



iVMS-4200 Client Software

User Manual

Legal Information

User Manual

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Please use this user manual under the guidance of professionals.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

Port List

For more details about port list, enter Hikvision official website.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Introduction	1
Chapter 2 Service Management	2
Chapter 3 Device Management	3
3.1 Activate Devices	3
3.2 Add Device	4
3.2.1 Add Online Device	4
3.2.2 Add Device by IP Address or Domain Name	7
3.2.3 Add Devices by IP Segment	9
3.2.4 Add Device by Cloud P2P	11
3.2.5 Add Device by EHome Account	13
3.2.6 Add Device by HiDDNS	14
3.2.7 Import Devices in a Batch	15
3.3 Edit Device's Network Information	17
3.4 Restore/Reset Device Password	18
3.4.1 Reset Device Password	18
3.4.2 Restore Device's Default Password	19
3.5 Check Device's QR Code	20
3.6 Upgrade Device Firmware Version	21
Chapter 4 Group Management	24
4.1 Add Group	24
4.2 Import Resources to Group	24
4.3 Edit Resource Parameters	25
4.4 Remove Resources from Group	26
Chapter 5 Cloud P2P	27
5.1 Register a Cloud P2P Account	27
5.2 Log into Cloud P2P Account	28

Chapter 6 Live View	29
6.1 Start Live View	29
6.1.1 Start Live View for One Camera	29
6.1.2 Start Live View for Camera Group	30
6.1.3 Add Custom View	31
6.1.4 Start Live View in Custom View Mode	31
6.2 Auto-Switch in Live View	32
6.2.1 Auto-Switch All Cameras	32
6.2.2 Auto-Switch Cameras in a Group	32
6.2.3 Auto-Switch Custom Views	33
6.3 PTZ Control	34
6.3.1 Configure Preset	36
6.3.2 Configure Patrol	37
6.3.3 Configure Pattern	38
6.4 Customize Window Division	38
6.5 Manually Record and Capture	39
6.5.1 Manually Record Video	39
6.5.2 View Local Videos	40
6.5.3 Capture Pictures	40
6.5.4 View Captured Pictures	41
6.6 Instant Playback	41
6.7 Live View for Fisheye Camera	42
6.7.1 Perform Live View in Fisheye Mode	42
6.7.2 PTZ Control in Fisheye Mode	43
6.8 Perform Master-Slave Linkage	47
6.8.1 Configure Master-Slave Tracking Rule	47
6.8.2 Enable Master-Slave Tracking	49
6.9 Live View for Thermal Camera	49

6.9.1 View Fire Source Information during Live View	49
6.9.2 Show Temperature Information on Live View Image	50
6.9.3 Manually Measure Temperature	51
6.10 Live View in Low Bandwidth	52
6.11 More Functions	52
Chapter 7 Remote Storage Configuration	54
7.1 Store Picture and Video on DVR, NVR, or Network Camera	54
7.2 Store Video on Storage Device	56
7.2.1 Activate Storage Server	56
7.2.2 Add Storage Server to Client	57
7.2.3 Format Storage Server's HDD	57
7.2.4 Configure Storage Settings	57
7.3 Store Picture and Additional Information on Local PC	58
7.4 Configure Recording Schedule Template	58
7.5 Configure Capture Schedule Template	60
Chapter 8 Remote Playback	61
8.1 Normal Playback	61
8.1.1 Search Video Files	62
8.1.2 Play Video Files	62
8.2 Alarm Input Playback	63
8.2.1 Search Video Files	63
8.2.2 Play Video Files	64
8.3 Event Playback	64
8.3.1 Search Video Files	65
8.3.2 Play Video Files	65
8.4 ATM Playback	66
8.4.1 Search Video Files	66
8.4.2 Play Video Files	66

8.5 POS Playback	67
8.5.1 Search Video Files	67
8.5.2 Play Video Files	68
8.6 VCA Playback	68
8.7 Synchronous Playback	70
8.8 Fisheye Playback	70
8.9 Playback in Low Bandwidth	71
Chapter 9 Download Video Footage	72
9.1 Download Video Footage by Date	72
9.2 Download for Multiple Cameras	72
Chapter 10 Configure Video Event	74
Chapter 11 Event Center	76
11.1 Enable Receiving Events from Devices	76
11.2 View Real-Time Events	77
11.3 Search Historical Events	78
11.4 View Pop-up Alarm Information	81
Chapter 12 Map Management	83
12.1 Add Map	83
12.2 Edit Map Scale	84
12.3 Manage Hot Spot	84
12.3.1 Add Camera as Hot Spot	85
12.3.2 Add Alarm Input as Hot Spot	86
12.3.3 Add Alarm Output as Hot Spot	87
12.3.4 Add Zone as Hot Spot	89
12.3.5 Add Security Radar as Hot Spot	91
12.3.6 Add Access Point as Hot Spot	93
12.3.7 Edit Hot Spot	95
12.3.8 Preview Hot Spot	95

12.4 Manage Hot Region	98
12.4.1 Add Hot Region	98
12.4.2 Edit Hot Region	99
12.4.3 Preview Hot Region	99
Chapter 13 Forward Video Stream through Stream Media Server	101
13.1 Import Certificate to Stream Media Server	101
13.2 Add Stream Media Server by IP Address	102
13.3 Add Cameras to Stream Media Server to Forward Video Stream	102
Chapter 14 Statistics	104
14.1 People Counting Report	104
14.2 View People Counting in Intersections Report	107
14.3 Queue Management	108
14.3.1 Queuing-Up Time Analysis	108
14.3.2 Queue Status Analysis	111
14.4 Heat Map Report	114
Chapter 15 Data Retrieval	116
15.1 Face Picture Retrieval	116
15.1.1 Search Face Picture by Uploaded Picture	116
15.1.2 Search Face Picture by Event	118
15.1.3 Search Face Picture by Person Name	120
15.2 Human Body Picture Retrieval	122
15.3 View Behavior Analysis Related Pictures and Videos	125
15.4 Vehicle Retrieval	125
15.5 Hard Hat Retrieval	127
15.6 Frequently Appeared Person Retrieval	128
Chapter 16 AI Dashboard	130
16.1 Face Application	130
16.1.1 Set List Types for Face Picture Libraries	130

16.1.2 Set Cameras for Showing AI Information	131
16.1.3 Show AI Information	131
16.2 Linked Capture Alarm	132
16.2.1 Set Basic Parameters	133
16.2.2 View Live View and Alarms	133
Chapter 17 Security Control Panel	135
17.1 Configure Client Linkage for Zone Event	135
17.2 Remotely Control Security Control Panel	136
17.2.1 Remotely Control Partitions	137
17.2.2 Remotely Control Zones	138
17.2.3 Remotely Control Relay	139
Chapter 18 Person Management	140
18.1 Add Organization	140
18.2 Add Single Person	140
18.2.1 Configure Basic Information	141
18.2.2 Issue a Card to One Person	141
18.2.3 Upload a Face Photo from Local PC	142
18.2.4 Take a Photo via Client	143
18.2.5 Collect Face via Access Control Device	144
18.2.6 Collect Fingerprint via Client	144
18.2.7 Collect Fingerprint via Access Control Device	145
18.2.8 Configure Access Control Information	146
18.2.9 Customize Person Information	147
18.2.10 Configure Resident Information	147
18.2.11 Configure Additional Information	148
18.3 Import and Export Person Identify Information	148
18.3.1 Import Person Information	148
18.3.2 Import Person Pictures	149

18.3.3 Export Person Information	150
18.3.4 Export Person Pictures	150
18.4 Get Person Information from Access Control Device	151
18.5 Move Persons to Another Organization	151
18.6 Issue Cards to Persons in Batch	152
18.7 Report Card Loss	152
18.8 Set Card Issuing Parameters	153
Chapter 19 Access Control	154
19.1 Configure Schedule and Template	154
19.1.1 Add Holiday	154
19.1.2 Add Template	155
19.2 Set Access Group to Assign Access Authorization to Persons	156
19.3 Configure Advanced Functions	157
19.3.1 Configure Device Parameters	158
19.3.2 Configure Remaining Open/Closed	165
19.3.3 Configure Multi-Factor Authentication	166
19.3.4 Configure Custom Wiegand Rule	168
19.3.5 Configure Card Reader Authentication Mode and Schedule	170
19.3.6 Configure Person Authentication Mode	172
19.3.7 Configure Relay for Elevator Controller	173
19.3.8 Configure First Person In	176
19.3.9 Configure Anti-Passback	177
19.3.10 Configure Multi-door Interlocking	178
19.4 Configure Other Parameters	179
19.4.1 Set Multiple NIC Parameters	179
19.4.2 Set Network Parameters	180
19.4.3 Set Device Capture Parameters	181
19.4.4 Set Parameters for Face Recognition Terminal	183

19.4.5 Enable M1 Card Encryption	184
19.4.6 Set RS-485 Parameters	184
19.4.7 Set Wiegand Parameters	185
19.4.8 Set Attendance Status	185
19.5 Configure Linkage Actions for Access Control	189
19.5.1 Configure Client Actions for Access Event	189
19.5.2 Configure Device Actions for Access Event	190
19.5.3 Configure Device Actions for Card Swiping	192
19.5.4 Configure Device Linkage for Mobile Terminal's MAC Address	193
19.5.5 Configure Device Actions for Person ID	194
19.6 Door/Elevator Control	196
19.6.1 Control Door Status	196
19.6.2 Control Elevator Status	197
19.6.3 Check Real-Time Access Records	198
Chapter 20 Time and Attendance	199
20.1 Configure Attendance Parameters	199
20.1.1 Configure General Rule	199
20.1.2 Configure Overtime Parameters	199
20.1.3 Configure Attendance Check Point	200
20.1.4 Configure Holiday	200
20.1.5 Configure Leave Type	202
20.1.6 Synchronize Authentication Record to Third-Party Database	202
20.1.7 Configure Break Time	203
20.1.8 Configure Attendance Calculation Accuracy	204
20.1.9 Configure Report Display	204
20.2 Add Timetable	205
20.3 Add Shift	207
20.4 Manage Shift Schedule	209

20.4.1 Set Department Schedule	209
20.4.2 Set Person Schedule	210
20.4.3 Set Temporary Schedule	211
20.4.4 Check Shift Schedule	212
20.5 Manually Correct Check-in/out Record	212
20.6 Add Leave and Business Trip	213
20.7 Calculate Attendance Data	214
20.7.1 Automatically Calculate Attendance Data	214
20.7.2 Manually Calculate Attendance Data	215
20.8 Attendance Statistics	215
20.8.1 Get Original Attendance Record	215
20.8.2 Generate Instant Report	216
20.8.3 Custom Attendance Report	217
Chapter 21 Video Intercom	219
21.1 Manage Calls between Client Software and an Indoor/Door Station/Access Control Device	219
21.1.1 Call Indoor Station from Client	219
21.1.2 Answer Call via Client	221
21.2 View Real-Time Call Logs	222
21.3 Release a Notice to Resident	223
Chapter 22 Log Search	224
Chapter 23 User Management	225
23.1 Add User	225
23.2 Change User's Password	226
Chapter 24 System Configuration	227
24.1 Set General Parameters	227
24.2 Set Live View and Playback Parameters	228
24.3 Set Image Parameters	229

24.4 Set Picture Storage	230
24.5 Set Alarm Sound	231
24.6 Set Access Control and Video Intercom Parameters	231
24.7 Set File Saving Path	232
24.8 Set Icons Shown on Toolbar	232
24.9 Set Keyboard and Joystick Shortcuts	233
24.10 Set Email Parameters	234
24.11 Manage Security Authentication	235
24.11.1 Export Certificate from Service Management	235
24.11.2 Import Certificate to Client	235
24.11.3 Certificate Verification for Transmission Encryption	236
Chapter 25 Operation and Maintenance	237
Appendix A. Custom Wiegand Rule Descriptions	238
Appendix B. Troubleshooting	240
B.1 Failed to get the live view of a certain device.	240
B.2 Local recording and remote recording are confused.	240
B.3 Failed to download the video files or the downloading speed is too slow.	240
Appendix C. FAQ (Frequently Asked Questions)	242
C.1 During live view, why an error message with error code 91 prompts ?	242
C.2 During live view, why the image is blurred or not fluent?	242
C.3 Why the memory leaked and the client crashed after running for a while?	242
C.4 During live view, when getting stream via the Stream Media Server, why an error message with error code 17 prompts?	243
C.5 How to get better performance of live view and playback when network bandwidth is low?	243
Appendix D. Error Code	245

Chapter 1 Introduction

iVMS-4200 Client Software is a versatile security management software for the DVRs, NVRs, IP cameras, encoders, decoders, security control panels, video intercom devices, access control devices, etc.

The software provides multiple functionalities, including real-time live view, video recording, remote search and playback, file backup, alarm receiving, person management, access control, video intercom, security control, time & attendance, etc., for the connected devices to meet the needs of monitoring task. With the flexible distributed structure and easy-to-use operations, the client software is widely applied to the surveillance projects of medium or small scale.

This user manual describes the functions, configurations and operation steps of the client software. To ensure the properness of usage and stability of the software, refer to the contents below and read the manual carefully before installation and operation.


Chapter 2 Service Management

iVMS-4200 Service is mainly applicable for data storage, data management, and data calculation. With continuous running and processing, it can manage the data, such as event records and attendance records, received by the iVMS-4200 Client Software. iVMS-4200 Service also provides management for user permissions, devices, groups, logs, etc.

You can view the module running status and edit its ports, including HTTP port and EHome port. You need to restart the iVMS-4200 Service to take effect.

Check **Auto-Launch** to enable launching the iVMS-4200 Service automatically after the PC started up.

 **Note**

- The iVMS-4200 Service will not show after running it. Enter the system tray and click  to open the service window.
 - After closing the service window, the client will logout and return to the login page. You need to run the service and then login again.
 - The service and the client should be installed on the same PC.
-

Chapter 3 Device Management

You can manage devices on the client, including adding, editing, and deleting the devices. You can also perform operations such as checking device's online users and checking devices' QR codes.

3.1 Activate Devices

For some devices, you are required to create the password to activate them before they can be added to the software and work properly.

Before You Start

Make sure the device to activate is connected to the network and is in the same subnet with the PC running the client.

Steps



This function should be supported by the device.

1. Enter the Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.

The searched online devices are displayed in the list.

4. Check the device status (shown on **Security Level** column) and select an inactive device.

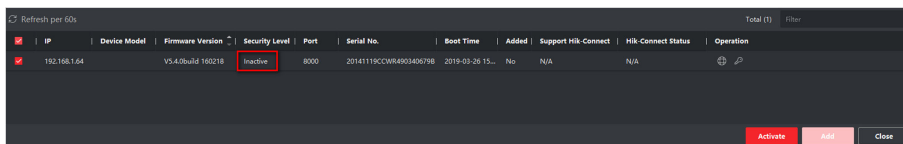


Figure 3-1 Online Inactive Device

5. Click **Activate** to open the Activation dialog.
 6. Create a password in the password field, and confirm the password.
-



The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

7. **Optional:** For the NVR device connecting with inactive network camera(s), create a password in **Network Cameras' Default Password** field and enter the confirm password for activating the network camera(s) via NVR.
8. **Optional:** Enable Cloud P2P service when activating the device if the device supports.
 - 1) Check **Enable Cloud P2P** to open the Note dialog.
 - 2) Create a verification code.
 - 3) Confirm the verification code.
 - 4) Click **Terms of Service** and **Privacy Policy** to read the requirements.
 - 5) Click **OK** to enable the Cloud P2P service.Go back to the Activate panel.
9. Click **OK** to activate the device.

3.2 Add Device

After launching the client, devices including network cameras, video encoders, DVRs, NVRs, access control devices, alarm devices, video intercom devices, etc., should be added to the client for the remote configuration and management, such as live view, playback, event management, access control, etc.

3.2.1 Add Online Device

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area. You can click **Refresh Every 60s** to refresh the information of the online devices.

Add an Online Device

You can add an online device to the client.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area.

The searched online devices are displayed in the list.
4. Select an online device from the **Online Device** area.

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to **Activate Devices** .

5. Click **Add** to open the device adding window.
6. Enter the required information.

Name

Enter a descriptive name for the device.

IP Address

Enter the device's IP address. The IP address of the device is obtained automatically in this adding mode.

Port

The port number of the device is obtained automatically in this adding mode.

User Name

By default, the user name is *admin*.

Password

Enter the device password.


**Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

7. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **Optional:** Check **Import to Group** to create a group by the device name.
9. Click **Add** to add the device.
10. **Optional:** Perform the following operation(s).


Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.


**Note**



For detail operation steps for the remote configuration, see the user manual of the device.

Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.

Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User	Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click  on Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click Delete to delete the selected device(s) from the client.

Add Multiple Online Devices

You can add multiple online devices to the client in a batch.

Before You Start

Make sure the to-be-added devices are online.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.

The searched online devices are displayed in the list.

4. Select multiple devices.



Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to **Activate Devices**.

5. Click **Add** to open the device adding window.
6. Enter the required information.

User Name

By default, the user name is **admin**.

Password

Enter the device password.




Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

7. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **Optional:** Check **Import to Group** to create a group by the device name.
9. Click **Add** to add the devices.
10. **Optional:** Perform the following operation(s).


Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.


 **Note**

For detail operation steps for the remote configuration, see the user manual of the device.


Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.


Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click  on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.2.2 Add Device by IP Address or Domain Name

When you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.
The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

Name

Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

Address

The IP address or domain name of the device.

Port

The devices to add share the same port number. The default value is **8000**.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device password.



Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

5. Optional: Add the offline devices.

- 1) Check **Add Offline Device**.
- 2) Enter the required information, including the device channel number and alarm input number.



Note

When the offline device comes online, the software will connect it automatically.

6. Optional: Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .



Note

- This function should be supported by the device.
 - If you have enabled Certificate Verification, you should click **Open Certificate Folder** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See **Certificate Verification for Transmission Encryption** for details about enabling certificate verification.
 - You can log into the device to get the certificate file by web browser.
-

7. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.

8. Optional: Check **Import to Group** to create a group by the device name.


9. Finish adding the device.

- Click **Add** to add the device and back to the device list page.

- Click **Add and New** to save the settings and continue to add other device.

10. Optional: Perform the following operation(s).


Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.


 **Note**

For detail operation steps for the remote configuration, see the user manual of the device.


Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.


Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click  on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.2.3 Add Devices by IP Segment

If the devices share the same port No., user name and password, and their IP addresses are sharing an IP segment. You can specify the start IP address and the end IP address, port No., user name, password, etc of the devices to add them to the client.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.

The added devices are displayed on the right panel.

3. Click **Add** to open the Add window.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

Start IP

Enter a start IP address.

End IP

Enter an end IP address in the same network segment with the start IP.

Port

Enter the device port No. The default value is **8000**.

User Name

By default, the user name is **admin**.

Password

Enter the device password.



Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

6. Optional: Add the offline devices.

- 1) Check **Add Offline Device**.
 - 2) Enter the required information, including the device channel number and alarm input number.
-



Note

When the offline device comes online, the software will connect it automatically.

7. Optional: Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .



Note

- This function should be supported by the device.
 - If you have enabled Certificate Verification, you should click **Open Certificate Folder** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See **Certificate Verification for Transmission Encryption** for details about enabling certificate verification.
 - You can log into the device to get the certificate file by web browser.
-

8. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.


9. Optional: Check **Import to Group** to create a group by the device name.

10. Finish adding the device.

- Click **Add** to add the device and back to the device list page.
- Click **Add and New** to save the settings and continue to add other device.

11. Optional: Perform the following operation(s).





Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.



Note

For detail operation steps for the remote configuration, see the user manual of the device.

Device Status	Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click  on Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click  on Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click Delete to delete the selected device(s) from the client.

3.2.4 Add Device by Cloud P2P

You can add the devices to the client via Cloud P2P domain.

Before You Start

Log in to Cloud P2P account first.

Steps

1. Enter Device Management module.
The added devices are displayed on the right panel.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window.
4. Select **Cloud P2P** as the adding mode.
 - If you log in for the first time, you will be required to log into the Cloud P2P account.
The logged-in Cloud P2P account is displayed.
5. Select a region to login in the drop-down list of **Select the Region to Login** and then log into the Cloud P2P account, or enter the device serial number.
 - Enter the serial number which you can find on the device label.
 - If the IP address of the device is in the same local subnet with the client, click **Online Device** and select an online device to get its serial number automatically.
6. Enter the verification code created when activating the device and enabling the Cloud P2P service.
7. **Optional:** Enable **DDNS** to access the device by Cloud P2P Domain.

Device Domain Name

Customize the device domain name, which is used to get the IP address and port of the device registered on Cloud P2P server.

UPnP Mode

Auto

Select **Auto** as the UPnP Mode to get the port number of the device automatically.

Manual

Select **Manual** as the UPnP Mode, and you need to input the port number of the device manually.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device password, which is created when you activate the device.



Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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



Note

If DDNS function is disabled, you cannot do some operations for the added device through client, such as viewing the device status, downloading the video files during remote playback, generating QR codes of devices, etc.

8. Optional: Check **Import to Group** to create a group by the device name.

9. Add device to the client software and Cloud P2P account.

- Click **Add** to add the device and return to the device list.
 - Click **Add and New** to add the device and continue to add the next device.
-




Note

If the client cannot connect the DDNS for three times, the device will be added by P2P.

10. Optional: Perform the following operation(s).


Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.

Note

For detail operation steps for the remote configuration, see the user manual of the device.

Edit Device Information

Click  to edit the device details.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.2.5 Add Device by EHome Account

For areas where devices using dynamic IP addresses instead of static ones, you can add access control device connected via EHome protocol by specifying the EHome account.

Before You Start

Set the network center parameter first. For details, refer to **Set Network Parameters** .

Steps

1. Enter Device Management module.
The added devices are displayed on the right panel.
2. Click **Add** to open the Add window.
3. Select **EHome** as the adding mode.
4. Enter the required information.

Device Account

Enter the account name registered on EHome protocol.

EHome Key

Enter the EHome key if you have set it when configuring network center parameter for the device.




Note

This function should be supported by the device.

5. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
6. **Optional:** Check **Import to Group** to create a group by the device name.
7. Finish adding the device.
 - Click **Add** to add the device and go back to the device list.
 - Click **Add and New** to save the settings and continue to add other device.
8. **Optional:** Perform the following operation(s).

Device Status

Click  on Operation column to view device status.

Edit Device Information	Click  on Operation column to edit the device information, such as device name, device account, and EHome key.
Check Online User	Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click  on Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click Delete to delete the selected device(s) from the client.

3.2.6 Add Device by HiDDNS

HiDDNS is a DNS server of Hikvision providing users free services. If you have no enough IP addresses for the devices, you can add device by HiDDNS to assign dynamic IP addresses to the devices for a good-quality connection to network.

Steps

1. Enter Device Management module.
The added devices are displayed on the right panel.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window.
4. Select **HiDDNS** as the adding mode.
5. Enter the required information.

Server Address

www.hik-online.com

Domain

Enter the device's domain name registered on HiDDNS server.

User Name

Enter the device user name.

Password

Enter the device password.



Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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


6. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
 7. **Optional:** Check **Import to Group** to create a group by the device name.
 8. **Optional:** Add the offline devices.
 - 1) Check **Add Offline Device**.
 - 2) Enter the required information, including the device channel number and alarm input number.
-

 **Note**

When the offline device comes online, the software will connect it automatically.

9. Finish adding the device.
 - Click **Add** to add the device and back to the device list page.
 - Click **Add and New** to save the settings and continue to add other device.
10. **Optional:** Perform the following operation(s).


Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.


 **Note**

For detail operation steps for the remote configuration, see the user manual of the device.


Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.


Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click  on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.2.7 Import Devices in a Batch

You can add multiple devices to the client in batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.

2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Adding Mode

Enter **0** or **1** or **2**. **0** refers to adding a device by IP address or domain name; **1** refers to adding a device by HiDDNS; **2** refers to adding a device by EHome protocol.

Address

Edit the address of the device. If you set IP/Domain as the adding mode, enter the IP address or domain name of the device here; if you set HiDDNS as the adding mode, enter **www.hik-online.com** here.



Note

If you set EHome as the adding mode, this parameter is not required.

Port

Enter the device port number. The default port number is **8000**.

Device Information

If you set IP/Domain as the adding mode, this parameter is not required; if you set HiDDNS as the adding mode, enter the device domain name registered on HiDDNS server; if you set EHome as the adding mode, enter the EHome account here.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device password.



Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

Add Offline Device

Enter **1** to enable adding an offline device, and then the software will automatically connect it when the device is online. Enter **0** to disable adding an offline device.

Import to Group


Enter **1** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter **0** to disable this function.

Channel Number


If you enable **Add Offline Device**, enter the channel number of the device. If you disable **Add Offline Device**, this field is not required.

Alarm Input Number

If you enable **Add Offline Device**, enter the alarm input number of the device. If you disable **Add Offline Device**, this field is not required.

- Click  and select the template file.
- Click **Add** to import the devices.
- Optional:** Perform the following operation(s).


Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.


Note

For detail operation steps for the remote configuration, see the user manual of the device.


Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.


Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click  on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.3 Edit Device's Network Information

After activating device, you can edit the network information (including IP address, port number, gateway, etc.) for the online device.


Before You Start

Activate the device if the device status is inactivated.

Steps

1. Enter Device Management page.

2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area.

All the online devices sharing the same subnet will be displayed in the list.
4. Select an activated device in **Online Device** area.
5. Click  on the Operation column to open the Modify Network Parameter window.

Note

This function is only available on the **Online Device** area.

6. **Optional:** Change the device IP address to the same subnet with your computer if you need to add the device to the client.
 - Edit the IP address manually.
 - Check **DHCP** to set the IP address as a static IP address.
7. Enter the password created when you activate the device.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

8. Click **OK** to complete the network settings.

3.4 Restore/Reset Device Password


If you forgot the password of the detected online devices, you can restore the device's default password or reset the device's password through the client.

3.4.1 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area.

All the online devices sharing the same subnet will be displayed in the list.
4. Select the device from the list and click  on the Operation column.

5. Reset the device password.

- Click **Export** to save the device file on your PC and then send the file to our technical support.



For the following operations for resetting the password, contact our technical support.

- Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.



For the following operations for resetting the password, contact our technical support.

- Select the Safe Mode according to actual needs.



For the following operations for resetting the password, contact our technical support.



The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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


3.4.2 Restore Device's Default Password

If you forget the password of the detected online devices, you can restore their default password via the client.

Steps

1. Enter Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.

All the online devices sharing the same subnet will be displayed in the list.

4. Select a device and click  on the Operation column to open the Reset Password window.
5. Restore the device password.
 - Enter the security code, and then you can restore the default password of the selected device.

Note

For getting the security code, contact our technical support.

- Click **Export** to save the device file on your PC and send the file to our technical support.

Note

For the following operations for resetting the password, contact our technical support.

What to do next

The default password (12345) for the admin account is for first-time login purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

3.5 Check Device's QR Code

The client can generate a QR code of the added device(s). You can add the device(s) to your mobile client after scanning the QR code.

Steps

Note

- Devices added via EHome protocol do not support this function.
 - Devices added via Cloud P2P with **DDNS** enabled do not support this function.
-

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.

The added devices are displayed in the list.

3. Select one or more device and click **QR Code** to open the QR Code window.

What to do next

Add the device to mobile client after scanning the QR code. For details, see user manual of the mobile client.

3.6 Upgrade Device Firmware Version

When there is a new firmware version available for the added device, you can upgrade its firmware version via the client.

 **Note**

- The device should support this function.
 - You can configure upgrading mode in System Configuration. See **Set General Parameters** for details.
-

Enter the Device Management module, and then click **Device** tab to show the device list.

Perform the following operations according to different upgrading modes.

Disable

On the Device for Management panel, if there is a new firmware version available, the status in the Firmware Upgrade column of the device will turn to **Upgradeable**.

Select the upgradeable device and click **Upgrade** to start upgrading the device firmware.

 **Note**

The upgrade progress will show. When the upgrade is completed, the status in the Firmware Upgrade column of the device will turn to **Upgraded**.

Prompt Me If Download and Upgrade

If there is a new firmware version available, a prompt window will pop up. Click **Upgrade All** to start downloading and upgrading.

Download and Prompt Me If Upgrade

A dialog will pop up for selecting whether to upgrade after downloading package of new version. Click **Upgrade All** to start upgrading the device firmware.

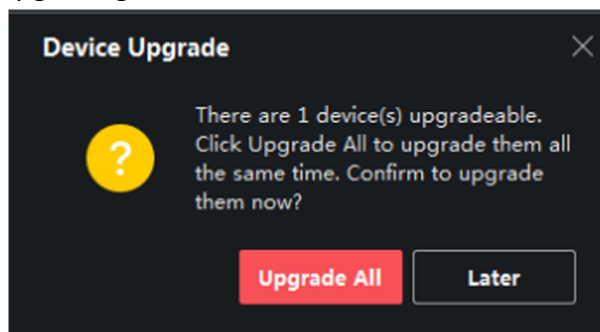


Figure 3-2 Device Upgrade Prompt

Note

After clicking **Upgrade All**, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt.

Download and Update Automatically

After the client detects the new version of the devices, it will download the new version and upgrade the new version without noticing the user.

On the device management page, the following updating status will be shown in the Firmware Update column.


No Available Version

No new firmware version available.

Upgradeable

A new firmware version available.

Note

Move the cursor on  to view the current version, latest version, and upgrade content of the firmware version.

Waiting

The device is waiting for upgrade.

Downloading

The client is downloading the package of the new firmware version.

Upgrading

The upgrading of the device firmware is going on.

Upgraded

Hover the cursor on **Upgraded** to show the version after upgrading.

Upgrading Failed

When the upgrade fails, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt. Hover the cursor on **Upgrading Failed** to show the error details, and click **Upgrade Again** to try again.

The screenshot shows a table of devices in the iVMS-4200 Client Software. The table has columns for Name, Connection, Network Parameters, Device Type, Serial No., Security Level, Resource Usage, Firmware Upgrade, and Operation. The second device in the list has a red box around the 'Upgradeable' status in the Firmware Upgrade column.

	Name	Connection...	Network Para...	Device Type	Serial No.	Security Le...	Resource U...	Firmware Upgrade	Operation	
<input type="checkbox"/>		IP/Domain		Encoding D...	DS...	10...	Strong	Online	No available version	
<input type="checkbox"/>		IP/Domain		Encoding D...	DS...	04...	Strong	Online	Upgradeable	
<input type="checkbox"/>		IP/Domain		Access Cont...	DS...	3V...	Strong	Online	No available version	
<input type="checkbox"/>		IP/Domain		Device			Strong	Offline	No available version	
<input type="checkbox"/>		IP/Domain		Encoding D...	DS...	80...	Strong	Online	No available version	
<input type="checkbox"/>		IP/Domain		Encoding D...	DS...	80...	Strong	Online	No available version	

Figure 3-3 Firmware Upgrade

Chapter 4 Group Management

The resources added should be organized into groups for convenient management, including encoding channels and alarm inputs. You can get the live view, play back the video files, and do some other operations of the device through the group.

4.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Create a group.
 - Click **Add Group** and enter a group name as you want.
 - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.



The encoding channels and alarm inputs of this device will be imported to the group by default.

4.2 Import Resources to Group

You can import the device resources (such as encoding channels and alarm input) to the added group in a batch.

Before You Start

Add a group for managing devices. Refer to **Add Group** .

Steps



Up to 256 encoding channels can be added to one group.

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Encoding Channel** or **Alarm Input**.
4. Click **Import**.
5. Select the thumbnails/names of the encoding channels or alarm inputs in the thumbnail/list view.

Note

You can click  or  to switch the camera display mode to thumbnail view or to list view.

6. Click **Import** to import the selected resources to the group.


4.3 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For encoding channel, you can edit the channel name, stream type, protocol type, etc. For alarm input, you can edit the resource name. Here we take encoding channel as an example.

Before You Start

Import the resources to group. Refer to *Import Resources to Group*.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
All the added groups are displayed on the left.
3. Select a group on the group list and click **Encoding Channel**.
The encoding channels imported to the group will display.
4. Click  in the Operation column to open the Edit Camera window.
5. Edit the camera information, including the camera name, the stream type, etc.

Video Stream

Select the stream type for live view of the camera as desired.

Note

You should start live view again to take effect.

Playback Stream Type

Select the stream type for playback of the camera as desired.

Note

- This field will display if the device supports dual-stream.
 - You should start live view again to take effect.
-

Rotation Type

Select the rotate type for the live view or playback of the camera as desired.

Protocol Type

Select the transmission protocol for the camera.

 **Note**

You should start live view again to take effect.

Streaming Protocol

Select the protocol as RTSP or private for getting stream when live view.

 **Note**

You should start live view again to take effect.

Stream Media Server

Get stream of the camera via stream media server. You can select and manage the available stream media server.

Copy to...

Copy the configured parameters to other camera(s).

Refresh

Get a new captured picture for the live view of the camera.

6. Click **OK** to save the new settings.

4.4 Remove Resources from Group

You can remove the added resources from the group.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
All the added groups are displayed on the left.
3. Click a group to show the resources added to this group.
4. Select the resource(s) and click **Delete** to remove the resource(s) from the group.

Chapter 5 Cloud P2P

The client software also supports to register a Cloud P2P account, log into your Cloud P2P account and manage the devices which support the Cloud P2P service.

5.1 Register a Cloud P2P Account

The client supports registering a Cloud P2P account to manage devices which supports Cloud P2P service.

Steps

1. Enter the login page of Cloud P2P.
 - Click **Log in** in the upper-right corner of the client.
 - a. Click **Device Management** → **Device** to enter the Device Management page.
 - b. Click **Add** to open the Add Device panel.
 - c. Select **Cloud P2P** as the adding mode.
 - d. Click **Login**.

The Login window pops up.

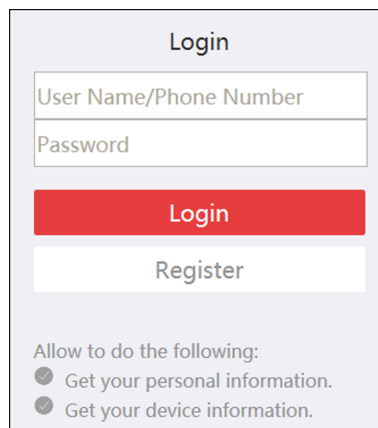


Figure 5-1 Login Window

2. Click **Register** to open the Register Account window.
3. Enter the required information, including user name, password, confirm password, and phone number/email address.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your

password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

4. Click **Send Message** to get a verification code.

The system will send verification code to your phone or email.

5. Enter the received verification code in the **Verification Code** text field.
6. Check **I have read and agreed Terms of Service Privacy Policy**.
7. Click **Register** to finish the registration.

5.2 Log into Cloud P2P Account

You can log into Cloud P2P account via the client, so as to operate devices managed by Cloud P2P account.

Before You Start

Register a Cloud P2P account.



For details, refer to *Register a Cloud P2P Account* .

Steps

1. Enter the login page of Cloud P2P.
 - Click **Log in** in the upper-right corner of the client.
 - a. Click **Device Management** → **Device** to enter the Device Management page.
 - b. Click **Add** to open the Add Device panel.
 - c. Select **Cloud P2P** as the adding mode.
 - d. Click **Login**.

The Login window pops up.

2. Enter user name/phone number, and password.
 3. Click **Log in** to log into your account.

Log in will turn to **Logged in**.
 4. **Optional:** Click **Logged in** → **Log out** to log out of your account.
-



- Devices added by Cloud P2P will be hidden after logging out the Cloud P2P.
 - Alarm-related pictures saved in Cloud P2P will be valid for 2 hours.
-

Chapter 6 Live View

For the surveillance task, you can view the live video of the added network cameras and video encoders on the Main View page. And some basic operations are supported, including picture capturing, manual recording, window division, PTZ control, etc.

6.1 Start Live View

You can start the live view of one camera or all cameras in a group. You can also start the live view in custom view mode.



6.1.1 Start Live View for One Camera

You can start the live view of only one camera.

Before You Start


A camera group is required to be defined for live view.

Steps

1. Open the Main View page.
2. **Optional:** Click  in live view toolbar to select a window division mode for live view.
3. **Optional:** Click  in the live view toolbar to set the parameters such as view scale, play performance, picture saving path, etc.

Note

You can also set the parameters in System Configuration. For details, refer to **System Configuration** .


4. Do one of the following operations to start the live view of one camera.
 - Drag a camera in the group from camera list to a display window to start the live view.
 - Double-click the camera name after selecting a display window to start the live view.
 - Move the cursor to the camera name and click  near the camera name to start live view after selecting a display window.

Note

If the device supports stream encryption, and the stream of its live view is encrypted, you are required to enter a stream key for double verification.

The live video of the camera will start playing in the selected window. The next window will be selected automatically.

5. **Optional:** Drag the video of the camera in live view to another window to change the display window for live view.

6. **Optional:** Move the cursor to the camera name and click  → **Stream** near the camera name to switch the stream type according to actual needs.
-

 **Note**

You can click **All Stream Types** to select the frequently used stream types to display on the right-click menu.


6.1.2 Start Live View for Camera Group

You can start the live view for all cameras in one group synchronously.

Before You Start


A camera group is required to be defined for live view.

Steps

1. Open the Main View page.
 2. **Optional:** Click  in the live view toolbar to set the parameters such as view scale, play performance, picture saving path, etc.
-


 **Note**

You can also set the parameters in System Configuration. For details, refer to **System Configuration**.

3. Perform one of the following operations to start the live view of all cameras in a group.
 - Drag a camera group from camera list to the display window to start the live view.
 - Double-click the group name to start the live view.
 - Move the cursor to the group name and click  near the group name to start live view for all the cameras in the group.
-

 **Note**

- The display window number is self-adaptive to the number of cameras in the group.
 - If the device supports stream encryption, and the stream of its live view is encrypted, you are required to enter a stream key for double verification.
-

4. **Optional:** Move the cursor to the group name and click  → **Stream** near the group name to switch the stream type for the cameras in the group according to actual needs.
-



 **Note**

Before switching to the sixth, seventh, eighth, ninth, and tenth stream, you should set these stream type in the device's web configuration page. For details, refer to the user manual of the device.

6.1.3 Add Custom View




A view is a window division with cameras configured to each window; View mode enables you to save the window division and the correspondence between cameras and windows as favorite to quickly access the related cameras later. For example, you can link camera 1, camera 2, and camera 3 located in your office to display windows and save them as a view called office. Besides the pre-defined default views, you can customize views for further operations.

Steps

1. Open the Main View page.
2. Move the cursor to the Custom View in the View panel and click  to create a new view.
3. Enter a name for the view.
4. **Optional:** Click  in the live view toolbar to set window division mode for the new view.

Note

By default, the new view is in 4-window division.

5. Start live view for specified camera in specified window according to actual needs.
6. Click  to directly save the view.
7. **Optional:** Perform the following operations after adding the custom view.
 - Edit View Name** Move the cursor over the new view and click  to edit the view name.
 - Delete View** Move the cursor over the new view and click  to delete the view.


6.1.4 Start Live View in Custom View Mode

After adding a custom view, you can start live view for the cameras in the custom view.

Before You Start


Customize a view which containing information such as window division, camera and correspondence between cameras and windows. See **Add Custom View** for details.

Steps

1. Open the Main View page.
2. **Optional:** Click  in the live view toolbar to set the parameters such as view scale, play performance, picture saving path, etc.



Note

You can also set the parameters in System Configuration. For details, refer to **System Configuration** .

3. Click  to expand the custom view list in the View panel.
4. Click a custom view to start live view.

The video of the added cameras in the selected view displays.

5. **Optional:** Perform the following operation(s) after starting live view in custom view mode.

Start Instant Playback	Move the cursor over the new view and click  to start instant playback for the cameras in the view. See Instant Playback for details.
Start Auto-Switch of All Custom Views	Move the cursor over Custom View and click  to start switching all views in the custom view list automatically. See details in Auto-Switch in Live View .

6.2 Auto-Switch in Live View

You can display live view of cameras or display the custom views in turn, which is called "auto-switch".


When auto-switching in live view, three modes are available:

- Auto-Switch All Cameras in Default View
- Auto-Switch Cameras in a Group
- Auto-Switch Custom Views

6.2.1 Auto-Switch All Cameras

The video of all the cameras in the camera list can switch automatically in a self-adaptive mode. If you start auto-switch of all cameras, the live view of all cameras can be displayed quickly, which is an effective way for live view. The auto-switch is performed with an interval which can be configured. You can also switch to playback and perform other operations on the auto-switch window.

Steps

1. Open the Main View page.
2. Click **Auto-Switch** → **Multi-Window Auto-Switch** on the left panel.
3. Hover the cursor on **Auto-Switch All Cameras**, and then click  .
All cameras in the camera list start auto-switching in a self-adaptive mode.
4. **Optional:** Click **20 Seconds** at the bottom of the page to change the auto-switch interval.

Example


If you set the interval as 10 seconds, the image of each camera will be displayed for 10 seconds and then switch to next camera.

6.2.2 Auto-Switch Cameras in a Group

The video stream of the cameras from the same group can switch automatically in a selected display window. For example, if you start auto-switch of a group containing 5 cameras, the live

view of the 5 cameras will be displayed in turn with an interval which can be configured. You can also switch to playback and perform other operations on the display window.

Steps

1. Open the Main View page.
2. Click **Auto-Switch** → **Single Window Auto-Switch** on the left panel to show the groups.
3. Select a display window on the right panel.
4. Hover the cursor on a group name and click .

The cameras in the selected group starts auto-switch in the display window.

Note

The audio is off by default after auto-switch starts.

5. **Optional:** Click **20 Seconds** at the bottom of the page to change the auto-switch interval.

Example

If you set the interval as 10 seconds, the image of each camera will be displayed for 10 seconds and then switch to next camera.

6.2.3 Auto-Switch Custom Views

A view is a window division with resource channels (e.g., cameras and access points) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows as favorite so that you can quickly access these channels later. If you saved a view containing all cameras on a floor beforehand, you can view the live view of all the cameras on the floor in turn by a one-stop operation. In this way, you do not have to search these cameras in the camera list every time you login. The auto-switch performs with an interval which can be configured manually.

Before You Start

Add the custom views. See **Add Custom View** for details.

Steps

1. Open the Main View page.
2. Click **Resource** → **Multi-Window Auto-Switch** on the left panel.
3. Hover the cursor on **Auto-Switch All Views** and click .

All custom views starts auto-switching.

4. **Optional:** Click **20 Seconds** at the bottom of the page to change the auto-switch interval.

Example

If you set the interval as 10 seconds, the image of each camera will be displayed for 10 seconds and then switch to next camera.

6.3 PTZ Control

The software provides PTZ control for cameras with pan/tilt/zoom functionality. During the PTZ control, you can set preset, patrol, and pattern, and you can also open a new window for controlling the PTZ.









Note











Cloud P2P device only supports the PTZ movements to the directions of up, down, left, and right.




Enter the **Main View** module, and select **PTZ Control** to open the PTZ control panel.

The following icons are available on the PTZ control panel.

Table 6-1 Icons on the PTZ Control Panel

Icon	Name	Description
	Direction Buttons	Click or hold the left mouse button to turn the PTZ around. Click  to turn around the PTZ horizontally and continuously; click again to stop turning.
	Speed Control	Drag the slider to adjust the PTZ moving speed.
	Zoom in/out	Zoom in to view close image for details; zoom out to view a panoramic image.
	Focus +/-	Click Focus + move the focal point forward, and click Focus - to move the focal point backward.
	Iris +/-	Used for adjusting the luminance of the image. The larger the iris is, the more the light enters, and the brighter the image will be.
	3D Positioning	Use the left key of mouse to click on the desired position in the video image and drag a rectangle area in the lower right direction, then the dome system will move the position to the center and allow the rectangle area to zoom in. Use the left key of mouse to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.
	Auxiliary Focus	Click to focus automatically.

Icon	Name	Description
	Lens Initialization	Initialize the lens and focus again for a clear image.
	Light	Click to fill light.  Note This function needs to be supported by the device.
	Wiper	Use the wiper to clear the dust on the camera lens.
	Manual Tracking	For speed dome with auto-tracking function, enable the auto-tracking (via right-click menu) for it and click the icon to manually track the target by clicking on the video.
	Menu	For analog speed dome, click the icon to display its local menu. For detailed operation of the menu, refer to user manual of the speed dome.
	One-Touch Patrol	For speed dome with one-touch patrol function, click the icon and the speed dome starts patrol from the predefined preset No.1 to preset No.32 in order after a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	One-Touch Park	For the speed dome with one-touch park function, click the icon and the speed dome saves the current view to the preset No.32. The device starts to park at preset No. 32 automatically after a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	Enable Manual De-Icing Heater	Enable this function to ensure the camera performance in environment under 0°C.
	Manual Face Capture	Click this button, and hold the left mouse button to select a face in the image to capture it. The picture will be uploaded to the server for viewing.

Icon	Name	Description
	Synchronize FOV	For thermal cameras. Click to synchronize the optical channel's field of view with that of the thermal channel.
	Regional Exposure	For speed domes, click the icon and draw a rectangle on the image to optimize the exposure effect in this region.
	Regional Focus	For speed domes, click the icon and draw a rectangle on the image to optimize the focus effect in this region.

6.3.1 Configure Preset

A preset is a predefined image position which contains information of pan, tilt, focus and other parameters. After setting preset, you can quickly locate the desired camera's position by calling the preset.

Steps

1. Open the Main View page and start the live view of the PTZ camera.
2. Click **PTZ Control** on the left to expand the PTZ Control panel.
3. Unfold the PTZ control panel in the lower-left corner of the page.

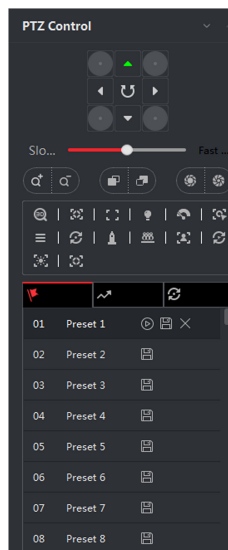






Figure 6-1 PTZ Control Panel

4. Select one PTZ window from the main view windows.
5. **Optional:** On the PTZ control panel, click the preset name (e.g. Preset 1) to edit the preset name.
6. On the PTZ control panel, click the direction button and function button on the PTZ control panel, to adjust the scene to the place you want to mark as a preset.

7. Click  to save the preset settings.

8. **Optional:** Perform the following operation(s) after setting the preset.

- | | |
|----------------------|--|
| Call Preset | Select the preset and click  to call the preset. You can also press the number key (e.g., 4) on keyboard to call the preset 1 to 9, and press [, number keys (e.g., 124), and J on keyboard to call the other preset. |
| Edit Preset | Adjust the direction, position and view of the PTZ camera, and then and click  to save the preset again. The old preset settings will be replaced. |
| Delete Preset | Select the configured preset from the list and click  to delete it. |

6.3.2 Configure Patrol

A patrol is a scanning track specified by a group of user-defined presets, with the scanning speed between two presets and the dwell time at the preset separately programmable.



Before You Start





Add two or more presets for one PTZ camera.

Steps

Note

For Cloud P2P device, patrol is not supported.

1. Open the Main View page and start the live view of PTZ camera.
2. Click **PTZ Control** on the left to expand the PTZ Control panel.
3. Click  tab to enter the PTZ patrol configuration panel.
4. Select a path No. from the drop-down list.
5. Click  to open Add Patrol No. dialog.
6. Select a preset from the drop-down list and set the dwell time and patrol speed for the preset in the dialog.
7. Click **OK**.
8. Repeat step 5, 6, and 7 to add other presets to the patrol.
9. **Optional:** Perform the following operation(s) after setting the patrol.

- | | |
|----------------------------------|--|
| Call Patrol | Click  to call the patrol. |
| Stop Calling Patrol | Click  to stop calling the patrol. |
| Edit Preset in Patrol | Select a preset in the patrol path and click  to edit the preset. |
| Remove Preset from Patrol | Select a preset in the patrol path and click  to remove the preset from the patrol. |




6.3.3 Configure Pattern





A pattern is a memorized, repeating series of pan, tilt, zoom, and preset functions.

Steps

Note

For Cloud P2P device, pattern is not supported.

1. Open the Main View page and start the live view of the PTZ camera.
2. Click **PTZ Control** on the left to expand the PTZ Control panel.
3. Click  tab to enter the PTZ pattern configuration panel.
4. Click  to start the recording of this pattern path.
5. Use the direction buttons to control the PTZ movement.
6. Click  to stop recording and save the recorded pattern.
7. **Optional:** Perform the following operation(s) after setting the pattern.

- | | |
|-----------------------------|--|
| Call Pattern | Click  to call the pattern. |
| Stop Calling Pattern | Click  to stop calling the pattern. |
| Delete Pattern | Select one pattern and click  to delete the pattern. |
| Delete All Patterns | Click  to delete all the patterns. |


6.4 Customize Window Division

The client software provides multiple kinds of predefined window divisions. You can also set custom the window division as desired.

Steps

Note


Up to 5 window divisions can be customized.

1. Open the Main View or Remote Playback page.
 2. Click  on the live view or playback toolbar to open the window division panel.
 3. Click **Add** to open the Add Custom Window Division dialog.
 4. Enter the window numbers in both horizontal and vertical dimension in the Dimension field, and then press **Enter** on your keyboard.
-

Note

For remote playback, up to 16 windows can be played at the same time, so the custom window division with more than 16 windows is invalid.

5. **Optional:** Drag your mouse to select the adjacent windows, and click **Joint** to joint them as a whole window.

6. **Optional:** Select the joint window and click **Restore** to cancel the joint.
7. Click **Save**.
8. **Optional:** Click or drag a division mode to the displaying window to apply the mode for displaying.
9. **Optional:** Edit a customized window division mode.
 - 1) Click  on the live view or playback toolbar to open the window division panel.
 - 2) Click **Edit** to open the Add Custom Window Division.
 - 3) Select a customized division mode and perform operations including renaming, setting dimension, jointing/undo jointing windows.

6.5 Manually Record and Capture

During live view, you can record videos and capture pictures manually, and then view the recorded video files and captured pictures in the local PC.


6.5.1 Manually Record Video

Manual recording function allows to record the live video on the Main View page manually, and you can store the video files in the local PC.

Steps

Note

Manual recording is not supported by Cloud P2P device during live view.

1. Open the Main View page.
2. Start the live view.
3. Perform one of the following operations to start manual recording.
 - Move the cursor to the display window in live view to show the toolbar and click  on the toolbar.
 - Right-click on the display window and click **Start Recording** on the right-click menu.

The icon  turns to . An indicator   appears in the upper-right corner of the display window.

4. Click  to stop the manual recording.

The recorded video file is automatically saved to the local PC, and a small window with the saving path information appears in the lower-right corner of desktop.

Note

The saving path of the recorded video files can be set on the System Configuration page. See **Set File Saving Path** for details.


6.5.2 View Local Videos

You can view the recorded video files stored in your local PC.

Before You Start

Record the live video.

Steps

1. Click  → **File** → **Open Video File** in the upper-right corner to open the Video Files page.
2. Select the camera to search the recorded video files from the Camera Group list.
3. Specify the start time and end time in the lower-left corner for the searching.
4. Click **Search**.

The video files recorded between the start time and end time displays in thumbnail format on the page.

5. **Optional:** Perform the following operation(s) after the search.

Delete Video File	Select the video file, and click Delete to delete the video file.
Send Email	Select the video file, and click Email to send an email notification with the selected video file attached.

Note

To send an email notification, the email settings need to be configured before proceeding. For details, refer to **Set Email Parameters** .


Save Local Video	Select the video file, and click Save as to save a new copy of the video file.
Playback	Double-click the video file to start the local playback.

6.5.3 Capture Pictures

You can capture pictures during the live view.

Perform this task when you need to capture pictures during the live view.

Steps

1. Open Main View page and start the live view of a camera.
2. Perform one of the following operations to capture pictures.
 - Move the cursor to the display window in live view to show the toolbar and click  on the toolbar.
 - Right-click the display window and click **Capture** on the right-click menu.

The captured picture is automatically saved to the local PC, and a small window with the picture preview and saving path information appears in the lower-right corner of desktop.



Note

The saving path of the captured pictures can be set on the System Configuration page. For details, refer to *Set File Saving Path*.


6.5.4 View Captured Pictures

The pictures captured in the live view are stored in the PC running the software. You can view the captured pictures if needed.

Before You Start

Capture pictures in the live view.

Steps

1. Click  → **File** → **Open Captured Picture** in the upper-right corner to open the Captured Picture page.
2. Select the camera to search the captured pictures from the Camera Group list.
3. Specify the start time and end time in the lower-left corner for the searching.
4. Click **Search**.

The pictures captured between the start time and end time display in thumbnail format on the page.

5. **Optional:** Perform the following operation(s) after the search.

- | | |
|------------------------|---|
| Enlarge Picture | Double-click the picture thumbnail to enlarge it for a better view. |
| Print Picture | Select the captured picture, and click Print to print the selected picture. |
| Delete Picture | Select the captured picture, and click Delete to delete the selected picture. |
| Send Email | Select the captured picture, and click Email to send an email notification with the selected picture attached. |
| Save Picture | Select the captured picture, and click Save as to save a new copy of the selected picture. |



6.6 Instant Playback

Instant playback shows a piece of the video which is remarkable, or which is unclear on the first sight. So you can play the video files instantly on the Main View page and get an immediate review if needed.

Before You Start

Record the video files and store them on the storage devices, such as the SD/SDHC cards and HDDs on the DVRs, NVRs, network cameras, etc., or on the storage servers.

Steps

1. Open Main View page and start the live view.
2. Perform one of the following operations to show the pre-play durations' list of instant playback.
 - Move the cursor to the display window to show the toolbar and click .
 - Right-click the display window and select **Switch to Instant Playback** on the right-click menu.
 - Move the cursor to default view or custom view node on the View panel and click .A list with pre-play durations of 30s, 1 min, 3 min, 5 min, 8 min, and 10 min displays.
3. Select a time period from the appeared list to start the instant playback.

Example

If you select 3 min, and the current time of the live view is 09:30:00, then the instant playback will start from 09:27:00.

During the instant playback, an indicator  appears in the upper-right corner of the display window.

4. **Optional:** Click  again to stop the instant playback and go back for the live view.





6.7 Live View for Fisheye Camera

For fisheye cameras, you can start the live view in fisheye mode, set presets and patrols, and perform PTZ control.

6.7.1 Perform Live View in Fisheye Mode

During live view of fisheye cameras, the whole wide-angle distorted view will be displayed. But you may have difficulty to view some details. To solve this problem, you can play the live videos in fisheye expansion mode. Fisheye expansion can expand images in various modes: 180° panorama, 360° panorama, PTZ, half sphere, etc. So that you can view the image clearly.

Steps

1. Open the Main View page and start the live view of fisheye camera.
2. Enter the Fisheye Expansion mode.
 - Right-click on the video and select **Fisheye Expansion**.
 - Click  in the toolbar. See **Set Icons Shown on Toolbar** for details about setting the toolbar. turns to .
3. Click  in the lower-left corner of the displaying window to open the Mounting Type & Expanding Mode Selection panel.
4. Select the mounting type of the fisheye camera according to its actual mounting position.
5. Select the expanding mode for live view as desired.

Fisheye

In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called Fisheye because it approximates the vision of a fish's convex eye. The lens

produce curvilinear images of a large area, while distort the perspective and angles of objects in the image.

Panorama

In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.

PTZ

The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.



Note

Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.

Half Sphere

By the half sphere mode, you can drag the image and rotate it centering on the diameter, in order to adjust the view to the desired angle.

AR Half Sphere

AR half sphere mode overlaps images far and near, so that you can view a dimensional image in a wide angle.

6. Optional: Perform the following operation(s) after starting live view in fisheye mode.

Capture	Right-click on the window and select Capture to capture the picture in the live view process.
Enter Full Screen	Right-click on a playing window and switch the selected window to full-screen mode.

6.7.2 PTZ Control in Fisheye Mode




In fisheye mode, you can control the PTZ to adjust the PTZ window.



Note

The PTZ panel varies according to different devices.

The following functions are available on the PTZ control panel.

- Select a PTZ window, and click the direction buttons to adjust view angle. Or drag the No. label in the fisheye or panorama window to change the view angle of the PTZ window.
- Select a PTZ window, click  to start auto-scan (the camera rotates in a horizontal direction) , and click it again to stop auto-scan.
- Drag the slider on  to adjust the speed for PTZ movement.
- Click  , or scroll the mouse wheel to zoom in or zoom out the selected PTZ window.

Configure Preset

In fisheye mode, you can configure the preset which is a user-defined monitor position/point and simply call the preset No. to change the monitor scene to the defined position.


Steps






Only the specific fisheye cameras support configuring the preset, and up to 256 presets can be configured in fisheye mode.

1. Open Main View page and start the live view of fisheye camera.
2. Right-click on the video and select **Fisheye Expansion** to enter the Fisheye Expansion window.
3. Unfold the PTZ control panel in the lower-left corner of the page.



4. Select one PTZ window from the main view windows.
5. **Optional:** On the PTZ control panel, click the preset name (e.g. Preset 1) to edit the preset name.
6. On the PTZ control panel, click the direction button and function button on the PTZ control panel, to adjust the scene to the place you want to mark as a preset.
7. Click  to save the preset settings.
8. **Optional:** Perform the following operation(s) after setting the preset.

Call Preset	Select the preset and click  to call the preset. You can also press the number key (e.g., 4) on keyboard to call the preset 1 to 9, and press [, number keys (e.g., 124), and J on keyboard to call the other preset.
Edit Preset	Adjust the direction, position and view of the PTZ camera, and then and click  to save the preset again. The old preset settings will be replaced.
Delete Preset	Select the configured preset from the list and click  to delete it.

Configure Patrol

In fisheye mode, you can configure the patrol, which is a scanning track specified by a group of user-defined presets, with the scanning speed between two presets and the dwell time at the preset separately programmable.

Before You Start



Configure two or more presets.




Steps




Note

Only the specific fisheye cameras support configuring the patrol, and up to 32 patrols can be configured in fisheye mode.

1. Open Main View page and start the live view of fisheye camera.
2. Right-click on the video and select **Fisheye Expansion** to enter the Fisheye Expansion window.
3. Click  tab to enter the patrol configuration panel.
4. Select a path No. from the drop-down list.
5. Click  to open Add Patrol No. window.
6. Click **OK**.
7. Repeat step 5, 6, and 7 to add other presets to the patrol.
8. **Optional:** Perform the following operation(s) after configuring the patrol.

Edit Preset in Patrol	Select a preset in the patrol path and click  to edit the preset.
Remove Preset from Patrol	Select a preset in the patrol path and click  to remove the preset from the patrol.
Call Patrol	Click  to call the patrol.

Stop Calling Patrol

Click  to stop calling the patrol.

6.8 Perform Master-Slave Linkage

The box or bullet camera which supports master-slave tracking function can locate or track the target according to your demand.

Note

- This function is only supported by the specific box or bullet camera.
 - A speed dome with the auto-tracking function is required to be installed near the box or bullet camera.
-



6.8.1 Configure Master-Slave Tracking Rule

Before performing master-slave tracking during live view, you should configure the master-slave tracking rules for the box or bullet camera, including setting VCA detection rule, linking to a speed dome, and calibrating camera and speed dome.

Set Intrusion Detection Rule

You should set the VCA detection rule for the bullet or box camera, and when the VCA event is triggered, the client can trigger speed dome to track the target. Here we take intrusion detection as an example.

Steps

1. Open Device Management page and select a box or bullet camera.
2. Click  → **Advanced Configuration** → **VCA Config** → **Rule** → **Rule Settings** to enter rule settings page.
3. Click **Add** in Rule List panel to add a rule.
4. Select **Intrusion** as the event type.
5. Click  to draw a detection region on the live video.
6. Click **Save**.


Link Speed Dome

When configuring the master-slave tracking for the box or bullet camera, you can link the camera to a speed dome and set the PTZ position for the speed dome for tracking.

Perform this task to link the box or bullet camera to a speed dome for master-slave tracking.

Steps

1. Open Device Management page and select a box or bullet camera.

2. Click  → **Advanced Configuration** → **Master-Slave Tracking** to enter master-slave tracking settings page.
3. Click **Login** on the display window to open the speed dome login window.
4. Input the speed dome's IP address, port No., user name, and password.
5. Click **Login** to log in to the speed dome.
6. Click **PTZ** and use the direction arrows to adjust the speed dome to a horizontal position.

What to do next

Calibrate the box or bullet camera and the linked speed dome, see ***Calibrate Camera and Speed Dome Automatically*** or ***Calibrate Camera and Speed Dome Manually*** for details.


Calibrate Camera and Speed Dome Automatically

When setting the bullet or box camera's master-slave tracking rule, you should calibrate the camera and the speed dome. Two calibration modes, including auto and manual, are available, here we introduce the auto calibration.

Before You Start

Link the camera to a speed dome, see ***Link Speed Dome*** for details.

Steps

1. Open Device Management page and select a box or bullet camera.
2. Click  → **Advanced Configuration** → **Master-Slave Tracking** to enter master-slave tracking settings page.
3. Select the calibration mode as **Auto Calibrating** in the lower-right corner of Calibration panel.
4. Move and zoom in/out the view of speed dome to make sure the live views of dome and camera are mostly same.
5. Click **Save**.



Calibrate Camera and Speed Dome Manually

When setting the bullet or box camera's master-slave tracking rule, you should calibrate the camera and the speed dome. Two calibration modes, including auto and manual, are available, here we introduce the manual calibration.

Before You Start

Link the camera to a speed dome. See ***Link Speed Dome*** for details.


Steps

1. Open Device Management page and select a box or bullet camera.
2. Click  → **Advanced Configuration** → **Master-Slave Tracking** to enter master-slave tracking settings page.
3. Select the calibration mode as **Manual Calibrating** in the lower-right corner of Calibration panel.
4. Select site No. 1 from the list and click .

A blue cross appears in the center of the live view page, and the digital zoom view of the selected site appears on the right.

5. Repeat step 4 to add other manual calibration sites.
6. Adjust the distances among the four calibration sites evenly in the live view page.
7. Select the calibration site No. 1.

The digital zoom view of site No. 1 appears at the right.

8. Move and zoom in or out the view of speed dome to make sure the live views of speed dome and the digital zoom view of selected site are mostly same.
9. Click  to save the current site position information.
10. Repeat step 7, 8, and 9 to set other sites' position.
11. Click **Save**.

6.8.2 Enable Master-Slave Tracking

During live view, you can enable the master-slave tracking to locate or track the target appeared in the view of bullet or box camera with a speed dome.

Before You Start

Configure the master-slave tracking rules for the box or bullet camera.

Perform this task when you need to enable the master-slave tracking for box or bullet camera.

Steps

1. Enter the Main View page and start the live view of box or bullet camera.
2. Right-click on the live view window and click **Enable Master-Slave Tracking**.

When the configured VCA rule is triggered by target, the linked speed dome performs the automatic master-slave tracking and the target frame turns from green into red.

6.9 Live View for Thermal Camera

For thermal camera, you can view the fire source information and temperature during live view. You can also measure the temperature manually to get temperature information in the live view image.

6.9.1 View Fire Source Information during Live View

During the live view, you can view the detected fire source information.

Before You Start

Configure the alarm rules for the thermal device, see the user manual of the device for details.

Perform this task when you need to view the fire source information during live view.

Steps

1. Enter Main View page and start the live view of a thermal camera.

Note

For starting and stopping live view, refer to *Start Live View for One Camera* and .

2. Right-click on the live view image and select **File Source Information** in the right-click menu to show the list of information types.
3. Select a information type in the list to display the information.

Fire Source Region

The region in which the temperature is higher than the configured alarm threshold.

Maximum Temperature Region

Mark the region in which the temperature is highest in the fire source region. It is marked in green.

Fire Source Target

Display the target location information.

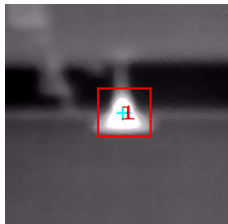


Figure 6-3 Fire Source Information on Live View Image

6.9.2 Show Temperature Information on Live View Image

You can show or hide the real-time temperature information of the monitoring scene when viewing the live video.

Before You Start

- Switch the device VCA source type as **Temperature Measurement + Behavior Analysis**.
- Enable the device temperature measurement function and set the temperature measurement rules, see the user manual of the device for details.

Perform this task when you need to show the temperature information on the live view image.

Steps

1. Enter Main View page and start the live view of a thermal camera.

Note

For starting live view, refer to *Start Live View for One Camera* .

2. Adjust the scene to the area configured with temperature measurement rule.
3. Right-click on the live view image and select **Show Temperature Information** in the right-click menu.

The temperature displays on the live view image.

4. Click on the image to view the detailed temperature information.

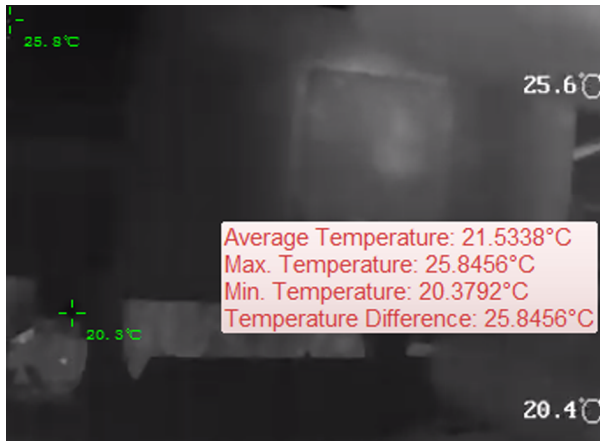


Figure 6-4 Temperature Information on Live View Image

5. **Optional:** Right-click on the live view image and select **Hide Temperature Information** to hide the temperature information.

6.9.3 Manually Measure Temperature

During the live view of thermal camera, you can click anywhere on the live view image to show the temperature of different points to locate the fire resource quickly.

Steps

Note

- The measured temperature will be displayed on the image for 5 seconds.
 - Only one point's temperature can be displayed.
 - When multiple clients are getting the live video of one camera, if one client adds or deletes the measurement points, other clients' live view will be affected as well. The measurement points will be cleared if all users stop live view of the camera.
-

1. Enter Main View page and start the live view of a thermal camera.
-

Note

For starting and stopping live view, refer to **Start Live View for One Camera** and .

2. Right-click on the live view image and select **Show Temperature Information**.
3. Click on the live view image to show the temperature of this position.
The temperature of the clicked points is shown on the image.

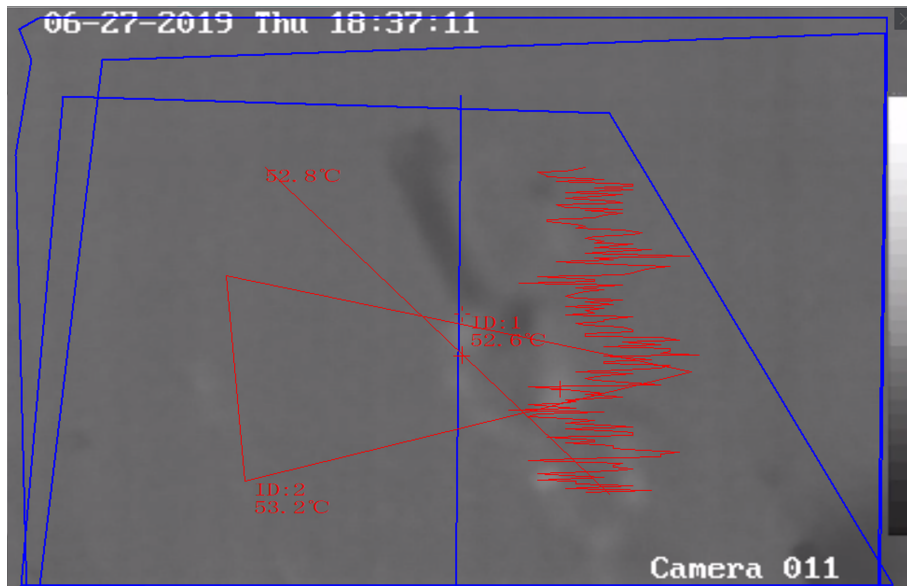


Figure 6-5 Manually Measure Temperature on Points

4. **Optional:** Right-click on the live view image and select **Hide Temperature Information** on the menu.

6.10 Live View in Low Bandwidth

In situation of low network bandwidth, the speed of video streaming might be much slower due to the bandwidth limit. To provide normal quality in less streaming speed for low bandwidth users, the client provides live view in low bandwidth mode. Before that, you need to set the streaming protocol and perform other operations first.

For details about the settings, refer to ***How to get better performance of live view and playback when network bandwidth is low?*** .

6.11 More Functions

There are some more functions supported in the live view, including auxiliary screen preview, digital zoom, channel-zero, two-way audio, camera status, and synchronization.

Auxiliary Screen Preview

Display the live video on different auxiliary screens for the convenient preview of multiple monitoring scenes.

Note

Up to 3 auxiliary screens are supported.

Digital Zoom

Drag the mouse to draw a rectangle area in the lower-right/upper-left direction to zoom in or out the drawn area. Or use the mouse wheel to zoom in or out the view in digital zoom mode.

Channel-Zero

For the channel-zero of the device, hold the **Ctrl** key and double-click to display the specific channel. Hold the **Ctrl** key and double-click again to restore.

Two-Way Audio

Two-way audio function enables the voice talk of the camera. You can get not only the live video but also the real-time audio from the camera. If the device has multiple two-way audio channels, you can select a channel to start two-way audio.



Note

- The two-way audio can be used for only one camera at one time.
 - Cloud P2P device doesn't support selecting channel during two-way audio.
-

Camera Status

The camera status, such as recording status, signal status, connection number, etc., can be detected and displayed for checking. The status information refreshes every 10 seconds.

Synchronization

The synchronization function provides a way to synchronize the device clock with the PC which runs the client software.

Chapter 7 Remote Storage Configuration

The video files and captured pictures can be stored on the HDDs, Net HDDs, or SD/SDHC cards on the local device, or on the storage server connected.

7.1 Store Picture and Video on DVR, NVR, or Network Camera

Some local devices, including the DVRs, NVRs, and Network Cameras, provide storage devices such as the HDDs, Net HDDs and SD/SDHC cards for video and picture files. You can set a recording schedule or capture schedule for the channels of the local devices.

Before You Start

Make sure the newly installed storage devices have been formatted. Refer to *Format Storage Server's HDD* for details.

Perform this task when you need to store the picture and video files on the encoding device such as DVR, NVR, or network camera.

Steps



Note

The pictures captured through the capture schedule are stored on the local device and can be searched on the remote configuration page of the device.

1. Enter the Storage Schedule module.
2. Select the camera in the Camera Group list.
3. Set **Recording Schedule** switch or **Capture Schedule** switch to ON on **Storage on Encoding Device** area to enable device local recording or capture.
4. Select the recording or capture schedule template from the drop-down list.

All-day Template

All-day continuous recording.

Weekday Template

Working-hours continuous recording from 8:00 AM to 8:00 PM.

Event Template

All-day event triggered recording.

Template 01 to 08

Fixed templates for specific schedules. You can edit the templates if needed.

Custom

Customize a template as you want.

 **Note**

If you need to edit or customize the template, refer to ***Configure Recording Schedule Template*** or ***Configure Capture Schedule Template***.

5. Click **Advanced** of Recording Schedule to set the recording advanced parameters.
-

 **Note**

The displayed items vary according to the devices.

Pre-record

Normally used for the event triggered record, when you want to record before the event happens.

Post-record

After the event finished, the video can also be recorded for a certain time.

Keep Video Files for

The time for keeping the video files in the storage device, once exceeded, the files will be deleted. The files will be saved permanently if the value is set as 0.

Redundant Recording

Save the video files not only in the R/W HDD but also in the redundant HDD.

Record Audio

Record the video files with audio or not.

Video Stream

Select the stream type for the recording.

 **Note**

For specific type of devices, you can select **Dual-Stream** for recording both main stream and sub-stream of the camera. In this mode, you can switch the stream type during remote playback. Refer to ***Normal Playback*** for stream switch during playback.

6. Click **Advanced** of Capture Schedule to set the capture advanced parameters.

Resolution

Select the resolution for the continuous or event captured pictures.

Picture Quality

Set the quality for the continuous or event captured pictures.

Interval

Select the interval which refers to the time period between two capturing actions.

Captured Picture Number

Set the picture number for event capture.

7. **Optional:** Click **Copy to...** to copy the recording schedule settings to other channels.
-

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

7.2 Store Video on Storage Device

You can store the video files recorded by the added encoding devices on the storage devices managed in the client.

You can add storage device to the client for storing the video files of the added encoding devices and you can search the files for remote playback. The storage device can be iVMS-4200 Storage Server, CVR (Center Video Recorder), or other NVR.

Here we take the settings of iVMS-4200 Storage Server as an example.


Note

The iVMS-4200 Storage Server application software needs to be installed and it is packed in the client installation package. After running the installation package, select **Storage Server** to enable the installation of iVMS-4200 Storage Server.

7.2.1 Activate Storage Server

If it is the first running the iVMS-4200 Storage Server, you are required to activate the storage server. Perform this task when you need to activate storage server.

Steps

1. Click  on the desktop to run the iVMS-4200 Storage Server.

Note

- If the storage server port (value: 8000) is occupied by other service, a dialog will pop up. You should change the port No. to other value to ensure the proper running of the storage server.
 - You can also record the video files on the iVMS-4200 Storage Server installed on another PC.
-

2. Enter the **New Password** and **Confirm Password**.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

3. Click **OK** to change the password.

After changing the password, the storage server will run automatically.

7.2.2 Add Storage Server to Client

You can add storage server to the client for storing the video files of the added encoding devices.

Steps

1. Enter the Device Management module.
2. Click **Device** tab.

The added devices are displayed in the list.

3. Add iVMS-4200 Storage Server.
 - You can add online storage server. For details, refer to **Add an Online Device** .
 - You can add storage server via IP address or domain name. For details, refer to **Add Device by IP Address or Domain Name**

7.2.3 Format Storage Server's HDD

You should format the HDDs of the storage server for the video file storage.


Perform this task to format storage server's HDD.

Steps



Formatting the HDDs is to pre-allocate the disk space for storage and the original data of the formatted HDDs will not be deleted.

1. Enter the Device Management module.
2. Click **Device** tab.

The added devices are displayed in the list.
3. Select the added storage server from the list.
4. Click  .
5. Click **Storage** → **General** to enter the HDD Formatting window.
6. Select the HDD from the list and click **Format**.

You can check the formatting process from the process bar and the status of the formatted HDD changes from **Unformatted** to **Normal Status**.

7.2.4 Configure Storage Settings

When the storage server is available, you can set the recording schedule for the cameras.

Before You Start

The newly installed storage devices need to be formatted.

Steps

1. Enter **Storage Schedule** module.
2. Select the camera in the Camera Group list.
3. Select a storage server from the **Storage Server** drop-down list.
4. Set **Recording Schedule** switch to ON to enable storing the video files.
5. Select the schedule template for recording from the drop-down list.

Note

If you need to edit or customize the template, refer to ***Configure Recording Schedule Template*** .

6. **Optional:** For Recording Schedule, click **Advanced** to set the pre-record time, post-record time, video stream, and other parameters.

Note

The iVMS-4200 Storage Server only supports main-stream.

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

7.3 Store Picture and Additional Information on Local PC

You can store the pictures and the additional information, such as the heat map, people counting data, and road traffic data, to the local PC.

Perform this task when you need to store pictures and additional information on local PC.

Steps

1. Enter **Storage Schedule** module.
2. Select the camera in the Camera Group list.

Note

This function should be supported by the device.

3. Select storage content.

Picture Storage

Store the alarm pictures of the camera when event occurs. You can click **System Configuration** → **File** to modify the saving path of pictures.

Additional Information Storage


Store the additional information (e.g., heat map, people counting data, etc.) on local PC.

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


7.4 Configure Recording Schedule Template

You can edit the recording schedule template, or customize a recording schedule template.


Steps

1. Enter the Storage Schedule module.
2. Open the template settings window.
 - Select **Template 01** to **Template 08** from the drop-down list and click **Edit**.
 - Select **Custom** from the drop-down list.
3. Drag on the time-line to set the time periods for the selected template when the cursor turns to  .

Continuous

Normal and continuous recording. The schedule time bar is marked with  .

Event Recording

The recording is triggered by event. The schedule time bar is marked with  .

Command

The recording triggered by command. The schedule time bar is marked with  .



Note






Command triggered recording is only available for the ATM transactions when the ATM DVR is added to the client.



Note

Up to 8 time periods can be set for each day in the recording schedule.

4. **Optional:** After setting the time periods, you can do one or more of the following:

Move	Drag a time period to move it when the cursors turns to  .
Lengthen or Shorten	Select a time period and then lengthen or shorten it when the cursor turns to  .
Set Accurate Time	Click a time period to set the accurate start time and end time of the period.
Delete	Select the configured schedule time period and click  to delete it.
Delete All	Click  to delete all the configured time periods.
Copy to	Select one date and click  to copy the date's time period settings to the other dates.
5. **Optional:** For template 01 to 08, you can edit the template name as you want.
6. Click **OK** to save the settings.




Note

If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.


7.5 Configure Capture Schedule Template

You can edit the capture schedule template, or customize a capture schedule template.


Steps

1. Enter the Storage Schedule module.
2. Open the template settings window.
 - Select **Template 01** to **Template 08** from the drop-down list and click **Edit**.
 - Select **Custom** from the drop-down list.
3. Drag on the time-line to set time periods for the selected template when the cursor turns to .






Continuous Capture

Normal and continuous capture. The schedule time bar is marked with .

Event Capture

The capture is triggered by event. The schedule time bar is marked with .

4. **Optional:** After setting the time period, you can do one or more of the followings

- | | |
|----------------------------|--|
| Move | When the cursor turns to  , you can move the time period you just edited. You can also edit the displayed time point to set the accurate time period. |
| Lengthen or Shorten | When the cursor turns to  , you can lengthen or shorten the selected time period. |
| Delete | Select a time period and click  to delete it. |
| Delete All | Click  to delete all the configured time periods. |
| Copy to | Select one date and click  to copy the date's time period settings to the other dates. |

5. **Optional:** For template 01 to 08, you can edit the template name as you want.

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



Note

If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.

Chapter 8 Remote Playback

You can search the video files stored in the local device or the storage server by camera or triggering event, and then play them remotely.


Note

You can set to play back the video files stored in the local device, in the storage server, or both in the storage server and local device. For details, refer to ***Set Live View and Playback Parameters***.

8.1 Normal Playback

You can search video files by camera or group for normal playback and download found video files to local PC. You can also add a tag to mark important video footage, and so on.

You can right-click the playback window to select the required operations from the shortcut menu. Some are listed as follows:

Name	Description
Show/Hide Temperature Information	Show/Hide Temperature Information  Note The temperature information overlay is only supported by thermal camera.
Tag Control	Add default (the default tag name is TAG) or custom tag (the tag name is customized) for the video file to mark the important video point. You can also edit the tag or go to the tag position conveniently.
Other Capture Modes	<ul style="list-style-type: none"> • Print Captured Picture: Capture a picture and print it. • Send Email: Capture the current picture and then send an Email notification to one or more receivers. The captured picture can be attached. • Custom Capture: Capture the current picture. You can edit its name and then save it.



Note

- The Cloud P2P device only supports normal playback and it also does not support the functions of reverse playback, slow forward or fast forward, and adding tag.
 - For NVR which is added to the client by device's other user name (except admin), if **Double Verification** is enabled on this NVR, when playing back videos on the client, you are required to enter the user name and password created for double verification. For details about double verification, refer to the user manual of the NVR.
-



8.1.1 Search Video Files

You can search the video files by date, and you can also enter keyword to filter the matched results for normal playback.

Steps

1. Enter the Remote Playback module.
 2. Click  on the left to enter the Event Playback page.
 3. **Optional:** Click  to set the start date and end date of searching time period.
-

Note

In the calendar, the date which has video files recorded by schedule will be marked with , and the date which has video files recorded based on event will be marked with .

4. Start the playback of camera (s) to search the video files of the selected camera (s). You can do one of the followings to start the playback.
-

Note

Up to 16 cameras can be searched simultaneously.

- Drag the camera or group to a display window.
 - Select a display window and double-click the camera or group to start playback in the selected window.
 - Double-click the cameras in turn to select the display window automatically and start playback in the windows.
-

8.1.2 Play Video Files



After searching the video files for the normal playback, you can play the video via time line.

Steps







1. Enter the Remote Playback module.
 2. Search the video files.
 3. Play video via time line.
-

The video files will play automatically. You can click on the time line to position the desired video segment of specified time for normal playback.

Note

- The time line indicates the time duration for the video files, and the video files of different types are color coded.
 - You can use mouse wheel or click  /  to scale up or scale down the time line bar.
-

4. **Optional:** Perform the following operations on the toolbar to control the playback.

Single Frame (Reverse)	Click  or scroll down the mouse wheel to play the video files frame by frame (reverse).
Audio Control	Click  or  to turn off/on the sound. You can also adjust the volume when turning on.
Download for Multiple Cameras	Click  to download video files of multiple cameras at the same time.
	<hr/>  Note For more details, refer to <i>Download for Multiple Cameras</i> . <hr/>
Download Video Files by Date	Click  to download the video files of the camera by date and store them to local PC.
Accurate Positioning	Click 2018/10/19 08:56:11 to set the accurate time point to play the video file.

8.2 Alarm Input Playback

When the alarm input is triggered and the linked video can be searched for alarm input playback. This function requires the support of the connected device.

For the description of the alarm input playback toolbar and right-click menu of display window, refer to ***Normal Playback*** .


Note


Some icons may be not available for alarm input playback.

8.2.1 Search Video Files

You can search the video files by date, and you can also enter keyword to filter the matched results for alarm input playback.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.

3. Select an alarm input channel at the left.
4. **Optional:** Click  to set the start date and end date of searching time period.
5. Select **Alarm Input** from the drop-down list as the event type.
6. Click **Search** to start the search.


The matched video files of the selected alarm input will display on the right page in chronological order. And by default, the first video file will play automatically.

7. **Optional:** Enter keyword in the **Search** field to filter the results.

8.2.2 Play Video Files

After searching the video files for the alarm input playback, you can play the video via file list or timeline.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.
3. Search the video files of the alarm input.





Note

See **Search Video Files** for details about searching video files of the alarm input.

4. Play video via file list or timeline.
 - Double-click the video file to play the video in the playback display window.
 - Click on the timeline to positioning the desired video segment of specified time for alarm input playback.



Note

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
 - You can use mouse wheel or click  /  to scale up or scale down the timeline bar.
-

8.3 Event Playback

The recorded video files triggered by event, such as motion detection, VCA detection, or behavior analysis, can be searched for event playback. This function requires the support of the connected device.

For the description of the event playback toolbar and right-click menu of display window, refer to **Normal Playback**.





Note

Some icons may be not available for event playback.



8.3.1 Search Video Files

You can search the video files by date and by event type. And you can also enter keyword to filter the matched results for event playback.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.
3. Select the camera at the left.
4. **Optional:** Click  to set the start date and end date of searching time period.

Note

In the calendar, the date which has video files recorded by schedule will be marked with , and the date which has video files recorded based on event will be marked with .


5. Select an event type from the drop-down list.
6. Click **Search** to start the search.

The matched video files will display on the right page in chronological order. And by default, the first video file will play automatically.
7. **Optional:** Enter keyword in the **Search** field to filter the results.



8.3.2 Play Video Files

After searching the video files for the event playback, you can play the video via file list or timeline.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the Event Playback page.
3. Search the video files recorded based on event.
4. Play the video file.
 - Double-click the video file to play the video in the playback display window.
 - Click on the timeline to positioning the desired video segment of specified time for event playback.

Note

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
 - You can use mouse wheel or click  /  to scale up or scale down the timeline bar.
-

8.4 ATM Playback

You can search the video files of ATM DVR for ATM playback. This function requires the support of the connected device which is configured with transaction rule.

For the description of the ATM playback toolbar and right-click menu of display window, refer to **Normal Playback**.





Some icons may be not available for ATM playback.

8.4.1 Search Video Files

You can search the video files of ATM DVR by card number, by transaction type, by transaction amount, by file type, or by date. And you can also enter keyword to filter the matched results for ATM playback.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the ATM Playback page.
3. Select the camera of ATM DVR at the left.
4. **Optional:** Click  to set the start date and end date of searching time period.
5. Set the search conditions.

by Card Number

Enter the card number contained in the ATM information.

Search by Transaction Type

Select transaction type for search, and enter the related transaction amount.

File Type

Select the type of video files for search.

6. Click **Search** to start searching.

The matched video files of selected ATM DVR will display on the right of the Remote Playback page in chronological order. By default, the first video file will play automatically.


7. **Optional:** Enter keyword in the **Search** field to filter the results.

8.4.2 Play Video Files

After searching the video files of the cameras connected with ATM DVR, you can play the video via file list or timeline.



Steps

1. Enter the Remote Playback module.

2. Click  on the left to enter the ATM Playback page.
3. Search the video files of cameras connected with ATM DVR.
4. Play the video file.
 - Double-click the video file to play the video in the playback display window.
 - Click on the timeline to positioning the desired video segment of specified time for ATM playback.



Note

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
 - You can use mouse wheel or click  /  to scale up or scale down the timeline bar.
-

8.5 POS Playback

You can search the video files which contain POS information for POS playback. This function requires the support of the connected device which is configured with POS text overlay.

For the description of the POS playback toolbar and right-click menu of display window, refer to **Normal Playback** .





Note

Some icons may be not available for POS playback.

8.5.1 Search Video Files

You can search the video files which contain POS information by keywords or by date.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the POS Playback page.
3. Select the camera at the left.
4. **Optional:** Click  to set the start date and end date of searching time period.
5. Set the search conditions.

Keywords

Enter the card number contained in the ATM information.



Note

Up to three keywords can be entered for once. And each two keywords should be separated with a comma.

Combination Mode

For more than one keyword, you can select "or (|)" to search the POS information containing any of the keywords, or select "and(&)" to search the POS information containing all of the keywords.

Case Sensitive

Check **Case Sensitive** to search the POS information by case-sensitive keywords.

6. Click **Search** to start searching.

The video files contain POS information will display on the right of the POS Playback page in chronological order. And by default, the first video file will play automatically.

7. **Optional:** Enter keyword in the **Search** field to filter the results.


8.5.2 Play Video Files

After searching the video files which contain POS information, you can play the video via file list or timeline.

Before You Start



Start the normal playback of cameras configured with POS information overlay.

Steps

1. Enter the Remote Playback module.
2. Click  on the left to enter the POS Playback page.
3. Search the video files which contain POS information.
4. Play video via file list or timeline.
 - Double-click the video file to play the video in the playback display window.
 - Click on the timeline to positioning the desired video segment of specified time for POS playback.



Note

- The timeline indicates the time duration for the video files, and the video files of different types are color coded.
 - You can use mouse wheel or click  /  to scale up or scale down the timeline bar.
-


8.6 VCA Playback

You can set VCA rule to the searched video files and find the video that VCA event occurs, such as motion detection, line crossing detection, and intrusion detection. This function helps to search out the video that you may be more concerned and mark it with red color.

Steps

Note

For some devices, you can filter the searched video files by setting the advanced attributes, such as the gender and age of the human and whether he/she wears glasses.

1. Enter the Remote Playback module.
 2. Click  on the left to enter the Camera Playback page.
 3. Select the camera and start the normal playback.
-

Note

Refer to ***Play Video Files*** for details.

4. Right-click the display window to pop up the shortcut menu.
5. Click **VCA Search** and enable the VCA Type, draw the detection region and set the sensitivity.

Motion Detection

Get all the related motion detection events that occurred in the pre-defined region.

Line Crossing Detection


Bi-directionally detect people, vehicles and other moving objects that cross a virtual line.

Intrusion Detection

Detect whether there are people, vehicles and other moving objects intruding into the pre-defined region.

Note

You can click **VCA Settings** to set the sensitivity and filter the searched video files by setting the target characters, such as the gender and age of the human and whether he/she wears glasses. This function should be supported by the device.

6. **Optional:** Click  to set the start date and end date of searching time period.
7. Start the VCA playback.

The VCA events occurred in the defined area will be red marked on the timeline.

Note

- By default, the playback speed of concerned video will be 1X, and the playback speed of unconcerned video will be 8X.
 - You can set to skip the unconcerned video during VCA playback in System Configuration and the unconcerned video won't be played during VCA playback. Refer to ***Set Live View and Playback Parameters*** for details.
-

8.7 Synchronous Playback



In synchronous playback, the video files can be played back in synchronization.

Perform this task when you need to play the video files in synchronization.

Steps

Note

Video files from up to 16 cameras can be played back simultaneously.

1. Enter the Remote Playback module.
2. Start playback of at least two cameras.
3. Click  in the toolbar to enable the synchronous playback.
The camera under playback will start synchronous playback.
4. Click  to disable the synchronous playback.

8.8 Fisheye Playback

You can play the video files of a fisheye camera in fisheye expansion mode.

Steps


Note

For other playback control instruction, refer to **Normal Playback** . Some icons may not be available for fisheye playback.

1. Enter the Remote Playback module.
 2. Select a fisheye camera to start playback.
-



Note

For detailed configuration about playback and playback control, refer to **Normal Playback** .

3. Enter the Fisheye Expansion mode.
 - Right-click on the display window and select **Fisheye Expansion**.
 - Click  in the toolbar. See **Set Icons Shown on Toolbar** for details about setting the toolbar.
-

Note

The mounting type in playback of fisheye expansion is set according to the mounting type in live view. For details, refer to **Perform Live View in Fisheye Mode**

 turns to .

4. Select the expanding mode for playback as you desired.
Fisheye

In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called **Fisheye** because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.

Panorama / Dual-180° Panorama / 360° Panorama

In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.

PTZ

The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.

Note

Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.

Half Sphere

By the half sphere mode, you can drag the image and rotate it centering on the diameter, in order to adjust the view to the desired angle.

AR Half Sphere

AR half sphere mode overlaps images far and near, so that you can view a dimensional image in a wide angle.

- 5. Optional:** Right-click on a playing window in the Fisheye view mode and you can switch the selected window to full-screen mode.

Note

You can right-click on the window and select **Quit Full Screen** to exit the full-screen mode.

8.9 Playback in Low Bandwidth

In situation of low network bandwidth, the speed of video streaming might be much slower due to the bandwidth limit. To provide normal quality in less streaming speed for low bandwidth users, the client provides playback in low bandwidth mode. Before that, you need to set the streaming protocol and perform other operations first.

For details about the settings, refer to ***How to get better performance of live view and playback when network bandwidth is low?*** .

Chapter 9 Download Video Footage

During playback, you can download the video files of one camera or multiple cameras to the local PC.

Note

- You cannot download the video files of Cloud P2P device.
 - For NVR which is added to the client by device's other user name (except admin), if **Double Verification** is enabled on this NVR, when playing back videos on the client, you are required to enter the user name and password created for double verification. For details about double verification, refer to the user manual of the NVR.
-

9.1 Download Video Footage by Date

During playback, you can download the video footage of the camera and save in the local PC.

Steps

1. Enter Remote Playback page and select a camera to start playback.

Note

For details about starting playback, refer to **Remote Playback** .

2. Right click on the image and click **Download**.
3. Set the start and end time of the video footage to download.
4. Enter a name for the video footage.
5. Click **OK** to start downloading the video footage to the local PC.

9.2 Download for Multiple Cameras


During the playback of multiple cameras, you can download the video files of multiple cameras by date simultaneously.

Steps

1. Enter Remote Playback page and select multiple cameras to start playback.

Note

For details about starting playback, refer to **Remote Playback** .

2. Click  to open the Download for Multiple Cameras window.
All the cameras in playback will be displayed.
3. Select the cameras you want to download video files for.
4. Set the start time and end time of video duration for each camera.

5. **Optional:** Check **Download Player** to download the player.
6. Click **Download** to start downloading the video files of the configured duration(s) to the local PC.

The progress bar shows the downloading process of each camera's video files.

7. **Optional:** Click **Stop** to stop downloading manually.



Note

Up to 16 cameras' video files can be downloaded simultaneously.

Chapter 10 Configure Video Event

Even if you are far away from the video device (cameras, alarm inputs and encoding devices, decoding devices), you can still know what happens and how urgent the event is by configuring linked actions of video event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of video devices in a batch at a time.

Steps

1. Click **Event Management** → **Video Event** to enter the video event configuration page.

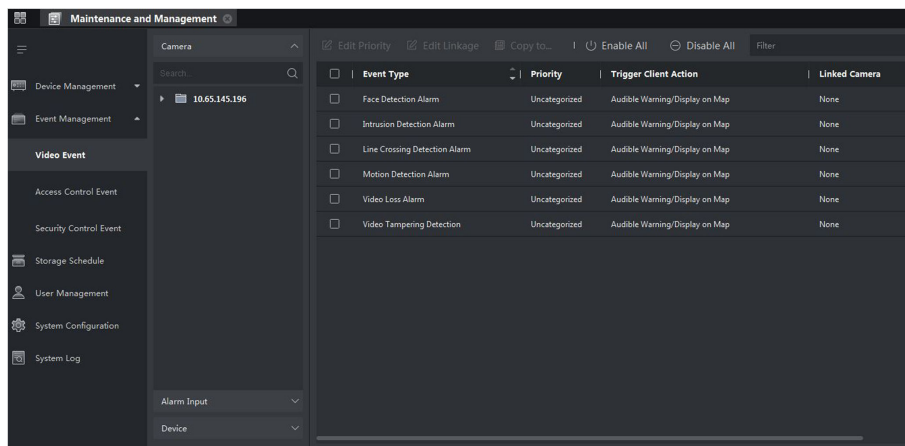


Figure 10-1 Video Event Configuration

2. On the left panel, select the event source type: **Camera**, **Alarm Input**, or **Device**, and then select the specific source in the device list.

Note

Make sure the device is online.

All the events supported by the selected device will be displayed.

3. **Optional:** Turn on the switch on the Enable column to enable the event, or click **Enable All** to enable all the events of this device.

Note

After enabled, the event can be received by the software client and trigger the linkage action(s).

4. **Optional:** Turn off the switch on the Enable column to disable this event, or Click **Disable All** to disable all the events of this device.

Note

After disabled, the event received by the software client can not trigger the linkage action(s).

5. **Optional:** Select the event(s), and then click **Edit Priority** to edit the priority of the event(s).

Note


Priority represents the emergency degree of the event.

6. Select the event(s), and then click **Edit Event Linkage** to edit the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click  to make an audition of the selected audio file.

Send Email


Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to **Set Email Parameters** .

Pop-up Window

Pop-up window to display the event related information (including event details, live video of the source camera, captured pictures of the linked camera, process record, and process field) on the software client when the event is triggered.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with  twinkling aside when the event is triggered, which helps to security guard to view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture picture when the event is triggered.

Select the camera in the drop-down list.

7. **Optional:** Select the event(s), and then click **Copy to** to copy the event settings of this device to other device(s).

Note

You can only copy the event settings to the device(s) with the same device type.

Chapter 11 Event Center

In the Event Center, you can view the real-time events, search the historical events and view the pop-up alarm information.

Before the client can receive the event information from the device, you need to arm the device first. For details, refer to *Enable Receiving Events from Devices* .

Before the you can view the pop-up alarm information, you need to enable alarm triggered pop-up image in the event center. For details, refer to *View Pop-up Alarm Information* .

11.1 Enable Receiving Events from Devices

Before the client can receive the event information from the device, you need to arm the device first.

Steps

1. Click  → **Tool** → **Device Arming Control** open Device Arming Control page.

All the added devices display on this page.

2. In the Operation column, turn on the switch to enable auto-arming, or click **Arm All** to arm all the devices.

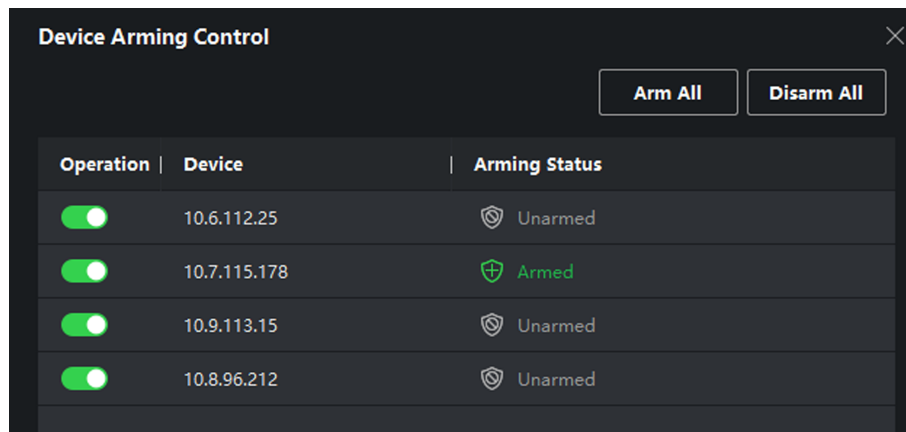


Figure 11-1 Device Arming Control

3. View the arming status of each device in the Arming Status column.

Result

The events of armed device(s) are automatically uploaded to the client when the event is triggered.

11.2 View Real-Time Events

In the Real-time Event module of the event center page, you can view the real-time event information, including event source, event time, priority, event key words, etc.

Before You Start

Enable receiving events from devices before the client can receive event information from the device, see *Enable Receiving Events from Devices* for details.

Steps

1. Click **Event Center** → **Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

Event Time

For video device, event time is the client time when it receives the event. For none-video device, event time is the time when the event is triggered.

2. Set the filter conditions or enter the event key word in the Filter text field to display the required events only.

Device Type

The type of device that occurred the event.

Priority

The priority of the event that indicates the urgent degree of the event.

3. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.
4. View the event information details.
 - 1) Select an event in the event list.
 - 2) Click **Expand** in the right-lower corner of the page.
 - 3) View the related picture, detail description and handing records of the event.
 - 4) **Optional:** Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.
5. **Optional:** Perform the following operations if necessary.

Handle Single Event

Click **Handle** to enter the processing suggestion, and then click **Commit**.

Note

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

Handle Events in a Batch

Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **Commit**.

- Enable/Disable Alarm Audio** Click **Enable Audio/Disable Audio** to enable/disable the audio of the event.
- Select the Latest Event Automatically** Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.
- Clear Events** Click **Clear** to clear the all the events in the event list.
- Send Email** Select an event and then click **Send Email**, and the information details of this event will be sent by email.

 **Note**

You should configure the email parameters first, see **Set Email Parameters** for details.

11.3 Search Historical Events

In the Event Search module of the event center page, you can search the historical events via time, device type, and other conditions according to the specified device type, and then process the events.

Before You Start

Enable receiving events from devices before the client can receive event information from the device, see **Enable Receiving Events from Devices** for details.

Steps

1. Click **Event Center** → **Event Search** to enter the event search page.

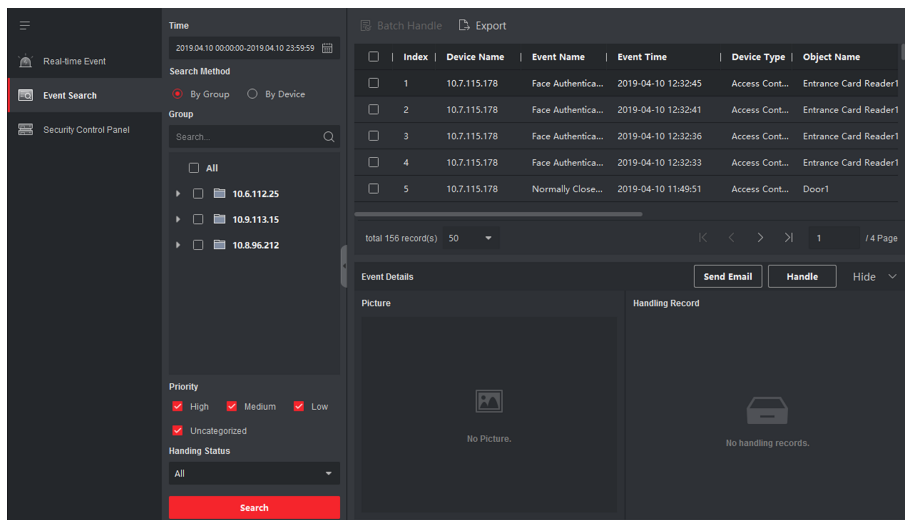


Figure 11-2 Search History Event

2. Set the filter conditions to display the required events only.

Time

The client time when the event starts.

Search by

Group: Search the events occurred on the resources in the selected group.

Device: Search the events occurred on the selected device.

Device Type

The type of device that occurred the event.

All

All the device types, and you can set the following filter conditions: group, priority, and status.

Security Control Panel

For the events of security control panel, you can set the following filter conditions: device, priority, acknowledgement status and event type.

Video Intercom

For the events of video intercom, you need to select searching scope: All Record and Only Unlocking.

- **All Records:** You can filter the events from all the video intercom events, and you need to set the following filter conditions: device, priority, status.
- **Only Unlocking:** You can filter the events from all the video intercom unlocking events, and you need to set the following filter conditions: device, unlocking type.

Access Control

For the events of access control, you can set the following filter conditions: device, priority, status, event type, card reader type, person name, card no., organization.



Note

Click **Show More** to set the event type, card reader type, person name, card no., organization.

Group

The group of the device that occurred the event. You should set the group as condition only when you select the Device Type as **All**.

Device

The device that occurred the event.

Priority

The priority including low, medium, high and uncategorized which indicates the urgent degree of the event.

Status

The handling status of the event.

3. Click **Search** to search the events according the conditions you set.

4. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.

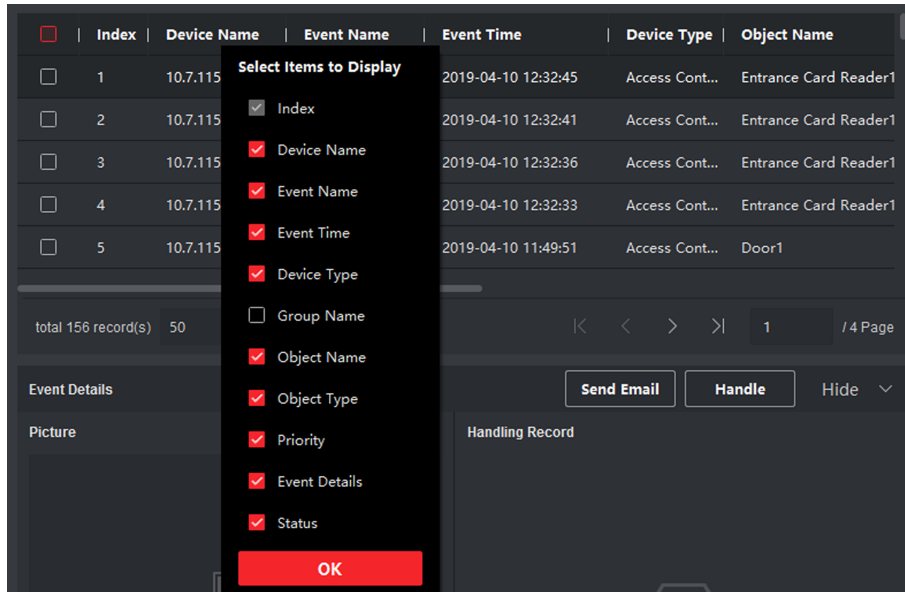


Figure 11-3 Customize Event Related Items to be Displayed

5. **Optional:** Handle the event(s).
- Handle single event: Select one event that need to be processed, and then click **Handle** in the event information details page, and enter the processing suggestion.
 - Handle events in a batch: Select the events which need to be processed, and then click **Handle in Batch**, and enter the processing suggestion.

 **Note**

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

6. **Optional:** Select an event and then click **Send Email**, and the information details of this event will be sent by email.

 **Note**

You should configure the email parameters first, see **Set Email Parameters** for details.

7. **Optional:** Click **Export** to export the event log or event pictures to the local PC in CSV format. You can set the saving path manually.
8. Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

11.4 View Pop-up Alarm Information

For the alarm configured with pop-up image, the alarm videos and pictures can display on a pop-up window when the corresponding alarm is triggered.

Before You Start

Configure the alarm linkage action as Alarm Triggered Pop-up Image.

Steps

1. Click **Event Center** on the control panel to enter the event center.
2. Click **Real-Time Event** on the left panel.
3. Click **Enable Alarm Triggered Pop-up Image** to enable alarm triggered pop-up function.
4. Trigger the alarm.

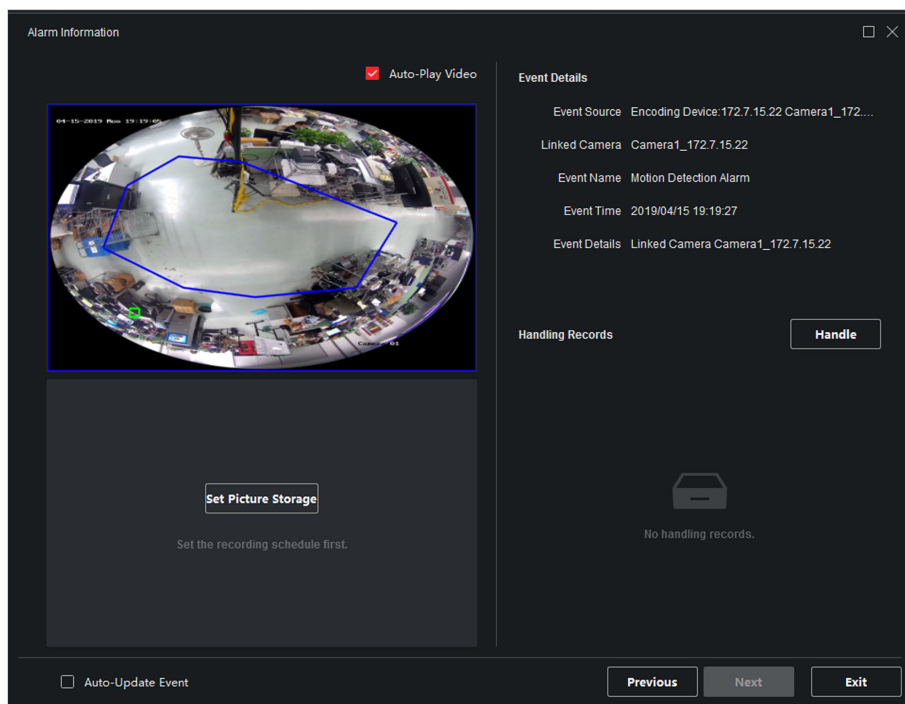



Figure 11-4 Result


A window, showing the alarm video, alarm picture, and alarm details, will pop up.


5. Perform the following operation(s) after popping up the image.

View Alarm Video

You can view the live video of the camera configured in Camera Linkage.

Move the cursor over the video and click  to view instant playback to see what happens when the alarm is triggered.

Click  to capture a picture of the live video and save the snapshot on the PC running the client.

Click  to record the live video and save the recorded video footage on the PC running the client.

Right-click on the alarm video to perform other operations. For details, refer to **Live View** .

View Alarm Picture The alarm picture captured by the camera configured in Camera Linkage will display on the field below the alarm video.

View Previous or Next Alarm Click **Prev Page** or **Next Page** to view the previous or next alarm information.

Handle Alarm For the first time to handle the alarm, click **Handle** to enter the handling suggestion.

For the handled alarm, click **Add Remark** to add more the handling suggestions.

Chapter 12 Map Management

The E-map function gives a visual overview of the locations and distributions of the installed cameras and alarm input devices. You can get the live view of the cameras on the map, and you will get a notification message from the map when alarm is triggered.

E-map is a static image (it do not have to be geographical maps, although they often are. Depending on your organization's needs, photos and other kinds of image files can also be used as e-maps) which gives you a visual overview of the locations and distributions of the hot spots (resources (e.g., camera, alarm input) placed on the map are called hot spots). You can see the physical locations of the cameras and alarm inputs, and in what direction the cameras are pointing. With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

12.1 Add Map

You should add a map as the parent map for the hot spots and hot regions.

Steps

 **Note**

Only one map can be added to one group.

1. Open the E-map page.
 2. Select a group for which you want to add a map.
-

 **Note**

For details about setting the group, refer to *Group Management* .

3. Click **Add Map** to open the map adding window.
 4. Enter a descriptive name of the added map.
 5. Select a map picture from the local path.
-

 **Note**

The picture format of the map can only be PNG, JPEG or BMP.

6. Click **OK**.
7. **Optional:** Perform the following tasks after adding the map.

Zoom in/out	Use the mouse wheel or click + or - to zoom in or zoom out on the map.
Adjust Map Area	Drag the yellow window in the lower-right corner or use the direction buttons and zoom bar to adjust the map area for view.

12.2 Edit Map Scale

The scale of a map is the ratio of a distance on the map to the corresponding distance on the ground. The client can calculate two locations' distance on the map according to the distance on the ground. An accurate map scale is essential for defining radar's monitoring range.

Before You Start

Make sure you have added a map. See **Add Map** for details.

Perform this task if you need to add a security radar to the map.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Edit Scale** to select two locations on the map.

The cursor will turn to  if you hover it on the map.



Figure 12-1 Edit Map Scale

4. Click on the map to select two locations.
The Edit Scale window pops up.
5. Enter the ground distance between the two locations, and then click **OK**.
The client will calculate the map scale automatically.

12.3 Manage Hot Spot

The devices added to the map are called hot spots. The hot spots show the locations of the devices, and you can also get the live view or alarm information of the surveillance scenarios

through the hot spots. The devices can be added to the map as hot spots includes: camera, alarm input/output, access point, security radar, and zone.

12.3.1 Add Camera as Hot Spot

You can add cameras to the map as hot spots.

Before You Start

Make sure you have added an e-map and a camera to the client. See **Add Map** and **Device Management** for details.

Steps

1. Enter the E-map page.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Click **Add Hot Spot** → **Camera Hot Spot** to open the Add Hot Spot window.

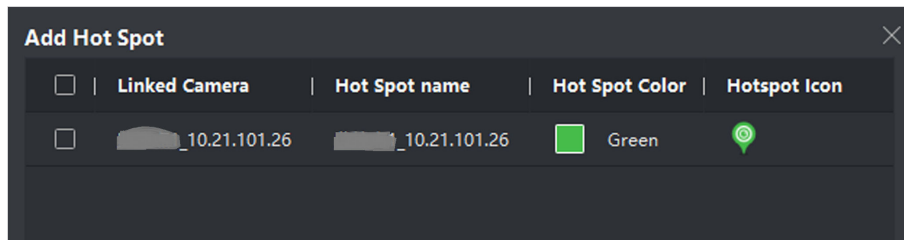


Figure 12-2 Add Hot Spot Panel

4. Select the cameras to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color and select the hot spot icon.
6. Click **OK** to save the settings.

Note

You can also drag the camera icons from the group list to the map directly to add the hot spots.

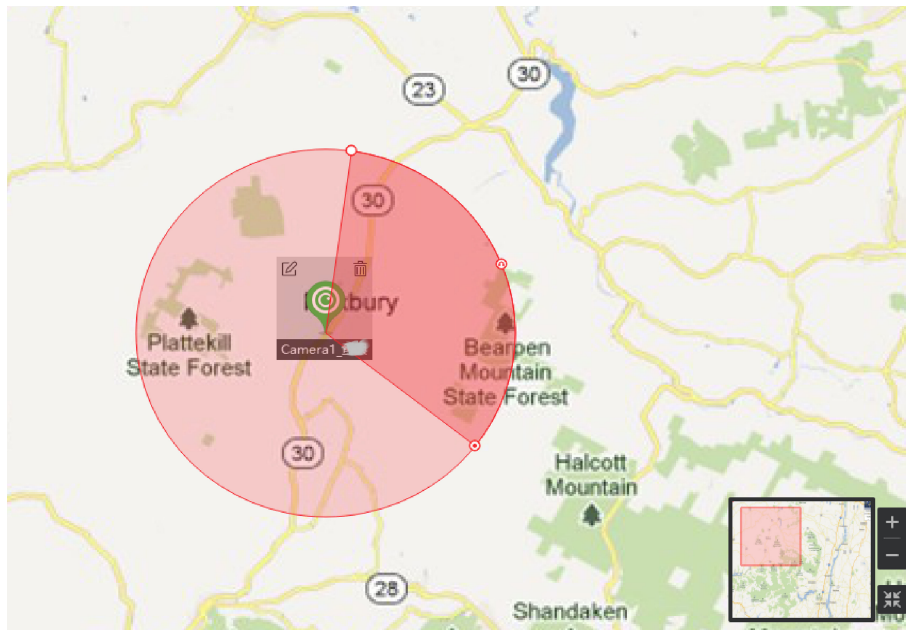







Figure 12-3 Camera on the Map

The camera icons are added on the map as hot spots and the icons of the added cameras in the group list change from  to . The sector indicates the camera's field of view.

7. Perform the following operation(s).

- Move the Hot Spot** Drag the hot spot to move it to a certain position.
- Change the FOV Angle** Drag  /  and revolve to change the camera's field of view.
- Change the FOV Size** Drag  to change the FOV size.

12.3.2 Add Alarm Input as Hot Spot

You can add the alarm inputs to the map as hot spots.

Steps

1. Enter the E-map module.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Click **Add Hot Spot** → **Alarm Input Hot Spot** to open the Add Hot Spot window.
4. Select the alarm inputs to be added to the map.
5. **Optional:** Edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK**.

Note

You can also drag the alarm input icons from the group list to the map directly to add the hot spot.

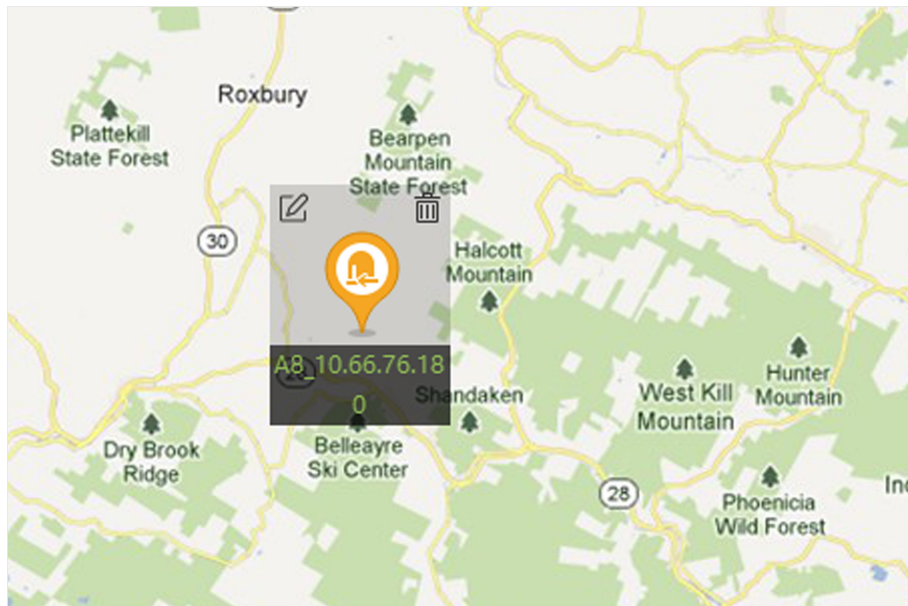




Figure 12-4 Alarm Input on the Map

The alarm input icons are added to the map as hot spots and the icons of the added alarm inputs in the group list change from  to .

7. Optional: Drag the hot spot to move it to a certain position.

12.3.3 Add Alarm Output as Hot Spot

You can add alarm outputs to the map as hot spots for management. After that, you can enable or disable it in a quick manner. If you enable an alarm output on the map, the security control devices (e.g. sirens, bells) connected to it will alarm for attention.

Before You Start

Make sure you have added an e-map and alarm output to the client. See **Add Map** and **Device Management** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot** → **Alarm Output Hot Spot** to open the Add Hot Spot panel.



Figure 12-5 Add Hot Spot Panel

4. Select the alarm output to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

 **Note**

You can also drag an alarm output icon from the alarm output list to the map to add the hot spot.

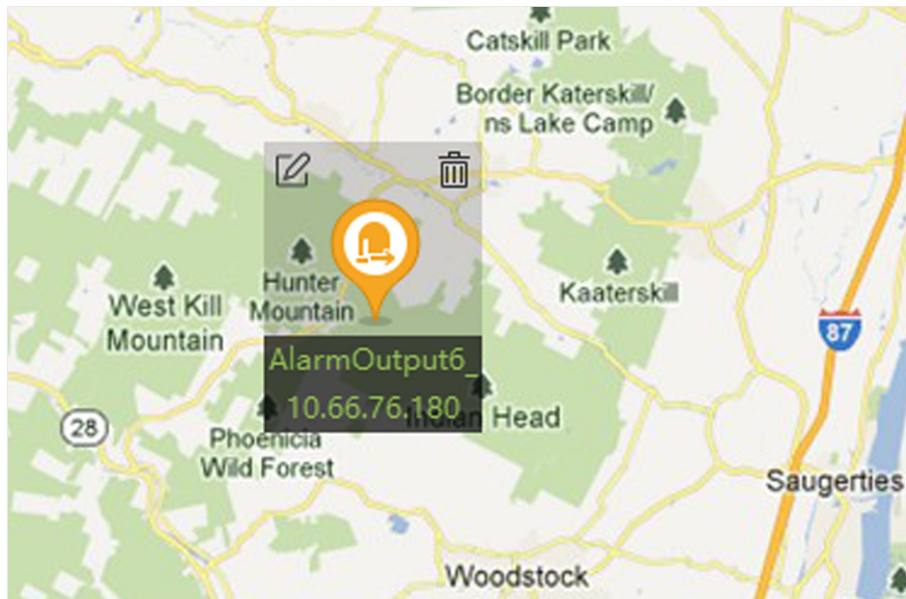




Figure 12-6 Alarm Output on the Map

The alarm output is added to the map as a hot spot and its icon in the group list changes from  to .

7. **Optional:** Drag the alarm output to move it to a certain position.

12.3.4 Add Zone as Hot Spot

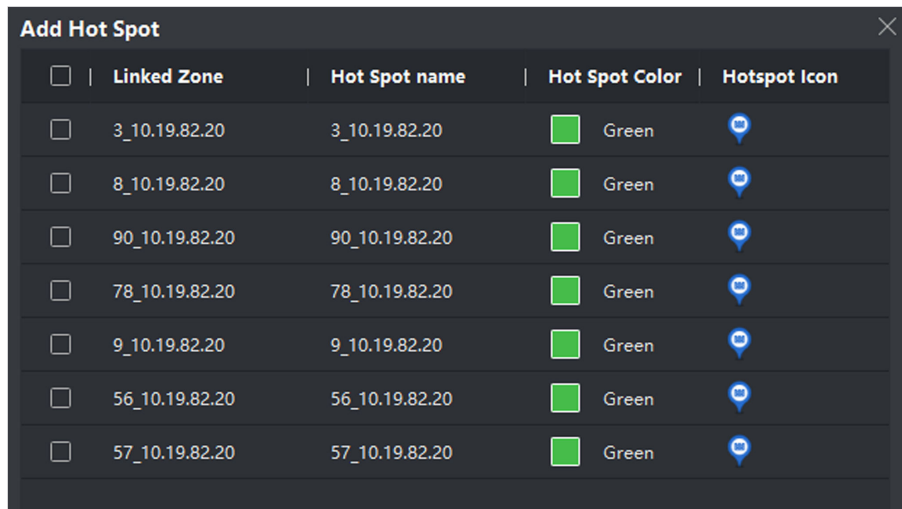
You can add zones to the map so that you can quickly locate the zone when an alarm is triggered.

Before You Start

Make sure you have added a map and zone to the client. See **Add Map** and **Add Device** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot** → **Zone Hot Spot** to open the Add Hot Spot panel.

















<input type="checkbox"/>	Linked Zone	Hot Spot name	Hot Spot Color	Hotspot Icon
<input type="checkbox"/>	3_10.19.82.20	3_10.19.82.20	 Green	
<input type="checkbox"/>	8_10.19.82.20	8_10.19.82.20	 Green	
<input type="checkbox"/>	90_10.19.82.20	90_10.19.82.20	 Green	
<input type="checkbox"/>	78_10.19.82.20	78_10.19.82.20	 Green	
<input type="checkbox"/>	9_10.19.82.20	9_10.19.82.20	 Green	
<input type="checkbox"/>	56_10.19.82.20	56_10.19.82.20	 Green	
<input type="checkbox"/>	57_10.19.82.20	57_10.19.82.20	 Green	

Figure 12-7 Add Hot Spot Panel

4. Select the zone(s) to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

 **Note**

You can also drag the alarm output icons from the alarm output list to the map to add the hot spot.

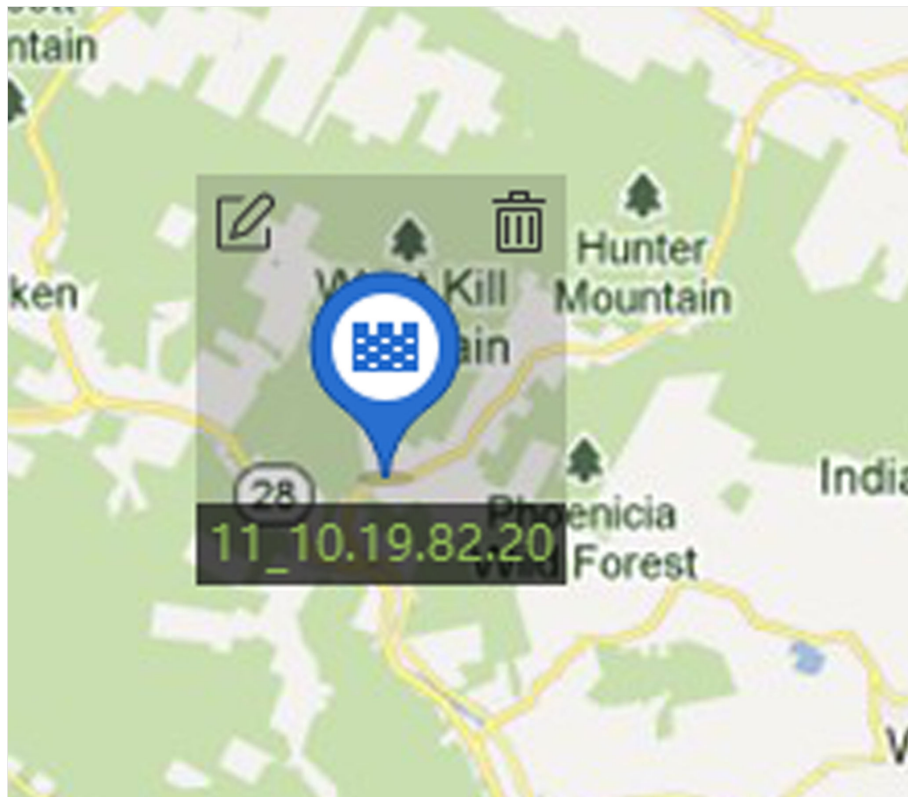




Figure 12-8 Zone on the Map

The zone is added to the map as a hot spot and its icon in the group list changes from  to .

7. Optional: Drag the zone hot spot to move it to a certain position.

When alarms are triggered, the number of the newest alarms will be displayed on the zone's icon. You can click the number to see the alarms details.

 **Note**

No more than 10 newest alarms can be displayed.

8. Optional: Click **Clear Alarms** to mark the alarms of the zones on the current map as read.

12.3.5 Add Security Radar as Hot Spot

For an effective monitoring, you can add a security radar to the map as a hot spot and paint zones in its monitoring filed. So that when someone intrudes the zone, an alarm will be triggered for attention.

Before You Start

Make sure you have added an e-map and a security radar to the client. See **Add Map** and **Device Management** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. **Optional:** Edit map scale. See **Edit Map Scale** .
4. Select a security radar in the device list and drag it to the map.

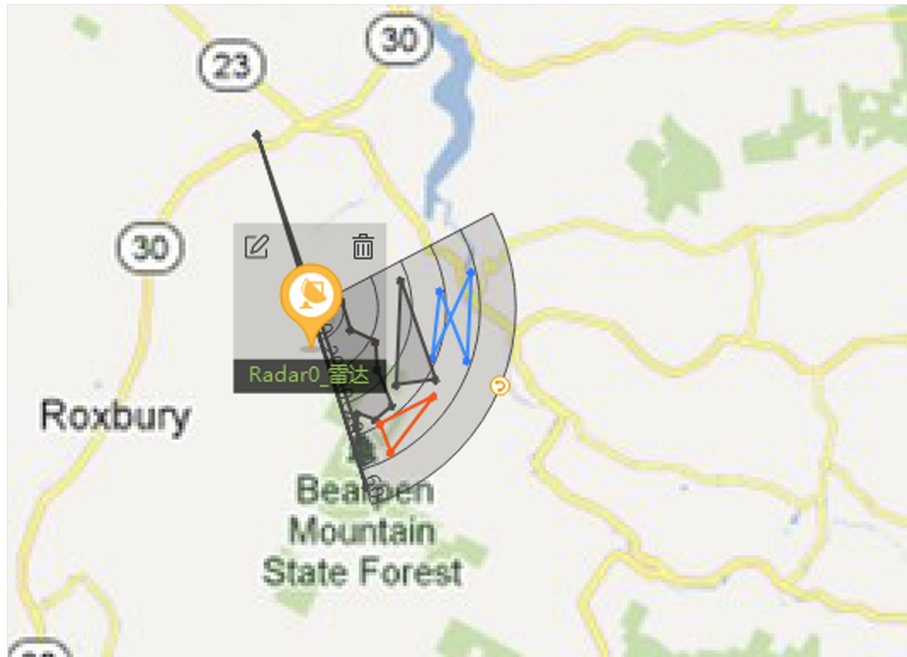





Figure 12-9 Radar on the Map

5. **Optional:** Click the added radar and then click  to edit the hot spot name, select the hot spot color, and select the hot spot icon.
6. Click **OK**.

The security radar is added to the map as a hot spot and its icon in the group list changes from  to . The sector indicates the monitoring field of the radar.

 **Note**

- Orange sector indicates an armed radar, while black sector indicates a disarmed radar.
- Red point indicates the detected intruder.

7. Add zone to the monitoring field of the security radar.

 **Note**

Make sure the security radar is disarmed.

- 1) Click **Edit** → **Add Radar Zone** to start painting a zone.
- 2) **Optional:** Switch the **Field Assistance** on to enable zone painting assistance function.

Example

Person A takes an on-site walk in the field which needs to be painted as a zone, which will be indicated as a moving pattern consists with red points and dashed lines. And then Person B paints a zone on the map according to the moving pattern.

- 3) Click in the sector to paint a zone and right-click to complete painting.

Zone Settings window pops up.

- 4) Enter a zone name and select a zone type.

Warning Zone

Defined by red line. If someone intrudes the warning zone, an alarm will be triggered with the whole zone turning to red. And the intruder's location and moving pattern will be displayed with a red point connected by a red dashed line. Only if the intruder goes out of the zone, the zone restores.

Pre-Warning Zone

Defined by blue line. If someone intrudes the warning zone, an alarm will be triggered and you can view the event details in the Event Center.

Disabled Zone

Defined by purple line. If someone intrudes the warning zone, no alarm will be triggered, and moving pattern will not be displayed.

- 5) **Optional:** Edit a zone: double-click a zone to enter editing mode of the zone (a dashed-line frame will be displayed around the zone). Hover the cursor on the edge of the zone to show a blue +, click to add a point for the zone. Drag a point to change the zone. Click any other place to quit editing mode.

8. **Optional:** Drag the security radar to move it to a certain position.

12.3.6 Add Access Point as Hot Spot

You can add access points to the map as hot spots, so that you can find the hot spots and view their status and alarm numbers.

Before You Start

Make sure you have added a map and an access point to the client. See **Add Map** and **Add Device** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot** → **Access Point Hot Spot** to open the Add Hot Spot window.

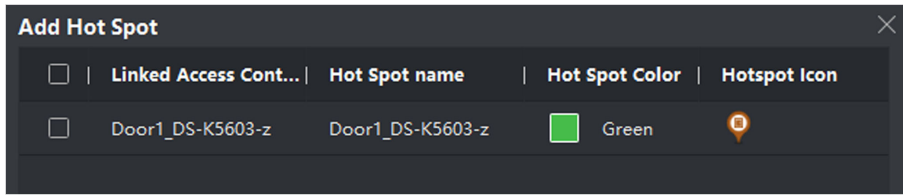


Figure 12-10 Add Hot Spot Panel

4. Select the access point(s) to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

 **Note**

You can also drag an access point icon from the access point list to the map.

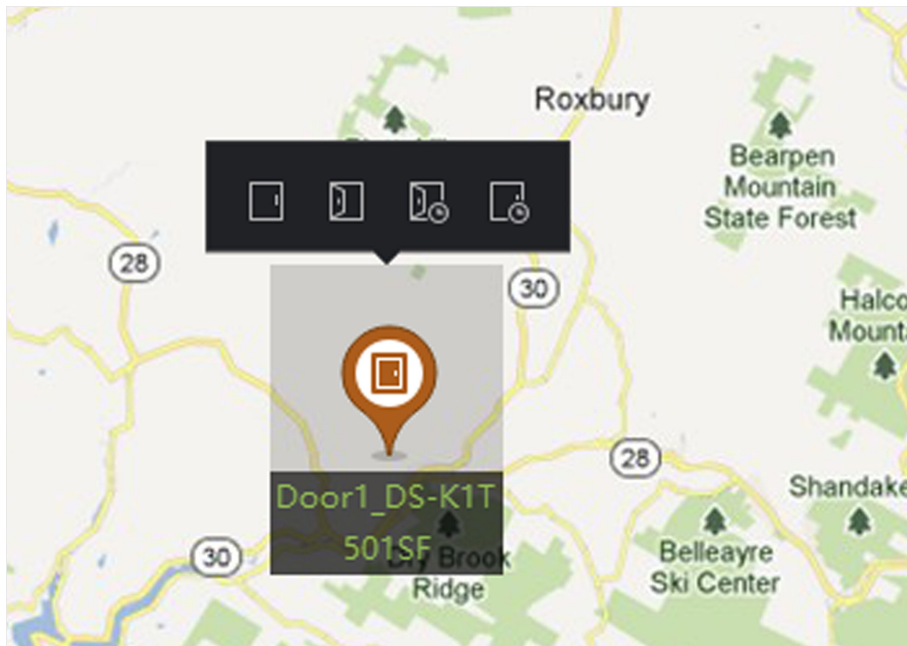




Figure 12-11 Access Point on the Map

The access point is added to the map as a hot spot and its icon in the group list changes from  to .

7. **Optional:** Drag the access point hot spot to move it to a certain position.
When alarms are triggered, the number of the newest alarms will be displayed on the hot spot icon. You can click the number to see the alarms details.



 **Note**

No more than 10 newest alarms can be displayed.

12.3.7 Edit Hot Spot

You can edit the information of the added hot spots on the map, including the name, the color, the icon, etc.

Steps

1. Enter the E-map module.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Select the hot spot icon on the map and then click  to open the Edit Hot Spot window.
4. Edit the hot spot name in the text field, select the hot spot name's color and hot spot icon shown on the map.
5. Check **Apply to Other Camera Hot Spots/Apply to Other Alarm Input Hot Spots/Apply to Other Alarm Output Hot Spots/Apply to Other Zone Hot Spots** to apply the color and icon settings to other hot spots.
6. Click **OK**.
7. **Optional:** Select the hot spot icon and click  to delete the hot spot.

12.3.8 Preview Hot Spot

After adding hot spots (including camera, alarm input/output, zone, security radar, and zone) to the map, you can view the live view of the camera hot spot and the triggered alarm information of all the types of hot spots on the map.

Before You Start

Make sure you have added hot spots to the map. See *Manage Hot Spot* for details.

Steps

1. Enter the E-map module.

Note

If you are in the editing map mode, click **Exit** on the upper-right corner to enter the map preview mode.

2. Click **Display** to show the hot spots on the map.

Note

Hot spot type with  will be shown on the map.

3. Click a hot spot to perform the following operation(s).

Hot Spot Type	Operations
---------------	------------

Camera	Live View: Click  to pop up the live view window of the camera.
--------	--

 **Note**

- When an alarm is triggered during live view, the client will play a video file of 30 s first.
 - You can capture, start recording and instant playback during live view.
-

Alarm Output

Click an alarm output, and select **Open/Close**.

 **Note**

The security control channels managed by the alarm output will also be opened/closed.

Access Point

View door status: the current door status of the access point is displayed on the icon. Click the icon to switch the door status.

Open Door

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Close Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Open

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Closed

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Security Radar

Arm/Disarm zones in the monitoring field of the radar: After exiting editing, click the icon of a security radar, and then select **Arm/Disarm**.

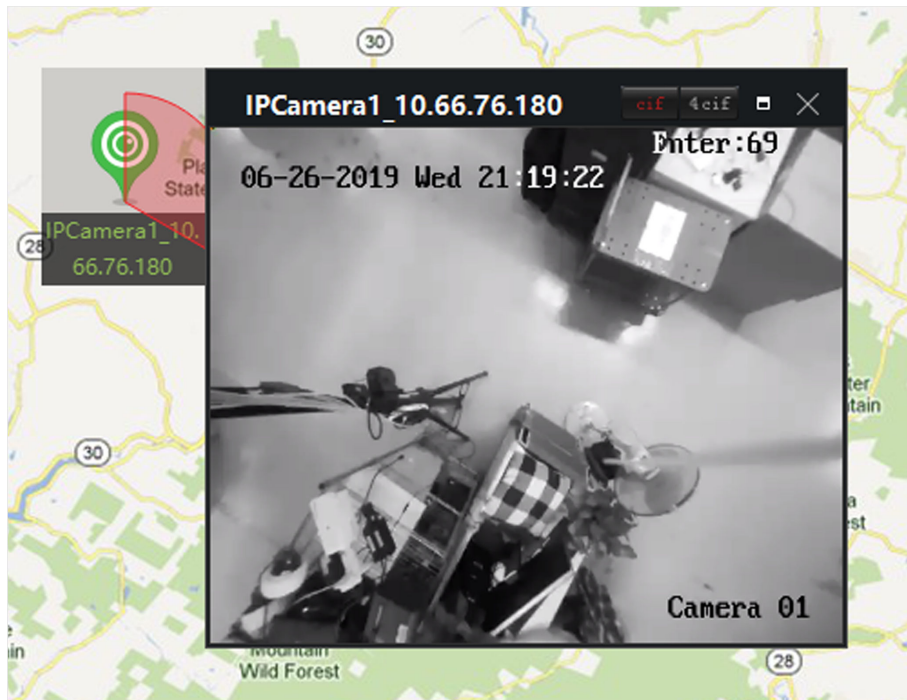


Figure 12-12 Live View of Camera on the Map

4. Optional: Perform the following operation(s).

View Alarm Information

Click the alarm number on a hot spot icon to open the alarm information page to view the alarm type and triggering time.

Clear Alarm

Click **Clear Alarm** on the top of the map to mark all the alarms of the hot spot as read.

View Multiple Cameras' Live View on the Map

- a. Click **Live View** to show 4 small windows on the bottom of the client.
- b. Drag a camera from the device list to a window to start the live view.

 **Note**

Up to 4 cameras' live view is supported at the same time.

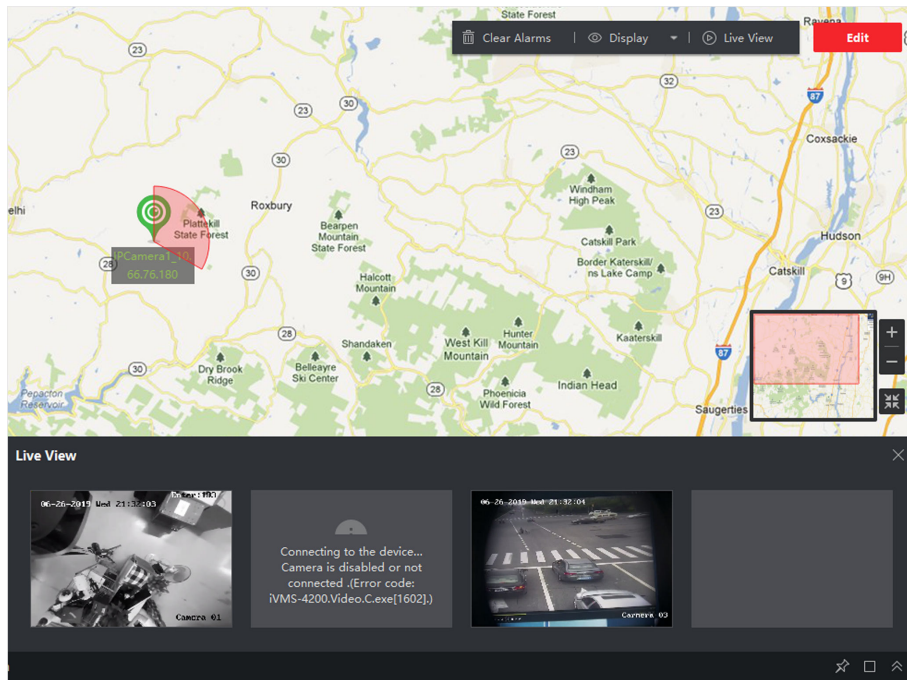


Figure 12-13 Preview Camera Hot Spot

12.4 Manage Hot Region

The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

After linking a child map to a parent map, a hot region icon will display on the parent map. You can click it to enter the child map to view the resources on the child map for convenience.

With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

12.4.1 Add Hot Region

You can add a map to another map as a hot region and an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Before You Start

At least two maps should be added. Refer to **Add Map** for details about adding maps.

Steps

Note

A map can only be added as the hot region for once.


1. Enter the E-map page.
2. Click **Edit** on the upper-right corner to enter the map editing mode.
3. Select an added map as the parent map.
4. Click **Add Hot Region** to open the Add Hot Region window.
5. Select the child map.
6. **Optional:** Edit the hot region name, and select the hot region color and icon by double-clicking the corresponding field.
7. Click **OK**.

The child map icons are added on the parent map as the hot regions.

12.4.2 Edit Hot Region

You can edit the information of the hot regions on the parent map, including name, color, icon, etc.

Steps

1. Enter the E-map module.
2. Click **Edit** on the upper-right corner to enter the map editing mode.
3. Select a hot region icon on the parent map and click  to open the Edit Hot Region window.
4. Edit the hot region name in the text field, select the hot region name's color and hot region icon.
5. Check **Apply to Other Hot Regions** to apply the color and icon settings to other hot regions.
6. Click **OK**.

12.4.3 Preview Hot Region

After adding a hot region, you can click the hot region icon on the parent map to enter the child map. You can view the resources and alarms on the child map.

Steps

1. Enter the E-map page.

Note

If you are in the editing map mode, click **Exit** on the upper-right corner to enter the map preview mode.

2. Click the hot region icon on the parent map to enter the linked child map.
You can view the resources on the child map. If there is any alarm triggered on the child map, you can view the alarm details.
3. **Optional:** Click **Back to Parent Map** on the upper-left corner to go back to the parent map.

- 4. Optional:** Click **Clear Alarm Info.** on the upper-right corner to clear the alarm information triggered by the resources on the current map.

Chapter 13 Forward Video Stream through Stream Media Server

There is always a limit of the device remote access number. When there are many users wanting to get remote access to the device to get the live view, you can add the stream media server and get the video data stream from the stream media server, thus to lower the load of the device.

Note



The stream media server application software needs to be installed and it is packed in the client installation package. After running the installation package, check **Stream Media Server** to enable the installation of stream media server.

13.1 Import Certificate to Stream Media Server

Before adding the stream media server to the client, you should import the client's security certificate to the stream media server first to perform security authentication and ensure data security.

Perform the following steps to import the security certificate to the stream media server.

Steps

1. Export the certificate from the client.
 - 1) Open client service.
 - 2) Click **Export**.
2. Copy the certificate to the PC which has installed with stream media server.
3. Click  on the desktop of the PC installed with stream media server to run it.
4. Import the certificate to the stream media server.
 - 1) Right click  on the task bar and click **Display**.
 - 2) Click **Configuration** to enter the Configuration window.
 - 3) In the security certificate field, click **Import** and select the certificate file you export from client in Step 1.
 - 4) Click **OK**.
5. Restart the stream media server to take effect.

Note

If the client's security certificate is updated, you should export the new certificate from the client and import it to the stream media server again to update.


13.2 Add Stream Media Server by IP Address

You can add stream media server by IP address one by one.

Steps



For one client, up to 16 stream media servers can be added.

1. Click  on the desktop to run the stream media server.



- You can also forward the video through the stream media server installed on other PC.
 - If the stream media server port (value: 554) is occupied by other service, a dialog box will pop up. You should change the port No. to other value to ensure the proper running of the stream media server.
-

2. In the client software, enter the Device Management page.
 3. Enter **Device → Stream Media Server**
 4. Click **Add** to open the Add window.
 5. Select **IP Address** as the adding mode.
 6. Enter the nickname and IP address of the stream media server.
-



The default port value is 554.

7. Finish adding the stream media server.
 - Click **Add** to add the server and back to the list page.
 - Click **Add and Continue** to save the settings and continue to add other server.
-




If the added Stream Media Server's security certificate doesn't match with the client's, it will prompt you. You can view exception message and follow the provided steps to keep certificates consistent.

13.3 Add Cameras to Stream Media Server to Forward Video Stream

To get the video stream of a camera via stream media server, you need to connect the camera to the stream media server.

Steps

1. Enter the Device Management module.
2. Enter **Device → Stream Media Server**

3. Select a server and click  on Operation column to open Stream Media Server Settings window.
4. Select the cameras of which the video stream is to be forwarded via the stream media server.
5. Click **OK**.
6. Go the Main View page and start the live view of the cameras again.

On the stream media server control panel, check the channel number of the video stream forwarded through or sent from the stream media server.

 **Note**

- For one stream media server, up to 64 channels of video stream can be forwarded through it and up to 200 channels of video stream can be sent to clients from it.
 - If the camera is offline, the client can still get the live video via the stream media server.
-

Chapter 14 Statistics

Reports, created for a specified period, are essential documents, which are used to check whether a business runs smoothly and effectively. In this software, reports can be generated daily, weekly, monthly, annually, and by custom time period. You can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc.

14.1 People Counting Report

People counting statistics is to calculate the number of line crossing people in a specific area and a certain time period by the people counting camera(s), which can help the storekeeper to analyze the customers flow and number in different time, and the storekeeper can flexibly do some business adjustment according to the report. You can view the people counting statistics in a line chart or histogram, and generate reports for exporting the detailed data to local storage.

Before You Start

Add a people counting device to the software and properly configure the corresponding area. The added device should have been configured with people counting rule. Refer to **Add Device** for details about adding people counting device.

Steps

1. Click **Report** → **People Counting** to enter People Counting page.
2. Select daily report, weekly report, monthly report, or annual report as the report type.

Daily Report

Daily report shows data on a daily basis. The system will calculate the number of people in a each hour of one day.

Weekly Report, Monthly Report and Annual Report

As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the number of people in each day of one week, in each day of one month, in each month of one year.

3. Select the statistics time type and click  to set the time.

One Period

Generate the statistics in one time period.

Multiple Periods

Generate the statistics in two time periods, which can help you to compare the people flow and number in two time periods.

For example, if you set the report type as month report, and set the March and April as the statistic time, the people counting results in March and April will be displayed in a same chart with different color, and you can compare the data in different day of each month.

4. On the upper-right corner of the page, select **Display by Device** or **Display by Camera**.

Display by Device

Display the report by device.

For example, if you select one NVR (with 4 people counting cameras), the report will display the total number of people summed by the 4 people counting cameras.

Display by Camera

Display the report by camera.

For example, if you select one NVR (with 4 people counting cameras), the report will display the each camera's statistics respectively, namely display the statistics in 4/8 colors (each/2 color represent one camera).

5. On the upper-right corner of the page, select **Display by Device** or **Display by Camera**.

Display by Device

Display the report by device.

You can select only one device with multiple people counting cameras inside, or select only one people counting camera to be displayed.

For example, if you select one NVR with 2 people counting cameras inside, the report will display the total number of people summed by the 2 cameras.

Display by Camera

Display the report by camera.

You can only select one people counting camera to be displayed.

6. Select the people counting camera(s) to be displayed.

7. Select the direction for statistics.

Entered

The people entered will be counted.

Exited

The people exited will be counted.

Passed

Both people entered and exited will be counted.

8. Click **Search** to get the people counting statistics and detailed data for each hour, day, or month.

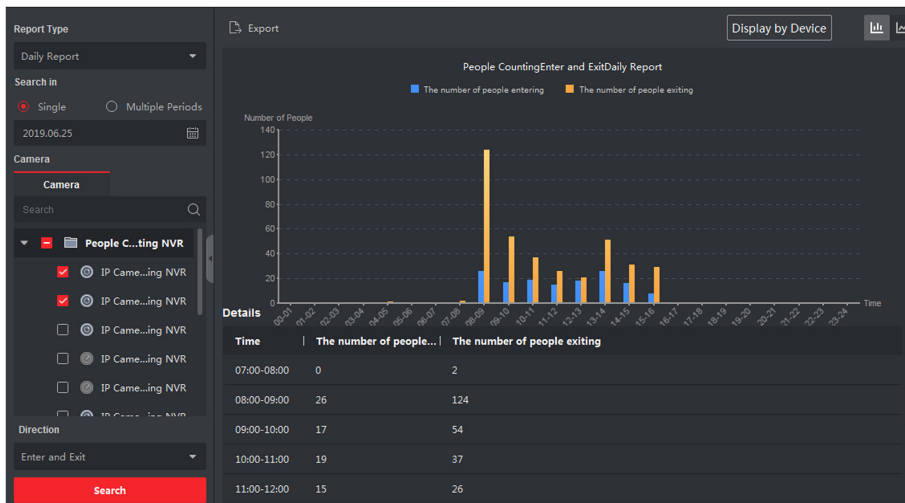


Figure 14-1 Display by Device

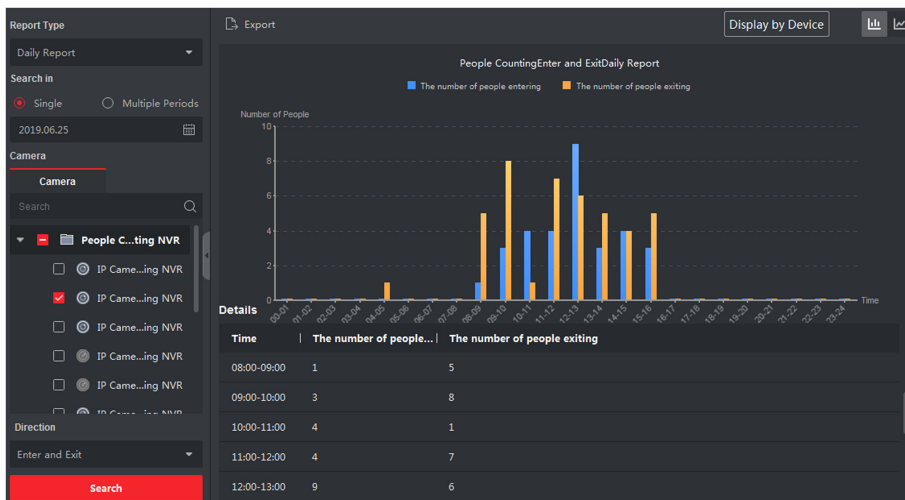


Figure 14-2 Display by Camera

By default, the statistics are shown in histogram form.

9. Optional: Perform the following operations after search.

Switch to Line Chart Click  to switch it to line chart.

 **Note**

By default, the statistics are shown in bar chart.

Switch to Bar Chart Click  to switch it to bar chart.

Save to Local PC Click **Export** to save the detailed data of people counting to your PC.

14.2 View People Counting in Intersections Report

Intersection analysis is used to monitor people flow and number in an intersection-like scene. The arrows in the image refer to different directions. By selecting one direction (e.g. A) as the entrance, the other directions will be set as the exits by default, so that multiple paths are generated (e.g., A to A, A to B, A to C, and A to D). You can view the people counting who passed by each path, respectively, which can help the shopkeeper to analyze the people flow in different door. The statistics result can show in daily, weekly, monthly, and annual report.

Before You Start

Make sure a fisheye camera which supports intersection analysis function has been configured properly and be added to the software. Refer to **Add Device** for details about adding the device.

Steps



Up to 10 intersections can be analyzed.

1. Click **Report** → **Intersection Analysis** to enter the intersection analysis module.
2. Select daily report, weekly report, monthly report, or annual report as the report type.

Daily Report

Daily report shows data on a daily basis. The system will calculate the number of people in intersection report in a each hour of one day.

Weekly Report, Monthly Report and Annual Report

As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the number of people in intersection report in each day of one week, in each day of one month, in each month of one year.

3. Set the start time for the report.
4. Select the camera for generating the report.
5. Select one direction as the entrance from the drop-down list in the **Flow in** filed.
6. Click **Search** to get the statistics result.

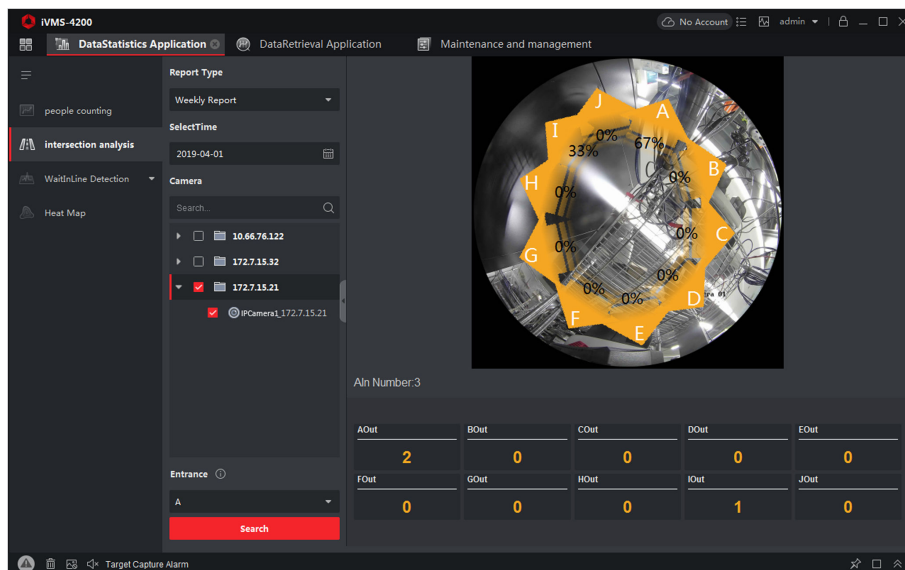


Figure 14-3 Results

The people number for each path will show on the right.

14.3 Queue Management

Queue management supports data analysis and report output from multiple dimensions.

Commonly Used Data Analysis

- To see queuing-up people number of a certain waiting time level in a queue/region, use queuing-up time analysis, check a target region and set a waiting time level.
- To compare queuing-up people number of a certain waiting time level in multiple queues/regions, use queuing-up time analysis, check target regions and set a waiting time level.
- To compare queuing-up people number of different waiting time levels in multiple queues/regions, use queuing-up time analysis, check target regions and set waiting time levels.
- To see the time and duration that a queue stays a certain length in a queue/region, use queue status analysis, check a target region and set a queue length level.
- To compare the time and duration that a queue stays a certain length in multiple queues/regions, use queue status analysis, check target regions and set a queue length level.
- To compare the time and duration that a queue stays at different length in multiple queues/regions, use queue status analysis, check target regions and set queue length levels.

14.3.1 Queuing-Up Time Analysis

Queuing-Up Time Analysis calculates people number of different waiting time levels. Regional comparison and multiple waiting time level comparison are supported.

Compare Queuing-up People Amount for Different Regions

You can search the queuing-up people amount for a certain waiting time level, and compare the people amount in different regions, which can help the storekeeper to analyze the customers' interested area (e.g, the regions with larger people amount are more popular than the regions with lower people amount, and you can arrange more goods in these regions.) . The statistics data can show in daily report, weekly report, or monthly report.

Before You Start

Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.

Steps



This function should be supported by the connected device.


1. Click **Report** → **Queue Management** to enter the queue management page.
2. Click **Queuing-up Time Analysis** Tab.
3. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.

Daily Report

Daily report shows data on a daily basis. The system will calculate the people amount for different regions in a each hour of one day.

Weekly Report, Monthly Report

As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the people amount for different regions in each day of one week, in each day of one month.

4. Set the statistic time.
 5. Click  to unfold the region list and select the region(s).
-



Up to 6 regions can be selected.

6. Select **Regional Comparison** as the report content.
7. Select a waiting time level and enter the seconds for calculating people amount waiting for the specified time period.
8. Click **Search** to generate the statistics result.

The line chart of the calculated people amount in the specified waiting time will show on the result area. The lines with different colors indicate the people from the selected regions.

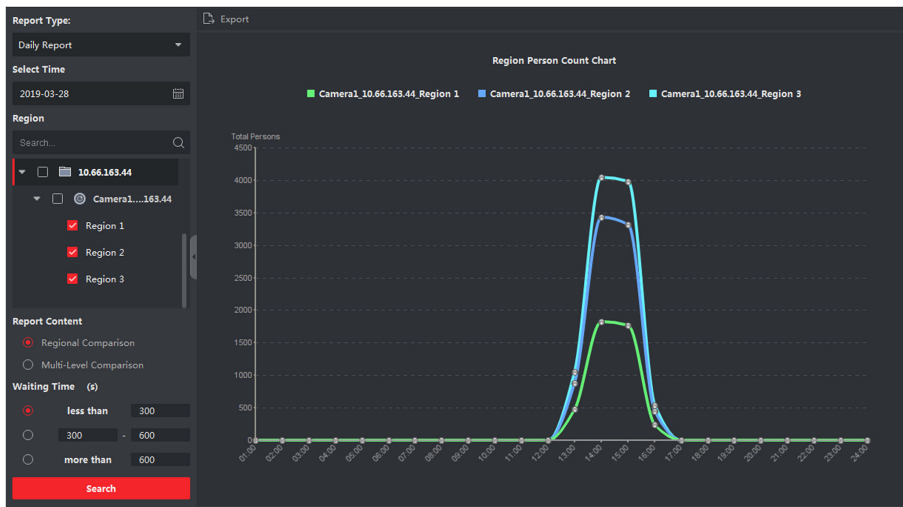


Figure 14-4 Result

9. **Optional:** Click **Export** to export the data in Excel file.

Compare Queuing-up People Amount for Different Waiting Time Levels

For a certain region, the queuing-up people amount can be calculated according to the waiting time level (e.g. the waiting time is shorter than the specified seconds.). You can search and compare the people amount for the multiple waiting time levels, which can help the customers to analyze the cashier efficiency. The statistics data can show in daily report, weekly report, or monthly report.

Before You Start

Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Report** → **Queue Management** to enter the queue management page.
2. Click **Queuing-up Time Analysis** Tab.
3. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.


Daily Report

Daily report shows data on a daily basis. The system will calculate the queuing-up people amount for different waiting time levels in a each hour of one day.

Weekly Report, Monthly Report

As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the queuing-up

people amount for different waiting time levels in each day of one week, in each day of one month.

4. Set the statistic time.
5. Click  to unfold the region list and select the region(s).
6. Select **Multi-level Comparison** as the report content.
7. Select the waiting time level and enter the seconds for calculating people amount waiting for the specified time period.
8. Click **Search** to generate the statistics result.

The line chart of the calculated people amount in the same region will show on the result area. The lines with different colors match the waiting time levels.

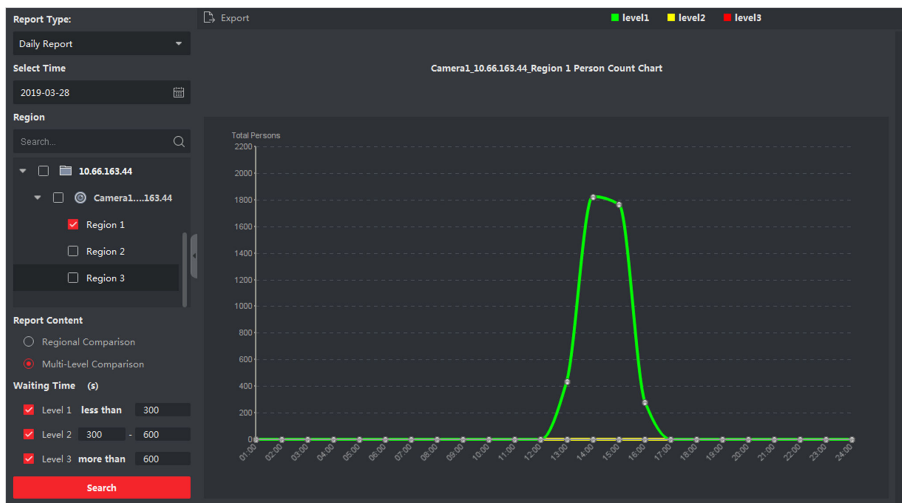


Figure 14-5 Result

9. **Optional:** Click **Export** to export the data in Excel file.

14.3.2 Queue Status Analysis

Queue Status Analysis calculates the time and duration that a queue stays with a certain length. Regional comparison and multiple queue length level comparison are supported.

Compare Queuing-up Duration for Different Regions

When the queue stays at a certain length, you can search and compare the durations in different regions, which can help the customers to analyze the cashier efficiency for different regions (e.g., the region with the shorter queuing-up duration has the higher efficiency than the region with the longer queuing-up duration). The statistics data can show in daily report, weekly report or monthly report.

Before You Start

Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.

Steps



Note

This function should be supported by the connected device.

1. Click **Report** → **Queue Management** .
2. Click **Status Analysis** Tab.
3. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.

Daily Report

Daily report shows data on a daily basis. The system will calculate the queuing-up duration for different regions in a each hour of one day.

Weekly Report, Monthly Report

As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the queuing-up duration for different regions in each day of one week, in each day of one month.

4. Set the statistic time.
5. Click to unfold the region list and select the region(s).
6. Select **Regional Comparison** as the statistics type.
7. Select a queue length level and enter the value for calculating duration when the queue stays at the length.
8. Click **Search** to generate the statistics result.

The line chart of the calculated duration for staying the specified queue length will show on the result area. The lines with different colors match the selected regions.

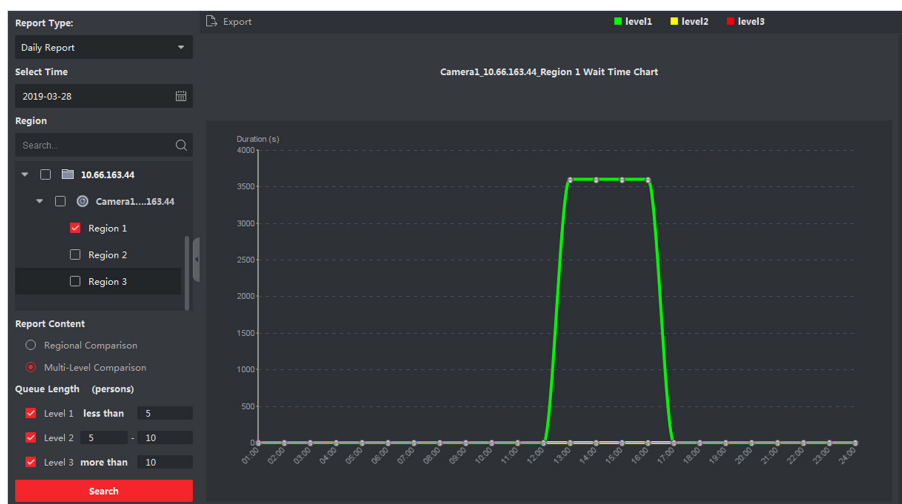


Figure 14-6 Result

9. **Optional:** Click **Export** to export the data in Excel file.

Compare Queuing-up Duration for Different Queue Length Levels

For the queue in a certain region, you can search the duration when a queue stays a certain length and compare the durations for different queue length levels, which can help the customers to analyze the cashier efficiency of different queue length levels. The statistics data can show in daily report, weekly report, or monthly report.

Before You Start

Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.

Steps



Note

This function should be supported by the connected device.


1. Click **Report** → **Queue Management** .
2. Click **Status Analysis** Tab.
3. Select the report type including **Daily Report**, **Weekly Report** and **Monthly Report**.

Daily Report

Daily report shows data on a daily basis. The system will calculate the queuing-up duration for different queue length levels in a each hour of one day.

Weekly Report, Monthly Report

As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the queuing-up duration for different queue length levels in each day of one week, in each day of one month.

4. Set the statistic time.
5. Click  to unfold the region list and select the region(s).
6. Select **Multi-level Comparison** as the report content.
7. Select the queue length level and enter the value for calculating duration when the queue stays at the length.
8. Click **Search** to generate the statistics result.

The line chart of the calculated duration in the same region will show on the result area. The lines with different colors match the queue length levels.

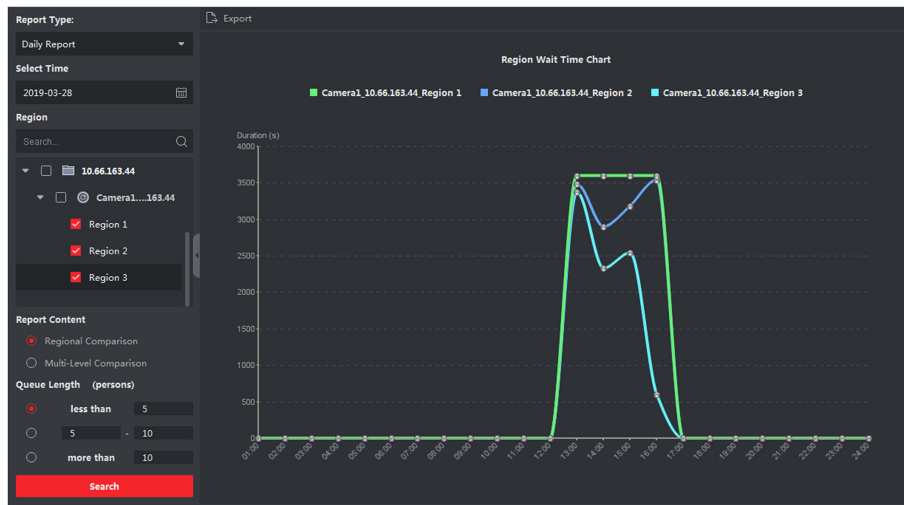


Figure 14-7 Result

9. **Optional:** Click **Export** to export the data in Excel file.

14.4 Heat Map Report

Heat map is a graphical representation of data represented by colors and the heat map data can be displayed in line chart. You can use the heat map function of the camera to analyze the visit times and dwell time of customers in a configured area, which can help the storekeeper analyze the customers' interested area and make the arrangement of goods.

Before You Start

Add a heat map network camera to the software and properly configure the corresponding area. The added camera should have been configured with heat map rule. See **Add Device** for details about adding heat map network camera.

Steps

1. Click **Report** → **Heat Map** to enter the heat map page.
2. Select daily report, weekly report, monthly report, or annual report as the time type for the report.

Daily Report

Daily report shows data on a daily basis. The system will calculate the data of heat map in a each hour of one day.

Weekly Report, Monthly Report and Annual Report

As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the data of heat map in each day of one week, in each day of one month, in each month of one year.

3. Select **By Dwell Time** or **By People Number** as the statistics type.

By Dwell Time

The system calculates the heat map value (the ordinate value in the line chart or the color in pictures) according to the people's dwell time.

By People Number

The system calculates the heat map value (the ordinate value in the line chart or the color in pictures) according to the people number.

4. Set the start time.
5. Select a heat map camera in the camera list.
6. Click **Generate Heat Map** to show the heat map of the camera.

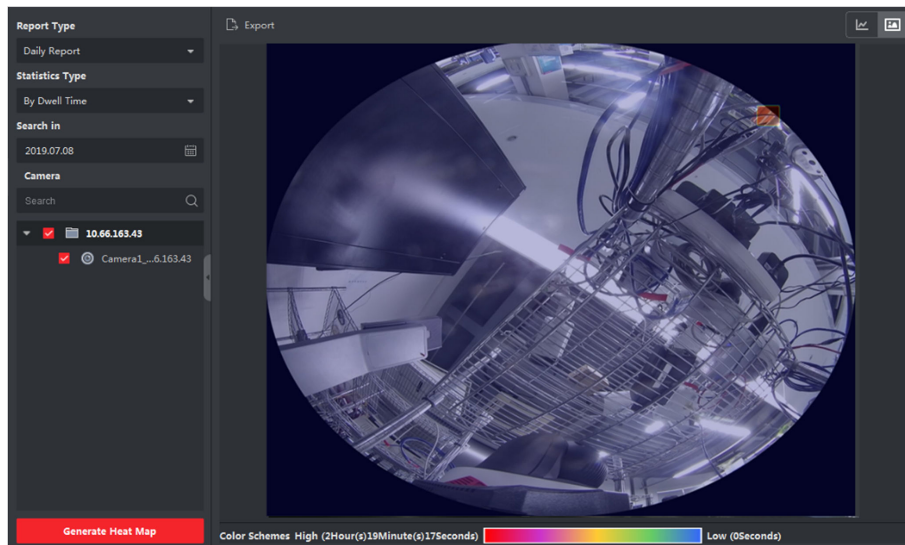




Figure 14-8 Results

7. **Optional:** After generating heat map report, you can perform the following operations.

Display in Line Chart Click  to display the statistics in line chart.

Display in Picture Mode Click  to display the statistics in picture mode.

The red color block (255, 0, 0) indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area.

Save Statistics Data Click **Export** to save the detailed data of heat map to your PC.

Chapter 15 Data Retrieval

In the Data Retrieval module, you can search the face pictures captured by the face recognition camera, search the human body pictures captured by DeepinMind device, view behavior analysis related pictures and videos, search the vehicle pictures captured by DeepinMind device, search the frequently appeared person pictures captured by DeepinMind device, and search the not wearing hard hat pictures.

15.1 Face Picture Retrieval

When the connected device (e.g. NVR or HDVR) supports face search, you can search the related picture and play the picture related video file.

15.1.1 Search Face Picture by Uploaded Picture

You can upload a face picture from your PC and compare the uploaded picture with the captured face pictures.


Before You Start

Add the device to the software and properly configure the corresponding settings. Refer to **Add Device** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval** → **Face Picture Retrieval** to enter the face picture retrieval page.
 2. Click  to set the start time and end time for searching the captured face pictures or video files.
 3. Select device(s) in the camera panel.
 4. Select **Picture** from the drop-down list to search by picture.
 5. Select a face picture for search.
 - 1) Click **Select Picture** to upload the pictures from your PC.
 - 2) Select a detected face from uploaded picture for matching the captured face pictures.
-

Note

- The resolution of the picture should be smaller than 4096×4080.
 - Only JPG and JPEG formats are supported.
-

6. Set the similarity level.

Example

If you set the similarity as 40, the captured pictures have no less than 40% similarity with the uploaded face picture will list.

7. Set the maximum number of displayed results.

8. Click **Search** to start searching.

The search results of the pictures are displayed in list.

9. Export the pictures and save them in your PC.

Export Picture

Select the pictures to be exported and save them in local PC.


Export Current Page

Export all the pictures in the current page.

Export Segment

You can download the pictures by packages. Each package contains up to 1,000 pictures.

10. **Optional:** Perform secondary search based on the search result.

1) Move to the searched picture and click 

All the faces in this picture will be analyzed and displayed.

2) Select a face you want to do secondary search.

3) Set the similarity and time period.

4) Click **Search**.

The client will search and compare the faces in the captured pictures based on the face picture you selected.

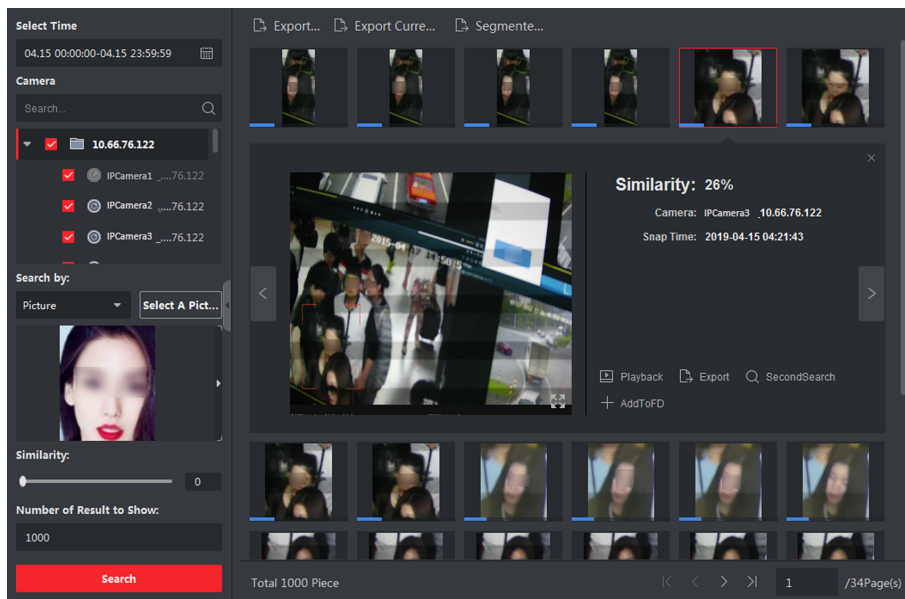









Figure 15-1 Result

11. **Optional:** After searching, you can do one or more the following operations.

- View Details** Click on a picture from the list to view details. You can also click  to show the large picture, and click  to restore.
- Play Related Videos** Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.
-

 **Note**

- You can click  to show the large video, and click  to restore.
 - You can click  to adjust the play speed of the playback, click  to play back the video files frame by frame, click  to enable audio, double-click the playback window to maximize the window.
-

- Save Pictures to PC** Click **Export Picture** and select the pictures as desired to export to local PC.

15.1.2 Search Face Picture by Event

You can search the device's captured face pictures by filtering different event types.


Before You Start

Add the device to the software and properly configure the corresponding settings. Refer to **Add Device** for details about adding the device.

Steps

 **Note**

This function should be supported by the connected device.

1. Click **Data Retrieval** → **Face Search** to enter the face picture retrieval page.
2. Click  to set the start time and end time for searching the captured face pictures or video files.
3. Select device(s) in the camera panel.
4. Select **Event Type** from drop-down list to search by event type.
5. Select event type.

All

Search all captured face pictures.

Face Picture Comparison

Search the captured pictures which match with the face pictures in face picture library.

Stranger Detection Alarm

Search the pictures captured when the stranger detection alarm is triggered.

6. Set the maximum number of displayed results.
7. Click **Search** to start searching.

The search results of the pictures are displayed in list.

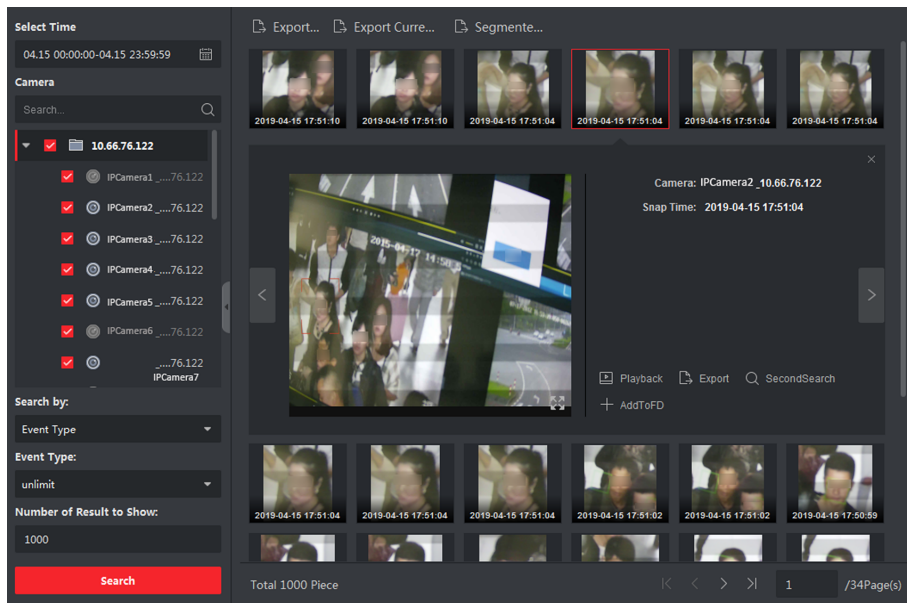


Figure 15-2 Search Result

8. Export the pictures and save them in your PC.

Export Picture

Select the pictures to be exported and save them in local PC.

Export Current Page

Export all the pictures in the current page.

Export Segment

You can download the pictures by packages. Each package contains up to 1,000 pictures.

9. **Optional:** Perform secondary search based on the search result



- 1) Move to the searched picture and click 

All the faces in this picture will be analyzed and displayed.

- 2) Select a face you want to do secondary search.
- 3) Set the similarity and time period.
- 4) Click **Search**.






The client will search and compare the faces in the captured pictures based on the face picture you selected.

10. **Optional:** After searching, you can do one or more the following operations.

View Details Click on a picture from the list to view details. You can also click  to show the large picture, and click  to restore.

Play Related Videos Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click  to show the large video, and click  to restore.
 - You can click  to adjust the play speed of the playback, click  to play back the video files frame by frame, click  to enable audio, double-click the playback window to maximize the window.
-

Save Pictures to PC

Click **Export Picture** and select the pictures as desired to export to local PC.

15.1.3 Search Face Picture by Person Name

You can search the device's captured face pictures by person name.


Before You Start

Add the device to the software and properly configure the corresponding settings. Refer to **Add Device** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval** → **Face Search** to enter the face picture retrieval page.
2. Select device(s) in the camera panel.
3. Select **Name** from the drop-down list to search by person name.
4. Click  to set the start time and end time for searching the captured face pictures or video files.
5. Enter a keyword for the person name.
6. Set the maximum number of displayed results.
7. Click **Search** to start searching.

All the persons whose name match the search condition (fuzzy match is supported) will be displayed.

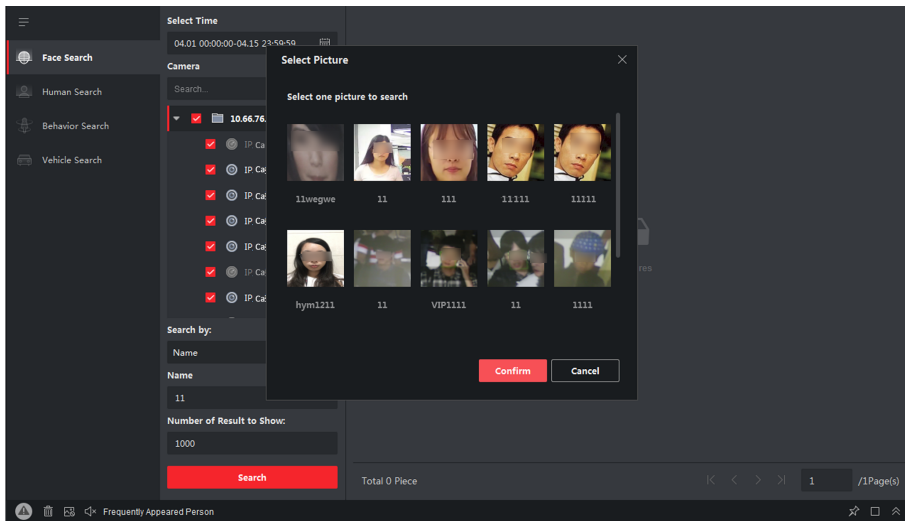


Figure 15-3 Results

8. Select one picture to search, and then click **Confirm**.

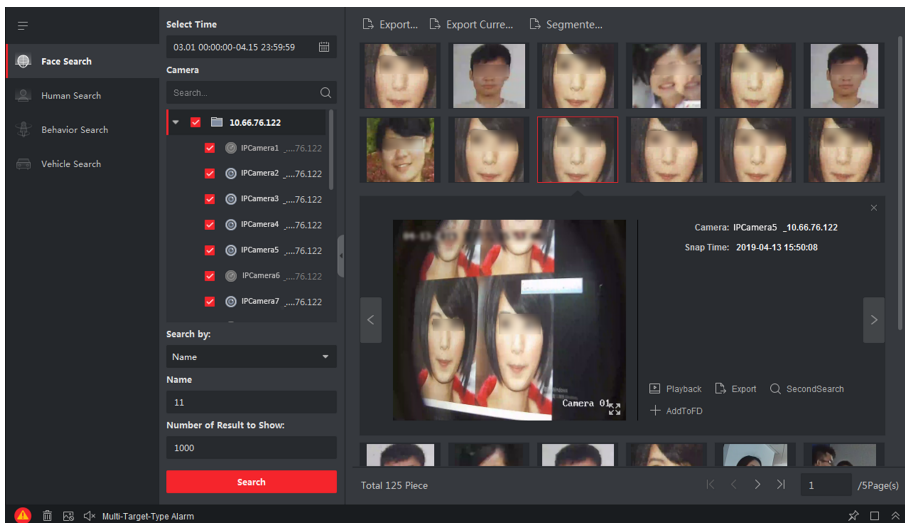


Figure 15-4 Results

The search results of the pictures are displayed in list.

9. Export the pictures and save them in your PC.

Export Picture

Select the pictures to be exported and save them in local PC.

Export Current Page

Export all the pictures in the current page.

Export Segment

You can download the pictures by packages. Each package contains up to 1,000 pictures.

10. Perform secondary search based on the search result.

1) Move to the searched picture and click

- All the faces in this picture will be analyzed and displayed.
- 2) Select a face you want to do secondary search.
 - 3) Set the similarity and time period.
 - 4) Click **Search**.

The search results of the pictures are displayed in list.

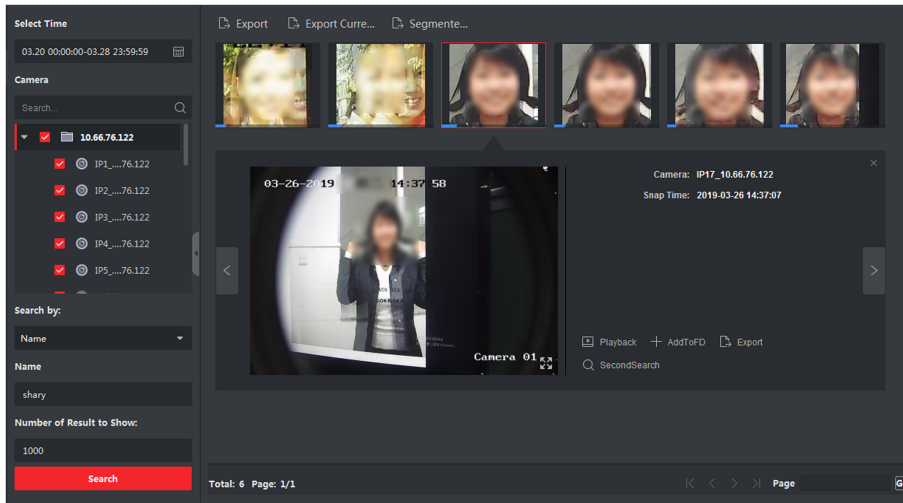









Figure 15-5 Search Result

11. After searching, you can do one or more the following operations.

View Details Click on a picture from the list to view details. You can also click  to show the large picture, and click  to restore.

Play Related Videos Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click  to show the large video, and click  to restore.
- You can click  to adjust the play speed of the playback, click  to play back the video files frame by frame, click  to enable audio, double-click the playback window to maximize the window.

Save Pictures to PC Click **Export Picture** and select the pictures as desired to export to local PC.

15.2 Human Body Picture Retrieval

For the DeepinMind device, you can upload a human body picture from local PC and compare the uploaded picture with the device's captured human body pictures, or search all the human body pictures captured by the specific camera(s) during a specific time.


Before You Start

Add the device to the software and properly configure the corresponding settings. Refer to **Add Device** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval** → **Human Search** to enter the face picture retrieval page.
2. Click  to set the start time and end time for searching the captured human body pictures or video files.
3. Select device(s) in the camera panel.
4. Select the search condition in the Search by field.

Picture

Upload a picture to compare the uploaded picture with the device's captured human body pictures. All the human bodies in this picture will be analyzed and displayed.

- a. Click **Select Picture** to select a picture for comparison from local PC.
-

Note

- The picture should be smaller than 4 MB.
 - The resolution of the picture should be smaller than 4096*4080.
 - Only JPG and JPEG formats are supported.
- b. Set the similarity level. For example, if you set the similarity as 40, the captured pictures have no less than 40% similarity with the uploaded human body picture will list.
-

None

Search all the pictures captured by the selected camera(s) during the time duration.

5. Set the maximum number of displayed results.
-

Note

If the number of pictures captured by the selected cameras(s) during the selected time duration exceeds the number of maximum number to be displayed, only the lasted pictures will be displayed.

For example, if the number of pictures captured by the selected cameras during the selected time duration is 2000, and the maximum number to be displayed is 1000, only the lasted 1000 pictures will be displayed.

6. Click **Search** to start searching.

The search results of the pictures are displayed in list.

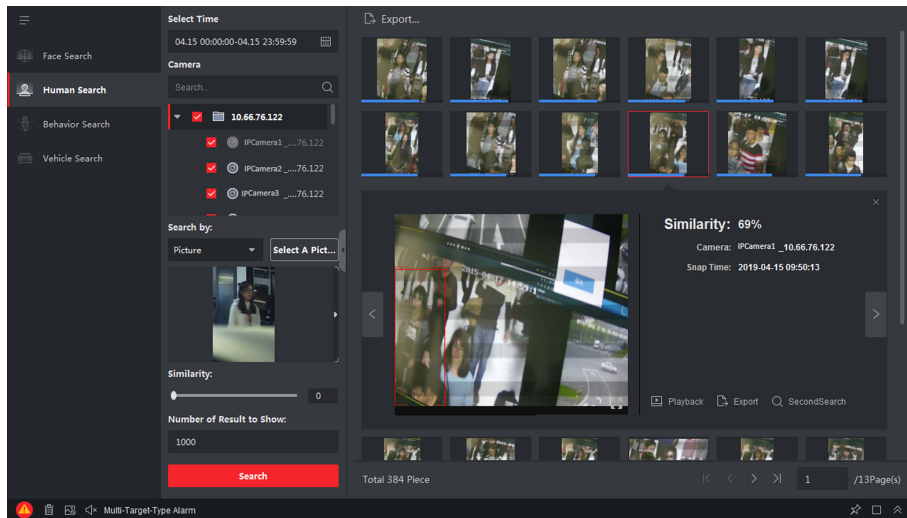


Figure 15-6 Search Result

7. Optional: Perform secondary search based on the search result

- 1) Move to the searched picture and click

All the human bodies in this picture will be analyzed and displayed.

- 2) Select a human body you want to do secondary search.
- 3) Set the similarity and time period.
- 4) Click **Search**.

The client will search and compare the human bodies in the captured pictures based on the human body picture you selected.

8. Optional: After searching human body, you can do one or more the following operations.

View Details Click on a picture from the list to view details. You can also click to show the large picture, and click to restore.

Play Related Videos Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click to show the large video, and click to restore.
- You can click to adjust the play speed of the playback, click to play back the video files frame by frame, click to enable audio, double-click the playback window to maximize the window.

Save Pictures to PC Click **Export Picture** and select the pictures as desired to export to local PC.


15.3 View Behavior Analysis Related Pictures and Videos

When the connected device supports behavior search (e.g., line crossing, people gathering and loitering), you can search the related picture and view the related pictures and video files.

Before You Start

Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the camera.



Steps

1. Click **Data Retrieval** → **Behavior Analysis** to enter the behavior analysis page.
2. Click  to set the start time and end time for searching the matched pictures.
3. Select a camera in the camera list.

Note






This function should be supported by the connected device (NVR or HDVR).

4. Select event type for behavior analysis report.
5. Click **Search** to start searching.
6. **Optional:** After searching the behavior, you can perform the following operations.

View Details Click on a picture from the list to view details. You can also click  to show the large picture, and click  to restore.

Play Related Videos Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click  to show the large video, and click  to restore.
 - You can click  to adjust the play speed of the playback, click  to play back the video files frame by frame, click  to enable audio, double-click the playback window to maximize the window.
-

Save Pictures to PC Click **Export Picture** and select the pictures as desired to export to local PC.

15.4 Vehicle Retrieval

For the DeepinMind device, you can search the device's captured vehicle pictures by setting the search conditions, such as plate number, captured time, etc.


Before You Start

Add the device to the software and properly configure the corresponding settings. See **Add Device** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval** → **Vehicle Retrieval** to enter the vehicle retrieval page.
2. Click  to set the start time and end time for searching the captured vehicle pictures or video files.
3. Select the search type.

Vehicle

Search and display the captured vehicle pictures by entering the vehicles' license plate number.

Plate

Search and display the captured license plate number pictures by entering the vehicles' license plate number.

Mix-traffic Detection

Search and display the mix-traffic detection related pictures of the specific vehicle by entering the vehicle's license plate number.

Note

The camera should support mix-traffic detection.

Traffic Violations

Search and display the traffic violation related pictures of the specific vehicle by entering the vehicle's license plate number.

Note

The camera should support traffic violation.

4. Select device(s) in the camera panel.
5. Enter the keyboard of license plate number for search.
6. Set the maximum number of displayed results.
7. Click **Search** to start searching.

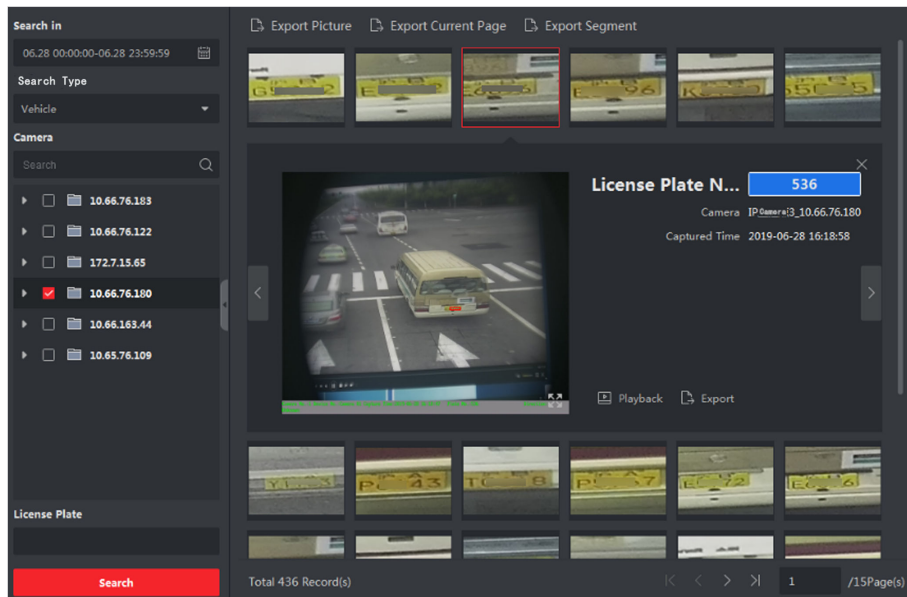


Figure 15-7 Results

The search results of the pictures are displayed in list.

8. **Optional:** Click the picture to view the whole captured picture, the captured time, etc.
9. **Optional:** Export the picture(s) to the local PC.
 - Click **Export Picture**, and then select the picture to be exported, and then click **Export**.
 - Click **Export Current Page** to export all the pictures and information on the current page.
 - Click **Export Segment** to download the pictures and capturing information by packages. Each package contains up to 1000 pictures.
10. **Optional:** Perform the following operations if needed.

Add to Face Picture Library	Click Add to face picture library to add current face picture to the library .
View Detailed Information	Click View to view the historical captured pictures of this person, the captured time.
Playback	Click Playback to play back the video of 5-seconds before and after the capturing time.
Export	Click the picture to be exported, and then click Export to export this picture.

15.5 Hard Hat Retrieval

After adding the hard hat detection device to the client, when the device detects a person who doesn't wear a hard hat, it will trigger an event and capture some pictures to notify the managers. You can search the alarm pictures in which the detected person doesn't wear a hard hat. By this way, you can remind the builders to wear hard hat, thus to improve builders' safety awareness.

Before You Start

Add the device(s) with hard hat detection function to the client.

Steps

1. Click **Data Retrieval** → **Hard Hat Search** to enter the hard hat search page.
2. Set the start time and end time for searching.
3. Select the camera for searching.
4. Click **Search**.

The captured pictures for hard hat alarm is displayed on the right panel. Up to 30 pictures can be displayed in one page.

5. Perform the following operations if needed.

Export Picture a. Click **Export Picture**.

b. Select one or more picture(s), or check **Select All** on the page below.

c. Click **Export** on the page below to export the selected picture(s).

View the Whole Picture Click a picture, and then the whole picture and captured time be displayed in the middle of the page.

Play Back Video Click a picture, and then click **Playback** to play back the video of 5-seconds before and after the capturing time.

15.6 Frequently Appeared Person Retrieval

The person's captured face picture can be compared with the face pictures in the face picture library. If mismatched, he/she will be judged as frequently appeared person, and trigger an event to notify the security person. For example, in some high-safety demanded scene (e.g. bank), if a stranger appears frequently, the event can be triggered to notify the security person or related person. If matched, he/she will be judged as a person in whitelist and will not trigger frequently appeared person alarm.. You can search the event information in a certain time, such as the captured pictures, captured time, and you can view the detailed pictures and play back the related video.

Before You Start

- Make sure the frequently appeared person alarm has been configured on the device.
- Make sure the device has been armed.

Steps

1. Click **Data Retrieval** → **Frequently Appeared Person** to enter the frequently appeared person page.
2. Set the start time and end time for searching.
3. Select the camera(s) for searching.
4. Click **Search**.

The frequently appeared person alarm related pictures will be displayed on the right panel.

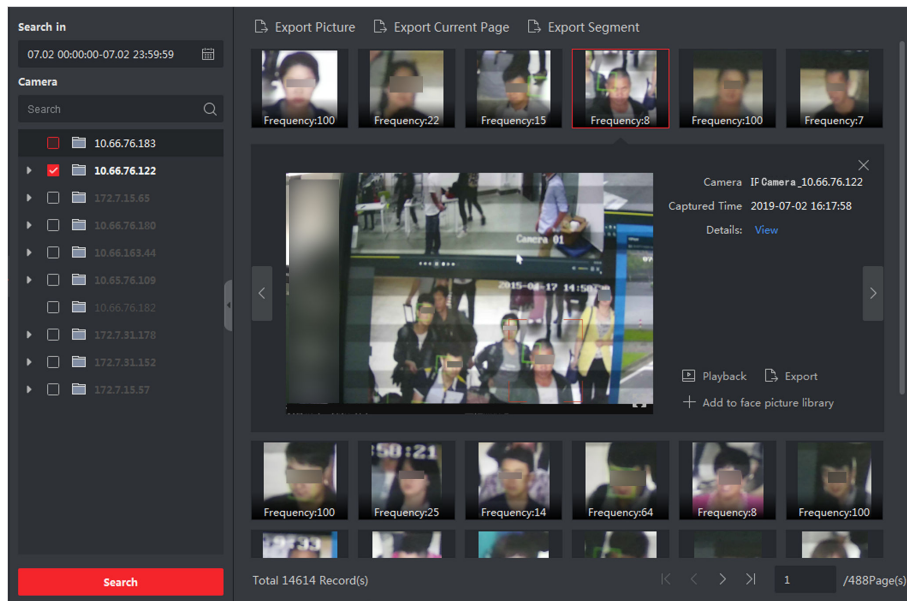


Figure 15-8 Results

5. **Optional:** Click the picture to view the whole captured picture, the captured time, etc.
6. **Optional:** Export the picture(s) to the local PC.
 - Click **Export Picture**, and then select the picture to be exported, and then click **Export**.
 - Click **Export Current Page** to export all the pictures and information on the current page.
 - Click **Export Segment** to download the pictures and capturing information by packages. Each package contains up to 1000 pictures.
7. **Optional:** Perform the following operations if needed.

Add to Face Picture Library

Click **Add to face picture library** to add current face picture to the library .

View Detailed Information

Click **View** to view the historical captured pictures of this person, the captured time.

Playback

Click **Playback** to play back the video of 5-seconds before and after the capturing time.

Export

Click the picture to be exported, and then click **Export** to export this picture.

Chapter 16 AI Dashboard


The client provides AI Dashboard module through which you can experience the advanced functions of the devices with AI features, such as face comparison and linked capture of fixed camera and panoramic camera.

16.1 Face Application

For some devices, such as DeepinMind series, DeepinView series, and dual-lens camera, Face Application function provides showing face comparison alarm for the persons in the blacklist, VIP or regular costumers during live view. If the detected face pictures are matched with the persons in the blacklist or VIP face picture library, the security center will receive relative alarms to take appropriate actions quickly and effectively. It can also help you to evaluate the regular costumers, which is widely used in the hospital, supermarket, shopping mall and so on.

16.1.1 Set List Types for Face Picture Libraries

You can configure list type for each face picture library of the device(s), so that the software can check whether the persons detected during live view are in the blacklist, very important person, or the regular costumers.

Click **AI Dashboard** → **Face Application** , and then click  in the upper-right corner to select the list type for each face picture library on the devices.

Blacklist

If the alarm type is set to **Blacklist**, AI dashboard will show the blacklist alarm once the captured pictures are matched with the ones in the face picture library.

VIP

If the face picture library is set to **VIP** , AI dashboard will show the VIP alarm once the captured pictures are matched with the ones in the face picture library.

Normal

The face pictures libraries which belong to neither the blacklist nor the VIP can be set to **Normal**. AI dashboard will not show any alarms when the captured face pictures are matched with the ones in the face picture library.




Note

This function should be supported by the device and the face picture library need be configured in the device firstly.

16.1.2 Set Cameras for Showing AI Information

You can specify the displaying camera(s) or other cameras in the camera list to show AI information during live view. For example, if you select a camera (not in live view in the displaying window) for showing VIP information, this camera will perform static detection in the background and show the AI information about VIP.

Click **AI Dashboard** → **Face Application** , and then click  in the upper-right corner to select cameras for showing the AI information in real-time.

Select the alarm type to be displayed for different cameras: Blacklist Alarm, VIP Alarm or Regular Customer Alarm.

All Cameras in Live View

If check **All Cameras in Live View**, only the AI information of the camera(s) in live view in the displaying window can be shown.

Custom Cameras

If check **Custom Cameras** and select the desired cameras, the AI information of the selected camera(s) can be shown, whether the cameras are in live view or not.

16.1.3 Show AI Information

After setting the cameras for showing AI information and list type for face picture libraries, you can view the AI information.

Click **AI Dashboard** → **Face Application** , and then select the camera(s) from the camera list to start live view and show AI information.



Note

This function should be supported by the device.

Camera List

The camera list on the left panel shows all the resources added to the client software, and you can select the appropriate window division and desired camera(s) to show AI information.





Note

The channels for live view at the same time are limited by the performance of the PC running the client.

Right-click the camera in the camera list, you can switch stream type between main stream and sub-stream.

Display Intelligent Information on Live View

You can view the real-time video of the selected camera(s).

Click  in the global toolbar of the live view area and select the window to enable the desired intelligent display. For example, if the line crossing detection is enabled for all live view windows, the recognized targets will be marked dynamically on the images of all windows. You can also click  at the bottom of each window to enable the intelligent display for the camera in this window.

Face Comparison

If you set **Face Comparison** switch to ON, when detecting blacklist person, VIP, or regular customer, the related alarm notification with corresponding colors will list on the right panel. You can view the alarm time, camera, and other details of the alarm.

Historical Captured Picture

You can view the historical captured pictures at the bottom of the page.

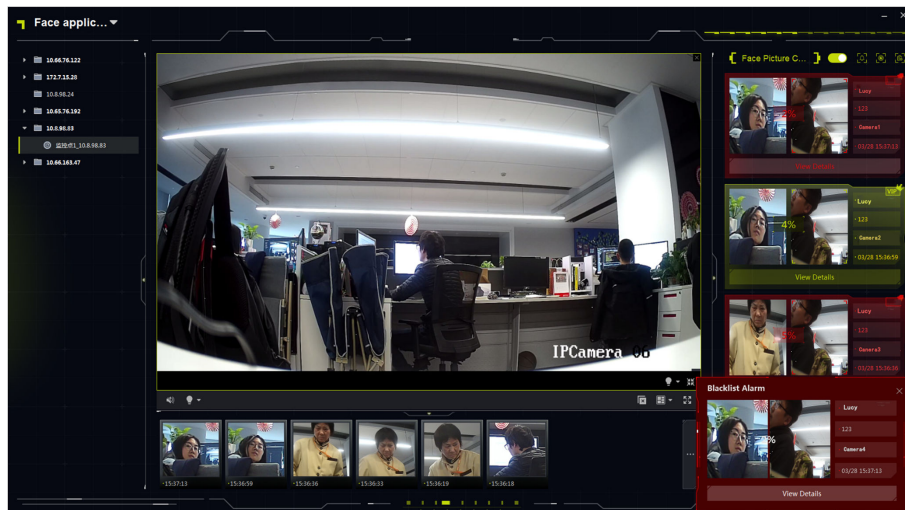



Figure 16-1 Show AI Information

Enable Alarm Triggered Pop-up Window

Click  to enable alarm triggered pop-up window, and after that, a window will be pop up when the blacklist alarm is triggered, including the captured pictures and alarm details information.

16.2 Linked Capture Alarm

This function allows the users to view two different channels (one fixed channel and one PTZ channel) of a device simultaneously. Therefore, you can view the panoramic image and captured details at the same time when an alarm is triggered.


Note

This function needs to be supported by the device.

16.2.1 Set Basic Parameters

The capture saving function can be enabled or disabled manually, and you can also set the saving path of the captured picture, so that you can view the captured pictures in your PC.

Steps

1. Enter the AI Dashboard module.
2. Select **Linked Capture Alarm** to open the Linked Capture Alarm window.
3. Click  to open the setting window.

The introduction of the displayed content shows.



4. Switch **Save Picture** on to enable picture saving function.
5. Click the **Saving Path** to select a saving path of the captured pictures.
6. Click **Save** to save the settings.

The pictures captured when events and alarms are triggered will be saved in the configured path.

16.2.2 View Live View and Alarms

When fixed camera triggers an alarm, the fixed camera will capture a panoramic picture related to the alarm, which will be displayed in the panoramic linked alarm window; and the linked PTZ camera will capture a picture with details about the alarm, and the picture will be displayed in the linked channel alarm window. In this way, the user views the panoramic image with details displayed simultaneously.

Generally speaking, Panoramic Channel Live View window is used to display the live view of fixed camera, while Linked Channel Live View window is used to display the live view of PTZ camera connected to the fixed camera.

1. Enter the **AI Dashboard** and select **Linked Capture Alarm** to open the Linked Capture Alarm window.
2. Click  to expand the device list.
3. Select a window and double-click a camera to start live view, or drag a camera from the device list to a window, or hover the cursor on a camera name and then click .

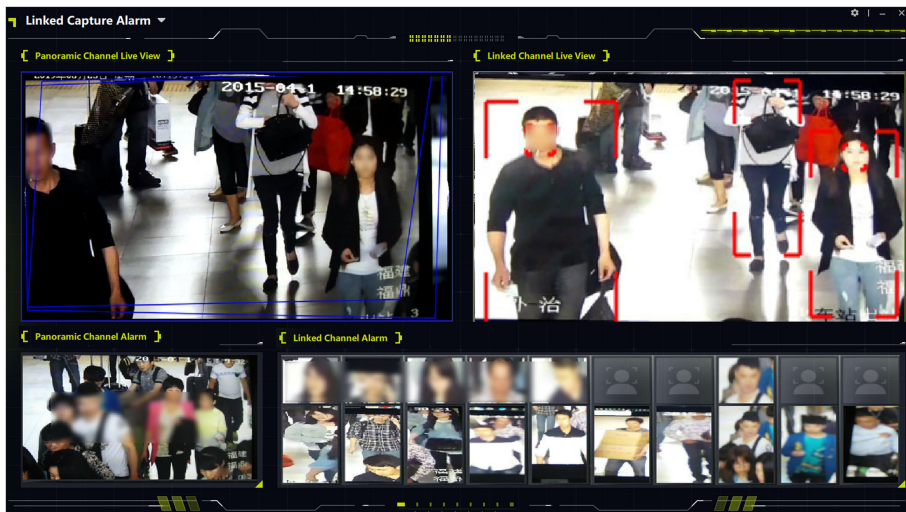


Figure 16-2 View Live View and Alarms

Chapter 17 Security Control Panel

A security control panel detects people, vehicle (etc.) entering a pre-defined virtual region, triggers events, and reports events information (such as event location) to security personnel. The Event Center module provides event management and remote control of partitions and zones via the client. After configuring client actions in event management page, you will receive notifications on the client when an event occurs. You can also manage the partitions and zones by the client even if you cannot operate the security control panel manually.



Permissions are required for Event Management, remote control of security control panel, and device arming & disarming. For details about setting user permissions, refer to **Add User** .

17.1 Configure Client Linkage for Zone Event

Even if you are far away from a zone, you can still know what happens and how urgent the event is in a zone by configuring linked actions of zone event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of multiple zones in a batch at a time.

Before You Start

- Make sure you have added a security control panel.
- Make sure zones have been defined beforehand.
- Make sure events have been configured beforehand.

Steps

1. Click **Event Management** → **Security Control Event** .
2. Expand the zone list of a security control panel, and then select a zone from the list.
3. Check one or more event.
4. Click **Edit Linkage** to configure client actions.

Audible Warning

The client software gives an audible warning when an event is triggered. You can select the alarm sound for audible warning.



Click **Add** to enter the alarm sound name and select a sound in your PC. For details, refer to **Set Alarm Sound** .

Send Email

Send an email of the alarm information to one or more receivers.

For details about setting email parameters, refer to **Set Email Parameters** .

Pop-up Window

Pop-up window to display the event related information (including event details, captured pictures of the linked camera, process record, and process field) on the software client when the event is triggered.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with red number (indicates the number of events, and the maximum number is 10) aside when the event is triggered, which helps the security guard to view the location of the event. You can also click the hot spot to view the event details and the live video of the linked camera (s).

Linked Camera

Link the selected camera(s) to capture picture when the zone event is triggered. Select the camera(s) in the drop-down list.



Note

Up to 4 cameras can be selected as the linked cameras for a zone event.

5. **Optional:** Click **Edit Priority** to set event priority as Uncatergorized/Low/Medium/High.
6. **Optional:** Click **Copy to...** to copy the event settings (including event priority, triggered client actions, and enabling/disabling the event) to other zones.
7. Enable or disable client actions for zone event.
 - Click **Enable All** or **Disable All** to enable or disable client actions of all zone events.
 - Switch **Enable** to ON/OFF to enable or disable client actions of one zone event.

Enable Client Actions

When client actions are enabled, client actions will be triggered when client receives zone event.

Disable Client Actions

When client actions are disabled, client actions will not work and actions will not be triggered when client receives zone event.

8. Click **Save**.

17.2 Remotely Control Security Control Panel

After adding the security control panel to the client, you can remotely control the partitions, zones, and relays of security control panel via the client software. For instance, you can arm, disarm, bypass, group bypass, etc. for both partitions and zones. You can also enable or disable relays.

 **Note**

- The displayed interface is subject to the types of added security control panels.
 - By default, axiom hub device uses HTTP port, and it does not support private ports.
-

17.2.1 Remotely Control Partitions

You can perform operations remotely on security control panel's partitions using the client such as away arming, stay arming, instant arming, disarming, clearing alarm, group bypass, and recovering group bypass.

Steps

 **Note**

- The supported functions are subject to the added devices.
 - If a zone of a partition does not work, you should bypass it before arming/disarming the partition, and then recover bypass when the zone works.
-

1. Click **Event Center** → **Security Control Panel** .

2. Select a security control panel and click **Partition**.

The name, status, arming status and linked zone of the partitions will be displayed in the list.

3. Select one or more partition and click the following button(s).

Away Arming

An arming mode that works when all persons are absent from the monitored region. When away arming is enabled, all zones of the partition work properly.

Stay Arming

An arming mode that works when persons stay in the monitored region. When stay arming is enabled, zones inside of the region are armed while zones outside of the region will be bypassed where you can move in the zones without triggering any event.

Instant Arming

After arming a partition, its zone will alarm instantly when an event is triggered.

Disarming

All the zones (except 24-hour zones) in the partitions does not work any more after clicking, so that no event will be triggered in the disarmed zones.

 **Note**

24-hour zones (e.g. 24-hour annunciating zones, 24-hour silent alarm zone, etc.) still can detect events and then alarm even if the partition is disarmed.

Clear Alarm

Stop the alarming of alarming devices.

Group Bypass

Bypass all the zones in one or more partition so that no event will be triggered in the bypassed zones before group bypass recovery.

Note

You should disarm the partition before bypassing it.


Group Bypass Recovery

Recover a group bypass to make all the zones in a partition work, so that you can arm the group.

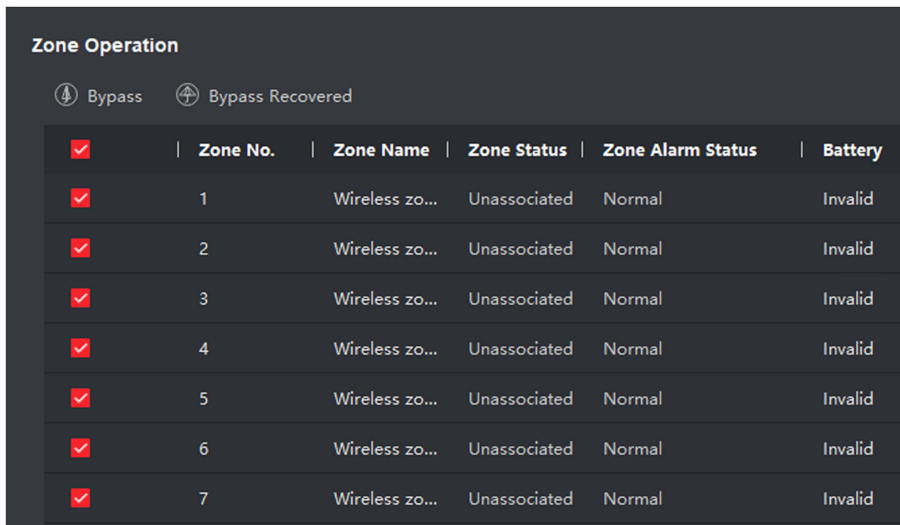
17.2.2 Remotely Control Zones

You can use the client to remotely control the security control panel's zones including bypassing and recovering bypass.

Steps

1. Click **Event Center** → **Security Control Panel** .
2. Select a security control panel and click **Partition**.
The name, status, arming status and linked zone of the partitions will be displayed in the list.
3. Click  to open the Zone Operation panel.

The zones linked with the partition, zone No., zone name, zone status, zone alarm status, battery will be displayed.



<input checked="" type="checkbox"/>	Zone No.	Zone Name	Zone Status	Zone Alarm Status	Battery
<input checked="" type="checkbox"/>	1	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	2	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	3	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	4	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	5	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	6	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	7	Wireless zo...	Unassociated	Normal	Invalid

Figure 17-1 Zone Operation

Zone Status

Zone status can be unassociated, armed, disarmed, fault, shield, tamper-proof, etc.

Battery

The power of a zone's detector.

4. Check one or more zone in the list and click the following buttons.

Bypass

When a zone is bypassed, no event will be triggered in the zone, and you are not allowed to arm or disarm the zone, while other zones can be armed or disarmed.



You should disarm the zone before bypassing it.

Bypass Recovery

After recovering bypass for a zone, you can arm it.

17.2.3 Remotely Control Relay

You can use the client to remotely change the on/off status of relay, and view the linked event of the relay.

Steps

1. Click **Event Center** → **Security Control Panel** .
2. Select a security control panel, and then click **Relay**.

The name, status, and linked event of the relay will be displayed.

3. Check one or more relay and click **Open** or **Close**.



For Axiom Hub, you should set the **Relay Associated Event** as **Manual Control** in Device Management module.

Chapter 18 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

18.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a subordinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.




Note

Up to 10 levels of organizations can be added.

4. **Optional:** Perform the following operation(s).

Edit Organization

Hover the mouse on an added organization and click  to edit its name.

Delete Organization

Hover the mouse on an added organization and click  to delete it.



Note

- The lower-level organizations will be deleted as well if you delete an organization.
 - Make sure there is no person added under the organization, or the organization cannot be deleted.
-

Show Persons in Sub Organization

Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

18.2 Add Single Person

You can add persons to the client software one by one. The person information contains basic information, detailed information, profiles, access control information, credentials, custom information, etc.

18.2.1 Configure Basic Information

You can add person to the client software one by one and configure the person's basic information such as name, gender, phone number, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.
The Person ID will be generated automatically.
4. Enter the basic information including person name, gender, tel, email address, etc.
5. **Optional:** Set the effective period of the person. Once expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors.

Example

For example, if the person is a visitor, his/her effective period may be short and temporary.

6. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

18.2.2 Issue a Card to One Person

When adding person, you can issue a card with a unique card number to the person as a credential. After issued, the person can access the doors which he/she is authorized to access by swiping the card on the card reader.

Steps



Up to five cards can be issued to one person.

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information** .

3. In the **Credential → Card** panel, click **+**.
4. Enter the card number.
 - Enter the card number manually.
 - Place the card on the card enrollment station or card reader and click **Read** to get the card number. The card number will display in the Card No. field automatically.

Note

You need to click **Settings** to set the card issuing mode and related parameters first. For details, refer to ***Set Card Issuing Parameters*** .

5. Select the card type according to actual needs.

Normal Card

The card is used for opening doors for normal usage.

Duress Card

When the person is under duress, he/she can swipe the duress card to open the door. The door will be unlocked and the client will receive a duress event to notify the security personnel.

Patrol Card

This card is used for the inspection staff to check the their attendance of inspection. By swiping the card on the specified card reader, the person is marked as on duty of inspection at that time.

Dismiss Card

By swiping the card on the card reader, it can stop the buzzing of the card reader.

6. Click **Add**.

The card will be issued to the person.

7. Confirm to add the person.

- Click **Add** to add the person and close the Add Person window.
- Click **Add and New** to add the person and continue to add other persons.

18.2.3 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.

Note

The picture should be in JPG or JPEG format and smaller than 200 KB.

6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

18.2.4 Take a Photo via Client

When adding person, you can take a photo of the person by the webcam of the PC running the client and set this photo as the person's profile.

Before You Start



Add at least one access control device checking whether the face in the photo can be recognized by the facial recognition device managed by the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Take Photo**.
5. Connect the face scanner to the PC running the client.
6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Take a photo.
 - 1) Face to the webcam of the PC and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a face photo.
 - 3) **Optional:** Click  to capture again.
 - 4) Click **OK** to save the captured photo.
8. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

18.2.5 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.


Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Remote Collection**.
5. Select an access control device which supports face recognition function from the drop-down list.
6. Collect face.
 - 1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a photo.
 - 3) Click **OK** to save the captured photo.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

18.2.6 Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Connect the fingerprint recorder to the PC running the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Local**.

5. Select the model of the connected fingerprint recorder.

 **Note**

If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.

6. Collect the fingerprint.
 - 1) Click **Start**.
 - 2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.
 - 3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

18.2.7 Collect Fingerprint via Access Control Device

When adding person, you can collect fingerprint information via the access control device's fingerprint module. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure fingerprint collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information** .

3. In the **Credential → Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Remote**.
5. Select an access control device which supports fingerprint recognition function from the drop-down list.
6. Collect the fingerprint.
 - 1) Click **Start**.
 - 2) Place and lift your fingerprint on the fingerprint scanner of the selected access control device to collect the fingerprint.
 - 3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

18.2.8 Configure Access Control Information

When adding a person, you can set her/his access control properties, such as setting the person as visitor or as blacklist person, or as super user who has super authorization.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Access Control** panel, set the person's access control properties.

PIN Code

The PIN code must be used after card or fingerprint when accessing. It cannot be used independently. It should contain 4 to 8 digits.

Super User

If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

Extended Door Open Time

When the person accessing door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

For details about setting the door's open duration, refer to ***Configure Parameters for Door/Elevator*** .

Add to Blacklist

Add the person to the blacklist and when the person tries to access doors/floors, an event will be triggered and send to the client to notify the security personnel.

Mark as Visitor

If the person is a visitor, set the maximum times of authentications, including access by card and fingerprint to limit the visitor's access times.



The maximum times of authentications should be between 1 and 100.

Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.

Note

The Super User, Extended Door Open Time, Add to Blacklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blacklist, or set her/him as visitor.

4. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

18.2.9 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
 - 1) Click **Custom Property**.
 - 2) Click **Add** to add a new property.
 - 3) Enter the property name.
 - 4) Click **OK**.
3. Set the custom information when adding a person.
 - 1) Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information** .

- 2) In the **Custom Information** panel, enter the person information.
- 3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

18.2.10 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Resident Information** panel, select the indoor station to link it to the person.
-

 **Note**

If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

18.2.11 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
 2. Select an organization in the organization list to add the person and click **Add**.
-

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

18.3 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

18.3.1 Import Person Information

You can enter the information of multiple persons in a predefined template (a CSV file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.



Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

-
7. Click  to select the CSV file with person information.
 8. Click **Import** to start importing.



Note

- If a person No. already exists in the client's database, delete the existing information before importing.
 - You can import information of no more than 10,000 persons.
-


18.3.2 Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click  to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
 - Each picture file should be in JPG format and should be no larger than 200 KB.
 - Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.
-

6. Click **Import** to start importing.

The importing progress and result will be displayed.

18.3.3 Export Person Information

You can export the added persons' information to local PC as a CSV file.

Before You Start

Make sure you have added persons to an organization.

Steps

1. Enter the Person module.
 2. **Optional:** Select an organization in the list.
-

Note

All persons' information will be exported if you do not select any organization.

3. Click **Export** to open the Export panel and check **Person Information** as the content to export.
 4. Check desired items to export.
 5. Click **Export** to save the exported CSV file in your PC.
-

18.3.4 Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

Make sure you have added persons and their face pictures to an organization.

Steps

1. Enter the Person module.
 2. **Optional:** Select an organization in the list.
-

Note

All persons' face pictures will be exported if you do not select any organization.

3. Click **Export** to open the Export panel and check **Face** as the content to export.
 4. Click **Export** to start exporting.
-

 **Note**

- The exported file is in ZIP format.
 - The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).
-

18.4 Get Person Information from Access Control Device

If the added access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the device and import them to the client for further operations.

Steps

 **Note**

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
 - The gender of the persons will be **Male** by default.
 - If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.
-

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select the access control device from the drop-down list.
5. Click **Get** to start importing the person information to the client.

The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

18.5 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.

The persons under the organization will be displayed in the right panel.

3. Select the person to move.
4. Click **Change Organization**.
5. Select the organization to move persons to.

6. Click **OK**.

18.6 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.



Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.
All the added persons with no card issued will display.
3. Set the card issuing parameters. For details, refer to *Set Card Issuing Parameters* .
4. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
5. Click the card number column and enter the card number.
 - Place the card on the card enrollment station.
 - Swipe the card on the card reader.
 - Enter the card number manually and press **Enter** key on your keyboard.The card number will be read automatically and the card will be issued to the person in the list.
6. Repeat the above step to issue the cards to the persons in the list in sequence.

18.7 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click  on the added card to set this card as lost card.
After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click  to cancel the loss.
After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

18.8 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station



Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

Chapter 19 Access Control

The Access Control module is applicable to access control devices and video intercom device. It provides multiple functionalities, including access group configuration, video intercom, and other advanced functions.

Note

For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings. For setting the user permission of Access Control module, refer to **Add User**.

19.1 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to **Set Access Group to Assign Access Authorization to Persons**.

19.1.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control** → **Schedule** → **Holiday** to enter the Holiday page.
 2. Click **Add** on the left panel.
 3. Create a name for the holiday.
 4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
 5. Add a holiday period to the holiday list and configure the holiday duration.
-






Note

Up to 16 holiday periods can be added to one holiday.

- 1) Click **Add** in the Holiday List field.
 - 2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.
-

Note

Up to 8 time durations can be set to one holiday period.

- 3) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
 - 5) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
 - 6) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.

19.1.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control** → **Schedule** → **Template** to enter the Template page.

Note

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

All-Day Authorized

The access authorization is valid in each day of the week and it has no holiday.



All-Day Denied

The access authorization is invalid in each day of the week and it has no holiday.

-
2. Click **Add** on the left panel to create a new template.
 3. Create a name for the template.
 4. Enter the descriptions or some notification of this template in the Remark box.
 5. Edit the week schedule to apply it to the template.
 - 1) Click **Week Schedule** tab on the lower panel.
 - 2) Select a day of the week and draw time duration(s) on the timeline bar.

Note

Up to 8 time duration(s) can be set for each day in the week schedule.

- 3) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.
-


Note

Up to 4 holidays can be added to one template.

- 1) Click **Holiday** tab.
 - 2) Select a holiday in the left list and it will be added to the selected list on the right panel.
 - 3) **Optional:** Click **Add** to add a new holiday.
-

Note

For details about adding a holiday, refer to **Add Holiday** .

- 4) **Optional:** Select a selected holiday in the right list and click  to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.
7. Click **Save** to save the settings and finish adding the template.
-

19.2 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Steps

- For one person, you can add up to 4 access groups to one access control point of one device.
 - You can add up to 128 access groups in total.
 - When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).
1. Click **Access Control** → **Access Group** to enter the Access Group interface.
 2. Click **Add** to open the Add window.
 3. In the **Name** text field, create a name for the access group as you want.
 4. Select a template for the access group.
-

Note

You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.

5. In the left list of the Select Person field, select person(s) and the person(s) will be added to the selected list .
 6. In the left list of the Select Door field, select door(s) or door station(s) for the selected persons to access, and the selected door(s) or door station(s) will be added to the selected list.
 7. Click **OK**.
 8. After adding the access groups, you need to apply them to the access control device to take effect.
 - 1) Select the access group(s) to apply to the access control device.


To select multiple access groups, you can hold the **Ctrl** or **Shift** key and select access groups.
 - 2) Click **Apply All to Devices** to start applying all the selected access group(s) to the access control device or door station.
-

Caution

- Be careful to click **Apply All to Devices**, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may brings risk to the devices.
 - You can click **Apply Changes to Devices** to only apply the changed part of the selected access group(s) to the device(s).
-

- 3) View the apply status in the Status column or click **Applying Statusto** view all the applied access group(s).


The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

9. **Optional:** Click  to edit the access group if necessary.

19.3 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

Note

- For the card related functions(the type of access control card/multi-factor authentication), only the card(s) with access group applied will be listed when adding cards.
 - The advanced functions should be supported by the device.
 - Hover the cursor on the Advanced Function, and then Click  to customize the advanced function(s) to be displayed.
-

19.3.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.


Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .

Note

If you can find Device Parameter in the Advanced Function list, Hover the cursor on the Advanced Function, and then Click  to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

Note

- The displayed parameters may vary for different access control devices.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

Upload the pictures captured by linked camera to the system automatically.

Save Pic. After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G


If you enable this function, the device can communicate in 3G/4G network.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door/Elevator

After adding the access control device, you can configure its access point (door or floor) parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. Select an access control device on the left panel, and then click  to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.



Note

- The displayed parameters may vary for different access control devices.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).



Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.

6. **Optional:** Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).




Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. In the device list on the left, click  to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

Name

Edit the card reader name as desired.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Entering PWD

When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).


Configure Parameters for Alarm Input

After adding the access control device, you can configure the parameters for its alarm inputs.

Steps



If the alarm input is armed, you cannot edit its parameters. Disarm it first.

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm input parameters.

Name

Edit the alarm input name as desired.

Detector Type

The detector type of the alarm input.

Zone Type

Set the zone type for the alarm input.

Sensitivity

Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

Trigger Alarm Output


Select the alarm output(s) to be triggered.

4. Click **OK**.
5. **Optional:** Click the switch on the upper-right corner to arm or disarm the alarm input.

Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

Passing Mode

Select the controller which will control the barrier status of the device.

- If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
- If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

Opening/Closing Door Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.



The recommended value is 6.

Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .



0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click **OK**.

19.3.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed and set the elevator controller as free and controlled. For example, you can set the door remaining closed in the holiday, and set the door remaining open in the specified period of the work day.

Before You Start



Add the access control devices to the system.

Steps

1. Click **Access Control** → **Advanced Function** → **Remain Open/Closed** to enter the Remain Open/Closed page.
 2. Select the door or elevator controller that need to be configured on the left panel.
 3. To set the door or elevator controller status during the work day, click the **Week Schedule** and perform the following operations.
 - 1) For door, click **Remain Open** or **Remain Closed**.
 - 2) For elevator controller, click **Free** or **Controlled**.
 - 3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.
-



Up to 8 time durations can be set to each day in the week schedule.

- 4) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
-

5) Click **Save**.

Related Operations

- | | |
|---------------------------|---|
| Copy to Whole Week | Select one duration on the time bar, click Copy to Whole Week to copy all the duration settings on this time bar to other week days. |
| Delete Selected | Select one duration on the time bar, click Delete Selected to delete this duration. |
| Clear | Click Clear to clear all the duration settings in the week schedule. |

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.



- 1) Click **Remain Open** or **Remain Closed**.
- 2) Click **Add**.
- 3) Enter the start date and end date.
- 4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.





Note


Up to 8 time durations can be set to one holiday period.

5) Perform the following operations to edit the time durations.

- Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
- Click the time duration and directly edit the start/end time in the appeared dialog.
- Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

6) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).

7) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.

8) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.

9) Click **Save**.

5. **Optional:** Click **Copy to** to copy the door status settings of this door to other door(s).

19.3.3 Configure Multi-Factor Authentication

You can manage the persons by group and set the authentication for multiple persons of one access control point (door).

Before You Start

Set access group and apply the access group to the access control device. For details, refer to **Set Access Group to Assign Access Authorization to Persons**.

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control** → **Advanced Function** → **Multi-Factor Auth** .
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
 - 1) Click **Add** on the right panel.
 - 2) Create a name for the group as desired.
 - 3) Specify the start time and end time of the effective period for the person/card group.
 - 4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

Note

Make sure you have issue card to the person.

Make sure you have set access group and apply the access group to the access control device successfully.

-
- 5) Click **Save**.
 - 6) **Optional:** Select the person/card group(s), and then click **Delete** to delete it(them).
 - 7) **Optional:** Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.
4. Select an access control point (door) of selected device on the left panel.
 5. Enter the maximum interval when entering password.
 6. Add an authentication group for the selected access control point.
 - 1) Click **Add** on the Authentication Groups panel.
 - 2) Select a configured template as the authentication template from the drop-down list.

Note

For setting the template, refer to **Configure Schedule and Template** .

-
- 3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

Local Authentication

Authentication by the access control device.

Local Authentication and Remotely Open Door

Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.

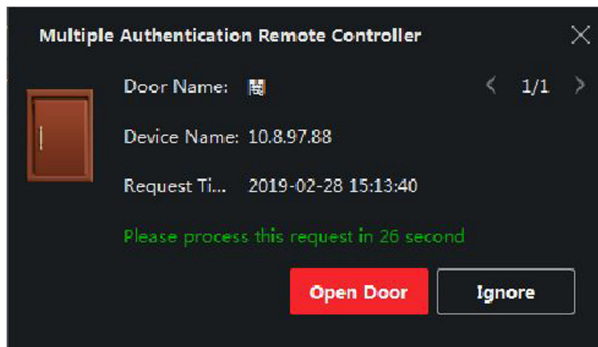


Figure 19-1 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

- 4) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.
 - 5) Click the added authentication group in the right list to set authentication times in the Auth Times column.
-

Note

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
 - The maximum value of authentication times is 16.
-

- 6) Click **Save**.
-

Note

- For each access control point (door), up to four authentication groups can be added.
 - For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
 - For the authentication group of which authentication type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.
-

7. Click **Save**.

19.3.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Steps

Note

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
 - Up to 5 custom Wiegands can be set.
 - For details about the custom Wiegand, see *Custom Wiegand Rule Descriptions* .
-

1. Click **Access Control** → **Advanced Function** → **Custom Wiegand** to enter the Custom Wiegand page.
 2. Select a custom Wiegand on the left.
 3. Create a Wiegand name.
-

Note

Up to 32 characters are allowed in the custom Wiegand name.

4. Click **Select Device** to select the access control device for setting the custom wiegand.
 5. Set the parity mode according to the property of the third party card reader.
-

Note

- Up to 80 bits are allowed in the total length.
 - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
 - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
-

6. Set output transformation rule.
 - 1) Click **Set Rule** to open the Set Output Transformation Rules window.

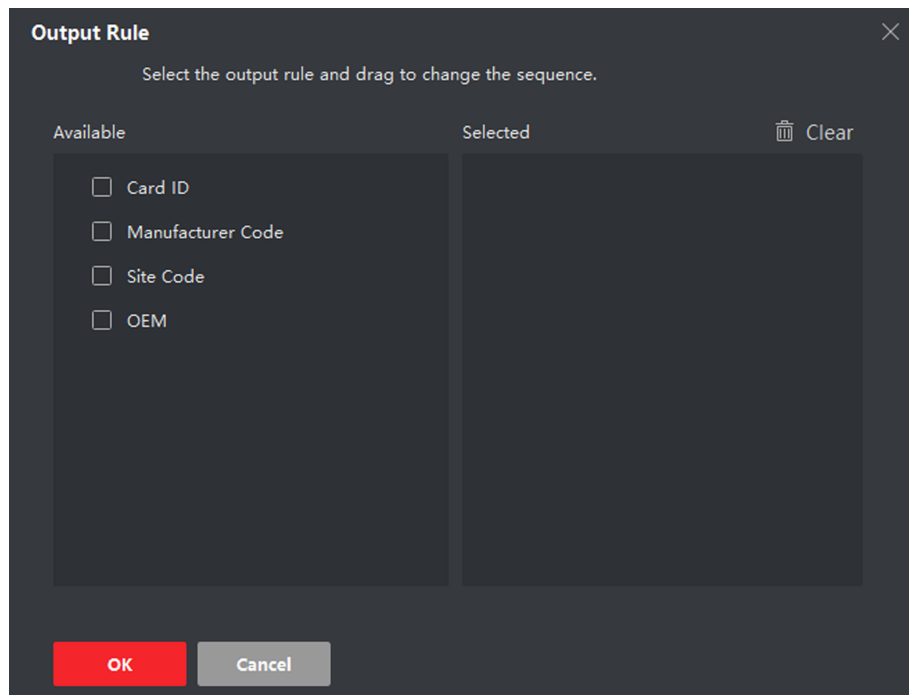


Figure 19-2 Set Output Transformation Rule

2) Select rules on the left list.

The selected rules will be added to the right list.

3) **Optional:** Drag the rules to change the rule order.

4) Click **OK**.

5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

19.3.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication** to enter the authentication mode configuration page.

2. Select a card reader on the left to configure.

3. Set card reader authentication mode.

1) Click **Configuration**.

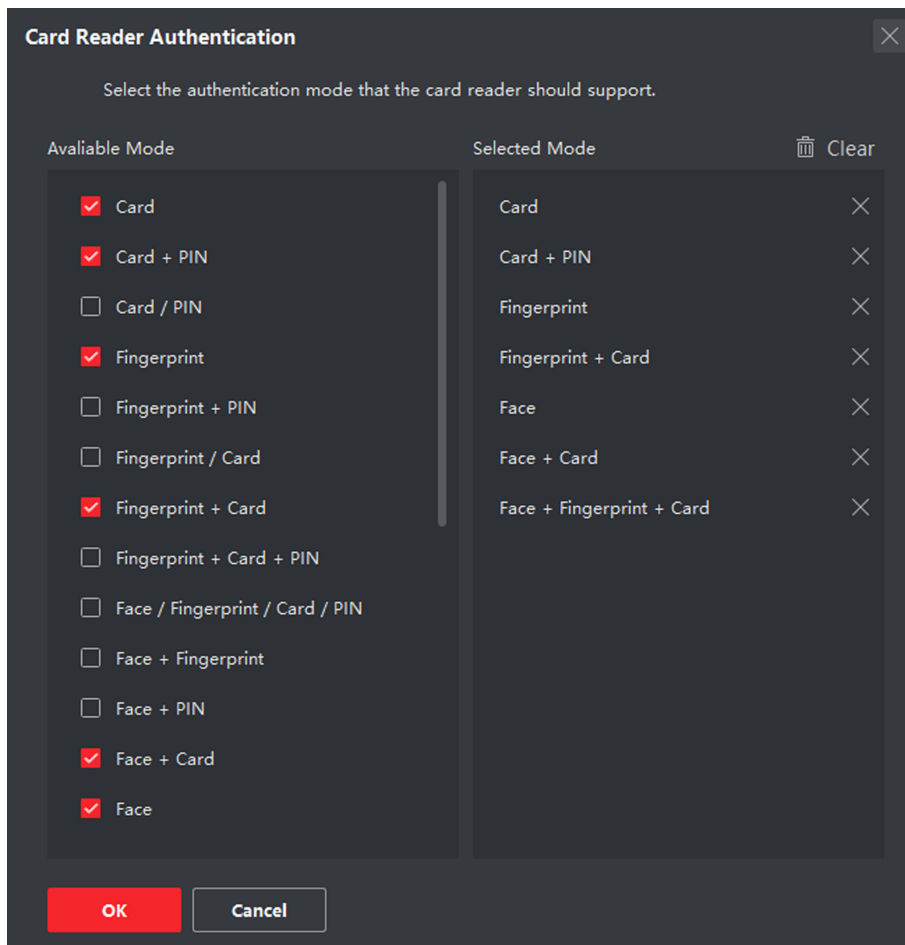


Figure 19-3 Select Card Reader Authentication Mode

 **Note**

PIN refers to the PIN code set to open the door. Refer to **Configure Access Control Information**.

- 2) Check the modes in the Available Mode list and they will be added to the selected modes list.
- 3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.
5. Repeat the above step to set other time periods.

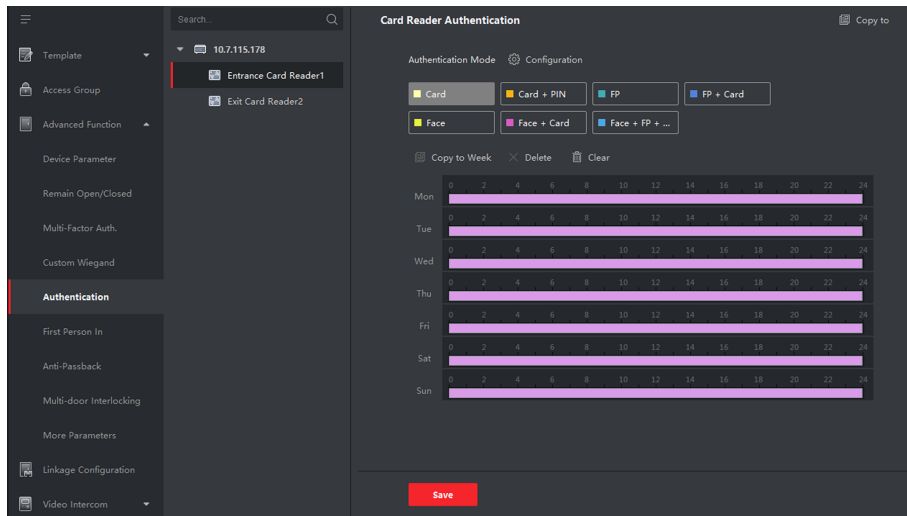


Figure 19-4 Set Authentication Modes for Card Readers

- 6. Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
- 7. Optional:** Click **Copy to** to copy the settings to other card readers.
- 8.** Click **Save**.

19.3.6 Configure Person Authentication Mode

You can set the passing rules for person to the specified the access control device according to your actual needs.

Before You Start

Make sure the access control device support the function of person authentication.

Steps

- Click **Access Control** → **Advanced Function** → **Authentication** .
- Select an access control device (support the function of person authentication) on the left panel to enter the person Authentication Mode page.
- Click **Add** to enter the Add window.
- Select the person(s) need to be configured on the left panel.
The selected person(s) will be added to the right panel.
- Select the authentication mode on the drop-down list of **Authentication Mode**.
- Click **OK**.

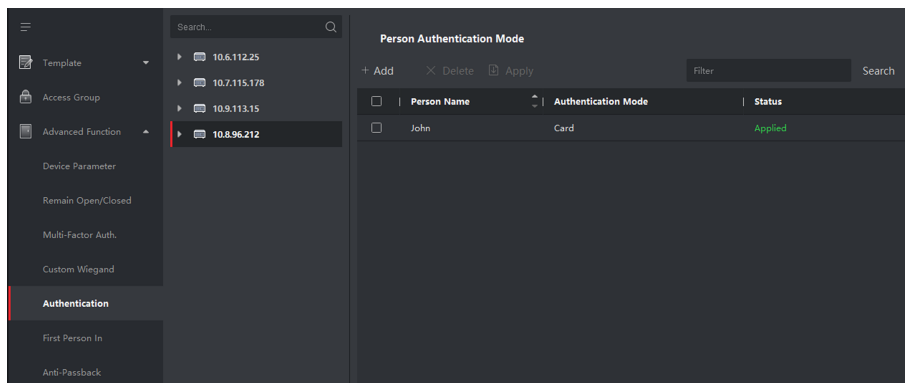


Figure 19-5 Set Authentication Modes for Persons

- 7. Optional:** Select person(s) on the Person Authentication mode page, and then click **Apply** to apply the person authentication mode to the device.

 **Note**

Person authentication has higher priority than other authentication mode. When the access control device has been configured person authentication mode, the person should authenticate on this device via person authentication mode.

19.3.7 Configure Relay for Elevator Controller

For elevator controller, you can manage the relationship between the floor and the relay and configure the floor's relay type. Different relay type can implement different functions. By configuring the relationship between the floor and the relay, you can assign different functions to the elevator and control the elevator.

Configure Relationship between Relay and Floor

You can assign different relay types to the target floors, and each floor can be assigned with 3 relay types. By this way, you can call the elevator, and assign the operations for different floors.

Before You Start

Add the elevator controller to the client.

Steps


1. Click **Access Control** → **Advanced Function** → **Elevator Configuration** to enter the Relay Settings page.
2. Select an elevator controller on the left.
3. Select an unconfigured relay in the Unconfigured Relay panel on the right.

There are three types of relay available.

Button

Control the validity for buttons of each floor.


 **Note**

 represents button relay.

Call Elevator

Control to call the elevator to go to the specified floor by indoor station or outdoor station.


 **Note**

 represents the call elevator relay.


Auto

Control to press the button when the user swipes card inside the elevator. The button of the floor will be pressed automatically according to the user's permission.

 **Note**

 represents the auto button relay.

Example

Take the following picture as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents the relay, and the icon  represents the relay type. You can change the relay type. For details, refer to **Configure Relay Type** .

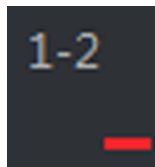


Figure 19-6 Relay

4. Configure the relationship between the relays and the floors.
 - Drag the unconfigured relay from the Unconfigured Relay panel to the target floor in the Floor List panel.
 - Drag the relay from the Floor List panel to the Unconfigured Relay panel.
 - Drag the relay from one floor to another floor in the Floor List panel. If the target floor has already configured with a relay of the same type as the dragged one, it will replace the existed one of the same type.

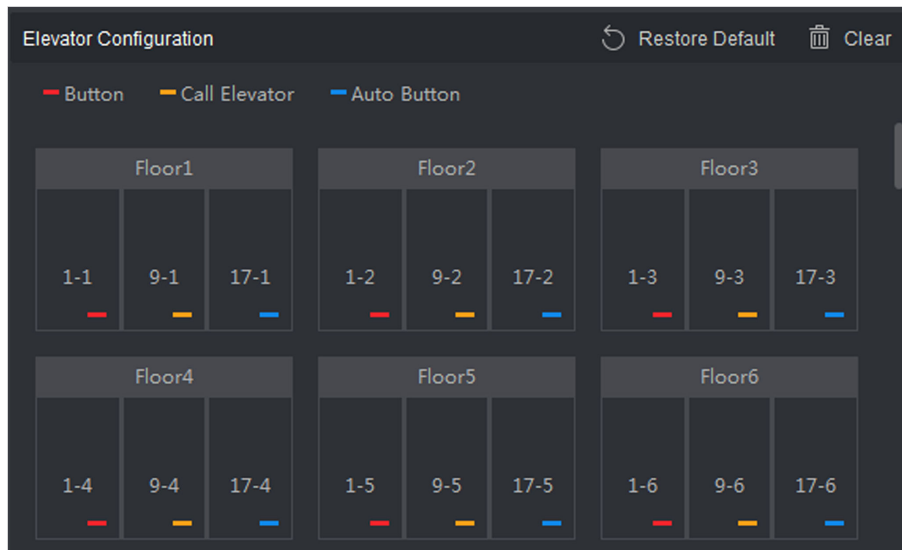


Figure 19-7 Relationship between Relay and Floor

Note

- An elevator controller can link to up to 24 distributed elevator controllers. A distributed elevator controller can link up to 16 relays.
- By default, the relay total amount is the added floor number *3 (three types of relay).
- Up to 3 types of relay can be dragged to one floor.
- If you change the floor number in the door group management, all relays in the Relay Settings interface will restore to the default settings.

5. Click **Save** to apply the settings to the selected elevator controller.




Configure Relay Type

To implement different functions, you can configure different relay type, including: button relay, call elevator relay and auto button relay. Different relay type can implement different functions. The button relay is to control the validity for buttons of each floor.. The call elevator relay is to call the elevator to the specified floor by indoor station or outdoor station. The auto button relay is to control to press the button when the user swipes card inside the elevator, the button of the floor will be pressed automatically according to the user's permission.

Steps

1. Click **Access Control** → **Advanced Function** → **Elevator Configuration** to enter the Relay Settings page.
2. Select an elevator controller on the left of the page.
3. Click **Relay Type Settings** to open the Relay Type Settings window.

 **Note**

- All relays in the Relay Type Settings window are unconfigured relays.
- Three types of relay are available:  represents the button relay,  represents the call elevator relay, and  represents the auto button relay.

4. Drag the relay from one relay type panel to the target one.

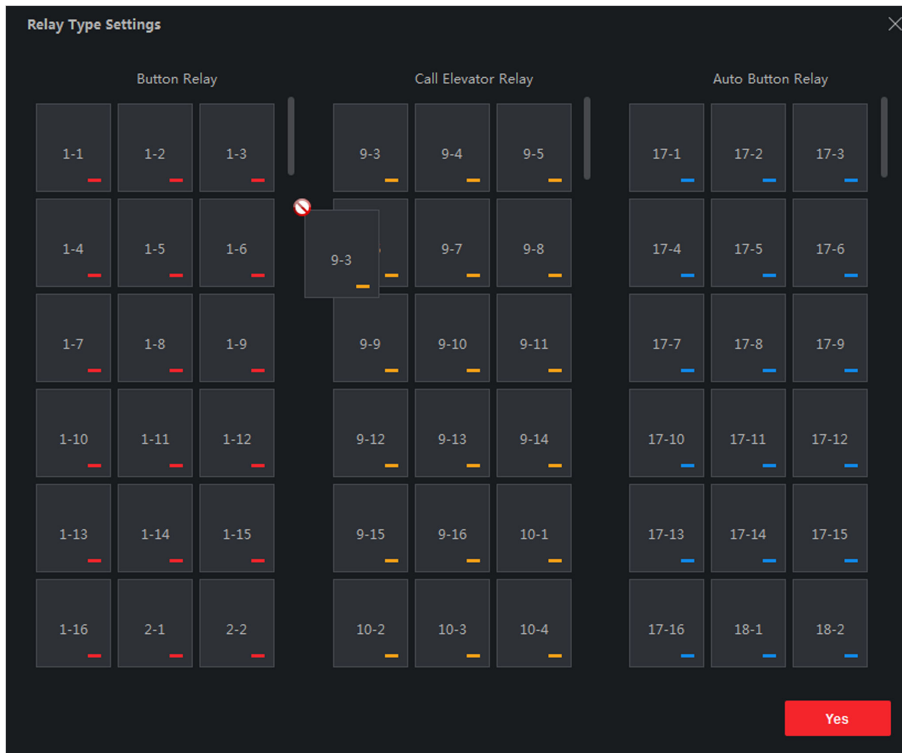


Figure 19-8 Configure Relay Type

5. Click OK.

19.3.8 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

Set the access group and apply the access group to the access control device. For details, refer to **Set Access Group to Assign Access Authorization to Persons**.

Perform this task when you want to configure opening door with first person.

Steps

1. Click **Access Control** → **Advanced Function** → **First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.

3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

Enable Remaining Open after First Person

The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the remain open duration.

Note

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

Authorization by First Person

All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

Note

You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.
The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

19.3.9 Configure Anti-Passback

You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Before You Start

Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.

Steps

Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to ***Configure Multi-door Interlocking*** .

1. Click **Access Control** → **Advanced Function** → **Anti-Passback** to enter the Anti-Passback Settings page.
 2. Select an access control device on the left panel.
 3. Select a card reader as the beginning of the path in the **First Card Reader** field.
 4. Click of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
 5. Select the afterward card readers for the first card reader.
-

Note

Up to four afterward card readers can be added as afterward card readers for one card reader.

6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping Path

If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

19.3.10 Configure Multi-door Interlocking

You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Perform this task when you want to realize interlocking between multiple doors.

Steps

Note

- Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
 - Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of anti-passing back function, refer to ***Configure Anti-Passback*** .
-

1. Click **Access Control** → **Advanced Function** → **Multi-door Interlocking** .
 2. Select an access control device on the left panel.
-

3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
4. Select at least two access control points(doors) from the list.



Note

Up to four doors can be added in one multi-door interlocking combination.

5. Click **OK** to add the selected access control point(s) for interlocking.
The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.
6. **Optional:** Select an added multi-door interlocking combination from the list and click **Delete** to delete the combination.
7. Click **Apply** to apply the settings to the access control device.

19.4 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

19.4.1 Set Multiple NIC Parameters

If the device supports multiple network interfaces, you can set the network parameters of these NICs via the client, such as IP address, MAC address, port number, etc.

Steps



Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **NIC** to enter Multiple NIC Settings page.
4. Select an NIC you want to configure from the drop-down list.
5. Set its network parameters such as IP address, default gateway, subnet mask, etc.

MAC Address

A media access control address (MAC address) is a unique identifier assigned to the network interface for communications on the physical network segment.

MTU

The maximum transmission unit (MTU) of the network interface.

6. Click **Save**.

19.4.2 Set Network Parameters

After adding the access control device, you can set the device log uploading mode, and create EHome account via wired or wireless network.

Set Log Uploading Mode

You can set the mode for the device to upload logs via EHome protocol.

Steps

Note

Make sure the device is not added by EHome.

1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
 3. Select an access control device in the device list and enter **Network → Uploading Mode** .
 4. Select the center group from the drop-down list.
 5. Check **Enable** to enable to set the uploading mode.
 6. Select the uploading mode from the drop-down list.
 - Enable **N1** or **G1** for the main channel and the backup channel.
 - Select **Close** to disable the main channel or the backup channel
-

Note

The main channel and the backup channel cannot enable N1 or G1 at the same time.

7. Click **Save**.

Create EHome Account in Wired Communication Mode

You can set the account for EHome protocol in wired communication mode. Then you can add devices via EHome protocol.

Steps

Note

- This function should be supported by the device.
 - Make sure the device is not added by EHome.
-

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and enter **Network → Network Center** .
4. Select the center group from the drop-down list.
5. Select the **Address Type** as **IP Address** or **Domain Name**.

6. Enter IP address or domain name according to the address type.
7. Enter the port number for the protocol.

 **Note**

The port number of the wireless network and wired network should be consistent with the port number of EHome.

8. Select the **Protocol Type** as **EHome**.
9. Set an account name for the network center.
10. Click **Save**.

Create EHome Account in Wireless Communication Mode

You can set the account for EHome protocol in wireless communication mode. Then you can add devices via EHome protocol.

Steps

 **Note**

- This function should be supported by the device.
 - Make sure the device is not added by EHome.
-

1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
 3. Select an access control device in the device list and enter **Network → Wireless Communication Center** .
 4. Select the **APN Name** as **CMNET** or **UNINET**.
 5. Enter the SIM Card No.
 6. Select the center group from the drop-down list.
 7. Enter the IP address and port number.
-

 **Note**

- By default, the port number for EHome is **7660**.
 - The port number of the wireless network and wired network should be consistent with the port number of EHome.
-

8. Select the **Protocol Type** as **EHome**.
9. Set an account name for the network center.
10. Click **Save**.

19.4.3 Set Device Capture Parameters

You can configure the capture parameters of the access control device, including manual capture and event triggered capture.

Note

- The capture function should be supported by the device.
 - Before setting the capture parameters, you should set the picture storage first to define where the event triggered pictures are saved. For details, refer to ***Set Picture Storage*** .
-

Set Triggered Capture Parameters

When an event occurs, the camera of the access control device can be triggered to capture picture(s) to record what happens when the event occurs. You can view the captured pictures when checking the event details in Event Center. Before that, you need to set the parameters for the capture such as number of pictures captured for one time.

Before You Start

Before setting the capture parameters, you should set the picture storage first to define where the captured pictures are saved. For details, refer to ***Set Picture Storage*** .

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters → Capture** .
3. Select an access control device in the device list and select **Linked Capture**.
4. Set the picture size and quality.
5. Set the capture times once triggered which defines how many pictures will be captures for one time.
6. If the capture times is more than 1, set the interval for each capture.
7. Click **Save**.

Set Manual Capture Parameters

In Status Monitoring module, you can capture a picture manually the access control device's camera by clicking a button. Before that, you need to set the parameters for the capture such as picture quality.

Before You Start

Before setting the capture parameters, you should set the saving path first to define where the captured pictures are saved. For details, refer to ***Set File Saving Path*** .

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters** → **Capture** .
3. Select an access control device in the device list and select **Manual Capture**.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as **High**, **Medium**, or **Low**. The higher the picture quality is, the larger size the picture will be.
6. Click **Save**.

19.4.4 Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function** → **More Parameters** .
 3. Select an access control device in the device list and click **Face Recognition Terminal**.
 4. Set the parameters.
-

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blacklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blacklist.

If matched (the person is in the blacklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blacklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

19.4.5 Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps



The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.
3. Select an access control device in the device list and click **M1 Card Encryption** to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.
The sector ID ranges from 1 to 100.
6. Click **Save** to save the settings.

19.4.6 Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Steps



The RS-485 Settings should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.

5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.
6. Click **Save**.
 - The configured parameters will be applied to the device automatically.
 - After changing the working mode or connection mode, the device will reboot automatically.

19.4.7 Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.
 3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
 4. Set the switch to on to enable the Wiegand function for the device.
 5. Select the Wiegand channel No. and the communication mode from the drop-down list.
-

Note

If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

6. Click **Save**.
 - The configured parameters will be applied to the device automatically.
 - After changing the communication direction, the device will reboot automatically.

19.4.8 Set Attendance Status

You can set the attendance mode on the device via the client. You can also set the attendance parameters as check in, check out, break out, break in, overtime in, and overtime out on the device according to your actual needs.

Note

This function should be supported by the device.

Disable Attendance Mode

Disable the attendance mode and the system will not display the attendance status on the device initial page.

Before You Start

Add at least one person, and set the person's authentication mode. For details, see *Person Management*.

Steps

1. Click **Access Control** → **Advanced Function** → **More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Disable**.
5. Click **Save**.

Result

The attendance status function is disabled, and you will not view or configure the attendance status on the device initial page.

Set Manual Attendance

Set the attendance mode as manual, and you can select a status manually when you take attendance on the device.

Before You Start

Add at least one person, and set the person's authentication mode. For details, see *Person Management*.

Steps

1. Click **Access Control** → **Advanced Function** → **More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Manual**.
5. Make sure **Attendance Status Required** is enabled.

Note

By default, **Attendance Status Required** is enabled.

6. Set shortcut key from the drop-down list for the attendance status.
7. Click **Save**.

Result

Press a key on the device keypad to select an attendance status and authenticate. The authentication will be marked as the configured attendance status according to the defined shortcut key.

Or when you authenticate on the device initial page, you will enter the Select Status page. Select a status to take attendance.

Note

If you do not select a status for about 20 s, the authentication will be failed and it will not be marked as a valid attendance.

Set Auto Attendance

Set the attendance mode as auto, and you can set the attendance status and its available time duration. The system will auto change the attendance status according to the configured parameters.

Before You Start

Add at least one person, and set the person's authentication mode. For details, see *Person Management* .

Steps

1. Click **Access Control** → **Advanced Function** → **More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Auto**.
5. Make sure **Attendance Status Required** is enabled.

Note

By default, **Attendance Status Required** is enabled.

6. Set available time for the target attendance status.
 - 1) Move the cursor on the target time and the enable checkbox will display.
 - 2) Check the checkbox and set the available time.
 - 3) Click anywhere on the page to confirm the settings. The configured time will be displayed in white.
7. Set shortcut key from the drop-down list for the attendance status.
8. Click **Save**.

The attendance status will be valid within the configured time duration.

Result

Enter the device initial page, the current attendance mode will be displayed on the page. When you authenticate on the initial page, the authentication will be marked as the configured attendance status according to the configured time.

Example

If set the Up key as check in and the Down key as check out, and set the check in's schedule as Monday 08:00, and check out's schedule as Monday 17:00, the valid person's authentication before 17:00 on Monday will be marked as check in. And the valid person's authentication after 17:00 on Monday will be marked as check out.

Set Manual and Auto Attendance

Set the attendance mode as manual and auto and the device system will auto change the attendance status according to the configured parameters. At the same time you can manually change the attendance status before the authentication.

Before You Start

Add at least one person, and set the person's authentication mode. For details, see *Person Management* .

Steps

1. Click **Access Control** → **Advanced Function** → **More Parameters** to enter the More Parameters page.
2. Select a device from the left panel.
3. Click **Attendance Status**.
4. Set the attendance mode as **Manual and Auto**.
5. Make sure **Attendance Status Required** is enabled.



Note

By default, **Attendance Status Required** is enabled.

6. Set status lasts time.
7. Set available time for the target attendance status.
 - 1) Move the cursor on the target time and the enable checkbox will display.
 - 2) Check the checkbox and set the available time.
 - 3) Click anywhere on the page to confirm the settings. The configured time will be displayed in white.
8. Set shortcut key from the drop-down list for the attendance status.
9. Click **Save**.

The attendance status will be valid within the configured time duration.

Result

Enter the device initial page, the current attendance mode will be displayed on the page. If you do not select a status, the authentication will be marked as the configured attendance status according to the configured time. If you press the key on the keypad, and select a status to take attendance, the authentication will be marked as the selected attendance status.

Example

If set the Up key as check in and the Down key as check out, and set the check in's time as Monday 08:00, and check out's time as Monday 17:00, the valid person's authentication before 17:00 on Monday will be marked as check in. And the valid person's authentication after 17:00 on Monday will be marked as check out.

19.5 Configure Linkage Actions for Access Control

The events triggered by the access control devices, doors, card readers, and alarm inputs, as well as the card swiping of persons, mobile terminal's MAC address detected, and employee No. detected, can trigger a series of linkage actions to notify the security personnel and record the events.

Two types of linkage actions are supported: client actions and device actions.

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client playing alarm sound and sending an email to notify the security personnel.
- **Device Actions:** When the event is detected, it will trigger the actions of this device, such as buzzing, door open/closed, audio play, etc., to notify the security personnel and allow/forbid access.

19.5.1 Configure Client Actions for Access Event

Even if you are far away from an access control point, you can still know what happens and how urgent the event is by configuring linked actions of access event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of access control points in a batch at a time.

Steps



Note

The linkage actions here refer to the linkage of the client software's own actions such as audible warning, email linkage, etc.

1. Click **Event Management** → **Access Control Event** .

The added access control devices will display in the device list.

2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.

The event types which the selected resource supports will display.

3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.
 - 1) Select the event(s) and click **Edit Linkage** to set the client actions when the events triggered.

Audible Warning

The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.



Note

For setting the alarm sound, please refer to **Set Alarm Sound**.

Send Email

Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to **Set Email Parameters**.

Pop-up Window

Pop-up window to display the event related information (including event details, live video of the source camera, captured pictures of the linked camera, process record, and process field) on the software client when the event is triggered.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with red number (indicates the number of events, and the maximum number is 10) aside when the event is triggered, which helps to security guard to view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture picture when the access event is triggered.

Select the camera in the drop-down list.

2) Click **OK**.

5. Enable the event so that when the event is detected, an event will be sent to the client and the linkage actions will be triggered.
6. **Optional:** Click **Copy to...** to copy the event settings to other access control device, alarm input, door/elevator, or card reader.

19.5.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. When the event is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Event Linkage**.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Buzzer on Reader

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, and remain close will be triggered.

Note

The target door and the source door cannot be the same one.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save**.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.

19.5.3 Configure Device Actions for Card Swiping

You can set the access control device's linkage actions for the specified card swiping. When you swipe the specified card, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps



It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Card Linkage**.
5. Enter the card number or select the card from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.



The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

 **Note**

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.

When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. **Optional:** After adding the device linkage, you can do one or more of the following:

- | | |
|--------------------------------|--|
| Delete Linkage Settings | Select the configured linkage settings in the device list and click Delete to delete it. |
| Edit Linkage Settings | Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target. |

19.5.4 Configure Device Linkage for Mobile Terminal's MAC Address

You can set the access control device's linkage actions for the specified MAC address of mobile terminal. When access control device detects the specified MAC address, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

 **Note**

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration** .
 2. Select the access control device from the list on the left.
 3. Click **Add** button to add a new linkage.
 4. Select the event source as **Mac Linkage**.
 5. Enter the MAC address to be triggered.
-

 **Note**

MAC Address Format: AA:BB:CC:DD:EE:FF.

6. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.



Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.



Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

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

8. **Optional:** After adding the device linkage, you can do one or more of the following:

- | | |
|--------------------------------|--|
| Edit Linkage Settings | Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target. |
| Delete Linkage Settings | Select the configured linkage settings in the device list and click Delete to delete it. |

19.5.5 Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps



Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration** .

2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Person Linkage**.
5. Enter the employee number or select the person from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.



Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.



Note

The device should support zone function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.
9. **Optional:** After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

19.6 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.



For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to **Add User** .

19.6.1 Control Door Status

You can control the status for a single door, including opening door, closing door, remaining the door open, and remaining the door closed.

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.



For managing the access point group, refer to **Group Management** .

The doors in the selected access control group will display.

3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.
4. Click the following buttons to control the door.

Open Door

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Close Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Open

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Closed

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to **Set File Saving Path** .

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

19.6.2 Control Elevator Status

You can control the elevator status of the added elevator controller, including opening elevator's door, controlled, free, calling elevator, etc.

Steps

Note

- You can control the elevator via the current client if it is not armed by other client. The elevator cannot be controlled by other client software if the elevator status changes.
 - Only one client software can control the elevator at one time.
 - The client which has controlled the elevator can receive the alarm information and view the elevator real-time status.
-

1. Click **Monitoring** to enter the status monitoring page.
 2. Select an access point group on the upper-right corner.
-

Note

For managing the access point group, refer to **Group Management** .

The elevators in the selected access point group will display.

3. Click a door icon to select an elevator.
4. Click the following buttons to control the elevator.

Open Door

When the elevator's door is closed, open it. After the open duration, the door will be closed again automatically.

Controlled

You should swipe the card before pressing the target floor button. And the elevator can go to the target floor.

Free

The selected floor's button in the elevator will be valid all the time.

Disabled

The selected floor's button in the elevator will be invalid and you cannot go to the target floor.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

19.6.3 Check Real-Time Access Records

The access records will display in real time, including card swiping records, face recognitions records, fingerprint comparison records, etc. You can view the person information and view the picture captured during access.

Steps

1. Click **Monitoring** and select a group from the drop-down list on the upper-right corner.
The access records triggered at the doors in the selected group will display in real time. You can view the details of the records, including card No., person name, organization, event time, etc.
2. **Optional:** Check the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. **Optional:** Check **Show Latest Event** and the latest access record will be selected and displayed at the top of the record list.
4. **Optional:** Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.



Note

You can double click the captured picture to enlarge it to view the details.

5. **Optional:** Right click on the column name of the access event table to show or hide the column according to actual needs.

Chapter 20 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

Note

In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

20.1 Configure Attendance Parameters

You can configure the attendance parameters, including the general rule, overtime parameters, attendance check point, holiday, leave type, etc.

20.1.1 Configure General Rule

You can configure the general rule for attendance calculation, such as the week beginning, month beginning, weekend, absence, etc.

Steps

Note

The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time & Attendance module.
2. Click **Attendance Settings** → **General Rule** .
3. Set the day as week beginning and the date as month beginning.
4. Select the day(s) as weekend.
5. Set absence parameters.
6. Click **Save**.

20.1.2 Configure Overtime Parameters

You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, attendance status for overtime, etc.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings** → **Overtime** .
3. Set required information.

Overtime Level for Workday

When you work for certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3 . You can set different work hour rate for three overtime levels, respectively.

Work Hour Rate

Set corresponding work hour rates for three overtime levels, which can be generally used to calculate total work hours.

Overtime Rule for Weekend

You can enable overtime rule for weekend and set calculation mode.

4. Click **Save**.

20.1.3 Configure Attendance Check Point

You can set the card reader(s) of the access point as the attendance check point, so that the authentication on the card readers will be recorded for attendance .

Before You Start

You should add access control device before configuring attendance check point. For details, refer to **Add Device** .

Steps



By default, all card readers of the added access control devices are set as attendance checkpoint.

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **Attendance Check Point** to enter the Attendance Check Point Settings page.
3. **Optional:** Set **Set All Card Readers as Check Points** switch to off.
Only the card readers in the list will be set as the attendance check points.
4. Check the desired card reader(s) in the device list as attendance check point(s).
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.
6. Click **Set as Check Point**.

The configured attendance check point displays on the right list.

20.1.4 Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Check **Regular Holiday** as holiday type.
4. Custom a name for the holiday.
5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
9. Click **OK**.

The added holiday will display in the holiday list and calendar.

If the date is selected as different holidays, it will be recorded as the first-added holiday.

10. **Optional:** After adding the holiday, perform one of the following operations.

Edit Holiday Click to edit the holiday information.

Delete Holiday Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Click **Add** to open the Add Holiday page.
4. Check **Irregular Holiday** as holiday type.
5. Custom a name for the holiday.
6. Set the start date of the holiday.

Example


If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.

7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.
9. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
10. Click **OK**.

The added holiday will display in the holiday list and calendar.

If the date is selected as different holidays, it will be recorded as the first-added holiday.



11. Optional: After adding the holiday, perform one of the following operations.

- Edit Holiday** Click  to edit the holiday information.
- Delete Holiday** Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

20.1.5 Configure Leave Type

You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **Leave Type** to enter the Leave Type Settings page.
3. Click **Add** on the left to add a major leave type.
4. **Optional:** Perform one of the following operations for major leave type.
 - Edit** Move the cursor over the major leave type and click  to edit the major leave type.
 - Delete** Select one major leave type and click **Delete** on the left to delete the major leave type.
5. Click **Add** on the right to add a minor leave type.
6. **Optional:** Perform one of the following operations for minor leave type.
 - Edit** Move the cursor over the minor leave type and click  to edit the minor leave type.
 - Delete** Select one or multiple major leave types and click **Delete** on the right to delete the selected minor leave type(s).

20.1.6 Synchronize Authentication Record to Third-Party Database

The attendance data recorded in client software can be used by other system for calculation or some other operations. You can enable synchronization function to apply the authentication record from client software to the third-party database automatically.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings** → **Third-Party Database** .
3. Set **Apply to Database** switch to on to enable synchronization function.
4. Set the required parameters of the third-party database, including database type, server IP address, database name, user name and password.

5. Set table parameters of database according to the actual configurations.
 - 1) Enter the table name of the third-party database.
 - 2) Set the mapped table fields between the client software and the third-party database.
6. Click **Connection Test** to test whether database can be connected.
7. Click **Save** to test whether database can be connected and save the settings for the successful connection.
 - The attendance data will be written to the third-party database.
 - During synchronization, if the client disconnects with the third-party database, the client will try to reconnect every 30 min. After reconnected, the client will synchronize the data recorded during the disconnected time period to the third-party database.

20.1.7 Configure Break Time

You can add break time and set start time, end time, duration, calculation mode and other parameters for the break. The added break time can also be edited or deleted.

Steps

1. Click **Time & Attendance → Timetable** .

The added timetables are displayed in the list.

2. Select an added timetable or click **Add** to enter setting timetable page.
3. Click **Settings** in the break time area to enter break time management page.
4. Add break time.
 - 1) Click **Add**.
 - 2) Enter a name for the break time.
 - 3) Set related parameters for the break time.

Start Time / End Time

Set the time when the break starts and ends.

No Earlier Than / No Later Than

Set the earliest swiping time for starting break and the latest swiping time for ending break.

Break Duration

The duration from start time to end time of the break.

Calculation

Auto Deduct

The fixed break duration will be excluded from work hours.

Must Check

The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.



If you select **Must Check** as calculation method, you need to set attendance status for late or early returning from break.

5. Click **Save** to save the settings.
6. **Optional:** Click **Add** to continue adding break time.

20.1.8 Configure Attendance Calculation Accuracy

To calculate the attendance data accurately, you can set the attendance calculation accuracy for different attendance items, including the minimum unit for attendance calculation and round-off control rule. For example, you can set the minimum unit as 1 hour for leave duration, and set the round-off control rule as round up.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Settings → Advanced Function** to enter the Advanced Function page.
3. Set the minimum units for different statistic items.
4. Set the round-off control rules for different statistic items.
5. Click **Save**.

Example

Set the minimum unit as 1 hour and the round-off control rule as round down for overtime duration, and if the overtime duration is less than 1 hour, it will be calculated as 0. If the overtime duration is 1.5 hour, it will be calculated as 1 hour.

20.1.9 Configure Report Display

You can configure display contents displayed in the attendance report, such as the company name, logo, date format, time format, and mark.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Statistics → Report Display**.
3. Set the display settings for attendance report.

Company Name

Enter a company name to display the name in the report.

Date Format / Time Format

Set the date format and time format according to the actual needs.

Attendance Status Mark in Report

Enter the mark and select the color. The related fields of attendance status in the report will display with the mark and color.

Weekend Mark in Report

Enter the mark and select the color. The weekend fields in the report will display with the mark and color.

4. Click **Save**.

20.2 Add Timetable

On the timetable page, you can set the start-work time, end-work time and set attendance rules for being late and leaving early, etc.

Steps

1. Click **Time and Attendance → Timetable** to enter the timetable settings page.
2. Click **Add** to enter Basic Settings page.

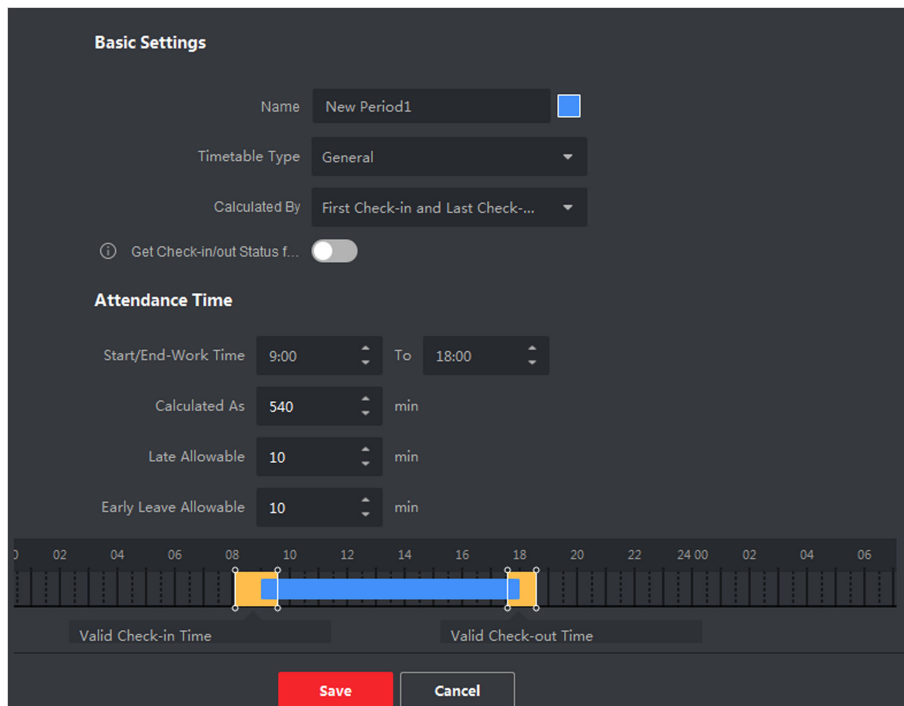


Figure 20-1 Add Timetable

3. Create a name for the timetable.

Note

You can click the color icon beside the name to customize the color for the valid timetable on the time bar on the bottom of the page.

4. Select the timetable type.

General

Suitable for general attendance scene, which requires the fixed start-work time and end-work time, and you can set valid check-in/out time, allowable timetable for being late and leaving early.

Flexible

Suitable for man-hour shift, which does not requires the check-in/out time and only requires the staffs' working time (from the start time you set) is equal or greater than the predefined work hours.

5. Select calculation method.

First Check-in & Last Check-out

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

Each Check-In/Out

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.

You need to set **Valid Auth. Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

6. **Optional:** Set **Get Check-in/out Status from Device** switch to on to calculate according to attendance status of the device.



Note

Make sure the device support this function if you need to enable this

7. If you select General as the timetable type, set the related attendance time parameters as the following:

Start/End-Work Time

Set the start-work time and end-work-time.

Valid Check-in/out Time

On the time bar, adjust the yellow bar to set the timetable during which the check-in or check-out is valid.

Calculated as

Set the duration calculated as the actual work duration.

Late/Early Leave Allowable

Set the timetable for late or early leave.

8. If you select **Flexible** as the timetable type, set the related attendance time parameters as the following:

Working Hours

The staffs' working hours should be equal or greater than the set value.

Start Time of Timetable

Calculate the working hours of each day from the set value.

For example, if you have set the working hours as 8 hours, and the start time of timetable as 9:00 am, and the staff A checked-in at 8:00 am and checked-out at 5:00 pm (effective working hours are 9:00 am to 5:00 pm, totally 8 hours), the attendance result for staff A will be calculated as normal.

- 9. Optional:** Select break time to exclude the duration from work hours.
-



Note

You can click **Settings** to manage break time. For more details about configuring break time, refer to **Configure Break Time**.

- 10.** Click **Save** to add the timetable.

- 11. Optional:** Perform one or more following operations after adding timetable.

- | | |
|-------------------------|--|
| Edit Timetable | Select a timetable from the list to edit related information. |
| Delete Timetable | Select a timetable from the list and click Delete to delete it. |

20.3 Add Shift

You can add the shift for the shift schedule.

Before You Start

Add a timetable first. See **Add Timetable** for details.

Steps

1. Click **Time & Attendance** → **Shift** to enter shift settings page.
2. Click **Add** to enter Add Shift page.
3. Enter the name for shift.
4. Select the shift period from the drop-down list.
5. Select the added timetable and click on the time bar to apply the timetable.

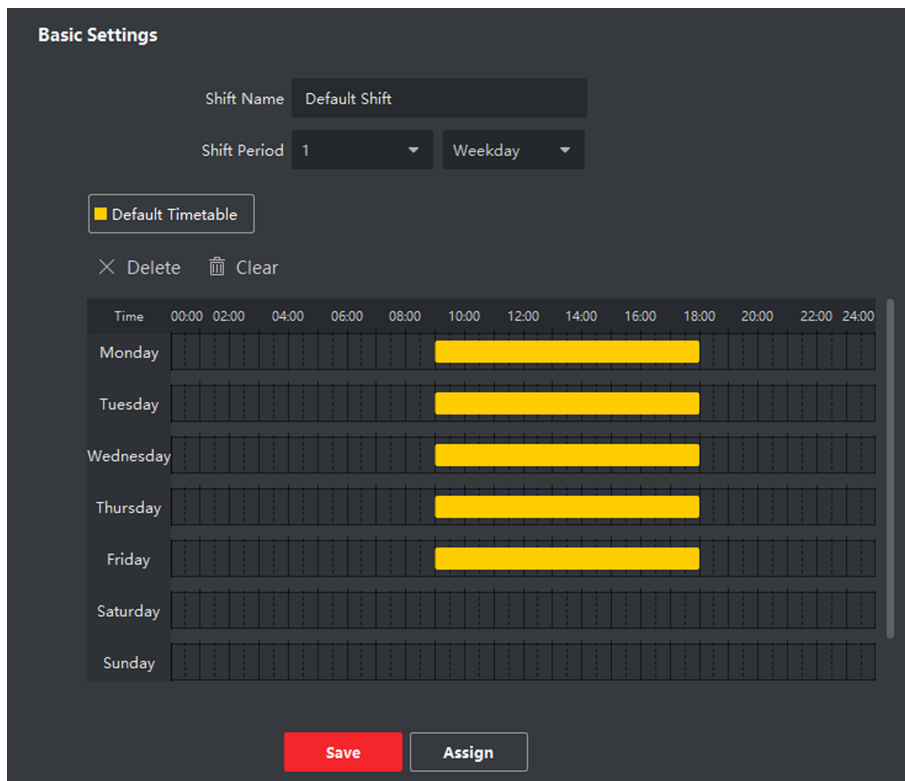


Figure 20-2 Add Shift

6. Click Save.

The added shift lists on the left panel of the page. At most 64 shifts can be added.

7. Optional: Assign the shift to organization or person for a quick shift schedule.

- 1) Click **Assign**.
- 2) Select **Organization** or **Person** tab and check the desired organization(s) or person(s) box.
The selected organizations or persons will list on the right page.
- 3) Set the effective period for the shift schedule.
- 4) Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

- 5) Click **Save** to save the quick shift schedule.

20.4 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.

You can set department schedule, person schedule, and temporary schedule.

20.4.1 Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

In Time & Attendance module, the department list is the same with the organization. You should add organization and persons in Person module first. See *Person Management* for details.

Steps

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Department Schedule** to enter Department Schedule page.
3. Select the department from the organization list on the left.

Note

If **Include Sub Organization** is checked, when selecting the organization, its sub organizations are selected at the same time.

4. Select the shift from the drop-down list.
5. Check the checkbox to enable **Multiple Shift Schedules**.

Note

After checking **Multiple Shift Schedules**, you can select the effective time period(s) from the added time periods for the persons in the department.

Multiple Shift Schedules

It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.

If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

8. Click **Save**.

20.4.2 Set Person Schedule

You can assign the shift schedule to one or more persons. You can also view and edit the person schedule details.

Before You Start

Add department and person in Person module. See *Person Management* for details.

Steps



Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule page.
 2. Click **Person Schedule** to enter Person Schedule page.
 3. Select the organization and select the person(s).
 4. Select the shift from the drop-down list.
 5. Check the checkbox to enable **Multiple Shift Schedules**.
-



Note

After checking the **Multiple Shift Schedules**, you can select the effective timetable(s) from the added timetables for the persons.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

8. Click **Save**.

20.4.3 Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start

Add department and person in Person module. See *Person Management* for details.

Steps



The temporary schedule has higher priority than department schedule and person schedule.

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Temporary Schedule** to enter Temporary Schedule page.
3. Select the organization and select the person(s).
4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

If **Non-Workday** is selected, you need to set the following parameters.

Calculated as

Select normal or overtime level to mark the attendance status for temporary schedule.

Timetable

Select a timetable from drop-down list.

Multiple Shift Schedule

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be

effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

Rule



Set other rule for the schedule, such as **Check-in Not Required**, and **Check-out Not Required**.

6. Click **Save**.

20.4.4 Check Shift Schedule

You can check the shift schedule in calendar or list mode. You can also edit or delete the shift schedule.

Steps

1. Click **Time & Attendance** → **Shift Schedule** to enter the Shift Schedule Management page.
2. Select the organization and corresponding person(s).
3. Click  or  to view the shift schedule in calendar or list mode.

Calendar

In calendar mode, you can view the shift schedule for each day in one month. You can click the temporary schedule for one day to edit or delete it.

List

In list mode, you can view the shift schedule details about one person or organization, such as shift name, type, effective period and so on. Check the shift schedule(s), and click **Delete** to delete the selected shift schedule(s).

20.5 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, search, or export the check-in or check-out record.


Before You Start

- You should add organizations and persons in Person module. For details, refer to **Person Management**.
- The person's attendance status is incorrect.



Steps

1. Click **Time & Attendance** → **Attendance Handling** to enter attendance handling page.
2. Click **Correct Check-In/Out** to enter adding the check-in/out correction page.
3. Select person from left list for correction.
4. Select the correction date.
5. Set the check-in/out correction parameters.
 - Select **Check-in** and set the actual start-work time.
 - Select **Check-out** and set the actual end-work time.

 **Note**

You can click  to add multiple check in/out items. At most 8 check-in/out items can be supported.

6. **Optional:** Enter the remark information as desired.
7. Click **Save**.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

View Click  or  to view the added attendance handling information in calendar or list mode.

 **Note**

In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

- Edit**
- In calendar mode, click the related label on date to edit the details.
 - In list mode, double-click the related field in Date, Handling Type, Time, or Remark column to edit the information.

Delete Delete the selected items.

Export Export the attendance handling details to local PC.

 **Note**

The exported details are saved in CSV format.

20.6 Add Leave and Business Trip

You can add leave and business trip when the employee want to ask for leave or go on a business trip.

Before You Start

You should add organizations and persons in the Person module. For details, refer to *Person Management* .



Steps

1. Click **Time & Attendance** → **Attendance Handling** to enter attendance handling page.
 2. Click **Apply for Leave/Business Trip** to enter adding the leave/business trip page.
 3. Select person from left list.
 4. Set the date(s) for your leave or business trip.
 5. Select the major leave type and minor leave type from the drop-down list.
-

 **Note**

You can set the leave type in Attendance Settings. For details, refer to *Configure Leave Type* .

6. Set the time for leave.
7. **Optional:** Enter the remark information as desired.
8. Click **Save**.
9. **Optional:** After adding the leave and business trip, perform one of the following operations.

View Click  or  to view the added attendance handling information in calendar or list mode.

 **Note**

In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

- Edit**
- In calendar mode, click the related label on date to edit the details.
 - In list mode, double-click the field in Date, Handling Type, Time, or Remark column to edit the related information.

Delete Delete the selected items.

Export Export the attendance handling details to local PC.

 **Note**

The exported details are saved in CSV format.

20.7 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

20.7.1 Automatically Calculate Attendance Data

You can set a schedule so that the client can calculate the attendance data automatically at the time you configured every day.

Steps

 **Note**

It will calculate the attendance data till the previous day.

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. In the Auto-Calculate Attendance area, set the time that you want the client to calculate the data every day.
4. Click **Save**.

20.7.2 Manually Calculate Attendance Data

You can calculate the attendance data manually by setting the data range.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics** → **Calculate Attendance** .
3. Set the start time and end time to define the attendance data range.
4. Set other conditions, including department, person name, employee No. and attendance status.
5. Click **Calculate**.

Note

It can only calculate the attendance data within three months.

6. Perform one of the following operations.

Correct Check-in/out	Click Correct Check-in/out to add check-in/out correction.
Report	Click Report to generate the attendance report.
Export	Click Export to export attendance data to local PC.

Note

The exported details are saved in CSV format.

20.8 Attendance Statistics

You can check the original attendance record, generate and export the attendance report based on the calculated attendance data.

20.8.1 Get Original Attendance Record

You can search the employee's attendance time, attendance status, check point, etc. in a time period to get an original record of the employees.

Before You Start

- You should add organizations and persons in Person module and the persons has swiped card. For details, refer to **Person Management** .
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
 - Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .
-

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Original Records** .
3. Set the attendance start time and end time that you want to search from.
4. Set other search conditions, such as department, person name, and employee No.
5. **Optional:** Click **Get from Device** to get the attendance data from the device.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

The result displays on the page. You can view the employee's required attendance status and check point.

8. **Optional:** After searching the result, perform one of the following operations.

Generate Report Click **Report** to generate the attendance report.

Export Report Click **Export** to export the results to the local PC.

20.8.2 Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start

Calculate the attendance data.

Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Report** .
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click **Report** to generate the statistics report and open it.

20.8.3 Custom Attendance Report

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

Steps



Set the email parameters before you want to enable auto-sending email functions. For details, refer to **Set Email Parameters** .

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Custom Report** .
3. Click **Add** to pre-define a report.
4. Set the report content.

Report Name

Enter a name for the report.

Report Type

Select one report type and this report will be generated.

Report Time

The time to be selected may vary for different report type.

Person

Select the added person(s) whose attendance records will be generated for the report.

5. **Optional:** Set the schedule to send the report to the email address(es) automatically.
 - 1) Check the **Auto-Sending Email** to enable this function.
 - 2) Set the effective period during which the client will send the report on the selected sending date(s).
 - 3) Select the date(s) on which the client will send the report.
 - 4) Set the time at which the client will send the report.

Example

If you set the effective period as **2018/3/10 to 2018/4/10**, select **Friday** as the sending date, and set the sending time as **20:00:00**, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.



Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to **Calculate Attendance Data** .

- 5) Enter the receiver email address(es).

 **Note**

You can click **+** to add a new email address. Up to 5 email addresses are allowed.

6) **Optional:** Click **Preview** to view the email details.

6. Click **OK**.

7. **Optional:** After adding the custom report, you can do one or more of the followings:

Edit Report Select one added report and click **Edit** to edit its settings.

Delete Report Select one added report and click **Delete** to delete it.

Generate Report Select one added report and click **Report** to generate the report instantly and you can view the report details.

Chapter 21 Video Intercom

Video intercom is an audiovisual communication system used within a building or a small collection of buildings. With microphones and video camera devices at both sides, it enables the intercommunication via video and audio signals. A video intercom system can provide a safe and easy monitoring solution for apartment buildings and private houses.

Be sure to add video intercom devices to the client and link the indoor stations to the persons beforehand. You should also set the access authorization for the persons to open doors via the linked indoor stations.

Note

- Up to 16 door stations and 512 indoor stations or master stations can be managed in the client. For details about adding video intercom devices, refer to **Add Device** .
 - For details about adding persons, refer to **Add Single Person** .
 - For details about setting person's access authorization, refer to **Set Access Group to Assign Access Authorization to Persons** .
-

21.1 Manage Calls between Client Software and an Indoor/Door Station/Access Control Device

You can call the residents by the client, and vice versa. You can also use an indoor station/door station or specified access control device to call the client.

Before making calls, you can set the parameters such as ring duration and speaking duration. For details, refer to **Set Access Control and Video Intercom Parameters** .

21.1.1 Call Indoor Station from Client

You can call the added indoor station by the client to perform video intercom.

Before You Start

- Be sure to have added a resident to the client. For details, refer to **Add Single Person** .
- Be sure to have linked the resident with an indoor station and configured the resident information (including floor No. and room No.) in Person module. For details about configuring the linkage and resident information, refer to **Configure Resident Information** .

Steps

Note

- A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.
 - You can remotely configure the Max. Ring Duration and the Max. Speaking Duration.
-

1. Click **Access Control** → **Video Intercom** → **Contacts** .

2. Unfold the organization list on the left panel and select an organization.

The information (including resident name, linked device name and device IP address) of all the residents in the selected group will be displayed on the right panel.

3. Select a resident, or enter a keyword in the Filter field to find the desired resident.

4. Click  to start calling the selected resident.

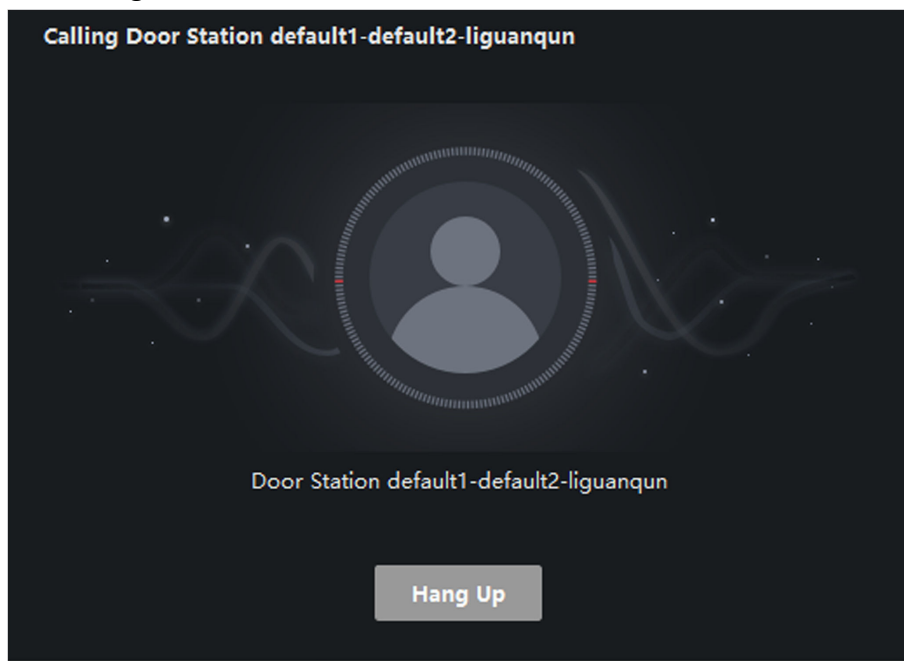



Figure 21-1 Start Calling Window

After the call is answered, you will enter the In Call window.

5. **Optional:** After the call is answered, perform the following operation(s).

Adjust Loudspeaker Volume Click  to adjust the volume of the loudspeaker.

End Speaking Click **Hang Up** to end speaking.

Adjust Microphone Volume Click  to adjust the volume of the microphone.

21.1.2 Answer Call via Client

The residents can call the client by an indoor station, door station, or specific access control devices and perform video intercom with the client.

Before You Start

- Be sure to have added a resident to the client. For details, refer to **Add Single Person** .
- Be sure to have linked the added resident with an indoor station/outdoor station/access control device and configured the resident information (including floor No. and room No.) in Person module. For details about configuring the linkage and resident information, refer to **Configure Resident Information** .

Steps


Note

- A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.
 - You can remotely configure the Max. Ring Duration and the Max. Speaking Duration.
-

1. Click **Access Control** → **Video Intercom** → **Contacts** .

2. Unfold the organization list on the left panel and select an organization.

The information (including resident name, linked device name and device IP address) of all the residents in the selected group will be displayed on the right panel.

3. Click  to start calling a desired resident.

An incoming call dialog will pop up.

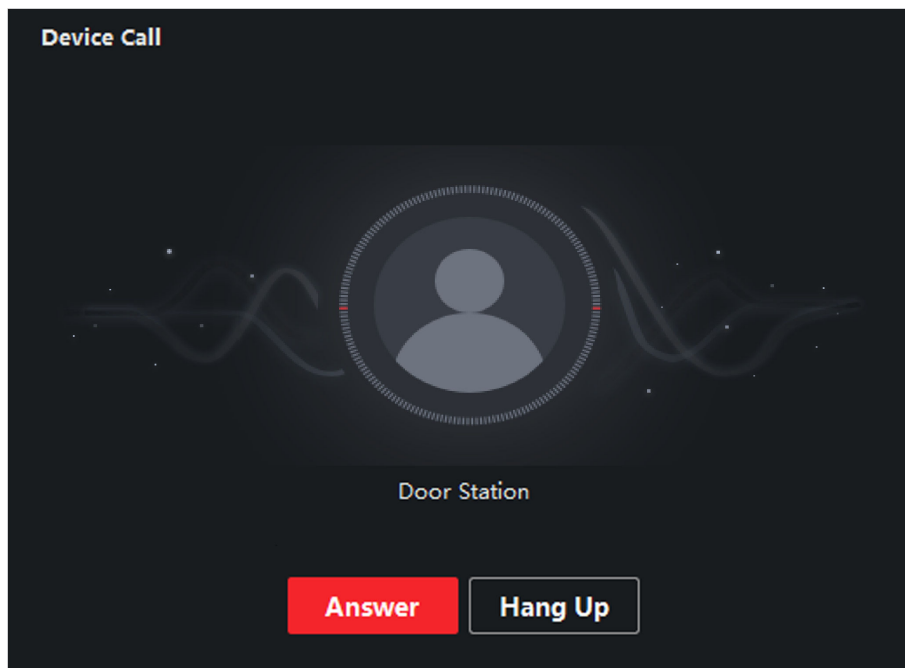



Figure 21-2 Incoming Call

4. Click **Answer** to answer the call.

After the call is answered, you will enter the In Call window.

5. **Optional:** In the In Call window, perform the following operation(s).


Adjust Loudspeaker Volume

Click  to adjust loudspeaker's volume.


End Speaking

Click **Hang Up** to end speaking.

Adjust Microphone Volume

Click  to adjust the microphone's volume.

Open Door

When an indoor station is linked with a door station, click  to open the door linked with the door station.

21.2 View Real-Time Call Logs

You can view details of all the calls, and you can call the residents or export the logs if they are needed.

Steps

1. Click **Access Control** → **Video Intercom** → **Call Log** .

Details of all the calls will be displayed on the right panel including call status, start time, speaking duration, device type and name, and organization and name of resident.


2. **Optional:** Click  to re-dial the resident.

- 3. Optional:** Set search conditions (including call status, device type, and time) on the top of the page to filter call logs.
- 4.** Click **Export** to save the logs (a CSV file) in your PC.

21.3 Release a Notice to Resident

You can send a notice to the residents by one-touch. Four notice types are available: advertising, property, alarm, and notice information.

Steps

1. Click **Access Control** → **Video Intercom** → **Notice** .
2. Click **Add** to open the Create Notice panel.
3. Click  to select the residents you are going to deliver notice to.
4. Enter the required information.



Note

- Up to 63 characters are allowed in the Subject field.
- Up to 1023 characters are allowed in the Content field.
- You can add up to 6 pictures. Each picture should be in JPG format and smaller than 512 KB.


-
- 5.** Click **Send** to send the notice to the selected resident(s).
Information about the sent notices will be displayed on the left panel. Click a notice to view its details on the right panel.
 - 6. Optional:** Click **Export** to save all the notices in your PC.

Chapter 22 Log Search

Two log types are provided: operation log and system log. The operation logs refer to the normal operations that the user did on the client, such as add device, reset password, and start live view; and the system logs record the system information, such as login, logout, log and unlock. You can search the log files and view the log details, including time, user, etc.

Perform the following steps to search the log files.

Steps

1. Enter the Log Search module.
2. Click  to specify the start time and end time.




Note

You can search the logs within one month.

3. Select a user to search the log files which are generated when this user log into the client.
4. Select **Operation Log** or **System Log** as log type.
5. Click **Search**.

The log files between the start time and end time will be displayed on the list. You can check the operation time, type and other information of the logs.

6. **Optional:** Perform the following operations if there are too many log files.

Filer Click  on each table header and select to filter the logs.

Sort Click the table header to sort the logs by the time or letter sequence.

Chapter 23 User Management

To improve the system security, the administrator should create different account for different user, and assign different permissions to the user. To avoid different people sharing the same user account, we recommend you manage the user accounts periodically.

23.1 Add User

The super user and administrator can add new users, and assign different permissions for different users if needed.

Perform this task to add an user account.

Steps



The user account you registered to log in the software is set as the super user.

1. Enter the User Management module.
2. Click **Add User** to show user information area.
3. Select the user type from the drop-down list.

Administrator

The administrator account has all permissions by default, and can modify the passwords and permissions of all operators and its own.

Operator

The operator account has no permission by default and you can assign the permissions manually. An operator can only change the passwords of its own account and the accounts which are added by it.

4. Enter the user name, password, and confirm password as desired.
-



The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

5. Check the checkboxes to assign the permissions to the created user.
6. **Optional:** Click **Default Value** to restore the default permissions of this user.

7. Click **Save**.



Up to 50 user accounts can be added for the client software.

After created user account successfully, the user account is added to the user list on the Account Management page.

8. **Optional:** Perform the following operations after the user account is created.

Edit User Click a user from the list to edit the user information.



Only the password of the super user can be edited.

Delete User Select the user from the list and click **Delete User**.



You cannot delete the super user.

23.2 Change User's Password

The administrator can change normal user's password without entering the old password, while the administrator should enter the old password when changing the password of itself.

Before You Start

Add user to the software client.

Steps

1. Enter the User Management module.
 2. Select the user need to be change password, click **Change**.
 3. **Optional:** Enter the old password.
-



When changing the administrator's password, you need to enter the old password first.

4. Enter the new password and confirm the password.
5. Click **OK**.

Chapter 24 System Configuration

The system parameters, including general parameters, live view and playback parameters, image parameters, file saving paths, etc., can be configured.

24.1 Set General Parameters

You can configure the frequently-used parameters, including log expired time, network performance, etc.

Steps

1. Enter the System Configuration module.
2. Click **General** tab to enter the General Settings page.
3. Configure the general parameters.

Log Expiry Date

The time for keeping the log files. Once exceeded, the files will be deleted.

Maximum Mode

Select **Maximize** or **Full Screen** as the maximum mode. **Maximize** mode can maximize the display and show the taskbar. **Full Screen** mode can display the client in full-screen mode.

Network Performance

Set the network conditions to **Normal**, **Better** or **Best**.

Enable Keyboard and Joystick

Enable the keyboard or joystick. After enabled, you can set the shortcuts for the keyboard and joystick.



Note

For details, refer to ***Set Keyboard and Joystick Shortcuts*** .

Detect New Software Version

After enabled, the client can automatically detect the new software version and remind the user to upgrade the software.

Automatic Time Synchronization

Automatically synchronize the time of the added devices with the time of the PC running the client at a specified time point.

Auto-Upgrade Device

Set the upgrading mode after the new version of device are detected.

Disable

After enabled, the client will not download the firmware package and upgrade even if the client detects a new version of the client.

Prompt Me If Download and Upgrade

After the client detects a new version of the device, it will prompt the user whether to download the firmware package and upgrade.

Download and Prompt Me If Upgrade

After the client detects the new version of the device, it will download the firmware package automatically, and prompt the user whether to upgrade.

Download and Prompt Automatically

After the client detects the new version of the devices, it will download the firmware package and upgrade the new version automatically.

You need to set a schedule in the **Upgrade Time** field, during which the client upgrades the new version automatically.

Cloud P2P Region

Select the server's region for cloud P2P, you can select the region you belong to or the nearest region around.

4. Click **Save**.

24.2 Set Live View and Playback Parameters

You can set the parameters for live view and playback, including picture format, pre-play duration, etc.

Steps

1. Enter the System Configuration module.
2. Click **Live View and Playback** tab.
3. Configure the live view and playback parameters.

Picture Format

Select **JPEG** or **BMP** as the image format for storing pictures.



Note

If **Display Temperature on Captured Pictures** switch is set to ON, JPEG is selected as the image format by default and cannot be changed.

Merge Downloaded Video Files

Set the maximum size of merged video file for downloading the video file by date.

Search Video Files Stored in

Search the video files stored in the local device, in the storage server, or both in the storage server and local device for playback.

Pre-play for

Set the pre-play time for event playback. By default, it is 30s.

Prioritize Playback of Video Files on Storage Server

Play back the video files recorded on the storage server preferentially. Otherwise, play back the video files recorded on the local device.

Resume Latest Live View Status After Restart

Resume the latest live view status after you log into the client again.

Disconnect Background Videos in Single Live View

In multiple-window division mode, double-click a live video to display it in 1-window division mode, and the other live videos will be stopped for saving the resource.

Enable Wheel for Zoom

Use the mouse wheel for zoom in or out of the video in PTZ mode, or for zoom in or restoring of the video in digital zoom mode. In this way, you can directly zoom in or out (or restore) the live video by scrolling the mouse.

Skip Unconcerned Video during VCA Playback

Skip the unconcerned video during VCA playback and the unconcerned video will not be played during VCA playback.

4. Click **Save**.

24.3 Set Image Parameters

The image parameters of the client can be configured, such as view scale, play performance, etc.

Steps

1. Open the System Configuration page.
2. Click **Image** tab to enter the Image Settings interface.
3. Configure the image parameters.

View Scale

The view scale of the video in live view or playback. It can be set as **Full Screen**, **4:3**, **16:9**, or **Original Resolution**.



Note

You can also set the view scale in Live View module. For details, refer to *Live View* .

Play Performance

The play performance of the live video. It can be set as **Shortest Delay**, **Balanced**, or **Fluency**. You can also select **Custom** and specify the frames according to actual needs.

Auto-change Stream Type

Change the video stream (main stream or sub-stream) automatically in live view according to the size of the display window.

 **Note**

When the window division is larger than 9, it will switch to sub-stream automatically.

Hardware Decoding Preferred

Set to enable decoding by hardware for live view and playback. Hardware Decoding can provide better decoding performance and lower CPU usage when playing the HD videos during live view or playback.

Enable Highlight

Mark the detected objects with green rectangles in live view and playback.

Display Transaction Information

Display the transaction information on the live view image.

VCA Rule

Display the VCA rule in the live view.

Enable Frame Extracting for High-speed Playback

When play back the video in high-speed (8x speed and above), you can disable this function to make the image of playback more fluent to view the details.

Display Target's Pattern

After enabled, you can view the target person's motion track on the view window.

The device should support this function.

Overlay Rules on Captured Picture

For the thermal device, set to display the temperature information and fire source information on the captured pictures.

 **Note**

After enabled this function, the Picture Format in **System Configuration → Live View and Playback** will change to JPEG and is not editable.

4. Click **Save**.

24.4 Set Picture Storage

The captured pictures triggered by the events on the devices, can be saved in the PC running the iVMS-4200 Service. The picture storage location can be manually set.

Steps

1. Enter the System Configuration module.
2. Click **Event Picture Storage**.
3. Set the **Store Pictures in Server** switch to on.
All the disks of the PC running the service will show.

4. Select the disk to save the pictures.



Note





The default saving path is: Disk/iVMS-4200alarmPicture

5. Click **Save**.

24.5 Set Alarm Sound

When the event, such as access control event, is triggered, the client can be set to give an audible warning and the sound of the audible warning can be configured.

Steps

1. Open the System Configuration page.
 2. Click **Alarm Sound** tab to enter the Alarm Sound Settings page.
 3. **Optional:** Click  and select the audio files from the local path for different events.
 4. **Optional:** Add customized alarm sound.
 - 1) Click **Add** to add customized alarm sound.
 - 2) Double click the **Type** field to customize the alarm sound name as desired.
 - 3) Click  and select the audio files from the local path for different alarms.
 5. **Optional:** Click  for a testing of the audio file.
 6. **Optional:** Click  in the Operation column to delete the custom sound.
 7. Click **Save**.
-



Note

The format of the audio file can only be WAV.



24.6 Set Access Control and Video Intercom Parameters

You can configure the access control and video intercom parameters according to actual needs.

Steps

1. Open the System Configuration page.
2. Click the **Access Control & Video Intercom** tab.
3. Input the required information.

Ringtone

Click  and select the audio file from the local path for the ringtone of indoor station.
Optionally, you can click  for a testing of the audio file.

Max. Ring Duration

Specify the seconds that the ring will last for at most. The maximum ring duration can be set from 15s to 60s.

Max. Speaking Duration with Indoor Station

Specify the seconds that the call with indoor station will last for at most. The maximum speaking duration between indoor station and the client can be set from 120s to 600s.

Max. Speaking Duration with Door Station

Specify the seconds that the call with door station will last for at most. The maximum speaking duration between door station and the client can be set from 90s to 120s.

Max. Speaking Duration with Access Control Device

Specify the seconds that the call with access control device will last for at most. The maximum speaking duration between access control device and the client can be set from 90s to 120s.


4. Click **Save**.

24.7 Set File Saving Path

The video files from manual recording and the captured pictures are stored on the local PC. The saving paths of these files can be set.

Perform the following task when you need to set the file saving path.

Steps

1. Open the System Configuration page.
2. Click **File** tab to enter the File Saving Path Settings page.
3. Click  and select a local path for the files.
4. Click **Save**.

24.8 Set Icons Shown on Toolbar



The icons and the order on the toolbar in the live view and playback window can be customized. You can set to display what icons and set the icon order.

Perform the following task when you need to set icons shown on Toolbar.

Steps

1. Enter the System Configuration module.
2. Click **Toolbar** tab to enter the Toolbar Settings page.
3. Set **Enable Screen Toolbar Display** switch to ON to enable displaying the toolbar on in the live view and playback window.
4. Click the required icon to display on the toolbar.
5. **Optional:** Drag the icon to set the icon order when displaying on the toolbar.

Table 24-1 Icons on Live View Toolbar

	Stop Live View	Stop the live view in the display window.
	Capture	Capture the picture in the live view process. The capture picture is stored in the PC.













	Record	Start manual recording. The video file is stored in the PC.
	PTZ Control	Start PTZ mode for speed dome. Click and drag in the view to perform the PTZ control.
	Two-way Audio	Start the two-way audio with the device in live view.
	Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Instant Playback	Switch to the instant playback mode.
	Remote Configuration	Open the remote configuration page of the camera in live view.

Table 24-2 Icons on Playback Toolbar

	Capture	Capture the picture in the live view process. The capture picture is stored in the PC.
	Record	Start manual recording. The video file is stored in the PC.
	Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Download	Download the video files of the camera and the video files are stored in the PC.
	VCA Playback	Set the VCA rules. For more details, refer to VCA Playback .
	Tag Control	Add default or custom tag for the video files to mark the important video point. You can also edit the tag.

6. Click **Save**.

24.9 Set Keyboard and Joystick Shortcuts

The keyboard can be connected to the client and be used to control the PTZ cameras. You can set the shortcuts for keyboard and joystick to get quick and convenient access to the commonly used actions.

Perform this task when you need to set keyboard and joystick shortcuts.

Steps

Note

This configuration page will display after enabling keyboard and joystick in General Settings. For details, refer to **Set General Parameters** .

1. Enter the System Configuration module.

2. Click **Keyboard and Joystick** to show the Keyboard and Joystick Shortcut Settings area.
3. Select the COM port from the drop-down list for keyboard if the keyboard is connected to the PC installed with the client.



Note

You can enter the Device Manger of the PC to check the COM port, which the keyboard is connected to.

4. Set shortcuts for keyboard and joystick.
 - 1) Select a certain function name on Function column.
 - 2) Double-click the item field under the PC Keyboard, USB Joystick or USB Keyboard column.
 - 3) Select the compound keys operation or number from the drop-down list to set it as the shortcuts for the function of the keyboard or USB joystick.
5. Click **Save**.

Example

For the **Focus (+)** function, if you set **Home**, **1**, and **F1** as the shortcuts of the PC Keyboard, USB Joystick and USB Keyboard, you can press the Home key on PC keyboard, control the joystick to the 1 direction, or press F1 key on USB keyboard to zoom in.

24.10 Set Email Parameters

An email notification can be sent when an event occurs. To send the email to some specified receivers, the settings of the email need to be configured before proceeding.

Steps

1. Enter the System Configuration module.
2. Click **Email** tab to enter the Email Settings interface.
3. Enter the required information.

SMTP Server

The SMTP server IP address of host name (e.g., smtp.263xmail.com)

Encryption Type

You can check the radio to select **Non-Encrypted**, **SSL**, or **STARTTLS**.

Port

Enter the communication port used for SMTP. The port is 25 by default.

Sender Address

The email address of the sender.

Security Certificate (Optional)

If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

User Name

Enter the user name of the sender email address if **Server Authentication** is checked.

Password

Enter the password of the sender Email address if **Server Authentication** is checked.

Receiver 1 to 3

Input the email address of the receiver. Up to 3 receivers can be set.

4. **Optional:** Click **Send Test Email** to send an email to the receiver for test.
5. Click **Save**.

24.11 Manage Security Authentication

For the data security purpose, the security certificate of clients and added servers (stream media server) should be same. You can set the verify certificate is required or not when enabling transmission encryption using TLS (Transport Layer Security) protocol.

Before adding the stream media server to the client, you should export the service certificate from the client service, and import it to the stream media server. If multiple clients use the same server, you should make the security certificates of the clients and the server same with each other.

24.11.1 Export Certificate from Service Management

You can export the security certificate from the current client service and import the exported certificate file to the stream media server or other clients.

Steps

1. Enter the Service Management.
2. Click **Export** to save the certificate file in the local PC.



Note

The certificate file is in XML format.

What to do next

After exporting the certificate, you can copy the certificate to the PC installed with the client and import it to the stream media server, or to other clients.

For importing to the stream media server, refer to ***Import Certificate to Stream Media Server*** .

24.11.2 Import Certificate to Client

If there are multiple clients accessing the same steam media server, you should import the same certificate to the clients and server.

Before You Start

Make sure you have exported the security certificate from one of the client service.

 **Note**

For details, refer to *Export Certificate from Service Management* .

Steps

1. Copy the certificate file exported from other client to the local PC.
 2. Enter the System Configuration module.
 3. Click **Security Authentication** tab to enter the security authentication setting interface.
 4. Click **Import**.
 5. Select the certificate file from your local PC and click **Open**.
-

 **Note**

Please restart the client to take effect.

24.11.3 Certificate Verification for Transmission Encryption

On the Security Authentication page, you can set the device certificate verification is required or not for transmission encryption.

Click **System Configuration** → **Security Authentication** to enter the security authentication interface. Select the Verify Certificate as **Yes** or **No**.

Yes


You must put the device certificate to the designed directory if you enable transmission encryption when adding device. And the device will be added with transmission encryption and the certificate will be verified, which improves the security level.

No

The device certificate is not required if you enable transmission encryption when adding device. And the device will be added with transmission encryption.

Chapter 25 Operation and Maintenance

You can perform maintaining operations in the menu to ensure a smooth and convenient usage of the client.

Click  in the upper-right corner, and then click **File/System/Tool** to perform the following operations.

Open Log File

You can open a log file saved in your local PC or log files of the client.

Import/Export Configuration File

You can import configuration files from local PC to the client if needed, and vice versa.

Auto Backup

Select day and time to backup configuration files and data in database, or restore the backed up data.

Skin

Change the skin of the client, including bright-color series and black-color series.

Batch Time Sync

Synchronize selected devices' time with your PC time.

Message Queue

After configuring email linkage, the triggered event(s) will be displayed here. Select an event and cancel sending the an email to the receiver.

Appendix A. Custom Wiegand Rule Descriptions

Take Wiegand 44 as an example, the setting values in the Custom Wiegand tab are as follows:

Custom Wiegand Name	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Mode	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Wiegand Data

Wiegand Data = Valid Data + Parity Data

Total Length

Wiegand data length.

Transportation Rule

4 bytes. Display the combination types of valid data. The example displays the combination of Card ID and Manufacturer Code. The valid data can be single rule, or combination of multiple rules.

Parity Mode

Valid parity for Wiegand data. You can select either odd parity or even parity.

Odd Parity Start Bit, and Length

If you select Odd Parity, these items are available. If the odd parity start bit is 1, and the length is 12, then the system will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0. (Bit 0 is the first bit.)

Even Parity Start Bit, and Length

If you select Even Parity, these items are available. If the even parity start bit is 12, and the length is 12, then the system will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

XOR Parity Start Bit, Length per Group, and Total Length

If you select XOR Parity, these items are available. Depending on the table displayed above, the start bit is 0, the length per group is 4, and the total length is 40. It means that the system will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits. (The result length is the same as the length per group.)

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

Appendix B. Troubleshooting

Here are some common symptoms when operating the client software. We provide the possible causes and corresponding solutions to solve the problems.

B.1 Failed to get the live view of a certain device.

Problem

Failed to get the live view of a certain device.

Possible Reasons

- Unstable network or the network performance is not good enough.
- The device is offline.
- Too many accesses to the remote device cause the load of the device too high.
- The current user has no permission for live view.
- The version of the client software is below the needed version.

Solutions

- Check network status and disable other not in use process on your PC.
- Check the device network status.
- Restart the device or disable other remote access to the device.
- Log in with the admin user and try again.
- Download the client software of the latest version.

B.2 Local recording and remote recording are confused.

Problem

Local recording and remote recording are confused.

Solutions

- The local recording in this manual refers to the recording which stores the video files on the HDDs, SD/SDHC cards of the local device.
- The remote recording refers to the recording action commanded by the client on the remote device side.

B.3 Failed to download the video files or the downloading speed is too slow.

Problem

Failed to download the video files or the downloading speed is too slow.

Possible Reasons

- Unstable network or the network performance is not good enough.
- The NIC type is not compatible.
- Too many accesses to the remote device.
- The current user has no permission for playback.
- The version of the client software is below the required version.

Solutions

- Check network status and disable other not in use process on your PC.
- Directly connect the PC running the client to device to check the compatibility of the NIC card.
- Restart the device or disable other remote access to the device.
- Log in with the admin user and try again.
- Download the client software of the latest version.

Appendix C. FAQ (Frequently Asked Questions)

Here are some frequently asked questions when operating the client software. We provide the corresponding answers to help the users to solve the problems.

C.1 During live view, why an error message with error code 91 prompts ?

Question

During live view, why an error message with error code 91 prompts ?

Answer

For live view of multiple windows, the channel may not support sub stream. You should disable the function of **Auto-change Stream Type** in **System Configuration** → **Image** , and select the appropriate steam type for live view.

C.2 During live view, why the image is blurred or not fluent?

Question

During live view, why the image is blurred or not fluent?

Answer

Check the driver of video card. We highly recommend you update the driver of video card to the latest version.

C.3 Why the memory leaked and the client crashed after running for a while?

Question

Why the memory leak and the client crashed after running for a while?

Answer

In the installation directory of the client software, open the **Setup.xml** file with Notepad and modify the value of **EnableNetandJoystickCheck** to **false**. Restart the client, and if the problem is still not solved, contact our technique support.

C.4 During live view, when getting stream via the Stream Media Server, why an error message with error code 17 prompts?

Question

During live view, when getting stream via the Stream Media Server, why an error message with error code 17 prompts?

Answer

Check the port mapping of Stream Media Server, especially RTSP port.


C.5 How to get better performance of live view and playback when network bandwidth is low?

Question

If the network bandwidth is low, how to get better performance of live view and playback?

Answer

This function should be supported by the device. You can perform the following operations to realize live view in low bandwidth:

- Firstly, after adding the encoding devices to the client, you need to set the camera's streaming protocol.
 1. Enter **Device Management** → **Group**
 2. Select the camera in the Encoding Channel list and click .
 3. In the Edit Camera window, set the **Protocol Type** (for live view) and **Playback Protocol Type** (for playback) as **Adaptive UDP**.

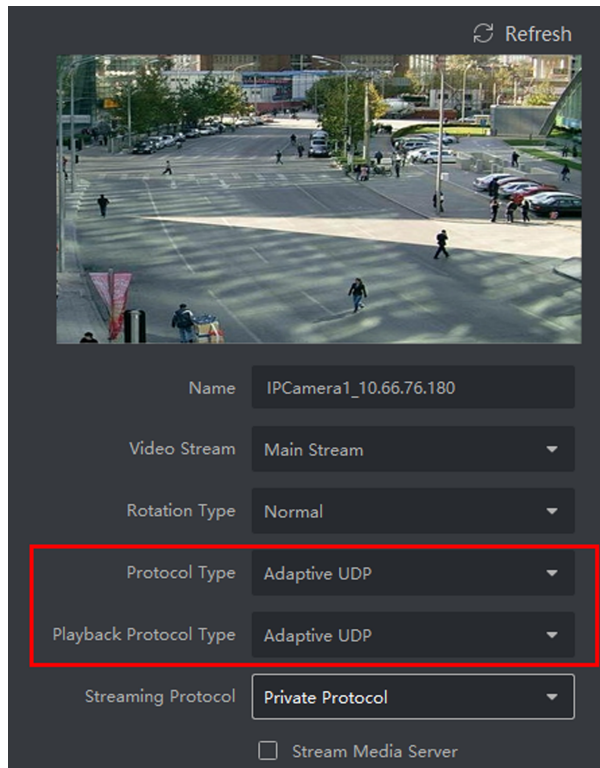


Figure C-1 Set Protocol Type

4. Click **OK** to save the settings.
- Then you need to disable the Auto-change Stream Type function.
 1. Enter **System Configuration** → **Image** .
 2. Disable the switch of **Auto-change Stream Type** function.
- Select stream type for live view.
 1. Enter Main View module.
 2. In the device list on the left, move the cursor to the camera name and click **⋮** → **Stream** .

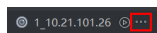


Figure C-2 Select Stream Type

3. For network camera, set the stream type as **Third Stream**.
For DVRs or NVRs, set the stream type as **Virtual Stream**.
4. Start live view.

Appendix D. Error Code

Code	Error Name	Description
iVMS-4200		
317	No videos.	It will be prompted when the user has no permission to play back.
HCNetSDK.dll		
1	Invalid user name or password.	
2	No permission.	The user in the device has no enough permission.
4	Invalid channel number.	It will be prompted in the live view of remote screen control.
5	No more devices can be connected.	
7	Failed to connect the device.	
23	Not supported.	
29	Operation failed.	
43	No buffer.	It will be prompted when adding a device and the device port is occupied by a web server.
55	Invalid IP address.	
56	Invalid MAC address.	
91	The channel does not support the operation.	It will be prompted when failed to get the sub stream.
96	The device is not registered on the DDNS.	
153	The user is locked.	
250	The device is not activated.	
404	Channel No. error or the device does not support the sub stream.	It will be prompted when failed to get the sub stream or the sub stream does not exist.
424	Failed to receive the data for RTSP SETUP.	It will be prompted when adding the live view for the software DVS via external network.
800	No more bandwidth can be used.	
Playctrl.dll		

Code	Error Name	Description
2		The stream is not a Video & Audio stream.
6		The playback window turns black when adopting H.265 in the 64-bit operating system.
SMS		
3		The connection problem between the software and the stream media server.
17		The streaming problem between the stream media server and the device.



See Far, Go Further