HikCentral Lite V1.1.1

User Manual

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.
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.

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.

Contents

Chapter 1 Learn About HikCentral Lite

The HikCentral Lite 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.

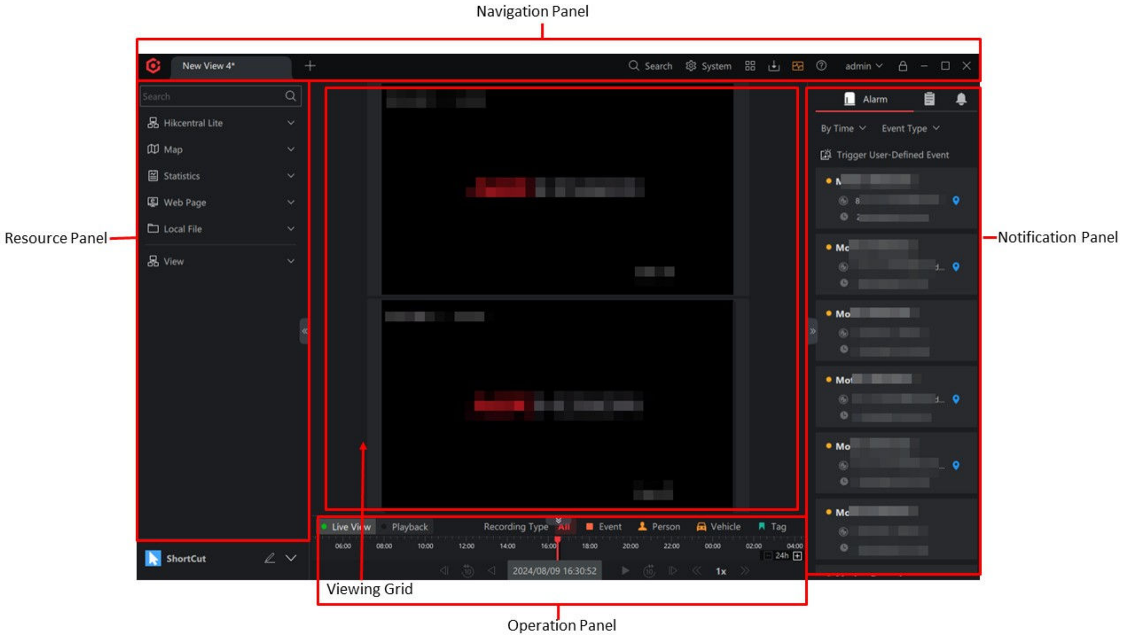
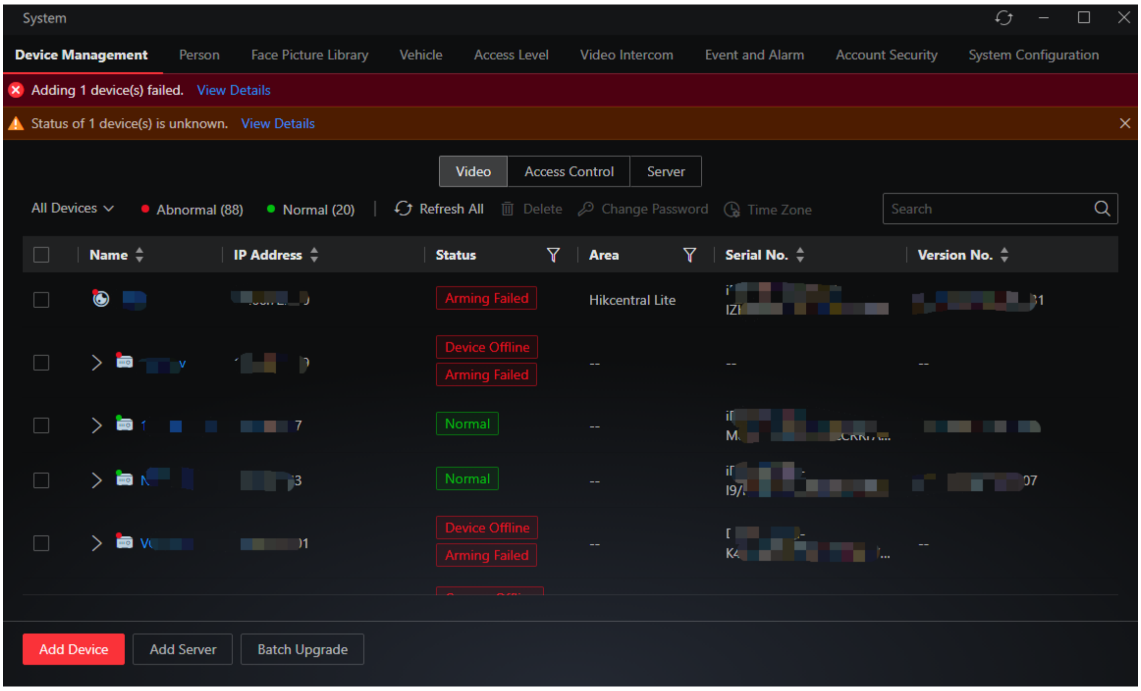


Figure 1-1 Main Page

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



Adding 1 device(s) failed. View Details

Status of 1 device(s) is unknown. View Details

□	Name	IP Address	Status	Area	Serial No.	Version No.
□	[redacted]	[redacted]	Arming Failed	Hikcentral Lite	[redacted]	[redacted]
□	[redacted]	[redacted]	Device Offline Arming Failed	--	--	--
□	[redacted]	[redacted]	Normal	--	[redacted]	[redacted]
□	[redacted]	[redacted]	Normal	--	[redacted]	[redacted]
□	[redacted]	[redacted]	Device Offline Arming Failed	--	[redacted]	--

Figure 1-2 System Window

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 • Microsoft® Windows Server 2012 R2 64-bit • Microsoft® Windows Server 2012 64-bit • Microsoft® Windows 11 64-bit • Microsoft® Windows 10 64-bit **Note** For Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) updated in April, 2014.
Desktop	• Microsoft® Windows Server 2025 • Microsoft® Windows Server 2022 • Microsoft® Windows Server 2019 64-bit

Platform	OS
	• Microsoft® Windows Server 2016 64-bit • Microsoft® Windows Server 2012 R2 64-bit • Microsoft® Windows Server 2012 64-bit • Microsoft® Windows 11 64-bit • Microsoft® Windows 10 64-bit **Note** For Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) updated in April, 2014.
Mobile Client	• iOS 14.0+ • Android 6.0+

1.2 Comparison Between Free and Full Version

This topic shows the differences of HikCentral Lite maximum performance and core features of the full version.

Maximum Performance

Table 1-2 Manageable Resources

Performance	Full Version	Free Version
Total Camera Channels	128 *Includes numbers of AcuSearch cameras, AcuSeek cameras, ANPR cameras, people counting cameras, cameras for face picture comparison & body recognition, and third-party cameras	16
People Counting Cameras	128	0
AcuSearch Cameras	128	0
AcuSeek Cameras	128	0
ANPR Cameras	8	0
Cameras for Face Picture Comparison and Body Recognition	16	0

Performance	Full Version	Free Version
Third-Party Cameras	128	0
Doors	32	2
External Streaming Servers	64	64

Table 1-3 Others

Performance	Full Version	Free Version
Vehicles	2,000	0

Table 1-4 Access Control

Performance	Full Version	Free Version
Persons	500	500
Credentials	Cards: 1,000 Face Pictures: 500 Fingerprints: 1,000 Irises: 1,000	Cards: 1,000 Face Pictures: 500 Fingerprints: 1,000 Irises: 1,000

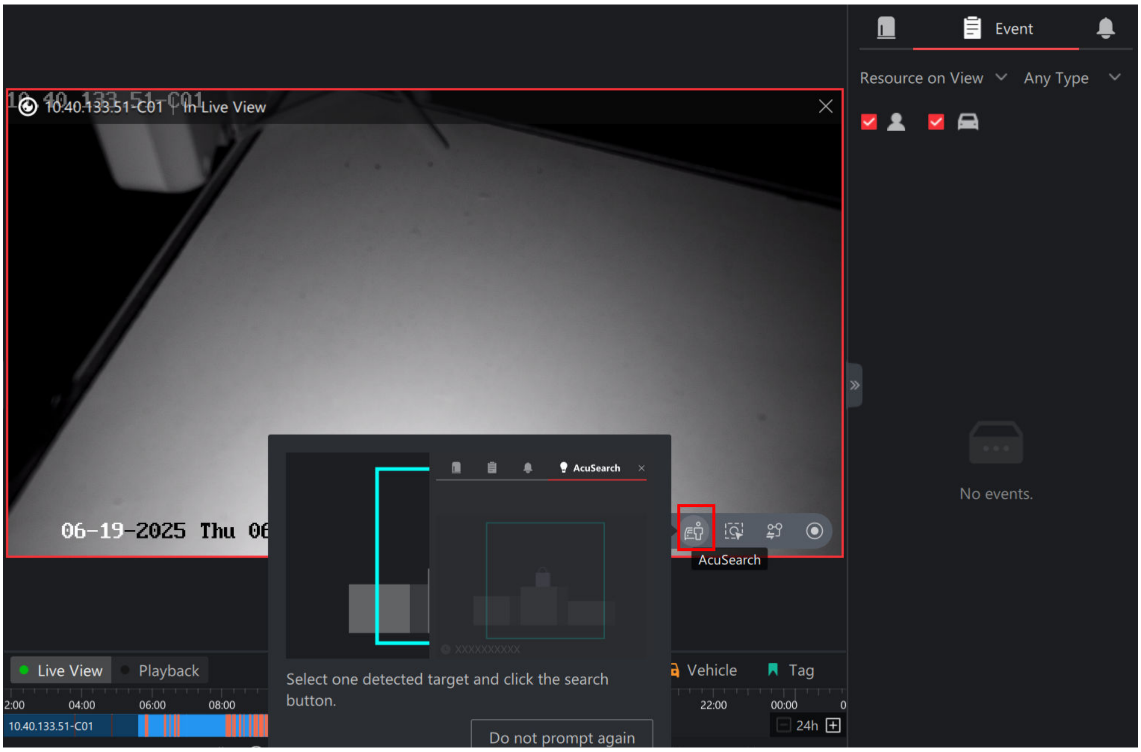
Table 1-5 Users

Performance	Full Version	Free Version
Users	128	128
Roles	64	64
Users Logged In Simultaneously via Desktop	64	3
Users Logged In Simultaneously via Mobile Client	64	3

Core Features

The following features are **available only in the full version**.

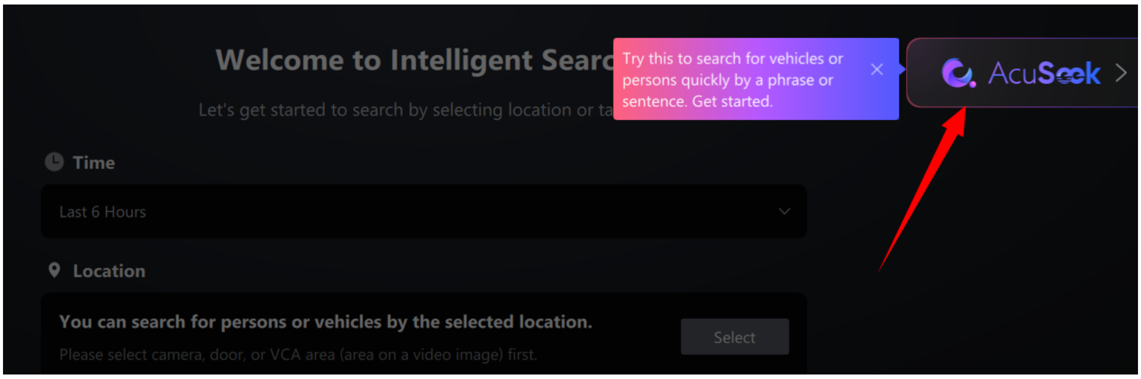
AcuSearch / Object Search



Select one detected target and click the search button.

Figure 1-3 AcuSearch / Object Search

AcuSeek


Welcome to Intelligent Searc
Let's get started to search by selecting location or ta
Time
Last 6 Hours
Location
Select
AcuSeek

Try this to search for vehicles or persons quickly by a phrase or sentence. Get started.

You can search for persons or vehicles by the selected location.

Please select camera, door, or VCA area (area on a video image) first.

Figure 1-4 AcuSeek Entry

People Counting Report

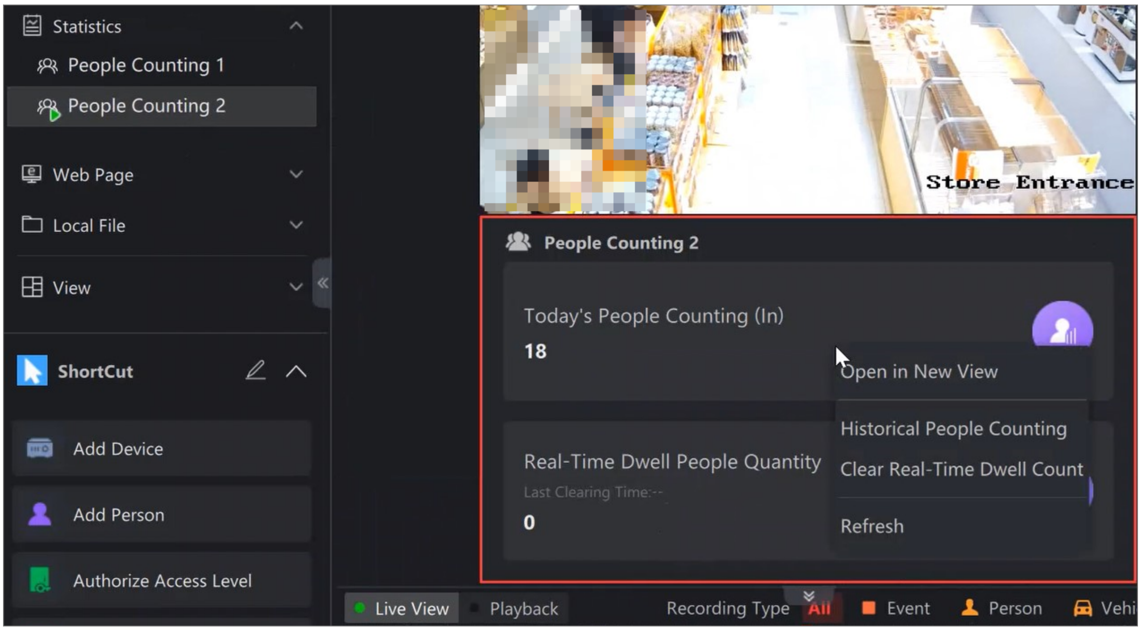


Figure 1-5 People Counting Report

Vehicle Search

- Search for vehicles by features. Go to **Search → Vehicle Passing Event** .

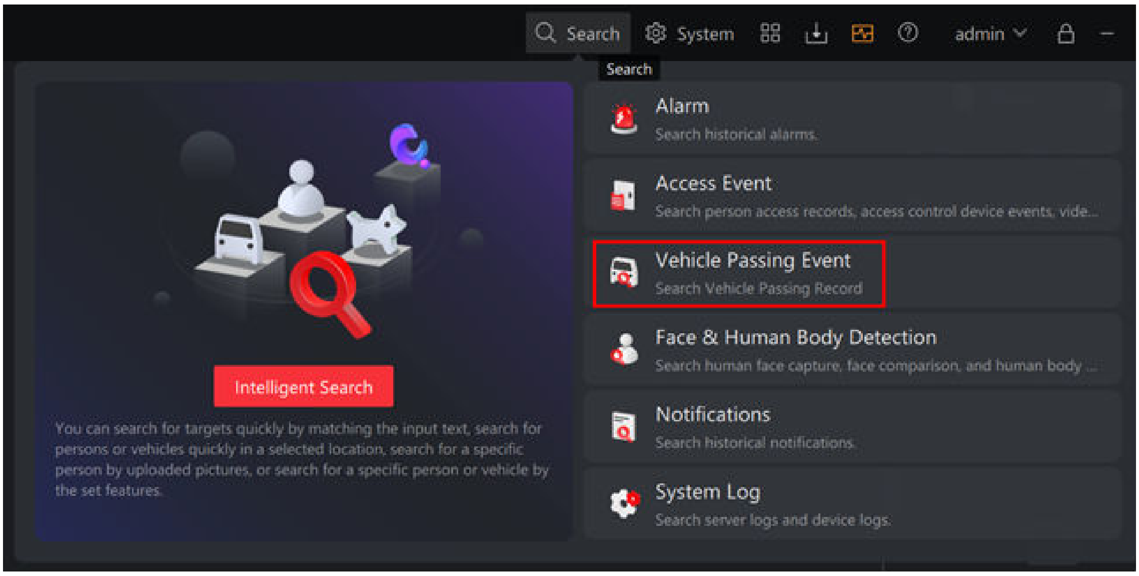
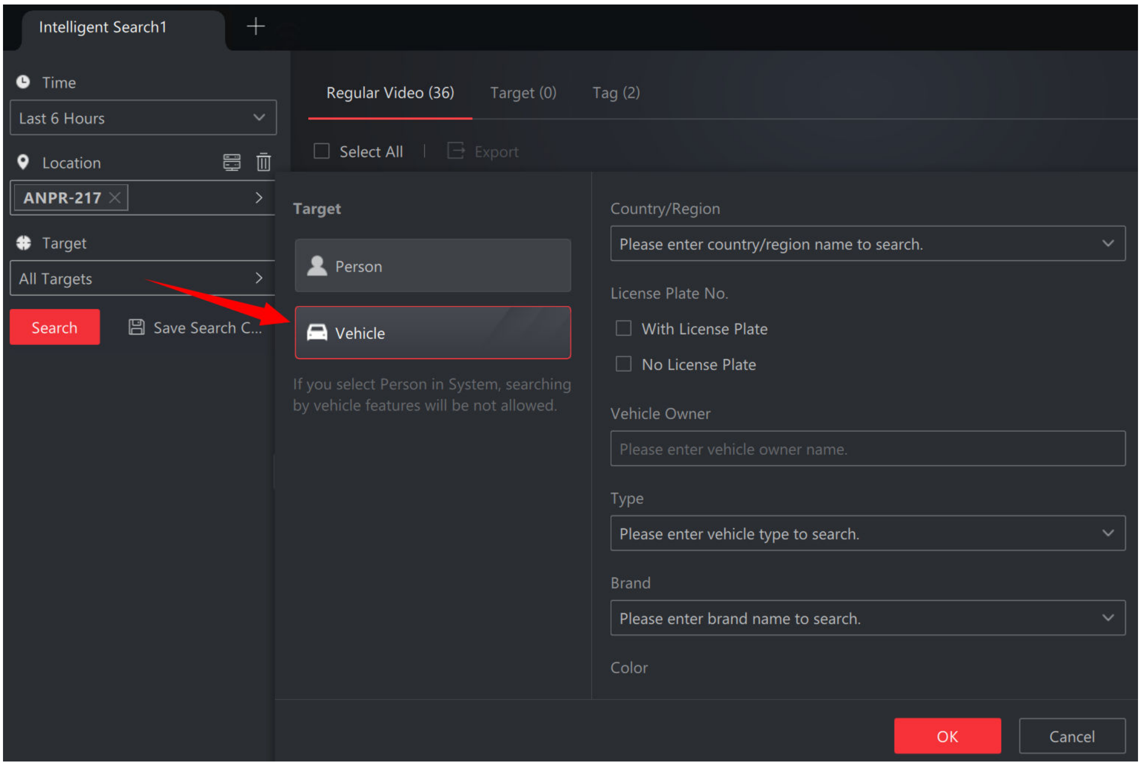

Search
System
admin
Search
Alarm
Search historical alarms.
Access Event
Search person access records, access control device events, vide...
Vehicle Passing Event
Search Vehicle Passing Record
Face & Human Body Detection
Search human face capture, face comparison, and human body ...
Notifications
Search historical notifications.
System Log
Search server logs and device logs.
Intelligent Search
You can search for targets quickly by matching the input text, search for persons or vehicles quickly in a selected location, search for a specific person by uploaded pictures, or search for a specific person or vehicle by the set features.

Figure 1-6 Vehicle Passing Event

- Search for vehicles by features. Go to **Search → Intelligent Search** .



Intelligent Search1

Time: Last 6 Hours

Location: ANPR-217

Target: All Targets

Search | Save Search C...

Regular Video (36) | Target (0) | Tag (2)

□ Select All | Export

Target

Person

Vehicle

If you select Person in System, searching by vehicle features will be not allowed.

Country/Region: Please enter country/region name to search.

License Plate No.

□ With License Plate

□ No License Plate

Vehicle Owner: Please enter vehicle owner name.

Type: Please enter vehicle type to search.

Brand: Please enter brand name to search.

Color

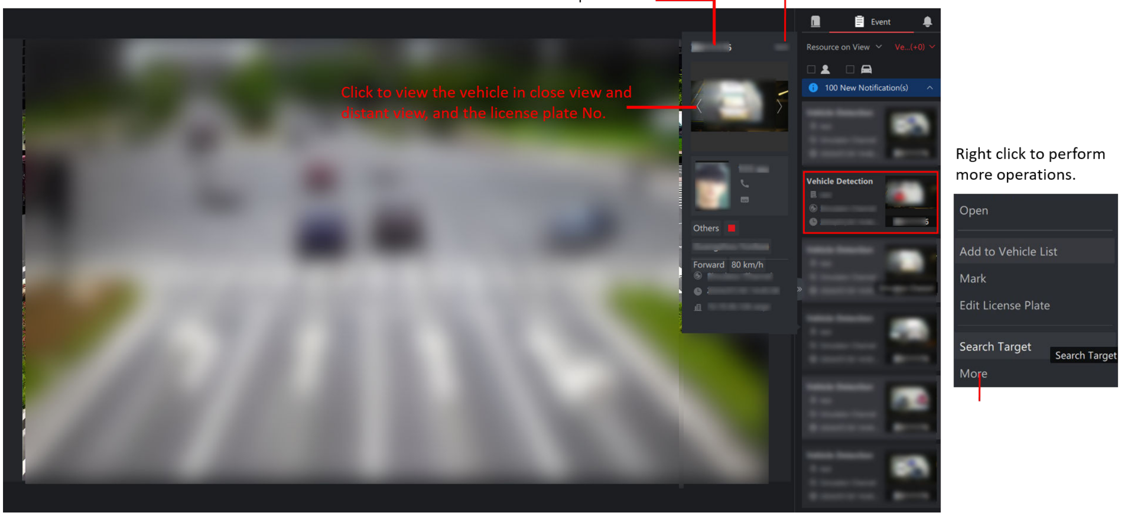
OK | Cancel

Figure 1-7 Search for Vehicles by Features

- Supports license plate No. and vehicle list management if ANPR cameras are added.

View the vehicle list if the vehicle has been added to the vehicle list.

License plate No.

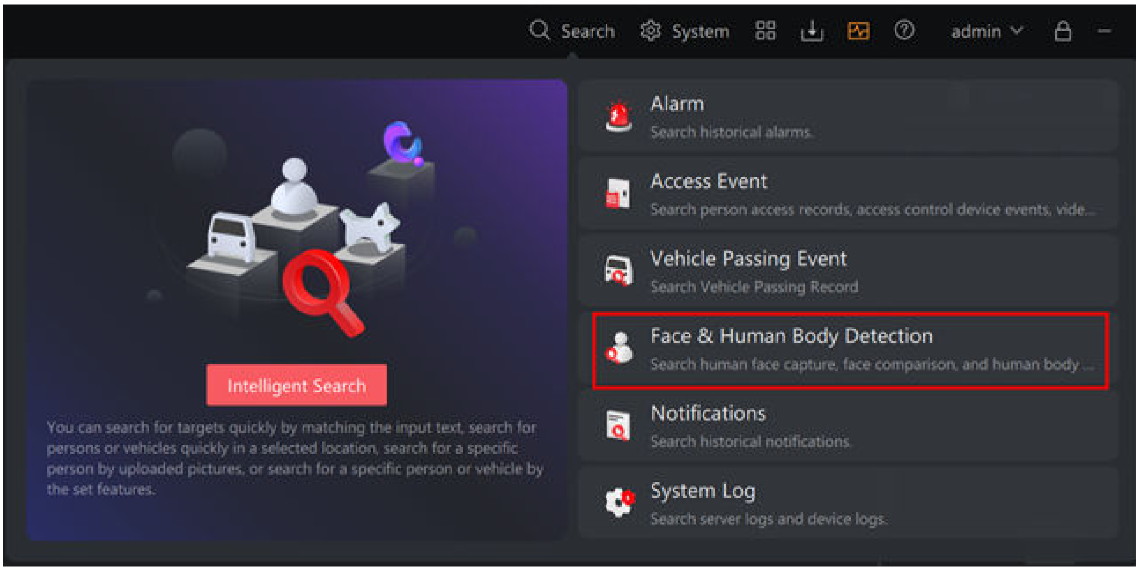


Right click to perform more operations.

Figure 1-8 ANPR Camera

Face Picture Comparison

- Supports searching for persons by features. Go to **Search → Face & Human Body Detection** .



You can search for targets quickly by matching the input text, search for persons or vehicles quickly in a selected location, search for a specific person by uploaded pictures, or search for a specific person or vehicle by the set features.

Alarm
Search historical alarms.

Access Event
Search person access records, access control device events, vide...

Vehicle Passing Event
Search Vehicle Passing Record

Face & Human Body Detection
Search human face capture, face comparison, and human body ...

Notifications
Search historical notifications.

System Log
Search server logs and device logs.

Figure 1-9 Face & Human Body Detection

- Supports searching for persons by features. Go to **Search → Intelligent Search** .

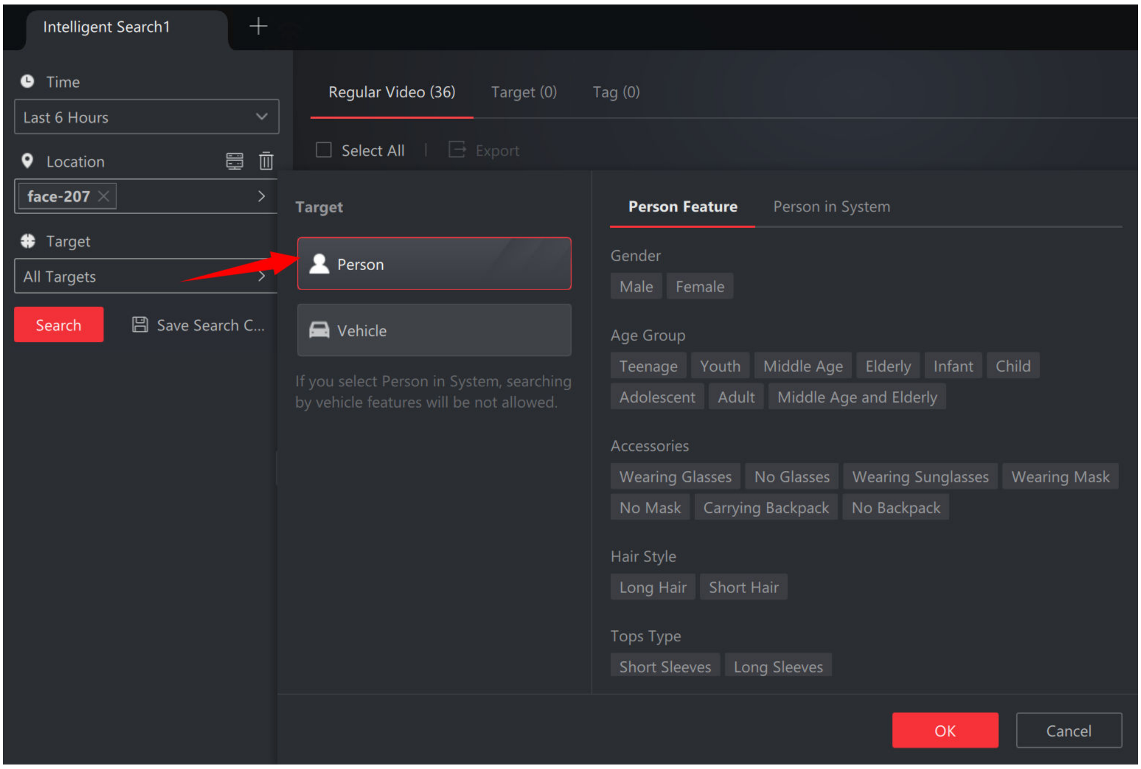
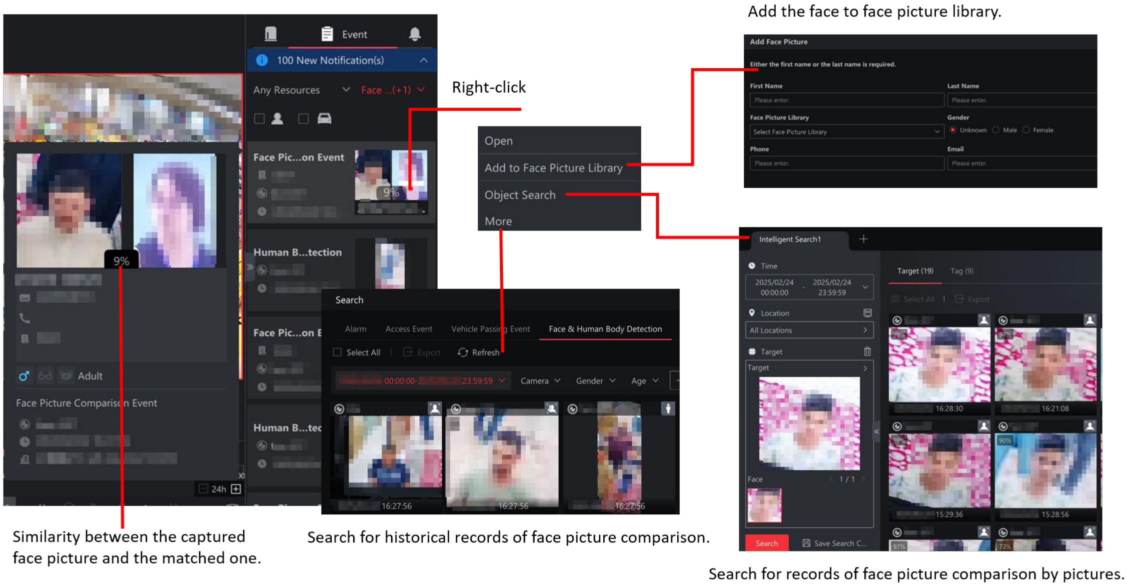


Figure 1-10 Search for Persons by Features

- Supports face picture comparison if cameras for face picture comparison are added and AcuSearch.



Add the face to face picture library.

Right-click

Similarity between the captured face picture and the matched one.

Search for historical records of face picture comparison.

Search for records of face picture comparison by pictures.

Figure 1-11 Camera for Face Picture Comparison

Search by Face/Body Pictures

Supports uploading a picture and setting other conditions to search for the corresponding pictures. You can also right-click on searched pictures to find similar ones.

Server Disk Storage

Supports storing videos on server disks.

Note

The free version supports only pictures and files.

Third-party Cameras

Supports cameras accessed via ONVIF, Dahua, Hanwha, and Axis protocol.

Upgrade to HikCentral Professional

Supports upgrading from HikCentral Lite to HikCentral Professional.

Mobile Client / Desktop

Supports up to 64 concurrent client logins.

Note

The free version supports up to 3 concurrent client logins.

1.3 System Configurations and Performance

The system performance is tested based on the following configurations.

System Configurations

Table 1-6 System Configurations

Feature	Configuration 1	Configuration 2
CPU	Intel® Core™ i5-12500	Intel® Core™ i7-12700
RAM	2*8 GB	2*8 GB
NIC	1 GbE Network Interface Card	1 GbE Network Interface Card
SSD for OS	Enterprise Class SSD	Enterprise Class SSD
HDD for Video Storage	Enterprise-class HDD or high performance network HDD. It should support writing or reading of 10 MB/s.	Enterprise-class HDD or high performance network HDD. It should support writing or reading of 20 MB/s.

Feature	Configuration 1	Configuration 2
SSD Capacity for Database	At least 500 GB	At least 500 GB
OS	Microsoft® Windows 10 64-bit or later	Microsoft® Windows 10 64-bit or later

1.3.1 Detailed Performance

Here shows the maximum system performance.

Manageable Resources

Table 1-7 Manageable Resources

Resource Type	Configuration 1	Configuration 2
Cameras (Including cameras accessed by ONVIF protocol and third-party cameras)	128 (No more than 8 ANPR cameras and 16 cameras for face picture comparison are allowed.)	128 (No more than 8 ANPR cameras and 16 cameras for face picture comparison are allowed.)
Doors	32	32
External Streaming Servers	64	

Video

Max. performance of internal streaming server: up to 200 channels, and no more than 400 Mbps for input/output bandwidth.
For channels that can be viewed simultaneously, see ***Decoding Performance of Desktop*** .

Access Control

Table 1-8 Access Control Related Performance

Parameter	Configuration 1	Configuration 2
Persons	500	500
Cards	1,500	1,500
Profile Pictures	500	500
Fingerprints	1,000	1,000
Irises	1,000	1,000

Performance of Main Panel for Monitoring and Control

Table 1-9 Performance of Main Panel for Monitoring and Control

Parameter	Configuration 1	Configuration 2
Resources in One View	64	64
Resources in Multiple Views	256	256
Areas	256	256
Map	• Total E-Maps: 16 • Maps in One View: 4	• Total E-Maps: 16 • Maps in One View: 4

Table 1-10 Performance Not Limited by Configurations

Parameter	Performance
New Windows	4
Views	64
Area Levels	5
Resources on GIS Map or Each E-Map	256

Users, Roles, and Permissions

Table 1-11 Performance of Users, Roles, and Permissions

Parameter	Configuration 1	Configuration 2
Users	128	128
Roles	64	64
Online Users on Desktop	64	64
Online Users on Mobile Clients	64	64

Event and Alarm

Table 1-12 Performance of Event and Alarm

Parameter	Configuration 1	Configuration 2
Events Receiving	20/s	20/s
Number of Alarm Rules	1000	1000
Speed of Pushing Alarms/ Events/Notifications from Server to One Client	20/s	20/s

Performance of Data Storage

Table 1-13 Performance of Data Storage

Parameter	Configuration 1	Configuration 2
Video Storage Throughput	480 Mbps	600 Mbps
Retention Period of Captured Faces, ANPR Records, Events, Intelligent Analysis Data, Access Records, and System Logs	3 Years	3 Years
Storage Capacity (including captured faces, ANPR records, events, intelligent analysis data, access records, and system logs)	10 million	10 million

1.4 Decoding Performance of Desktop

The performance is tested in the following configuration.

Table 1-14 Configuration

Feature	Configuration
Recommended Model	DS-VP41D-C/HW5
CPU	Intel® Core™ i5-12500 3.0.0 GHz
RAM	16 (8+8) GB

Feature	Configuration
NIC	Intel® Ethernet Connection (17) I219-LM
Graphics Card	Intel®UHD Graphics 770
OS	Microsoft® Windows 10 (64-bit)

1.4.1 Detailed Performance

This topic introduces the hardware and software decoding performance of different encoding formats including H.264 and H.265.

H.264

Table 1-15 Performance of H.264 with Hardware Decoding

Frame Rate (fps)	Bit Rate (Mbps)	Resolution	Max. Live View Channels
30	6	1080p	35
30	12	8 MP	10
25	6	1080p	42
25	12	8 MP	12

Table 1-16 Performance of H.264 with Software Decoding

Frame Rate (fps)	Bit Rate (Mbps)	Resolution	Max. Live View Channels
30	6	1080p	15
30	12	8 MP	5
25	6	1080p	17
25	12	8 MP	6

H.265

Table 1-17 Performance of H.265 with Hardware Decoding

Frame Rate (fps)	Bit Rate (Mbps)	Resolution	Max. Live View Channels
30	3	1080p	41
30	6	8 MP	11

Frame Rate (fps)	Bit Rate (Mbps)	Resolution	Max. Live View Channels
25	3	1080p	45
25	6	8 MP	15

Table 1-18 Performance of H.265 with Software Decoding

Frame Rate (fps)	Bit Rate (Mbps)	Resolution	Max. Live View Channels
30	3	1080p	13
30	6	8 MP	4
25	3	1080p	15
25	6	8 MP	5

For environments where the iVMS-4200 is running, with a CPU earlier than Intel® Core™i3-8100, 4 GB of RAM, and a SATA 7200 RPM Enterprise Class HDD, see recommendations in ***Other System Configurations and Performance*** for migrating from iVMS-4200 to HikCentral Lite.

1.5 Document Guide

- ***Release Notes*** (What's new about the current version and history versions)
- ***Data Sheet*** (Helps make a buying decision about the product by providing technical specifications)
- ***Compatibility List of Devices*** (Provides supported Hikvision devices and third-party devices)
- ***Hardening Guide*** (Informs users of the factors affecting the system security and provides security suggestions for users in terms of system overall security)
- ***User Manual*** (Gives you detailed guidance of how to use the product)
- ***Quick Start Guide of Mobile Client*** (Provides simple introduction of functions on different pages for beginners)

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 two major service capabilities: **Access Control** and **Video**. Each service capability, once activated, corresponds to a set of features as outlined below.

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, both capabilities are enabled. At least one business capability will remain operational. If the only active capability is disabled, another capability will automatically activate to maintain system functionality.

If access control and/or video device type in the service capability has been added in the system, disabling the corresponding service capability is not allowed. Once the corresponding devices are removed from the system, the service capability can then be disabled.

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.

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

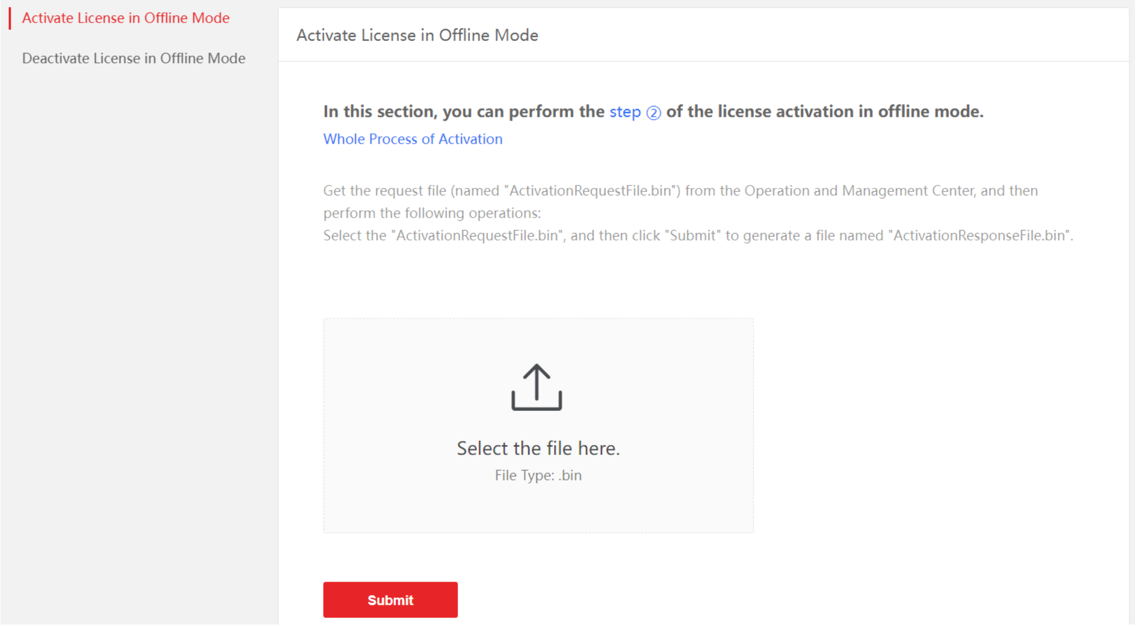
1. Select **Offline Activate** as the activation type to activate the license in offline mode.
2. Enter the activation code received when you purchased your License.

   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*** .



Activate License in Offline Mode
Deactivate License in Offline Mode
Activate License in Offline Mode

In this section, you can perform the step ② of the license activation in offline mode.

Whole Process of Activation

Get the request file (named "ActivationRequestFile.bin") from the Operation and Management Center, and then perform the following operations:
Select the "ActivationRequestFile.bin", and then click "Submit" to generate a file named "ActivationResponseFile.bin".

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, 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.

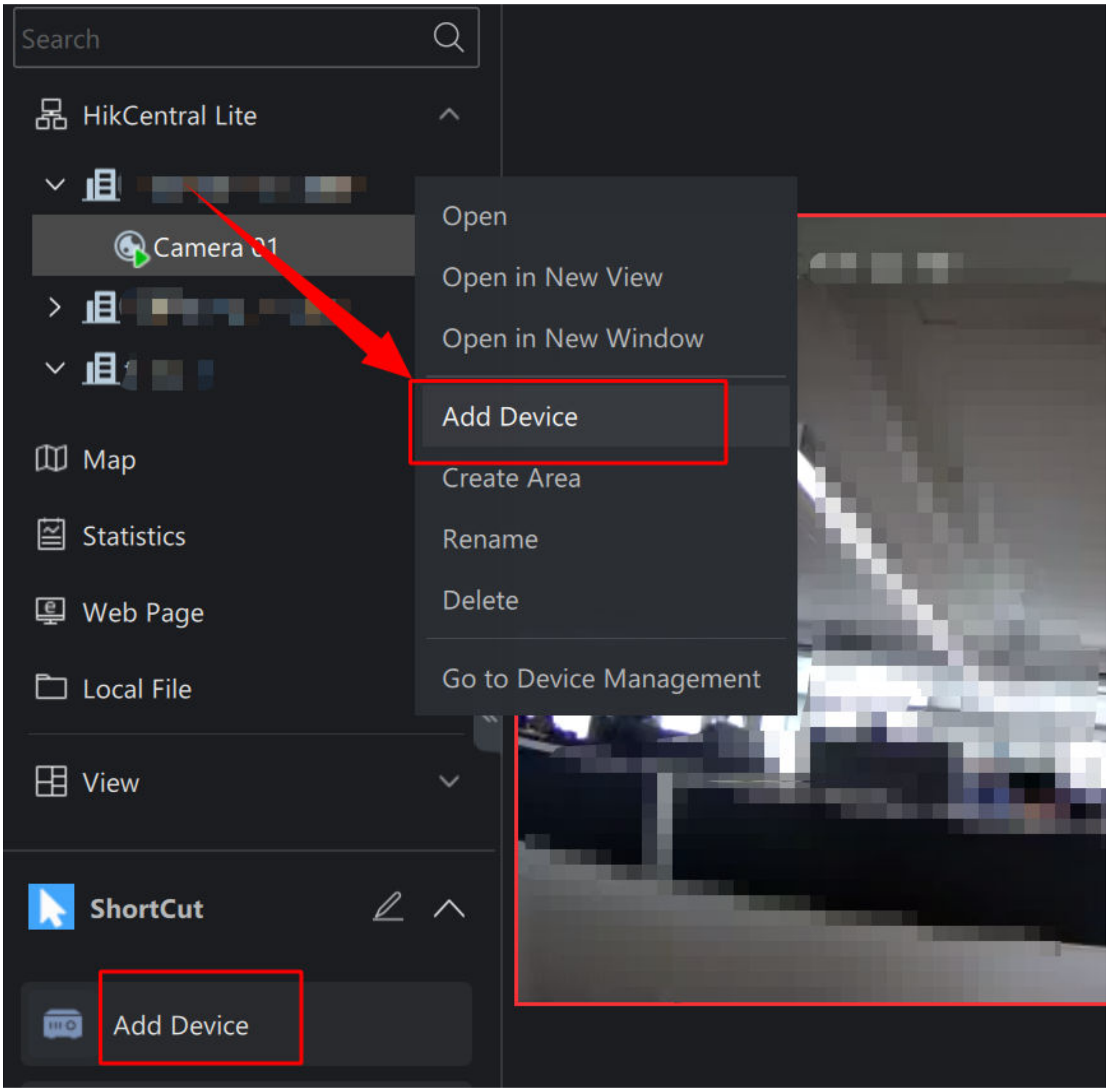


Figure 2-1 Other Entries for Adding Devices

Data Migration

- On the Home page, go to **System → Device Management → Move Now** .
- (Only supported on the Server) On the Home page, go to **Username → 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.
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.
Manually Add	Select this one if the IP address, port No., ID, and secret key of single device are known. 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 enable ONVIF before using this feature for security reasons.
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

Mode	Description
	- 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.

Note

You can only set time zone for online devices.

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.

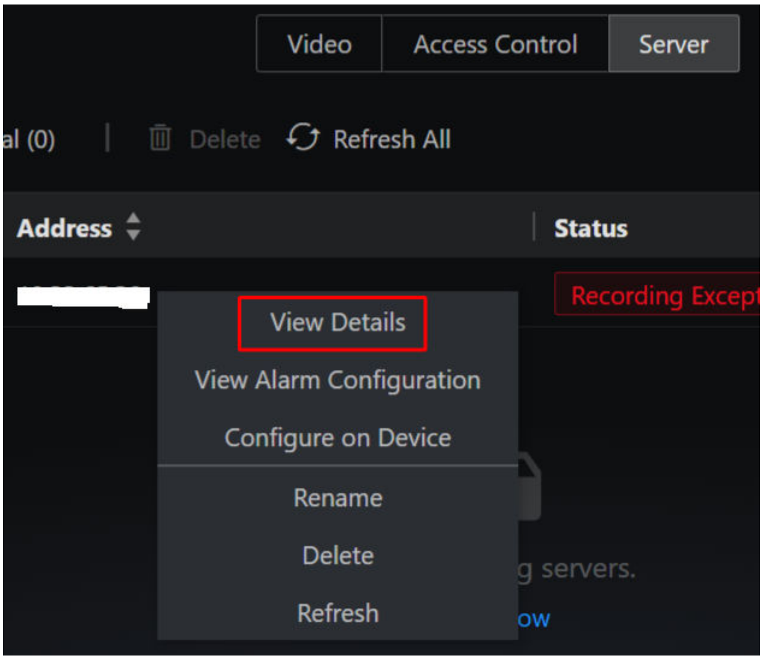


Figure 2-2 View Server Details

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

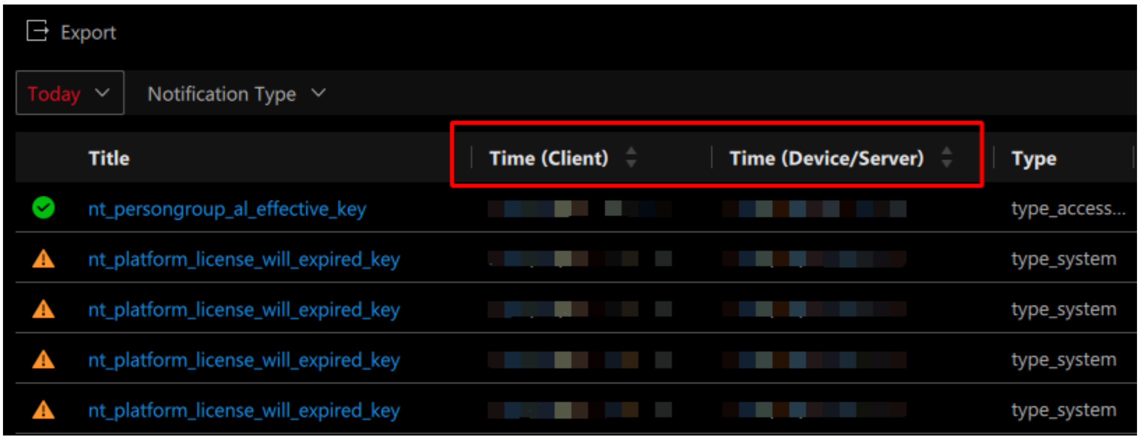
- **Voice Engine (Requires the Operating System's Support)**: Play the voice text configured (the audible alarm in ***Supported Linkage Actions***), by the voice engine supported by the computer system.
- **Local Audio Files**: Play the uploaded local files. The configured voice text will be irrelevant.

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.



	Title	Time (Client)	Time (Device/Server)	Type
✓	nt_persongroup_al_effective_key	[redacted]	[redacted]	type_access...
⚠	nt_platform_license_will_expired_key	[redacted]	[redacted]	type_system
⚠	nt_platform_license_will_expired_key	[redacted]	[redacted]	type_system
⚠	nt_platform_license_will_expired_key	[redacted]	[redacted]	type_system
⚠	nt_platform_license_will_expired_key	[redacted]	[redacted]	type_system

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.

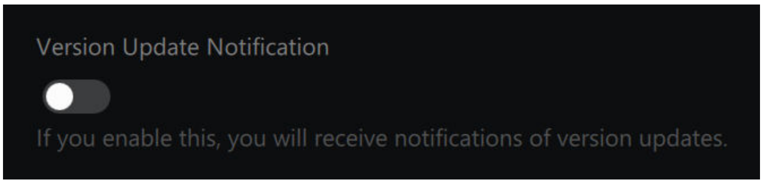
Streaming Access Mode

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.



Version Update Notification

If you enable this, you will receive notifications of version updates.

Figure 2-3 Version Update

Basic Video Preference

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

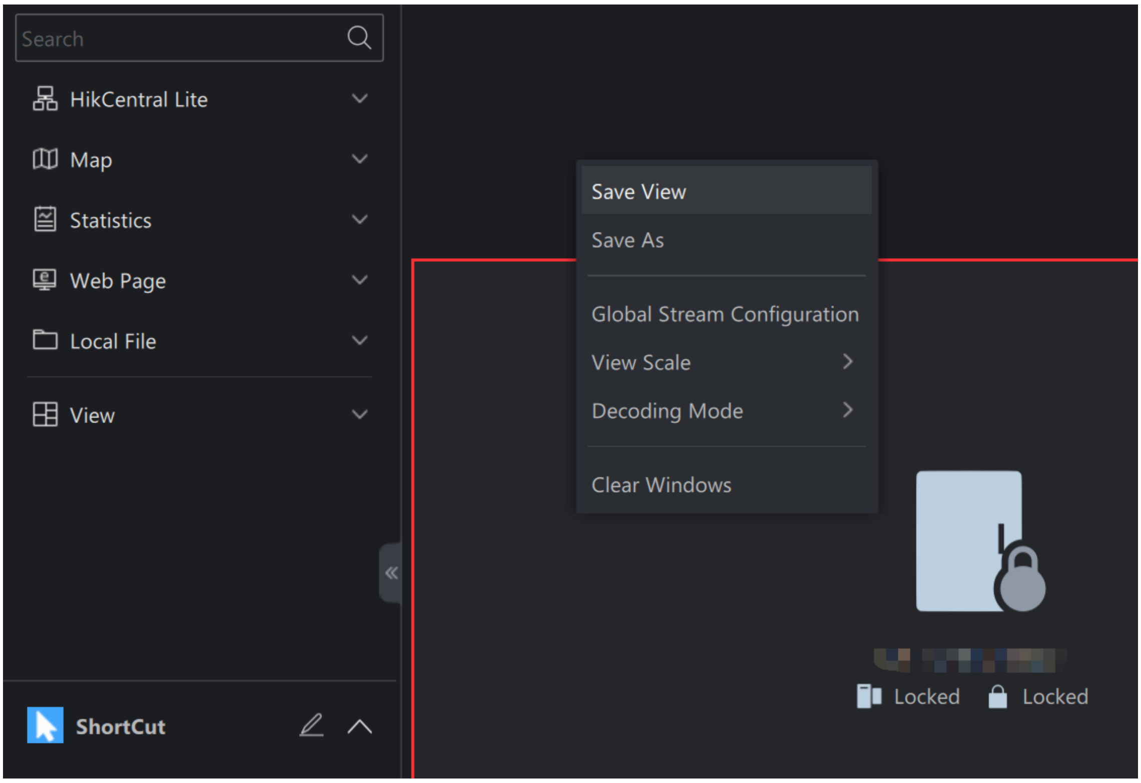


Figure 2-4 Access to Basic Video Preference

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.

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 of Camera***
- ***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 / Object Search

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.

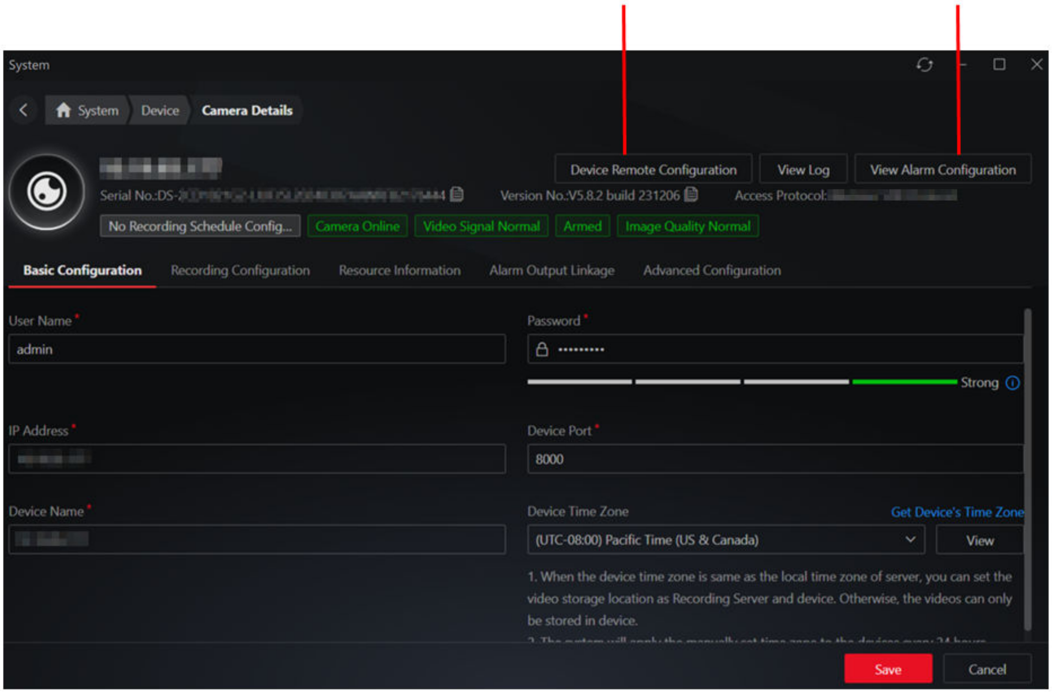
3.1.2 View and Configure Details of Encoding Devices

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.

Open device web configuration page

Open device alarm configuration page



[redacted]

Serial No.:DS-[redacted]

Version No.:V5.8.2 build 231206

Access Protocol:[redacted]

User Name *: admin

Password *: ••••••••••

IP Address *: [redacted]

Device Port *: 8000

Device Name *: [redacted]

Device Time Zone: (UTC-08:00) Pacific Time (US & Canada)

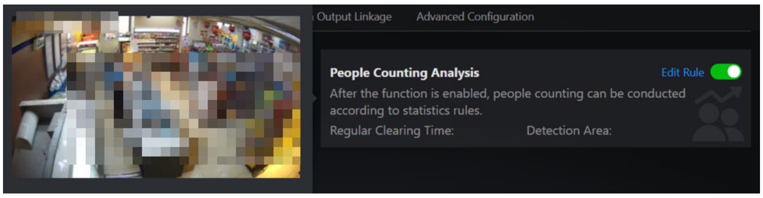
1. When the device time zone is same as the local time zone of server, you can set the video storage location as Recording Server and device. Otherwise, the videos can only be stored in device.

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.

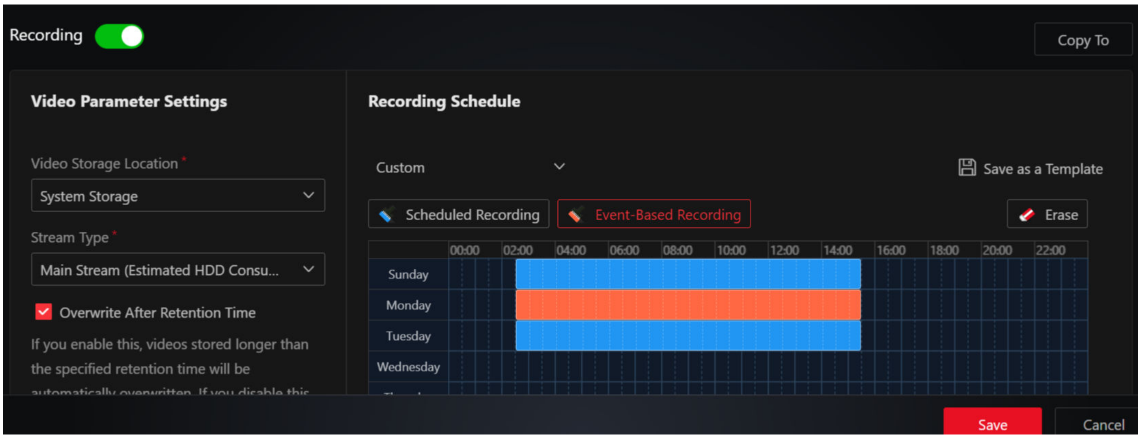
Device Details Tab Page Introduction

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.  People Counting Analysis After the function is enabled, people counting can be conducted according to statistics rules. Regular Clearing Time: Detection Area:
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.

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 type during playback.



Recording ●

Video Parameter Settings

Video Storage Location *: System Storage

Stream Type *: Main Stream (Estimated HDD Consu...

☑ Overwrite After Retention Time

If you enable this, videos stored longer than the specified retention time will be automatically overwritten. If you disable this

Recording Schedule

Custom

Figure 3-2 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 system or local device.

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

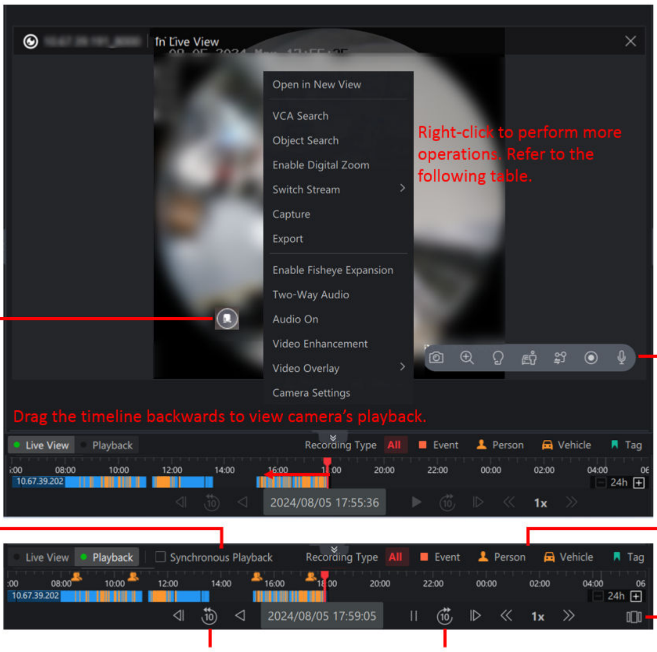
The video monitoring basic functions include live view, playback, PTZ control, and monitoring on the map.

3.2.1 Start Live View / Playback of Camera

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

Start Live View / Playback of One Camera

- 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.
  During playback,



Right-click to perform more operations. Refer to the following table.

Turn on/off alarm output.

Control the live view / playback window.

Drag the timeline backwards to view camera's playback.

Start synchronous playback of cameras.

Click a tag to filter the video.

Display thumbnails of video above the timeline.

Rewind playback for 10 seconds.

Fast forward playback for 10 seconds.

Note: You can also press shortcuts on the keyboard to control playback. Cursor on the icons to view the corresponding shortcuts.

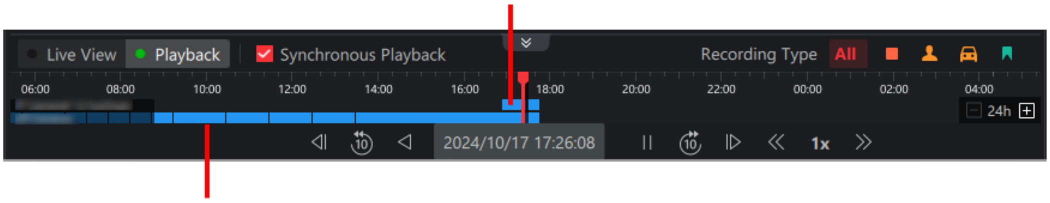
Figure 3-3 Start Live View / Playback of One Camera

Note

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

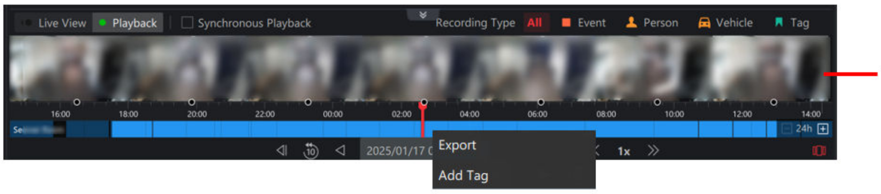
- To enable the tags, make sure that at least one VCA event, such as intrusion or line crossing, is configured on the device. Human or/and vehicle target detection should be enabled.
- ***Subscription*** of the corresponding event on HikCentral Lite should be enabled.
- Videos recorded before the device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

The playback timeline of the currently selected camera.



The playback timeline of all cameras in the viewing grid.

Figure 3-4 Synchronous Playback



Thumbnails of the video.

Right click the timeline to export the video or add tag for it. The video content changes as you change the time for exporting or tagging.

Figure 3-5 Video Thumbnails

During live view or playback, you can right click the window or click the icons in the lower right corner of the window to control the live view or playback window. Refer to the following table for the 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 / Object Search	**AcuSearch** Detects human bodies and vehicles and search for objects similar to them in captured pictures. **Object Search** Detects faces and human bodies and search for objects similar to them in captured pictures.	√	√

Function	Explanation	Live View	Playback
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.	√	√
Capture	Take a snapshot of the current video image.	√	√
Export	Export the video.	×	√
Start Recording	Record a video for the desired time period.	√	×
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.	√	√

Function	Explanation	Live View	Playback
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*** .	√	√

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

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.

Start Live View / Playback of Multiple Cameras

- Start Live View of Multiple Cameras:
  - Press the ctrl key, select cameras, and drag them from the camera list to the right window to start live view of multiple cameras.
  - Press the ctrl key, select cameras, right click the cameras and click **Open** to start live view of multiple cameras.
- Start Playback of Multiple Cameras: Select a live view window, and drag the timeline on the playback panel backwards to start playback of the camera. Repeat the above operations to view playback of multiple cameras.

During live view or playback, you can select multiple live view or playback windows and right click to batch control them. Refer to the following table for the supported operations.

Function	Explanation
Export Video File	Export the video file within the selected time range.
Audio On/Off	Turn on/off the audio of the video.
Close Window	Close the live view / playback windows.

Configure Parameters for Video Monitoring

Right click the blank area in the viewing grid, and configure the following parameters.

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

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

3.2.2 PTZ Control During Live View

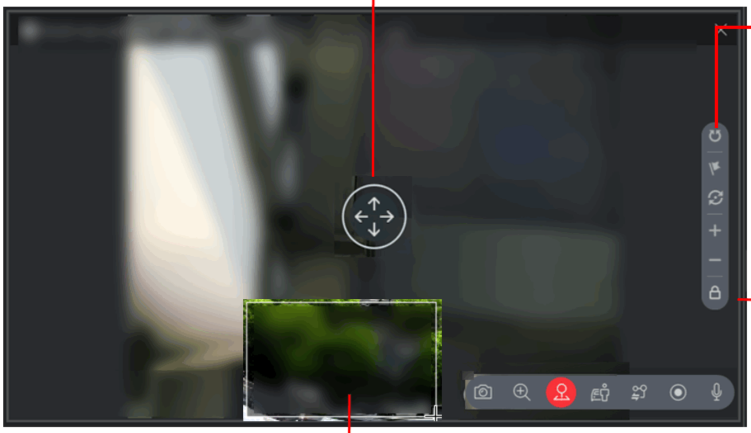
You can control cameras with pan/tilt/zoom functionality during live view. You can set the preset and patrol for the cameras on the PTZ control pane.

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.

Two methods to control the direction of PTZ:

- Click the button in the middle, and then drag and move the arrow to the desired direction.
  The rotation speed of PTZ becomes faster as you move the arrow further away from the middle button.
- Click on the video image to let the PTZ turn to the direction where the mouse is clicked.



Click to start auto scanning.

Click to lock PTZ. When the PTZ is locked by a user, other users with the same or lower PTZ control permission levels cannot control the PTZ.

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.

Figure 3-6 PTZ Control

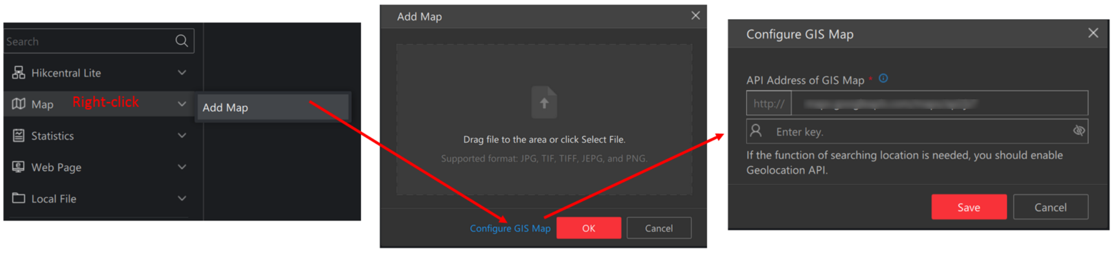
3.2.3 Monitor via Cameras on the Map

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



Drag file to the area or click Select File.

Supported format: JPG, TIF, TIFF, JEPG, and PNG.

API Address of GIS Map *

http:// [redacted]

Enter key.

If the function of searching location is needed, you should enable Geolocation API.

Figure 3-7 Add GIS Map

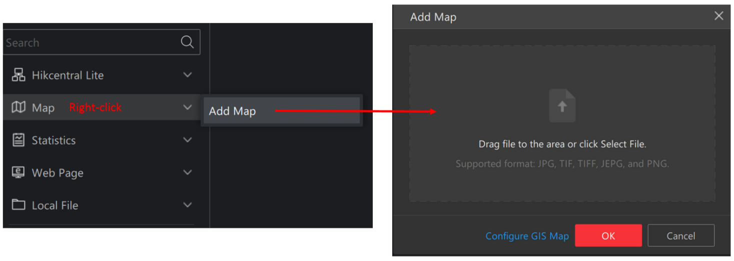
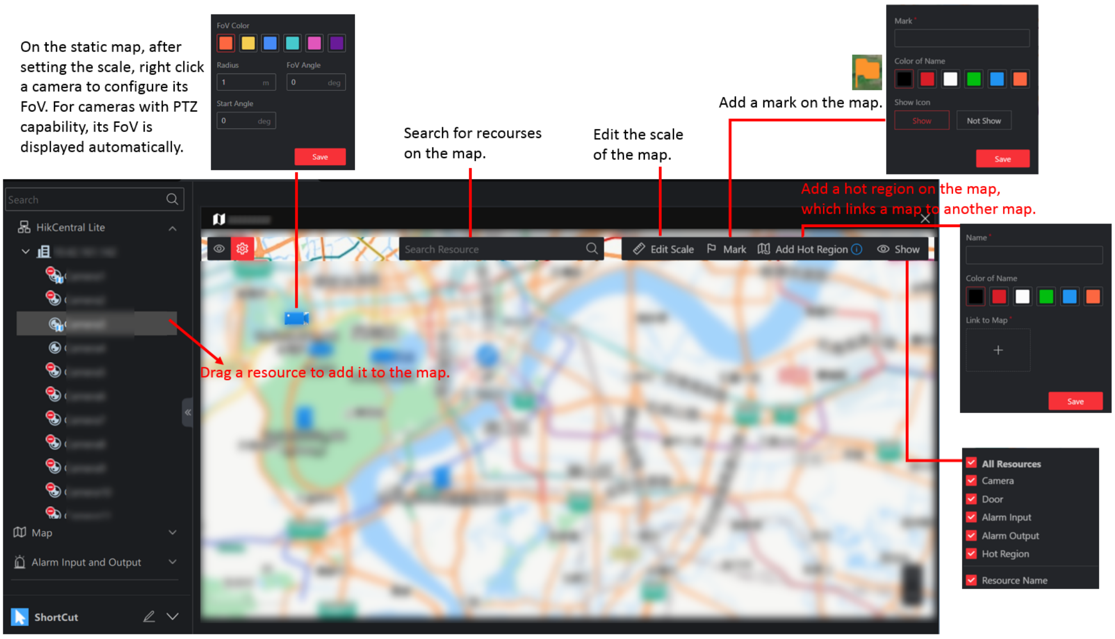


Figure 3-8 Add E-Map

Configuration Mode


On the static map, after setting the scale, right click a camera to configure its FoV. For cameras with PTZ capability, its FoV is displayed automatically.

Search for recourses on the map.

Edit the scale of the map.

Add a mark on the map.

Add a hot region on the map, which links a map to another map.

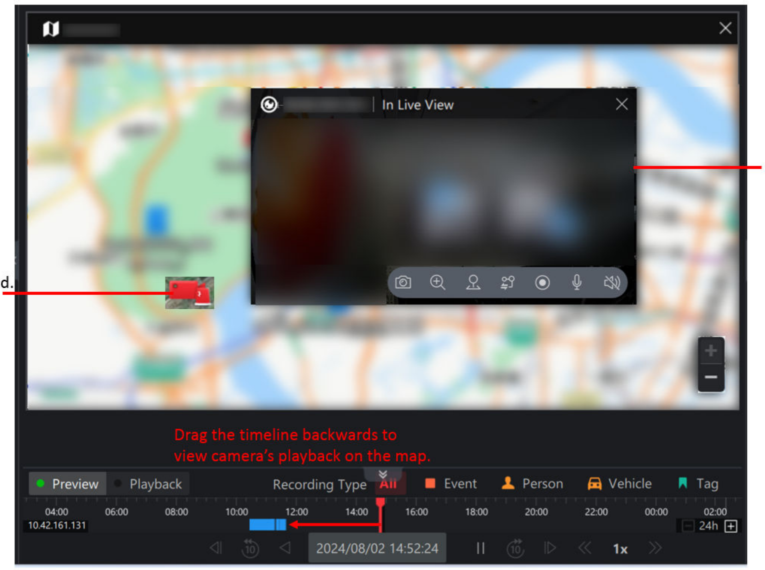
Drag a resource to add it to the map.

Figure 3-9 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.



There is alarm not acknowledged.

View camera's live view on the map.

Drag the timeline backwards to view camera's playback on the map.

Figure 3-10 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.

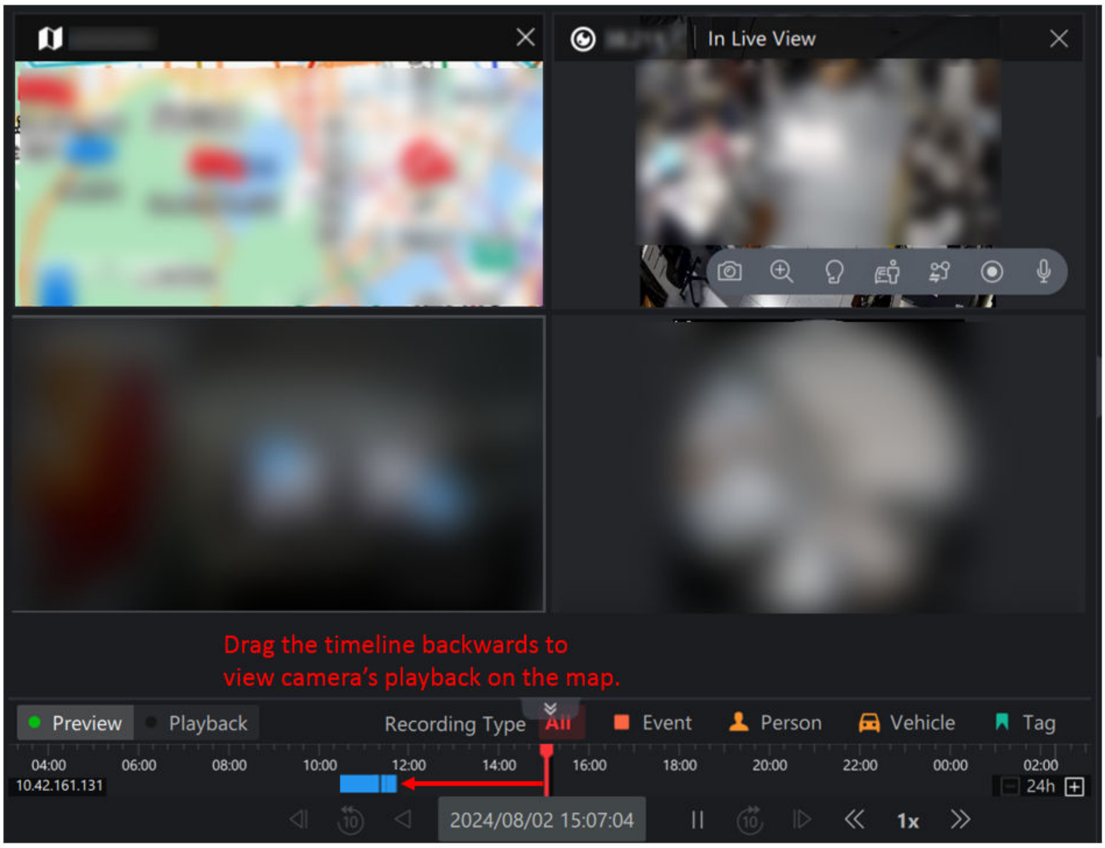


Figure 3-11 Batch View Cameras' Live View and Playback

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 of Camera*** 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.

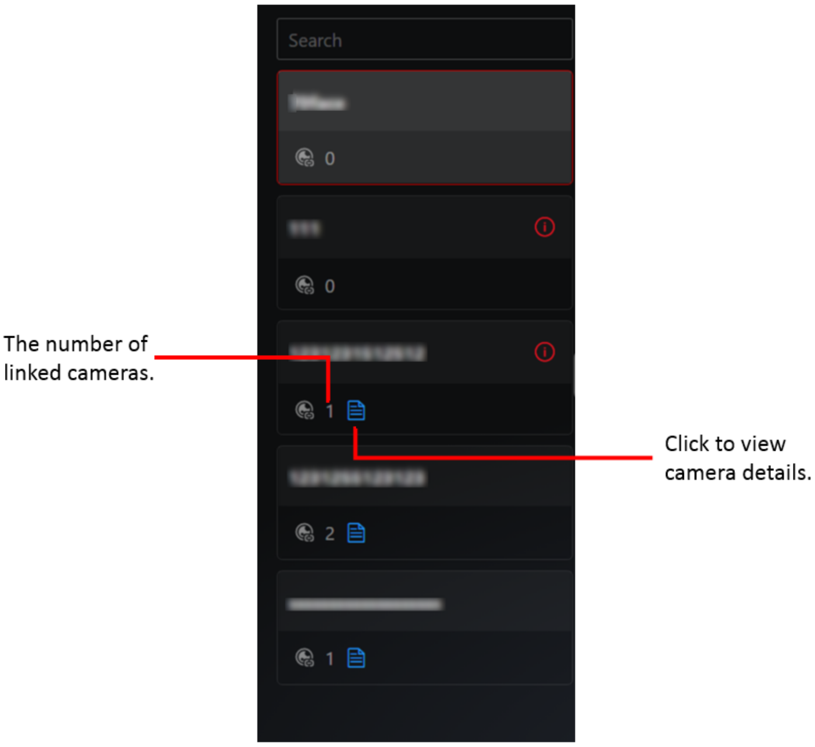


Figure 3-12 Cameras Linked with Face Picture Libraries

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

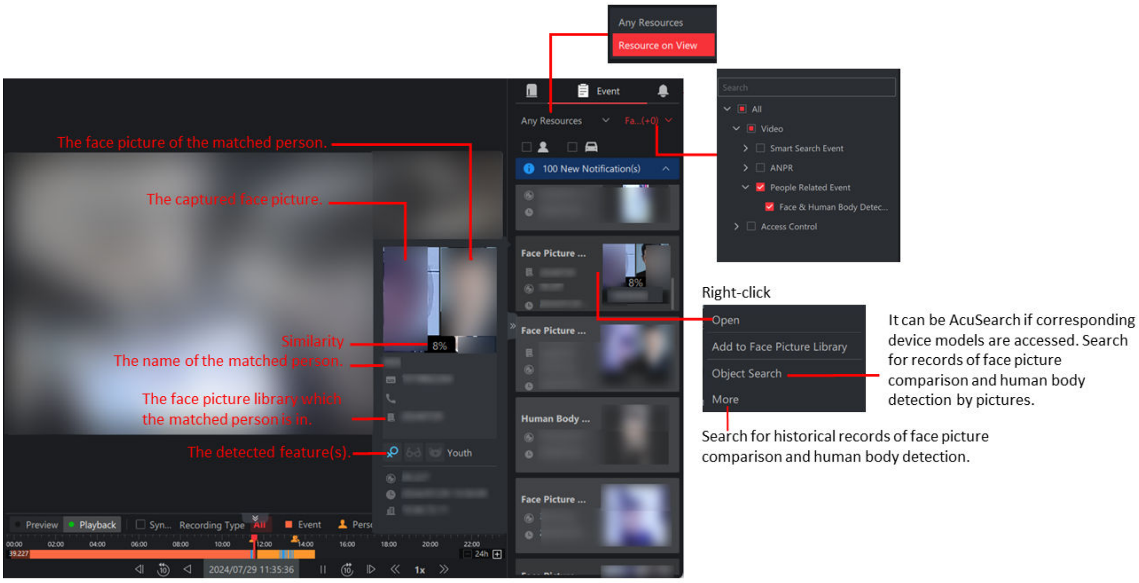
3.3.2 View Videos Related to Face and Human Body Recognition

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.



It can be AcuSearch if corresponding device models are accessed. Search for records of face picture comparison and human body detection by pictures.

Search for historical records of face picture comparison and human body detection.

Figure 3-13 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.

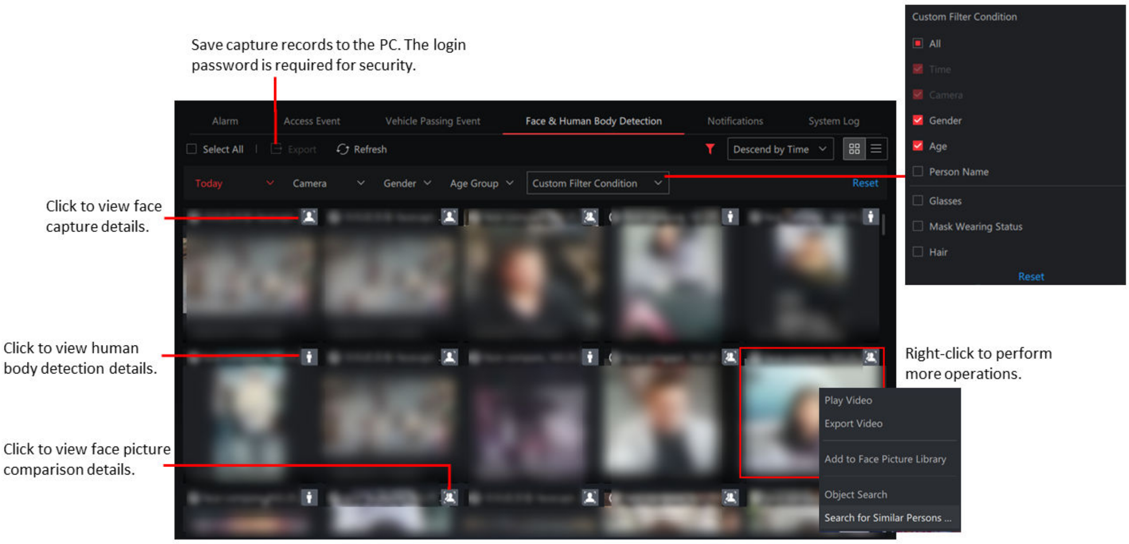
3.3.3 Search for Recognized Face Pictures and Human Body Pictures

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.



Save capture records to the PC. The login password is required for security.

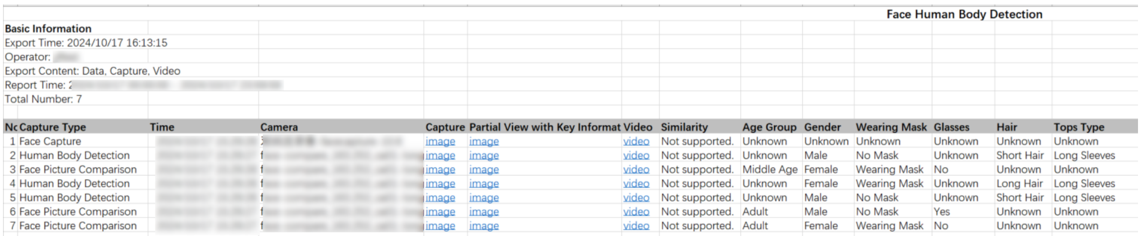
Click to view face capture details.

Click to view human body detection details.

Click to view face picture comparison details.

Right-click to perform more operations.

Figure 3-14 Face & Human Body Detection

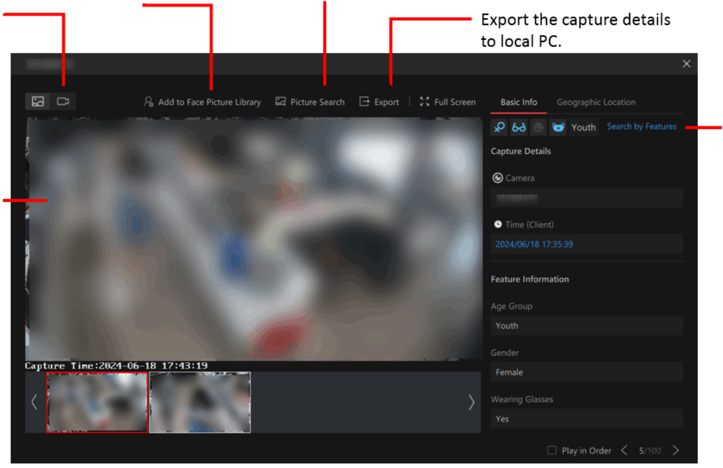


Face Human Body Detection

Basic Information
Export Time: 2024/10/17 16:13:15
Operator: [redacted]
Export Content: Data, Capture, Video
Report Time: 2[redacted]
Total Number: 7

Nc	Capture Type	Time	Camera	Capture	Partial View with Key Informat	Video	Similarity	Age Group	Gender	Wearing Mask	Glasses	Hair	Tops Type
1	Face Capture	[redacted]	[redacted]	image	image	video	Not supported.	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
2	Human Body Detection	[redacted]	f[redacted]	image	image	video	Not supported.	Unknown	Male	No Mask	Unknown	Short Hair	Long Sleeves
3	Face Picture Comparison	[redacted]	f[redacted]	image	image	video	Not supported.	Middle Age	Female	Wearing Mask	No	Unknown	Unknown
4	Human Body Detection	[redacted]	f[redacted]	image	image	video	Not supported.	Unknown	Female	Wearing Mask	Unknown	Long Hair	Long Sleeves
5	Human Body Detection	[redacted]	f[redacted]	image	image	video	Not supported.	Unknown	Male	No Mask	Unknown	Short Hair	Long Sleeves
6	Face Picture Comparison	[redacted]	f[redacted]	image	image	video	Not supported.	Adult	Male	No Mask	Yes	Unknown	Unknown
7	Face Picture Comparison	[redacted]	f[redacted]	image	image	video	Not supported.	Adult	Female	Wearing Mask	No	Unknown	Unknown

Figure 3-15 Export Capture Records



Capture Time:2024-06-18 17:43:19

Capture Details

Camera

Time (Client)
2024/06/18 17:35:39

Feature Information

Age Group
Youth

Gender
Female

Wearing Glasses
Yes

Play the video.

Add the face picture to the face picture library.

Search for the related faces and/or human bodies by the current picture.

Export the capture details to local PC.

Search for face pictures or human bodies by features.

View the captured picture.

Figure 3-16 Supported Operations on Face Capture Details Page

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.

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.

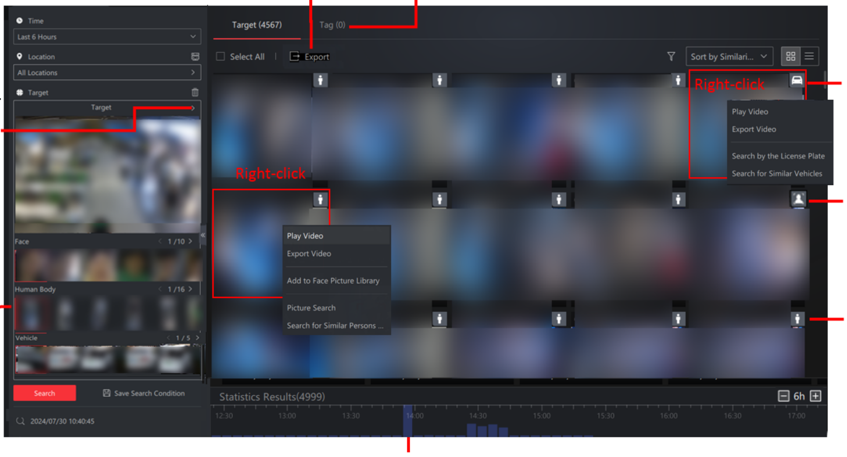
If there is only one face / human body in the picture, the search results will be automatically displayed. Otherwise, you should select a face and/or a human body and/or a vehicle in the picture for searching.

Export record(s) to local PC in Excel/PDF/CSV format.

View tags which are added when viewing the video related with the record.

Select another picture for searching.

Select a face and/or a human body and/or a vehicle for searching.



View vehicle capture details.

View face capture details.

View human body detection details.

Hover on a column to view the number of captured pictures during a specific time period. Click a column to view search results during this time period.

Figure 3-17 Search Conditions and Supported Operations on Search Results Page

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.

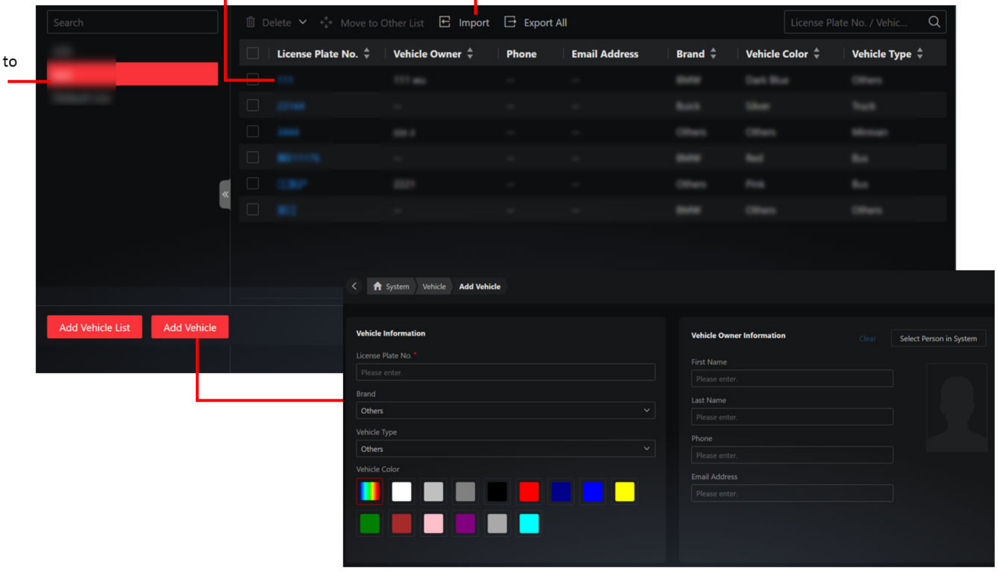
Note

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** .

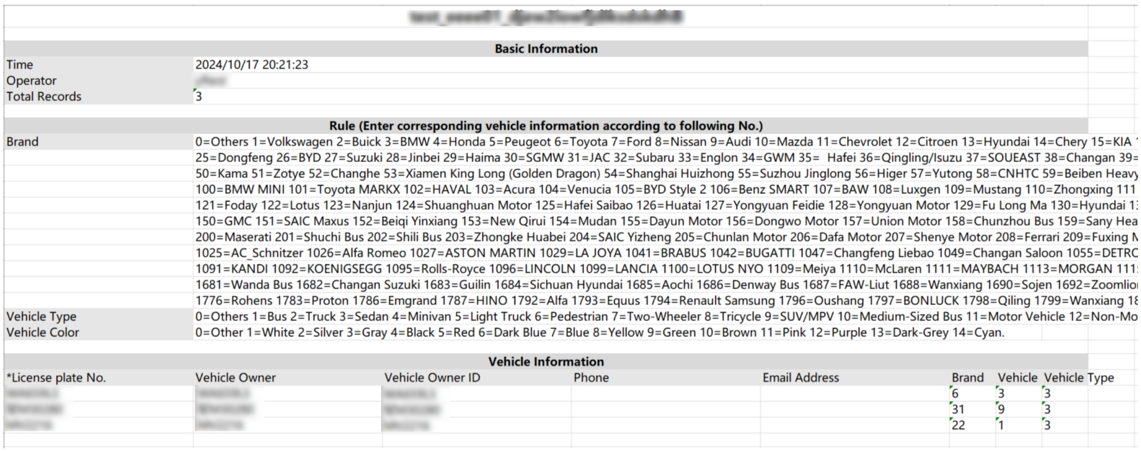


Click the vehicle name to edit the vehicle.

Batch add vehicles by a template.

Click a vehicle list to show the added vehicles.

Figure 3-18 Vehicle Page



[redacted]

	Basic Information						
Time	2024/10/17 20:21:23						
Operator	[redacted]						
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 N						
	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
[redacted]	[redacted]	[redacted]			6	3	3
[redacted]	[redacted]	[redacted]			31	9	3
[redacted]	[redacted]	[redacted]			22	1	3

Figure 3-19 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.

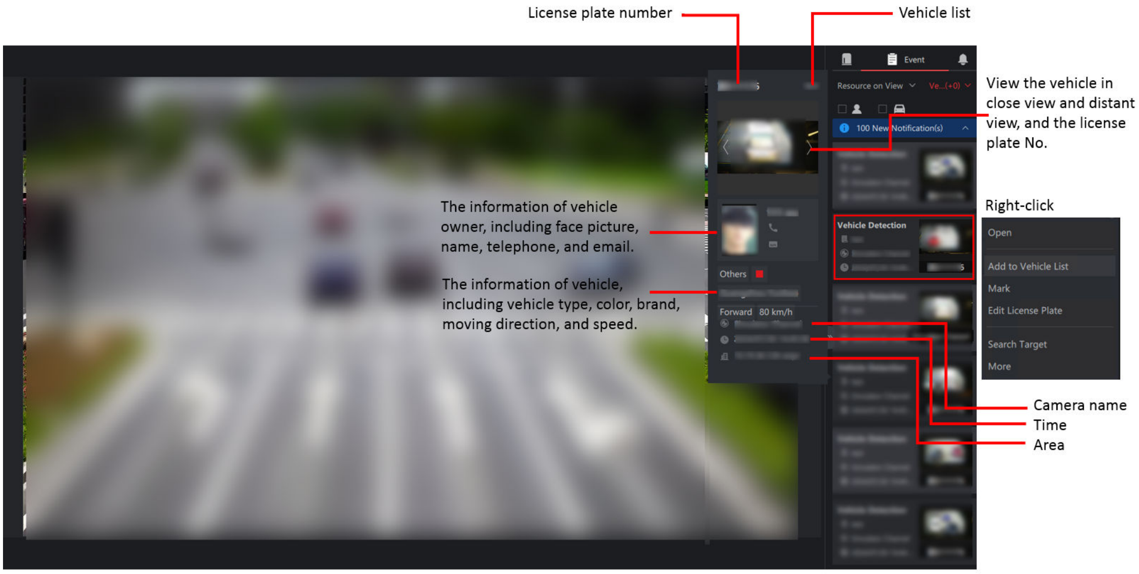

License plate number
Vehicle list
Event
Resource on View
100 New Notification(s)
View the vehicle in close view and distant view, and the license plate No.
Right-click
Vehicle Detection
Open
Add to Vehicle List
Mark
Edit License Plate
Search Target
More
The information of vehicle owner, including face picture, name, telephone, and email.
Others
The information of vehicle, including vehicle type, color, brand, moving direction, and speed.
Forward 80 km/h
Camera name
Time
Area

Figure 3-20 ANPR Event Details

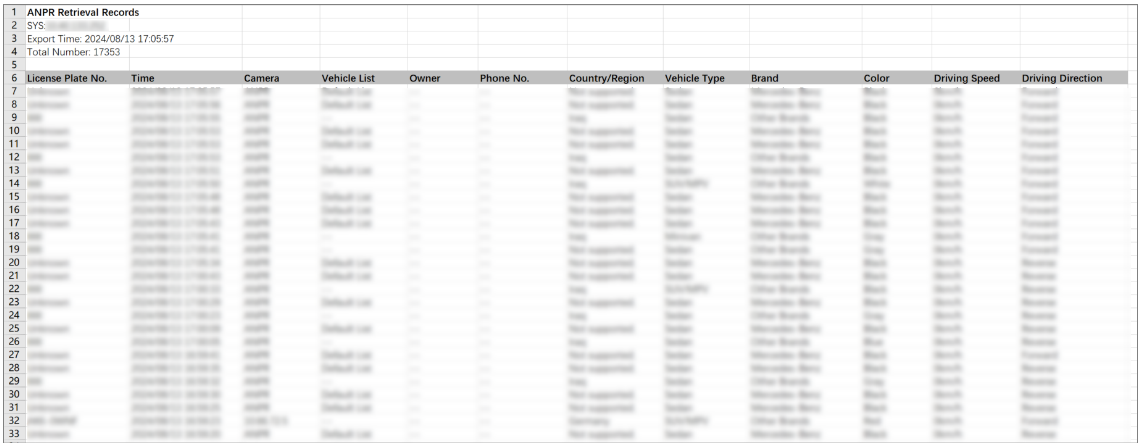
3.4.3 Search and Export ANPR Events

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, camera, vehicle list, and license plate number.
- Click **Export** to export all the events in the needed format (Excel, PDF, or CSV).

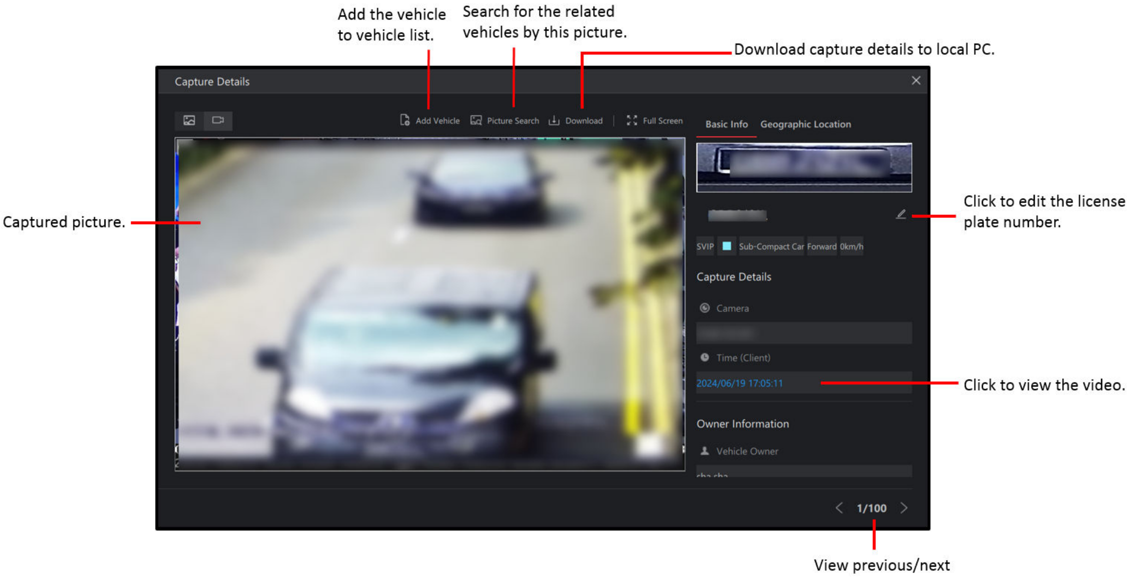


ANPR Retrieval Records
SYS:
Export Time: 2024/08/13 17:05:57
Total Number: 17353

License Plate No.	Time	Camera	Vehicle List	Owner	Phone No.	Country/Region	Vehicle Type	Brand	Color	Driving Speed	Driving Direction

Figure 3-21 Export Vehicle Passing Events in Excel Format

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



SVIP Sub-Compact Car Forward 0km/h

2024/06/19 17:05:11

Add the vehicle to vehicle list.

Search for the related vehicles by this picture.

Download capture details to local PC.

Captured picture.

Click to edit the license plate number.

Click to view the video.

View previous/next

Figure 3-22 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*** .

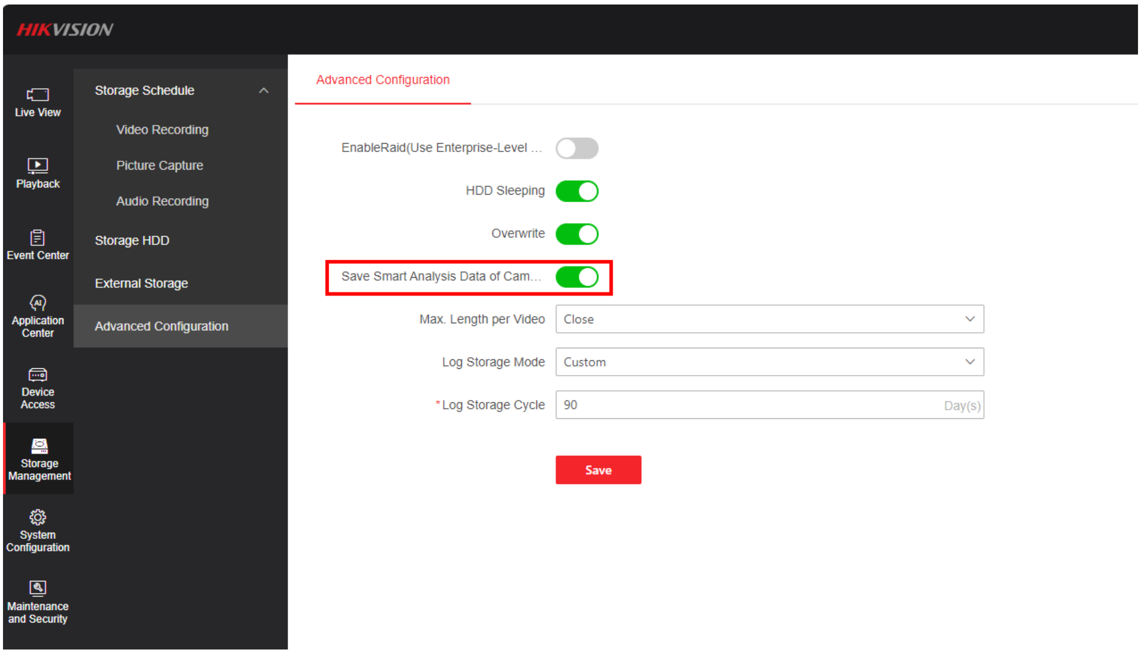
3.5.1 Compatible NVR Series for Smart Search

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**.



Advanced Configuration

EnableRaid(Use Enterprise-Level ... ○

HDD Sleeping ●

Overwrite ●

Save Smart Analysis Data of Cam... ●

Max. Length per Video: Close

Log Storage Mode: Custom

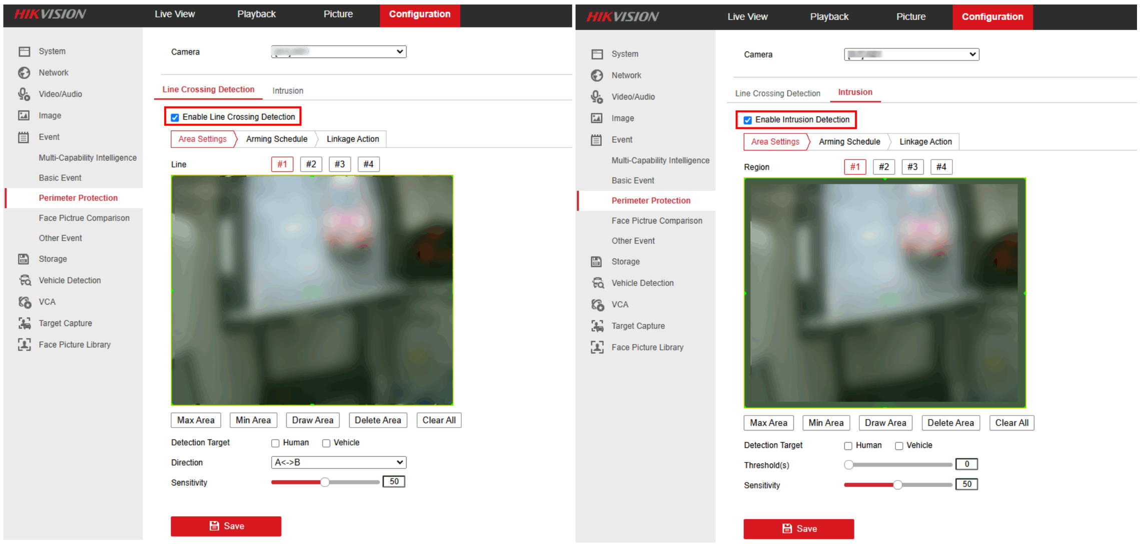
*Log Storage Cycle: 90 Day(s)

Figure 3-23 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**.



☑ Enable Line Crossing Detection

Detection Target □ Human □ Vehicle

Direction A<->B

Sensitivity 50

☑ Enable Intrusion Detection

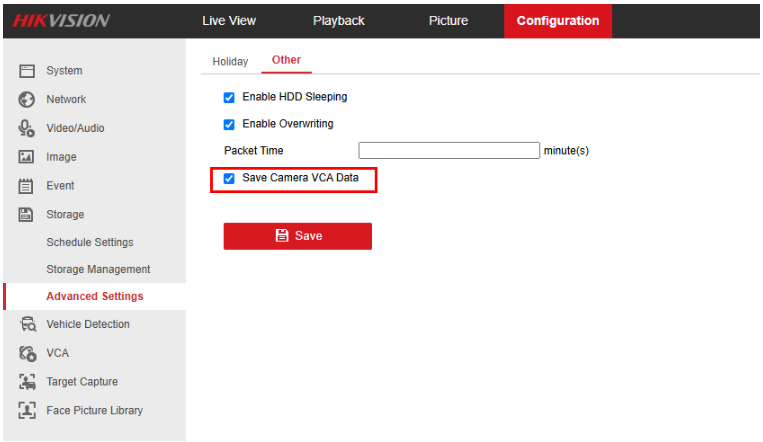
Detection Target □ Human □ Vehicle

Threshold(s) 0

Sensitivity 50

Figure 3-24 Enable Line Crossing Detection & Enable Intrusion Detection

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



☑ Enable HDD Sleeping

☑ Enable Overwriting

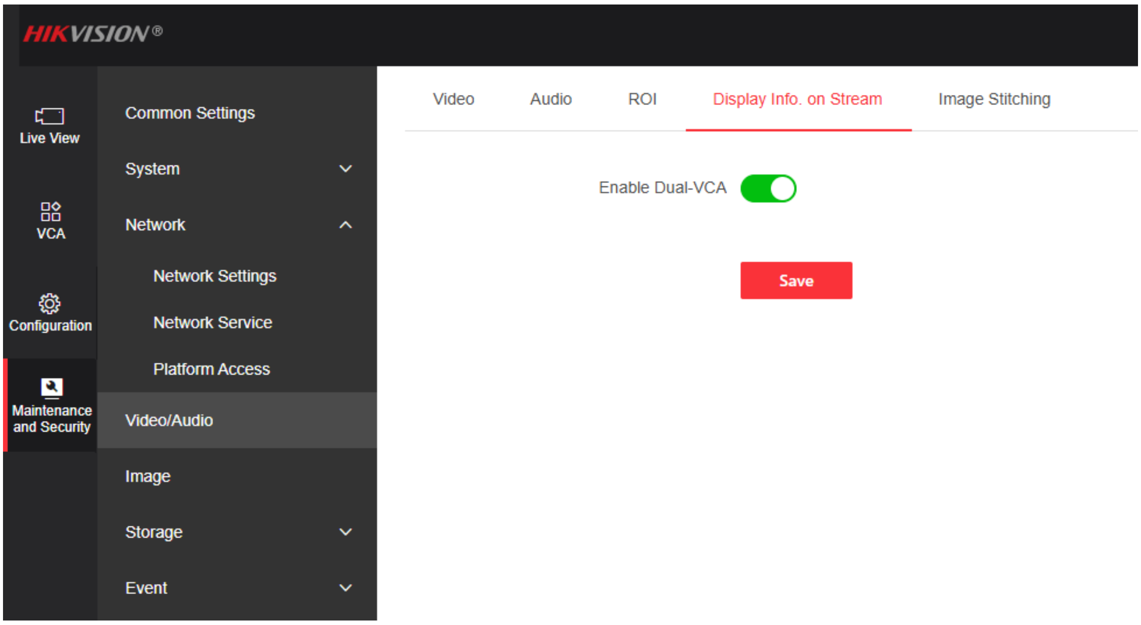
Packet Time minute(s)

☑ Save Camera VCA Data

Figure 3-25 Save Camera VCA Data

When Network Camera Added to HikCentral Lite Directly or Via NVR/DVR That Do Not Support VCA

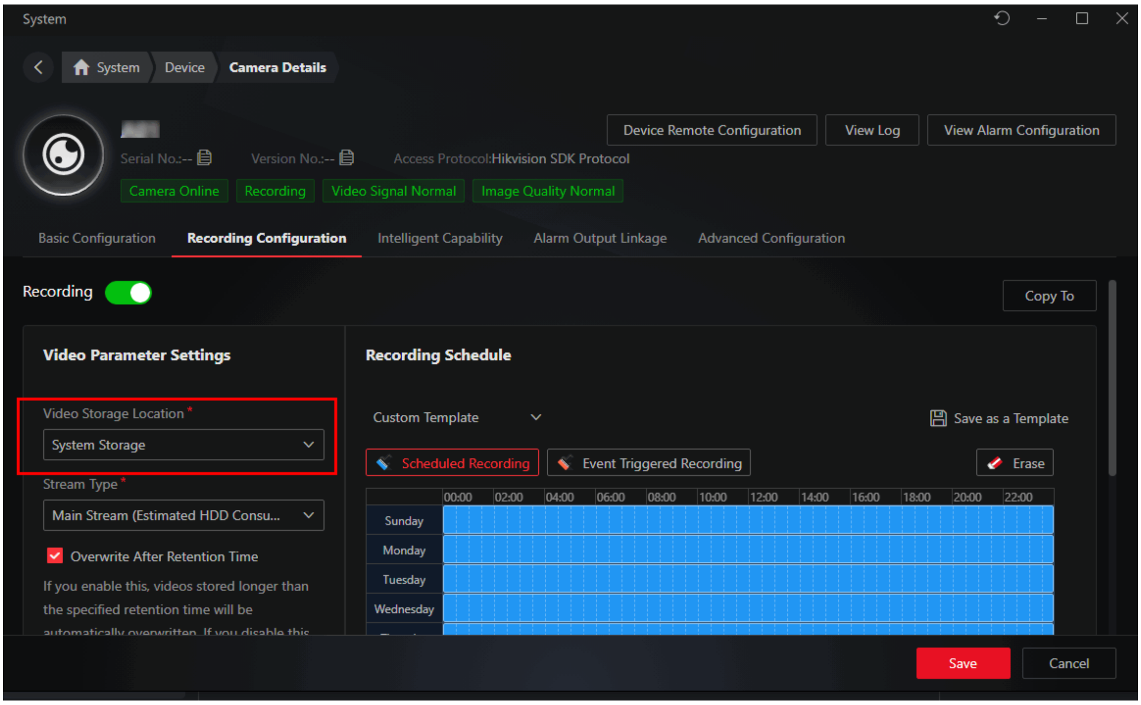
1. Enable **Dual-VCA** for the network camera on the web page of the camera.



Enable Dual-VCA ●

Figure 3-26 Enable Dual-VCA

2. Configure the video storage location as **System Storage** on the Camera details page.



Serial No.:--

Version No.:--

Access Protocol:Hikvision SDK Protocol

Recording ●

Video Storage Location *: System Storage

Stream Type *: Main Stream (Estimated HDD Consu...

☑ Overwrite After Retention Time

If you enable this, videos stored longer than the specified retention time will be automatically overwritten. If you disable this

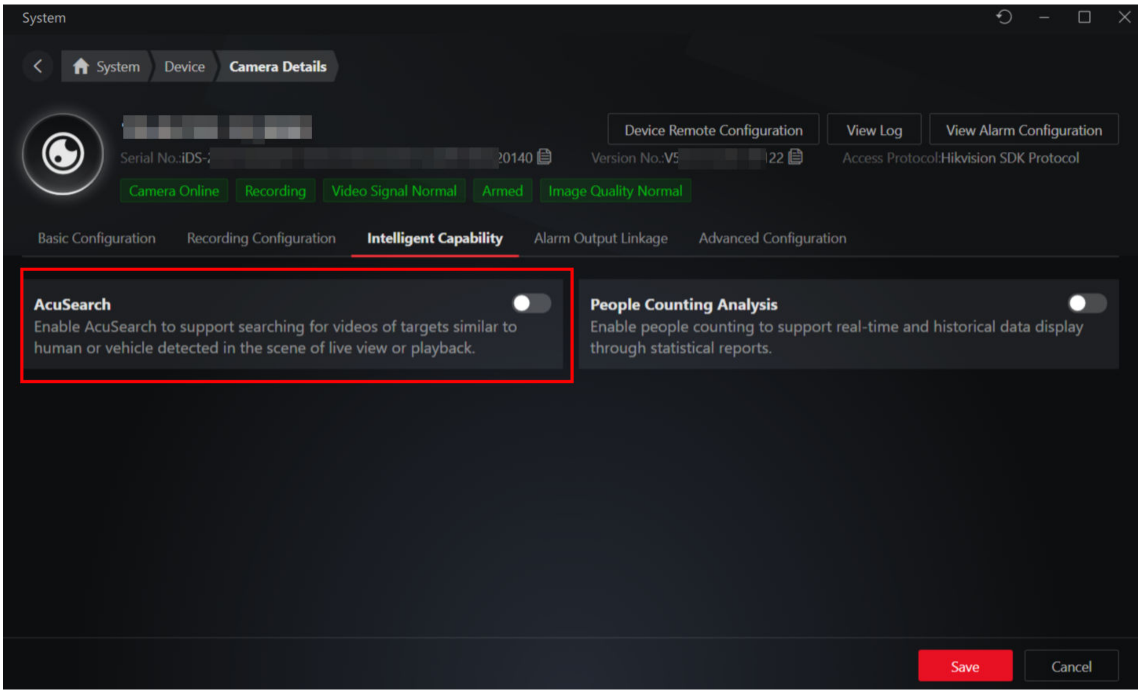
Figure 3-27 Configure Video Storage Location

3.6 AcuSearch / Object Search

The AcuSearch / Object Search 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 activated at least one channel of video monitoring license and have enabled it on the Camera Details page.



Serial No.:iDS-[redacted]20140

Version No.:V5[redacted]22

Access Protocol:Hikvision SDK Protocol

AcuSearch ○
Enable AcuSearch to support searching for videos of targets similar to human or vehicle detected in the scene of live view or playback.

People Counting Analysis ○
Enable people counting to support real-time and historical data display through statistical reports.

Figure 3-28 Camera Details

Supported Device Series

The following is supported device series for using AcuSearch or smart search. 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	• DeepinMind M • I series with AcuSense(E) • K series with AcuSense (Except version B)

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

Table 3-3 Recommended Devices for Object Search

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 / Object Search

For the similarity between Acusearch and Object Search, the two functions share the same button. The button name changes according to models of added devices. If there is no devices supporting object search in the system, the button will be named as **AcuSearch**; if there is any devices supporting object search in the system, the button will be named as **Object Search**.

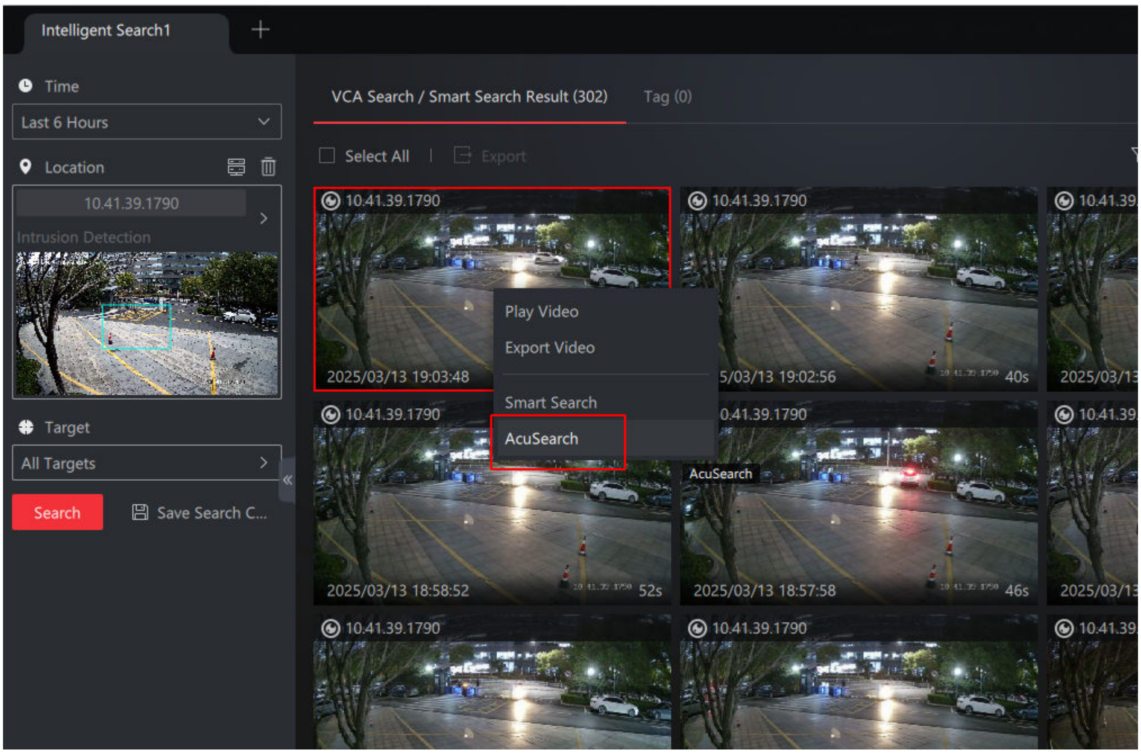


Figure 3-29 AcuSearch

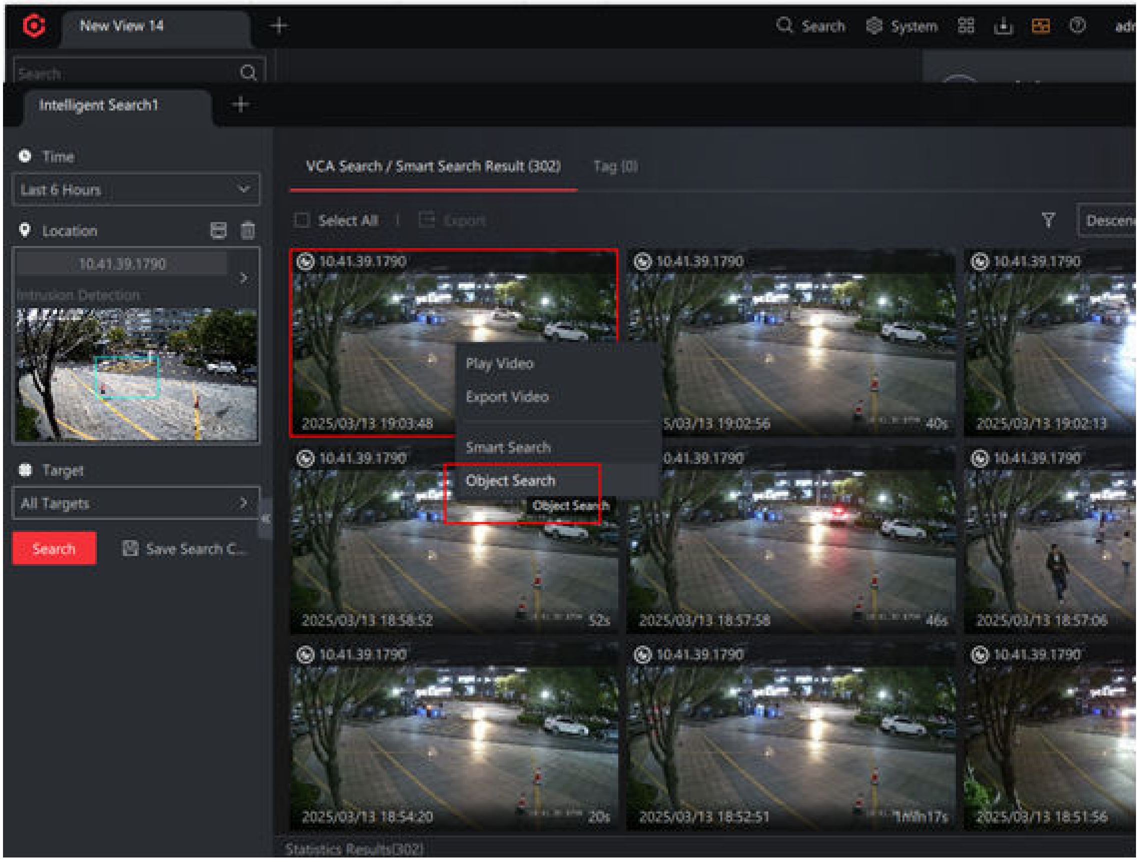
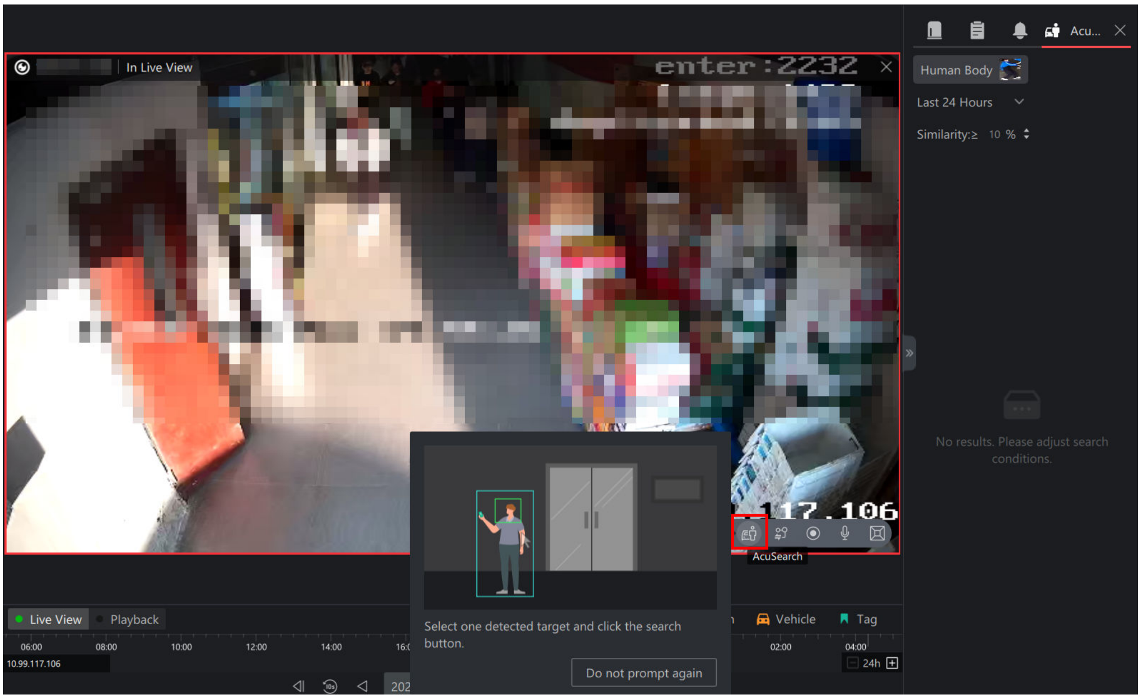


Figure 3-30 Object Search

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



Select one detected target and click the search button.

No results. Please adjust search conditions.

Figure 3-31 Live View Window

On the live view or playback page, click to start AcuSearch / Object Search. The search results will be displayed on the right panel.

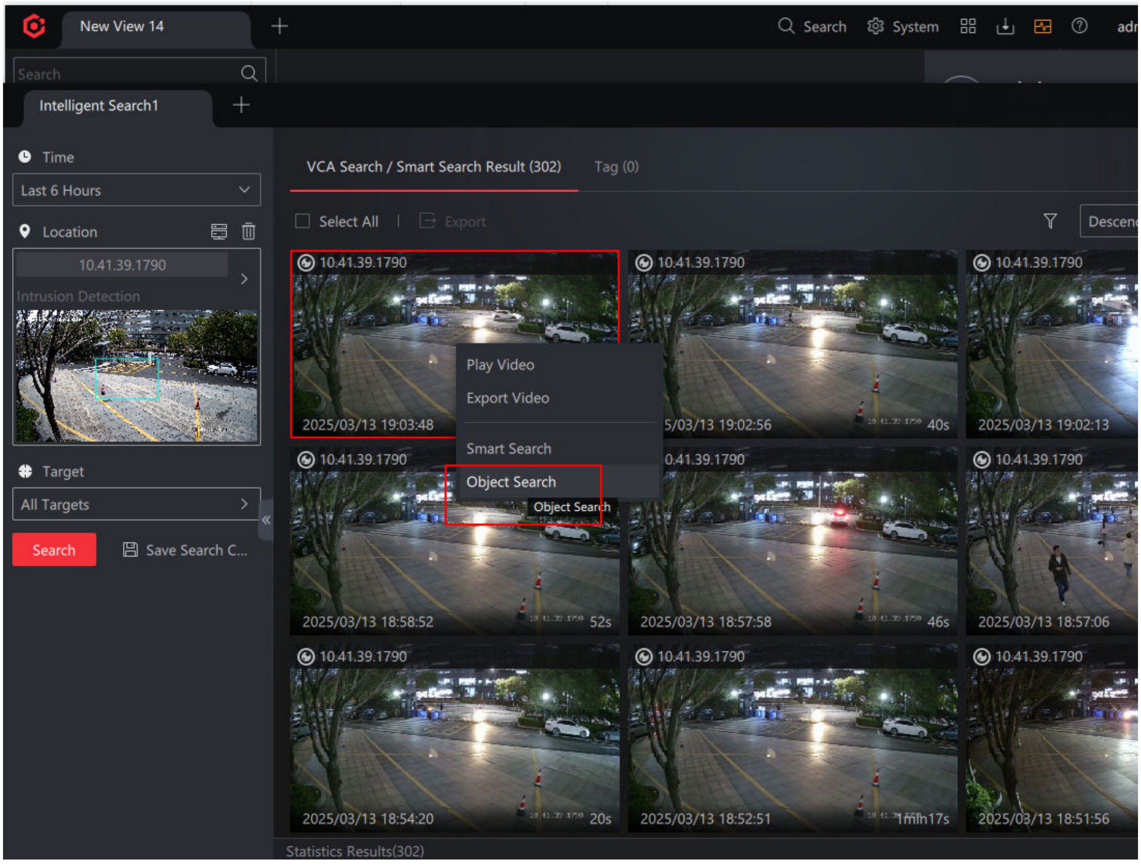


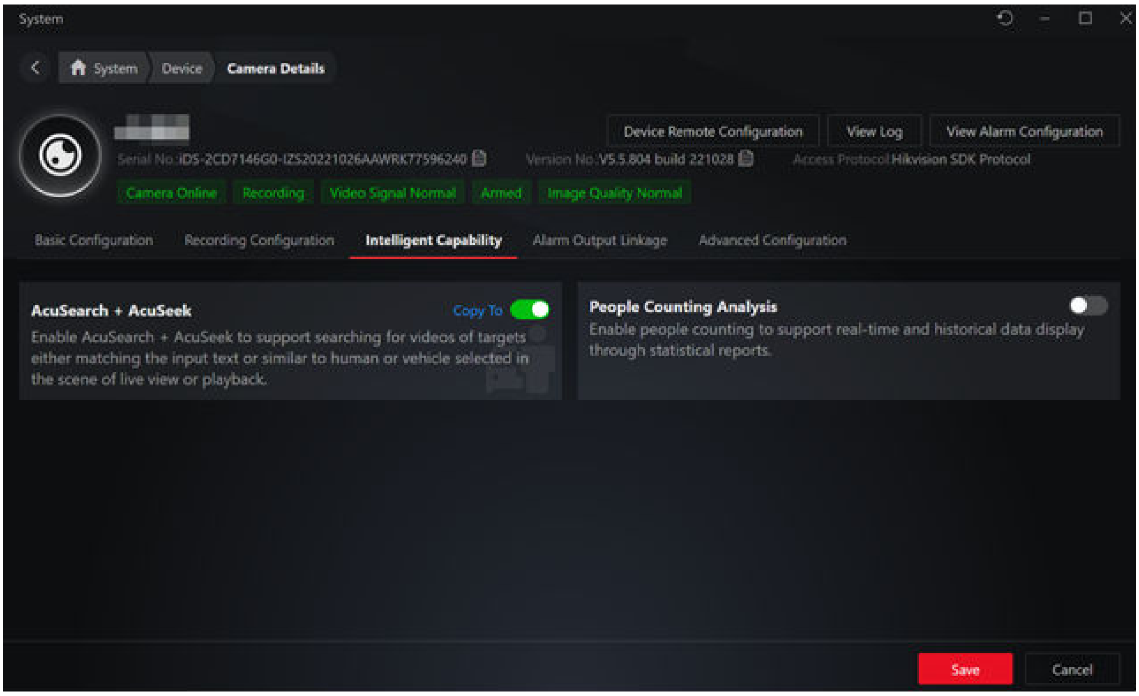
Figure 3-32 Object Search

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, vehicles, or objects.
- **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 activated at least one channel of video monitoring license and have enabled it on the Camera Details page.



[redacted]

Serial No.:iDS-2CD7146G0-IZS20221026AAWRK77596240

Version No.:V5.5.804 build 221028

Access Protocol:Hikvision SDK Protocol

AcuSearch + AcuSeek

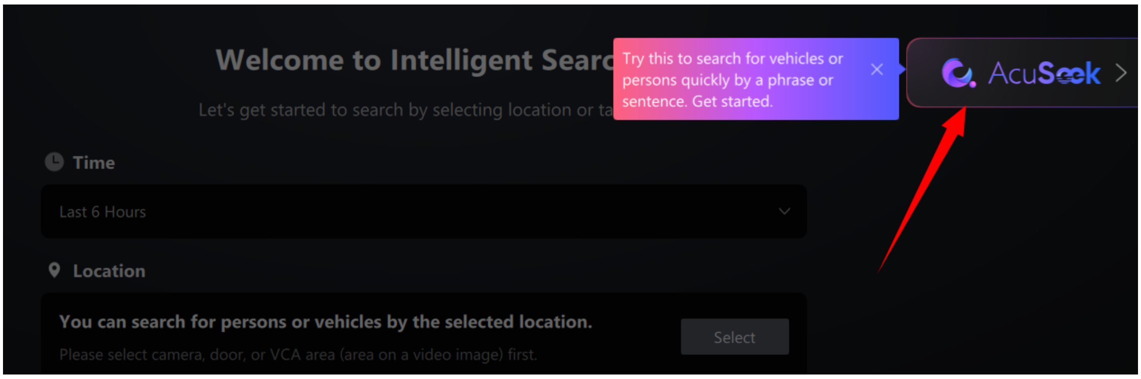
Enable AcuSearch + AcuSeek to support searching for videos of targets either matching the input text or similar to human or vehicle selected in the scene of live view or playback.

People Counting Analysis

Enable people counting to support real-time and historical data display through statistical reports.

Figure 3-33 Enable AcuSeek

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



Welcome to Intelligent Searc

Let's get started to search by selecting location or ta

Try this to search for vehicles or persons quickly by a phrase or sentence. Get started.

Last 6 Hours

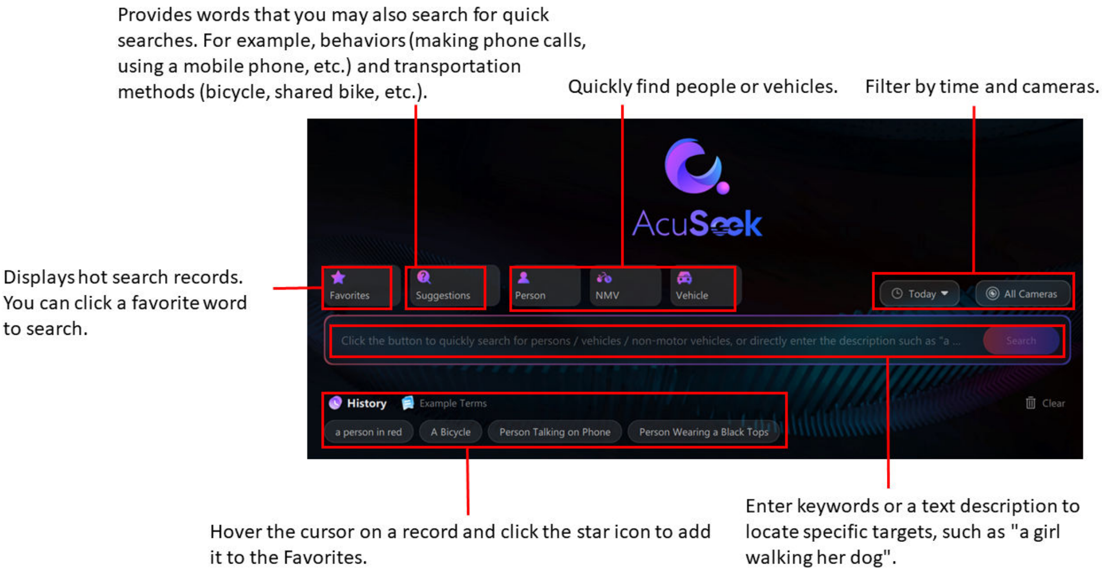
You can search for persons or vehicles by the selected location.

Please select camera, door, or VCA area (area on a video image) first.

Figure 3-34 AcuSeek Entry

Search

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



Click the button to quickly search for persons / vehicles / non-motor vehicles, or directly enter the description such as "a ...

Provides words that you may also search for quick searches. For example, behaviors (making phone calls, using a mobile phone, etc.) and transportation methods (bicycle, shared bike, etc.).

Quickly find people or vehicles.

Filter by time and cameras.

Displays hot search records. You can click a favorite word to search.

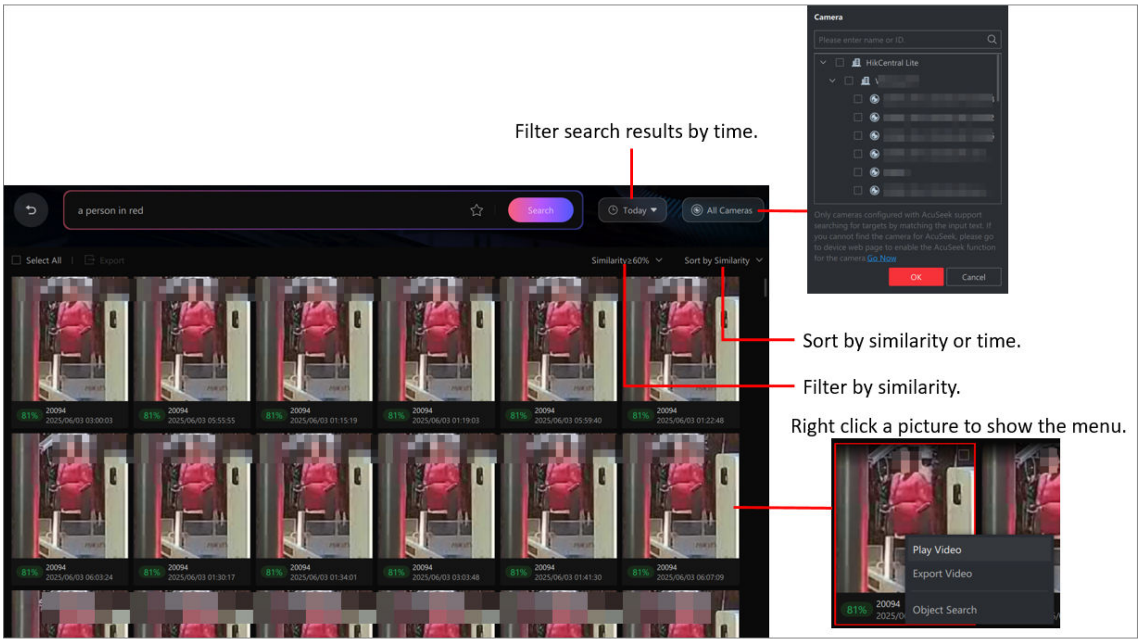
Hover the cursor on a record and click the star icon to add it to the Favorites.

Enter keywords or a text description to locate specific targets, such as "a girl walking her dog".

Figure 3-35 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 Red", you can perform the following operations:



Only cameras configured with AcuSeek support searching for targets by matching the input text. If you cannot find the camera for AcuSeek, please go to device web page to enable the AcuSeek function for the camera.Go Now

Filter search results by time.

Sort by similarity or time.

Filter by similarity.

Right click a picture to show the menu.

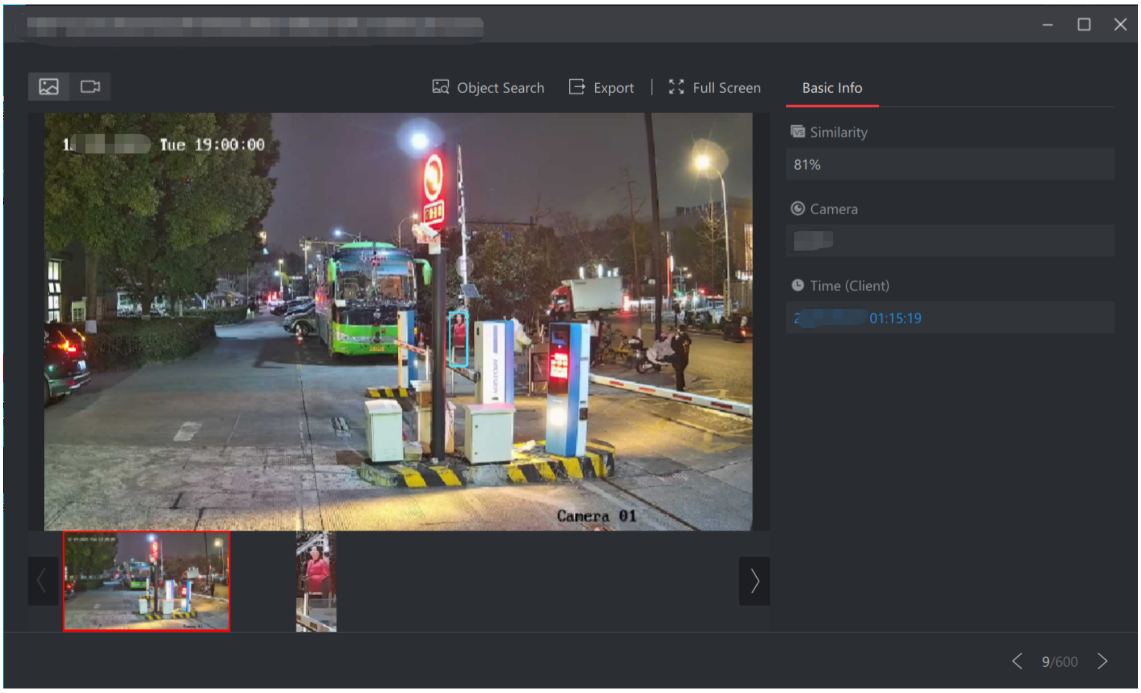
Figure 3-36 Search Results

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.



Similarity

81%

Camera

[redacted]

Time (Client)

[redacted] 01:15:19

Figure 3-37 Search Result Details

AcuSearch / Object Search

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

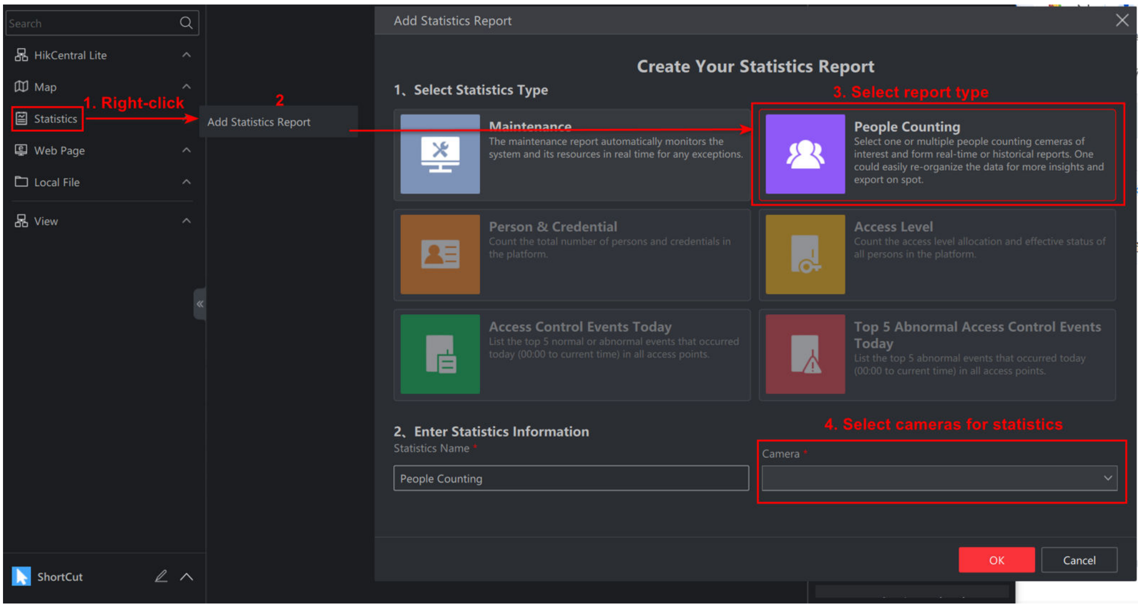
3.8 Generate and View People Counting Report

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.



Add Statistics Report

Create Your Statistics Report

1、Select Statistics Type

Maintenance
The maintenance report automatically monitors the system and its resources in real time for any exceptions.

People Counting
Select one or multiple people counting cameras of interest and form real-time or historical reports. One could easily re-organize the data for more insights and export on spot.

Person & Credential
Count the total number of persons and credentials in the platform.

Access Level
Count the access level allocation and effective status of all persons in the platform.

Access Control Events Today
List the top 5 normal or abnormal events that occurred today (00:00 to current time) in all access points.

Top 5 Abnormal Access Control Events Today
List the top 5 abnormal events that occurred today (00:00 to current time) in all access points.

2、Enter Statistics Information

Statistics Name *: People Counting

Camera *

OK Cancel

Figure 3-38 Generate People Counting Report

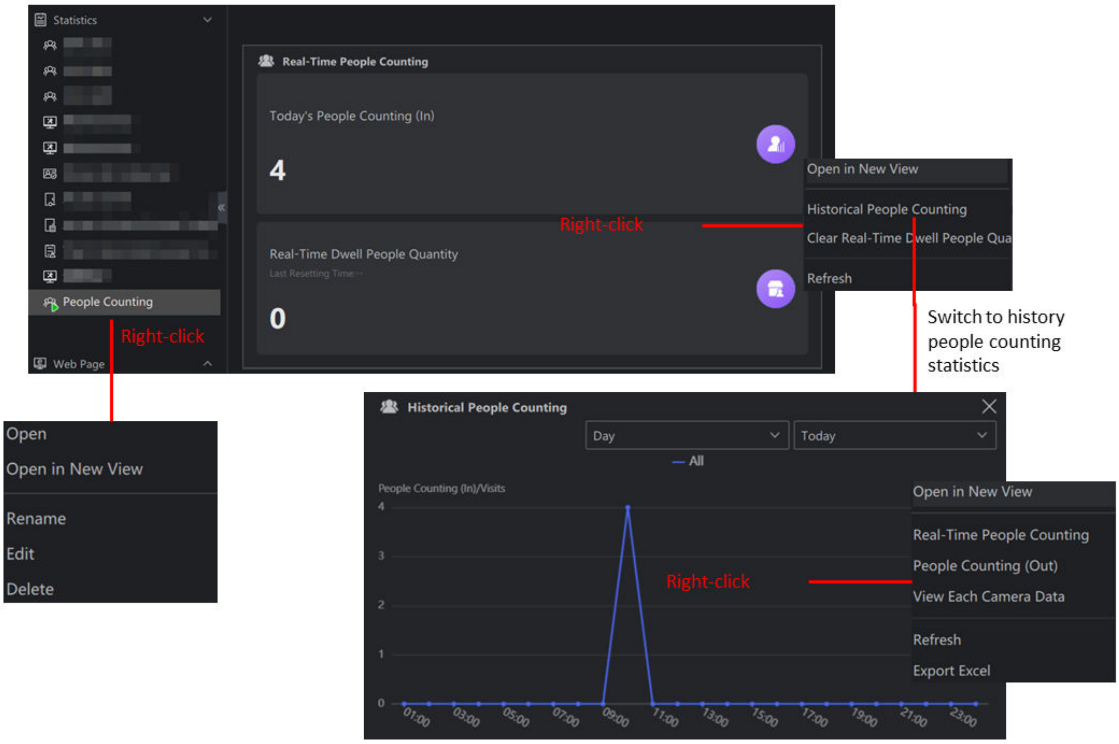
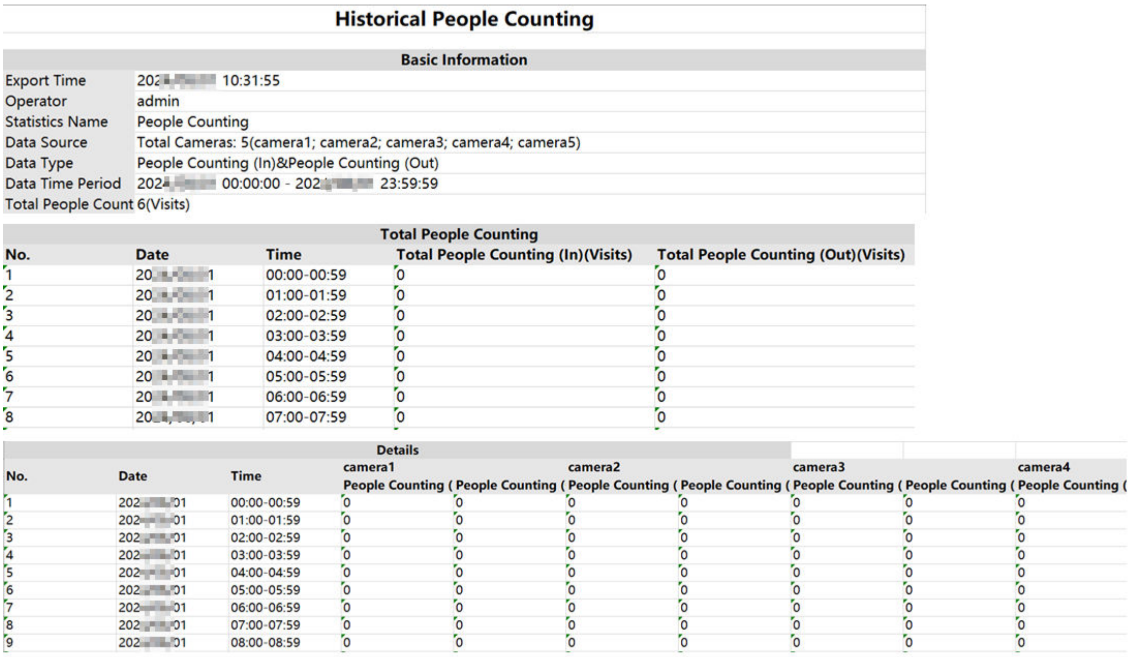


Figure 3-39 View Generated People Counting Report



Historical People Counting

Basic Information

Export Time	202[redacted] 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[redacted] 00:00:00 - 202[redacted] 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[redacted]1	00:00-00:59	0	0
2	20[redacted]1	01:00-01:59	0	0
3	20[redacted]1	02:00-02:59	0	0
4	20[redacted]1	03:00-03:59	0	0
5	20[redacted]1	04:00-04:59	0	0
6	20[redacted]1	05:00-05:59	0	0
7	20[redacted]1	06:00-06:59	0	0
8	20[redacted]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[redacted]01	00:00-00:59	0	0	0	0	0	0	0
2	202[redacted]01	01:00-01:59	0	0	0	0	0	0	0
3	202[redacted]01	02:00-02:59	0	0	0	0	0	0	0
4	202[redacted]01	03:00-03:59	0	0	0	0	0	0	0
5	202[redacted]01	04:00-04:59	0	0	0	0	0	0	0
6	202[redacted]01	05:00-05:59	0	0	0	0	0	0	0
7	202[redacted]01	06:00-06:59	0	0	0	0	0	0	0
8	202[redacted]01	07:00-07:59	0	0	0	0	0	0	0
9	202[redacted]01	08:00-08:59	0	0	0	0	0	0	0

Figure 3-40 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 or cameras) 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.
- 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.

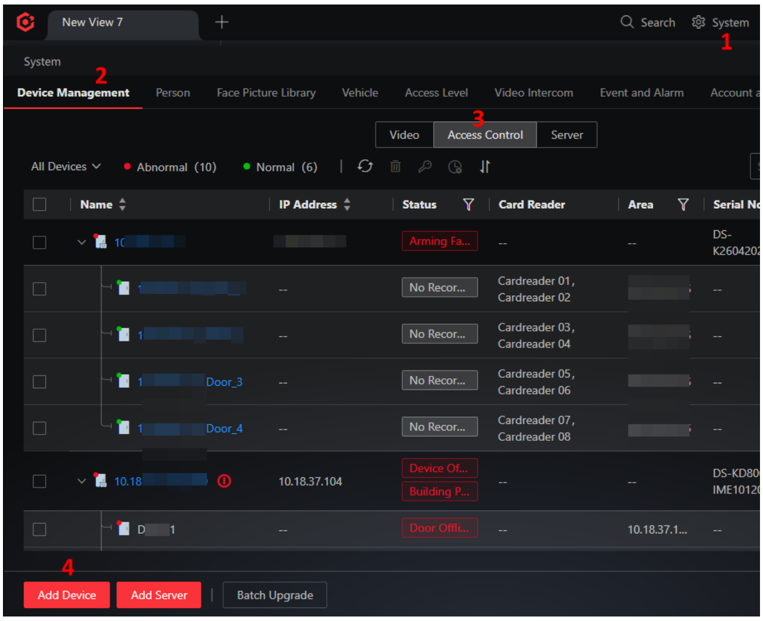
View Statistics

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.



□	Name	IP Address	Status	Card Reader	Area	Serial No
□	10[redacted]	[redacted]	Arming Fa...	--	--	DS- K2604202
□	1[redacted]	--	No Recor...	Cardreader 01, Cardreader 02	[redacted]	--
□	1[redacted]	--	No Recor...	Cardreader 03, Cardreader 04	[redacted]	--
□	1[redacted]Door_3	--	No Recor...	Cardreader 05, Cardreader 06	[redacted]	--
□	1[redacted]Door_4	--	No Recor...	Cardreader 07, Cardreader 08	[redacted]	--
□	10.18[redacted]	10.18.37.104	Device Of... Building P...	--	--	DS-KD80 IME10120
□	D[redacted]1	--	Door Offli...	--	10.18.37.1...	--

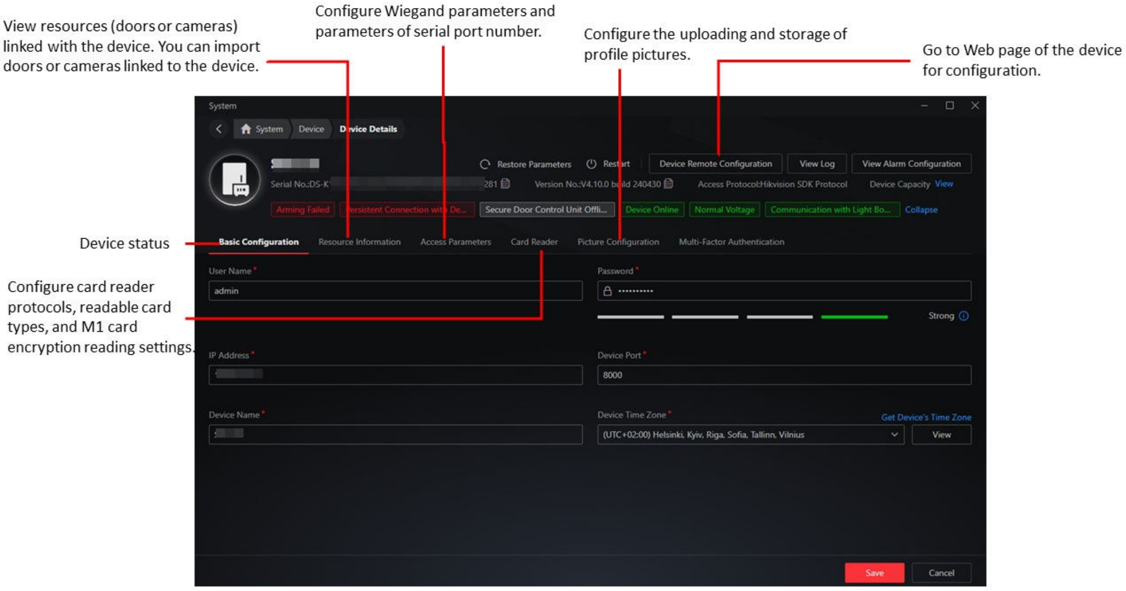
Figure 4-1 Device List

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**.


View resources (doors or cameras) linked with the device. You can import doors or cameras linked to the device.
Configure Wiegand parameters and parameters of serial port number.
Configure the uploading and storage of profile pictures.
Go to Web page of the device for configuration.
Device status
Configure card reader protocols, readable card types, and M1 card encryption reading settings.
System
System
Device
Device Details
Restore Parameters
Restart
Device Remote Configuration
View Log
View Alarm Configuration
Arming Failed
Persistent Connection with De...
Secure Door Control Unit Offli...
Device Online
Normal Voltage
Communication with Light Bo...
Collapse
Basic Configuration
Resource Information
Access Parameters
Card Reader
Picture Configuration
Multi-Factor Authentication
Strong
Get Device's Time Zone
View
Save
Cancel

[redacted]

Serial No.:DS-K[redacted]281 Version No.:V4.10.0 build 240430 Access Protocol:Hikvision SDK Protocol Device Capacity View

User Name * admin

Password * ••••••••••

IP Address * [redacted]

Device Port * 8000

Device Name * [redacted]

Device Time Zone * (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

Figure 4-2 Details of an Access Control Device

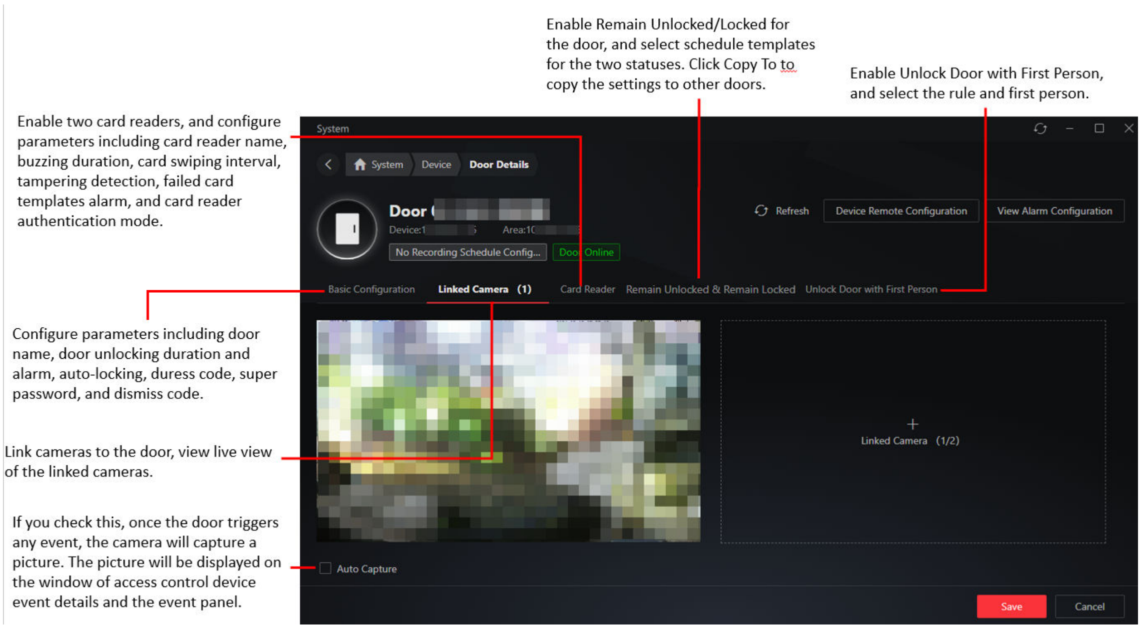
Multi-Factor Authentication

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.

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**.



Enable Remain Unlocked/Locked for the door, and select schedule templates for the two statuses. Click Copy To to copy the settings to other doors.

Enable Unlock Door with First Person, and select the rule and first person.

Enable two card readers, and configure parameters including card reader name, buzzing duration, card swiping interval, tampering detection, failed card templates alarm, and card reader authentication mode.

Configure parameters including door name, door unlocking duration and alarm, auto-locking, duress code, super password, and dismiss code.

Link cameras to the door, view live view of the linked cameras.

If you check this, once the door triggers any event, the camera will capture a picture. The picture will be displayed on the window of access control device event details and the event panel.

Figure 4-3 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.

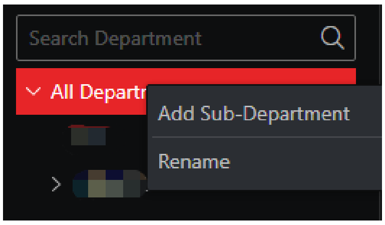


Figure 4-4 Department Tree

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

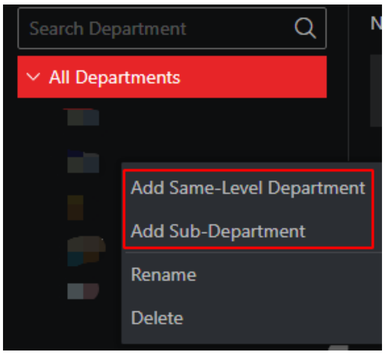
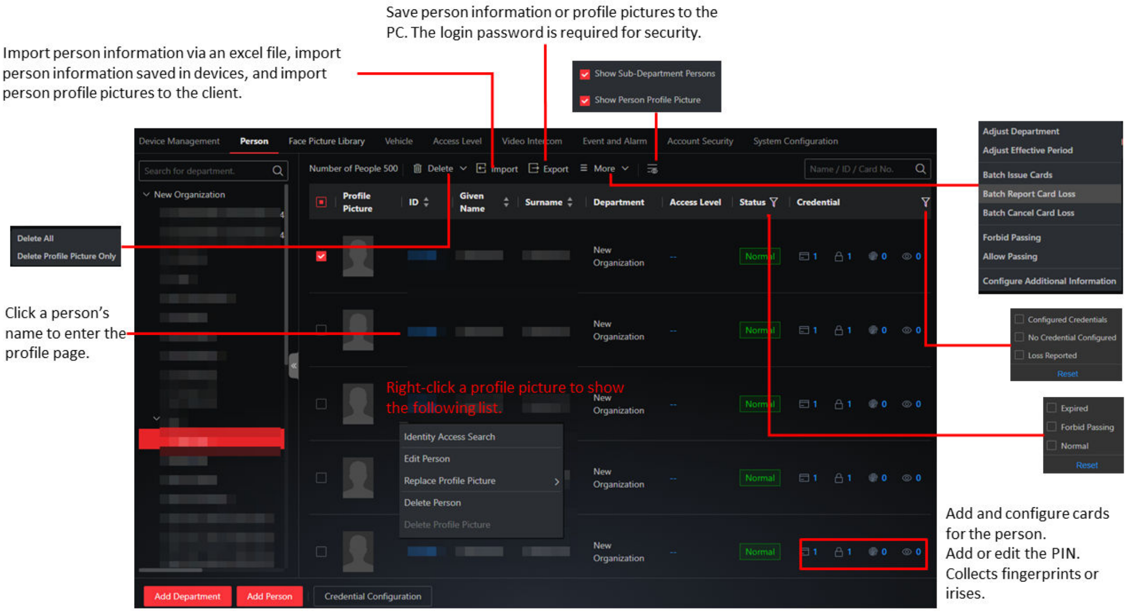


Figure 4-5 Department Tree

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

Add Persons


Save person information or profile pictures to the PC. The login password is required for security.

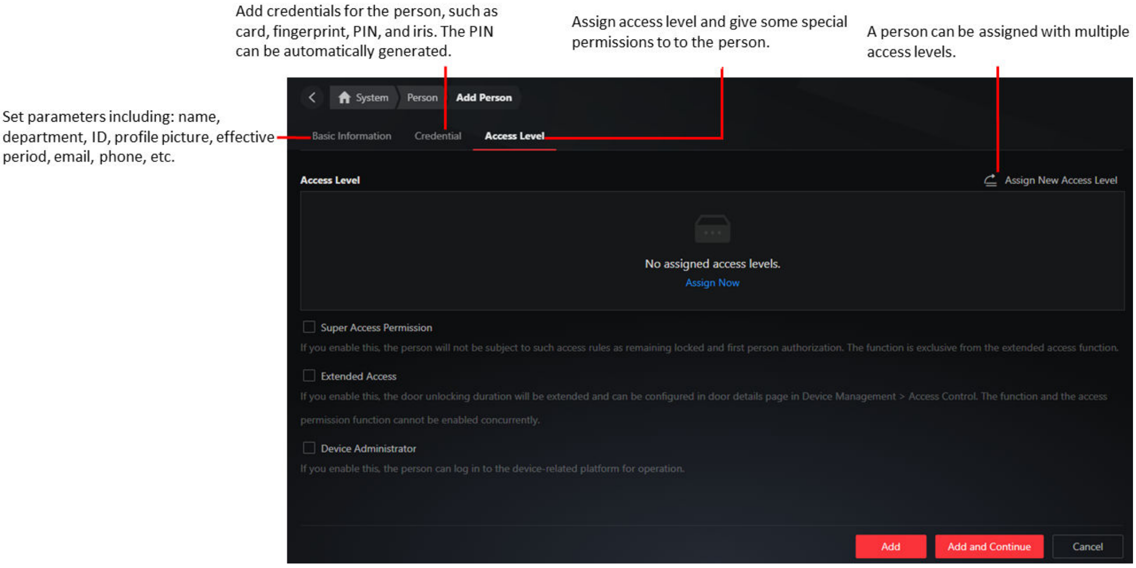
Import person information via an excel file, import person information saved in devices, and import person profile pictures to the client.

Click a person's name to enter the profile page.

Right-click a profile picture to show the following list.

Add and configure cards for the person. Add or edit the PIN. Collects fingerprints or irises.

Figure 4-6 Person List



Add credentials for the person, such as card, fingerprint, PIN, and iris. The PIN can be automatically generated.

Assign access level and give some special permissions to to the person.

A person can be assigned with multiple access levels.

Set parameters including: name, department, ID, profile picture, effective period, email, phone, etc.

□ Super Access Permission

If you enable this, the person will not be subject to such access rules as remaining locked and first person authorization. The function is exclusive from the extended access function.

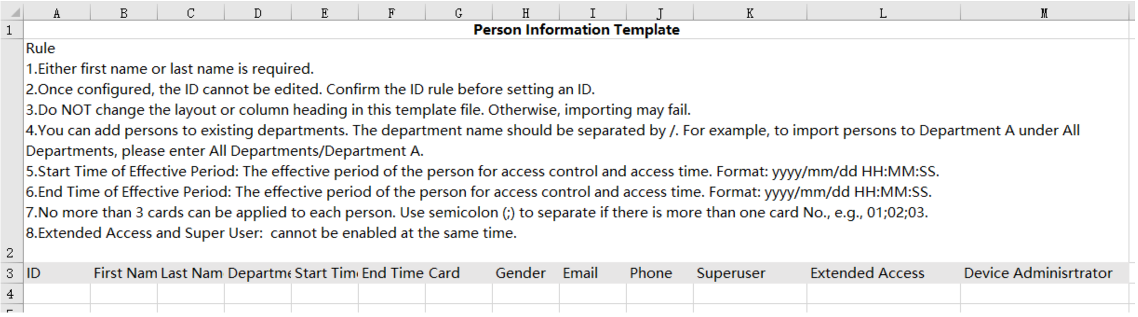
□ Extended Access

If you enable this, the door unlocking duration will be extended and can be configured in door details page in Device Management > Access Control. The function and the access permission function cannot be enabled concurrently.

□ Device Administrator

If you enable this, the person can log in to the device-related platform for operation.

Figure 4-7 Add Person Page

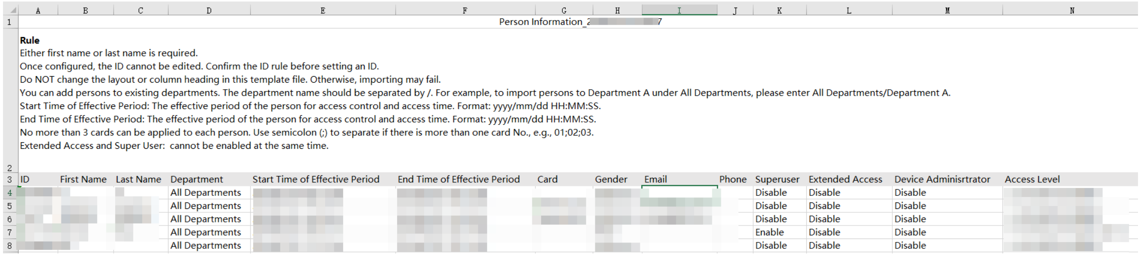


Person Information Template

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 4-8 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]			Disable	Disable	Disable	[redacted]
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		Disable	Disable	Disable	[redacted]
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		Disable	Disable	Disable	[redacted]
[redacted]	[redacted]	[redacted]	All Departments	[redacted]	[redacted]		[redacted]			Enable	Disable	Disable	[redacted]
[redacted]			All Departments	[redacted]	[redacted]		[redacted]			Disable	Disable	Disable	[redacted]

Figure 4-9 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.

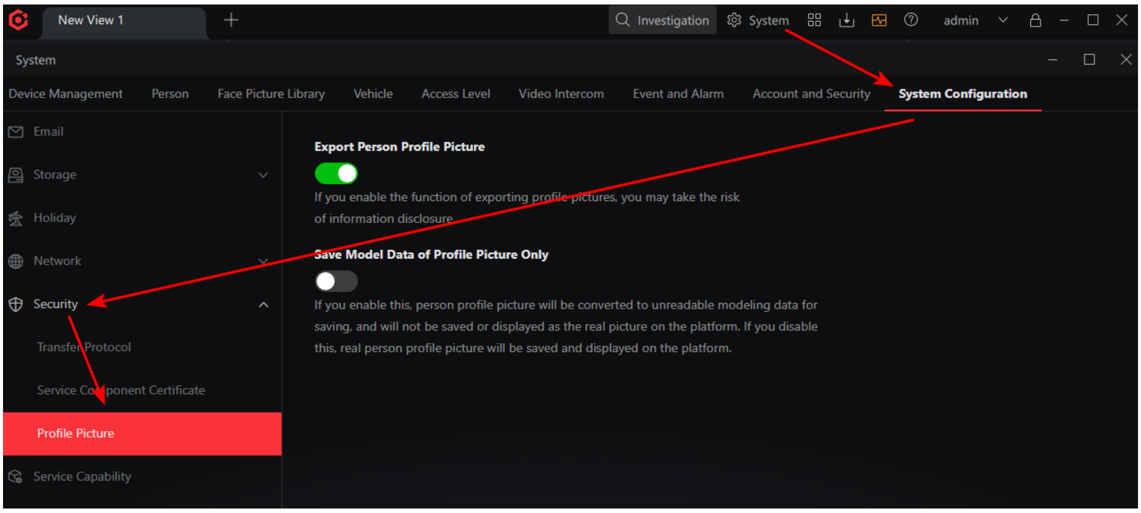
On the Person page, click **Credential Configuration**. Select a collection mode according to the following table.

Table 4-1 Scenarios Applicable for Different Collection Mode

Collection Device	Scenario
• Card Enroller • Fingerprint Enroller • 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.



Export Person Profile Picture

If you enable the function of exporting profile pictures, you may take the risk of information disclosure.

Save Model Data of Profile Picture Only

If you enable this, person profile picture will be converted to unreadable modeling data for saving, and will not be saved or displayed as the real picture on the platform. If you disable this, real person profile picture will be saved and displayed on the platform.

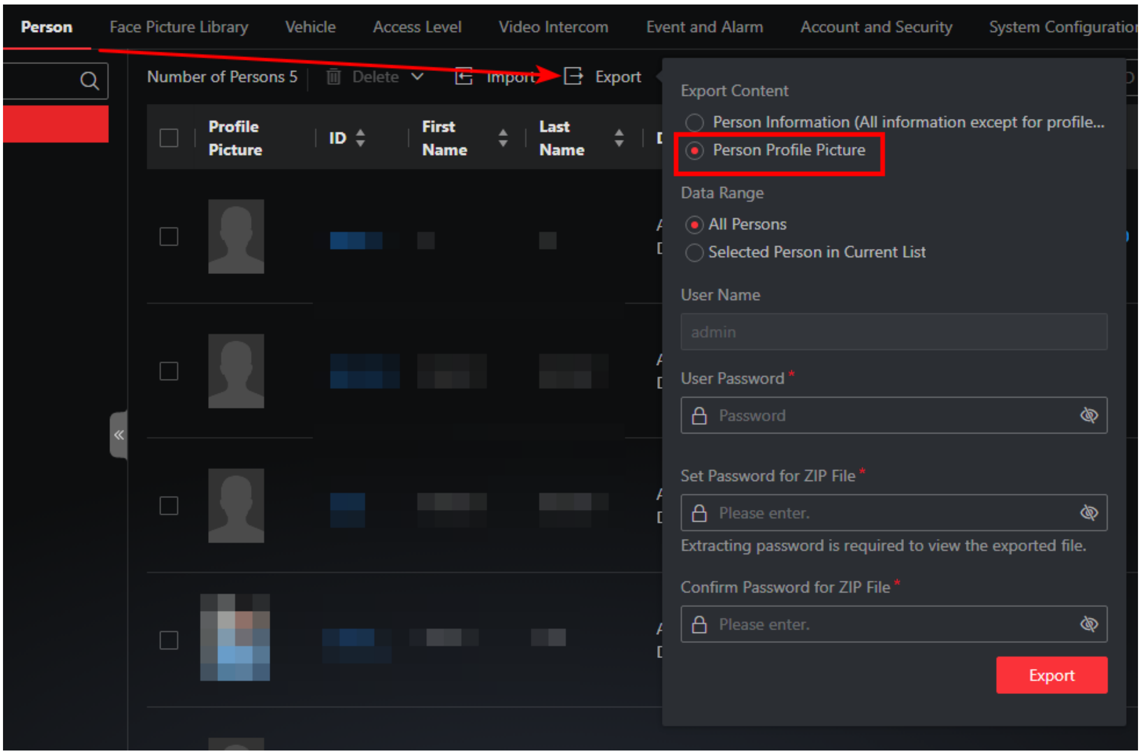
Figure 4-10 Entry of Protect Profile Pictures

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.



Export Content

○ Person Information (All information except for profile...

● Person Profile Picture

Data Range

● All Persons

○ Selected Person in Current List

User Name: admin

User Password *: Password

Set Password for ZIP File *: Please enter.

Extracting password is required to view the exported file.

Confirm Password for ZIP File *: Please enter.

Export

Figure 4-11 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.

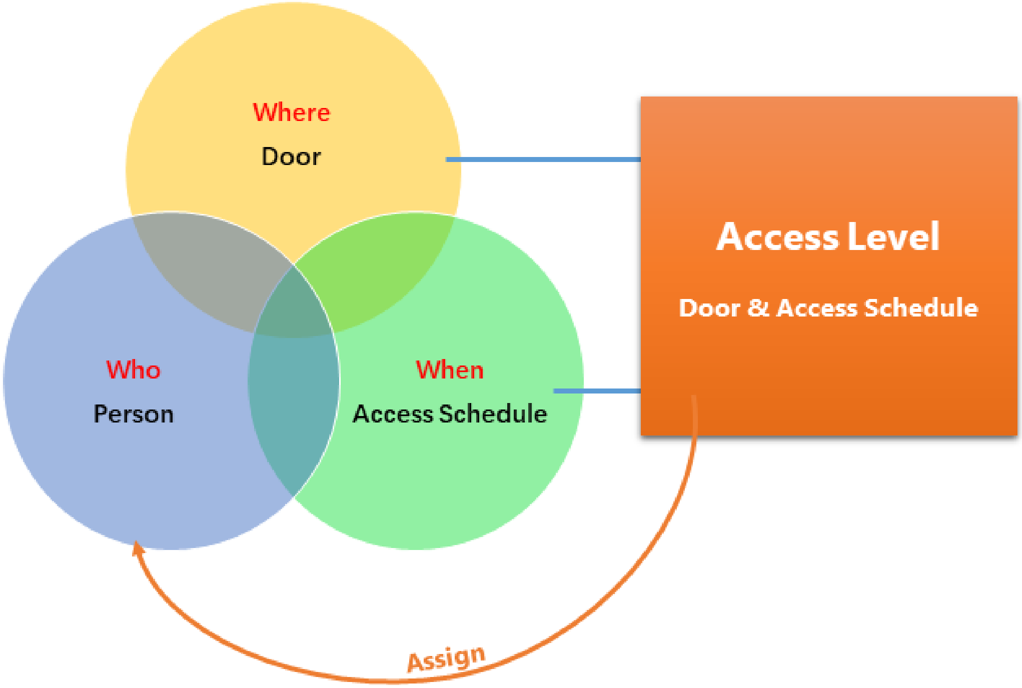


Figure 4-12 Access Level

Be careful using this function because the access levels stored in devices will be cleared and cannot be restored!

Access level overview

Right-click a department to assign a new access level or clear the person access levels.

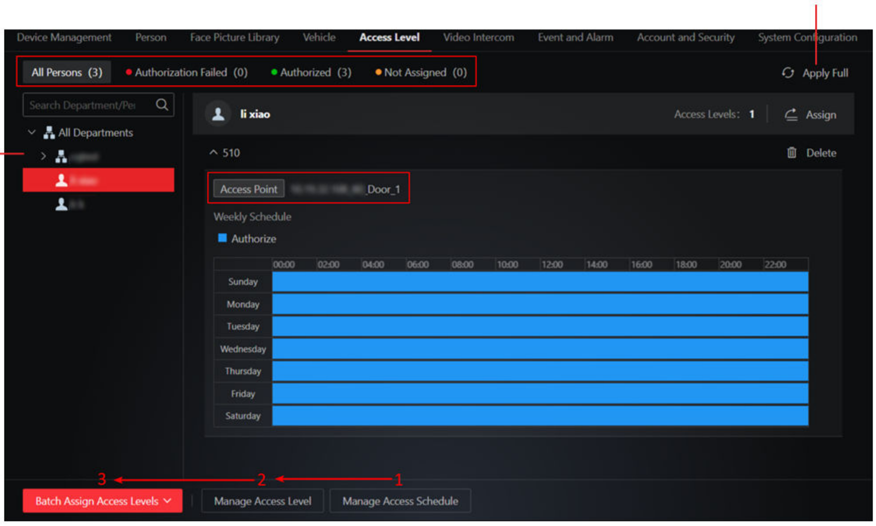
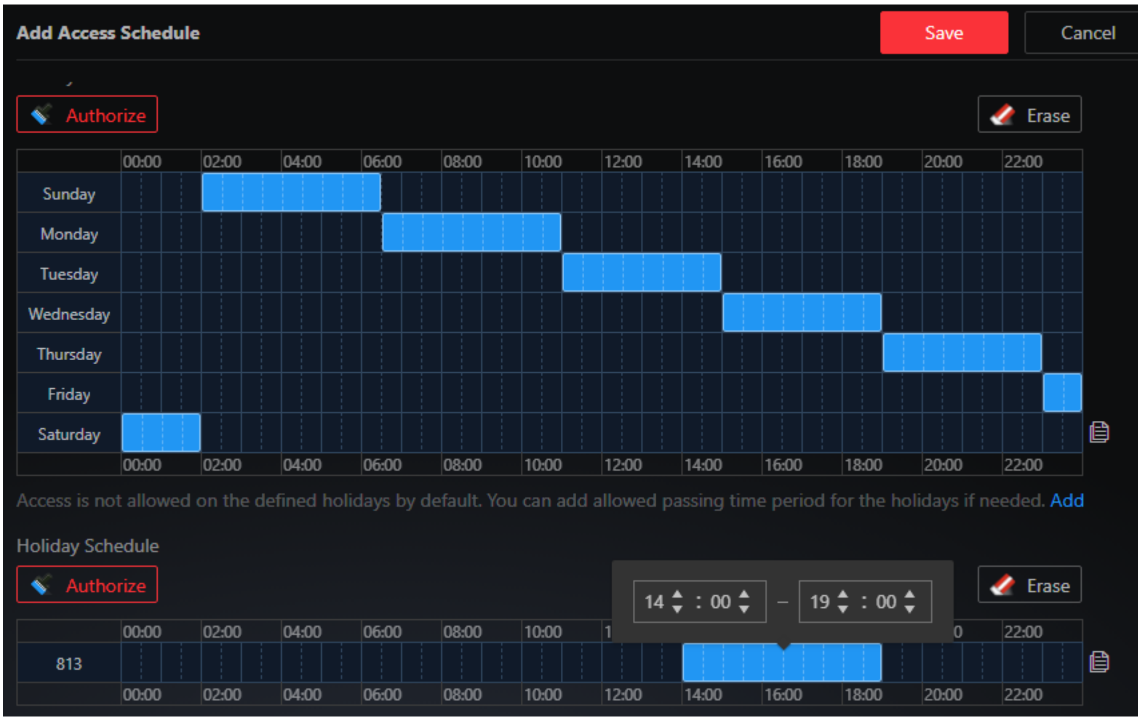


Figure 4-13 Access Level Page

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.



Access is not allowed on the defined holidays by default. You can add allowed passing time period for the holidays if needed. Add

Figure 4-14 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.

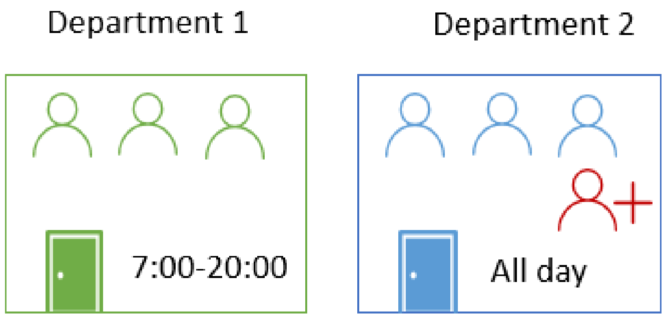


Figure 4-15 Assign Access Level by Department

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.

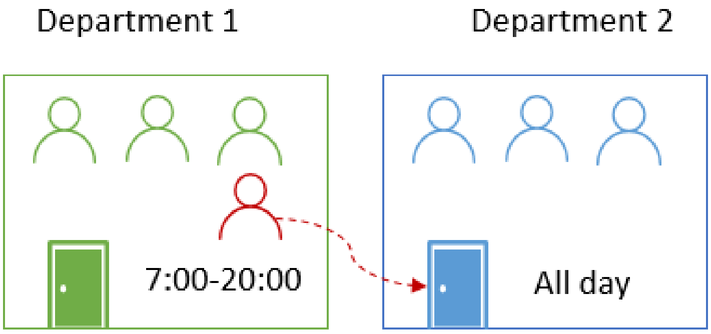


Figure 4-16 Assign Access Level by Person

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.

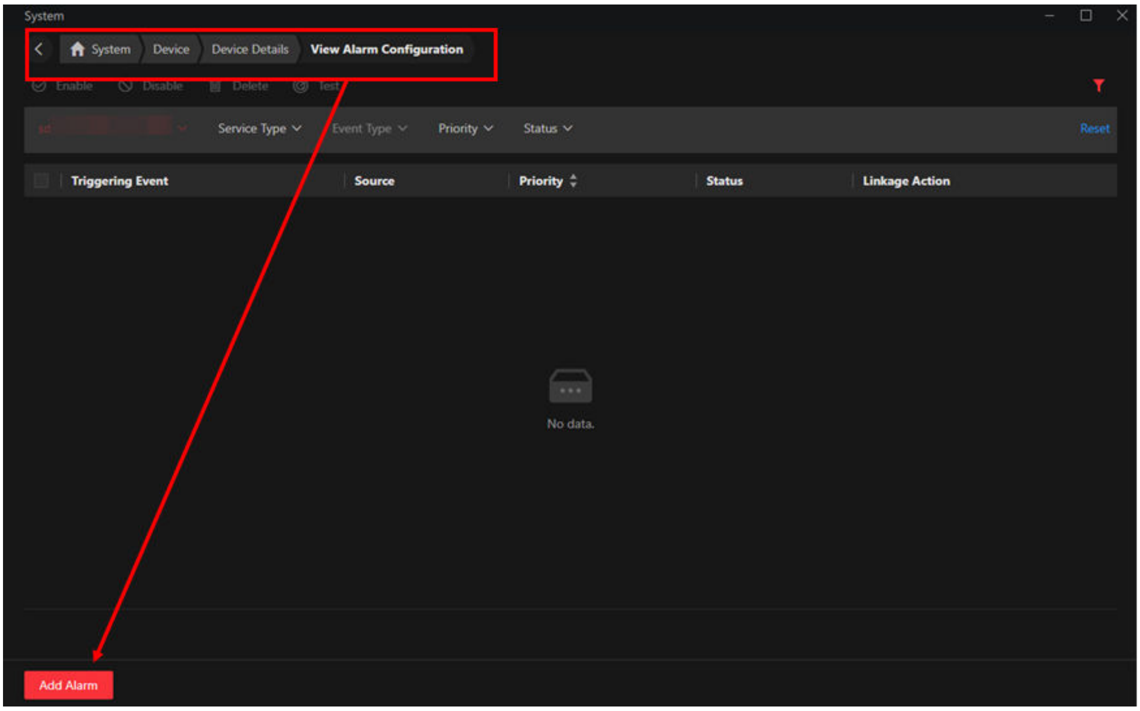


Figure 4-17 Alarm Configuration Page

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

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 of door status.

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

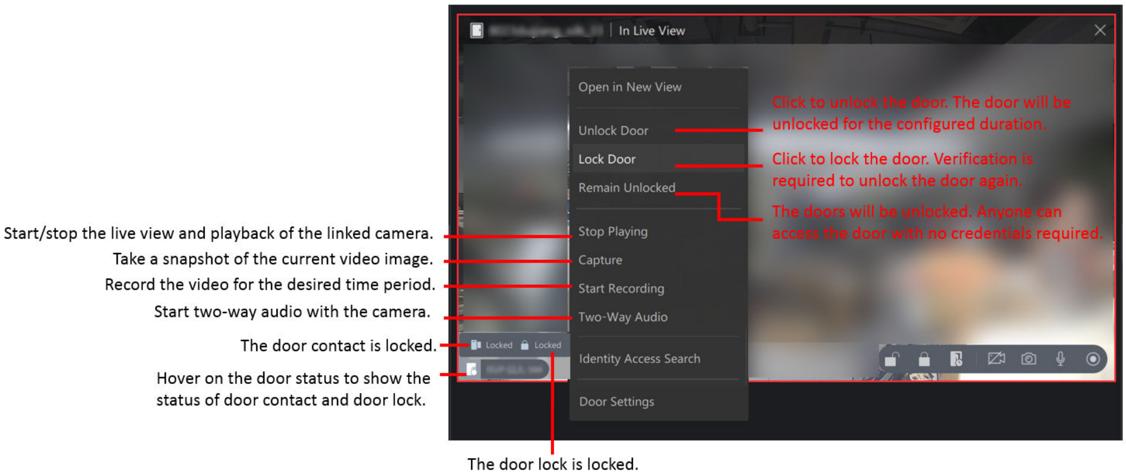
Status	Icon	Explanation
Door Status	🚪🔒	Door Locked Door Lock Locked
	🚪🔒	Door Locked Door Lock Remain Locked
	🚪🔓	Door Locked Door Lock Unlocked
	🚪🔓	Door Locked Door Lock Remain Unlocked
	🚪🔒	Door Unlocked Door Lock Locked
	🚪🔒	Door Unlocked Door Lock Remain Locked
	🚪🔓	Door Unlocked Door Lock Unlocked
	🚪🔓	Door Unlocked Door Lock Remain Unlocked
	?	Unknown
Door Contact Status	▮▮	Door Contact Unlocked
	▮▮	Door Contact Locked
Door Lock Status	🔓	Door Lock Unlocked
	🔒	Door Lock Locked

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.



Click to unlock the door. The door will be unlocked for the configured duration.

Click to lock the door. Verification is required to unlock the door again.

The doors will be unlocked. Anyone can access the door with no credentials required.

Start/stop the live view and playback of the linked camera.

Take a snapshot of the current video image.

Record the video for the desired time period.

Start two-way audio with the camera.

The door contact is locked.

Hover on the door status to show the status of door contact and door lock.

The door lock is locked.

Figure 4-18 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.

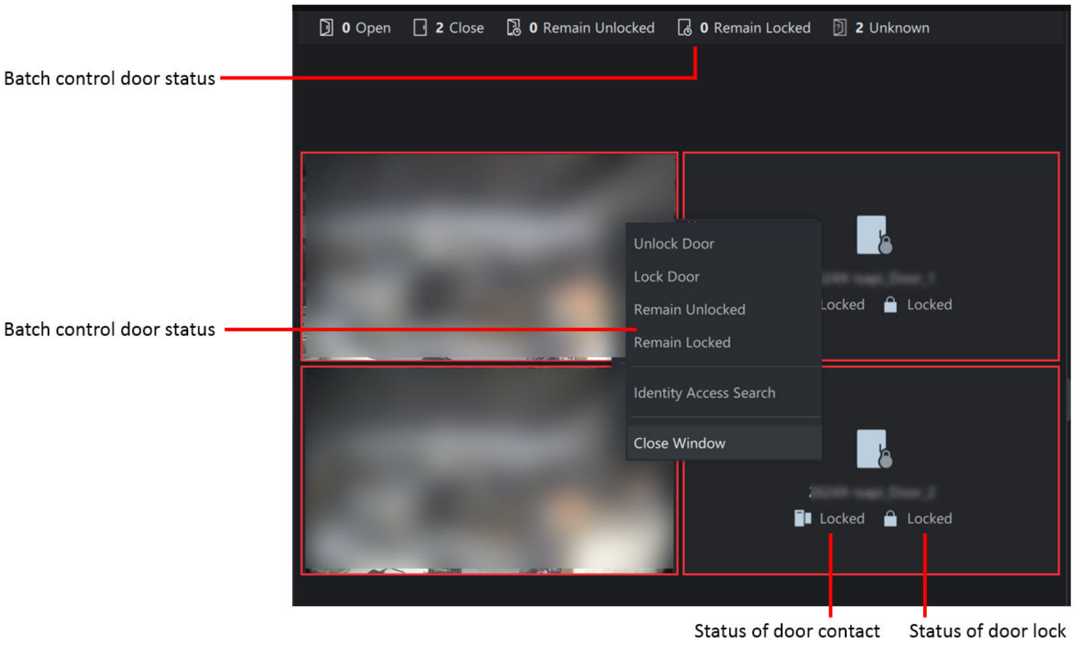


Figure 4-19 Select a Way to Control Doors on The Current View

- 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.

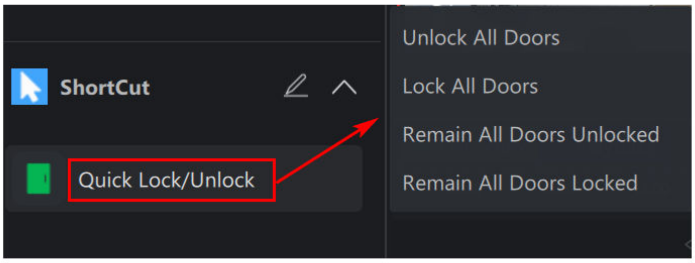


Figure 4-20 The Entry to Control All Doors

4.5.2 Display and Control Doors on the Map

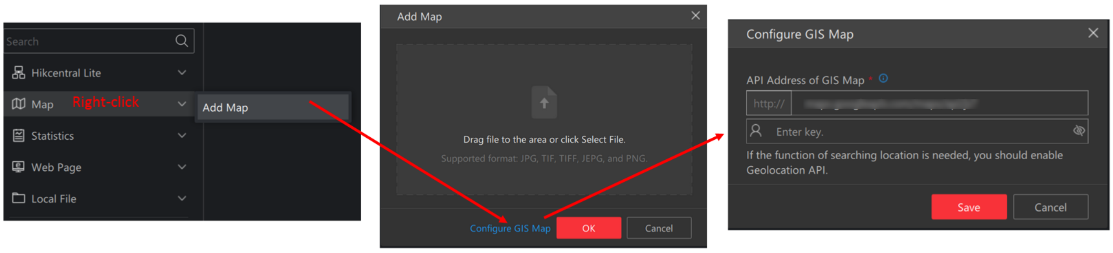
After adding doors to the map, you can control door status such as locking and unlocking doors. For the doors of MinMoe face recognition terminal or doors linked with cameras, you can also monitor doors and perform more operations during monitoring such as capturing and recording.

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

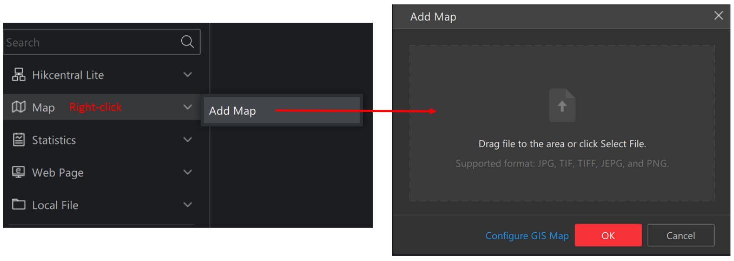


Drag file to the area or click Select File.

Supported format: JPG, TIF, TIFF, JEPG, and PNG.

If the function of searching location is needed, you should enable Geolocation API.

Figure 4-21 Add GIS Map

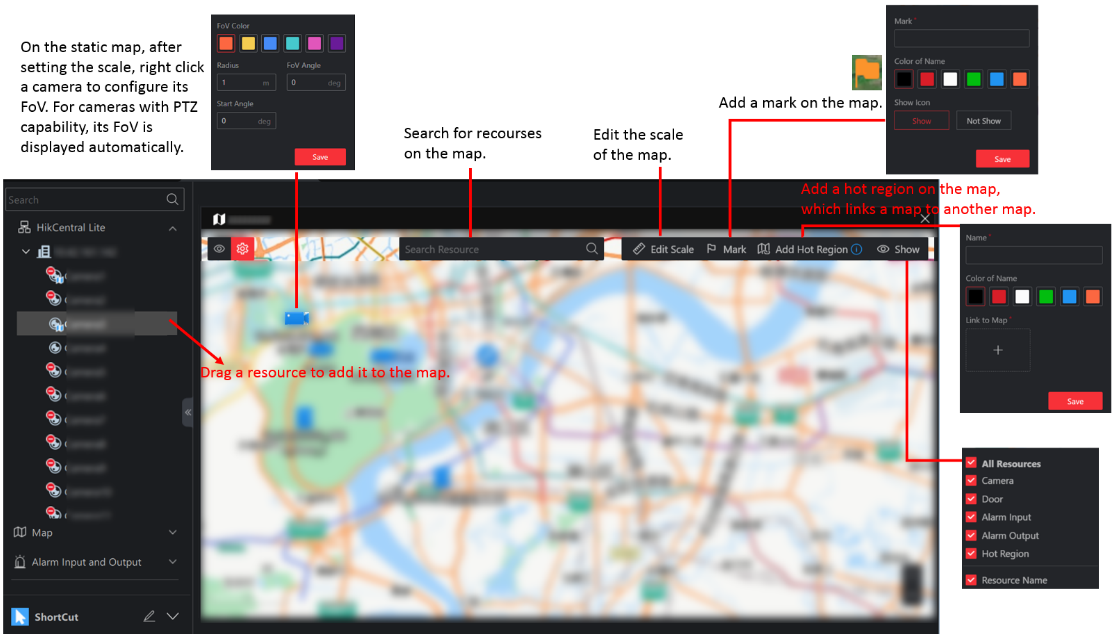


Drag file to the area or click Select File.

Supported format: JPG, TIF, TIFF, JEPG, and PNG.

Figure 4-22 Add E-Map

Configuration Mode



On the static map, after setting the scale, right click a camera to configure its FoV. For cameras with PTZ capability, its FoV is displayed automatically.

Search for recourses on the map.

Edit the scale of the map.

Add a mark on the map.

Add a hot region on the map, which links a map to another map.

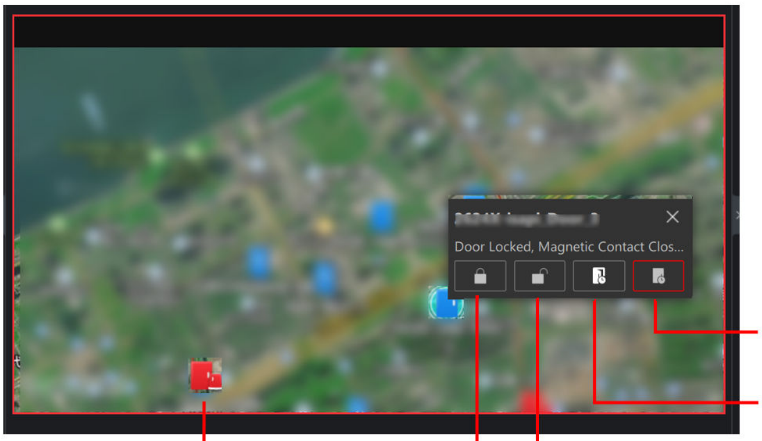
Drag a resource to add it to the map.

Figure 4-23 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.



The door will be closed and locked with no one except for users with super access permission can access.

The doors will be unlocked. Anyone can access the door with no credentials required.

Click to unlock the door. The door will be unlocked for the configured duration.

Click to lock the door. Verification is required to unlock the door again.

There is alarm not acknowledged.

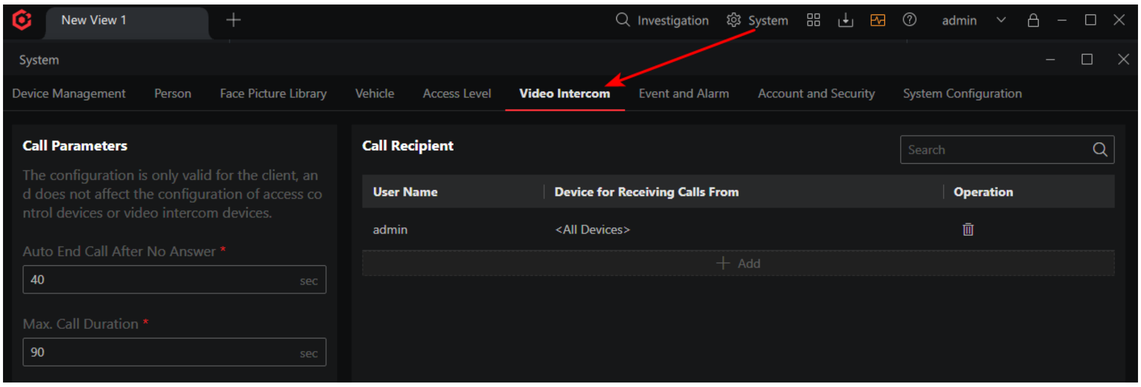
Figure 4-24 Control One Door

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.



Call Parameters

The configuration is only valid for the client, and does not affect the configuration of access control devices or video intercom devices.

Auto End Call After No Answer *: 40 sec

Max. Call Duration *: 90 sec

Call Recipient

Search

User Name	Device for Receiving Calls From	Operation
admin	<All Devices>	🗑

+ Add

Figure 4-25 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.

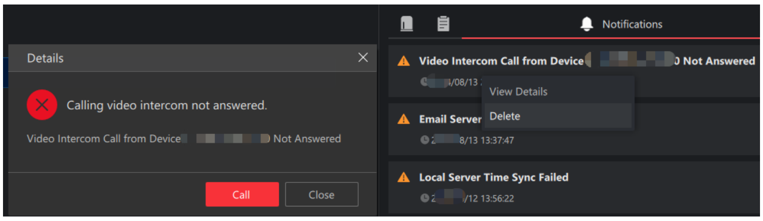
Call Recipient

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.



Details

Calling video intercom not answered.

Video Intercom Call from Device [redacted] Not Answered

Notifications

Video Intercom Call from Device [redacted] Not Answered

[redacted]/08/13

Email Server

[redacted]8/13 13:37:47

Local Server Time Sync Failed

[redacted]/12 13:56:22

Figure 4-26 Call Device

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

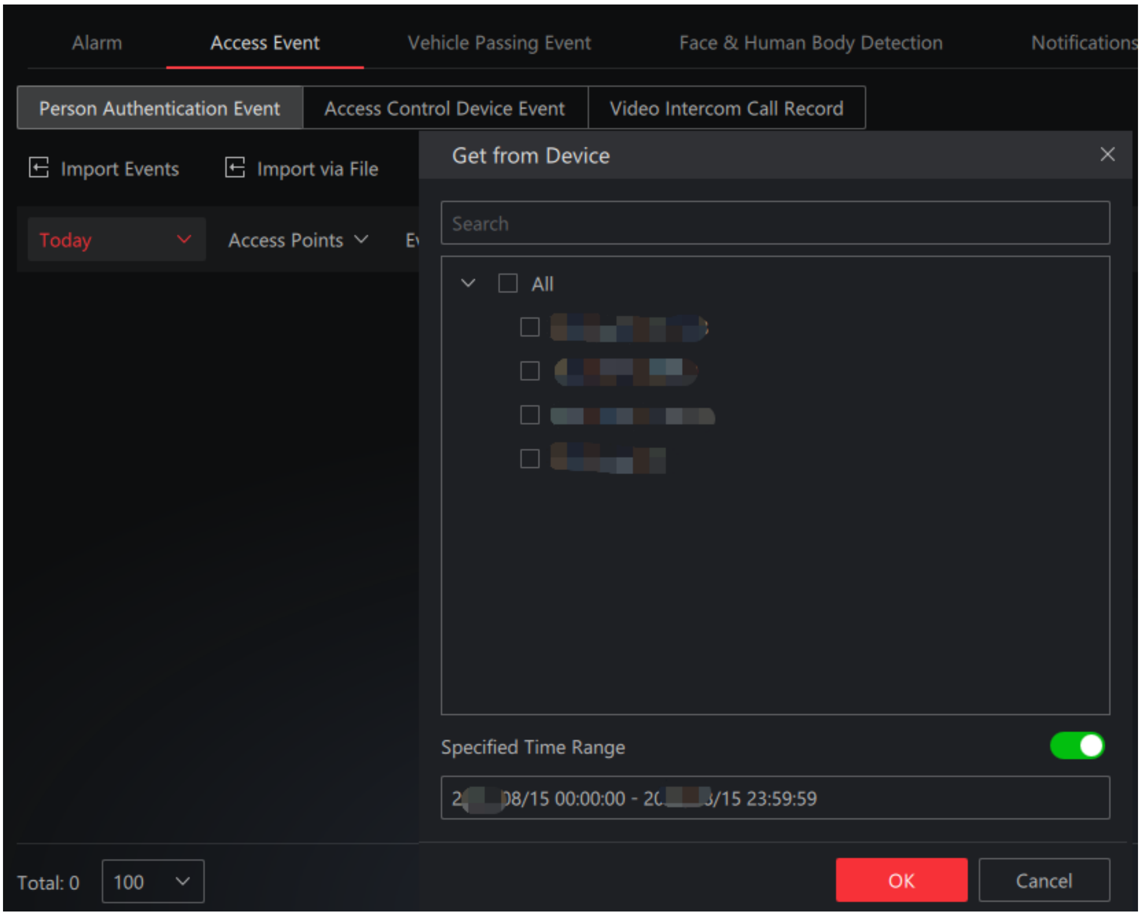
For details about how to search for video intercom call records, see ***Search for Video Intercom Call Records*** .

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.



☐ All

☐ [redacted]

☐ [redacted]

☐ [redacted]

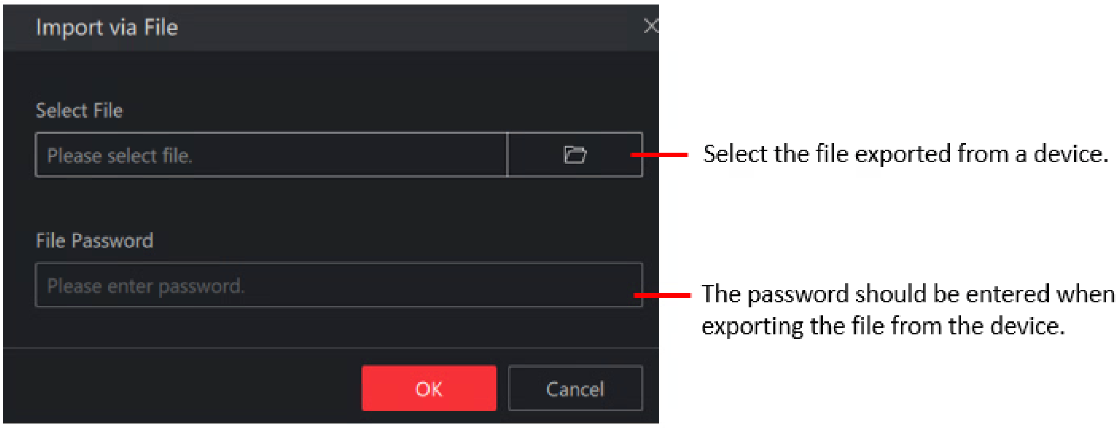
☐ [redacted]

Specified Time Range: on

2[redacted]08/15 00:00:00 - 20[redacted]3/15 23:59:59

Figure 4-27 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.



Import via File

Select File

Please select file.

File Password

Please enter password.

Select the file exported from a device.

The password should be entered when exporting the file from the device.

Figure 4-28 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.

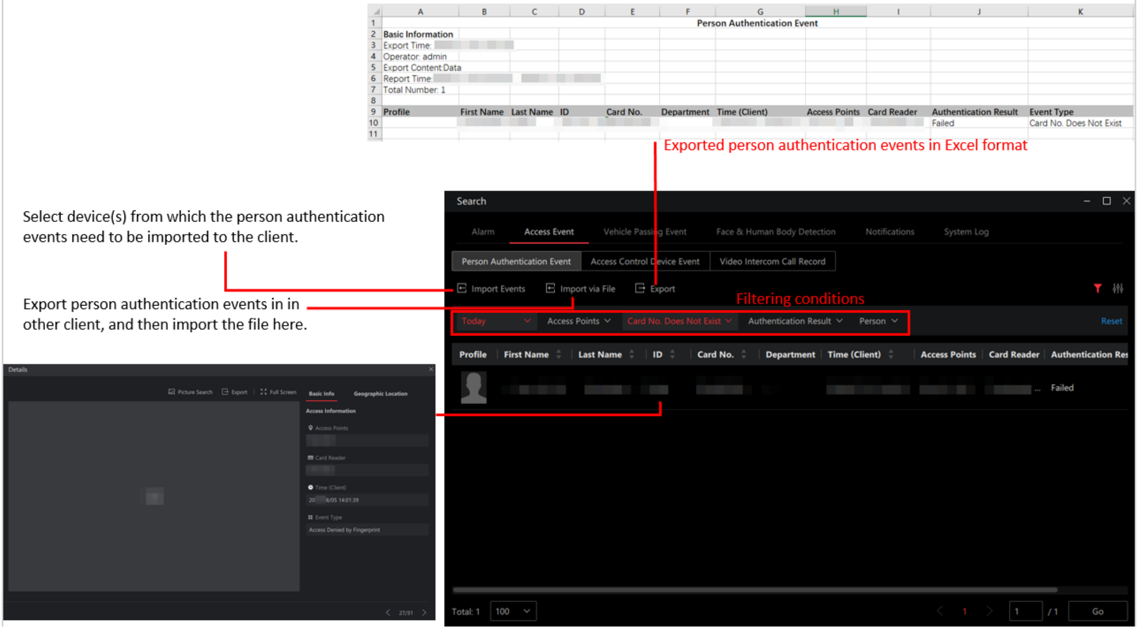
4.8 Search for Access Events

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.



	A	B	C	D	E	F	G	H	I	J	K
1	Person Authentication Event										
2	Basic Information										
3	Export Time: [redacted]										
4	Operator: admin										
5	Export Content:Data										
6	Report Time: [redacted]										
7	Total Number: 1										
8											
9	Profile	First Name	Last Name	ID	Card No.	Department	Time (Client)	Access Points	Card Reader	Authentication Result	Event Type
10		[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	Failed	Card No. Does Not Exist
11											

Exported person authentication events in Excel format

Select device(s) from which the person authentication events need to be imported to the client.

Export person authentication events in in other client, and then import the file here.

Filtering conditions

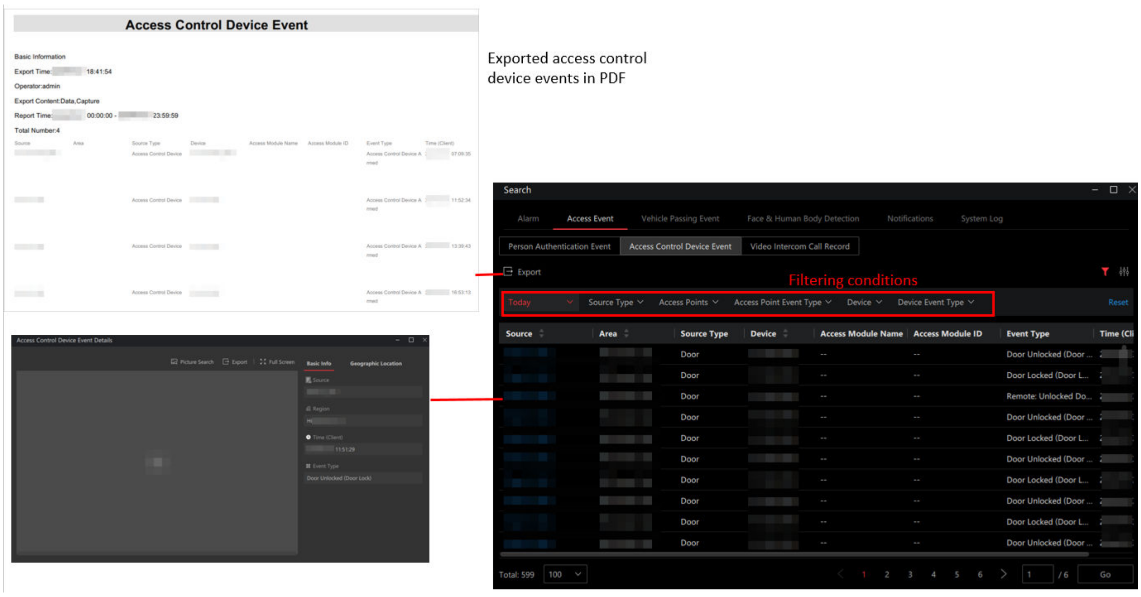
Profile	First Name	Last Name	ID	Card No.	Department	Time (Client)	Access Points	Card Reader	Authentication Res
	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	Failed

Access Denied by Fingerprint

Figure 4-29 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.



Access Control Device Event

Basic Information
Export Time: [redacted] 18:41:54
Operator:admin
Export Content:Data,Capture
Report Time: [redacted] 00:00:00 - [redacted] 23:59:59
Total Number:4

Exported access control device events in PDF

Filtering conditions

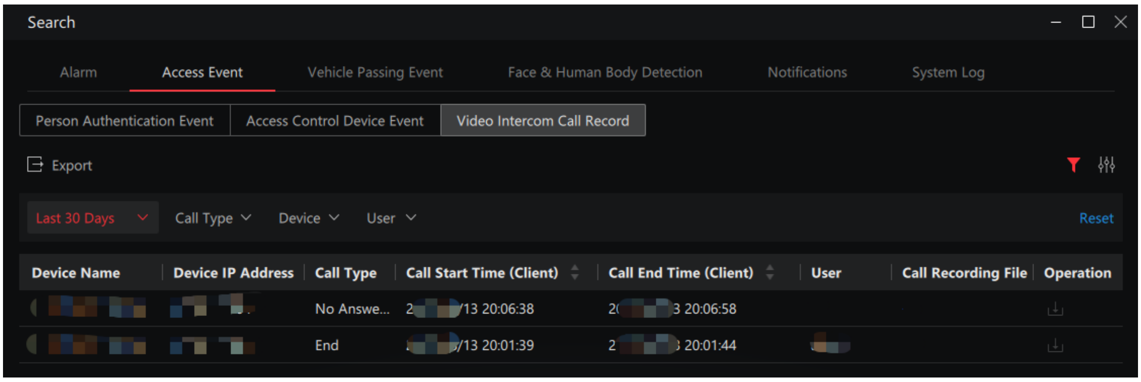
Source	Area	Source Type	Device	Access Module Name	Access Module ID	Event Type	Time (Cli
[redacted]	[redacted]	Door	[redacted]	--	--	Door Unlocked (Door ...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Locked (Door L...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Remote: Unlocked Do...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Unlocked (Door ...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Locked (Door L...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Unlocked (Door ...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Locked (Door L...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Unlocked (Door ...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Locked (Door L...	[redacted]
[redacted]	[redacted]	Door	[redacted]	--	--	Door Unlocked (Door ...	[redacted]

Door Unlocked (Door Lock)

Figure 4-30 Access Control Device Event

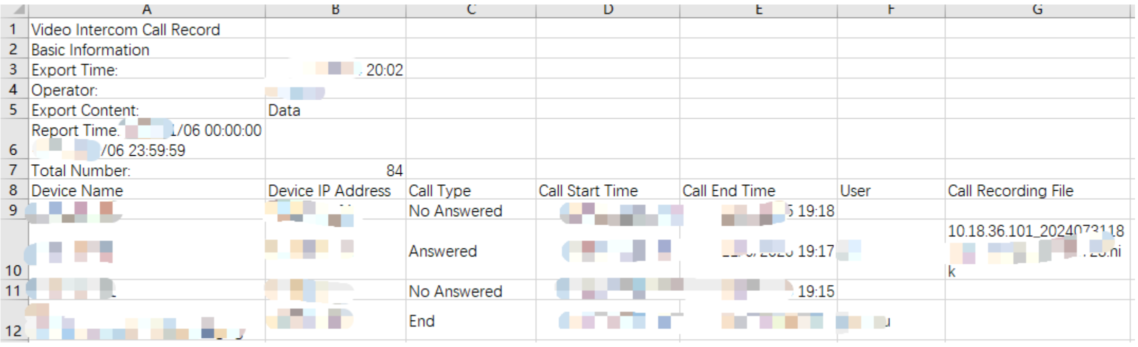
Search for Video Intercom Call Records

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.



Device Name	Device IP Address	Call Type	Call Start Time (Client)	Call End Time (Client)	User	Call Recording File	Operation
[redacted]	[redacted]	No Answe...	2[redacted]/13 20:06:38	2([redacted]3 20:06:58			⇩
[redacted]	[redacted]	End	[redacted]/13 20:01:39	2[redacted]3 20:01:44	[redacted]		⇩

Figure 4-31 Video Intercom Call Records

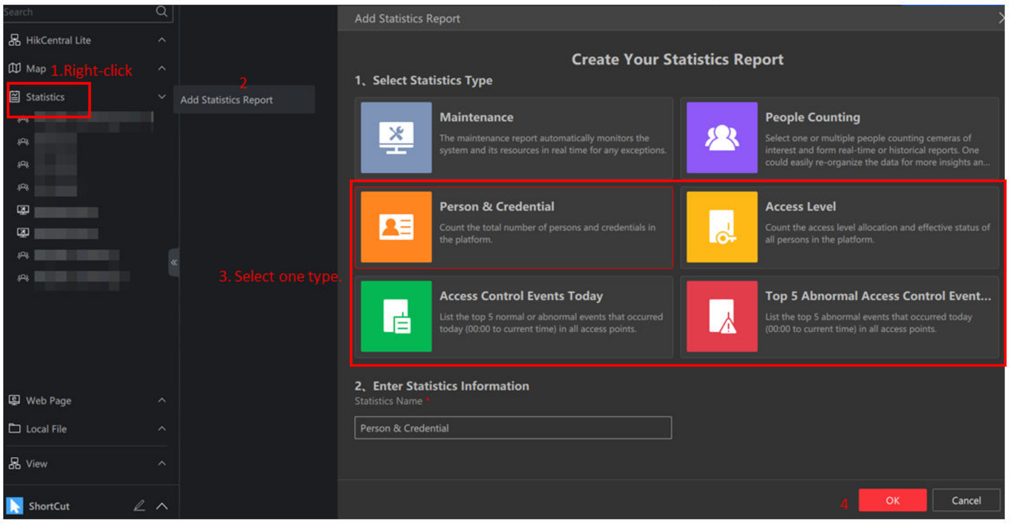


	A	B	C	D	E	F	G
1	Video Intercom Call Record						
2	Basic Information						
3	Export Time:	[redacted] 20:02					
4	Operator:	[redacted]					
5	Export Content:	Data					
6	Report Time:[redacted]1/06 00:00:00 [redacted]/06 23:59:59						
7	Total Number:	84					
8	Device Name	Device IP Address	Call Type	Call Start Time	Call End Time	User	Call Recording File
9	[redacted]	[redacted]	No Answered	[redacted]	[redacted]5 19:18		
10	[redacted]	[redacted]	Answered	[redacted]	[redacted] 19:17	[redacted]	10.18.36.101_2024073118[redacted]k
11	[redacted]	[redacted]	No Answered	[redacted]	[redacted] 19:15		
12	[redacted]	[redacted]	End	[redacted]	[redacted]	[redacted]	

Figure 4-32 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.



Add Statistics Report

Create Your Statistics Report

1、Select Statistics Type

Maintenance
The maintenance report automatically monitors the system and its resources in real time for any exceptions.

People Counting
Select one or multiple people counting cameras of interest and form real-time or historical reports. One could easily re-organize the data for more insights an...

Person & Credential
Count the total number of persons and credentials in the platform.

Access Level
Count the access level allocation and effective status of all persons in the platform.

Access Control Events Today
List the top 5 normal or abnormal events that occurred today (00:00 to current time) in all access points.

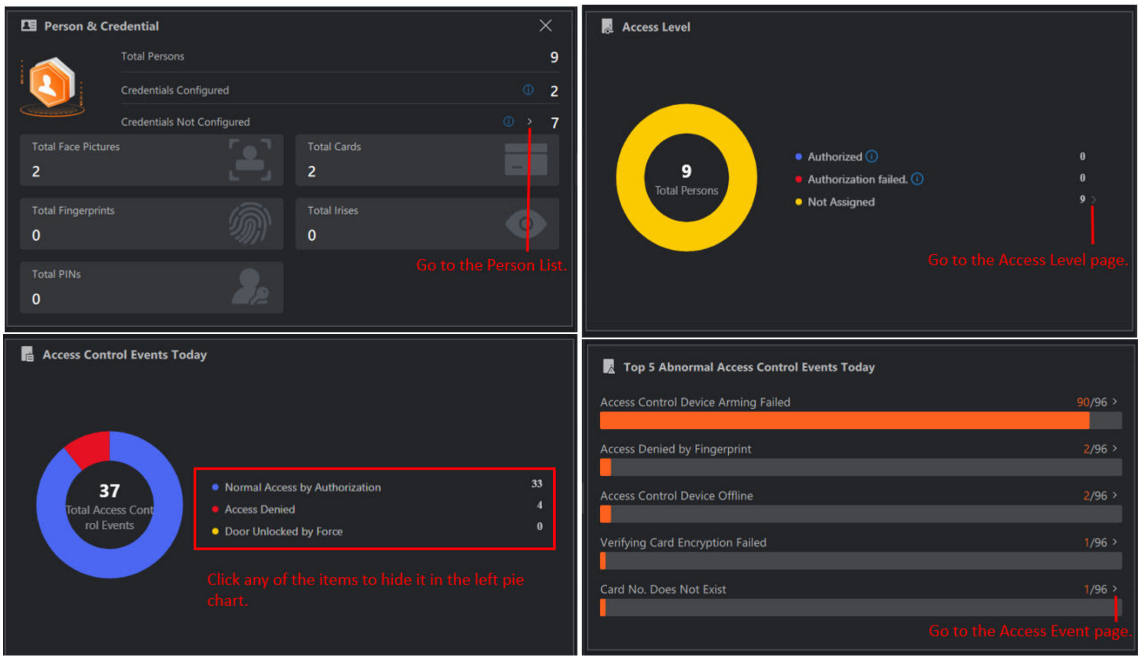
Top 5 Abnormal Access Control Event...
List the top 5 abnormal events that occurred today (00:00 to current time) in all access points.

2、Enter Statistics Information

Statistics Name *

Person & Credential

Figure 4-33 Add Statistics Report



Go to the Person List.
Go to the Access Level page.
Click any of the items to hide it in the left pie chart.
Go to the Access Event page.
37
Total Access Control Events
9
Total Persons

Person & Credential

Total Persons	9
Credentials Configured	2
Credentials Not Configured	7
Total Face Pictures	2
Total Cards	2
Total Fingerprints	0
Total Irises	0
Total PINs	0

Access Level

● Authorized	0
● Authorization failed.	0
● Not Assigned	9

Access Control Events Today

● Normal Access by Authorization	33
● Access Denied	4
● Door Unlocked by Force	0

Top 5 Abnormal Access Control Events Today

Access Control Device Arming Failed	90/96
Access Denied by Fingerprint	2/96
Access Control Device Offline	2/96
Verifying Card Encryption Failed	1/96
Card No. Does Not Exist	1/96

Figure 4-34 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 Storage

System storage offers a comprehensive solution for storing videos, pictures, and files on server disks. It allows you to allocate storage space for videos and pictures/files and configure recording schedules for cameras, ensuring efficient and effective storage management. In addition, you can specify the period of keeping data (such as logs, events, records, and analysis data) on the system.

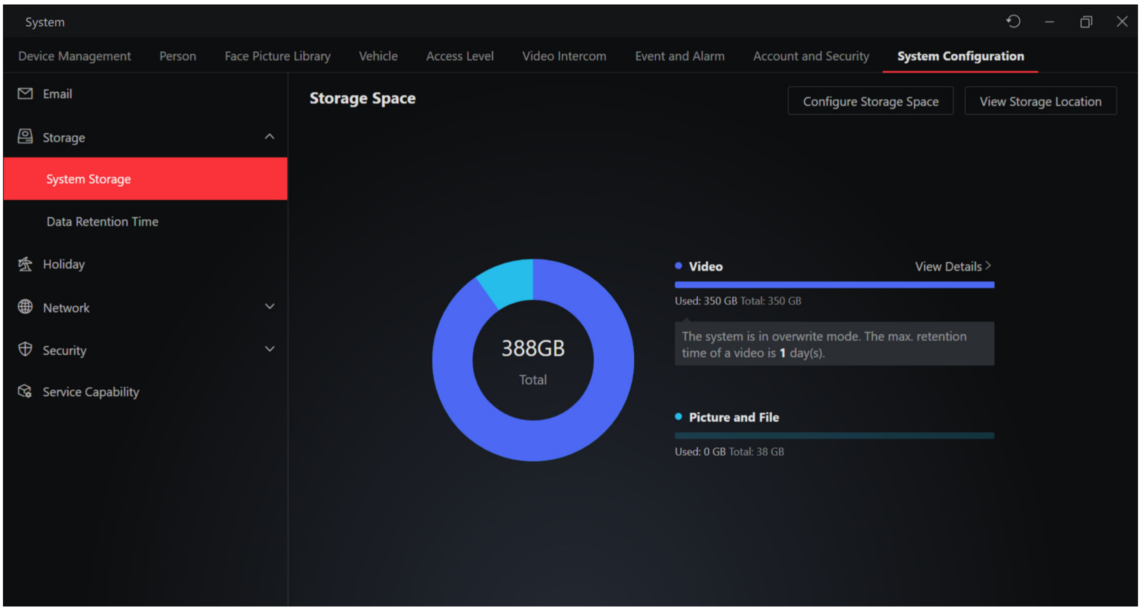
- **Video**: After adding storage schedule of cameras, time-based and event-based recordings of cameras will be stored in the video resource pool.
- **Picture and File**: Pictures include those captured during event reporting, manual capture, alarm linkages, etc. Files refer to audio files from video intercom.

If you are new to system storage, you can now try 30 days of free video storage for up to 4 channels. Videos, pictures, and files will be directly stored on the HikCentral Lite server.

Note

- The trial opportunity is only available to new users who have never used the system storage feature (users who have already started a trial or activated a formal license cannot start a trial again).
- If a trial has already been started, activating a formal license will keep the trial features available until the trial expires.

In the upper-right corner of the Desktop, click **System → System Configuration → Storage → System Storage / Data Retention Time** .



Used: 350 GB Total: 350 GB

The system is in overwrite mode. The max. retention time of a video is **1** day(s).

Used: 0 GB Total: 38 GB

Figure 5-1 Storage Configuration

5.1 Preparations

The video storage feature becomes available after purchasing and activating a formal video storage license. You can also activate a trial license to try this feature before purchasing a formal one.

5.2 Configure Storage Location and Storage Space

You should configure the storage location and allocate the storage space ratio for video and picture/file according to your needs.

Configure Storage Location

Click **View Storage Location** in the upper-right corner.
The default storage location is the disk with the largest space. Disk circular overwrite is enabled by default. When the space is full, the system will overwrite the oldest files.
You can click ○ to add and initialize additional disks.
The recommended hard drive model is as follows. If the hard drive you use is not on the recommended list, it is strongly recommended to use an enterprise hard drive with similar performance to ensure storage quality.

- SSD: 1TB M.2 2230 PCIe NVMe Class 35
- HDD: 20TB 7.2K SATA 6Gbps 3.5'', Hot-swappable

Note

- Manually deleting files already stored on the disk or the disk going offline can result in the loss of key information, such as recordings, though you will receive a system notification.
- When replacing the current disk with a new one, back up your data first. Ensure the new hard drive has at least the same capacity as the original.
  You need to disable the current logical disk and delete its associated files. Create a new drive letter for the storage location and verify that it works normally.
- Do not modify the drive letter in the operating system, as it may cause anomalies.

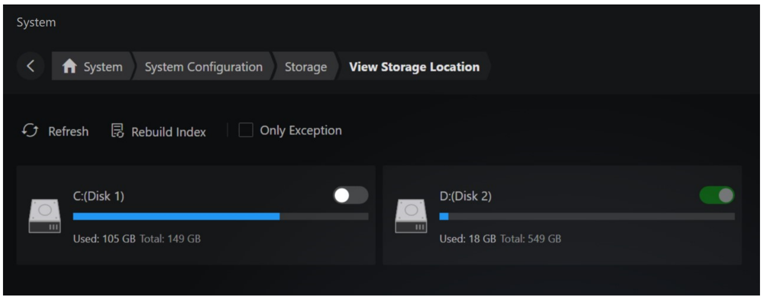


Figure 5-2 Storage Location

Configure Storage Space

Click **Configure Storage Space** in the upper-right corner.
Drag ⧹⧹ on the pie chart to allocate the storage space ratio for video and picture/file, or manually enter one value to automatically fill in the other.

Note

If you upgrade from HikCentral Lite V1.0.1:

- The processing logic for the storage space of pictures and files after the upgrade is the same as before the upgrade. For example, if the quota for pictures and files in HikCentral Lite is 120 GB, there will be a total of 120 GB storage space for pictures and files after the upgrade.
- When space is insufficient, the space for pictures and files, as well as the total space is calculated based on the remaining disk capacity, not the actual used capacity.

5.3 Configure Storage Schedule

You can configure storage schedules for a single camera or multiple cameras.

Click **View Details** to enter the **Video Storage Details** page.

To add a recording schedule, click **Add** to set the recording parameters of cameras(s). Schedules added can be edited in the list. You can configure the recording schedule for a single camera or batch configure multiple cameras.

Note

When configuring storage schedules, make sure there is sufficient storage space.

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.

Stream Type

Choose the **Main Stream**, **Sub-Stream**, or **Dual-Stream** based on your actual needs for playback quality, power consumption, etc. When choosing **Sub-Stream** as the stream type, you can check **Use Main Stream to Record Event Triggered Video** to automatically record event-triggered videos using the main stream, ensuring the clarity of the recordings when the event is triggered. During event playback, the system will prioritize the main stream.

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

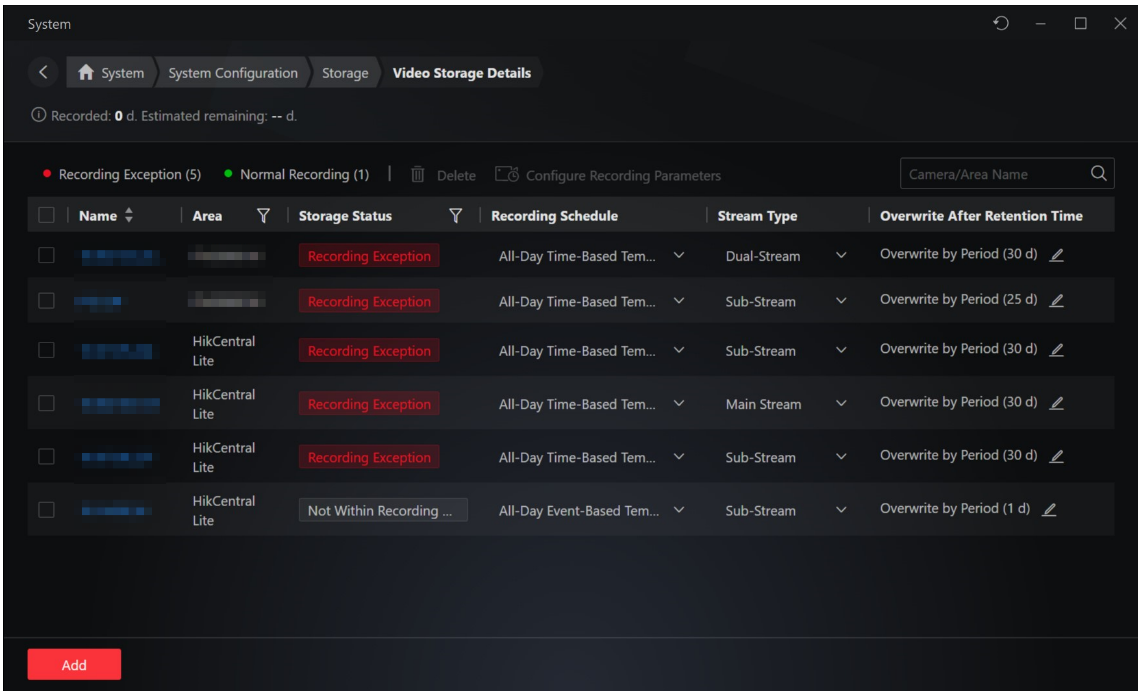
Enable this to temporarily store the video in the device when network fails, and transport the video to storage device when network recovers.

Streaming Server

Choose a streaming server for streaming will save more bandwidth, not applicable to devices accessed via the Hikvision SDK protocol.

Batch Configure Recording Parameters

After adding storage schedules, cameras with storage schedules will be displayed in the list. You can select multiple cameras and click **Configure Recording Parameters** to edit recording parameters.



System > System Configuration > Storage > **Video Storage Details**

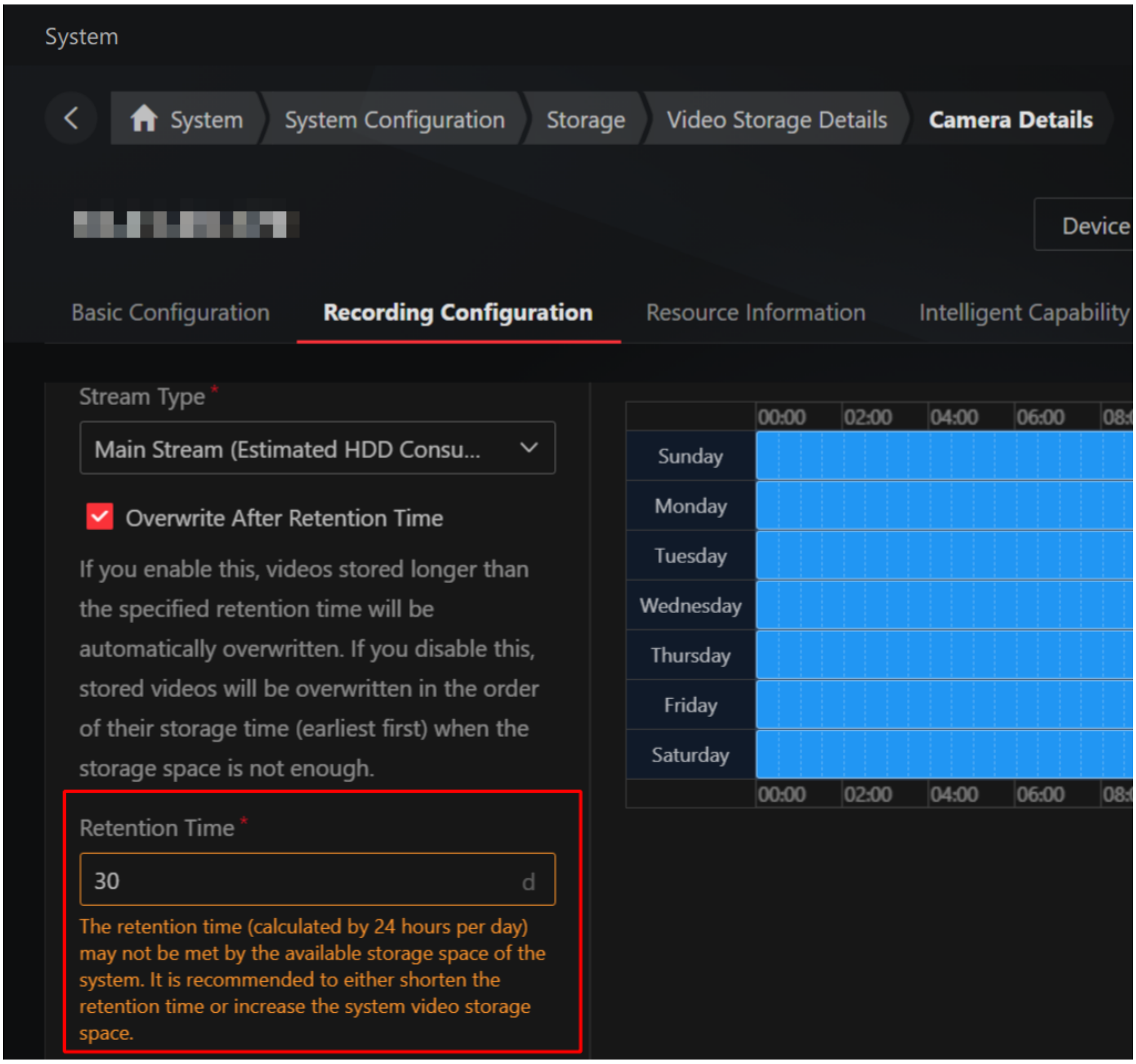
Recorded: **0** d. Estimated remaining: -- d.

● Recording Exception (5) ● Normal Recording (1)

□	Name	Area	Storage Status	Recording Schedule	Stream Type	Overwrite After Retention Time
□	[redacted]	[redacted]	Recording Exception	All-Day Time-Based Tem...	Dual-Stream	Overwrite by Period (30 d)
□	[redacted]	[redacted]	Recording Exception	All-Day Time-Based Tem...	Sub-Stream	Overwrite by Period (25 d)
□	[redacted]	HikCentral Lite	Recording Exception	All-Day Time-Based Tem...	Sub-Stream	Overwrite by Period (30 d)
□	[redacted]	HikCentral Lite	Recording Exception	All-Day Time-Based Tem...	Main Stream	Overwrite by Period (30 d)
□	[redacted]	HikCentral Lite	Recording Exception	All-Day Time-Based Tem...	Sub-Stream	Overwrite by Period (30 d)
□	[redacted]	HikCentral Lite	Not Within Recording ...	All-Day Event-Based Tem...	Sub-Stream	Overwrite by Period (1 d)

Figure 5-3 Storage Schedule

In the camera's recording configuration, the system checks the overall storage space to ensure the retention time for stored videos is appropriate. If the retention time is too long, it may affect other cameras' storage configurations or fail to meet the current camera's storage requirements. You need to assess and set an appropriate retention time. For more details, see ***View and Configure Details of Encoding Devices*** .



[redacted]

Stream Type *

Main Stream (Estimated HDD Consu...

☑ Overwrite After Retention Time

If you enable this, 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.

Retention Time *

30 d

The retention time (calculated by 24 hours per day) may not be met by the available storage space of the system. It is recommended to either shorten the retention time or increase the system video storage space.

Figure 5-4 Recording Configuration for a Camera

5.4 Playback & VCA Search

Supports playback of recordings in system storage and VCA Search. For more details, see ***Smart Search / VCA*** and ***Search for Detected Persons or Vehicles in VCA Areas*** .

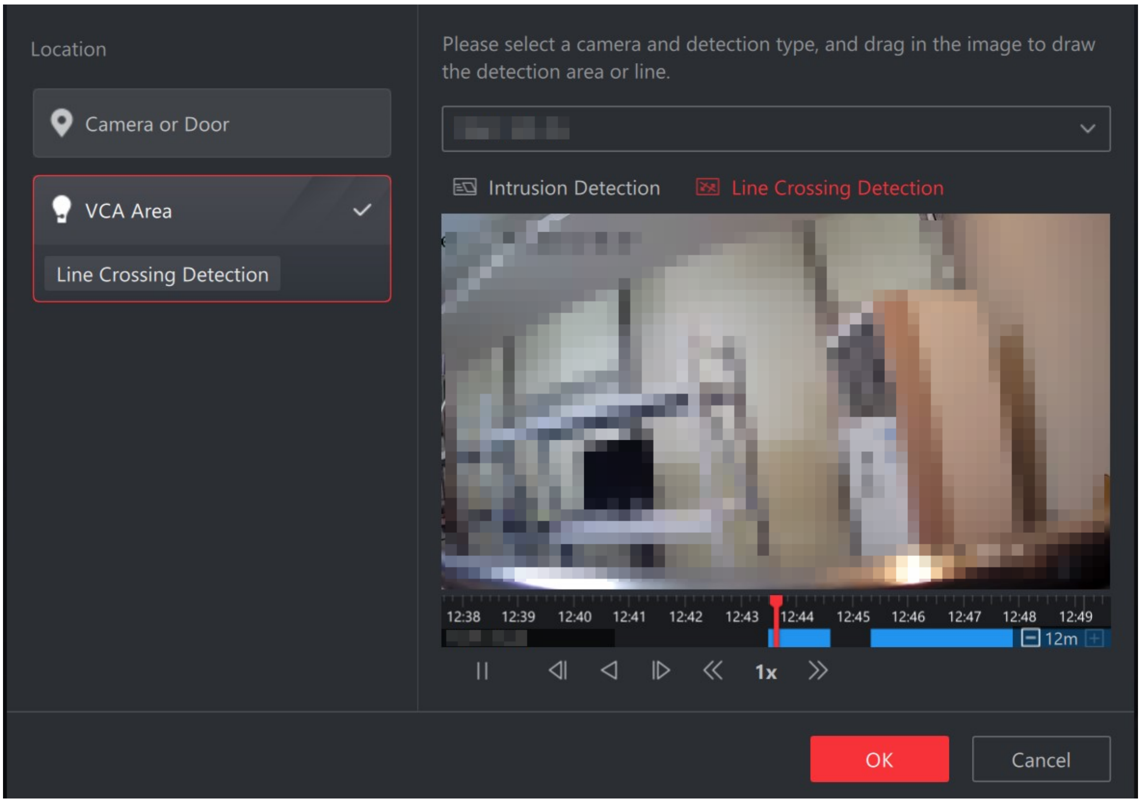


Figure 5-5 VCA Search

5.5 Specify Data Retention Time

Click **Storage → Data Retention Time** .

Define the retention period to keep the data as desired according to the data type. The general data, video data, and access control data will be automatically cleared once the set retention period is exceeded.

5.6 Advanced Configurations

In addition to basic configuration, you can configure a dedicated NIC for system storage, rebuild disk index if index files are damaged or other issues occur, and view the maintenance report of storage.

5.6.1 System Storage NIC

The system storage service can use a dedicated NIC. You can configure a separate NIC for system storage or use the same NIC for both SYS and system storage. For WAN access, you can assign the same IP address for SYS and system storage, or use different IP addresses for each. For more details, see the sections **Configure WAN Access** and **Configure Server Address** in ***Configure NTP Synchronization / Device Access Protocol / WAN Access / NIC, and Reset Network Info*** .

5.6.2 Rebuild Index

When index corruption, storage exceptions, or other issues occur, making it difficult to search stored content or leading to a decrease in search efficiency, you can rebuild the index to restore search functionality. Please do not shut down the system during this period.

Go to **System Storage → View Storage Location → Rebuild Index** .

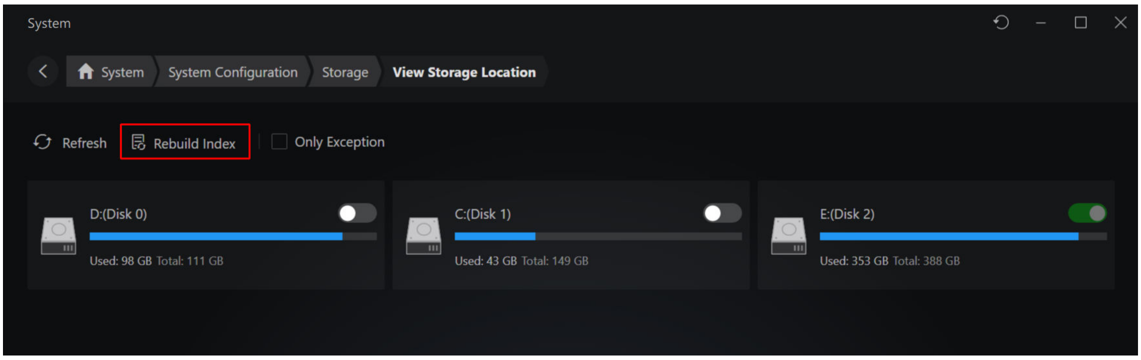
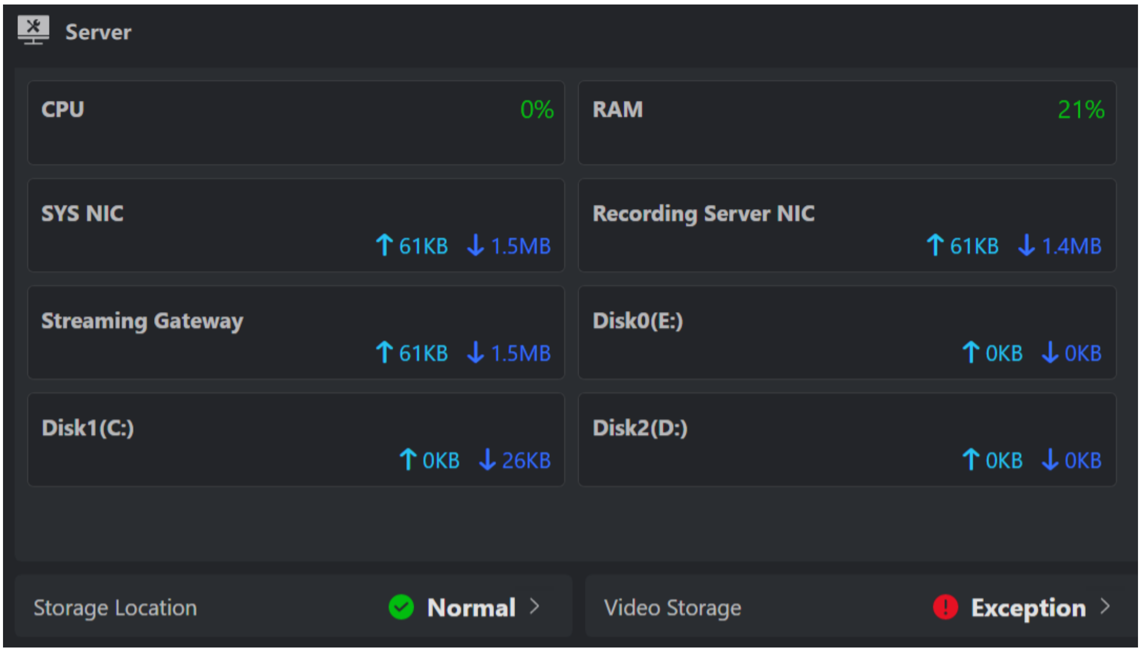


Figure 5-6 Rebuild Index

5.6.3 Maintenance

On the Maintenance Report page, supports statistics for Recording Server NIC, disk status, storage location, and video storage. For more details, see ***Generate and Display Maintenance Report*** .



Server

CPU 0%

RAM 21%

SYS NIC ↑61KB ↓1.5MB

Recording Server NIC ↑61KB ↓1.4MB

Streaming Gateway ↑61KB ↓1.5MB

Disk0(E:) ↑0KB ↓0KB

Disk1(C:) ↑0KB ↓26KB

Disk2(D:) ↑0KB ↓0KB

Storage Location ✓ Normal >

Video Storage ! Exception >

Figure 5-7 Server Statistics

Chapter 6 Main Panel for Monitoring and Control

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

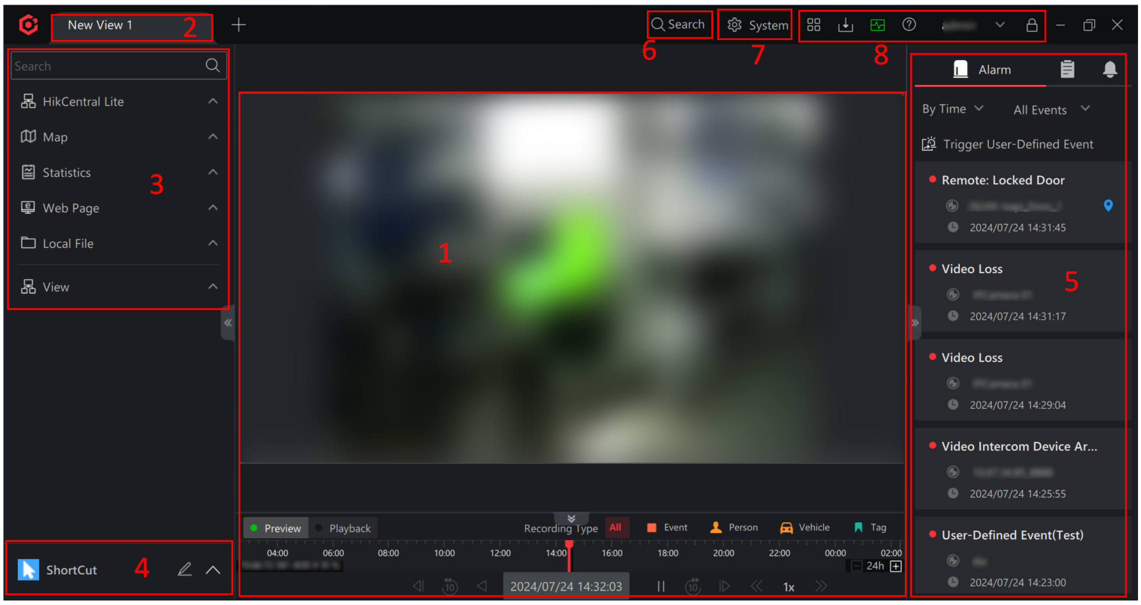


Figure 6-1 Main Panel for Monitoring and Control

Table 6-1 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.
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. 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.
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.

No.	Function
	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*** . At most 100 alarms can be displayed in the list. You can hover on an alarm to view alarm details, drag an alarm to view the related video. Also, you can enable/disable certain alarm types. The enabled types of alarm will be displayed here. Refer to ***Alarm List*** . 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, 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.
	Object Search / AcuSearch: View object search / 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.
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. • [redacted] ⌄ : View the information of the login user, manage Licenses, back up data, change password, etc. • 🔒 : Lock the client.

Chapter 7 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 7-1 General Search Content

Search Type	Description
Alarm	Search for historical alarms by time, 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 7-2 Intelligent Search Condition

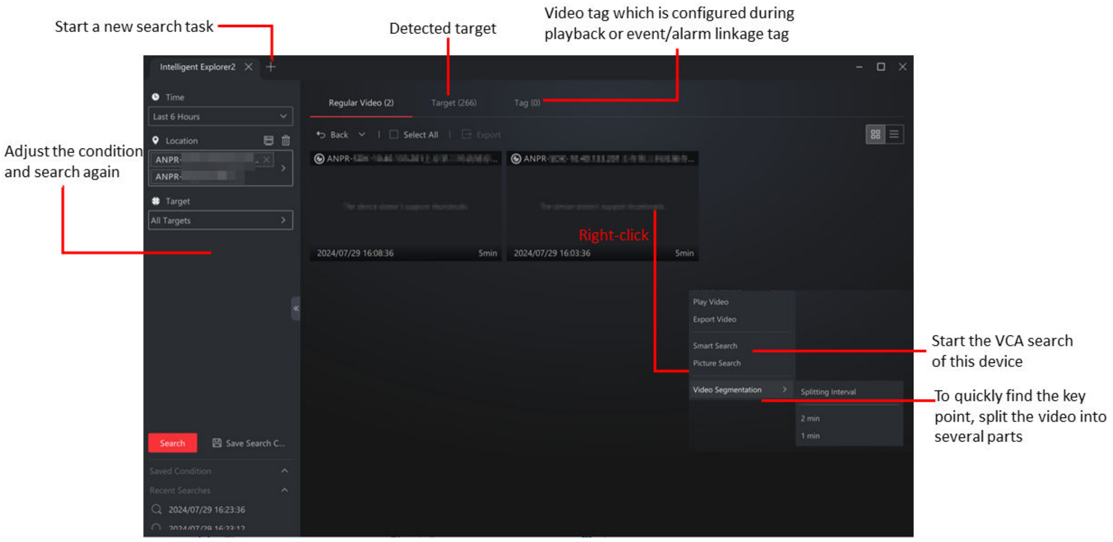
Search Condition	Scenario
Location	• Search for persons/vehicles captured by specified cameras or accessed doors. Refer to ***Search for Detected Vehicles or Persons by Cameras/Doors*** . • Search for specific targets related to line-crossing / intrusion event by drawing a VCA area on the video. Refer 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 / Object Search*** , 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*** .

7.1 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.

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.

Search for Vehicles by Cameras



Start a new search task

Detected target

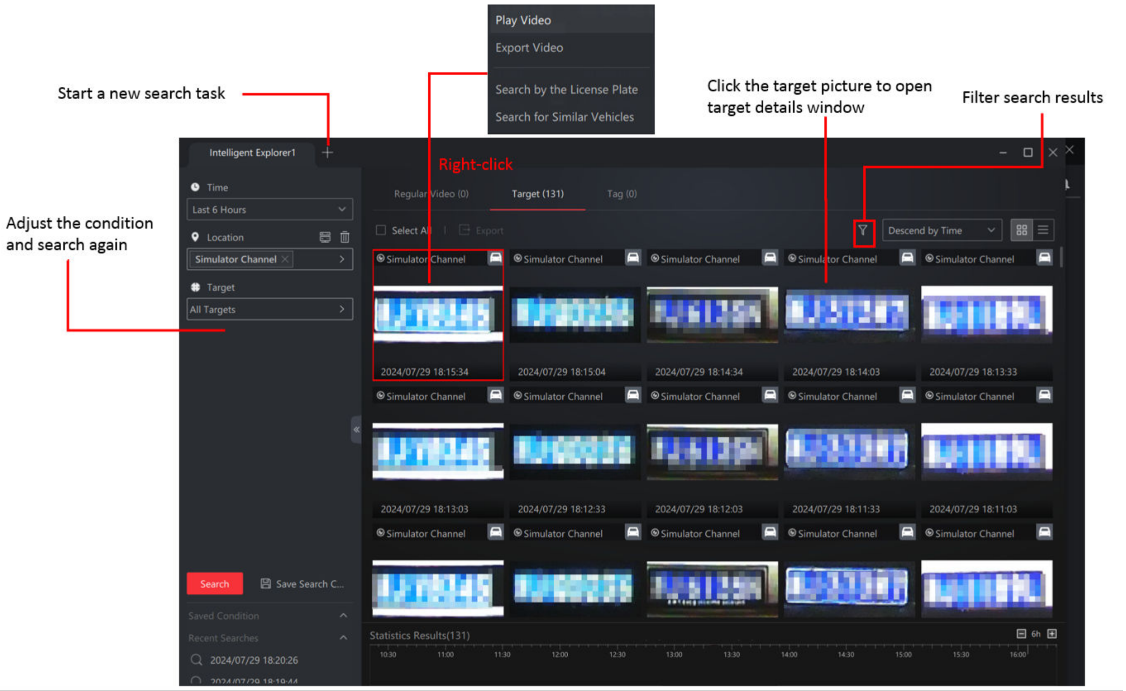
Video tag which is configured during playback or event/alarm linkage tag

Adjust the condition and search again

Start the VCA search of this device

To quickly find the key point, split the video into several parts

Figure 7-1 Result of Searched Videos



Start a new search task

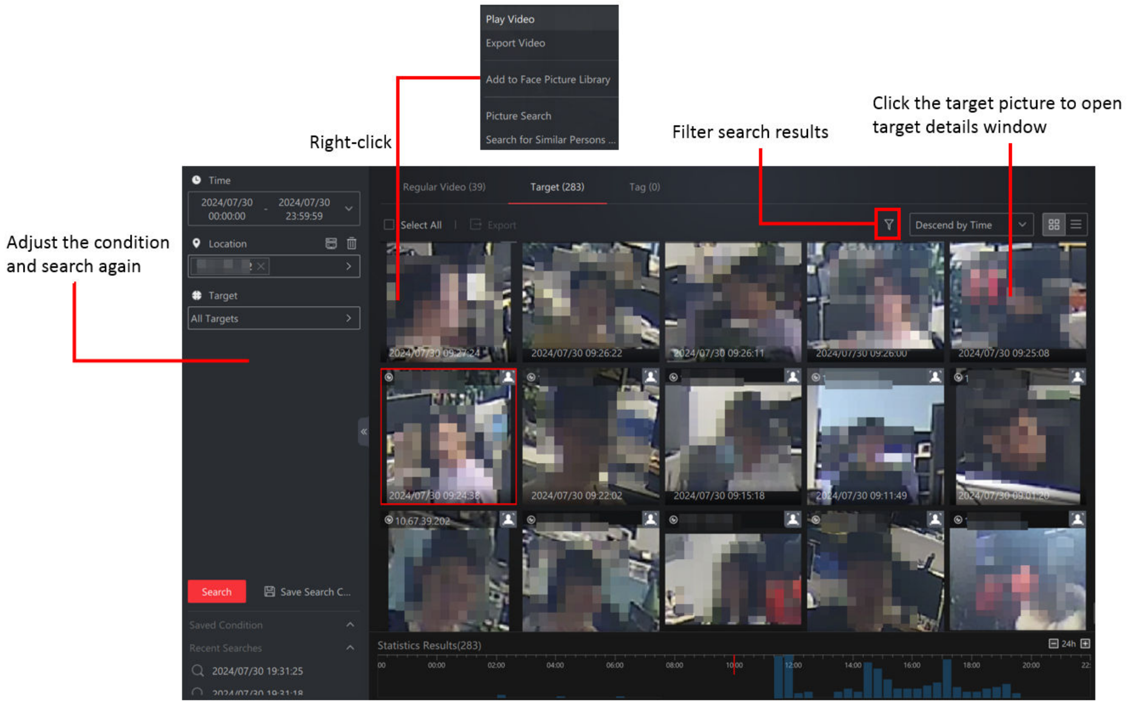
Click the target picture to open target details window

Filter search results

Adjust the condition and search again

Figure 7-2 Result of Searched Vehicles

Search for Persons by Cameras



Right-click

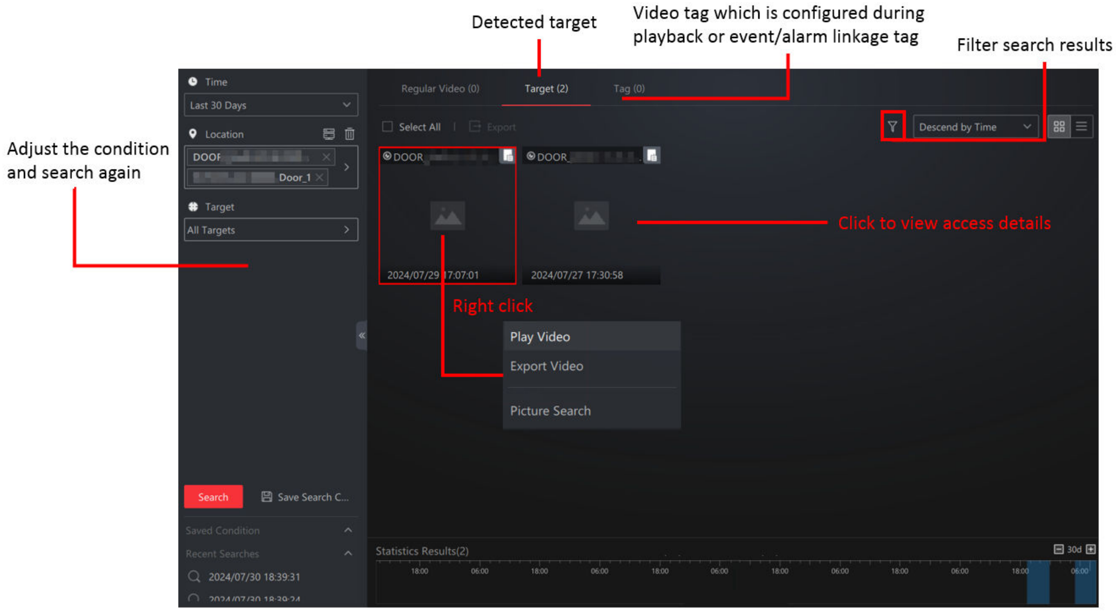
Filter search results

Click the target picture to open target details window

Adjust the condition and search again

Figure 7-3 Search for Persons by Cameras

Search for Persons by Doors



Detected target

Video tag which is configured during playback or event/alarm linkage tag

Filter search results

Adjust the condition and search again

Click to view access details

Right click

Figure 7-4 Search for Persons by Doors

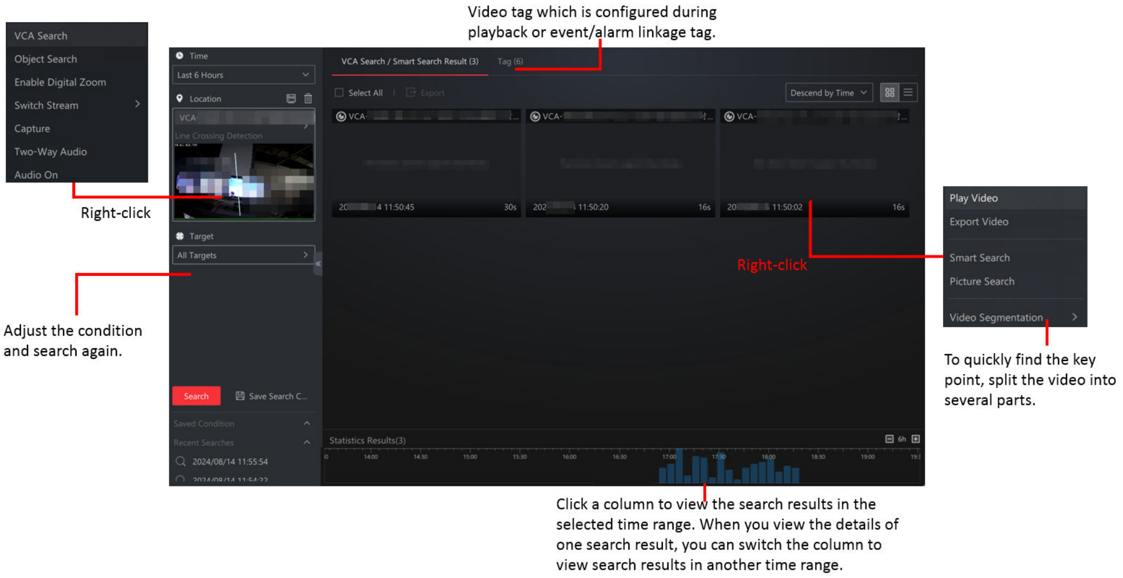
7.2 Search for Detected Persons or Vehicles in VCA Areas

You can search for VCA events related videos, and filter them by targets (persons/vehicles). 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, set the time period and set the **Location** to **VCA Area**.
2. Select a camera to search for the VCA event related videos.
3. Select the VCA event type (**Intrusion Detection** or **Line Crossing Detection**), and draw a detection area/line for search.
4. Click **Search**.



Video tag which is configured during playback or event/alarm linkage tag.

Right-click

Adjust the condition and search again.

To quickly find the key point, split the video into several parts.

Click a column to view the search results in the selected time range. When you view the details of one search result, you can switch the column to view search results in another time range.

Figure 7-5 VCA Search

7.3 Search for Detected Persons/Vehicles by Features

On the Intelligent Search page, set the time and target features for search.

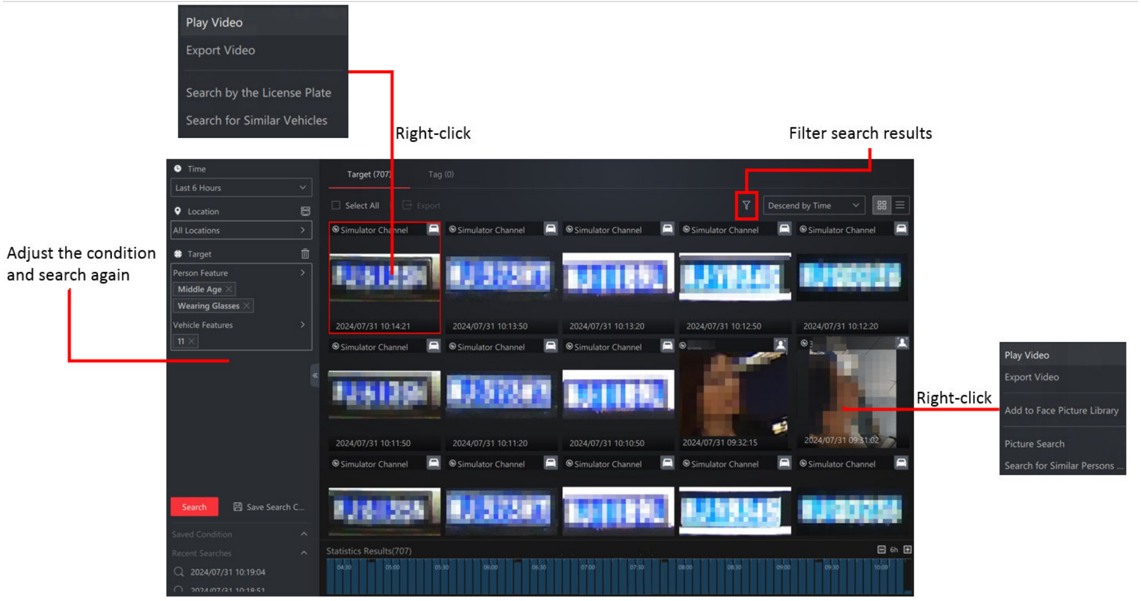


Figure 7-6 Search for Persons/Vehicles by Features

Chapter 8 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.

8.1 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 8-1 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
Maintenance (Service)	Storage Exception

Alarms of Access Control

Table 8-2 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

Category	Specific Event
	Access Granted by Fingerprint
	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

Category	Specific Event
	No Access Level Assigned
	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

Category	Specific Event
	Person Not in Multi-Factor Authentication Group
	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

Category	Specific Event
	Door Bell Rang
	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

Category	Specific Event
	Multi-Factor Authentication: Access Granted
	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 8-3 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

Category	Specific Event
	Local: Login
	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

Category	Specific Event
	Battery Voltage Recovered
	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

Alarms of Maintenance

Table 8-4 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 8-5 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
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

Specific Event
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 8-6 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
Vibration Detection Alarm
Audio Exception Detection
Video Stream Transcoding Exception

Table 8-7 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

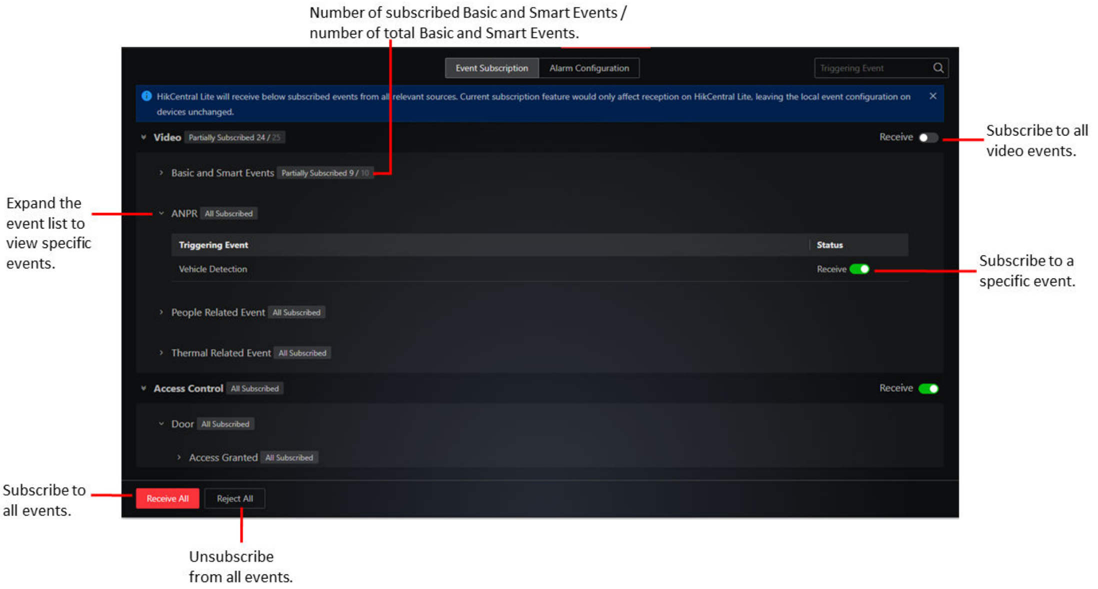
Alarms of Custom Event

Table 8-8 Custom Event

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

8.2 Event Subscription

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



HikCentral Lite will receive below subscribed events from all relevant sources. Current subscription feature would only affect reception on HikCentral Lite, leaving the local event configuration on devices unchanged.

Triggering Event	Status
Vehicle Detection	Receive

Number of subscribed Basic and Smart Events / number of total Basic and Smart Events.

Subscribe to all video events.

Expand the event list to view specific events.

Subscribe to a specific event.

Subscribe to all events.

Unsubscribe from all events.

Figure 8-1 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.

8.3 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**.

8.4 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**, and **Trigger User-Defined Event**.

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).

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*** .

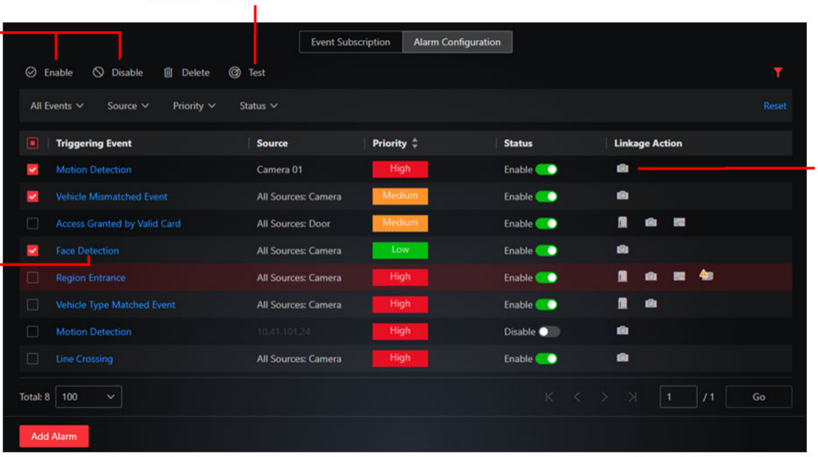
Trigger Pop-up Window

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

8.5 Alarm List

After you configure the alarm, it is enabled by default. You can manually disable the alarm so that the alarm will not be triggered and the linkage action(s) will not happen, either.

Test-trigger selected alarm(s) to check if the alarm has been properly configured. The alarm will be triggered and displayed in the list of triggered alarms (**Search** > **Alarm**).



☐	Triggering Event	Source	Priority	Status	Linkage Action
☑	Motion Detection	Camera 01	High	Enable	📷
☑	Vehicle Mismatched Event	All Sources: Camera	Medium	Enable	📷
☐	Access Granted by Valid Card	All Sources: Door	Medium	Enable	🚪 📷 ✉
☑	Face Detection	All Sources: Camera	Low	Enable	📷
☐	Region Entrance	All Sources: Camera	High	Enable	🚪 📷 ✉ 🔔
☐	Vehicle Type Matched Event	All Sources: Camera	High	Enable	🚪 📷
☐	Motion Detection	10.41.101.24	High	Disable	📷
☐	Line Crossing	All Sources: Camera	High	Enable	📷

Total: 8 100 1 / 1 Go

Click the event name to edit the alarm.

Hover over a linkage action to view the action details

Figure 8-2 List of Configured Alarms

8.6 Search for and Export Alarms

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

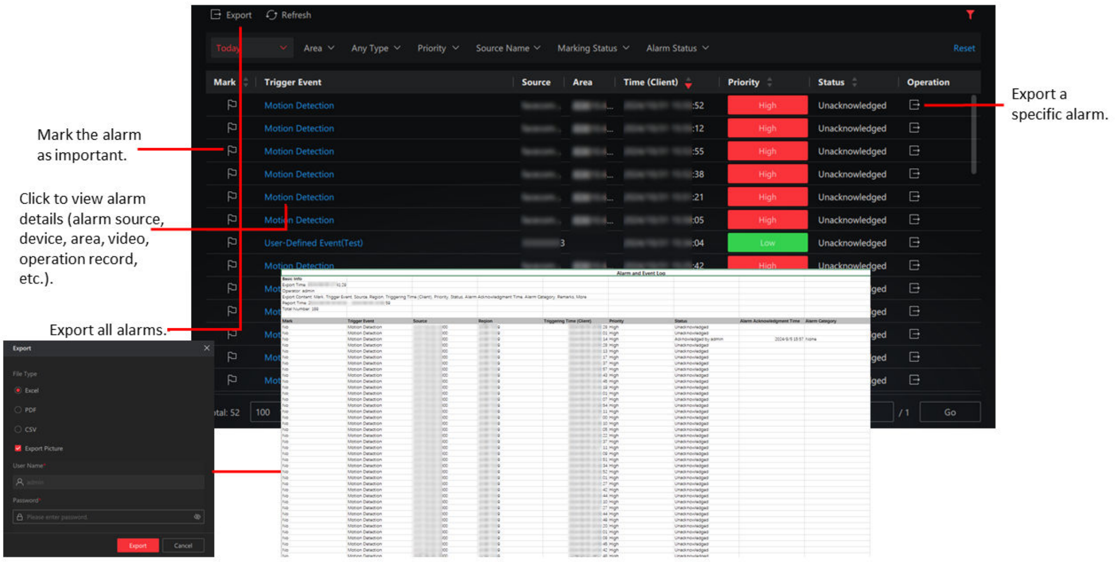


Figure 8-3 Triggered Alarm List

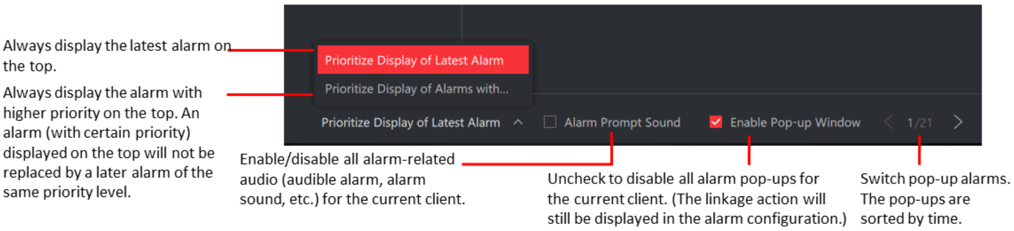

Prioritize Display of Latest Alarm
Prioritize Display of Alarms with...
Prioritize Display of Latest Alarm
☐ Alarm Prompt Sound
☑ Enable Pop-up Window
1/21
Always display the latest alarm on the top.
Always display the alarm with higher priority on the top. An alarm (with certain priority) displayed on the top will not be replaced by a later alarm of the same priority level.
Enable/disable all alarm-related audio (audible alarm, alarm sound, etc.) for the current client.
Uncheck to disable all alarm pop-ups for the current client. (The linkage action will still be displayed in the alarm configuration.)
Switch pop-up alarms. The pop-ups are sorted by time.

Figure 8-4 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** .

8.7 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 9 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** .

9.1 Add a User

You can add normal users and assign roles to them for accessing the system. Normal users refer to all users except the super user.

Enter the Add User page and set the basic information.

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.

9.2 Supported Operations on the User List

Only user(s) assigned with the Administrator role can inactivate or activate a user. If a user is inactivated, login with the user account is not allowed.

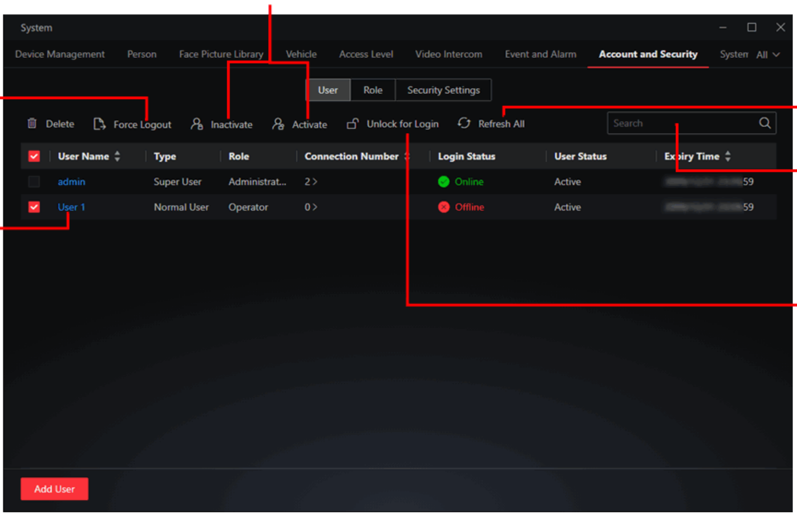
Force log out an online user.

Click user name to view and edit user settings.

Get the latest status of all users.

Enter a keyword of the user name to search for users.

For users whose account is locked due to too many failed login attempts, user(s) assigned with the Administrator role can unlock their accounts for login.



☑	User Name	Type	Role	Connection Number	Login Status	User Status	Expiry Time
□	admin	Super User	Administrat...	2 >	● Online	Active	[redacted]59
☑	User 1	Normal User	Operator	0 >	☒ Offline	Active	[redacted]59

Figure 9-1 User List

9.3 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

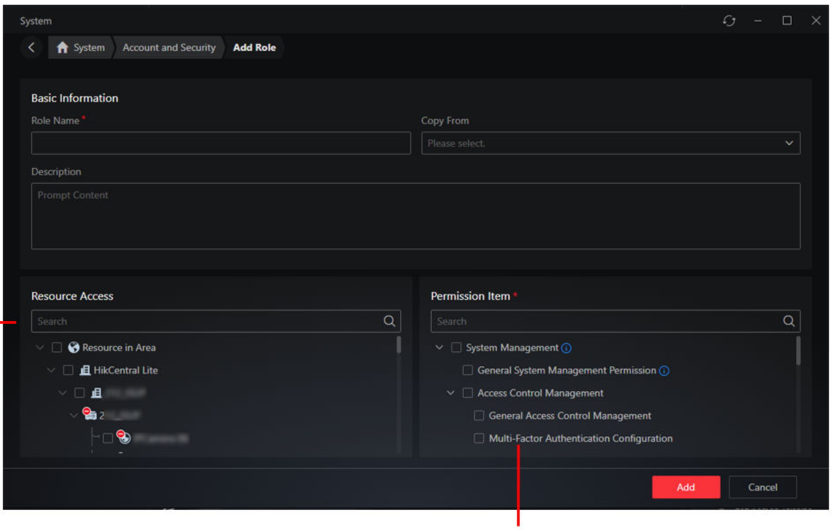
The platform has predefined two default roles: Administrator and Operator. You can click the role name to view details. The two default roles cannot be edited or deleted.

Administrator

Role that has all permissions of the platform.

Operator

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



Select resource(s) for the permission item(s) to be applied to.

Select permission item(s). For example, if **Device Management** is checked, you will have the permission to configure and manage all accessible devices (i.e., add, edit, and delete devices, and search for logs).

Figure 9-2 Add a Role

Table 9-1 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. For this permission, the resource permission for department(s) and persons within the department is required, and the specific

Category	Sub-Category	Specific Permission
		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.
	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 and video intercom devices, 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 alarm outputs: The resource permission for relevant devices is required, and the specific

Category	Sub-Category	Specific Permission
		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
		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.

9.4 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.

9.5 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 10 System Configuration

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

- Email account configuration: ***Configure Email Parameters*** .
- Configure the storage location and quota of pictures and files, and the data retention time: ***Storage*** .
- 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***

10.1 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**.

10.2 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

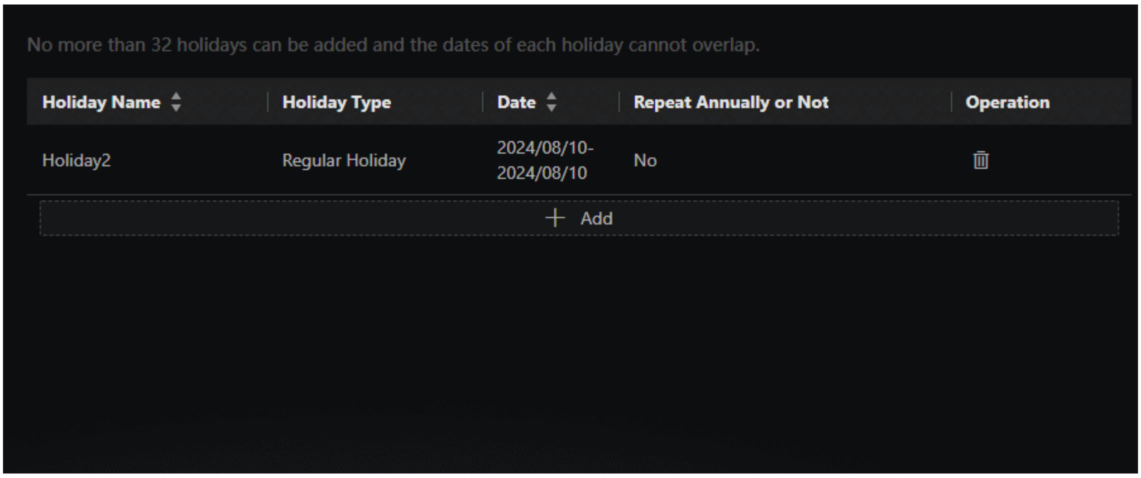
Click **Add**, enter the holiday name, and set the following parameters.

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.



No more than 32 holidays can be added and the dates of each holiday cannot overlap.

Holiday Name	Holiday Type	Date	Repeat Annually or Not	Operation
Holiday2	Regular Holiday	2024/08/10- 2024/08/10	No	🗑

Figure 10-1 Edit Holiday Parameters (.gif)

10.3 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.

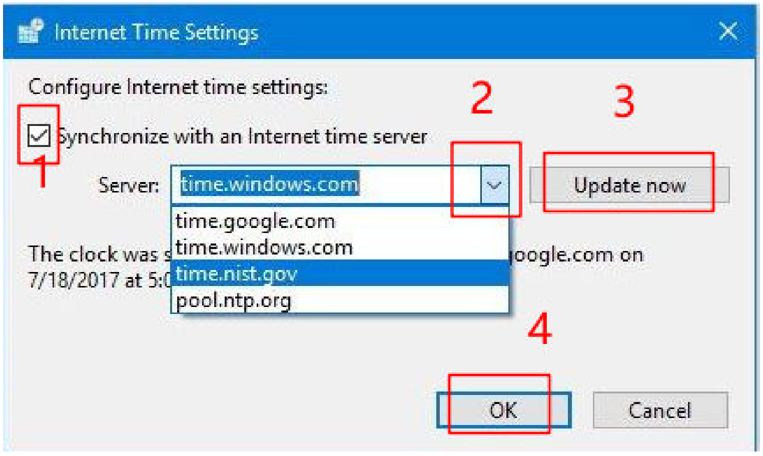
On the Home page, go to **System → System Configuration → Network** .

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 10-1 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** .  Internet Time Settings Configure Internet time settings: ☑ Synchronize with an Internet time server Server: time.windows.com time.google.com time.windows.com time.nist.gov pool.ntp.org The clock was s oogle.com on 7/18/2017 at 5:0 Update now OK Cancel 1 2 3 4 **Figure 10-2 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

Mode	Description
	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 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

- 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 (Wide Area Network).
Go to **WAN Access** and enable the button.

1. Fill in SYS and/or System Storage Network Addresses
   - For single NIC environment: You can only configure one network address, which is used for both system network access and storage services. The interface will display this as **SYS / System Storage Network Address**.
   - For dual NIC environment: You can configure different network addresses for system services and storage services. The interface will display this as **SYS Network Address** and **System Storage 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.

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** .

10.4 Use SSL/TLS Certificate for HTTPS Connections

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.

Get Your SSL/TLS Certificate

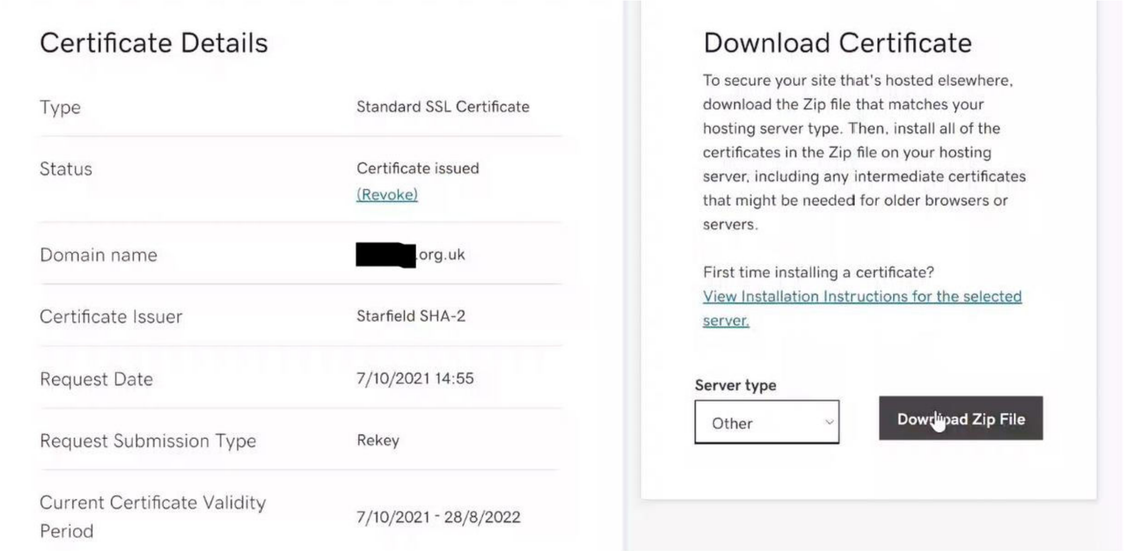
Note

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.



Certificate Details

Type	Standard SSL Certificate
Status	Certificate issued (Revoke)
Domain name	[redacted].org.uk
Certificate Issuer	Starfield SHA-2
Request Date	7/10/2021 14:55
Request Submission Type	Rekey
Current Certificate Validity Period	7/10/2021 - 28/8/2022

Download Certificate

To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the certificates in the Zip file on your hosting server, including any intermediate certificates that might be needed for older browsers or servers.

First time installing a certificate?
View Installation Instructions for the selected server.

Server type: Other

Figure 10-3 SSL/TLS Certificate Example

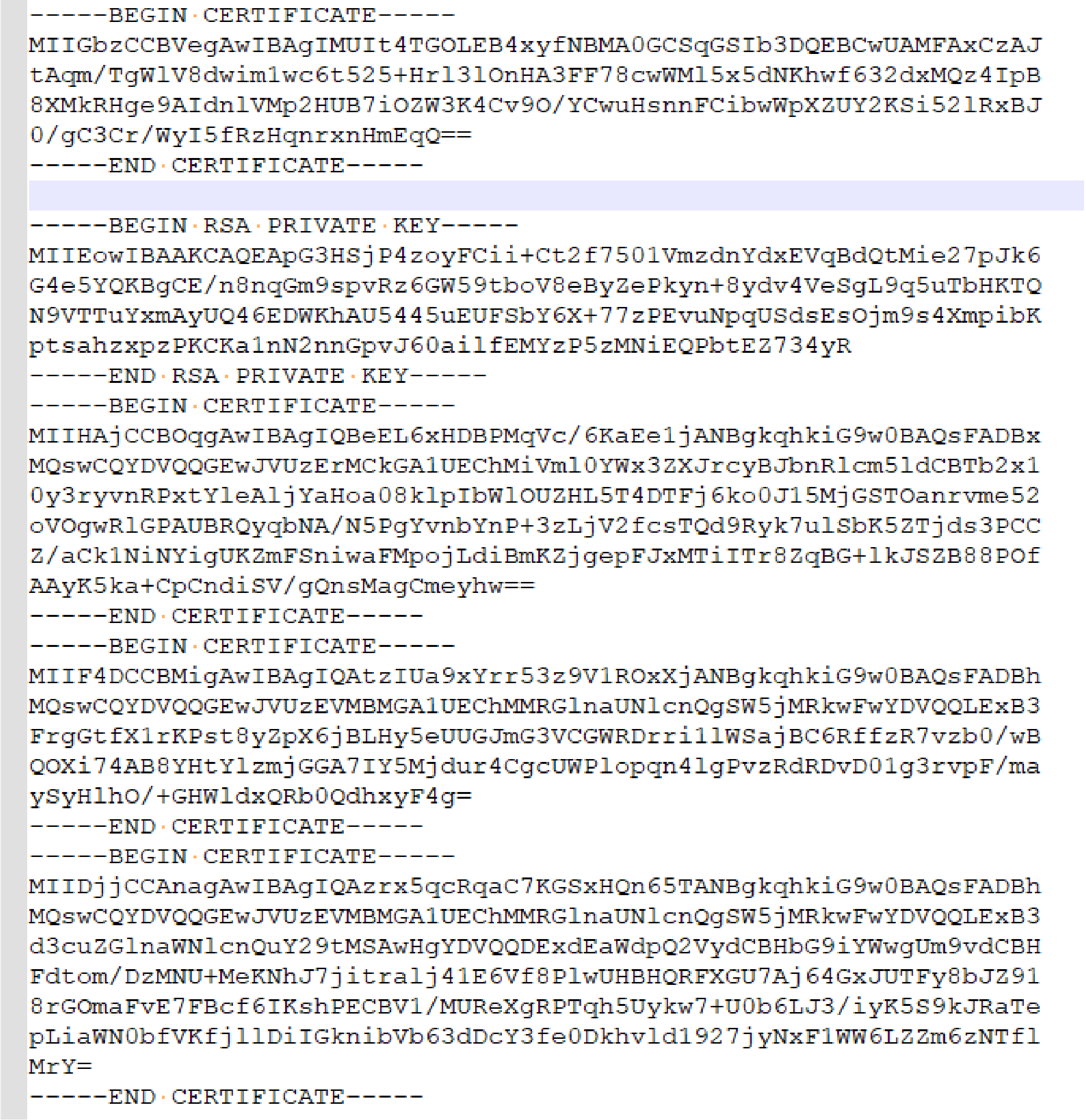
4. Download your SSL/TLS certificate to your local PC.
   Make sure that the certificate is in PEM format. You can try to edit the file extension to ***.pem*** or use a tool to convert its format to PEM.

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/TgW1V8dwim1wc6t525+Hrl3lOnHA3FF78cwWMl5x5dNKhwf632dxMQz4IpB
8XMkRHge9AIdnlVMp2HUB7iOZW3K4Cv9O/YCwuHsnnFCibwWpXZUY2KSi52lRxBJ
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 10-4 Example of Concatenated Certificate

3. On the top of the Desktop, click **System → System Configuration → Security → Certificate Management** .
4. Click **New Certificate →** 🗁 to upload the concatenated certificate.

Note

The Desktop will restart automatically when the certificate is uploaded.

5. (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.

10.5 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.

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

Chapter 11 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.

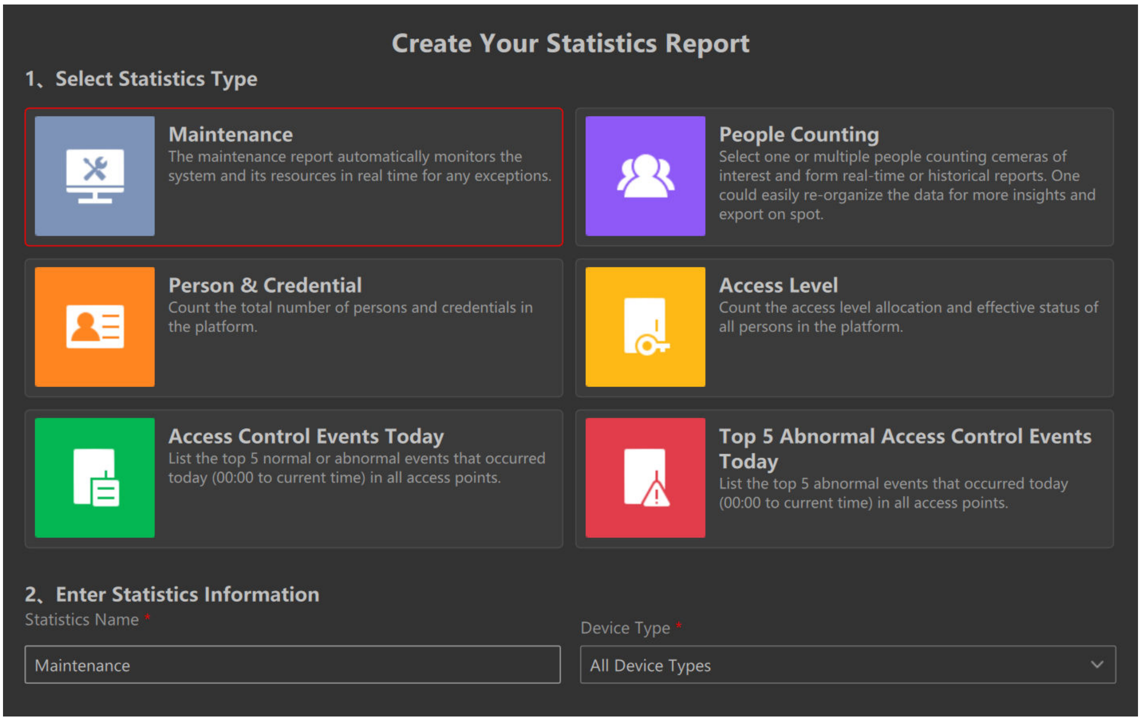
In this chapter, detailed information about ***Generate and Display Maintenance Report*** , ***Search for Notifications*** , and ***Search for System Logs*** is provided.

11.1 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, 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**.



Create Your Statistics Report

1、Select Statistics Type

Maintenance
The maintenance report automatically monitors the system and its resources in real time for any exceptions.

People Counting
Select one or multiple people counting cameras of interest and form real-time or historical reports. One could easily re-organize the data for more insights and export on spot.

Person & Credential
Count the total number of persons and credentials in the platform.

Access Level
Count the access level allocation and effective status of all persons in the platform.

Access Control Events Today
List the top 5 normal or abnormal events that occurred today (00:00 to current time) in all access points.

Top 5 Abnormal Access Control Events Today
List the top 5 abnormal events that occurred today (00:00 to current time) in all access points.

2、Enter Statistics Information

Statistics Name *
Maintenance

Device Type *
All Device Types

Figure 11-1 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.

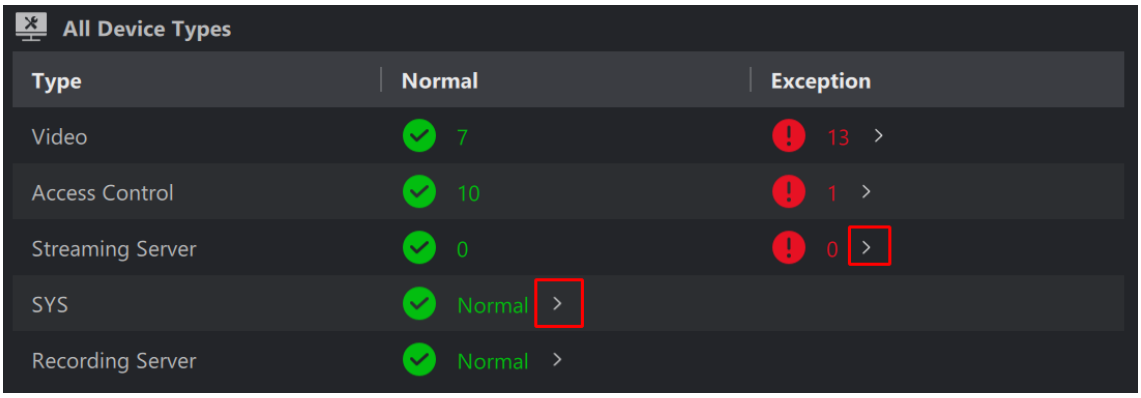
The styles of reports displayed can vary across different device types. See below for details.

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, and servers.



All Device Types

Type	Normal	Exception
Video	✓ 7	! 13 >
Access Control	✓ 10	! 1 >
Streaming Server	✓ 0	! 0 >
SYS	✓ Normal >	
Recording Server	✓ Normal >	

Figure 11-2 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.

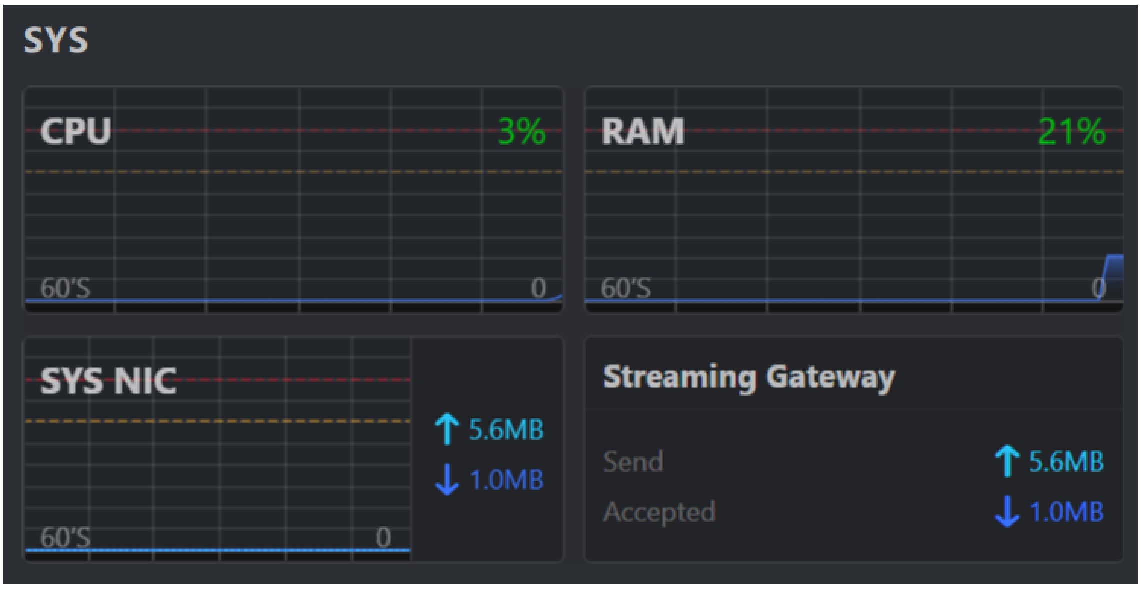


Figure 11-3 SYS

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

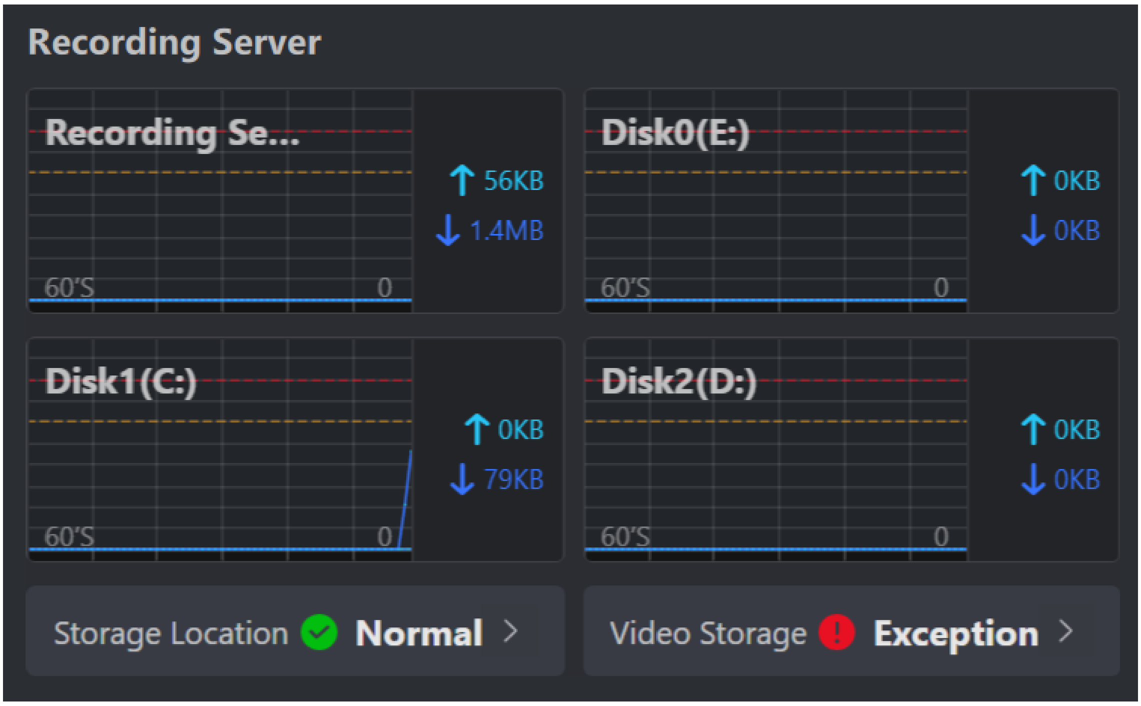
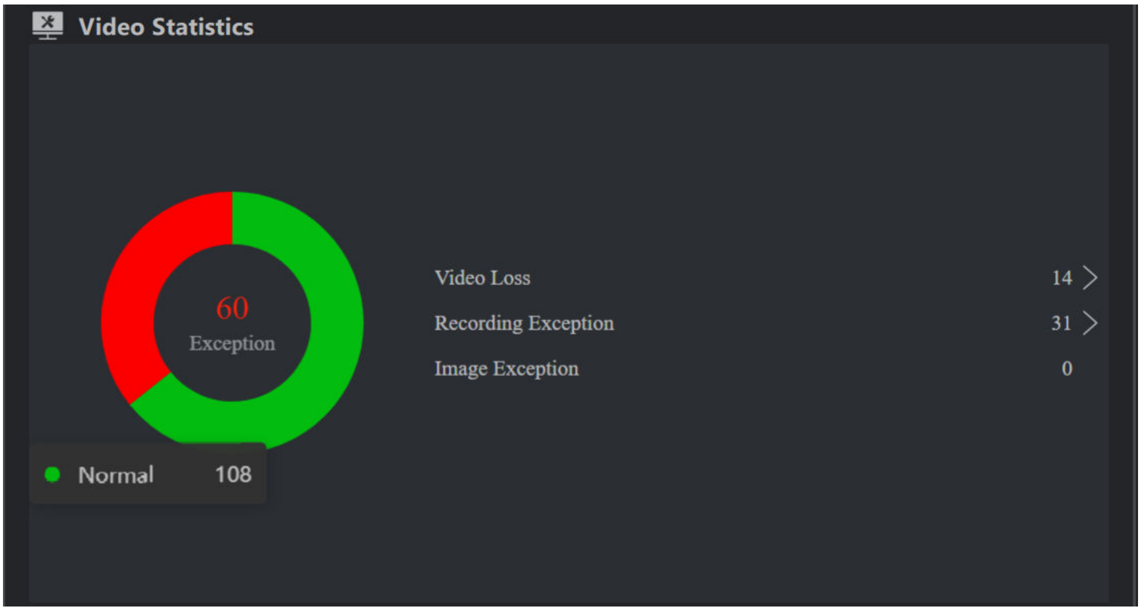


Figure 11-4 Recording Server

- 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.

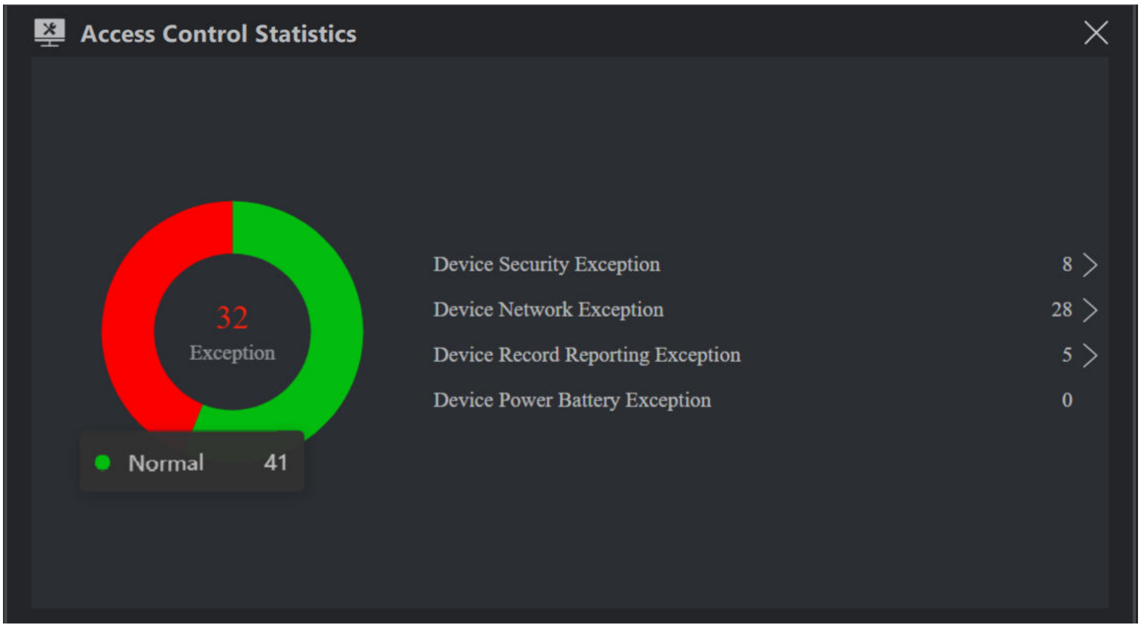


Video Loss	14 >
Recording Exception	31 >
Image Exception	0

Figure 11-5 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.


Access Control Statistics

32 Exception

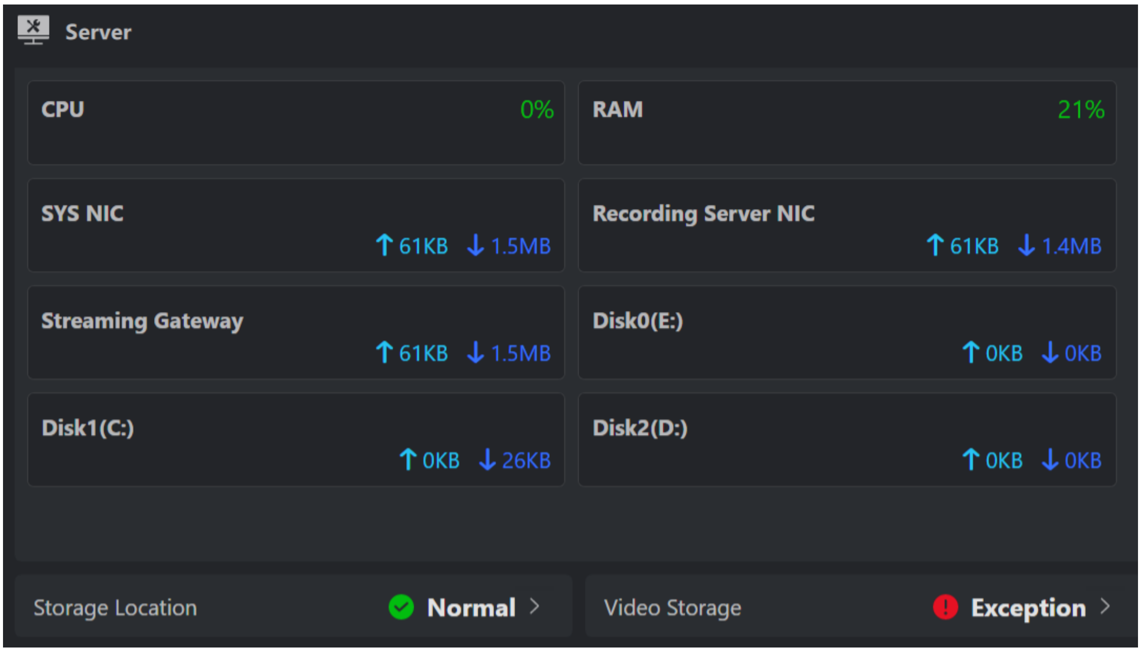
● Normal 41

Device Security Exception	8
Device Network Exception	28
Device Record Reporting Exception	5
Device Power Battery Exception	0

Figure 11-6 Access Control Statistics

Server

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


Server

CPU 0%	RAM 21%
SYS NIC ↑61KB ↓1.5MB	Recording Server NIC ↑61KB ↓1.4MB
Streaming Gateway ↑61KB ↓1.5MB	Disk0(E:) ↑0KB ↓0KB
Disk1(C:) ↑0KB ↓26KB	Disk2(D:) ↑0KB ↓0KB

Storage Location ✓ Normal >

Video Storage ! Exception >

Figure 11-7 Server Statistics

11.2 Search for Notifications

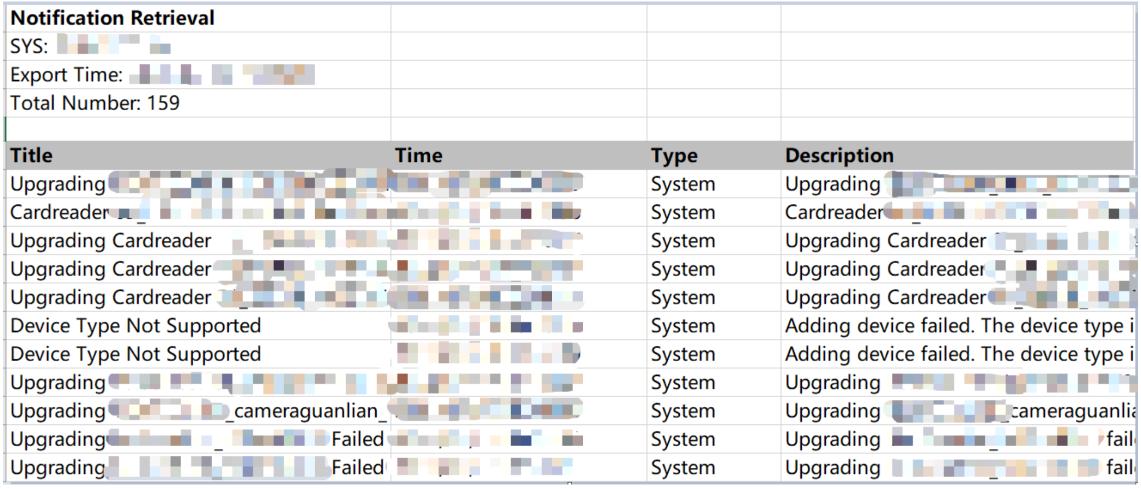
You can search for notification information to promptly detect and respond to alerts or updates, ensuring swift action on security incidents.

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

Figure 11-8 Notification Retrieval Excel Template

11.3 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

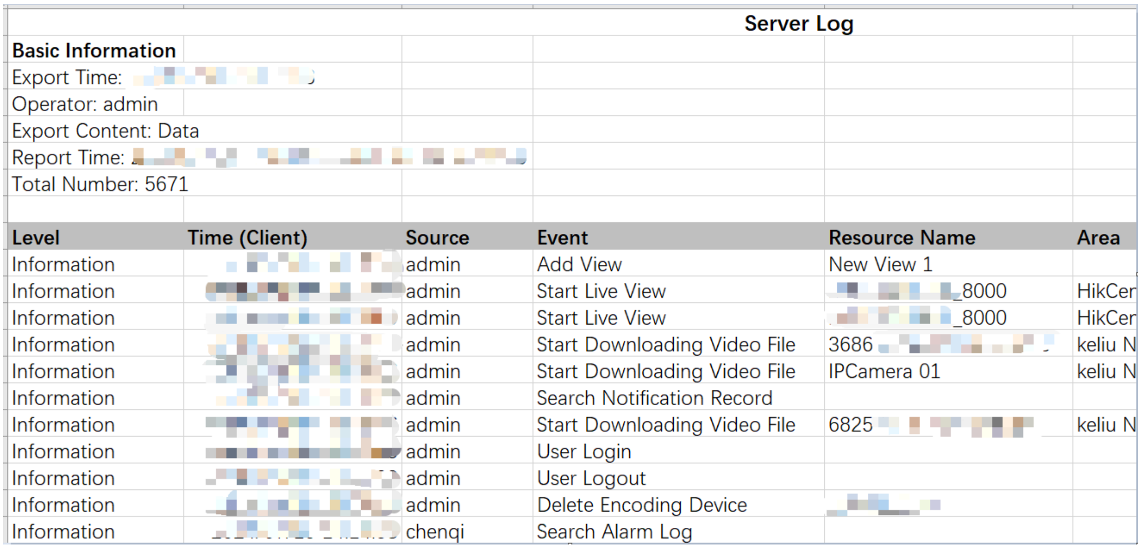
1. On the Home page, go to **System → Device Management** .
2. Hover on one device then right-click and select **View Log** to search local device logs.

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

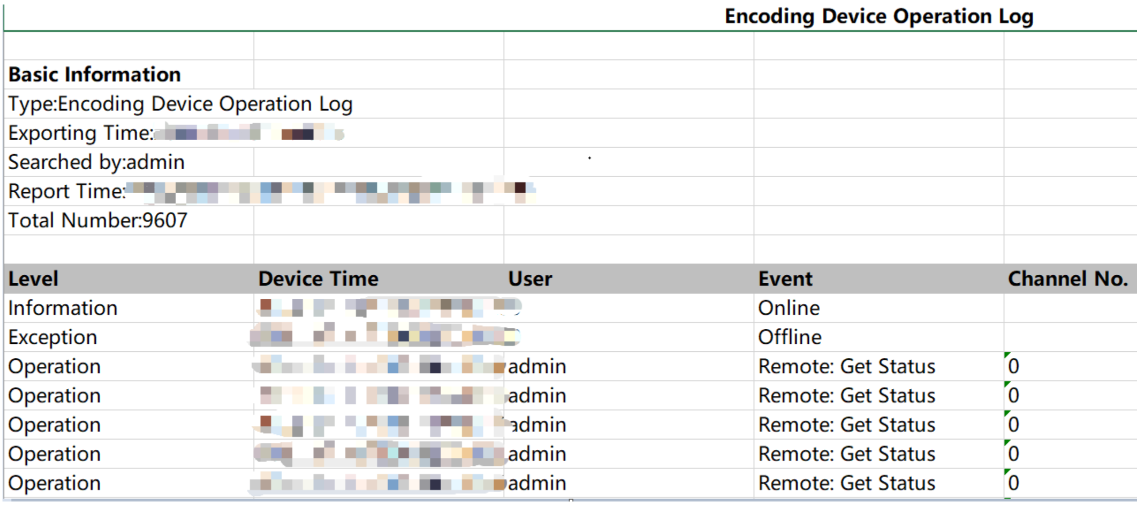
Basic Information
Export Time: [redacted]
Operator: admin
Export Content: Data
Report Time: [redacted]
Total Number: 5671

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

Figure 11-9 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:[redacted]
Searched by:admin
Report Time:[redacted]
Total Number:9607

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

Figure 11-10 Device Log Excel Template

Appendix A. Other System Configurations and Performance

For environments where iVMS-4200 is running, with a CPU earlier than i3-8100, 4 GB of RAM, and a SATA 7200 RPM Enterprise Class HDD, the following configurations are recommended for migrating from iVMS-4200 to HikCentral Lite.

It is recommended that the configuration be no less than the following:

Table A-1 System Configurations

Feature	Configuration
CPU	8th Generation of Intel® Core™ i3-8100
RAM	4 GB
NIC	GbE Network Interface Card
HDD	SATA 7200 RRM Enterprise Class HDD
HDD Capacity for Database	At least 500 GB
OS	Microsoft® Windows 10 64-bit or later

Under this configuration, the performance is as follows:

Table A-2 System Performance

Feature	Performance	
Cameras	64	
Events Receiving	1/s	
Storage Capacity of Captured Faces / ANPR Records / Events / Intelligent Analysis Data / Access Records / System Logs	2 million	

Table A-3 Performance of H.264 with Software Decoding

Frame Rate (fps)	Bit Rate (Mbps)	Resolution	Max. Live View Channels
30	2	1080p	2

Appendix B. 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.
- 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.

Video Monitoring

- When using acusearch / object search, 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 is 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.

System Storage

- Up to 128 cameras are supported for video storage.
- Only pictures and files can be stored in the system if the video storage license is not activated.
- Ensure that each disk has at least 34 GB of available space; otherwise, it will not be usable for system storage.
- Initialization of the disk uses 90% of the remaining disk space.
- Since videos, pictures, and files are stored on the system disk, system hibernation or sleep can result in the disk losing power, potentially causing storage exceptions. It is recommended to turn off hibernation or sleep mode.
- The minimum space required for each file type is 4 GB (for example, 4 GB for videos, 4 GB for pictures, and 4 GB for files), which includes necessary files for storage management.
- Auto-Copyback is effective only when the stream type is set to main stream and is supported only by Hikvision cameras.
- Rebuilding the index may temporarily affect search and playback functionality, but it will not cause data loss.

- Supports 6 data overwritten options.
- In the virtual machine environment, the performance of drive C will not be displayed in the maintenance report. See ***Generate and Display Maintenance Report*** for more details.

Appendix C. Past User Manuals

V1.1.0

V1.0.1

See Far, Go Further