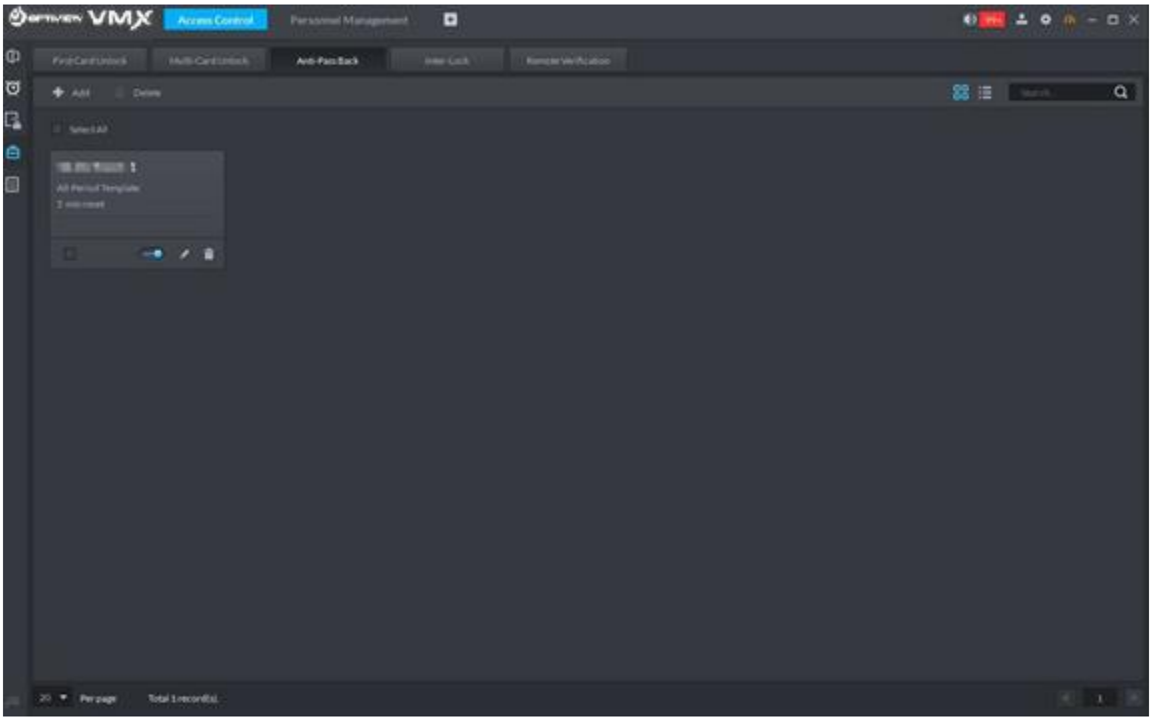

VMX
Access Control
Personnel Management
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Select All
All Period Template
Per page
Total 1 record(s)

Figure 3-356 Anti-pass back

Step 5 Click .

The icon changing into indicates Anti-Pass Back is enabled.

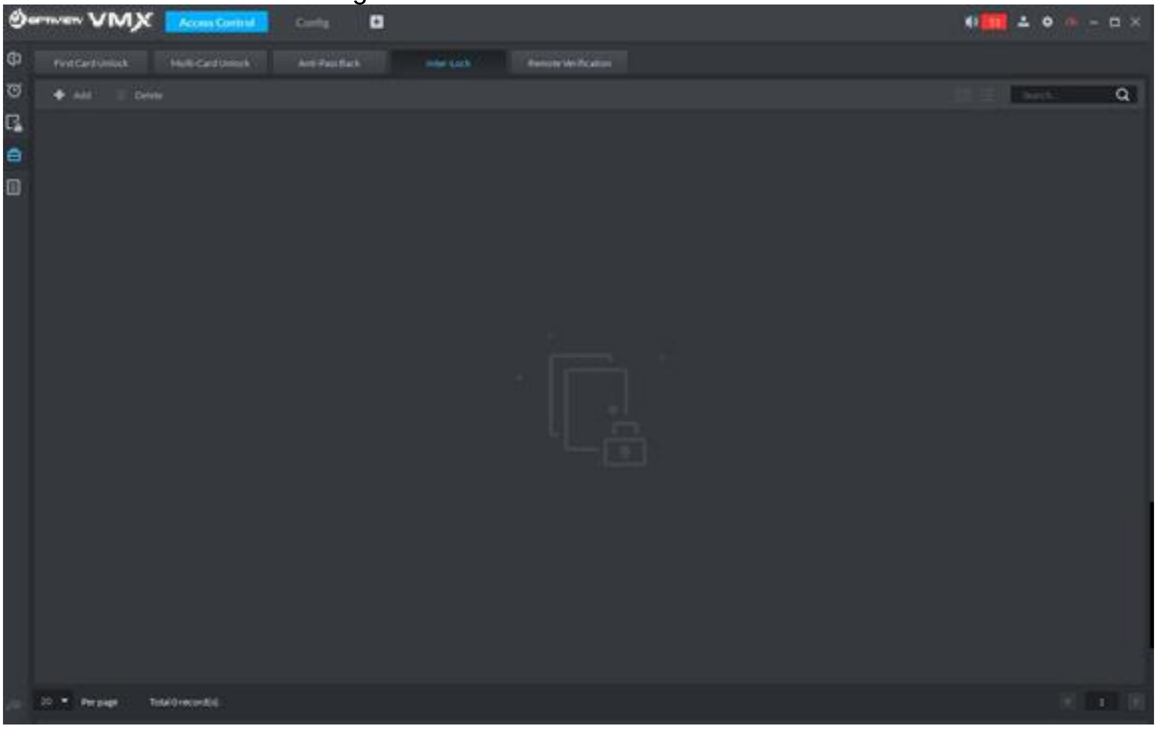
3.17.5.4 Inter-door Lock

A regular access controller employs inter-lock within the group. When one of the access control channels is opened, other corresponding channels are closed. To open one of the access control channels (under normal access control), other corresponding access control channels must be closed; otherwise the door cannot be unlocked. The A&C Central Controller employs inter-group inter-lock, where the access control channels are independent of the inter-lock and can all be opened. However, whenever an access control channel in a group is opened, no channels of other groups can be opened. The configuration steps in this chapter are for an A&C Central Controller.

Step 1 On the **Access Control** interface, click and select **Inter-loc**k.

The **Inter-Lock** interface is displayed. See Figure 3-357.

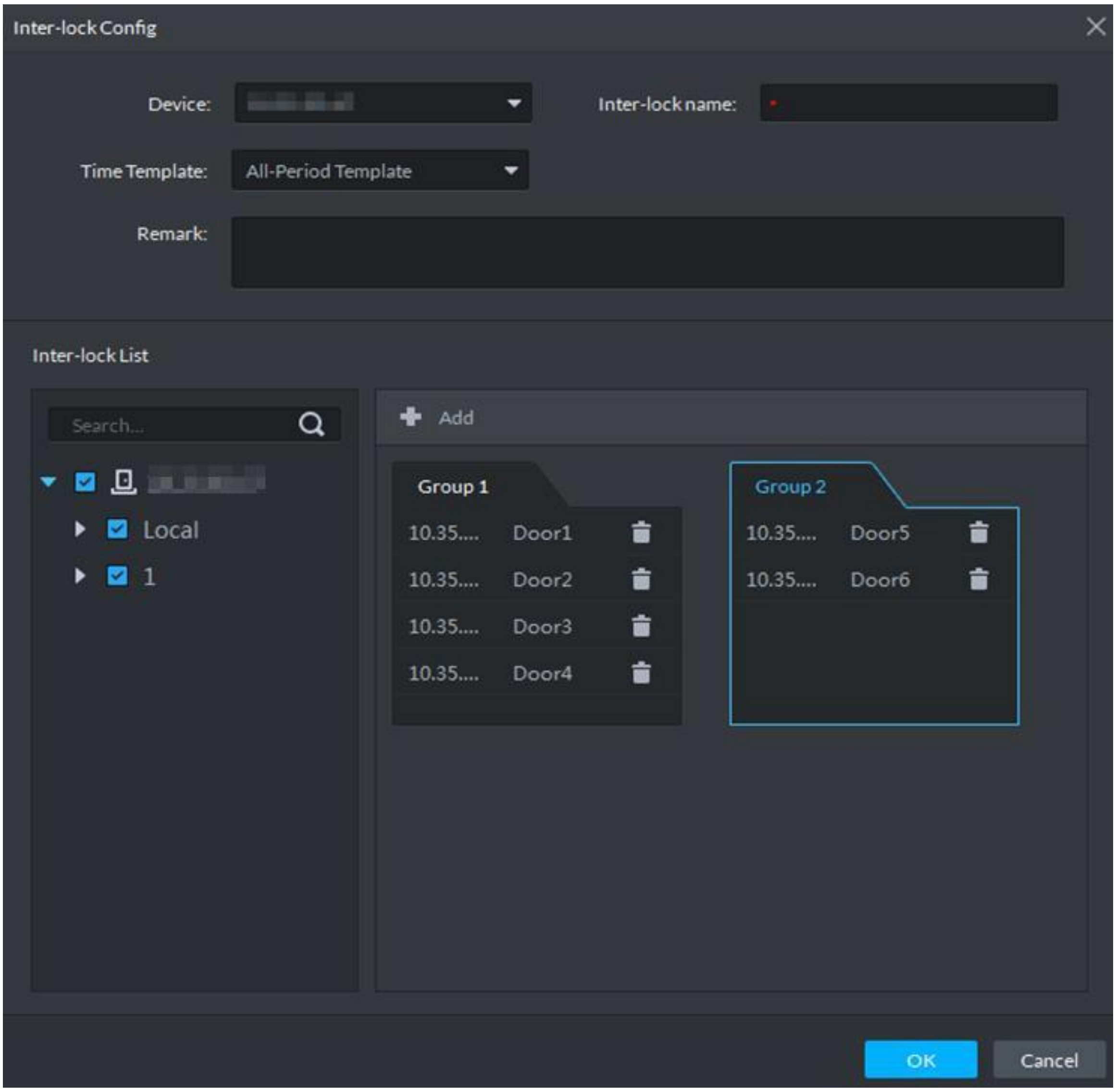
Figure 3-357 Inter-lock


VMX
Access Control
Config
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Search...
20
Per page
Total 0 record(s)
1

Step 2 Click **Add**.

The **Inter-lock Config** interface is displayed. See Figure 3-358.

Figure 3-358 Inter-lock config



Time Template: All-Period Template

Group 1
10.35.... Door1
10.35.... Door2
10.35.... Door3
10.35.... Door4

Group 2
10.35.... Door5
10.35.... Door6

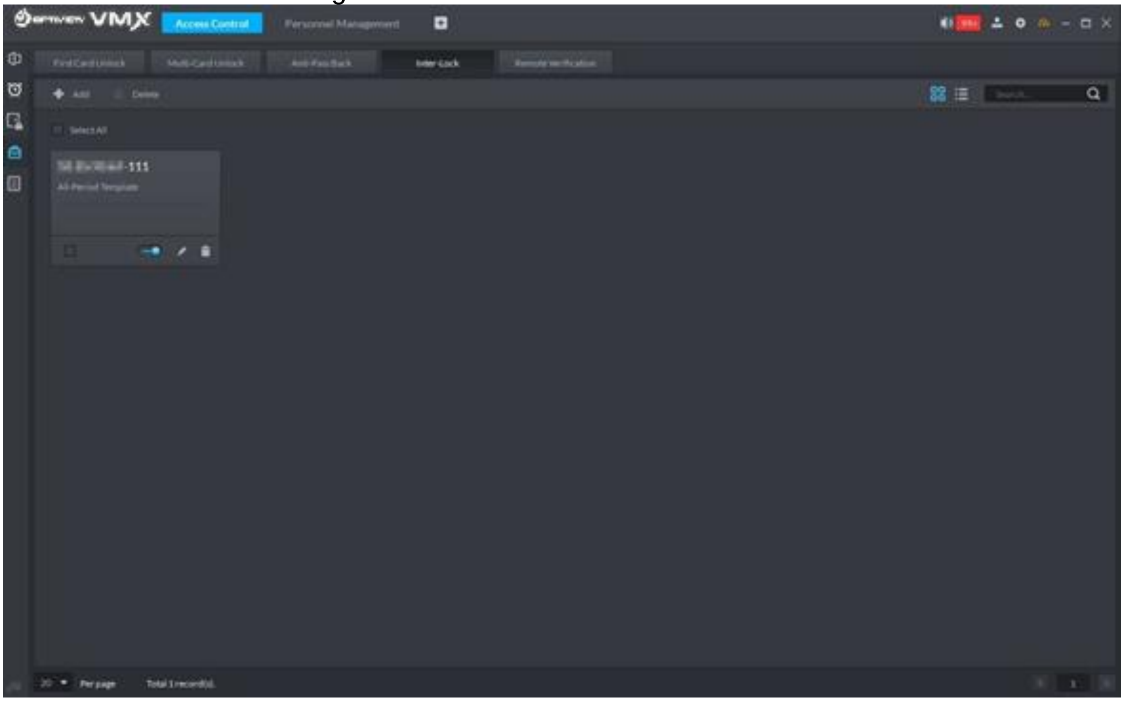
Step 3 Configure inter-lock parameters and click **OK**. For details of the parameters, see Table 3-57.

The system displays the inter-lock information. See Figure 3-359.

Table 3-57 Inter-lock config

Parameter	**Description**	
Device	You can select the device to set up inter-lock.	
Inter-lock name	You can customize the name of the inter-lock rule.	
Time Template	You can select the time period to implement inter-lock.	When the selected device is a multi-door controller, you must set up these parameters.
Remark	Note info.	
Group X X is a number.	You can set up inter-lock across different door groups. If a door in Group 1 is opened, no doors can be opened in Group 2 until all doors in Group 1 are closed. Supports up to 16 door groups, with up to 16 doors in each group.	

Figure 3-359 Inter-lock list


VMX
Access Control
Personnel Management
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Search...
Select All
-111
All-Period Template
20
Per page
Total 1 record(s).
1

Step 4 Click .

The icon changing into ![] indicates Inter-Lock is enabled.

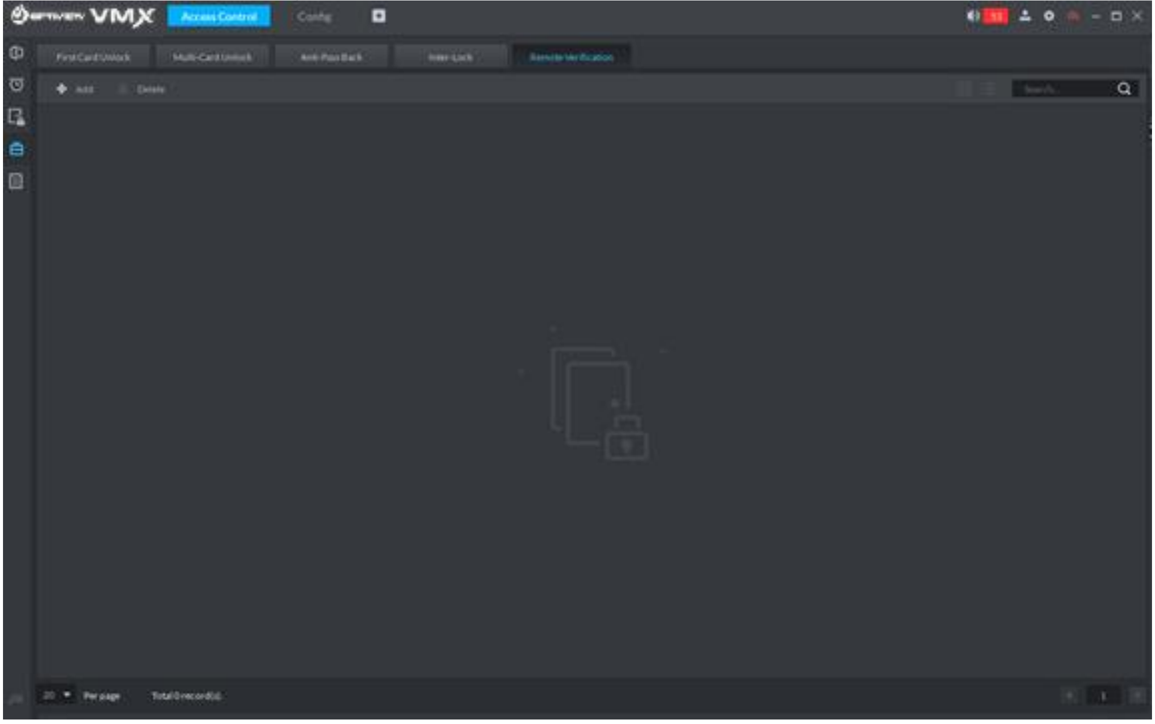
3.17.5.5 Remote Verification

For devices with remote verification, when users unlock the doors with card, fingerprint, or password in the specified time period, it must be confirmed on the platform client before the access controller can be opened.

Step 1 On the **Access Control** interface, click ![] and select **Remote Verification**.

The **Remote Verification** interface is displayed. See Figure 3-360.

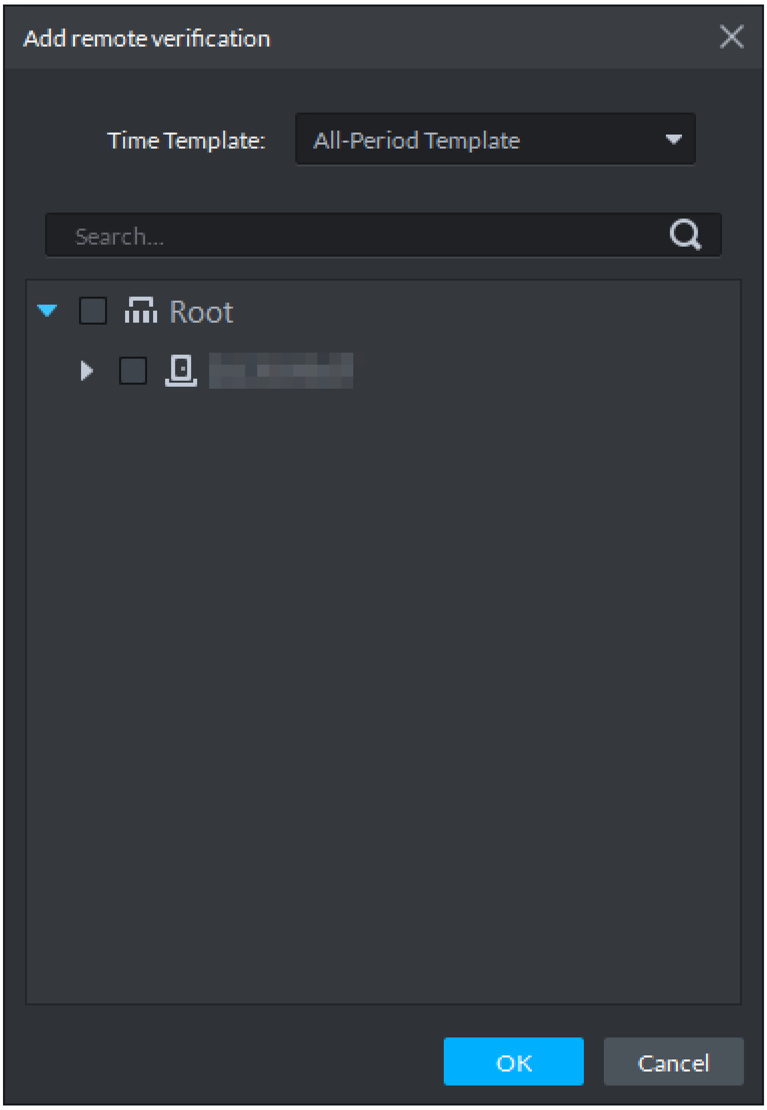
Figure 3-360 Remote verification


VMX
Access Control
Config
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter-Lock
Remote Verification
Add
Delete
Search
20
Per page
Total 0 record(s)
1

Step 2 Click **Add**.

The **Add remote verification** interface is displayed. See Figure 3-361.

Figure 3-361 Add remote verification

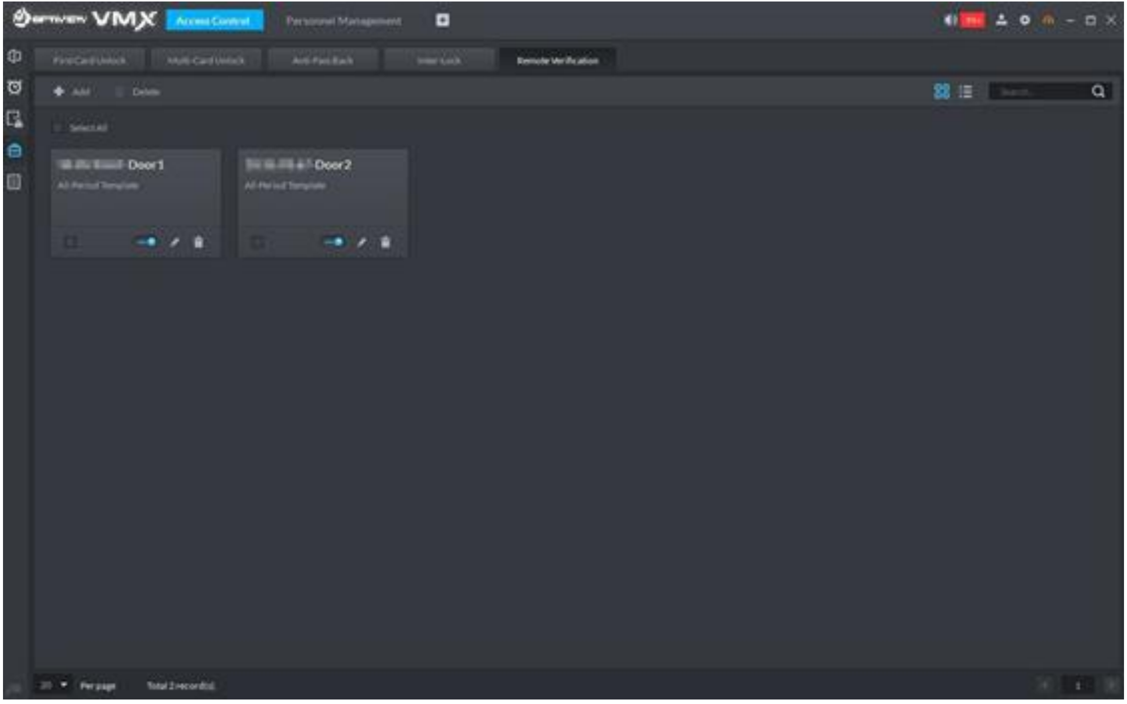

Add remote verification
Search...
☐ Root
☐ [redacted]
OK
Cancel

Time Template: All-Period Template

Step 3 Select **Time Template** and access control channel, and click **OK**.

The system displays the remote verification information. See Figure 3-362.

Figure 3-362 Remote verification list


VMX
Access Control
Personnel Management
First Card Unlock
Multi-Card Unlock
Anti-Pass Back
Inter Lock
Remote Verification
Add
Delete
Select All
Door1
All Period Template
Door2
All Period Template
20
Per page
Total 2 record(s)

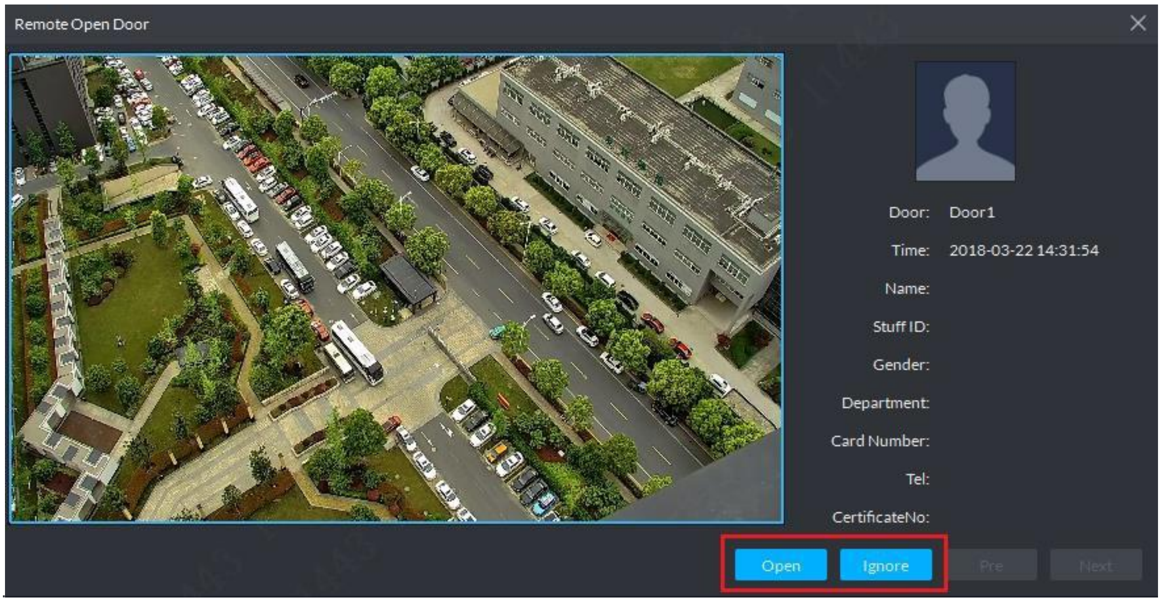
Step 4 Click .

The icon changing into indicates First Card Unlock is enabled.

Step 5 After the setup, door unlocking by card, fingerprint, or password that takes place in the corresponding access control channel triggers a popup on the client. See Figure 3-363.

Step 6 You can choose to unlock the door or ignore it by clicking the corresponding button, and the popup automatically disappears.

Figure 3-363 Remote open door


Remote Open Door
Open
Ignore
Pre
Next

Door: Door1
Time: 2018-03-22 14:31:54
Name:
Stuff ID:
Gender:
Department:
Card Number:
Tel:
CertificateNo:

3.17.6 Setting Record Plan

Video before and after alarm can be stored only when record storage plan is configured, and the platform can play video 10 seconds before and after event alarm. If you want to set record storage plan, see **3.2.5 Setting Record Plan**

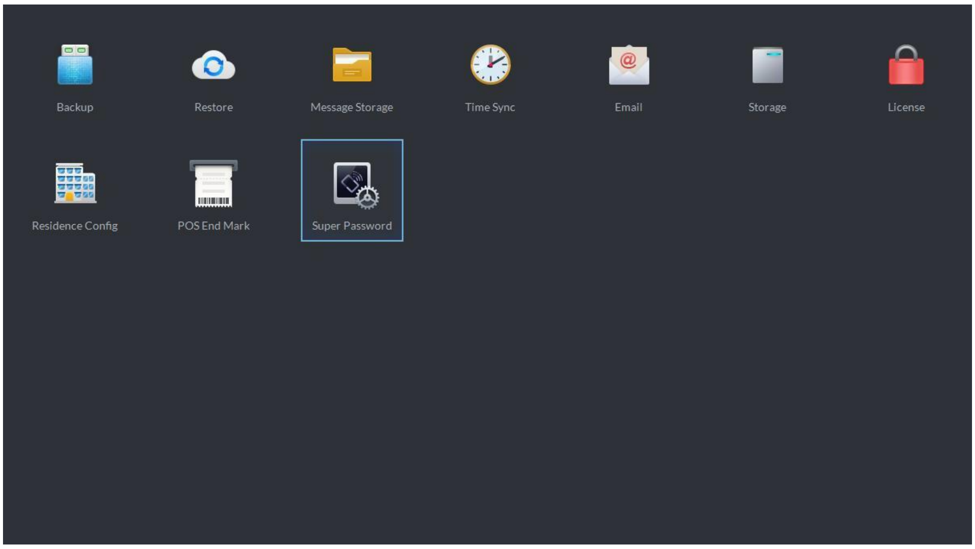
3.17.7 Configuring Super Password

2nd generation access control supports using super password to open door. You only need to enter super password to open door.

Step 1 On client homepage, click **Config**.

The system displays **Config** interface, see Figure 3-364.

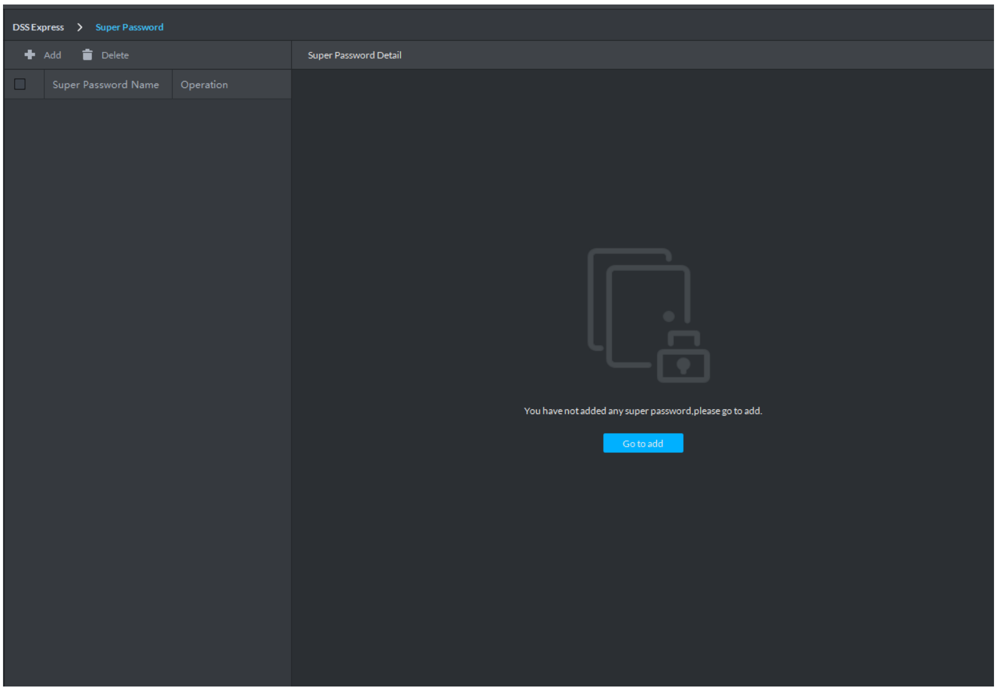
Figure 3-364 Config interface


Backup
Restore
Message Storage
Time Sync
Email
Storage
License
Residence Config
POS End Mark
Super Password

Step 2 Click Super Password.

The system displays Super Password interface, see Figure 3-365.

Figure 3-365 Super password

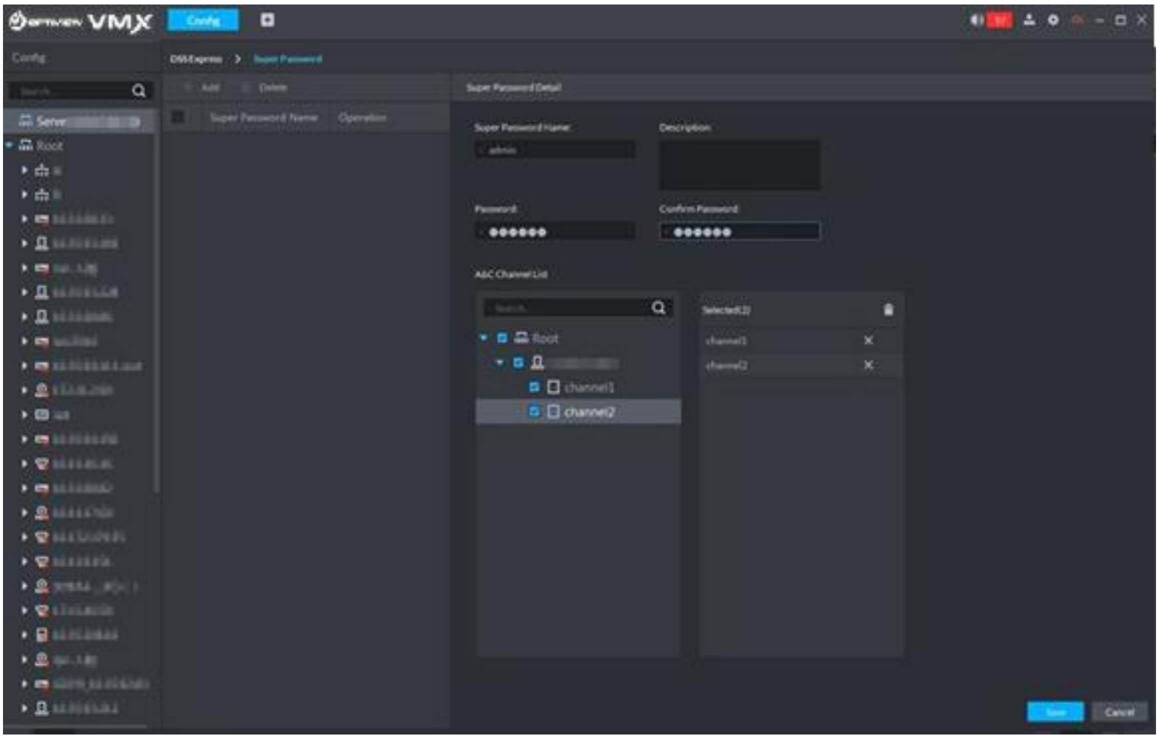

DSS Express
Super Password
Add
Delete
Super Password Detail
☐
Super Password Name
Operation
Go to add

You have not added any super password,please go to add.

Step 3 Click **Add**.

The system displays interface of adding super password, see Figure 3-366

Figure 3-366 Add super password


VMX
Config
Config
DSS Express > Super Password
Add
Delete
Super Password Name
Operation
Super Password Detail
Root
A&C Channel List
Selected(2)
Save
Cancel

Super Password Name: admin

Description:

Password: ●●●●●●

Confirm Password: ●●●●●●

- Root
  - channel1
  - channel2

Selected(2): channel1, channel2

Step 4 After setting super password, you can select AC channel (only supported by 2nd generation device), click **Save** and complete config.

3.17.8 Access Control Application

You can control lock, unlock and view related video and event info on console, and enter door config interface.

3.17.8.1 Viewing Video of Bound Channel

When adding access control devices, if you have already bound a video channel to the channel, you can view the real-time videos of the bound video channels on the console. To bind video channels, see **3.17.1 Adding Access Control**

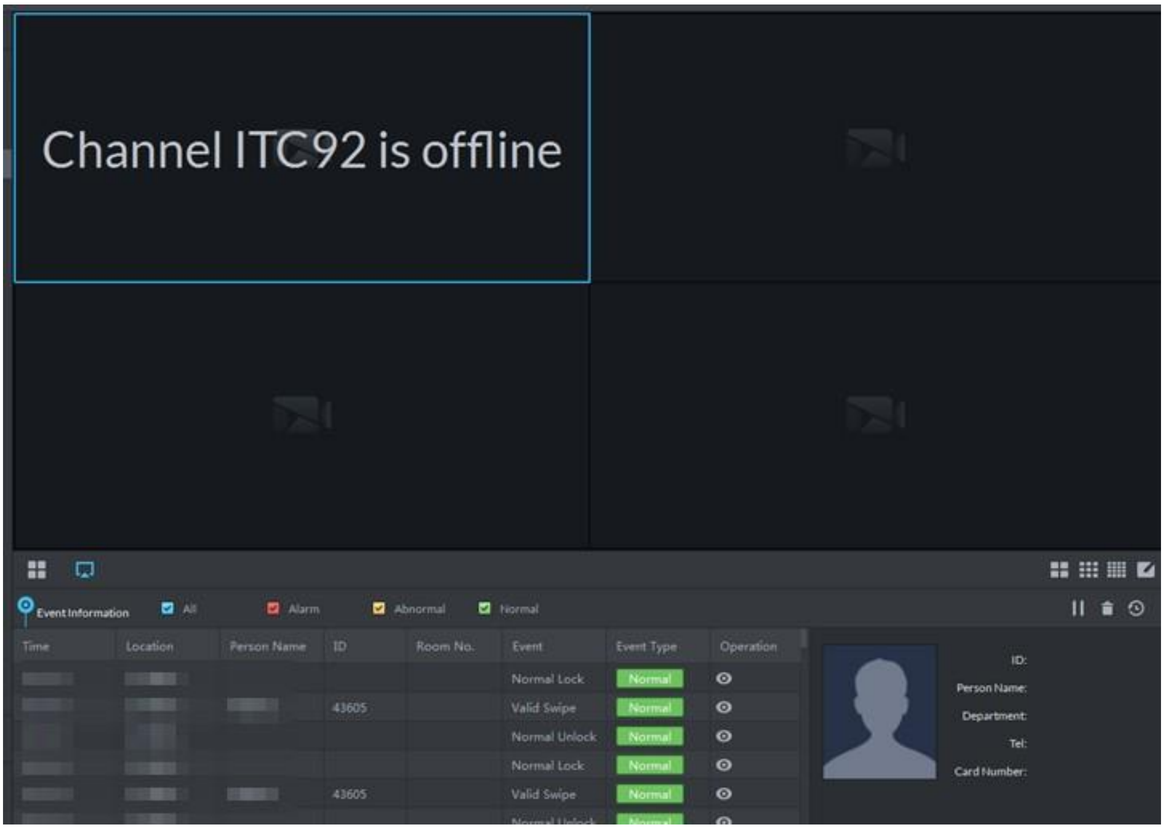
Step 1 On client homepage, click **Access Control**.

The system displays **Access Control** interface.

Step 2 Click .

The system displays **Console** interface, see Figure 3-367.

Figure 3-367 Console



Time	Location	Person Name	ID	Room No.	Event	Event Type	Operation
[redacted]	[redacted]				Normal Lock	Normal	👁
[redacted]	[redacted]	[redacted]	43605		Valid Swipe	Normal	👁
[redacted]	[redacted]				Normal Unlock	Normal	👁
[redacted]	[redacted]				Normal Lock	Normal	👁
[redacted]	[redacted]	[redacted]	43605		Valid Swipe	Normal	👁

ID:
Person Name:
Department:
Tel:
Card Number:

Step 3 View related video of AC channel.

- On the right side of the console interface, click in the access control channel list. The system displays videos in real time. See Figure 3-368
- Click on the console interface. The system displays the video interface. Drag the access control channel on the left side of the screen to the live view interface on the right side. The system displays videos in real time. See Figure 3-368

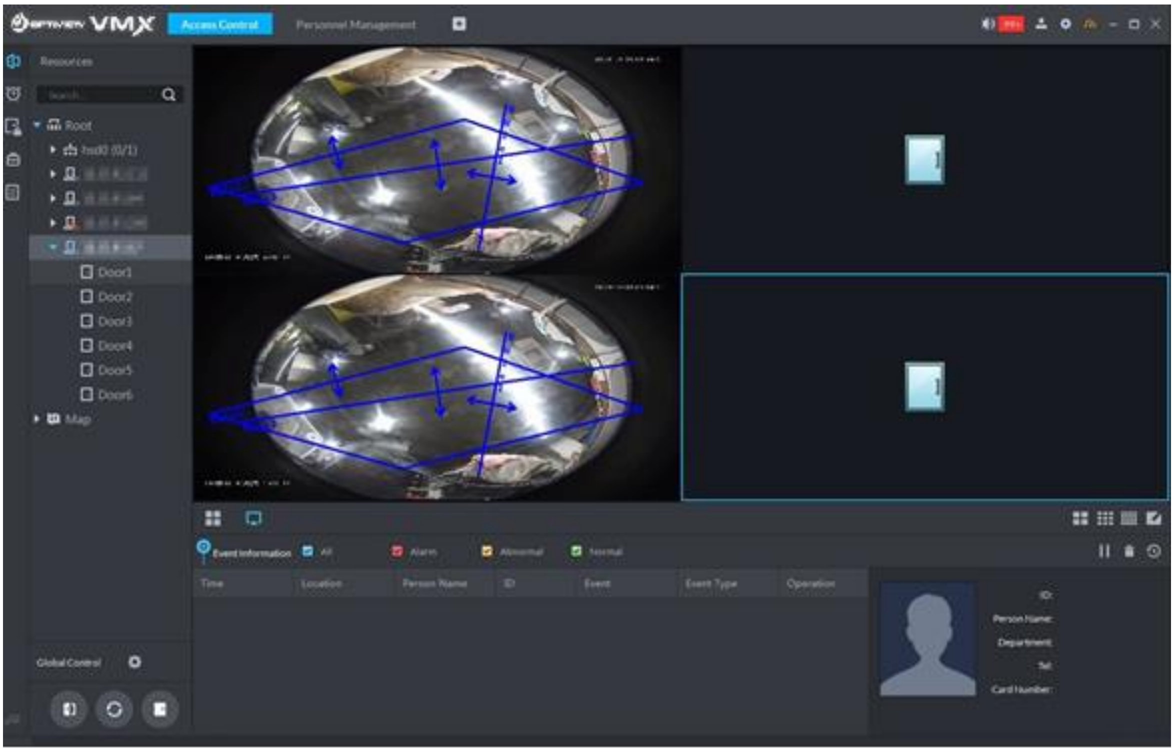

VMX
Access Control
Personnel Management
Resources
Search...
Root
hsd0 (0/1)
Door1
Door2
Door3
Door4
Door5
Door6
Map
Global Control
Event Information
All
Alarm
Abnormal
Normal
Time
Location
Person Name
ID
Event
Event Type
Operation
ID:
Person Name:
Department:
Tel:
Card Number:

Figure 3-368 Linked channel video

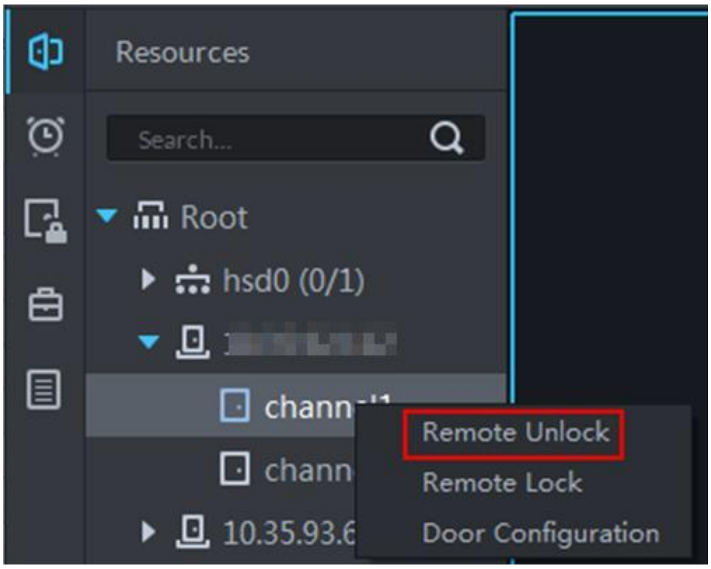
3.17.8.2 Manual Unlock

In addition to Always Open or linked unlock in specified periods, the console also supports unlocking by manually controlling the access control channel. After unlock, the door automatically locks up after a specified time period (5s by default, and 10s in this example) set up in Door Config.

You can unlock the door in the following ways:

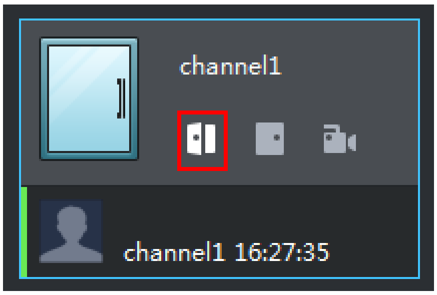
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Unlock** in the popup menu. See Figure 3-369. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as .

Figure 3-369 Remote unlock (1)


Resources
Search...
Root
hsd0 (0/1)
[redacted]
chann
chann
10.35.93.6
Remote Unlock
Remote Lock
Door Configuration

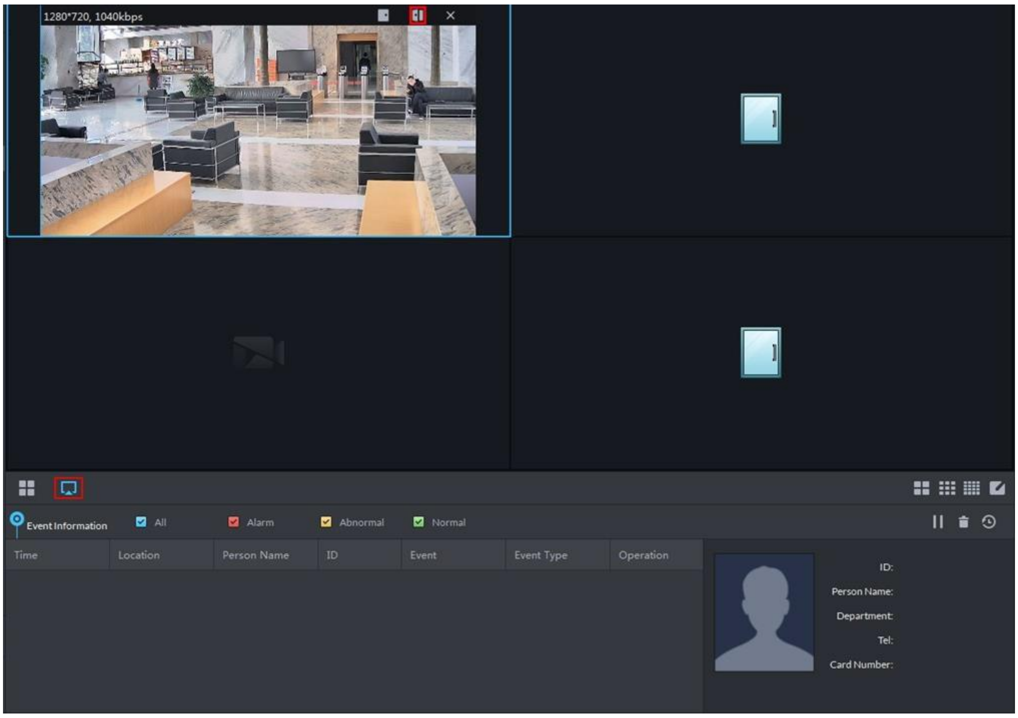
- Click ◫ on the door channel interface to unlock the door. See Figure 3-370. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as ◫

Figure 3-370 Unlock (2)


channel1
channel1 16:27:35

- When viewing videos bound to the channel, click ◫ on the video interface to unlock the door. See Figure 3-371.

Figure 3-371 Unlock(3)


1280*720, 1040kbps
Event Information
All
Alarm
Abnormal
Normal
Time
Location
Person Name
ID
Event
Event Type
Operation
ID:
Person Name:
Department:
Tel:
Card Number:

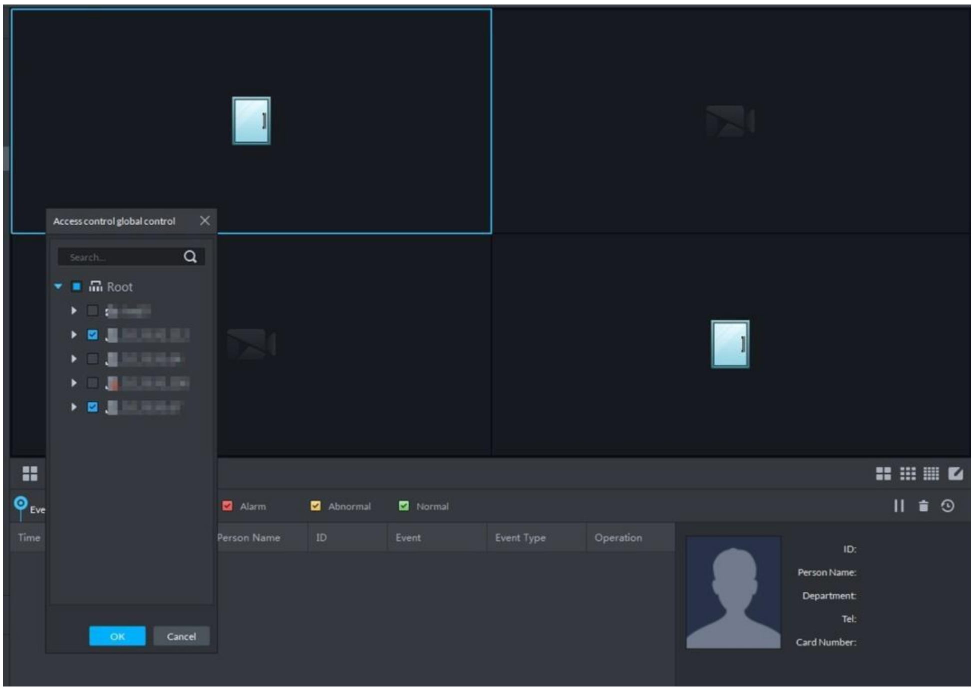
- Temporary Always Open of multiple doors

  Select a door channel through global control and you can set the door to be Always Open. Recovery to normal status after unlocking requires manual operations.

Step 1 Click ⚙ on the bottom left of the console interface of the Access Control module.

Step 2 The **Access control global control** interface is displayed. See Figure 3-372.

Figure 3-372 Global control


Access control global control
Search...
Root
Eve
Alarm
Abnormal
Normal
Time
Person Name
ID
Event
Event Type
Operation
ID:
Person Name:
Department:
Tel:
Card Number:
OK
Cancel

Step 3 Select an access control channel to be set to Always Open via global control, and click **OK**.

Step 4 Click **Always Open** on the bottom left of the interface.

The **Password Verification** interface is displayed.

Step 5 Input current user's password, and click **OK**.

Step 6 All the doors of the selected access control channels are set to Always Open. The status of all the doors in the access control channel list on the right side of the interface changes to open, as . The interface control changes from **Always Open** to **Recover**.

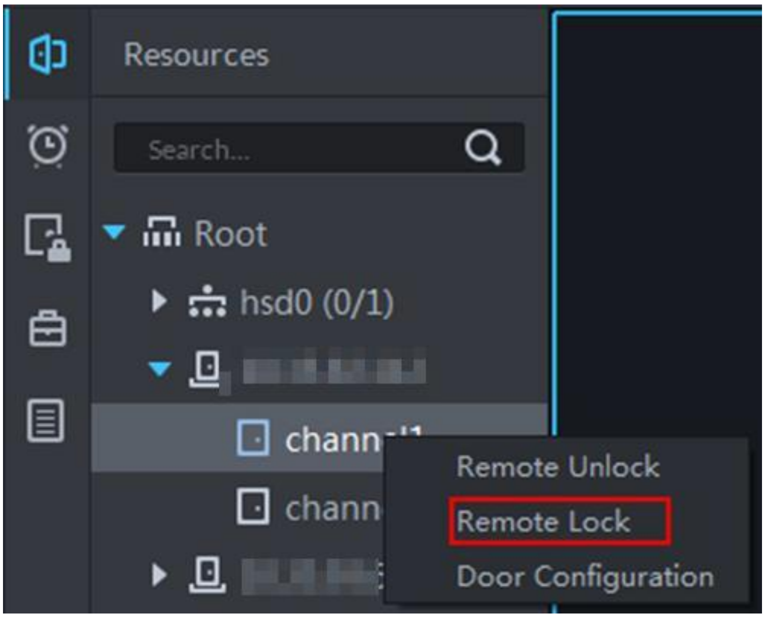
Click **Recover** and the doors return to normal status.

3.17.8.3 Manual Lock

In addition to Always Close or linked lock in specified periods, the console also supports locking by manually controlling the access control channel. You can lock the door in the following ways:

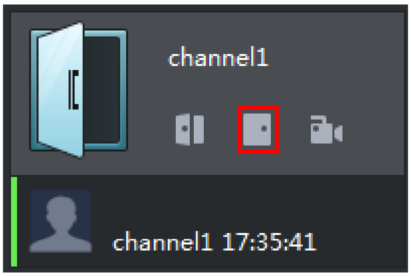
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Lock** in the popup menu. See Figure 3-373. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as .

Figure 3-373 Lock (1)


Resources
Search...
Root
hsd0 (0/1)
[redacted]
chann
chann
[redacted]
Remote Unlock
Remote Lock
Door Configuration

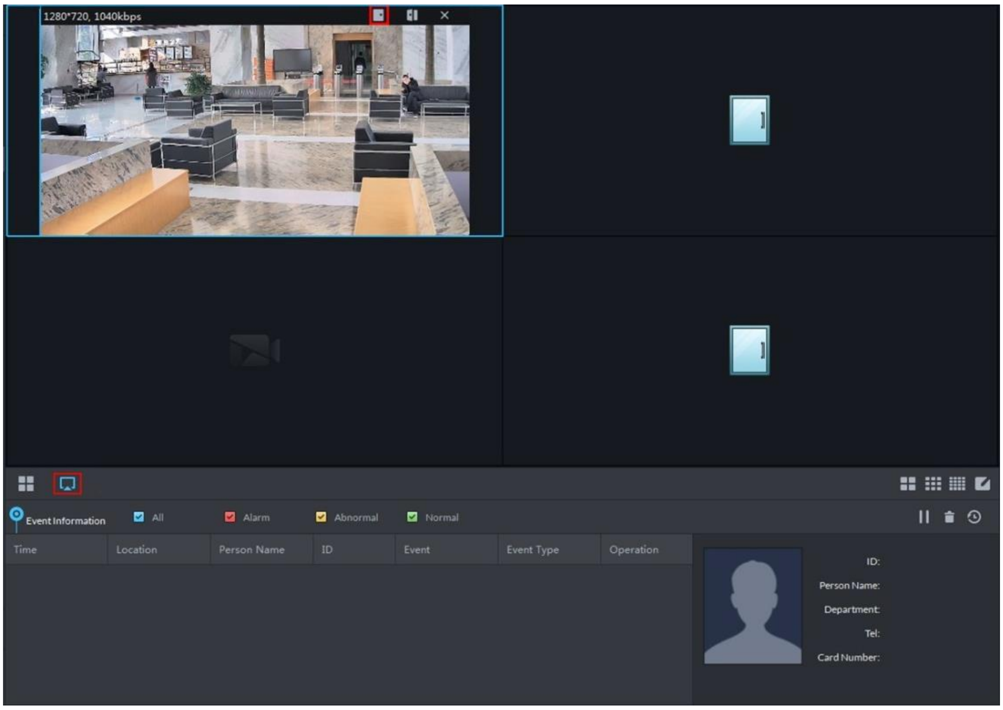
- Click on the door channel interface to lock the door. See Figure 3-374. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as .

Figure 3-374 Lock (2)


channel1
channel1 17:35:41

- When viewing videos bound to the channel, click on the video screen to lock the door. See Figure 3-375.

Figure 3-375 Lock (3)

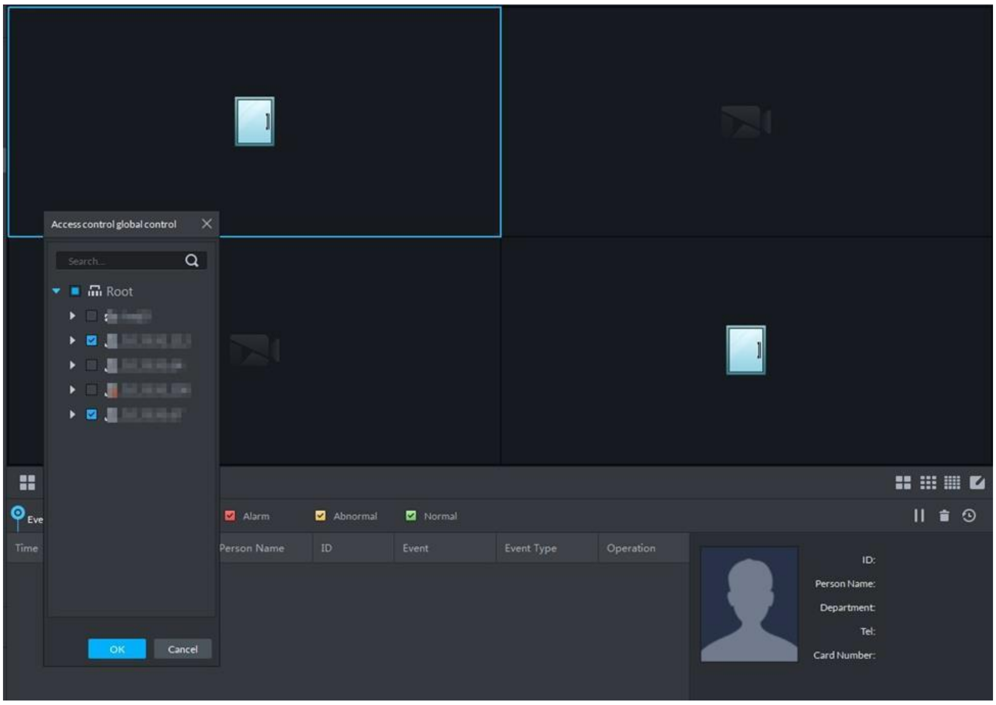

1280*720, 1040kbps
Event Information
All
Alarm
Abnormal
Normal
Time
Location
Person Name
ID
Event
Event Type
Operation
ID:
Person Name:
Department:
Tel:
Card Number:

- Temporary Always Open of multiple doors
  Select a door channel through global control and you can set the door to be Always Close. Recovery to normal status after locking requires manual operations.

Step 1 Click on the bottom left of the console interface of the Access Control module.

The **Access control global control** interface is displayed. See Figure 3-376.

Figure 3-376 Global control


Access control global control
Search...
Root
Eve
Time
Alarm
Abnormal
Normal
Person Name
ID
Event
Event Type
Operation
ID:
Person Name:
Department:
Tel:
Card Number:
OK
Cancel

Step 2 Select an access control channel to be set to Always Close via global control, and click **OK**.

Step 3 Click **Always Close** on the bottom left of the interface.

The **Password Verification** interface is displayed.

Step 4 Input current user's password, and click **OK**.

Step 5 All the doors of the selected access control channels are set to Always Close. The status of all the doors in the access control channel list on the right side of the interface changes to closed, as . The interface control changes from **Always Close** to **Recover**.

Click **Recover** and the doors return to normal status.

3.17.8.4 Viewing Event Details

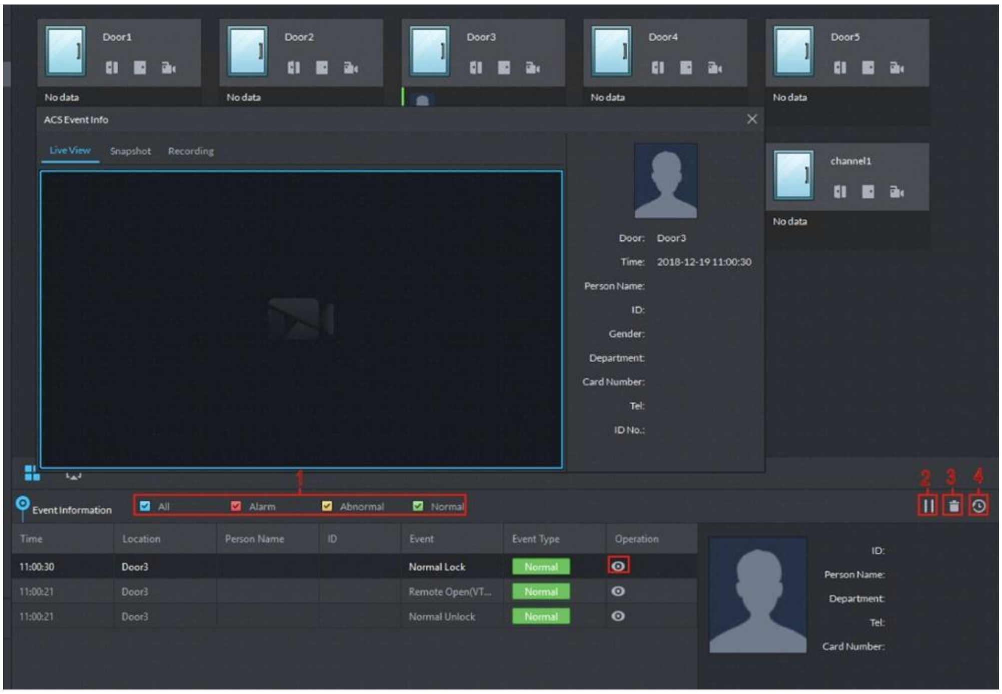
Supports viewing details of the events reported on door locking and unlocking, including: Event Info, Live View, Snapshot, and Recording.

- Live View is only available when a video channel is bound to the access control channel. To bind video channels, see Bind Resources.
- When snapshot and video recording require configuring event management, access control-related alarm devices are linked with the camera.
- The console displays all event information except for locking related info, including unlock, duress unlock, invalid swipe.

Step 1 In the event list below the console interface, click next to the event records.

Step 2 The **AC Event Info** interface is displayed. See Figure 3-377. See Table 3-58 for more descriptions on the controls.

Figure 3-377 Event detail


Door1
No data
Door2
No data
Door3
Door4
No data
Door5
No data
channel1
No data
ACS Event Info
Live View
Snapshot
Recording
Event Information
☑ All
☑ Alarm
☑ Abnormal
☑ Normal
1
2
3
4
ID:
Person Name:
Department:
Tel:
Card Number:

Door: Door3
Time: 2018-12-19 11:00:30
Person Name:
ID:
Gender:
Department:
Card Number:
Tel:
ID No.:

Time	Location	Person Name	ID	Event	Event Type	Operation
11:00:30	Door3			Normal Lock	Normal	
11:00:21	Door3			Remote Open(VT...	Normal	
11:00:21	Door3			Normal Unlock	Normal	

Table 3-58 Operation description

No.	Description
1	You can choose to view the events of certain event types. For instance, if you select **Normal**, the list only displays **normal** events.
2	- Click ⏸ to stop displaying reported event information. In this case, the interface no longer displays the reported new events. After clicking, the button changes to ▶. - Click ▶ to start refreshing reported event information. The interface does not display events during the stopping period. After clicking, the button changes to ⏸.
3	Clearing the events from the current event list, does not delete them from the log.
4	Click to jump to the **A&C Log** interface.

Step 3 Click the corresponding tab to view the live view, snapshots, and video recordings of the linked video channel.

3.17.9 Searching Access Control Log

You can view the reported AC log and device local log.

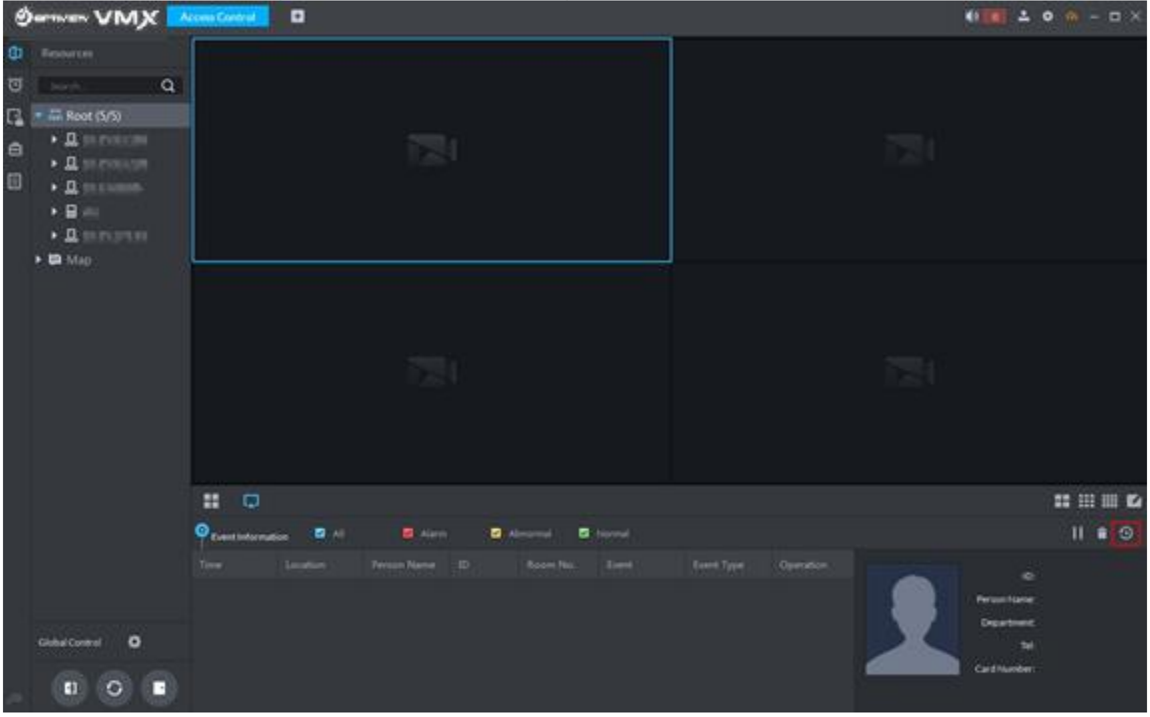
3.17.9.1 Searching Logs on Platform

Step 1 Enter AC log interface.

Supports following two methods.

- On **Access Control** interface, click 📄.
- On **Access Control** interface, click ◫ and enter console, click 🕘 and see Figure 3-378.

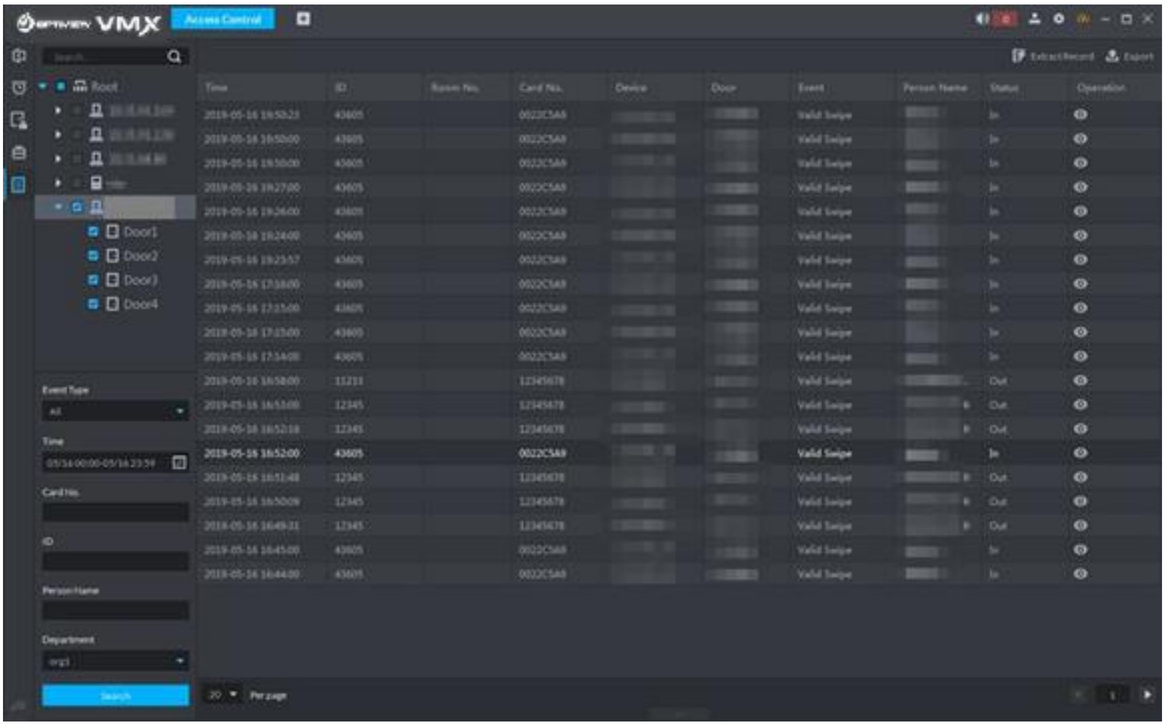
Figure 3-378 Enter AC log interface


VMX
Access Control
Resources
Root (5/5)
Map
Global Control
Event Information
All
Alarm
Abnormal
Normal
Time
Location
Person Name
ID
Room No.
Event
Event Type
Operation
Person Name:
Department:
Tel:
Card Number:

Step 2 Set condition, click **Search**.

The system displays log info, see Figure 3-379.

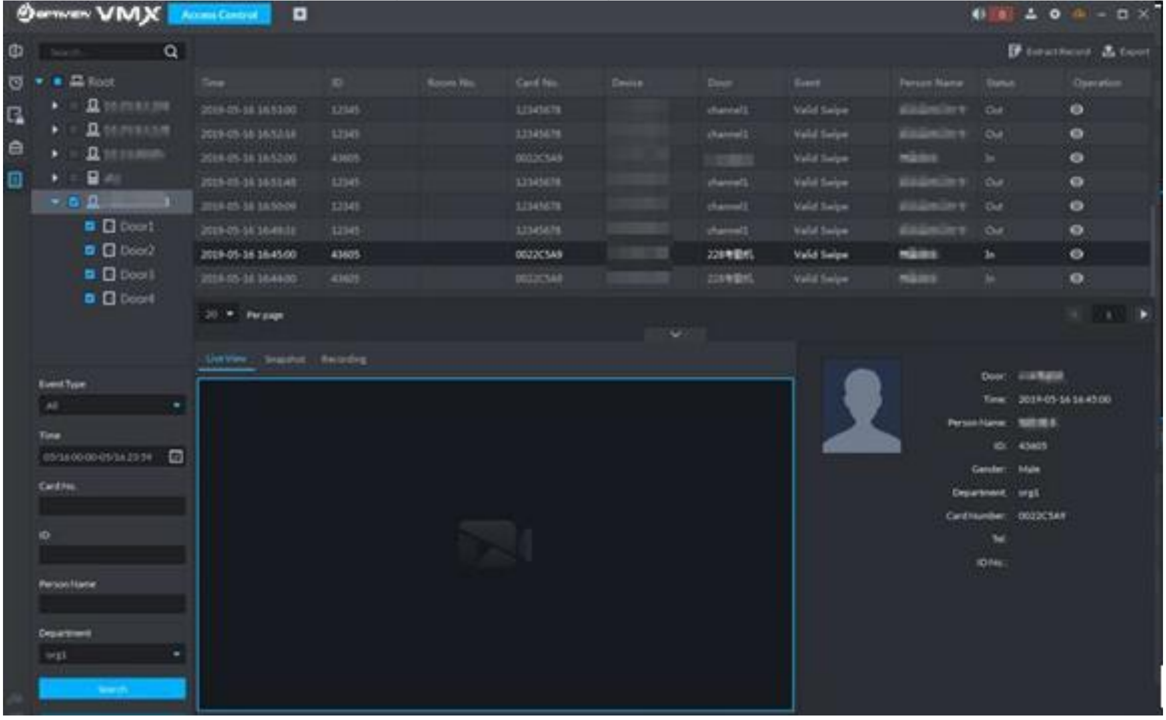
Figure 3-379 Search AC log


VMX
Access Control
Root
Door1
Door2
Door3
Door4
Event Type
All
Time
Card No.
ID
Person Name
Department
Search
Extract Record
Export
Time
ID
Room No.
Card No.
Device
Door
Event
Person Name
Status
Operation
Valid Swipe
In
Out
Per page

Step 3 Click ◉.

The system displays AC info and live view, snapshot and record of linked video channel. See Figure 3-380.

Figure 3-380 AC log details


Access Control
Extract Record
Export
Time
ID
Room No.
Card No.
Device
Door
Event
Person Name
Status
Operation
Per page
Live View
Snapshot
Recording
Event Type
Card No.
Person Name
Department
Search

Step 4 Click **Export** and save log to local according to system prompt.

3.17.9.2 Extracting Log during Device Offline

If device is offline during application, you can extract offline AC logs to platform.

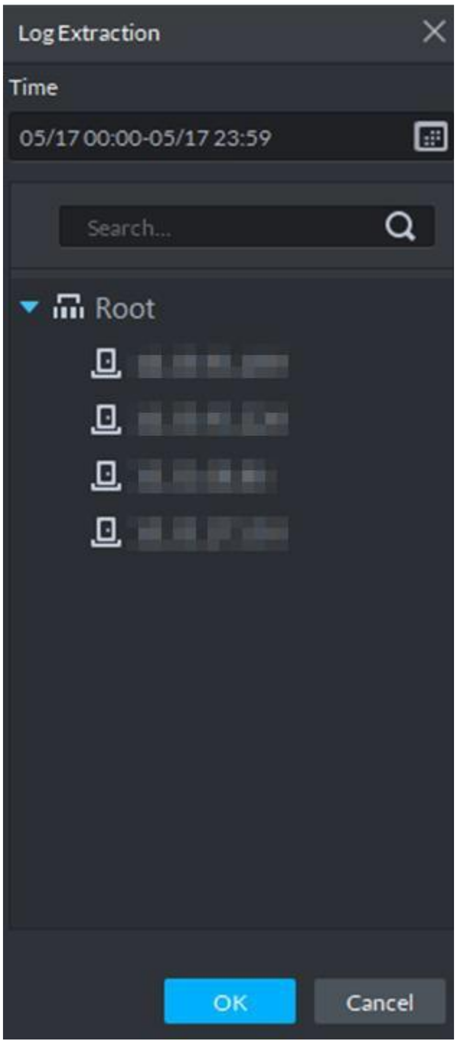
Step 1 Enter AC log interface.

Supports following two methods.

- On **Access Control** interface, click .
- On **Access Control** interface, click and enter console, click and see Figure 3-378.

Step 2 Click Extract Record on upper right corner.

Figure 3-381 Extract logs during device offline


Log Extraction
Time
05/17 00:00-05/17 23:59
Search...
Root
OK
Cancel

Step 3 Click ▦ and set period.

Step 4 Click ▶ and display AC devices, select channel.

Step 5 Click **OK**.

The system displays extracted logs.

3.17.9.3 Searching Device Logs

You can search log info of AC device.

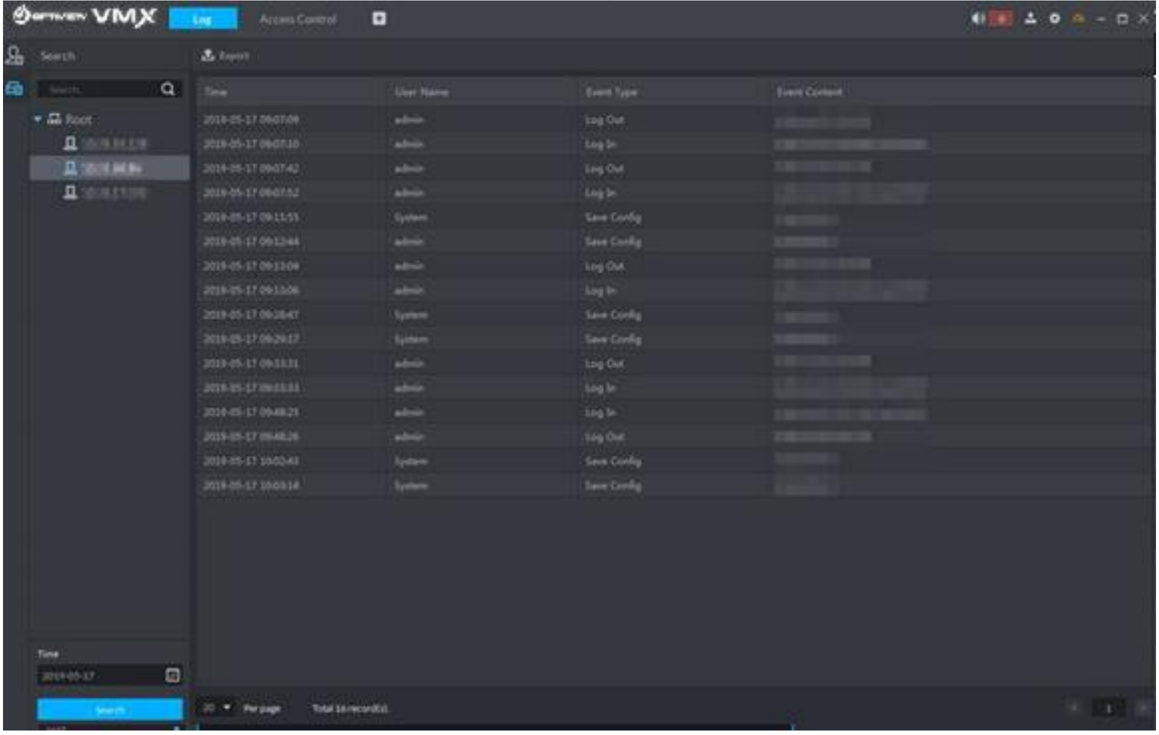
Step 1 On client homepage, click **Log**.

The system displays Log interface.

Step 2 Click ▤.

The system displays **Device Log** interface, see Figure 3-382.

Figure 3-382 Device log


VMX
Log
Access Control
Search
Export
Root
Time
User Name
Event Type
Event Content
Search
Per page

Step 3 Select AC device and time, click **Search**.

The system displays search results.

3.17.10 AC Device Maintenance

Support update or AC device reboot by platform. Please skip the chapter if you do not need to update or restart AC device.

3.17.10.1 Updating AC Device

You can update AC device remotely by platform. Before update, please make sure you have acquired AC device program, otherwise, please contact technical support for the program.

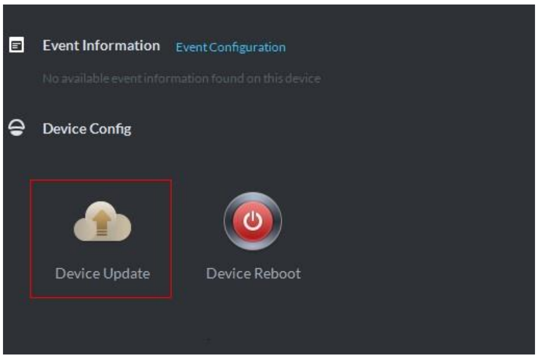
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 In left device tree, select AC device, click **Device Update** and see Figure 3-383.

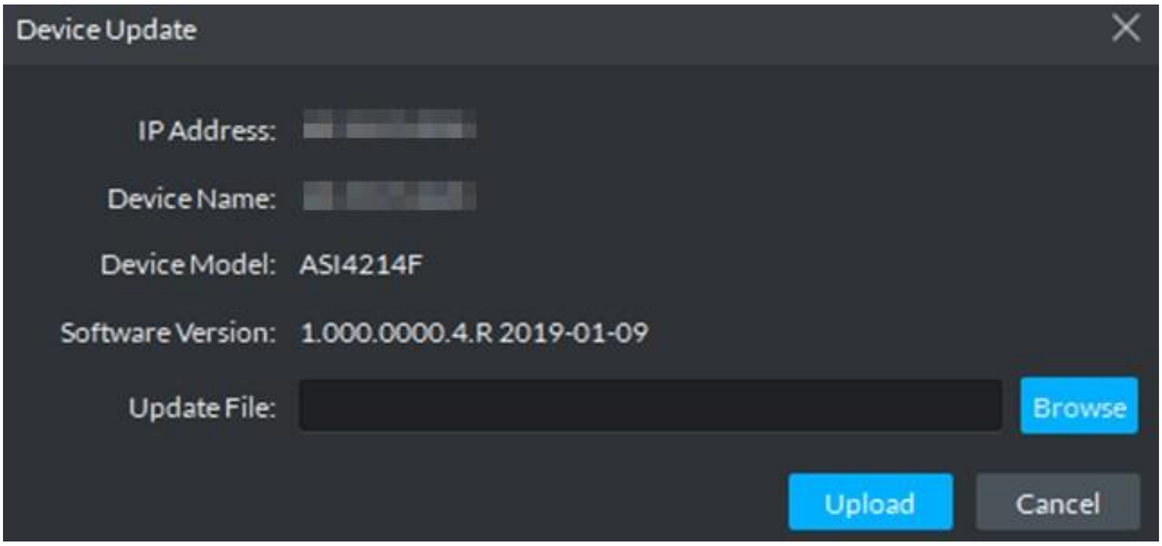
The system displays **Device Update** interface, and version info of AC device. See Figure 3-384.

Figure 3-383 Enter device update interface


Event Information
Event Configuration
Device Config
Device Update
Device Reboot

No available event information found on this device

Figure 3-384 Device update



Device Update

IP Address: [redacted]

Device Name: [redacted]

Device Model: ASI4214F

Software Version: 1.000.0000.4.R 2019-01-09

Update File:

Browse
Upload
Cancel

Step 3 Click **Browse** and select update file.

Step 4 Click **Upload** and update AC device.

3.17.10.2 Rebooting AC Device

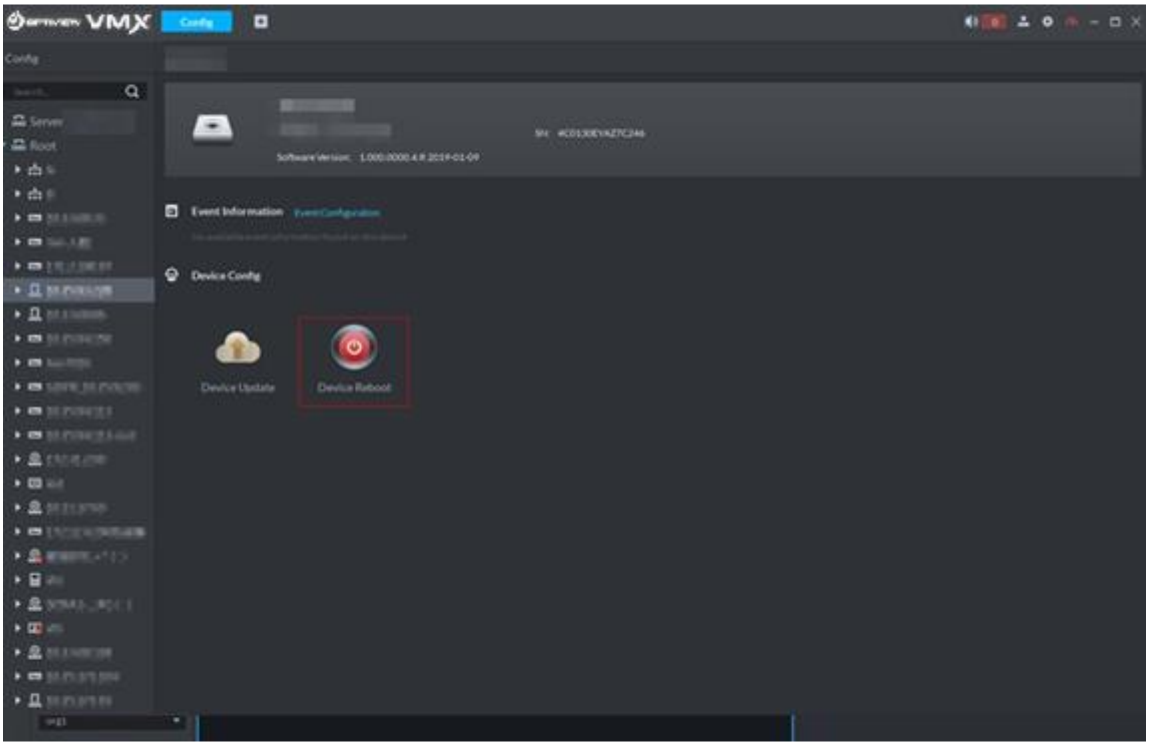
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 In left device tree, select AC device, click **Device Reboot**, and see Figure 3-385.

The system displays prompt box of rebooting device.

Figure 3-385 Enter device reboot



VMX
Config
Server
Root
Event Information
Event Configuration
Device Config
Device Update
Device Reboot

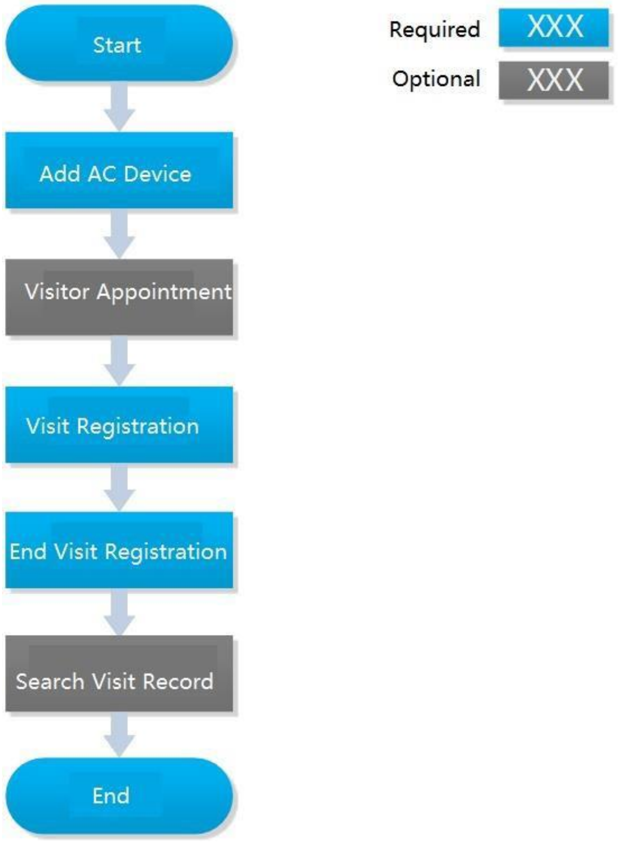
Software Version: 1.000.0000.4.R 2019-01-09

Step 3 Click **Yes** and reboot device.

3.18 Visitor Management

After appointment is made on platform, and visitor is registered in the company, then you can have access permission. Access permission is disabled when leaving the company. The visitor management flow is shown in Figure 3-386.

Figure 3-386 Visitor flow


Start
Add AC Device
Visitor Appointment
Visit Registration
End Visit Registration
Search Visit Record
End
Required
XXX
Optional
XXX

3.18.1 Adding AC Device

Add access control device. For more details, refer to **3.2.2.4 Adding Device**

3.18.2 Visitor Appointment

Record visitor info on platform.

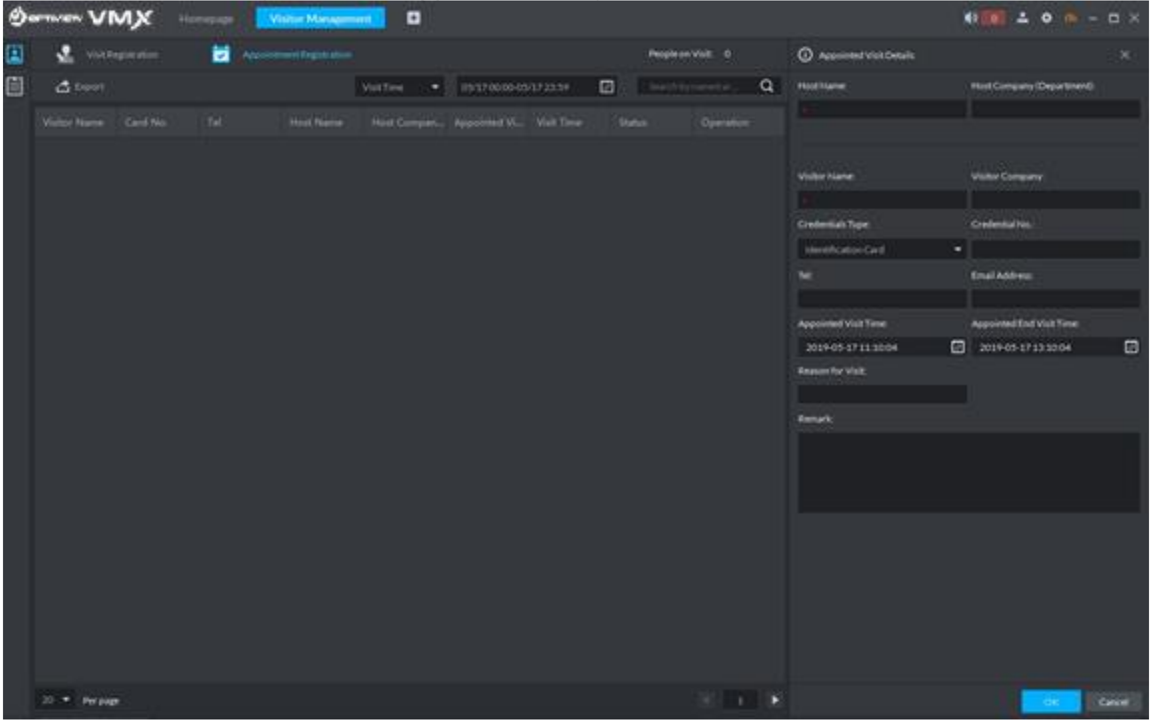
Step 1 On client homepage, click **Visitor Management**.

The system displays **Visitor Management** interface.

Step 2 Click Appointment Registration.

The system displays interface of registration info, see Figure 3-387.

Figure 3-387 Appointment registration


VMX
Homepage
Visitor Management
Visit Registration
Appointment Registration
People on Visit: 0
Export
Visit Time
05/17 00:00:00-05/17 23:59:59
Search by name/car...
Visitor Name
Card No.
Tel
Host Name
Host Compan...
Appointed Vi...
Visit Time
Status
Operation
20
Per page
1
Appointed Visit Details
OK
Cancel

Host Name:

Host Company (Department):

Visitor Name:

Visitor Company:

Credentials Type: Identification Card

Credential No.:

Tel:

Email Address:

Appointed Visit Time: 2019-05-17 11:10:04

Appointed End Visit Time: 2019-05-17 13:10:04

Reason for Visit:

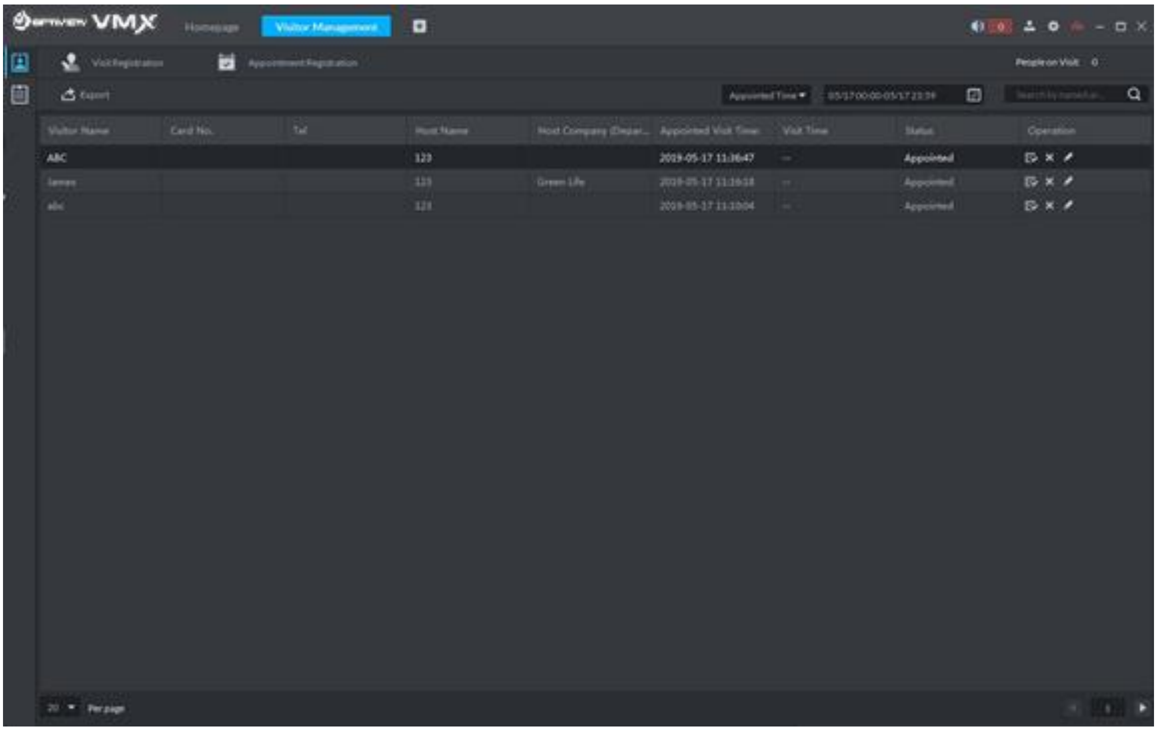
Remark:

Step 3 Enter visitor and some other info, click **OK** and complete appointment.

The platform displays appointment info, see Figure 3-388.

Click and skip to visit registration interface.

Figure 3-388 Appointed visitor info


VMX
Homepage
Visitor Management
Visit Registration
Appointment Registration
People on Visit: 0
Export
Appointed Time
05/17 00:00:00-05/17 23:59:59
Search by name/car...
20
Per page
1

Visitor Name	Card No.	Tel	Host Name	Host Company (Depar...	Appointed Visit Time	Visit Time	Status	Operation
ABC			123		2019-05-17 11:36:47	--	Appointed	
James			123	Green Life	2019-05-17 11:26:18	--	Appointed	
abc			123		2019-05-17 11:10:04	--	Appointed	

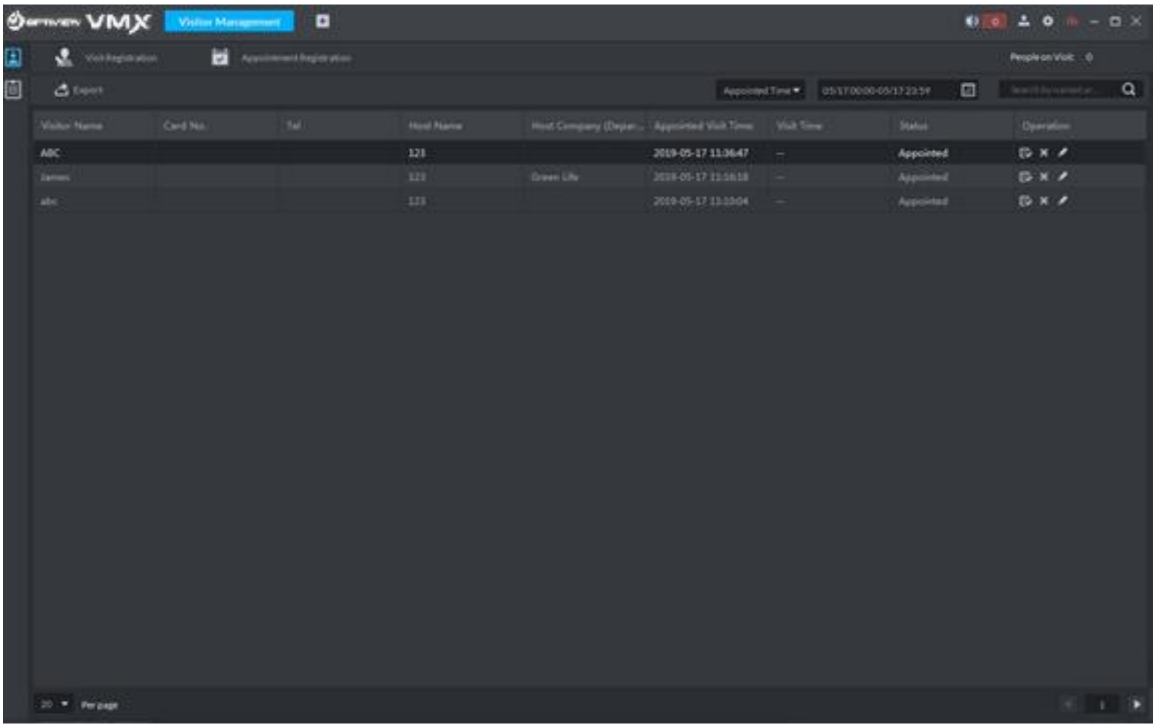
3.18.3 Visit Registration

When appointed visitor comes to visit, you need to confirm person info and grant access permission. On-site registration is supported when there is temporary visitor, and grant access permission. Visitor can have access by swiping card or face recognition.

Step 1 On **Visitor Management** interface, click .

The system displays **Visitor Management** interface. The interface displays appointed visitor info, see Figure 3-389.

Figure 3-389 Visitor management


VMX
Visitor Management
Visit Registration
Appointment Registration
People on Visit: 0
Export
Appointed Time
05/17 00:00-05/17 23:59
20
Per page
1

Visitor Name	Card No.	Tel	Host Name	Host Company (Depar...	Appointed Visit Time	Visit Time	Status	Operation
ABC			123		2019-05-17 11:36:47	--	Appointed	
James			123	Green Life	2019-05-17 11:16:18	--	Appointed	
abc			123		2019-05-17 11:10:04	--	Appointed	

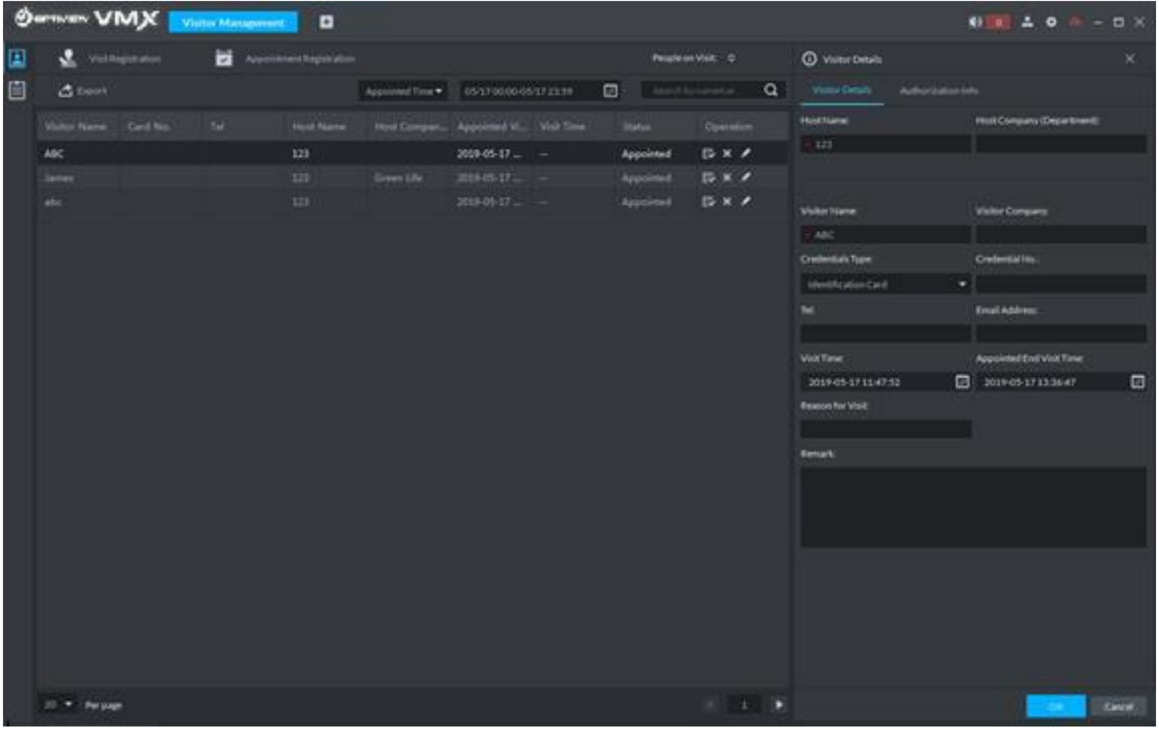
Step 2 Enter visit registration info interface.

- If visitor is appointed.

  Search visitor info, click . The system displays visitor registration details, see Figure 3-390.
- If visitor is not appointed.

  Click **Visit Registration**, the system displays visitor registration detail interface. You need to enter info manually if there is no person info.

Figure 3-390 Visit details


VMX
Visitor Management
Visit Registration
Appointment Registration
People on Visit
Export
Appointed Time
Visitor Name
Card No.
Tel
Host Name
Host Company
Appointed Vi...
Visit Time
Status
Operation
Per page
Visitor Details
Authorization Info
OK
Cancel

Visitor Name	Card No.	Tel	Host Name	Host Compan...	Appointed Vi...	Visit Time	Status	Operation
ABC			123		2019-05-17 ...	--	Appointed	
James			123	Green Life	2019-05-17 ...	--	Appointed	
abc			123		2019-05-17 ...	--	Appointed	

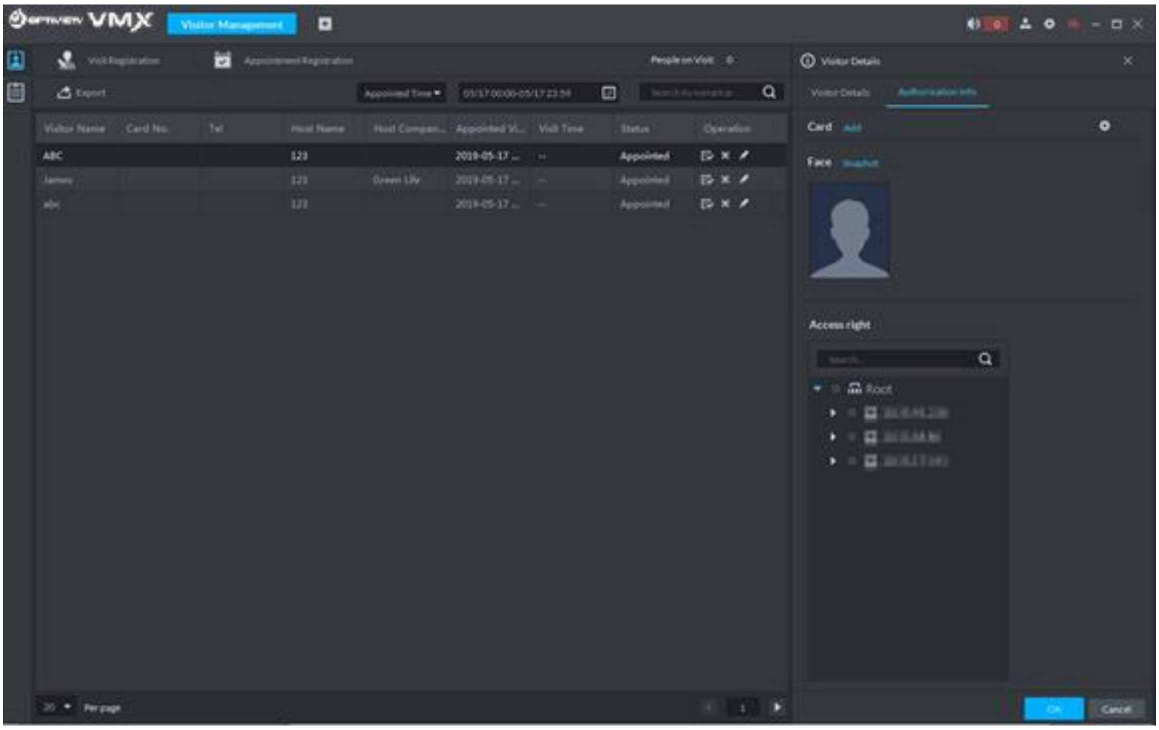
Host Name: 123
Host Company (Department):
Visitor Name: ABC
Visitor Company:
Credentials Type: Identification Card
Credential No.:
Tel:
Email Address:
Visit Time: 2019-05-17 11:47:52
Appointed End Visit Time: 2019-05-17 13:36:47
Reason for Visit:
Remark:

Step 3 On Visit Detail interface, confirm visitor info or enter visitor info, see Figure 3-390.

Step 4 Click Authorization Info tab.

The system displays **Authorization Info** interface, see Figure 3-391.

Figure 3-391 Visitor authorization


VMX
Visitor Management
Visit Registration
Appointment Registration
People on Visit
Export
Appointed Time
Visitor Details
Visitor Details
Authorization Info
Card
Add
Face
Snapshot
Access right
Search...
Root
Per page
OK
Cancel

Step 5 Issue card for visitor.

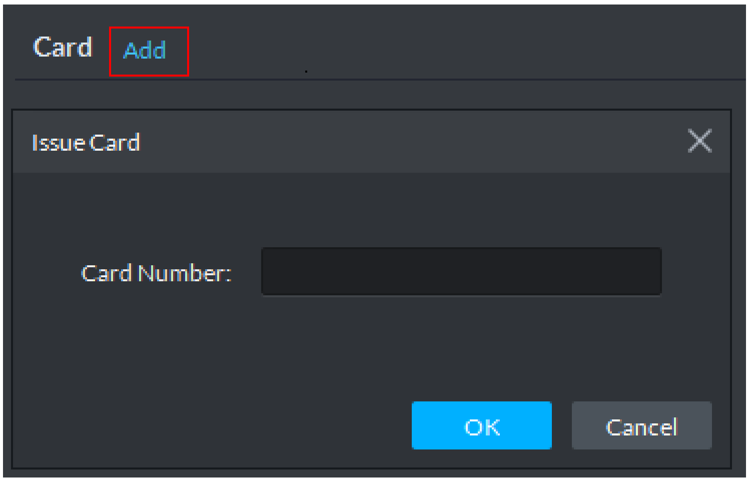
You can issue card by entering card No. manually or card reader. Card No. supports 8 and 16 digits, if the card No. is less than 8 or 16 digits, the platform adds 0 by default to meet the card No. requirement. For example, if you enter card number 8004, then the platform will change it to 00008004. If you enter card number 1000056821, then the platform will change it to 0000001000056821.

- Issue card by entering card No. manually

1) Click **Add** next to **Card**.

The system displays Issue Card interface, see Figure 3-392.

Figure 3-392 Add card


Card
Add
Issue Card
OK
Cancel

Card Number:

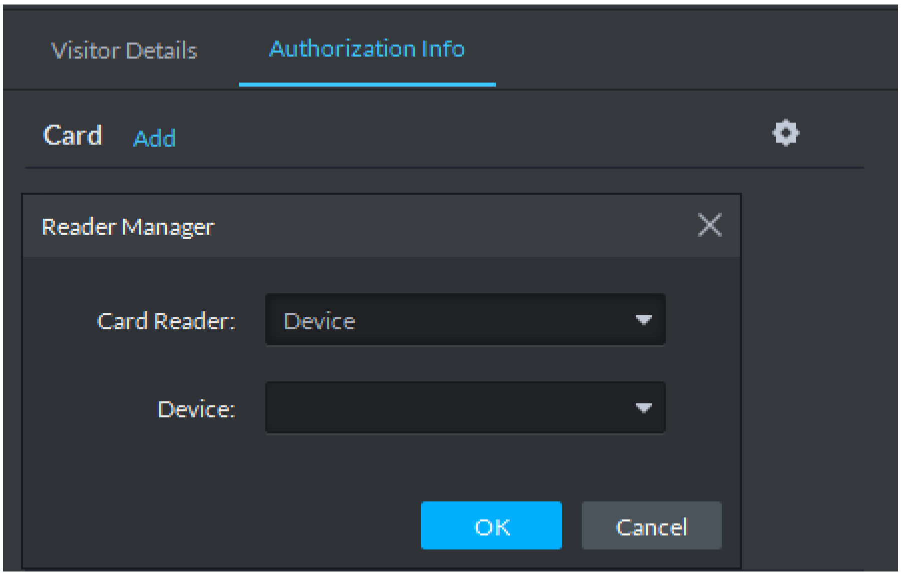
2) Enter card number, click **OK**, and card is issued.

- Issue card by reader

1) Click Reader Manager.

The system displays **Reader Manager** interface, see Figure 3-393.

Figure 3-393 Reader manager


Visitor Details
Authorization Info
Card
Add
Reader Manager
OK
Cancel

Card Reader: Device

Device:

2) Select card reader or device, click **OK**.

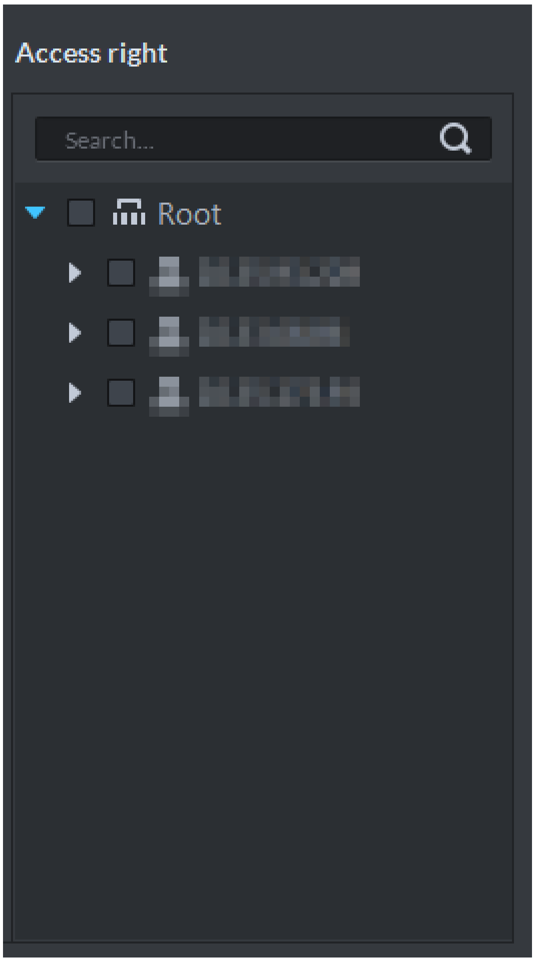
3) Swipe card on reader or device, and card is issued.

Step 6 Click **Snapshot**, and you can take face snapshot according to system prompt.

The face snapshot is used for face recognition and unlock door.

Step 7 In **Access Right** area, select AC channel that visitor can pass, see Figure 3-394.

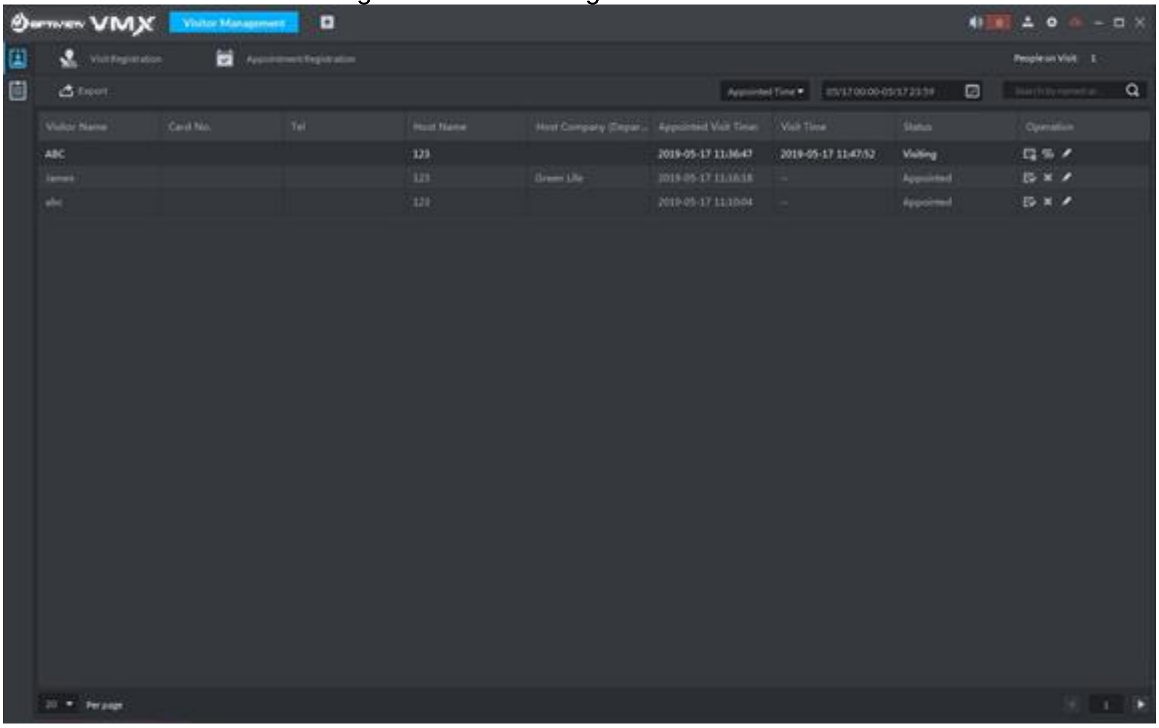
Figure 3-394 Select channel


Access right
Search...
Root

Step 8 Click **OK** and complete visitor registration, see Figure 3-395.

- Click and skip to end visit interface.
- Click and view visitor swiping card records.

Figure 3-395 Visit registration



VMX
Visitor Management
Visit Registration
Appointment Registration
People on Visit 1
Export
Appointed Time
05/17 00:00-05/17 23:59
20
Per page
1

Visitor Name	Card No.	Tel	Host Name	Host Company (Depar...	Appointed Visit Time	Visit Time	Status	Operation
ABC			123		2019-05-17 11:36:47	2019-05-17 11:47:52	Visiting	
James			123	Green Life	2019-05-17 11:16:18	--	Appointed	
abc			123		2019-05-17 11:10:04	--	Appointed	

3.18.4 End Visit Registration

When visitor leaves, close access permission.

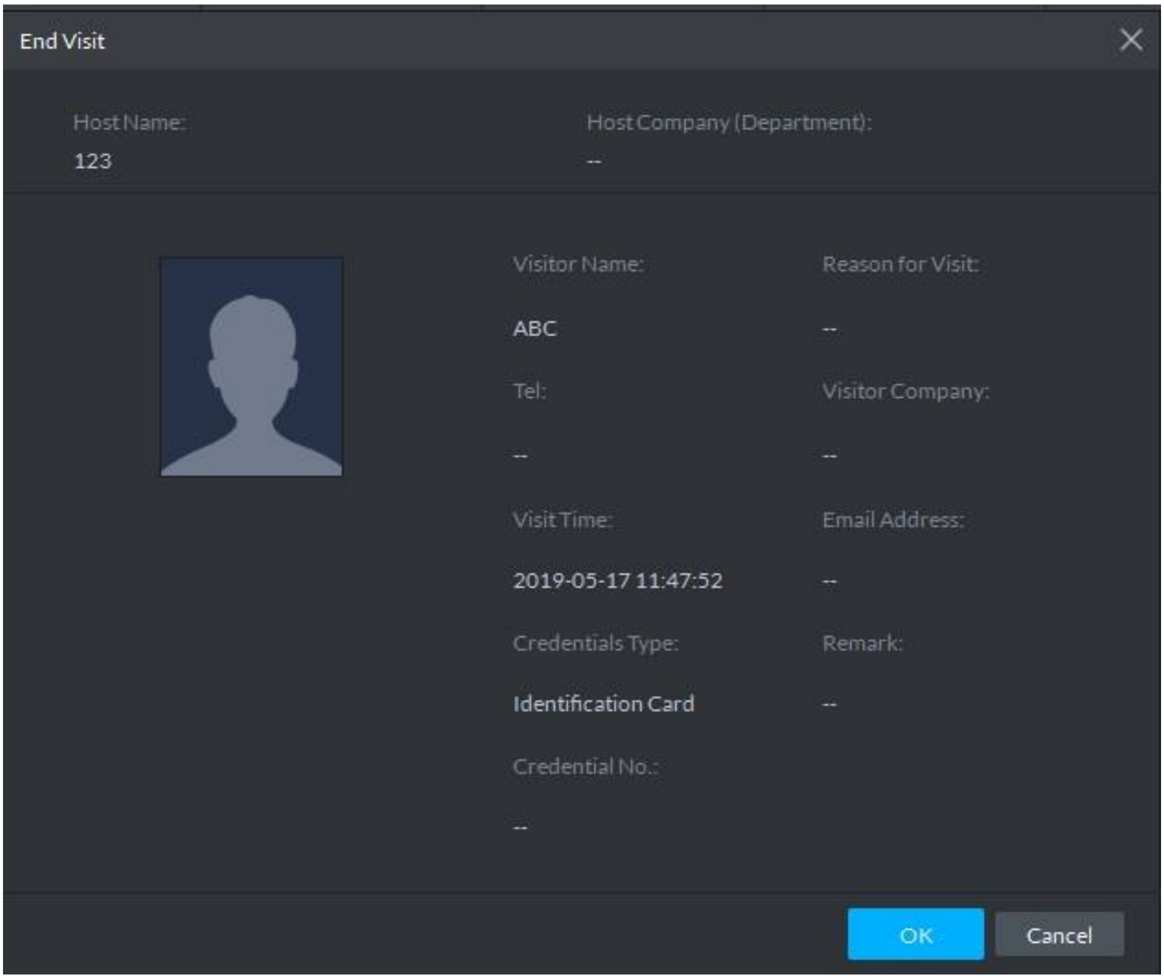
Step 1 On **Visitor Management** interface, click .

The system displays **Visitor Management** interface.

Step 2 Click .

The system displays **End Visit** interface, see Figure 3-396.

Figure 3-396 End visit



Host Name:
123

Host Company (Department):
--

Visitor Name:
ABC

Reason for Visit:
--

Tel:
--

Visitor Company:
--

Visit Time:
2019-05-17 11:47:52

Email Address:
--

Credentials Type:
Identification Card

Remark:
--

Credential No.:
--

Step 3 Click **OK** and close access permission.

If you issue card to visitor, make sure the card is returned when visitor leaves.

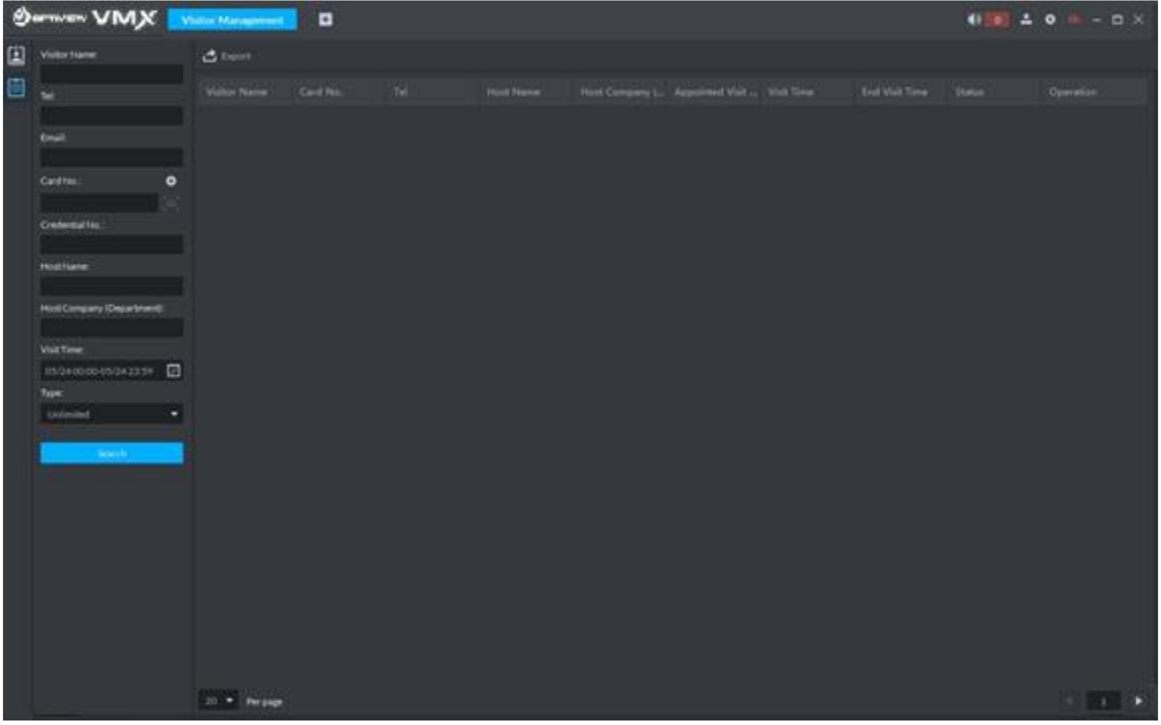
3.18.5 Searching Visit Record

You can set condition and search visit record, and view visitor details and card swiping records.

Step 1 On **Visitor Management** interface, click 📋.

The system displays **Visit Record** interface, see Figure 3-397.

Figure 3-397 Visit record

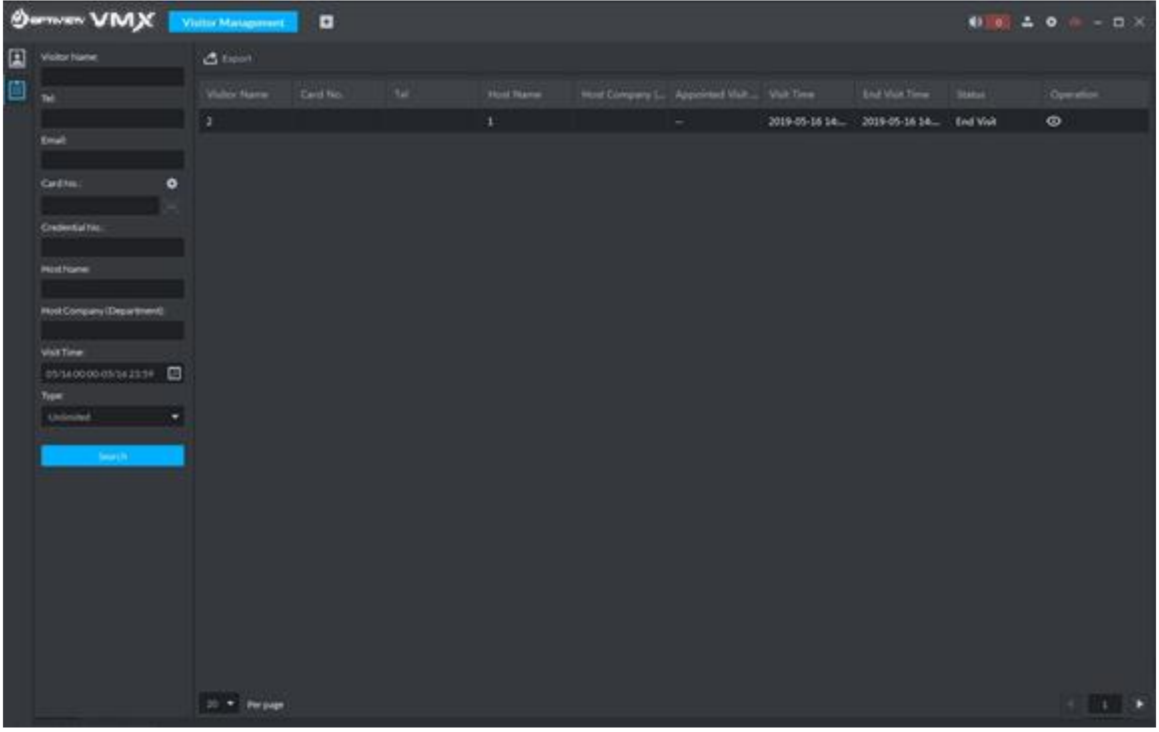

VMX
Visitor Management
Visitor Name:
Tel:
Email:
Card No.:
Credential No.:
Host Name:
Host Company (Department):
Visit Time:
Type:
Unlimited
Search
Export
Visitor Name
Card No.
Tel
Host Name
Host Company (...
Appointed Visit ...
Visit Time
End Visit Time
Status
Operation
20
Per page
1

Step 2 Set search condition, click **Search**.

The system displays results. See Figure 3-398.

Click ⚙ to set card reader, and then the card reader will automatically get card information.

Figure 3-398 Search visit result


VMX
Visitor Management
Visitor Name:
Tel:
Email:
Card No.:
Credential No.:
Host Name:
Host Company (Department):
Visit Time:
Type:
Unlimited
Search
Export
20
Per page
1

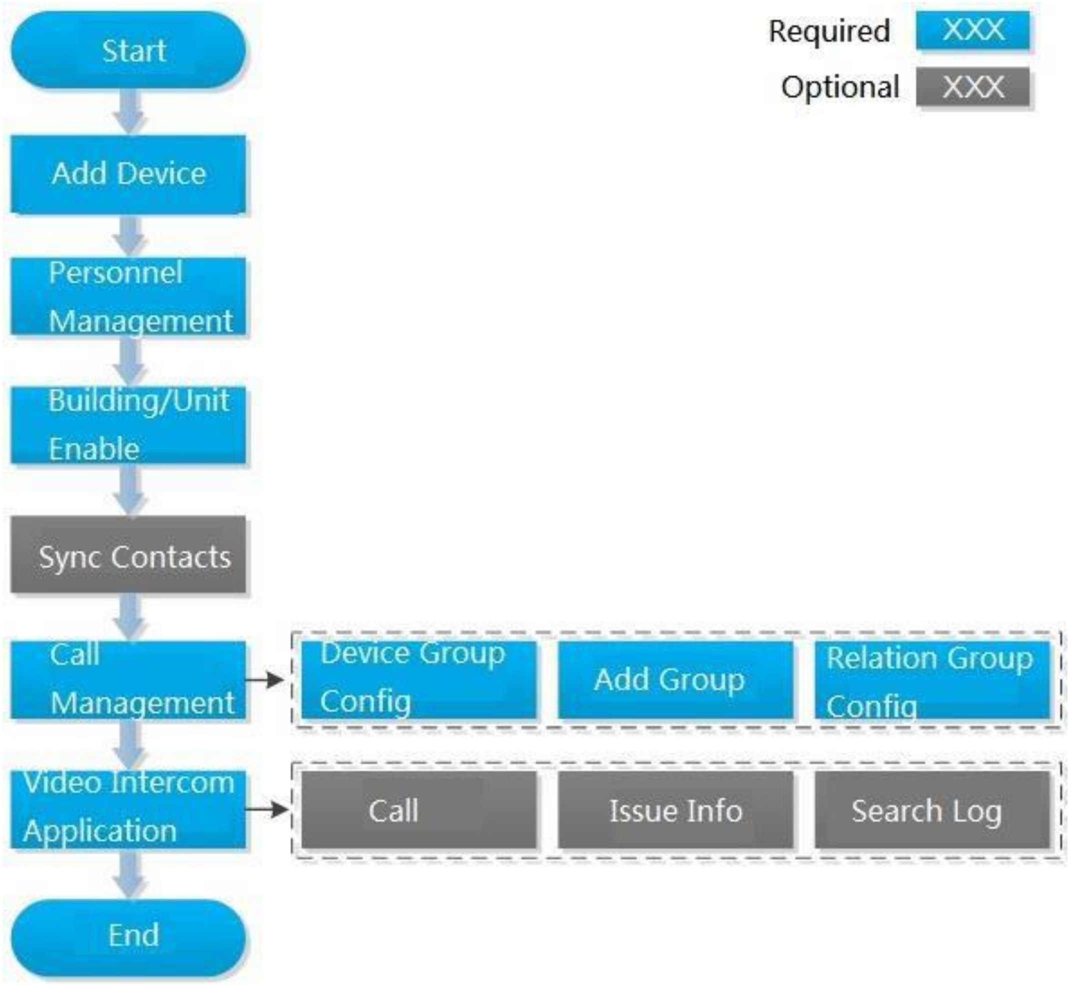
Visitor Name	Card No.	Tel	Host Name	Host Company (...	Appointed Visit ...	Visit Time	End Visit Time	Status	Operation
2			1		--	2019-05-16 14:...	2019-05-16 14:...	End Visit	👁

Step 3 Click 👁 and view visitor details and card swiping records.

3.19 Video Intercom

After integrating video talk module and adding video intercom device, you can realize device talk, real-time monitoring and issuing info. The video intercom operation flow is shown in Figure 3-399

Figure 3-399 Operation flow


Required XXX
Optional XXX
Start
Add Device
Personnel Management
Building/Unit Enable
Sync Contacts
Call Management
Device Group Config
Add Group
Relation Group Config
Video Intercom Application
Call
Issue Info
Search Log
End

Configure video intercom on platform, the device is required to be configured. For more details, refer to user manual.

3.19.1 Adding Video Intercom Device

Add video intercom devices such as unit VTO, VTH and fence VTO. For more details, see **3.2.2.4 Adding Device**

If you modify configuration when using device, the device will not actively push message to platform. You need to acquire device info manually from platform. For more details, see "3.2.2.5 Editing Device."

3.19.2 Personnel Management

For video intercom, you can add personnel by the module of personnel management. See **3.16 Personnel Management** for more details. Room number is required to be configured when adding personnel.

3.19.3 Configuring Building/Unit

It needs to make sure the enable of building and unit is in accordance with the device if you want to use the video talk module of the platform, otherwise, the device is offline after adding device. The setting of building and unit affects the dialing rule. Take room 1001 unit 2 building 1 as an example, the dialing rule is shown as follows after it is enabled.

- If building is enabled, unit is not enabled, and then the number is "1#1001".
- If building is enabled, unit is enabled as well, and then the number is "1#2#1001".
- If building is not enabled, unit is not enabled either, and then the number is "1001".

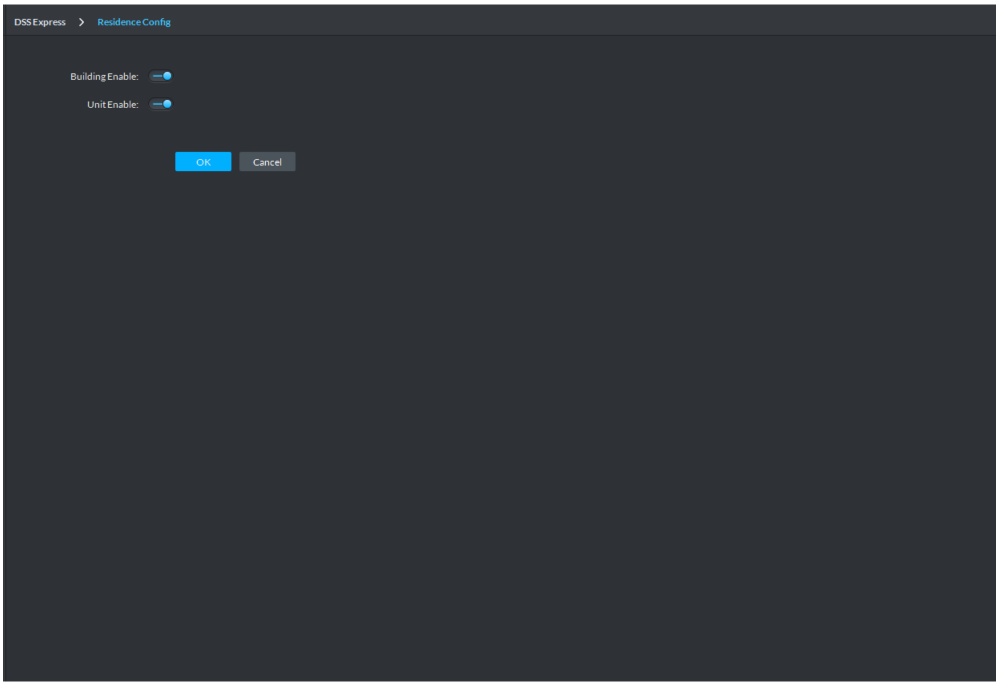
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Residence Config**.

The system displays **Residence Config** interface. See Figure 3-400.

Figure 3-400



Step 3 Enable or disable building and unit according to the actual situation, it is required to be in accordance with that of the device, click **Save** and complete config.

3.19.4 Synchronizing Contacts

Synchronize contacts information to VTO and then you can view contacts on the VTO display screen or WEB interface.

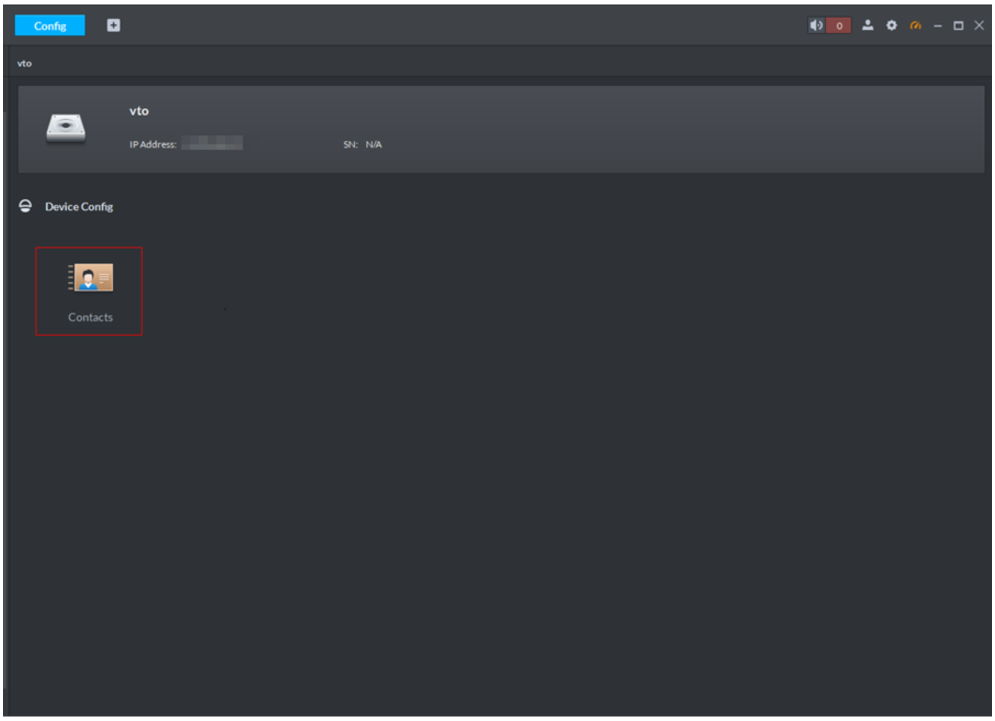
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Select VTO from the device list, and click **Contacts**, see Figure 3-401.

The system displays **Release Contact** interface, see Figure 3-402.

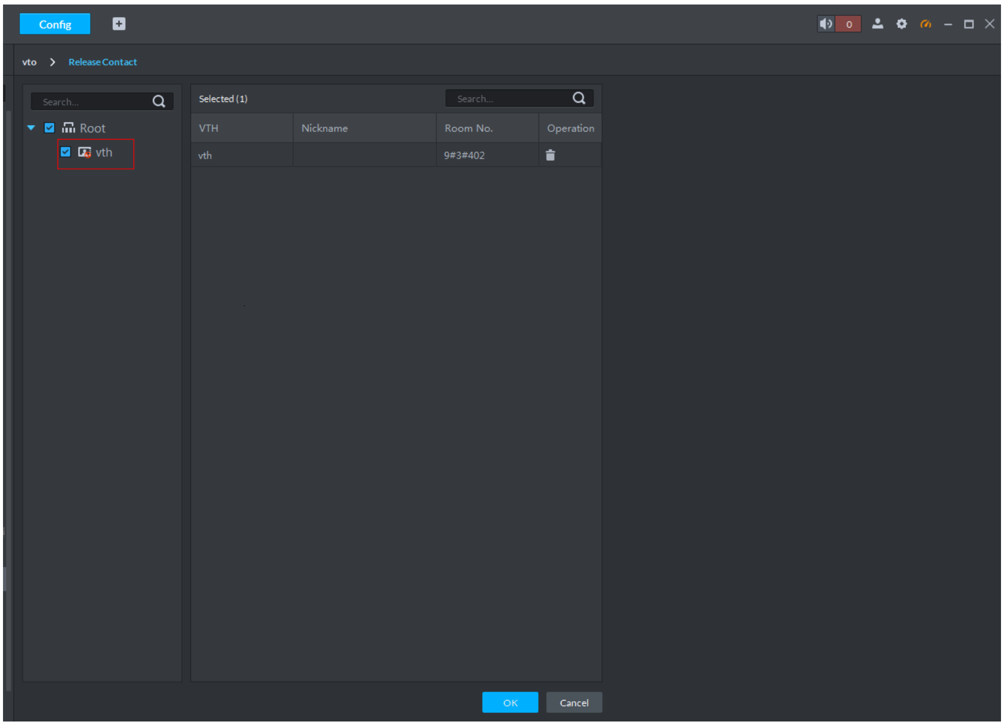
Figure 3-401


Config
0
vto
vto
Device Config
Contacts

IP Address: [redacted]

SN: N/A

Figure 3-402 Release contact


Config
0
vto > Release Contact
Search...
Root
vth
Selected (1)
Search...
OK
Cancel

VTH	Nickname	Room No.	Operation
vth		9#3#402	🗑

Step 3 Select VTH, click **OK**.

You can view contacts on VTO screen or WEB interface after it is released.

3.19.5 Call Management

Create device group, management group and relation group respectively; realize mutual call in the specific group. Only default system account supports the function.

Click on the interface of device group, management group or relation group, the system will restore management group and relation group to original status.

3.19.5.1 Device Group Config

It can realize mutual call only when VTO and VTH are added into the same device group. Pro will automatically generate corresponding device group when VTO, verifying VTO and fence station are added to Pro.

- Add VTO and automatically generate a device group, add VTH of the unit into the group, and realize mutual call between VTH and VTO within the group.
- Add verifying VTO and automatically generate a device group, add it to the group together with the VTH of the same room, and realize mutual call between VTH and verifying VTO within the group.
- Add fence station and automatically generate a device group, add all the VTH into the group. Realize mutual call between fence station and all the VTH.
- Add VTH, if the VTH is automatically connected to unit VTO, verifying VTO, fence station, and then it will be automatically added to the device group, and realize mutual call among unit VTO, verifying VTO or fence station.

Call between VTH is not restricted by device group; mutual call can be realized among VTH in different device groups.

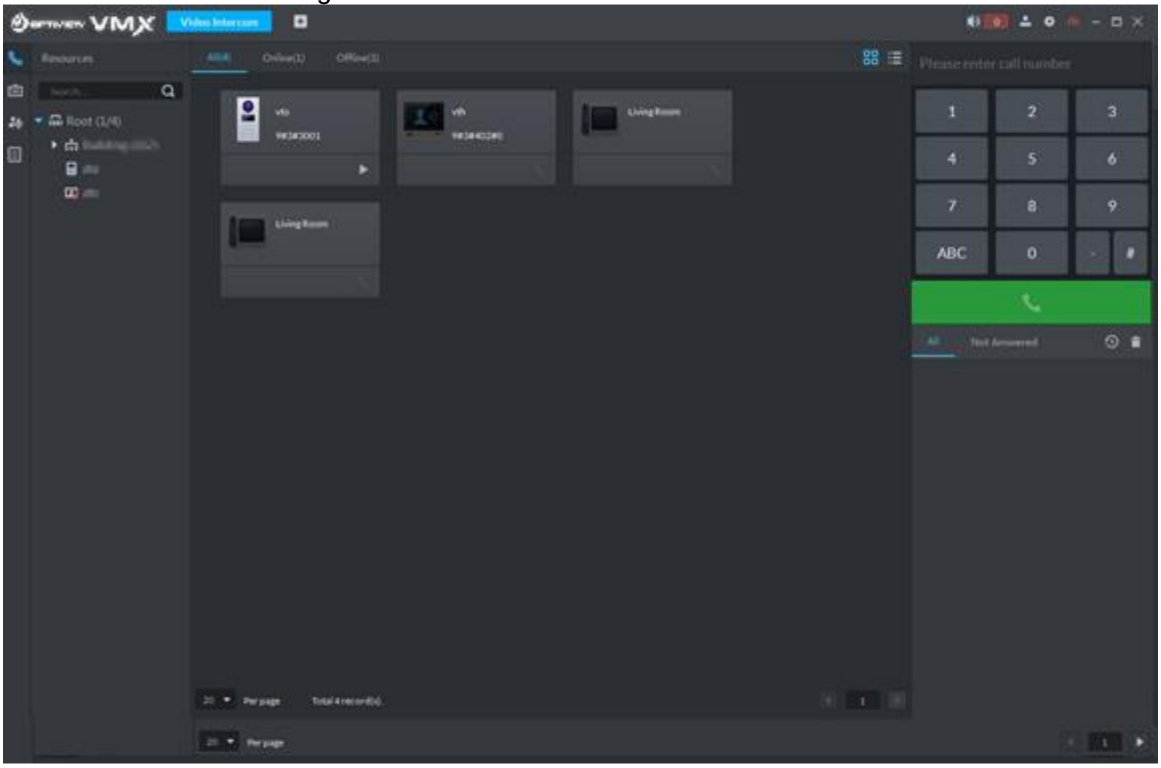
3.19.5.2 Adding Management Group

Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include Pro administrator and VTS. If there is default management group, VTS will be automatically added to management group when it is added.

- Before configuring management group, it needs to create user, select video intercom menu permission and device permission, and add new users into management group.
- Use system user to configure group relation, need to switch to new user for login. If system logs onto many devices, then it cannot be used as administrator.

Step 1 On client homepage, click **Video Intercom**.
The system displays Video Intercom interface, see Figure 3-403.

Figure 3-403 Video intercom



VMX
Video Intercom
Resources
All(4)
Online(1)
Offline(3)
Root (1/4)
vto
vth
Living Room
Please enter call number
1
2
3
4
5
6
7
8
9
ABC
0
#
All
Not Answered
Per page
Total 4 record(s)

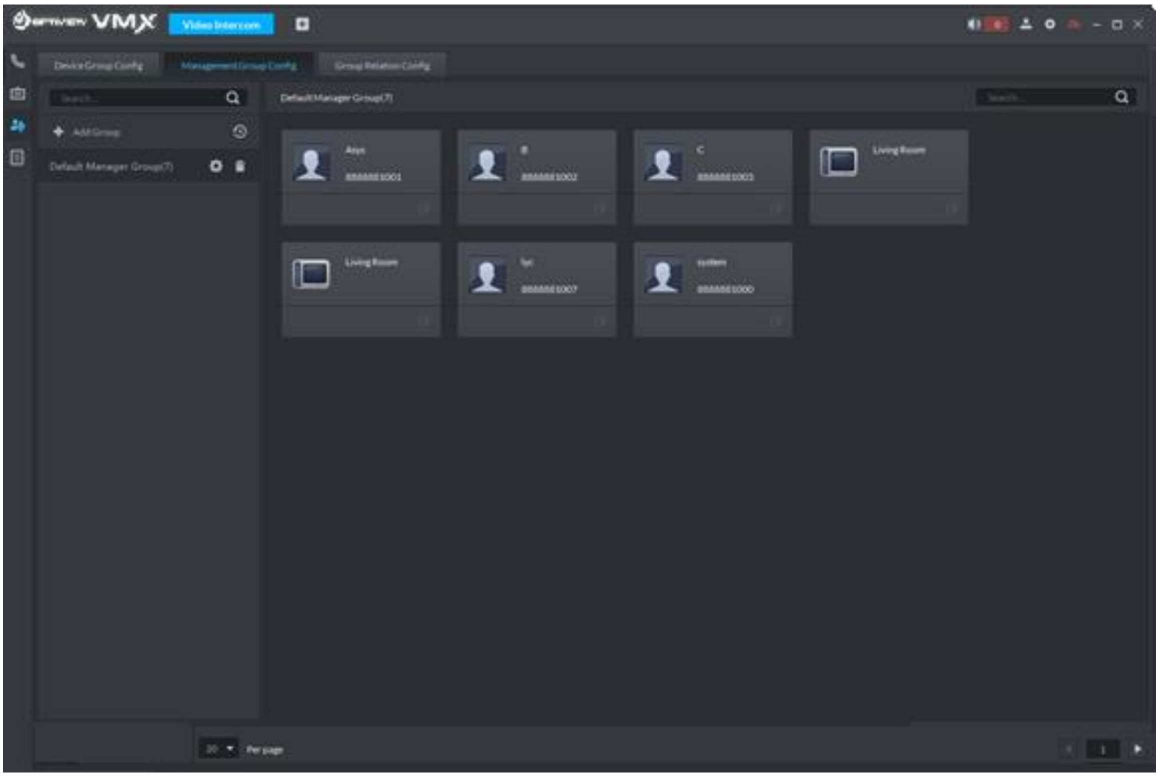
Step 2 Click .

The system displays the interface of **Call Management**.

Step 3 Click Management Group Config.

The system displays the interface of **Management Group Config**. See Figure 3-404.

Figure 3-404 Call management

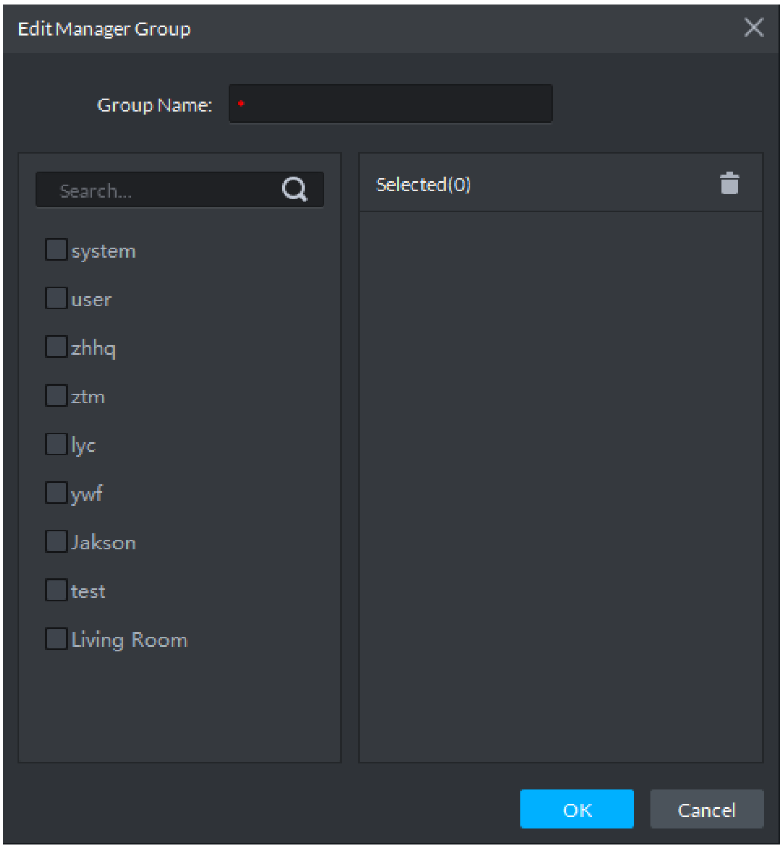


VMX
Video Intercom
Device Group Config
Management Group Config
Group Relation Config
Add Group
Default Manager Group(7)
B
C
Living Room
system
Per page

Step 4 Click Add Group.

The system displays the interface of **Edit Manager Group**. See Figure 3-405.

Figure 3-405 Manager group


Edit Manager Group
Group Name:
Search...
Selected(0)
OK
Cancel

☐ system
☐ user
☐ zhhq
☐ ztm
☐ lyc
☐ ywf
☐ Jakson
☐ test
☐ Living Room

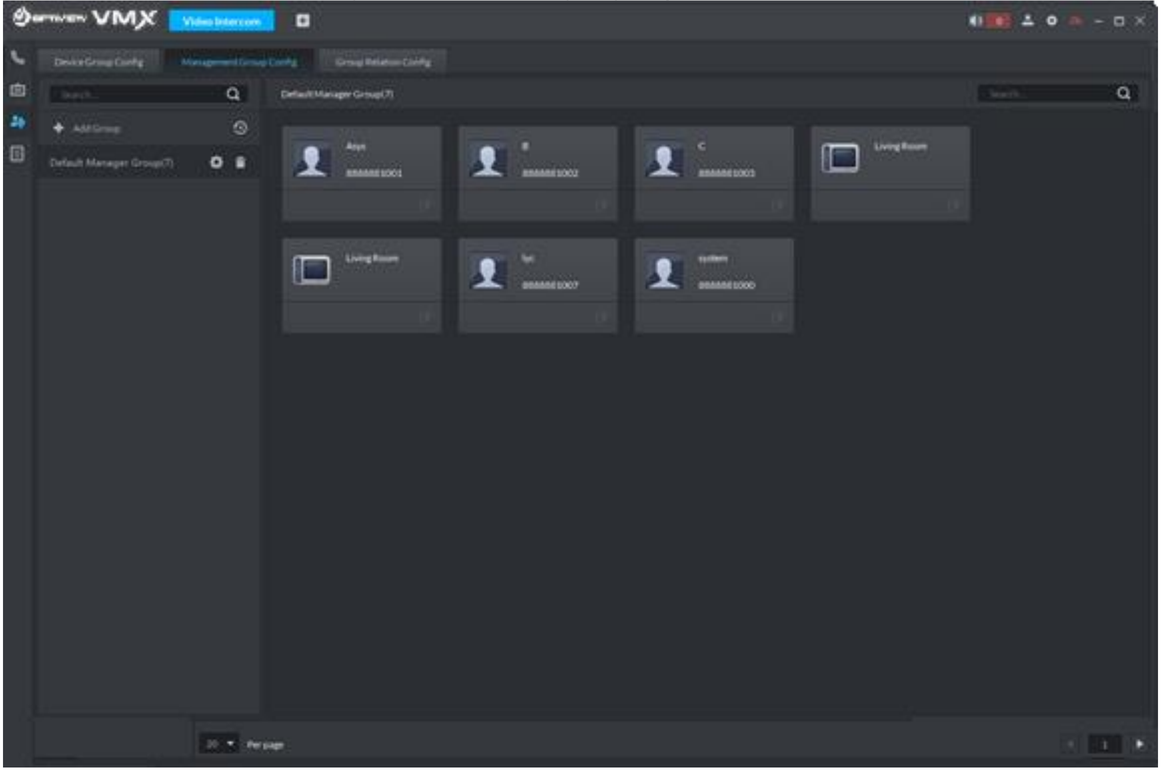
Step 5 Enter group name, select administrator account or VTS, and click **OK**.

The added management group is displayed in the list. See Figure 3-406.

The members in management group support following operation.

- Transfer members, click and move the member to the group.
- Manage group members, clic to add or delete group member.

Figure 3-406 Manager group


VMX
Video Intercom
Device Group Config
Management Group Config
Group Relation Config
Search...
Add Group
Default Manager Group(7)
Default Manager Group(7)
Search...
Aoys
B
C
Living Room
Living Room
lyc
system
20
Per page
1

3.19.5.3 Group Relation Config

Relation group configuration means adding both device group and management group to the same relation group, making then related. VTO or VTH can only call the administrator device in the related group.

There are two situations for relation binding

- Device group only binds one management group

  Any device in the group can call administration with one click, all the bound administrators within the management group will generate ring bell. At this moment, all other ring bell will stop as long as there is on administrator answers. The device call request can be rejected as long as all the administrators reject to answer.

- Device group binds several management groups

  There is priority among several management groups. When any device in the group calls administrator with one click, and all the online administrators of management group with highest priority will generate ring bell. If none of these administrators answer, then it will call next management group. The interval between two calls is 30s; it can skip up to one management group. If neither of two groups answers, the device will prompt “Call overtime.”

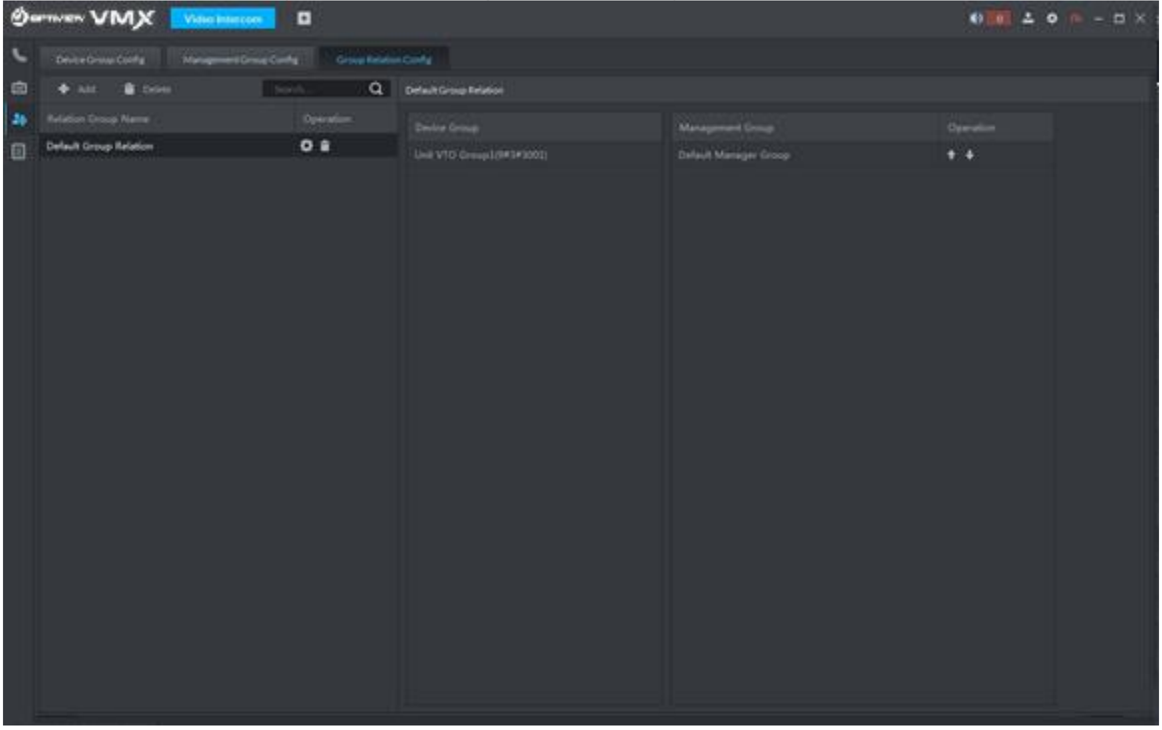
Step 1 Click on the interface of **Video Intercom**.

The system displays the interface of **Relation Group Config**.

Step 2 Click the tab of Relation Group Config.

The system displays the interface of **Relation Group Config**. See Figure 3-407.

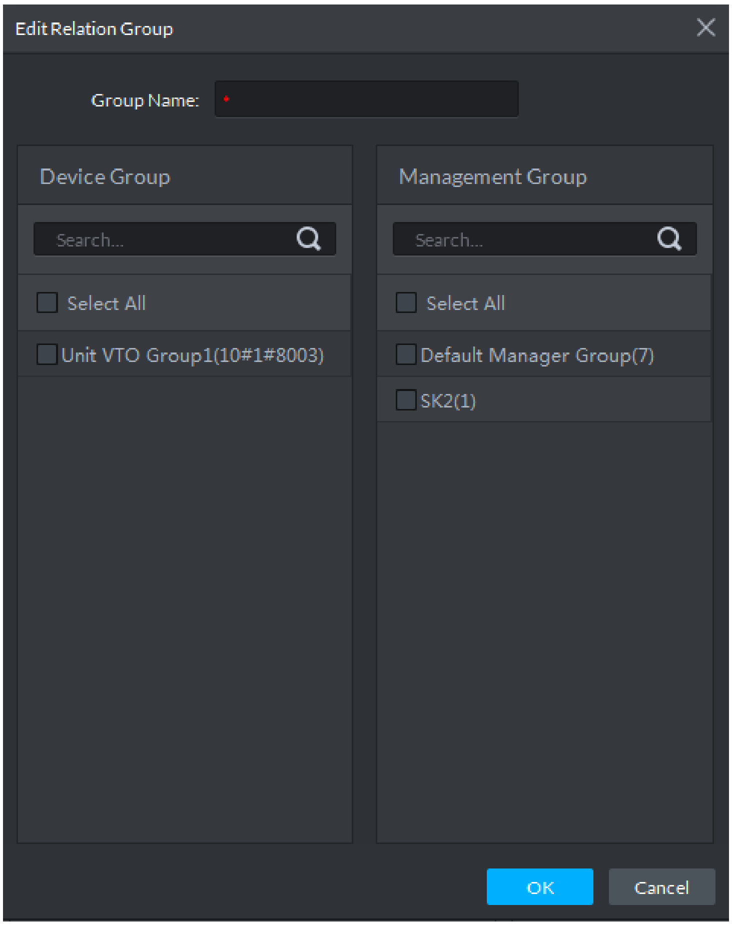
Figure 3-407 Group relation config


VMX
Video Intercom
Device Group Config
Management Group Config
Group Relation Config
Add
Delete
Default Group Relation
Relation Group Name
Operation
Default Group Relation
Device Group
Management Group
Operation
Default Manager Group

Step 3 Click **Add**.

The system displays the interface of **Edit Relation Group**. See Figure 3-408.

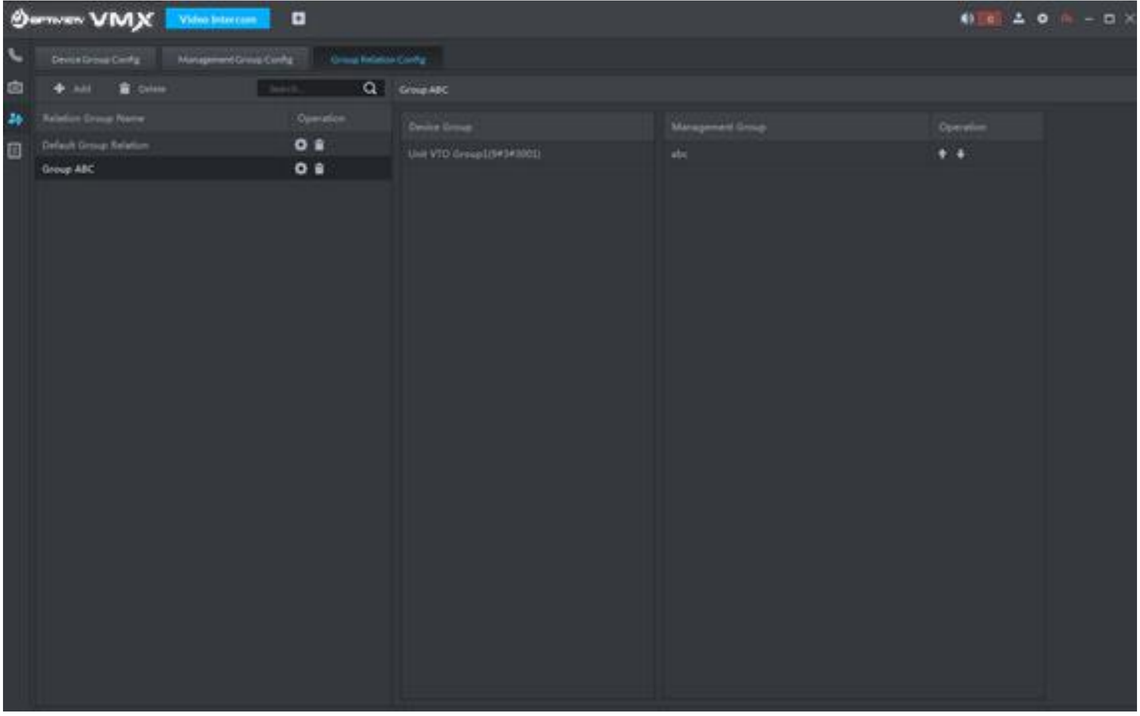
Figure 3-408 Edit relation group


Edit Relation Group
Group Name:
Device Group
Search...
☐ Select All
☐ Unit VTO Group1(10#1#8003)
Management Group
Search...
☐ Select All
☐ Default Manager Group(7)
☐ SK2(1)
OK
Cancel

Step 4 Enter name, select device group and management group, Click **OK**.

Added relation group is displayed in the list. See Figure 3-409. If there are several relation groups, you can click ⬆ or ⬇ to adjust priority level. When there is call, the online administrators with high priority will generate ring bell first.

Figure 3-409 Edit relation group


VMX
Video Intercom
Device Group Config
Management Group Config
Group Relation Config
Add
Delete
Search...
Group ABC

Relation Group Name	Operation
Default Group Relation	
Group ABC	

Device Group	Management Group	Operation
Unit VTO Group1(5#3#3001)	abc	⬆ ⬇

3.19.6 Video Intercom Application

3.19.6.1 Call Center

Step 1 Click ☎ on the interface of **Video Intercom**.

The system displays the interface of **Call Center**. See Figure 3-410.

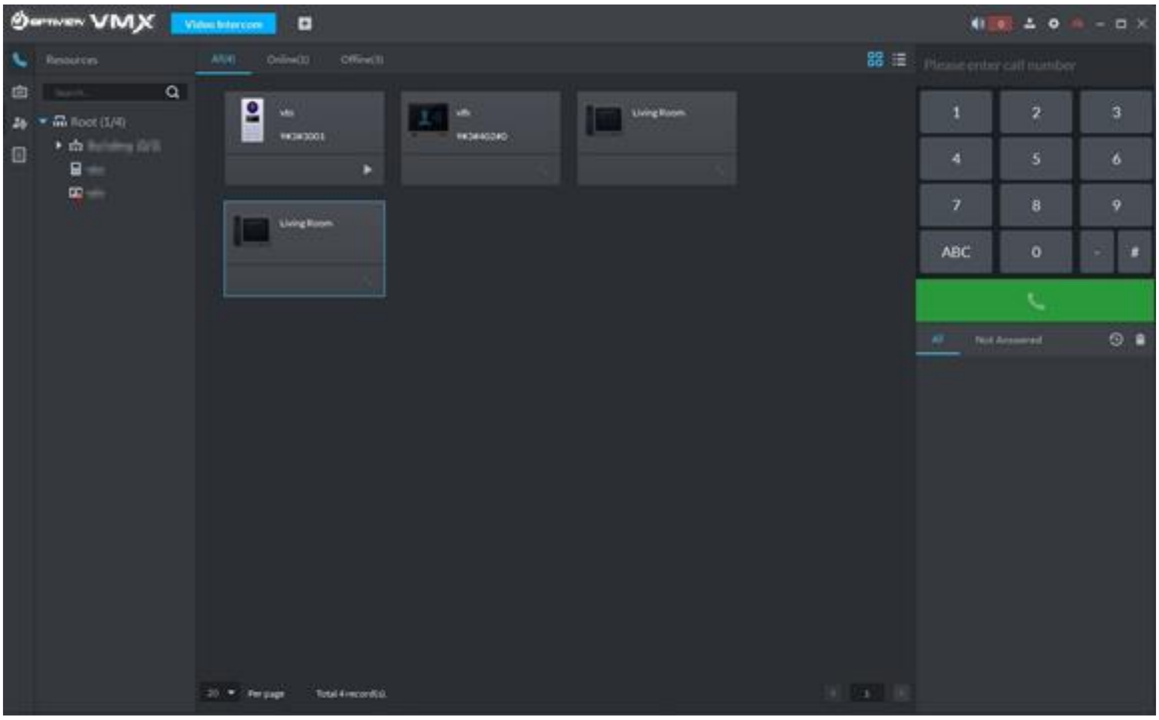

VMX
Video Intercom
Resources
All(4)
Online(1)
Offline(3)
Root (1/4)
Living Room
Living Room
Please enter call number
1
2
3
4
5
6
7
8
9
ABC
0
-
#
All
Not Answered
Per page
Total 4 record(s)

Figure 3-410 Call center

Step 2 You can call VTO and VTH on the interface of **Call Center**.

- Platform calls VTO

  Select VTO in the device list; click corresponding ▶ of VTO and call VTO. The system pops out call interface and realizes video talk. See Figure 3-411. Following operations are supported during call.

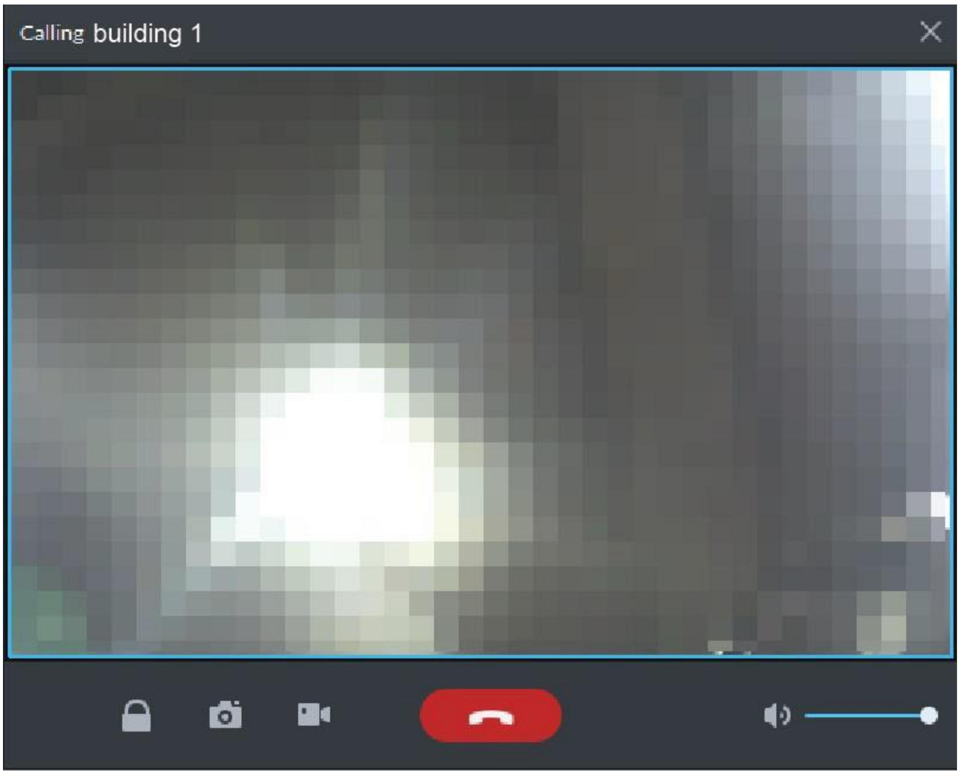
  ◇ 🔒, if VTO is connected to lock, click the icon to unlock.

  ◇ 📷, click the icon to capture picture, the snapshot is saved into the default directory installed by client. If you need to modify the save path of snapshot, refer to **3.3.4 Setting Snapshot** for more details.

  ◇ 📹, click the icon to start record, and click again to stop record. The video is saved in default path installed by client. If you need to modify the save path, refer to **3.3.5 Setting Recording Parameter** for more details.

  ◇ 📞, click the icon to hang up.

Figure 3-411 Call VTO



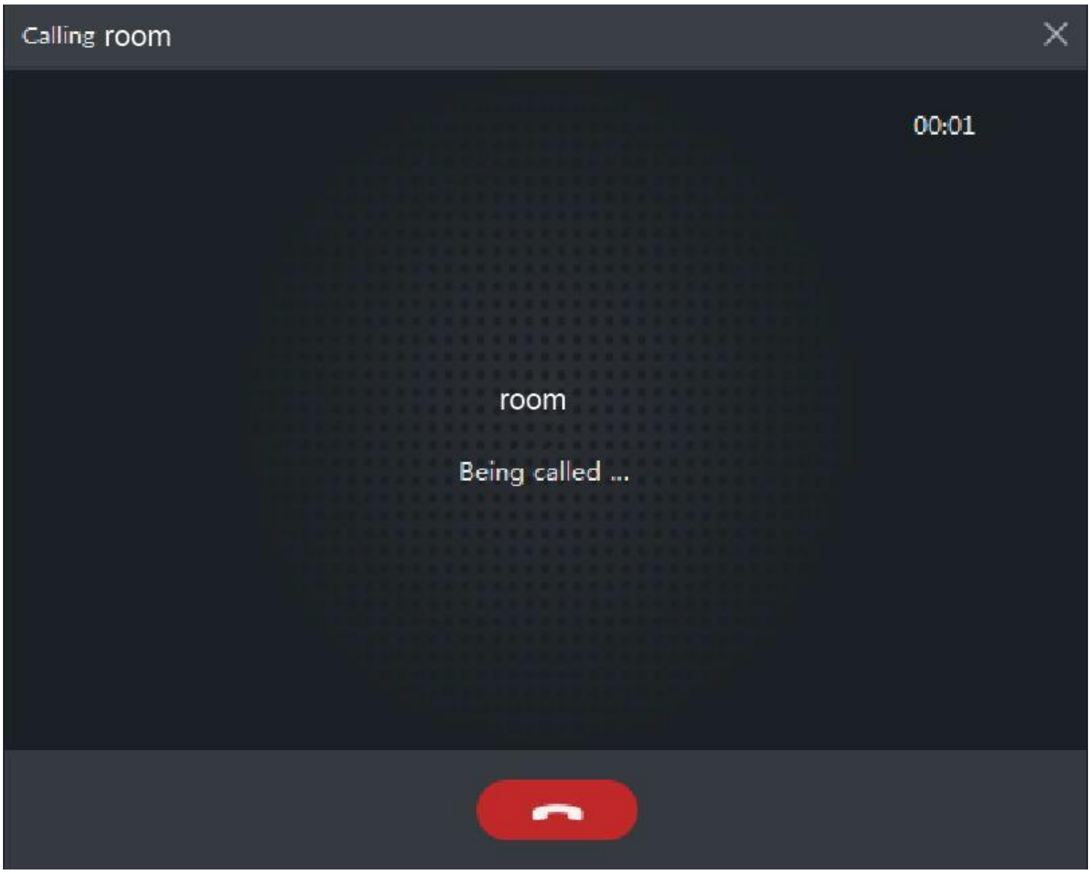
- Platform call VTH

  Select VTH from the device list, click ☎ on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait …**, see Figure 3-412. There are two modes for answering the call.

  ◇ Answer by VTH, bidirectional talk between client and VTH. Press ☎ to hang up when you answer the call.

  ◇ If VTH fails to answer over 30s, busy or hang up direcly, then it means the callee is busy.

Figure 3-412 Call VTH



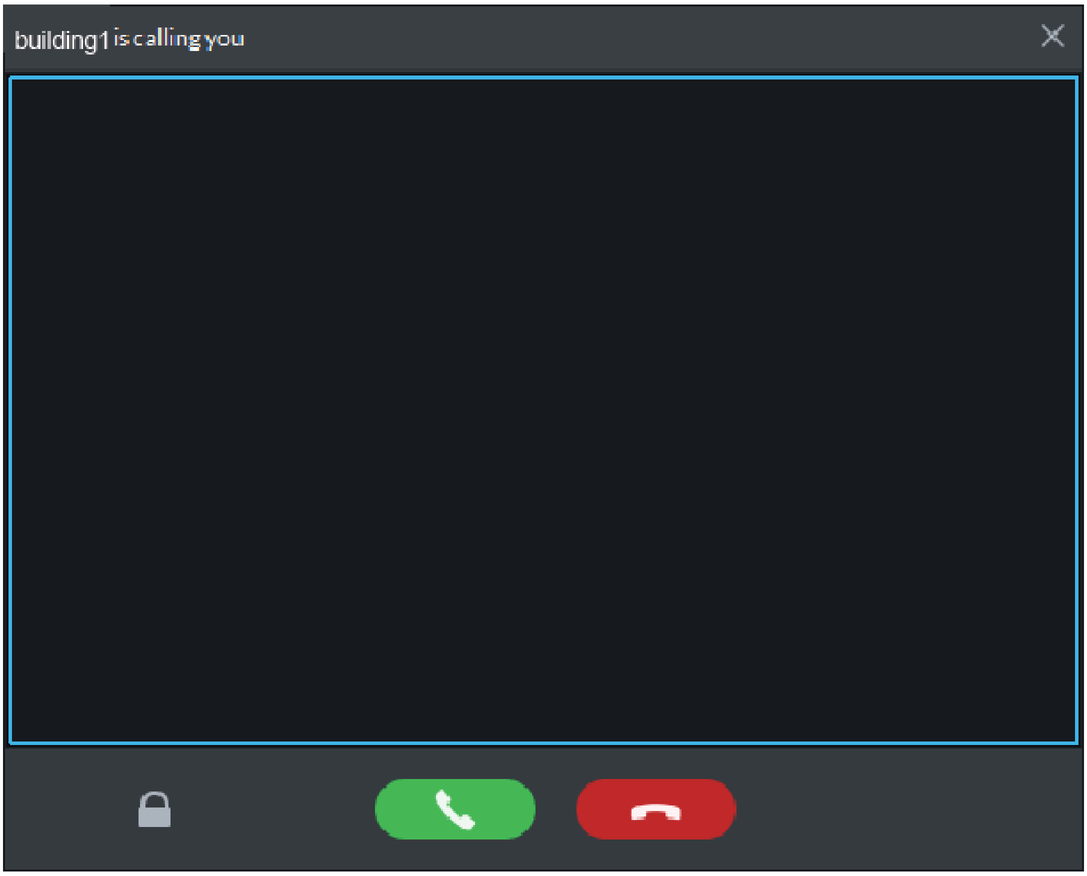
Being called ...

- VTO calls platform

  VTO calls platform, client pops up the dialog box of VTO calling. See Figure 3-413.

  - 🔒, if VTO is connected to lock, click the icon to unlock.
  - 📞, click the icon, answer VTO, realize mutual call after connected.
  - ☎, click the icon to hang up.

Figure 3-413 VTO calling platform



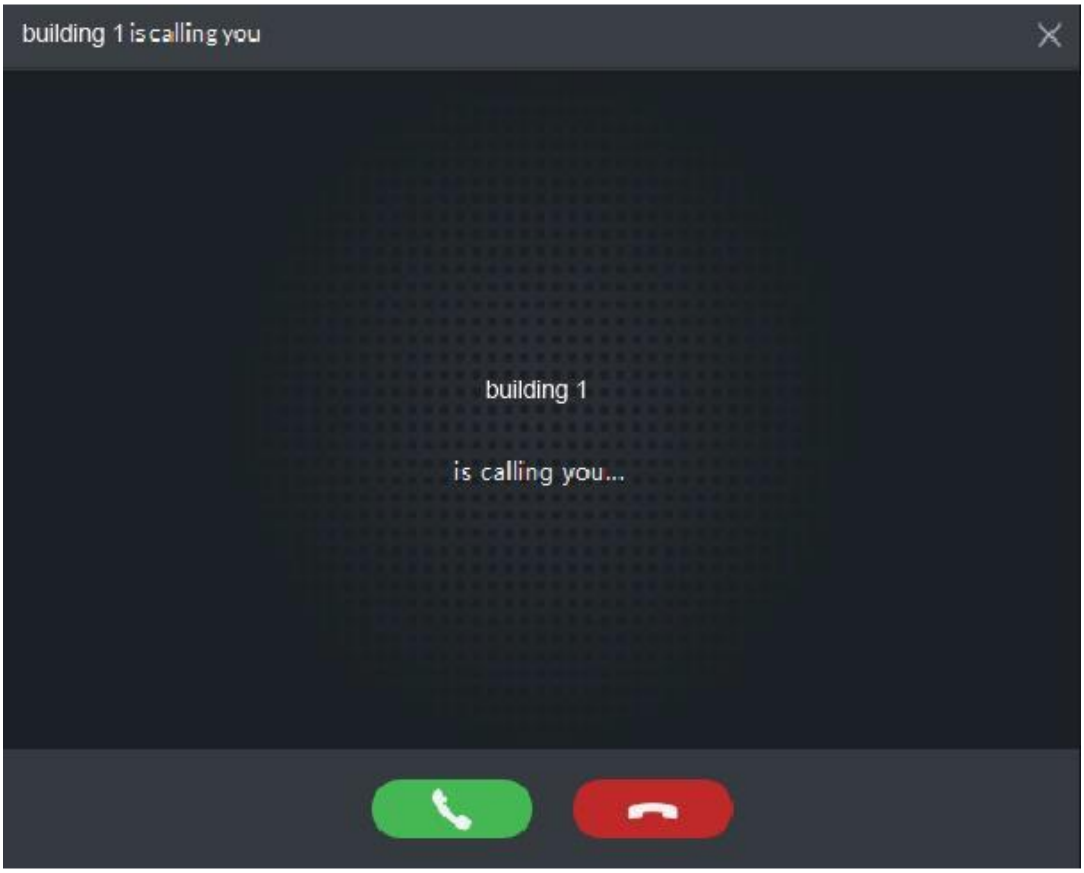
- VTH calls client

The client pops out the dialog box of VTH calling. See Figure 3-414. Click ☎ and realize talk with VTH.

◇ ☎, click the icon and answer VTO, realize mutual talk after connected.

◇ ☎, click the icon and hang up.

Figure 3-414 VTH calling client



building 1 is calling you

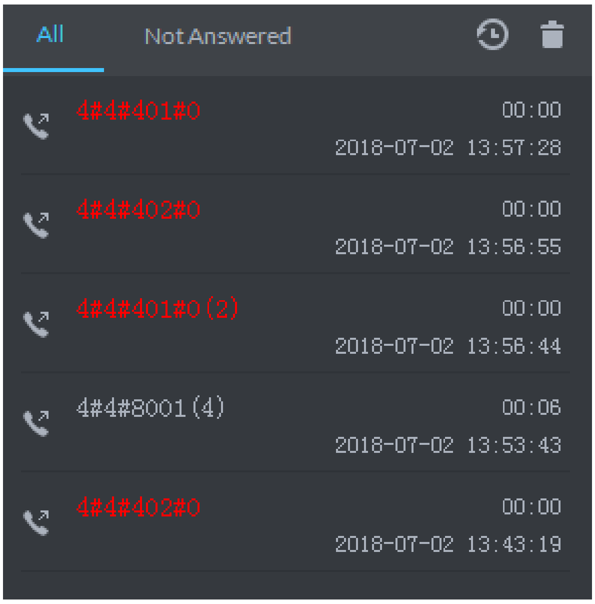
building 1

is calling you...

- Call via call record

  All the call records are displayed in the **Call Record** in the lower right corner of the interface of **Video Intercom**. See Figure 3-415. Move the mouse to the record, click ☎ and call back.

Figure 3-415 Call records



4#4#401#0 00:00
2018-07-02 13:57:28

4#4#402#0 00:00
2018-07-02 13:56:55

4#4#401#0 (2) 00:00
2018-07-02 13:56:44

4#4#8001 (4) 00:06
2018-07-02 13:53:43

4#4#402#0 00:00
2018-07-02 13:43:19

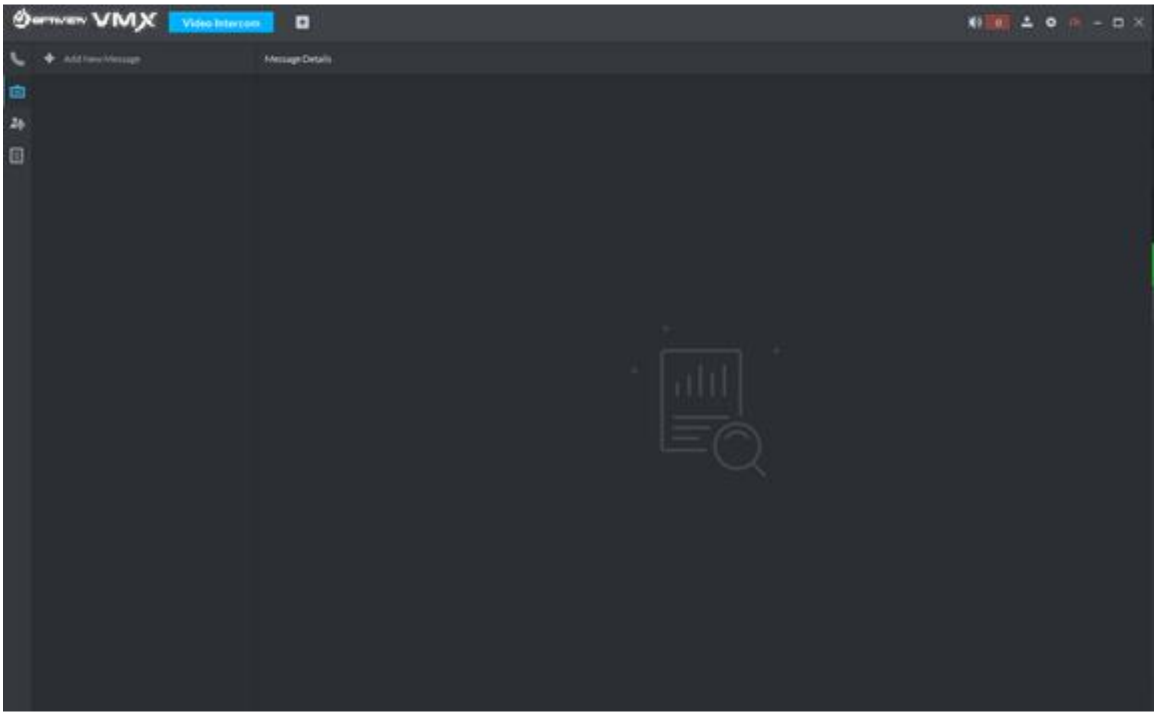
3.19.6.2 Releasing Info

The platform sends message to designated VTO.

Step 1 Click on the interface of **Video Intercom**.

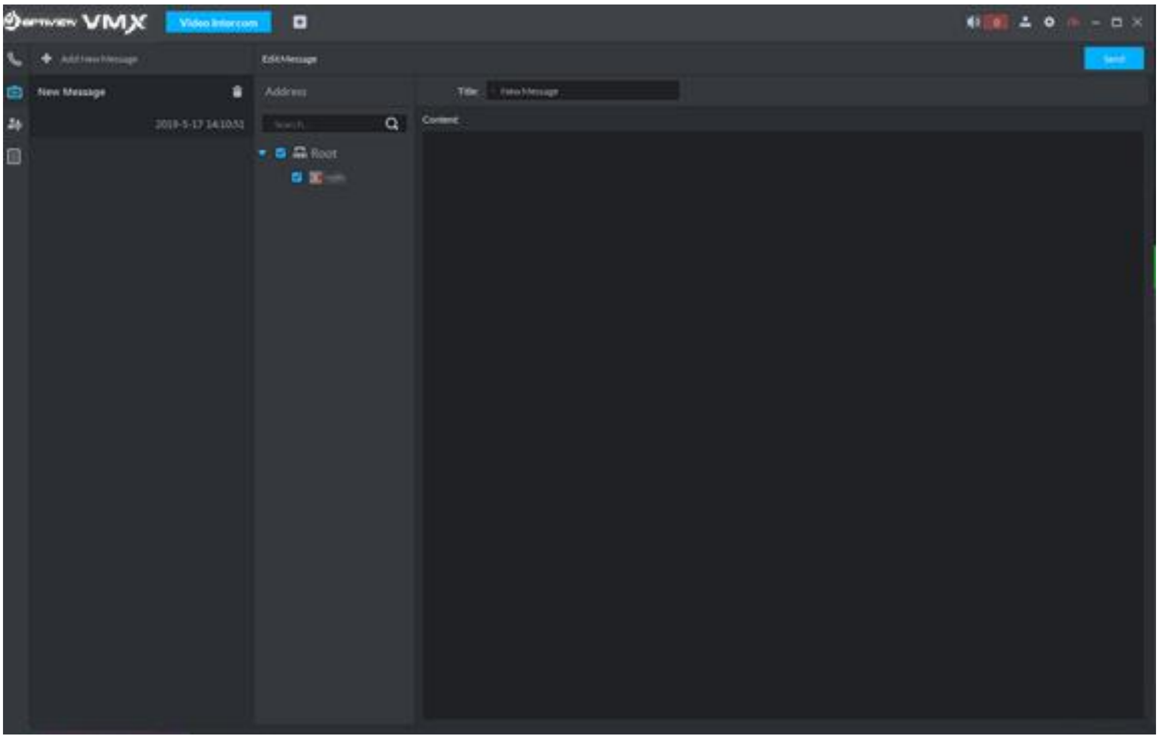
The system displays the interface of **Release Info**. See Figure 3-416.

Figure 3-416 Release info (1)


VMX
Video Intercom
Add New Message
Message Details

Step 2 Click **Add New Message**, select VTH and add release info. See Figure 3-417.

Figure 3-417 Release info (2)


VMX
Video Intercom
Add New Message
Edit Message
Send
New Message
Address
Title
Content
Root

Step 3 Click **Send**.

The VTH will receive the message after it is sent successfully.

3.19.6.3 Searching Video Intercom Log

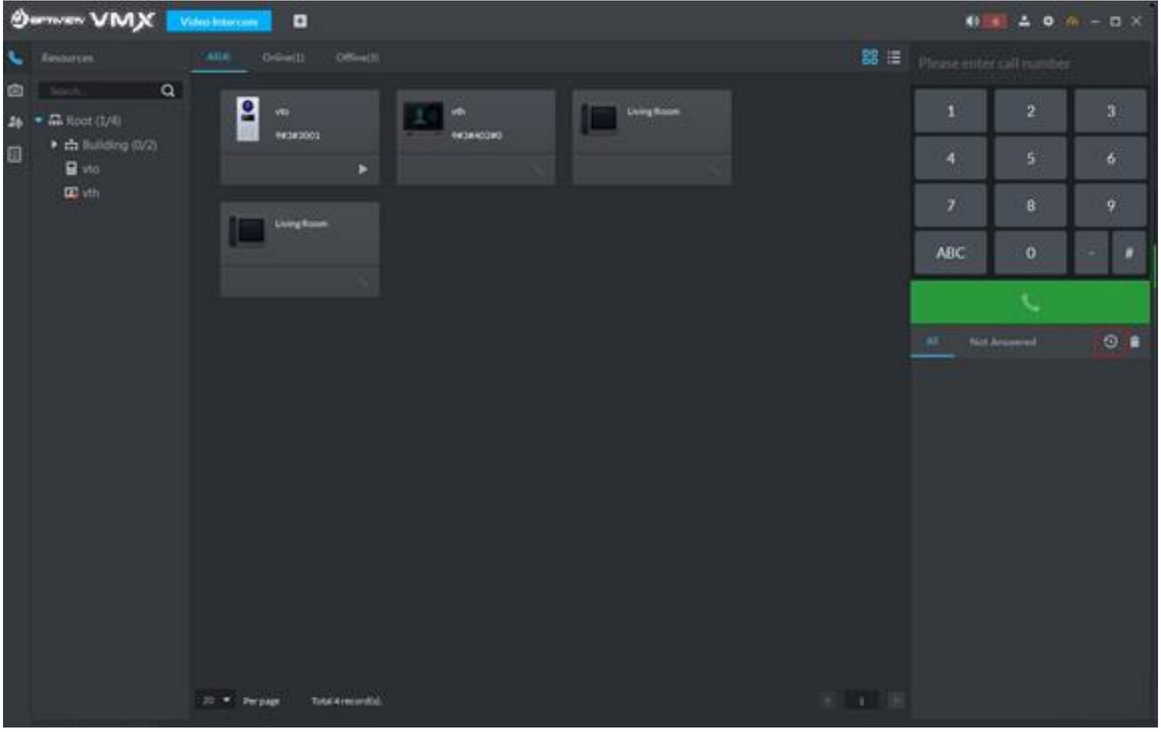
View log records and you can trace recorded calls.

Step 1 Enter the interface of video intercom log.

The system supports following two ways to enter.

- Click ▤ on the interface of **Video Intercom**.
- Click ☎ and enter console on the interface of **Video Intercom**. See Figure 3-418.

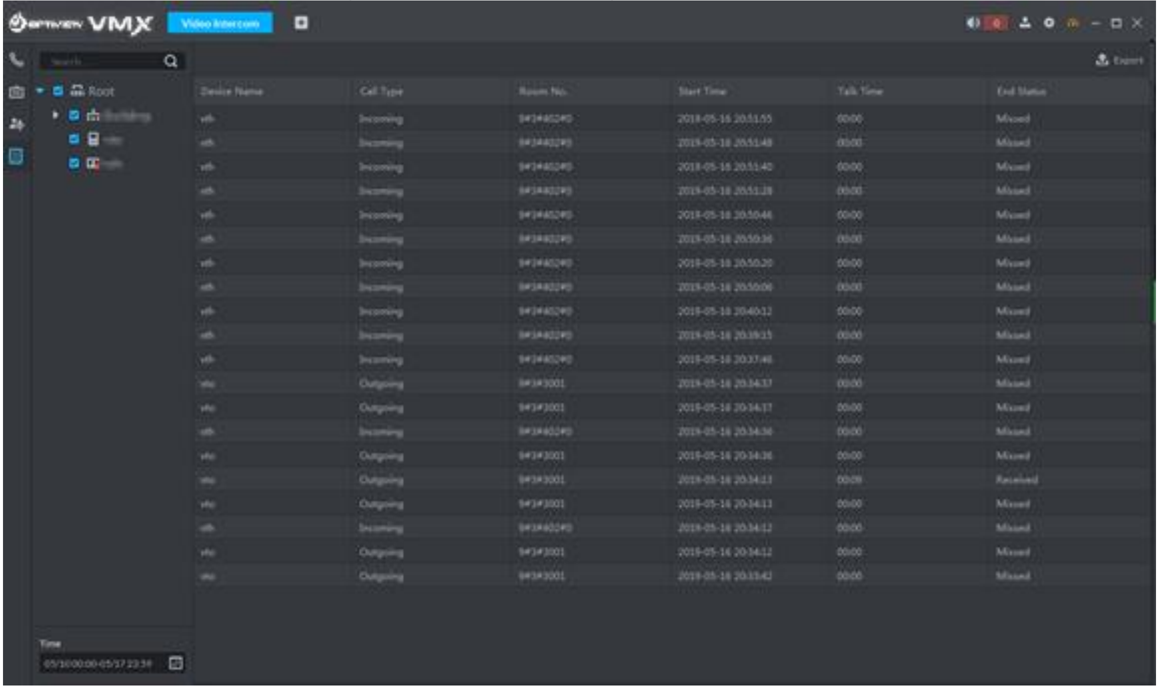
Figure 3-418 Enter log interface


VMX
Video Intercom
Resources
All(4)
Online(1)
Offline(3)
Root (1/4)
Building (0/2)
vto
vth
Living Room
Living Room
Please enter call number
1
2
3
4
5
6
7
8
9
ABC
0
-
#
All
Not Answered
20
Per page
Total 4 record(s).

Step 2 Set conditons, click **Search**.

The system displays the log info. See Figure 3-419

Figure 3-419 Search log

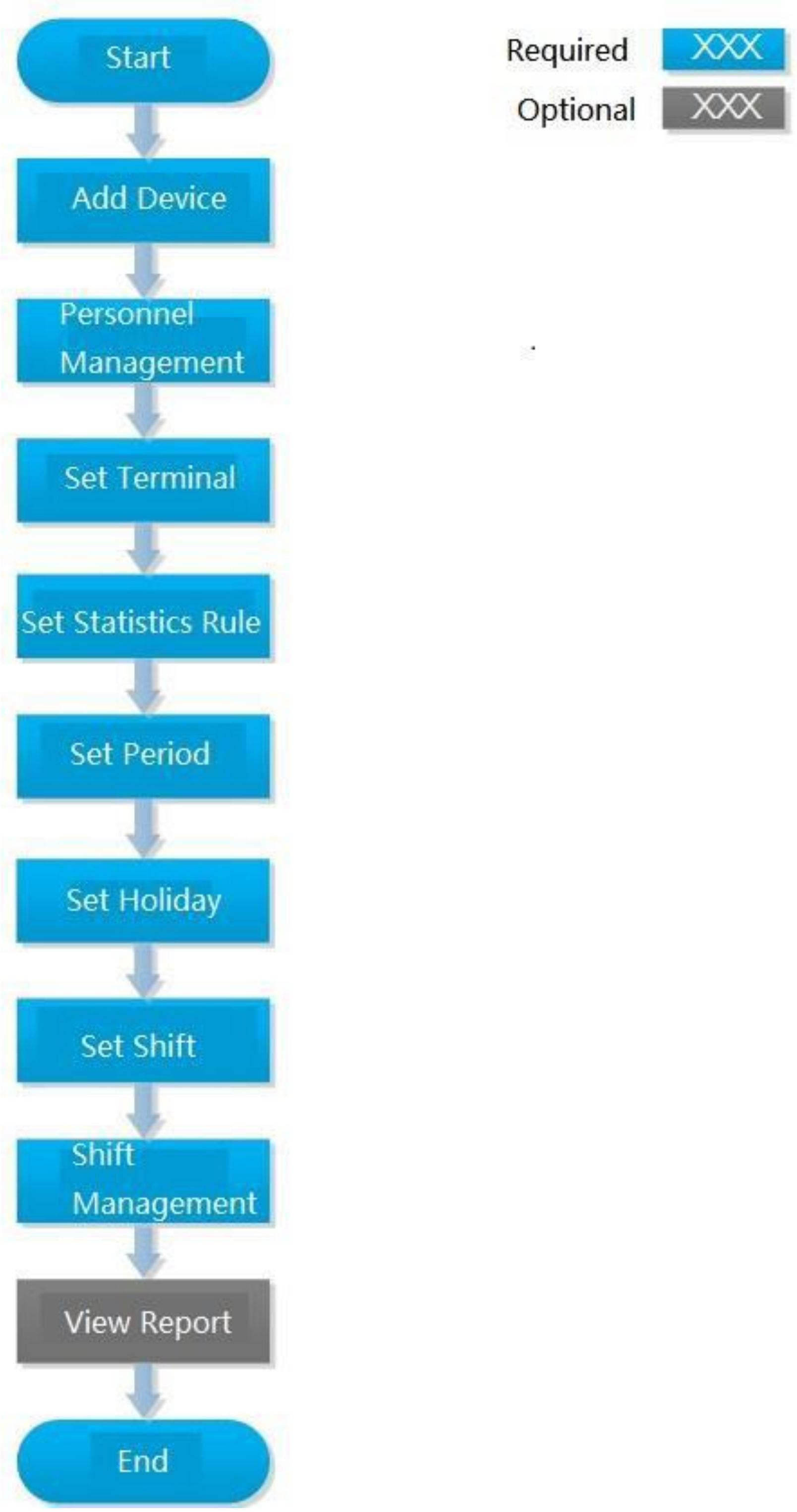

VMX
Video Intercom
Export
Root
Device Name
Call Type
Room No.
Start Time
Talk Time
End Status
Time

Step 3 Click **Export** and the logs will be saved locally according to system prompt.

3.20 Attendance Management

Add attendance device on platform, and you can manage and configure attendance, view attendance data on platform. The attendance operation flow is shown in Figure 3-420.

Figure 3-420 Attendance flow


Start
Add Device
Personnel Management
Set Terminal
Set Statistics Rule
Set Period
Set Holiday
Set Shift
Shift Management
View Report
End
Required XXX
Optional XXX

3.20.1 Adding Attendance Device

Add access control or face attendance for attendance. For more details, see **3.2.2.4 Adding Device**

3.20.2 Personnel Management

Use the module of personnel management for attendance personnel. If you want to add person, see **3.16 Personnel Management**

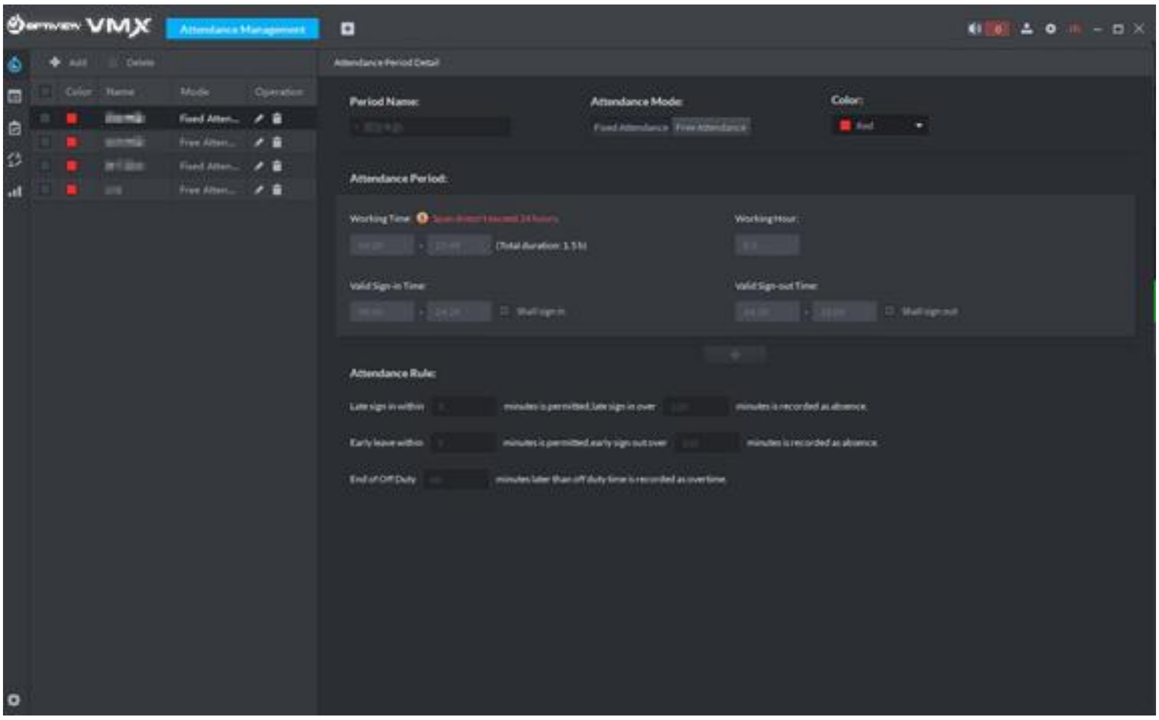
3.20.3 Setting Attendance Terminal

Make sure access control is used as attendance device, used to swipe card, record attendance info and upload attendance data.

Step 1 Click ⊞ and select **Attendance Mangement** on the interface of **Homepage**.

The system displays the interface of **Attendance Management**. See Figure 3-421.

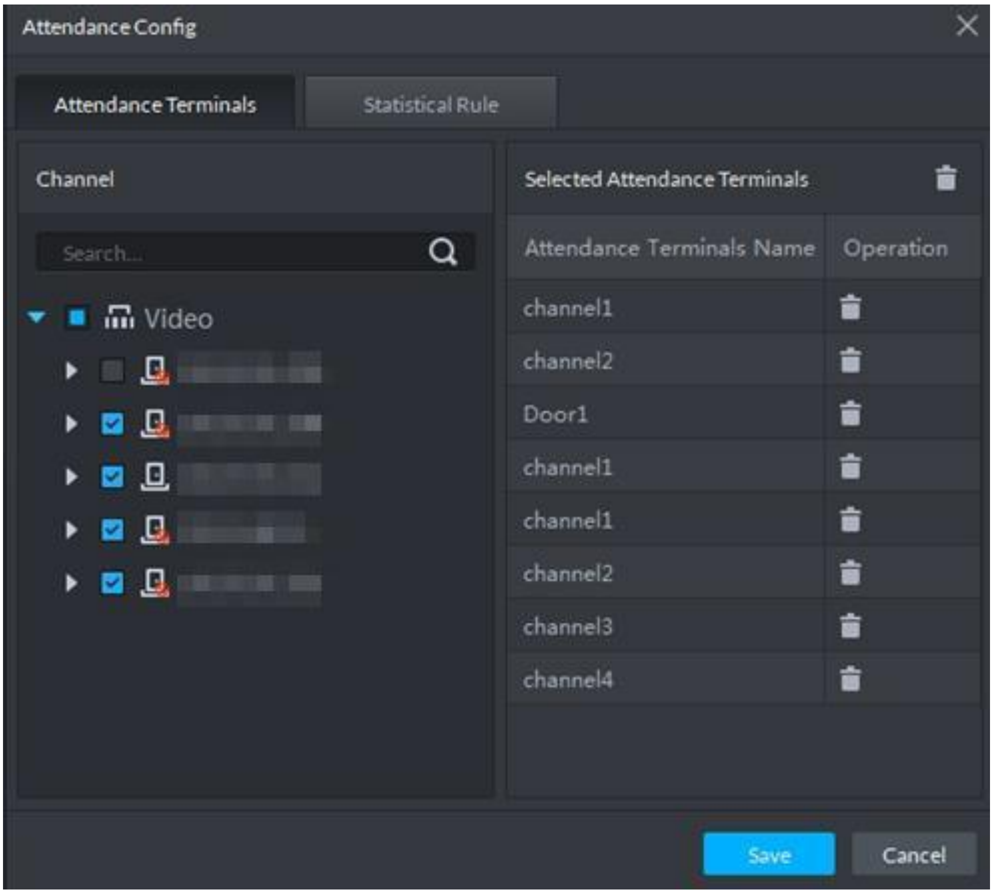
Figure 3-421 Attendance management


VMX
Attendance Management
Add
Delete
Color
Name
Mode
Operation
Fixed Atten...
Free Atten...
Fixed Atten...
Free Atten...
Attendance Period Detail
Period Name:
Attendance Mode:
Fixed Attendance
Free Attendance
Color:
Red
Attendance Period:
Working Time:
Working Hour:
(Total duration: 1.5 h)
Valid Sign-in Time:
Shall sign in
Valid Sign-out Time:
Shall sign out
Attendance Rule:
Late sign in within
minutes is permitted, late sign in over
minutes is recorded as absence.
Early leave within
minutes is permitted, early sign out over
minutes is recorded as absence.
End of Off Duty
minutes later than off duty time is recorded as overtime.

Step 2 Click ⚙ on the lower left corner of the interface, select **Attendance Terminal**.

The system displays the interface of **Attendance Terminal**. See Figure 3-422.

Figure 3-422 Attendance config


Attendance Config
Attendance Terminals
Statistical Rule
Channel
Search...
Video
Selected Attendance Terminals
Save
Cancel

Attendance Terminals Name	Operation
channel1	🗑
channel2	🗑
Door1	🗑
channel1	🗑
channel1	🗑
channel2	🗑
channel3	🗑
channel4	🗑

Step 3 Select access control channel from the left list, click **Save**.

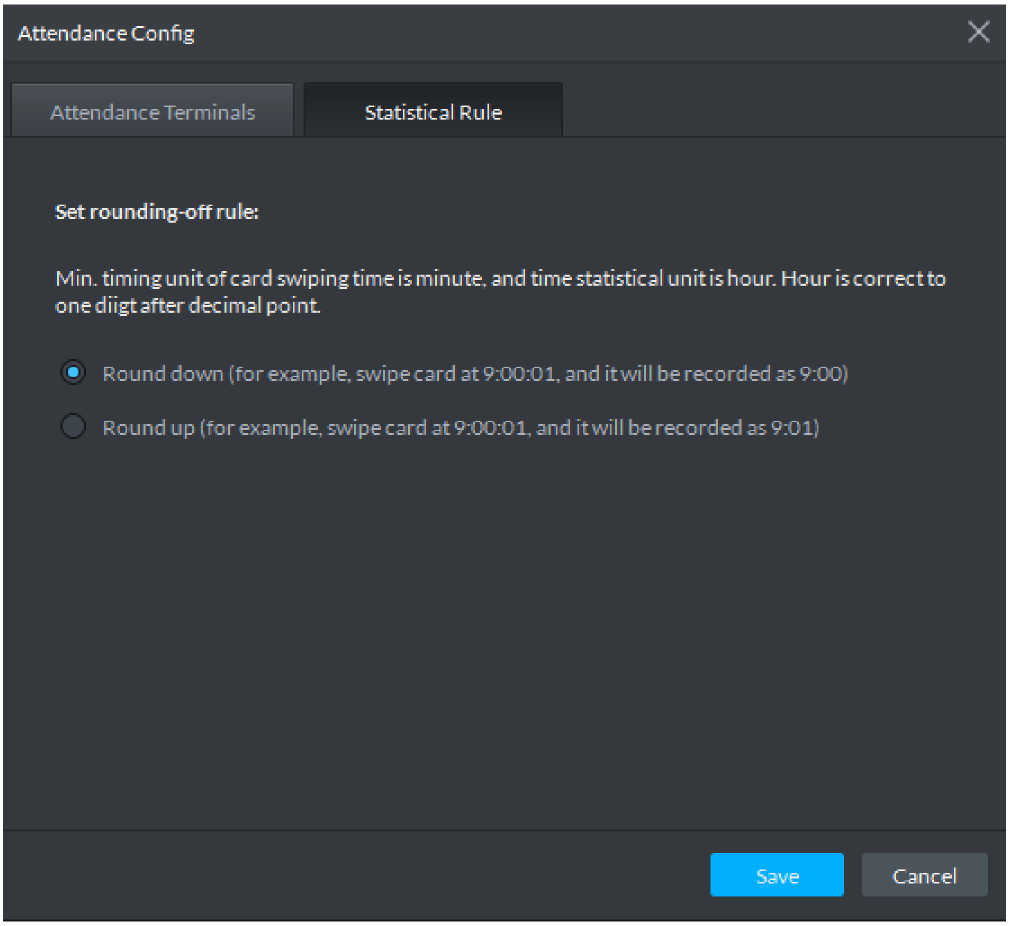
You can find needed device by search function, the system supports fast search.

3.20.4 Setting Statistics Rule

Minimun timing unit of swiping card is minute, the satistics rule of dealing with second is round up and round down. For example, swipe card at 09:00:01, if the rule is set as round down, then the time of swiping card is 09:00; if the rule is set as round up, then the time of swiping card is 09:01.

Step 1 Click at the lower left corner on the interface of **Attendance Management**, select **Statistics Rule**. The interface of **Statistical Rule** is displayed. See Figure 3-423

Figure 3-423 Set statistics rule


Attendance Config
Attendance Terminals
Statistical Rule

Set rounding-off rule:

Min. timing unit of card swiping time is minute, and time statistical unit is hour. Hour is correct to one diigt after decimal point.

● Round down (for example, swipe card at 9:00:01, and it will be recorded as 9:00)

○ Round up (for example, swipe card at 9:00:01, and it will be recorded as 9:01)

Save
Cancel

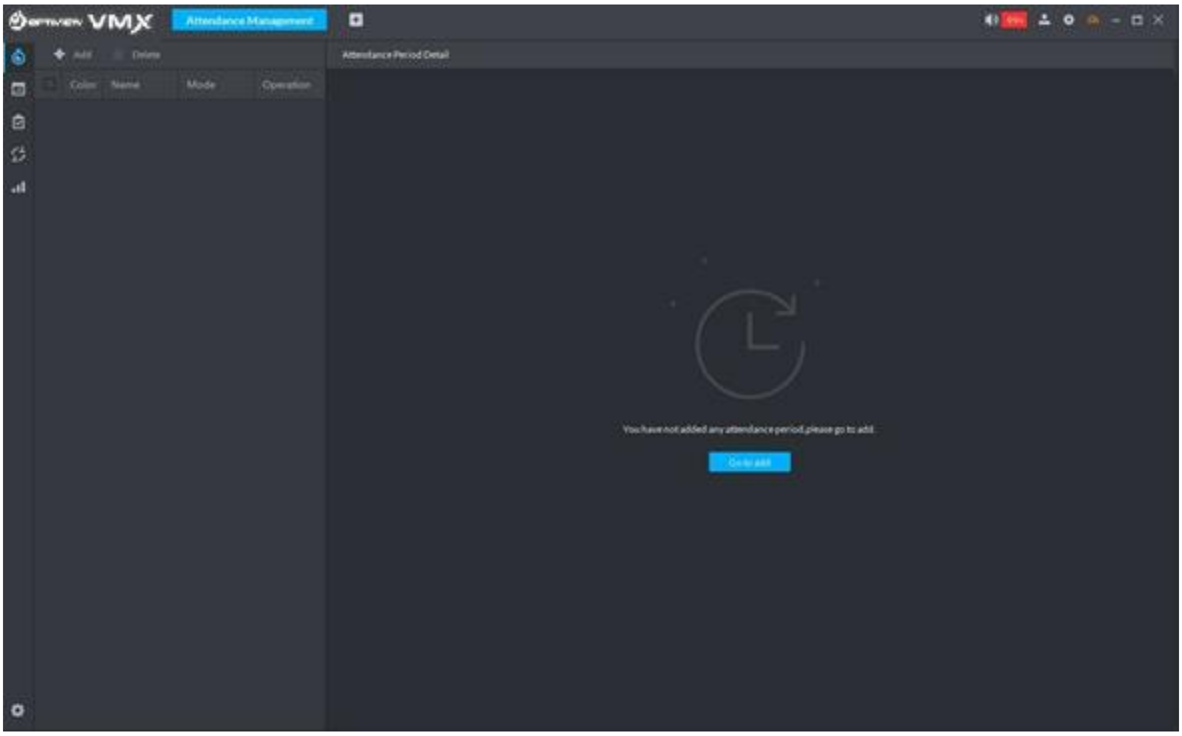
Step 2 Select rule and click **Save**.

3.20.5 Setting Attendance Period

Set attendance period, which can be used as time evidence to judge if people attend, late or leave early.

Step 1 Click ⏱ on the interface of **Attendance Management**.

The interface of **Attendance Management** is displayed. See Figure 3-424.


VMX
Attendance Management
Add
Delete
Color
Name
Mode
Operation
Attendance Period Detail
Go to add

You have not added any attendance period,please go to add.

Figure 3-424 Attendance period

Step 2 Click on top left corner of the interface.

The new attendance period interface is displayed.

Step 3 Set parameters of attendance period.

The priority of rules set by Pro is higher than that of the device itself.

There are two types of attendance according to different attendance mode and different config.

- Fixed attendance requires you to sign in and sign out within the designated period. For configuration details, see Figure 3-425 and Figure 3-426. For parameter details, see Table 3-59.

Figure 3-425 Attendance period detail (1)

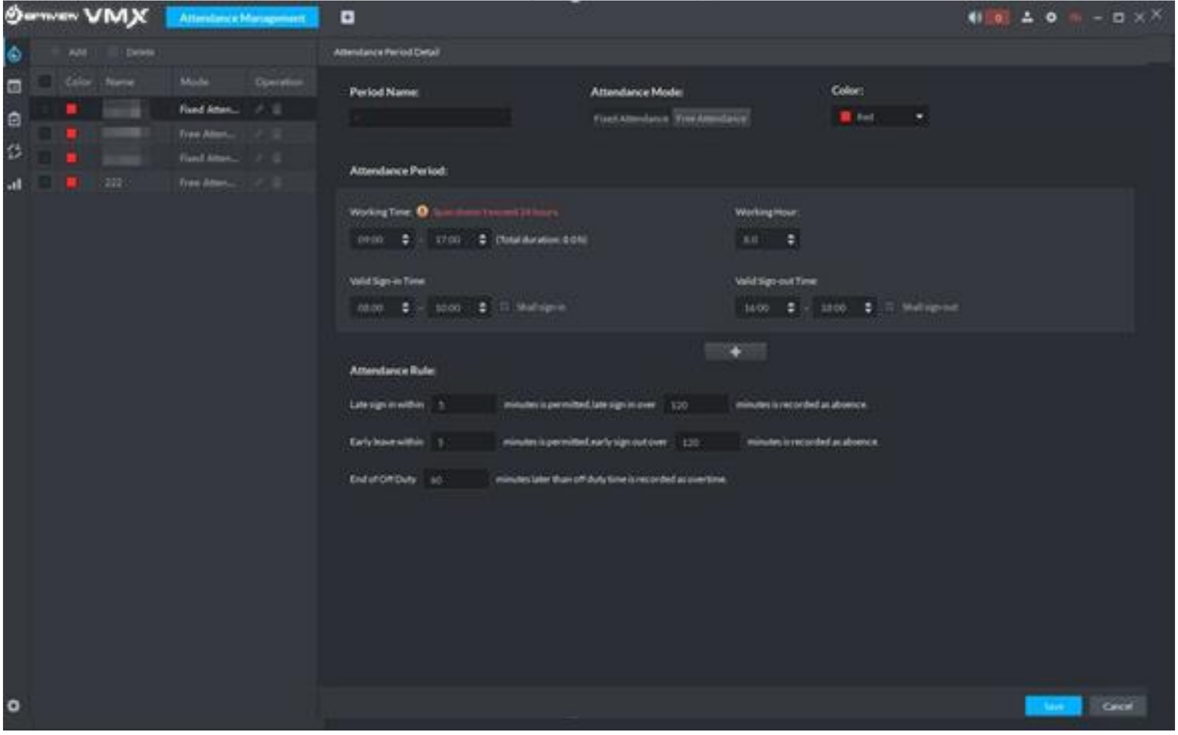

Attendance Management
Attendance Period Detail
Period Name:
Attendance Mode:
Color:
Attendance Period:
Attendance Rule:

Figure 3-426 Attendance period detail (2)

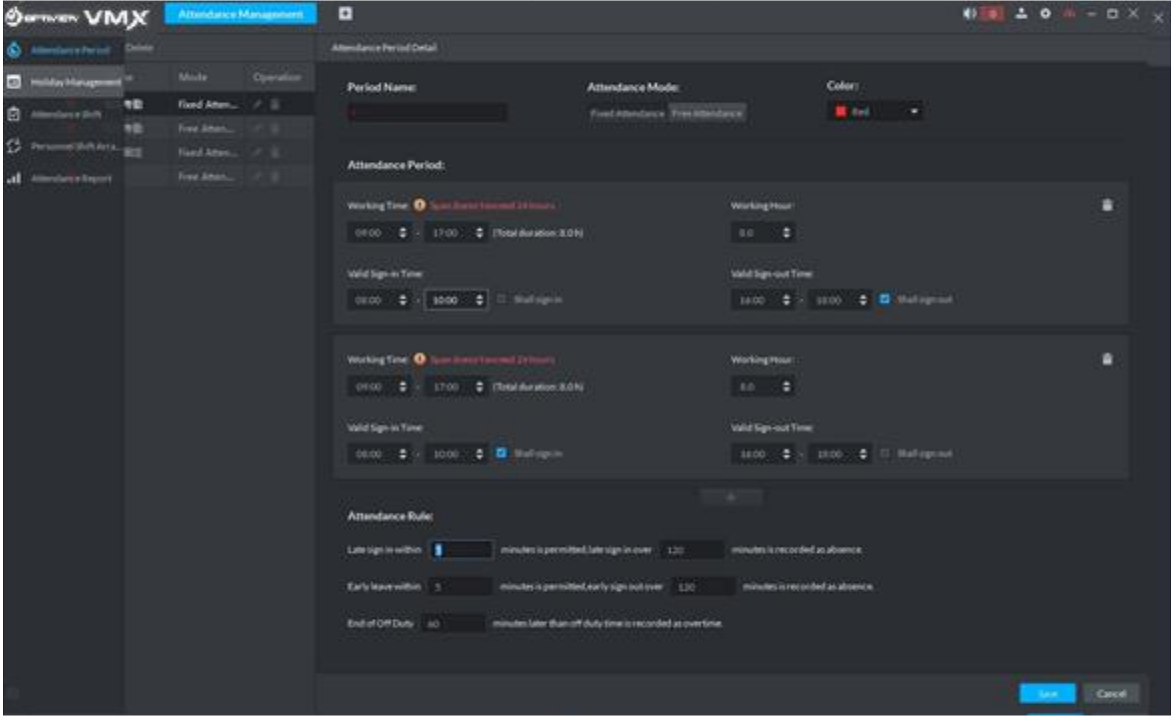

Attendance Management
Attendance Period Detail
Period Name:
Attendance Mode:
Color:
Attendance Period:
Attendance Rule:

Table 3-59 Fixed attendance parameter description

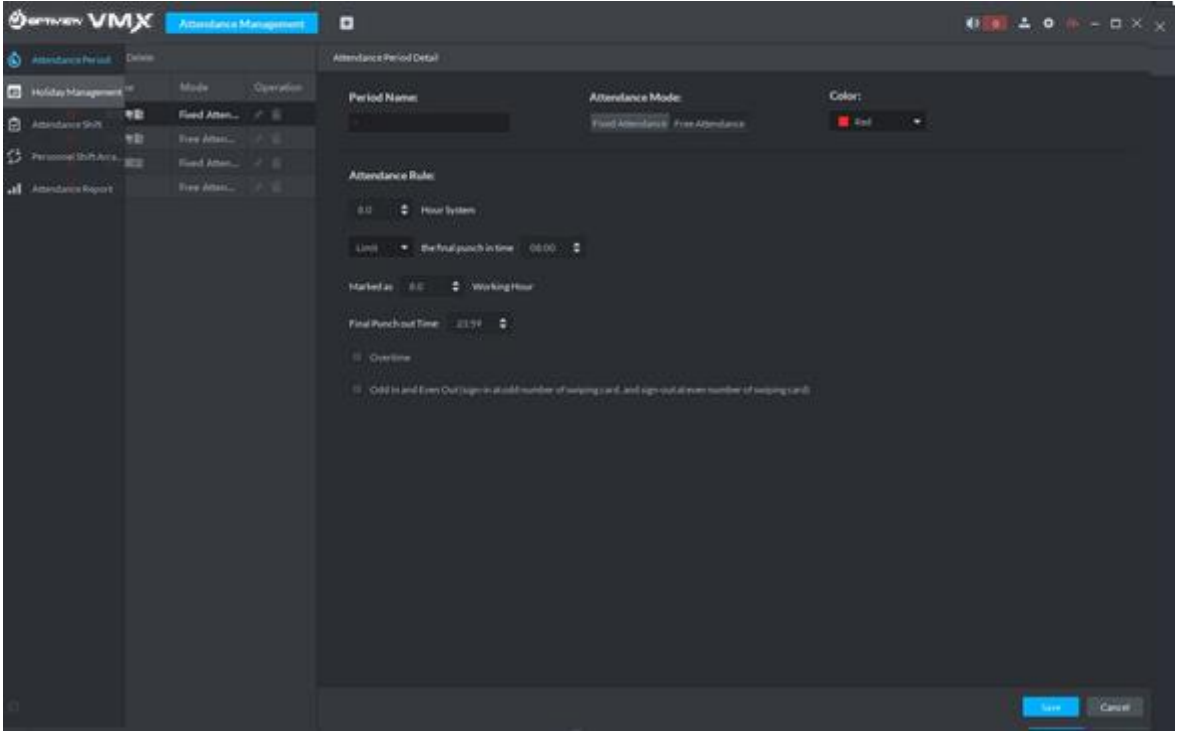
Parameter	Description
Period name	Custom period name, used to recognize period, such as early shift and night shift.
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Attendance mode	Set as **Fixed Attendance**.

Parameter	Description
Working time	Set corresponding working hour of period. Attendance time supports cross-day, but not exceeds 24 hours. One attendance period supports max two types of attendance time. ● If attendance time needs to be split into twice, such as morning and afternoon, then it needs to click +, set second working time and sign-in sign-out period. ● If you set two types of attendance time, then it needs to sign in and sign out accoriding to the configured attendance time, which can be considered as normal attendance.
Working hour	Please fill in according to actual situation.
Valid sign-in time	If working time is set from 09:00-18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Configurerules are as follows: ● The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is considered as sign-in time. ● The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Valid sign-out time	
Shall sign in	If you set two working time, then the second working time can cancel sign in, you don’t have to sign in when you work at the second working time, and the start time of working time can be used as sign-in time.
Shall sign out	If you set two working time, then the first working time can cancel sign in, you don’t have to sign out when you finish work at the second working time, and the end time of working time can be used as sign-out time.
Work sign-in over _minutes recorded as late	Define the rules of late, absence and early leave. Suppose set **Work sign-in over_minutes recorded as late** as 5 minutes; **Late sign-in over _minutes recorded as absence** is set as 60 minutes**; Off duty _ minutes in advance recorded as early leave** is set as 10 minutes; **Early leave exceeds_ minutes recorded as absebce** is set as 30 minutes. Details are as follows. ● Late When work sign-in is later than start time of working time, and 5 minutes< period ≤60 minutes, then it is recorded as late.
Late sign-in over _minutes recorded as absence	
Off duty_ minutes in advance recorded as early leave	

Parameter	Description
Early leave exceeds_ minutes recorded as absebce	● Early leave When off duty sign-out time is earlier than end time of working time, and 10 minutes< period ≤30 minutes, then it is recorded as early leave. ● Absence When work sign-in time is later than start time of working time, and period > 60 minutes, then it is recorded as absence. When off duty sign-out time is earlier than end time of working time, and period> 30 minutes, then it is recorded as absence.
Off duty sign-out over_minutes recorded as overtime	Define overtime rule. Suppose **Off duty sign-out over_minutes recorded as overtime** is set as 120 minutes, off duty sign-out time is later than end time of working time, and period >120 minutes, then it is recorded as overtime, overtime period is **Period – 120 minutes**.

- Free Attendance, you are required to sign in and sign out within the specific period. See Figure 3-427. For parameter details, see Table 3-60.

Figure 3-427 Free attendance


VMX
Attendance Management
Attendance Period
Holiday Management
Attendance Shift
Personnel Shift Arra...
Attendance Report
Delete
Mode
Operation
Fixed Atten...
Free Atten...
Fixed Atten...
Free Atten...
Attendance Period Detail
Period Name:
Attendance Mode:
Fixed Attendance
Free Attendance
Color:
Red
Attendance Rule:
Save
Cancel

8.0 Hour System

Limit the final punch in time 08:00

Marked as 8.0 Working Hour

Final Punch out Time 23:59

☐ Overtime

☐ Odd In and Even Out (sign-in at odd number of swiping card, and sign-out at even number of swiping card)

Table 3-60 Free attendance parameter description

Parameter	Description
Period name	Custom period name, used to recognize period, such as flexible attendance.
Attendance mode	Set as **Free Attendance**.
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Hour system	Set how many hours you have to work a day. For example, if you set 8,

Parameter	Description
	then it means you are required to work 8 hours.
Final punch in time	Set if it restricts latest punch in time; sign in after restricted time is recorded as late.
Mark as_working hour	Fill in working hout according to actual situation.
Final punch out time	You are required to sign out before the designated time, otherwise no sign out is recorded.
Overtime	Working over__hours is recorded as overtime. For example, working hour is 8 hours a day, and if you work overtime for 2.5 hours, then it is recorded as overtime, then you can set 10.5 here.
Work over_hours recorded as overtime	
Odd in even out	System counts the times of card-swiping within one day. If the card-swiping times number of a person is an odd number, 1 for example, system thinks he has not checked out yet; if the number is an even number, 2 for example, system thinks he has checked out. If the time duration between 2 card-swiping records is shorter than the threshold value configured on the platform, they will be taken as one swiping record. (The second one is too close to the first one and is taken as invalid.)
Continuous twice card swiping interval≥_minutes	

Step 4 Click **Save** and save period config.

If attendance period is already applied to attendance shift, then before deleting attendance period, first enter the interface of **Attendance Shift**, modify attendance shift, and delete attendance period before removing application of the attendance period.

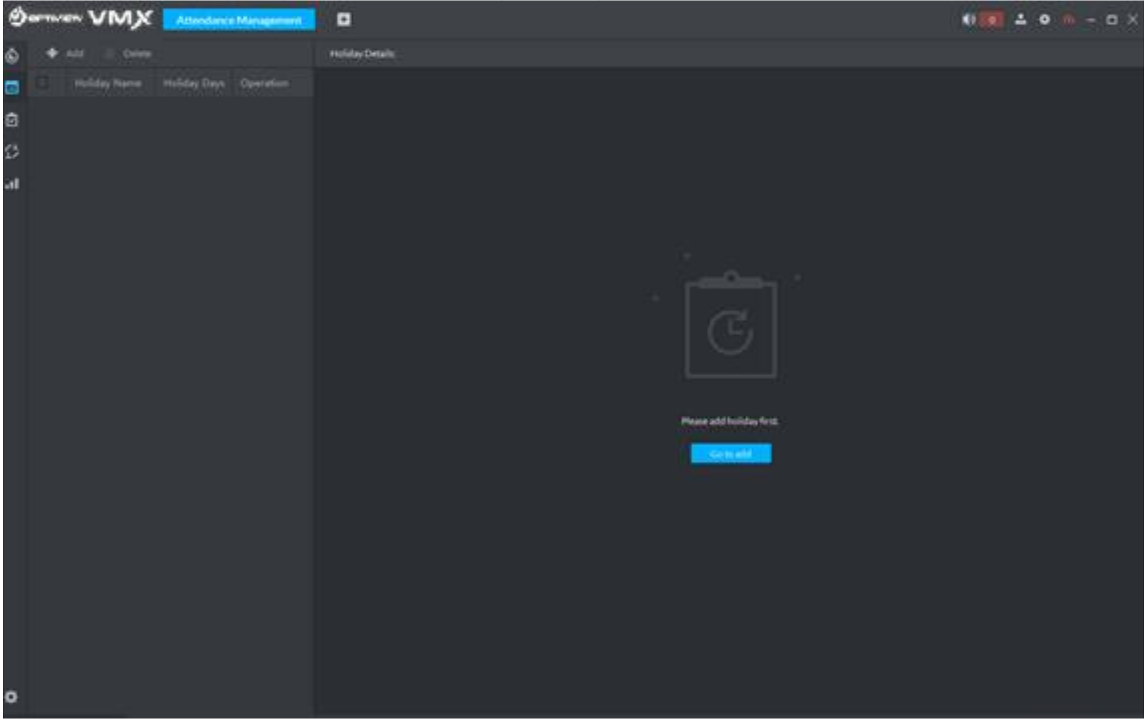
3.20.6 Setting Holiday

Set holiday time, used to judge overtime type during attendance statistics.

Step 1 Click on the interface of **Attendance Management**.

The interface of **Holiday Management** is displayed. See Figure 3-428.

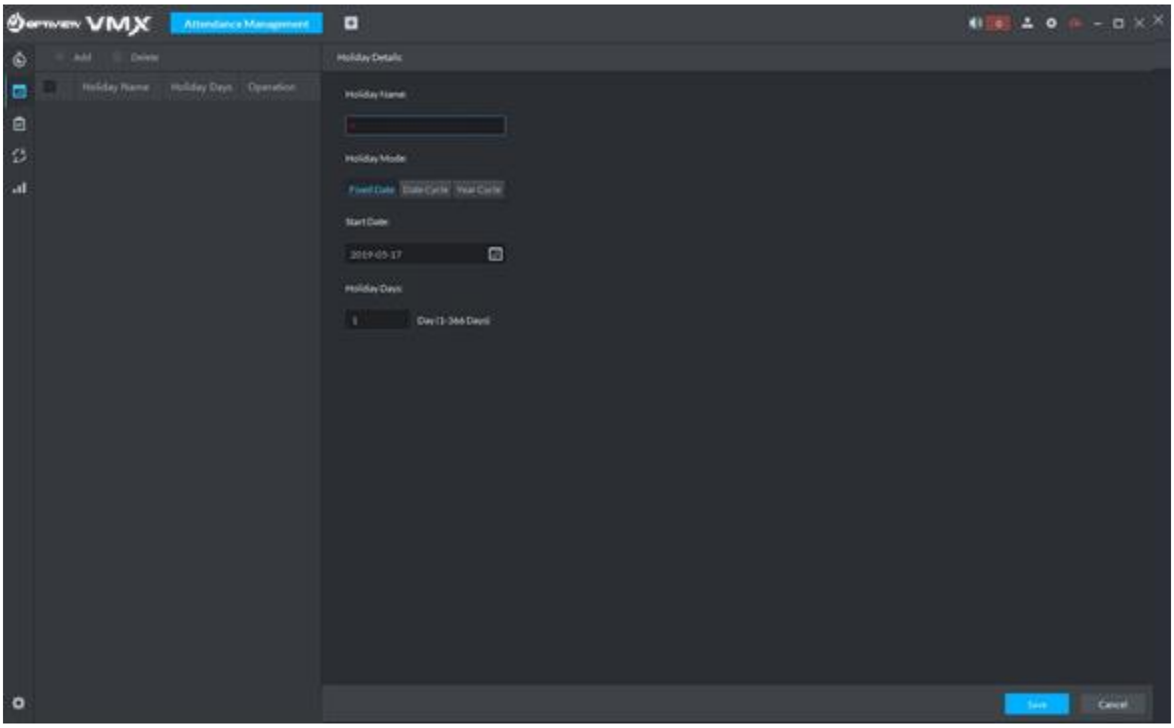
Figure 3-428 Holiday management


VMX
Attendance Management
Add
Delete
Holiday Name
Holiday Days
Operation
Holiday Details
Please add holiday first.
Go to add

Step 2 Click + on the upper left corner of the interface.

The add holiday interface is displayed. See Figure 3-429.

Figure 3-429 Add holiday


VMX
Attendance Management
Add
Delete
Holiday Name
Holiday Days
Operation
Holiday Details
Holiday Name
Holiday Mode
Fixed Date
Date Cycle
Year Cycle
Start Date
Holiday Days
Day (1-366 Days)
Save
Cancel

Start Date: 2019-05-17

Holiday Days: 1

Step 3 Set holiday details, three modes available. See Table 3-61 for more parameter details.

Table 3-61 Holiday mode description

Holiday mode	Description
Fixed Date	Set some specific date as holiday. For example, set June 7, 2019 (Dragon Boat Festival) as holiday, and lasts for 1 day, then set **Start**

Holiday mode	Description
	Date as June 7, 2019 and **Holiday Days** as 1.
Date Cycle	If the holiday is the fixed weekday of some week in some specific month, and it cycles according to year, which can be configured as data cycle. For example, if you want to set Mother’s Day as holiday, and it lasts for 1 day, then you can set **Start Date** as the second Sunday in May, and **Holiday Days** as 1.
Year Cycle	If the holiday is fixed date and it cycles according to year, which can be configured as year cycle. For example, set New Year’s Day as holiday, and it lasts for 1 day, then you can set **Start Date** as January 1 and **Holiday Days** as 1.

Step 4 Click **Save**.

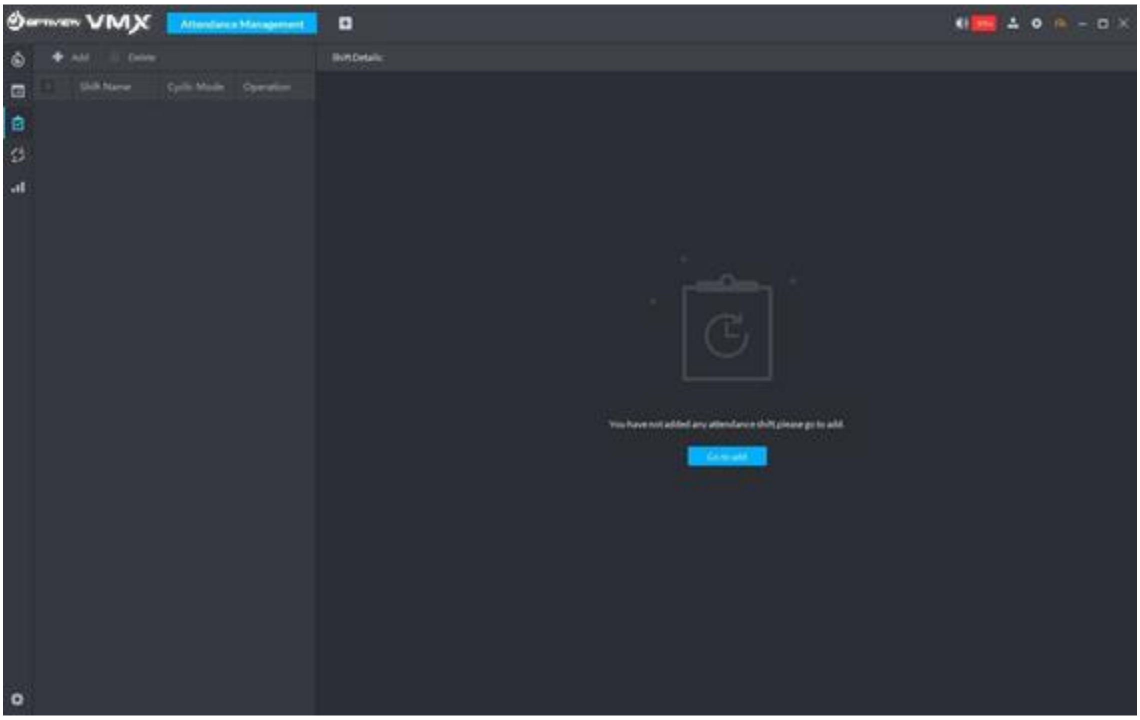
3.20.7 Setting Attendance Shift

Set attendance shift according to attendance period, used for department and personnel shift.

Step 1 Click ☑ on the interface of **Attendance Management**.

The interface of **Attendance Shift** is displayed. See Figure 3-430.

Figure 3-430 Attendance shift

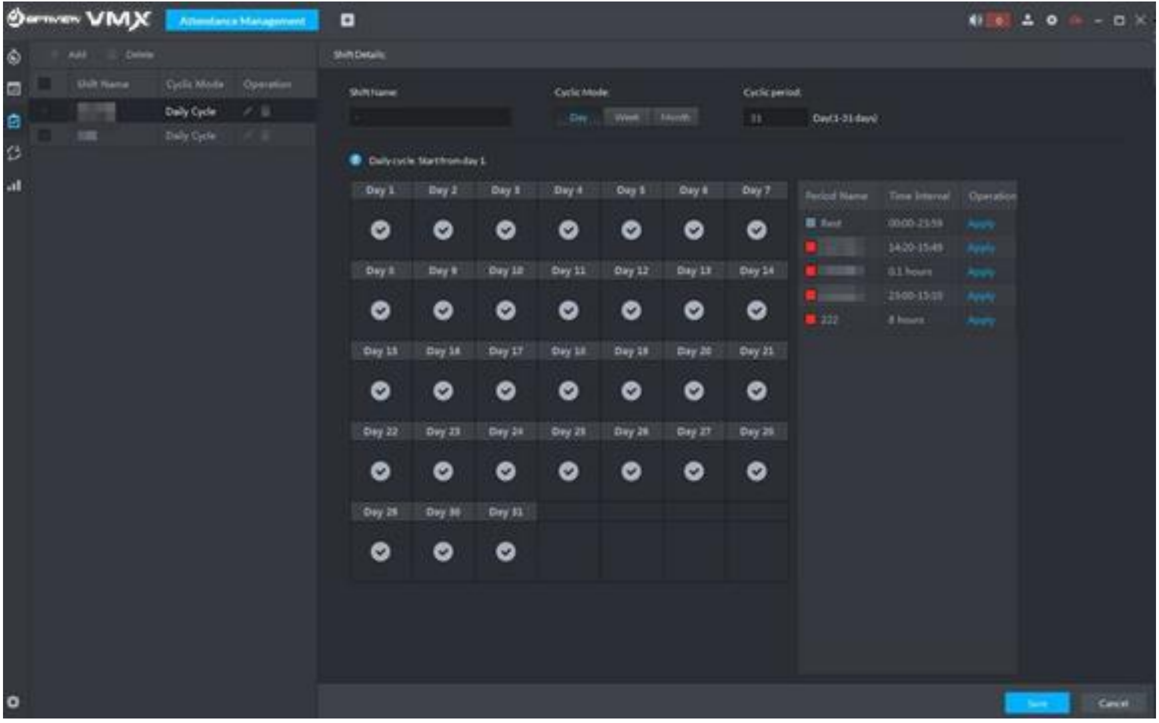


You have not added any attendance shift,please go to add.

Step 2 Click ✚ on the top left corner of the interface.

The add attendance shift interface is displayed. See Figure 3-431.

Figure 3-431 Set attendance shift (1)


VMX
Attendance Management
Add
Delete
Shift Name
Cyclic Mode
Operation
Daily Cycle
Daily Cycle
Shift Details
Shift Name
Cyclic Mode
Day
Week
Month
Cyclic period
31
Day(1-31 days)
Daily cycle. Start from day 1
Period Name
Time Interval
Operation
Rest
00:00-23:59
14:20-15:49
0.1 hours
23:00-15:10
222
8 hours
Apply
Save
Cancel

Step 3 Set shift details, select date, click Apply and arrange attendance period for date. See Figure 3-432. For parameter details, see Table 3-62.

Press the left mouse button and drag it on the date display area, you can select several dates quickly. ✓ means that the date is selected.

Figure 3-432 Set attendance shift (2)

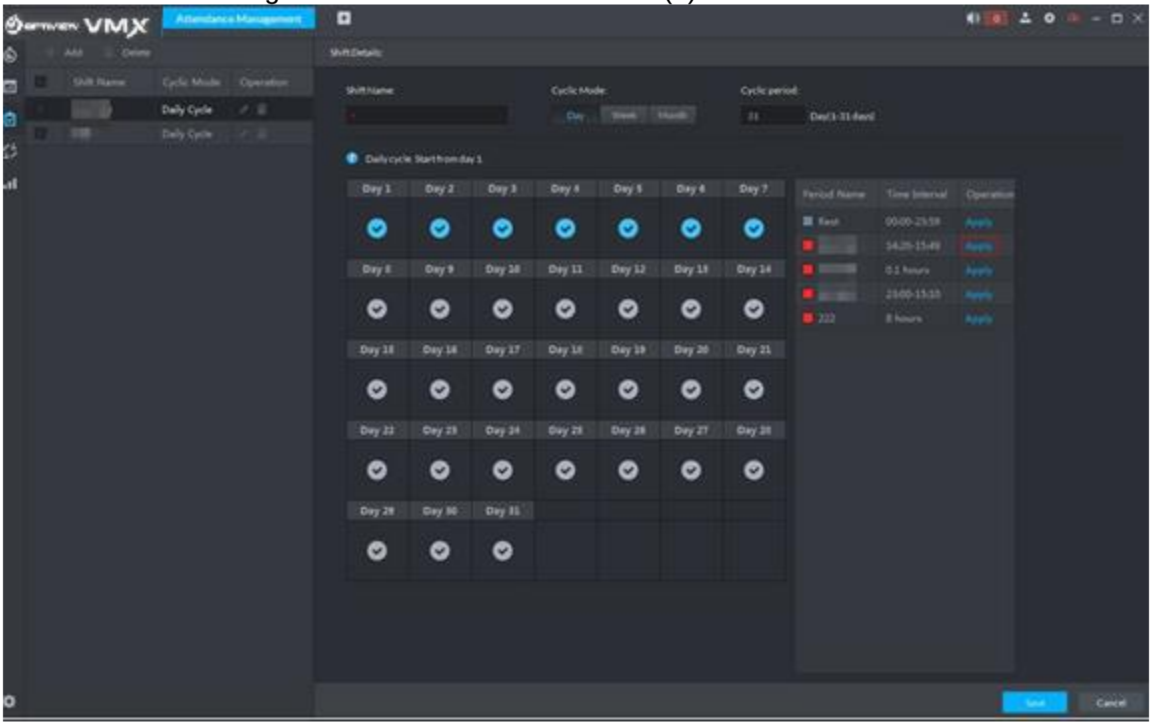

VMX
Attendance Management
Add
Delete
Shift Name
Cyclic Mode
Operation
Daily Cycle
Daily Cycle
Shift Details
Shift Name
Cyclic Mode
Day
Week
Month
Cyclic period
31
Day(1-31 days)
Daily cycle. Start from day 1
Period Name
Time Interval
Operation
Rest
00:00-23:59
14:20-15:49
0.1 hours
23:00-15:10
222
8 hours
Apply
Save
Cancel

Table 3-62 Attendance shift parameter description

Parameter	Note
Shift name	Custom period name, used to recognize shift.
Cycle mode	Day: Start cycle from the first day, cycle period can be set as any number from 1 to 31 according to day. For example, if you set 2, then the cycle period is 2 days. Week: There are 7 days in a week by default, it starts cycle from Sunday, and so Sunday is required to be set as the first day. Cycle period can be set as any number from 1 to 4. For example, if you set 2, then 2 weeks can be a cycle period. Month: There are 31 days in a month by default, it starts cycle from the current day (If the date does not exist, then it will be deleted during shift arrangement), cycle period can be set as any number from 1 to 3 according to month. For example, if you set 2, then 2 months can be a cycle period.
Cycle period	

Step 4 Click **Save** to save shift config.

Delete in-use attendance shift: Enter the interface of **Personnel Shift Arrangement**, check if there are shifts need to be deleted for all personnel shifts, please delete after remove the relation.

3.20.8 Shift Management

Make shifts for personnel or department, meanwhile it makes temporary shift for personnel. The shift priority is temporary shift > holiday > personnel shift > department shift.

3.20.8.1 Personnel/Department Shift Arrangement

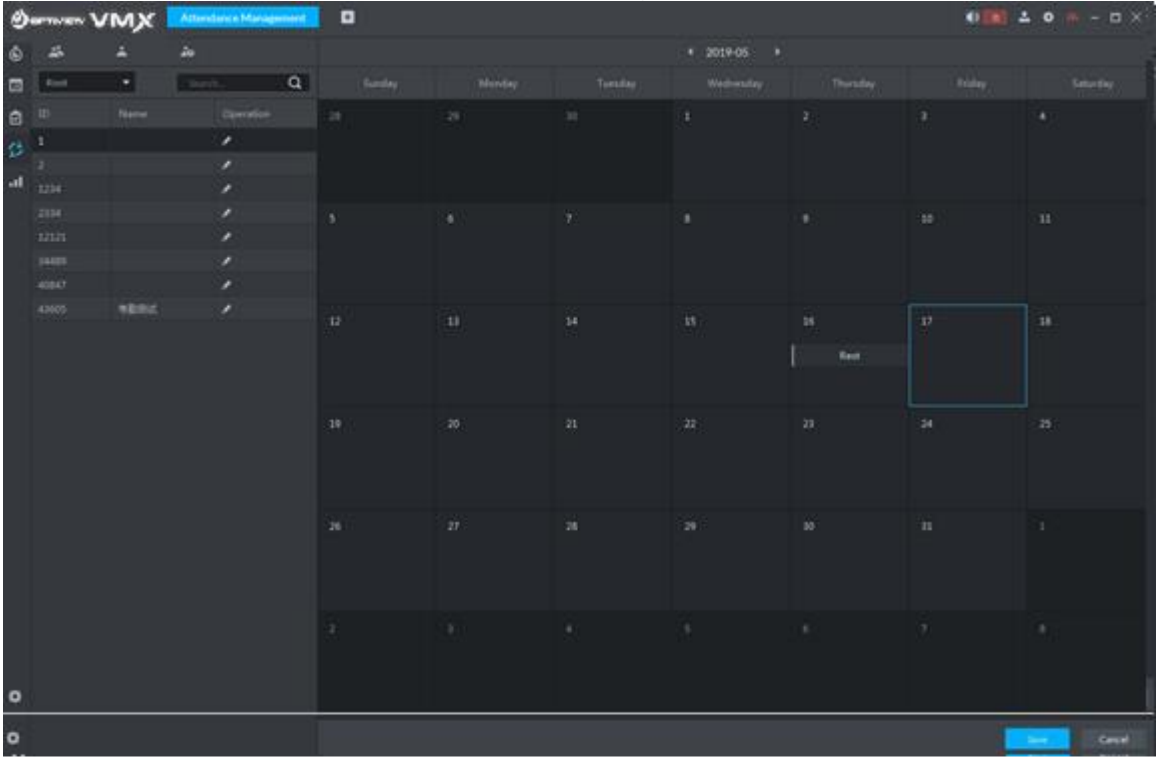
The operations over both personnel shift and department shift are similar, in this chapter; it takes personnel shift as an example to introduce config.

- If you configure department shift, then all the personnel of the department need to conform to the shift.
- If both personnel and department are configured with shift, then the latest personnel shift shall prevail. For example, after configuring the personnel shift, and the corresponding department is configured as well, then personnel shift is based on the latest department shift.
- If the department where new personnel belong is configured with shift, then the shift of new personnel should conform to department shift.

Step 1 Click on the interface of **Attendance Management**.

The interface of **Personnel Shift Arrangement** is displayed. See Figure 3-433

Figure 3-433 Personnel shift arrangement

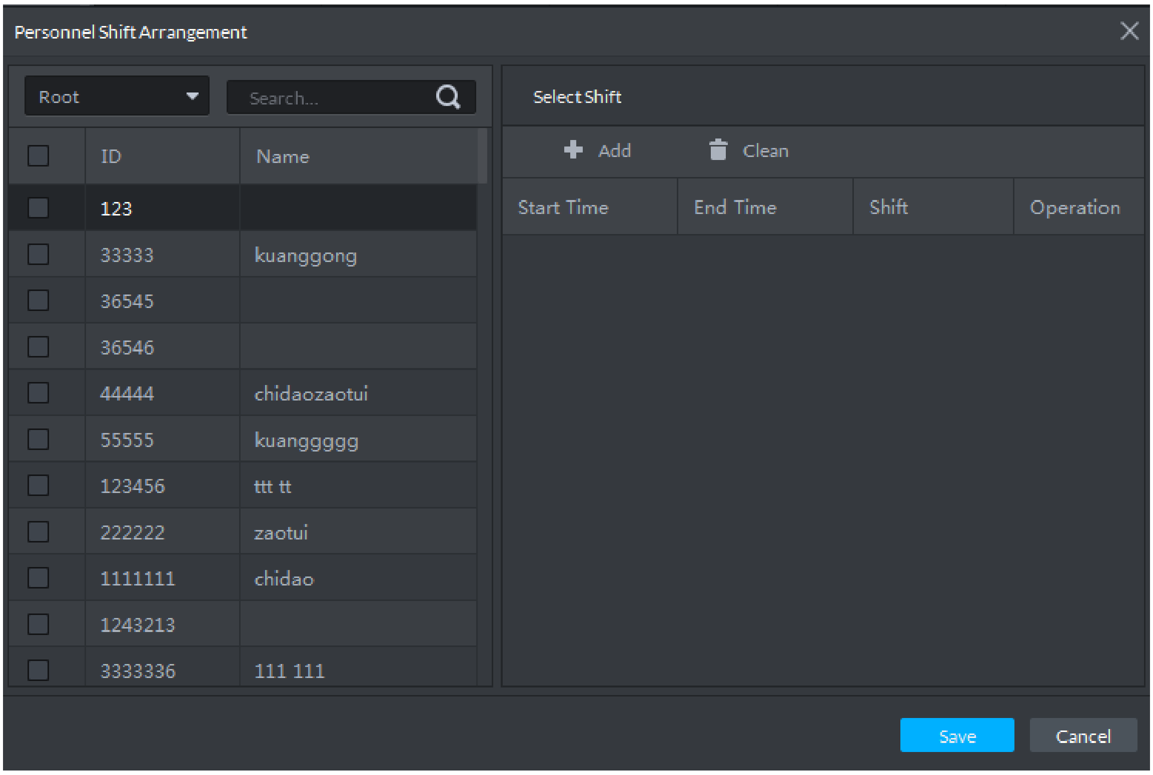

VMX
Attendance Management
2019-05
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Root
ID
Name
Operation
Rest
Save
Cancel

Step 2 Click on the top left corner of the interface.

The interface of **Personnel Shift Arrangement** is displayed. See Figure 3-434.

- If you need to configure shift for department, click on the top left corner and enter the interface of department shift arrangement. The following operation is the same as personnel shift arrangement.
- On the interface of personnel shift arrangement, select personnel and view the shift situation.
- Click next to the personnel and you can view the shift details.

Figure 3-434 Personnel shift arrangement

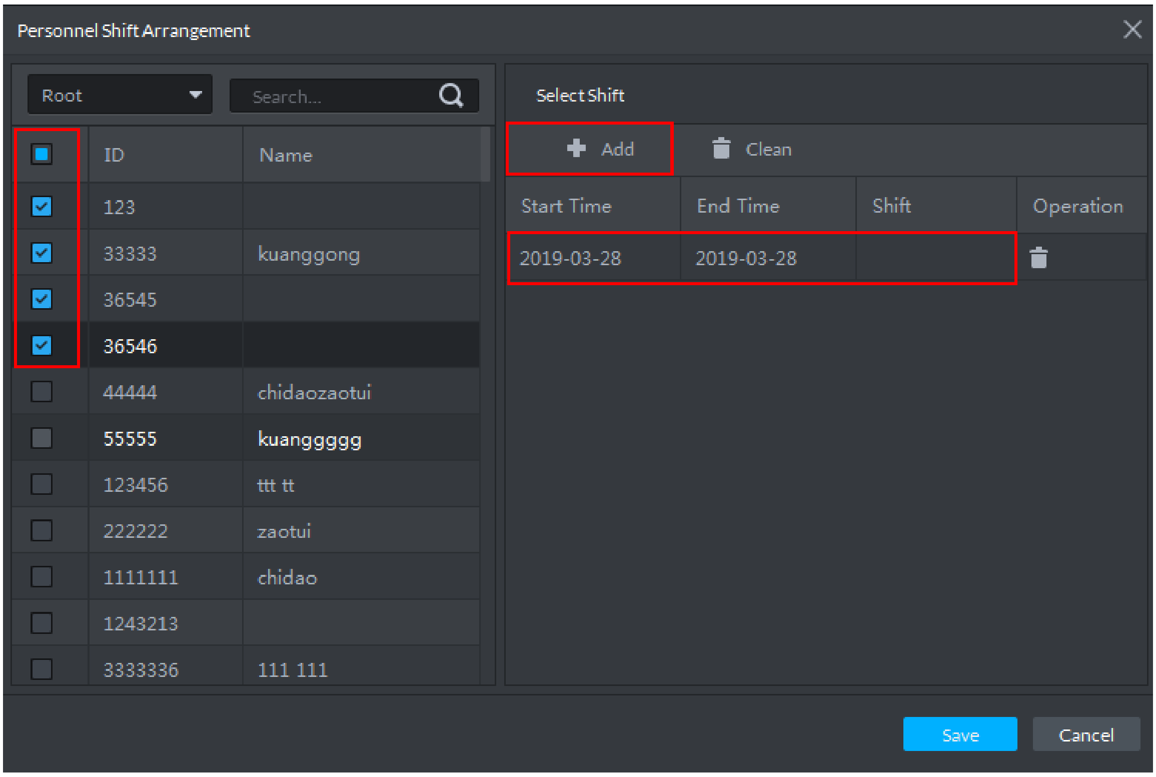

Personnel Shift Arrangement
Root
Search...
Select Shift
Add
Clean
Save
Cancel

☐	ID	Name
☐	123	
☐	33333	kuanggong
☐	36545	
☐	36546	
☐	44444	chidaozaotui
☐	55555	kuanggggg
☐	123456	ttt tt
☐	222222	zaotui
☐	1111111	chidao
☐	1243213	
☐	3333336	111 111

Start Time	End Time	Shift	Operation

Step 3 Select shift personnel, click + to add shift info. See Figure 3-435. For parameter details, see Table 3-63.

Figure 3-435 Select shift


Personnel Shift Arrangement
Root
Search...
Select Shift
Add
Clean
Save
Cancel

☑	ID	Name
☑	123	
☑	33333	kuanggong
☑	36545	
☑	36546	
☐	44444	chidaozaotui
☐	55555	kuanggggg
☐	123456	ttt tt
☐	222222	zaotui
☐	1111111	chidao
☐	1243213	
☐	3333336	111 111

Start Time	End Time	Shift	Operation
2019-03-28	2019-03-28		🗑

Table 3-63 Shift parameter description

Parameter	**Description**
Start time	Set start date and end date of personnel shift. Click the

Parameter	Description
End time	column of **Start Time** and display calendar, select date and time, and then click **OK** to complete date setting
Shift	Select needed shifts. Shift range means all the attendance shifts set in **3.20.7 Setting Attendance Shift**

Step 4 Click **Save** to save personnel shift information.

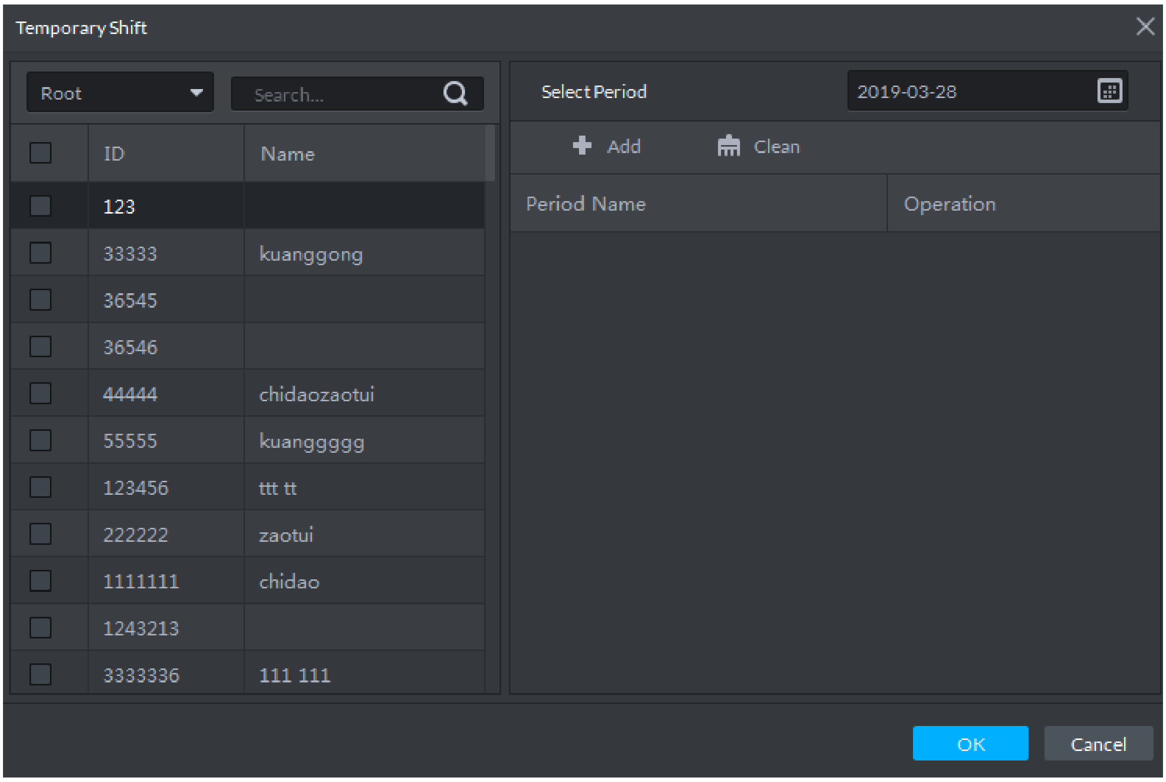
3.20.8.2 Temporary Shift

Temporary shift is needed when work changes temporarily.

Step 1 Click on the interface of Attendance Management or select personnel on the right, Double-click date on the left.

The interface of **Temporary Shift** is displayed. See Figure 3-436.

Figure 3-436 Temporary shift



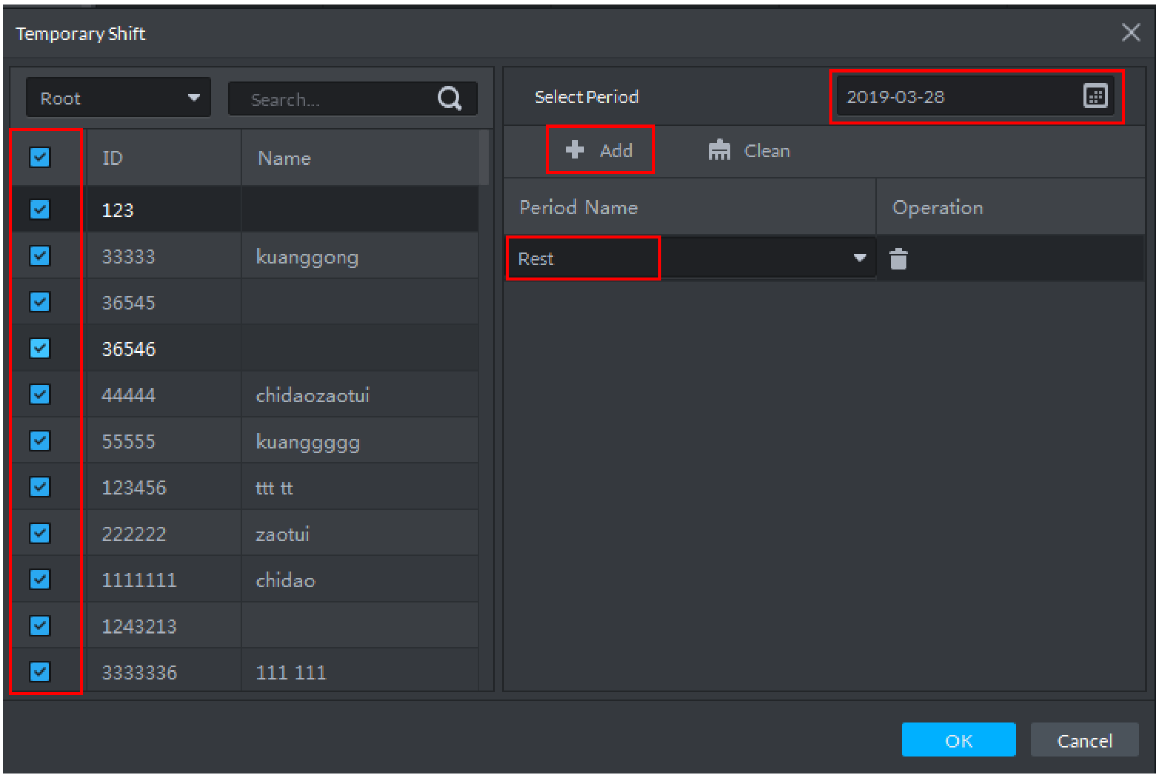
Select Period: 2019-03-28

☐	ID	Name
☐	123	
☐	33333	kuanggong
☐	36545	
☐	36546	
☐	44444	chidaozaotui
☐	55555	kuangggggg
☐	123456	ttt tt
☐	222222	zaotui
☐	1111111	chidao
☐	1243213	
☐	3333336	111 111

Period Name	Operation

Step 2 Select personnel and date, click and select temporary attendance period. See Figure 3-437.You can add max 2 attendance periods and 1 free attendance period.

Figure 3-437 Temporary shift



Select Period: 2019-03-28

☑	ID	Name
☑	123	
☑	33333	kuanggong
☑	36545	
☑	36546	
☑	44444	chidaozaotui
☑	55555	kuangggggg
☑	123456	ttt tt
☑	222222	zaotui
☑	1111111	chidao
☑	1243213	
☑	3333336	111 111

Period Name	Operation
Rest	

Step 3 Click **OK** and save shift information.

Temporary shift can be deleted, right-click the date which is configured with temporary shift, and delete temporary shift according to system prompt.

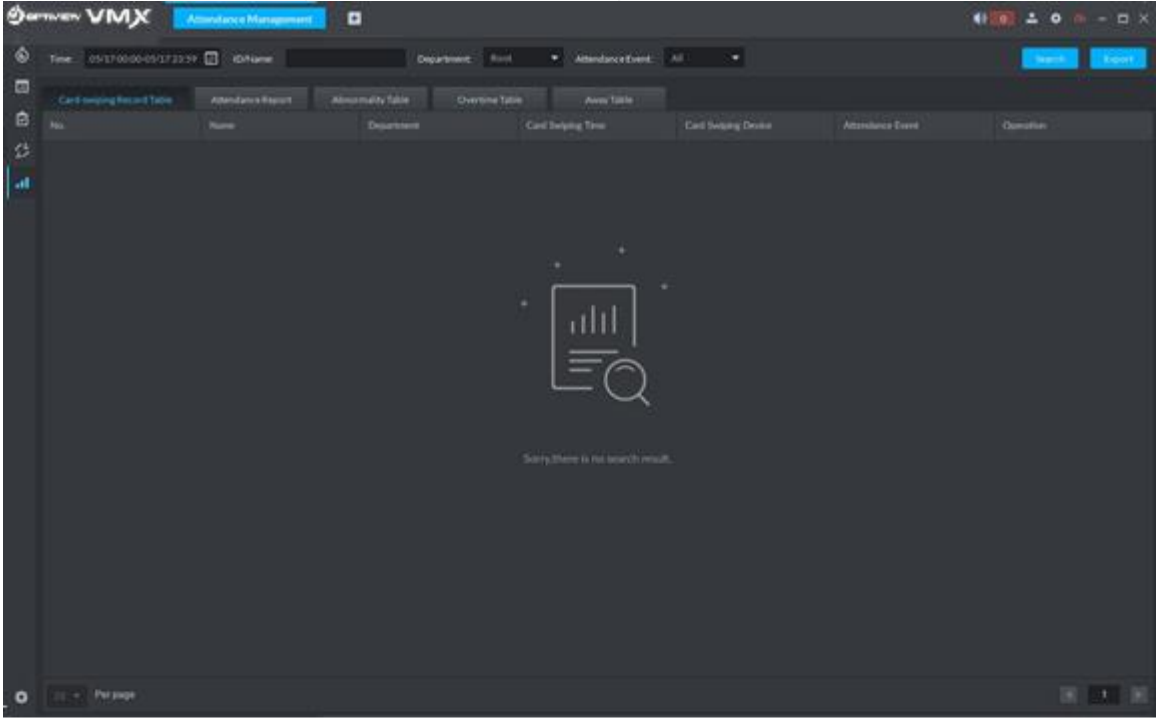
3.20.9 Viewing Attendance Report

View attendance data, displayed in the form of report, including card swiping record table, attendance report, abnormity table, overtime table and away table.

Step 1 Click 📊 on the interface of **Attendance Management**.

The interface of **Attendance Report** is displayed. See Figure 3-438.

Figure 3-438 Attendance report

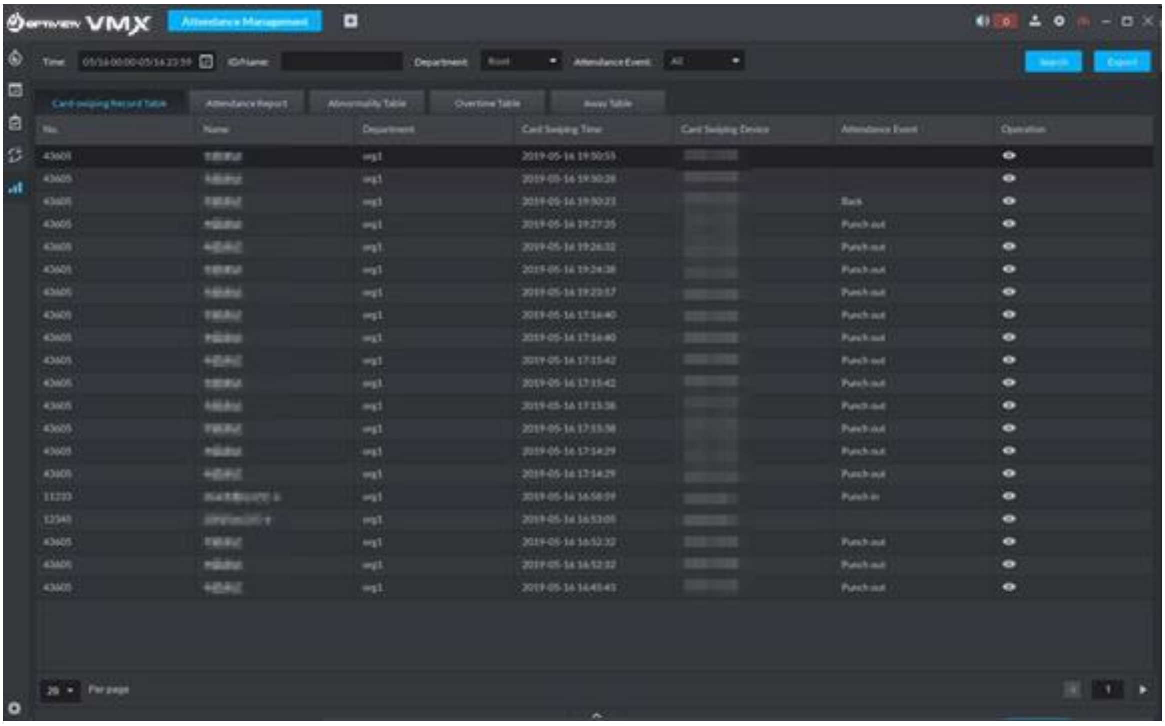

VMX
Attendance Management
Time
ID/Name
Department
Attendance Event
Search
Export
Card-swiping Record Table
Attendance Report
Abnormality Table
Overtime Table
Away Table
No.
Name
Department
Card Swiping Time
Card Swiping Device
Attendance Event
Operation
Sorry, there is no search result.
Per page

Step 2 Click corresponding tab, set serach condition, click **Search**.

The search result is displayed, exported by excel and saved locally, it can export up to 10,000 records.

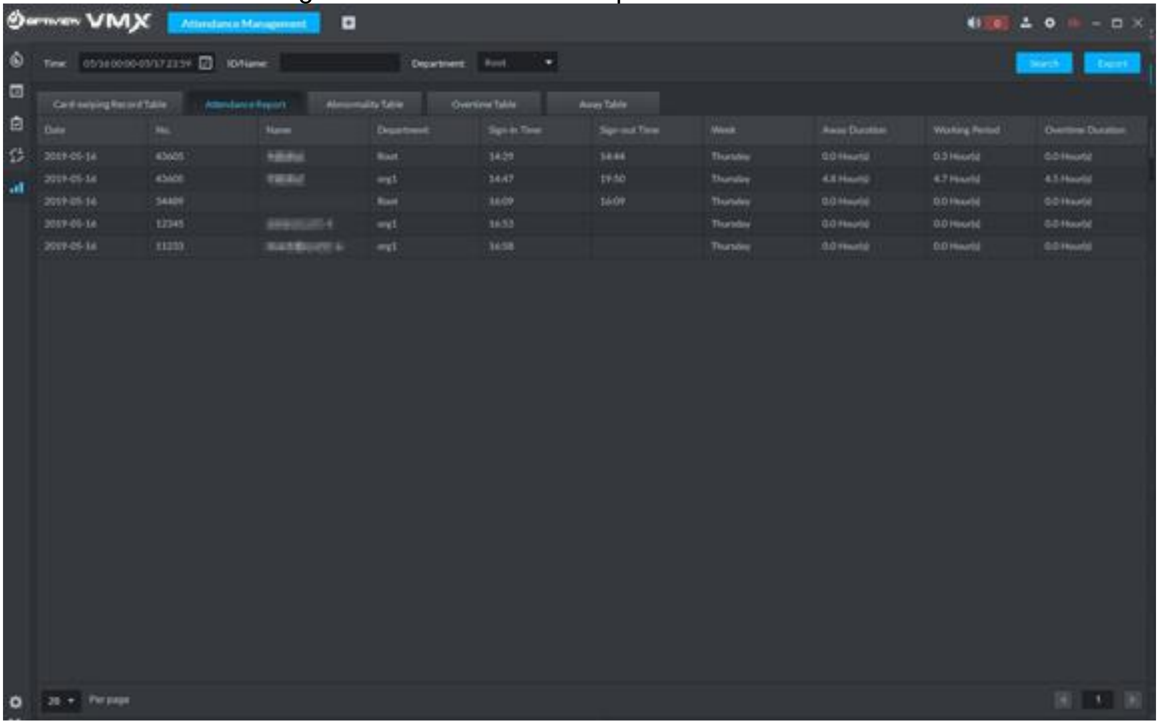
- Card swiping record table is shown in Figure 3-439. Click 👁 and view more details of the person who swipes card.

Figure 3-439 Card-swiping record table


VMX
Attendance Management
Time
ID/Name
Department
Attendance Event
Search
Export
Card-swiping Record Table
Attendance Report
Abnormality Table
Overtime Table
Away Table
No.
Name
Department
Card Swiping Time
Card Swiping Device
Attendance Event
Operation
Per page

- See Figure 3-440 for attendance report.

Figure 3-440 Attendance report



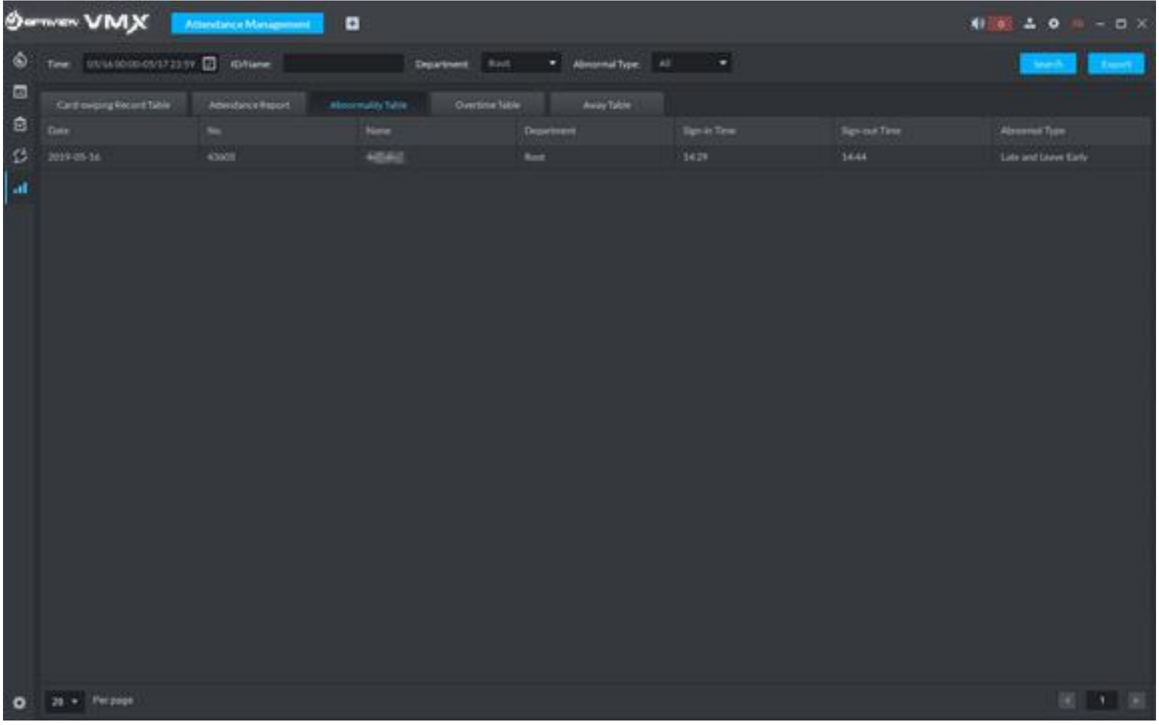
VMX
Attendance Management
Search
Export
Card swiping Record Table
Attendance Report
Abnormality Table
Overtime Table
Away Table
20
Per page
1

Time: 05/16 00:00-05/17 23:59 ID/Name: Department: Root

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Week	Away Duration	Working Period	Overtime Duration
2019-05-16	43605	[redacted]	Root	14:29	14:44	Thursday	0.0 Hour(s)	0.3 Hour(s)	0.0 Hour(s)
2019-05-16	43606	[redacted]	org1	14:47	19:50	Thursday	4.8 Hour(s)	4.7 Hour(s)	4.5 Hour(s)
2019-05-16	34409		Root	16:09	16:09	Thursday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)
2019-05-16	12345	[redacted]	org1	16:53		Thursday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)
2019-05-16	11233	[redacted]	org1	16:58		Thursday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)

- See Figure 3-441 for abnormity table.

Figure 3-441 Abnormity table



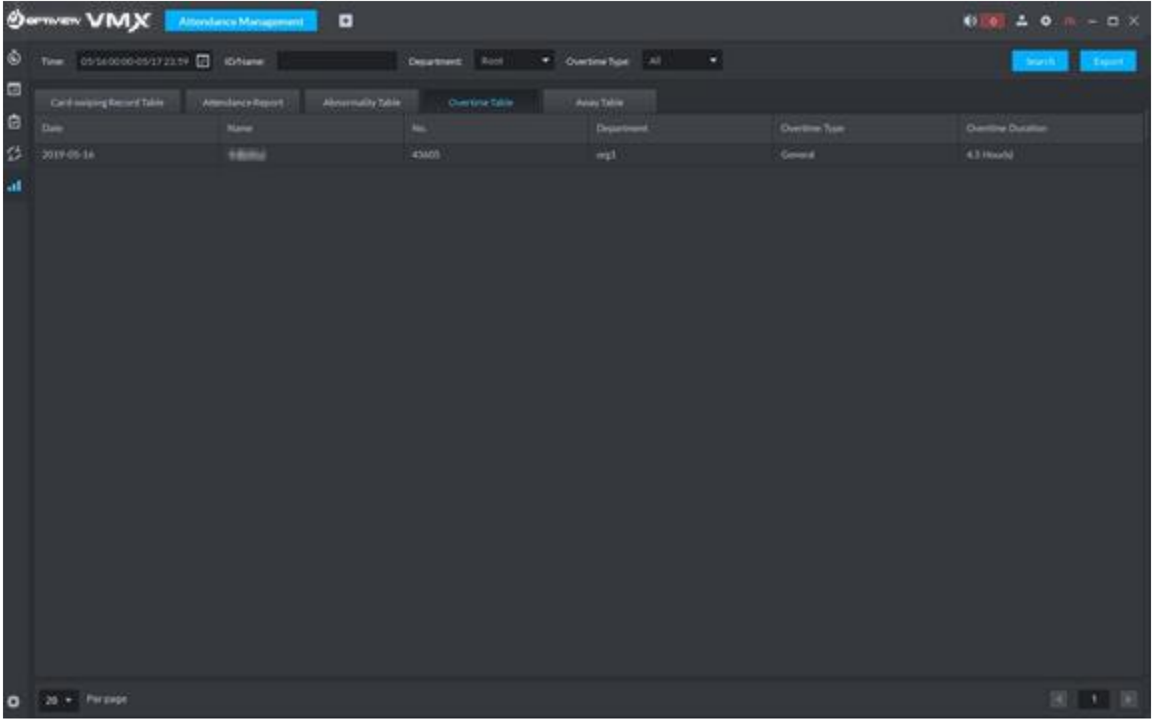
VMX
Attendance Management
Search
Export
Card swiping Record Table
Attendance Report
Abnormality Table
Overtime Table
Away Table
20
Per page
1

Time: 05/16 00:00-05/17 23:59 ID/Name: Department: Root Abnormal Type: All

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Abnormal Type
2019-05-16	43605	[redacted]	Root	14:29	14:44	Late and Leave Early

- See Figure 3-442 for overtime table.

Figure 3-442 Overtime table


VMX
Attendance Management
Search
Export
Card-swiping Record Table
Attendance Report
Abnormality Table
Overtime Table
Away Table
Per page

Time: 05/16 00:00-05/17 23:59

ID/Name:

Department: Root

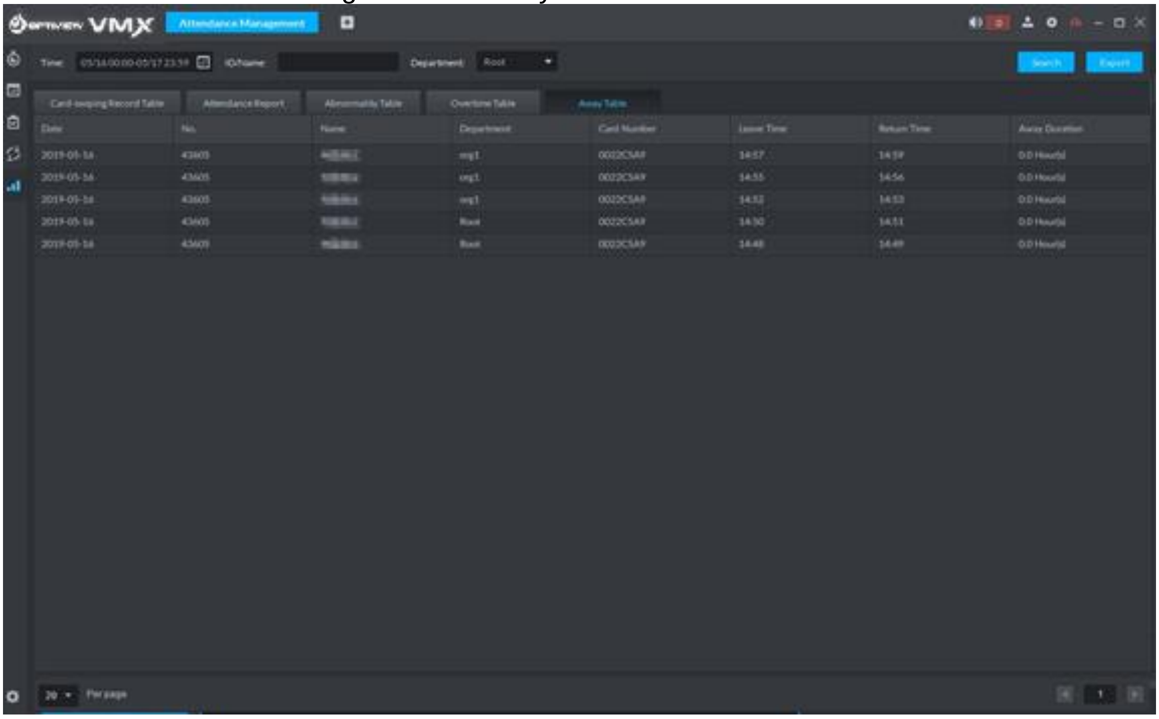
Overtime Type: All

Date	Name	No.	Department	Overtime Type	Overtime Duration
2019-05-16	[redacted]	43605	org1	General	4.5 Hour(s)

20 Per page

- See Figure 3-443 for away table.

Figure 3-443 Away table


VMX
Attendance Management
Search
Export
Card-swiping Record Table
Attendance Report
Abnormality Table
Overtime Table
Away Table
Per page

Time: 05/16 00:00-05/17 23:59

ID/Name:

Department: Root

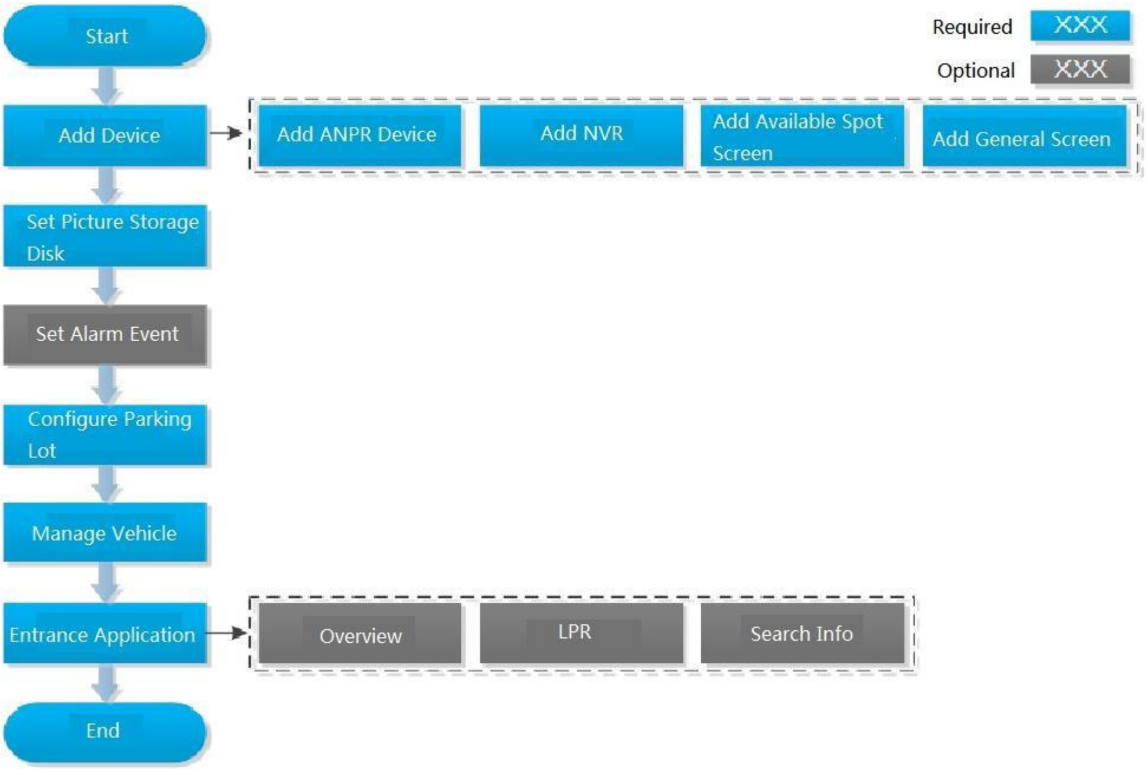
Date	No.	Name	Department	Card Number	Leave Time	Return Time	Away Duration
2019-05-16	43605	[redacted]	org1	0022C5A9	14:57	14:59	0.0 Hour(s)
2019-05-16	43605	[redacted]	org1	0022C5A9	14:55	14:56	0.0 Hour(s)
2019-05-16	43605	[redacted]	org1	0022C5A9	14:52	14:53	0.0 Hour(s)
2019-05-16	43605	[redacted]	Root	0022C5A9	14:50	14:51	0.0 Hour(s)
2019-05-16	43605	[redacted]	Root	0022C5A9	14:48	14:49	0.0 Hour(s)

20 Per page

3.21 Entrance

Integrare entrance module, realize entrance and exit recognition barrier unlock, remaining parking space info display, blacklist vehicle alarm, message search and other functions. When it fails to recognize vehicle by entrance, then it can unlock by VTO password, swipe card to unlock, fingerprint unlock and unlock by face recognition to open barrier. The supported VTO unlock mode is based on the performance of accessed VTO. The entrance operation flow is shown in Figure 3-444.

Figure 3-444 Entrance operation flow


Start
Add Device
Set Picture Storage Disk
Set Alarm Event
Configure Parking Lot
Manage Vehicle
Entrance Application
End
Add ANPR Device
Add NVR
Add Available Spot Screen
Add General Screen
Overview
LPR
Search Info
Required XXX
Optional XXX

3.21.1 Adding Device

If users want to use the new device, it needs to select **User Management** > **User** on WEB, enter **User** interface, and edit user to make him or her have access to device, otherwise the device cannot be used.

3.21.1.1 Adding ANPR Camera

ANPR device is used to recognize license plate and vehicle info.

- Please make sure ANPR device is fully configured before adding, for example, complete initialization config, and modify IP etc.
- The device category is **ANPR Device**.

Step 1 Add encoder ANPR, for more details, refer to 3.2.2.4 Adding Device

Modify device type.

1) On the **Device** interface of Web, click ✎ of added ANPR device. See Figure 3-445. The device displays the interface of Edit Device. See Figure 3-446.

Figure 3-445 Enter ANPR device

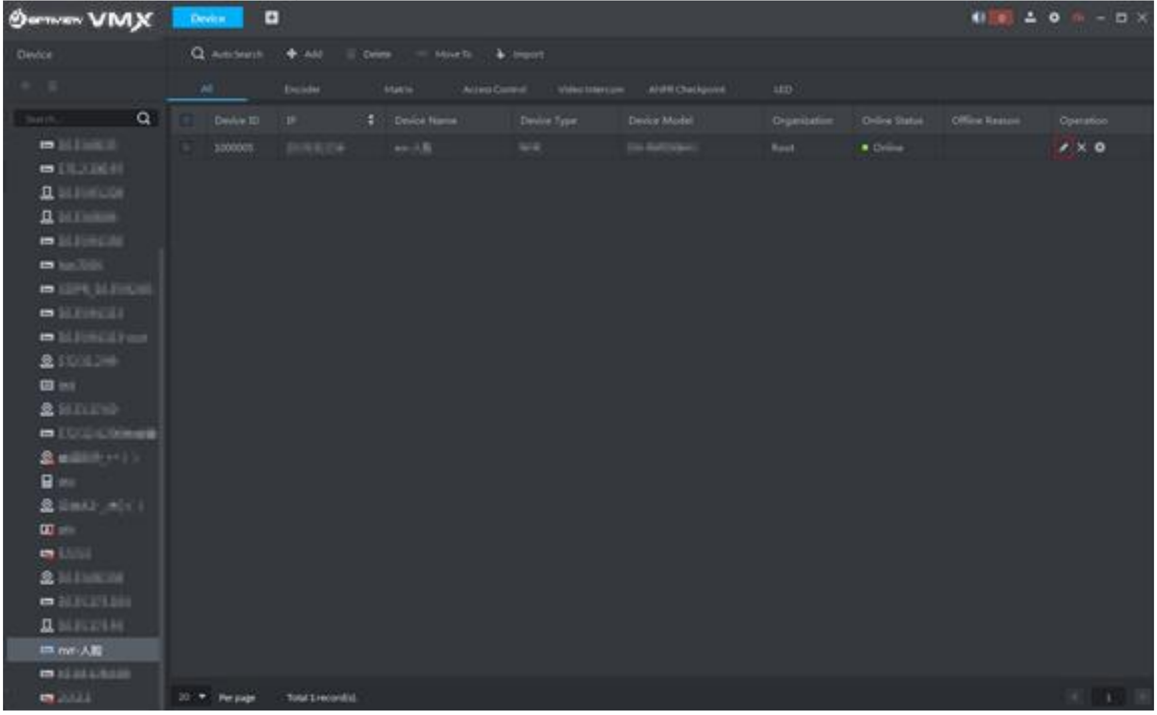
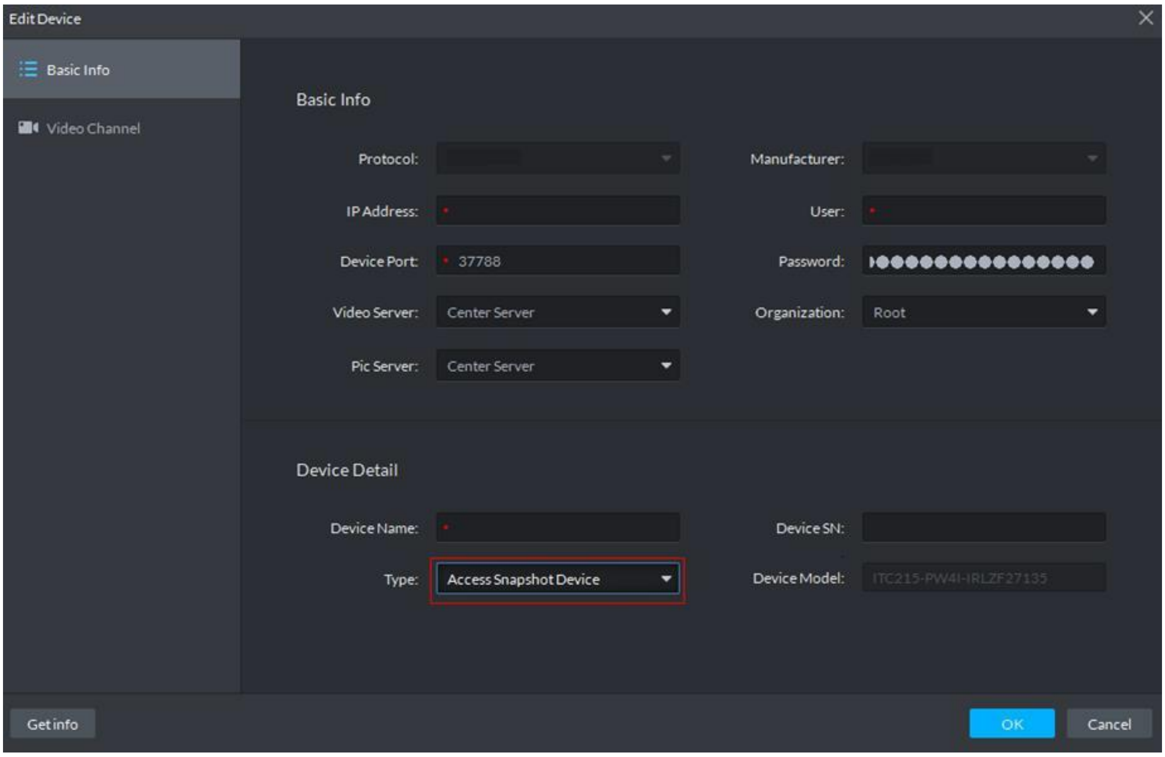

VMX
Device
Auto Search
Add
Delete
Move To
Import
All
Encoder
Matrix
Access Control
Video Intercom
ANPR Checkpoint
LED
Device ID
IP
Device Name
Device Type
Device Model
Organization
Online Status
Offline Reason
Operation
1000005
Root
Online
Per page
Total 1 record(s)

Figure 3-446 Edit device


Edit Device
Basic Info
Video Channel
Get info
OK
Cancel

Basic Info

Protocol:

Manufacturer:

IP Address:

User:

Device Port: 37788

Password: ●●●●●●●●●●●●●●

Video Server: Center Server

Organization: Root

Pic Server: Center Server

Device Detail

Device Name:

Device SN:

Type: Access Snapshot Device

Device Model: ITC215-PW4I-IRLZF27135

2) Set Type as Access Snapshot Device.

3) Click **OK** and complete config.

Step 2 Bind Resource

If there is camera installed at the entrance to view entrance panoramic picture, support binding ANPR and video camera. License plate recognition can view real-time video image. You can view video of bound camera.

1) On client homepage, click **Config**.

The system displays **Config** interface.

2) In left device tree, select access control channel, click **Bind Resource**, and see Figure 3-447.

Figure 3-447 Enter resource bind interface

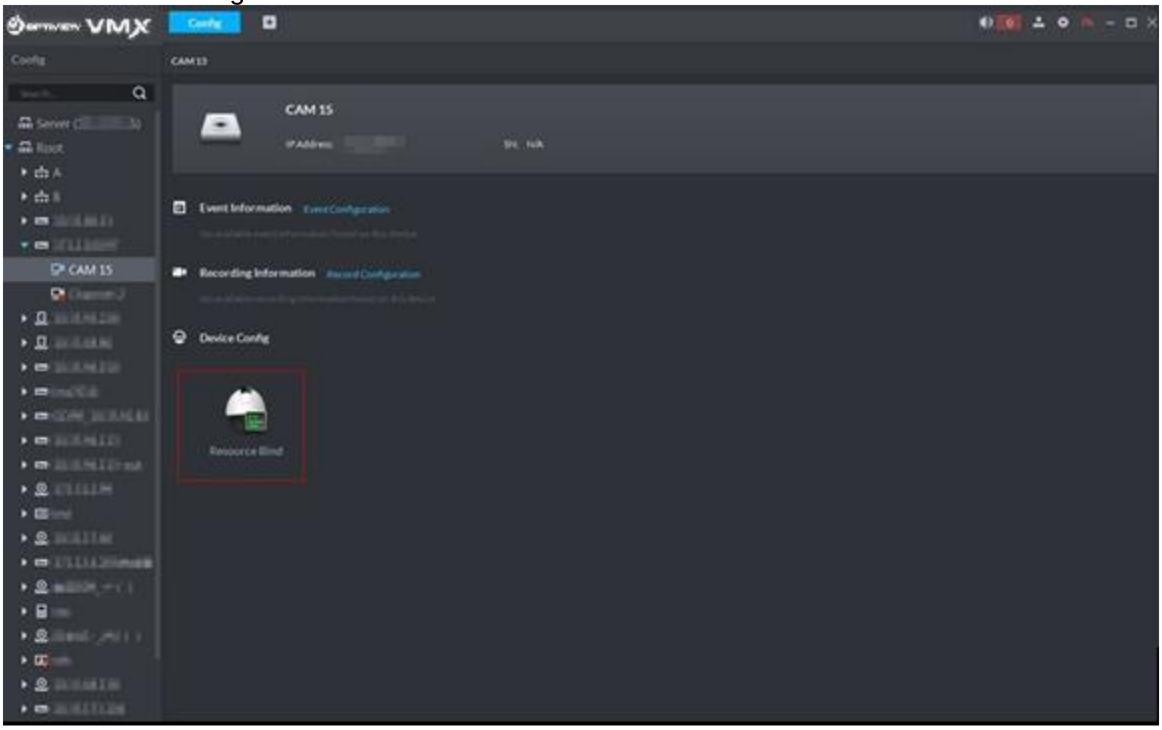
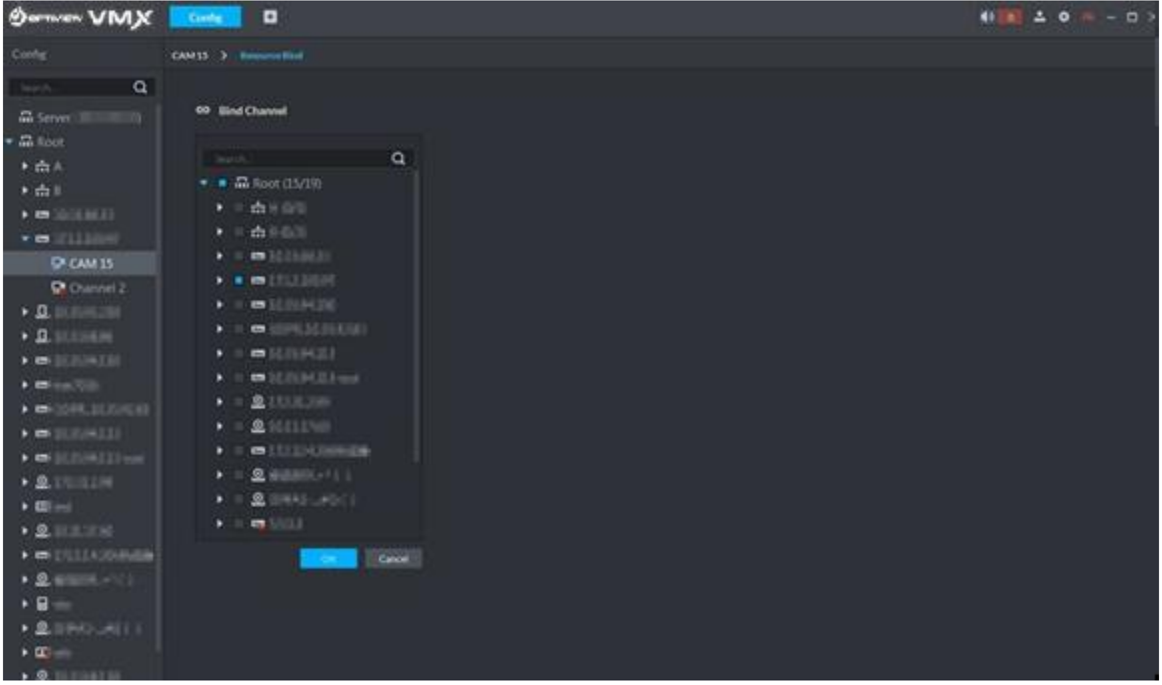

VMX
Config
CAM 15
Event Information
Recording Information
Device Config
Resource Bind

Figure 3-448 Resource bind


VMX
Config
CAM 15
Resource Bind
Bind Channel
Root (15/19)
OK
Cancel

3) Select bound panoramic camera.
4) Click **OK** and complete config.

3.21.1.2 Adding NVR

NVR is used to connect ANPR and Optiview VMX, and implement data transmission.

- Please make sure NVR is fully configured before adding. For example, modify IP address, add remote device.
- NVR device category is Encoder.

Step 1 Add encoder NVR, for detailed operation, refer to 3.2.2.4 Adding Device.

Step 2 Modify device capacity set.

1) Click ✎ of added NVR on the **Device** interface on Web. See Figure 3-449.

The system displays the interface of **Edit Device**. See Figure 3-450.

Figure 3-449 Enter encoder edit interface

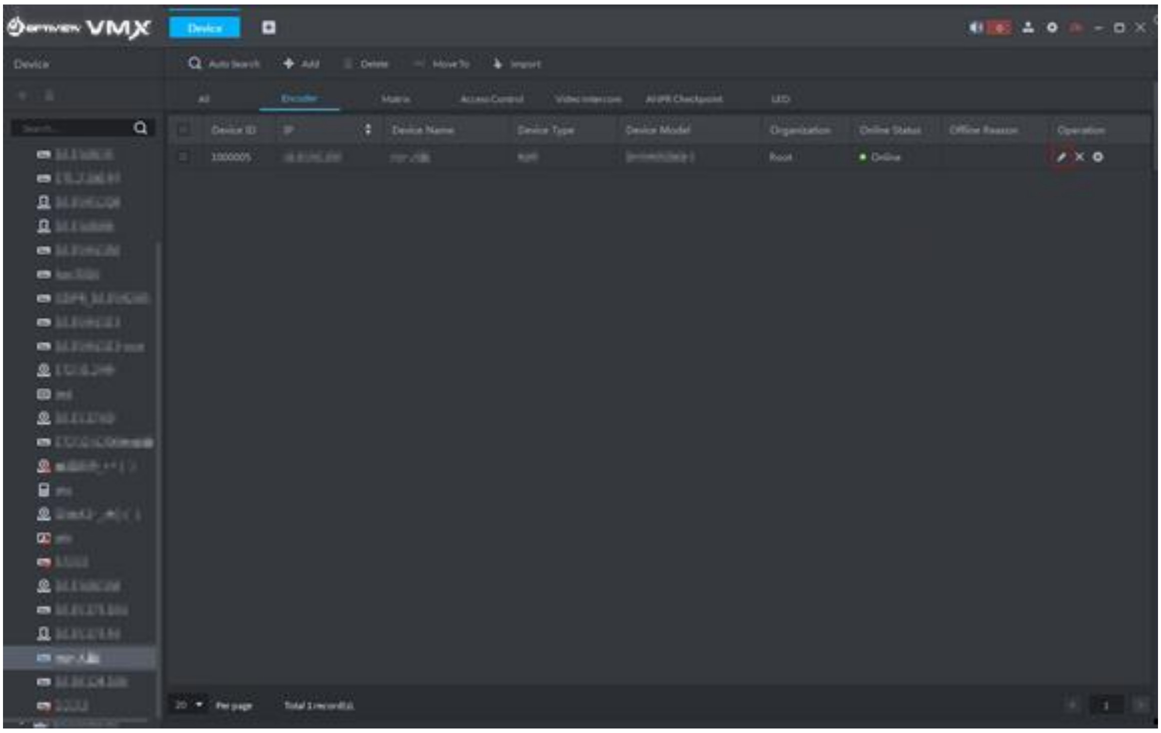
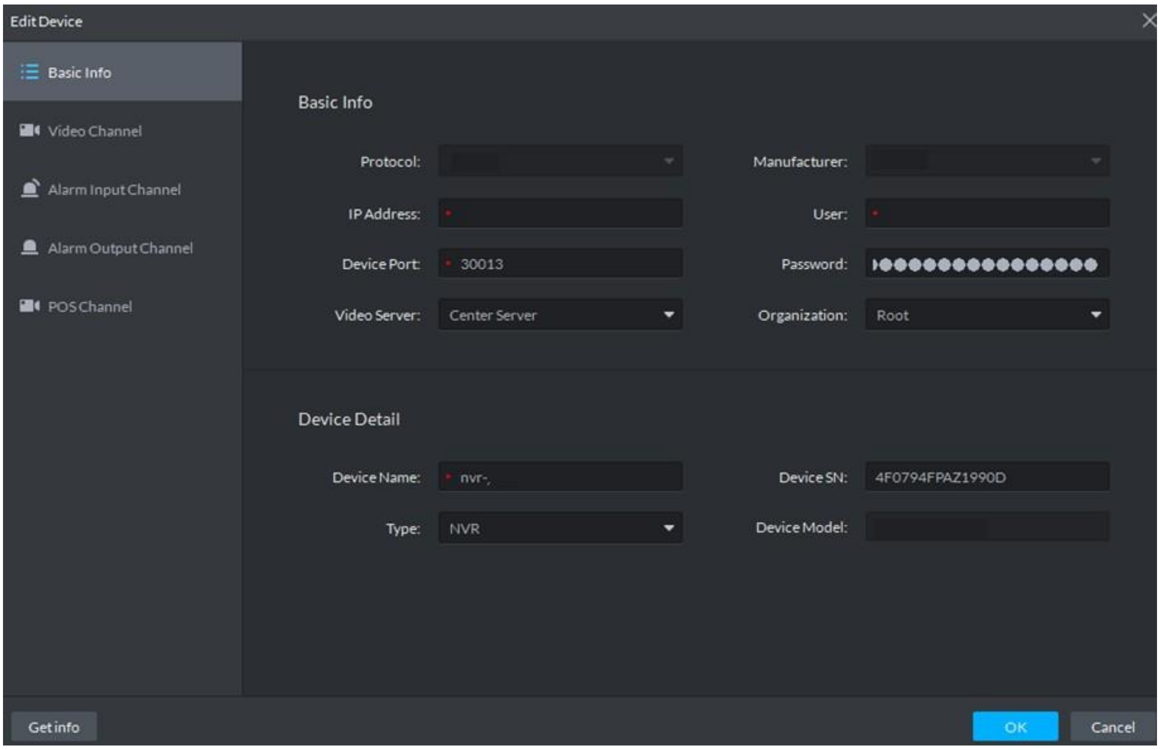

VMX
Device
Device
Auto Search
Add
Delete
Move To
Import
All
Encoder
Matrix
Access Control
Video Intercom
ANPR Checkpoint
LED
Device ID
IP
Device Name
Device Type
Device Model
Organization
Online Status
Offline Reason
Operation
1000005
Root
Online
20
Per page
Total 1 record(s)

Figure 3-450 Edit device


Edit Device
Basic Info
Video Channel
Alarm Input Channel
Alarm Output Channel
POS Channel
Get info
OK
Cancel

Basic Info

Protocol:
Manufacturer:
IP Address:
User:
Device Port: 30013
Password: ●●●●●●●●●●●●●●●●
Video Server: Center Server
Organization: Root

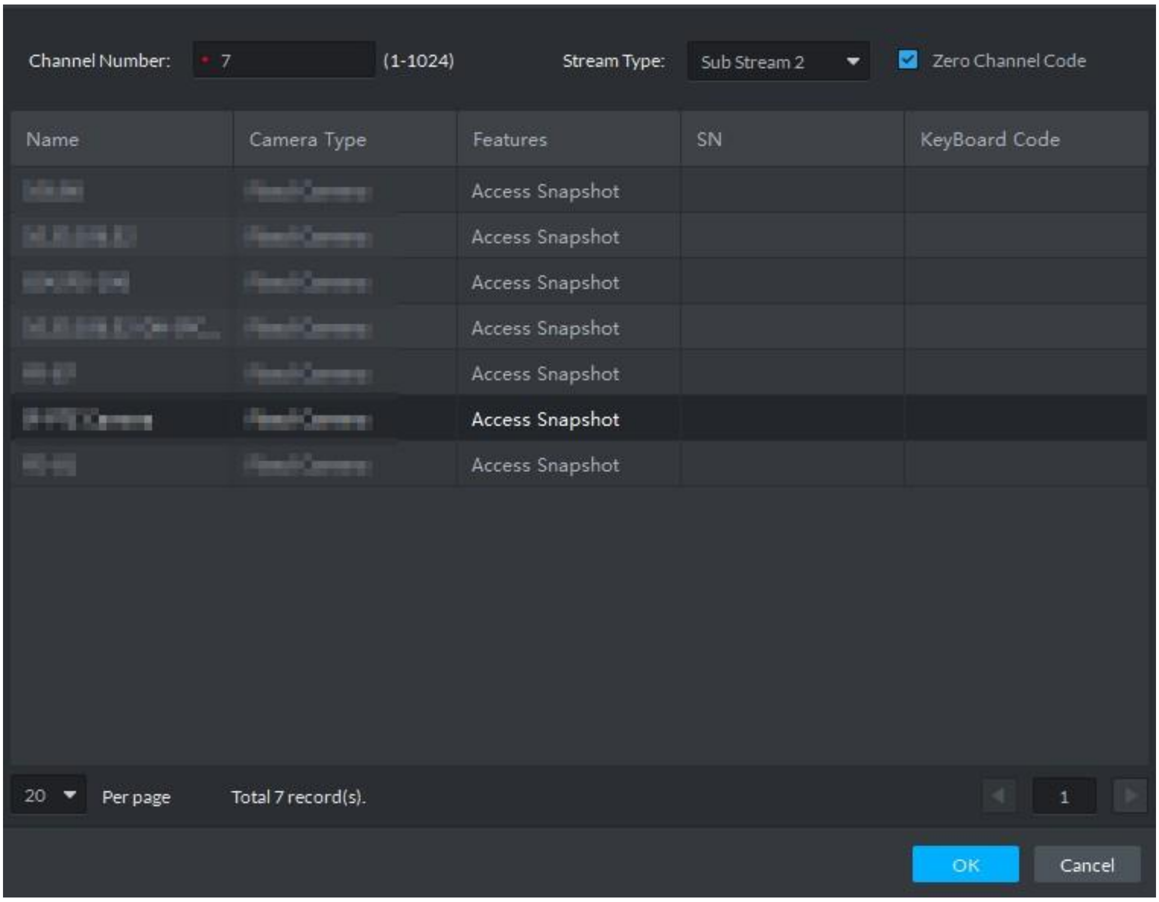
Device Detail

Device Name: nvr-,
Device SN: 4F0794FPAZ1990D
Type: NVR
Device Model:

2) Click the tab of **Video Channel**, set **Features** as **Access Snapshot**. See Figure 3-451.

The feature of all the bound ANPR device channel is set as **Access Snapshot**.

Figure 3-451 Modify features



Channel Number: 7 (1-1024) Stream Type: Sub Stream 2 ☑ Zero Channel Code

Name	Camera Type	Features	SN	KeyBoard Code
[illegible]	[illegible]	Access Snapshot		
[illegible]	[illegible]	Access Snapshot		
[illegible]	[illegible]	Access Snapshot		
[illegible]	[illegible]	Access Snapshot		
[illegible]	[illegible]	Access Snapshot		
[illegible]	[illegible]	Access Snapshot		
[illegible]	[illegible]	Access Snapshot		

20 Per page Total 7 record(s). 1

3) Click **OK** and complete config.

3.21.1.3 Adding Remaining Parking Screen

Collect the data of vehicle entrance and exit from ANPR camera; make statistics of parking space quantity, then parking space quantity will be displayed on the screen.

- Please make sure remaining parking space is completely configured before adding. For example, modify IP address.
- The device category of remaining parking screen is **LED Device**.

Step 1 Add remaining parking screen. For detailed operation, refer to 3.2.2.4 Adding Device.

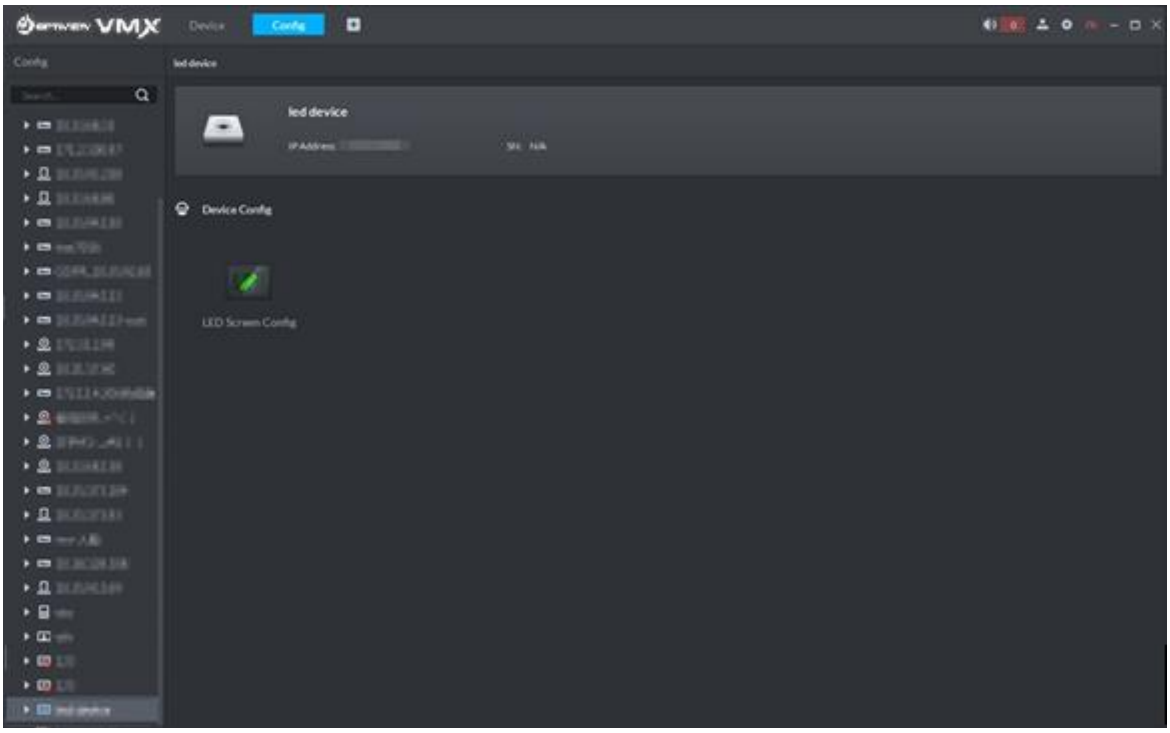
Step 2 On client homepage, click **Config**.

The system displays **Config** interface.

Step 3 Select remaining parking screen from left device list.

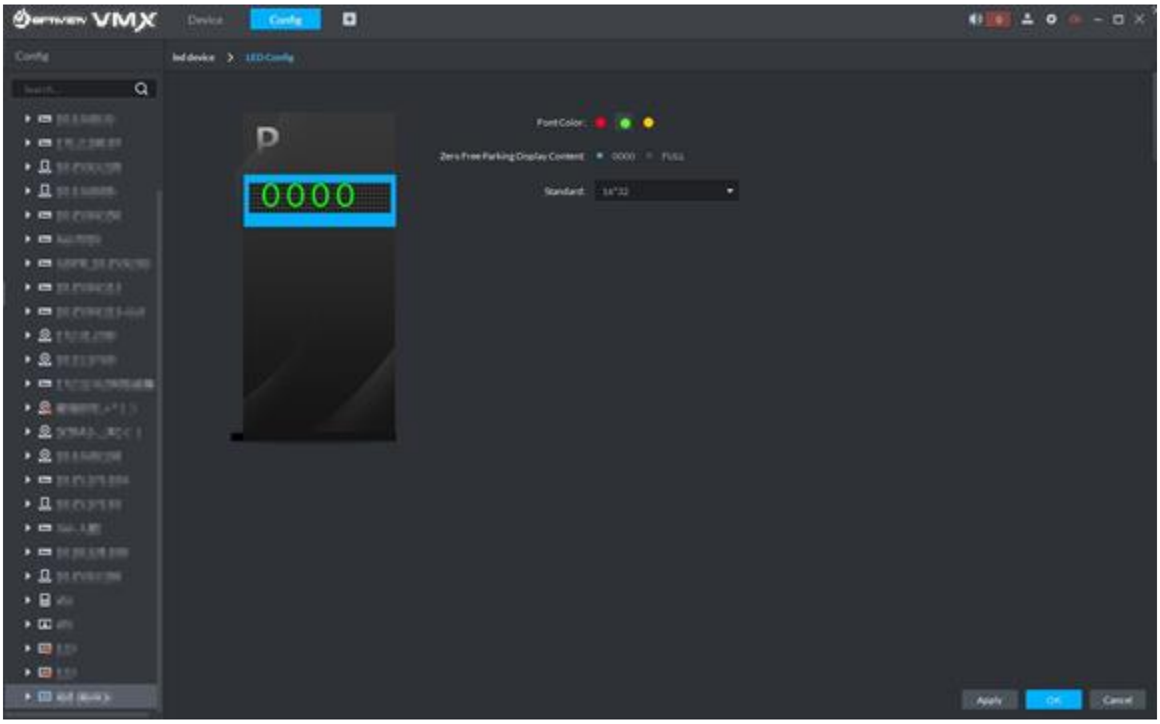
The system displays **LED Screen Config** button. See Figure 3-452.

Figure 3-452 LED screen config


VMX
Device
Config
Config
led device
led device
IP Address:
SN: N/A
Device Config
LED Screen Config

Step 4 Click LED Screen Config.

The system displays **LED Config** interface, see Figure 3-453.



Font Color: 🟥 🟩 🟨

Zero Free Parking Display Content: ● 0000 ○ FULL

Standard: 16*32

Figure 3-453 LED config

Step 5 You can set **Font Color** and **Zero Free Parking Display Content**. See Figure 3-453. Font color is the color of the words displayed on the screen; Zero free parking display content is the information displayed on the screen when there is no parking space available.

Step 6 Click **OK** to complete config.

3.21.1.4 Adding Common Screen

Add common screen and display vehicle info. Currently the platform supports Jezetek common screen.

- Please make sure common screen is configured before adding, such as modifying IP address.
- Common screen is categorized as **LED Device**.

Step 1 Add common screen, for more details. See 3.2.2.4 Adding Device.

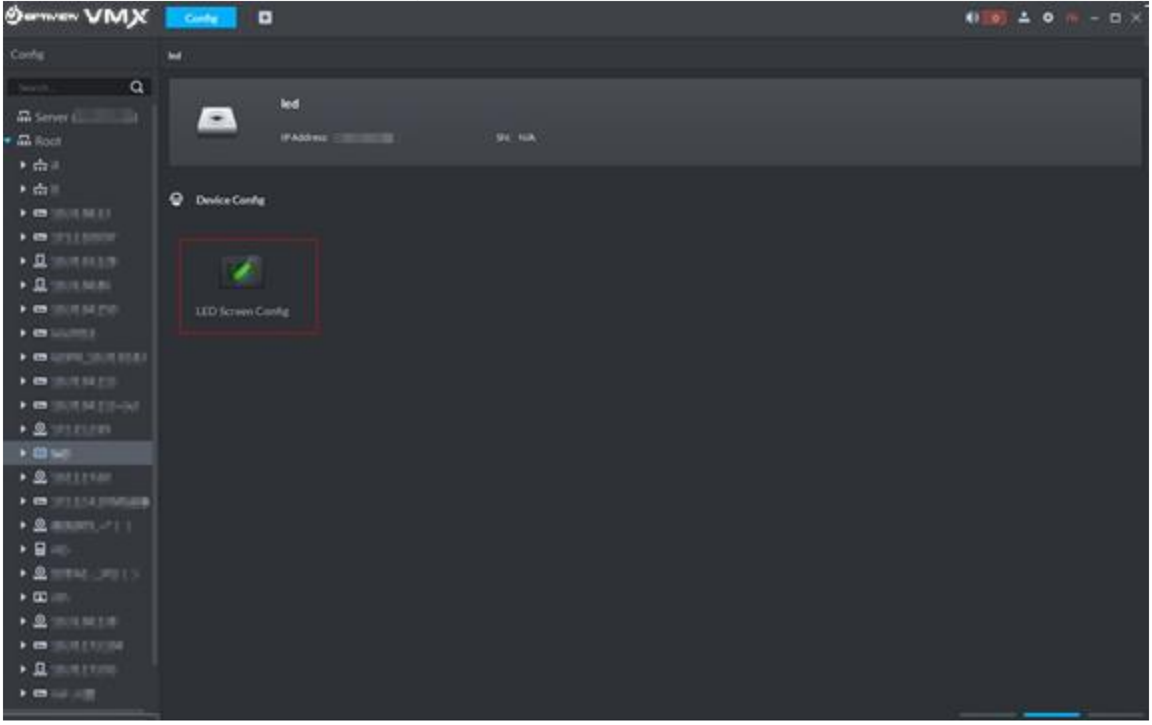
Step 2 On client homepage, click **Config**.

The system displays **Config** interface.

Step 3 Select common screen from left device list.

The system displays the button of **LED Screen Config.**

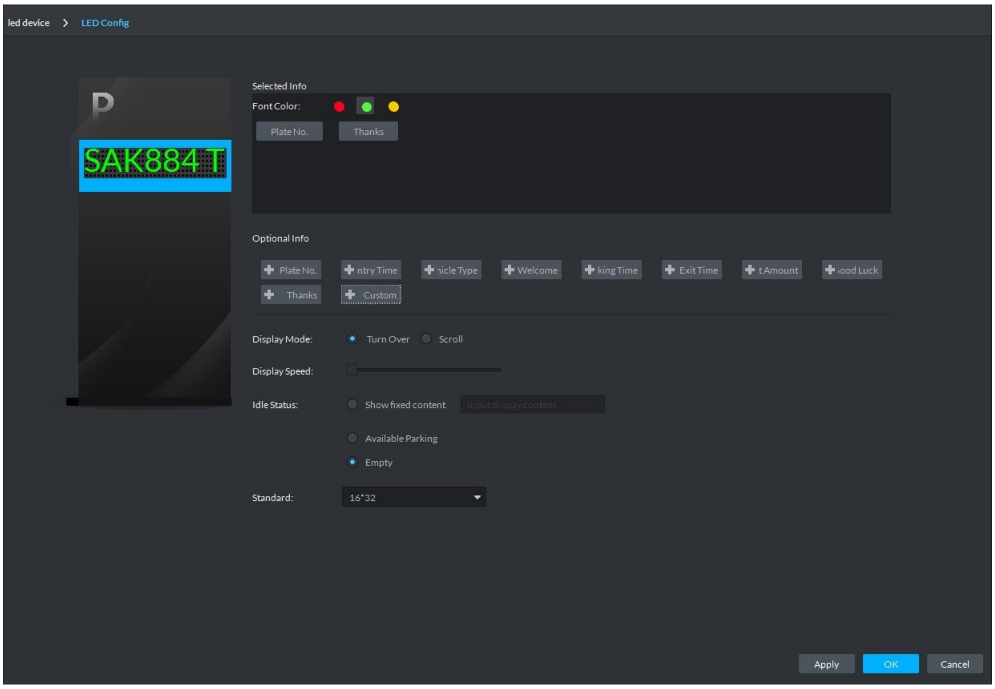
Figure 3-454


VMX
Config
Config
Search...
Server
Root
led
led
IP Address:
SN: N/A
Device Config
LED Screen Config

Step 4 Click LED Screen Config.

The system displays **LED Screen Config** interface, see Figure 3-455.

Figure 3-455 LED config


led device
LED Config
P
SAK884 T
Selected Info
Optional Info
Plate No.
ntry Time
ıicle Type
Welcome
king Time
Exit Time
t Amount
ıood Luck
Thanks
Custom
Input display content
Apply
OK
Cancel

Font Color: ● ● ●

Plate No. Thanks

Display Mode: ● Turn Over ○ Scroll

Display Speed:

Idle Status: ○ Show fixed content ○ Available Parking ● Empty

Standard: 16*32

Step 5 Set font color and info content, select display mode, display speed and show fixed content during idle status.

Step 6 Click **OK** and complete config.

3.21.2 Setting Picture Storage Disk

Configure local storage disk, you must reserve an ANPR picture disk to store ANPR snapshots, otherwise, snapshots cannot be stored or displayed. For more details, see **3.2.1.4 Setting Storage Space.**

3.21.3 Setting Alarm Event

This chapter introduces entrance alarm, for more alarm events and details, refer to **3.2.4 Setting Alarm Event**. Entrance alarms include following types.

- LPR (License plate recognition)

  After license plate is recognized by ANPR, reported to platform by NVR, the platform triggers alarm, and extract video before and after license plate recognition, saved into platform. The default video duration is 20s, 10s before and 10s after alarm is triggered.
- Blocked list alarm

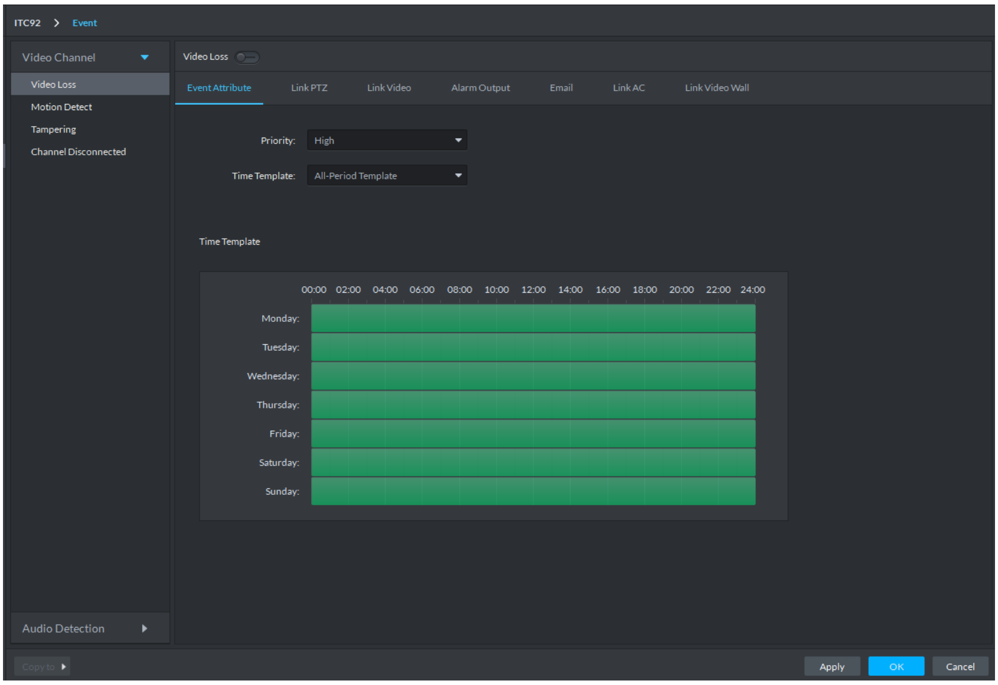
  The platform supports marking some plate number as blocked list vehicle, meanwhile, compare the recognized plate number with blocked plated number, if it is the blocked plated number, then alarm is triggered.

  If you want to mark some plate number as blocked plate number, see 3.21.5 Vehicle Management
- Parking timeout

  The parking duration exceeds the threshold, and then alarm is triggered.

Set alarm events, see Figure 3-456.

Figure 3-456 Alarm event



Priority: High

Time Template: All-Period Template

ITC92
Event
Video Channel
Video Loss
Motion Detect
Tampering
Channel Disconnected
Audio Detection
Video Loss
Event Attribute
Link PTZ
Link Video
Alarm Output
Email
Link AC
Link Video Wall
Time Template
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
24:00
Monday:
Tuesday:
Wednesday:
Thursday:
Friday:
Saturday:
Sunday:
Copy to
Apply
OK
Cancel

3.21.4 Configuring Parking Lot

Generally one parking lot is considered as an area. Parking lot configuration includes setting parking space quantity, release situation and other information. Bind ANPR device channel and use it to recognize vehicles, bound VTO is used to recognize people.

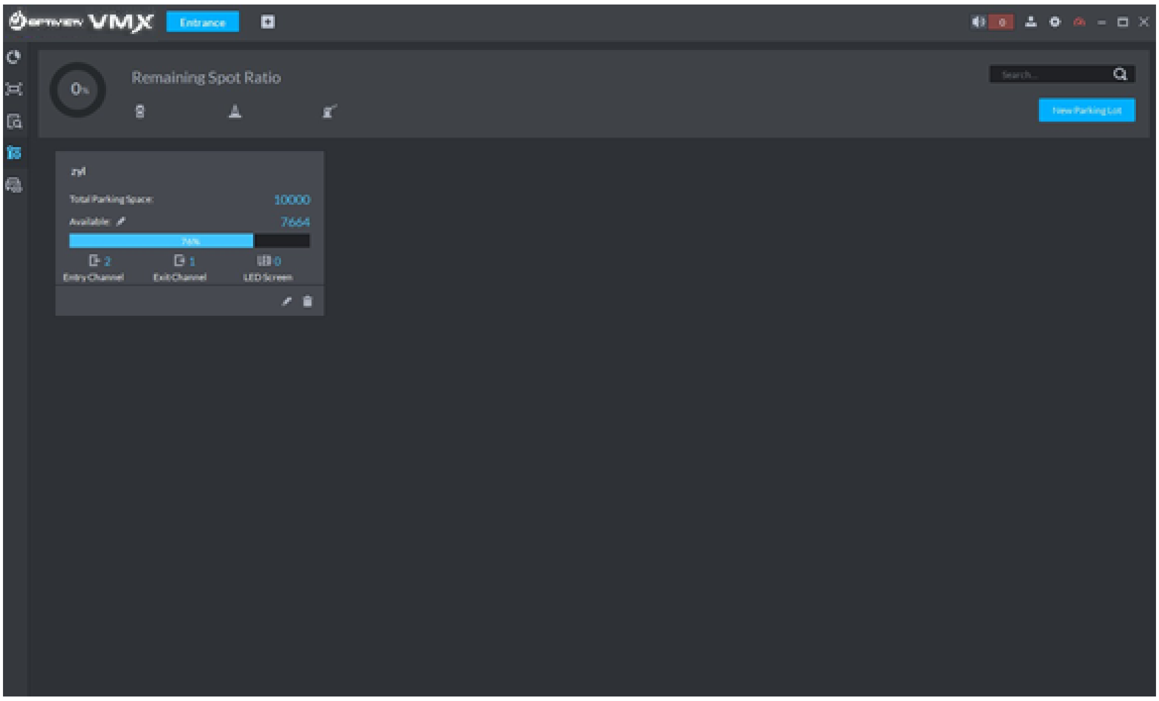
Step 1 On client homepage, click **Entrance**.

The system displays the interface of **Entrance**.

Step 2 Click .

The system displays the interface of **Parking Lot Config**. See Figure 3-457.

Figure 3-457 Parking lot info

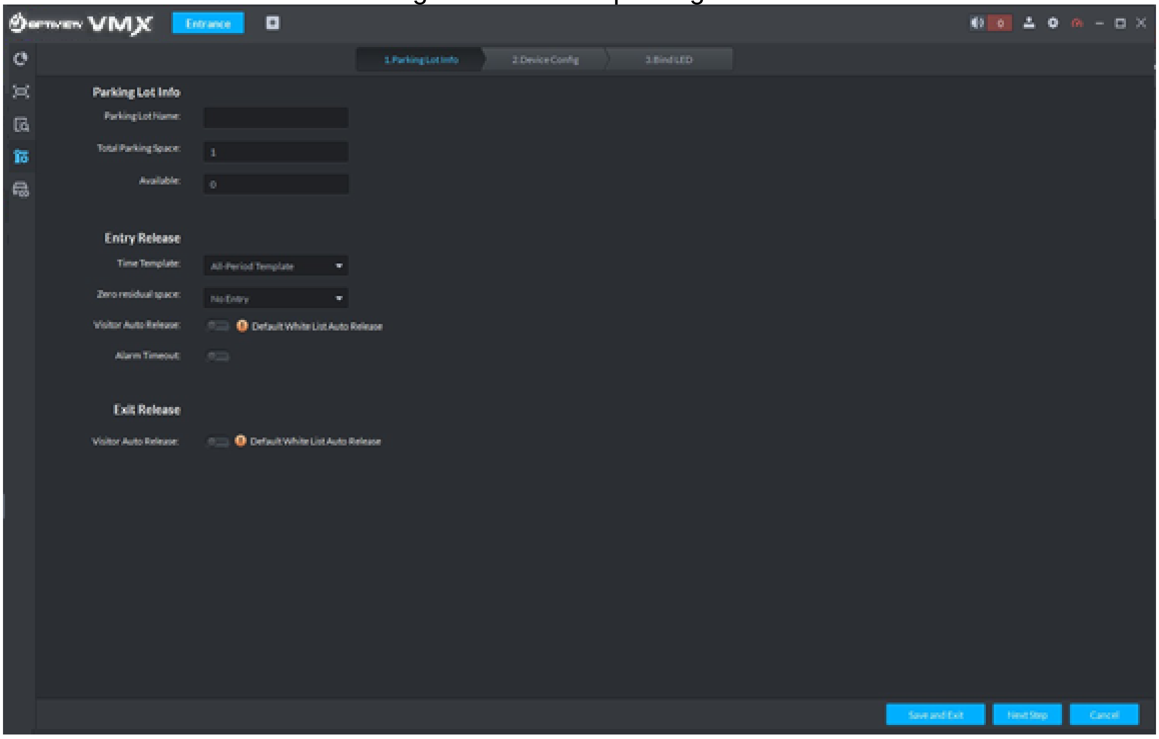

VMX
Entrance
Remaining Spot Ratio
0%
Search...
New Parking Lot
zyl
Total Parking Space: 10000
Available: 7664
76%
2 Entry Channel
1 Exit Channel
0 LED Screen

Step 3 Add parking lot.

1) Click New Parking Lot.

The system displays interface of new parking lot, see Figure 3-458.

Figure 3-458 Add parking lot



Parking Lot Info

Parking Lot Name:

Total Parking Space: 1

Available: 0

Entry Release

Time Template: All-Period Template

Zero residual space: No Entry

Visitor Auto Release: Default White List Auto Release

Alarm Timeout:

Exit Release

Visitor Auto Release: Default White List Auto Release

2) Configure parking lot info. For more parameter details, see Table 3-64.

Table 3-64 Parking lot info

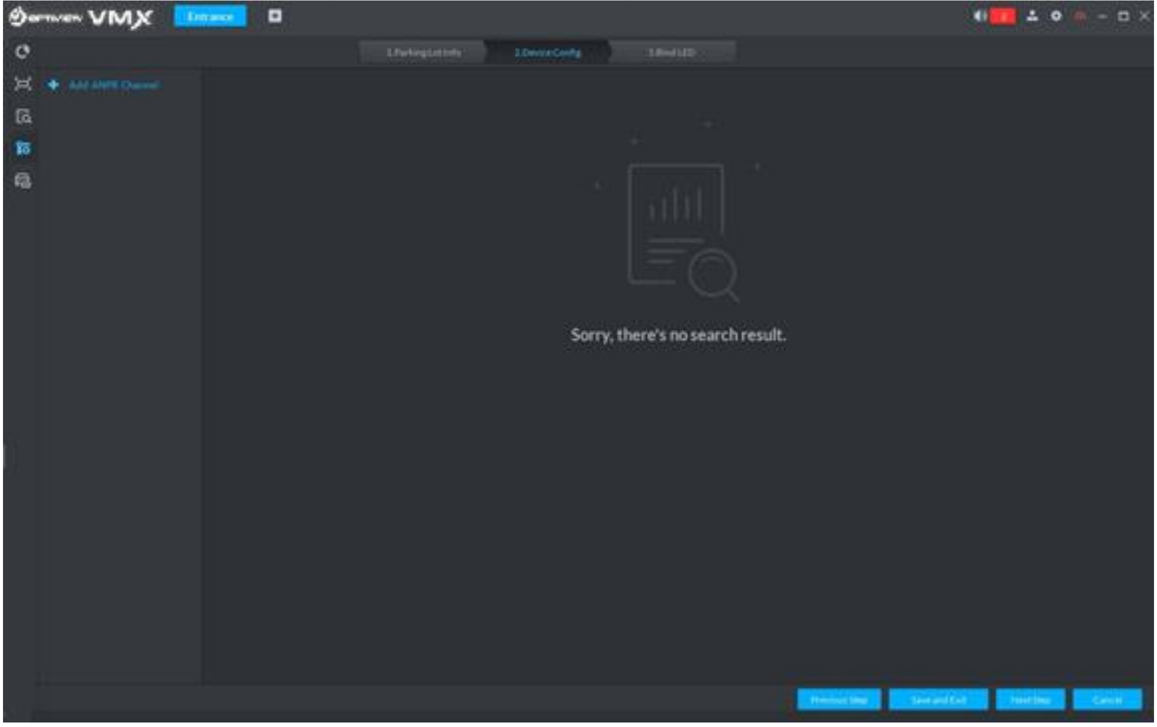
Parameter		Description
Parking Lot Info	Name	Parking lot name, used to recognize different areas.
	Total parking space	Total available parking space of the area.
	Available	Available parking lot quantity when configuring area.
Entry Release	Time template	Select the time template which conforms to entry release. If default template fails to meet the requirement, you can select **Manage Time Template** to set custom time template. Default templates include: ● All-period template: 00:00 to 24:00 daily. ● Weekday template: 00:00 to 24:00 Mon to Fri ● Weekend template: 00:00 to 24:00 Sat and Sun

Parameter		Description
	Zero residual space	Release option when remaining space is zero. ● No entry. Any vehicle is not allowed to enter. ● All Any vehicle is allowed to enter. ● Whitelist Whitelist vehicles include several vehicle types, such as no group, general and VIP. Only three types of vehicle above are allowed to enter when remaining space is zero. ● VIP Only VIP vehicle is allowed to enter when remaining space is zero. 📖 Vehicle type should be set during vehicle management.
	Visitor auto release	Those which are not registered on Optiview VMX are considered as visitor vehicles. Confirm if it unlocks barrier automatically when visitor vehicle enters according scenario design. If it is required to release, and then click ○, the icon displays as ●. Otherwise, it remains as ○, and it will not unlock barrier to release when visitor wants to enter parking lot.
	Alarm timeout	Vehicle enters parking lot and stays longer than threshold, alarm is triggered.
Exit Release	Visitor auto release	Those which are not registered on Optiview VMX are considered as visitor vehicles. Confirm if it unlocks barrier automatically when visitor vehicle exits according scenario design. If it is required to release, and then click ○, the icon displays as ●. Otherwise, it remains as ○, and it will not unlock barrier to release when visitor wants to exit parking lot.

3) Click **Next**.

The system displays the interface of **Device Config**. See Figure 3-459

Figure 3-459 Device config

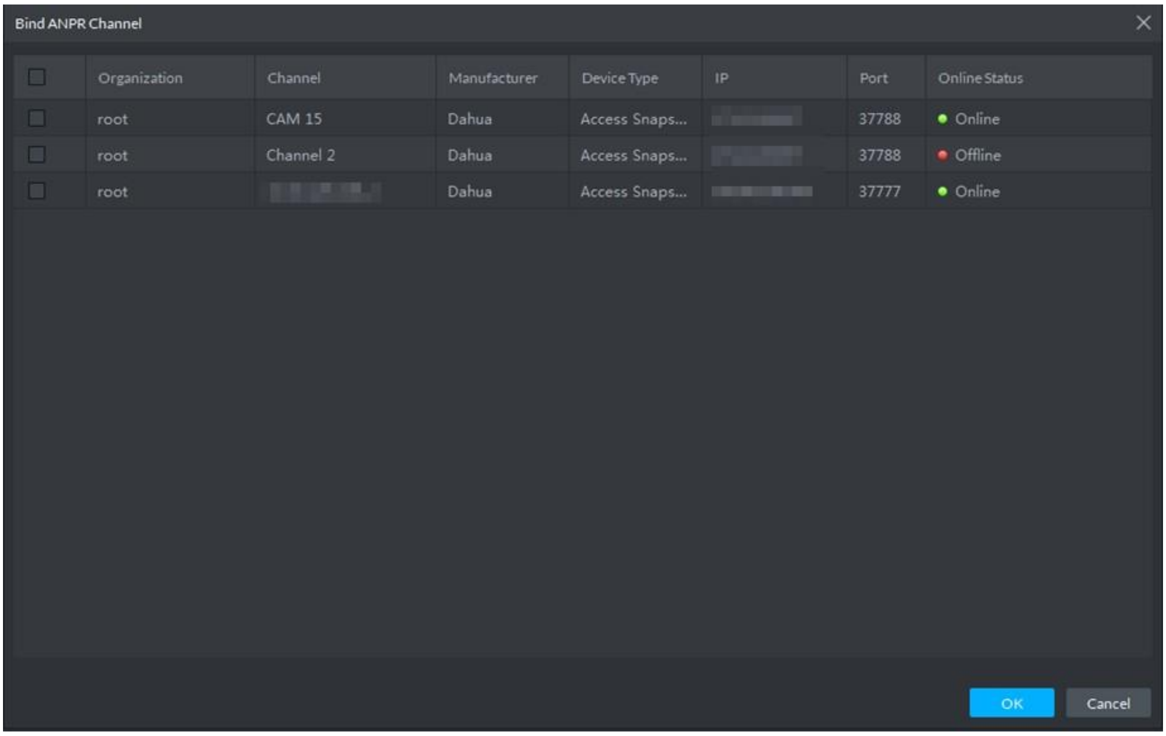

VMX
Entrance
1.Parking Lot Info
2.Device Config
3.Bind LED
Add ANPR Channel
Previous Step
Save and Exit
Next Step
Cancel

Sorry, there's no search result.

Step 4 Add ANPR device.

1) Click **Add ANPR Channel** and you can select all the ANPR devices deployed at entrance and exit of the parking lot on the interface. See Figure 3-460.

Figure 3-460 Add ANPR device



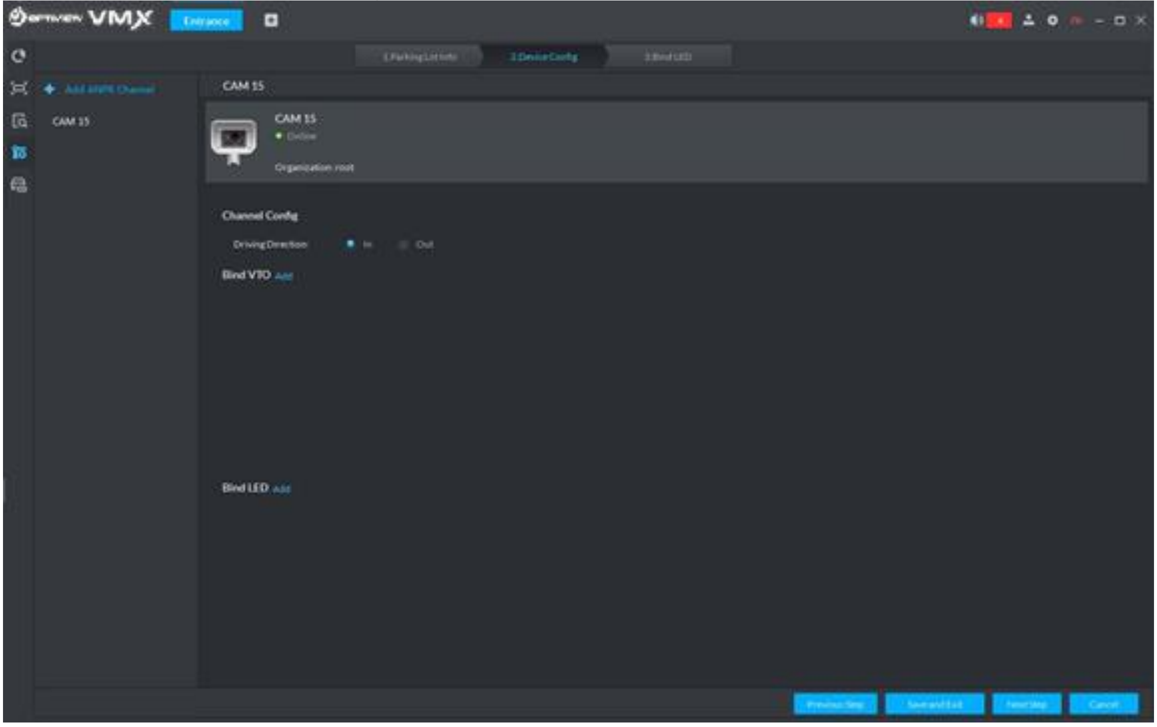
Bind ANPR Channel

☐	Organization	Channel	Manufacturer	Device Type	IP	Port	Online Status
☐	root	CAM 15	Dahua	Access Snaps...	[redacted]	37788	● Online
☐	root	Channel 2	Dahua	Access Snaps...	[redacted]	37788	● Offline
☐	root	[redacted]	Dahua	Access Snaps...	[redacted]	37777	● Online

2) Click **OK**.

The system displays the information of added ANPR device. See Figure 3-461.

Figure 3-461 ANPR device info


VMX
Entrance
1.Parking Lot Info
2.Device Config
3.Bind LED
Add ANPR Channel
CAM 15
CAM 15
CAM 15
Online
Organization: root
Channel Config
Driving Direction
In
Out
Bind VTO
Add
Bind LED
Add
Previous Step
Save and Exit
Next Step
Cancel

3) Select ANPR device from device list in sequence, and set corresponding driving direction. Default driving direction is **In**.

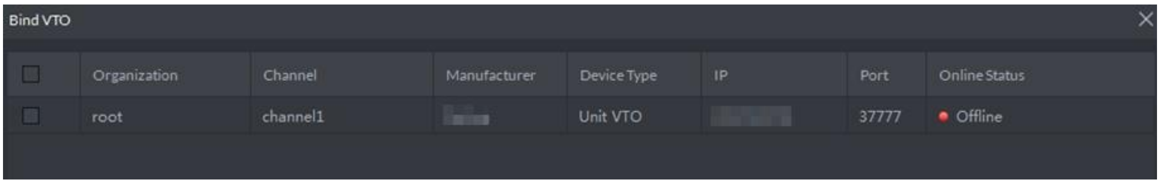
Step 5 Bind VTO device.

VTO device is used to recognize people, and unlock barrier. Please skip this step if there is no VTO in the networking.

1) Click **Add** next to **Bind VTO**.

The system displays the interface of **Bind VTO**. See Figure 3-462.

Figure 3-462 VTO device info



Bind VTO

☐	Organization	Channel	Manufacturer	Device Type	IP	Port	Online Status
☐	root	channel1	[redacted]	Unit VTO	[redacted]	37777	● Offline

2) Select the VTO that is deployed next to barrier, and click **OK**.

The interface displays the VTO information.

Step 6 Click **Next**.

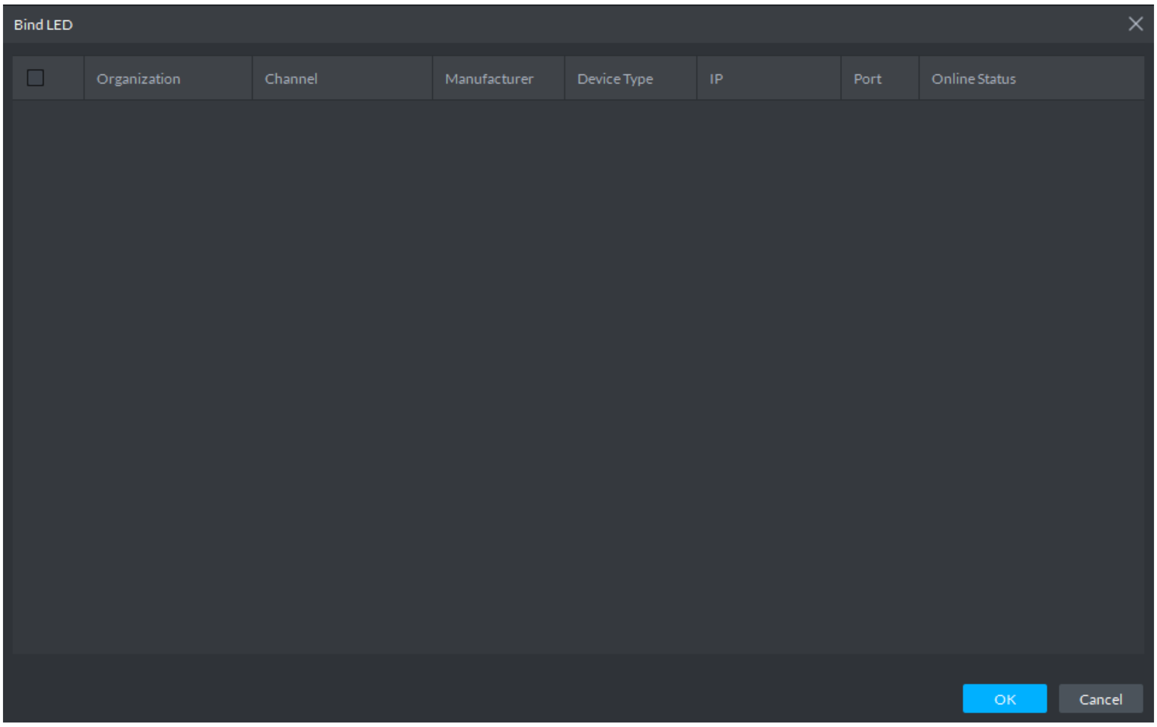
The system displays Bind LED.

Step 7 Add LED.

1) Click **Add LED**.

The system displays the interface of **Bind LED**. See Figure 3-463.

Figure 3-463 LED device info


Bind LED
☐
Organization
Channel
Manufacturer
Device Type
IP
Port
Online Status
OK
Cancel

2) Select all the LED of the parking lot and click **OK**.

The system displays the information of LED.

3.21.5 Vehicle Management

Vehicle info management includes vehicle type, department, related personnel and release ANPR, which are used as judgment basis to confirm if the vehicle can enter some area. Vehicle management can synchronize added vehicle info from personnel management module.

Step 1 Click 🚗 on the interface of **Entrance**.

The system displays the interface of Vehicle Management. See Figure 3-464.

📖

You can set serach condition, click **Search** and the system displays vehicle info including vehicle information added on personnel management module.

Figure 3-464 Vehicle management

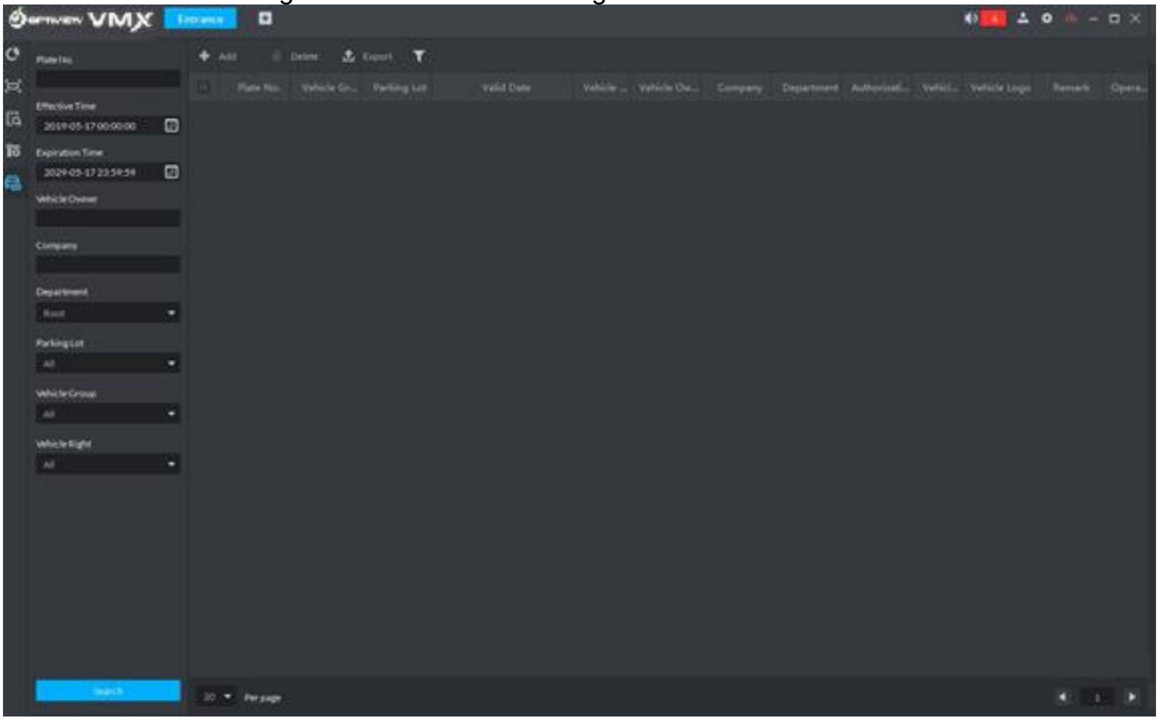

VMX
Entrance
Add
Delete
Export
Plate No.
Vehicle Gr...
Parking Lot
Valid Date
Vehicle ...
Vehicle Ow...
Company
Department
Authorizati...
Vehicl...
Vehicle Logo
Remark
Opera...
Search
Per page

Plate No.

Effective Time: 2019-05-17 00:00:00

Expiration Time: 2029-05-17 23:59:59

Vehicle Owner

Company

Department: Root

Parking Lot: All

Vehicle Group: All

Vehicle Right: All

20 Per page

Step 2 Click **Add**.

The system displays the interface of **Add**. See Figure 3-465.

Figure 3-465 Add vehicle

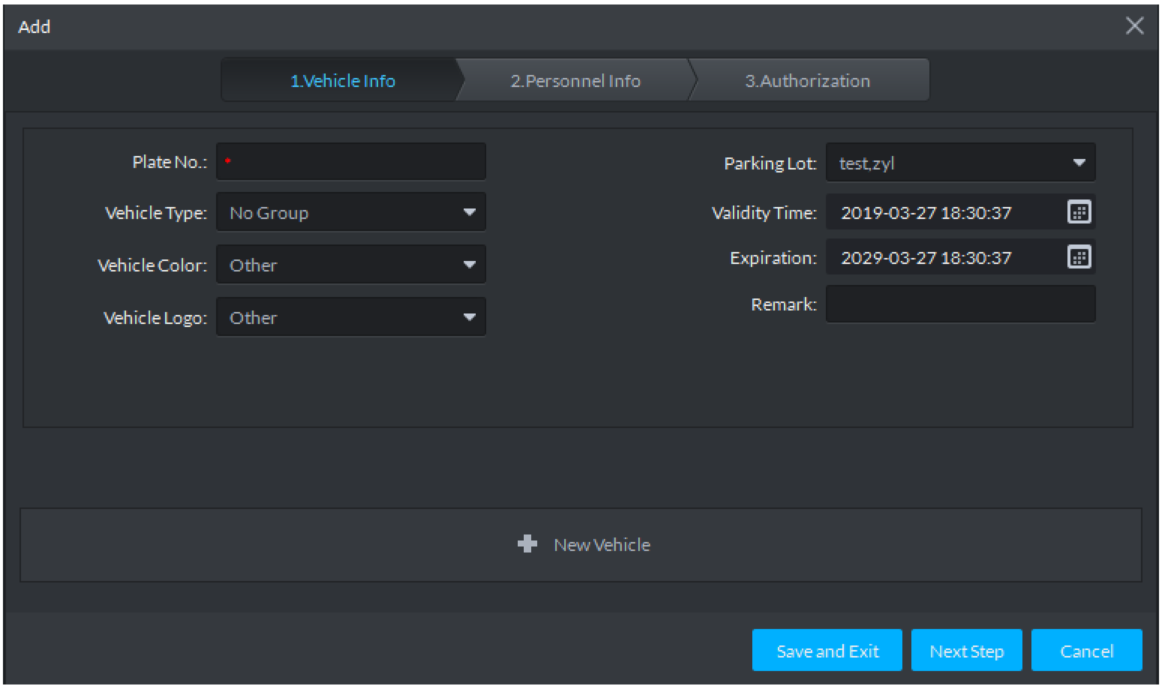

Add
1.Vehicle Info
2.Personnel Info
3.Authorization
New Vehicle
Save and Exit
Next Step
Cancel

Plate No.: *

Vehicle Type: No Group

Vehicle Color: Other

Vehicle Logo: Other

Parking Lot: test,zyl

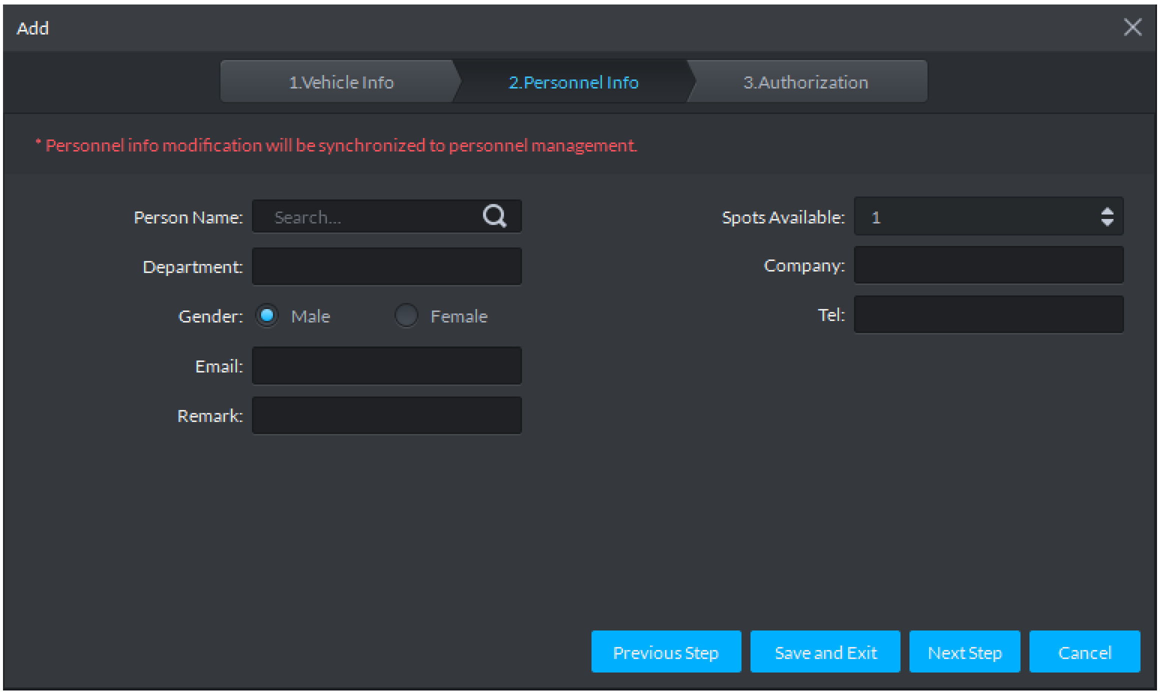
Validity Time: 2019-03-27 18:30:37

Expiration: 2029-03-27 18:30:37

Remark:

Step 3 Click the tab of **Vehicle Info** and add vehicle info, click **Next** and the system displays the interface of **Personnel Info**. Refer to Figure 3-466. Refer to Table 3-65 for parameter details.

Figure 3-466 Personnel info



* Personnel info modification will be synchronized to personnel management.

Person Name: Search...

Department:

Gender: ● Male ○ Female

Email:

Remark:

Spots Available: 1

Company:

Tel:

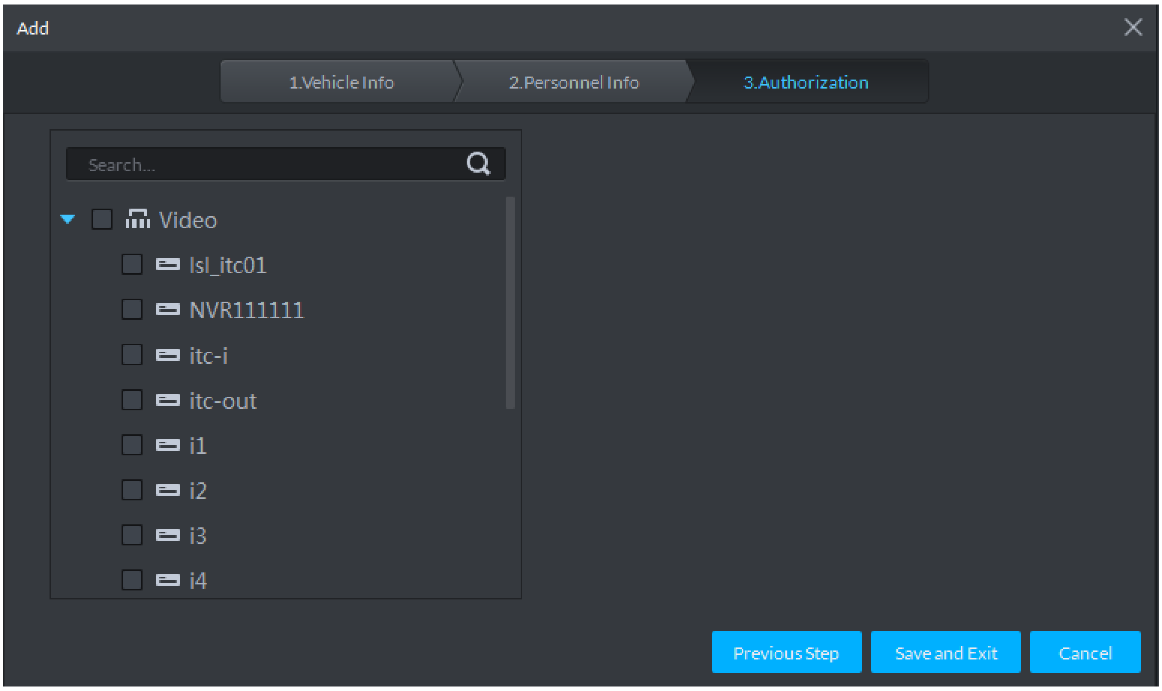
Table 3-65 Vehicle info

Parameter	Description
Plate No.	The plate number of added vehicle.
Vehicle Type	Include no group, general, VIP and blacklist. The first three types make up whitelist. If blacklist alarm scheme is set, then set vehicle type as blacklist, it will trigger alarm when vehicle is recognized.
Vehicle Color	Vehicle color of added vehicle. You can set **Not Recognized** if vehicle color cannot be recognized. If the color is beyond the selected range, then you can set is as **Other**.
Vehicle Logo	Main vehicle logos on the market.
Parking Lot	Area where vehicle belongs (required)
Validity Time	Validity period of added vehicle.
Expiration	
New Vehicle	If there are several vehicles, then click the button to add continuously. One person can add up to 5 vehicles.

Step 4 Set vehicle related personnel info, click **Next**.

The system displays the Authorization interface. See Figure 3-467.

Figure 3-467 Authentication


Add
1.Vehicle Info
2.Personnel Info
3.Authorization
Search...
Video
Isl_itc01
NVR111111
itc-i
itc-out
i1
i2
i3
i4
Previous Step
Save and Exit
Cancel

Step 5 Select all the ANPR devices that allow entrance and exit of the parkling lot, click **Save and Exit**. Synchronize vehicle info to corresponding ANPR device, and make sure the ANPR device can make judgment if it has to release the vehicle even if ANPR device is disconnected to platform.

3.21.6 Entrance Application

3.21.6.1 Overview

View the free parking ratio of current parking area; make statistics over real-time quantiy and on-site vehicle quantity, view quantity of entrance and exit vehicle within some period.

Click on the Entrance interface. The system displays the interface of Overview. See Figure 3-468. Refer to Table 3-66 for parameter details.

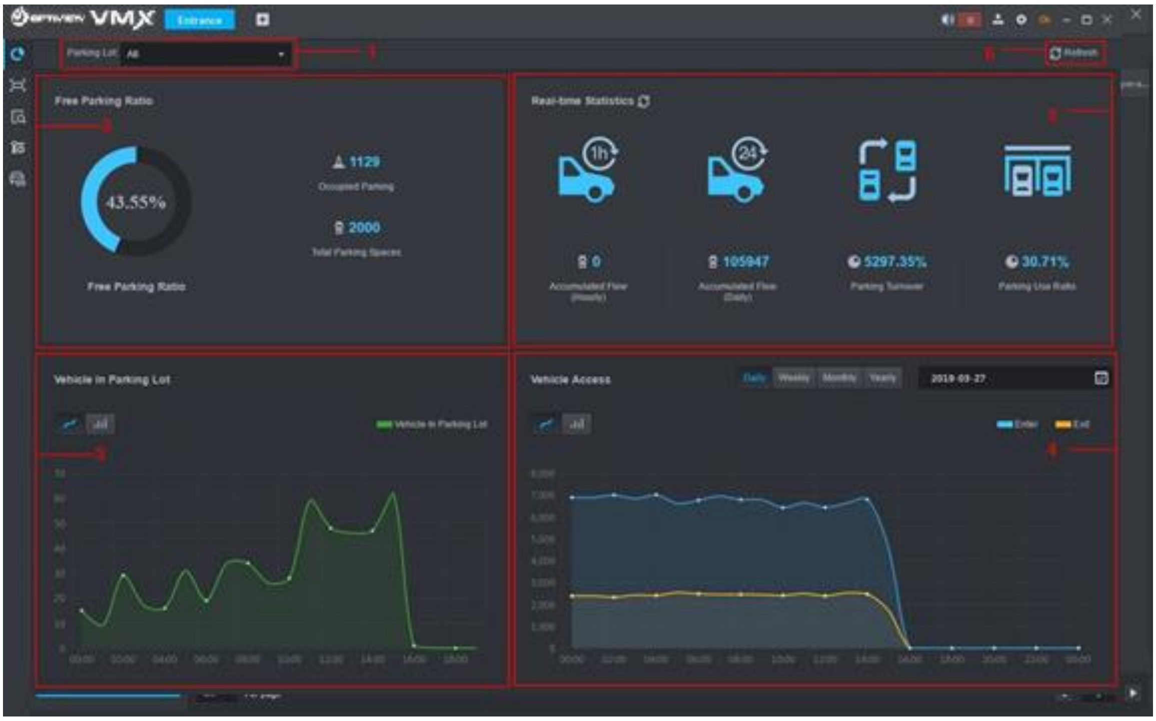

VMX
Entrance
Parking Lot
All
1
6
Refresh
Free Parking Ratio
2
43.55%
1129
Occupied Parking
2000
Total Parking Spaces
Free Parking Ratio
Real-time Statistics
5
0
Accumulated Flow (Hourly)
105947
Accumulated Flow (Daily)
5297.35%
Parking Turnover
30.71%
Parking Use Ratio
Vehicle in Parking Lot
3
Vehicle in Parking Lot
Vehicle Access
Daily
Weekly
Monthly
Yearly
2019-03-27
Enter
Exit
4

Figure 3-468 Overview

Table 3-66 Vehicle info overview

No.	Description
1	Interface displays the information of selected area; refer to other items for included content.
2	Display total parking spaces, occupied parking and free parking ratio of the selected parking lot.
3	Select occupied parking space quantity of selected area, the result can be displayed by line chart or bar chart. Move mouse on the image and displays corresponding time and occupied parking lot quantity.
4	Select vehicle access quantity of some period, supports day, week, month and year. Select time after period is selected; the system displays vehicle access quantity of selected period within the area. Blue means entered vehicle while orange means exited vehicle. The result can be displays by line chart or bar chart. Move the mouse on the image and display corresponding time and occupied parking space quantity.
5	Display following data. 1. Accumulated vehicle flow (hourly) Vehicle flow within current hour (for example, it is 8:42, and then it will make statistics about vehicle flow between 8:00 and 8:42). 2. Accumulated vehicle flow (Daily) Vehicle flow of the day (Start statistics from 00:00) 3. Parking turnover The bigger the parking turnover is, the shorter the vehicle stays in the parking lot, and then parking space reuse ratio is higher. If it is a paid parking lot, then it will make more money. 4. Parking Use Ratio The bigger the parking use ratio is, the average time of vehicle parking is longer.
6	Auto refresh overview info every 5 minutes. Click **Refresh** to sync real-time data.

3.21.6.2 License Plate Recognition

Click on the **Entrance** interface. The system displays the interface of **License Plate Recognition**. See Figure 3-469. Refer to Table 3-67 for more parameter details.

Figure 3-469 LPR

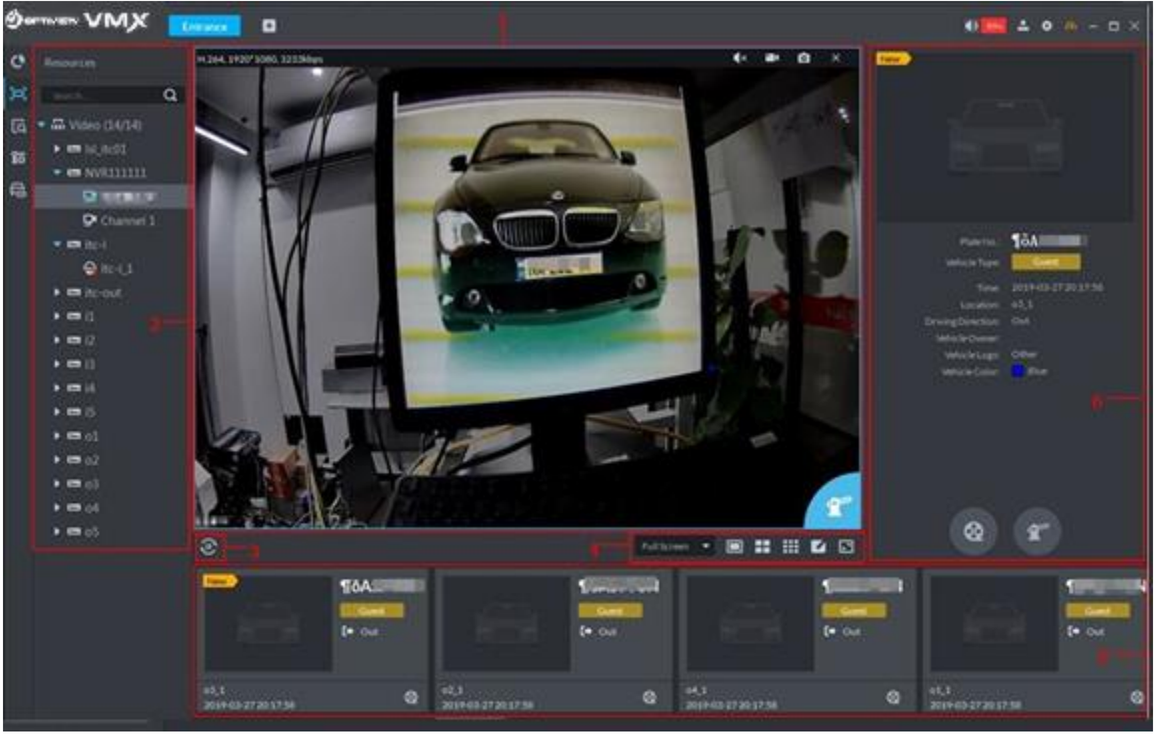


Table 3-67 LPR interface description

No.	Description
1	Real-time image display area. Select window, and Double-click video channel bound by ANPR in the device list, or drag the video channel bound by ANPR to window, and the interface displays real-time image. Move the mouse on the image, interface displays unlock button, click it to unlock barrier.
2	Device list. Display ANPR device and bound video channel.
3	Click the icon and it becomes ▶, and the interface will no longer ANPR recognition info. Click ▶ and the icon becomes ⏸, the interface will update real-time ANPR recognition info.

No.	Description
4	Full Screen ▾, set height and width ratio of video window, it plays video by two modes which are original scale and full screen. 1. , used to set image split mode, which includes 1 split, 4 splits and 9 splits, or click and customize split mode. 2. , switch video window to **Full Screen** mode. If you want to exit **Full Screen**, you can also press ESC button or right-click to select **Exit Full Screen**.
5	Display latest 4 snapshots of LPR. More details as follows. 1. Double-click a piece of ANPR record to display the details which includes vehicle information, scene picture of the snapshot moment and license plate picture. 2. Click and view video of linked channel.
6	Display license plate snapshot and vehicle which need to be released manually. More operation as follows. 1. Click and unlock barrier to release vehicle. 2. Click and view video of linked channel.

3.21.6.3 Info Query

Search accessed vehicle, on-site vehicle and snapshot record.

Step 1 Click on the **Entrance** interface.

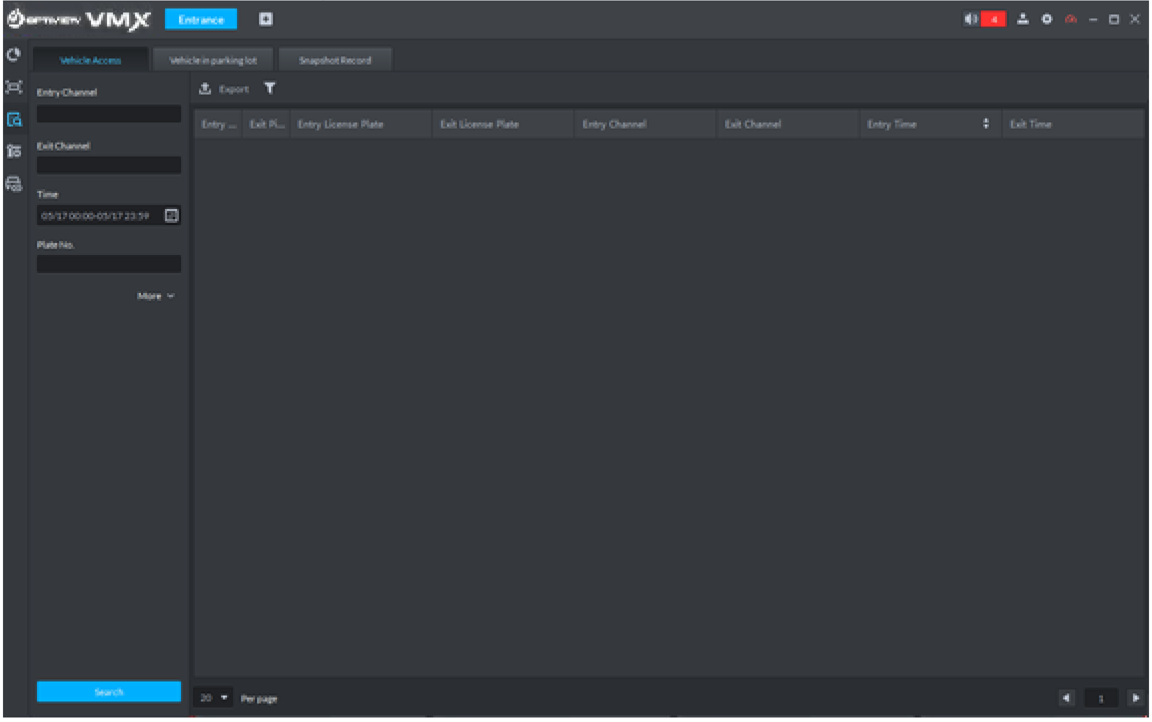
The system displays the interface of **Info Query**.

Step 2 Search vehicle in and out information.

1) Click the tab of **Vehicle Access**.

The system displays the interface of **Vehicle Access**. See Figure 3-470.

Figure 3-470 Vehicle access

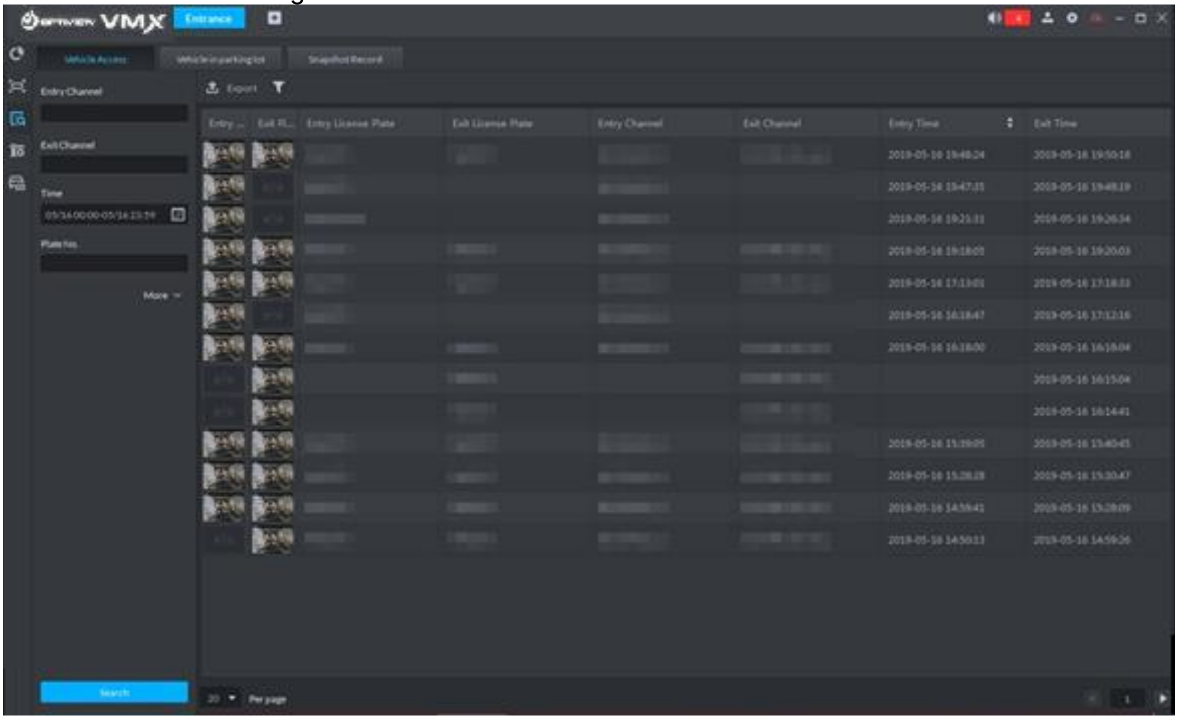

VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Entry Channel
Exit Channel
Time
05/17 00:00-05/17 23:59
Plate No.
More
Search
Export
Entry ...
Exit Pi...
Entry License Plate
Exit License Plate
Entry Channel
Exit Channel
Entry Time
Exit Time
20
Per page
1

2) Set search condition, click Search.

The system displays search results. See Figure 3-471.

Click **More** and you can search by vehicle owner, department and vehicle type etc.

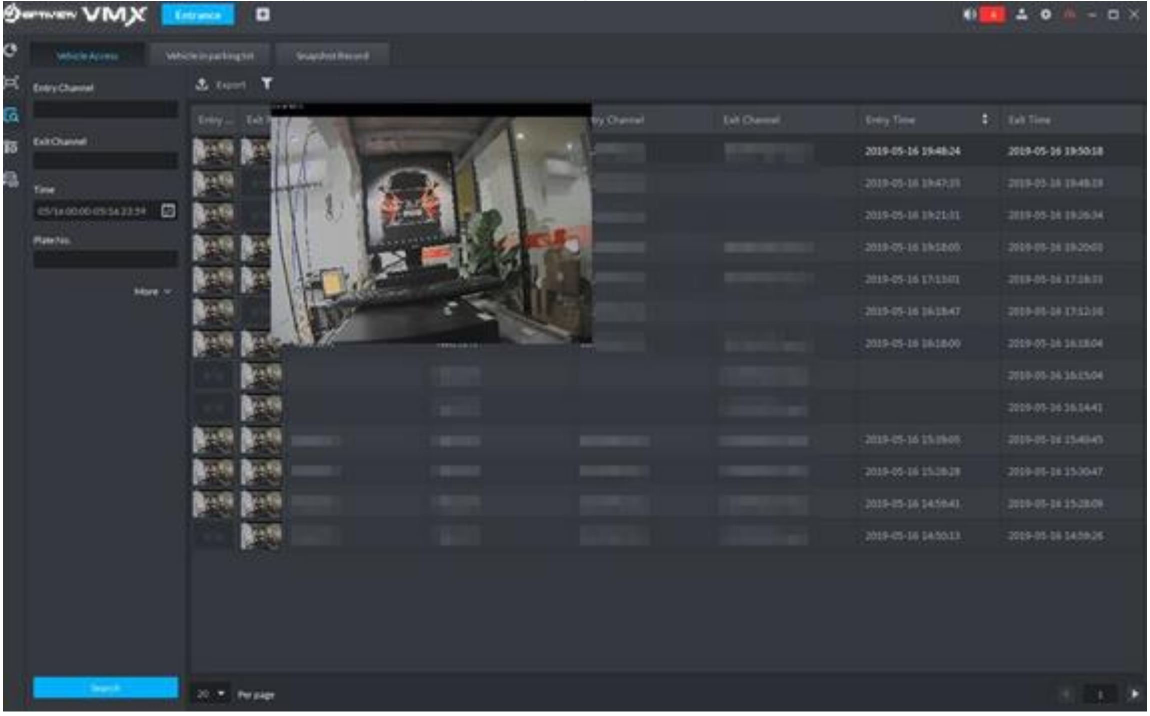
Figure 3-471 Vehicle access info


VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Entry Channel
Exit Channel
Time
05/16 00:00-05/16 23:59
Plate No.
More
Search
Export
Entry ...
Exit Pi...
Entry License Plate
Exit License Plate
Entry Channel
Exit Channel
Entry Time
Exit Time
20
Per page
1

3) The related operations of vehicle access are as follows.

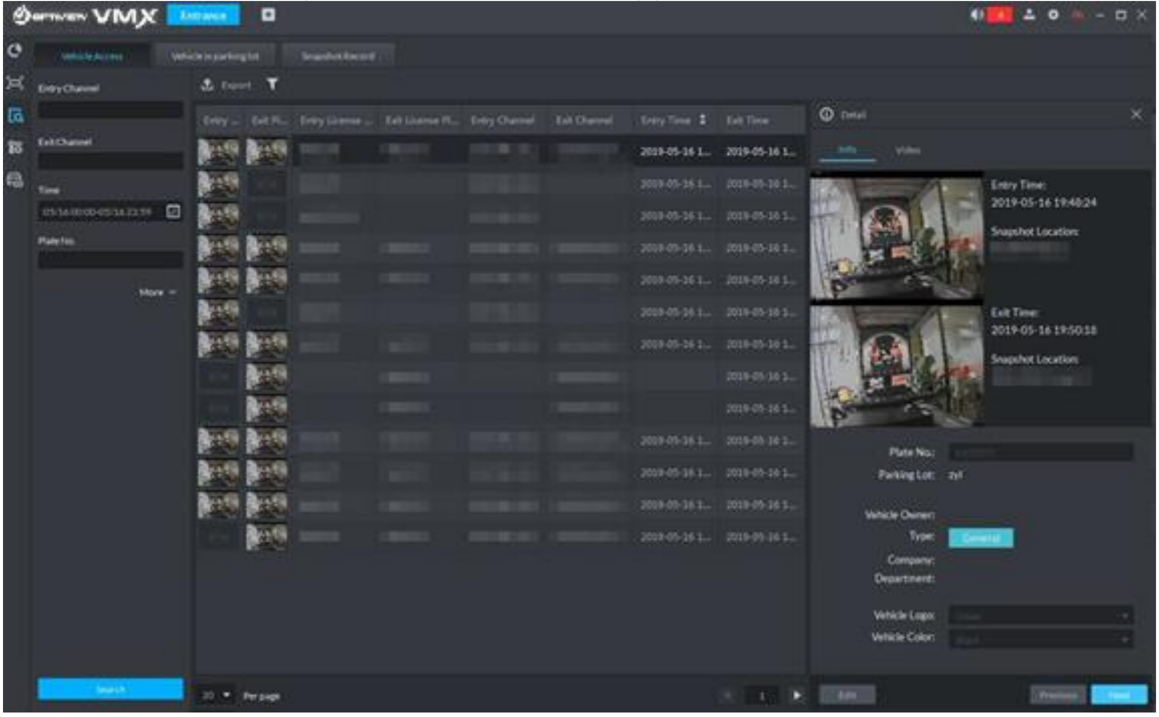
◇ Move the mouse to the recorded entry picture or exit picture, and the system will display a bigger picture. See Figure 3-472.

Figure 3-472 Big vehicle picture


VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Entry Channel
Exit Channel
Time
Plate No.
More
Search
Export
Entry Time
Exit Time
Per page

◇ Double-click the record, and detailed info is displayed on the right of interface. See Figure 3-473. Double-click the picture in the Info, display big picture, drag green box and the big picture will be displayed in the lower right corner. See Figure 3-474. Click **Edit** to modify vehicle info, click **OK** to save config. Click **Video** to view linked video.

Figure 3-473 Vehicle details (1)


VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Entry Channel
Exit Channel
Time
Plate No.
More
Search
Export
Detail
Info
Video
Type:
General
Edit
Previous
Next
Per page

Entry Time: 2019-05-16 19:48:24

Snapshot Location:

Exit Time: 2019-05-16 19:50:18

Snapshot Location:

Plate No.:

Parking Lot: zyl

Vehicle Owner:

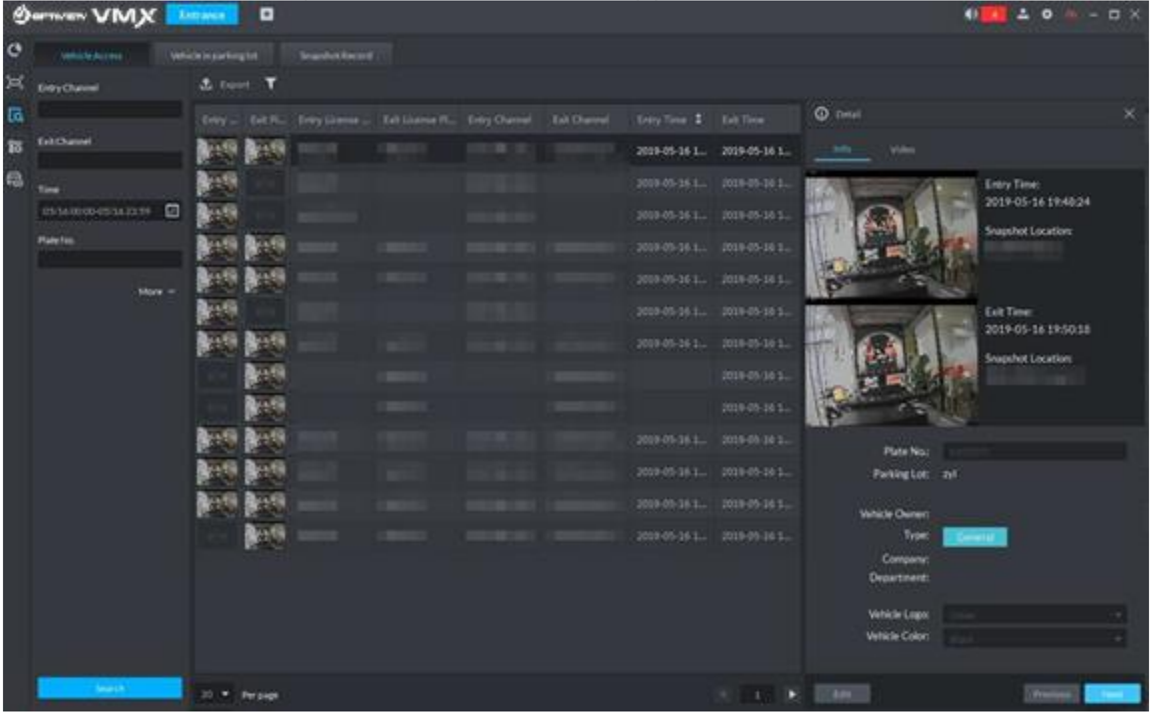
Company:

Department:

Vehicle Logo:

Vehicle Color:

Figure 3-474 Vehicle details (2)


VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Entry Channel
Exit Channel
Time
Plate No.
More
Search
Export
Entry Time
Exit Time
Detail
Info
Video
Entry Time:
2019-05-16 19:48:24
Snapshot Location:
Exit Time:
2019-05-16 19:50:18
Snapshot Location:
Plate No.:
Parking Lot:
Vehicle Owner:
Type:
General
Company:
Department:
Vehicle Logo:
Vehicle Color:
Per page
Edit
Previous
Next

◇ Export info. Click **Export** to export all the searched vehicle access info.

◇ Set info display item. Click ▼ and select display item.

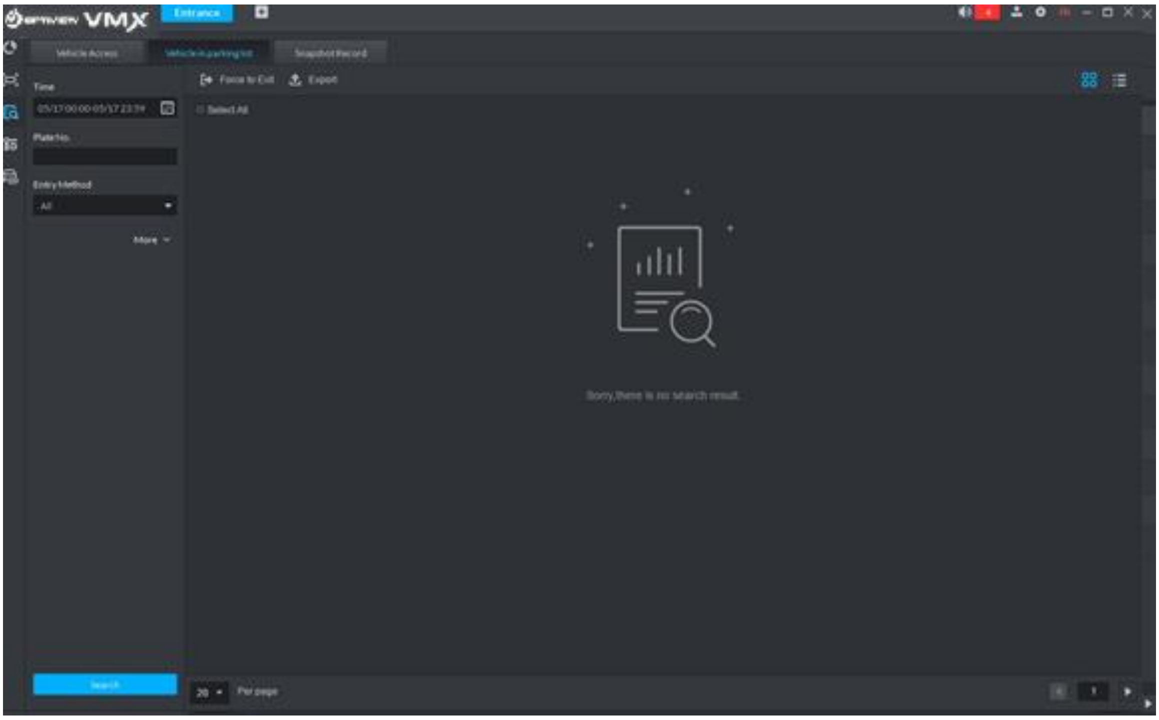
◇ Click **Next** and display next info detail. Click **Previous** and display previous info detail.

Step 3 Search on-site vehicle.

1) Click the tab of Vehicle in parking lot.

The system displays the interface of **Vehicle in Parking Lot**. See Figure 3-475.

Figure 3-475 Vehicle in parking lot

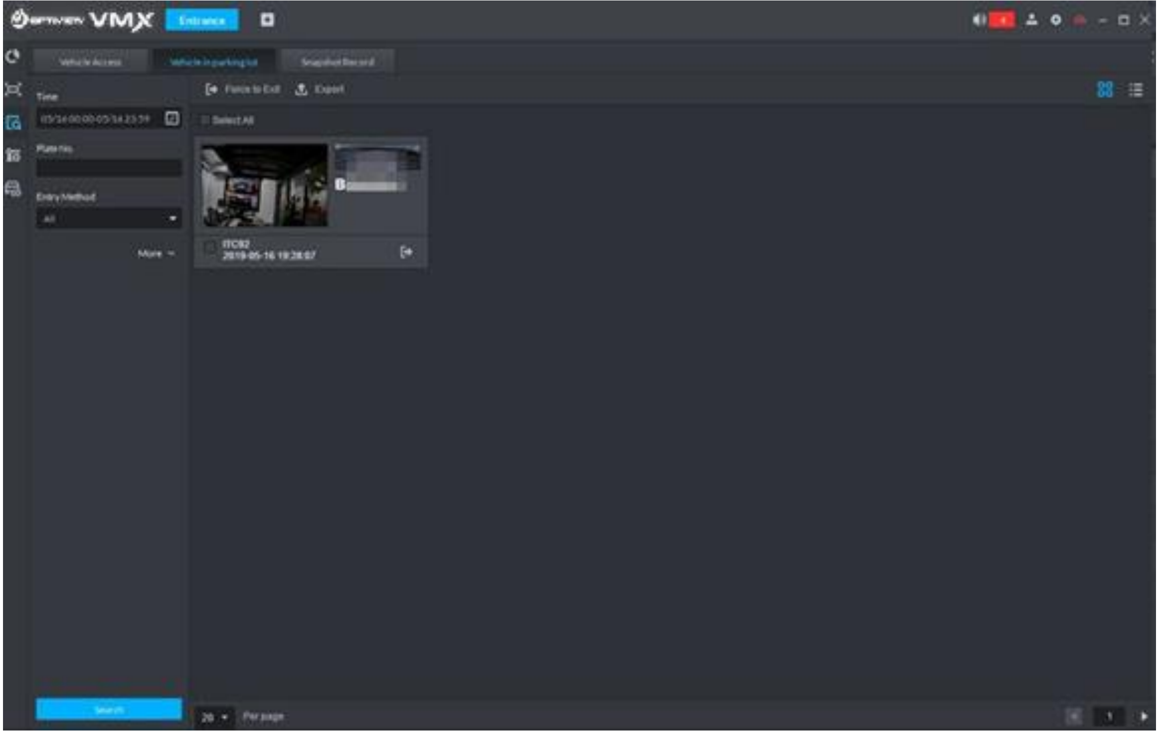

VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Time
Plate No.
Entry Method
All
More
Force to Exit
Export
Select All
Sorry, there is no search result.
Search
20
Per page

2) Set search condition, Click **Search**.

The system displays the search results. See Figure 3-476.

Click **More** and you can search info via vehicle owner, department and vehicle type etc.

Figure 3-476 Vehicle in parking lot info


VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Force to Exit
Export
Time
Select All
Plate no.
Entry Method
All
More
Search
20
Per page

ITC02
2019-05-16 19:28:07

3) Related operations of vehicle in and out are as follows.

◇ If the vehicle is confirmed not to be in the area, then click to select information (several items supported), and click **Force to Exit** or ⇥. Make sure the vehicle exits by Pro.

◇ Export information. Click **Export** and export all the information of on-site vehicles that can be searched.

◇ Set info display item. Click ▼ and select display item.

◇ Click view mode (▦) or list mode (☰) to select different display mode.

Step 4 Search Snapshot Record

1) Click the tab of **Snapshot Record**.

The system displays the interface of **Snapshot Record**. See Figure 3-477.

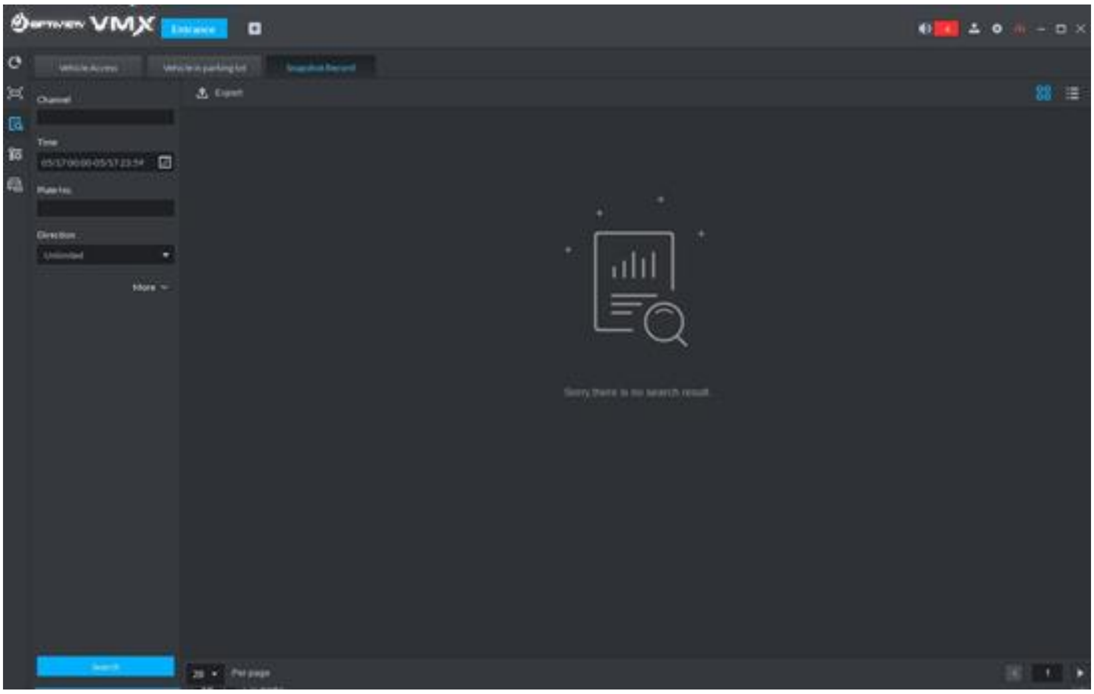

VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Channel
Time
Plate No.
Direction
Unlimited
More
Export
Sorry, there is no search result.
Search
Per page

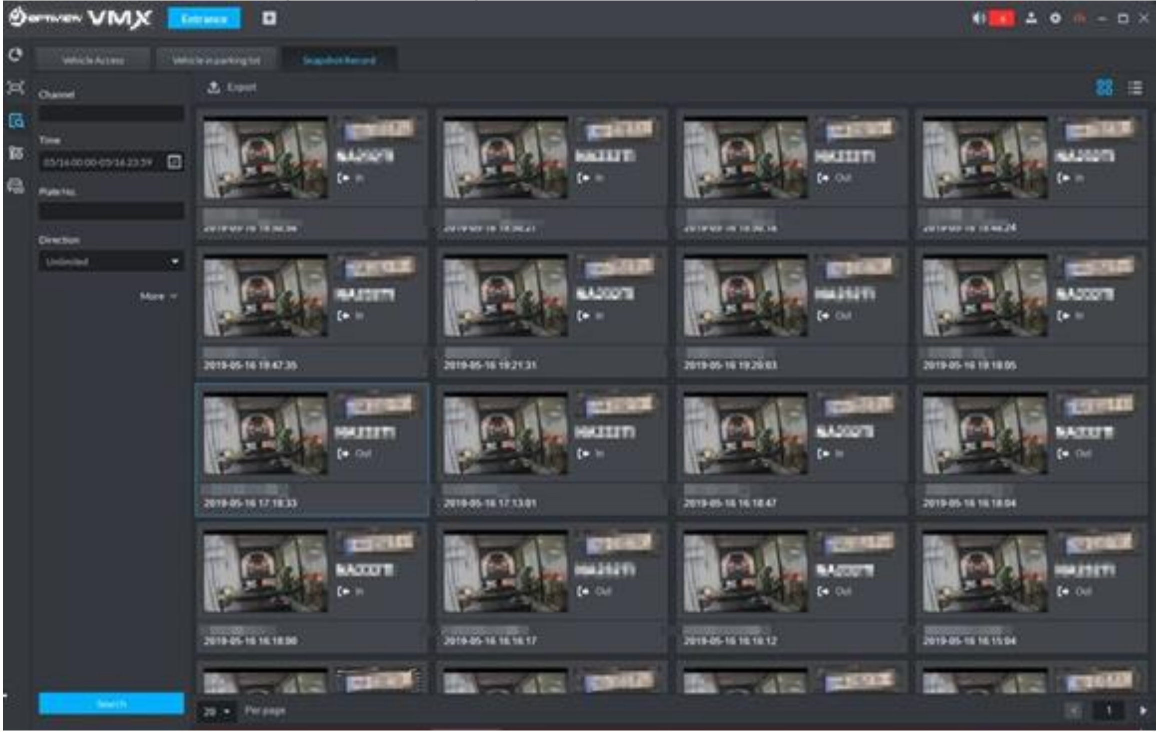
Figure 3-477 Snapshot record

2) Set search condition, click **Search**.

The system displays search results. See Figure 3-478.

Click **More** and you can search info via vehicle owner, department and vehicle type etc.

Figure 3-478 Snapshot record info


VMX
Entrance
Vehicle Access
Vehicle in parking lot
Snapshot Record
Channel
Time
Plate No.
Direction
Unlimited
More
Export
In
Out
Search
Per page

3) Related operations of vehicle snapshot are as follows.

- ◇ Export info. Click **Export** to export all the info of on-site vehicles that can be searched.

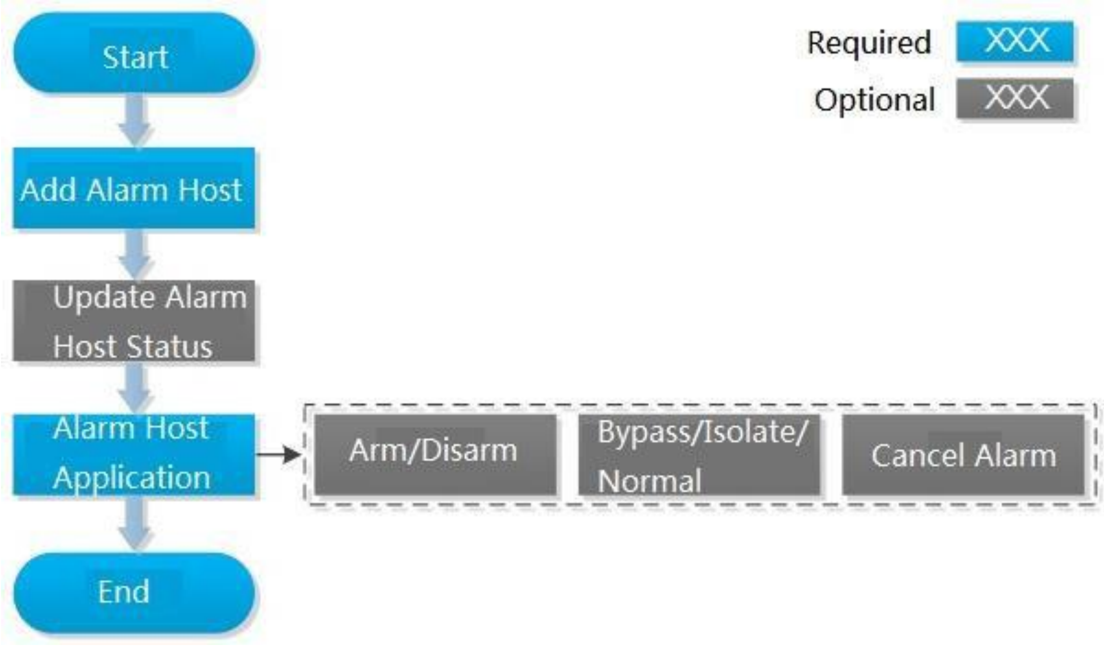
◇ Click view mode (⊞) or list mode (☰) and select different display modes.

3.22 Alarm Host

After adding alarm host to platform, you can manage and configure alarm zone and sub system.

The alarm host operation flow is shown in Figure 3-479.

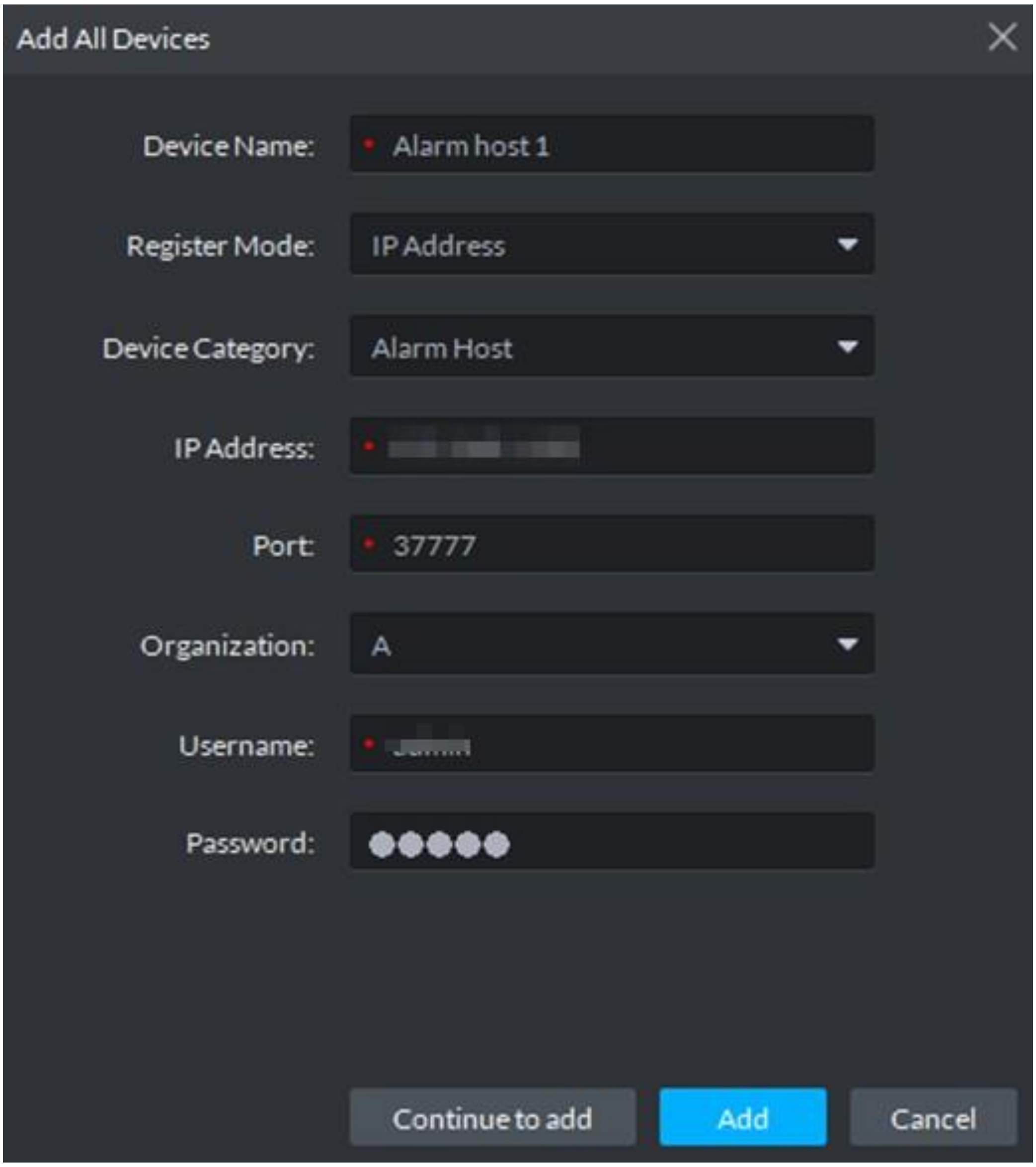
Figure 3-479 Alarm host management flow


Start
Add Alarm Host
Update Alarm Host Status
Alarm Host Application
End
Arm/Disarm
Bypass/Isolate/ Normal
Cancel Alarm
Required
XXX
Optional
XXX

3.22.1 Adding Alarm Host

Step 1 Add alarm host, set Device Category as Alarm Host, and see Figure 3-480. For more details, see 3.2.2.4 Adding Device

Figure 3-480 Add alarm host



Add All Devices

Device Name: * Alarm host 1

Register Mode: IP Address

Device Category: Alarm Host

IP Address: * [redacted]

Port: * 37777

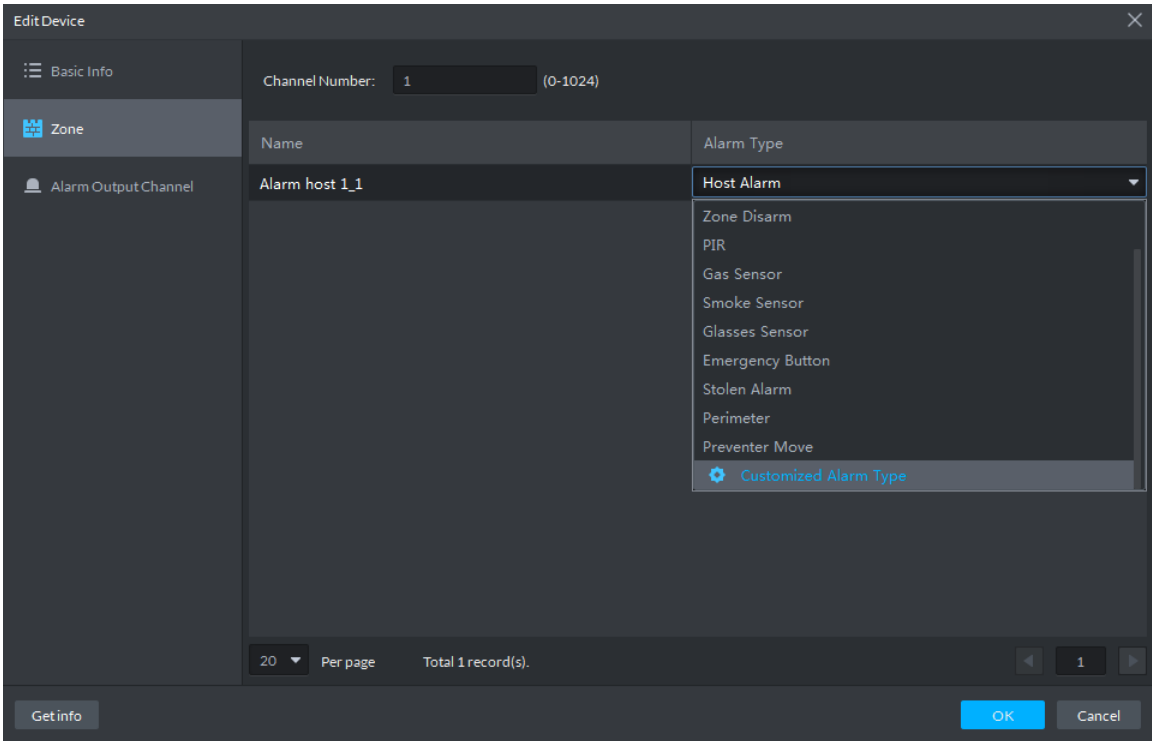
Organization: A

Username: * [redacted]

Password: ●●●●●

Step 2 Modify device zone info. For example, zone is connected to smoke sensor, then select **Alarm Type** as **Smoke Sensor**, see Figure 3-481. Alarm type supports custom, you can select **Customized Alarm Type** from the **Alarm Type** box, and set the alarm type you need, used to quickly recognize alarm. With the zone type configured correctly here, you can set the corresponding alarm types when configuring event rules for the zones. For example, if the zone type is selected as “smoke detector”, the “smoke alarm” type will appear for you to select when configuring alarm rule for this zone.

Figure 3-481 Modify zone


Edit Device
Basic Info
Zone
Alarm Output Channel
Zone Disarm
PIR
Gas Sensor
Smoke Sensor
Glasses Sensor
Emergency Button
Stolen Alarm
Perimeter
Preventer Move
Customized Alarm Type
Get info
OK
Cancel

Channel Number: 1 (0-1024)

Name	Alarm Type
Alarm host 1_1	Host Alarm

20 Per page Total 1 record(s).

3.22.2 Entering Alarm Controller Interface

Click + and select Alarm Controller on the client homepage, the system displays Alarm Controller interface, see Figure 3-482.

Figure 3-482 Alarm controller interface

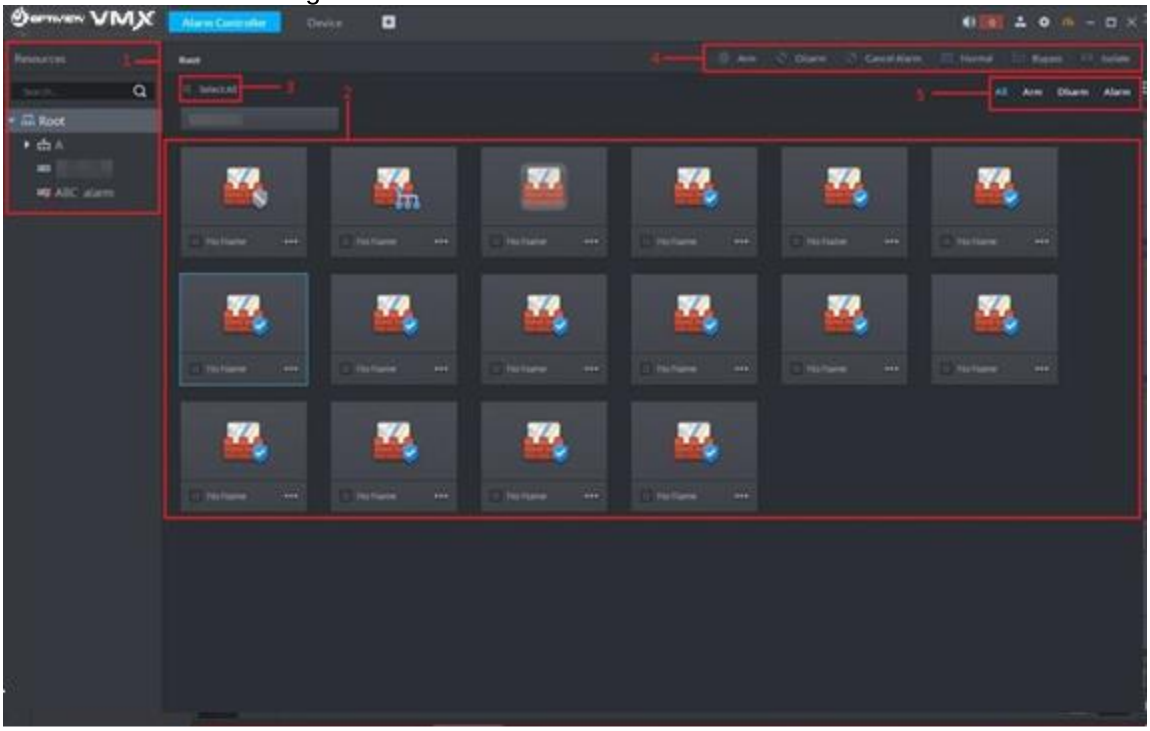


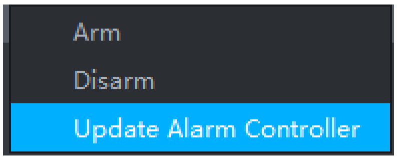
Table 3-68 Alarm controller interface description

No.	Name	Description
1	Device list	Display all alarm controller devices and subsystems under device. Icon status of subsystem ● , no zone under subsystem. ● , zone exists under subsystem The subsystem and zone info displayed on platform can be acquired from device; the platform does not support config.
2	Subsystem and zone list	● Clicking on an alarm controller name in the device tree, its subsystems and the zones not yet added to subsystems will be displayed on the right. ● Clicking on a subsystem name, the zones in this subsystem will be displayed on the right. The description of icon status is shown as follows. ● Zone status icon ◇ , arm. ◇ , disarm. ◇ , bypass. ◇ , isolate. ● Subsystem status icon ◇ , all zones armed under subsystem. ◇ , all zones disarmed under subsystem. ◇ , zones are not distributed by subsystem. ◇ , some zones under subsystem are armed.
3	Select all	Select all subsystems and zones displayed in list.
4	Operation button	Operation buttons supported by zone or subsystem.
5	Filter button	Click the button, the subsystem and zone of corresponding status are displayed in the list.

3.22.3 Updating Alarm Controller Status

In the device tree area, right-click the alarm controller that needs to be updated, select **Update Alarm Controller**, and see Figure 3-483. The platform synchronizes status of alarm controller.

Figure 3-483 Update alarm controller



3.22.4 Alarm Controller Application

3.22.4.1 Arm/Disarm

After armed, the alarm controller makes response upon the alarm signal from zone; You can disarm the zone and controller will not upload alarm message.

3.22.4.1.1 Global Arm/Disarm

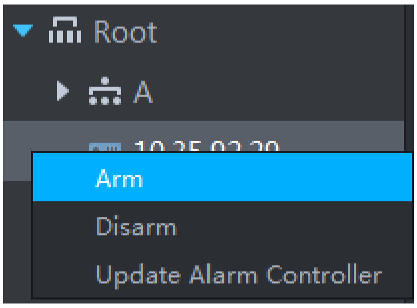
Globally arm or disarm all zones under alarm controller.

Arm

In device tree area, right-click the alarm controller that needs to be armed globally, select **Arm**, and see Figure 3-484.

Arm fails when alarm input exists in zone. Please disarm if you continue to arm, clear alarms in each zone, zone with alarm input exists in bypass, and then arm again.

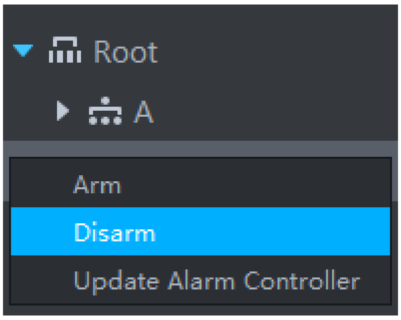
Figure 3-484 Global arm



Disarm

In device tree area, right-click the alarm controller that needs to be disarmed globally, select **Disarm**, and see Figure 3-485.

Figure 3-485 Global disarm


Root
A
Arm
Disarm
Update Alarm Controller

3.22.4.1.2 Arm/Disarm Zone or Subsystem

Arm or disarm single zone.

Arm

- Arm fails when alarm input exists in zone. Please disarm if you continue to arm, clear alarms in each zone, zone with alarm input exists in bypass, and then arm again.
- If subsystem has no zone, then you cannot arm or disarm subsystem.

You can arm by following two methods

- Click the zone you want to arm or ••• of corresponding subsystem, select **Arm**, see Figure 3-486 and Figure 3-487.

Figure 3-486 Arm zone

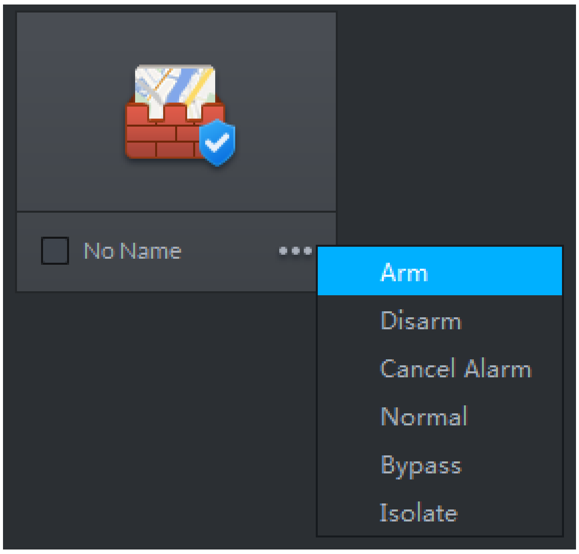
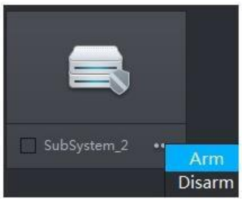
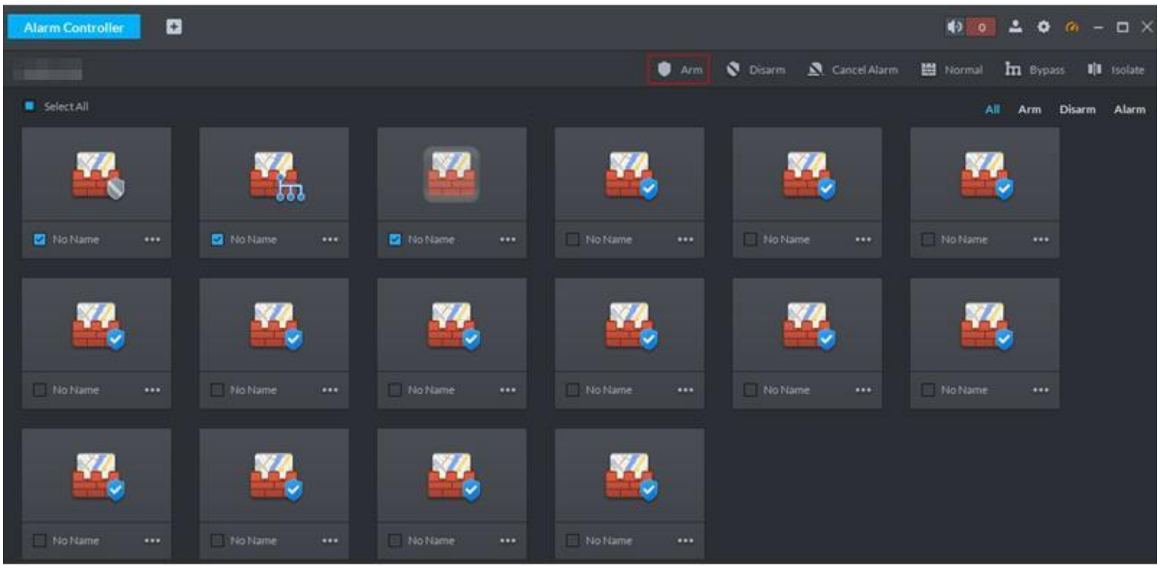

No Name
Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate

Figure 3-487 Arm subsystem


SubSystem_2
Arm
Disarm

- Select the zone or subsystem you want to arm (multiple choice supported), click **Arm** on top of the interface, and see Figure 3-488.

Figure 3-488 Arm


Alarm Controller
Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate
Select All
All
Arm
Disarm
Alarm
No Name

Disarm

Supports disarm by following two methods.

- Click the zone you want to disarm or ••• of corresponding subsystem, select **Disarm**, see Figure 3-489 and Figure 3-490.

Figure 3-489 Disarm zone

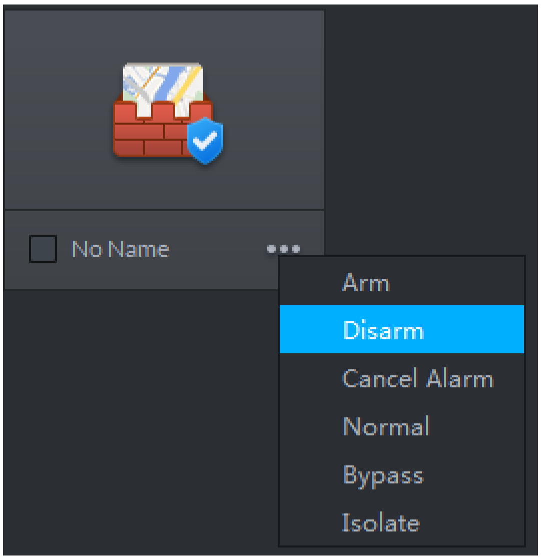
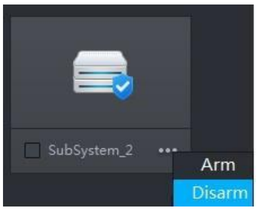
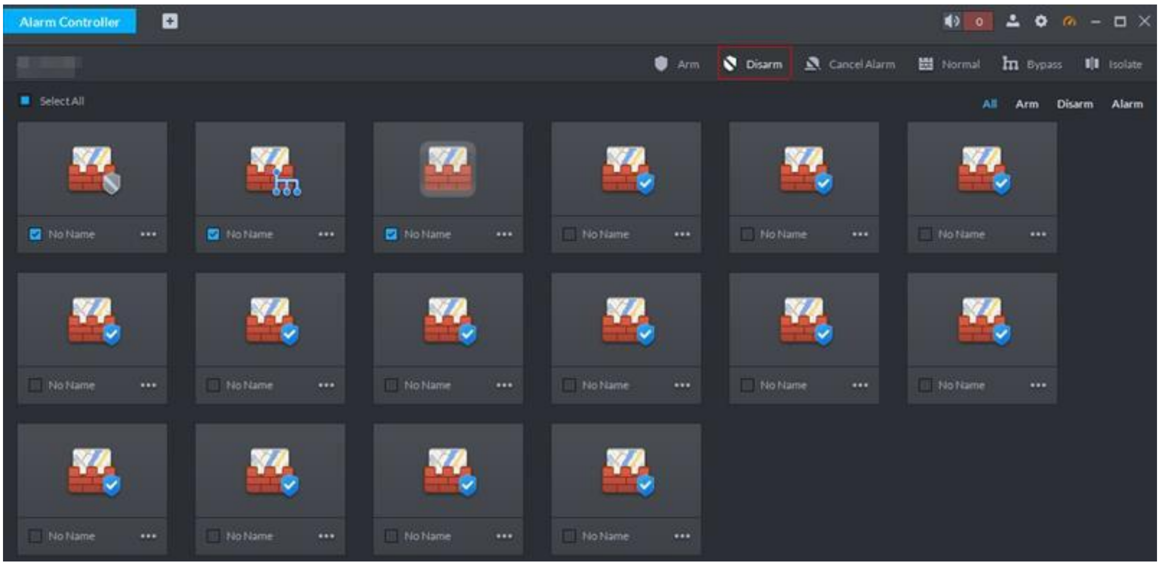

No Name
Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate

Figure 3-490 Disarm subsystem


SubSystem_2
Arm
Disarm

- Select the zone or subsystem you want to disarm (multiple choice supported), click **Disarm** on top of the interface, and see Figure 3-491.

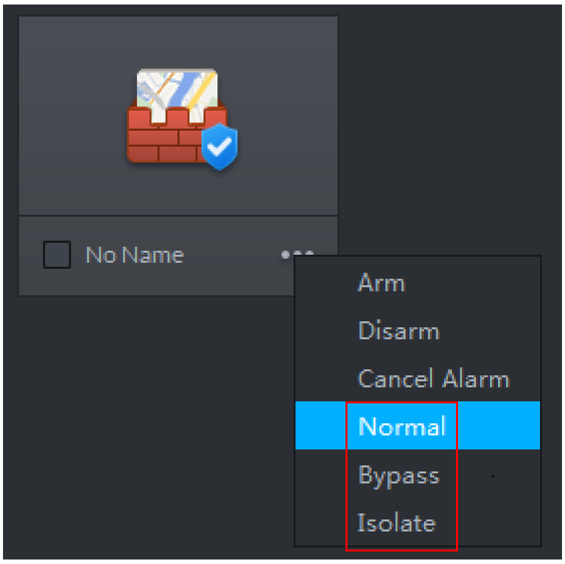
Figure 3-491 Disarm


Alarm Controller
Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate
Select All
All
Arm
Disarm
Alarm
No Name

3.22.4.2 Bypass/Isolate/Normal

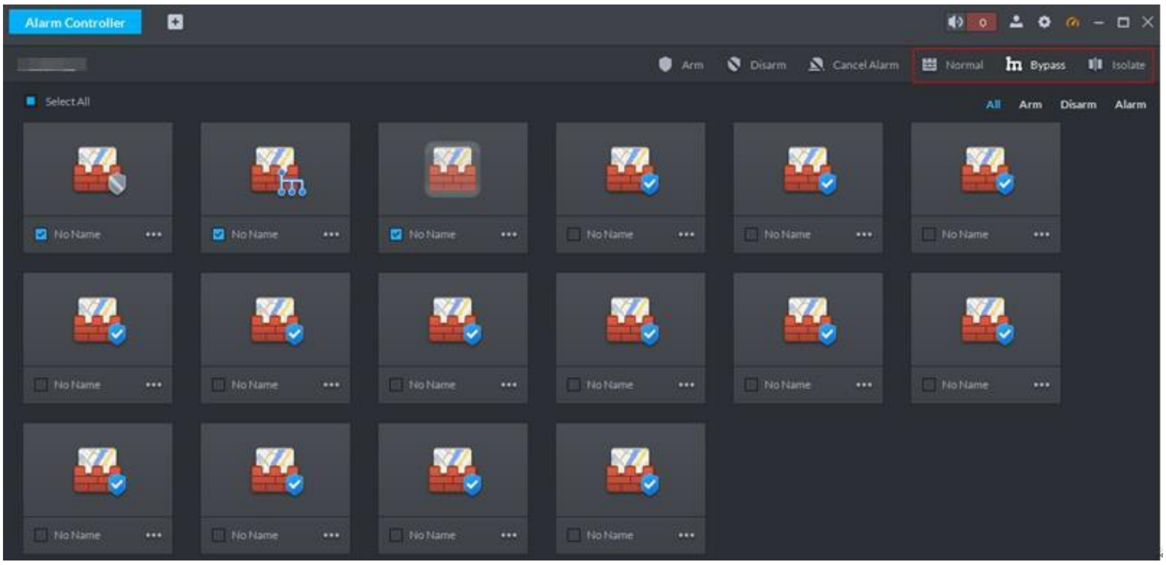
- Bypass zone, the alarm controller still monitors external detector and make records, but not forward to users. If you want to arm the bypassed zone, please disarm the zone into non-bypass and arm again.
- Isolate zone, the alarm controller still monitors external detector and make records, but not forward to users. When the zone is disabled or you want to disarm and arm again, the isolated zone is still disabled.
- Normal zone, the zone can trigger alarm normally when it is armed.
- Two ways to arm/disarm a zone. Click ••• of the zone that needs to be bypassed, isolated or recovered to normal, select operation and see Figure 3-492.

Figure 3-492 Bypass/isolate zone (1)


No Name
Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate

- Select the zone that needs to be bypassed, isolated or recovered normal (multiple choice supported), click the operation buttons on top of the interface, see Figure 3-493.

Figure 3-493 Bypass/isolate zone (2)

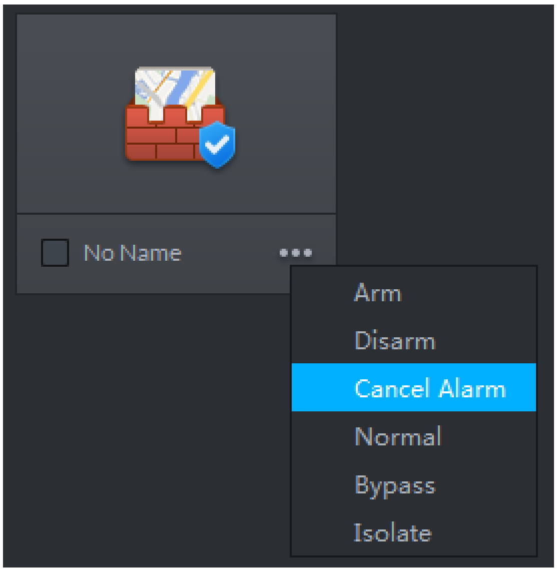

Alarm Controller
Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate
Select All
All
Arm
Disarm
Alarm
No Name

3.22.4.3 Cancel Alarm

You remove alarm by **Cancel Alarm** when alarm is triggered.

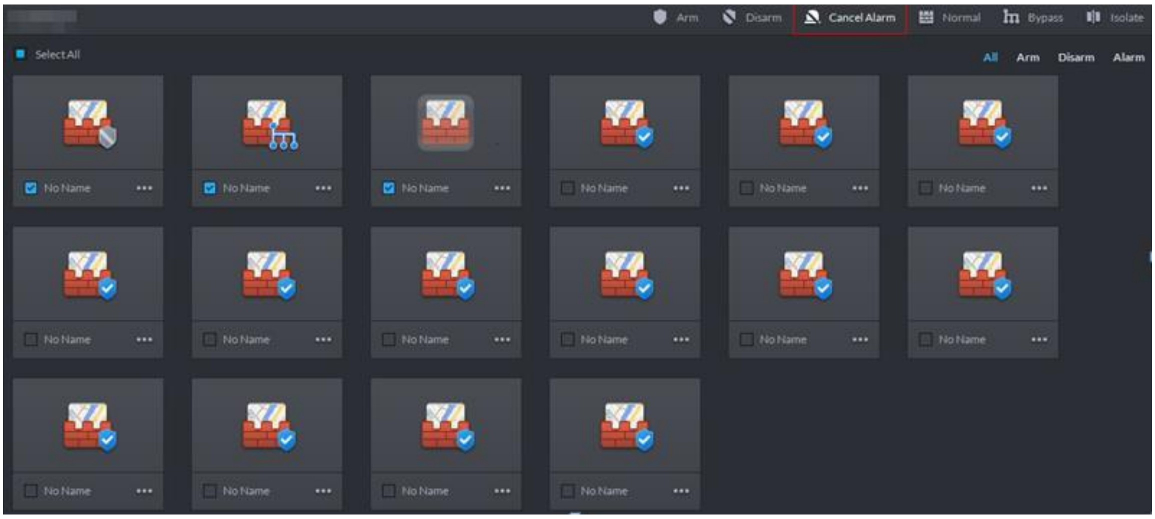
- Click the zone you want to cancel alarm, select **Cancel Alarm** and see Figure 3-494.

Figure 3-494 Cancel alarm


No Name
Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate

- Select the zone you want to cancel alarm (multiple choices supported), click **Cancel Alarm** on top of the interface and see Figure 3-495.

Figure 3-495 Cancel alarm (2)


Arm
Disarm
Cancel Alarm
Normal
Bypass
Isolate
Select All
All
Arm
Disarm
Alarm
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name
No Name

4 Maintenance Guide

The chapter introduces daily maintenance, and make sure the platform runs safely and normally.

4.1 Backup and Restore

4.1.1 Backup

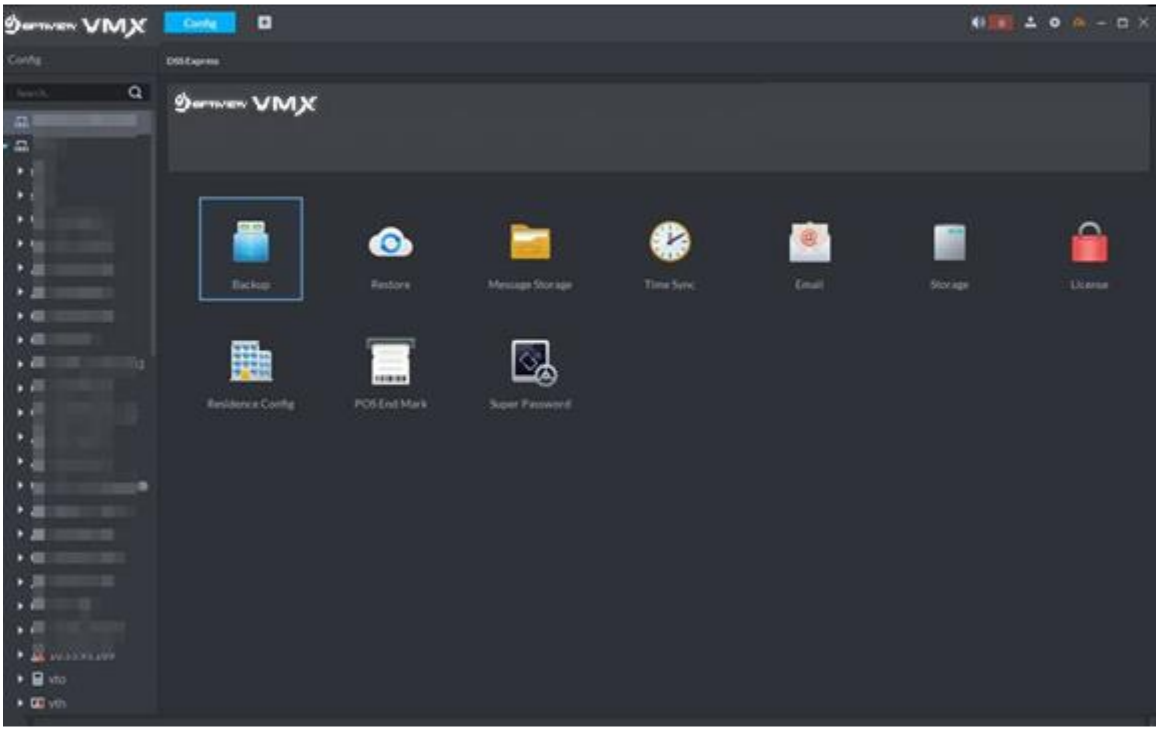
To guarantee data security, the platform provides data backup function; backup mode includes auto backup and manual backup. You are recommended to enable auto backup for regular data backup.

4.1.1.1 Auto Backup

Step 1 On client homepage, click **Config**.

The system displays **Config** interface, see Figure 4-1.

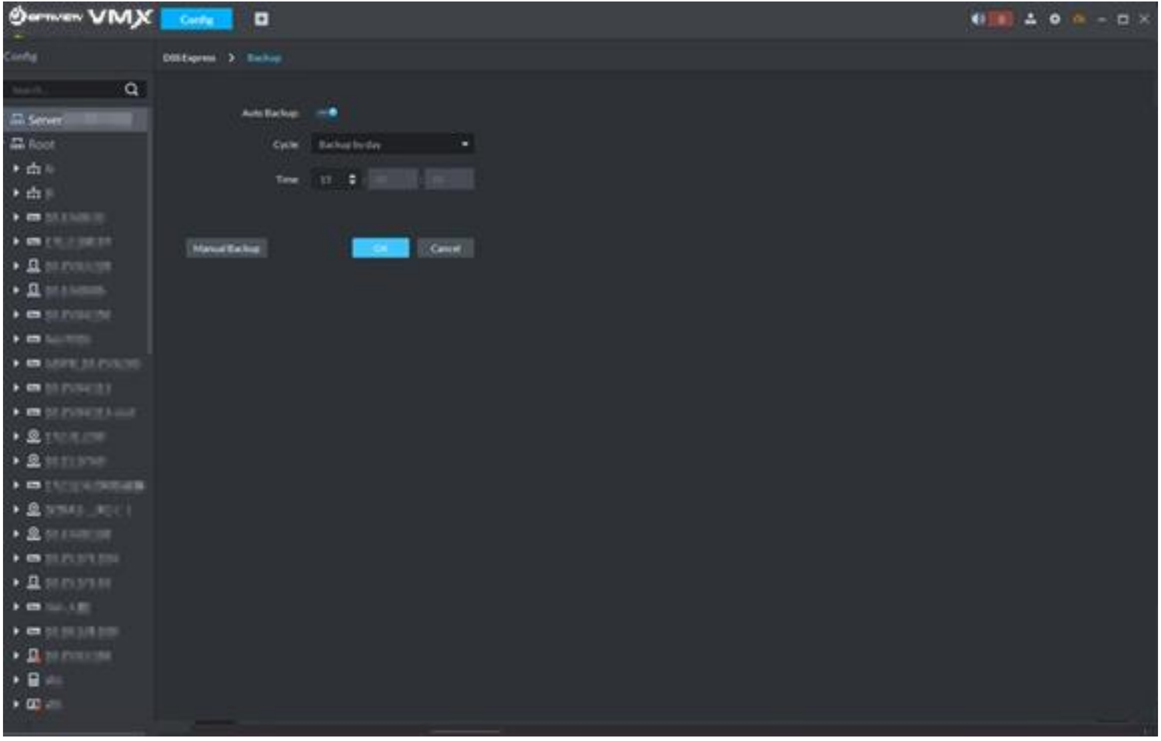
Figure 4-1 Config


VMX
Config
Config
DSS Express
VMX
Backup
Restore
Message Storage
Time Sync
Email
Storage
License
Residence Config
POS End Mark
Super Password

Step 2 Click Backup.

The system displays **Backup** interface, see Figure 4-2.

Figure 4-2 Backup



Auto Backup

Cycle: Backup by day

Time: 17

Step 3 Click next to Auto Backup.

The icon becomes , and auto back is enabled.

Step 4 Set **Cycle** and **Time**, click **OK**.

The system pops out the interface of **Set Backup File Password**.

You can select any whole hour between 3:00 and 23:00 to implement backup.

Step 5 Enter file password, click **OK**.

- File password, used to guarantee backup data file security, you need to enter password for verification if you want to open or restore backup file.
- Backup file is stored under server installation path, which is "..\Server\WEBCLIENT\webclient\apache-tomcat\tmp\systemBackup".

4.1.1.2 Manual Backup

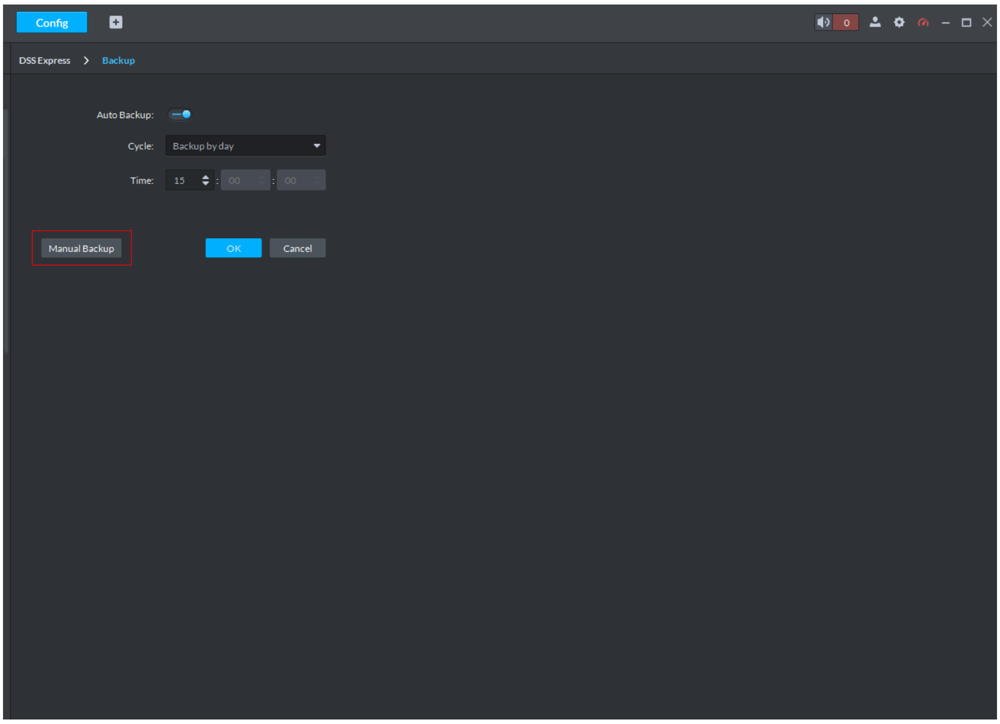
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Backup**.

The system displays **Backup** interface, see Figure 4-3.

Figure 4-3 Backup



Auto Backup: ●
Cycle: Backup by day
Time: 15 : 00 : 00

Step 3 Click Manual Backup.

The system pops up the interface of **Set Backup File Password**

Step 4 Enter file password, click **OK**.

- File password, used to guarantee backup data file security, you need to enter password for verification if you want to open or restore backup file.
- Backup file is stored under server installation path, which is "..\Server\WEBCLIENT\webclient\apache-tomcat\tmp\systemBackup".

4.1.2 Restore

You can restore the system and data back to the latest backup time during database exception. The system can be quickly recovered and lower user loss.

⚠

Other users cannot operate the system when restoring the database. The data information will change after being restored, please operate with care.

4.1.2.1 Restoring Local File

Local file restoration is to restore manually backup file to server.

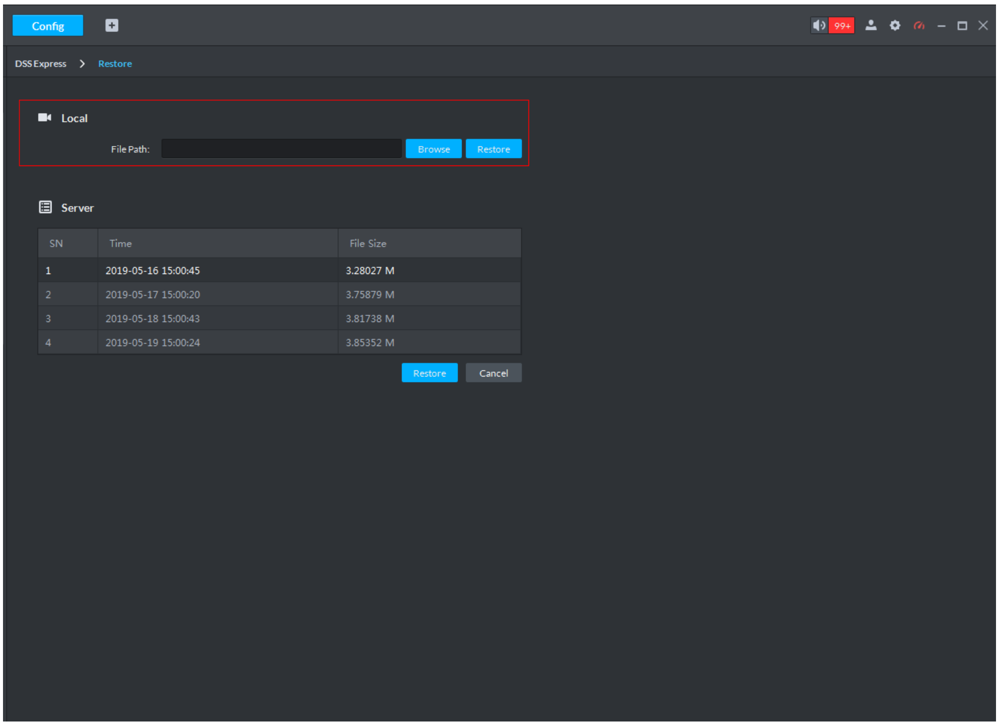
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Restore**.

The system displays **Restore** interface, see Figure 4-4.

Figure 4-4 Local


Config
DSS Express
Restore
Local
File Path:
Browse
Restore
Server
Restore
Cancel

SN	Time	File Size
1	2019-05-16 15:00:45	3.28027 M
2	2019-05-17 15:00:20	3.75879 M
3	2019-05-18 15:00:43	3.81738 M
4	2019-05-19 15:00:24	3.85352 M

Step 3 Click **Browse** and select backup data file.

Step 4 Click Restore.

The system pops out **Restore** box.

Step 5 Enter administrator login password and file password, click **OK**.

The system displays restoration progress, and the system will prompt restored successfully on the lower right corner.

4.1.2.2 Restoring Server File

Restore data from backup file of server, the backup file on server is automatically backed up from system.

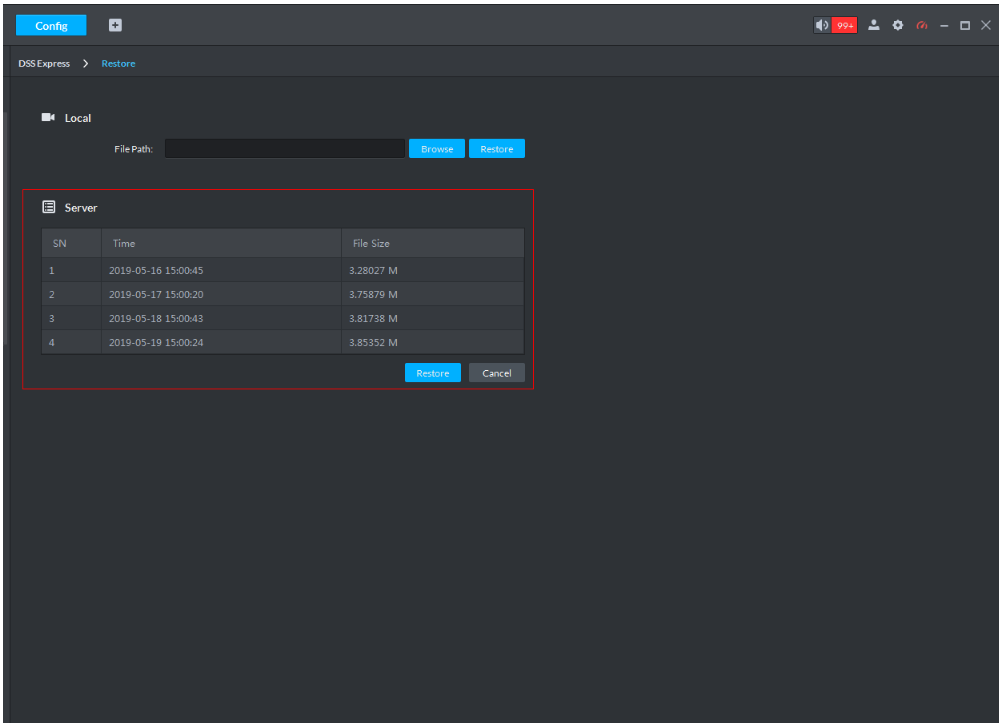
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Restore**.

The system displays **Restore** interface, see Figure 4-5.

Figure 4-5 Restore server file



SN	Time	File Size
1	2019-05-16 15:00:45	3.28027 M
2	2019-05-17 15:00:20	3.75879 M
3	2019-05-18 15:00:43	3.81738 M
4	2019-05-19 15:00:24	3.85352 M

Step 3 Select backup file from server, click **Restore**.

The system pops out prompt box.

Step 4 Enter administrator login password and file password, click **OK**.

The system displays restoration progress; the system will prompt restored successfully on lower right corner.

4.2 Update

If the platform version is too low, you can install new software version and update. Please make sure you have acquired the new program, otherwise, please contact technical support for it.

- Program name includes version number and date, please check before installation.
- Update will not cause data and configuration loss.
- If you modify SC service port of platform before update, when the program is updated to version 1.000.0000003, SC service port will be reset to default. Please modify port number after update is completed, make sure the the port number of platform is in accordance with that of the device.

Double-click installation program, install according to system prompt. For more installation requirement, please see “2.2 Installing Program (Update).”

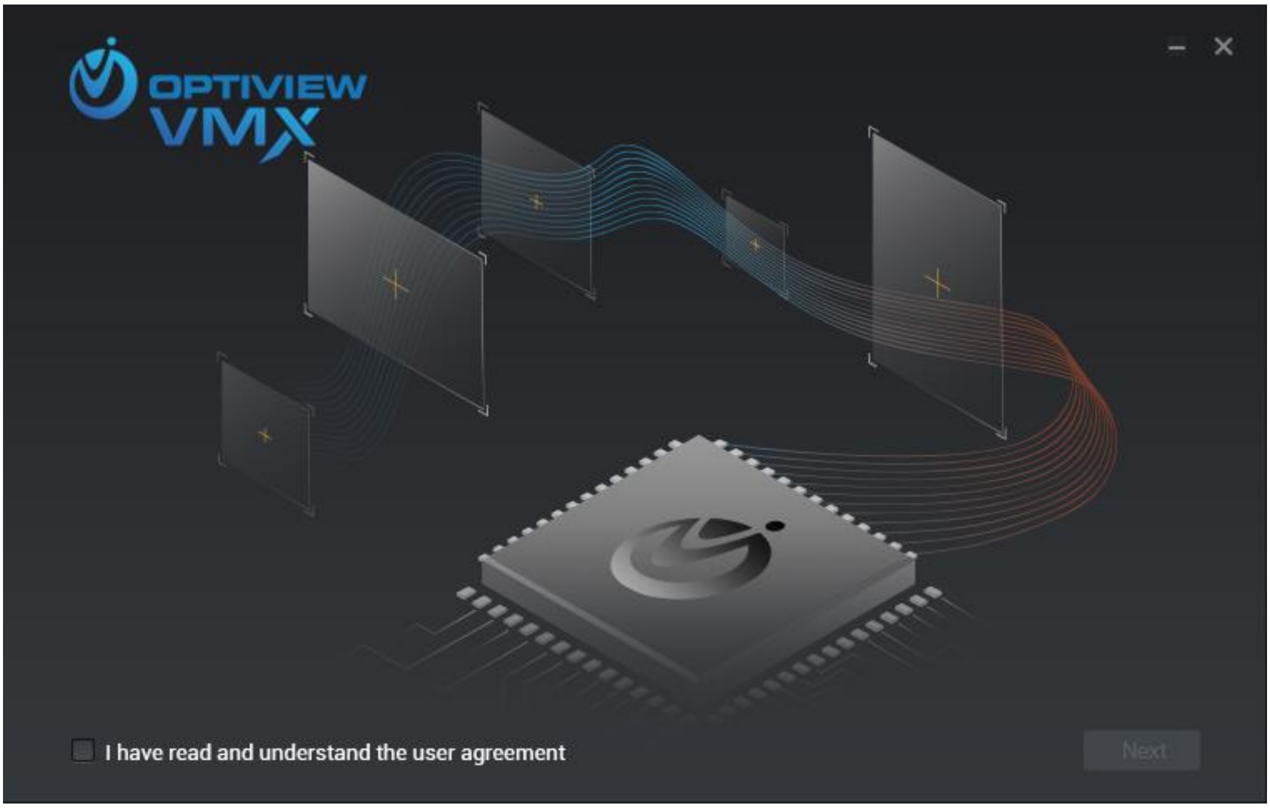
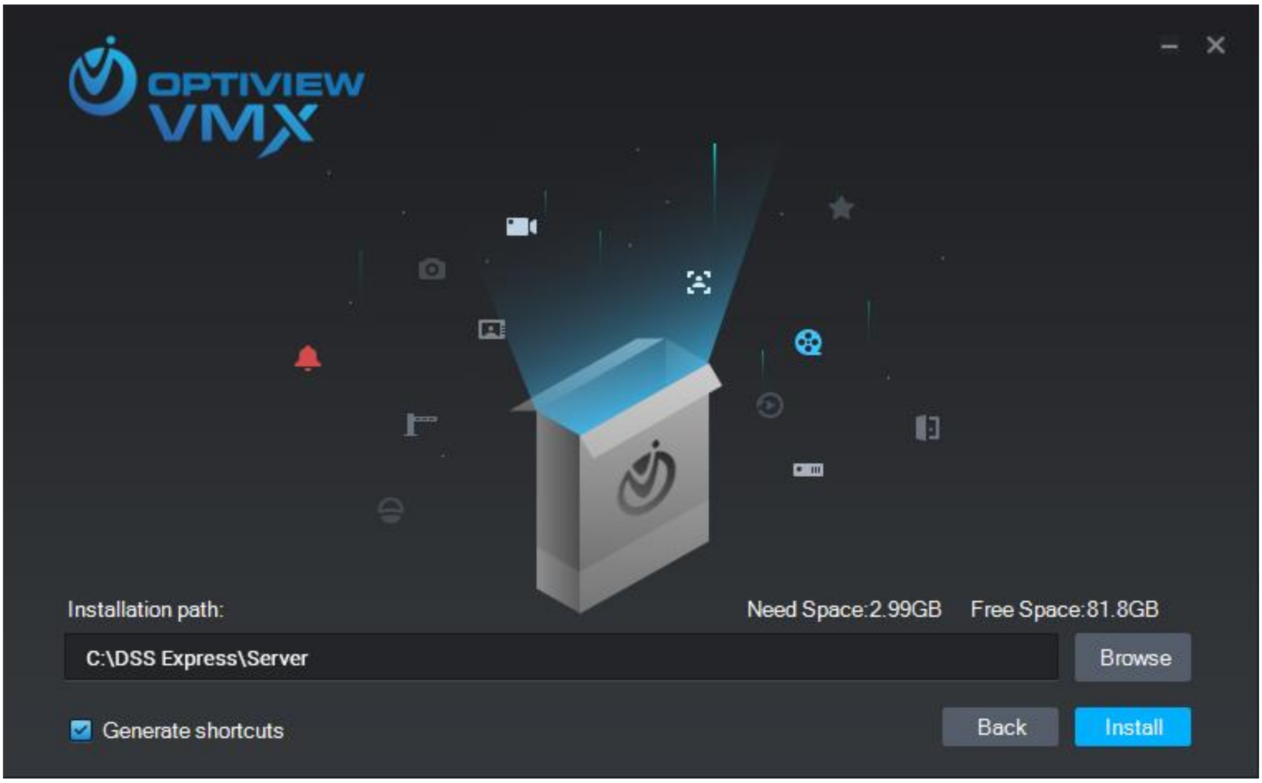

OPTIVIEW VMX
☐ I have read and understand the user agreement
Next

Figure 4-6 Confirm agreement

Step 1 Select I have read and agree the OPTIVIEW VMX agreement, click Next. The installation path interface is displayed. See Figure 4-7.

Figure 4-7 Select installation path


OPTIVIEW VMX
Browse
Back
Install

Installation path:

Need Space:2.99GB Free Space:81.8GB

C:\DSS Express\Server

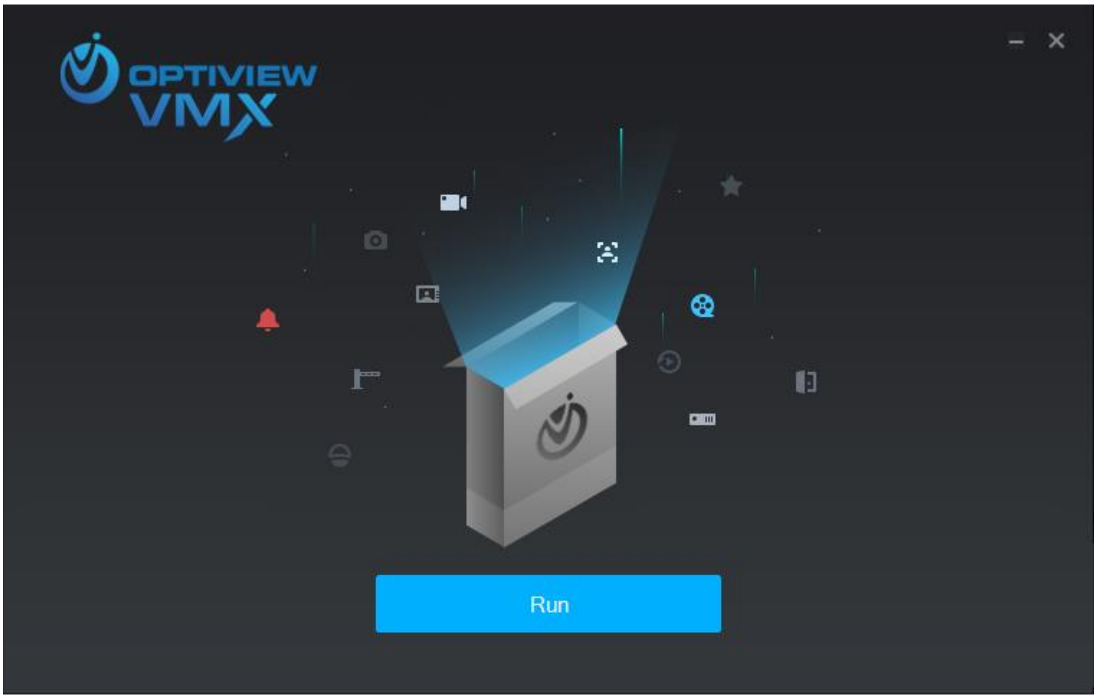
☑ Generate shortcuts

Step 2 Click **Browse** and select installation path, click **Install**.

The system displays installation progress, the whole installation needs 5-10 minutes. See Figure 4-8 after installation is completed. The server starts automatically after installation.

- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** beomes gray, and installation cannot be implemented.
- Do not select **Generate Shortcuts** if it is not necessary.
- If port conflict exists, the system will prompt conflicted port during installation. Open Optiview VMX Server and modify port after installation is completed. See **2.3.2 Modifying Service Port** for more details.

Figure 4-8 Installation completed



4.3 Log

In log module, you can view operator log and access control device log.

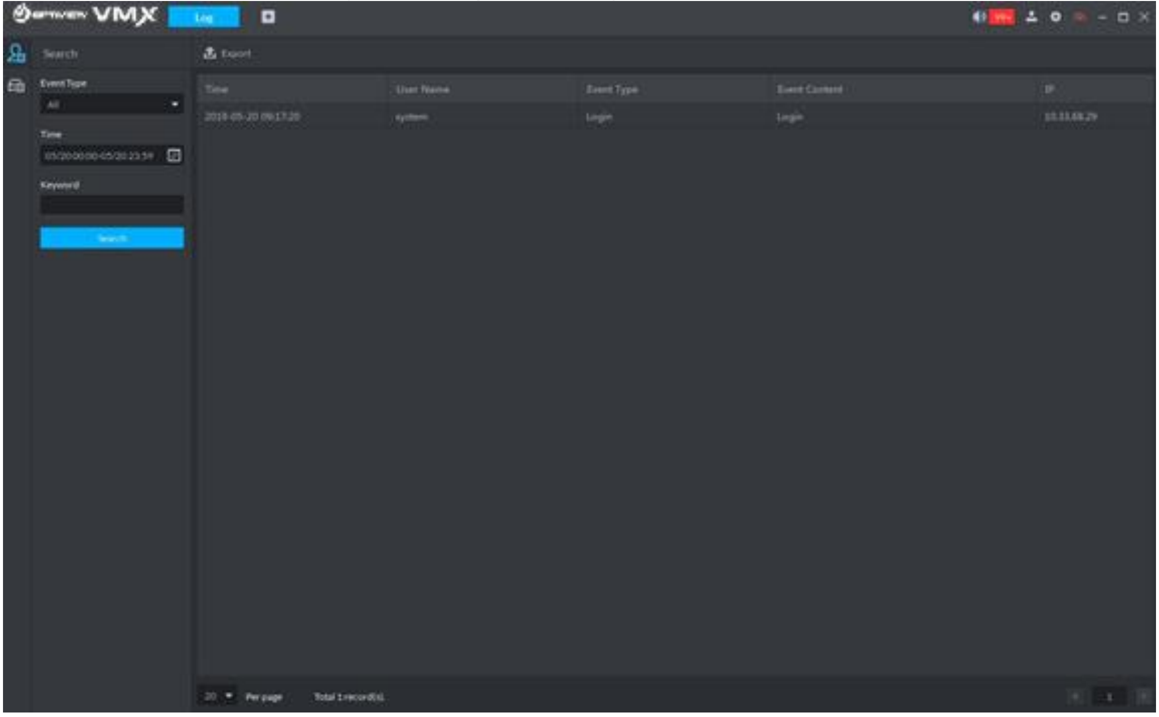
Step 1 On client homepage, click **Log**.

The system displays **Log** interface.

Step 2 Click 👤.

The system displays **Operator Log** interface, see Figure 4-9.

Figure 4-9 Operation log


VMX
Log
Search
Event Type
All
Time
Keyword
Search
Export
Time
User Name
Event Type
Event Content
IP
Per page

Step 3 Select event typetime and enter keyword, click **Search**.

The system displays results.

4.4 Password Maintenance

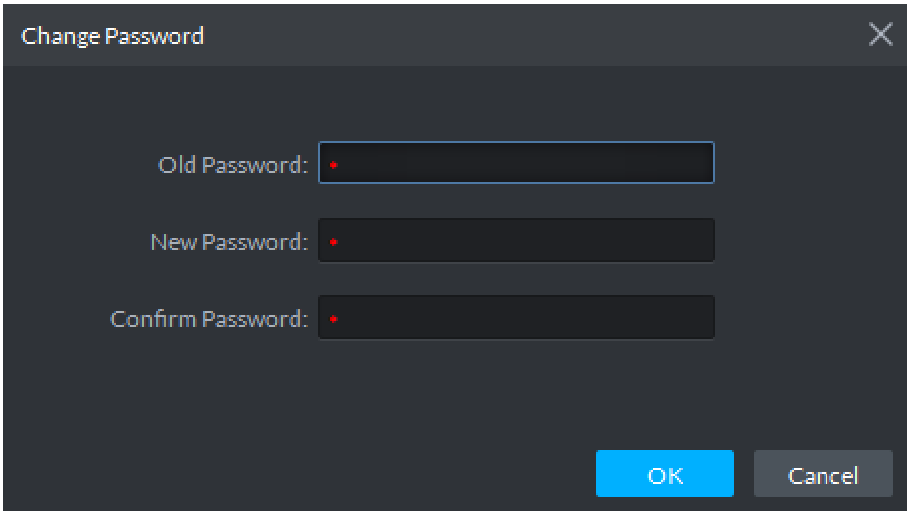
4.4.1 Changing Password

To make sure the account is safe, you are recommended to change login password regularly.

Step 1 After logging in client, click on top right corner of the interface, select **Change Password**.

The system displays **Change Password** interface, see Figure 4-10.

Figure 4-10 Change password


Change Password
Old Password:
New Password:
Confirm Password:
OK
Cancel

Step 2 Enter Old Password, New Password and Confirm Password, click **OK**.

4.4.2 Resetting Password

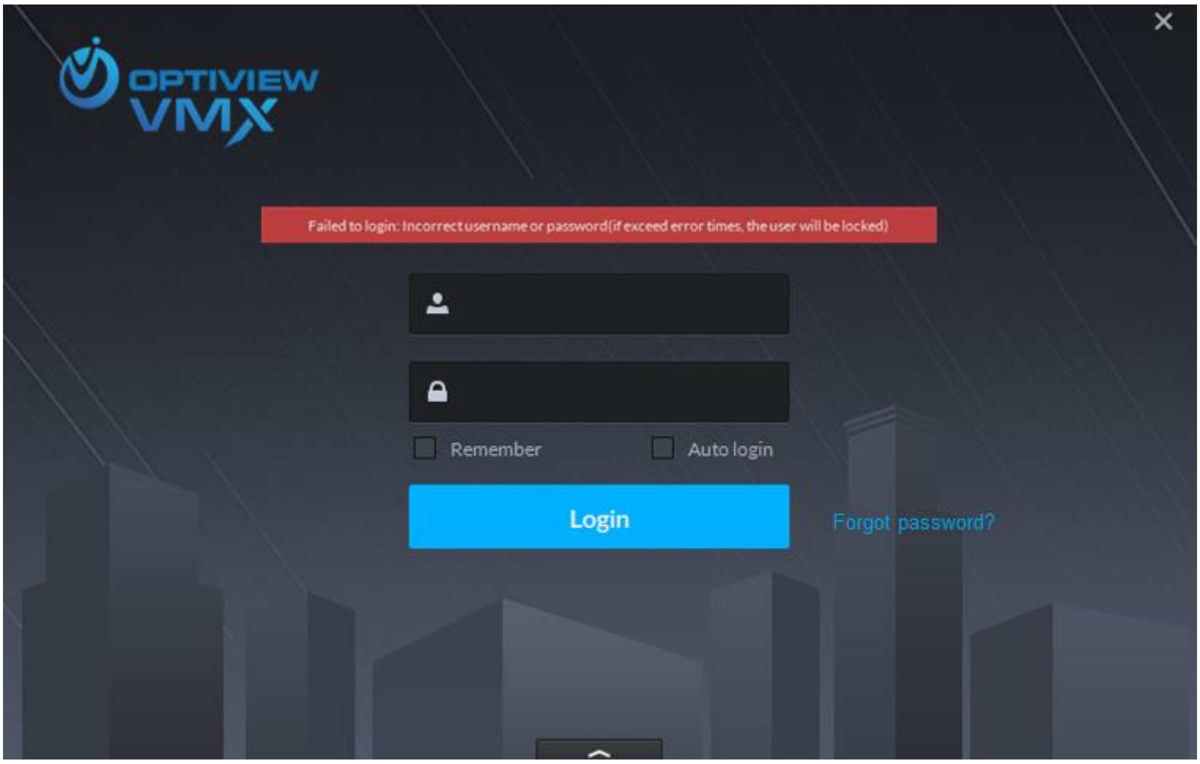
When users forget password, you can reset a new password.

System User Password Reset

When system user forgets password, you can reset password by answering security question.

Step 1 Users forget password when logging in client, enter wrong password to log in client. The login interface displays **Forget Password**, see Figure 4-11.

Figure 4-11 Forget password

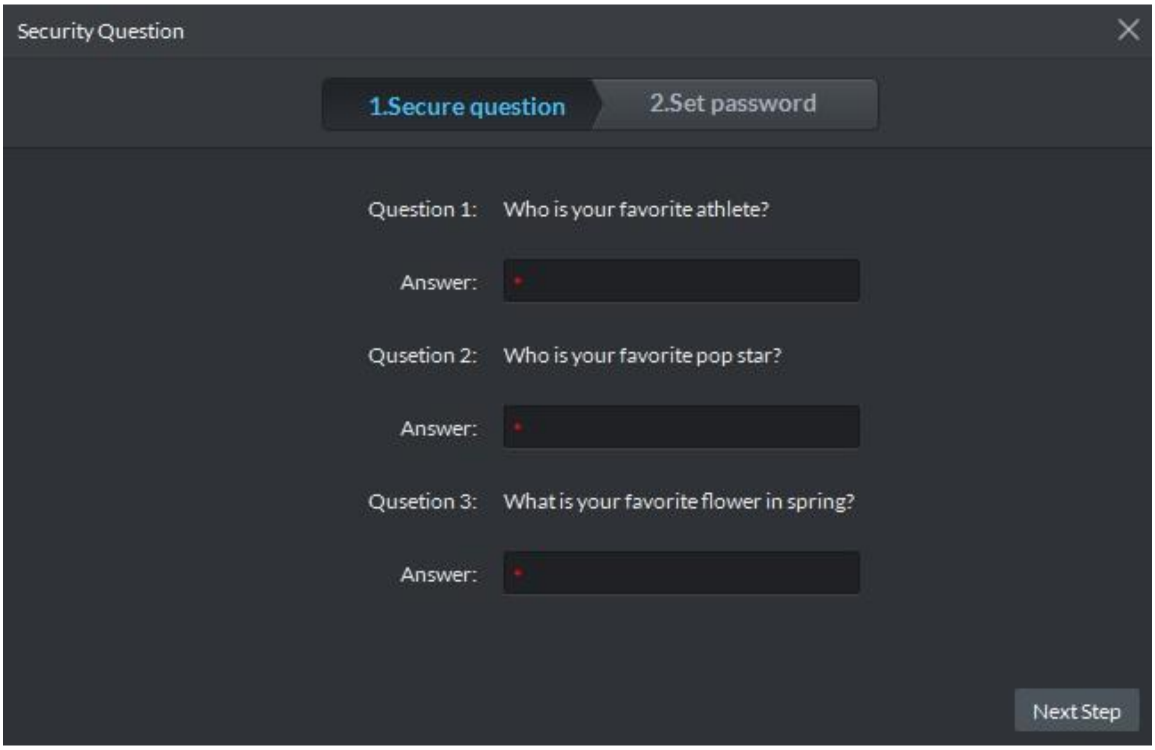


Failed to login: Incorrect username or password(if exceed error times, the user will be locked)

Step 2 Click Forget Password.

The system displays **Security Question** interface, see Figure 4-12.

Figure 4-12 Security question


Security Question

1.Secure question
2.Set password

Question 1: Who is your favorite athlete?

Answer: *

Qusetion 2: Who is your favorite pop star?

Answer: *

Qusetion 3: What is your favorite flower in spring?

Answer: *

Next Step

Step 3 Enter answers to three questions, click **Next Step**.

The system displays **Set Password** interface.

Step 4 Enter new password, click **OK** and password is reset.

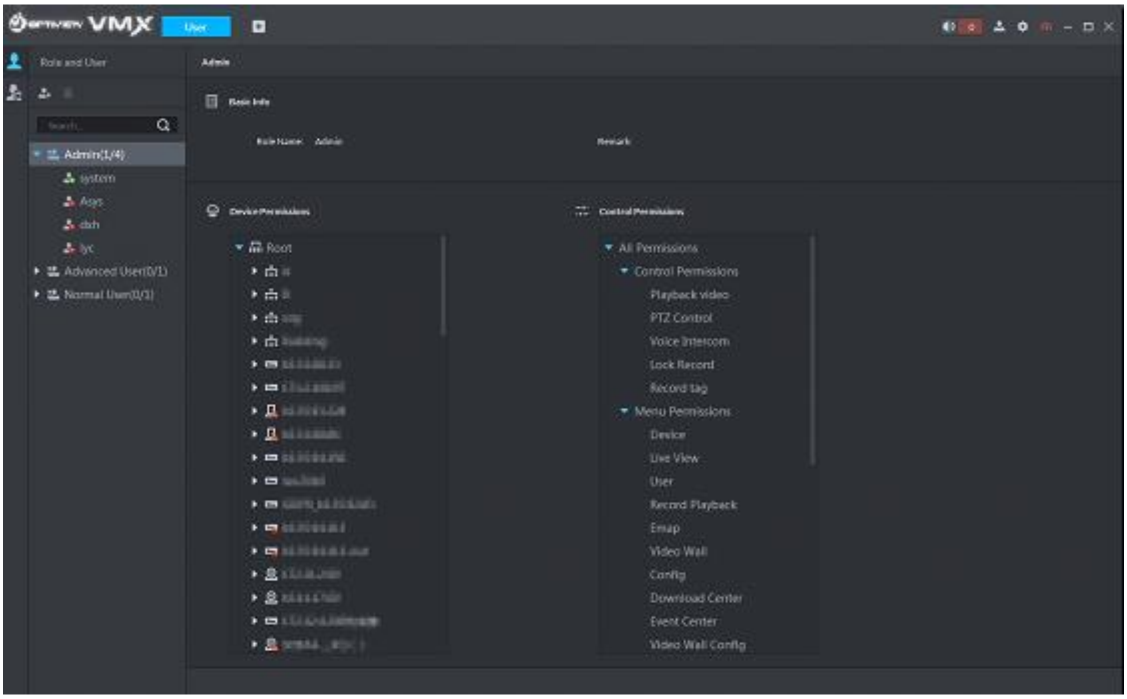
Non-system User Password Reset

When non-system user forgets password, you can only let system user set new password.

Step 1 On client homepage, click **User**.

The system displays **User** interface, see Figure 4-13.

Figure 4-13 User

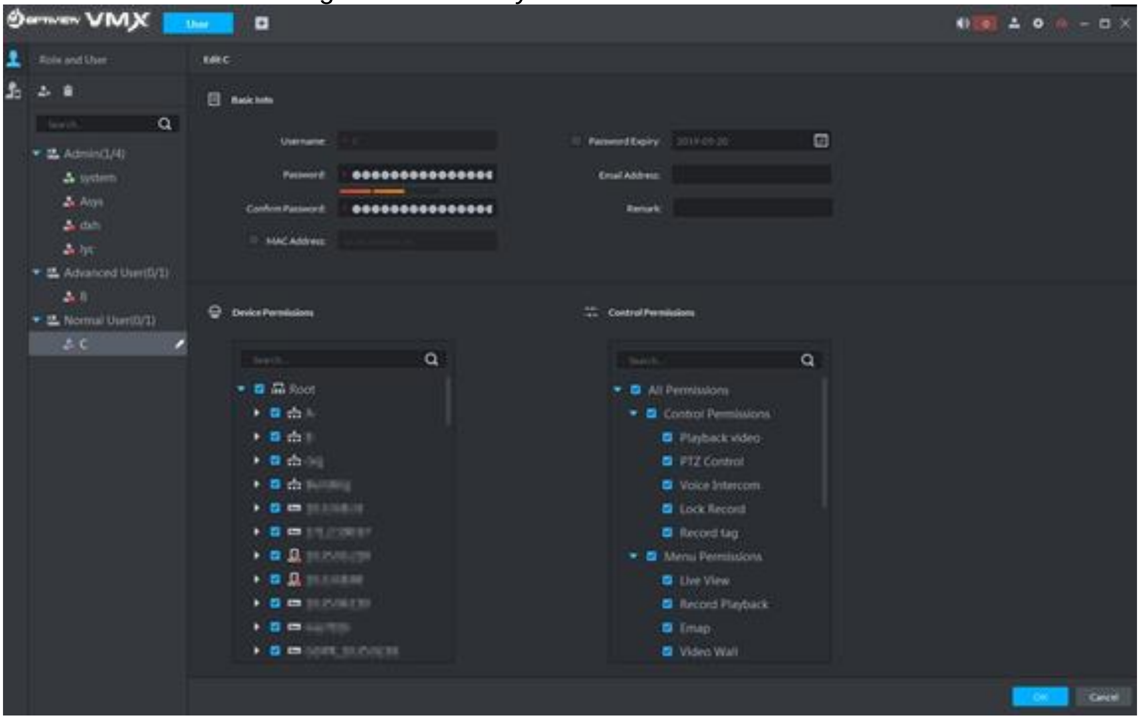

VMX
User
Role and User
Search...
Admin(1/4)
system
Asys
dxh
lyc
Advanced User(0/1)
Normal User(0/1)
Admin
Basic Info
Remark
Device Permissions
Root
Control Permissions
All Permissions
Control Permissions
Playback video
PTZ Control
Voice Intercom
Lock Record
Record tag
Menu Permissions
Device
Live View
User
Record Playback
Emap
Video Wall
Config
Download Center
Event Center
Video Wall Config

Role Name: Admin

Step 2 Select the user you want to reset password, click ✎.

The system displays the interface of modifying user info, see Figure 4-14.

Figure 4-14 Modify user info


VMX
User
Role and User
Edit C
Basic Info
Username:
Password:
Confirm Password:
MAC Address:
Password Expiry
Email Address:
Remark:
Admin(1/4)
system
Anys
dxh
lyt
Advanced User(0/1)
B
Normal User(0/1)
C
Device Permissions
Root
Control Permissions
All Permissions
Control Permissions
Playback video
PTZ Control
Voice Intercom
Lock Record
Record tag
Menu Permissions
Live View
Record Playback
Emap
Video Wall
OK
Cancel

Step 3 Enter password and confirm password, click **OK** and password is changed.

Appendix 1 Service Module Introduction

Service Name	**Function Description**	**Port**	**Protocol Type**
OPTIVIEW VMX_WEB (Center Management Service)	Center management service is to manage each service and provide accessing port.	H HTTP: 80 HTTPS: 443 CMS: 9000	TCP
OPTIVIEW VMX_MQ (Message Queue Service)	Message queue service is to transfer messages between the platforms.	61616	TCP
OPTIVIEW VMX_DMS (Device Management Service)	Device management service is to register front-end encoder, receive alarm, transfer alarm and send out sync time command.	9200	TCP
OPTIVIEW VMX_MTS (Media Transmission Service)	Media transmission service is to get the audio/video bit stream from the front-end device and then transfer these data to the SS, client and decoder.	9100	TCP
OPTIVIEW VMX_SS (Storage Service)	Storage service is to storage/search/playback record.	9320	TCP
OPTIVIEW VMX_VMS (Video Matrix Service)	Video matrix service is to login the the decoder and send out task to the decoder to output to the TV wall.	Not fixed, do not need to be mapped to the outside.	TCP
OPTIVIEW VMX_MGW (Media Gateway Service)	Media gateway service is to send out MTS service to the decoder.	9090	TCP
OPTIVIEW VMX_PCPS (ProxyList control Proxy Service)	Login Onvif device and then get the stream and transfer the data to MTS.	SIP: 5060 REGISTER: 9550	UDP TCP
OPTIVIEW VMX_ADS (Alarm Dispatch Service)	Alarm dispatch service is to send out alarm information to different objects according to the plans.	9600	TCP

OPTIVIEW VMX_SOSO (Device Search Service)	Search devices by adding IP address	12366	TCP

OPTIVIEW VMX_SC (Video Intercom Service)	Video intercom SIP service	SIP：5080 RTP：554	TCP
OPTIVIEW VMX_MCDDOOR (Access Control Service)	Access control device accessed to service, interacted with access control device.	Not fixed, do not need to be mapped to the outside.	TCP

Appendix 2 Shortcut Key List

Function	**Shortcut Key**	**Function**	**Shortcut Key**
Wnd Move up	Up	Snap Single Wnd	P
Wnd Move down	Down	Snap pic	Ctrl+P
Wnd Move Left	Left	Local Record	Ctrl+R
Wnd Move Right	Right	Lock	Ctrl+L
Aperture-	Insert	PreSet1	1
Aperture+	Delete	PreSet2	2
Focus-	Home	PreSet3	3
Focus+	End	PreSet4	4
Wiper	PgUp	PreSet5	5
Light	PgDn	PreSet6	6
Open Single Wnd	L	PreSet7	7
Close Single Wnd	L	PreSet8	8
Open Full Screen	Ctrl+F	PreSet9	9
Close Full Screen	ESC	PreSet10	10

Appendix 3 Deleting Videos on Central Server

If you want to delete 1000001$0 record period[2018-07-08 10:00:00   2018-07-08 10:30:00], do the following steps.

Step 1 Log in central server.

Step 2 Enter...\Optiview VMX\Server\SS directory, drag **./CQFSTools.exe list** file to cmd input window, find disk uuid.

The disk info is displayed as follows:

```
[[Disk List]]
[Disk Path]     [Target (Size) (Portal) (slot)]
D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd
D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd (10.00GB) () (-1)
11:32:57.355 TID 584188 [INFO] cmd[cmd.exe /c "getmac /FO
list >cqfs_tmp_584188.txt.tmp & type cqfs_tmp_584188.txt.tmp >cqf
[[CQFS List]]
[Disk Path]     [CQFS UUID (Service Type) (Allocation Type)]
D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd
{1bdb9a6e-41a6-4058-87ef-d944f630edf1} (1) (0)
```

Step 3 Search stream ID.

Use tool to connect to platform database, and implement the following SQL, the searched ID field is stream ID.

```
SELECT ID FROM adm_record_stream where DEVICE_CODE= device No. and
CHANNEL_SEQ = channel No.
```

Step 4 Implement the command of deleClip.

```
./CQFSTools.exe deleteClip <streamID> <beginTS> <endTS> <diskUUID>
```

Appendix 4 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Regularly**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer’s IP address and the accompanying equipment’s IP address to the whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

    If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.