

HikCentral Mini Cube V1.4.0

User Manual

Contents

Chapter 1 Learn About HikCentral Mini Cube 1
1.1 Recommended Running Environment 1
1.2 System Configurations and Performance 2
Chapter 2 Get Started 3
2.1 Configure the System Capability 3
2.2 Activate License 4
2.2.1 Activate the License Online 4
2.2.2 Activate the License Offline 5
2.3 Add Devices 6
2.4 Add a Server and View Server Details 10
2.5 Configure User Preference 11
Chapter 3 Video Monitoring 16
3.1 Preparations 16
3.1.1 Add Encoding Devices 16
3.1.2 View and Configure Details of Encoding Devices 17
3.1.3 Add an Alarm for an Encoding Device 21
3.2 Basic Functions Related to Video Monitoring 21
3.2.1 Start Live View / Playback 21
3.2.2 PTZ Control During Live View 25
3.2.3 Monitor via Cameras on the Map 26
3.3 Face Picture Comparison and Human Body Detection 29
3.3.1 Add Face Picture Libraries and Face Pictures 30
3.3.2 View Videos Related to Face and Human Body Recognition 31
3.3.3 Search for Recognized Face Pictures and Human Body Pictures 32
3.3.4 Search Targets by a Picture 34
3.4 Vehicle Monitoring 35

3.4.1 Add Vehicle Lists and Vehicles 35
3.4.2 View Video Related to Vehicle Monitoring 37
3.4.3 Search and Export ANPR Events 38
3.5 Smart Search / VCA 39
3.5.1 Compatible NVR Series for Smart Search 40
3.5.2 Configuration for NVR and Network Camera 40
3.6 AcuSearch 41
3.7 AcuSeek 44
3.8 Generate and View People Counting Report 47
3.9 (Optional) Local Configurations Related to Video Monitoring 49
Chapter 4 Access Control and Video Intercom 50
4.1 Preparations 51
4.1.1 Add Devices 51
4.1.2 View Details of a Device 52
4.1.3 View Details of a Door 54
4.2 Add Departments and Persons 55
4.2.1 Configure Credential-Related Parameters 58
4.2.2 Protect Profile Pictures 58
4.3 Add and Assign Access Levels 60
4.4 Add an Alarm 63
4.5 Real-Time Monitoring of Doors 65
4.5.1 Monitor Doors and Control Door Status 66
4.5.2 Display and Control Doors on the Map 68
4.6 Video Intercom 70
4.7 Import Person Authentication Events from Devices to the Client 71
4.8 Search for Access Events 73
4.9 Display Statistics of Person&Credentials, Access Levels, and Access Events 75
Chapter 5 Attendance 78

5.1 Enable the Attendance Capability 78
5.2 Quick Schedule 78
5.3 Apply for a Leave / Business Trip 87
5.3.1 Add a Leave Type 87
5.3.2 Apply for a Leave / Business Trip 88
5.4 Check-In/Out Correction 90
5.5 View Attendance Records 91
5.5.1 Transaction 92
5.5.2 Attendance Calculation 94
Chapter 6 Visitor 97
6.1 Enable the Visitor Capability 97
6.2 Basic Configuration 97
6.2.1 Role and Permission 97
6.2.2 Visitor Group and Access Level Configuration 98
6.2.3 Card Configuration 99
6.3 Visitor Reservation and Approval 101
6.3.1 Option 1: Admin Reservation 101
6.3.2 Option 2: Visitor Self-Service 103
6.4 Visitor Check-In & Check-Out 104
6.5 Visitor List Management 104
6.6 Statistic Reports & Logs 106
Chapter 7 Alarm Detection 109
7.1 Enable the Alarm Detection Capability 109
7.2 Add Security Control Devices 109
7.3 Monitoring of Security Control Devices 111
7.4 Event and Alarm 114
7.5 Role and Permission 115
7.6 Display Security Control Panel Statistics 115

Chapter 8 Server Cascading 117
8.1 Introduction 117
8.2 Add a Cascaded Server 117
8.3 Operations After Adding Cascaded Servers 119
8.4 Cascaded Server Management Capabilities 120
Chapter 9 Main Panel for Monitoring and Control 122
Chapter 10 Search 125
10.1 Search for Detected Vehicles or Persons by Cameras/Doors 126
10.2 Search for Detected Persons or Vehicles in VCA Areas 128
10.3 Search for Detected Persons/Vehicles by Features 128
Chapter 11 Event and Alarm 130
11.1 Supported Triggering Events 130
11.2 Event Subscription 147
11.3 Add an Alarm 148
11.4 Supported Linkage Actions 149
11.5 Alarm List 151
11.6 Search for and Export Alarms 151
11.7 Local Configuration About Event and Alarm 152
Chapter 12 Cloud Connection 153
Chapter 13 Management of Users and Roles 155
13.1 Add a Local User 155
13.2 Add a Cloud User 155
13.3 Supported Operations on the User List 157
13.4 Add a Role 157
13.5 Configure Account Security Rules 161
13.6 Reset Login Password 161
Chapter 14 System Configuration 163
14.1 Configure Email Parameters 163

14.2 Add or Edit a Holiday 163
14.3 Configure NTP Synchronization / Device Access Protocol / WAN Access / NIC, and Reset Network Info 164
14.4 Use SSL/TLS Certificate for HTTPS Connections 167
14.5 Configure Service Component Certificate 170
14.6 Privacy and Security 170
Chapter 15 Maintenance 171
15.1 Generate and Display Maintenance Report 171
15.2 Search for Notifications 177
15.3 Search for System Logs 178
Appendix A. Product Usage Restrictions: Scenarios & Guidelines 180
Appendix B. Third-Party Device Integration 182
B.1 Add Third-Party Devices 182
B.2 Video Monitoring 183
B.3 Supported Alarms 185
B.4 Linkage Actions 186
Appendix C. Symbol Conventions 187
Appendix D. Legal Information 188

Chapter 1 Learn About HikCentral Mini Cube

The HikCentral Mini Cube is a light-weight Video Management Software product which requires limited system resources providing an enhanced user experience. It integrates configuration and application functions relating to monitoring of video, ANPR, access control, and video intercom.

The system has a simple and clear interactive design and guidance that allows users to quickly get started. It supports quickly importing the configuration file downloaded from the iVMS-4200. The product is compatible with third-party devices.

The Mobile Client is provided with features of live view, playback, alarm checking, etc.

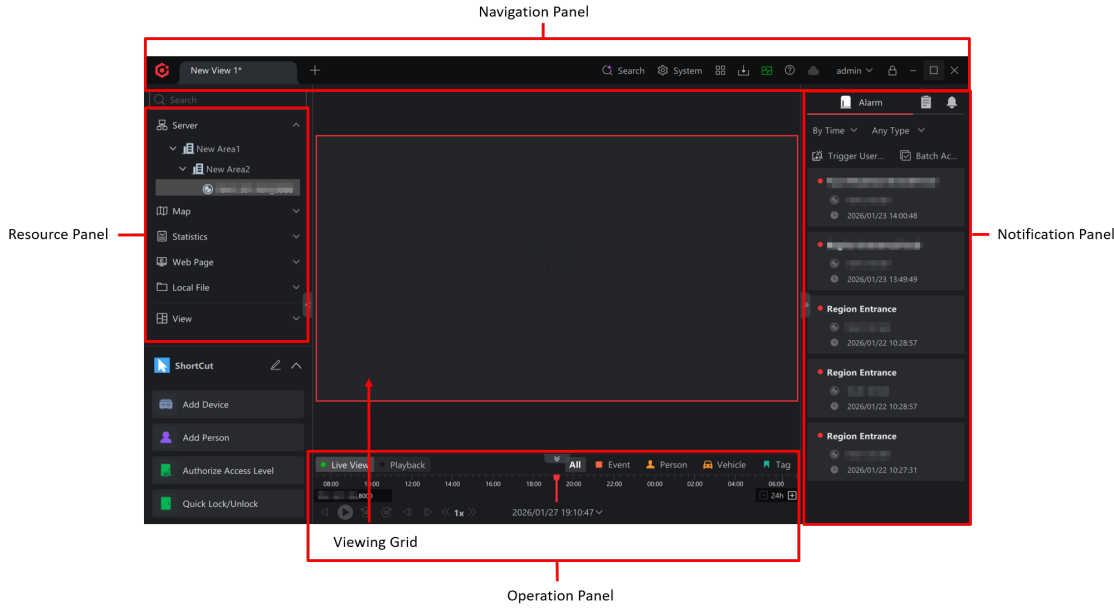


Figure 1-1 Main Page

See ***Main Panel for Monitoring and Control*** for details about the main page.

1.1 Recommended Running Environment

Table 1-1 Recommended Running Environment

Platform	OS
Server	• Microsoft® Windows Server 2025 • Microsoft® Windows Server 2022 • Microsoft® Windows Server 2019 64-bit • Microsoft® Windows Server 2016 64-bit

Platform	OS
	• Microsoft® Windows 11 64-bit • Microsoft® Windows 10 64-bit
Desktop	• Microsoft® Windows Server 2025 • Microsoft® Windows Server 2022 • Microsoft® Windows Server 2019 64-bit • Microsoft® Windows Server 2016 64-bit • Microsoft® Windows 11 64-bit • Microsoft® Windows 10 64-bit
Mobile Client	• iOS 14.0+ • Android 8.0+

1.2 System Configurations and Performance

The system performance is tested based on the following configurations.

Table 1-2 Detailed Performance

Features	Out of Box	Max
Video Channels	64	128
Doors	8	32
Face & Body Recognition Channels	2	16
ANPR Channels	2	8

Chapter 2 Get Started

This chapter is designed to help you quickly understand and deploy the product as a guideline for setting up and initial use.

2.1 Configure the System Capability

The system supports the configuration of service capabilities: **Access Control**, **Video**, **Alarm Detection**, **Visitor**, and **Attendance**.

You can configure the service capability via two options:

- During the initial deployment and setup process.
- On the Home page, go to **System → System Configuration → Service Capability** .

By default, all capabilities are enabled. For Access Control or Video:

- At least one business capability must remain active. If you disable the only active one, another will automatically activate to maintain system operations.
- If devices of a specific type (Access Control and/or Video) have been added to the system, the corresponding service capability cannot be disabled. You must remove these devices from the system before disabling the capability.

Only enable Video

When only enabling **Video**, the following features are disabled:

- Access control and video intercom devices are not allowed to add when adding devices.
- **Access Control** on the device management page, and **Video Intercom**.
- The pre-defined **ShortCut** for access control in the main panel for monitoring and control.
- On the Home page, access control-related records in **Alarm**, **Event**, and **Notifications** in the right navigation bar.
- Access control operation in **Permission Item** when adding roles in **Account Security**.
- On the Home page, the corresponding device type filter conditions in **Map** in the left navigation bar.
- The access control events and linkage action in **Event and Alarm**.
- The ISAPI protocol type when manually adding devices.
- The **Save Model Data of Profile Picture Only** feature (person profile picture will be converted to unreadable modeling data for saving) in Profile Picture.

Only enable Access Control

When only enabling **Access Control**, the following features are disabled:

- Encoding devices and streaming servers are not allowed to add when adding devices.
- On the system page, hide the entry of **Face Picture Library** and **Vehicle**.
- Video-related operation in **Permission Item** when adding roles in **Account Security**.

- The retrieval of **Vehicle Passing Record**, **Face Capture**, and video-related events in **Alarm** and **Notifications**.
- **Person** and **Vehicle** on the right side of the Main Panel.
- Video-related events and linkage action in **Event and Alarm**.
- On the Home page, the corresponding device type filter conditions in **Map** in the left navigation bar.
- The pre-defined **ShortCut** for video in the Main Panel.

When Enabling Alarm Detection

See ***Alarm Detection*** .

When Enabling Visitor and Access Control

See ***Visitor*** .

When Enabling Attendance and Access Control

See ***Attendance*** .

2.2 Activate License

After installing the client, you will have a temporary License for a specified number of devices and limited functions. To ensure the proper use of the client, you can activate the Server to access more functions and manage more devices. If you do not want to activate the Server now, you can skip this chapter and activate it later.

Note

- Only the admin user can perform the activation, update, and deactivation operation.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to our technical support engineers.

On the License Overview page, you can click to select available resources to configure Facial and Human Body Recognition cameras or ANPR cameras.

On the Home page, click the user name in the top-right corner, then select **License Management** to open the license management panel. Click the **Activate License** button in the lower left corner to proceed.

2.2.1 Activate the License Online

If your computer can connect to the Internet, you can activate the Server in online mode.

Steps

1. Select **Online Activate** as the activation type to activate the license in online mode.
2. Enter the activation code received when you purchased your License.

If you have purchased more than one Licenses, you can click **Add** and enter other activation codes.

Note

The activation code should contain 32 characters (except dashes).

3. Check **I accept the terms of the agreement Hikvision Software User License Agreement** and **I accept the terms of the agreement Data Protection Statement** to open the License Agreement panel and click **OK**.
4. Click **Activate**.

2.2.2 Activate the License Offline

If your computer cannot connect to the Internet, you can activate the License in offline mode.

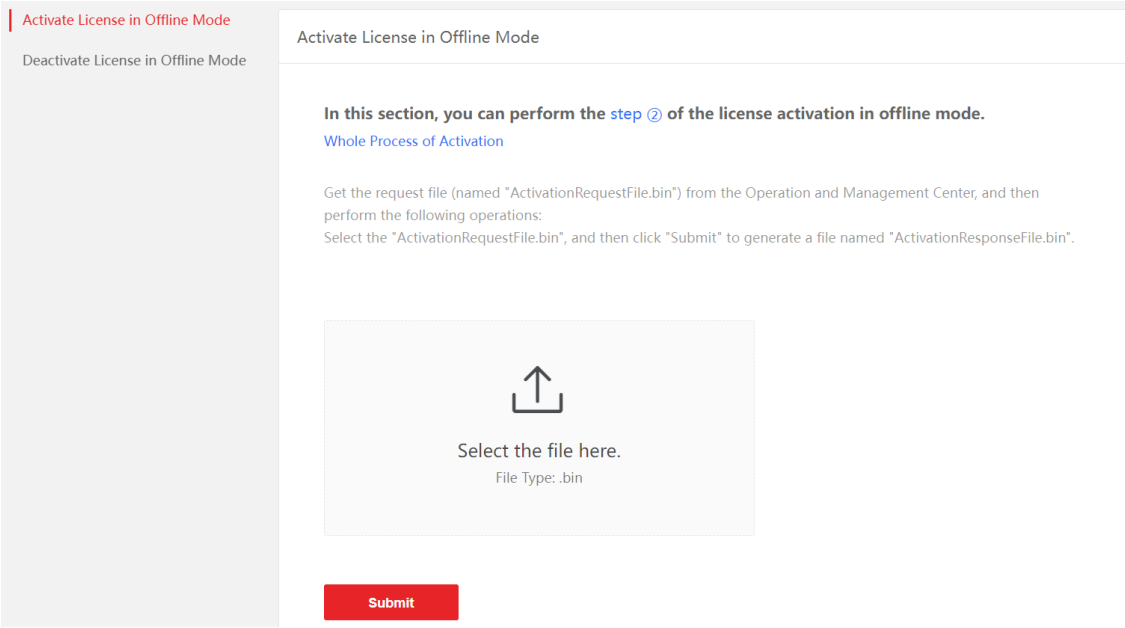
Steps

1. Select **Offline Activate** as the activation type to activate the license in offline mode.
2. Enter the activation code received when you purchased your License.
   If you have purchased more than one Licenses, you can click **Add** and enter other activation codes.

   Note

   The activation code should contain 32 characters (except dashes).
3. Check **I accept the terms of the agreement Hikvision Software User License Agreement** and **I accept the terms of the agreement Data Protection Statement** to open the License Agreement pane and click OK.
4. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Click **View File** to save the request file to the proper directory or the removable storage medium (e.g., USB flash disk) or click on the home page to view downloading records.
5. Copy the request file to the computer that can connect to the Internet.
6. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .



7. Click and then select the downloaded request file.
8. Click **Submit**.

   A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
9. Go back to the **Activate License** panel and click to select the downloaded respond file or drag the file.
10. Click **Activate**.

2.3 Add Devices

You can add encoding devices, access control devices, security control panels, and video intercom devices by auto detect, batch import, manually add, as well as data migration from iVMS-4200.

Add Device

On the Home page, go to **System → Device Management → Add Device** to select supported adding modes: **Auto Detect**, **Batch Import**, and **Manually Add**.

You can also add device(s) by right-clicking an area or through a shortcut.

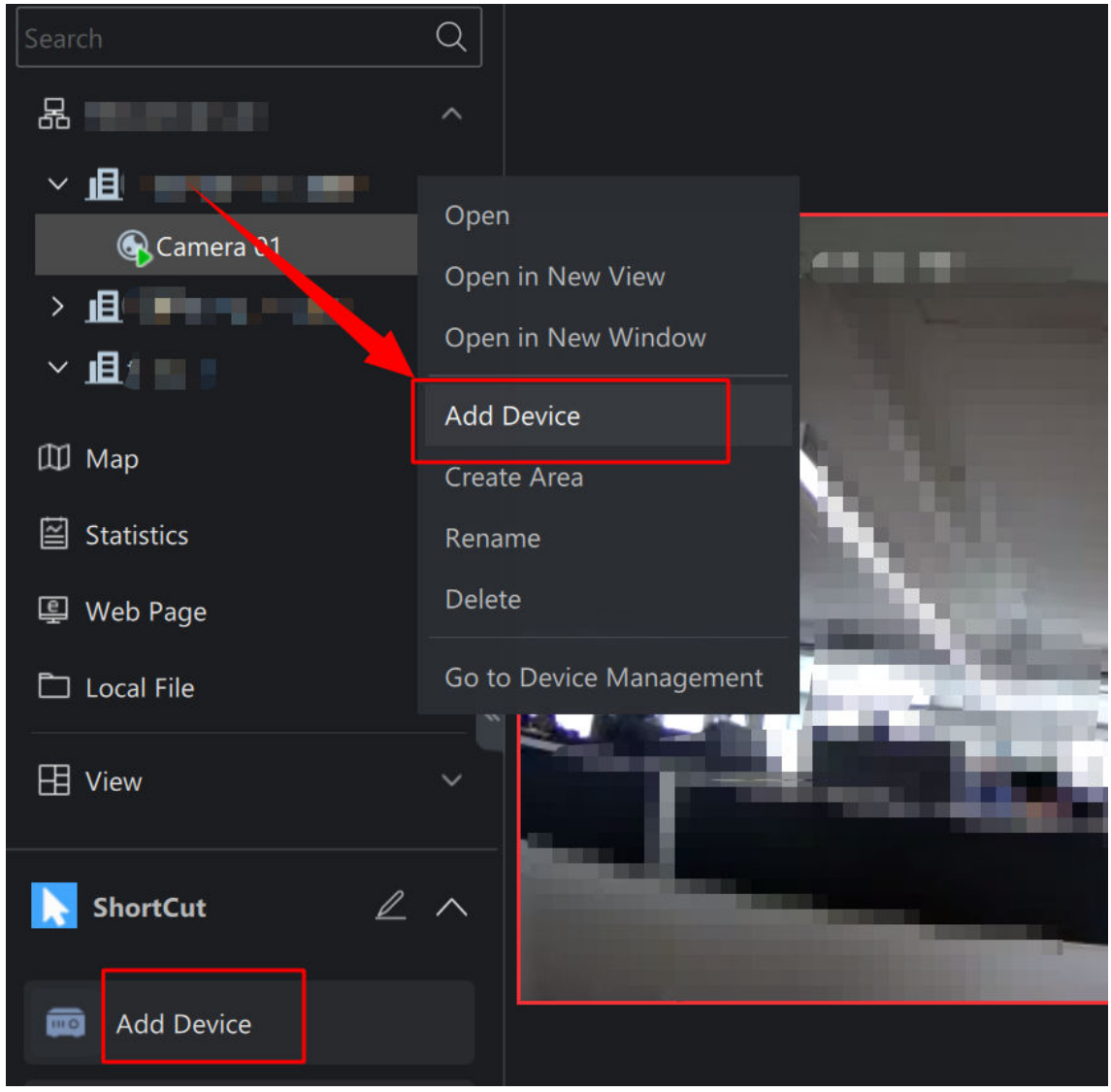


Figure 2-1 Other Entries for Adding Devices

Data Migration

- On the Home page, go to **System → Device Management → Move Now** .
- (Only supported on the Server) On the Home page, go to **User name → Data Migration** .

Table 2-1 Add Device

Mode	Description
Auto Detect	Select this one to detect devices that are on the same LAN as the server or client. You can perform the following operations.

Mode	Description
	• **Specify IP Range** supports discovering all accessible networks by the current client, regardless of whether these networks are on the same network as the client or server. **Note** The feature is only effective when the device supports the ONVIF protocol. • Click to edit Device IP Address and Port number. • Click to reset the password. • Click to filter by **Activated** or **Unactivated**, as well as device type. • If the device status is unactivated, click **Activate** to activate the device before adding it. • Check **Sync Device Name** to sync the device-side name to the platform. The feature is only available when Hikvision Private Protocol or Hikvision ISAPI Protocol is chosen. • Select **Device Time Zone**. The default device time zone is the same as that of the server. If the device time zone matches the server's local time zone, you can set the video storage location to both the recording server and the device. Otherwise, videos can only be stored on the device. The system will apply the manually set time zone to the devices (devices accessed via ONVIF are excluded) every 24 hours.
Batch Import	Select this one if the IP address, port No., ID, and secret key of multiple devices are known. You can quickly add a batch of devices without verifying their validity. Select this one if the device is offline or the device and the server or the client are not on the same LAN. Select **Device Time Zone**. The default device time zone is the same as that of the server. If the device time zone matches the server's local time zone, you can set the video storage location to both the recording server and the device. Otherwise, videos can only be stored on the device. The system will apply the manually set time zone to the devices (devices accessed via ONVIF and third-party SDK protocol are excluded) every 24 hours.
Manually Add	Select this one if the IP address, port No., ID, and secret key of single device are known.

Mode	Description
	You can choose from the following access protocols and enter the required device information. If you have installed addons, you can select protocols specific to those addons. • Hikvision Private Protocol • Hikvision ISUP Protocol • Hikvision ISAPI Protocol • ONVIF Protocol **Note** ◦ You need to enable ONVIF before using this feature for security reasons. ◦ For devices added via ONVIF and third-party SDK protocol, you need to manually set time zone to the devices. ◦ When choosing Hikvision Private Protocol or Hikvision ISAPI Protocol, you can click **Get Device Name** to sync the device name to the platform.
Data Migration from iVMS-4200	Only supported on the server when an admin performs the operation. You can import the following information from iVMS-4200: • Devices and resources (encoding devices and access control devices) • Recording schedules • Person information, credentials, and access level permissions • Access control event records

After adding devices, right-click the device to perform further operations on the device list. Viewing the serial number and version number of cameras under NVRs is supported.

Set Time Zone

Select one or more device(s), click **Time Zone** to set / edit the time zone.

Enable this if you need to set the time zone manually. Otherwise, the system will sync and use the time zone of the device by default.

Note

You can only set time zone for online devices.

If a time synchronization exception occurs, it will be indicated in the **Status** column. Additionally, relevant notifications will appear in the **Notifications** panel on the right side of the Main Panel. For example, if a time exception is detected on a video or access control device, a notification will be displayed as:

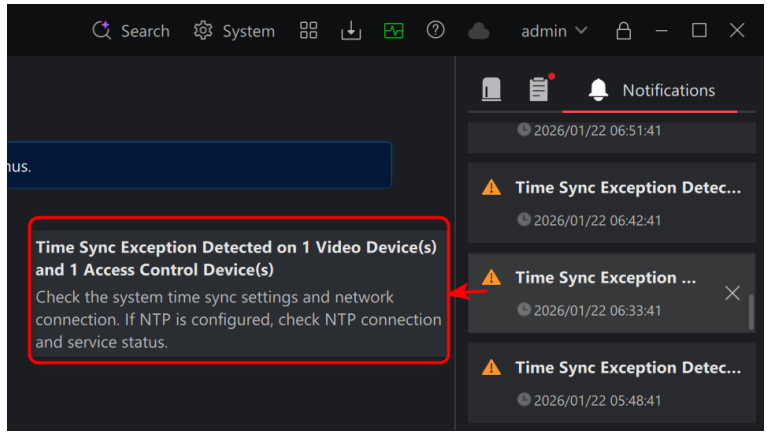


Figure 2-2 Time Sync Exception

Remote Configuration

Hover on one device, then right-click and select **Device Remote Configuration**.

Apply Settings Manually to Access Control Devices

For offline device(s), parameters are stored on the platform. After the device(s) goes online, the stored parameter configurations need to be manually pushed to the device.

- You need to apply platform access control settings (including multi-factor authentication, multi-door interlocking, first person in, and remaining unlocked/locked) to device manually, after you restore device parameters to default values, restore database, or set doors to remain locked/unlocked.
- On the **Access Control** panel, click **Apply Manually**.

See ***System Configurations and Performance*** for the number of devices supported by the client.

Note

For devices configured with the linkage action of capturing, and devices added by Hikvision ISUP Protocol, the pictures from the devices may be transmitted to the Server via HTTP.

2.4 Add a Server and View Server Details

You can add an external streaming server to the system for distributing and streaming the media content in real-time to multiple clients or devices. This setup allows for efficient management of video data, ensuring immediate accessibility as needed.

Add a Server

On the Home page, go to **System → Device Management → Add Server** .
The server is for the live view, playback, video intercom, etc. **Max. Streaming Channel** refers to the max. channel of streams that the streaming server can support.
After adding servers, you can perform further operations on the server list.

View Alarm Configuration

Hover on one server, then right-click and select **View Alarm Configuration** to view and edit the alarm configurations of the corresponding server.

Remote Configuration

Hover on one server, then right-click and select **Configure on Device** to open the device's web configuration page.

View Server Details

Hover on the server, then right-click and select **View Details** to view the specific information of the corresponding server.

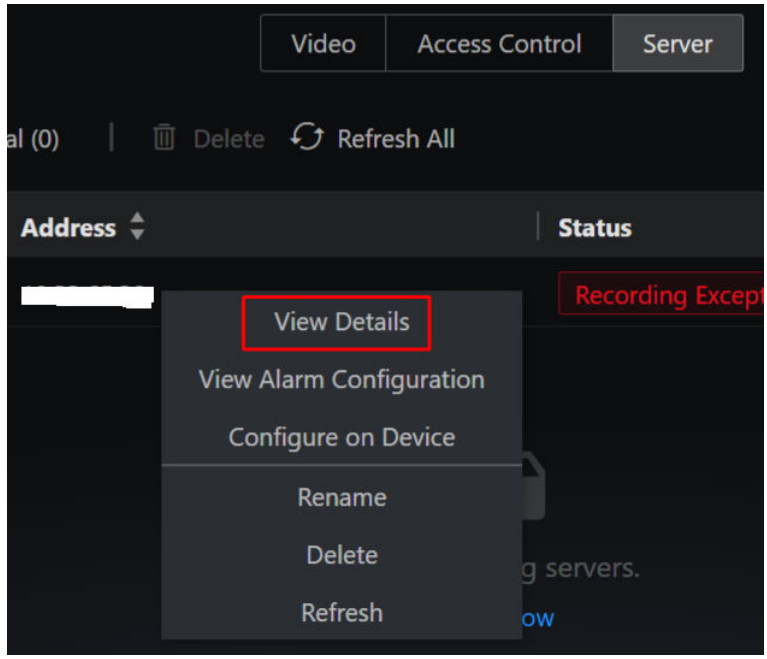


Figure 2-3 View Server Details

You can perform the following operations.

- View the normal and abnormal status under the server name. The abnormal status is displayed by default. Click **More** to view all status information.
- Edit the **Basic Configuration** of the server.

2.5 Configure User Preference

You can configure desktop-specific preferences from different aspects (video playing, alarm notification, and login).

Event and Alarm

In the upper-right corner of the Desktop, go to **User Name** → → **Local Configuration** .

Display

- **Audio**: Enable/disable all alarm-related audio (audible alarm, alarm sound, etc.) for the current client.
- **Pop-Up Window**: Enable/disable all pop-up windows for the current client. The pop-up window will be displayed in the center by default. If you moved it, the new position will be remembered for the next time.

Note

When **Audio** or **Pop-Up Window** is disabled, you can still add relevant linkage actions but they will not come into effect.

Alarm Sound

- **Voice Engine (Requires the Operating System's Support)**: Play the voice text configured (the audible alarm in ***Supported Linkage Actions***), by the voice engine supported by the computer system.
- **Local Audio Files**: Play the uploaded local files. The configured voice text will be irrelevant.

Advanced Settings

In the upper-right corner of the Desktop, go to **User Name** → → **Local Configuration** .

Time Zone

Enable **Display Multiple Time Zones** to display the client and device/server time zone in the list at the same time. You can view multiple time zones when searching for events such as **Alarm**, **Access Control**, **Vehicle Passing Event**, etc., in the **Investigation** page.

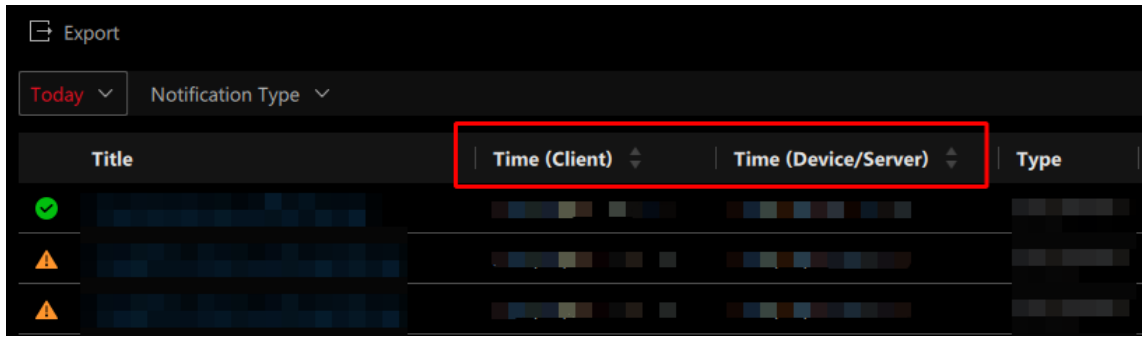


Figure 2-4 Time Zone

File Saving Path

Click and then select a folder as the saving path for files such as images, downloads, manual recordings, etc.

Ringtone

You can customize and preview call ringtones for your device. An audio file, restricted to WAV format, will play as the ringing tone when the device is called.

Note

The feature is available only after access control devices or video intercom devices have been added to the system.

Streaming Access Mode

Define how to access all the added encoding devices and decoding devices.

- **Automatically Judge**: Automatically adjust the access mode according to the domain of devices. If the Desktop is in the same domain as devices, it will get streams directly from devices, otherwise, it will get steams via streaming server.
- **Via Streaming Server**: The Desktop will access devices via streaming severs, which can lower the load of devices. When there are multiple Desktops to get streams from the same device, you can use this mode.

Version Update Notification

Enable this to receive notifications of version updates. Updated version will provide you with latest features with better experience. The cloud server will automatically push updates. If multiple clients are connected, it will notify them to automatically update.

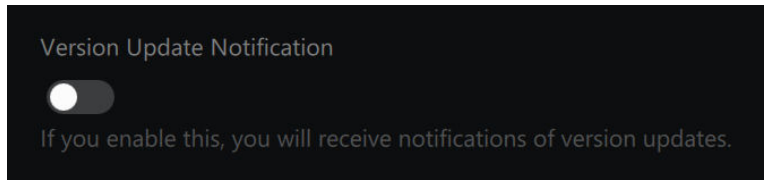


Figure 2-5 Version Update

Basic Video Preference

Right-click on any blank area of the main panel for monitoring and control.

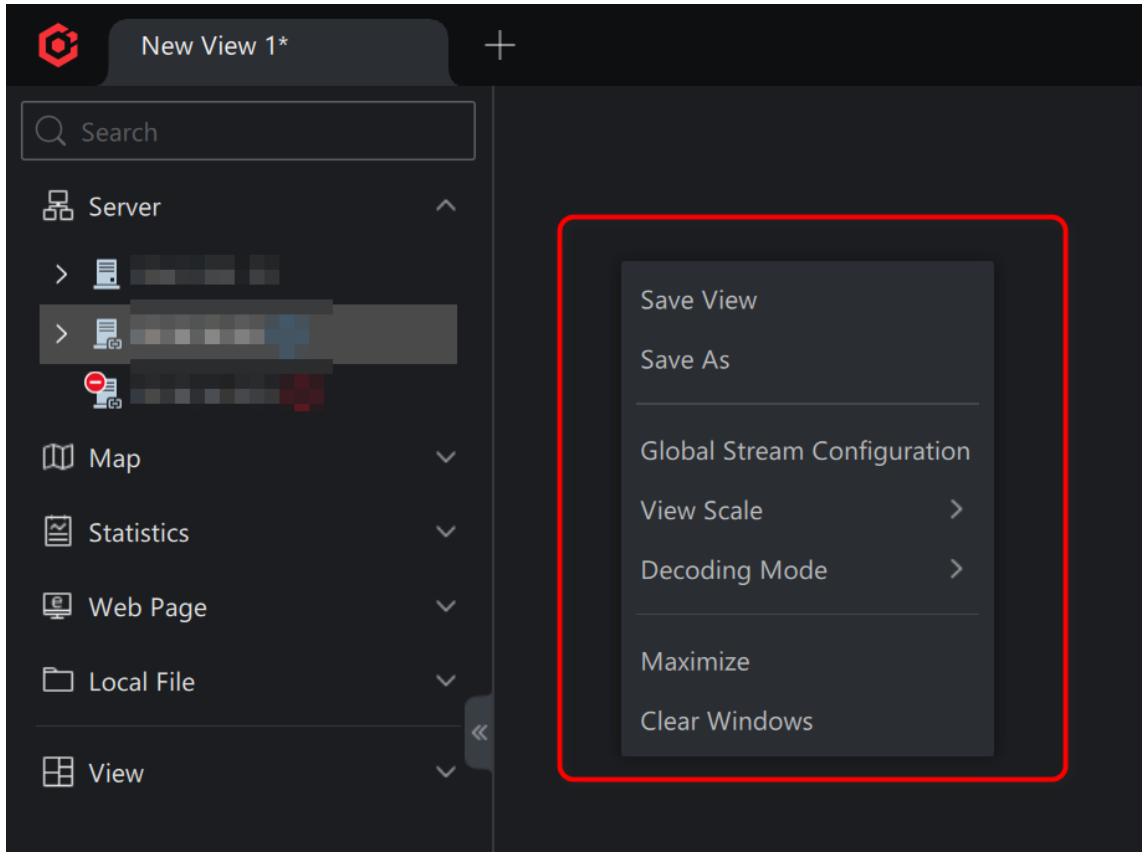


Figure 2-6 Access to Basic Video Preference

Global Stream Configuration

- If you check **Stream Adaption**, the system will automatically switch between the main and sub-stream according to the window resolution when playing video.
  Select the appropriate video resolution based on device and network conditions. When the playback window size is smaller than the selected resolution, the video will automatically switch to a lower sub-stream to ensure performance:
  - Extra Large (1920*1080)
  - Large (704*576)
  - Medium (640*360)
  - Small (320*180)
- If you do not check **Stream Adaption**, videos in the window will be played according to the selected mode **Main Stream** or **Sub-Stream**. If the device does not support the mode, the system will switch to the supported mode automatically.

View Scale

Original Resolution indicates to play a video in original size, and the image may not fill the live view / playback window. **Full Screen** indicates that the image is filled the entire live view / playback window.

Decoding Mode

Hardware decoding is to decode based on GPU, while software decoding is on CPU. Choose the decoding mode according to your GPU/CPU performance.

Maximize

Show the Viewing Grid in Full Screen.

Chapter 3 Video Monitoring

Video monitoring centers on the security based on video-related functions. You can perform real-time monitoring to view the real-time status of monitored places, get the notification of events/alarms, and know the trend of different targets.

Preparations

- ***Add Encoding Devices***
- ***View and Configure Details of Encoding Devices***
- ***Add an Alarm for an Encoding Device***

Basic Functions Related to Video Monitoring

- ***Start Live View / Playback***
- ***PTZ Control During Live View***
- ***Monitor via Cameras on the Map***

Face Picture Comparison and Human Body Detection

- ***Add Face Picture Libraries and Face Pictures***
- ***View Videos Related to Face and Human Body Recognition***
- ***Search for Recognized Face Pictures and Human Body Pictures***
- ***Search Targets by a Picture***

Vehicle Monitoring

- ***Add Vehicle Lists and Vehicles***
- ***View Video Related to Vehicle Monitoring***
- ***Search and Export ANPR Events***

Smart Search / VCA

AcuSearch

AcuSeek

Generate and View People Counting Report

(Optional) Local Configurations Related to Video Monitoring

3.1 Preparations

3.1.1 Add Encoding Devices

Before starting live view, video recording, and event/alarm configurations, you should add encoding devices (e.g., cameras, NVRs, DVRs).

On the top of the Desktop, click **System → Device Management → Add Device** . Refer to ***Add Devices*** for details.

3.1.2 View and Configure Details of Encoding Devices

The device basic configuration, recording schedule, connected resource (alarm input and alarm output), intelligent capability, alarm output linkage, and advanced configurations (such as transfer protocol and PTZ settings) are displayed according to the device type and capability.

On the top of the Desktop, click **System → Device Management** to show the added device list. Click a device name to open the device details page.

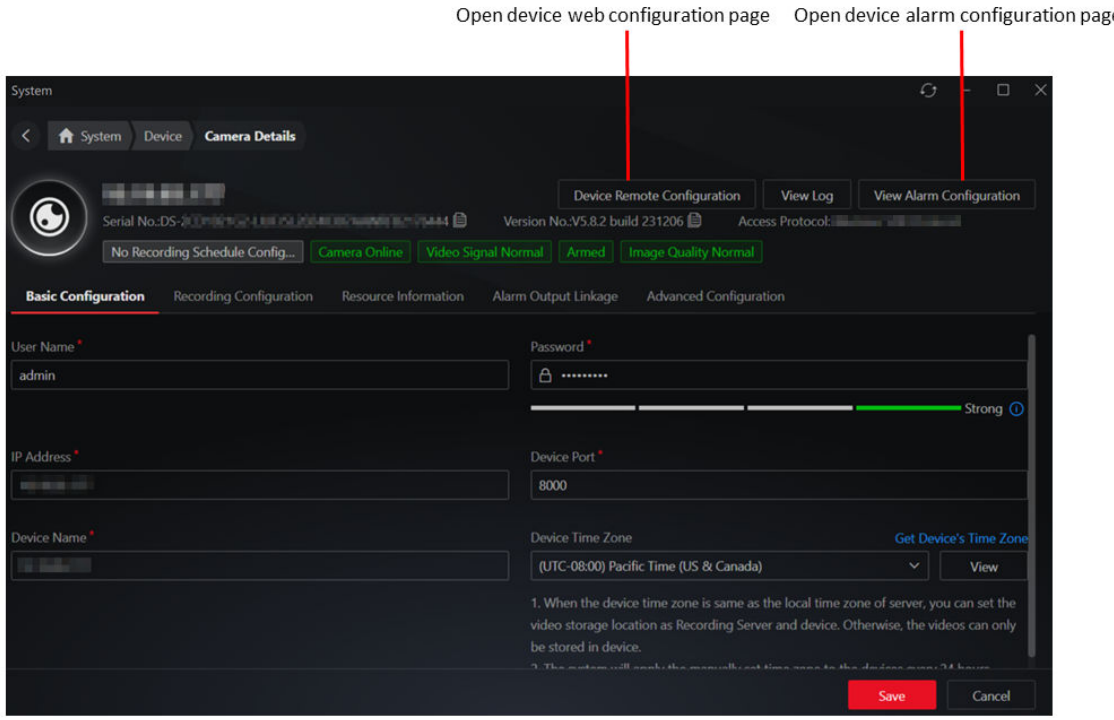
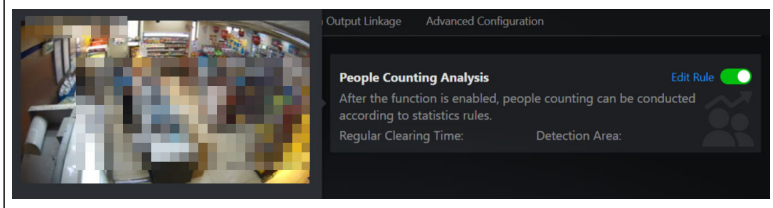


Figure 3-1 Camera Details

Note

The device details vary according to the device type, access protocol, and device adding method. Configurations should be subject to the actual situation.

Device Details Tab Page Introduction

Tab Name	Description
Recording Configuration	It is valid for cameras only.
Resource Information	• Display resources (such as cameras, alarm inputs, and alarm outputs) that are connected to the device. • Right-click a resource for further operations, that depend on the resource type. For example, if the resource is a camera, you can open the device web configuration page, device log search page, and device alarm configuration page, rename the device, and delete it from the resource list.
Intelligent Capability	Intelligent functions such as face picture comparison, AcuSearch, AcuSeek, Smart Search, people counting, and ANPR of the camera are displayed according to the camera capability and License. Before applying the intelligent functions of cameras, you need to enable them. In addition, editing intelligent function rules and copying rules to other cameras are supported on the current page. 
Alarm Output Linkage	It is valid for cameras only. Add or edit the alarm outputs of cameras on the live view image.
Advanced Configuration	Set **Transfer Protocol**, or select media profile of main/sub stream for the camera. You can manually set the camera type to PTZ camera in case the PTZ capability recognition is incorrect. For a PTZ camera, you can perform the PTZ control directly on current page. Refer to ***PTZ Control During Live View*** for details.

PTZ Camera

PTZ: Pan, tilt, and zoom.

Select the camera type as **PTZ Camera**.

You can manually set the camera type to PTZ camera in case the PTZ capability recognition is incorrect. For a PTZ camera, you can perform the PTZ control directly on current page. Refer to ***PTZ Control During Live View*** for details.

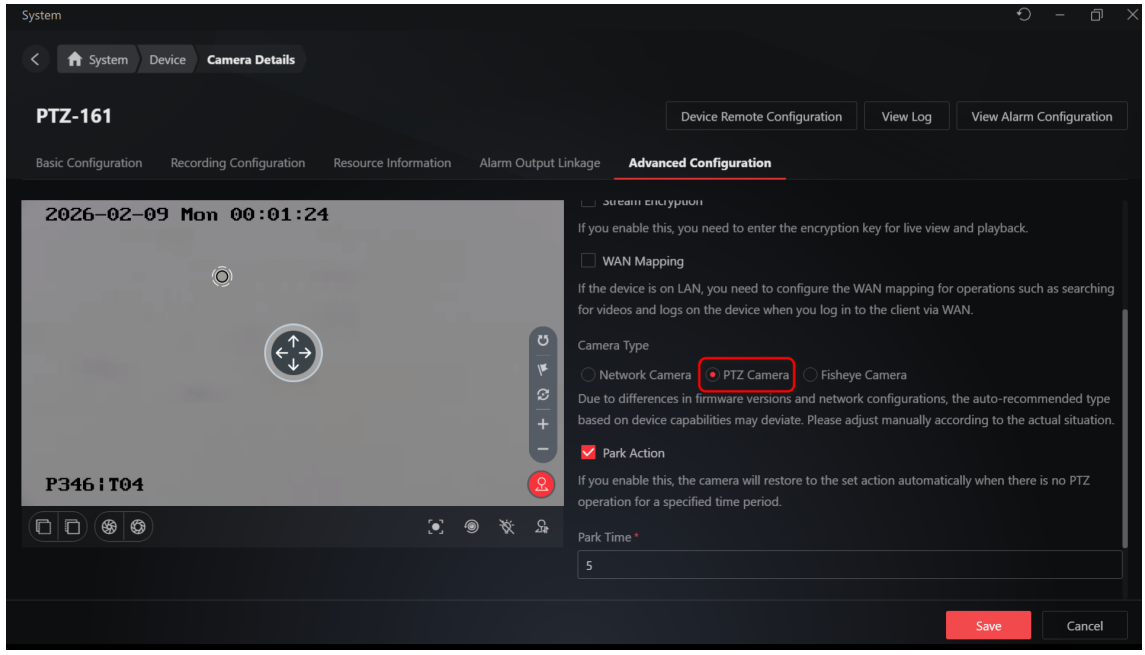


Figure 3-2 PTZ Camera

PTRZ Camera

PTRZ: Pan, tilt, rotate, and zoom.

Click **PTRZ Configuration**.

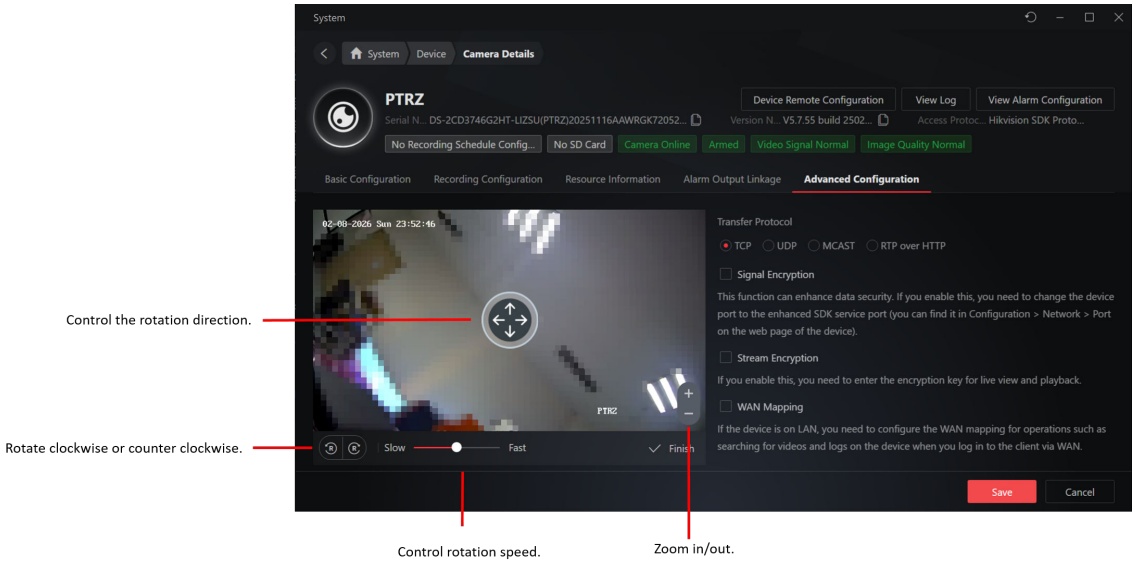


Figure 3-3 PTRZ Camera

Configure Recording Parameters

Note

- The recording schedule of added encoding devices will be automatically synchronized to the system. That is, if a camera already has recording schedule configured, the system will automatically enable recording according to the configured schedule when the camera is added.
- The stream type for video storage is set to dual-stream by default if the camera supports. You can switch the stream during playback.

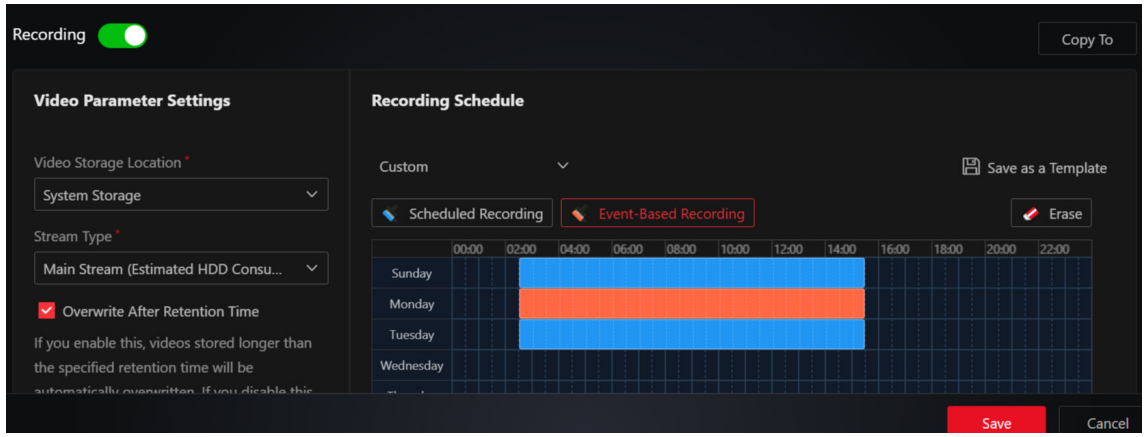


Figure 3-4 Recording Configuration

Switch on **Recording**, and set the video recording parameters.

Video Storage Location

The storage location of recorded video files. You can store these files in the local device. The system allows simultaneous recording of both main and sub-streams, which can be assigned to different storage locations.

Stream Type

Choose the **Main Stream**, **Sub-Stream**, or **Dual-Stream** based on your actual needs for playback quality, power consumption, etc.

Overwrite After Retention Time / Retention Time

If you enable **Overwrite After Retention Time**, videos stored longer than the specified **Retention Time** will be automatically overwritten. If you disable this, stored videos will be overwritten in the order of their storage time (earliest first) when the storage space is not enough.

Auto Copy-Back

Enable this to temporarily store the video in the device when network fails, and transport the video to storage device when network recovers.

Note

The feature is only effective when the **Stream Type** is set to **Main Stream** and is supported only by Hikvision cameras.

Recording Schedule

You can use the schedule template or define a custom schedule. The scheduled recording is to record continuously within the time duration, while the event triggered recording is to record when alarm occurs.

Back up Video

Enable this to back up videos on the backup device. You can search and play the videos on the backup device when the original videos are damaged, lost, or deleted.

Copy To

Click this to copy the recording configurations to other devices.

3.1.3 Add an Alarm for an Encoding Device

Before receiving the event/alarm detailed information which helps handle the situation promptly, you need to configure the alarm rule in advance.

On the top of the Desktop, click **System → Event and Alarm → Alarm Configuration → Add Alarm** .

Refer to ***Add an Alarm*** for details.

Supported triggering events and sources for encoding devices are categorized according to their properties. For the complete event list supported by encoding devices, refer to ***Supported Triggering Events*** .

3.2 Basic Functions Related to Video Monitoring

The video monitoring basic functions include live view, playback, PTZ control, and monitoring on the map.

3.2.1 Start Live View / Playback

You can start live view or playback of one or multiple cameras.

- Start Live View of One Camera: Double click a camera, or drag a camera from the camera list to the viewing grid, or right click a camera and click **Open** to start live view of the camera.
- Start Playback of One Camera: After starting live view of a camera, draw the timeline backwards, or click **Playback** on the lower left corner to start playback of the camera.
- Start Live View of Multiple Cameras: Press the **Ctrl** key, select cameras, and drag them from the camera list to the right window, or right-click the selected cameras and click **Open**.

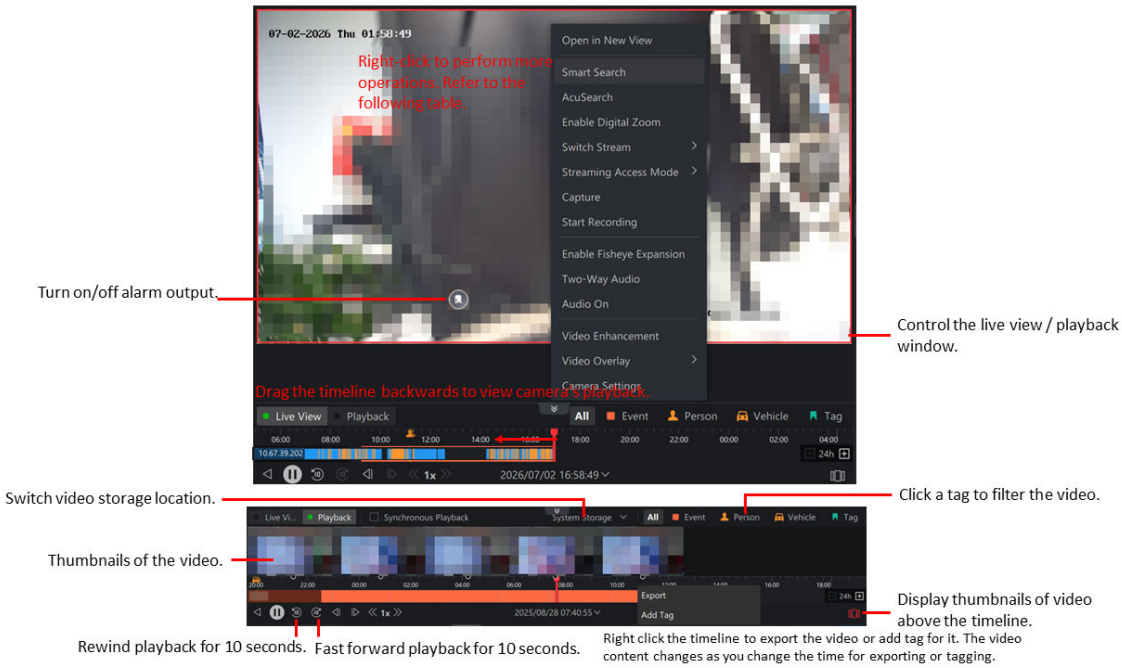


Figure 3-5 Start Live View / Playback of One Camera

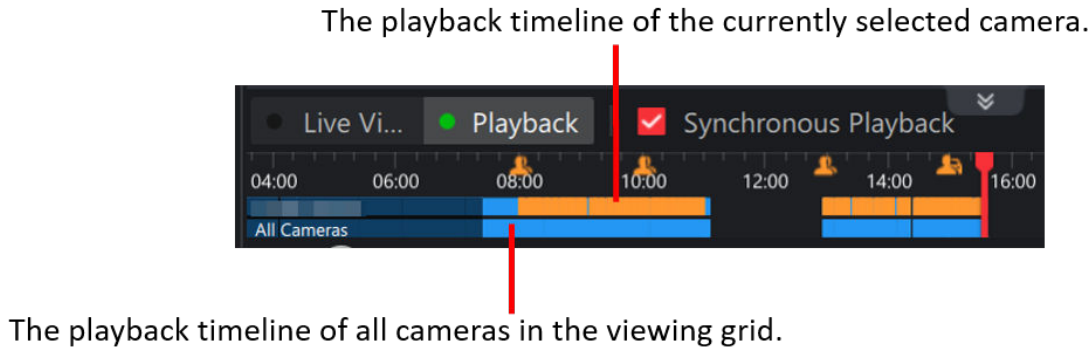


Figure 3-6 Synchronous Playback

During live view or playback, you can right-click on the window or click the icons in the lower right corner to control the window. You can also press and hold the **Ctrl** key, select multiple windows, and right-click to perform operations. Refer to the table below for supported operations.

Function	Explanation	Live View	Playback
Open in New View	Open the live view / playback window in a new view.	√	√
Smart Search / VCA Search	Smart Search: draw an area on the video to detect whether there are persons and/or vehicles entering this area. VCA Search: draw an area on the video to detect whether there are moving objects in this area or objects entering this area. You can view the detected results on the right side of the page. Click a result to view the related video or right click a result to enter the Intelligent Search page. For details about VCA configuration, refer to ***Smart Search / VCA*** .	√	√
AcuSearch	Detects human bodies and vehicles and search for objects similar to them in captured pictures.	√	√
Enable Digital Zoom	• Click and then click on the video image to zoom in. • Draw a frame from left side to right side on the video image to zoom in the selected area; and draw a frame in the opposite direction to zoom out. • Scroll the mouse wheel forwards or backwards to zoom in or out the video image.	√	√
Stream Switch	Switch streams to main stream, sub stream, fourth stream, or smooth stream.	√	√
Streaming Access Mode		√	√
Capture	Take a snapshot of the current video image.	√	√
Export	Export the video.	×	√
Start Recording	Record a video for the desired time period.	√	×

Function	Explanation	Live View	Playback
Enable PTZ Control	Refer to ***PTZ Control During Live View*** for details.	√	×
Enable Target Tracking	Continuously track the selected target (person/vehicle) in the video.	√	×
Enable Smart Linkage	Locate the target appeared in the video.	√	×
Enable Fisheye Expansion	The wide-angle view of the camera is displayed. In this mode, the perspective and angles of objects in the video image will be distorted.	√	√
Two-Way Audio	Start two-way audio with the camera or NVR device.	√	√
Audio On/Off	Turn on/off the audio of the video.	√	√
Light On/Off	Turn on/off the light of the camera.	√	×
Video Enhancement	Adjust the video image such as brightness and saturation.	√	√
Video Overlay	Display the needed information on the live view / playback image.	√	√
Camera Settings	Set camera parameters such as recording parameters. Refer to ***View and Configure Details of Encoding Devices*** .	√	√

Note

These functions should be supported by the device: PTZ control, smart linkage, target tracking, two-way audio, audio on/off and light on/off.

Note

For videos tagged with Person or Vehicle, you should notice the following:

- To enable the tags, make sure that at least one VCA event, such as intrusion or line crossing, is configured on the device. Human or/and vehicle target detection should be enabled.
- ***Subscription*** of the corresponding event on HikCentral Mini Cube should be enabled.
- Videos recorded before the device is added to the platform will not be tagged.

During playback, you can control the image via shortcuts on the keyboard.

Table 3-1 Shortcuts

Key	Functionality
↑	Fast Forward
↓	Fast Rewind
←	Single-Frame Reverse Playback
→	Single-Frame Fast Forward
[	Reverse Playback
]	Normal Playback
Space	Pause/Play

3.2.2 PTZ Control During Live View

You can control cameras with pan/tilt/zoom functionality during live view. You can set the preset and patrol for the cameras on the PTZ control pane.

Double click a PTZ camera, or drag a PTZ camera to the right window, or right click a PTZ camera and click **Open** to start live view of the camera.

Click in the lower right corner to pop up the PTZ control icons on the right side. See the following figure for the supported operations.

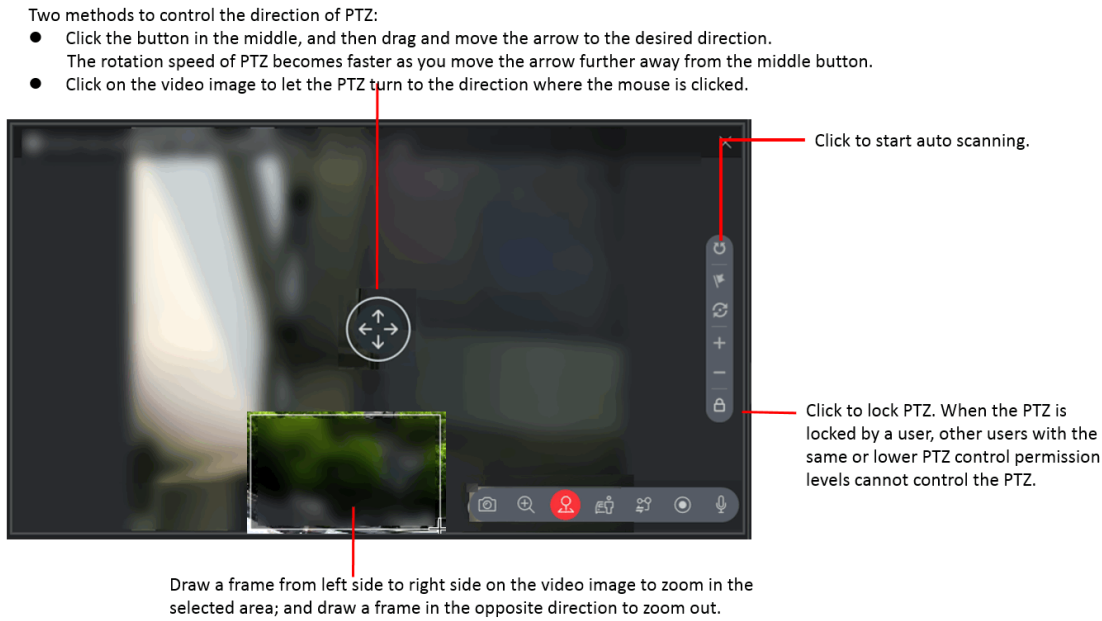


Figure 3-7 PTZ Control

3.2.3 Monitor via Cameras on the Map

After adding cameras to the map, you can view live view and playback of cameras and camera status on the map.

In the **Map** module, double click a map, or drag a map to the right window, or right click a map and click **Open** to view the map and its resources. For details about adding maps, refer to ***Add Map*** .

There are two modes for the map. In the Monitoring mode ( ), you can view live view and playback via cameras on the map. In the Configuration mode ( ), you can add cameras, marks, and hot regions to the map, set the types of resources to be displayed on the map, etc.

Add Map

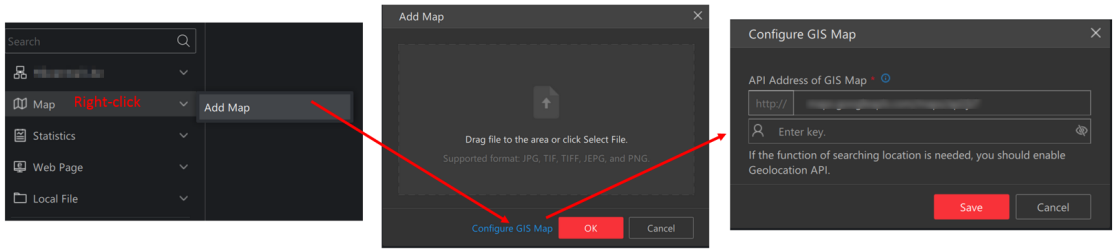


Figure 3-8 Add GIS Map

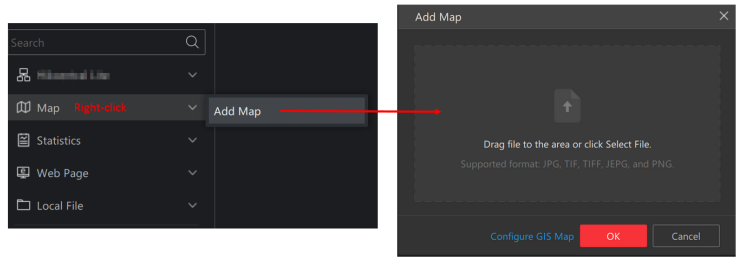


Figure 3-9 Add E-Map

Configuration Mode

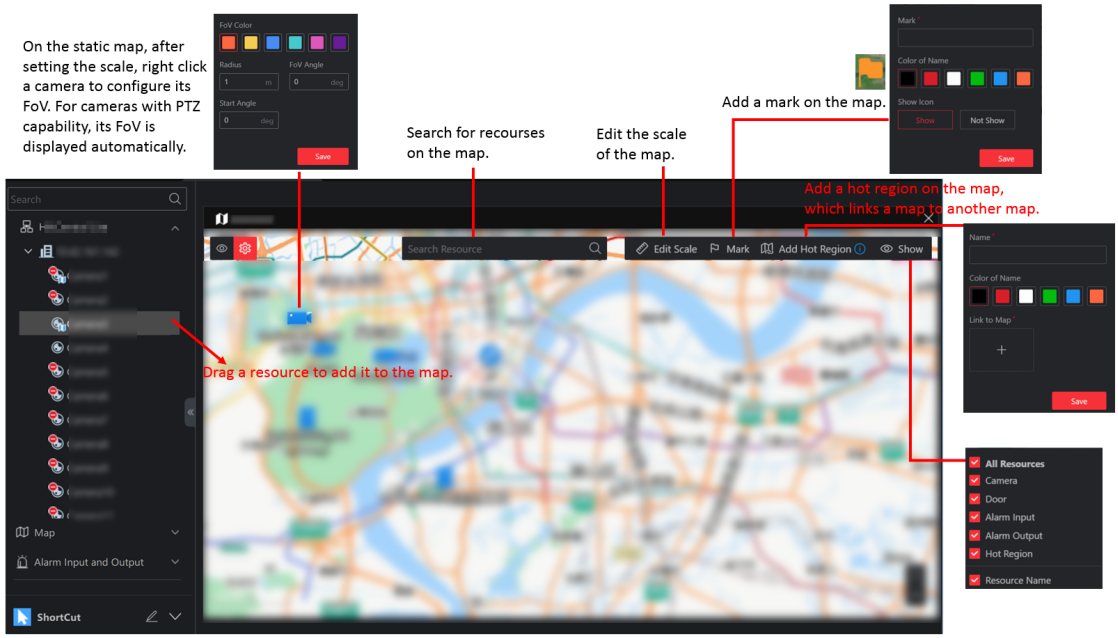


Figure 3-10 Supported Operations in Configuration Mode

Monitoring Mode

You can monitor via cameras on the map.

- Click a camera to view the live view of the camera on the map.

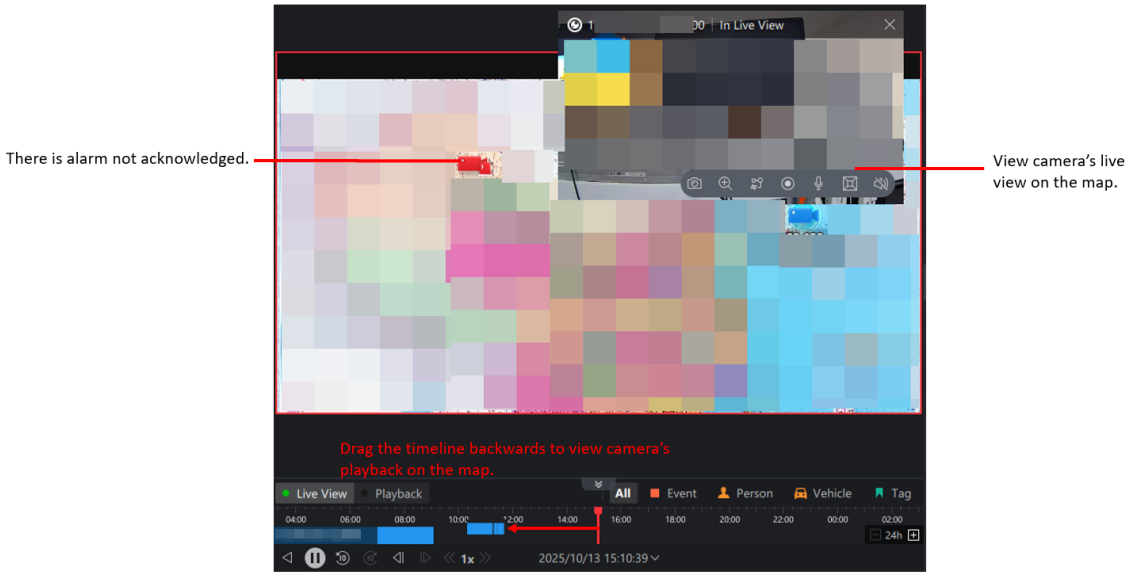


Figure 3-11 View Camera's Live View and Playback on the Map

- Click **Batch Select**, draw an area to select multiple cameras, and click **Batch Play** to view the live view of cameras in a batch.
  Press the Ctrl key, select multiple cameras, and drag them to the windows outside of the map to view the live view of cameras in a batch.



Figure 3-12 Batch View Cameras' Live View and Playback

Note

When viewing the live view or playback of the camera, right click the live view or playback image to perform more operations. Refer to ***Start Live View / Playback*** for details.

3.3 Face Picture Comparison and Human Body Detection

Face picture comparison refers to comparing two face pictures to determine if they are the same person. Human body detection focuses on detecting human bodies in different environments. These two functions are crucial for security purposes and are widely used in various sectors such as retail stores and enterprises.

Note

Make sure the cameras or DeepinMind NVRs have the compatibility of face picture comparison. You can contact our technical supports for detailed models.

3.3.1 Add Face Picture Libraries and Face Pictures

Face pictures are used to compare with the face pictures of the capture persons. Face picture libraries are used to manage or group face pictures, for example, you can add the face pictures of VIP customers in to a specific face picture library named "VIP Customer".

Click **System → Face Picture Library** to enter the managing face picture libraries and face pictures page.

- Add Face Picture Library:
  Click **Add Face Picture Library** in the down left corner to add face picture libraries.
  If you link cameras with the face picture library, you can view the number of cameras and the corresponding camera names below the name of face picture library.

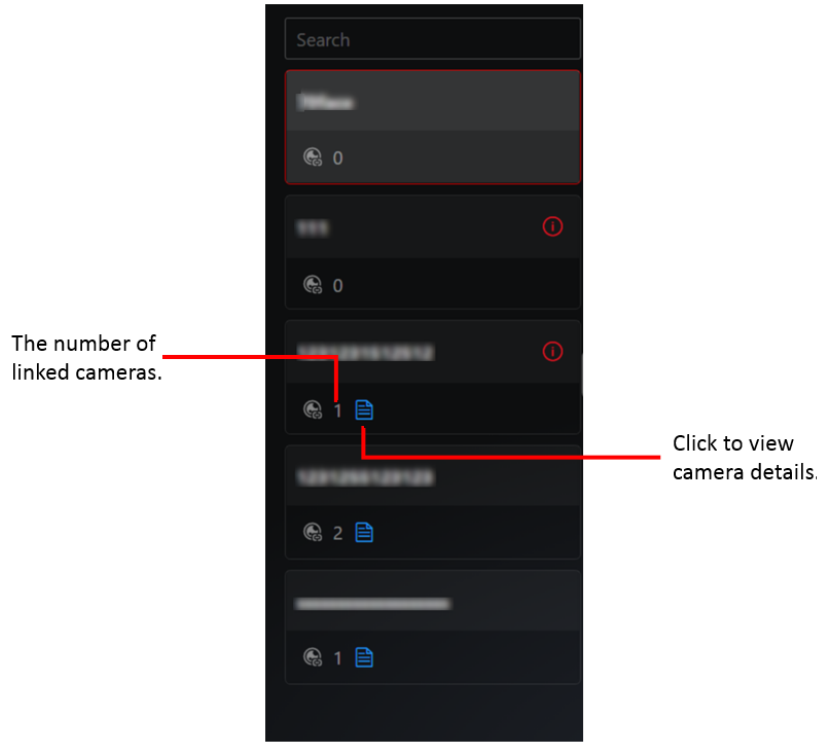


Figure 3-13 Cameras Linked with Face Picture Libraries

- Add Face Picture:
  - Click **Add Face Picture** in the down left corner to add a single face picture.

    Note

    You can configure the effective period for face pictures; once expired, they will no longer trigger face picture alarms.
  - Click **Import → Add from Existing Person** to add face picture(s) of the added person(s).
  - Click **Import → Import Face Picture Information via Excel** to batch import face pictures by a template file.

- Click **Import → Import Face Pictures** to batch import face pictures after manually packing them.
- Click **Import Device Face Picture Library** to batch import face pictures from the device face picture libraries.

3.3.2 View Videos Related to Face and Human Body Recognition

After adding face and human body recognition cameras, you can view videos related to face picture comparison and human body detection. At the same time, events related to the current videos will be displayed in real-time. You can view the similarity between the captured face picture and the face picture in the specific library, the name of the matched face picture library, etc. And you can perform more operations such as searching for the related face pictures and human body pictures if needed.

Note

To use this function, make sure you have added face and human body recognition cameras and have added channels for the cameras in **License Management → License Overview →** .

During live view, the events of face and human body recognition camera(s) on the current view are displayed in real time. Hover on the event to view its details or right-click the event to perform more operations. Refer to the following figure.

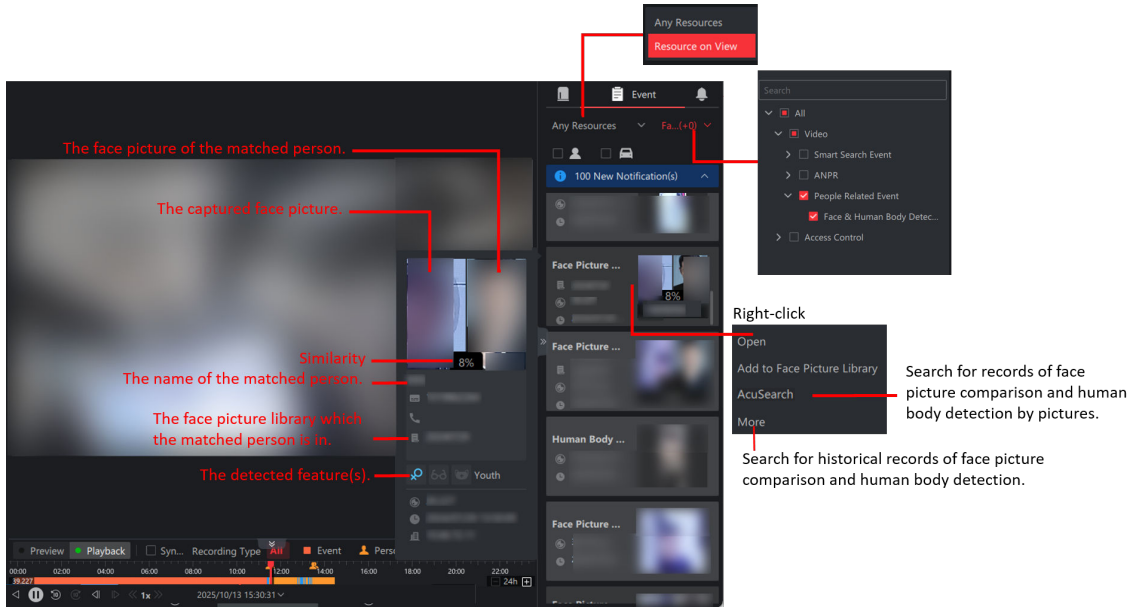


Figure 3-14 Face Picture Comparison Details

Due to the UI similarity of face picture comparison and human body detection, the above only takes face picture comparison as an example.

On the Alarm Details window of face matched events, you can enlarge the captured picture and picture compared with the captured one, making the comparison easier.

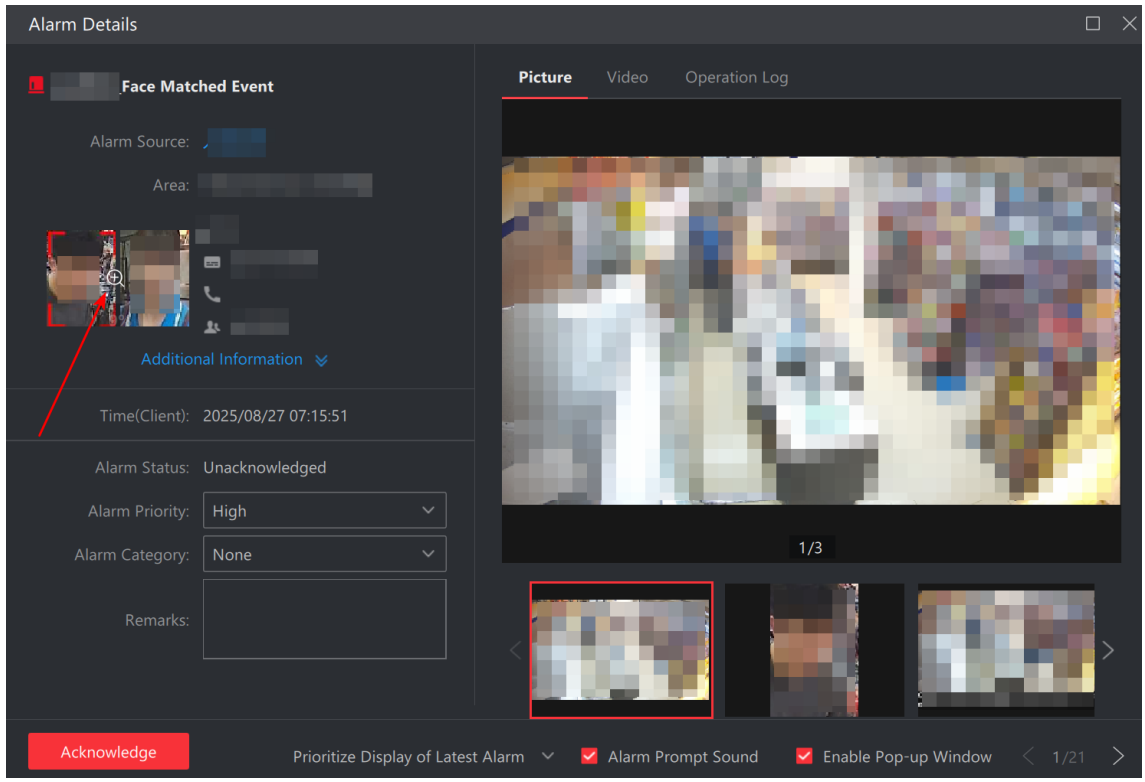


Figure 3-15 Alarm Details

3.3.3 Search for Recognized Face Pictures and Human Body Pictures

You can set conditions to search for capture records including face capture records, face picture comparison records, and human body detection records. For the searched records, you can view record details, export records, etc.

Note

This function should be supported by device.

Click **Search → Face & Human Body Detection** to view the capture records.

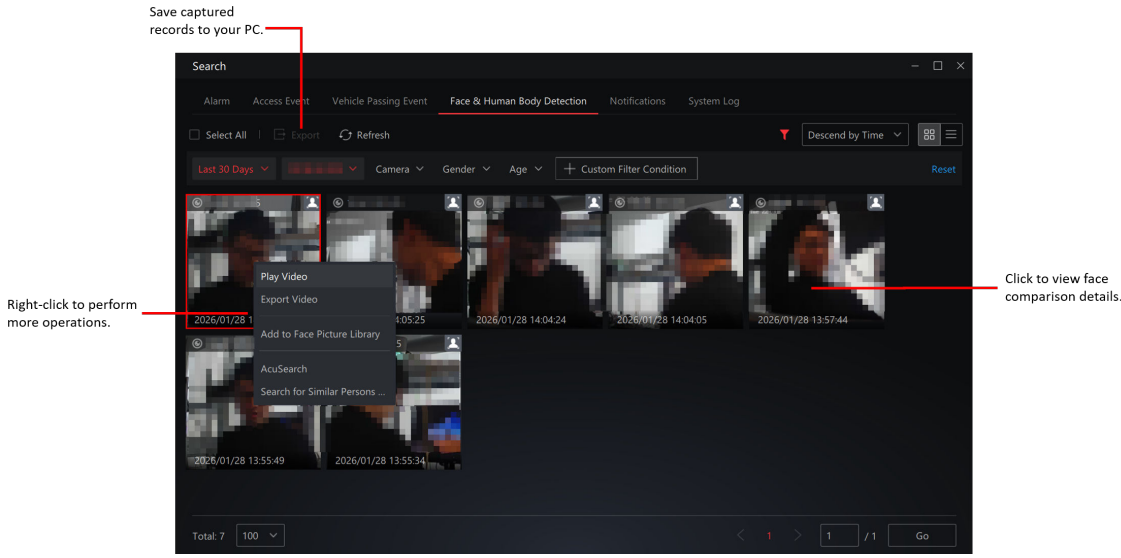
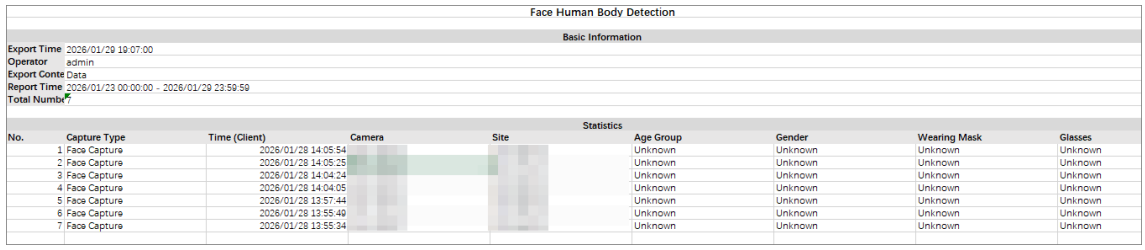


Figure 3-16 Face & Human Body Detection



Face Human Body Detection

Basic Information

Export Time	2026/01/29 19:07:00
Operator	admin
Export Conte	Data
Report Time	2026/01/23 00:00:00 - 2026/01/29 23:59:59
Total Numbe	7

Statistics

No.	Capture Type	Time (Client)	Camera	Site	Age Group	Gender	Wearing Mask	Glasses
1	Face Capture	2026/01/28 14:05:54			Unknown	Unknown	Unknown	Unknown
2	Face Capture	2026/01/28 14:05:25			Unknown	Unknown	Unknown	Unknown
3	Face Capture	2026/01/28 14:04:24			Unknown	Unknown	Unknown	Unknown
4	Face Capture	2026/01/28 14:04:05			Unknown	Unknown	Unknown	Unknown
5	Face Capture	2026/01/28 13:57:44			Unknown	Unknown	Unknown	Unknown
6	Face Capture	2026/01/28 13:55:49			Unknown	Unknown	Unknown	Unknown
7	Face Capture	2026/01/28 13:55:34			Unknown	Unknown	Unknown	Unknown

Figure 3-17 Export Capture Records

Due to the UI similarity of face capture / face picture comparison / human body detection details page, the following only explains the face capture details page for an example.

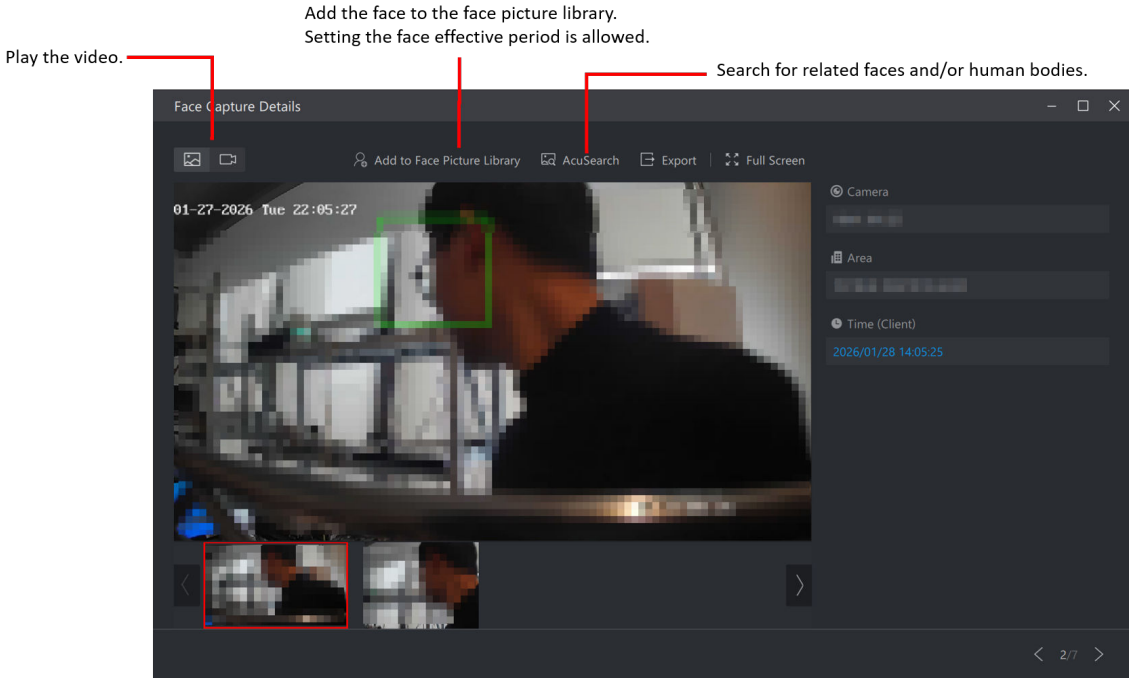


Figure 3-18 Supported Operations on Face Capture Details Page

3.3.4 Search Targets by a Picture

You can upload a picture and setting other conditions to search for the corresponding faces and/or human bodies. For the searched results, you can view the capture details, play the related video files, etc.

Note

Make sure you have added DeepinMind series NVR.

Click **Search → Intelligent Search → Upload Picture** and select a picture from local PC, or drag a picture to the window to start searching.

If there is only one face / human body in the picture, the search results will be automatically displayed. Otherwise, you should select a face and/or a human body and/or a vehicle in the picture for searching.

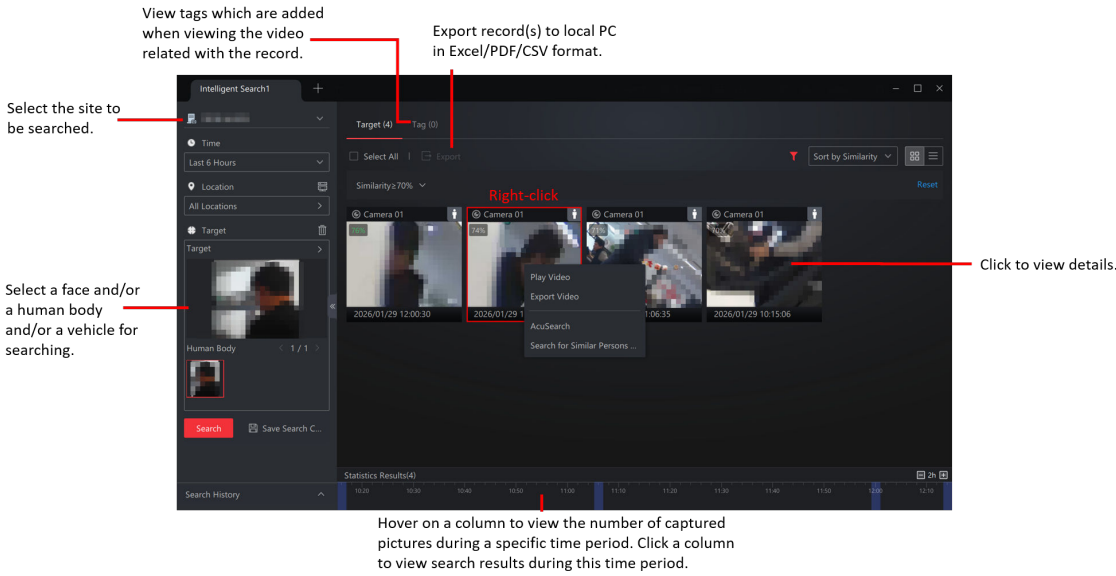


Figure 3-19 Search Result

3.4 Vehicle Monitoring

You can add vehicle lists and vehicles, and then monitor vehicles by viewing the related videos on ANPR cameras and searching for vehicle passing records.

Note

Make sure the devices have the compatibility of ANPR. You can contact our technical supports for detailed models.

3.4.1 Add Vehicle Lists and Vehicles

You can manage vehicles in the vehicle lists, including exporting vehicle information in a list, moving vehicles in one list to the other list, and so on.

Click **System → Vehicle** .

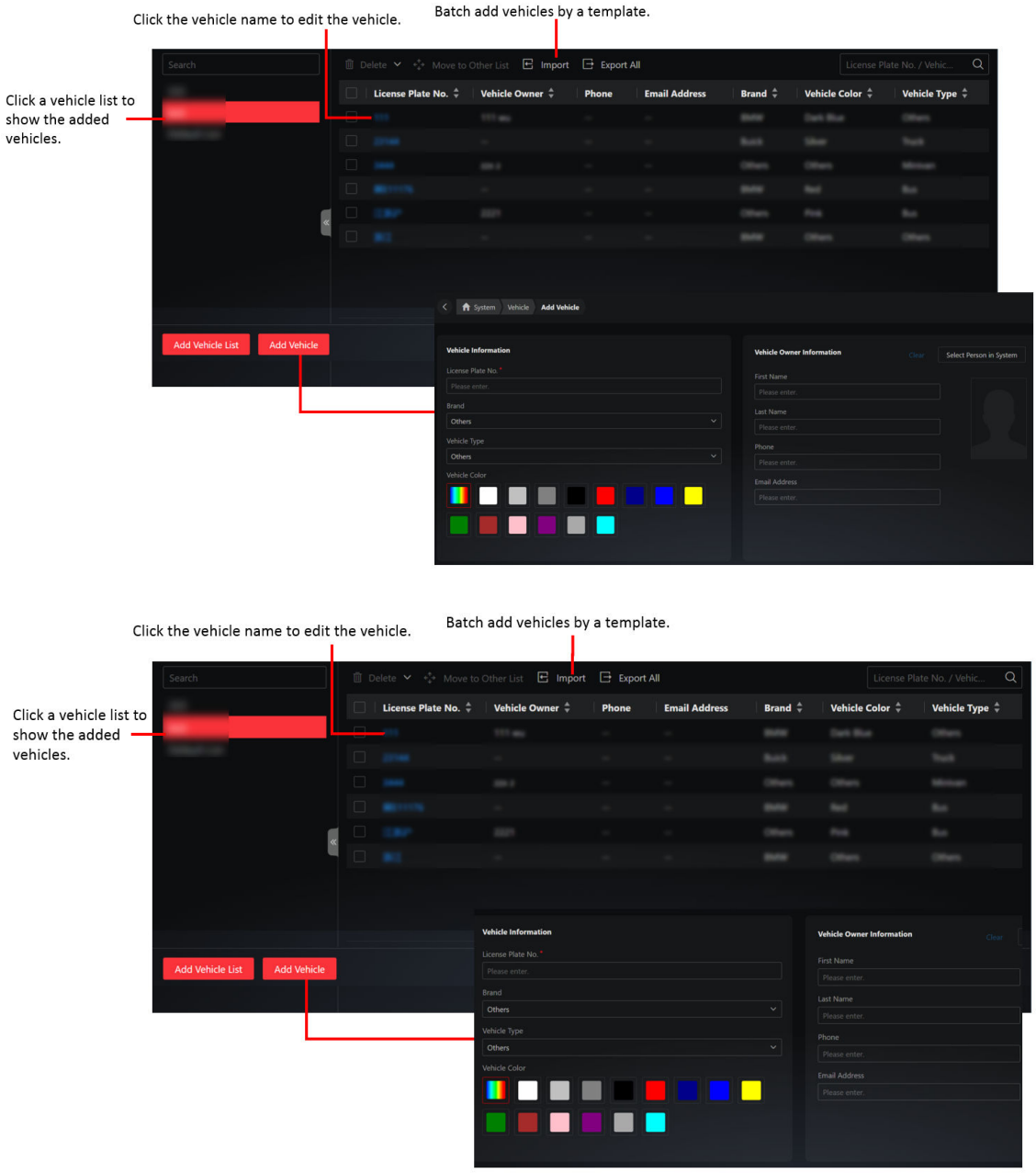
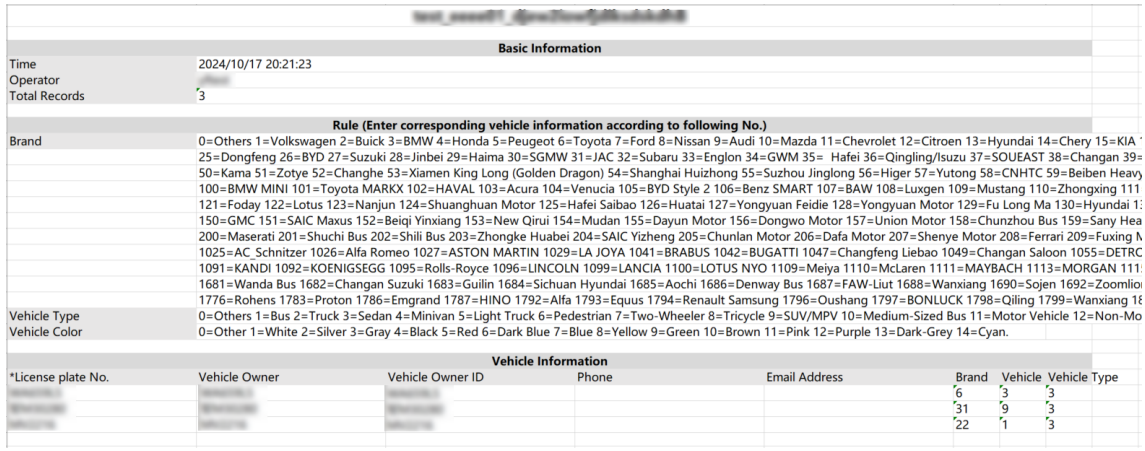


Figure 3-20 Vehicle Page



Basic Information	
Time	2024/10/17 20:21:23
Operator	
Total Records	3

Rule (Enter corresponding vehicle information according to following No.)	
Brand	0=Others 1=Volkswagen 2=Buick 3=BMW 4=Honda 5=Peugeot 6=Toyota 7=Ford 8=Nissan 9=Audi 10=Mazda 11=Chevrolet 12=Citroen 13=Hyundai 14=Chery 15=KIA 25=Dongfeng 26=BYD 27=Suzuki 28=Jinbei 29=Haima 30=SGMW 31=JAC 32=Subaru 33=Englon 34=GWM 35= Hafei 36=Qingling/Isuzu 37=SOUEAST 38=Changan 39= 50=Kama 51=Zotye 52=Changhe 53=Xiamen King Long (Golden Dragon) 54=Shanghai Huizhong 55=Suzhou Jinglong 56=Higer 57=Yutong 58=CNHTC 59=Beiben Heavy 100=BMW MINI 101=Toyota MARKX 102=HAVAL 103=Acura 104=Venucia 105=BYD Style 2 106=Benz SMART 107=BAW 108=Luxgen 109=Mustang 110=Zhongxing 111 121=Foday 122=Lotus 123=Nanjun 124=Shuanghuan Motor 125=Hafei Saibao 126=Huatai 127=Yongyuan Feidie 128=Yongyuan Motor 129=Fu Long Ma 130=Hyundai 1 150=GMC 151=SAIC Maxus 152=Beiqi Yinxiang 153=New Qirui 154=Mudan 155=Dayun Motor 156=Dongwo Motor 157=Union Motor 158=Chunzhou Bus 159=Sany Hea 200=Maserati 201=Shuchi Bus 202=Shili Bus 203=Zhongke Huabei 204=SAIC Yizheng 205=Chunlan Motor 206=Dafa Motor 207=Shenye Motor 208=Ferrari 209=Fuxing M 1025=AC_Schnitzer 1026=Alfa Romeo 1027=ASTON MARTIN 1029=LA JOYA 1041=BRABUS 1042=BUGATTI 1047=Changfeng Liebao 1049=Changan Saloon 1055=DETRC 1091=KANDI 1092=KOENIGSEGG 1095=Rolls-Royce 1096=LINCOLN 1099=LANCIA 1100=LOTUS NYO 1109=Meiya 1110=McLaren 1111=MAYBACH 1113=MORGAN 111 1681=Wanda Bus 1682=Changan Suzuki 1683=Guilin 1684=Sichuan Hyundai 1685=Aochi 1686=Denway Bus 1687=FAW-Liut 1688=Wanxiang 1690=Sojen 1692=Zoomlio 1776=Rohens 1783=Proton 1786=Emgrand 1787=HINO 1792=Alfa 1793=Equus 1794=Renault Samsung 1796=Oushang 1797=BONLUCK 1798=Qiling 1799=Wanxiang 18
Vehicle Type	0=Others 1=Bus 2=Truck 3=Sedan 4=Minivan 5=Light Truck 6=Pedestrian 7=Two-Wheeler 8=Tricycle 9=SUV/MPV 10=Medium-Sized Bus 11=Motor Vehicle 12=Non-Mo
Vehicle Color	0=Other 1=White 2=Silver 3=Gray 4=Black 5=Red 6=Dark Blue 7=Blue 8=Yellow 9=Green 10=Brown 11=Pink 12=Purple 13=Dark-Grey 14=Cyan.

Vehicle Information							
*License plate No.	Vehicle Owner	Vehicle Owner ID	Phone	Email Address	Brand	Vehicle	Vehicle Type
					6	3	3
					31	9	3
					22	1	3

Figure 3-21 Export Vehicle Information

3.4.2 View Video Related to Vehicle Monitoring

When you view videos related to passing vehicles, events related to the current videos will be displayed in real-time. You can view the name of the matched vehicle list, the vehicle owner information, etc. And you can perform more operations such as editing the license plate and adding the vehicle to the vehicle list.

Note

To use this function, make sure you have added ANPR cameras and have added channels for the cameras in **License Management → License Overview →**  .

During live view, the events of ANPR camera(s) on the current view are displayed in real time. You can hover on the event to view more details, or right click the event to perform more operations.

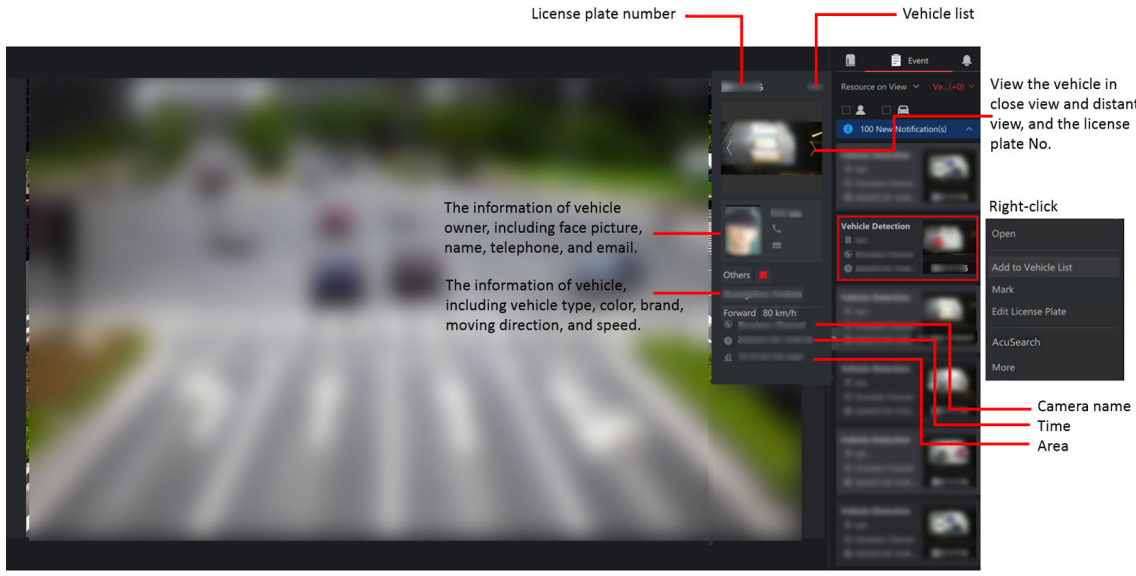


Figure 3-22 ANPR Event Details

3.4.3 Search and Export ANPR Events

You can search for the historic vehicle passing events and export the events to local PC.

Click **Search → Vehicle Passing Event** to view the historic vehicle passing events.

The following operations are supported on this page.

- Filter vehicle passing events by different conditions such as time, server, camera, vehicle list, and license plate number.

  Note

  Once you have added cascaded servers, you can also search for their vehicle passing events. For adding cascaded servers, see ***Server Cascading*** .

- Click **Export** to export all the events in the needed format (Excel, PDF, or CSV).

ANPR Retrieval Records

Basic Info

Export Time	2026/01/26 14:29:02
Operator	admin
SYS	
Time	2025/12/28 00:00:00 - 2026/01/26 23:59:59
Total Number	387

Statistics Data

License Plate No.	Time (Client)	Camera	Server Name	Vehicle List	Owner	Phone No.	Country/Region	Vehicle Type	Brand	Color	Driving Speed	Driving Direction
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward
				--	--	--	Not supported.	Others		Other Colors	80km/h	Forward

Figure 3-23 Export Vehicle Passing Events in Excel Format

- Click a license plate number in the License Plate No., column to view the capture details.

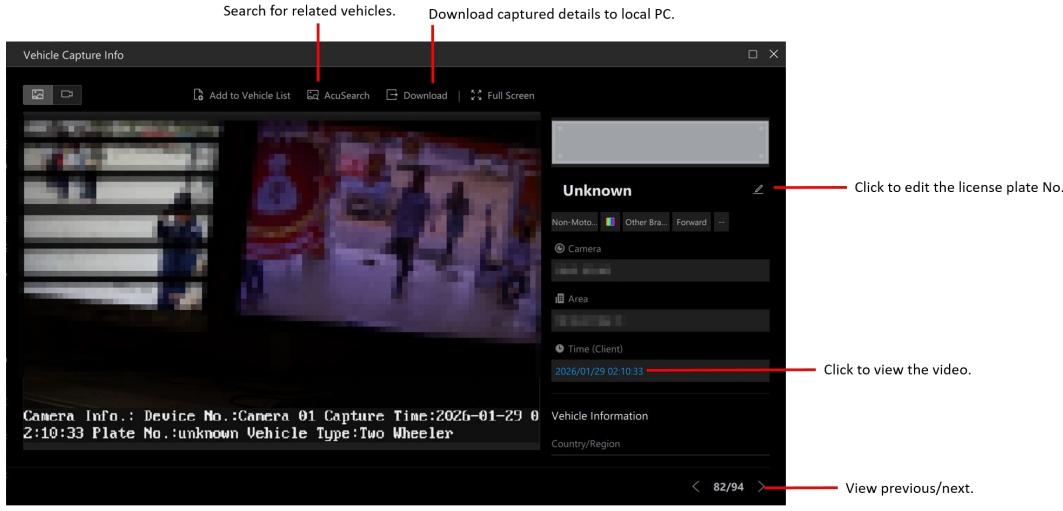


Figure 3-24 Capture Details

3.5 Smart Search / VCA

You can use smart search or VCA search function based on whether your device supports the corresponding function. To use smart search function, make sure you have used the compatible

NVRs that support smart search. To use VCA search function, make sure you have completed the configurations for NVR and network camera.

- Before using smart search or VCA search function, make sure you have configured recording schedules for the network cameras. For details, refer to ***View and Configure Details of Encoding Devices*** .

3.5.1 Compatible NVR Series for Smart Search

The supported series of NVRs that support smart search include: K Series NVR with AcuSense (V4.83.006), I Series NVR with AcuSense (V5.03.020), M-VPro Series (V5.03.020), DeepinMind M Series (V5.03.020), and DeepinMind Super H Series (V5.03.020). For the detailed compatible firmware versions of NVRs, refer to *Compatibility List*.

3.5.2 Configuration for NVR and Network Camera

For NVR With Firmware Versions Higher Than V5.01

On the web page of NVR, enable **Save Smart Analysis Data of Camera**.

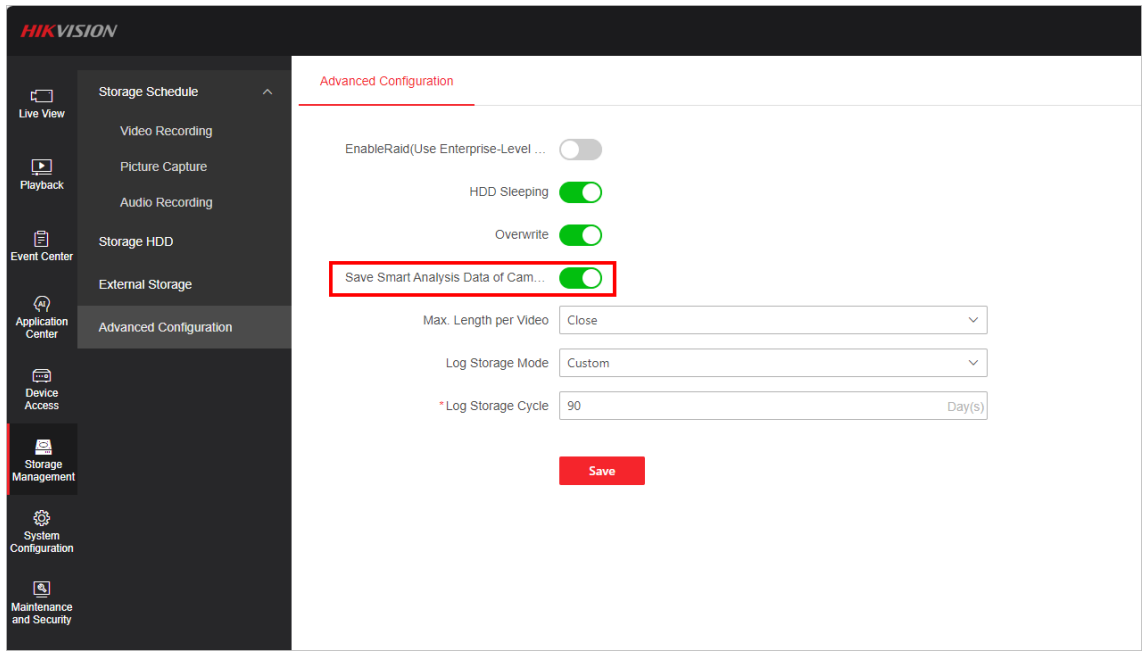


Figure 3-25 Save Smart Analysis Data of Camera

For NVR With Firmware Versions Lower Than V5.01

Perform the following on the web page of NVR.

1. Enable **Dual-VCA** for the network camera.
2. Check **Enable Line Crossing Detection** and **Enable Intrusion**.

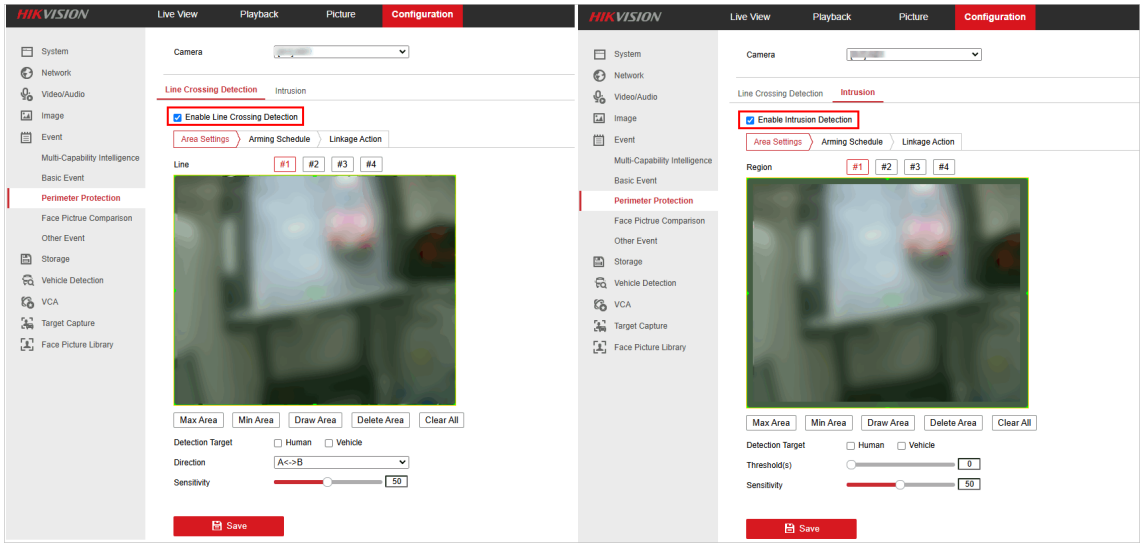


Figure 3-26 Enable Line Crossing Detection & Enable Intrusion Detection

3. Check **Save Camera VCA Data**.

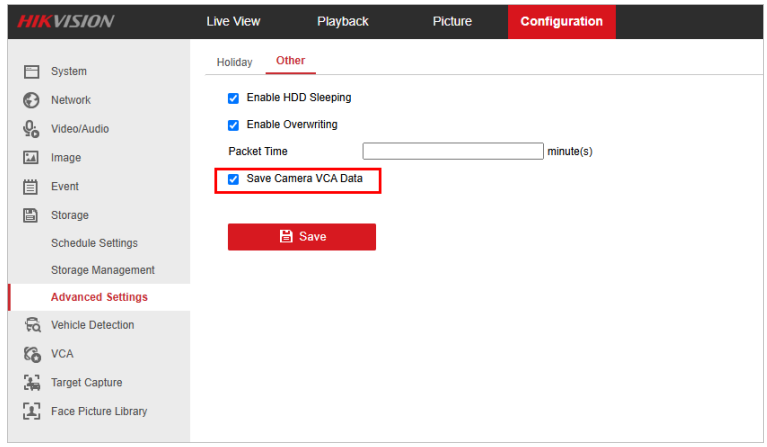


Figure 3-27 Save Camera VCA Data

3.6 AcuSearch

The AcuSearch function firstly extracts pictures of human bodies or vehicles during live view or playback, then compares the extracted targets with captured human bodies or vehicles, and eventually finds out videos that contains the target.

Before You Start

Before using this function, make sure you have enabled it on the Camera Details page.

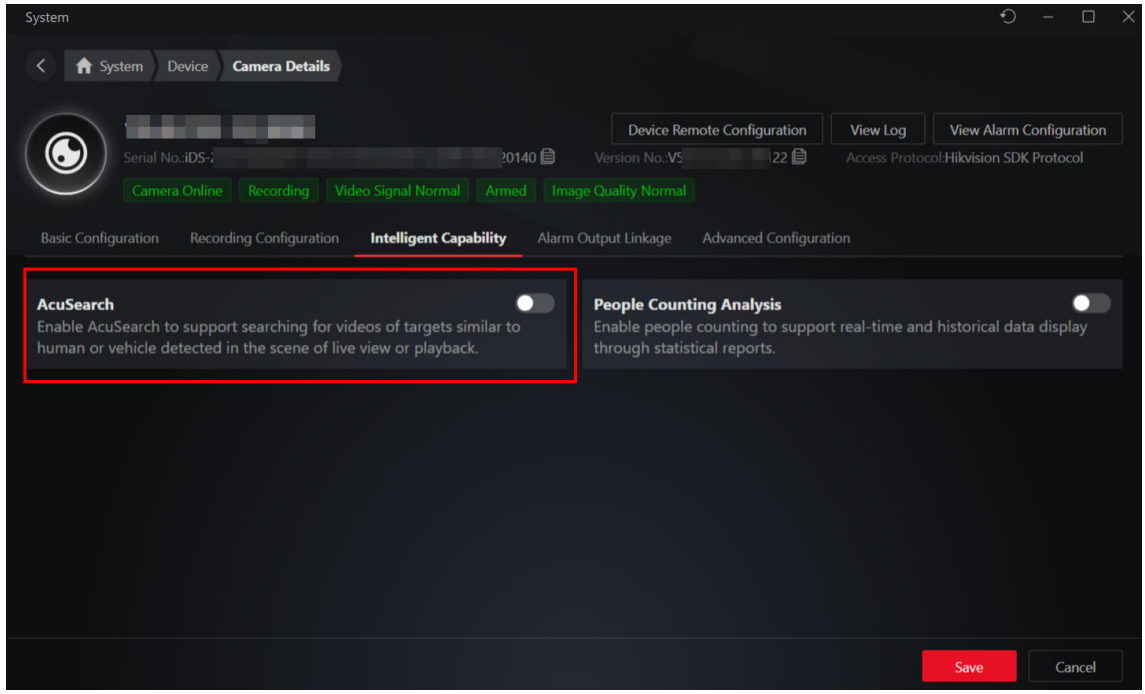


Figure 3-28 Camera Details

Supported Device Series

The following is supported device series for using AcuSearch. You are suggested to upgrade the devices to the latest firmware versions. You can contact our technical supports for detailed models.

Table 3-2 Recommended Devices for AcuSearch

Device Types	Series
NVR/DVR	• M series • DeepinMind M • I series with AcuSense(E) • K series with AcuSense (Except version B) • I/Vpro • K series with AcuSense(E) • M/VPro • PowerX DVR
Network Cameras	• 2 series • 3 series • DeepinView series • PTZ series

How to Start AcuSearch

On the searched result page of Intelligent Search, right click a video thumbnail and select **AcuSearch**. The system will start searching for targets similar to the selected object in recorded videos.

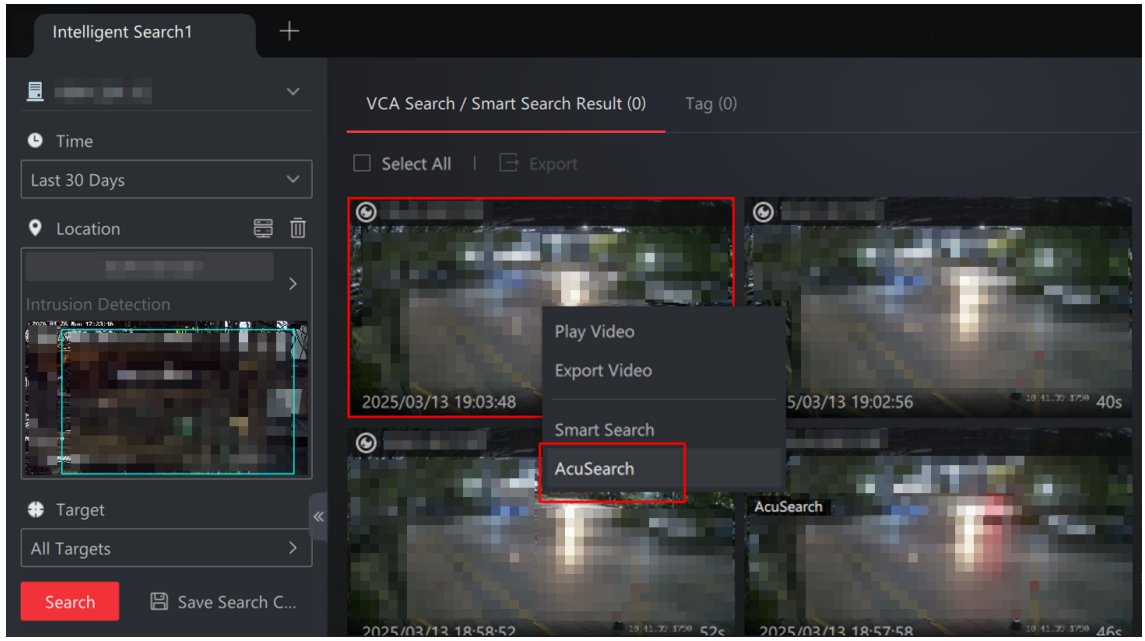


Figure 3-29 AcuSearch

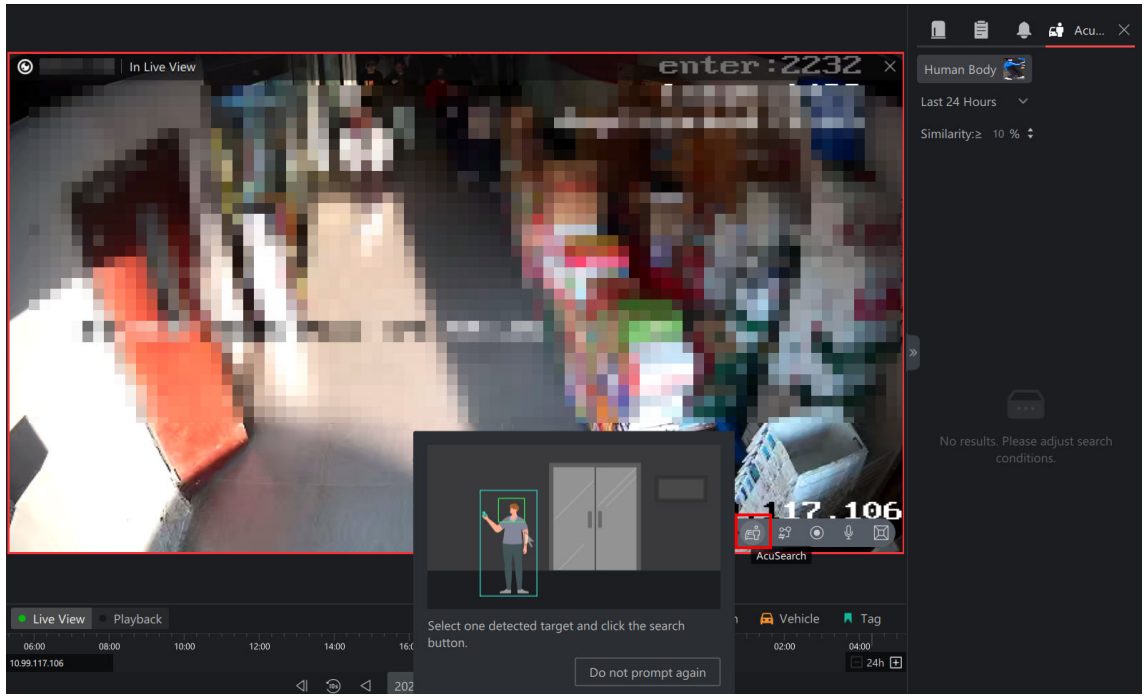


Figure 3-30 Live View Window

3.7 AcuSeek

The AcuSeek's key features include:

- **Natural language search**: Enables open-ended queries (e.g., "a person in red clothing") to pinpoint targets instantly via text input.
- **Rapid target search**: Quick lookup of people or vehicles.
- **Advanced filters**: Filters results by cameras, time range, or similarity; supports playback, AcuSearch, and exporting target images.

Before using this function, make sure you have enabled it on the Camera Details page.

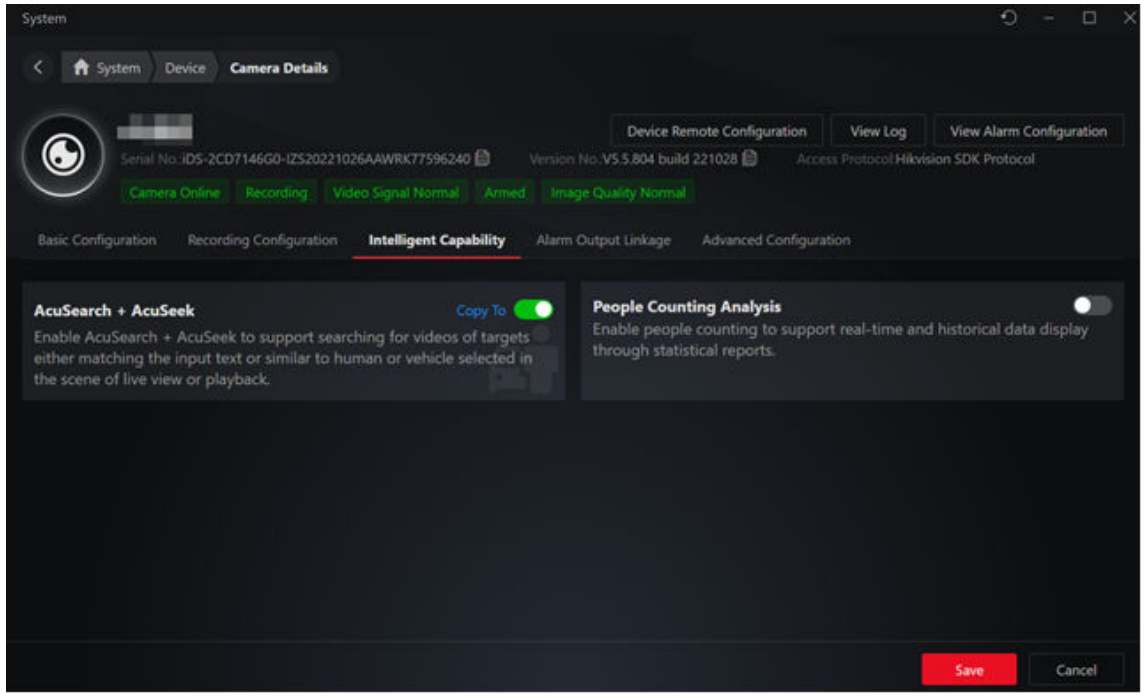


Figure 3-31 Enable AcuSeek

On the Welcome page of Intelligent Search, click **AcuSeek** on the top right.

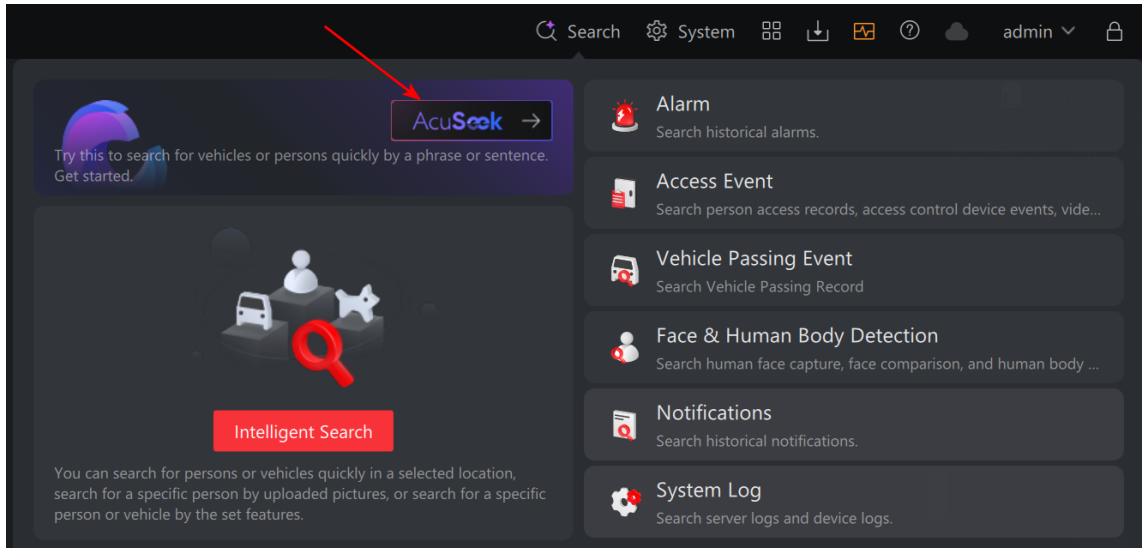


Figure 3-32 AcuSeek Entry

Search

The AcuSeek supports instant searches for people/vehicles/objects/animals or text-based queries, boosted by smart recommendations and favorites for faster retrieval.

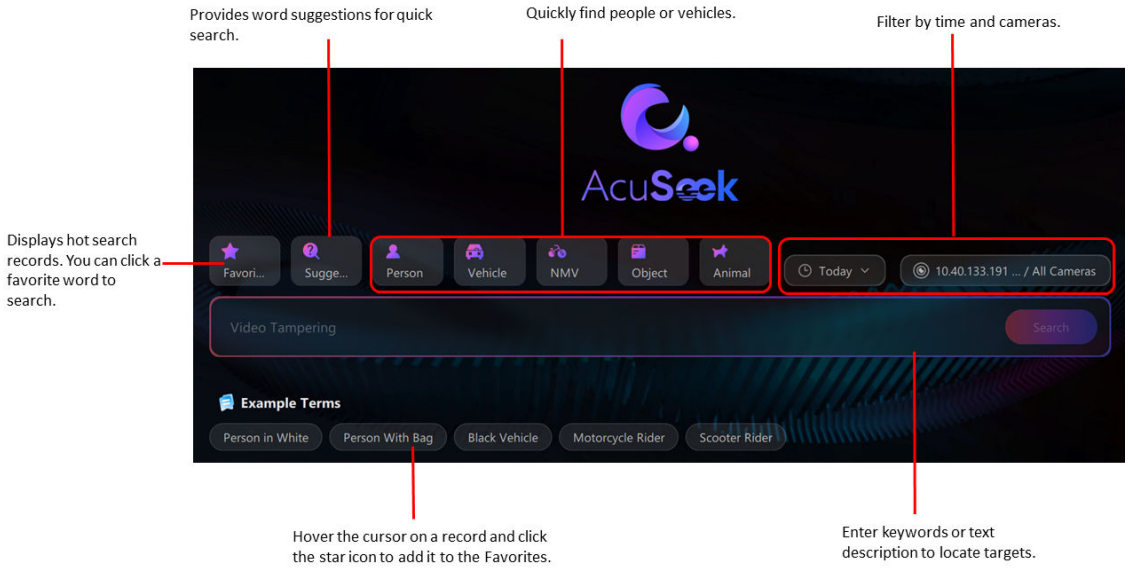


Figure 3-33 Search Page

View Search Results

After retrieving search results, you can filter them by similarity or time, view or export video clips containing the targets, or perform an image-based search. Using the query "Person in Black", you can perform the following operations:

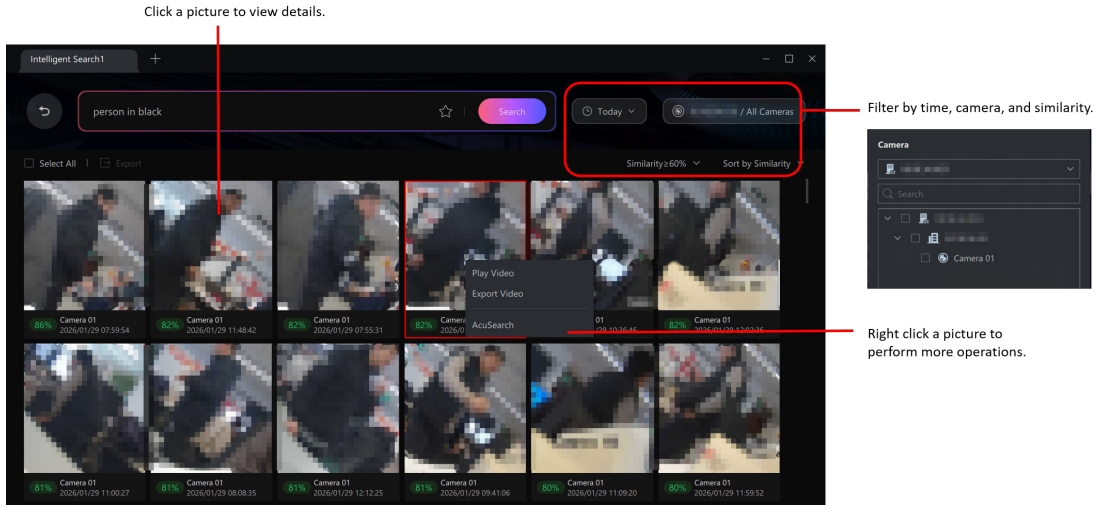


Figure 3-34 Search Results

Export Images

Select one or more images, then click **Export** to save the selected images.

View Details

Click an image to open the video or captured pictures, which pauses at the target's position by default. Playback can be resumed manually.

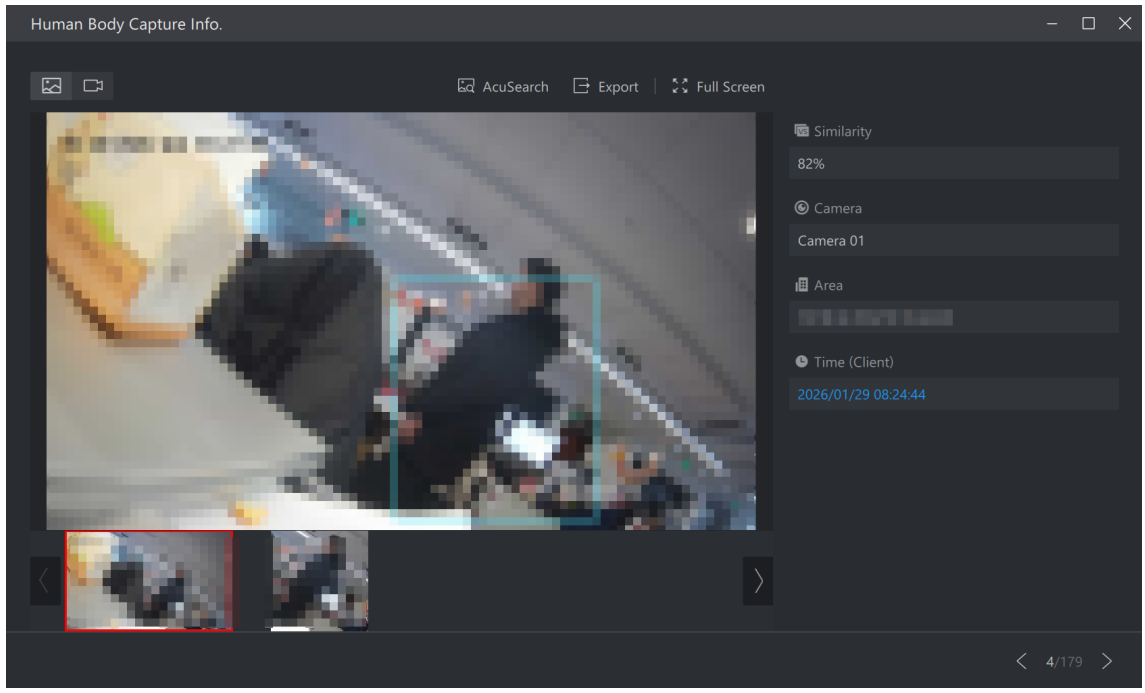


Figure 3-35 Search Result Details

AcuSearch

Hover the cursor on a video and click  to perform an image-based search.

3.8 Generate and View People Counting Report

The people counting report of specified cameras provides a visual view of real-time people counting, real-time dwell people quantity, and history people counting in specified locations. And downloading the historical people counting report to the local PC is supported.

Note

Make sure the License for people counting report is purchased before generating the report.

- On Real-Time People Counting pane, today's people counting (in) / visits and real-time dwell people quantity are displayed.
- On Historical People Counting pane, people counting (in) / visits and people counting (out) / visits are displayed.

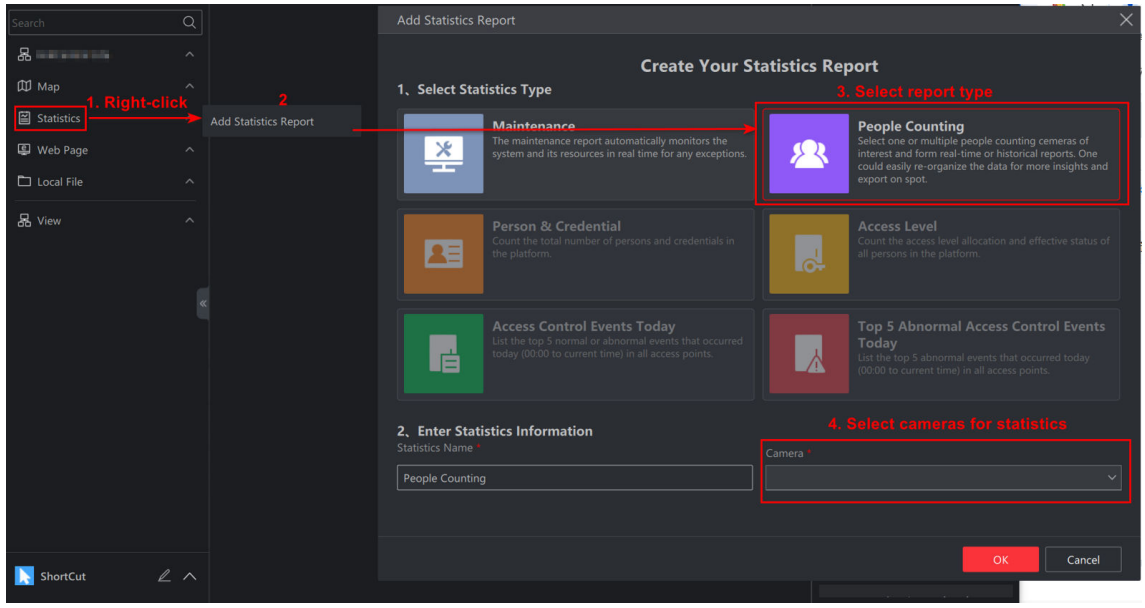


Figure 3-36 Generate People Counting Report

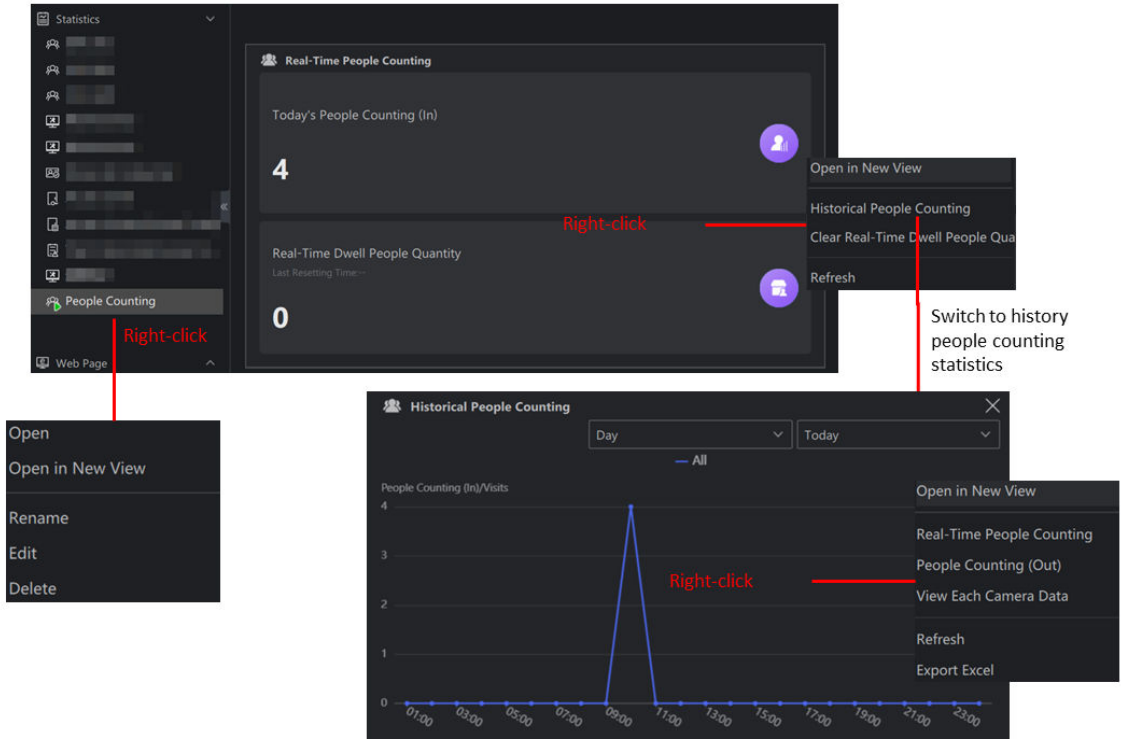
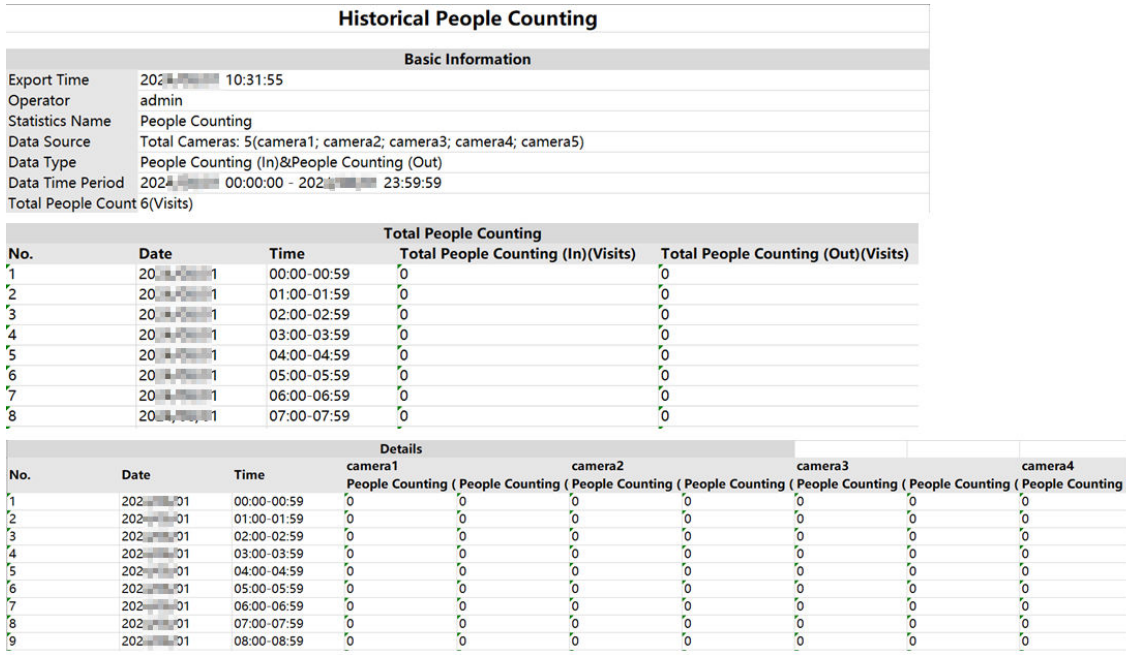


Figure 3-37 View Generated People Counting Report



Historical People Counting

Basic Information	
Export Time	202 10:31:55
Operator	admin
Statistics Name	People Counting
Data Source	Total Cameras: 5(camera1; camera2; camera3; camera4; camera5)
Data Type	People Counting (In)&People Counting (Out)
Data Time Period	202 00:00:00 - 202 23:59:59
Total People Count	6(Visits)

Total People Counting

No.	Date	Time	Total People Counting (In)(Visits)	Total People Counting (Out)(Visits)
1	20 1	00:00-00:59	0	0
2	20 1	01:00-01:59	0	0
3	20 1	02:00-02:59	0	0
4	20 1	03:00-03:59	0	0
5	20 1	04:00-04:59	0	0
6	20 1	05:00-05:59	0	0
7	20 1	06:00-06:59	0	0
8	20 1	07:00-07:59	0	0

Details

No.	Date	Time	camera1		camera2		camera3		camera4	
			People Counting (	People Counting (	People Counting (	People Counting (	People Counting (	People Counting (	People Counting (	
1	202 01	00:00-00:59	0	0	0	0	0	0	0	
2	202 01	01:00-01:59	0	0	0	0	0	0	0	
3	202 01	02:00-02:59	0	0	0	0	0	0	0	
4	202 01	03:00-03:59	0	0	0	0	0	0	0	
5	202 01	04:00-04:59	0	0	0	0	0	0	0	
6	202 01	05:00-05:59	0	0	0	0	0	0	0	
7	202 01	06:00-06:59	0	0	0	0	0	0	0	
8	202 01	07:00-07:59	0	0	0	0	0	0	0	
9	202 01	08:00-08:59	0	0	0	0	0	0	0	

Figure 3-38 Downloaded Reports

3.9 (Optional) Local Configurations Related to Video Monitoring

Before starting the live view / playback, you can define whether to play video in full screen, the monitoring window size, decoding mode, and streaming access mode.

Refer to ***Basic Video Preference*** and ***Configure User Preference*** for details.

Chapter 4 Access Control and Video Intercom

In this module, includes functions including the management of devices and persons, door monitoring, and statistics of persons, credentials, and events, helping you monitor devices and persons via multiple tools.

The following is supported functions:

Device Management

You can ***add devices*** and ***view details of a device*** or ***details of a door*** .

- On the device details page, the following tasks can be performed.
  - Configuring basic parameters, including the device's user name, password, IP address, port, name, and time zone.
  - Viewing resources (doors, cameras, alarm inputs, or alarm outputs) linked with the device, or importing the resources linked to the device.
  - Configuring Wiegand parameters and parameters of serial port number.
  - Configuring card reader protocols, readable card types, and M1 card encryption reading settings.
  - Configuring the uploading and storage of profile pictures.
  - Jumping to the Web page of the device.
  - Configuring multi-factor authentication.
  - Configuring multi-door interlocking.
  - Configuring authentication password.
- On the Door Details page, the following tasks can be performed.
  - Configuring basic parameters of the door, including name, door unlocking duration and alarm, auto-locking, duress code, super password, and dismiss code.
  - Linking cameras to the door, and viewing live view of the linked cameras.
  - Enabling the function of automatically capturing pictures for the door.
  - Enabling card readers for the door and configuring parameters of card readers, including name, buzzing duration, card swiping interval, tampering detection, failed card template alarm, and card reader authentication mode.
  - Configuring Remain Unlocked & Remain Locked, multi-door interlocking, and Unlock Doors with First Person.

Manage Departments And Persons

Add/edit/delete departments and persons. On the Person page, you can go to the ***Credential Configuration*** page to select collecting mode of credentials and configure the collecting devices. For collected profile pictures, if you need to ***protect the persons' privacy*** , you can disable the function of exporting profile pictures or convert the profile pictures to unreadable models.

Add and Assign Access Levels

Persons with assigned access levels can access to specific doors during defined time periods.

Real-Time Monitoring of Doors

You can view the live view of cameras linked to a door. During the live view, you can ***change door status*** in real time if necessary. You can also drag doors to a map and ***monitor them via the map*** so as to know situation of multiple doors quickly. The map supports viewing live view of doors and changing door statuses.

Video Intercom

- View records of missed calls from devices, and call the device back
- Start two-way audio with a device.
- ***Configure parameters of two-way audio for the current client.***

Import Person Authentication Events from Devices to the Client

Person authentication events include normal and abnormal authentication records. When the system misses events, you can import events stored in devices to the system.

Search for Access Events

Access events include person authentication events, access control device events, and video intercom call records.

View Statistics

The statistics show an overview of persons, person credentials, access levels of persons, and access events. When viewing the statistics, users can go to corresponding page to configure these items in real time.

4.1 Preparations

4.1.1 Add Devices

The system supports adding access control devices, door stations, and barrier gates.

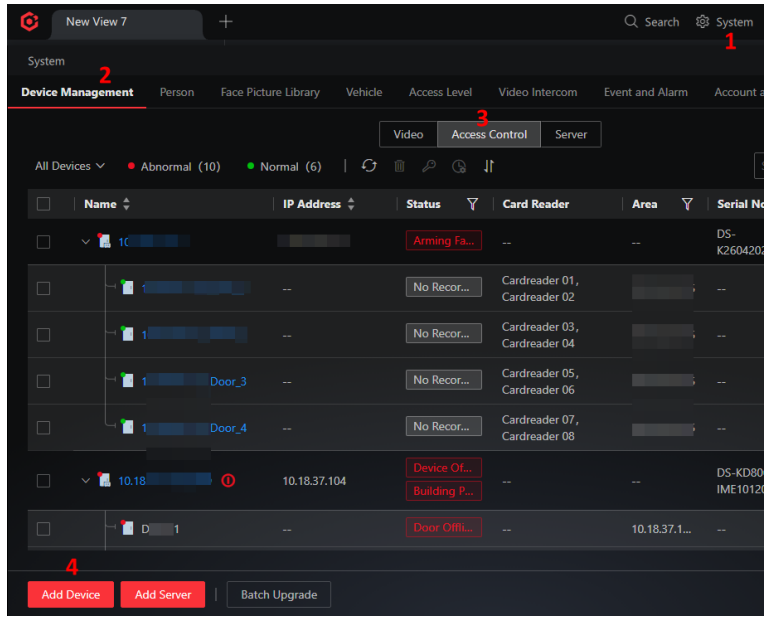


Figure 4-1 Device List

See ***Add Devices*** for details.

4.1.2 View Details of a Device

View configuration and status of a selected device, and edit its configurations.

In the device list, click the name of a device, or right-click a device/door, and then select **View Details**.



Figure 4-2 Details of an Access Control Device

Resource Information

For alarm inputs and alarm outputs, you can also import them in the device list.

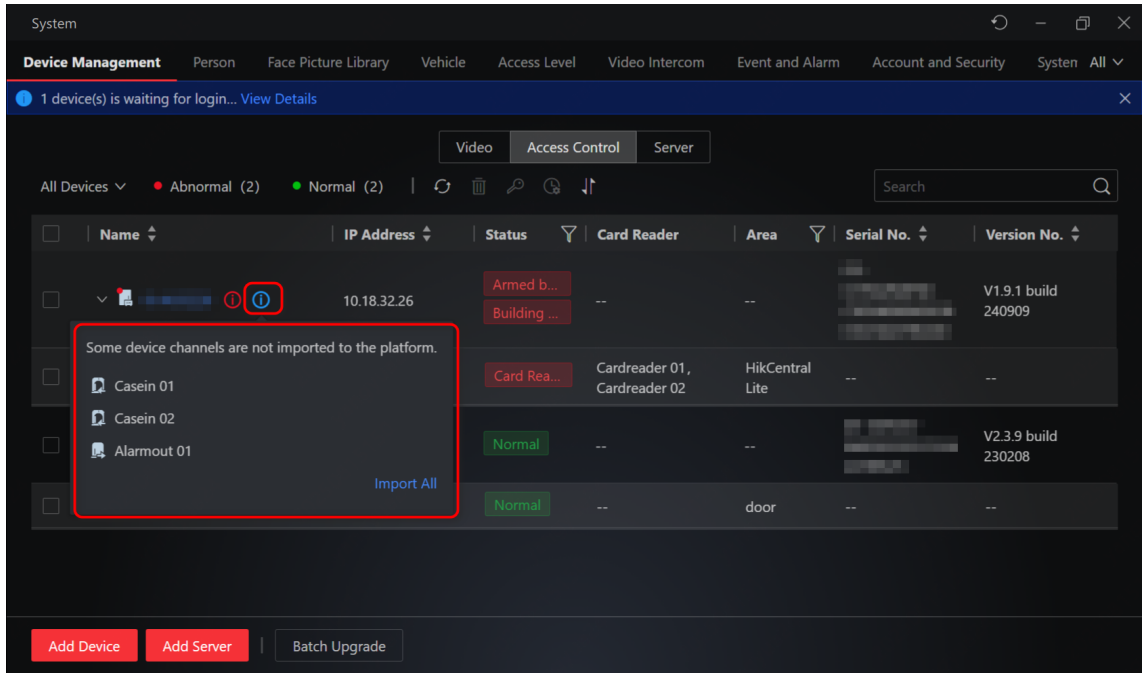


Figure 4-3 Device List

Multi-Factor Authentication

Authentication Interval

Make sure the interval between two authentications is within this value. For example, when you set the interval as 5s, if the interval between two authentications is longer than 5s, the multi-factor authentication will be invalid, and you should authenticate again from the beginning.

Authentication Password

This feature requires both device support and that the role assigning permissions (admin or operator) has access to **Authentication Code Configuration**. For more details, see ***Add a Role*** .

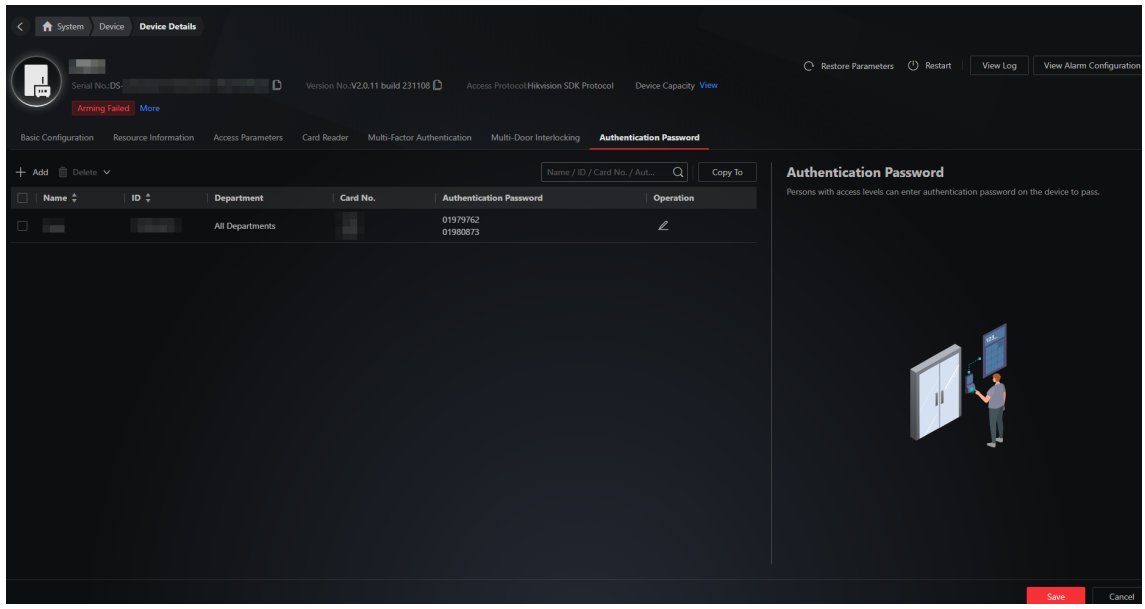


Figure 4-4 Authentication Password

4.1.3 View Details of a Door

In the device list, click the name of a door, or right-click a door, and then select **View Details**.

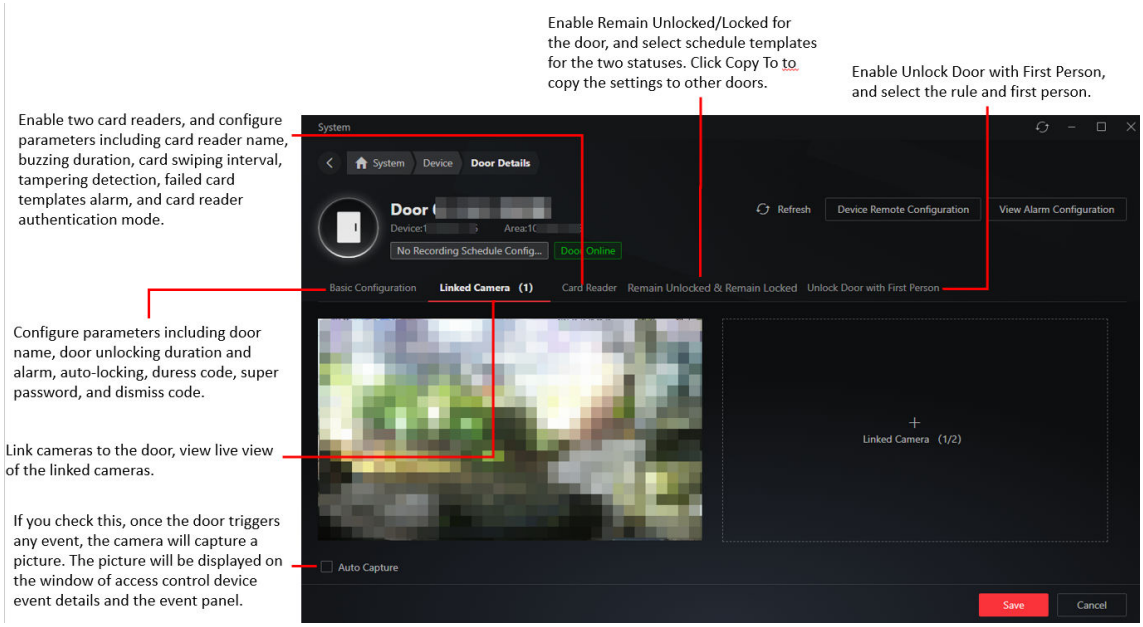


Figure 4-5 Door Details

4.2 Add Departments and Persons

On the Person page, you can add persons via different methods, export person information or profile pictures to the PC, or manage existing persons.

Add a Department

Right-click the root node of department, and select **Add Sub-Department** to add a department.

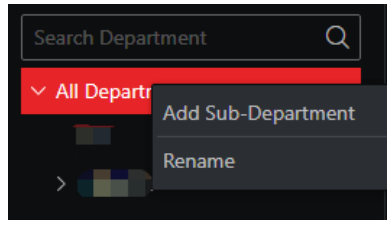


Figure 4-6 Department Tree

Right-click an added department, and select **Add Same-Level Department** or **Add Sub-Department**.

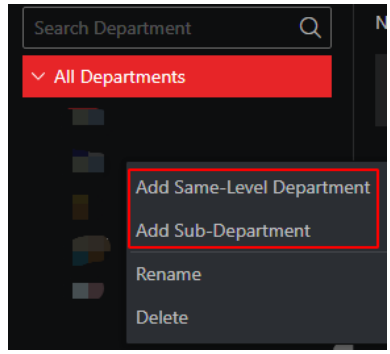


Figure 4-7 Department Tree

In the department tree, drag a department to change its level.

Add Persons

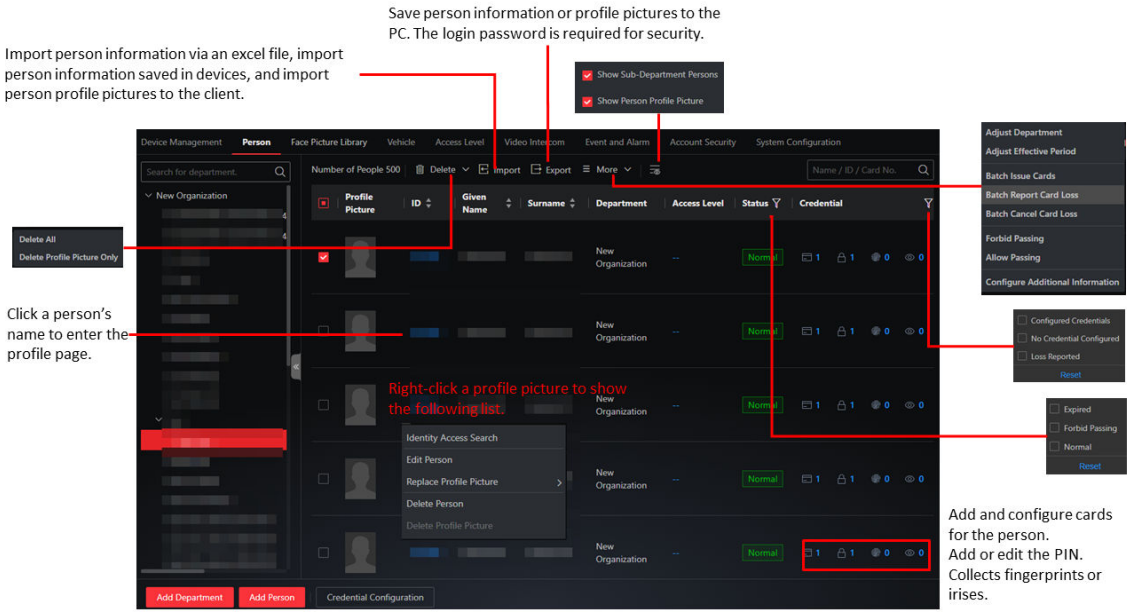


Figure 4-8 Person List

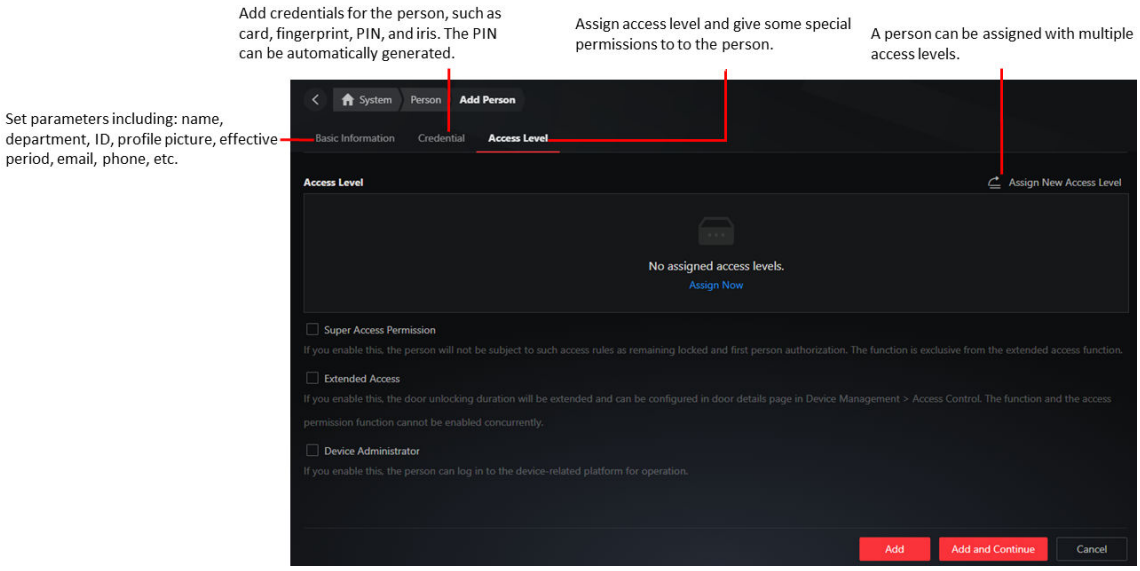
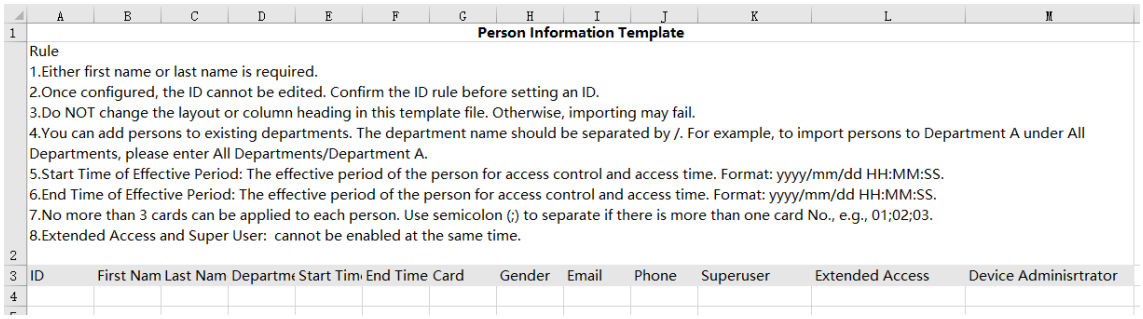


Figure 4-9 Add Person Page

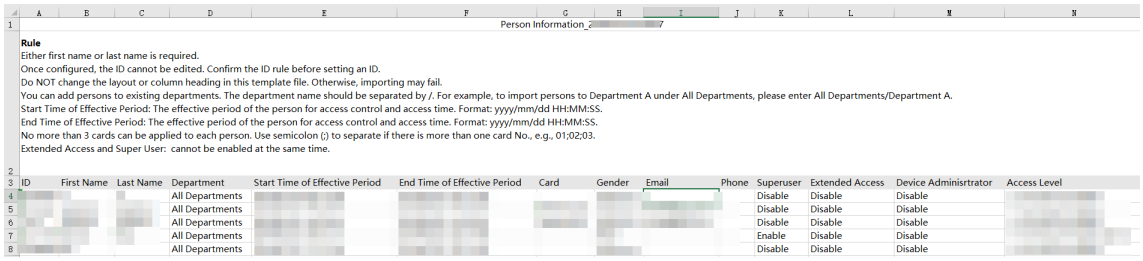


Person Information Template

Rule
1.Either first name or last name is required.
2.Once configured, the ID cannot be edited. Confirm the ID rule before setting an ID.
3.Do NOT change the layout or column heading in this template file. Otherwise, importing may fail.
4.You can add persons to existing departments. The department name should be separated by /. For example, to import persons to Department A under All Departments, please enter All Departments/Department A.
5.Start Time of Effective Period: The effective period of the person for access control and access time. Format: yyyy/mm/dd HH:MM:SS.
6.End Time of Effective Period: The effective period of the person for access control and access time. Format: yyyy/mm/dd HH:MM:SS.
7.No more than 3 cards can be applied to each person. Use semicolon (;) to separate if there is more than one card No., e.g., 01;02;03.
8.Extended Access and Super User: cannot be enabled at the same time.

ID	First Nam	Last Nam	Departme	Start Tim	End Time	Card	Gender	Email	Phone	Superuser	Extended Access	Device Adminisrtrator

Figure 4-10 Template for Importing Persons



Person Information_2[redacted]7

Rule
Either first name or last name is required.
Once configured, the ID cannot be edited. Confirm the ID rule before setting an ID.
Do NOT change the layout or column heading in this template file. Otherwise, importing may fail.
You can add persons to existing departments. The department name should be separated by /. For example, to import persons to Department A under All Departments, please enter All Departments/Department A.
Start Time of Effective Period: The effective period of the person for access control and access time. Format: yyyy/mm/dd HH:MM:SS.
End Time of Effective Period: The effective period of the person for access control and access time. Format: yyyy/mm/dd HH:MM:SS.
No more than 3 cards can be applied to each person. Use semicolon (;) to separate if there is more than one card No., e.g., 01;02;03.
Extended Access and Super User: cannot be enabled at the same time.

ID	First Name	Last Name	Department	Start Time of Effective Period	End Time of Effective Period	Card	Gender	Email	Phone	Superuser	Extended Access	Device Adminisrtrator	Access Level
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Disable	Disable	Disable	[redacted]
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Disable	Disable	Disable	[redacted]
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Disable	Disable	Disable	[redacted]
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Enable	Disable	Disable	[redacted]
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Disable	Disable	Disable	[redacted]

Figure 4-11 Exported Person Information

Additional information will be included in the downloaded template if any.

To export person profile pictures, you should enable this function first on the Profile Picture page (**System → System Configuration → Security → Profile Picture**). See ***Protect Profile Pictures*** .

For deleted persons, their information (including name, ID, validity period, credentials, etc.) will still be kept (Go to **System → Storage → Data Retention Time → Deleted Person Data** to configure data retention time for them.) During the retention time, the data of deleted persons can still be found; otherwise the data will be deleted.

4.2.1 Configure Credential-Related Parameters

Make sure you select the right collecting mode and configure the collecting device properly.

On the Person page, click **Credential Configuration**. Select a collection mode according to the following table.

Table 4-1 Scenarios Applicable for Different Collection Mode

Collection Device	Scenario
• Card Enrollment Station • Fingerprint Recorder • USB Camera	Credentials of persons in different places are needed to collect (so that you should take the devices to different places). You can collect cards anywhere, and persons can come up and sit beside you for collecting fingerprints and taking face pictures.
Access Control Device	The collection device is already installed and cannot be moved. So you should add the device to the system first, and then collect credentials remotely. This function should be supported by devices. If you fail to collect the card No., go to the Door Details page and check whether the door is armed.
Enrollment Station	The enrollment station can be used for collecting credentials via USB or network. It supports collecting cards, face pictures, and fingerprints. You can take it to anywhere, and the collected credentials can be stored in the device.

4.2.2 Protect Profile Pictures

Read this topic if you have requirement for protecting profile picture.

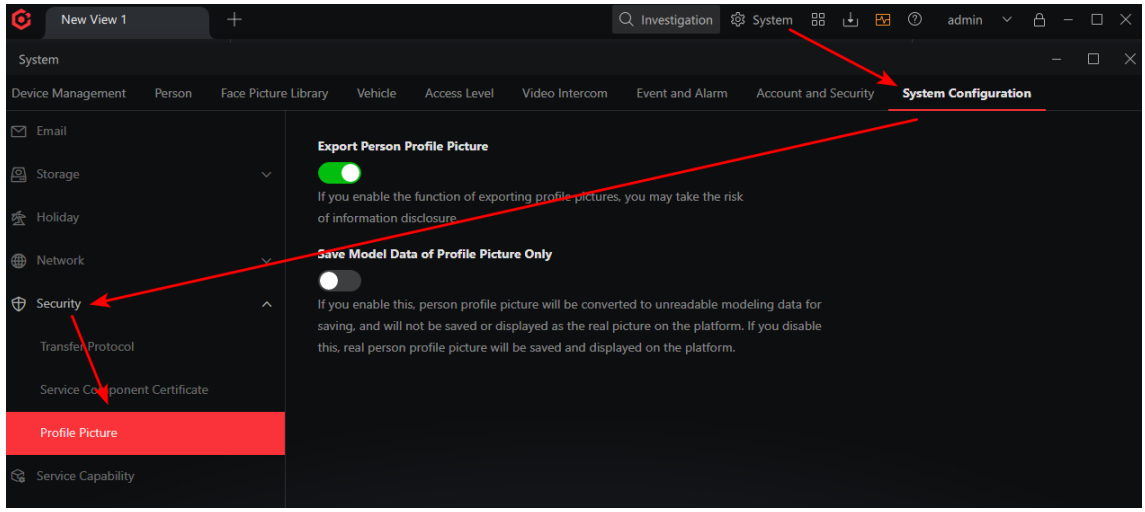


Figure 4-12 Entry of Protect Profile Pictures

Export Person Profile Picture

If you enable this function, you will be able to export persons' profile pictures to the PC.

Note

Only the admin user can enable this function.

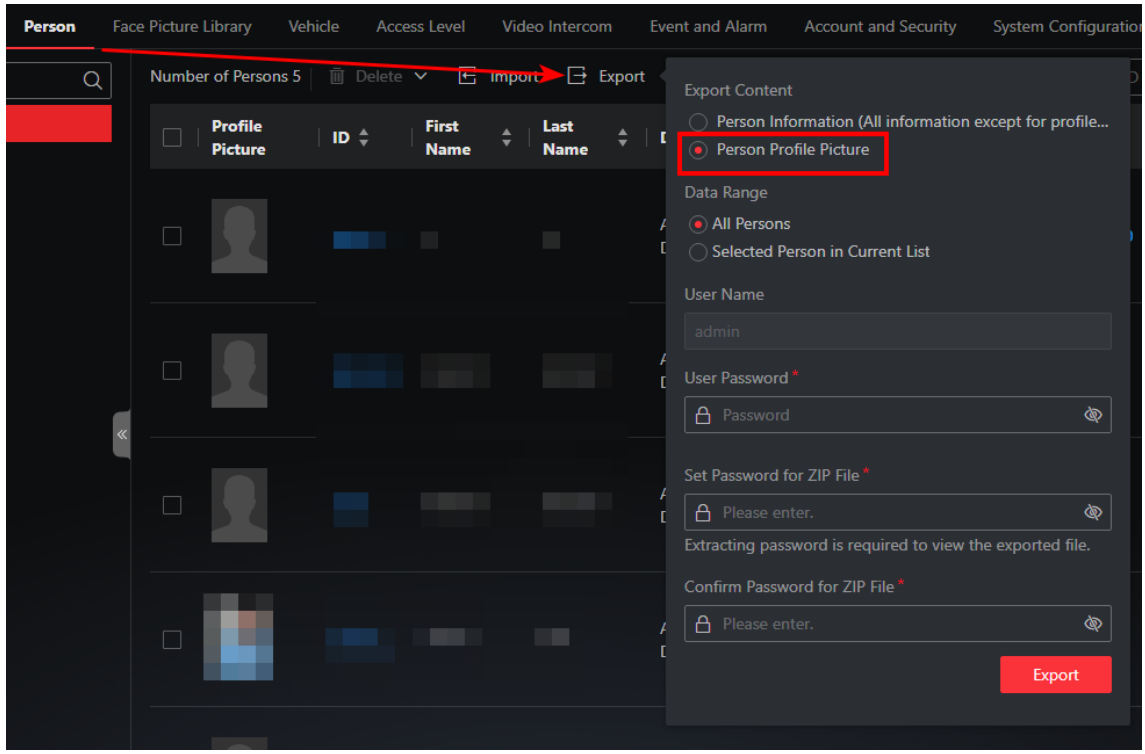


Figure 4-13 Entry of Exporting Profile Pictures

4.3 Add and Assign Access Levels

By selecting doors and an access schedule, you can add an access level. After this, you can assign the access level to persons or departments. In this way, the persons can authenticate and open the selected doors during the defined time periods.

What is the Access Level?

The access level is a group of doors sharing the same access schedule. Assigning access level to persons or departments can define the access permission that which persons can get access to which doors during the authorized time period.

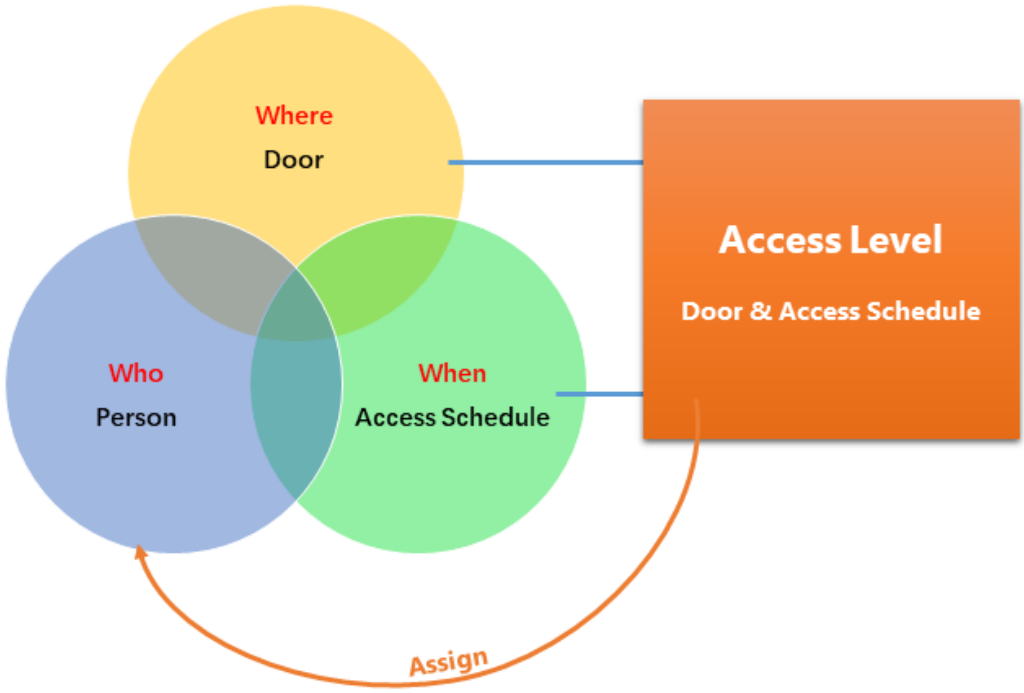


Figure 4-14 Access Level

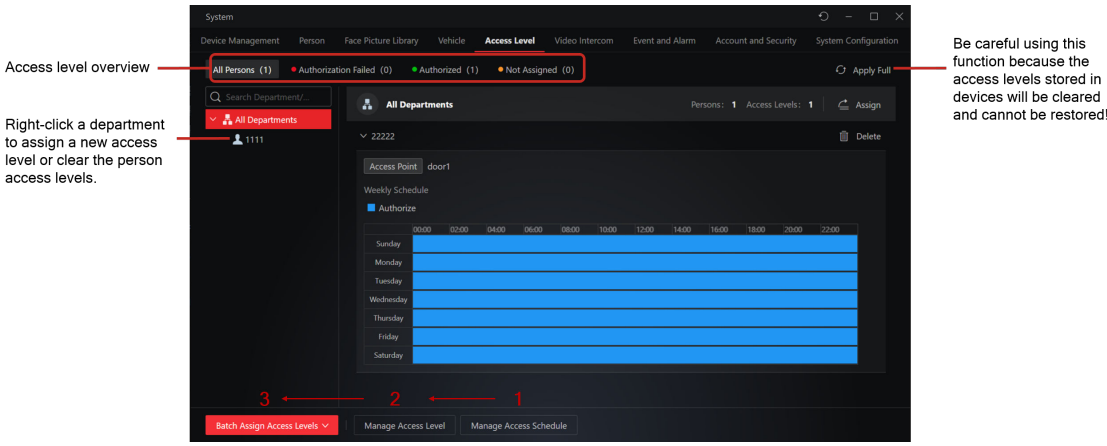


Figure 4-15 Access Level Page

Add an Access Schedule

An access schedule defines when people can open the door. Three default access schedule templates are provided: all-day template, workday template, and weekend template.

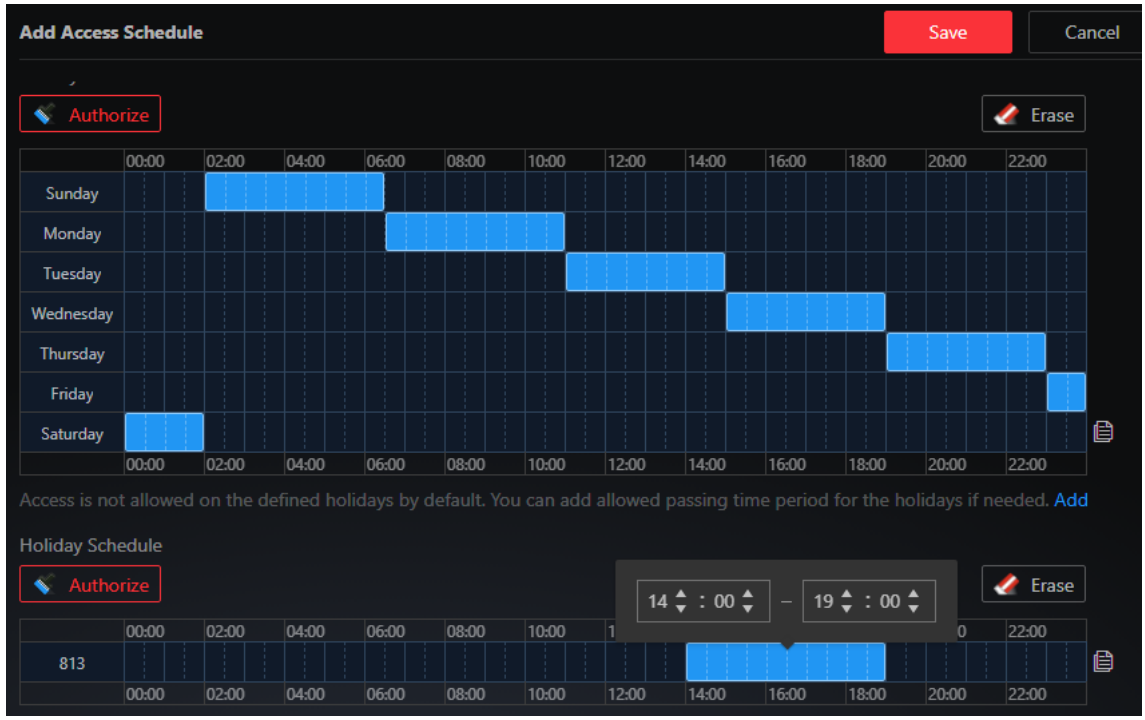


Figure 4-16 Add an Access Schedule

Click **Authorize**, and then drag on the time bar to draw authorized time periods. After drawing, you can hover the cursor on the blue area and enter a time or adjust the time by clicking the arrows in the box popped up. For details about adding or editing a holiday, see ***Add or Edit a Holiday*** .

Add an Access Level

When creating an access level, users can select multiple doors. A door can be added to different access levels.

About the Assignment of Access Levels

Assign Access Level by Department

Used for scenarios where persons need to authenticate for entering fixed places (such as offices). After assigning an access level to a department, newly-added persons will be automatically assigned with the same access level.

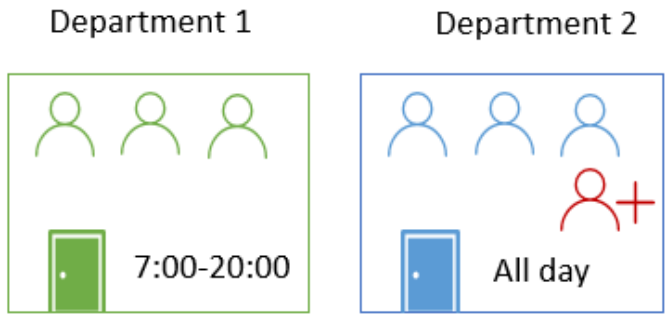


Figure 4-17 Assign Access Level by Department

Assign Access Level by Person

Used for scenarios where a person needs the access level of a special door, or a person needs a temporary access level of a door.

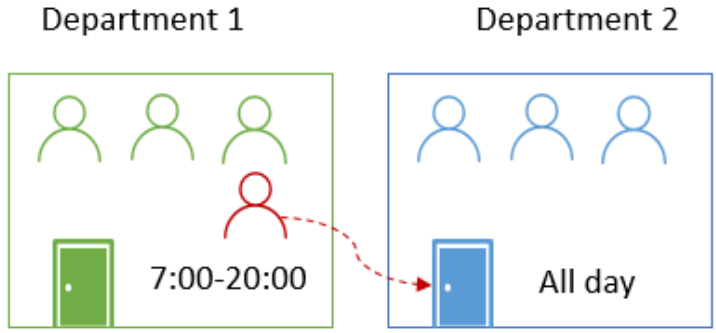


Figure 4-18 Assign Access Level by Person

Apply Assigned Access Levels to Devices

After assigning access levels to persons via the client, the assignment will be automatically applied to devices. The following reasons may cause the failure of access level assignment:

1. The device to which the access level is applied is offline.
2. The network connection is unstable.

4.4 Add an Alarm

You can add an alarm for a specified device, or all resources in the system.

Both doors and access control / video intercom devices can trigger alarms. You can go to the Add Alarm page from the device details page, or the Event and Alarm module. See ***Add an Alarm*** for details about adding an alarm.

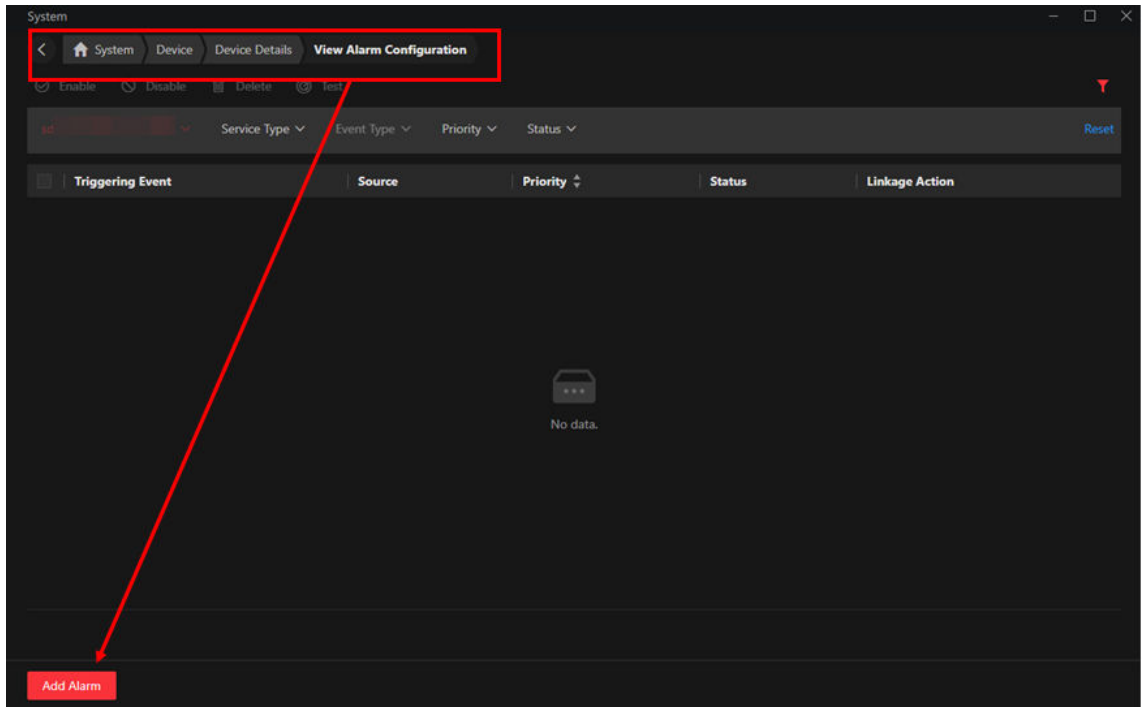


Figure 4-19 Alarm Configuration Page

Supported alarm categories are as follows. See ***Supported Triggering Events*** for details.

Resources that Can Trigger Alarms	Alarm Category
Door	• Normal Card Swiping • Abnormal Card Swiping • Other Door Events
Access Control / Video Intercom Device	• Device Security • Device Network • Device Battery • Device Record Reporting • Device Disk/HDD • Device Component Communication • Local Operation on Device • Remote Operation on Platform

Resources that Can Trigger Alarms	Alarm Category
Alarm Input	• Alarm Input Triggered • Alarm Input Restored
Person	• Person Matched Event • Card Number Matched Event

4.5 Real-Time Monitoring of Doors

You can monitor doors and control door status in real time. Refer to the following table for the explanations.

Table 4-2 Explanations of Door Status, Door Contact Status, Door Lock Status, and Door Status Control

Status	Icon	Explanation
Door Status		Door Locked Door Lock Locked
		Door Locked Door Lock Remain Locked
		Door Locked Door Lock Unlocked
		Door Locked Door Lock Remain Unlocked
		Door Unlocked Door Lock Locked
		Door Unlocked Door Lock Remain Locked
		Door Unlocked Door Lock Unlocked
		Door Unlocked Door Lock Remain Unlocked
		Unknown

Status	Icon	Explanation
Door Contact Status		Door Contact Unlocked
		Door Contact Locked
Door Lock Status		Door Lock Unlocked
		Door Lock Locked
Door Status Control		Close Door
		Open Door
		Set to Door Remain Locked
		Set to Door Remain Unlocked

4.5.1 Monitor Doors and Control Door Status

After adding doors, you can control door status such as locking and unlocking doors. For the doors with build-in cameras or doors linked with cameras, you can also monitor doors and perform more operations during monitoring such as capturing and recording.

For the detailed explanations of door status, refer to ***Real-Time Monitoring of Doors*** .

- Control one door: double click a door or drag a door to the viewing grid, and then right click a door or click the icons in the lower right corner to control the door.

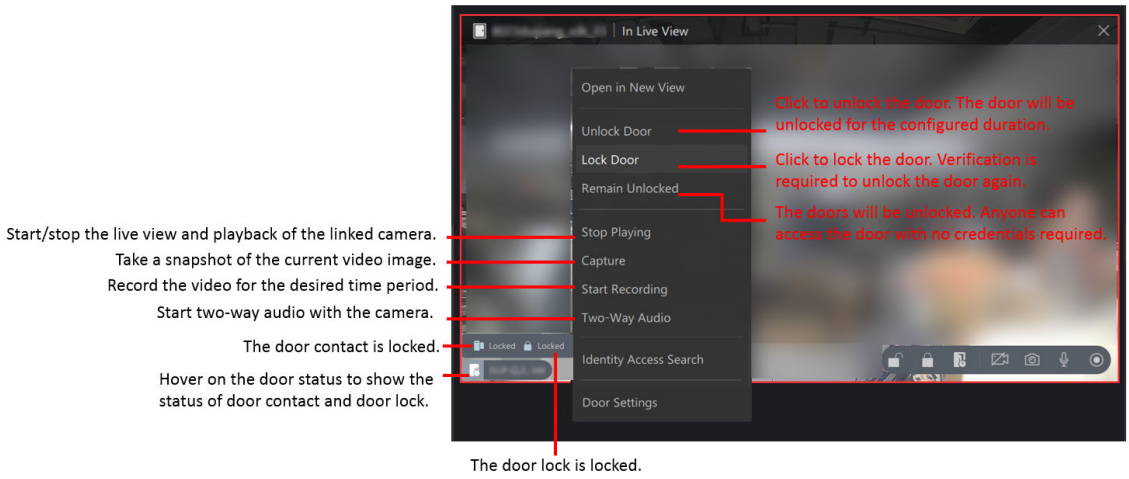


Figure 4-20 Supported Operations to Control One Door

These operations are only available for the doors with build-in cameras or doors linked with cameras: playing / stop playing video, capturing, recording, and two-way audio.

- Control doors on the current view: draw a frame to select doors and then right click the window to control the selected doors, or click the door status on the top of the viewing grid to batch control door status.

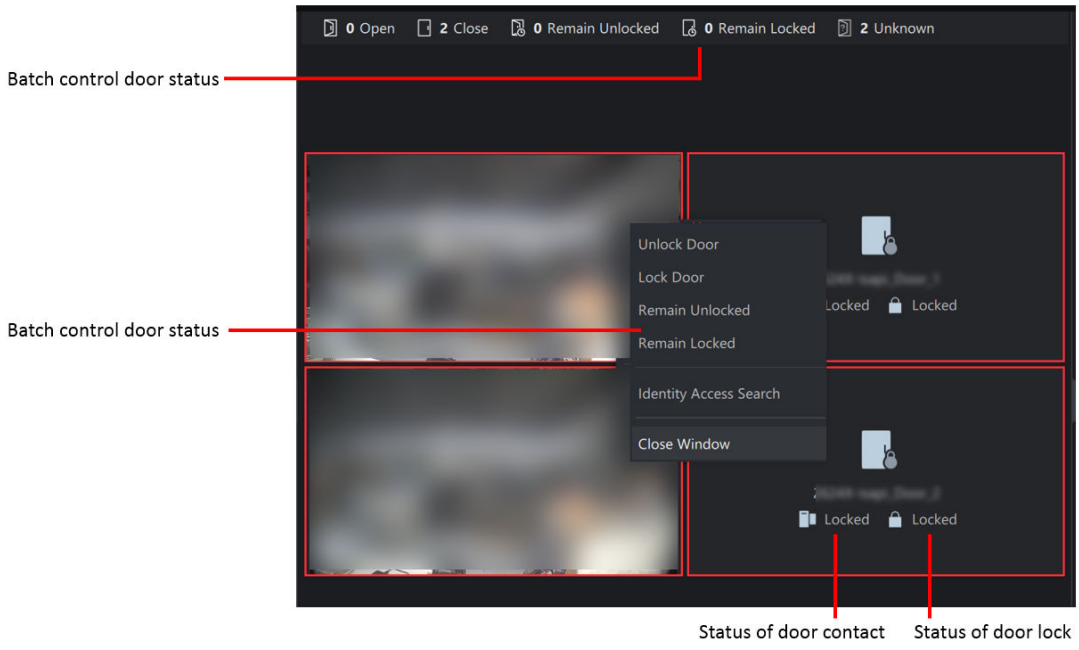


Figure 4-21 Select a Way to Control Doors on The Current View

- Control all the doors: in the **Shortcut** area, click **Quick Lock/Unlock**, and then you can batch unlock/lock all doors, or remain all doors unlocked/locked.

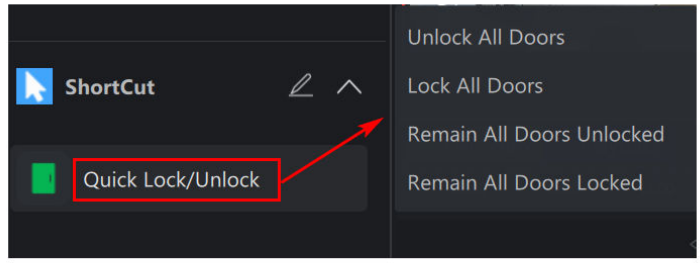


Figure 4-22 The Entry to Control All Doors

- Door status exceptions may occur. For example, when the magnetic contact and door lock status does not match, this typically indicates a physical obstruction preventing proper closure. The device should be checked immediately.

4.5.2 Display and Control Doors on the Map

After adding doors to the map, you can control door status such as locking and unlocking doors. For the doors of MinMoe face recognition terminal or doors linked with cameras, you can also monitor doors and perform more operations during monitoring such as capturing and recording.

For the detailed explanations of door status, refer to ***Real-Time Monitoring of Doors*** .

In the **Map** module, double click a map, or drag a map to the right window, or right click a map and click **Open** to view the map and the doors added to the map. For details about adding maps, refer to ***Add Map*** .

There are two modes for the map. In the Monitor mode ( ), you can monitor and control doors on the map. In the Configuration mode ( ), you can add doors, marks and hot regions to the map, set the types of resources to be displayed on the map, etc.

Add Map

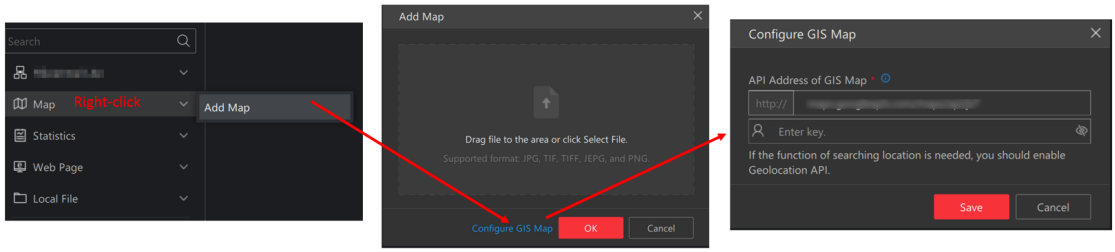


Figure 4-23 Add GIS Map

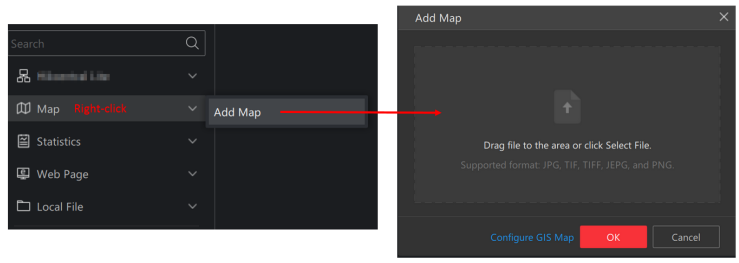


Figure 4-24 Add E-Map

Configuration Mode

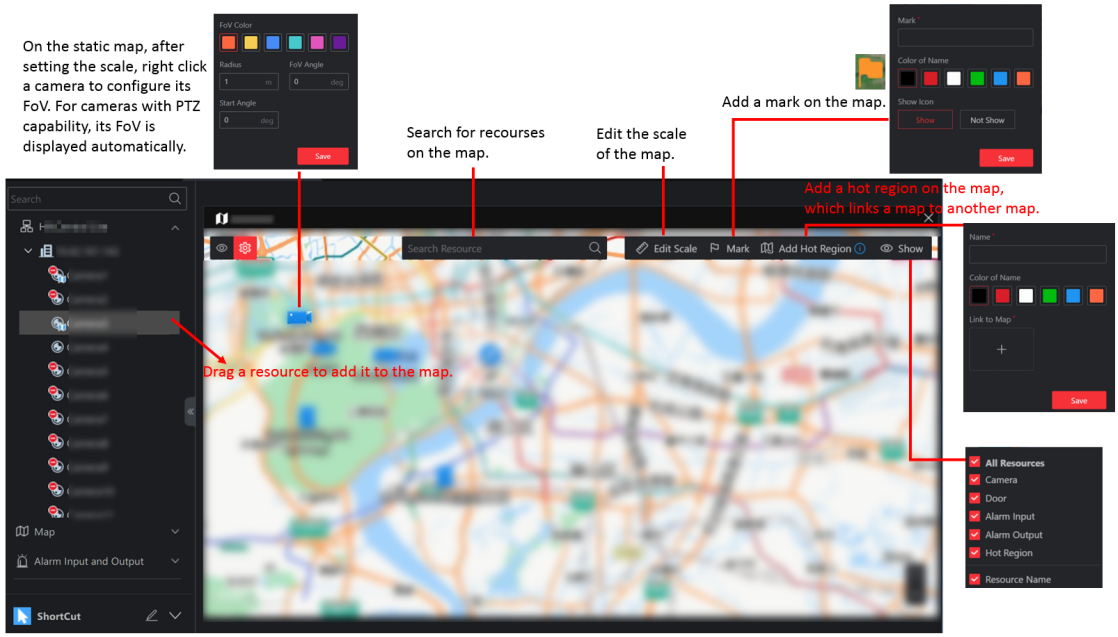


Figure 4-25 Supported Operations in Configuration Mode

Monitoring Mode

You can perform the following to monitor and control doors on the map.

- Monitor One Door: click a door to view the live view of its linked camera.
  Monitor Doors: click **Batch Select**, draw an area to select multiple doors, and click **Batch Play** to view the live view of its linked cameras in a batch.
  For details about supported operations when monitoring door(s), refer to ***Monitor Doors and Control Door Status*** .
- Control One Door: click the door or right click the door.

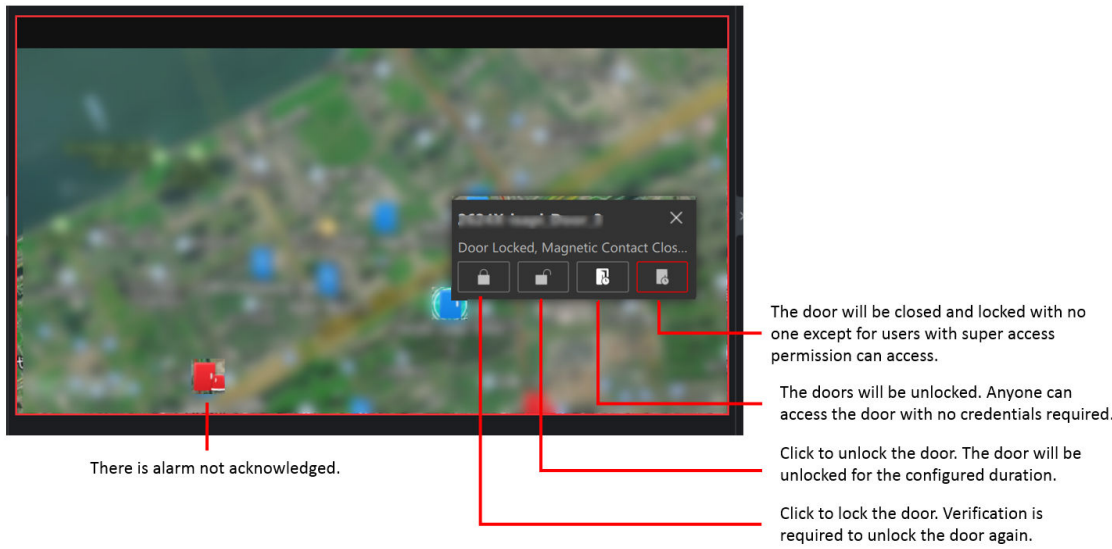


Figure 4-26 Control One Door

4.6 Video Intercom

People can call the system users via access control devices (including MinMoe face recognition terminals) and video intercom devices, and users can also call the device via the client.

Configure Parameters

Before two-way audio, you can configure parameters of calls from devices to the current client, and configure call recipients for different devices.

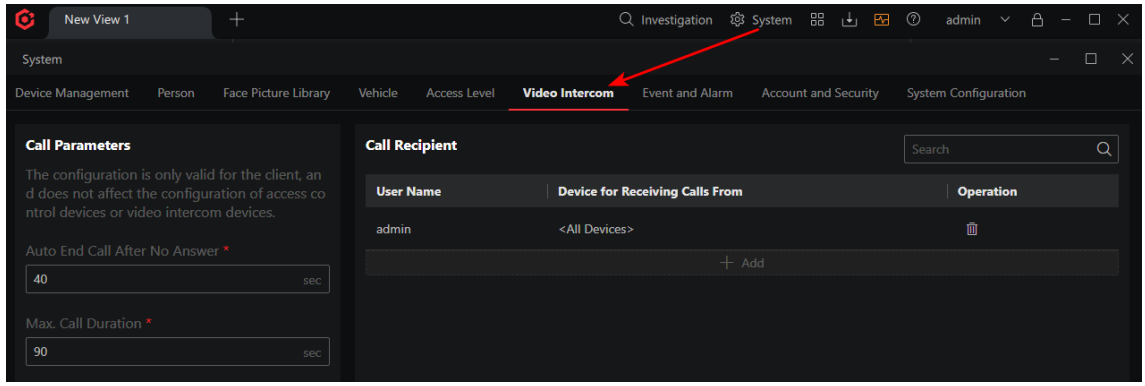


Figure 4-27 Entry of Video Intercom

Automatic Call End Time After No Answer

If a device calls the client and no one answers the call, the call will be ended automatically after the duration you set.

Max. Call Duration

The Max. duration of a talk between the client and a device.

Call Recipient

Select different devices for different users so that they can receive calls from different devices.

Video Intercom Call

You can call the device by the following two ways:

1. If a person called the client and the call was not answered, a notification will be displayed on the notification panel. Right-click the notification and select **View Details → Call Again** to call the device.

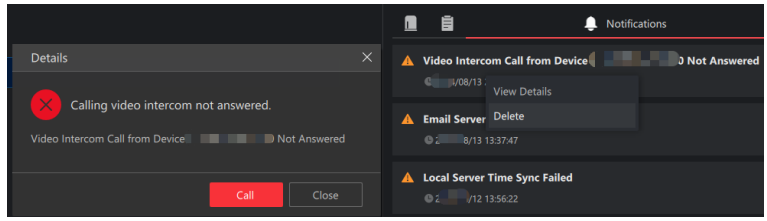


Figure 4-28 Call Device

2. In the live view window of a camera linked to a door, click

For details about how to search for video intercom call records, see ***Search for Video Intercom Call Records*** .

4.7 Import Person Authentication Events from Devices to the Client

Person authentication events include normal and abnormal authentication records. When the system misses events, you can import events stored in devices to the system.

Click **System → Access Event → Person Authentication Event** .

For online devices, you can import events by selecting devices. Specifying the time range of generating events is supported.

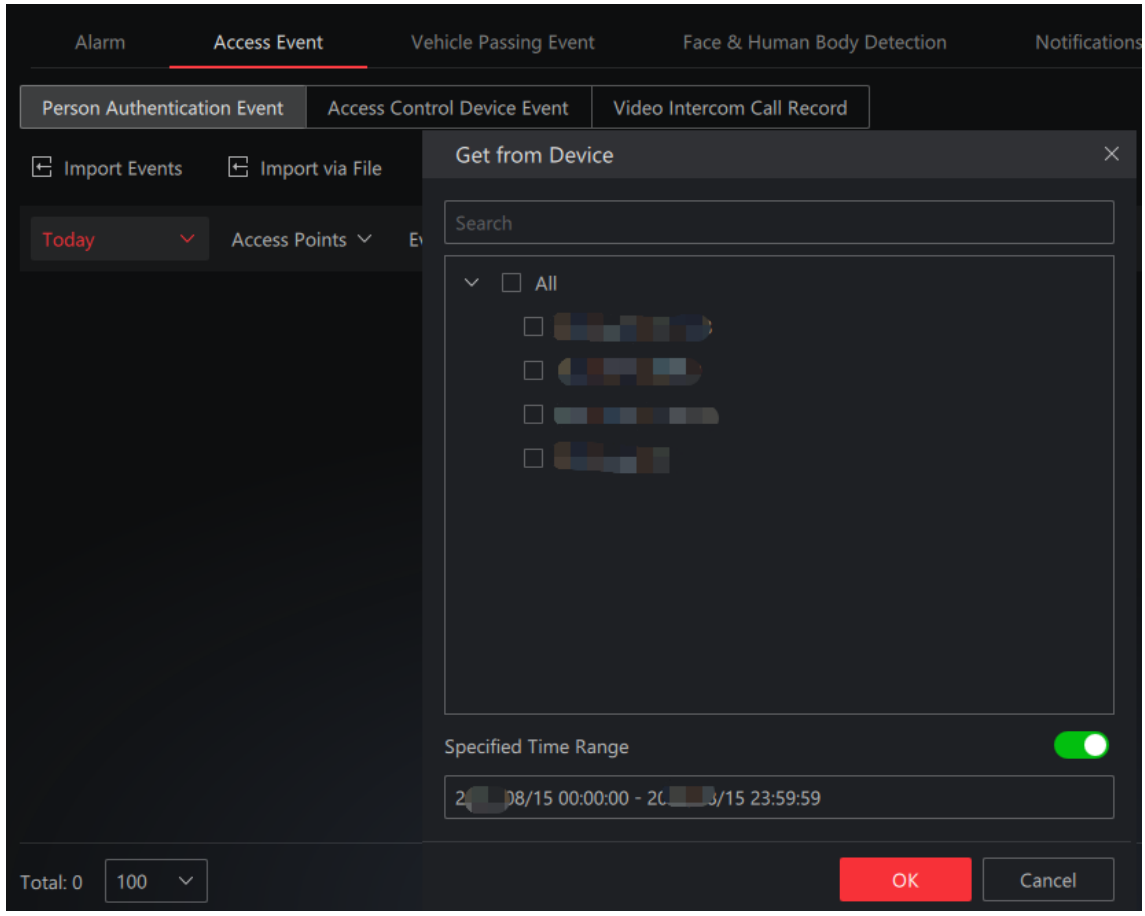


Figure 4-29 Get Events from Device

For devices that are unable to connect to the network, or devices are disconnected from the network which cannot restore for a long time, events can be imported via a CSV file. Plug a flash drive in the device, and start exporting events to the flash drive from the device. When the exporting finishes, plug the flash drive to the PC, and start importing the file.

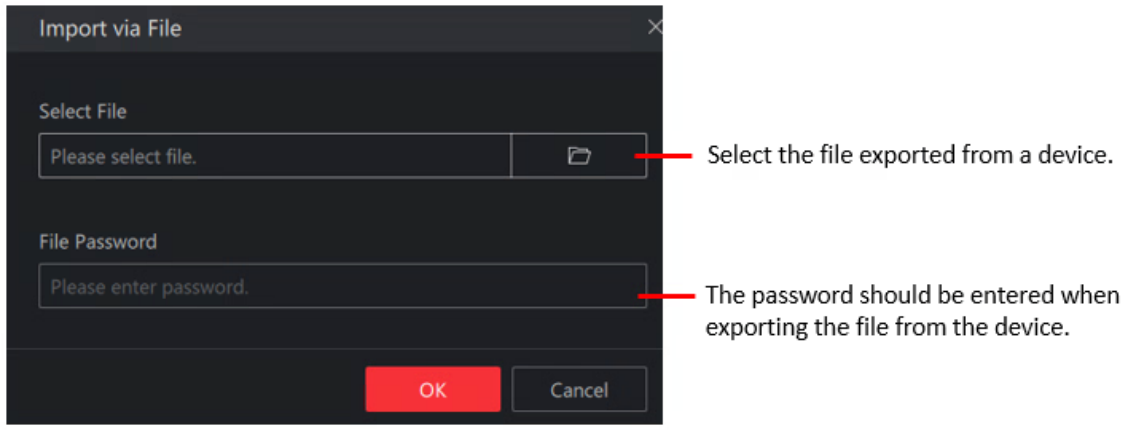


Figure 4-30 Import Events via File

Note

- Only encrypted files can be imported.
- The file name should meet the format requirement, e.g. recordlist_ device serial No. For example, recordlist_FC2922753.

4.8 Search for Access Events

Access events include person authentication events, access control device events, and video intercom call records.

Click **System → Access Event** .

Search for Person Authentication Event

Person authentication events include normal and abnormal authentication records.

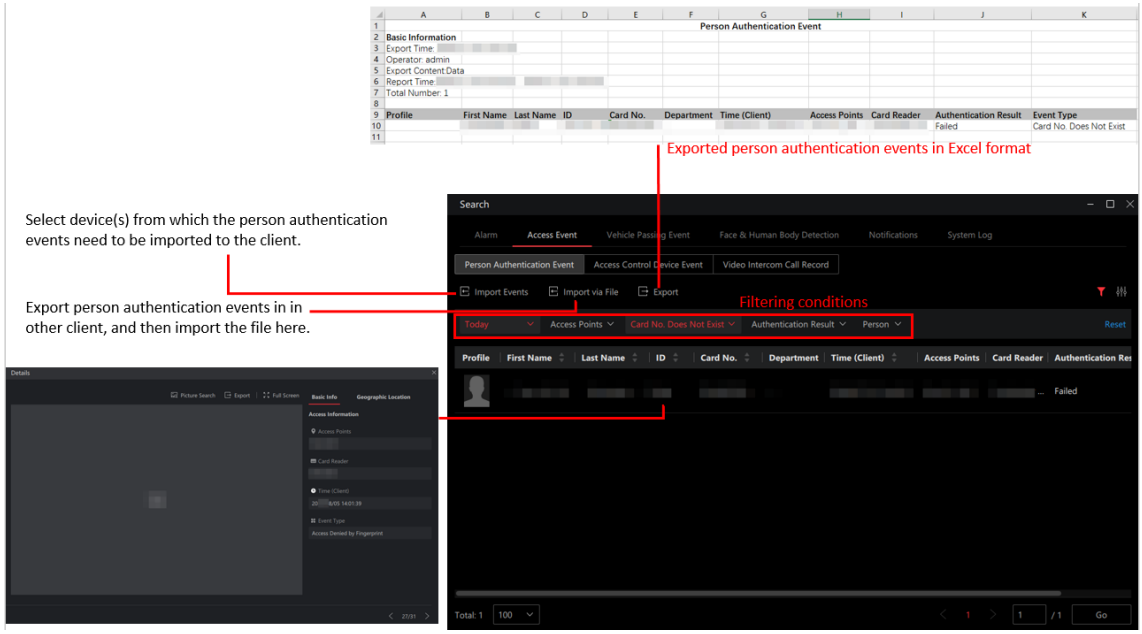


Figure 4-31 Person Authentication Event

Search for Access Control Device Event

Access control device events are events triggered when there is something happens to doors, access control devices, or video intercom devices, such as low battery voltage, door unlocked.

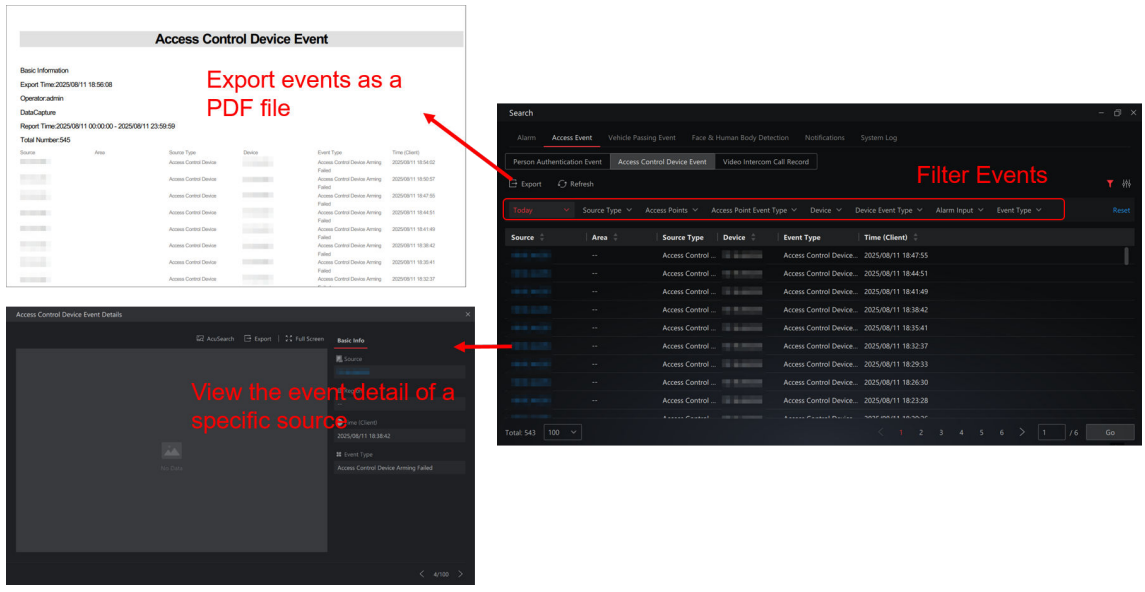


Figure 4-32 Access Control Device Event

Search for Video Intercom Call Records

The video intercom call record refers to the record of devices calling the client. Click **Export** to save all of the searched records to the PC, or select one record and then click to download it.

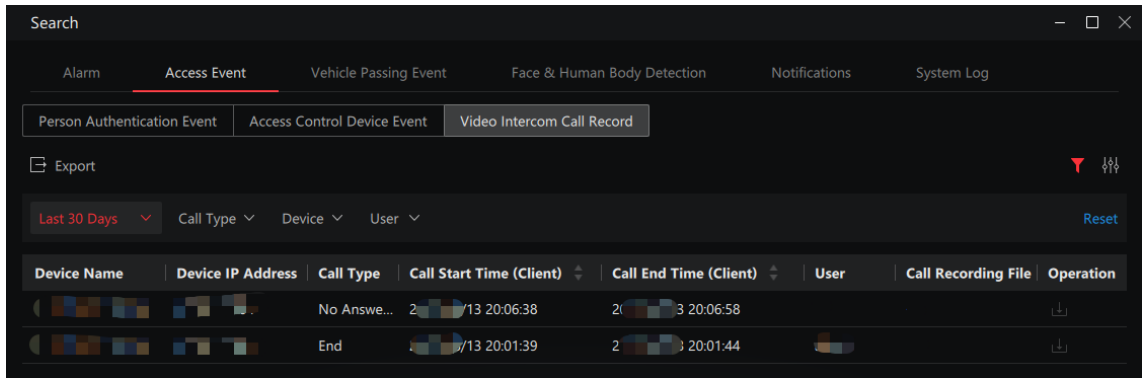


Figure 4-33 Video Intercom Call Records

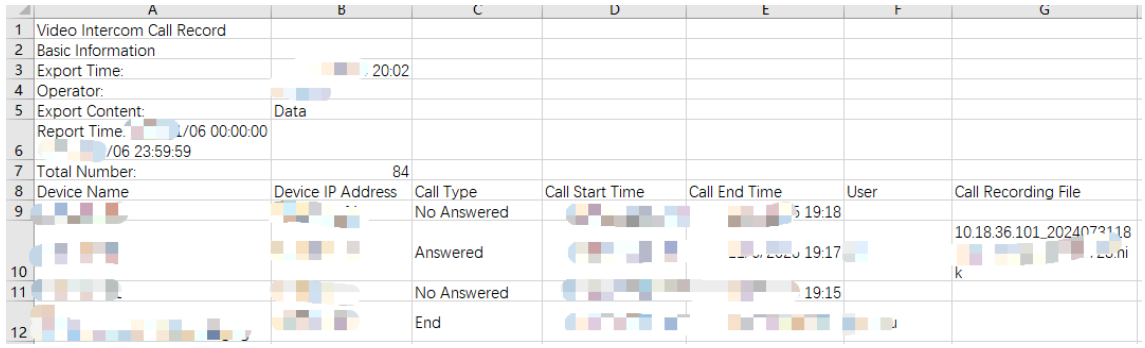


Figure 4-34 Exported Video Intercom Call Records

4.9 Display Statistics of Person&Credentials, Access Levels, and Access Events

The statistics show an overview of persons, person credentials, access levels of persons, and access events. When viewing the statistics, users can go to corresponding page to configure these items in real time.

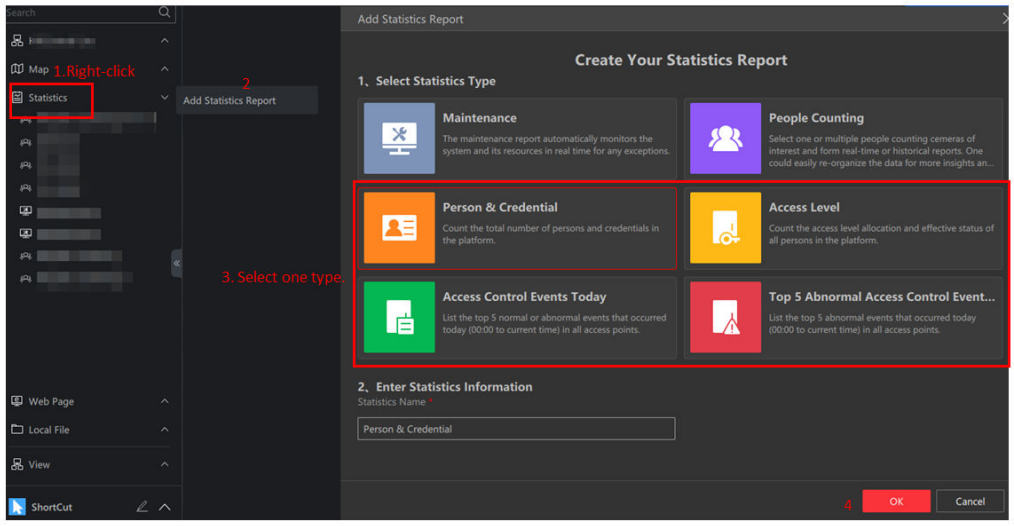


Figure 4-35 Add Statistics Report

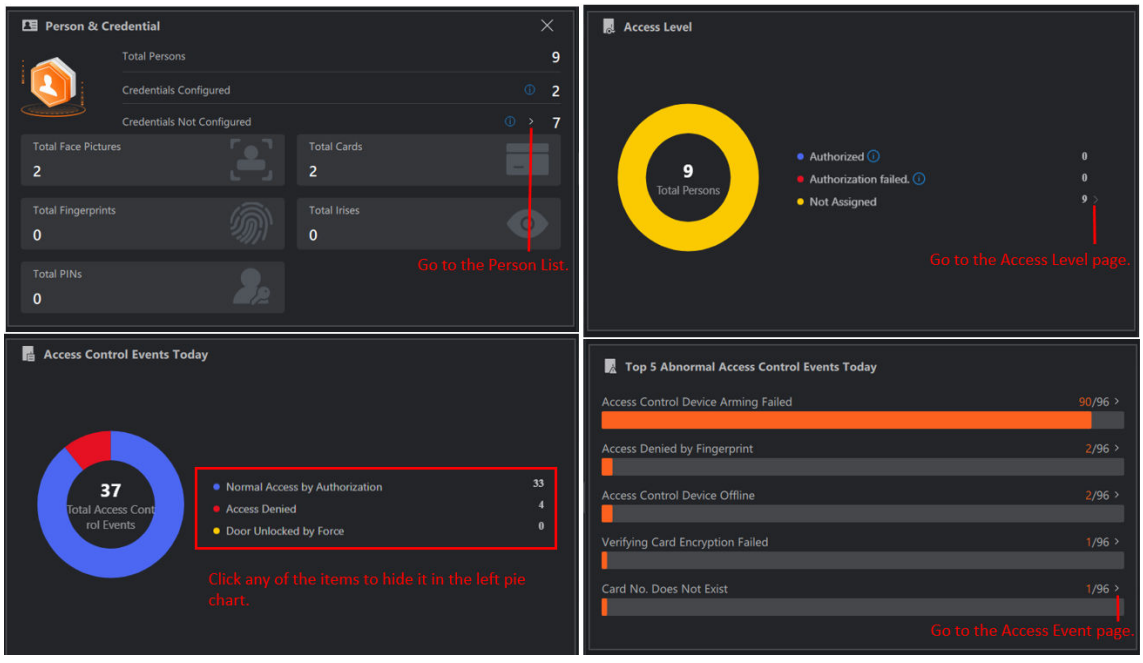


Figure 4-36 Statistics

Access Control Events Today

Normal Access by Authentication

Persons successfully unlocked doors via authentication of different credentials.

Access Denied

Persons' authentications failed, and doors were not unlocked.

Right-click a report to display the report in a new view, refresh the report, or export the report as a PDF file.

Chapter 5 Attendance

In the Attendance module, you can easily manage the attendance calculation rules, schedules, and attendance check points, correct employees' attendance, apply for leaves or business trips, and export attendance records.

Go to **System → Attendance** to enter the Schedule Table.

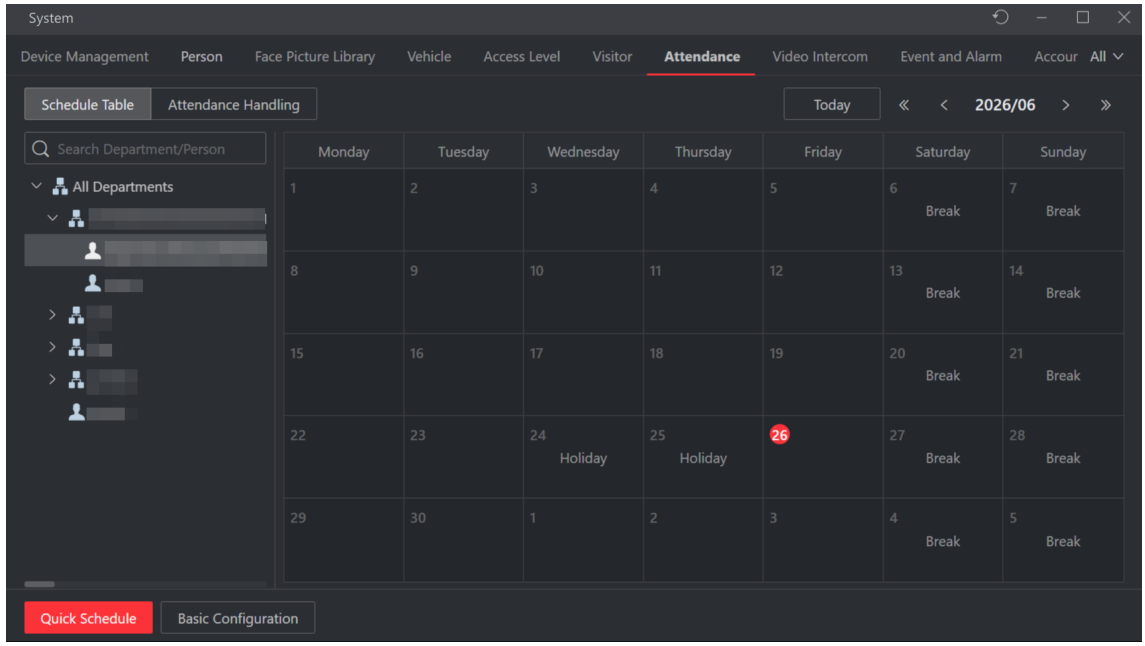


Figure 5-1 Schedule Table

5.1 Enable the Attendance Capability

To use the Attendance feature, you must enable both the **Attendance** and **Access Control** service capabilities.

Go to **System → System Configuration → Service Capability** . For details, see ***Configure the System Capability*** .

5.2 Quick Schedule

Create and manage quick schedule rules to assign work shifts and time periods to employees or departments, and view scheduling results in list or calendar format.

Before You Start

Configure the fundamental attendance rules that determine how attendance is calculated, including authentication type, overtime settings, attendance check points, and calculation accuracy. Click **Basic Configuration** at the bottom of the Attendance page.

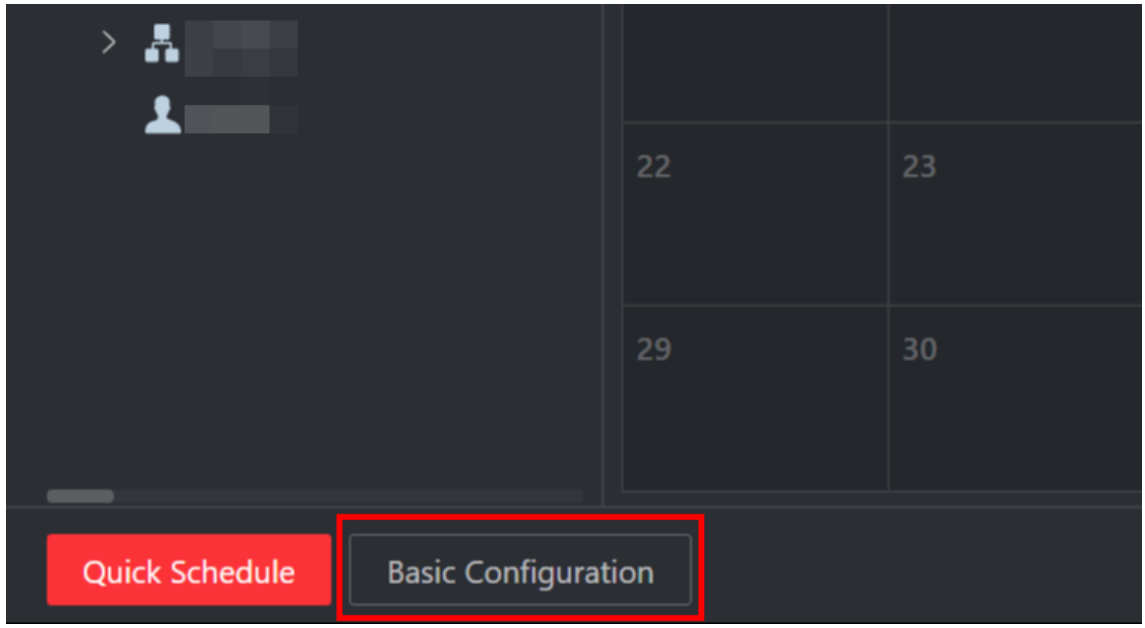


Figure 5-2 Basic Configuration Entry

- Authentication Type and Attendance check Point
  Select which authentication types should be used for attendance calculation. Only records from selected authentication types will be considered during attendance calculation.

  Authentication Type

  Select credentials for authentication.

  Attendance Check Point

  Configure which devices serve as attendance check points for check-in and check-out.

  All Check Points

  All access points can be used as check points, which means any authentication on all access points will be regarded as a checking in/out.

  Designated Attendance Check Point

  Only authentications on specified access points will be regarded as checking in/out.

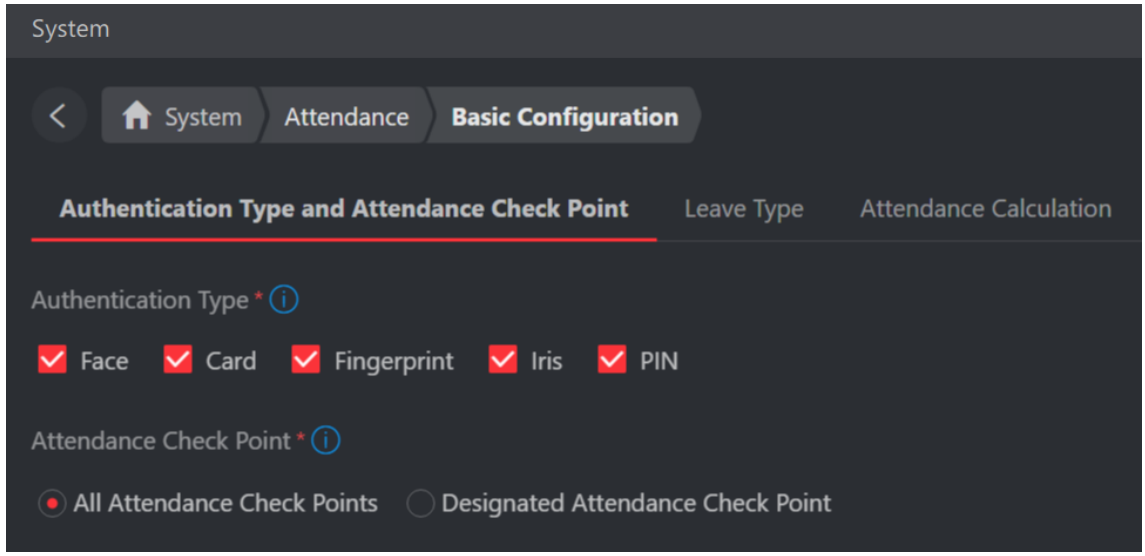


Figure 5-3 Authentication Type and Attendance Check Point

- Attendance Calculation Accuracy
  On this page, you can configure the calculating rules of attendance data, e.g., setting parameters such as the unit, time format, and rounding rule.

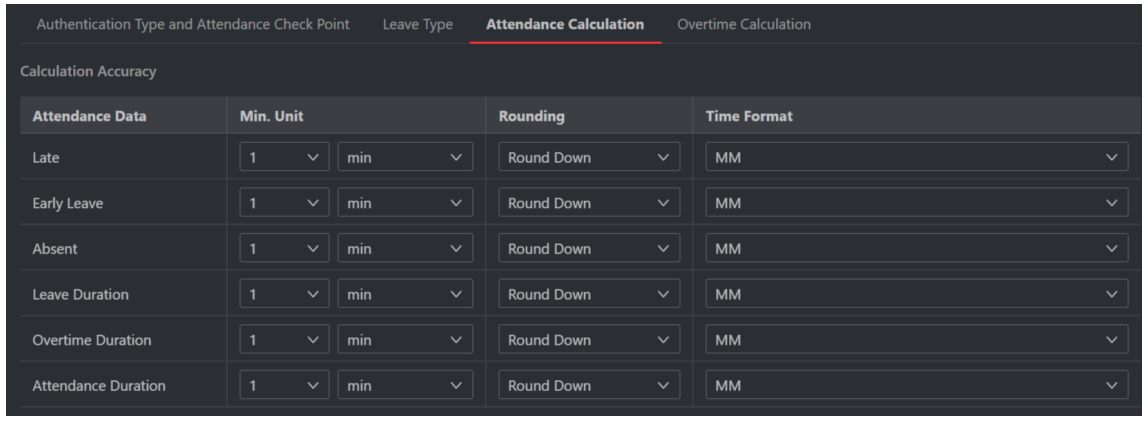


Figure 5-4 Calculation Accuracy

Round Up

Round the number of duration up, e.g., if you make 0.5 go up, then 6.5 rounds up to 7.

Round Down

Round the duration down, e.g., if you make 0.5 go down, then 6.5 rounds down to 6.

Round Nearest

Round decimal numbers to nearest integers either by rounding up or rounding down based on the tenths places, e.g., 6.5 rounds to 7 and 6.4 rounds to 6.

- Overtime Calculation

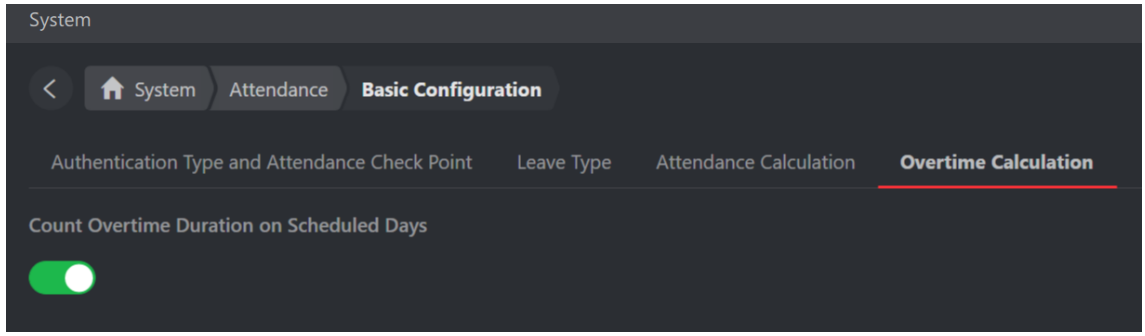


Figure 5-5 Overtime Calculation

When enabled, the system calculates overtime duration and display it on the Attendance Calculation page.

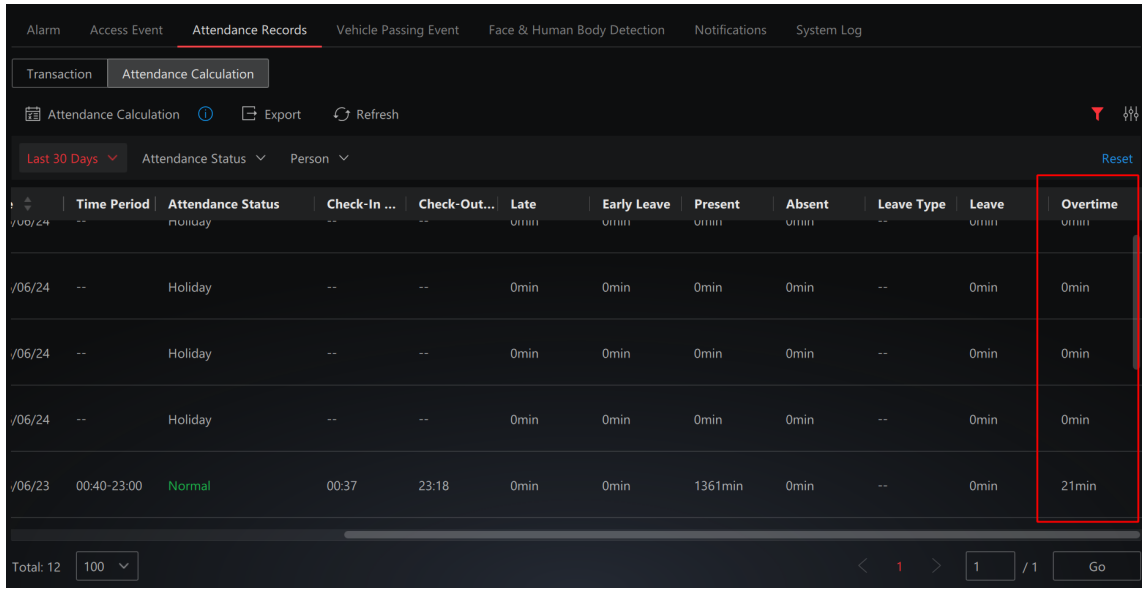


Figure 5-6 Attendance Calculation

Work Flow of Quick Schedule

Quick Schedule allows you to quickly managing schedules by selecting persons and setting shift and time period quickly.

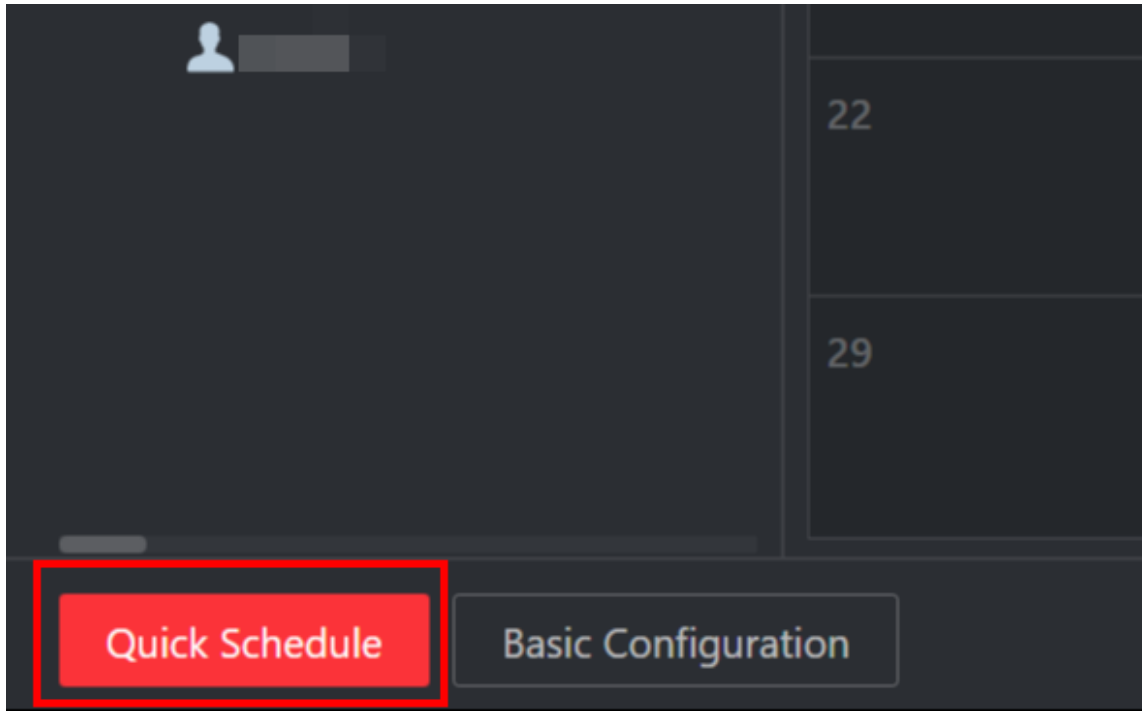


Figure 5-7 Quick Schedule Entry

1. Select Person
   Select persons in the department list, or select a department to check all persons in it.

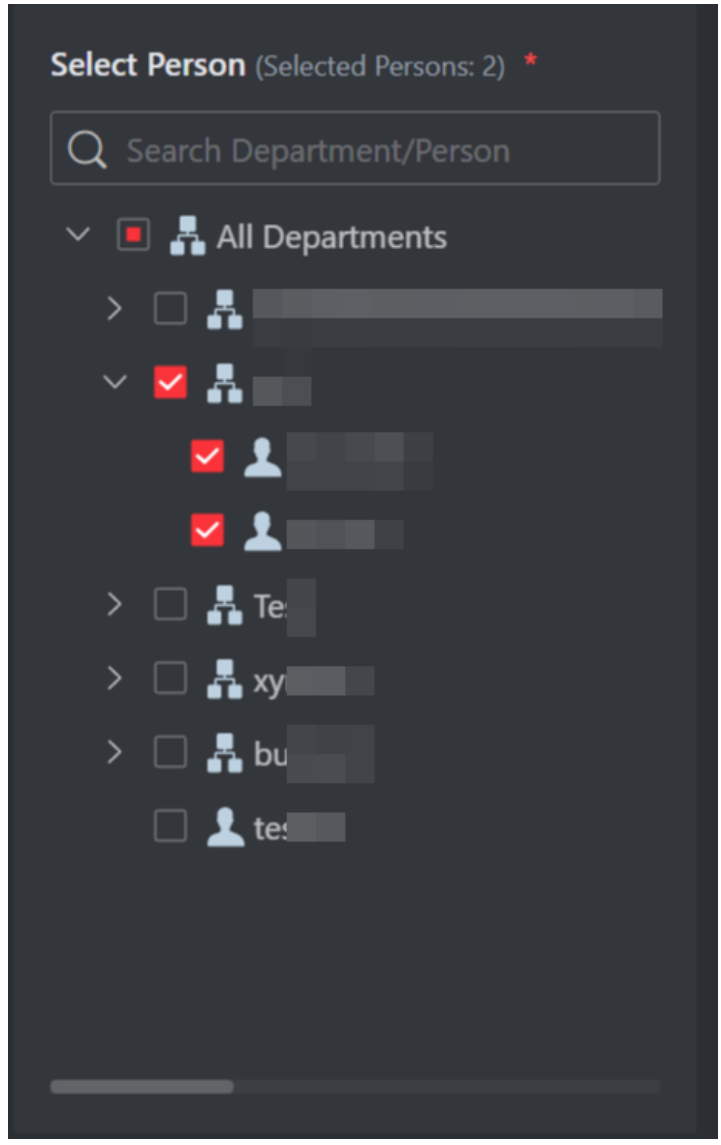


Figure 5-8 Select Person

2. Shift Settings

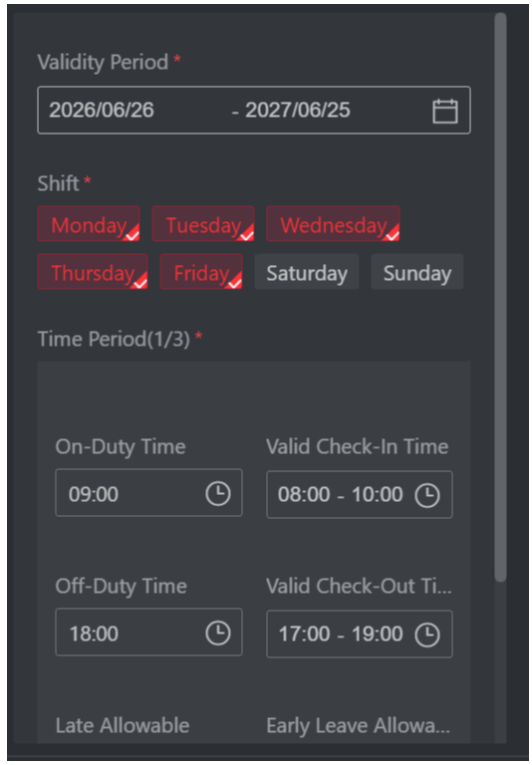


Figure 5-9 Shift Settings

Valid Period

Set the start and end dates during which this schedule rule is valid.

Shift

Configure which days of the week require scheduling under this rule. Select the specific weekdays that this schedule applies to.

Time Period

You can configure up to three time periods for each schedule rule. For each time period, specify the following:

On-Duty Time

The scheduled start time for work.

Valid Check-In Time

The time window during which a check-in is considered valid. Only check-ins within this window are recorded as successful. Check-ins outside this window will result in a no-check-in status.

Off-Duty Time

The scheduled end time for work.

Valid Check-Out Time

The time window during which a check-out is considered valid. Only check-outs within this window are recorded as successful.

Late Allowable

Enter the time duration to permit late check-ins within a defined grace period.

Early Leave Allowable

Enter the time duration to permit early check-outs within a defined grace period.

The system calculates working hours based on the first check-in record and the last check-out record within the valid check-in and check-out times. Schedule rules do not support cross-day scheduling.

3. View Schedule Results
   After saving a schedule rule, you can see the calendar view to visually inspect the scheduling results across days and weeks.

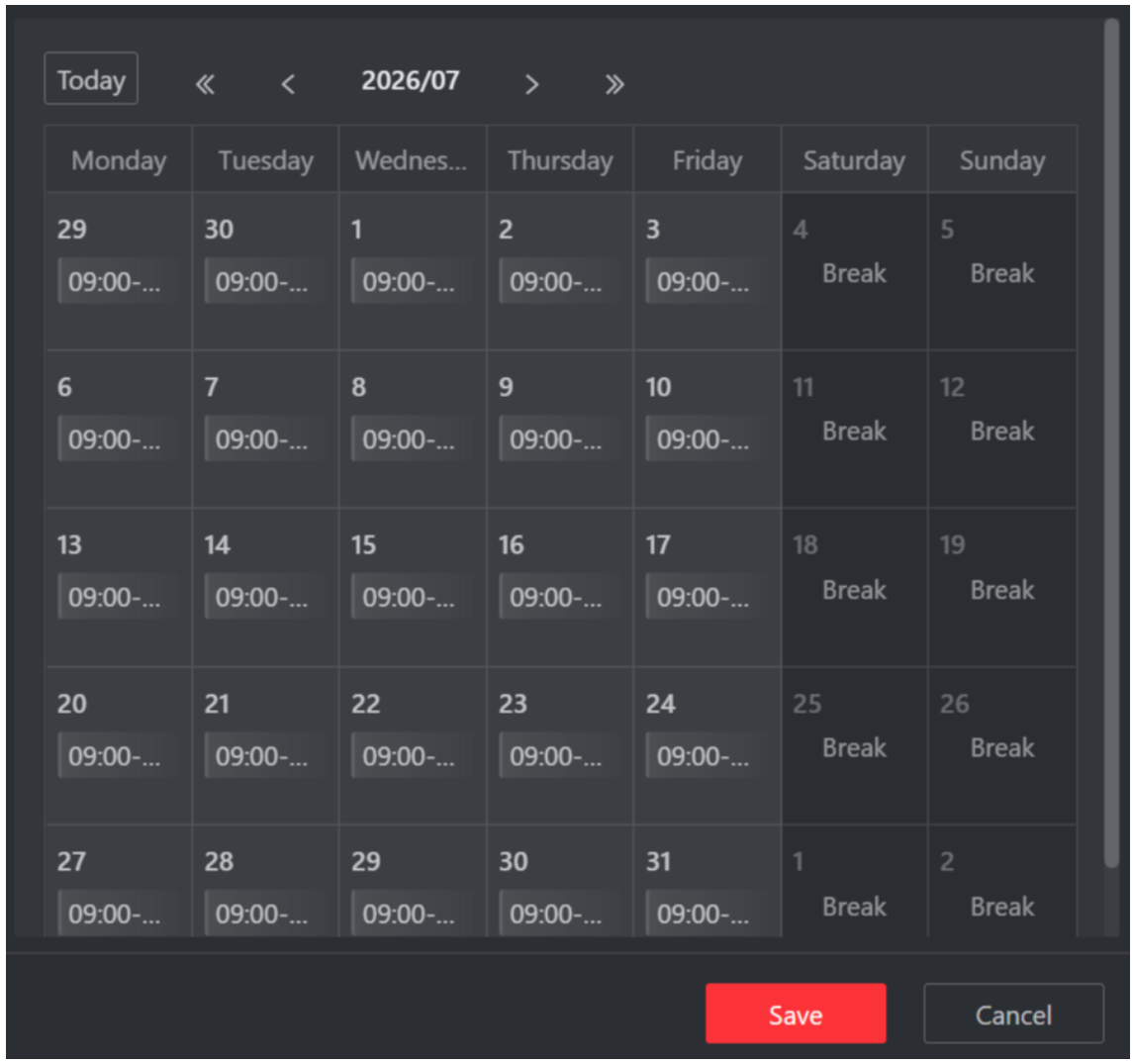


Figure 5-10 Schedule Results

Streamlined Operations of Quick Schedule

You can right-click a department or a person and select **Assign Schedules to Persons in Department** or **Assign Schedules to Person** to quickly make and assign a schedule.

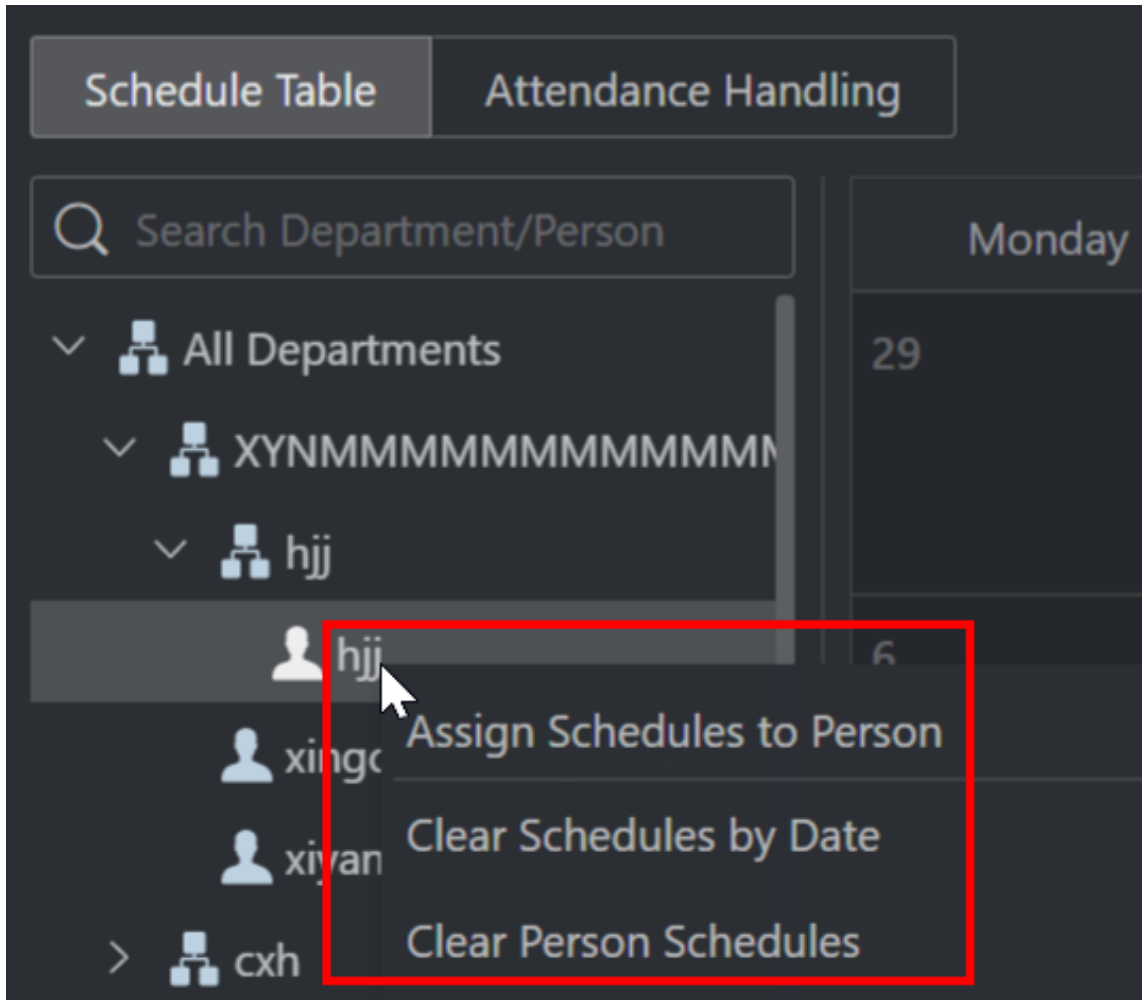


Figure 5-11 Right-Click a Person

Or select a person on the left, press **Ctrl** button on your keyboard and select dates on the calendar, then right-click the dates and select **Schedule**.

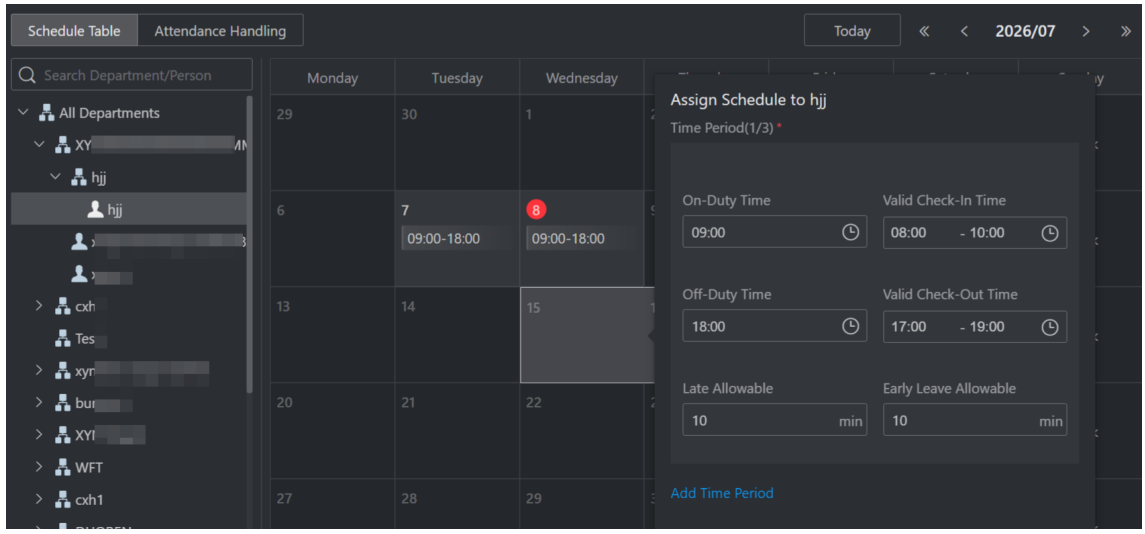


Figure 5-12 Quick Schedule on Calendar

5.3 Apply for a Leave / Business Trip

5.3.1 Add a Leave Type

Configure custom leave categories and their corresponding leave types. You can add, edit, and delete leave type entries as needed.

Click **Add Type** to add a leave type, and the click  to add a sub-type.

For example, you can add a type called "Leave", and then add sub types of leave such as annual leave, sick leave, maternal leave, etc.

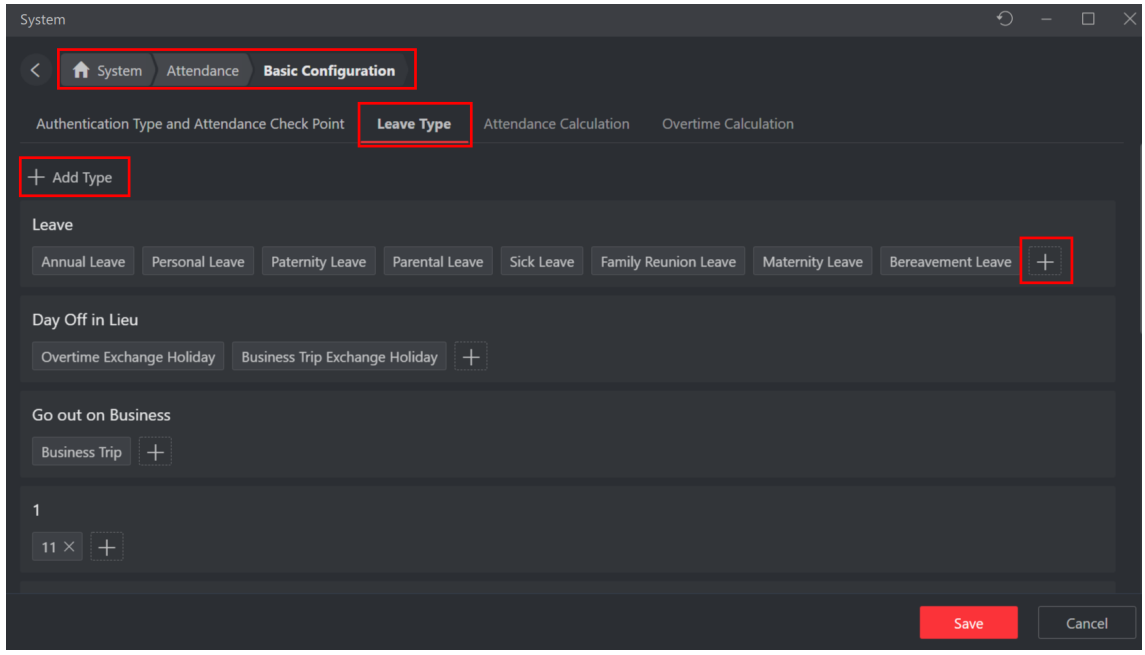


Figure 5-13 Leave Type

5.3.2 Apply for a Leave / Business Trip

Use this feature to record leave or business trip information for employees. This feature allows HR administrators to process leave and business trip records for one or multiple employees, which will then be reflected in the attendance calculation results.

For Multiple Persons

Go to **System → Attendance → Attendance Handling → Leave/Business Trip** .

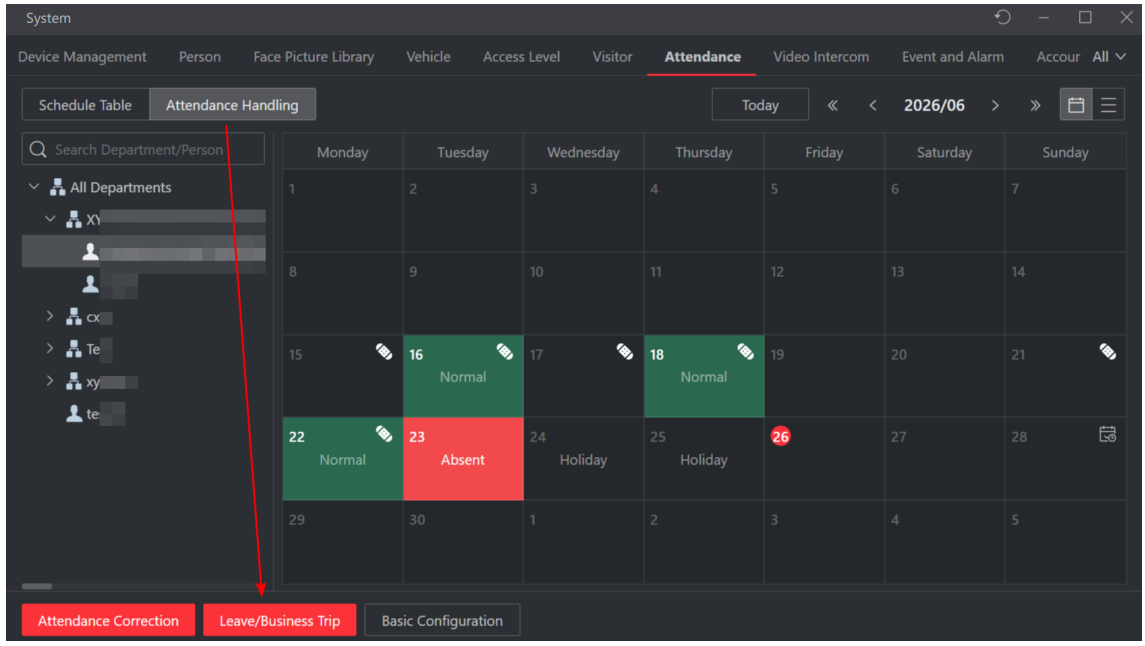


Figure 5-14 Entry of Leave / Business Trip

Select persons or departments on the left list, select date(s) in the middle, select a leave type, a sub-type, time, and enter the remark on the right.

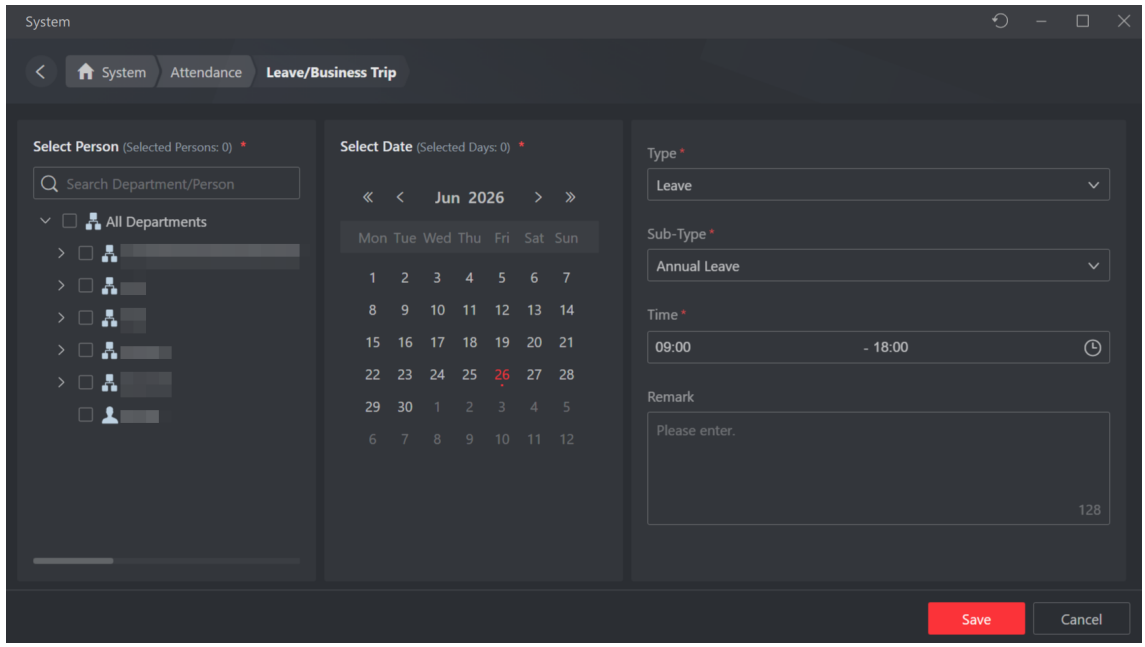


Figure 5-15 Leave/Business Trip

For a Single Person

On the Attendance Handling page (in calendar mode), Select a person in the left list, right-click a date in the calendar, and then select **Leave/Business Trip**.

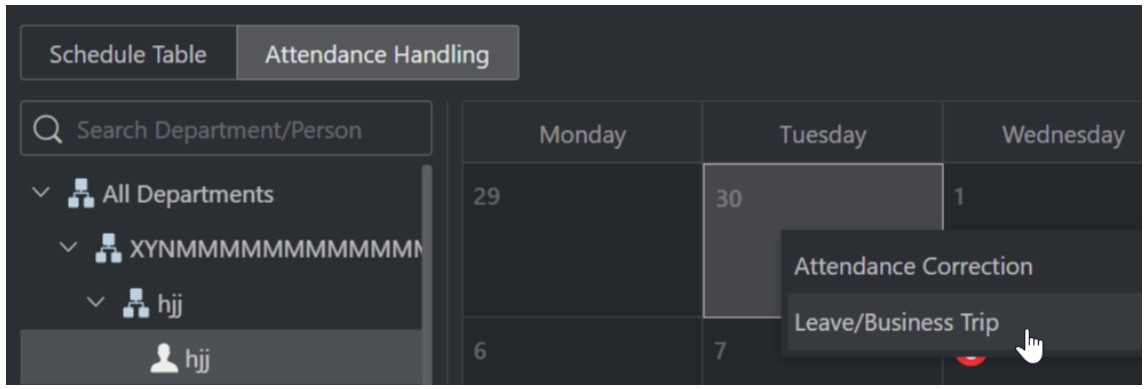


Figure 5-16 Right-Click a Date for Leave/Business Trip

5.4 Check-In/Out Correction

Add make-up check-in or check-out records for employees who missed their scheduled check-in or check-out. This feature allows HR administrators to process corrections for one or multiple employees on specific dates.

For Multiple Persons

1. At the bottom of the Attendance Handling page, click **Attendance Correction**.
2. Select one or multiple employees from the employee list.
3. Select the date(s) for which you want to add the correction record.
4. Choose the check in and/or out type.
5. Select the corresponding time for the selected correction type.
6. (Optional) Enter remarks to provide additional context for the correction.
7. Click **Save** to submit the correction record.

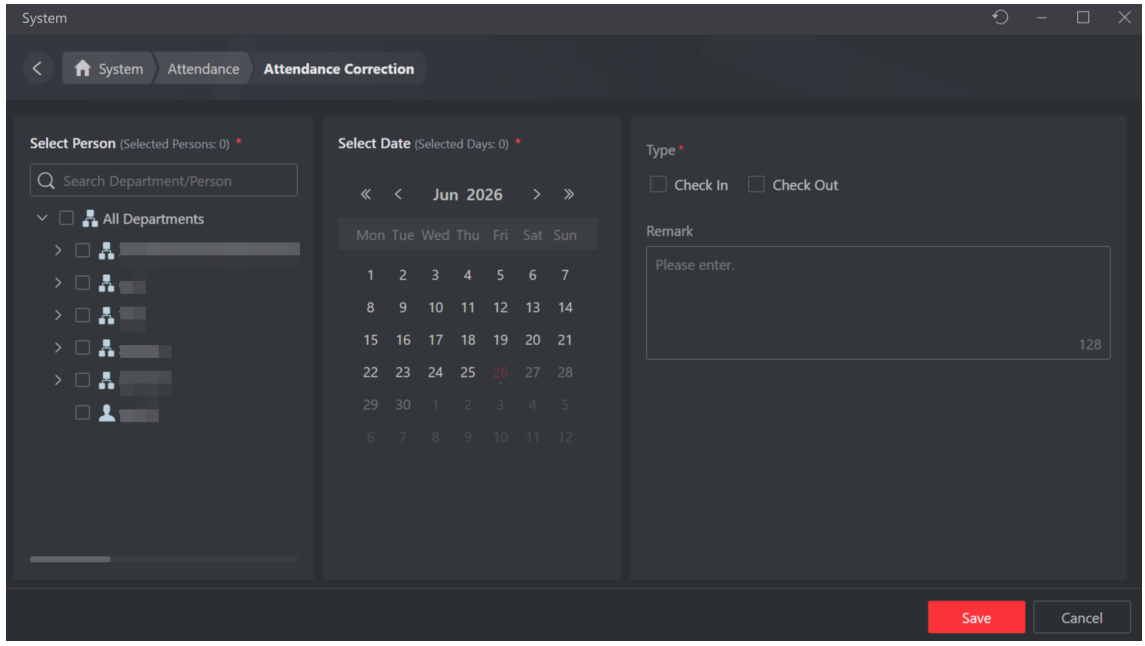


Figure 5-17 Attendance Correction

For a Single Person

On the Attendance Handling page (in calendar mode), select a person in the left list, right-click a date in the calendar, and then select **Attendance Correction** to quickly correct attendance results.

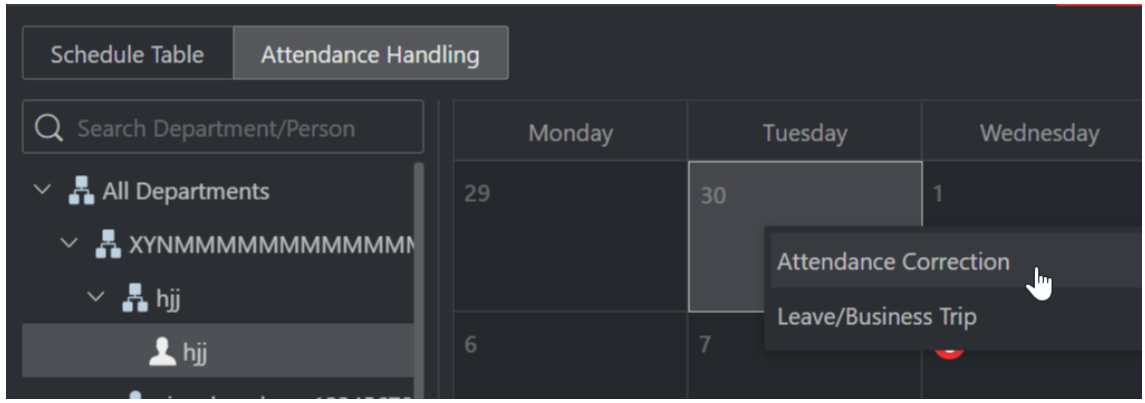


Figure 5-18 Right-Click Date for Correction

5.5 View Attendance Records

Attendance records include transactions and attendance calculation results.

Go to **Search → Attendance Records** .

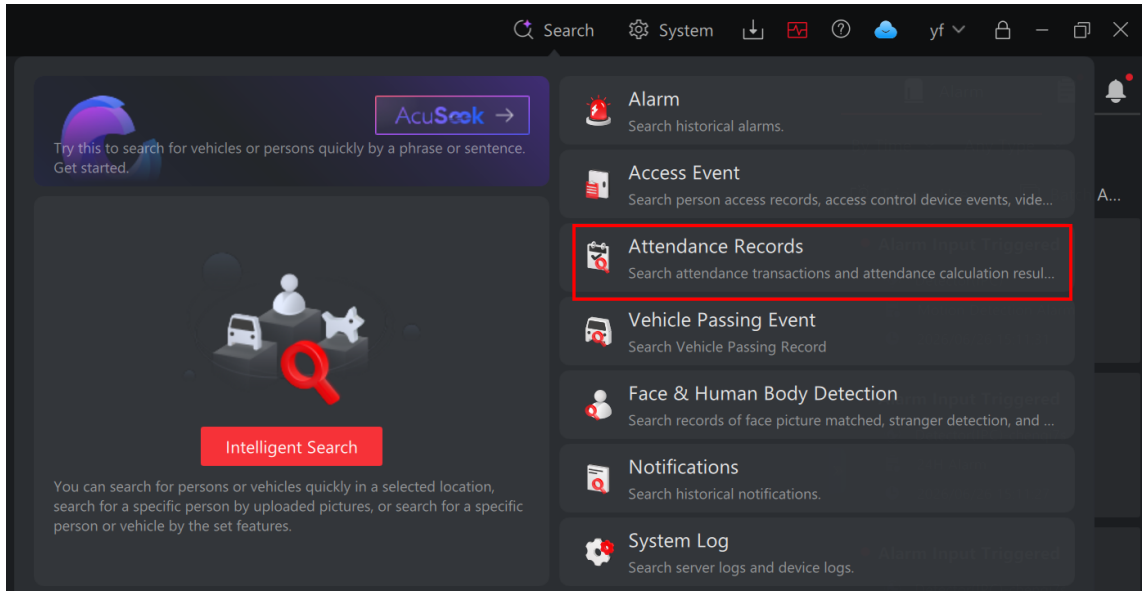


Figure 5-19 Attendance Record Entry

5.5.1 Transaction

Transaction refers to the initial, unaltered source data of employee attendance, typically generated automatically by the system and attendance check points. These records include basic information like authentication times, authentication types, and devices. They serve as the foundation for attendance calculations and payroll processing.

- Filter Conditions
  Filter attendance records by different conditions.

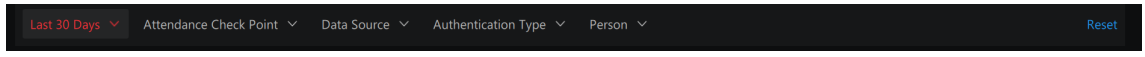


Figure 5-20 Filtering Conditions

- Import Records from Device
  If the platform goes offline for a period, the authentication records saved on the device side during the offline period can be imported into the platform once it comes back online.

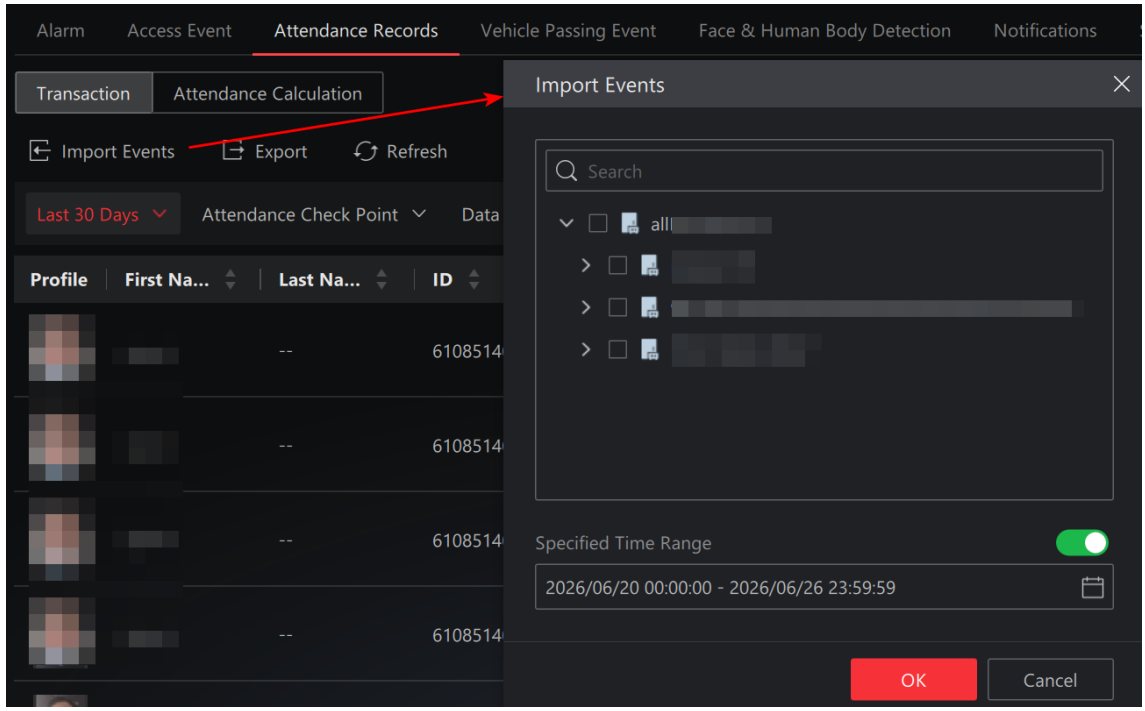


Figure 5-21 Import Records from Device

- Export Records
  The transaction supports exporting data to Excel format. Select the records you wish to export and click **Export** to download the attendance data as an Excel file.

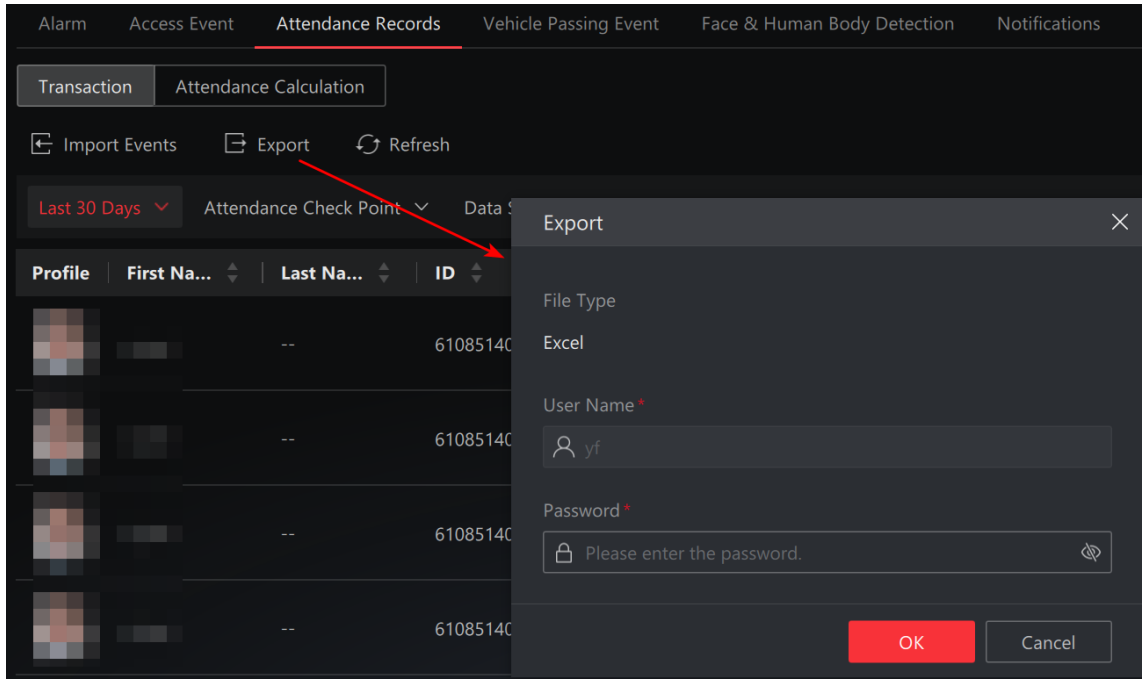


Figure 5-22 Export Records

5.5.2 Attendance Calculation

The Attendance Calculation page displays the daily attendance results, automatically calculated at 1:00 AM every day based on your configured attendance rules and original attendance records. After performing a search or making attendance-related changes, you can manually trigger a recalculation to update the results.

Navigate to **Attendance → Attendance Calculation** to view the calculated attendance results. The page displays the results based on the attendance calculation rules and transactions configured in the system.

- Filtering Attendance Calculation Results
  You can filter the attendance calculation results using the following search fields:



Figure 5-23 Filtering Conditions

- Manual Recalculation
  After performing a search or making changes to attendance records, you can manually trigger a recalculation to update the attendance results. Click **Attendance Calculation** on the Attendance Calculation tab page to recompute the attendance results based on the current search criteria or updated records.

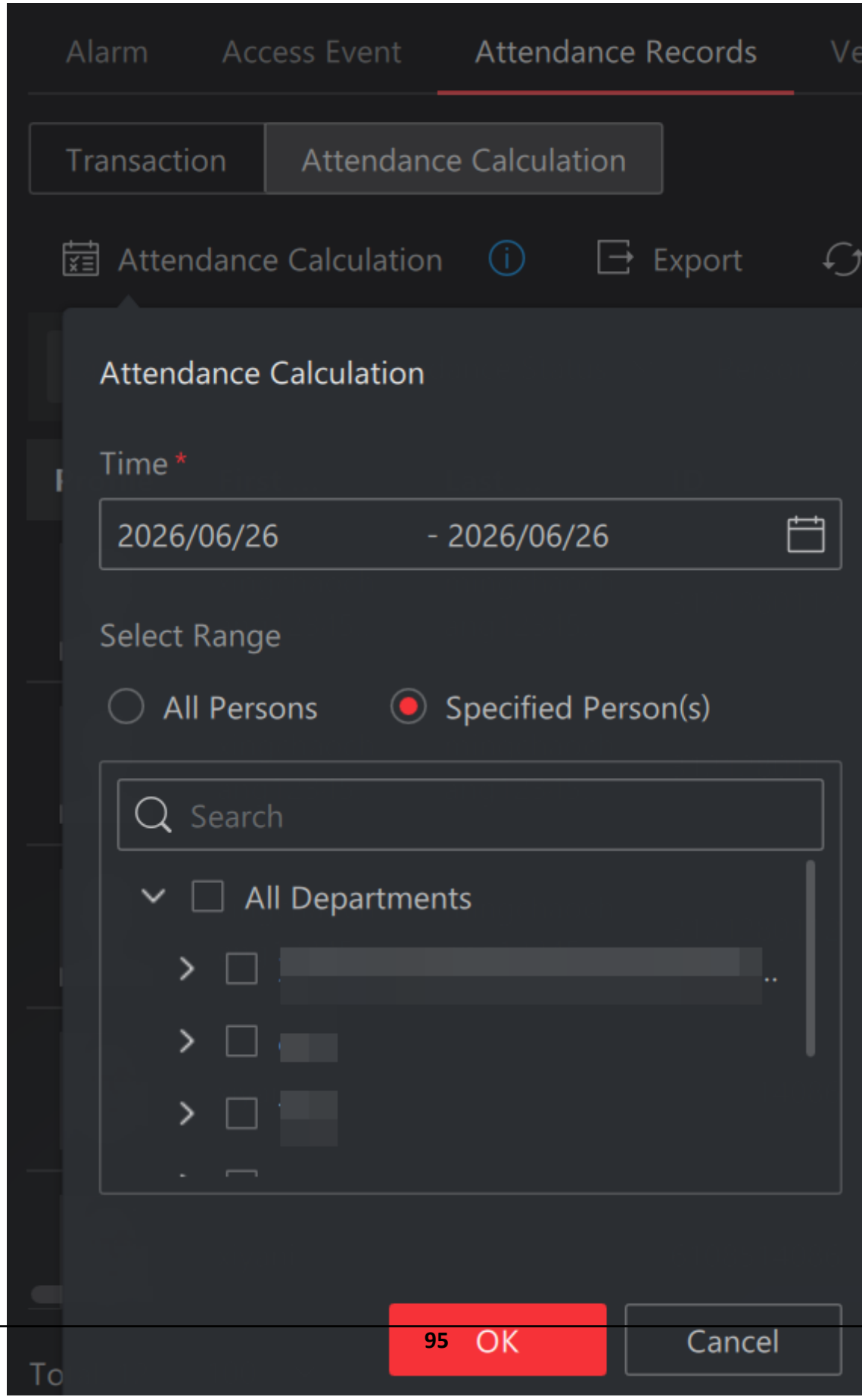


Figure 5-24 Attendance Calculation

- Export Attendance Calculation Results

The attendance calculation results support exporting data to Excel format. Select the records you wish to export and click **Export** to download the attendance calculation data as an Excel file.

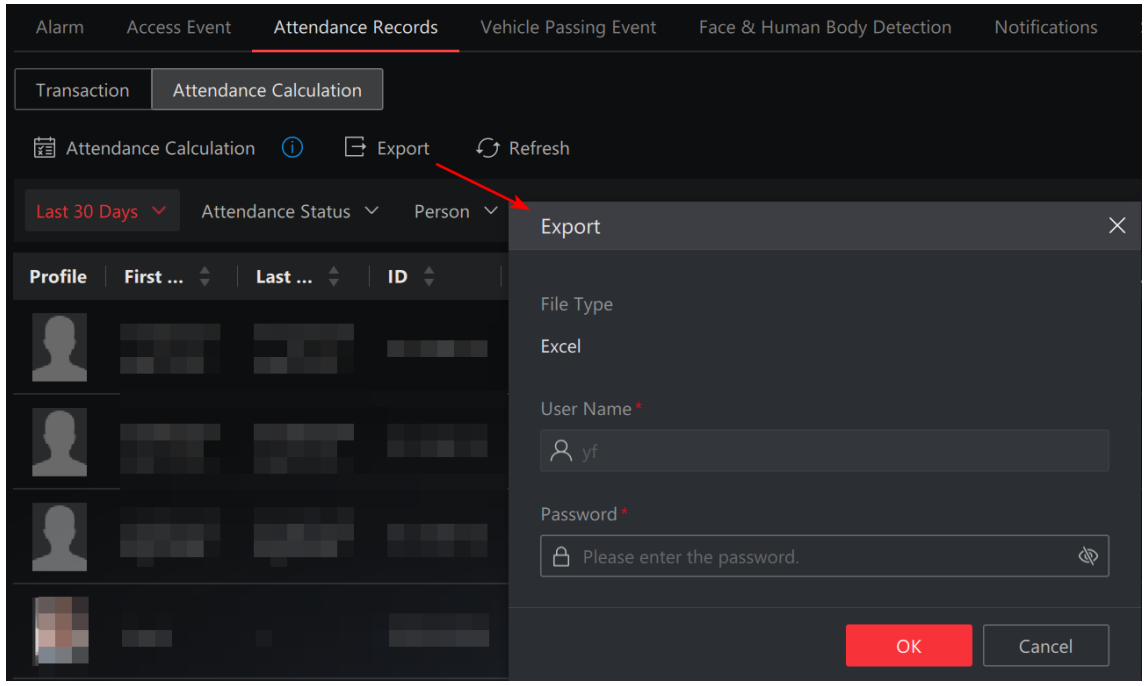


Figure 5-25 Export

Chapter 6 Visitor

The Visitor module provides a comprehensive visitor management system:

- ***Basic Configuration*** : Set up essential rules for visitor management, including visitor groups, access levels, card configurations, and role permissions.
- ***Visitor Reservation and Approval*** : Visitors can reserve via a shared QR code or link, or admins can create reservations on their behalf. Admins review self-service reservation applications.
- ***Visitor Check-In & Check-Out*** : Upon successful reservation, visitors can check in with their credentials to enter. After check-in, administrators can manually check them out.
- ***Visitor List Management*** : Perform actions such as reviewing, checking out, and viewing visitor details on the visitor list.
- ***Statistic Reports & Logs*** : View the details of visitor authentication events and generate statistical reports to check pending applications, today's entries, etc.

6.1 Enable the Visitor Capability

To use the Visitor feature, you must enable both the **Visitor** and **Access Control** service capabilities. Go to **System → System Configuration → Service Capability** . For details, see ***Configure the System Capability*** .

6.2 Basic Configuration

Set up essential rules for visitor management, including visitor groups, access levels, card configurations, and role permissions.

6.2.1 Role and Permission

You can assign module, operation, and visitor group permissions to users based on your needs.

Visitor Group Permission

Select the visitor groups to grant the corresponding permissions to this role.

Module Permission

Accessing the Visitor module requires the **System Configuration → Visitor Management** permission.

Operation Permission

Editing, reviewing, checking out, or deleting visitors on the list requires the **Operation Permission → Visitor Operation** permission.

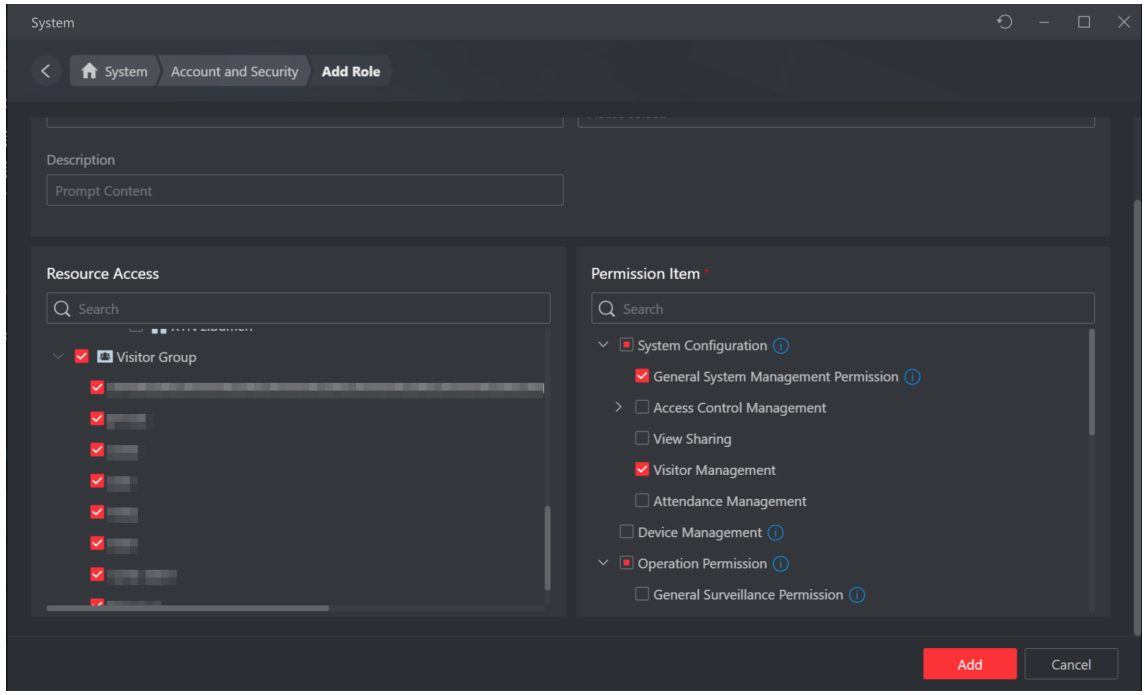


Figure 6-1 Role and Permission

6.2.2 Visitor Group and Access Level Configuration

You can create visitor groups to categorize visitors for easier management. For example, you can create a Business group for business visitors and a Tour group for tour groups. After creating a group, you can assign an access level to it, defining which doors the group members can access and when. Consequently, when adding a new visitor, you can simply select the relevant group to automatically assign the predefined access levels.

System administrators or other roles who have the permission to manage roles can define which users have permission to access the visitor group. See *Role and Permission*.

1. Click **Add Visitor Group** and enter a group name.
2. Right-click an added visitor group and click **Assign Access Level**.
3. Select an access level and click **OK**.

Note

For adding access levels, see ***Add and Assign Access Levels*** .

4. Other Operations:

Clear Access Levels of Visitor Group

It will not affect visitors assigned with access levels.

Set as Default Visitor Group

If self-service reservation is enabled, you can set access level for the default visitor group. Self-service reservation visitors will be automatically added to this group and be assigned with its default permissions.

For self-service reservations, see ***Visitor Reservation and Approval*** .

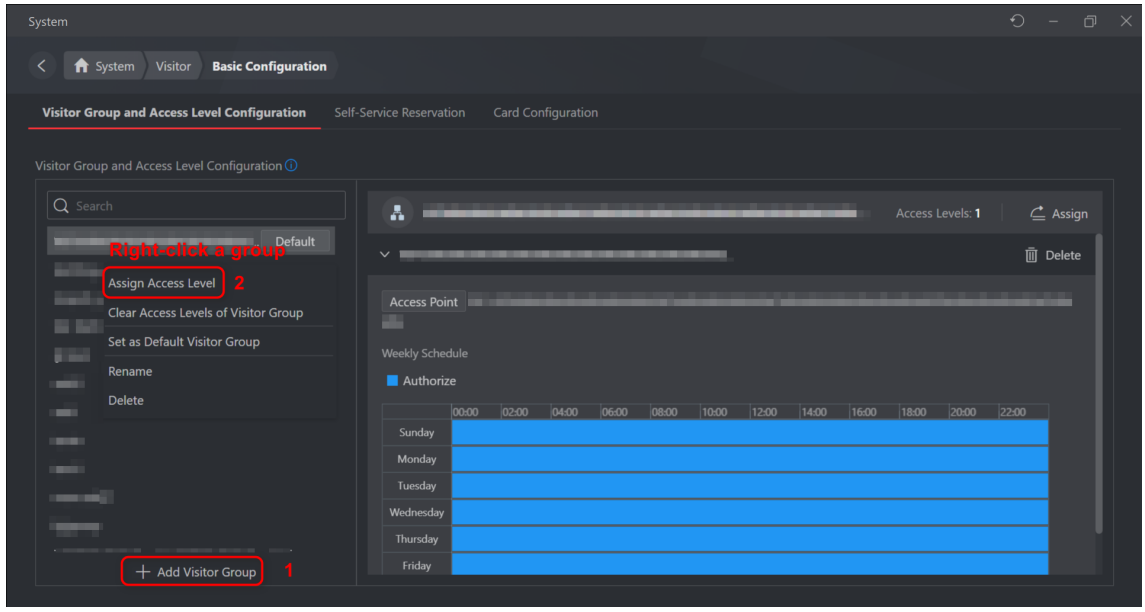


Figure 6-2 Visitor Group and Access Level

6.2.3 Card Configuration

When adding a visitor, you can issue a card to him/her as an access credential. Before issuing a card, you need to set the card issuing mode to get the card number. Except for manually entering the card number, HikCentral Mini Cube also provides three modes for reading the card number: Card Enrollment Station, Card Reader, and Enrollment Station.

Card Enrollment Station

Connect a card enrollment station to the PC on which the client runs. You can place the card on the card enrollment station to get the card No.

Reading Frequency

If your card supports dual frequency (both IC and ID), select **Dual**. If not, select **Single**.

Note

If you select **Dual**, you cannot set card encryption for the card.

Card Encryption

You can enable the card encryption function and select section(s) to be encrypted for security purpose.

Audio Effect

Turn on or turn off the audio when the card number is read successfully.

Card Reader

Select one card reader of one access control device on the platform. You can swipe the card on the card reader to get the card number.

Enrollment Station

You can enroll the card number via the enrollment station and copy back to the platform.

Access Mode

The access mode of the enrollment station. Click **Network** or **USB** from the drop-down list.

Access Protocol / Device Address / Device Port / User Name / Password

Configure the access protocol, IP address, port number, user name, and password for the enrollment station.

RF Card Type

Select the needed card type(s), including EM card, M1 card, etc.

Note

When selecting **M1 Card**, you can switch on **Card Encryption** and select section(s) if needed.

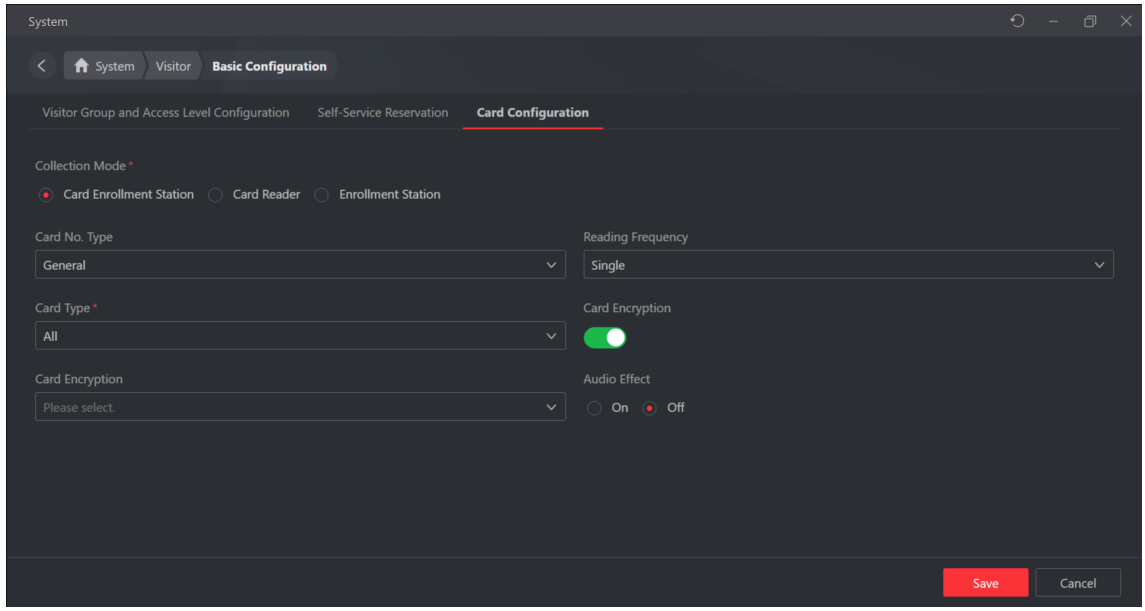


Figure 6-3 Card Configuration

6.3 Visitor Reservation and Approval

After basic configuration, administrators can reserve for visitors or allow self-service reservations with an optional approval flow.

6.3.1 Option 1: Admin Reservation

Administrators can directly create reservations for visitors without requiring approval. Go to **Visitor → Reserve/Import** for single reservation or batch import.

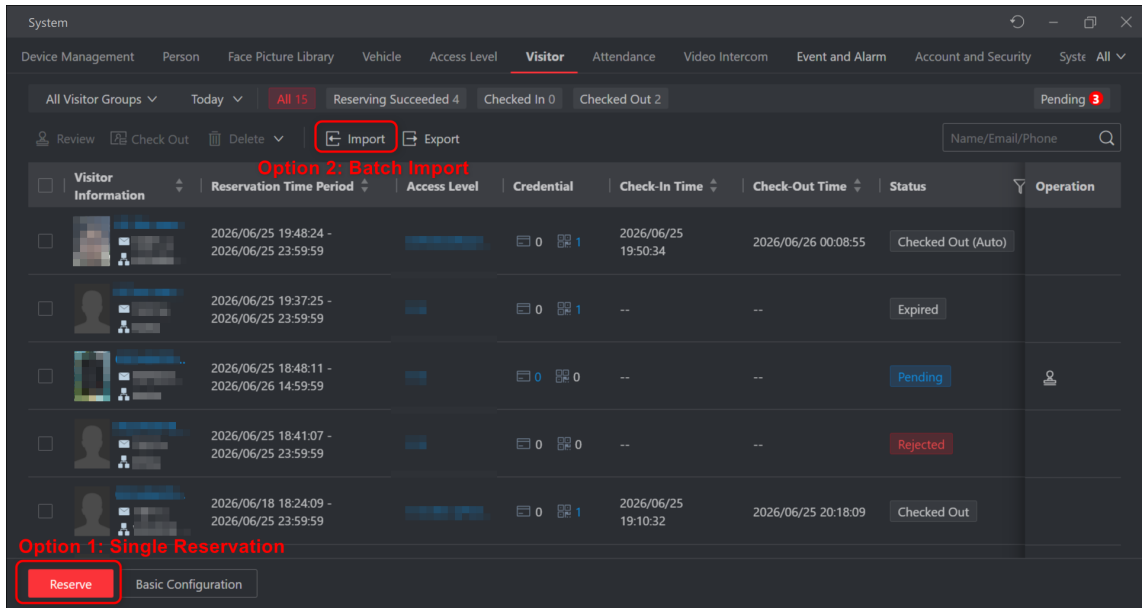


Figure 6-4 Admin Reservation

Take single reservation as an example:

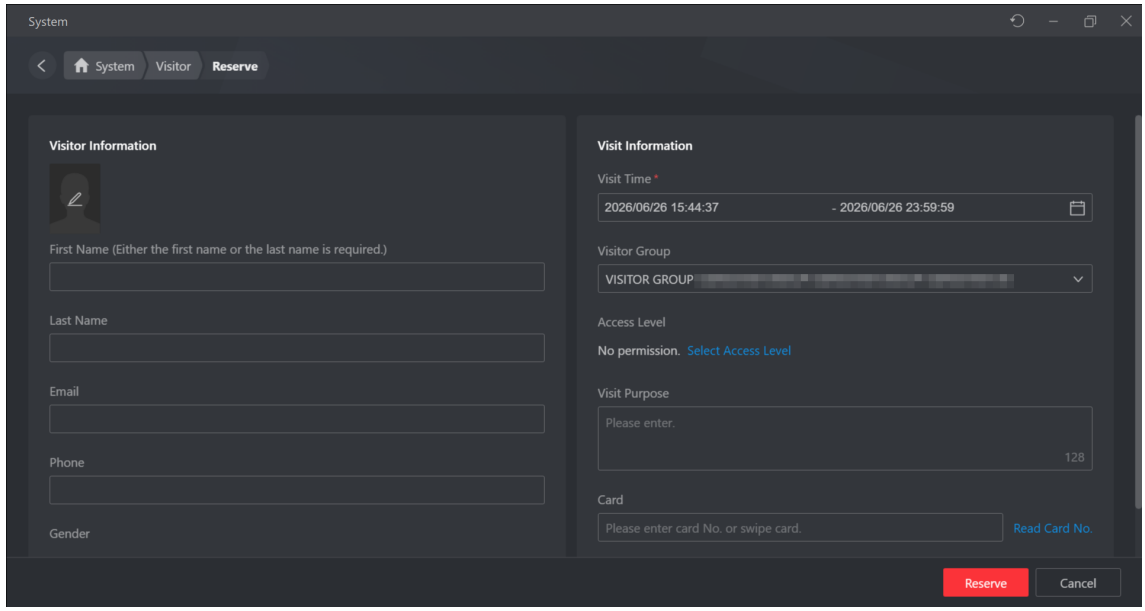


Figure 6-5 Single Reservation

Profile Picture

Hover over the profile picture and click to upload one via From Device (Access Control Device, Video Intercom Device, Enrollment Station), Take a Picture, or Upload Picture.

Visit Time

Checked-in visitors will be automatically checked out once they fail to check out within their reservation period.

Visit Group

Select an existing Visit Group or add a new one. For details, see ***Basic Configuration*** .

Access Level

Select an existing Access Level or add a new one (determines which doors the visitor can access and when). For details, see ***Basic Configuration*** .

Card

Read the card number using the configured Card No. Collection Mode, or enter the card number manually. For card number reading:

- If the card No. collection mode is configured: Place the card according to the selected mode to read the card number.
- If not, go to **Basic Configuration → Card Configuration** to set it up.

6.3.2 Option 2: Visitor Self-Service

HikCentral Mini Cube allows you to generate QR codes or links for visitors to self-reserve and schedule appointments. Visitors are required to provide their name, email address, phone number, gender, purpose of visit, and the start and end times of their visit.

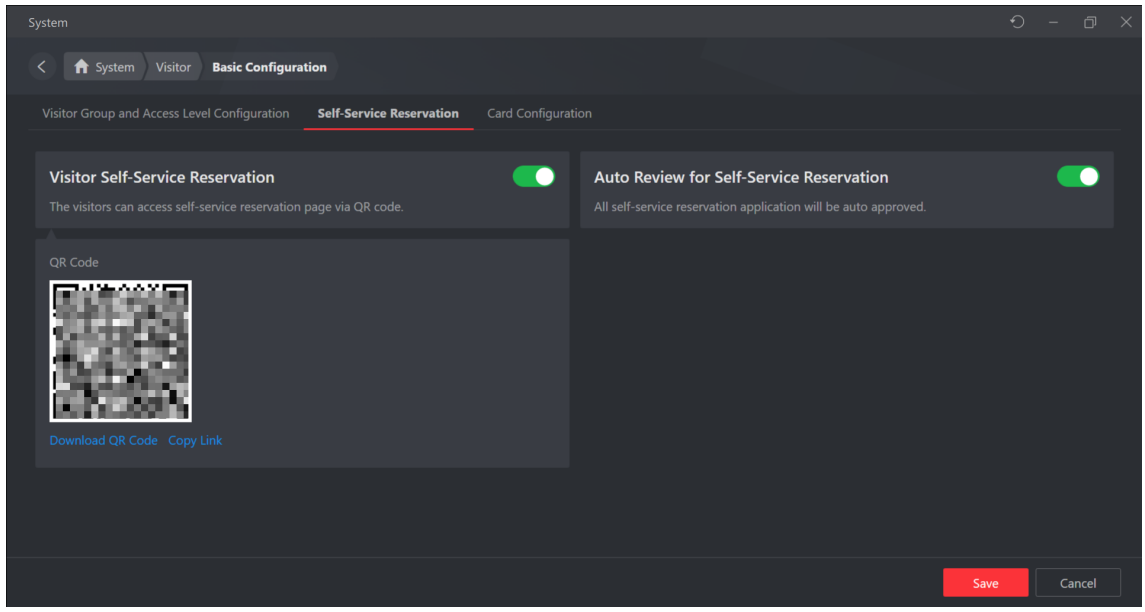


Figure 6-6 Visitor Self-Service

Steps:

1. Go to **Basic Configuration → Self-Service Reservation** and enable **Visitor Self-Service Reservation**.
2. Download/print the QR code for visitors to scan, or copy the reservation link to share with them.
3. Review Applications: After submission, approval depends on your settings.
   - **Auto Review for Self-Service Reservation** Enabled: Applications are approved automatically.
   - **Auto Review for Self-Service Reservation** Disabled: Administrators must manually approve applications on the visitor list page. Select one or more visitors, and click **Review** for batch approval, or click in the Operation column for individual approval.

Note

You need to have the permission (**System Configuration → Visitor Management** and **Operation Permission → Visitor Operation → Review**) before you can review reservations and you can only review visitors in visitor groups you have resource access.

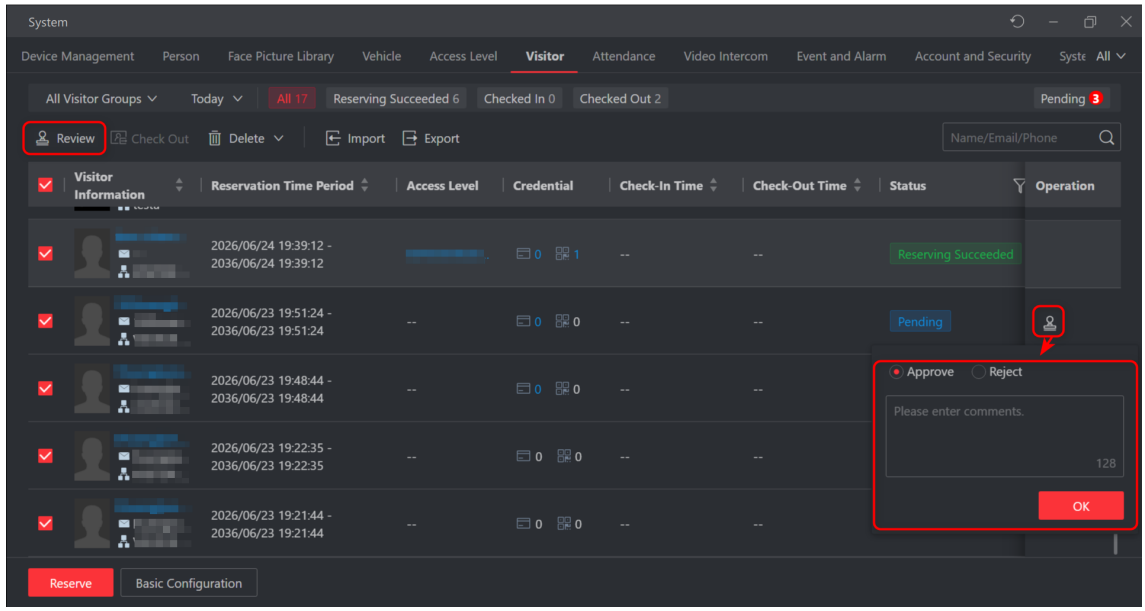


Figure 6-7 Review

6.4 Visitor Check-In & Check-Out

Upon successful reservation, visitors can check in with their credentials to enter. After check-in, administrators can manually check them out.

Check-In

Visitors are automatically checked in when they use a credential (e.g., swiping a card, face recognition, or QR code) to access a door.

Check-Out

Once checked out, visitors will no longer have access level permissions.

- **Checked Out (Manual)**: Administrators can manually check out visitors from the client. Select the checked-in visitor(s) and click **Check Out**, or click in the Operation column for a specific visitor.
- **Checked Out (Auto)**: If a checked-in visitor fails to check out within their reservation period, the system will automatically check them out upon expiry.

For more visitor status information, see ***Visitor List Management*** .

6.5 Visitor List Management

You can perform the following operations on the visitor list.

Review

Select one or more pending approvals, and click **Review** for batch approval, or click in the Operation column for individual approval.

Check Out

Select the checked-in visitor(s) and click **Check Out**, or click in the Operation column for a specific visitor.

Import / Export

Import multiple visitors at once or export all/selected visitors.

View Visitor / Access Level Details

Click a visitor name or access level name to view its details.

Add or View Credential

Click a credential to add or view details.

Status

Table 6-1 Status

Status	Description
Pending	Self-service visitors require approval. (Available when Auto Review for Self-Service Reservation is disabled)
Rejected	Self-service visitors rejected by admins. (Available when Auto Review for Self-Service Reservation is disabled)
Reserving Succeeded	• Visitors reserved by admins. • Self-service visitors approved by admins. (Available when Auto Review for Self-Service Reservation is disabled) • Self-service visitors. (Available when Auto Review for Self-Service Reservation is enabled)
Checked In	Visitors who have checked in and are still within their reservation period.
Checked Out	Visitors who have been manually checked out by admins.
Checked Out (Auto)	Checked-in visitors who did not check out within their reservation period. The client will automatically check them out upon expiry.
Expired	• Visitors who did not check in within their reservation period. • Visitors whose approval was not completed within their reservation period.

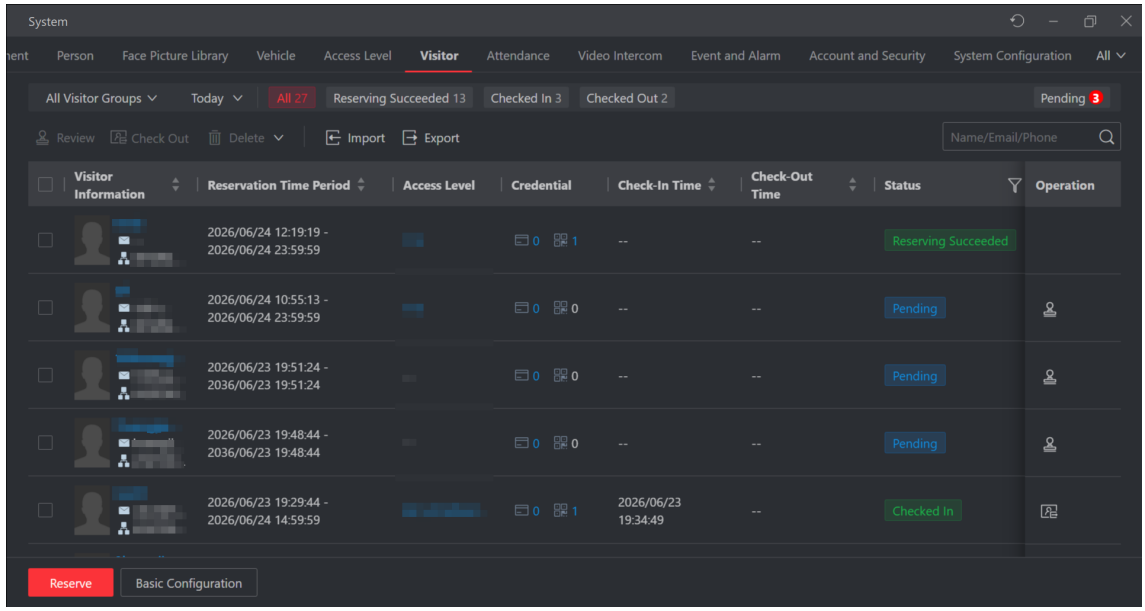


Figure 6-8 Visitor List

6.6 Statistic Reports & Logs

You can view the details of visitor authentication events, including profile, name, ID, authentication result, etc. Additionally, you can generate statistical reports to check pending applications, today's entries, etc.

Statistic Reports

For generating visitor statistics and reports, see ***Generate and Display Maintenance Report*** .

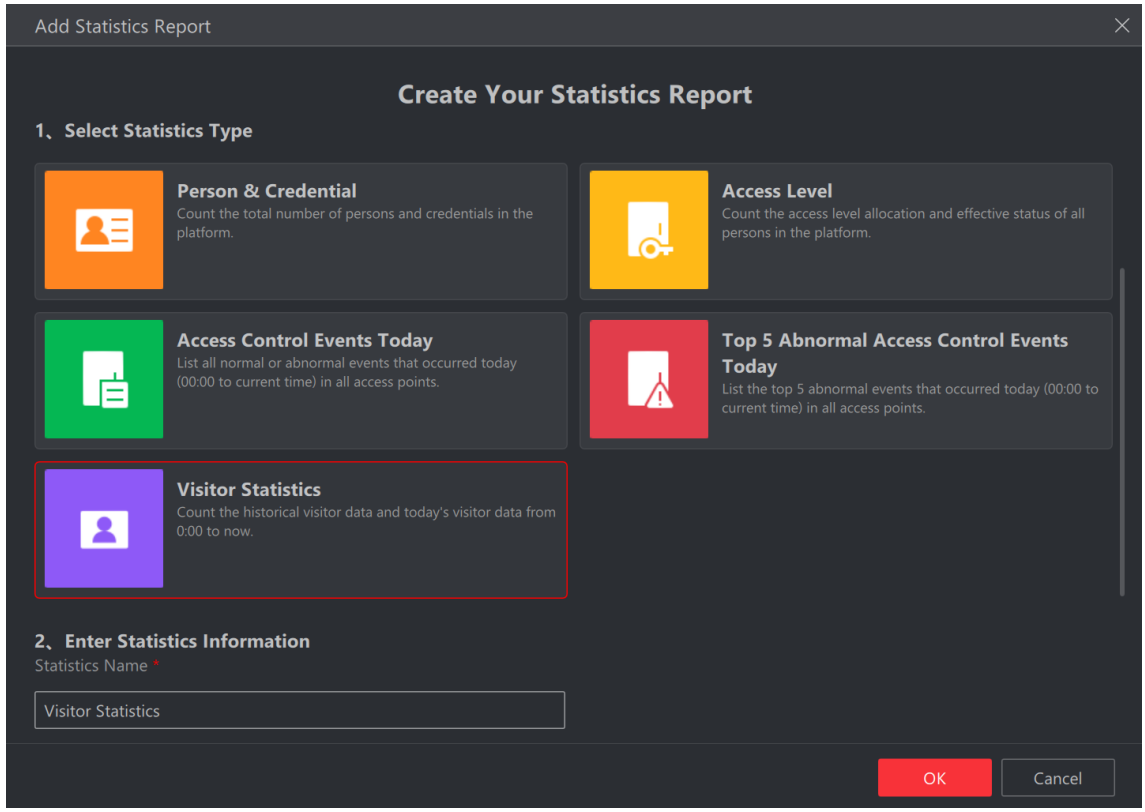


Figure 6-9 Visitor Statistics

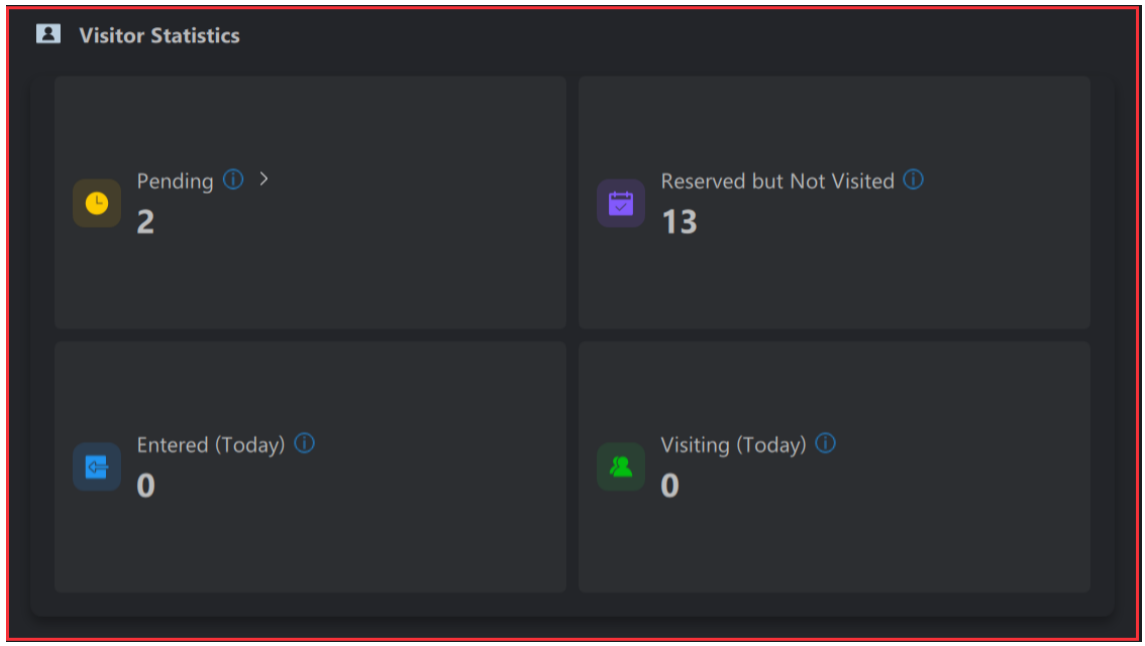


Figure 6-10 Details

Visitor Authentication Events

Go to **Search → Access Event → Person Authentication Event** and select the type as **Visitor**. For details, see ***Search for Access Events*** .

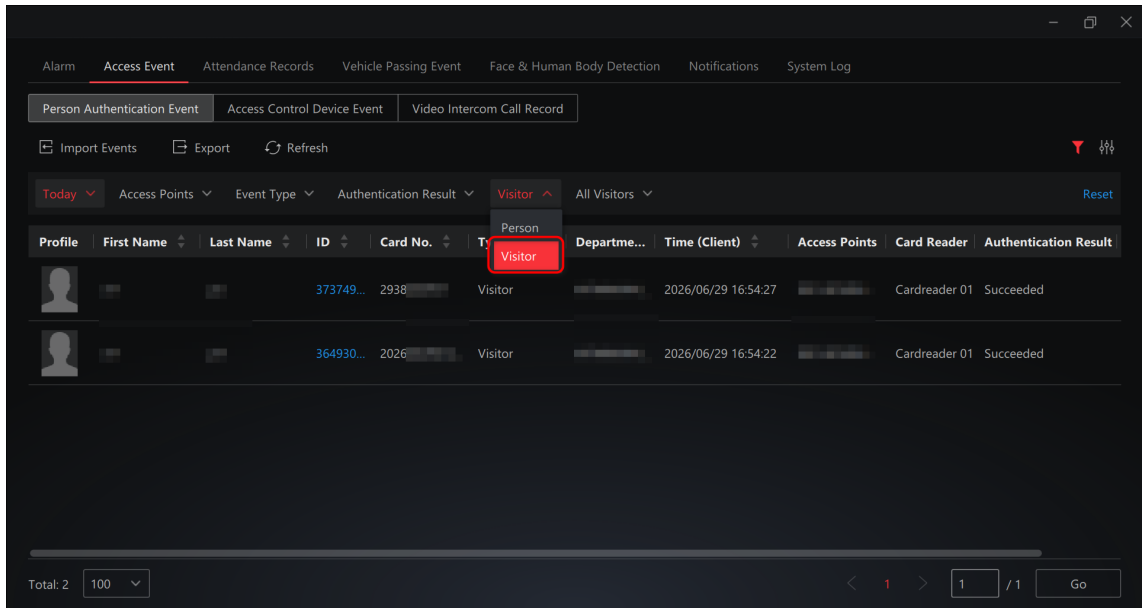


Figure 6-11 Visitor Authentication Events

Chapter 7 Alarm Detection

A security control device detects persons, vehicles, or other emergency events in the detection region, and reports event/alarm information (such as location) to the security personnel. In this module, you can add security control panels with partition (areas), zones, and peripherals to form a complete alarm detection system. Here are key definitions:

- **Partition (Area)**: An independent logical partition that groups multiple zones and peripherals for centralized management. It allows specific areas to be armed, disarmed, or alarmed independently without affecting the rest of the system.
- **Zone**: The basic unit of an alarm detection system. It typically corresponds to the coverage area of a single zone detector.
- **Peripheral**: Sounders and relays.

The module provides the following key features:

- Add security control panels, partitions (areas), zones, and peripherals. See ***Add Security Control Devices*** .
- Monitor security control panels on the main panel. See ***Monitoring of Security Control Devices*** .
- Subscribe to alarm detection events and add alarms. See ***Event and Alarm*** .
- Generate statistical reports for security control panels. See ***Display Security Control Panel Statistics*** .

7.1 Enable the Alarm Detection Capability

You must enable the **Alarm Detection** service capability before you can use this feature.

Go to **System → System Configuration → Service Capability** . For details, see ***Configure the System Capability*** .

7.2 Add Security Control Devices

To add security control panels, go to **System → Device Management → Alarm Detection → Add Device / Add Now** .

Note

You can only add security control panels via Hikvision OTAP Protocol.

After adding devices, right-click the security control panel to add partitions (areas), zones, and peripherals. You can also right-click a partition (area) to add zones and peripherals.

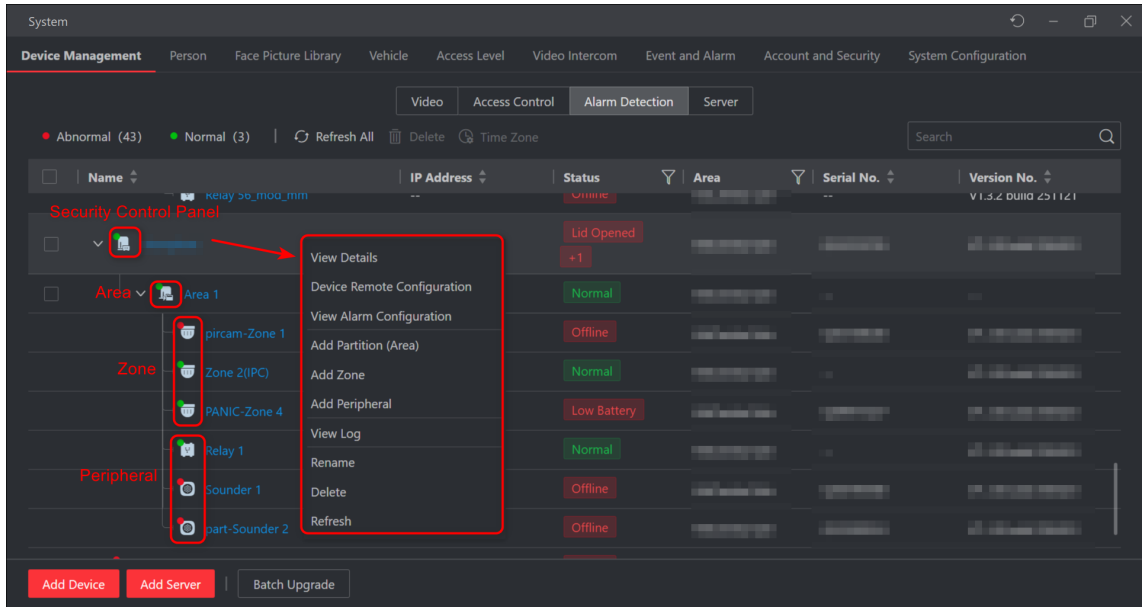


Figure 7-1 Alarm Detection

You can also right-click or click a security control panel / partition(area) / zone / peripheral to view details, configure device remotely, etc.

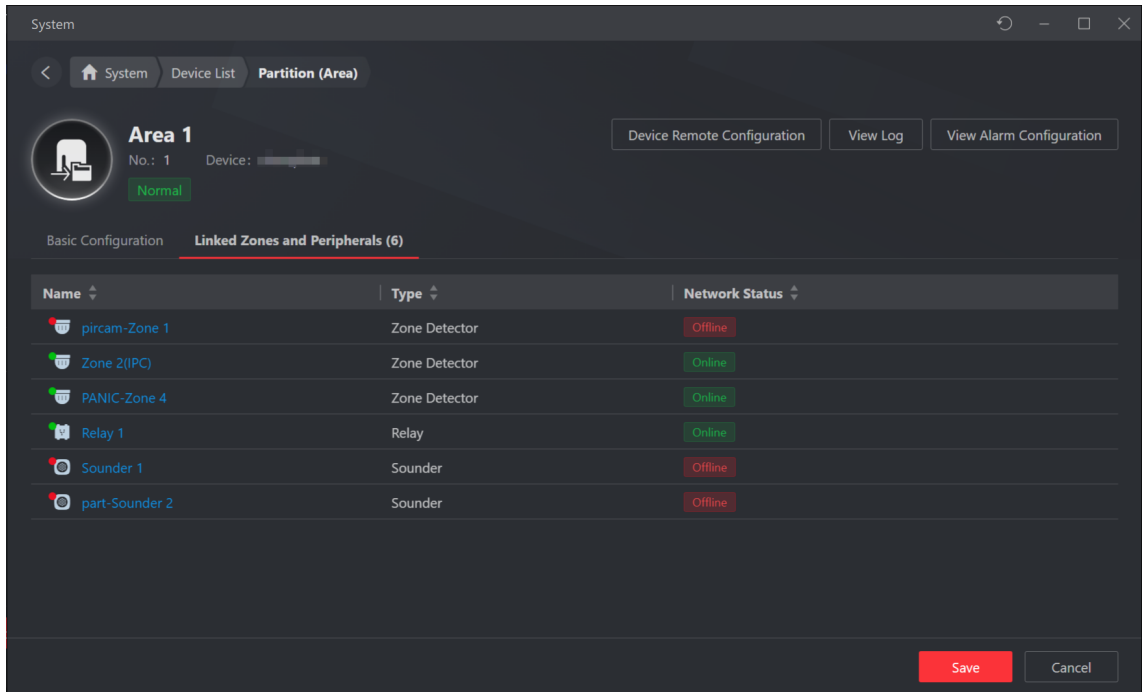


Figure 7-2 Details

7.3 Monitoring of Security Control Devices

Security control panels, partitions (areas), and zones can be added to the viewing grid for monitoring.

- Monitoring of Security Control Panel
  Double-click a security control panel, or drag a security control panel to the viewing grid to display all partitions (areas).

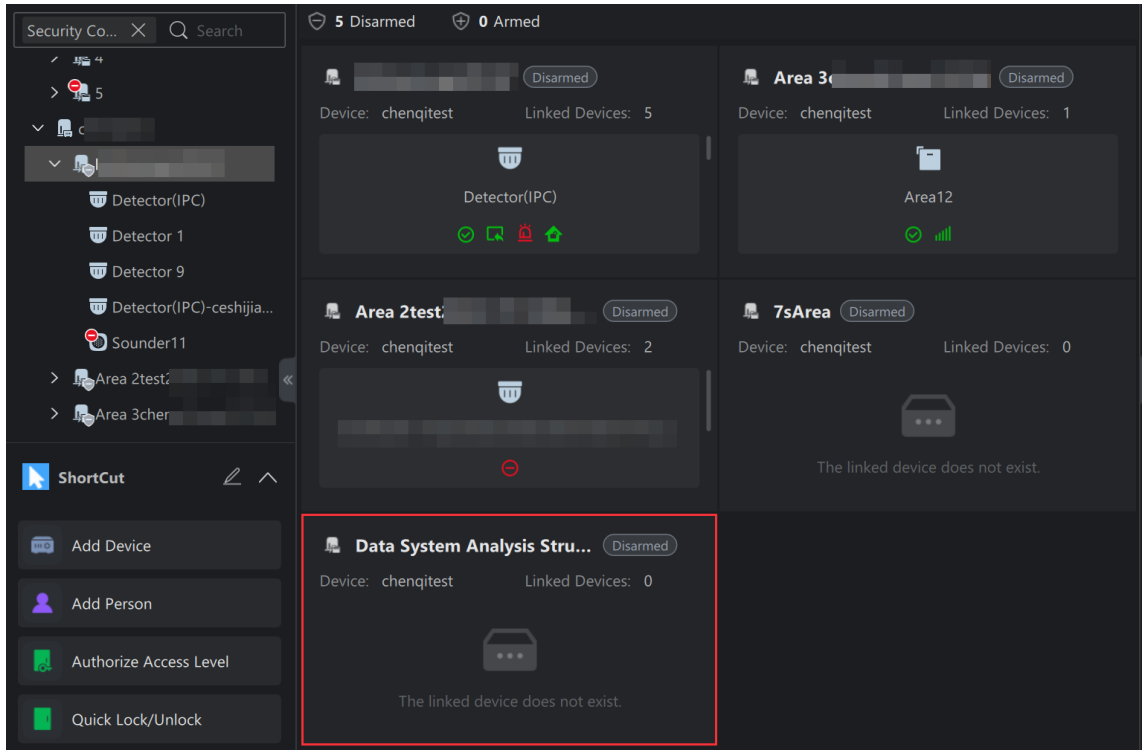


Figure 7-3 Monitoring of Security Control Panel

- Monitoring of Partition (Area)
  Click **Linked Devices** to show peripherals.

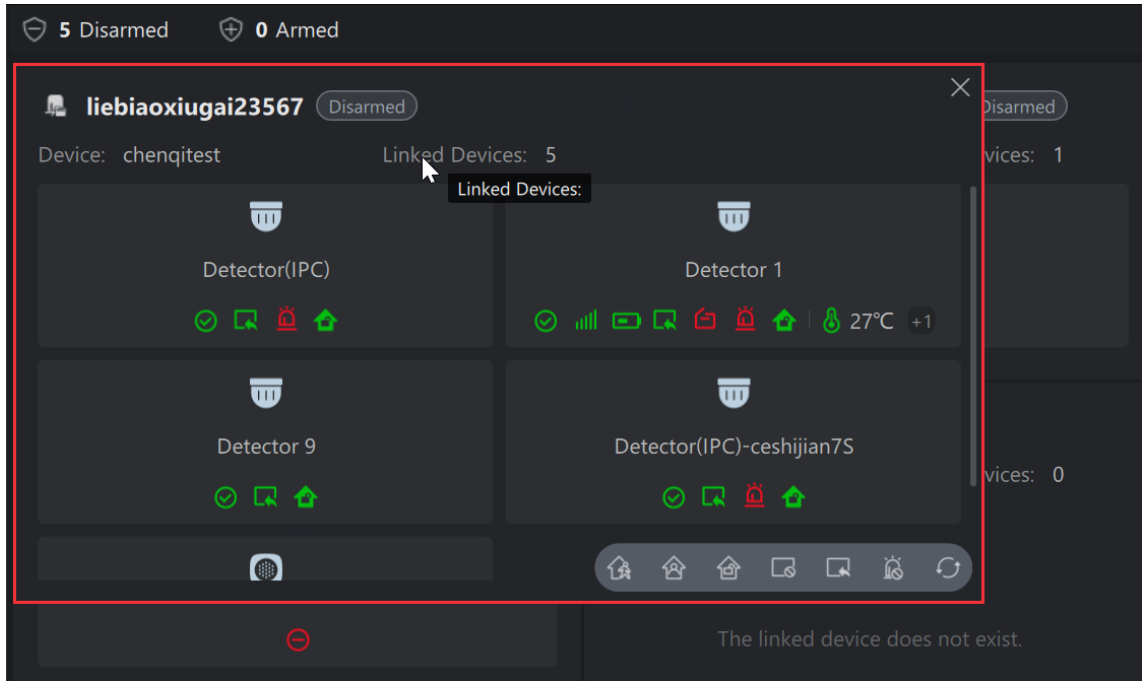


Figure 7-4 Linked Devices

You can double-click a partition (area), or drag one to the viewing grid to display the partition (area).

Zones and peripherals under partitions (areas) will also be displayed.

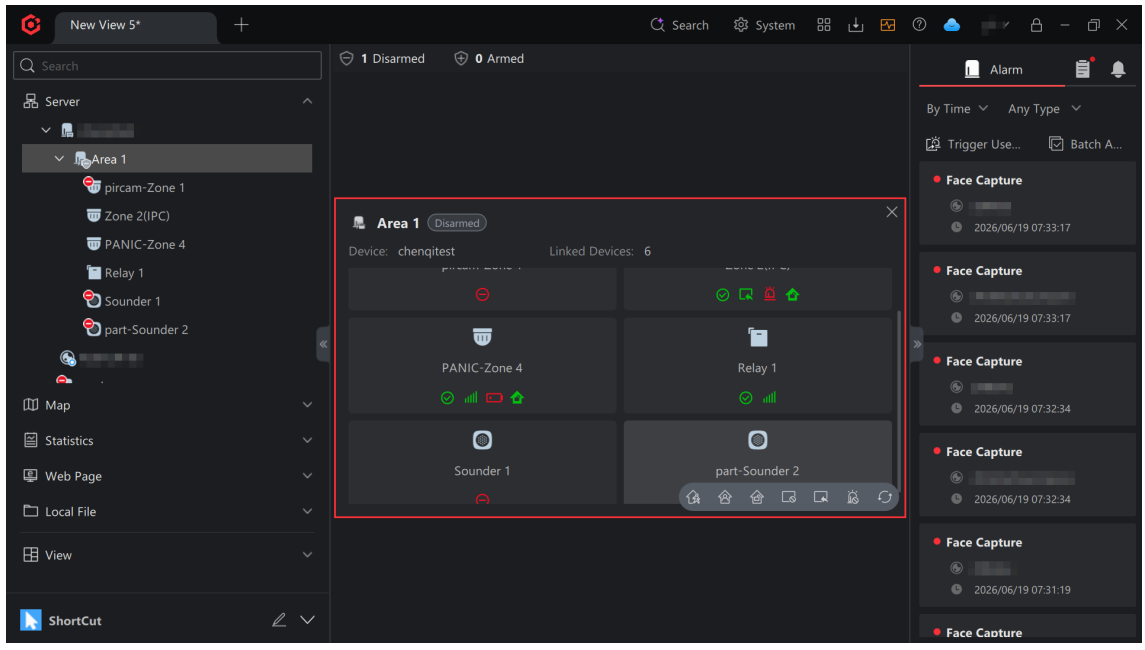


Figure 7-5 Monitoring of Partition (Area)

- More Operations

You can right-click a security control panel, a partition (area), a peripheral to perform more operations such as arming/disarming.

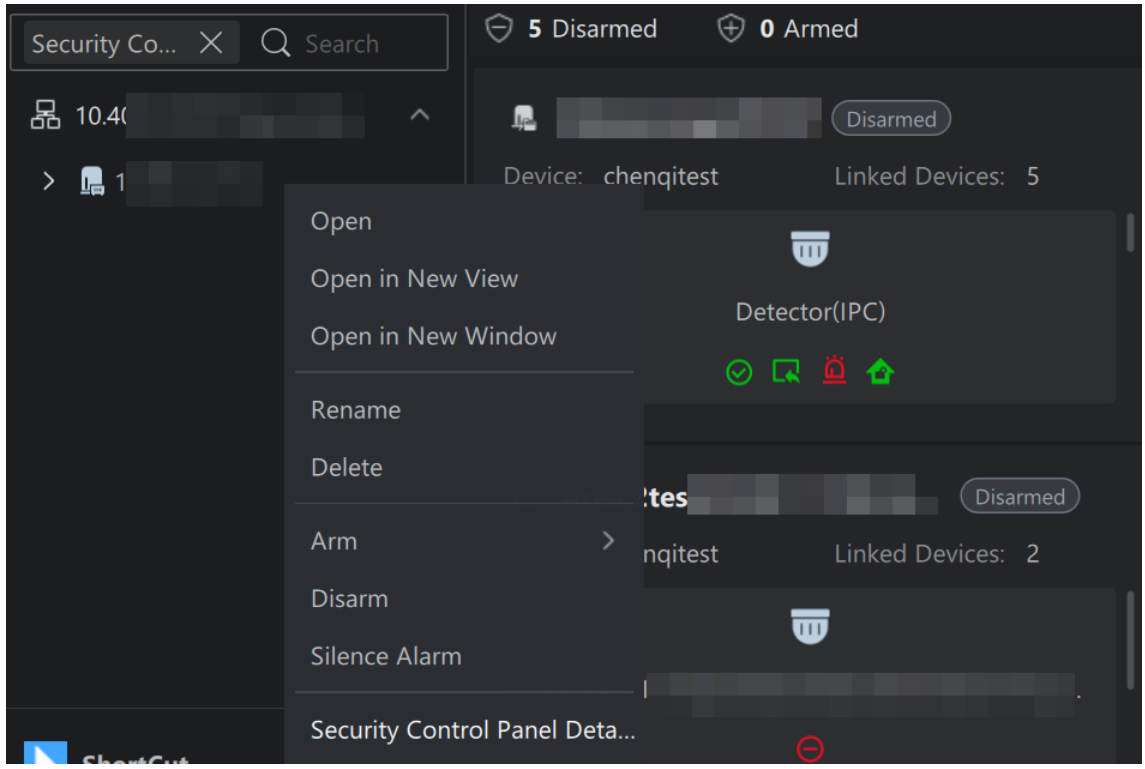


Figure 7-6 Right-Click a Device

- Move Device
  Drag a security control panel to other areas. When you move a security control panel, the partitions (areas), zones, and peripherals will also be moved.

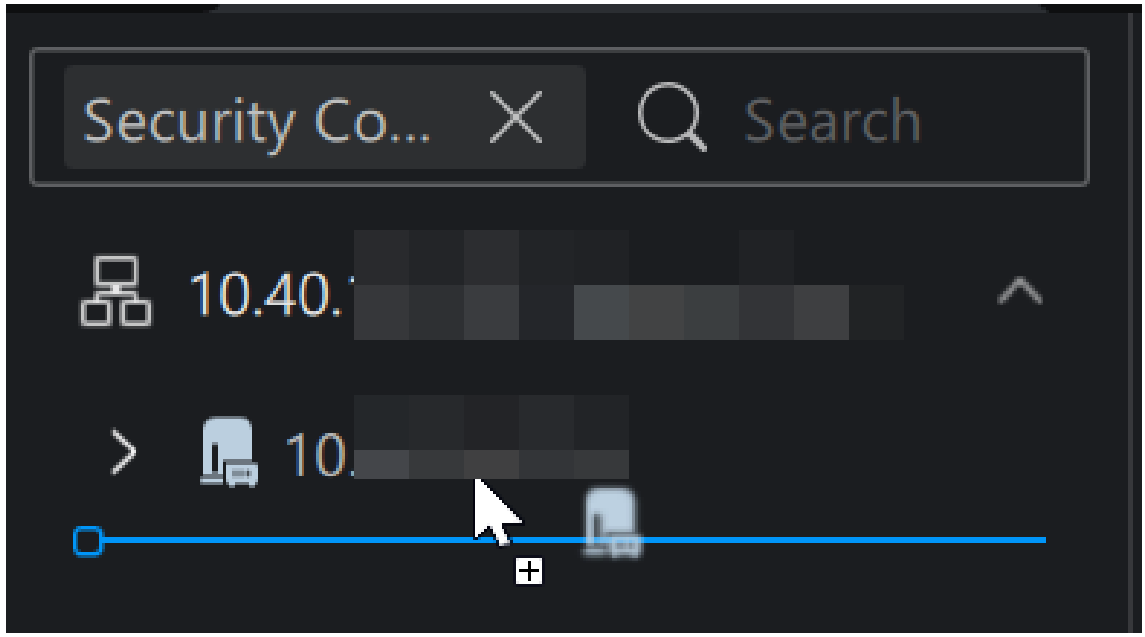


Figure 7-7 Move Device to Another Area

7.4 Event and Alarm

For alarm detection, you can subscribe to events and configure alarms for Alarm Inputs, Partitions (Areas), and Peripherals, as well as maintenance alarms for security control panels. For details on subscribing to events and configuring alarms, see ***Event Subscription*** and ***Add an Alarm*** .

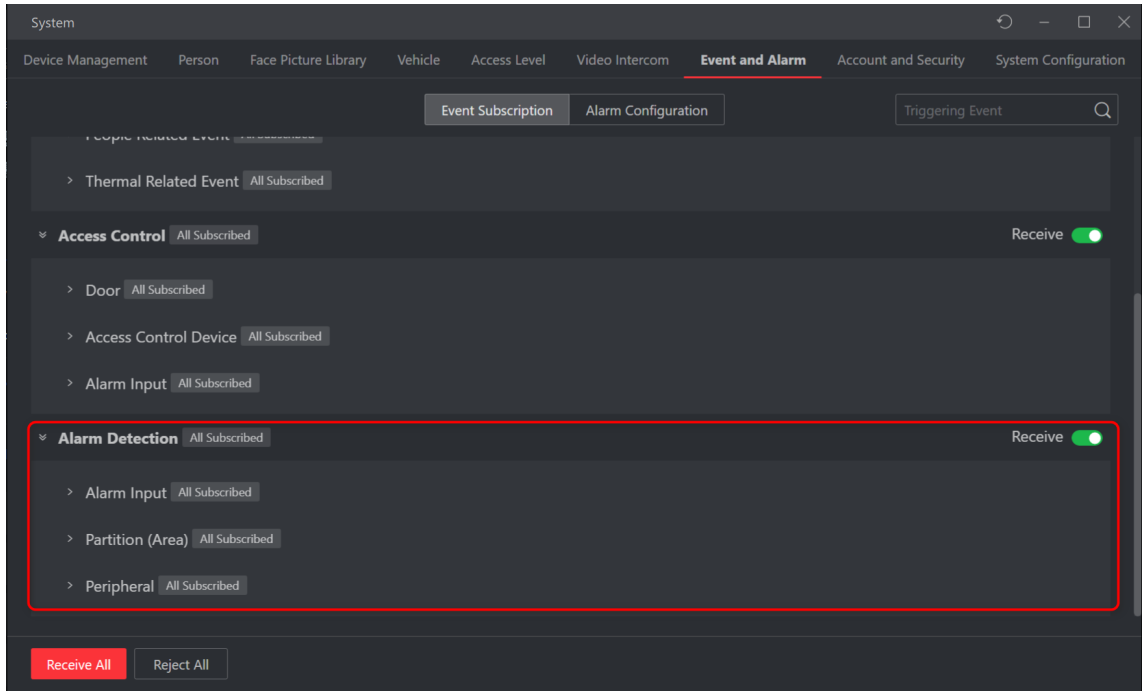


Figure 7-8 Event and Alarm

7.5 Role and Permission

You can configure users with permissions for device management, general surveillance, and resource access (e.g., viewing resources or performing operations on them). Based on their assigned role, the user can access the corresponding alarm detection service. See ***Add a Role*** for details.

7.6 Display Security Control Panel Statistics

You can generate and view statistical reports of security control panels. See ***Generate and Display Maintenance Report*** for details.

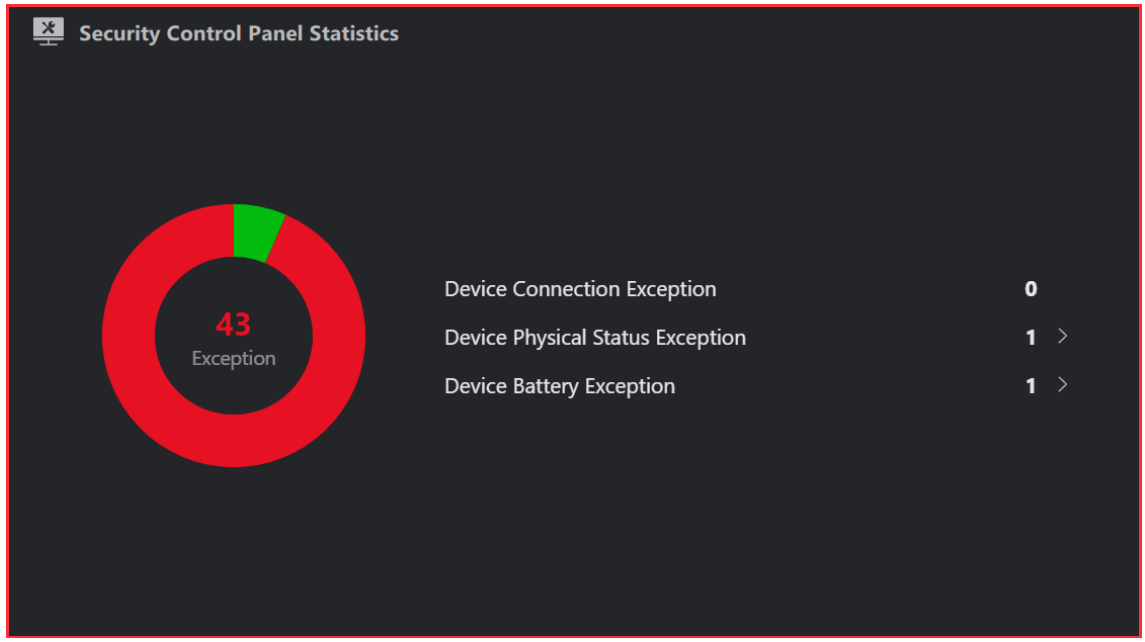


Figure 7-9 Security Control Panel Statistics

Chapter 8 Server Cascading

8.1 Introduction

Server cascading is a management model that allows a central server to incorporate independent servers as subordinate nodes (referred to as cascaded servers), creating a logically unified and centrally managed system. Admins can log in to the central server to manage all cascaded servers and import their associated resources.

Central Server

The server that admins log into directly.

Cascaded Server

Servers added to the central server. Resources (cameras and devices) managed by these cascaded servers will be synchronized to the central server.

For example, If an administrator logs into the system via **10.xx.xx.20** and adds a cascaded server **10.xx.xx.30**, then:

- **10.xx.xx.20** becomes the central server.
- **10.xx.xx.30** is the cascaded server.
  Resources (cameras and devices) under **10.xx.xx.30** can be imported to **10.xx.xx.20** (i.e., the currently logged-in system).

8.2 Add a Cascaded Server

To add a cascaded server, go to **System → System Configuration → Add Cascaded Server** .

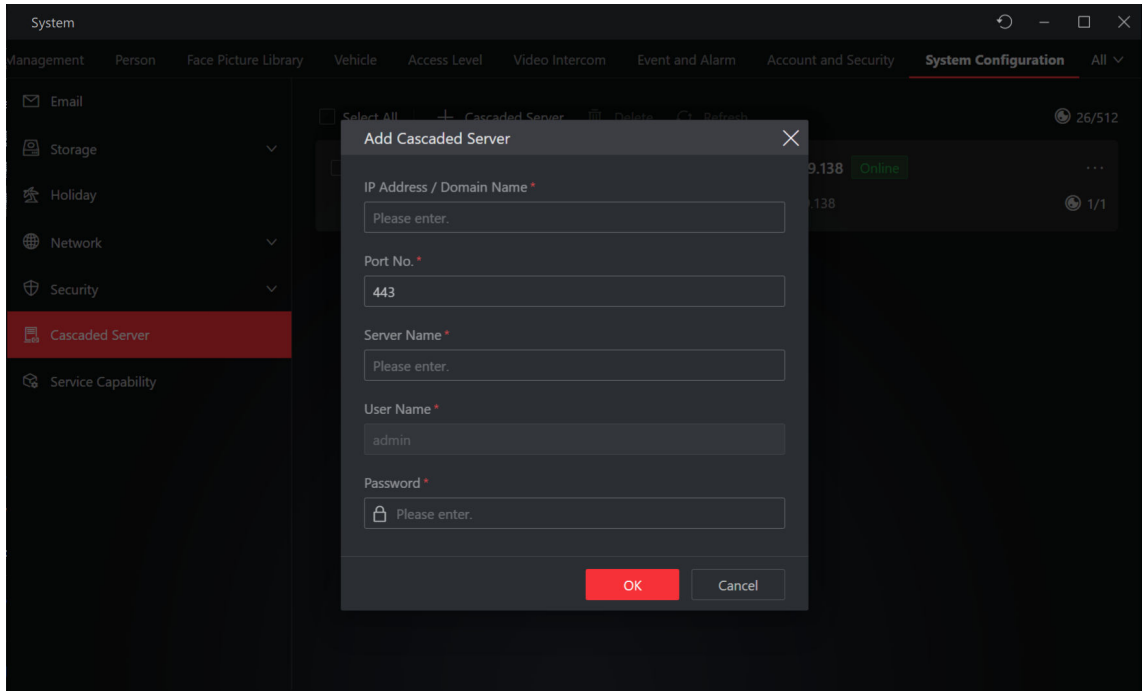
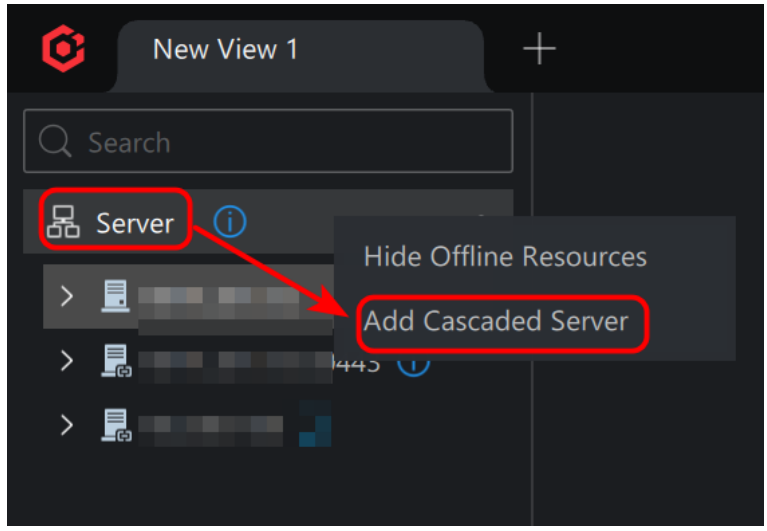


Figure 8-1 Add Cascaded Server

Alternatively, in the Resource Panel, right-click the Server or the Central Server and select **Add Cascaded Server**.



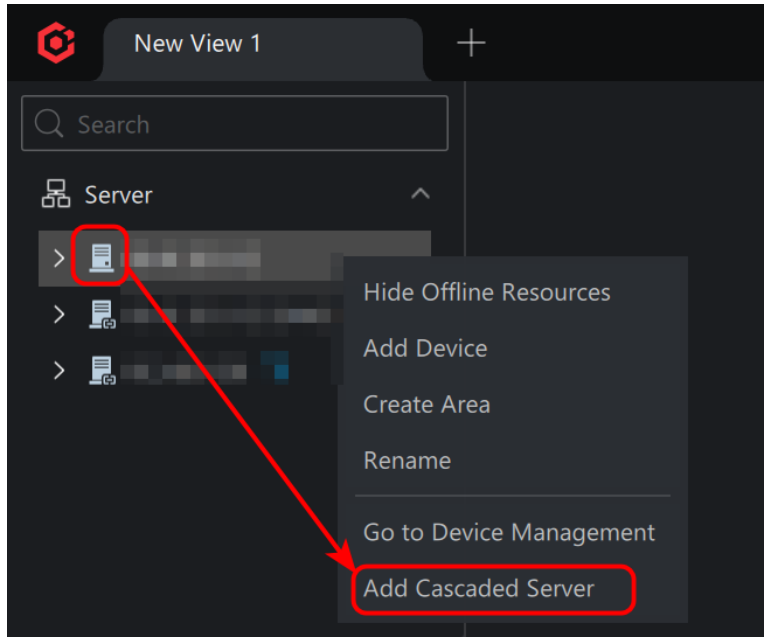


Figure 8-2 Resource Panel

On the Add Cascaded Server page, enter IP address / domain name, port No., server name, and password. Up to 20 cascaded servers, 512 channels (central servers and cascaded servers), and 1,000 areas are supported.

Note

- Only admins can add cascaded servers.
- The version of the cascaded server must match that of the central server.

8.3 Operations After Adding Cascaded Servers

After adding cascaded servers, you can:

- View the online/offline/abnormal status and added / total channels of cascaded servers.
- Click ··· to edit, delete, or refresh servers. Removing a cascaded server also deletes all its synchronized resources from the central server.
- Click ··· → **Select Resource** to import resources under cascaded servers to the central server.

In the Resource panel, you can also right-click the cascaded servers to edit or delete them.

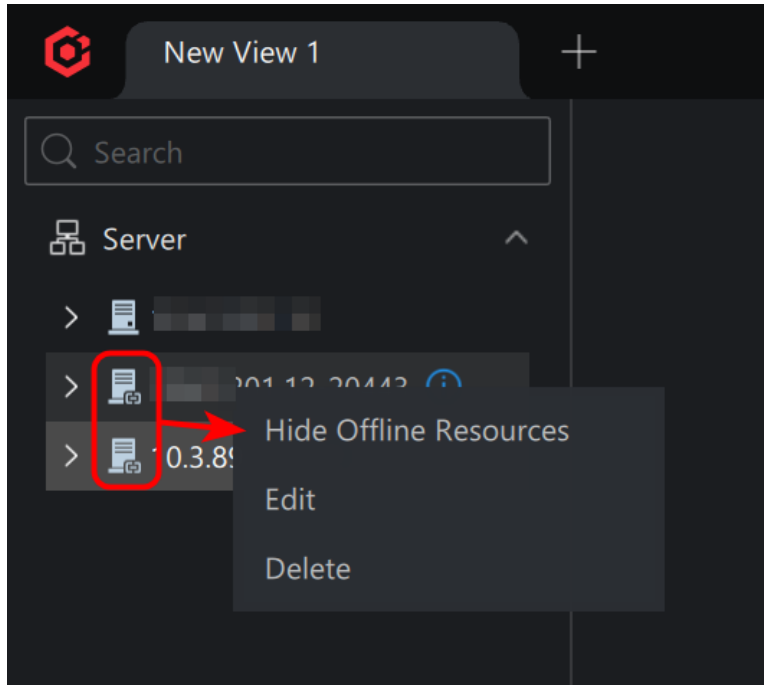


Figure 8-3 Resource panel

8.4 Cascaded Server Management Capabilities

Function	Whether Supported	Note
Resource Access	√	Configure resource access permissions for cascaded servers. See ***Add a Role*** .
Live View & Playback	√	Live view, playback, toolbar, timeline, and right-click operations of cameras under cascaded servers.
Custom View	√	Create custom views by grouping cameras from cascaded servers.
Remote Configuration	×	Redirecting to device management page is not supported.
Access Control	×	All features related to access control are not supported.
Event & Alarm Notification	√	Receive real-time event and alarm notifications pushed from cascaded servers.

Function	Whether Supported	Note
Intelligent Search & AcuSeek	√	Alarm, vehicle passing event, face & human body detection, and intelligent search on cascaded servers. See ***Search*** .
Mobile Client	√	Manage cascaded servers via cloud account on the Mobile Client.

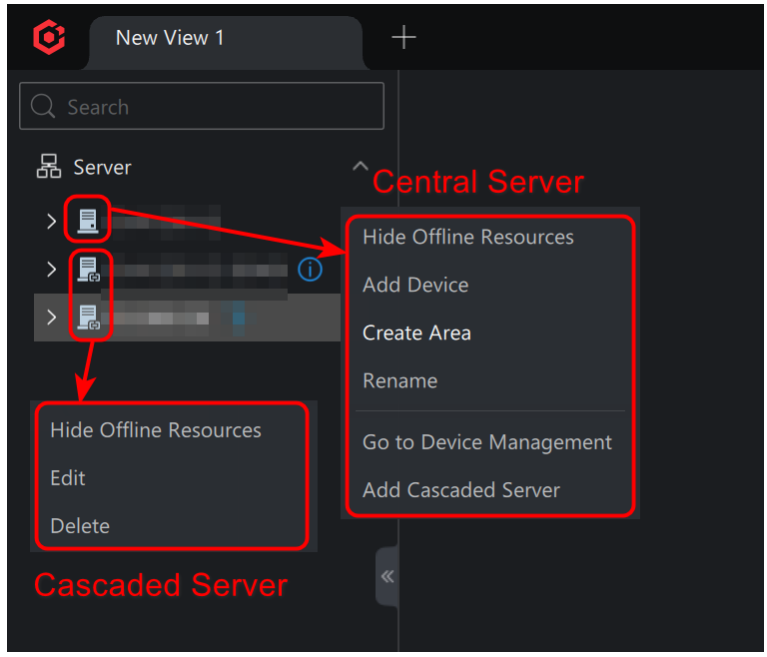


Figure 8-4 Central and Cascaded Server

Chapter 9 Main Panel for Monitoring and Control

The following is the introduction of main panel for monitoring and control.

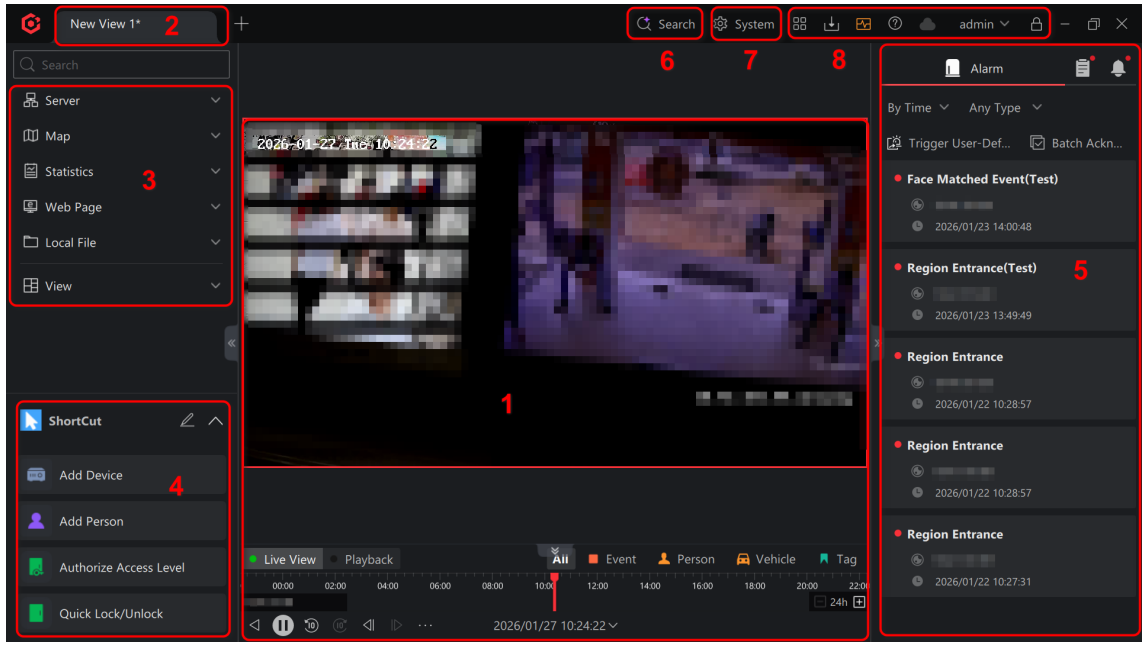


Figure 9-1 Main Panel for Monitoring and Control

Table 9-1 Main Panel Introduction

No.	Function
1	Display resources, maps, statistics reports, web pages, local files, and views in the viewing grid. Local files include captured pictures and recorded videos during live view and playback. You can also drag a picture or video from local PC to the viewing grid. Right-click the blank area around the video images to use the following functions: saving the current image(s) as a view, saving an existing view as a new view, global stream configuration, view scale adjustment, switching decoding mode, maximize the current displayed image, and clear windows. **View Scale** **Original Resolution** indicates to play a video in its original size, and the image may not fill the live view / playback window. **Full Screen** indicates that the image will fill the entire live view / playback window. **Decoding Mode**

No.	Function
	Hardware decoding is to decode based on GPU, while software decoding is on CPU. Choose the decoding mode according to your GPU/CPU performance.
2	Drag a view upwards or downwards, or right-click a view and click **Open in New Window** to open the current view in a new window.
3	Right-click to add areas, resources, maps, statistics reports, web pages, local files, and views / view groups. You can double-click an area, a resource, a map, a statistics report, a web page, a local file or a view for display, or drag them one by one to the viewing grid for display. You can also right-click an area and select **Go to Device Management** to filter and display the resources under that area in the device list.
4	Click to pop up the menu of the client, and click to add a module to the **Shortcut**, which provides a quick access to the corresponding module. You can drag the added modules to adjust their sequences.
5	**Alarm**: View the alarm list in real time. If there is no alarm added, click **Configure** to add alarms. For details, refer to ***Add an Alarm*** . You can display alarms by time or priority order, and filter alarms by event types. You can right-click an alarm to view the alarm details, (batch) acknowledge the alarm, mark the alarm, export the alarm, view alarm configuration, etc.
	Event: View all the events configured in the client. You can view events related with the resources on the current view or events related with all resources. You can hover on an event to view event details, drag an event to view the related video, and right-click an event to perform more operations. **Note** Operations after right clicking are different according to different event types.
	Notification: View the system notifications which indicate status or operations.
	VCA / Smart Search: View the VCA / smart search results. You can filter by time and click a picture to view the corresponding video at the specific time.
	AcuSearch: View AcuSearch results. You can filter by time and similarity, view the similarity between objects detected in the image and that in other captured pictures and view the comparison details.

No.	Function
6	The entry to the Search module, where you can search for historical alarms, person access records, vehicle passing records, etc. For details, refer to ***Search*** .
7	The entry to the System module, where you can add and manage devices, persons, face picture libraries, vehicles, access levels, events and alarms. Also, you can set parameters related with account and security, and configure system parameters.
8	•  : Install and manage third-party integration applications. •  : Enter the Download Center. •  : View the performance of PC on which the client is installed. •  : Get the User Manual of the client. •  : View the information of the login user, manage Licenses, back up data, change password, etc. •  : Lock the client.

Chapter 10 Search

The Search module allows to search for alarms, access events, ANPR events, detected face & human body pictures, system notifications, and system logs. In addition, it provides an intelligent search function, which combines video search, person search, vehicle search, and VCA search.

On the top of the Desktop, click **Search**.

General Search

Table 10-1 General Search Content

Search Type	Description
Alarm	Search for historical alarms by time, server, area, source type (i.e., event category), event name, priority, and source name (device name). Refer to ***Search for and Export Alarms*** for details.
Access Event	Access Event: Search for person authentication events, access control device events, and video intercom call records. Refer to ***Search for Access Events*** for details.
Vehicle Passing Event	Refer to ***Search and Export ANPR Events*** .
Face & Human Body Detection	Refer to ***Search for Recognized Face Pictures and Human Body Pictures*** .
Notifications	Refer to ***Search for Notifications*** .
System Log	Refer to ***Search for System Logs*** .

Intelligent Search

To implement the quick search of targets, the supported search conditions can be used in a flexible combination according to actual needs.

Table 10-2 Intelligent Search Condition

Search Condition	Scenario
Server	Search for data on the current server or cascaded servers. Refer to ***Server Cascading*** .
Location	• Search for persons/vehicles captured by specified cameras or accessed doors. Refer to ***Search for Detected Vehicles or Persons by Cameras/Doors*** . • Search for specific targets related to line-crossing / intrusion event by drawing a VCA area on the video. Refer to ***Search for Detected Persons or Vehicles in VCA Areas*** for details.
Target	Upload a picture to search for persons. Refer to ***Search Targets by a Picture*** and ***AcuSearch*** , and ***AcuSeek*** .
Features	Search for persons/vehicles by specific features (such as face picture library or vehicle license plate number). Refer to ***Search for Detected Persons/Vehicles by Features*** .

10.1 Search for Detected Vehicles or Persons by Cameras/Doors

Search for videos captured by specified devices, detected vehicles/persons, and access records within specified time period.

Select the server to be searched, time, and set the **Location** to **Camera or Door**.

Note

The server includes the currently logged-in server and added cascaded servers. For adding cascaded servers, see ***Server Cascading*** .

Location	Search Result
Camera	• Regular videos captured by the camera. • Passing vehicles. • Captured face pictures. • Video tags that are configured during playback or the event/alarm linkage tags.
Door	• Regular videos. • Captured face pictures. • Card-swiping records.

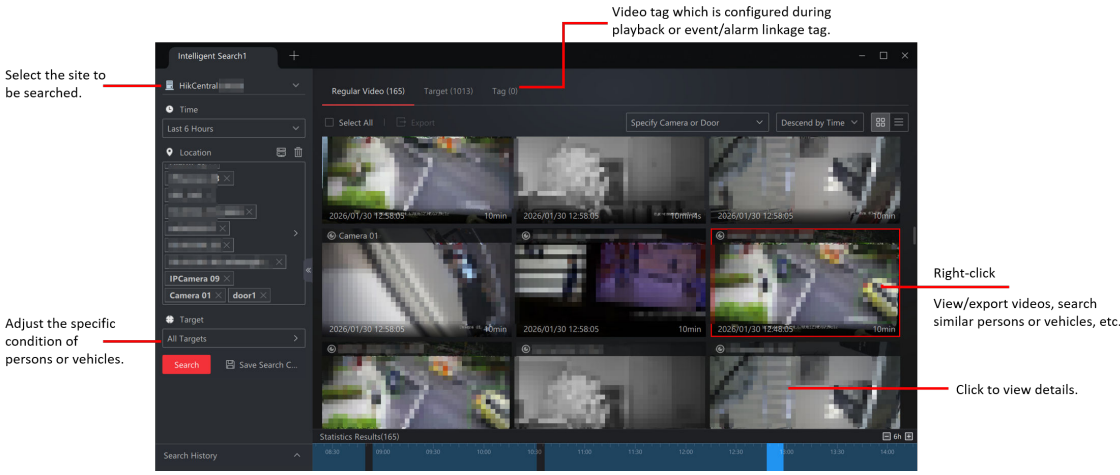


Figure 10-1 Search Result

For Video Playback

Double-click or right-click a video to play it. You can control playback speed, jump to the resource details page, etc.

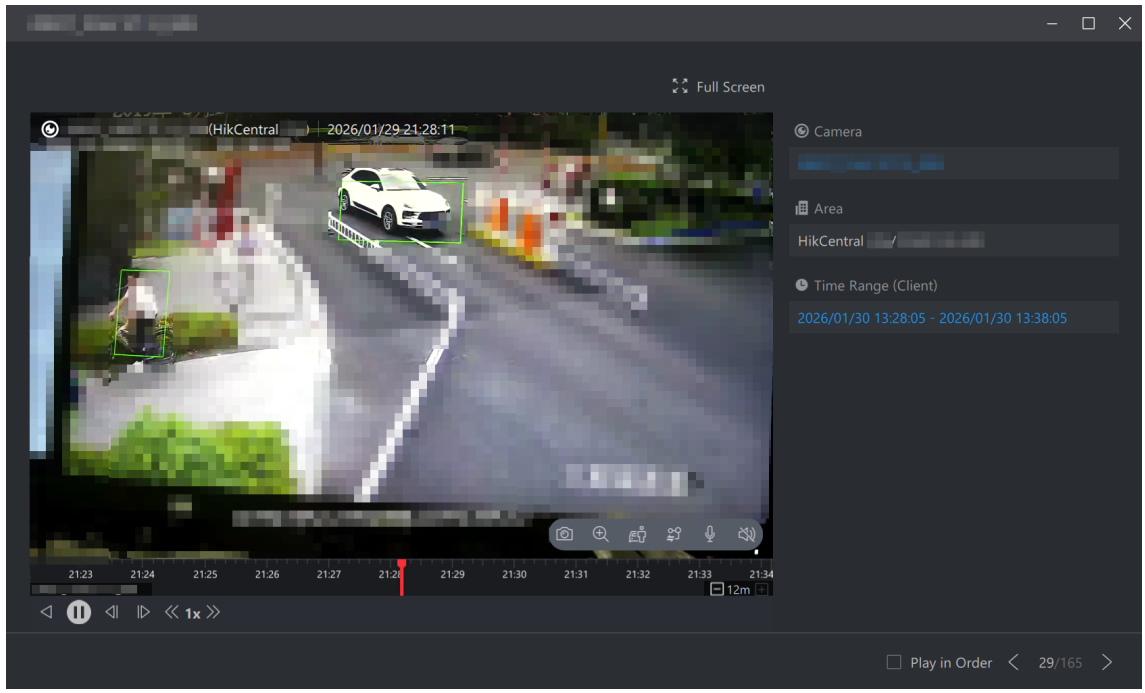


Figure 10-2 Video Playback

10.2 Search for Detected Persons or Vehicles in VCA Areas

You can search for VCA events related videos. The VCA events include intrusion detection and line crossing detection.

Note

Make sure that the VCA functions are already enabled on the device.

1. On the Intelligent Search page, select the server to be searched.

   Note

   The server includes the currently logged-in server and added cascaded servers. For adding cascaded servers, see ***Server Cascading*** .
2. Set the time period and set the **Location** to **VCA Area**.
3. Select a camera to search for the VCA event related videos.
4. Select the VCA event type (**Intrusion Detection** or **Line Crossing Detection**), and draw a detection area/line for search.
5. Click **Search**.

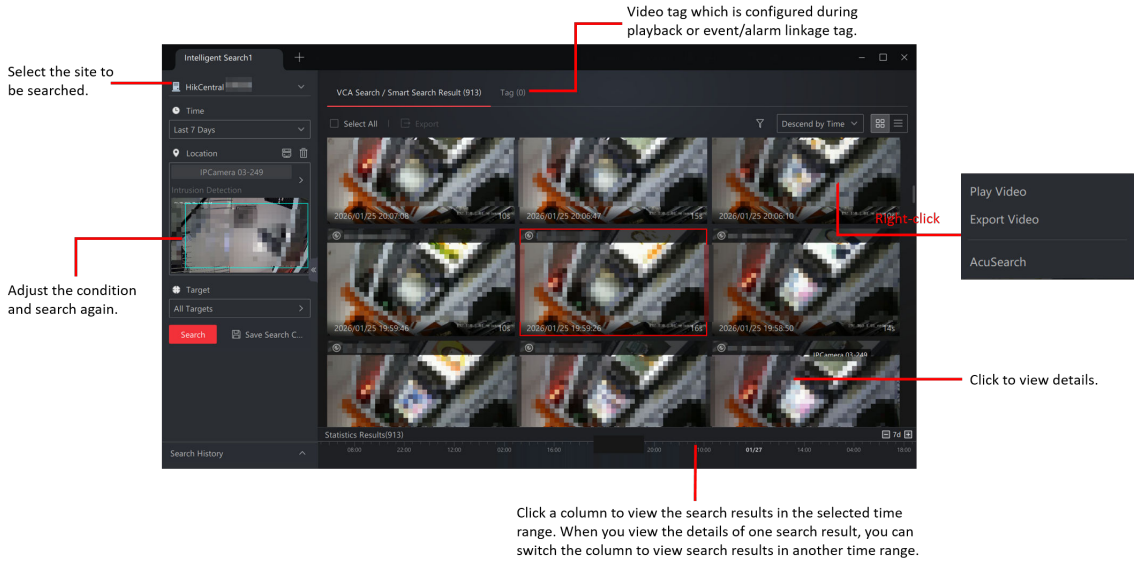


Figure 10-3 VCA Search

10.3 Search for Detected Persons/Vehicles by Features

On the Intelligent Search page, select the server to be searched, time, and target features.

Note

The server includes the currently logged-in server and added cascaded servers. For adding cascaded servers, see ***Server Cascading*** .

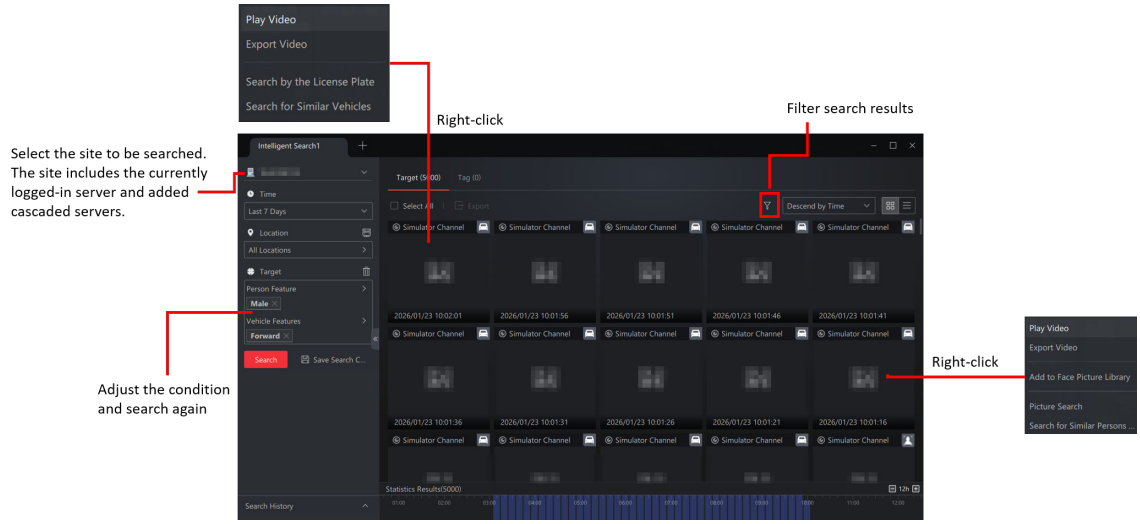


Figure 10-4 Search for Persons/Vehicles by Features

Chapter 11 Event and Alarm

In the Event and Alarm module, you can add and configure alarms, view the list of triggered alarms, searching for and export alarms, subscribe to events, etc.

Event is the signal that resource (e.g., device, camera, server) sends when something occurs. Some events can be subscribed directly for records.

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. The triggering event should be configured for an alarm for further notification and linkage actions. You can check the received real-time alarm information and search for history alarms.

Go to **System → Event and Alarm** to enter the Event and Alarm module.

11.1 Supported Triggering Events

Go to **Alarm Configuration → Add Alarm** . In the Add Alarm window, you can view all supported triggering events in the **Triggering Event** list:

Alarms of Video

Table 11-1 Video

Category	Specific Event
VCA Event	Fast Moving
	Intrusion
	Line Crossing
	Motion Detection
	Object Removal
	Object Thrown from building
	Region Entrance
	Region Exiting
	Reverse Entering Alarm
	Unattended Baggage
ANPR	Vehicle Type Matched Event
	Vehicle Matched Event
	Vehicle Mismatched Event

Category	Specific Event
	No License Plate
People Related Event	Face Matched Event
	Face Mismatched Event
	Multi-Target-Type Detection
	Frequently Appeared Person
	Loitering
	Face Detection
	Face Capture
	People Queuing-Up Alarm
	Waiting Time Detection Alarm
	People Gathering
	People Density
Thermal-Related Event	PIR
	Ship Detection
	Temperature Difference Alarm
	Temperature Alarm
	Temperature Pre-Alarm
	Fire and Smoke Detection
Alarm Input	Alarm Input Triggered

Alarms of Access Control

Table 11-2 Door

Category	Specific Event
Normal Card Swiping	Access Granted by Card and Fingerprint
	Access Granted by Card, Fingerprint, and PIN
	Access Granted by Valid Card
	Access Granted by Card and PIN
	Access Granted by Fingerprint

Category	Specific Event
	Access Granted by Fingerprint and PIN
	Duress Alarm
	Access Granted by Face and Fingerprint
	Access Granted by Face and PIN
	Access Granted by Face and Card
	Access Granted by Face, PIN, and Fingerprint
	Access Granted by Face, Card, and Fingerprint
	Access Granted by Face
	Access Granted by Employee ID and Fingerprint
	Access Granted by Employee ID, Fingerprint, and PIN
	Access Granted by Employee ID and Face
	Access Granted by Employee ID and PIN
	Access Granted via Combined Authentication Modes
	Skin-Surface Temperature Measured
	Access Granted by PIN
	Access Granted by Iris
Abnormal Card Swiping	Verifying Card Encryption Failed
	Max. Card Access Failed Attempts
	Card No. Expired
	Authentication via Card + PIN Timed Out
	Access Denied (Door Remained Locked or Inactive)
	Access Denied (First Person Not Authorized)
	Access Denied by Card and PIN
	Authentication via Card + Fingerprint + PIN Timed Out
	Access Denied by Card, Fingerprint, and PIN
	Access Denied by Card and Fingerprint
	Authentication via Card + Fingerprint Timed Out
	No Access Level Assigned

Category	Specific Event
	Card No. Does Not Exist
	Invalid Time Period
	Fingerprint Does Not Exist
	Access Denied by Fingerprint
	Access Denied by Fingerprint and PIN
	Authentication via Fingerprint + PIN Timed Out
	Access Denied by Face and Fingerprint
	Authentication via Face + Fingerprint Timed Out
	Access Denied by Face and PIN
	Authentication via Face + PIN Timed Out
	Access Denied by Face and Card
	Authentication via Face + Card Timed Out
	Access Denied by Face, PIN, and Fingerprint
	Authentication via Face + PIN + Fingerprint Timed Out
	Access Denied by Face, Card, and Fingerprint
	Authentication via Face + Card + Fingerprint Timed Out
	Access Denied by Face
	Face Capture Failed
	Interlocking Door Not Closed
	Access Denied by Employee ID and Fingerprint
	Authentication via Employee ID + Fingerprint Timed Out
	Access Denied by Employee ID, Fingerprint, and PIN
	Authentication via Employee ID + Fingerprint + PIN Timed Out
	Access Denied by Employee ID and Face
	Authentication via Employee ID + Face Timed Out
	Access Denied by Employee ID and PIN
	Authentication via Employee ID + PIN Timed Out
	Person Not in Multi-Factor Authentication Group

Category	Specific Event
	Person Not in Multi-Factor Authentication Time Period
	Combined Authentication Timed Out
	Access Denied by Invalid M1 card
	Verifying CPU Card Encryption Failed
	Access Denied (NFC Card Reading Disabled)
	EM Card Reading Not Enabled
	M1 Card Reading Not Enabled
	CPU Card Reading Disabled
	Authentication Mode Mismatch
	Lost Card Authenticated
	Authentication Attempts via Card + PIN Exceeded Limit
	Password Mismatch
	Employee ID Does Not Exist
	Failed Password Attempts Alarm
	Verifying DESFire Card Encryption Failed
	DESFire Card Recognition Disabled
	Authentication Failed Due to Abnormal Features
	Access Denied via Iris
	Iris Anti-Spoofing Detection Failed
Other Door Events	Door Unlocked (Door Lock)
	Door Locked (Door Lock)
	Exit Button Pressed
	Exit Button Released
	Card Reader Tampering Alarm
	Door Abnormally Open (Door Contact)
	Remote: Unlocked Door
	Remote: Locked Door
	Door Bell Rang

Category	Specific Event
	Remote: Remained Unlocked (Free Access)
	Remote: Remained Locked (Credential Failed)
	Remaining Unlocked Status Started
	Remaining Unlocked Status Ended
	Remaining Locked Status Started
	Remaining Locked Status Ended
	First Person In Started
	First Person In Ended
	First Person Authorization Started
	First Person Authorization Stopped
	Door Open (Door Contact)
	Door Closed (Door Contact)
	Unlocking Timed Out
	Face Recognition Terminal Online
	Face Recognition Terminal Offline
	Tailgating
	Reverse Passing
	Force Access
	Climbing Over Barrier
	Passing Timed Out
	Intrusion
	Access Denied When Free Passing
	Barrier Blocked
	Barrier Restored
	Multi-Factor Authentication: Access Denied by Super Password
	Multi-Factor Authentication: Access Denied by Remote Authentication
	Multi-Factor Authentication: Access Granted

Category	Specific Event
	Multi-Factor Authentication: Remotely Open Door
	Multi-Factor Authentication: Super Password Access Granted
	Multi-Factor Authentication: Repeated Authentication
	Multi-Factor Authentication: Timed Out
	Card Reader Lid Closed
	Secure Door Control Unit Lid Opened
	Enter Dismiss Code
	Fire Alarm Relay Triggers Door Remain Open
	Fire Alarm Relay Recovered and Door Recovered
	Blocklist Event
	Opening Door via Exit Button Failed When Door Remaining Closed or in Sleep Mode
	Opening Door by Linkage Failed When Door Remaining Closed or in Sleep Mode
	Overstay
	Unlock by Center
	Door Not Open
	Door Not Closed
	Secure Door Control Unit Disconnected
	Secure Door Control Unit Connected
	Motion Detection

Table 11-3 Access Control Device

Category	Specific Event
Device Security	Device Tampering Alarm Restored
	Secure Door Control Unit Tampering Alarm
Local Operation on Device	Local: Login Locked
	Local: Login Unlocked
	Local: Login

Category	Specific Event
	Local: Logout
	Local: Upgrade
	NTP Auto Time Synchronization
	Local: Restored Default Parameters
	Edit Network Center Configuration
	Edit GPRS Parameters
	Edit Central Group Configuration
	Import Normal Configuration File
	Export Normal Configuration File
	Import Card Permission Parameters
	Export Card Permission Parameters
	Local: Upgrade Device Firmware via USB Flash Drive
	Local: Upgrading Failed
Device Component Communication	Lane Controller Fire Input Alarm
	Pedestal Temperature Too High
	Communication with Light Board Exception
	Indicator Turned Off
	Lane Controller Disconnected
	Lane Controller Connected
	CAN BUS Recovered
	Lane Controller Fire Input Recovered
	Communication with IR Adaptor Recovered
	Active Infrared Intrusion Detector Recovered
	Extension Module Offline
Device Disk/HDD	No Memory Alarm for Unreported Events
	No Memory for Unreported and Access Granted Events
Device Battery	AC Power On
	Battery Voltage Recovered

Category	Specific Event
	Battery Voltage Restored
	Device Power On
Device Record Reporting	Access Control Device Armed
	Video Intercom Device Armed
Device Network	Access Control Device Online
	Video Intercom Device Online
Remote Operation on Platform	Remote: Login
	Remote: Logout
	Remote: Arming
	Remote: Disarming
	Remote: Restart
	Remote: Upgrade
	Remote: Export Configuration File
	Remote: Import Configuration File
	Alarm Output On
	Alarm Output Off
	Remote: Manual Time Synchronization
	Remote: Clear Card No.
	Remote: Restored Default Parameters
	Remote: Capture
	Remote: Upgrading Failed
	Remote: Extension Module Upgraded
	Remote: Extension Module Upgrading Failed
	Remote: Fingerprint Module Upgraded
	Remote: Fingerprint Module Upgrading Failed
	SOS

Table 11-4 Alarm Input

Specific Event	Description
Alarm Input Triggered	Occurs when an abnormal signal is detected at the device's alarm input (e.g., smoke detector measuring concentration beyond the threshold), activating the alarm. This event indicates the beginning of an alarm condition.
Alarm Input Restored	Occurs when the abnormal signal ceases and the alarm state returns to normal. This event signifies the end of an alarm condition.

Note

To fully track the alarm cycle—Normal → Triggered → Restored—it is recommended to subscribe to both events.

Table 11-5 Person

Specific Event
Person Matched
Card Number Matched

Alarms of Alarm Detection

Table 11-6 Alarm Detection

Category	Specific Event
Alarm Input	Alarm Input Triggered
	Alarm Input Restored
	Tampering
	Tampering Restored
	Bypass
	Bypass Restored
Partition (Area)	Disarming
	Alarm Cleared
	Away Arming
	Stay Arming

Category	Specific Event
Peripheral	Permanent Deactivation
	Permanent Deactivation Restored
	One-Time Deactivation
	One-Time Deactivation Restored
	Lid Only for One-Time Deactivation
	Lid Only for One-Time Deactivation Restored

Alarms of Maintenance

Table 11-7 Service

Category	Specific Event
Streaming Server	Streaming Server Offline
Storage Server	Storage Exception
System Management Service	CPU Exception
	CPU Warning
	RAM Exception
	RAM Warning
	System Service Abnormally Stopped

Table 11-8 Access Control Device

Specific Event
Device Tampered
Lane Controller Tampering Alarm
Secure Door Control Unit Tampering Alarm
Access Control Device Offline
Video Intercom Device Offline
AC Power Off
Device Power Off
Low Storage Battery Voltage
Battery Voltage Restored

Specific Event
Low Battery Voltage
Arming Device failed
Video Intercom Device Arming Failed
Memory Card Full
Flash Writing/Reading Exception
Motor or Sensor Exception
CAN BUS Exception
Active Infrared Intrusion Detector Exception
Communication with IR Adaptor Exception
Indicator Turned On
Lane Controller Disconnected
Lane Controller Connected
Extension Module Offline
Access Control Device Call Center
Video Intercom Device Call Center

Table 11-9 Camera

Specific Event
Camera Online
Camera Offline
Channel Armed
Channel Arming Failed
Defocus Detection
Video Loss
Camera Recording Exception
Camera Recording Recovered
Image Exception Event
Video Tampering Detection
Scene Change Detection

Specific Event
Vibration Detection Alarm
Audio Exception Detection
Video Stream Transcoding Exception

Table 11-10 Encoding Device

Specific Event
Device Reconnected
Device Offline
HDD Full
HDD High Temperature
HDD Impact Detection
HDD Server Failure
R/W HDD Failure
Array Exception
Illegal Login
Device Armed
Arming Device Failed

Table 11-11 Security Control Device

Specific Event
Disk Exception
Forced Arming
Late to Disarm
Keypad/Keyfob Panic Alarm
Keypad/Keyfob Fire Alarm
Duress Alarm
Keypad Locked
Keypad Unlocked
Lid Opened

Specific Event
BUS Open-Circuit Alarm
BUS Short-Circuit Alarm
AC Power Down
Battery Low
Reset to Defaults
Extension Module Exception
Expander Lid Opened
Telephone Communication Failed
Bus Expander Offline
Auto Arming Failed
Expander Offline
Cellular Data Network Exception
SIM Card Exception
Wired Network Fault
Device Offline
Device Online
IP Conflict
Repeater Lid Opened
Repeater Offline
Repeater Deleted
Repeater Enrolled
Sounder Lid Opened
Sounder Offline
Sounder Deleted
Sounder Enrolled
Expander Deleted
Expander Enrolled
Device Motion Alarm

Specific Event
Radar Transmitter Fault
Video Tampering Alarm Started
Wi-Fi Signal Exception
RF Signal Exception
Data Limitation Reached
Sounder Battery Low
Device Armed
Arming Device Failed
Video Standard Mismatch
HDD Full
Partition Auto-Disarmed
Partition Auto-Armed
Partition Arming Failed
Battery Disconnected
Peripheral Lid Opened
Peripheral Undervoltage
Peripheral Offline
Peripheral Deleted
Peripheral Enrolled
AC Power Restored
Emergency Alarm
Overcurrent Protection Triggered
Overcurrent Protection Restored
Overvoltage Protection Triggered
Overvoltage Protection Restored
Repeater Battery Low
Repeater Battery Voltage Restored
Repeater AC Power Down

Specific Event
Repeater AC Power Restored
Repeater Battery Disconnected
Repeater Battery Reconnected
Keyswitch Zone Armed
Key Zone Disarming
Network Switched
Incorrect Password
External Module Disconnected
Expander AC Power Down
Expander AC Power Restored
Main Signaling Path ATP Fault
Main Signaling Path ATP Restored
Backup Signalling ATP Path Fault
Backup Signalling ATP Path Restored
Manual Test Report
Scheduled Test Report
Walk Test Enabled
Walk Test Disabled
Enter Programming
Exit Programming
Intrusion Detection
Intrusion Detection Restored
Sudden Increase of Sound Intensity Alarm
Sudden Increase of Sound Intensity Alarm Restored
Sudden Decrease of Sound Intensity Alarm
Sudden Decrease of Sound Intensity Alarm Restored
Region Entrance Detection
Fire Source Alarm

Specific Event
Fire Source Alarm Restored
Power Output Short Circuit Restored
Temperature Exception Alarm Restored
Drilling Alarm
Drilling Alarm Restored
Panel Reset Operation
Start Upgrade
Upgrade Fail
Lid Deactivated
Lid Deactivated Restored
External battery Fault
High Temperature Pre-Alarm
High Temperature Pre-Alarm Restored
Low Temperature Pre-Alarm
Low Temperature Pre-Alarm Restored
Keypad/Keyfob Medical Alarm
Unregistered Tag Operation
Tag Reader Locked
Tag Reader Unlocked
Keyfob Undervoltage
Keyfob Undervoltage Restored
Sending Email Failed
Network Camera Disconnected
Network Camera Reconnected
Patrol Signing
Region Exiting Detection
Power Output Short Circuit
Power Running Out

Specific Event
Temperature Exception Alarm
Battery Fault
Battery Fault Restored
Upgrade Success
SIM Card Conflict
External Battery Fault Restored
External Battery Loss
Peripheral Battery Lost Restored
Bus Overload
External Module Connected
Battery Low
Battery Disconnected
Battery Restored in Alarm Panel

Alarms of Custom Event

Table 11-12 Custom Event

Category	Specific Event
User-Defined Event	User-Defined Event
Generic Event	Generic Event

11.2 Event Subscription

You can subscribe to some events to receive them for records on the platform. Batch subscription or unsubscription is supported.

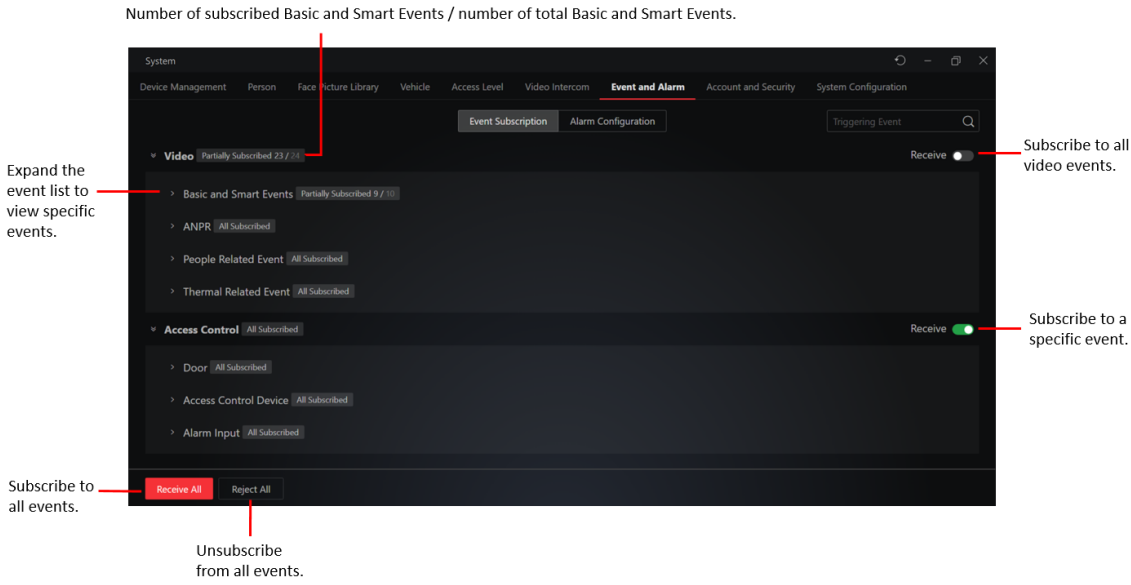


Figure 11-1 Event Subscription

- You can receive alarms without subscribing to events.
- If an event is unsubscribed, you will not be able to find the event in the Search module, or receive the event on the main panel for monitoring and control.

11.3 Add an Alarm

The platform provides multiple triggering event types for you to configure rules for detection or triggering alarms.

Steps

1. In the **Event and Alarm** module, click **Alarm Configuration → Add Alarm** to open the Enter the Add Alarm window.
2. Select the triggering event (***Supported Triggering Events***) and source(s), and set the alarm priority. Click **Next**.
3. Configure the receiving schedule. Click **Next**.

   For holiday schedules, see details in ***Add or Edit a Holiday*** .
4. Select the alarm recipient(s). Click **Next**.
5. **Optional:** Add linkage action(s) as needed. See detail in ***Supported Linkage Actions*** .
6. Click **Complete**.

11.4 Supported Linkage Actions

The supported linkage actions are **Trigger Recording**, **Trigger Pop-up Window**, **Trigger Audible Alarm**, **Capture Picture**, **Create Tag**, **Trigger PTZ**, **Link Access Point**, **Link Alarm Output**, **Send Email**, **Trigger User-Defined Event**, and **Link Partition (Area)**.

For **Trigger Recording**, **Capture Picture**, and **Create Tag**:

If you have selected **Source Camera** and the source is a door without a linked camera, the linkage action can still be added but will not come into effect.

Trigger Recording

Select the camera to record the alarm video when the alarm is triggered.

- **Source Camera**: Record videos by the camera that triggered the alarm and storing the video files in the selected storage location (i.e., Store in Main Storage, Store in Auxiliary Storage, and Not Store).
- **Specified Camera**: Record videos by other cameras and storing the video files in the selected storage location(s) for specified camera(s) respectively.

Note

- The recording will start from 3 seconds before to 15 seconds after the alarm triggering.
- The recording will be kept for 7 days at least and then will be processed following the overwriting mechanism of device.

Create Tag

To add this linkage action, **Trigger Recording** should be configured as well. The tag will be added to the event-triggered video footage for convenient search.

You can customize the tag name as desired or select existing ones ($Event Name / $Event Time / $Event Source).

Note

- The tag will be placed from 3 seconds before to 15 seconds after the alarm triggering.
- After tags are created, you can perform playback by tag, and search for triggered alarms by tag (***Search for and Export Alarms***).

Capture Picture

Select cameras to capture pictures during the alarm.

- **Source Camera**: Capture picture by the camera that triggered the alarm.
- **Specified Camera**: Capture picture by other cameras.

Note

Only one picture will be captured by each camera.

Trigger PTZ

Call the preset, patrol, or pattern of the selected cameras when the alarm is triggered.

Link Access Point

The selected door(s) will be locked, be unlocked, remain locked, or remain unlocked as configured when the alarm is triggered.

Link Alarm Output

Link alarm output device(s) (peripherals such as speaker).

Set the linkage status to On or Off, and the closing method to Manually Close or Auto Close. If Auto Close is selected, set the duration between 1 and 600 seconds.

When alarm outputs linked with devices are imported, you can select these alarm outputs. For importing alarm outputs, see ***View Details of a Device*** .

Trigger User-Defined Event

Before adding this linkage action, you should configure alarm(s) for user-defined event(s) first. As the user-defined event(s) cannot be automatically detected, it needs to be manually triggered by clicking **Trigger User-Defined Event** on the notification panel of the main page, or added as a linkage action for another alarm.

Trigger Audible Alarm

Play the voice text on the PC in case the monitoring personnel is not looking at the screen. The voice text will come into effect only when the audio function is enabled and the system voice engine is selected as the alarm sound. See details in ***Event and Alarm*** .

Trigger Pop-up Window

Display the alarm window to show the alarm details, alarm linked cameras' live videos and playback, etc. when the alarm is triggered.

Link Partition (Area)

Add partitions (areas) and set their arming status (such as Stay Arming, Away Arming, or Disarming). When an alarm is triggered, the associated partitions will automatically arm or disarm according to your linkage settings.

You can add up to 64 partitions (areas).

Note

Ensure your current role has both General Surveillance and Device Management permissions for the corresponding partitions (areas). For details, ***Add a Role*** .

11.5 Alarm List

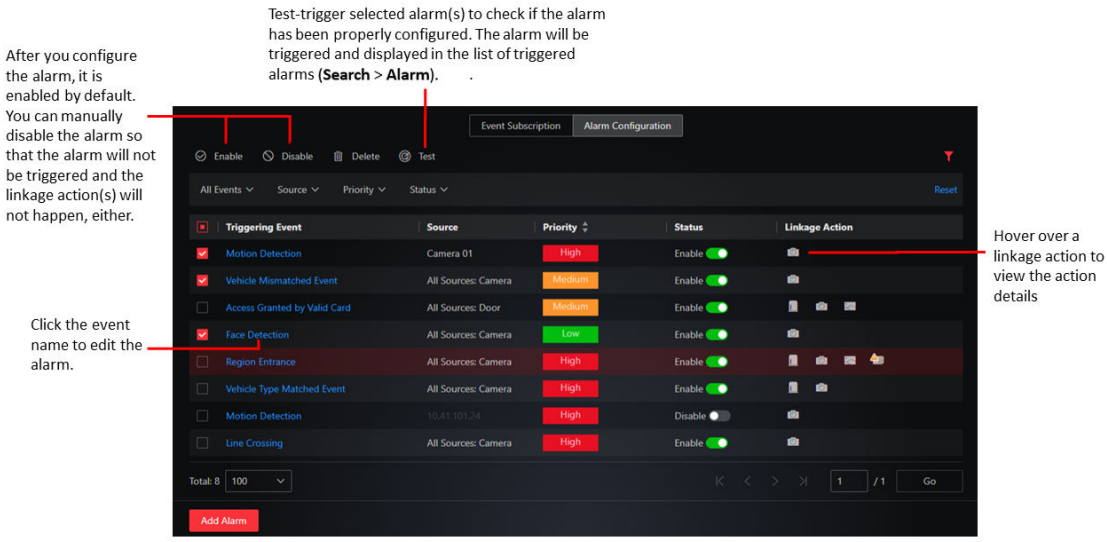


Figure 11-2 List of Configured Alarms

11.6 Search for and Export Alarms

Go to **Search → Alarm** to view the list of triggered alarms.

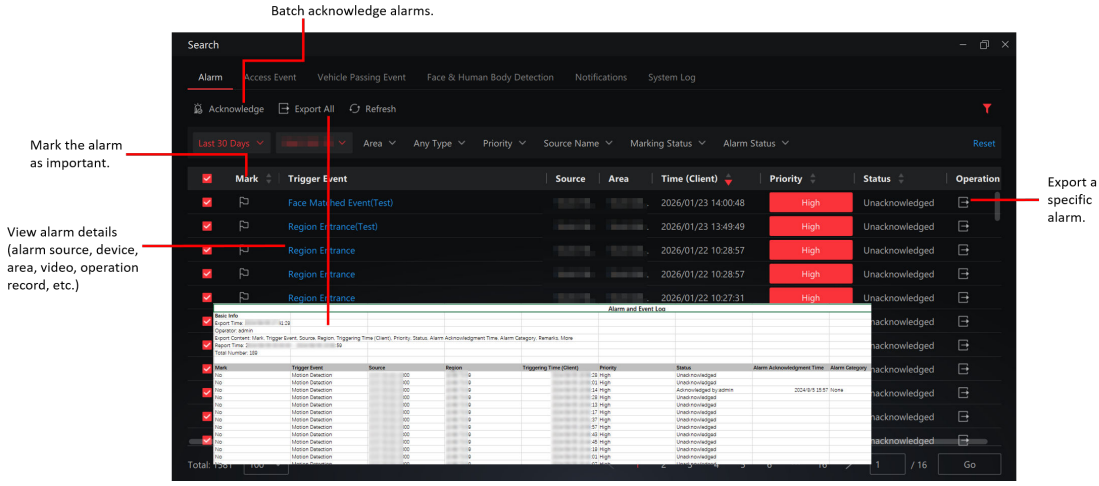


Figure 11-3 Triggered Alarm List

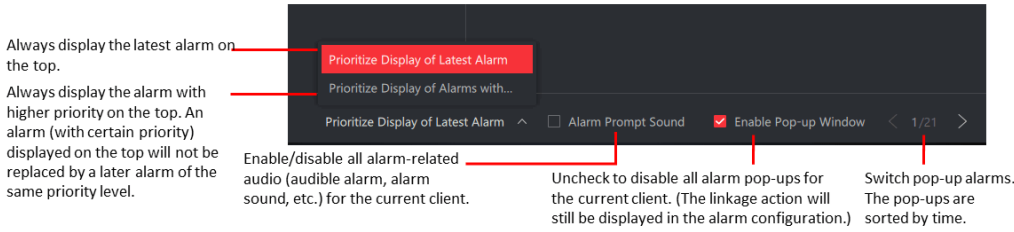


Figure 11-4 Alarm Pop-up Window

You can also enable/disable the alarm prompt sound by enabling/disabling the audio in **Local Configuration → Event and Alarm → Display** .

11.7 Local Configuration About Event and Alarm

You can configure event and alarm related parameters including display type, alarm sound, whether to play the audio repeatedly, and times of playing.

See details in ***Event and Alarm*** .

Chapter 12 Cloud Connection

The Cloud gives the ability to:

1. Log in to the system through the WAN without port mapping configuration.
2. Add users to your Systems via an email invite.
3. Log in to the Mobile Client through the Internet.

Even if you log in to the system via the WAN, the data are still stored in the local PC. This makes the system access convenient and safe.

To access Cloud features, a System must be connected to the cloud, which makes it a Cloud System (as opposed to a Local System). This requires the activation of at least one license. After a System is connected to Cloud, it has access to all Cloud features, and can be disconnected from Cloud at any time. After being disconnected, a System becomes a local System again. All Cloud users will be deleted.

To connect the system to Cloud, you must create a cloud account for the administrator first. A cloud account can be granted with different permissions. Users with Cloud accounts are also referred to as Cloud users. Users with local accounts are referred to as Local users.

Create a Cloud Account

Before You Start: To create a cloud account, you need to connect the server to the Internet first.

1. On the top right corner of the Desktop, click → **Register Now** to open the Create Cloud Account window.
2. Select the nation/region of the server.

   Note

   The system will automatically get the location of the server, and you can edit it.
3. Enter the user's email address, verification code, and password for login, and check the agreement of terms.
4. Click **Create Account and Connect to Cloud**. The system will send a verification email for activating the cloud account.
   After the user activates the cloud account via the email, the Connect to Cloud window will pop up.

Note

- Only Administrator can create a Cloud account and connect to the Cloud on the Server.
- To connect to the Cloud, the PC should be connected to the WAN.

Log into HCL Cloud from the Desktop

1. On the top right corner of the Desktop, click  → **Connect to Cloud** to open the Connect to Cloud window.
2. Enter the verification information and click **Connect**.

   The icon will turn to  if you connect to the cloud successfully.

After connecting to Cloud, you can ***add other cloud users*** who can access the system via the Mobile Client in the WAN.

Change Password of Admin's Cloud Account

1. Click  → **Change Password** .
2. Select a mode for changing password.

   Old Password

   Enter the old password for verification.

   Verification Code

   Click **Get Verification Code**. Enter the verification code you received in your email.
3. Enter the new password and confirm password.
4. Click **Save**.

Disconnect the System from Cloud

Click  → **Disconnect** .

Note

Disconnecting will revoke access for all users with whom the system has been shared.

Chapter 13 Management of Users and Roles

In the Account and Security module, you can manage users and roles, configure account security rules, resetting login password, etc.

Go to **System → Account and Security** .

13.1 Add a Local User

You can add regular users and assign roles to them for accessing the system. Regular users refer to all users except the super user and cloud users.

Enter the Add User page and set the basic information.

User Type

Users with Cloud accounts are referred to as Cloud users. Users with local accounts are referred to as Local users.

Status and Login

User Status

If you select Inactive, you will not be able to log in with the user account.

Configure permission settings for the user.

PTZ Control Permission

Enter a number that stands for the permission level. Operation from a user with lower permission level can be interrupted by that from another user with higher permission level. During PTZ control for live view, you can also lock the PTZ so that other users with the same or lower PTZ control permission levels cannot perform PTZ control at all.

Assign Role

Select the roles that you want to assign to the user.

You can hover over a role on the list and then click **View Role Details** to view the basic information and permission settings of the role.

13.2 Add a Cloud User

Adding a cloud user means inviting a person to register a cloud account by sending an email invite. The added cloud user can log in to the Mobile App via the WAN.

Steps

1. On the Account and Security page, click **Add User** on the lower left corner.
2. Select **Cloud** as the user type.
3. Enter email of a person to invite and click **Next**.

4. Assign the PTZ Control Permission and a role to the person.

Note

For views created on the Desktop, you need to share them to Cloud users for Mobile App manually to make the views available on the Mobile App.

5. Click **Save**.

After finishing the above steps, the invited user's information will be displayed on the user list, and the icon will be displayed in front of the user name. The user needs to accept the invitation via the email within 24 hours, or you need to resend the invitation. For email address which is not registered to the Cloud, the user should create and activate a cloud account via the email first. Once the invitation expires, the icon will show beside the user name. You can hover the cursor on this icon and click **Invite Again** to resend an invitation.

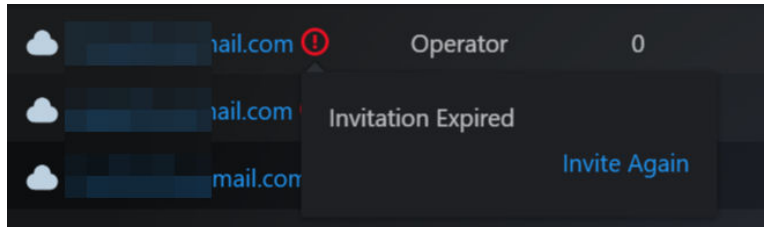


Figure 13-1 Invite Again

13.3 Supported Operations on the User List

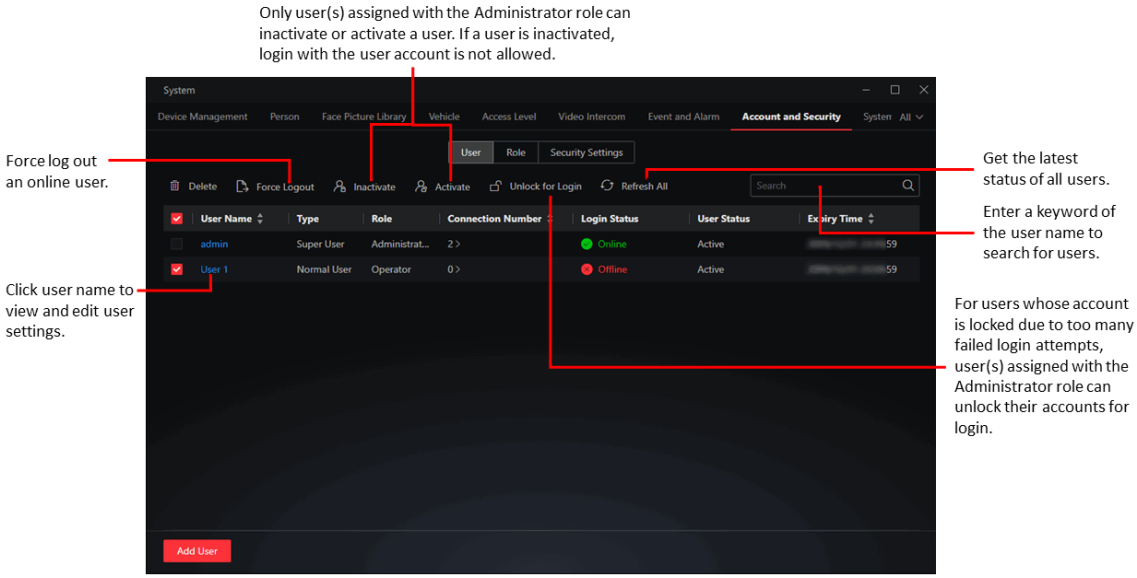


Figure 13-2 User List

13.4 Add a Role

Role is a group of platform permissions. You can add roles and assign permissions to roles, so that users can be assigned with different roles to get different permissions.

Note

The platform has predefined two default roles: Administrator and Operator. You can click the role name to view details. The two default roles cannot be edited or deleted.

Administrator

Role that has all permissions of the platform.

Operator

Role that has all permissions for accessing resources and operating the applications.

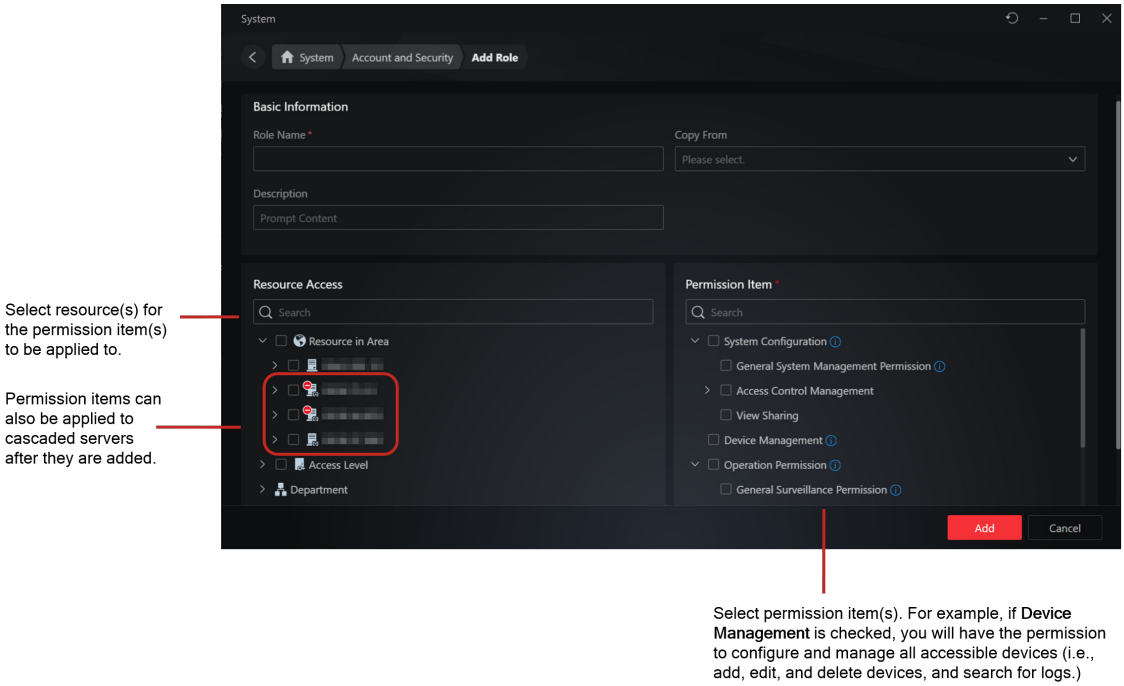


Figure 13-3 Add a Role

Table 13-1 Permission Items

Category	Sub-Category	Specific Permission
System Management	General System Management Permission	Permission for system configuration, management of face pictures and human bodies, ANPR, persons, managing events and alarms, managing users and roles, viewing permissions, configuring security settings, and adding/deleting/editing permission for maps.
	Access Control Management	**General Access Control Management**: Entry to the Access Level module in **System**: applying access levels by department/ person; entry to access schedule management and configuring schedules; entry to access level management and configuring access levels; re-applying access level when applying failed; statistics and details by access level status.

Category	Sub-Category	Specific Permission
		For this permission, the resource permission for department(s) and persons within the department is required, and the specific permission items are assigned according to the resource.
		Multi-Factor Authentication Configuration: Entry to the multi-factor authentication configuration and configuring multi-factor authentication. For this permission, the resource permission for door(s) is required, and the specific permission items are assigned according to the resource.
		Multi-Door Interlocking Configuration: Entry to the multi-door interlocking configuration and configuring multi-door interlocking. For this permission, the resource permission for door(s) is required, and the specific permission items are assigned according to the resource.
		Configuration of First Person In: Entry to the first person in configuration and configuring first person in. For this permission, the resource permission for door(s) is required, and the specific permission items are assigned according to the resource.
		Authentication Code Configuration: Entry to the **Authentication Password** configuration and configuring authentication password on the device. For this permission, the resource permission for door(s) is required, and the specific permission items are assigned according to the resource.

Category	Sub-Category	Specific Permission
	View Sharing	Permission for sharing views with other persons and viewing the list of sharees.
Device Management	Permission for adding/deleting/editing all accessible access control, video intercom devices, and security control panels, monitoring the resources' status in real time, checking the maximum capacity and current number of persons, cards, fingerprints, face pictures, irises, and events under the device, editing the device configuration, importing alarm output/input resources, managing areas and resources under areas, adjusting the hierarchy of areas and belonged resources, and searching for device logs.	
Operation Permission	**General Surveillance Permission**	• Permission for controlling cameras,doors, alarm partitions (areas), and zones. • Permission for controlling alarm outputs: The resource permission for relevant devices is required, and the specific permission items are assigned according to the resource. • Permission for accessing and controlling all maps. • Permission for creating/viewing/exporting statistics and reports of access control and video intercom service: The resource permission for relevant reports is required, and the specific permission items are assigned according to the resource. • Permission for receiving and handling events and alarms: The permission for relevant resources and alarms is required, and the specific permission items are assigned according to the resource.
	Search Permission	
	Video Operation	Playback
		Export Video
		Tag Management
	Access Control Operation	Remote: Unlock Door
		Remote: Lock Door
		Remote: Remain Unlocked

Category	Sub-Category	Specific Permission
		Remote: Remain Locked
		Quick Control All Doors: This permission item only exists in the Administrator role, therefore only available to users assigned with the Administrator role.

13.5 Configure Account Security Rules

Account security is crucial for your system and property. You can lock IP address to prevent malicious attacks, enable auto lock the Client, and set other security settings to increase the system security.

In the Account and Security module, click **Security Settings**.

Login and Lock

Allowed Consecutive Login Attempts

Failed login attempts only refer to failed password attempts (failed verification code attempts excluded).

Lock Duration

When the number of allowed failed login attempts is reached, the current account on the current IP address will be locked. Set the lock duration.

Security Question Settings

Security questions are valid to the super user (admin user) only. They are used to verify the identity when the super user forgets the password. The answers to security questions are case-insensitive.

13.6 Reset Login Password

You can reset the password when you forget your password, or change the password of your currently logged-in user account.

- On the login page, click **Forget Password** to reset your password.
  - The admin user can reset password by answering security questions or verifying via activation code (license code): when the license is activated, you can find the license code in the license file, and enter the code to retrieve password; when the license is not activated, the password can be retrieved by verification code sent to the configured email.
  - Non-admin users can reset password by entering verification code sent to the configured email, or asking users with higher-level role (users with administrator role can ask the admin

user; users without administrator role can ask users with administrator role) to retrieve their password.

- Click the logged-in account name on the top right corner, and select **Change Password**.

Chapter 14 System Configuration

In the upper-right corner of the Desktop, click **System → System Configuration** .

- Email account configuration: ***Configure Email Parameters*** .
- Configure holidays: ***Add or Edit a Holiday*** .
- Configure network related configurations such as the time synchronization, device access protocol, and WAN access: ***Configure NTP Synchronization / Device Access Protocol / WAN Access / NIC, and Reset Network Info*** .
- Configure account security parameters: ***Configure Service Component Certificate*** , ***Use SSL/TLS Certificate for HTTPS Connections*** , and ***Protect Profile Pictures*** .
- ***Configure the System Capability***

14.1 Configure Email Parameters

The email account is used to receive a verification code when you forgot your account password and send the message to the designated email account(s) as the email linkage.

1. In the upper-right corner of the Desktop, click **System → System Configuration → Email** .
2. Configure the parameters according to actual needs.

   SMTP Server Address

   The SMTP server's IP address or host name (e.g., smtp.gmail.com).

   Cryptographic Protocol

   It is used to protect the email content if required by the SMTP server.

   Server Authentication

   If your mail server requires authentication, check this checkbox to use authentication to log in to this server.

   Note

   For users of Google email, you should log in to your Google account, enable the 2-step verification function, generate the APP password, and enter here.
3. Click **Test** to verify whether the email settings take effect.
4. Click **Save**.

14.2 Add or Edit a Holiday

The Holiday templates are mainly used for access control and event and alarm service. You can add holidays to define the special days.

In the **System Configuration** module, select **Holiday**.

Add Holiday

Click **Add**, enter the holiday name, and set the following parameters.

Holiday Type

Select **Regular Holiday** or **Irregular Holiday** according to the actual scene. The regular holiday is suitable for the holiday that has a fixed date. For example, Christmas is on December 25th of each year; the irregular holiday is suitable for the holiday that is calculated by the weekdays, and the specified date might be different in a different year. For example, Mother's Day is on the second Sunday of each May.

Edit Holiday

In the holiday list, select a holiday and directly click a parameter of the holiday to edit it as needed.

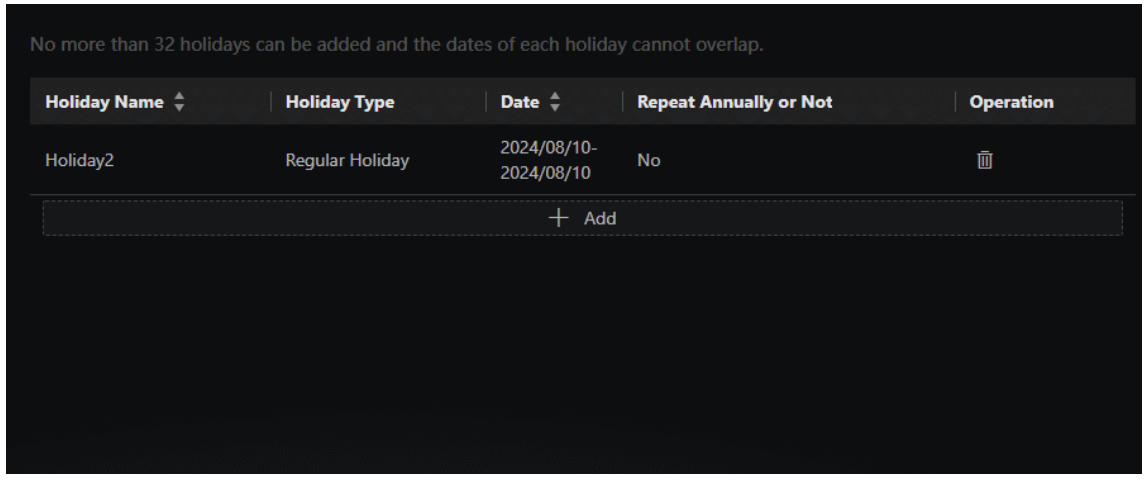


Figure 14-1 Edit Holiday Parameters (.gif)

14.3 Configure NTP Synchronization / Device Access Protocol / WAN Access / NIC, and Reset Network Info

The network settings provided by the client encompass configuring NTP synchronization, device access protocols, WAN access, server addresses, and resetting network information. These settings are essential for ensuring devices operate correctly within network environments.

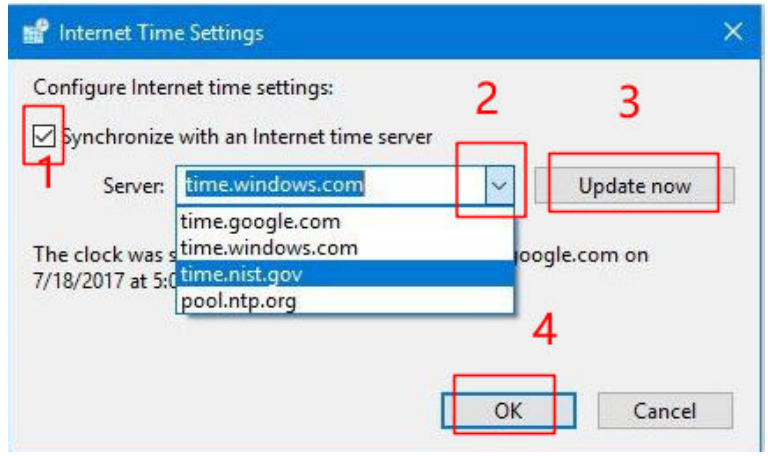
On the Home page, go to **System → System Configuration → Network** .

Configure NTP Synchronization

You can set NTP parameters for synchronizing the time between resources managed on the platform and the NTP server. Three system time sync modes are supported. See the table below for details.

Select **Internet Time Sync**.

Table 14-1 System Time Sync Mode

Mode	Description
Operating System Time Sync	1. You need to configure Internet time settings before configuring Operating System Time Sync. Go to **Control Panel → Clock and Region → Data and Time → Internet Time → Change settings** .  **Figure 14-2 Internet Time Settings** 2. - Select **Operating System Time Sync** and enter the synchronization **Interval**, which is set to 60 minutes by default. - Click **Test** to test the communication between resources and the NTP server. **Note** During the initial deployment, if the operating system has an NTP server configured and the NTP client is running, the system will choose the Operating System Time Sync mode by default.
Local Server Time Sync	• Select **Local Server Time Sync**, and enter the synchronization **Interval**, which is set to 60 minutes by default. • There will be a server providing time synchronization for devices, which only supports Hikvision devices.
NTP Time Sync	• Select **NTP Time Sync** and enter the synchronization **NTP Server Address**, **NTP Port**, and **Interval** • For the local NTP server, you can enable **Configure WAN Mapping** to synchronize time and enter the IP address and

Mode	Description
	port No. for WAN mapping. • Click **Test** to test the communication between resources and the NTP server.

Configure Device Access Protocol

Before adding devices supporting ISUP and/or ONVIF protocol to the platform, you need to set the related configuration to allow these devices to access the platform.
Go to **Device Access Protocol → Access via ONVIF Protocol / Allow ISUP Registration** to allow devices to access the platform via the ONVIF protocol or ISUP.

Note

- Enabling ONVIF may increase security risks. Use it only in isolated networks with protection.
- After enabling or disabling **Allow ISUP Registration**, the Server will be restarted.
- Only ISUP protocol 5.0 is supported.

Configure WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for the client to access WAN.
Go to **WAN Access** and enable the button.

1. Fill in SYS Network Addresses
   - For single NIC environment: You can only configure one network address. The interface will display this as .
   - For dual NIC environment: You can configure different network addresses for system services. The interface will display this as **SYS Network Address**.

     Note

     In a dual NIC environment, ensure that both the SYS network address and the Recording Server network address are on the same network domain, and that the SYS NIC and the Recording Server NIC are also on the same network domain.
2. Select Application Scenarios
   You can select one or more application scenario(s).
3. Configure Mapping Port
   Configure the mapping port No. for data transmission.
4. Click **Save** or click **Export** to export an Excel file about the port information for WAN configuration, including port name, LAN port, WAN port, protocol, etc.

Note

When changes to the LAN port occur, it is necessary to adjust the port mapping configuration on the router correspondingly.

Configure NIC Settings

You can select the NIC of the current Server (SYS NIC) for receiving the alarm information of the device connected via ONVIF protocol, and performing live view and playback for the devices connected via ISUP, as well as the system storage NIC for the data transmission for the storage of video, pictures, and files.
Go to **NIC Settings**.

Reset Network Info

When system network domain changes (such as server migration), you must reset the network information of the added device to adapt to the new network environment. Otherwise the live view or playback will be affected.
Go to **Reset Network Information → Reset** .

14.4 Use SSL/TLS Certificate for HTTPS Connections

To ensure that the client connects only to trusted servers, HikCentral Mini Cube supports server certificate validation, preventing connections to untrusted server addresses and thereby securing the communication channel. The system offers three certificate validation modes to meet security requirements in different scenarios:

Maximum

Only allows connections to servers with public certificates issued by a trusted Certificate Authority (CA) or PKI certificates built by users. In this mode, servers using self-signed certificates will be rejected by the client, ensuring the highest level of authentication and security. When users attempt to connect to a system with an invalid certificate or a mismatched hostname, a warning message will be displayed.

High (Recommended)

The Server can use only self-signed certificates.

If users try to connect to the Server via a domain name, the domain name should be added as a custom server.

Basic

No certificate validation is performed when connecting to a server. The system connects directly without displaying warning messages. However, disabling validation is not recommended, as certificate validation is an essential part of system security hardening.

Step 1 Get Your SSL/TLS Certificate

As a digital certificate issued by the Certificate Authority (CA), the SSL/TLS certificate secures all types of information transferred to and from the server and proves the identity of the server owner. Compared with the platform provided certificate, the SSL/TLS certificate has a higher security level.

Note

The SSL/TLS certificate is purchased from a certificate authority.

1. Choose a CA that you trust.
2. Generate a certificate signing request (CSR) and a private key.
   There are multiple methods to generate a CSR and a private key: via Microsoft IIS, OpenSSL, or a trusted website.
3. Send the generated CSR to the CA to get the authorized SSL/TLS certificate.

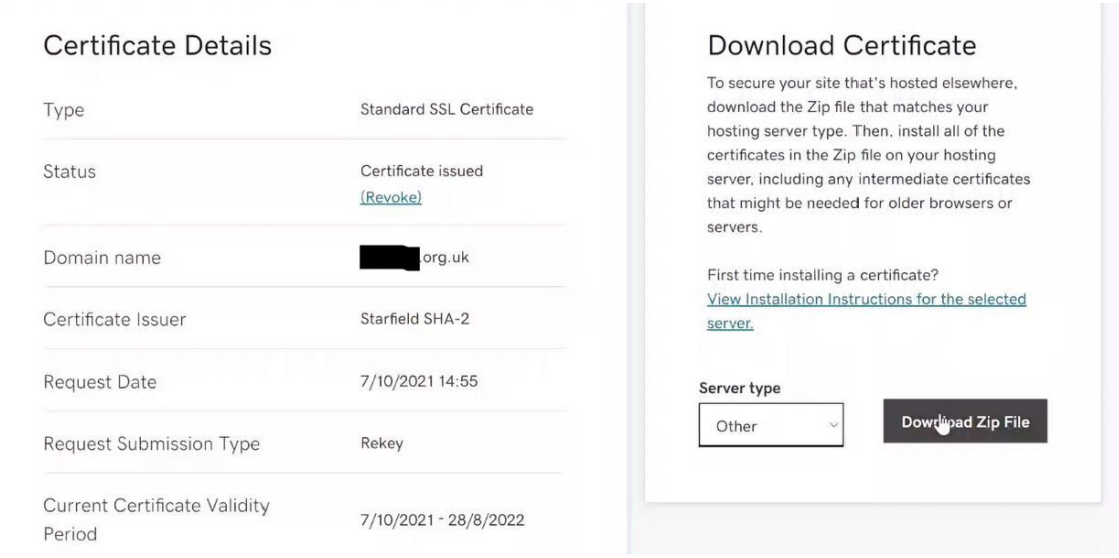


Figure 14-3 SSL/TLS Certificate Example

4. Download your SSL/TLS certificate to your local PC.
   Make sure that the certificate is in PEM format. You can try to edit the file extension to ***.pem*** or use a tool to convert its format to PEM.

Step 2 Upload Your SSL/TLS Certificate to the System

1. Check your SSL/TLS certificate.
   Generally, the issued SSL/TLS certificate contains the certificate file in PEM format, certificate chain in PEM format, and certificate file in other formats (such as CRT and PLCS-7).
2. Get the certificate file in PEM format, the private key which is generated together with the CSR, and the certificate chain in PEM format. And concatenate them into one PEM file in order.
   You can use the CertTool provided by Hikvision to concatenate a certificate. (Tool download address: ***https://www.hikvision.com/en/support/download/software/hikcentral-professional-v2-6-0/*** .)

Note

- The PEM file encoding method should be UTF-8.
- The order of contents in the PEM file should be certificate file -> private key -> certificate chain.

```
-----BEGIN CERTIFICATE-----
MIIGbzCCBVegAwIBAgIMUIt4TGOLEB4xyfNBMA0GCSqGSIb3DQEBCwUAMFAxCzAJ
tAqm/TgWlV8dwim1wc6t525+Hrl3lOnHA3FF78cwWMl5x5dNKhwf632dxMQz4IpB
8XMkRHge9AIdnlVMp2HUB7iOZW3K4Cv9O/YCwuHsnnFCibwWpXZUY2KSi521RxBJ
0/gC3Cr/WyI5fRzHqnrxnHmEqQ==
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEApG3HSjP4zoyFCii+Ct2f7501VmzdnYdxEVqBdQtMie27pJk6
G4e5YQKBgCE/n8nqGm9spvRz6GW59tboV8eByZePkyn+8ydv4VeSgL9q5uTbHKTQ
N9VTTuYxmAyUQ46EDWKhAU5445uEUFSbY6X+77zPEvuNpqUSdsEsOjm9s4XmpibK
ptsahzxpzPKCKa1nN2nnGpvJ60ailfEMYzP5zMNiEQPbtEZ734yR
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIHAjCCBOqgAwIBAgIQBeEL6xHDBPMqVc/6KaEe1jANBgkqhkiG9w0BAQsFADBx
MQswCQYDVQQGEwJVUzErMCkGA1UEChMiVml0YWx3ZXJrcyBJbnRlcm5ldCBTb2x1
0y3ryvnRPxtYleAljYaHoa08klpIbWlOUZHL5T4DTFj6ko0J15MjGSTOanrvme52
oVOgwRlGPAUBRQyqbNA/N5PgYvnbYnP+3zLjV2fcsTQd9Ryk7ulSbK5ZTjds3PCC
Z/aCk1NiNYigUKZmFSniwaFMpojLdiBmKZjgepFJxMTiITr8ZqBG+lkJSZB88POf
AAyK5ka+CpCndiSV/gQnsMagCmeyhw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIF4DCCBMigAwIBAgIQAtzIUa9xYrr53z9V1ROxXjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
FrgGtfX1rKPst8yZpX6jBLHy5eUUGJmG3VCGWRDrri1lWSajBC6RffzR7vzb0/wB
QOXi74AB8YHtYlzmjGGA7IY5Mjdur4CgcUWPlopqn4lgPvzRdRDvD01g3rvpF/ma
ySyHlhO/+GHWldxQRb0QdhxyF4g=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
-----END CERTIFICATE-----
```

Figure 14-4 Example of Concatenated Certificate

3. On the top of the Desktop, click **System → System Configuration → Security → Certificate Management** .
4. Select **Maximum** as the Security Requirements for Certificate.
5. In the Upload Certificate area, click to upload the concatenated certificate.

Note

The Desktop will restart automatically when the certificate is uploaded.

6. (Optional) In the Upper-Level Certificate section, you can click **Add** to upload the certificate chain to the server.
   The invalid or incomplete certificate chain of operating system will result in SSL/TLS certificate verification failure. In this case, users can download the certificate chain, convert it to CRT format, and double-click to install it on their PCs.

14.5 Configure Service Component Certificate

For data security, before adding the Streaming Server, you should generate the service component certificate stored in the Server and input the certificate information to the Streaming Server you want to add, so that the certificates of the Streaming Server and the Server are the same.

On the Home page, go to **System → System Configuration → Security → Service Component Certificate** .

Certificate between Services in System

Required certificate when adding the streaming server.

Click to follow the specific instructions. You can enter the admin password to view or copy the certificate or generate a new one.

After completing the service component certificate, see ***Add a Server and View Server Details*** for further operations on adding the streaming server.

14.6 Privacy and Security

Click **System → System Configuration → Security → Privacy and Security** .

User Experience Improvement Program

Enable this to report your operation logs and software usage data to us. These data is only used for product enhancement. Once the system is connected to the Cloud, the system will start reporting these data. You can disable it if necessary.

Chapter 15 Maintenance

Maintenance is responsible for the real-time monitoring of devices and servers. This ensures swift response to alerts and efficient issue resolution for enhanced security and operations.

In this chapter, detailed information about ***Generate and Display Maintenance Report*** , ***Search for Notifications*** , and ***Search for System Logs*** is provided.

15.1 Generate and Display Maintenance Report

The maintenance report automatically monitors the system and its resources in real time for any exceptions. You can add and display the maintenance report for all device types, video devices, access control devices, security control panels, visitors, and servers.

Generate Maintenance Report

Navigate to the Home page, right-click **Statistics** in the Resource Panel and click **Add Statistics Report**.

Select statistics type as **Maintenance** and customize the **Statistics Name** for the selected **Device Type**.

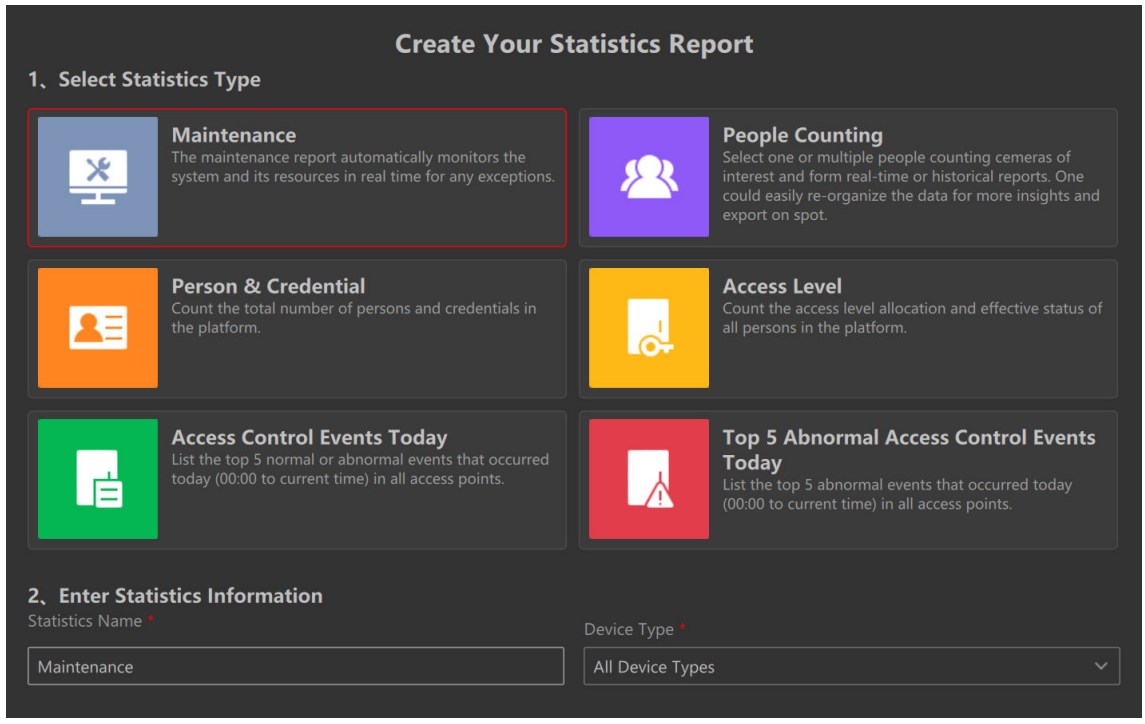


Figure 15-1 Generate Maintenance Report

Display Maintenance Report

After adding the maintenance report(s), click to see the statistics report list and double-click the maintenance report to view details.
The styles of reports displayed can vary across different device types. See below for details.

Note

- You need to restart the SYS before the statistics for the NIC, disk, storage location, and video storage are displayed.
- In the virtual machine environment, the report does not support displaying data for drive C.
- If reports fail to show, first check system logs for disk-related error messages.

All Device Types

The page provides counts for both **Normal** and **Exception** statuses, encompassing all device types, including video devices, access control devices,, security control panels, and servers.



Figure 15-2 All Device Types

You can click to view sever and device details in a normal or an exception status.

- For SYS, you can check CPU usage, RAM usage, NIC traffic, streaming gateway data transfer.

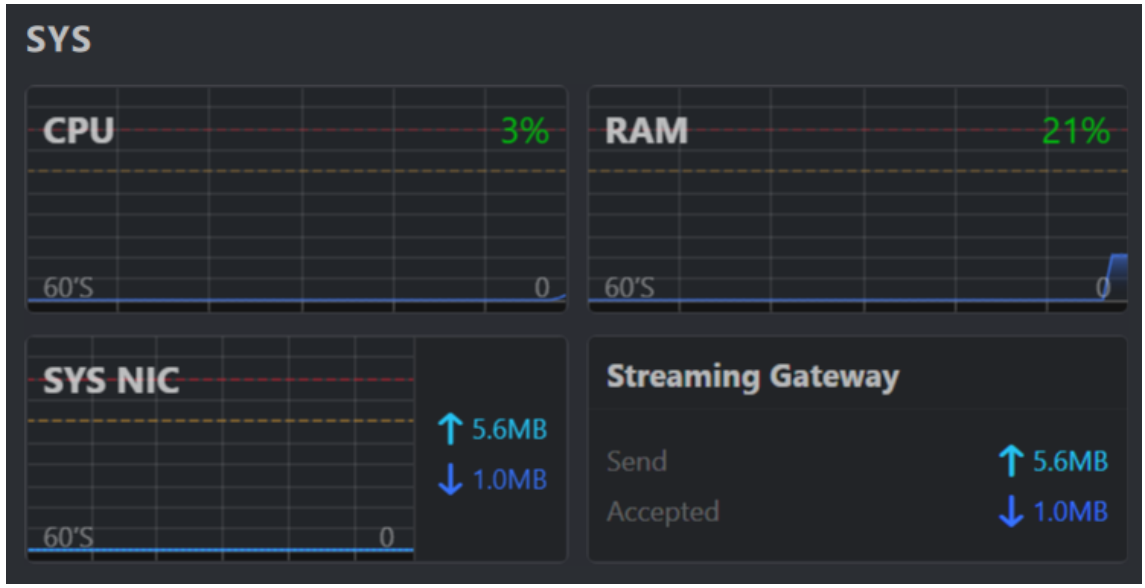


Figure 15-3 SYS

- For Recording Server, you can check NIC traffic, disk I/O, storage location, and video storage.

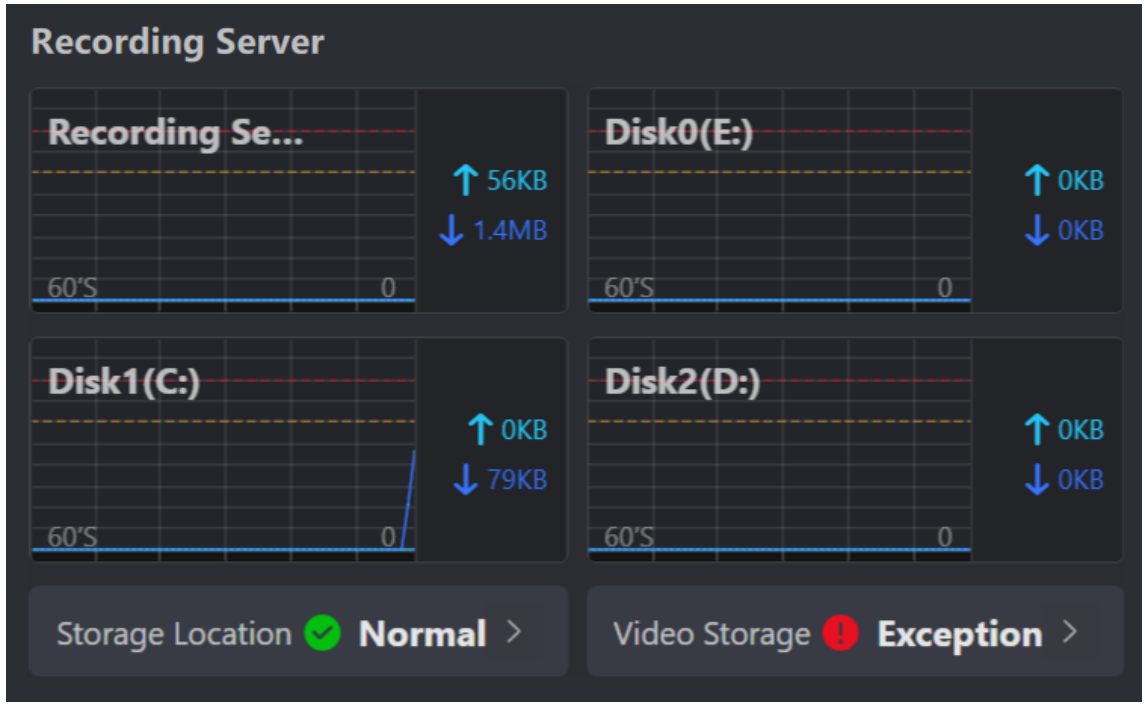


Figure 15-4 Recording Server

- For devices, you will be navigated to the **Device management** page to view exception details.

Video

- Click beside the number to navigate to the device management page. Here, you can inspect detailed information about video devices that are in video loss/recording exception/image exception state.
- Hover on the pie chart to view the number of normal or exception devices.

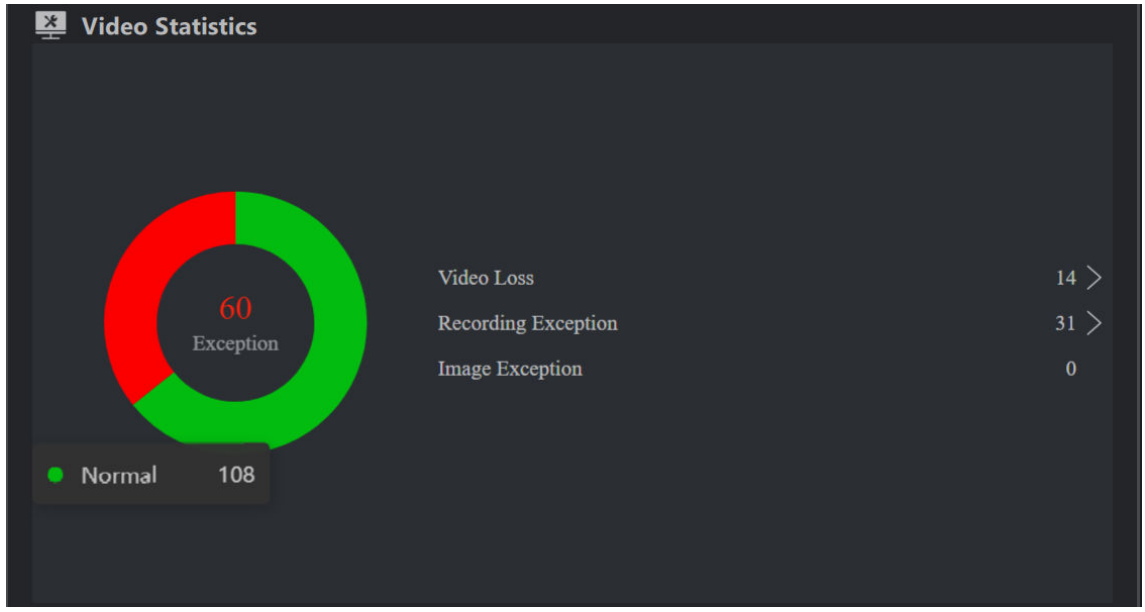


Figure 15-5 Video Statistics

Access Control

- Click beside the number to navigate to the device management page. Here, you can inspect detailed information about access control devices that are in device security exception/device network exception/device record reporting exception/device power battery exception state.
- Hover on the pie chart to view the number of normal or exception devices.

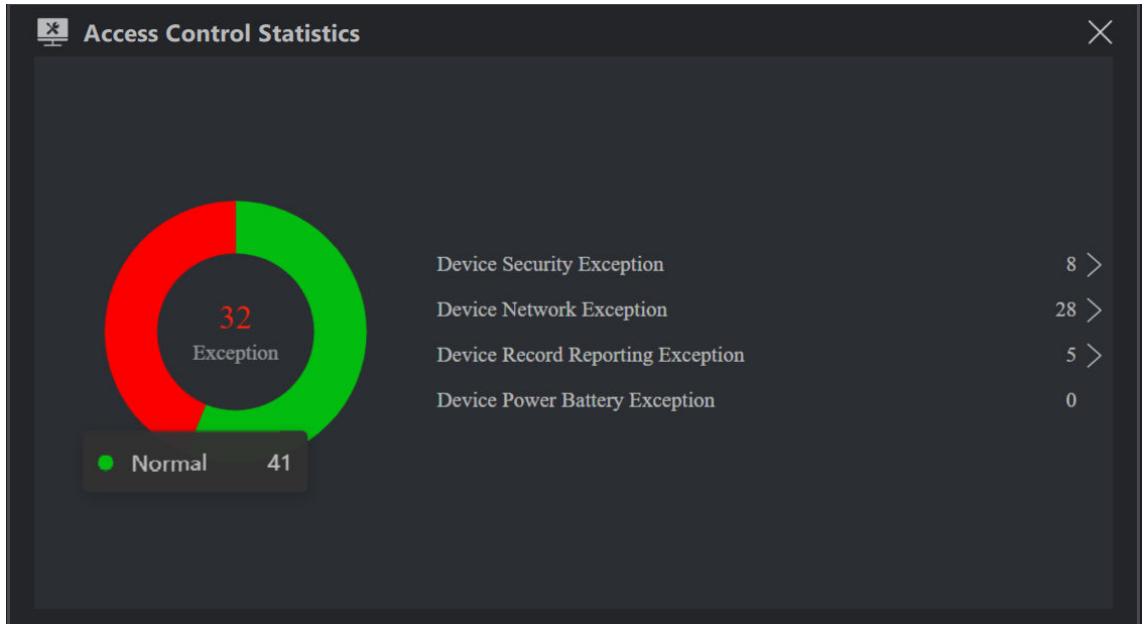


Figure 15-6 Access Control Statistics

Security Control Panel

Hover over the pie chart to view the number of normal or exception devices. Or click the icon next to the number to go to the **Device Management → Alarm Detection** page, where you can view devices in Exception status.

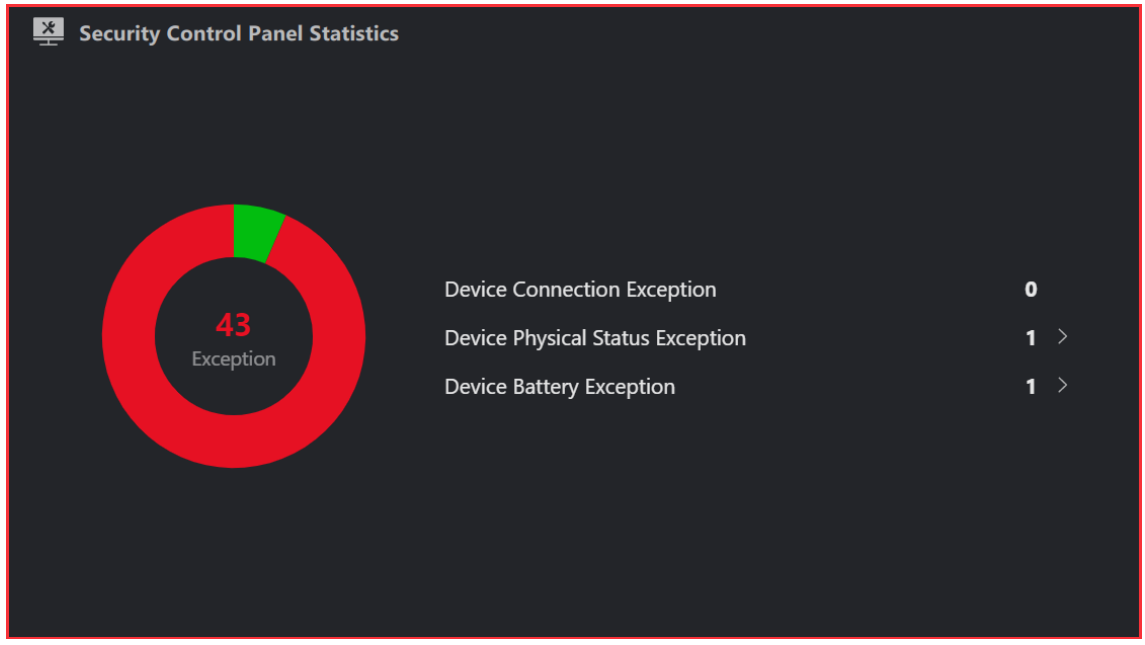


Figure 15-7 Security Control Panel Statistics

Server

Provides an overview of SYS and Recording Server, including CPU usage, NIC traffic, disk I/O, etc.

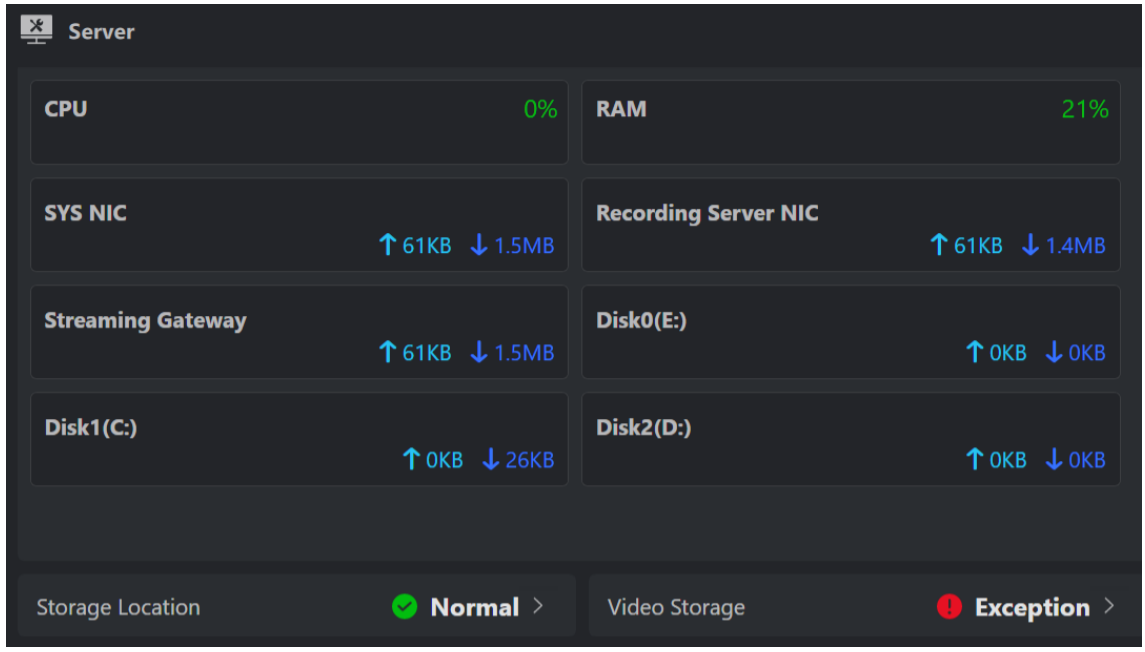


Figure 15-8 Server Statistics

Visitor Statistics

Provides statistics on pending visitor applications, the number of scheduled but unvisited visitors, entries (today), and current visitors (today).

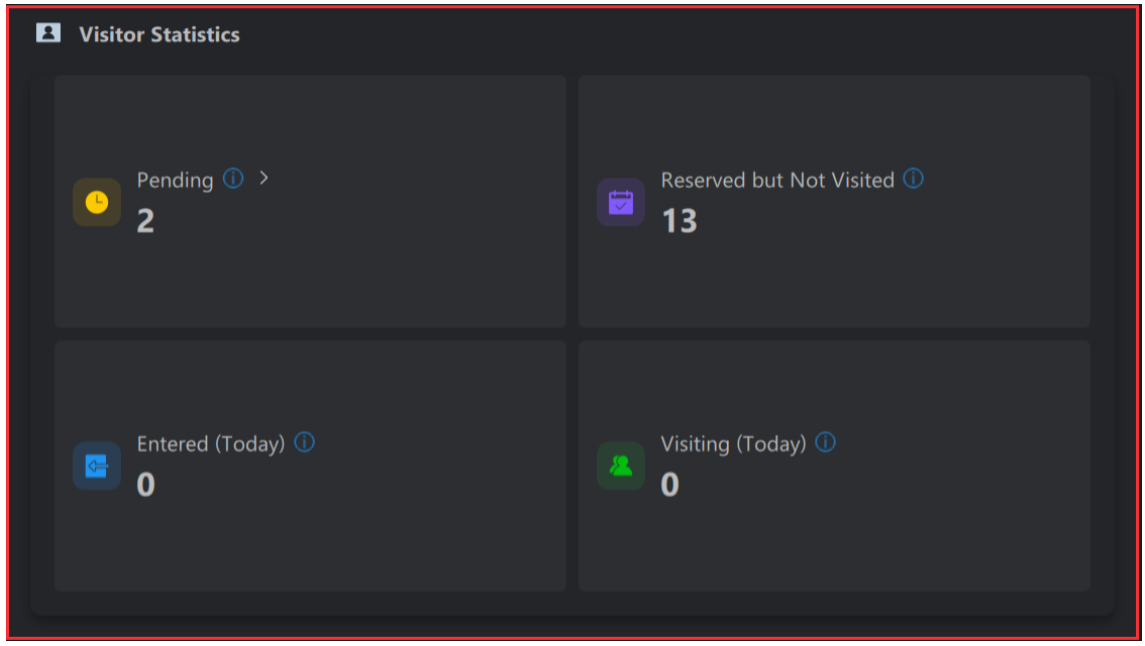


Figure 15-9 Details

15.2 Search for Notifications

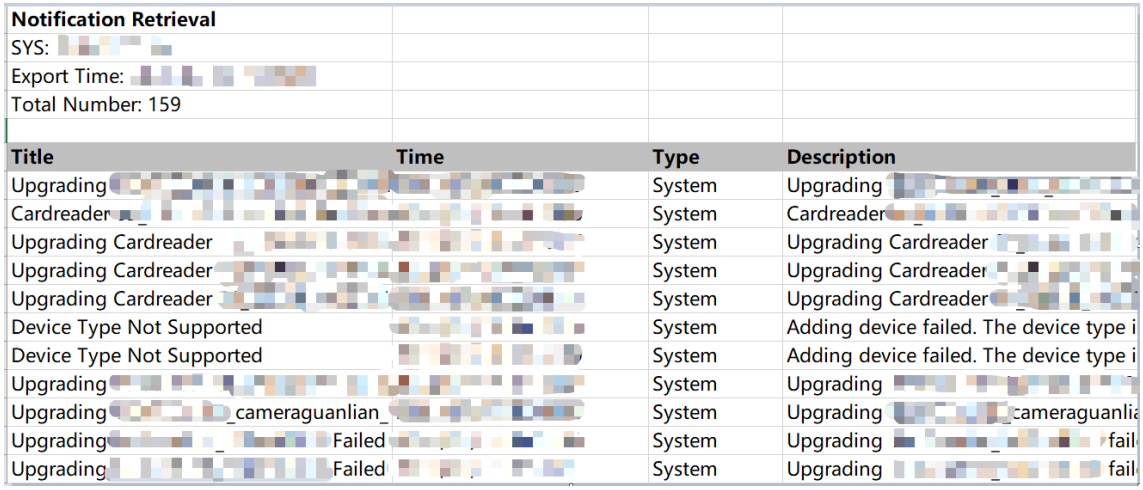
You can search for notification information to promptly detect and respond to alerts or updates, ensuring swift action on security incidents.

On the Home page, go to **Investigation → Notifications** .

You can filter the information by selecting **Date** and **Notification Type**. These notifications primarily consist of:

- System-related alerts, such as "device type not supported".
- User operation prompts, such as "calling video intercom not answered".

Based on the filter criteria you set, click **Export** in the upper-left corner to export notification files to **Excel**, **PDF**, or **CSV** formats.



Notification Retrieval			
SYS:			
Export Time:			
Total Number: 159			
Title	**Time**	**Type**	**Description**
Upgrading		System	Upgrading
Cardreader		System	Cardreader
Upgrading Cardreader		System	Upgrading Cardreader
Upgrading Cardreader		System	Upgrading Cardreader
Upgrading Cardreader		System	Upgrading Cardreader
Device Type Not Supported		System	Adding device failed. The device type i
Device Type Not Supported		System	Adding device failed. The device type i
Upgrading		System	Upgrading
Upgrading _cameraguanlian_		System	Upgrading cameraguanli
Upgrading Failed		System	Upgrading fail
Upgrading Failed		System	Upgrading fail

Figure 15-10 Notification Retrieval Excel Template

15.3 Search for System Logs

You can search for server and/or device logs to promptly identify and address issues, enhancing the efficiency of incident response. Server logs and device logs respectively refer to the logs generated by the server that are stored on the server and the logs stored on the device.

Access is available via two options:

To search server logs and device logs

On the Home page, go to **Investigation → System Log** .

To search local device logs

1. On the Home page, go to **System → Device Management** .
2. Hover on one device then right-click and select **View Log** to search local device logs.

Note

- This feature should be supported by the device.
- You can also view logs when viewing device details. On the Device Details page, hover on one device then right-click and select **View Details**. Click **View Log** in the upper-right corner.

For Server Log

- You can filter the event type by **Information**, **Warning** and **Error**. For instance, an Information event could be an Add Generic Event notification, a Warning could indicate a License Expiration, and an Error could signify a Door Lock Failure.
- Click **Resource Name** to quickly search the resource.
- Click **Export** in the upper-left corner to export server log in **Excel** or **CSV** file.

Server Log

Basic Information

Export Time:
Operator: admin
Export Content: Data
Report Time:
Total Number: 5671

Level	Time (Client)	Source	Event	Resource Name	Area
Information		admin	Add View	New View 1	
Information		admin	Start Live View	_8000	HikCer
Information		admin	Start Live View	_8000	HikCer
Information		admin	Start Downloading Video File	3686	keliu N
Information		admin	Start Downloading Video File	IPCamera 01	keliu N
Information		admin	Search Notification Record		
Information		admin	Start Downloading Video File	6825	keliu N
Information		admin	User Login		
Information		admin	User Logout		
Information		admin	Delete Encoding Device		
Information		chenqi	Search Alarm Log		

Figure 15-11 Server Log Excel Template

For Device Log

Click **Export** in the upper-left corner to export device log in **Excel** or **CSV** file.

Encoding Device Operation Log

Basic Information

Type:Encoding Device Operation Log
Exporting Time:
Searched by:admin
Report Time:
Total Number:9607

Level	Device Time	User	Event	Channel No.
Information			Online	
Exception			Offline	
Operation		admin	Remote: Get Status	0
Operation		admin	Remote: Get Status	0
Operation		admin	Remote: Get Status	0
Operation		admin	Remote: Get Status	0
Operation		admin	Remote: Get Status	0

Figure 15-12 Device Log Excel Template

Appendix A. Product Usage Restrictions: Scenarios & Guidelines

This topic provides restricted scenarios for the system to help users avoid unintended misuse. It serves as a quick reference for verifying permitted activities across specific use cases.

System

- When you run the client as Administrator, importing data into the system may fail.
- Microsoft Office shall be installed in order to view exported excel files.
- Do not drag the client across screens with varying DPI settings, as this may result in unintended UI scaling issues. Specifically, if your computer is connected to multiple monitors with different DPI scaling (e.g., Monitor A at 150% and Monitor B at 200%), moving the client window between them may cause subsequent pop-up windows to appear offset or mispositioned.
  To ensure the best experience, we recommend enabling high DPI compatibility for the client:
  1. Right-click the desktop client shortcut and go to **Properties → Compatibility → Change high DPI settings** .
  2. Check the box for **Override high DPI scaling behavior** and select **System** from the drop-down menu.
  3. Click **OK** to save the settings, then restart the client.
- Make sure the available disk space is no less than 10 GB to avoid the installation failure of the Server.

Device Management

- Cameras containing special characters including \ / : * ? " < > | in their names cannot be imported.
- For ISUP devices performing FTP-based firmware upgrades, the maximum supported path length for upgrade packages is limited to 32 bytes.
- Be careful to remove information imported from iVMS-4200, because information removed from the system cannot be imported again.
- When importing configuration files from iVMS-4200, device offline events cannot be imported.
- When editing device password on the Web page, stop live view and playback on all clients, and change the password on the device list as quickly as possible. Try to change device password via the system instead of the Web page.
- The urban road ANPR camera iDS-TCM403-GIR cannot be added to the platform as a channel of an NVR via ISUP protocol. Instead, you can make it via SDK protocol. And this model only supports campus speed detection.

Video Monitoring

- When using AcuSearch, if an incorrect prompt pops up, you can check whether this function is enabled on the device configuration page.
- Do not arbitrarily modify whether the device's stream is encrypted or the specific encryption keys.
- Do not use smooth stream and stream encryption simultaneously.
- For devices configured with dual-stream recording schedule, main stream will be used when playing videos.
- Starting recording manually is not supported during live view via smooth stream.
- Live view via smooth stream is not supported for devices added by Hikvision ISUP Protocol.
- Live view is not supported on the remote configuration page of Bi-spectrum Thermography Speed Dome Series cameras.
- When DS-7616NXI-K2/16P series NVRs are connected to the platform with DST enabled, recording retrieval inaccuracies may occur during DST transition periods (when entering/exiting DST), and timeline jumps might appear during playback due to local time adjustments (e.g., clock shifts forward/backward by 1 hour).
- If connected devices do not support UTC time, when using search functionalities (AcuSeek/ video retrieval / Smart Search / all searches via NVR) during Daylight Saving Time (DST) transitions, the system cannot distinguish duplicate time periods (e.g., 01:30 appearing twice when DST ends). All search results will display local device time without UTC offset adjustments. For real-time events & alarms (Alarm Log Retrieval) based on devices without UTC support, duplicate timestamps may appear during DST exit periods (e.g., two entries showing "01:30").
- For live view and playback via Axis and Hanwha devices, make sure you have selected H.264 as the encoding format.
- Reverse playback of videos stored in Axis, Dahua, or Hanwha devices is not supported.
- No more than 12 views supports synchronized playback simultaneously.
- To enlarge a fisheye-expanded image, double-click the image before enabling Fisheye Expansion.
- Two-way audio via channels of DVR is not supported.
- When drawing people counting detection areas, only rectangular area is supported.
- Devices added by Hikvision ISUP Protocol does not support live view, playback, or two-way audio via IPV6.
- For cameras managed via an NVR/DVR, the system cannot get their presets.
- Videos in AVI format may fail to be played by Windows-provided players, so free-charged players that support all video formats is recommended.

Access Control and Video Intercom

- When importing the zip file of profile pictures, make sure the system language of the PC compressing profile pictures is the same with the system language of the Server.
- Two-way audio is not supported by access control devices or video intercom devices added by Hikvision ISUP Protocol even if the devices have the capability of two-way audio.

Appendix B. Third-Party Device Integration

The **Axis** add-on supports adding Axis devices via private protocols. After adding the devices, users can start live view or playback, configure and receive events and alarms, monitor device status, etc.

The Axis add-on supports the following:

- Live view (only main stream supported)
- PTZ control: zoom in and zoom out
- Local playback on network camera
- Capture pictures (thumbnails and alarm linkage)
- Retrieve recording schedules from the device
- NTP time synchronization
- Go to the device's web page

The **Dahua** add-on supports adding Dahua devices via private protocols. After adding the devices, users can start live view or playback, configure and receive event and alarms, monitor device status, etc.

The Dahua addon supports the following: .

- Retrieve recording schedules from the device
- NTP time synchronization
- Sync camera names to the platform
- Go to the device's web page

The **Hanwha** add-on supports adding Hanwha devices via private protocols. After adding the devices, users can start live view or playback, configure and receive events and alarms, monitor device status, etc.

The Hanwha addon supports the following:

- Live view (only main stream supported)
- PTZ control: basic operation, zoom in and zoom out, and preset related operations
- Normal playback on network camera and NVR
- Retrieve recording schedules from the device
- NTP time synchronization
- Sync camera names to the platform
- Calendar search
- Go to the device's web page

B.1 Add Third-Party Devices

You can add **Axis** network camera(s) by batch import or manually add by **Axis SDK Protocol**.

Axis Devices are accessed via VAPIX Version 3 of 2024-10-25.

Full Tested Device: Network Camera (IPC): AXIS M3086-V

You can add **Dahua** encoding devices by batch import and manually add by **Dahua Private Protocol**.

Table B-1 Supported Dahua Device Type

Device Type	Device Model
Digital Video Recorder (DVR)	DVRxx04HF, DVRxx04LF, DVRxx04LE, DVRxx04HE, DVRxx04HG, DH-DVRxx04FG, 3104, 3108, 3116
Hybrid DVR	DVRxx04HG-U, DVRxx04FG-U, DVRxx04HF-U, DVRxx04HG-U, LE, HE
Network Video Recorder (NVR)	NVR3204/08/16, NVR3204/08/16-P, NVR3804/08/16/32, NVR3808/16/32-E, NVR3204/08/16V, NVR3204/08/16V-P, NVR4432-HDS2/L
Network Camera	IPC-HF3211-I, IPC-HF3100, HF3200, HF3300, HF3500, HF3110, IPC-HFW3110, HFW3300, HFW3300C, HFW3200C, HFW3100C, HFW3101C IPC-HDB(W)3300, IPC-HDB(W)3110, IPC-HF2100, IPC-HFW2100, IPC-HFW2100BP, IPC-HFW3100, IPC-HD2100, IPC-HDB3100C, IPCHDB3200C, SD6220

Devices other than these mentioned, if compatible with Dahua's proprietary protocol, inherently support integration.

You can add **Hanwha** encoding devices by batch import or manually add by **Hanwha SDK Protocol**.

Hanwha Devices are accessed via SUNAPI_2.6.1.

Full Tested Devices:

- Network Camera (IPC): ANV-L7012R
- Network Video Recorder (NVR): QRN-1620S

Note

- The availability of features varies depending on the device model and its implementation.
- For devices accessed via third-party SDK protocols, the selected time zone cannot be automatically applied to the devices. Manual configuration is required (Go to **Device Management → Time Zone**).

B.2 Video Monitoring

You can start live view or playback of one or multiple cameras. The supported functions are listed below.

Table B-2 Basic Functions Supported by Axis Add-on

Function	Live View	Playback
Open in New View	√	√
Enable Digital Zoom	√	√
Capture	√	√
Export	×	√
Start Recording	√	×
Enable PTZ Control	√	×
Video Enhancement	√	√
Video Overlay	√	√
Camera Settings	√	√

Table B-3 Basic Functions Supported by Dahua Add-on

Function	Live View	Playback
Open in New View	√	√
Enable Digital Zoom	√	√
Switch Stream Type	√	√
Capture	√	√
Export	×	√
Start Recording	√	×
Enable PTZ Control	√	×
Video Enhancement	√	√
Video Overlay	√	√
Camera Settings	√	√

Table B-4 Basic Functions Supported by Hanwha Add-on

Function	Live View	Playback
Open in New View	√	√
Enable Digital Zoom	√	√
Switch Stream Type	√	√

Function	Live View	Playback
Capture	√	√
Export	×	√
Start Recording	√	×
Enable PTZ Control	√	×
Audio On/Off	√	√
Video Enhancement	√	√
Video Overlay	√	√
Camera Settings	√	√

B.3 Supported Alarms

Table B-5 Alarms Supported by Axis Devices

Specific Event
Camera Online / Camera Offline
Motion Detection

Table B-6 Alarms Supported by Dahua Devices

Specific Event
Camera Online / Camera Offline
Motion Detection
Video Tampering Detection
Video Loss
Camera Recording Exception
Intrusion
Line Crossing
Region Entrance
Region Exiting
Scene Change Detection
Defocus Detection

Table B-7 Alarms Supported by Hanwha Devices

Specific Event
Camera Online / Camera Offline
Motion Detection
Video Loss
Line Crossing
Region Entrance
Region Exiting
Scene Change Detection
Defocus Detection

B.4 Linkage Actions

Triggering recording is not supported.

The Hanwha add-on does not support triggering picture capture by an alarm.

Appendix C. 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.

Appendix D. Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE

PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.


See Far, Go Further