

Hik-Connect for Teams Portal

User Manual

Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

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

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

Contents

Chapter 1 Introduction 1

1.1 What are the differences between the Portal and the Mobile Client? 1

1.2 What are the related entities? 1

1.3 What's the running environment of Hik Connect for Teams? 2

1.4 How to get accounts, log in, and create accounts? 3

Chapter 2 Video Management 5

2.1 Example Scenario 5

2.2 How to add encoding devices? 6

2.3 How to configure recordings for cameras? 6

2.3.1 How to configure local storage for cameras? 6

2.3.2 How to configure cloud storage for cameras linked to Hik-ProConnect Box or NVRs? 7

2.3.3 How to configure cloud storage service and set events? 7

2.4 How to add a focus? 11

2.5 How to view the camera wall and view the daily summary of a camera? 14

2.6 How to start intelligent search? 15

2.7 How to start live view and control PTZ? 18

2.8 How to start playback? 20

2.9 How to manage persons of interest? 21

2.10 How to set timelapse? 21

2.11 How to set alarms for video devices? 22

Chapter 3 Access Control 23

3.1 How to add the three elements: devices, access levels, and persons? 24

3.1.1 How to add access control devices? 24

3.1.2 How to add access levels? 24

3.1.3 How to add persons? 24

3.2 How to grant access to persons? 27

3.3 How to grant temporary access? 29
3.4 How to monitor real-time door status? 29
3.4.1 View Real-Time Access Events 29
3.4.2 Control Door 31
3.5 How to retrieve access control records? 32
3.6 How to set remain unlocked and remain locked rule? 33
3.7 How to set access control parameters? 33
3.7.1 Set Holidays 33
3.7.2 Set Access Schedule Template 34
3.7.3 Set General Parameters 34
3.7.4 Subscribe to Device and Access Events 35
3.8 How to set alarms for access control devices? 35
Chapter 4 Elevator Control 36
4.1 Example Scenario 36
4.2 How to get an elevator control license? 37
4.3 How to add elevator control devices? 37
4.4 How to control elevator floor access? 39
4.5 How to grant floor access permissions to persons? 41
4.5.1 How to add an access level? 41
4.5.2 How to grant access by person, department, or temporary credential? 41
4.5.3 How to view the overview access? 42
4.6 How to grant elevator control module to a team member? 42
4.7 How to set elevator control events? 43
Chapter 5 Time & Attendance 44
5.1 Example Scenario 44
5.2 How to add access control devices? 47
5.3 How to add employees? 47
5.4 How to configure attendance settings? 48

5.5 How to assign schedules to employees? 50
5.6 How to submit applications? 50
5.7 How to review applications? 51
5.8 How to view attendance records? 52
5.9 How to view and export reports? 53
Chapter 6 Video Intercom 57
6.1 Example Scenario 57
6.2 How to add and configure video intercom devices? 58
6.2.1 How to add a single intercom device? 58
6.2.2 How to batch import intercom devices in LAN? 58
6.3 How to batch configure the intercom system? 58
6.3.1 Step 1: Download the Import Template 58
6.3.2 Step 2: Fill Out the Template 60
6.3.3 Step 3: Upload and Import the File 61
6.3.4 Step 4: Check the Import Results 61
6.4 How to add communities, units, buildings, rooms, and residents? 62
6.4.1 How to add communities? 62
6.4.2 How to add buildings, units, and rooms? 67
6.5 How to manage notices? 70
6.6 How to view call history? 71
6.7 How to add call manager? 71
6.8 How to create temporary passes? 72
Chapter 7 On-board Monitoring 74
7.1 Example Scenario 74
7.2 How to add on-board monitoring devices? 75
7.3 How to configure parameters for on-board monitoring? 77
7.4 How to use related applications? 82
7.5 How to set alarms for on-board devices? 93

Chapter 8 Intrusion Protection 94
8.1 Add Alarm Devices and Import Areas 94
8.2 Perform Arming Control for Resources 94
Chapter 9 Analysis Report 96
9.1 How to configure analysis report service? 96
9.2 How to activate analysis report service? 97
9.3 How to configure devices for analysis report? 98
9.3.1 How to configure device on web page? 98
9.4 How to add encoding devices to Hik Connect for Teams? 105
9.5 How to add analysis configuration? 105
9.6 How to add employee face picture libraries? 114
9.7 How to view analysis reports? 114
Chapter 10 Commercial Display 117
10.1 Example Scenario 117
10.2 How to verify device compatibility? 117
10.3 How to configure commercial display devices? 118
10.4 How to control devices? 121
10.5 How to manage applications? 123
10.6 How to generate usage reports? 126
Chapter 11 ANPR 128
11.1 Example Scenario 128
11.2 How to activate the ANPR service? 129
11.3 How to add lists and add vehicles to lists? 130
11.4 How to set cameras as ANPR cameras and configure barrier gate control? 133
11.5 How to retrieve passing vehicle records? 135
11.6 How to view passing vehicle reports? 136
11.7 How to configure LED Display? 137
11.8 How to configure broadcast? 138

Chapter 12 Audio Broadcast 140
12.1 Add Network Speakers 140
12.2 Speak via a Single or Multiple Speakers 140
12.3 Upload Audio File 143
12.4 Add a Scheduled Broadcast Task 145
Chapter 13 Network Device 149
13.1 Set Up Captive Portal 149
13.2 Mange Users 150
Chapter 14 Device Management 152
14.1 How to set parameters on the device local page before adding devices to the system? 152
14.2 How to add devices to Hik Connect for Teams? 154
Chapter 15 Services 159
15.1 How to invite a service provider to manage your system? 159
15.2 How to activate services and purchase services? 159
15.3 How to transfer cloud storage? 159
15.4 How to view password usage records? 160
15.5 What are the AI services and how to use them? 160
15.5.1 Focus 160
15.5.2 AI Notification 162
15.5.3 AI Deterrence 163
15.5.4 Daily Summary 164
15.5.5 Fusion Search 165
15.5.6 AI Timeline 167
15.5.7 Gun Detection 168
15.5.8 AI Assistant (Video) 169
15.5.9 AI Assistant (Access Control & Attendance) 171
Chapter 16 Alarms 174

16.1 How to set alarms? 174
16.1.1 How to add a general alarm? 174
16.1.2 How to add an AI notification? 179
16.1.3 How to configure a receiving schedule template? 180
16.2 How to search for alarms? 181
16.3 How to view resources' real-time alarms? 183
16.4 How to view pop-up window triggered by alarm? 186
Chapter 17 Map Management 189
Chapter 18 Maintenance 191
18.1 How to view real-time status? 191
18.2 How to monitor device health? 191
18.3 How to search for logs stored on devices? 194
18.4 How to search for operation logs? 196
18.5 How to view user login reports? 196
Chapter 19 Accounts 197
19.1 How to get accounts, log in, and create accounts? 197
19.2 How to configure Azure AD settings and log in to Hik Connect for Teams via Azure AD? 200
19.3 How to add a user? 217
19.4 How to import users? 218
19.5 How to assign roles to users? 219
19.6 How to change password of the current user? 221
19.7 How to delete a super user? 221
19.8 How to enable Two-Factor Authentication (2FA)? 222

Chapter 1 Introduction

Hik Connect for Teams (HCT) offers a comprehensive solution for both residential and business needs. An HCT system (hereinafter referred to as "the System") can be remotely handed over to an enterprise user via the Internet without the inconvenience of onsite server deployment. By subscribing to the HCT services (e.g., video management service, access control service, video intercom service, attendance service, on-board monitoring service, intrusion service, and analysis report service), the enterprise users can manage resources remotely, perform video-based monitoring, handle alarms, locate and track vehicles, control doors, manage calls, and so forth. HCT is suitable for single-site or multi-site scenarios including the monitoring and management of retail stores, petrol stations, factories, office buildings, and vehicle fleets.

1.1 What are the differences between the Portal and the Mobile Client?

Table 1-1 Portal and Mobile Client

Client	Description
Portal	Log in to HCT to manage resources and perform related configuration and operations (Portal URL: ***https://www.hik-connect.com/***). All features of the services (except for those related to call answering and the self-service features) are available on the Portal.
Mobile Client	Log in to HCT to use more basic features of the services, such as live view, playback, driving monitoring, remote door controls, person/resident management, arming control of security control partitions (areas) or zones, etc. It is also for self-service users to use features such as door opening via mobile credentials, call answering and management, temporary pass management.

1.2 What are the related entities?

Here we introduce the entities (any physical or conceptual object) related to HCT.

Table 1-2 Entities Related to HCT

Entity	Description
Service Provider	The service provider who creates the HCT system and hands it over to the enterprise user, or who is invited to manage an HCT account. A service provider can be a system integrator or an installer, dealer, reseller, etc.
Hik-Partner Pro	The platform used by the service provider to create HCT systems and/or purchase more services for HCT users.
System Handover	The process in which the service provider hands over the ready-to-use HCT system together with devices added on Hik-Partner Pro to the enterprise user via the Internet.
Super User	The enterprise user who accepts the ready-to-use HCT system or self-registers an HCT account and plays the role of the initial administrator of HCT. The super user has full access to resources and features in HCT.
Normal User	All other users except the super user. Different roles can be assigned to normal users to let them have different permissions to access resources and features in HCT. In other words, a normal user might have limited access to resources and features in HCT.
Resource	All physical resources and logical resources managed in HCT. Physical resources refer to devices including NVRs, DVRs, network cameras, on-board devices, alarm devices, Hik-ProConnect boxes, etc. Logical resources refer to abstractions of components of physical resources. For example, video channels are the logical resources of NVRs.

1.3 What's the running environment of Hik Connect for Teams?

The following is the recommended environment for running the Portal.

Operating System

Microsoft® Windows 7 (32-bit and 64-bit)
Microsoft® Windows 8.1 (32-bit and 64-bit)
Microsoft® Windows 10 (64-bit)
Microsoft® Windows 11 (64-bit)

Web Browser Version

Google Chrome® 100 and above
Firefox® 100 and above
Microsoft® Edge 100 and above

1.4 How to get accounts, log in, and create accounts?

How to register a super Admin account and log in?

1. Register a personal account first: Go to ***https://www.hik-connect.com/*** , click **Register Now**, and enter required information to register a person account.
2. Log in to Hik-Connect using the registered personal account, and click **Create Team** to enable more service.

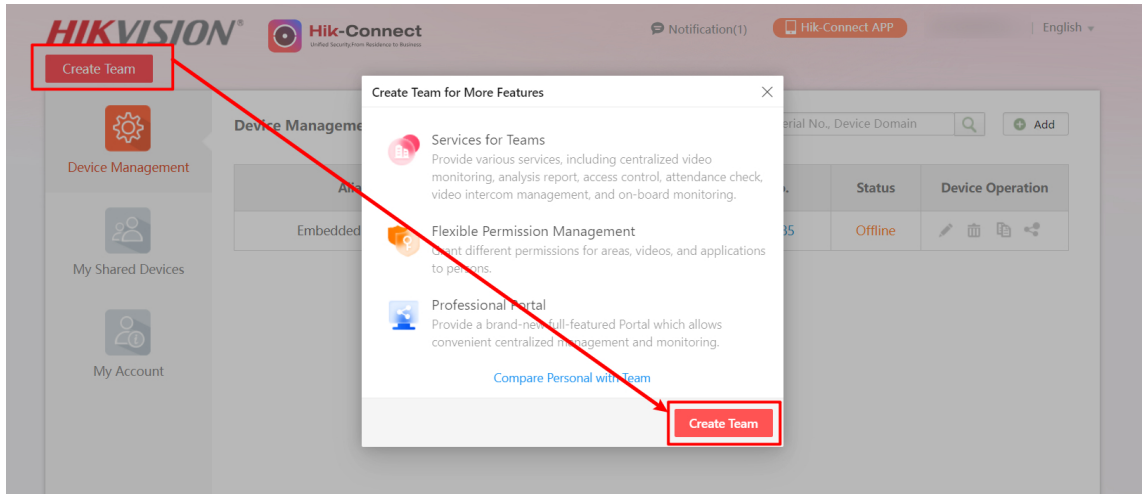


Figure 1-1 Create Team

How to accept system handed over by your service provider?

A service provider can hand over a system to you by sharing.

- The ownership of the system and its devices belongs to the service provider, who reserves the right to revoke the account and devices at any time. To protect your legal rights, please reach an agreement with the service provider before accepting the system, specifying the service details and validity.
- If the service provider shares the system with a third party, the third party will have access to the system's history data. If such data involves personal information or business secrets, please contact the service provider to change the encryption password promptly after the system sharing is canceled to prevent data leakage.

- If the service provider stops sharing the system with you, sub-accounts will be retained, and you may choose whether the sub-accounts will exit the team. Sub-accounts cannot join multiple teams; to join a new team account, you must first exit the current team.
- Please note that the ownership of the system and its devices always belongs to the service provider. You are not authorized to delete devices added to the system.
- The service provider reserves the right to access the device data under the system at any time, including but not limited to device configuration, live view, playback, intercom, PTZ (pan-tilt-zoom), PIRCAM GIFs, and video clips. These permissions may involve your personal information or privacy.

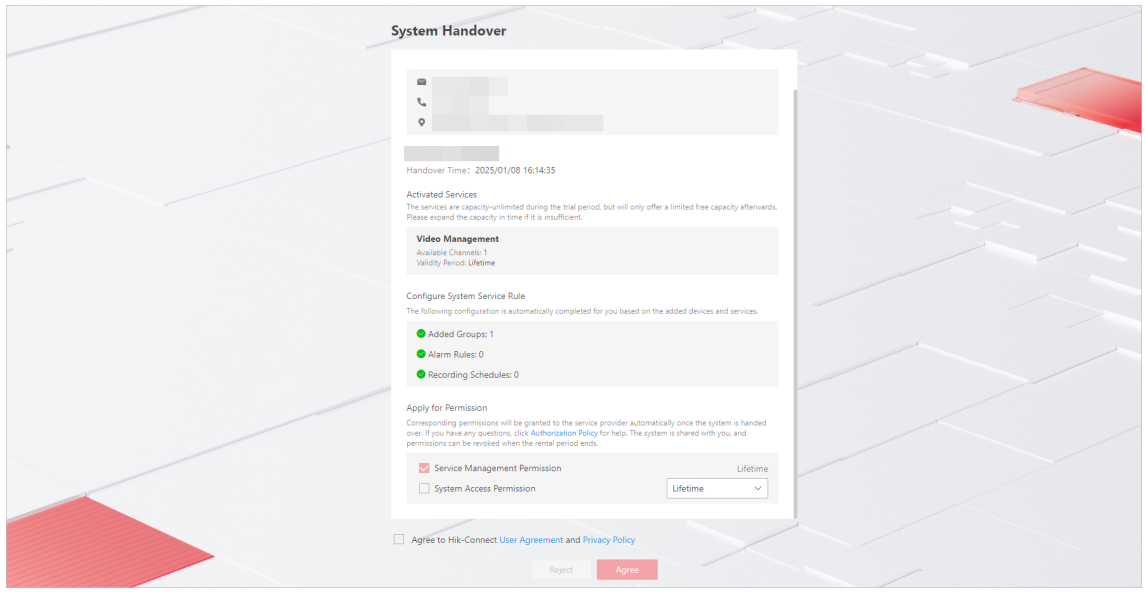


Figure 1-2 Hand Over by Sharing

How to create accounts for your team members?

Go to ⁞⁞ → **Team** → **User Management** → **Add** to add a user.

Account Type

The added user can log into Hik Connect for Teams through the email or phone number.

User Status

Freezing an account will prevent the user from log in to the system and revoke them the granted resource and operation permissions.

Role Name

A role has specific operation permissions, and assign a role to a user will grant them the operation permissions of the role.

Chapter 2 Video Management

2.1 Example Scenario

1. ***Add Encoding Devices***
   - Install and configure encoding devices such as cameras and NVRs. Ensure they are connected to the network and properly integrated.
   - **Example:** For a corporate campus, deploy IP cameras at entrances and critical areas, and connect them to centralized NVRs for storage and management.
   - Path: ⁞⁞ → **Device → Encoding Device**
2. ***Configure Recordings for Cameras***
   - Set local storage or cloud storage for cameras. Setting recordings is required before you can start playback.
   - **Local Storage:** Insert an SD card to the network camera, or install a disk inside the NVR. Then go to **Video → Recording Schedule Template Settings** to set when to record and what to record.
   - Path: ⁞⁞ → **Video → Recording Schedule Template Settings**
3. ***Configure Cloud Storage for Cameras***
   - Enable cloud storage service for cameras linked to Hik-ProConnect Box or NVRs. Event-related videos will be uploaded to the cloud.
   - **Example:** If the device does not support cloud storage, link the camera to a Hik-ProConnect box channel, set the stream type, and select a cloud storage plan for activation.
   - Path: **Device → Configure Storage → Configure Cloud Storage**
4. ***Add a Focus***
   - Add specific people, vehicles, or natural language descriptions as focus targets. With AI, you can define who to watch for.
   - **Example:** Add a focus for "people not wearing a badge" or "white minivan" to detect specific targets.
   - Path: ⁞⁞ → **Video → Focus**
5. ***View Camera Wall and Daily Summary***
   - View and manage the video module by camera. Get an overview of all camera live views categorized by group.
   - **Example:** Click Daily Summary to view AI-generated daily overview with counts of people, vehicles, animals, suspicious events, and AI alarms.
   - Path: ⁞⁞ → **Video → Camera**
6. ***Start Intelligent Search***
   - Search videos by text or image. Describe targets in everyday language or upload images to find relevant footage across multiple cameras.
   - **Example:** Search for "person in white" to instantly find footage, with results filterable by time.
   - Path: ⁞⁞ → **Video → Intelligent Search**
7. ***Start Live View and Control PTZ***

- Start live view and control PTZ functions such as direction, zoom, iris, focus, 3D positioning, light, and wiper.
- Path: ⁞⁞ → **Video → Video Security**

8. ***Start Playback***
   - Play back videos stored on cloud or local device. Double-click a camera to view playback, then select Cloud Storage or Local Storage.
   - Path: ⁞⁞ → **Video → Video Security → Playback**
9. ***Manage Persons of Interest***
   - Manage persons of interest by adding groups and face pictures. Add new persons or select from Person Module.
   - **Example:** Add a group named VIP customers and add face pictures to the group.
   - Path: ⁞⁞ → **Video → Persons of Interest**
10. ***Set Timelapse***
    - Time-lapse cameras capture images at set intervals over extended periods. Set parameters such as scenario, camera, start date, generate timelapses, time, interval, and timelapse package.
    - **Example:** For a sunrise scenario, set the time to 05:00-7:00 and interval to 5 minutes.
    - Path: ⁞⁞ → **Video → Timelapse**
11. ***Set Alarms for Video Devices***
    - Set alarms for video devices. Refer to the alarm configuration guide for details.
    - **Example:** Configure alarm triggers and notification methods for video devices.
    - Path: ⁞⁞ → **Alarm**

2.2 How to add encoding devices?

Refer to ***Device Management*** .

2.3 How to configure recordings for cameras?

Setting recordings is required before you can start playback. You can either set local storage or cloud storage for cameras.

2.3.1 How to configure local storage for cameras?

Note

Make sure you insert an SD card to the network camera, or install a disk inside the NVR.

On the top navigation bar, select **Video → Recording Schedule Template Settings** so set when to record and what to record.

Time-based

Continuously recording according to the time you arranged.

Event-based

Recording videos when alarm is triggered.

2.3.2 How to configure cloud storage for cameras linked to Hik-ProConnect Box or NVRs?

- If the device to which a camera belongs does not support cloud storage, you can enable cloud storage service for the camera by linking it to a Hik-ProConnect box channel, setting the stream type based on your network conditions, and selecting a cloud storage plan for activation. After cloud storage is enabled for a camera, event-related videos of the camera will be uploaded to the cloud.
- You can enable cloud storage service for a camera linked to an NVR that supports cloud storage by setting the stream type based on your network conditions and selecting a cloud storage plan for activation. After cloud storage is enabled for a camera, event-related videos of the camera will be uploaded to the cloud.

1. Go to **Device**, click a camera name or select cameras and click **Configure Storage → Configure Cloud Storage** .
2. Select a Hik-ProConnect box from the drop-down list as the storage location.
3. Set the required parameters.

Note

For camera(s) with a cloud storage plan already activated, you cannot switch to another plan within the validity period of the current plan. Click **Cloud Storage Management** to go to the cloud storage management page to manage the cloud storage service if needed, such as pausing or disabling cloud storage for the camera.

2.3.3 How to configure cloud storage service and set events?

This guide provides step-by-step instructions for configuring cloud storage service and setting up events for cameras.

Note

The cloud storage feature is only available in some countries/regions. Please contact Hikvision for details.

Configure Cloud Storage Service

1. Go to → → **Device Compatibility List** to make sure the device supports cloud storage.
2. Go to **Device → Encoding Device** .

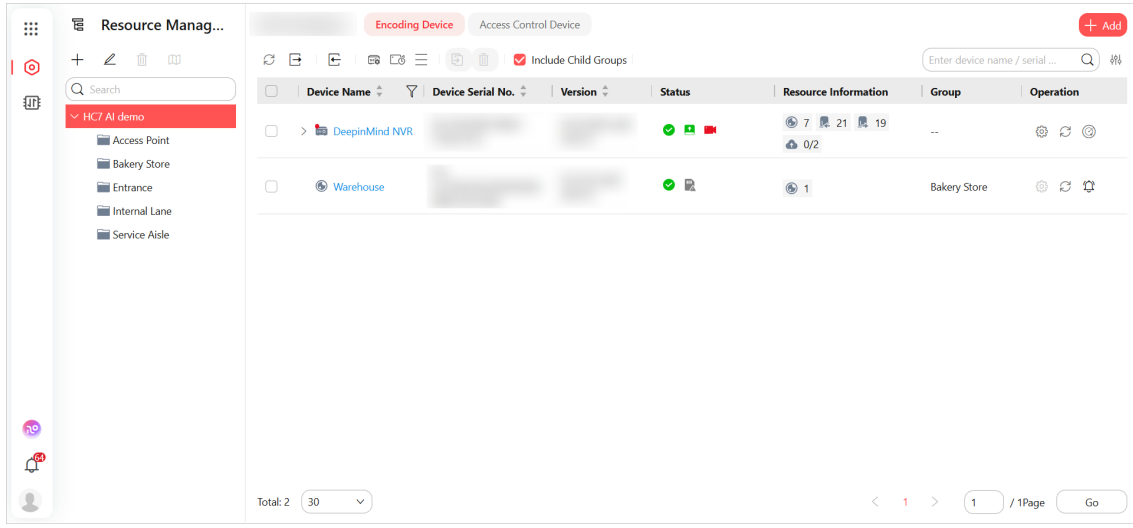


Figure 2-1 Resource Page

3. Find the camera you want to configure cloud storage for and click its name.
4. Click the **Cloud Storage Server** tab.
5. Switch on **Cloud Storage Server**, and select a storage location.

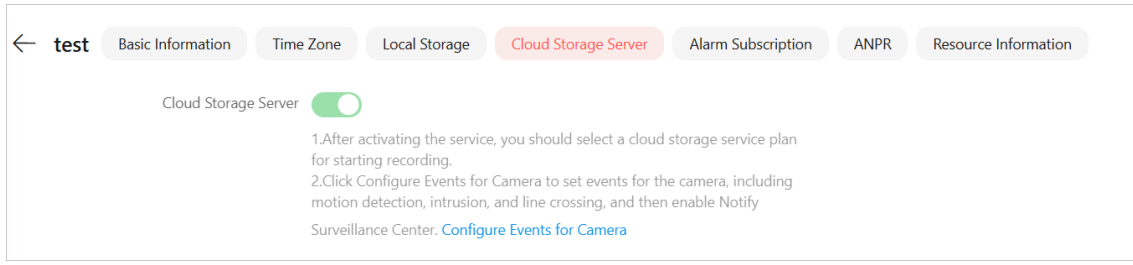


Figure 2-2 Enable Cloud Storage Server

Note

- You can test your network environment using the Network Test function, and determine whether to set HD or SD for the stream type.
- If the device supports cloud storage, then you can select **Encoding Device** (itself). However, not all devices support cloud storage, and in that case you will need to select a Hik-ProConnect box.

6. Select an available cloud storage plan to activate the cloud storage service.

Note

If you have no available packages, contact your service provider to purchase for you.

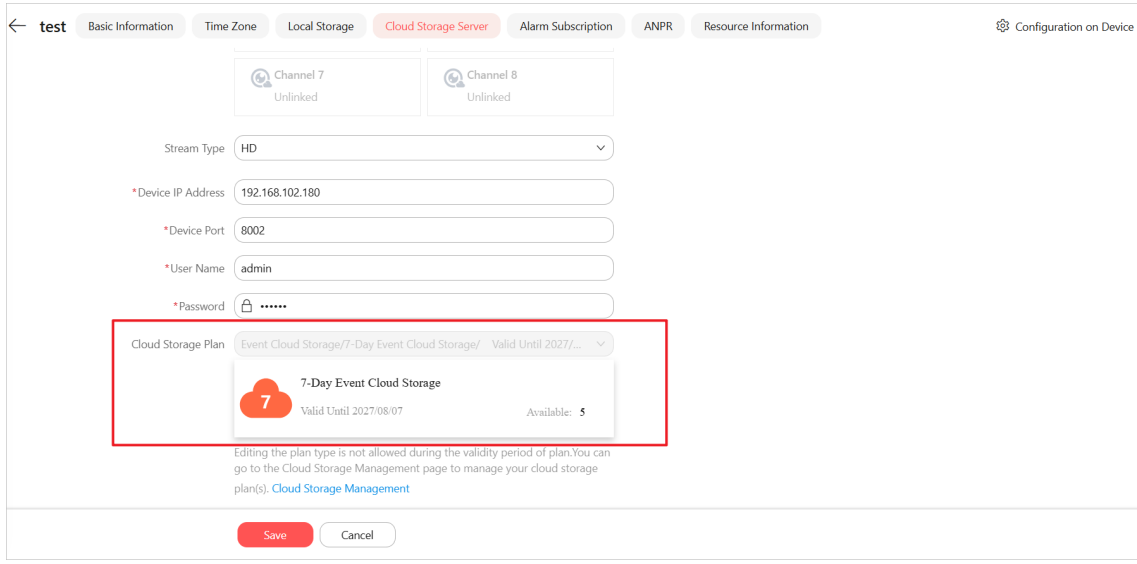


Figure 2-3 Select a Plan

Configure Events for Camera

Configure events for the camera and then save the cloud storage server settings. Here we only take setting options under basic event as an example.

1. Go to the camera configuration page, and click **Basic Event → Motion** .
2. Select the camera and check **Enable Motion Detection and Dynamic Analysis for Motion**.
3. Go to **Area Settings** to draw the area.

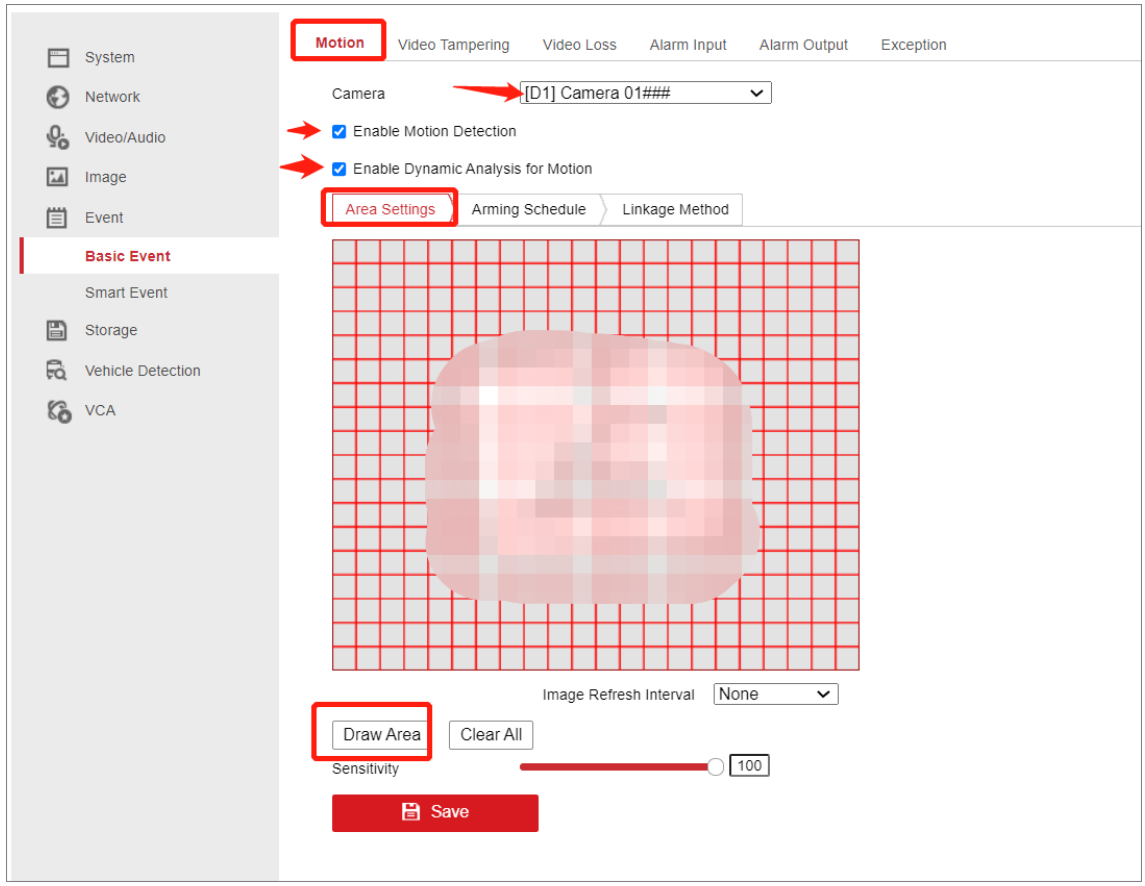


Figure 2-4 Event Configuration

4. Go to **Linkage Method** and check the **Notify Surveillance Center**. Then click **Save**.

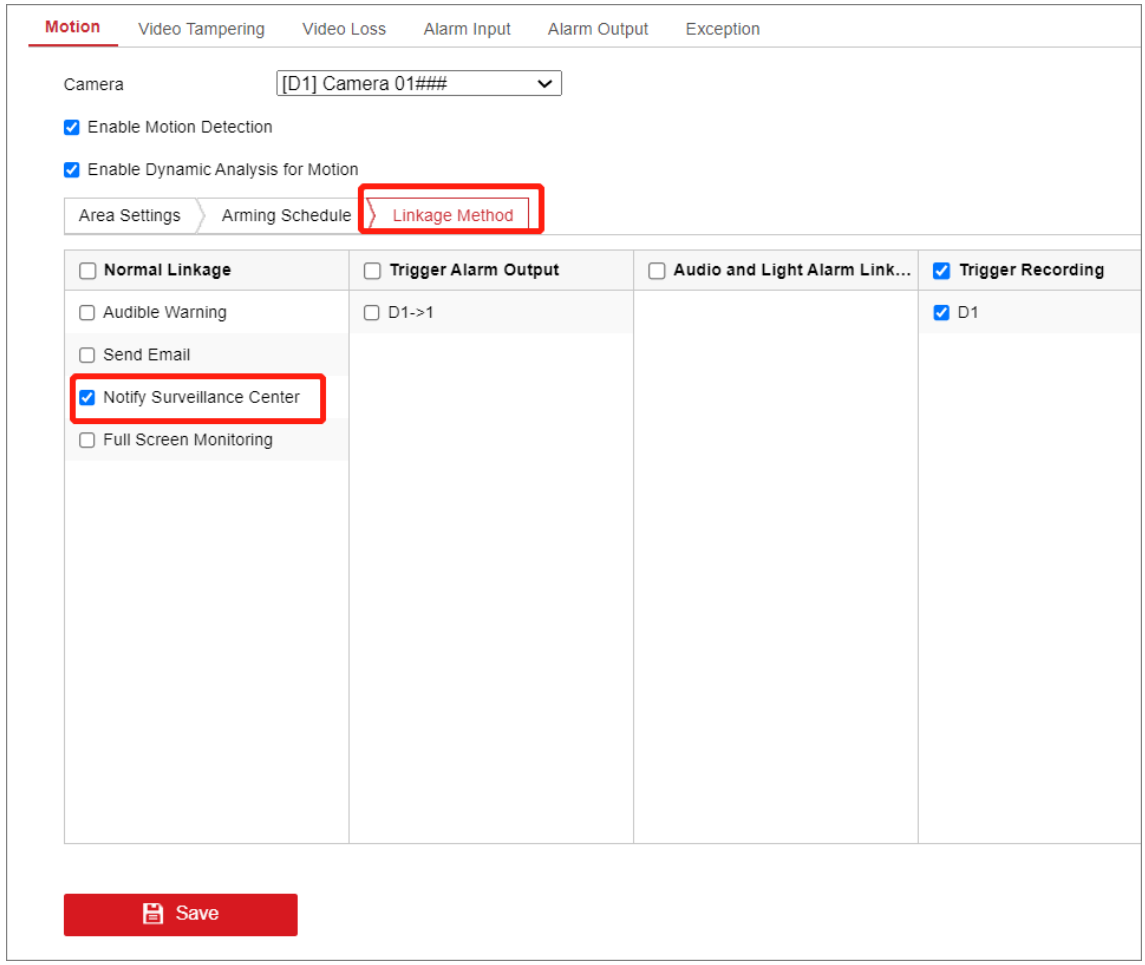


Figure 2-5 Notify Surveillance Center

2.4 How to add a focus?

You can add the following as focus: specific people, vehicles, or describe what you're looking for in natural language. With AI, you can define who to watch for, such as people not wearing a badge or specific visitors.

1. Go to ⁝⁝⁝ → **Video** → **Focus** .
2. Click **Add Focus**.

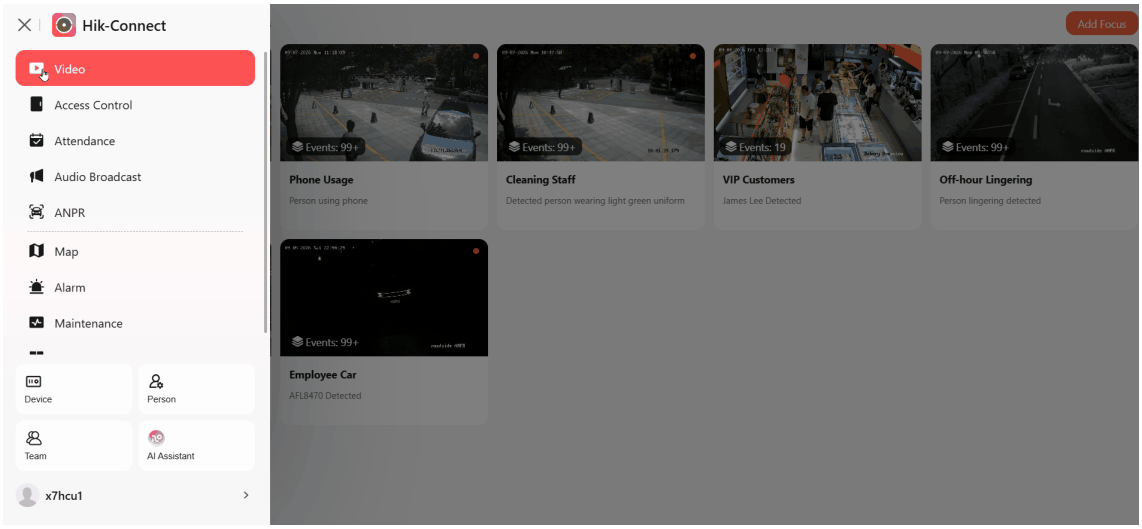


Figure 2-6 Focus

3. Set name, target (Supports three types of focus objects.), recognition type, and other parameters.
   - **Person:** Select specific targets from the personnel database, or focus on all "unknown persons."
   - **Vehicle:** Select specific targets from the license plate database, or focus on all "unknown vehicles."
   - **AI Prompt:** Input text descriptions (e.g., "white minivan"), and the system performs semantic matching.
4. Click **OK**.
5. After the focus is added, you can view events about the focus.

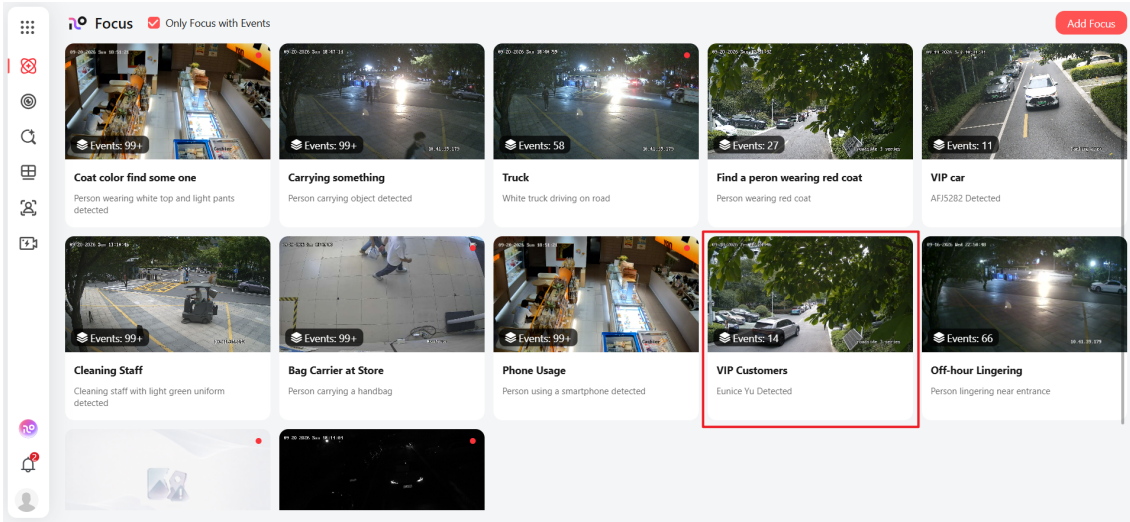


Figure 2-7 Focus List

6. Click on a Focus to view all clips with the focused target detected. Scroll on the right pane and you can get a fast view of all the cameras with recordings of the target. Click a card to play the video.

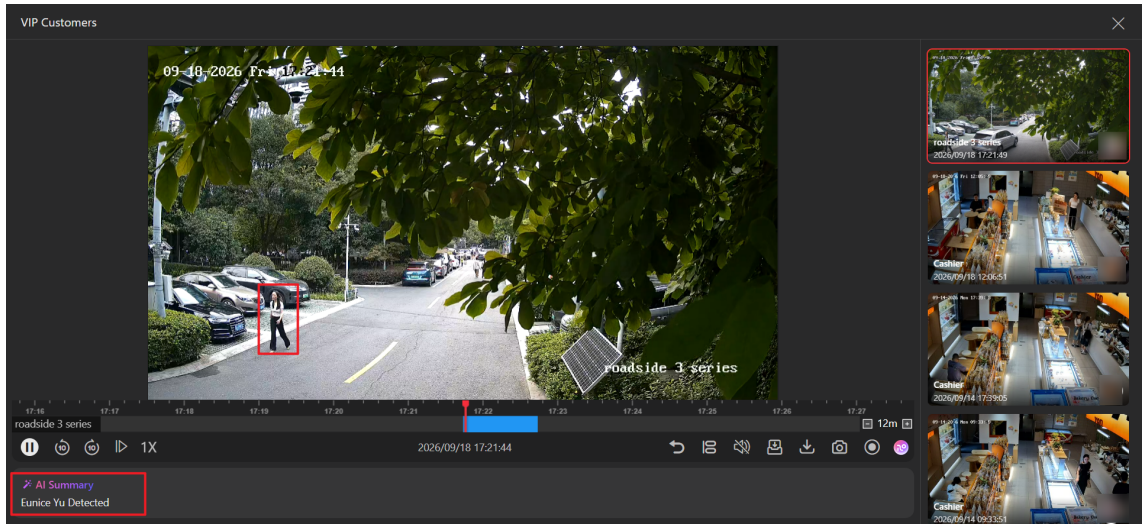
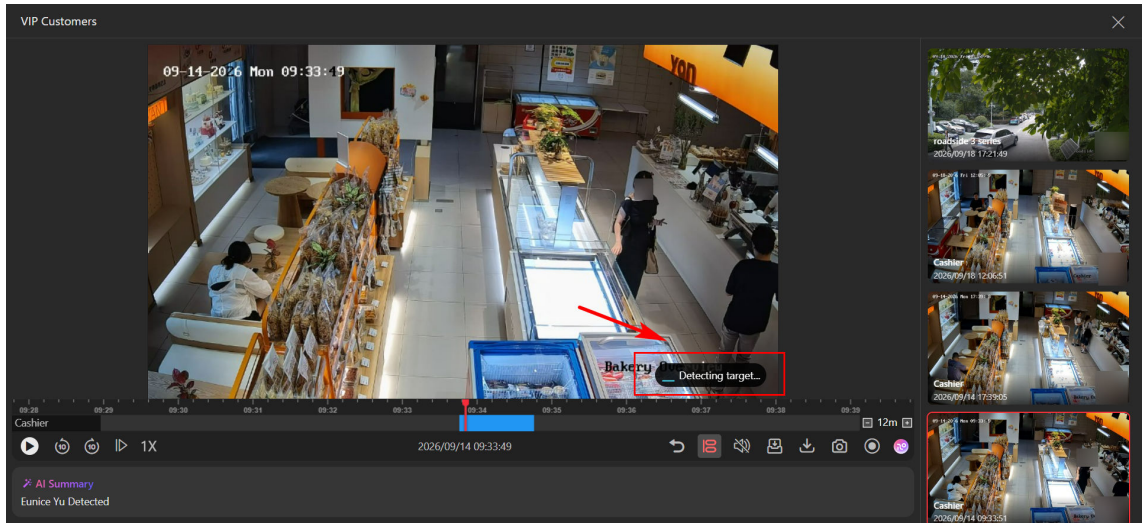
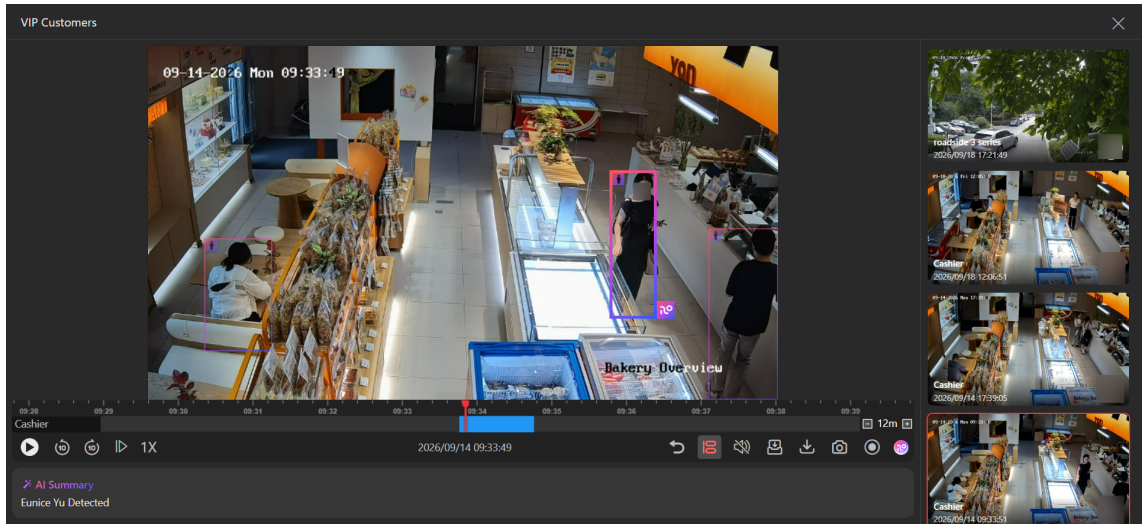
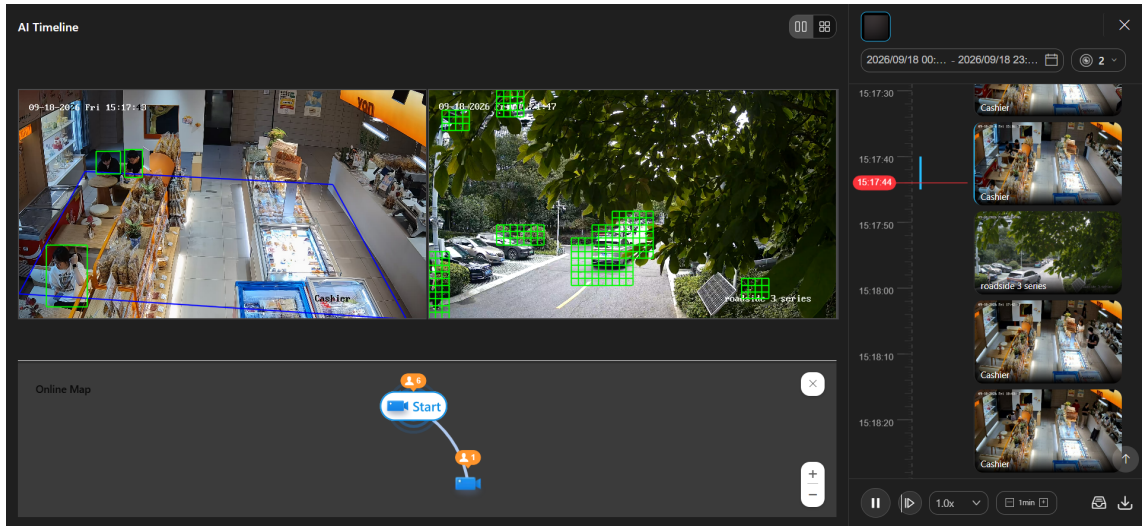


Figure 2-8 Focus Clips

7. (Optional) Generate an AI Timeline of the target.







2.5 How to view the camera wall and view the daily summary of a camera?

You can view and manage the video module by camera.

1. Go to ⋮⋮⋮ → **Video** → **Camera** .
2. You can have an overview all camera live view categorized by group.

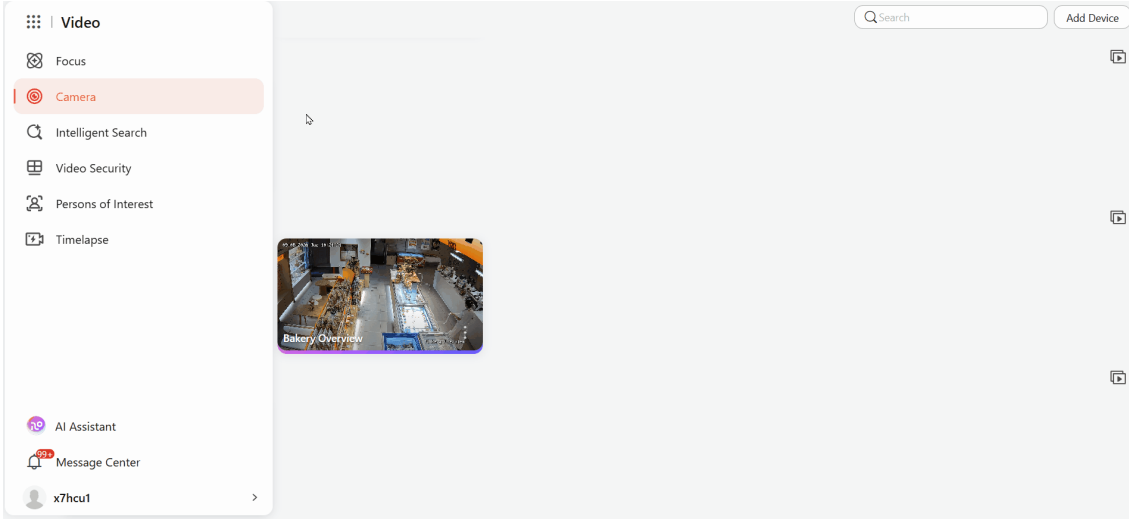


Figure 2-9 Camera

3. Click to batch play the cameras in a group.
4. (Optional) Click **Daily Summary** in the upper-left corner. AI helps generate a daily overview with counts of people, vehicles, animals, suspicious events, and AI alarms. Click an event to instantly view clip details.

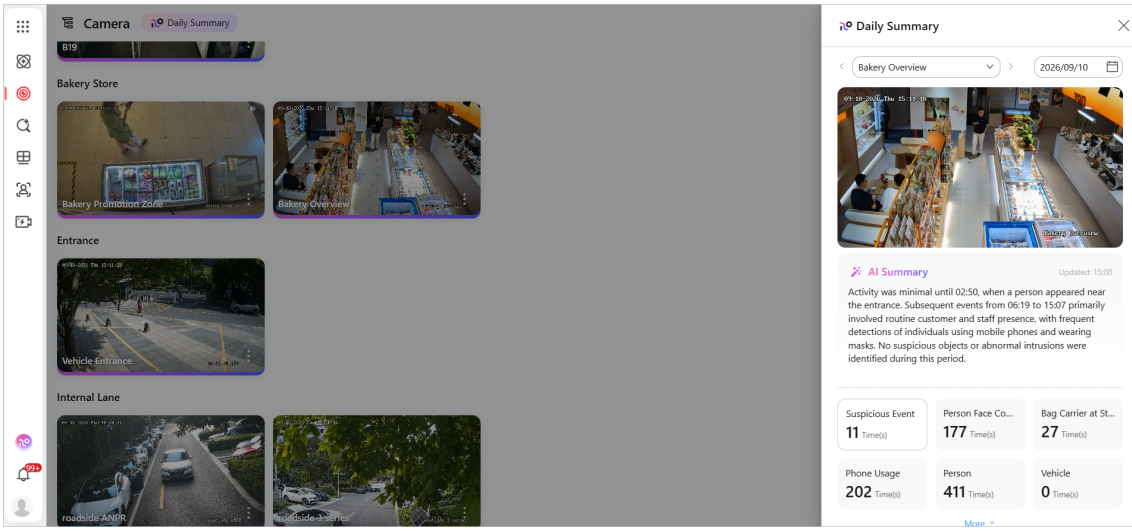


Figure 2-10 Daily Summary

2.6 How to start intelligent search?

1. You can search videos by text. Describe targets in everyday language like "person in white" to instantly find relevant footage across multiple cameras, with results filterable by time.

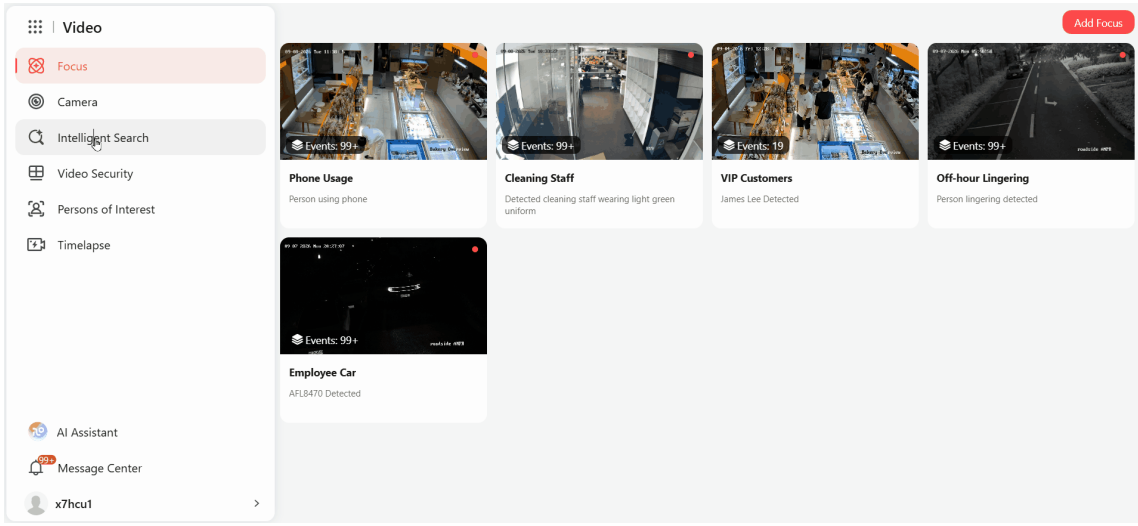
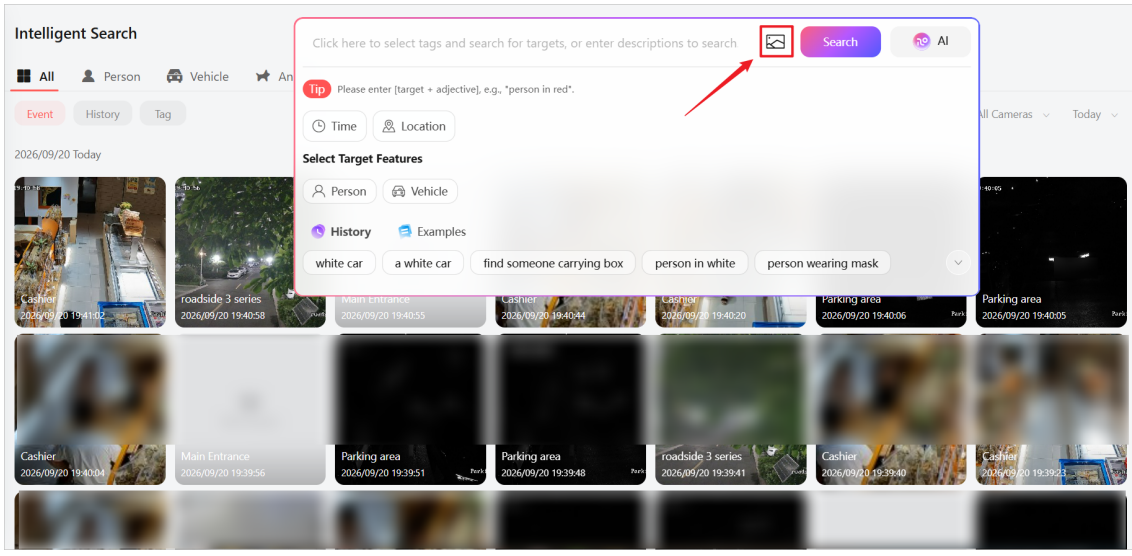
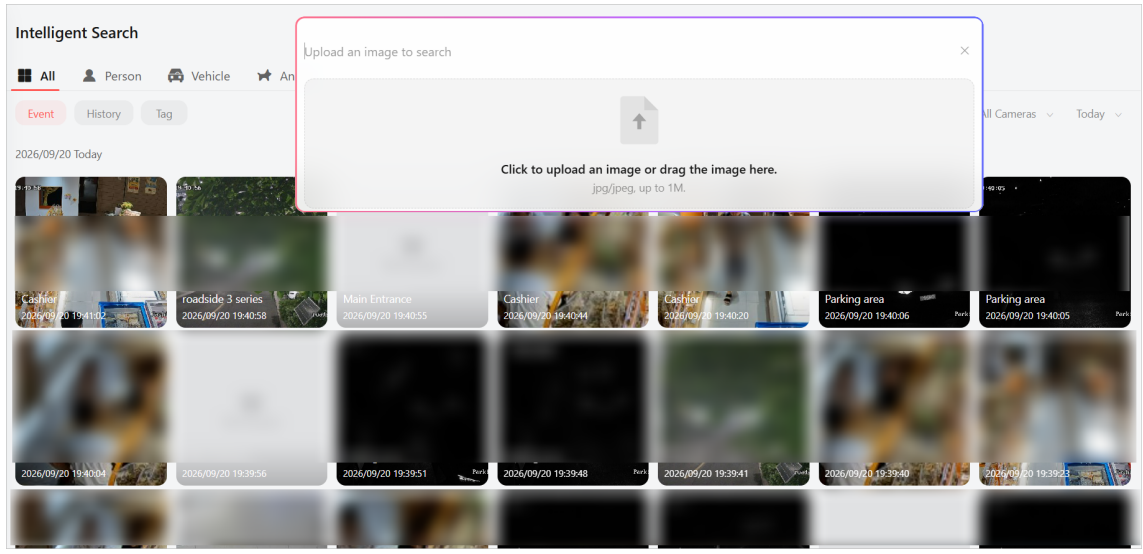
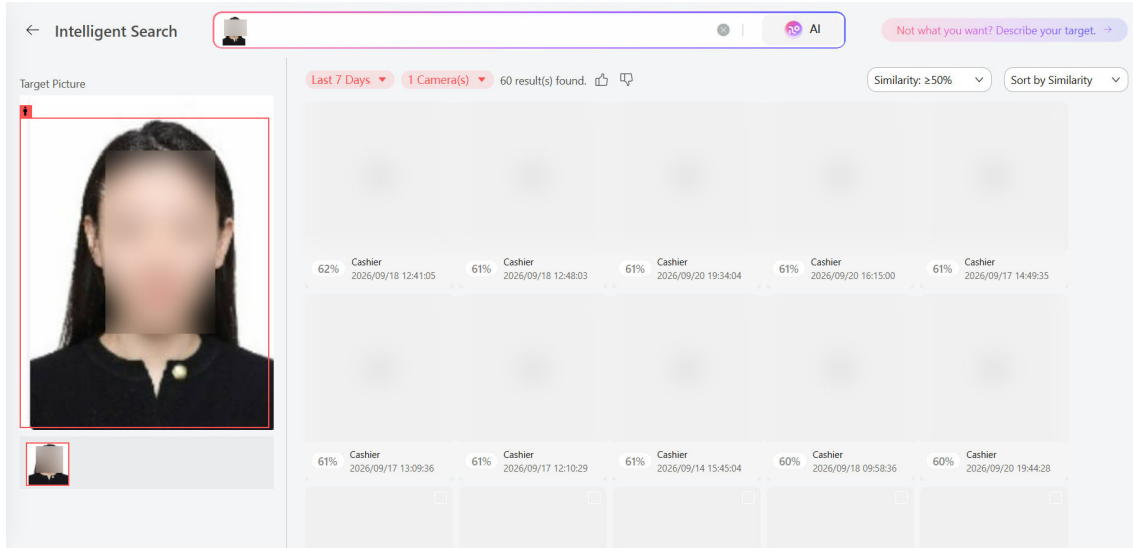


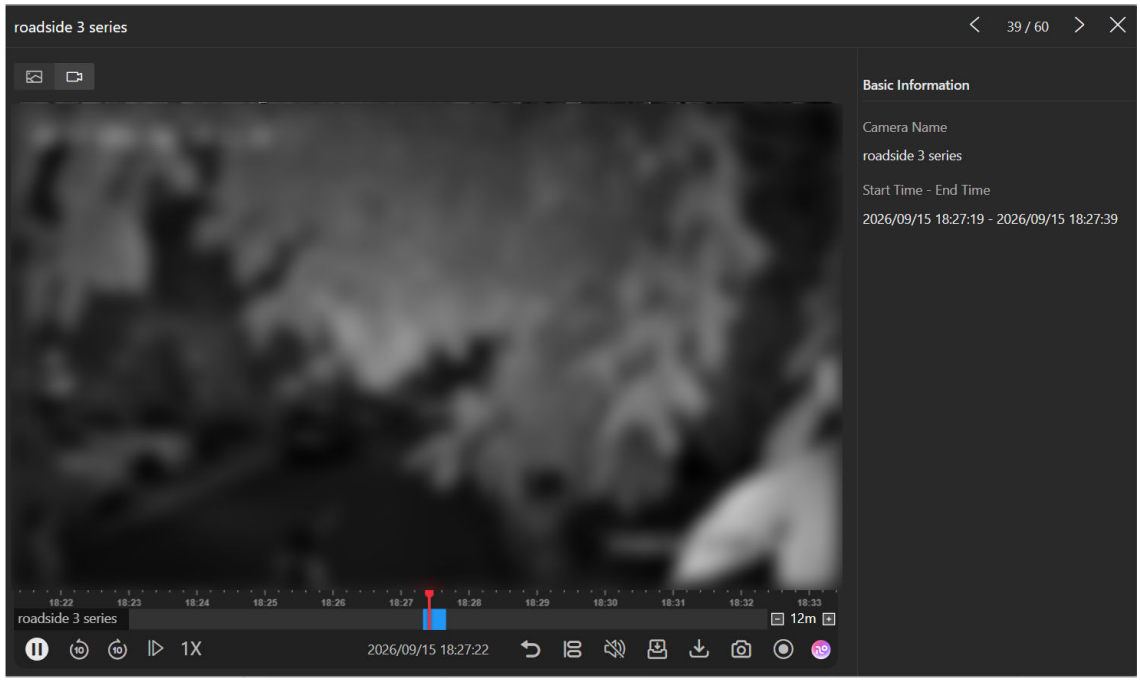
Figure 2-11 Intelligent Search

2. You can search videos by image on the Intelligent Search page.




Intelligent Search
All
Person
Vehicle
Event
History
Tag
2026/09/20 Today
Upload an image to search
Click to upload an image or drag the image here.
jpg/jpeg, up to 1M.
All Cameras
Today
Cashier
roadside 3 series
2026/09/20 19:40:58
Main Entrance
2026/09/20 19:40:55
Cashier
2026/09/20 19:40:44
Cashier
2026/09/20 19:40:20
Parking area
2026/09/20 19:40:06
Parking area
2026/09/20 19:40:05
2026/09/20 19:40:04
2026/09/20 19:39:56
2026/09/20 19:39:51
2026/09/20 19:39:48
2026/09/20 19:39:41
2026/09/20 19:39:40
2026/09/20 19:39:23


Intelligent Search
AI
Not what you want? Describe your target.
Target Picture
Last 7 Days
1 Camera(s)
60 result(s) found.
Similarity: ≥50%
Sort by Similarity
62% Cashier 2026/09/18 12:41:05
61% Cashier 2026/09/18 12:48:03
61% Cashier 2026/09/20 19:34:04
61% Cashier 2026/09/20 16:15:00
61% Cashier 2026/09/17 14:49:35
61% Cashier 2026/09/17 13:09:36
61% Cashier 2026/09/17 12:10:29
61% Cashier 2026/09/14 15:45:04
60% Cashier 2026/09/18 09:58:36
60% Cashier 2026/09/20 19:44:28



2.7 How to start live view and control PTZ?

Go to ⁞⁞ → **Video** → **Video Security** .

Start Live View

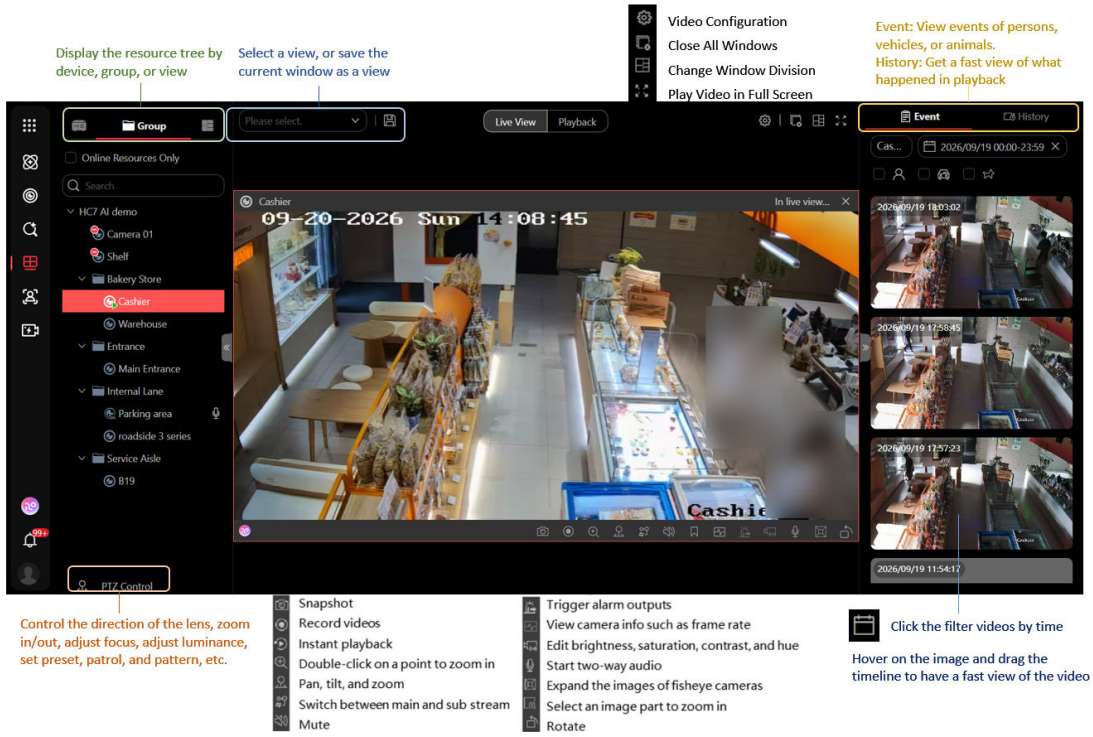


Figure 2-12 Live View Page

Control PTZ

	Direction Button, Auto-scan and PTZ speed.
	Zoom in or out the video for cameras that do not have their own optical zoom capabilities. Click again to disable the function.
	Used for adjusting the luminance of the image. The larger the iris is, the more the light enters, and the brighter the image will be.
	Click  to move the focal point backward, and click  to move the focal point forward.
	3D Positioning: Click on the desired position in the video image and drag a rectangle area in the lower right direction, then the dome system will move the position to the center and allow the rectangle area to zoom in. Click to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.

	Light: Click to fill light.
	Wiper: Use the wiper to clear the dust on the camera lens.

2.8 How to start playback?

Go to → **Video** → **Video Security** → **Playback** .

Playback Overview

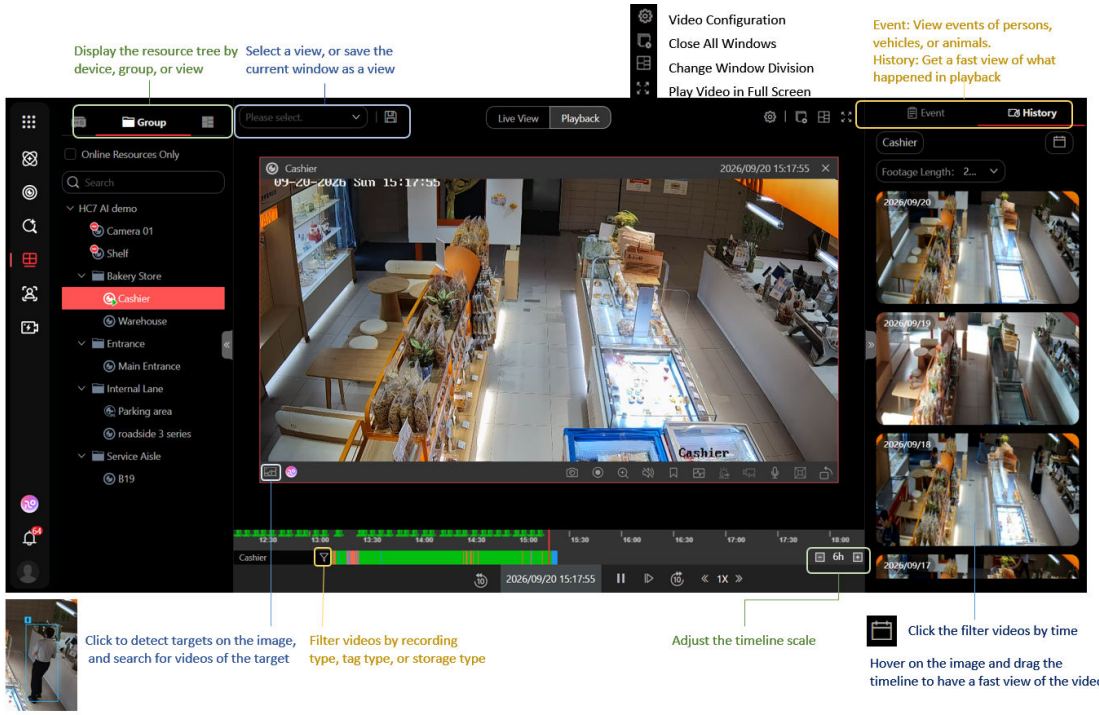


Figure 2-13 Playback

How to play back the videos stored on the cloud / local device?

1. Double click a camera.
   The playback of the selected camera will appear on the right side.
2. Click and select **Cloud Storage** / **Local Storage**.
3. Click **Save**.
   The time periods of all videos stored on cloud will be displayed on the timeline. You can select a period to play back the video.

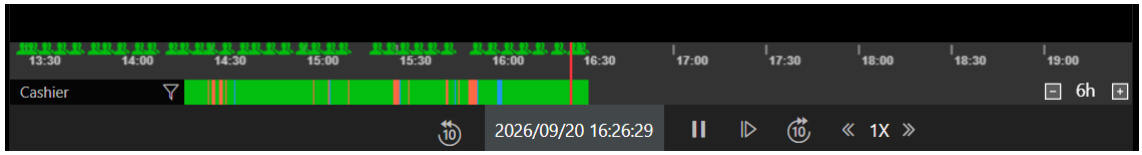


Figure 2-14 Timeline

2.9 How to manage persons of interest?

1. Go to ⁝⁝ → **Video** → **Persons of Interest** .
2. Click ＋ to add a group to manage persons. For example, you can add a group named VIP customers.
3. Select the added group, and click **Add Face Picture** on the right page to add faces to the group.
4. Select **New** to add a new person or click **Select from Person** to select persons from the Person Module.
5. Click **Add**.

2.10 How to set timelapse?

Time-lapse cameras capture images at set intervals over extended periods—hours, days, or weeks. These images can be compiled into a video to create a fast-forward effect of recorded events or scenes.

1. Go to ⁝⁝ → **Video** → **Timelapse** .
2. Supports adding a timelapse, and setting the following parameters:
   - the parameters about picture capturing such as start date and capturing intervals.
   - the parameters about generated videos such as video generation frequency and encryption status.

Parameters	Descriptions
Scenario	- **Construction:** A typical slowly-changing and long-term scenario in which the timela are by default generated monthly and the capturing interval is by def relatively long period - 1 hour. - **Intersection:** A typical fast-changing and short-term scenario in which the timelaps by default generated daily and the capturing interval is by default a relatively short period – 5 min. - **Custom:** Customize the capturing and timelapse generation parameters.
Camera	Select cameras or cameras linked to NVRs.

Parameters	Descriptions
Start Date	The start date of capturing pictures.
Generate Timelapses	For fast-changing scenarios such as sunset, select daily/weekly; for slow changing scenarios such as construction, select monthly or yearly.
Time	The daily capturing time. For example, set the time to 05:00-7:00 for a s scenario.
Interval	Set the picture capturing interval. For example, set it as 5 min, and pictu will be captured every 5 minutes.
Timelapse Package	- Contact your service provider to purchase packages. - Activate the service by yourself on the Services Details page. **Note** The video management service is already included in the cloud timela service.

3. You can end timelapses and restart timelapses.
4. You can generate timelapses by customizing time range. For example, for a 5-month timelapse schedule, you can generate timelapses for any period within that timeframe—whether a week, a month, or a custom interval.
5. Hover on an image, and you can download the captured pictures and generated videos to your local PC.

2.11 How to set alarms for video devices?

Refer to ***Alarms*** for details.

Chapter 3 Access Control

On the Portal, the Administrator can add access control devices to the System, group resources into different groups, and grant access to door or door groups to persons. After grant access to persons, persons will be authorized to access doors with their credentials during the authorized time period. Moreover, you can create temporary passes for people (e.g., visitors) with temporary access needs.



Figure 3-1 Steps of Setting an Access Control Scenario for a Company

1. ***Add Access Control Devices***
   Install and configure encoding devices such as access control devices. Ensure they are connected to the network and properly integrated.
2. ***Add Access Levels***
   - Add access control levels and add devices in step 1 to the access levels.
   - E.g., **Full Access**: The access level involves ①②③④⑤⑥
   - **For Stuff**: The access level involves ①②③⑤⑥
   - **For Visitors**: The access level involves ①②
   - **For Delivery Personnel**: The access level involves ①②⑥
3. ***Add Persons and Credentials***
   Add persons (e.g., managers, employees, and visitors) and add credentials such as face picture and fingerprints for the persons to open doors.
4. ***Grant Long-Term Access***
   Grant long-term access to persons: grant the access of access levels in step 2 or doors in step 1 to persons added in step 3.
5. ***Grant Temporary Access***

Grant temporary access to persons: grant the access of access levels in step 2 or doors in step 1 to visitors added in step 3 and set the validity and allowed passes.

6. ***Monitor Real-Time Door Status***
   Monitor real-time door status.
7. ***Retrieve Access Control Records***
   Retrieve access control records.
8. ***Set Remain Unlocked and Remain Locked Rule***
   (Optional) Set Remain Unlocked and Remain Locked rule.
9. ***Set Access Control Parameters***
   (Optional) Set access control parameters including holidays, access schedule templates, general parameters, and event subscriptions.

3.1 How to add the three elements: devices, access levels, and persons?

3.1.1 How to add access control devices?

Refer to ***Device Management*** .

3.1.2 How to add access levels?

An access level is a group of multiple access points. For example, you can add access points on the first floor to an access level and name it as First Floor, so when you grant a person the access to the access points on the first floor, you just need to grant the person the access of the First Floor access level instead of selecting all doors on the first floor.

1. Go to ⁝⁝ → **Access Control → Access Granting → Manage Access Level** to add an access level.
2. Create a name such as Visitor Access Level for the access level.
3. (Optional) Add descriptions to the access level if any.
4. Select individual doors or groups with multiple doors, and persons granted the access of the access level will be granted the access to all selected doors.
5. Select an access schedule which defines when persons are granted the access of selected doors. For example, you can grant retail store stuff the door access only during business hours, and they will not be allowed to enter stores during non-business hours.

3.1.3 How to add persons?

The System provides two ways of adding persons.

Add Department

When there are a large number of persons (e.g., employees of a company) managed on the platform, you can group persons into different department for better management.

1. Click ⁞⁞ → **Person** to enter the person management page.
2. At the top of the left pane (i.e., the department list), select an existing department as the parent department and click + to open the Add Department page.
3. Reselect the group(s) to change the default accessible group(s) for the new department, change a parent department, enter a name and description, and click **Add**.

Note

- By default, the accessible groups of the parent department are selected. If the selected group of the parent department is the root group, you can click **Reselect** to open the group selection panel. If not, you can directly reselect the group(s) on the area selection panel.
- The unavailable areas are controlled by permissions assigned to the current user.

Add Person

1. - One is to add users in ⁞⁞ → **Team** to automatically generate persons in the Person module.
   - The other is to go to ⁞⁞ → **Person** → **Add** to add persons.
2. Fill in the basic information, and click **Credential Management** to add credentials for the person to open doors.

Table 3-1 Add Credentials For Persons to Open Doors

Credentials	Descriptions
Face	Hover on the blank profile picture to select a method of adding faces.
Card	Click **Configuration**, and select a card issuing mode.
Bluetooth/NFC	Opening doors via Bluetooth or NFC is dependent on the phone app use, so you need to create an app account for the person first to allow them to open doors via Bluetooth/NFC on the phone.
Fingerprint	Click **Configuration**, and select a fingerprint collection mode.
PIN	Create a PIN, and the PIN can be used to open doors.

3. Set access granting parameters for persons.

Table 3-2 Access Granting Parameters

Parameters	Descriptions
Access Granting	Click **Configure** to select doors or access levels to the person.
Temporary Pass	Switch on to allow the person to grant temporary access to others on the APP. The person can only grant the temporary

Parameters	Descriptions
	access of the doors and access levels that the person has access to.
App Use	Switch on **App Use** to generate an account for the person to log into the app to open doors via Bluetooth, start intercom, etc.

Batch Import Persons

Table 3-3 Batch Import Persons

Method	Parameters
Import Persons from Device If the added access control devices and video intercom devices have been configured with person information, you can get the person information from these devices and import it to the System. The person information that can be imported includes person names, person IDs, profile pictures, credentials (PIN codes, cards, fingerprints, and faces), effective periods, etc.	1. Select a department from the department list on the left, and click **Import → Import from Device** at the top of the person list to open the Import from Device pane. 2. Specify the device type and area to select the device(s) from which the person information is imported. 3. Select the person(s) to be imported, and select a department to which persons will be imported. **All** Import all persons stored in the selected device(s). **Specified Person ID** Specify up to five persons by entering their IDs to import the specified person information to the System. 4. Check **Replace Profile Picture** to replace existing persons' profile pictures by new ones from devices. 5. Click **Import** to start importing. **Note** During the importing process, the System will compare the person information on devices with that in the System based on person names. If a person name exists on the device but does not exist in the System, the System will add a new person. If a person name exists on both sides, the corresponding person information in the System will be replaced by the one on the device.
Import Persons via Template If there are multiple persons to be added to the System, you can import them with the minimum	Select a department from the department list on the left, and click **Import → Import Person Information via Excel** above the person list to open the corresponding pane.

Method	Parameters
effort via an Excel template that contains the person information such as person names, departments, and effective periods.	Click **Download Template** on the Import Person Information via Excel pane or click **Import → Download Template for Importing Person Information** above the person list to open the Download Template for Importing Person Information window/pane. Check the basic information items to be included in the template,and click **Download** to save the template to the local PC. Enter the required information and click and select the template (with person information) from the local PC to upload. Check **Replace Repeated Person** to replace the person information if the imported ID information is the same with that of the existing persons in the System.

3.2 How to grant access to persons?

You need to assign access levels to persons, so that the assignees can have the access to the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person or department.

Grant Access by Department

Go to → **Access Control → Access Granting → Grant by Department** .

- Select department(s) and click **Grant Access** to grant access to the department(s).
  1. In the department list, click on a department.
  2. In the assigned access level pane on the right, click **Grant**.
  3. In the Assign Access Level pane, select the access levels you want to assign to the selected department.
  4. Click **Save**.
- Select **Batch Grant Access** to grant access to multiple departments.
  1. Click **Batch Grant**.
  2. In the department list, select the departments where you want to assign access levels.

     Note

     Sub-departments are excluded from selection by default. To include all sub-departments of each department, check **Select Sub-Groups**.
  3. In access level list, select the access levels you want to assign to the departments.
  4. Click **Save**.

Note

- After assigning access levels to a department, you can still modify the access levels for each person in the group, and it will not affect the settings for the department.
- The access level settings will be applied to devices automatically.
- To revoke access from a department, select an access level and click **Revoke**. To revoke all access levels, click → **Revoke All** .

Grant Access by Person

1. Go to → **Access Control** → **Access Granting** → **Grant by Person** → **Grant Access** to grant a person the access to specific doors or specific access levels.
2. On the Assign Access Level pane, click , select the persons, and click **Add**.
   To apply the access level settings of all persons, check **Select All Persons**.
3. Check access levels, and click **Save** to automatically grant access to persons.

Note

To revoke access from a department, select an access level and click **Revoke**. To revoke all access levels, click → **Revoke All** .

Manually Apply Access Granting

If you have changed access level settings, or assigning access levels failed, you need to apply the relations between persons and access points to the devices manually.

1. Go to → **Access Control** → **Access Granting** → **Overview** → **Apply Access Level Settings** to manually apply the settings if you changes access granting settings or failed to grant access.
2. Select the access points to apply the persons' access level settings.
   - To apply the access level settings of all access points, switch off **Specified Device(s)**.
   - To apply the access level settings of specific access points, switch on **Specified Device(s)** and select the access points.
3. Apply access level settings to devices.
   - To clear all persons' access level configurations on the devices first and then apply the configurations in the platform to the devices, check **Apply (Initial)** and click **Apply**.

     Note

     During the initialization process, the devices will be offline, and persons cannot access these access points.
   - To apply changed (newly added, edited, deleted) access level settings to the devices, uncheck **Apply (Initial)** and click **Apply**.

3.3 How to grant temporary access?

By setting the access level(s) and validity period, you can create a temporary pass which contains a corresponding password and a QR code. A person with the temporary access need (e.g., delivery person) can use the temporary pass to unlock doors according to the set access level.

Note

Persons can create temporary passes only on the Mobile Client.

1. Go to → **Access Control → Temporary Pass Management** to add temporary passes.
2. Set the required information.

   Name

   The name for the temporary pass.

   Allowed Uses

   The number of times the temporary pass can be used to open each door.

   Validity Period

   The validity period of the temporary pass.

   Access Level

   The access level(s) of the temporary pass. The person using this temporary pass is assigned with the access level(s) added here.
3. Click **OK**.
4. After a pass is added, move your cursor to and click **Download** (if supported by device) to download and send the PIN or QR code to visitors to grant them temporary access to selected doors or access levels.
   Click in the Operation column to view the door unlock records of the temporary pass.

3.4 How to monitor real-time door status?

3.4.1 View Real-Time Access Events

You can view the real-time access events by customizing the event types/sources and columns to be displayed. You can also perform further operations including searching for records/data and viewing access event details.

Go to the real-time monitoring page by either of the following entrances:

- On the top navigation bar, click → **Access Control → Real-Time Monitoring** .
- In the service overview section on the Home page, click **Access Control → Go to Real-Time Monitoring** .

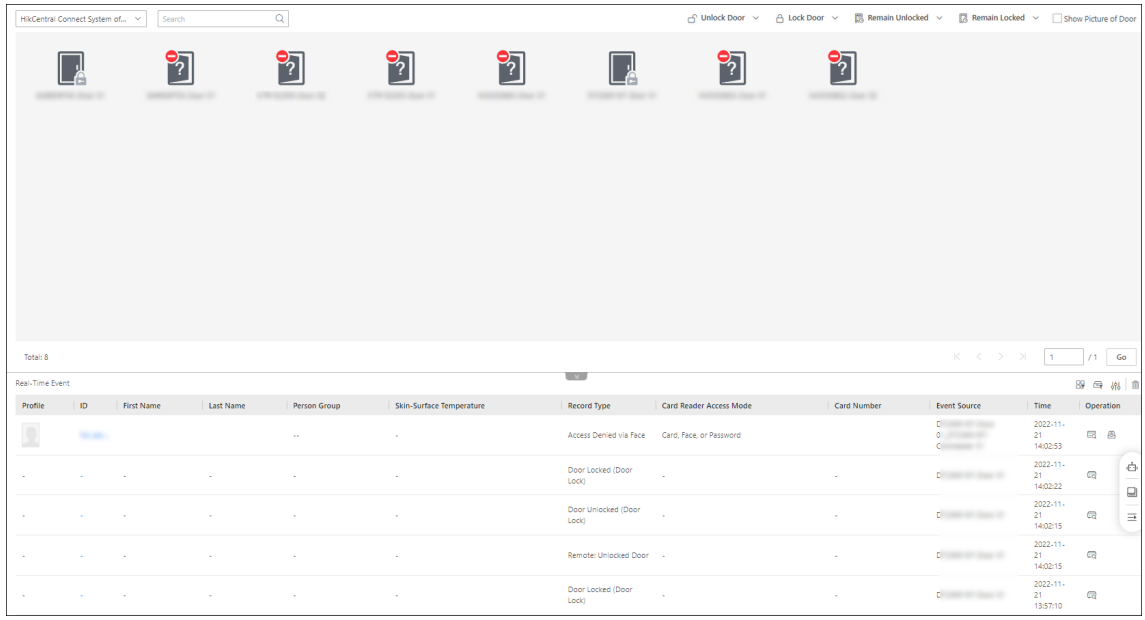


Figure 3-2 Real-Time Monitoring

Select the area of which you want to view the access events. Real-time access events are displayed at the bottom of the page. You can perform operations as needed.

Filter Events	You can filter the real-time events by setting the event types and event sources. Click and respectively to set conditions.
Customize Columns to be Displayed	Click to customize the columns to be displayed in the event list.
Clear Events	Click to clear all events in the list.
View Related Video	For doors with linked cameras, you can click in the Operation column to view the event-related video.
Search for Records/ Data	Click and respectively in the Operation column to go to the Access Record Retrieval page and Device Recorded Data Retrieval page to search records/data by conditions.
Archive Events	Click in the Operation column to archive the event.
View Event Details	In the lower-right corner of the page, click to expand the event details if it is collapsed. You can view the person information contained in the access records. You can check **Auto-Switch to the Latest Record** to view the person information contained in the latest access record.

3.4.2 Control Door

There are four kinds of door status: locked, unlocked, remaining locked, and remaining unlocked. You can control the status of a single door or doors in a batch.

Note

Make sure you have added doors to areas and they are online.

Go to the real-time monitoring page by either of the following entrances:

Click → **Access Control** → **Access Control** .

Select an area from the area list in the upper-right corner and control online doors in the selected area.

Unlock Door(s)	**Note** The door will be unlocked only for a specific period and be locked again automatically. • Click on a door card and click **Unlock Door**. • Select one or multiple doors and click **Unlock Door**. • Hover your mouse over beside **Unlock Door** and click **Unlock All** to unlock all doors.
Lock Door(s)	**Note** When the door is locked, person who has the access permission can access the door with credentials. • Click on a door card and click **Lock Door**. • Select one or multiple doors and click **Lock Door**. • Hover your mouse over beside **Lock Door** and click **Lock All** to lock all doors.
Remain Door(s) Unlocked	**Note** This function is used when an emergency occurs and all persons are required to leave as quickly as possible, such as in a fire escape. All persons can access the door with no credentials required (free access). • Click on a door card and click **Remain Unlocked**. • Select one or multiple doors and click **Remain Unlocked**. • Hover your mouse over beside **Remain Unlocked** and click **Remain All Doors Unlocked** to remain all doors unlocked.

Remain Door(s) Locked	**Note** This function is applicable for situations such as preventing a theft in the building from getting away. Only the super users can access the door. • Click on a door card and click **Remain Locked**. • Select one or multiple doors and click **Remain Locked**. • Hover your mouse over beside **Remain Locked** and click **Remain All Doors Locked** to remain all doors locked.
Live View	For doors with built-in and/or linked cameras, starting live view is supported. Click on a door card and click **Live View** to start live view and perform operations, including capturing pictures, recording videos, and starting two-way audio.
View Alarm/Event Details	For doors with triggered alarms/events, viewing alarm/event details is supported. Click on a door card and click **Alarm Details** to view alarm/event details.

3.5 How to retrieve access control records?

For the access records, triggered events/alarms, and card-swiping records, etc, that are uploaded to the System or stored on devices, you can set the search conditions to get the matched record list and export them to your local PC.

Search for Access Records

You can search for access records (that are uploaded to the System or imported from devices) by conditions, including time, persons, doors, event types, authentication result, skin-surface temperature status, and wearing mask or not.

1. On the top navigation bar, click → **Access Control** → **Search** → **Access Record Retrieval** .
2. Import access records from devices to the System.
   a. Click **Import Events**.
   b. Select the devices from the list, specify time range, and click **OK**,
3. Specify time, range, person, door, and other parameters and click **Search** to find the records.
4. After the results are found, click a person name to view the record details. You can also click or **Export** to export a record or all records to your PC.

Search for Data Recorded on Device

You can search for data recorded on devices, including triggered events/alarms and access records, by specifying the time, doors, devices, and alarm inputs.
On the top navigation bar, click → **Access Control → Search → Device Recorded Data Retrieval** .
Set conditions including time, doors, devices, and alarm inputs, and click **Search**.
After the results are found, click a person name to view the record details. You can also click or **Export** to export a record or all records to your PC.

3.6 How to set remain unlocked and remain locked rule?

To set access points accessible or inaccessible during certain periods, configure this rule for certain access points.

1. Go to → **Access Control → Application → Remain Unlocked & Remain Locked** .
2. Click **Configure Now** or **Add** to enter the Add Remain Unlocked & Remain Locked Rule page.
3. Enter the rule name.
4. Select an access point from the following group list.
5. Select weekly schedule for the access point(s).
6. Click **Add**.
   The system will automatically apply the schedule(s) to devices.

3.7 How to set access control parameters?

3.7.1 Set Holidays

On the top navigation bar, click → **Access Control → Access Control Configuration → Holiday Settings** .

Regular Holiday

The regular holiday is suitable for the holiday that has a fixed date. For example, Christmas is on December 25th of each year.

Irregular Holiday

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.

Start Date

Take the irregular holiday as an example, select **May**, **Second**, and **Sunday** for Mother's Day.

Number of Days

The lasting days of the holiday.

Repeat Annually

If you check **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year's calendar of the SYS server.

Note

For example, Mother's Day in 2019 and 2020 is on May 12th, 2019, and on May 10th, 2020. The system will automatically set these two days as holidays for Mother's Day if you have checked **Repeat Annually**.

3.7.2 Set Access Schedule Template

Access schedule defines when persons can open access points in an access level with credentials, or when access points remain unlocked so that persons can open the access points with free access. The system provides the All-day Template as a default access control schedule templates. You can also add customized templates according to your needs.

1. On the top navigation bar, click → **Access Control → Access Control Configuration → Access Schedule Template** .
2. Click + to create a blank template.
3. Create a name for the template, and optionally, you can copy the settings from existing templates.
4. In the **Weekly Schedule Template** box, set a schedule pattern for each day.
   - Click **Authorize** and select or draw in the box to define the authorized time periods.
   - Click **Erase** and select or draw on the authorized time periods to clear the selection.

   Note

   You can set up to 3 separate time periods for each day.
5. Set a holiday schedule if you want different schedules for specific days.

   Note

   Holiday schedule has a higher priority than weekly schedule.
6. Click **Add** to save the template.

3.7.3 Set General Parameters

On the top navigation bar, click → **Access Control → Access Control Configuration → General** .

- Select QR code mode as static or dynamic. To ensure security of access control devices, supports setting dynamic QR codes for temporary passes. The differences between static QR codes and dynamic QR codes are:

Table 3-4 Differences Between Static and Dynamic QR Codes

Comparison Items	Static QR Code	Dynamic QR Code
Form	QR Code	A link that contains a QR code that is automatically refreshed every minute.
Validity	For residents and employees: valid as long as the person is authorized. For temporary passes: up to 7 days.	
Allowed Passes	For residents and employees: as long as the person is authorized. For temporary passes: up to 200 times.	For residents and employees: as long as the person is authorized, but up to 60 times per minute. For temporary passes: up to 200 times.

- You can enable access records synchronization to system regularly. In this way, access records stored in devices can be synchronized to the system for central management. You can specify a fixed time in order to automatically synchronize access records from devices to the system at the specified time every day.

3.7.4 Subscribe to Device and Access Events

You can subscribe to device events and access events, so that when these events occur, you can see the real-time event records via the Portal and Mobile Client.

1. On the top navigation bar, click → **Access Control → Access Control Configuration → Event Notification** .
2. On the top of the page, select an event category from **Device Event**, **Normal Access Event**, and **Abnormal Access Event**.
3. Switch on the event types to subscribe to these events.
4. Switch off the event types whose real-time event records you do not want to receive.

Note

If you switch off an event type, the Web Client and Mobile Client will no longer receive real-time event records of the event. However, you can still search for the device/access records via the Web Client.

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

3.8 How to set alarms for access control devices?

Refer to ***Alarms*** for details.

Chapter 4 Elevator Control

4.1 Example Scenario

1. ***Get an Elevator Control License***
   - The platform offers elevator control license packages, charged based on the number of elevator controller, with options for monthly, yearly, etc.
   - **Example:** You can contact your service provider to purchase a license or activate a license on the Portal to get the service.
2. ***Add Elevator Control Devices***
   - **Before You Begin:** Ensure the elevator controller is powered on, connected to the network, activated, and online on the cloud.
   - **Example:** On the Portal, you can add the elevator controller DS-K2220X to integrate with access control for enhanced security. Use QR code scanning, serial number entry, SADP discovery, or Excel batch import.
   - Path: ⁞⁞ → **Device → Add**
3. ***Control Elevator Floor Access***
   - This feature controls whether a floor can be selected and accessed, not the physical movement of the elevator car itself. You can issue four types of control commands to specific floors.
   - **Example:** Use Temporary Access to unlock a floor once, Access with Credential to lock it down, Free Access to keep it permanently open, or Access Forbidden to keep it permanently locked.
   - Path: ⁞⁞ → **Access Control → Access Control**
4. ***Grant Floor Access Permissions to Persons***
   - This article guides you on how to grant floor access permissions, extending traditional door access control to elevator control within a building. This feature allows administrators to assign access permissions based on floors, enhancing both security and operational efficiency.
   - **Example:** Add an access level to assign permissions by floor alongside the existing door-based method. Grant access by person, department, or temporary credential.
   - Path: ⁞⁞ → **Access Control → Access Granting → Manage Access Level**
5. ***Set Elevator Control Events***
   - On the Portal, you can configure alarm rules based on elevator control events, view real-time and historical events, and export records for enhanced security monitoring.
   - **Example:** Click Add to add an alarm rule for elevator control events.
   - Path: ⁞⁞ → **Alarm → General Alarm Configuration**

4.2 How to get an elevator control license?

The platform offers elevator control license packages, charged based on the number of elevator controller, with options for monthly, yearly, etc.

You can contact your service provider to purchase a license or activate a license on the Portal to get the service.

Note

On the Portal, elevator control features are now available only when both access control and elevator control services are enabled, with permissions managed similarly to access control.

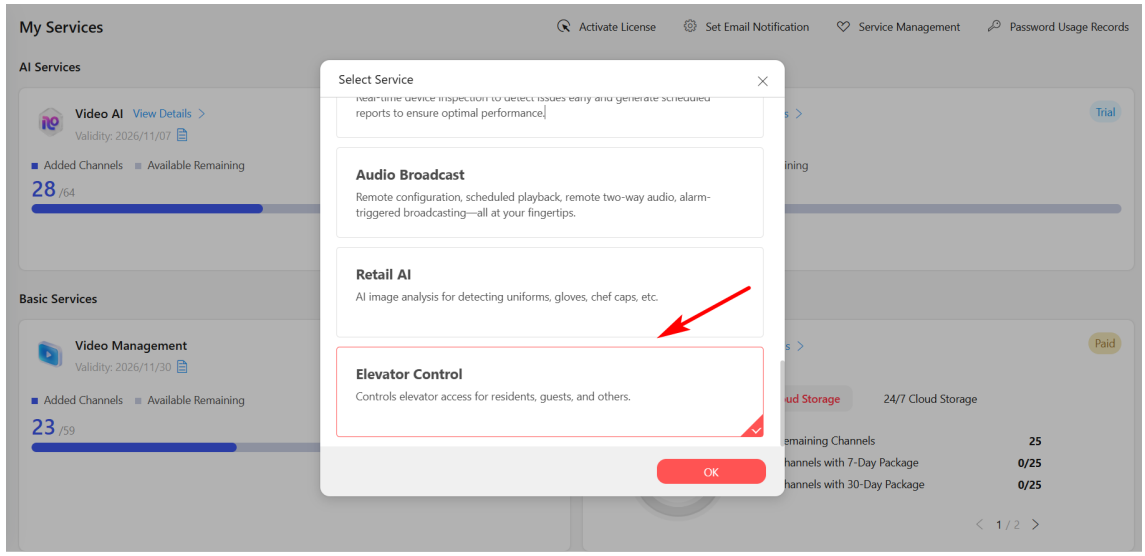


Figure 4-1 Elevator Control Service

4.3 How to add elevator control devices?

Before You Begin: Ensure the elevator controller is powered on, connected to the network, activated, and online on the cloud.

On the Portal, you can add the elevator controller DS-K2220X to integrate with access control for enhanced security.

How to add elevator devices?

1. Go to → **Device** → **Add** .
2. you can add the elevator controller DS-K2220X.
   - **QR Code Scanning (App):** Use the App to scan the QR code on the device or its configuration interface.
   - **Serial Number:** Manually enter the device's serial number on the Web Portal or App.

- **Device Discovery (SADP):** Ensure your phone/PC is on the same LAN as the device to automatically discover and add it via the SADP protocol.
- **Excel Batch Import (Portal):** Download the import template and fill in the device information. The template requires specifying a floor range (Min Floor and Max Floor columns). The range is limited to 1-128, and the minimum floor value must be less than the maximum.

3. The system will prompt you to specify the number of floors. The default range is 1-16, which you can modify based on the actual elevator.
4. After the devices are added, click **Elevator Control Device** to view the devices.

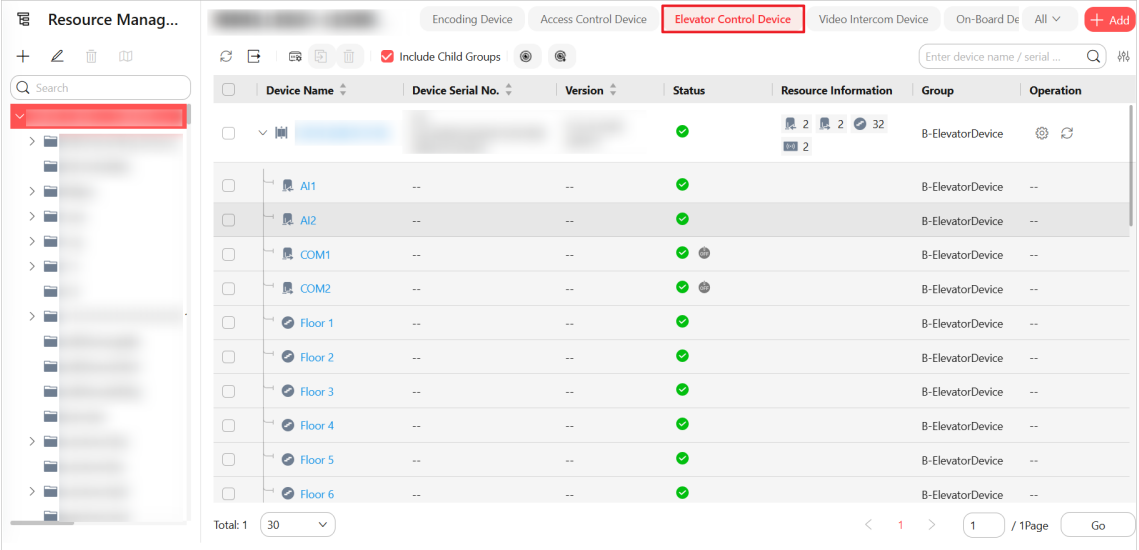


Figure 4-2 Elevator Control Device List

How to set basic parameters?

Tap the name of a elevator control device, and perform the following operations:

- **Extended Open Duration**: Configure the delay for the elevator door to remain open or allow button presses after a card swipe.
- **Reset Floor Range**: Re-specify the floor number range.
- **Edit/Apply Floor Names**: Get floor names from the device or edit and apply names to it.

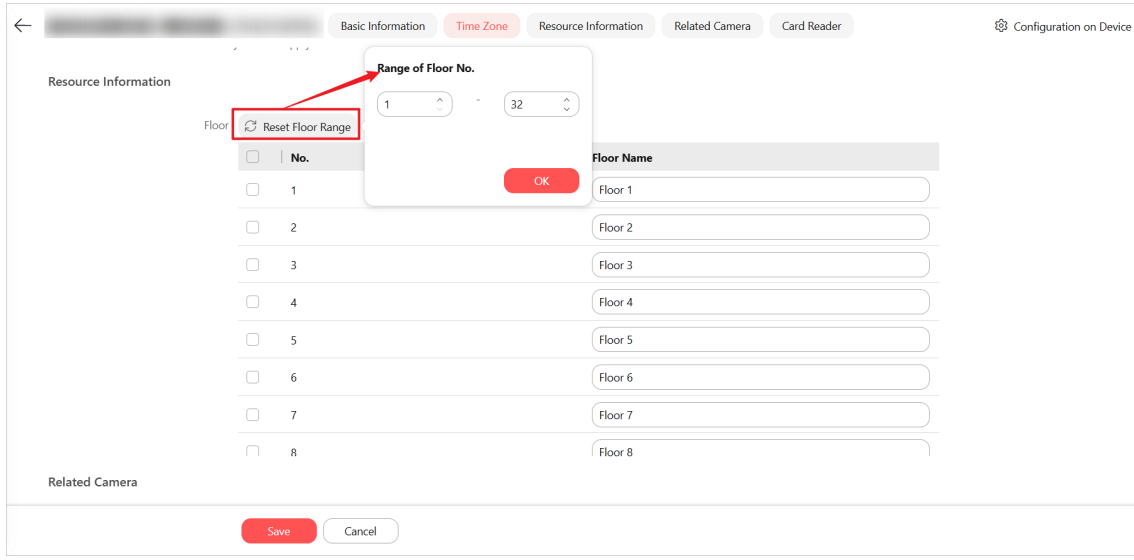


Figure 4-3 Link Floor

- **Linked Cameras**: Link cameras to the elevator, up to a maximum of 2 channels.

  Note

  The linking is automatically removed if the elevator or the camera is deleted.

- **Device Parameters**:
  - **M1 Card Encryption:** Set the encryption key and authentication mode for M1 cards.
  - **RS-485 Settings (Downstream Backup):** Configure RS-485 communication parameters for connecting downstream devices (e.g., card reader expansion modules).

4.4 How to control elevator floor access?

The Elevator Floor Control feature allows authorized administrators or users to remotely manage access permissions for individual floors within an elevator car via the Portal.

Overview

This feature controls **whether a floor can be selected and accessed**, not the physical movement of the elevator car itself. You can issue four types of control commands to specific floors to meet different access management needs. Additionally, you can view the live video feed from the elevator's linked camera directly on the control page for visual verification.

How to control a floor in real-time?

1. Log in to the Portal and navigate to → **Access Control** → **Access Control** .
2. In the device card list, locate and click the elevator you wish to control.
3. Click **>** next to the target floor.

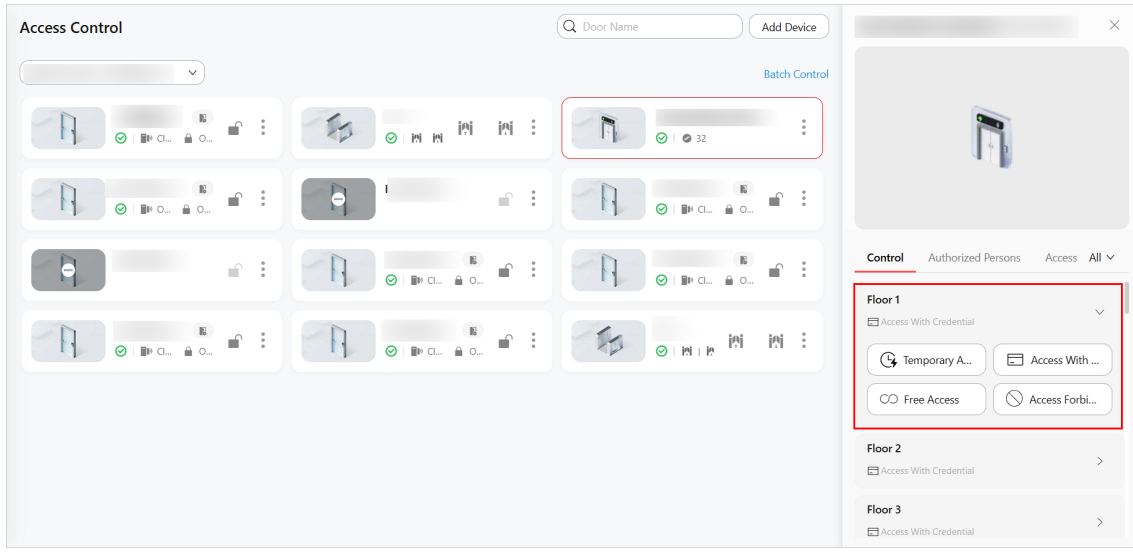


Figure 4-4 Control Elevators

4. From the pop-up menu, select the desired command:

Command	Door Access Equivalent	Behavior Description
Temporary Access	Unlock	Unlocks the floor once, allowing a user to select and access it after swiping a card. After this one-time use, the floor reverts to its previous state.
Access with Credential	Lock	Locks the floor down. Regular users cannot select or access this floor by swiping their cards, except for those with special privileges.
Free Access	Always Open	Keeps the floor in a permanently unlocked state. All users can select and access the floor without needing to swipe a card.
Access Forbidden	Always Closed	Keeps the floor in a permanently locked state. No card can be used to select or access this floor.

5. The system will execute the command and update the floor status in real time.

How to view the linked camera video?

1. On the **Access Control** page, click an elevator device.
2. The live feed from the associated camera will automatically play in a video panel on the right side of the page or in a pop-up window.
3. You can use any features supported by the camera, such as PTZ control, snapshot, and recording.

4.5 How to grant floor access permissions to persons?

This article guides you on how to grant floor access permissions, extending traditional door access control to elevator control within a building. This feature allows administrators to assign access permissions based on floors, enhancing both security and operational efficiency

4.5.1 How to add an access level?

This is the core module for permission assignment, where you can assign permissions by floor alongside the existing door-based method.

1. Navigate to ⁝⁝ → **Access Control** → **Access Granting** → **Manage Access Level** .
2. Define a name for the access level.
3. In the Access Point section, you will see a filter for the **Elevators** type. Select it to display elevator devices and their linked floors.
4. Check the box next to one or more floors you wish to grant access. You can select both **Door** devices and **Elevator Control** floors simultaneously to create a mixed permission set.
5. Complete other configurations, such as the access schedule, and click **Add**.

4.5.2 How to grant access by person, department, or temporary credential?

Grant by Person

1. Navigate to ⁝⁝ → **Access Control** → **Access Granting** → **Grant by Person** .
2. Locate the target person and click **Grant Access**.
3. In the pop-up window, you can add or remove floor permissions for this person.
4. (Optional) Click **Revoke** to revoke granted floor permissions.

Grant by Department

1. Navigate to ⁝⁝ → **Access Control** → **Access Granting** → **Grant by Department** .
2. You can view a summary of floor permissions for all members of a specific department.
3. Use the **Batch Grant Access** feature to uniformly add or modify floor access for an entire department.

Temporary Credentials

1. Go to ⁞⁞ → **Access Control** → **Temporary Pass Management** .
2. When creating or editing a temporary access credential, you can also assign floor permissions for visitors or temporary staff.

4.5.3 How to view the overview access?

View by Person

1. Navigate to ⁞⁞ → **Access Control** → **Access Granting** → **Overview** and select the **Person** view.
2. Search for a specific person. Their detail panel will show associated door and floor permissions.
3. You can view the deployment status of each floor permission, such as invalid, effective, or not granted. If an applying task fails, specific error details and an error code will be displayed to help you troubleshoot.

View by Device

1. Switch to the **Device** view.
2. Select a specific elevator device. The system will display all personnel permissions deployed to that device, including the authorized floors for each person.

4.6 How to grant elevator control module to a team member?

Note

The feature is only supported if you are an admin user.

1. Go to ⁞⁞ → **Team** → **User Management**
2. In the Permission section, you can grant the permission of the elevator control module to users, and the permissions are the same as the access control module.

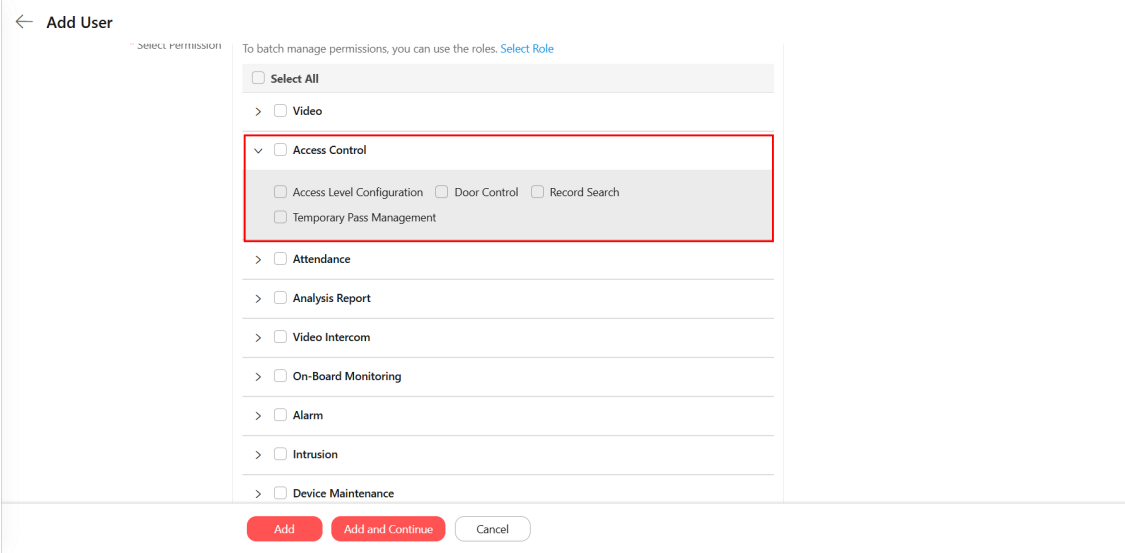


Figure 4-5 Elevator Control Permission

4.7 How to set elevator control events?

On the Portal, you can configure alarm rules based on elevator control events, view real-time and historical events, and export records for enhanced security monitoring.

1. Go to → **Alarm → General Alarm Configuration** .
2. Click **Add** to add an alarm rule.

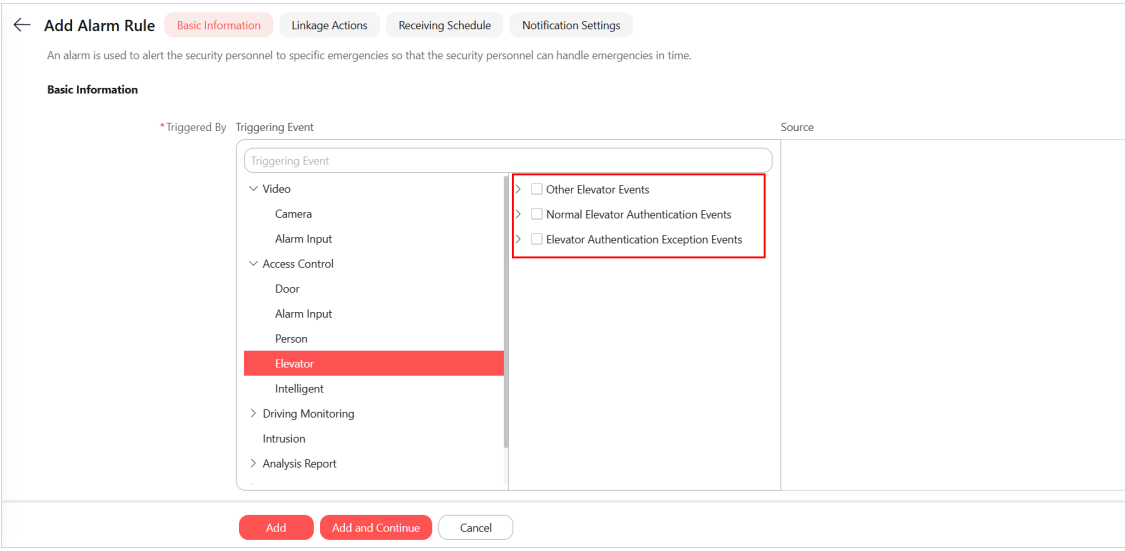


Figure 4-6 Elevator Control Events

Chapter 5 Time & Attendance

Time & attendance is a management system that tracks employees' working hours and attendance. It ensures accurate recording of hours and effective management of leave and overtime. By automating these processes, it reduces administrative burdens and minimizes errors. Commonly used in offices, factories, and retail stores, this system improves payroll accuracy, workforce productivity, and HR management. Employees typically clock in and out through the mobile client, while managers can access detailed reports for analysis and decision-making on both the Portal and Mobile Client.

5.1 Example Scenario

This guide provides a step-by-step configuration process for setting up a comprehensive attendance system in a large company that includes fixed shifts (e.g., for Administration and Finance), flexible shifts (e.g., for Research and Development or Design), and shift-based systems (e.g., for Production or Customer Service). It also covers additional features such as holiday and leave type setup, leave applications and approvals, and report generation. The table below outlines the configuration steps in logical order, with references to the corresponding concepts and menu paths for easy navigation.

1. ***Add Access Control Devices***
   - Install and configure physical hardware such as door controllers, readers, and biometric devices. Ensure they are connected to the network and integrated with the software.
   - **Example:** For a large tech company, deploy facial recognition devices at main entrances for high-security areas and card readers at internal doors for general access. Use IP-based controllers to support remote management.
   - Path: ⁞⁞ **→ Device → Access Control Device**
2. ***Add Employees to the System***
   - Create employee accounts in the Person module, either manually or by importing from Team Management. Assign each employee to a specific department (e.g., Administration, Finance, Research and Development, Production, Customer Service) to align with attendance policies. Add credentials like faces, cards, or PINs for access control.
   - **Example:** For a tech company, add employees such as John Doe to the Research and Development department with flexible shift options, and Jane Smith to the Administration department with fixed shifts. Ensure credentials are set for both physical and mobile access.
   - Path:
     - ⁞⁞ **→ Person → Add**
     - ⁞⁞ **→ Team → User Management**
3. ***Configure Shift Types***

- Set up shift types by selecting normal and/or flexible shift. This determines the attendance method for employees based on their roles and department requirements.
- **Example:** For a tech company, configure fixed shifts for Administration and Finance departments with standard hours (e.g., 9 AM to 6 PM), and flexible shifts for Research and Development allowing employees to work within a range (e.g., 7 AM to 10 PM) while meeting daily hour targets.
- Path: ⁞⁞ → **Attendance → Basic Configuration → General**

4. ***Define Weekends***
   - Specify the days considered as weekends for the company. Attendance on these days is typically excluded from regular calculations or treated as special shifts.
   - **Example:** Set weekends to Saturday and Sunday for all departments.
   - Path: ⁞⁞ → **Attendance → Basic Configuration → General → Weekend**
5. ***Configure Overtime Rules***
   - Define overtime policies, including when overtime starts, calculation methods (e.g., daily or weekly), approval workflows, and compensation rates.
   - **Example:** For fixed shifts, enable Count early check-ins and late check-outs as overtime; For flexible shifts, calculate overtime based on daily excess hours beyond 30 minutes.
   - Path: ⁞⁞ → **Attendance → Basic Configuration → General → Overtime**
6. ***Establish Attendance Rules***
   - Define attendance rules, including tolerance times for late arrivals and early departures, absence thresholds, and grace periods. Set reasonable limits to accommodate real-world scenarios without compromising accountability.
   - **Example:** Implement a 15-minute tolerance for late arrivals and a 10-minute tolerance for early departures. Mark an employee as absent if they arrive more than 30 minutes late or leave more than 30 minutes early without approval. For flexible shifts, allow a 5-minute grace period for check-in variations.
   - Path: ⁞⁞ → **Attendance → Basic Configuration → General → Attendance Rule**
7. ***Set Attendance Check Points***
   - Set all devices as attendance check points or select certain devices as attendance check points.
   - **Example:** Set device A as check point, and only check-ins/outs on device A are count as attendance records.
   - Path: ⁞⁞ → **Attendance → Basic Configuration → Attendance Check Point**
8. ***Set Up Mobile Client Check-In/Out***
   - Enable mobile check-in/out for employees, with options to require photo uploads and define valid check-in areas using GPS.
   - **Example:** Allow mobile check-in for Research and Development staff with GPS restrictions within the office campus. Require photo verification for remote workers to prevent fraud.
   - Path: ⁞⁞ → **Attendance → Basic Configuration → General → Check In/Out via Mobile Client**
9. ***Define Timetables for Each Shift Type***

- Create detailed timetables for each shift type, specifying work periods, break times, and overtime rules. Ensure timetables align with department needs.
- **Example:** For Production shifts, set a 12-hour timetable with two 30-minute breaks. For Research and Development flexible shifts, define a core period from 10 AM to 4 PM with flexible start and end times.
- Path: ⁞⁞ → **Attendance → Basic Configuration → General → Timetable**

10. ***Configure Holidays***
    - Set company holidays to exclude them from attendance calculations. Include both national and company-specific holidays.
    - **Example:** Add standard holidays like New Year's Day and company-specific days such as Foundation Day. Ensure holidays are applied uniformly across all departments.
    - Path: ⁞⁞ → **Attendance → Basic Configuration → General → Holiday**
11. ***Set Leave Types***
    - Define leave types such as sick leave, vacation, and personal leave, with approval workflows.
    - Path: ⁞⁞ → **Attendance → Basic Configuration → General → Leave Type**
12. ***Assign Schedules to Employees***
    - Assign work schedules to individuals or groups, with options for repetition and specific time periods. Ensure schedules match department requirements.
    - **Example:** Assign fixed shifts to Customer Service teams from 8 AM to 5 PM, and flexible shifts to Research and Development employees with weekly hour targets. Use bulk assignment for departments like Production.
    - Path: ⁞⁞ → **Attendance → Schedule**
13. ***Configure Application Management***
    - Set up processes for submitting and reviewing leave and attendance correction applications. Enable notifications and approvals based on roles.
    - **Example:** Configure leave applications for Research and Development staff to be approved by project managers, and attendance corrections by team leads. Use automated reminders for pending requests.
    - Path: ⁞⁞ → **Attendance → Review**
14. ***View Attendance Records***
    - Access and review attendance data captured through different sources, including device transactions, mobile submissions, and consolidated time card summaries.
    - Path: ⁞⁞ → **Attendance → Attendance Records**
15. ***Set Up Reports***
    - Configure and export attendance reports for daily, monthly, or custom periods, with filters for departments or individuals.
    - **Example:** Generate monthly reports for HR, highlighting trends in Research and Development flexible attendance. Export data for payroll integration, with filters for specific departments like Finance.
    - Path: ⁞⁞ → **Attendance → Report**

5.2 How to add access control devices?

Refer to ***Device Management*** .

5.3 How to add employees?

The System provides two ways of adding employees.

1. - One is to ***add users*** in ⁞⁞ → **Team** to automatically generate persons in the Person module.
   - The other is to go to ⁞⁞ → **Person** → **Add** to add persons.
2. Fill in the basic information, and click **Credential Management** to add credentials for the person to open doors.

Table 5-1 Add Credentials For Persons to Open Doors

Credentials	Descriptions
Face	Hover on the blank profile picture to select a method of adding faces.
Card	Click **Configuration**, and select a card issuing mode.
Bluetooth/NFC	Opening doors via Bluetooth or NFC is dependent on the phone app use, so you need to create an app account for the person first to allow them to open doors via Bluetooth/NFC on the phone.
Fingerprint	Click **Configuration**, and select a fingerprint collection mode.
PIN	Create a PIN, and the PIN can be used to open doors.

3. Set required parameters.

Table 5-2 Set Attendance Parameters

Parameter	Descriptions
Check In/Out via Mobile Client	Enable it so the person will be allowed to check in/out via the mobile client.
Must Upload Picture	Check **Must Upload Picture**, and a picture will be required when the person check in/out via the mobile client.
Role	Select **Supervisor** or **Employee**. A supervisor has the permission to approve applications of the department and its sub-departments, and can check the employees' attendance on the Mobile Client.
Schedule	Go to ⁞⁞ → **Attendance** → **Schedule** to schedule shifts.

5.4 How to configure attendance settings?

Table 5-3 Attendance Configuration

Type	Description
Set Shift Type	The platform provides two shift types: normal shift and flexible shift. For entering the Attendance module for the first time, you should select at least one shift type. Normal Shift: The check in/out time is fixed according to the set work period (e.g., between 9 AM and 6 PM). Checking in/out outside the required time period (e.g., after 9 AM or before 6 PM) will be regarded as late or early leave. Flexible Shift: The check in/out time is flexible, while the work hours are fixed. I.e., there are no limitations on the specific check in/out time, but the total work hours should meet the time requirement (e.g., 8 hours). Go to → **Attendance → Basic Configuration → General** to select and edit the shift type.
Define Weekend	The days of a weekend may vary in different countries and regions. With the weekend definition feature, you can select one or more days as the weekend as you need. On the top navigation bar, click → **Attendance → Basic Configuration → General → Weekend** to define weekend.
Define Overtime	Overtime is the amount of time a person works beyond the scheduled work hours. You can configure overtime parameters for the normal shift, flexible shift, and weekend. On the top navigation bar, click → **Attendance → Basic Configuration → General → Overtime** .
Set Attendance Rule	On the top navigation bar, click → **Attendance → Basic Configuration → General → Attendance Rule** . **Mark as Late if Checks In Late For** If the rule is enabled and an employee checks in later than the valid check-in time for a time longer than the set tolerance time, the employee's attendance result will be marked as **Late**. The value you set for this rule should be less than that for marking late check-in as **Absent**. **Mark as Absent if Checks In Late For**

Type	Description
	If the rule is enabled and an employee checks in later than the valid check-in time for a time longer than the set tolerance time, the employee's attendance result will be marked as **Absent**. The value you set for this rule should be greater than that for marking late check-in as **Late**. **Mark as Early Leave if Checks Out Early For** If the rule is enabled and an employee checks out earlier than the valid check-out time for a time longer than the set tolerance time, the employee's attendance result will be marked as **Early Leave**. The value you set for this rule should be less than that for marking early check-out as **Absent**. **Mark as Absent if Checks Out Early For** • If **Absent** is selected, the attendance result of an employee will be marked as **Absent** if no check-in record is found for that person for the day. • If **Late** is selected, you can set the late duration to be recorded in minutes. The attendance result of an employee will be marked as **Late** if no check-in record is found for that person for the day, and the employee is late for the set late duration. **Mark Attendance Without Check-Out As** • If **Absent** is selected, the attendance result of an employee will be marked as **Absent** if no check-out record is found for that person for the day. • If **Early Leave** is selected, you can set the early leave duration to be recorded in minutes. The attendance result of an employee will be marked as **Early Leave** if no check-out record is found for that person for the day, and the employee leaves early for the set early leave duration.
Enable Custom Check Point	On the top navigation bar, click → **Attendance → Basic Configuration → Attendance Check Point** . You can designate specific access points for attendance tracking. Only punches at selected devices count toward attendance calculations.
Check In/Out via Mobile Client	On the top navigation bar, click → **Attendance → Basic Configuration → General → Check In/Out via Mobile Client** . Click **Add** to enable certain employees for checking in/out via mobile client.

Type	Description
	Enable **Must Upload Picture**, and employees must check in/out with a picture uploaded. (Optional) Check **Enable Check-In/Out Area** to add an area where checking in is valid for specified employees.
Set Timetable	The timetable defines the detailed time rules for attendance, such as work time and break time. You can add a timetable for normal or flexible shift. On the top navigation bar, click → **Attendance → Basic Configuration → General → Timetable** .
Set Holiday	On the top navigation bar, click → **Attendance → Basic Configuration → General → Holiday** .
Set Leave Type	On the top navigation bar, click → **Attendance → Basic Configuration → General → Leave Type** .

5.5 How to assign schedules to employees?

On the Schedule Overview page, you can assign a work period to a single person or multiple persons in a batch.

1. Select → **Attendance → Schedule** .
2. Hover the cursor over a box of a person and click to open the Schedule pane.
3. (Optional) Select a shift type if the two shift types are configured.
4. Select a work period, or click **Add** to add one.
5. In the Time field, select a time period during which the schedule works.
6. (Optional) Enable **Repeat** to open the Set Repetition Parameters window and set related parameters.
   On the Set Repetition Parameters window, users can select a work period's repetition mode and repetition interval (with examples provided), define on which day(s) the work period repeats, and select the start and end date of the repetition.
7. Click **Save**.

5.6 How to submit applications?

On the Portal, administrators can check the details of all applications of the departments which they have the permission to manage, submit leave applications and attendance correction applications for employees upon requests when the employees are unable to do so themselves,

and help supervisors to review applications when the supervisors are too busy to deal with the applications.

Table 5-4 Submit Applications

Type	Description
Submit Leave Application	On the Portal, the administrator can submit a leave application for an employee upon the employee's request. On the top navigation bar, click ⁞⁞ → **Attendance** → **Review** → **Leave** .
Submit Attendance Correction Application	On the Portal, the administrator can submit an attendance correction application for an employee upon the employee's request. On the top navigation bar, click ⁞⁞ → **Attendance** → **Review** → **Attendance Correction** .

5.7 How to review applications?

As the administrator of your company, you can view the status and application flow of all applications of the departments which you have the permission to manage, approve/reject applications upon the request of supervisors when they do not have the time to do so themselves, and withdraw applications for the employees to edit and submit again.

On the top navigation bar, click ⁞⁞ → **Attendance** → **Review** and select an application type from **Leave** and **Attendance Correction** to enter the corresponding page. You can perform the following operations:

Table 5-5 Available Operations

Operation	Description
View Application Flow	Click an application to view its application flow on the right, which displays information such as the current status, the person involved in each phase, the specific time the application is submitted/ reviewed, etc.
View and Download Attachments	If there are attachments submitted along with an application, you can click **View** in the Attachment column of the application to view them in a pop-up window. While viewing the attachments, you can click **Download Now** to download each of them to your local PC as needed.

Operation	Description
Approve Application	• Click in the Operation column of an application, enter your comments (optional), and click **Approve** to approve it. • Select one or multiple applications, click **Approve** at the top, enter your comments (optional), and click **Approve** to batch approve them. **Note** Only applications in the Under Review status can be approved.
Reject Application	• Click in the Operation column of an application, enter your comments (optional), and click **Reject** to reject it. • Select one or multiple applications, click **Reject** at the top, enter your comments (optional), and click **Reject** to batch reject them. **Note** Only applications in the Under Review status can be rejected.
Withdraw Application	• Click in the Operation column of an application to withdraw it. • Select one or multiple applications and click **Withdraw** at the top to batch withdraw them. **Note** The application that is withdrawn can be edited and resubmitted by the applicant on the Mobile Client.

5.8 How to view attendance records?

Access and review attendance data captured through different sources, including device transactions, mobile submissions, and consolidated time card summaries.

Attendance Record Types

The system maintains three distinct record types for tracking employee attendance:

- **Transaction** Raw clock events from physical access control devices (biometric scanners, card readers).
- **Mobile Transaction** Clock events submitted via the mobile application with verification data (GPS location, photos).
- **Time Card** Processed attendance summaries calculating work hours, breaks, and exceptions for payroll and reporting.

Access Device Transaction Records

View clock events captured by physical attendance terminals:

1. Navigate to ⁝⁝ → **Attendance** → **Attendance Records** → **Transaction** .
2. Filter records by date range, employee, or specific device.
3. Review individual clock events with timestamps and device identifiers.

Access Mobile Transaction Records

Review attendance data submitted through the mobile application:

1. Select ⁝⁝ → **Attendance** → **Attendance Records** → **Mobile Transaction** .
2. Apply filters by date, employee, or location data.
3. Examine mobile submissions including verification metadata.

Access Time Card Reports

Generate consolidated attendance summaries for reporting periods:

1. Go to ⁝⁝ → **Attendance** → **Time Card Report** .
2. Specify the reporting period and apply organizational filters.
3. Analyze calculated metrics including regular hours, overtime, and attendance exceptions.

Record Type Comparison

The following table contrasts the characteristics of each record type:

Record Type	Data	Primary Application
Transaction	Individual events.	Device audit trails, real-time monitoring, etc.
Mobile Transaction	Individual events with validation data.	Remote workforce management, flexible work tracking, etc.
Time Card	Aggregated period summaries.	Payroll integration, managerial reporting, compliance analysis, etc.

5.9 How to view and export reports?

The Attendance module provides 9 types of reports for you to view the attendance statistics and details from different dimensions. You can specify the conditions to filter the attendance records, customize the columns to be displayed on the reports, and export the reports to your local PC.

On the top navigation bar, click ⁝⁝ → **Attendance** → **Report** and select the report type as needed to enter its page.

You can specify the employee name, ID, department, and time period to filter the attendance records.

Table 5-6 Daily and Monthly Reports

Time	Type	Description
Daily Report	Total Time Card	Employees' daily attendance details are displayed, including the employee information, date, weekday, timetable, scheduled/actual work start/end time, attendance status, worked hours, absent duration, late duration, early leave duration, break duration, overtime duration, leave duration, weekend overtime duration, and workday overtime duration.
	Worked Hours	Employees' daily worked hours details are displayed, including the employee information, date, weekday, worked hours, absent duration, late duration, early leave duration, break duration, overtime duration, leave duration, weekend overtime duration, and workday overtime duration.
	Exception Report	Employees' records of exception attendance status are displayed, including the employee information, date, weekday, timetable, scheduled/actual work start/end time, and attendance status. Exception: Any attendance status other than normal or leave.
	Late Report	Employees' records of being late are displayed, including the employee information, date, weekday, timetable, scheduled/actual work start/end time, worked hours, and late duration.
	Early Leave Report	Employees' records of early leave are displayed, including the employee information, date, weekday, timetable, scheduled/actual work start/end time, worked hours, and early leave duration.
	Absent Report	Employees' records of being absent are displayed, including the employee information, date, weekday, timetable, scheduled/actual work start/end time, worked hours, and absent duration.
	Overtime Report	Employees' attendance records of overtime are displayed, including the employee information, date, weekday, weekend overtime duration, and workday overtime duration.
	Break Report	Detailed in/out timestamps and durations for employee breaks. You can filter data by department or date range, and export to Excel/PDF for analysis.

Time	Type	Description
Monthly Report	Monthly Status	Employees' attendance records of each day and their times of normal, absent, late, early leave, late and early leave, and leave.
	Monthly Worked Hours	Employees' attendance records of each day and their duration of working, absent, late, early leave, break, leave, overtime, weekend overtime, and workday overtime.
	Person Attendance	Employees' attendance records of each day and their times of normal, absent, late, early leave, late and early leave, and leave. Employees' duration of leave, overtime, weekend overtime, and workday overtime.
	Department Attendance	Records of times of normal, absent, late, early leave, late and early leave, and leave of employees from a department. Records of duration of leave, overtime, weekend overtime, and workday overtime of employees from a department.
	Attendance Overview	Employees' all detailed attendance records of each day and their times of normal, absent, late, early leave, late and early leave, and leave. Records of duration of leave, overtime, weekend overtime, and workday overtime of employees from a department.
	Attendance Status	Employees' attendance records of each day and their times of normal, absent, late, early leave, late and early leave, and leave. Records of duration of leave, overtime, weekend overtime, and workday overtime of employees from a department.
	Attendance Summary	Employees' attendance records of each day and their times of normal, absent, late, early leave, late and early leave, and leave. Records of duration of leave, overtime, weekend overtime, and workday overtime of employees from a department.

You can perform the following operations:

Table 5-7 Available Operations

Filter Records	Click in the upper-right corner, set conditions, and click **Filter** to view the matched records.
Enable/Disable Self-Adaptive Column Width	Click in the upper-right corner and select **Best Fit With Scale** or **Best Fit**.
Customize Columns to Be Displayed	Click in the upper-right corner and select the columns to be displayed as needed.
Export Reports	Click **Export** in the upper-left corner, select the format, and click **Export**. **Note** If you select **PDF**, you can also customize the print format, including the paper size and direction.
Recalculate Attendance	Click **Recalculate** on the top left to open the Recalculate pane. Set a time period and select the target person (all persons or specified persons), and then click **Recalculate** to correct attendance results of selected person(s) again. A green circle indicating the recalculation progress will appear after you start recalculating and you can hover the cursor over the circle to show a prompt about recalculating. Once finished, a prompt about recalculating completed will appear.
Send Scheduled Reports to Specified Email	Go to **Attendance → Basic Configuration → Scheduled Report** to add a schedule to regularly send a type of reports to a specified email.

Chapter 6 Video Intercom

This video intercom configuration guide is designed for property managers who need to set up a smart access and communication system in multi-building residential communities. It explains how to deploy video intercom devices, create building and room structures, register residents with face and other credential access, manage call history, and issue temporary visitor passes—all through a unified platform.

6.1 Example Scenario

Set up Intercom System

1. ***Add and Configure Video Intercom Devices***
   - Add Single Intercom Device: Activate and add devices to the system by configuring network parameters and entering serial numbers. Ensure devices are online and accessible.
   - Path: ⁞⁞ → **Device → Device → Video Intercom Device**
2. ***Add Communities (Optional), Buildings (Required), Units (Optional), and Rooms (Required)***
   - Create community structures and batch-add rooms, then link them to video intercom devices for access control.
   - Path: ⁞⁞ → **Video Intercom**
3. ***Add Residents***
   - Add residents by selecting from existing persons or creating new ones, upload face pictures, and assign them to rooms. Credentials like cards or fingerprints can be added for access.
   - Path: ⁞⁞ → **Video Intercom → Resident**

Intercom Applications

1. ***Manage Notices***
   - Add notices so property managers can send regular and emergency notices directly to the resident app.
   - Path: ⁞⁞ → **Video Intercom → Management Center → Notice Management**
2. ***View Call History***
   - Configure access to view and export call history, including missed and answered calls from video intercom devices.
   - Path: ⁞⁞ → **Video Intercom → Management Center → Call History**
3. ***Manage Call Managers***
   - Add a call manager and specify devices for them to manage. When a visitor/resident calls from a call manager's managed device, the call manager can receive and answer the call.
   - Path: ⁞⁞ → **Video Intercom → Management Center → Call Manager**
4. ***Configure Temporary Pass Management***

- Create temporary passes for visitors with QR codes or passwords, set validity periods, and track unlock records.
- Path: ⁞⁞ → **Video Intercom → Temporary Pass Management**

6.2 How to add and configure video intercom devices?

6.2.1 How to add a single intercom device?

Refer to ***Device Management*** .

6.2.2 How to batch import intercom devices in LAN?

Refer to ***Use the SADP Tool to Quick Initialize LAN Devices*** to batch add devices in LAN.

After adding the devices, refer to ***How to Hand Over Site & Devices to Your Customer*** to hand over the site to your account.

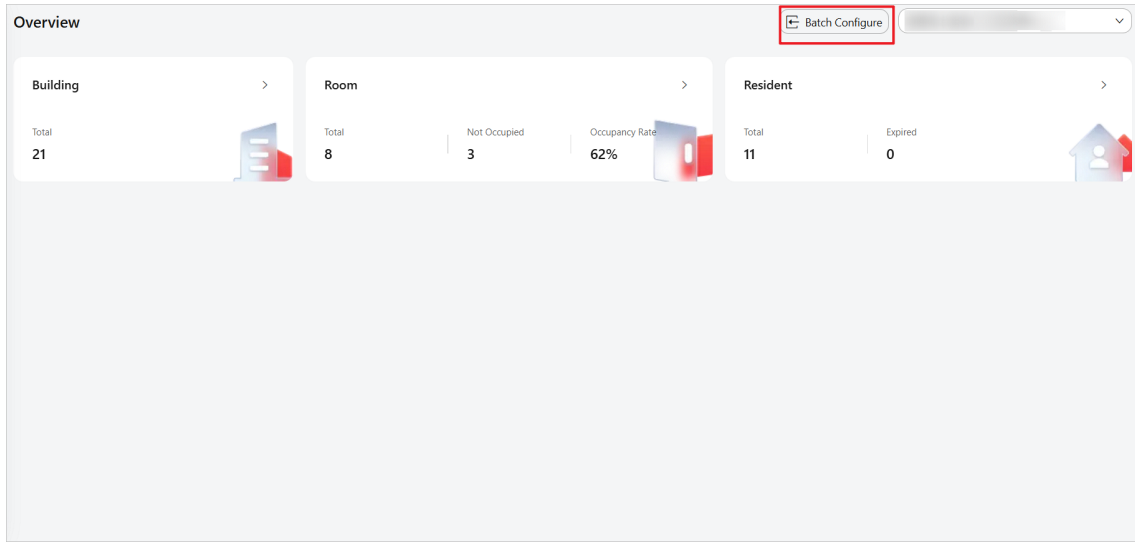
6.3 How to batch configure the intercom system?

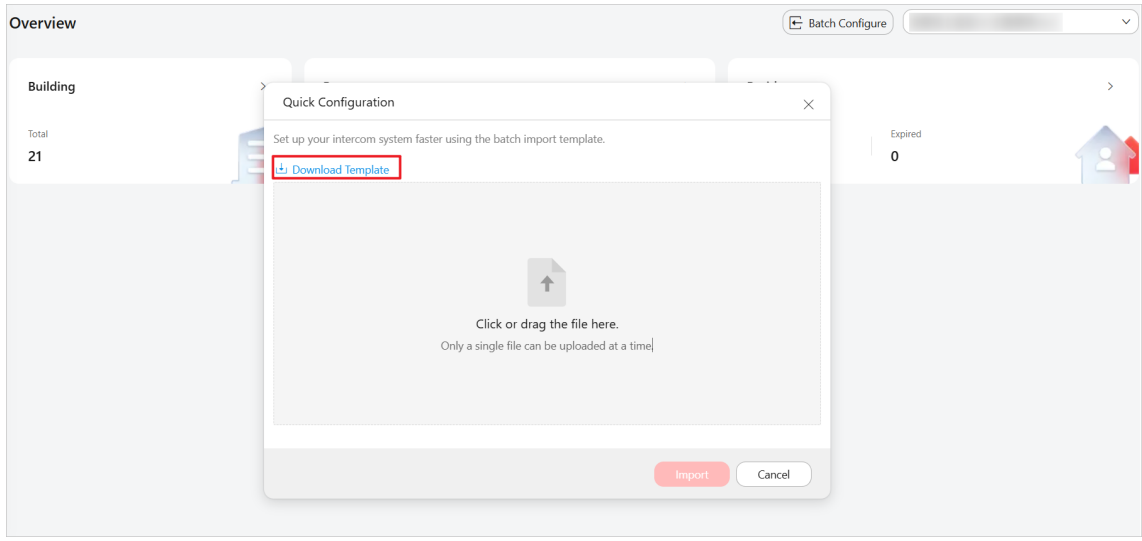
The Excel Batch Import feature in the HCT platform's Intercom module allows installers and project managers to configure devices, physical hierarchies (Community, Building, Unit, and Room), and resident information all at once. Simply download the template, fill in the required details, and upload the file. The system will automatically handle the creation, binding, and permission assignment, drastically reducing setup time and minimizing errors.

Log in to the platform, go to ⁞⁞ → **Video Intercom → Overview** .

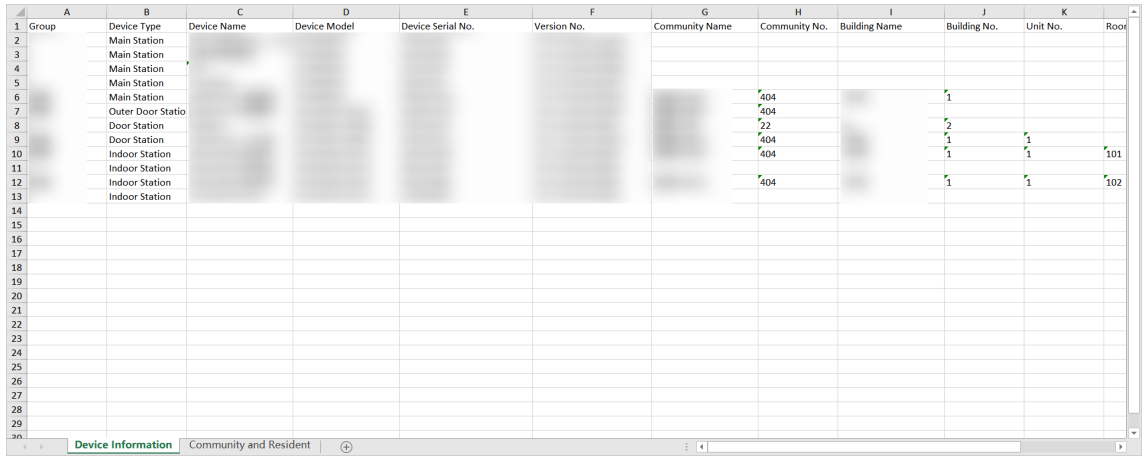
6.3.1 Step 1: Download the Import Template

1. Click **Batch Configure**, then select **Download Import Template**.





2. An Excel template will be generated and saved to your computer automatically.
   The template contains two sheets:
   - **Sheet1 – Device Information:** Use this sheet to configure intercom devices (door stations, outdoor stations, indoor monitors, and management consoles) and assign them to specific physical locations.

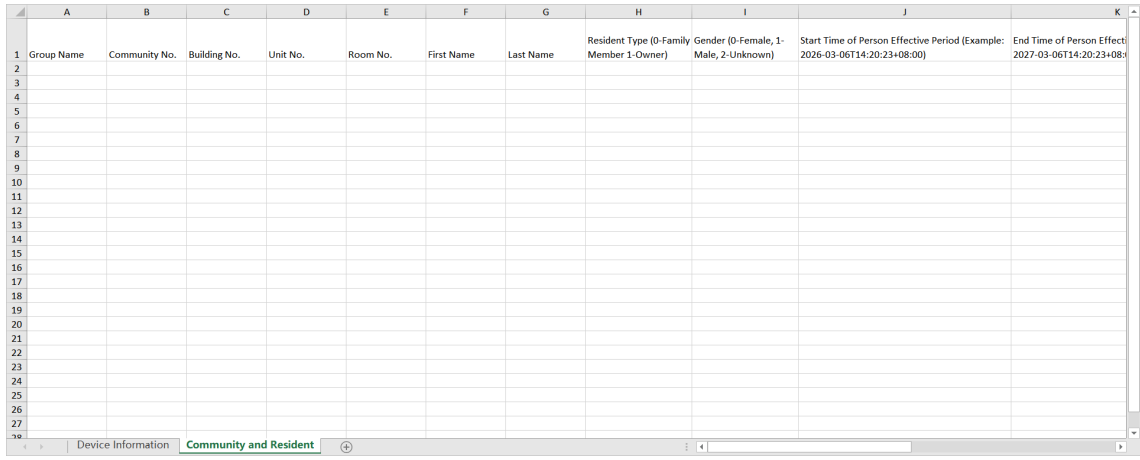


	A	B	C	D	E	F	G	H	I	J	K
1	Group	Device Type	Device Name	Device Model	Device Serial No.	Version No.	Community Name	Community No.	Building Name	Building No.	Unit No.
2		Main Station									
3		Main Station									
4		Main Station									
5		Main Station									
6		Main Station						404		1	
7		Outer Door Statio						404			
8		Door Station						22		2	
9		Door Station						404		1	1
10		Indoor Station						404		1	1
11		Indoor Station									
12		Indoor Station						404		1	1
13		Indoor Station									

Device Information | Community and Resident

Figure 6-1 Sheet 1

- **Sheet2 – Community and Resident:** Use this sheet to add residents in bulk and set up their personal details and access permissions.



	A	B	C	D	E	F	G	H	I	J	K
1	Group Name	Community No.	Building No.	Unit No.	Room No.	First Name	Last Name	Resident Type (0-Family Member 1-Owner)	Gender (0-Female, 1-Male, 2-Unknown)	Start Time of Person Effective Period (Example: 2026-03-06T14:20:23+08:00)	End Time of Person Effect 2027-03-06T14:20:23+08:

Device Information | Community and Resident

Figure 6-2 Sheet 2

6.3.2 Step 2: Fill Out the Template

Sheet1 – Device Information:

1. Open the template and navigate to the **Device Information** sheet.
2. The sheet comes pre-filled with the basic details of all existing intercom devices under your account (e.g., device name, serial number) and their current location bindings.
3. Only modify the entries that need to be changed or added:

- **To assign a location to an unbound device:** Enter the target location details in the corresponding columns—such as Community Name/No., Building Name/No., Unit No., and Room No./Name.
- **To relocate a device:** Update the hierarchy information directly. Upon import, the device will be unbound from its previous location and reassigned to the new one.
- **To unbind a device:** Clear the hierarchy fields. Upon import, the device will no longer be linked to any location.
- **To keep a device unchanged:** Leave the row as is.

Sheet2 – Community and Resident:

1. Switch to the **Community and Resident** sheet.
2. This sheet is blank. Follow the column headers to enter the resident information row by row.
3. Key fields include:
   - **Basic Information:** Name, account, mobile number, email, gender, resident type, etc.
   - **Location Binding:** Enter the Community No., Building No., Unit, and Room No. for each resident. The system will automatically link them to the corresponding room.
   - **Access Permissions:** Set the validity period, accessible floors, access level, app usage permission, and access PIN code.

Note

If you are only configuring devices in this batch, simply leave Sheet 2 blank.

6.3.3 Step 3: Upload and Import the File

1. Save the completed Excel file.
2. On the HCT platform, click **Batch Configure** again.
3. In the dialog that appears, choose the file you just saved and confirm the upload.
4. The system will validate the data. A progress bar will show the current stage of the import (e.g., Importing devices, Creating buildings, etc.).

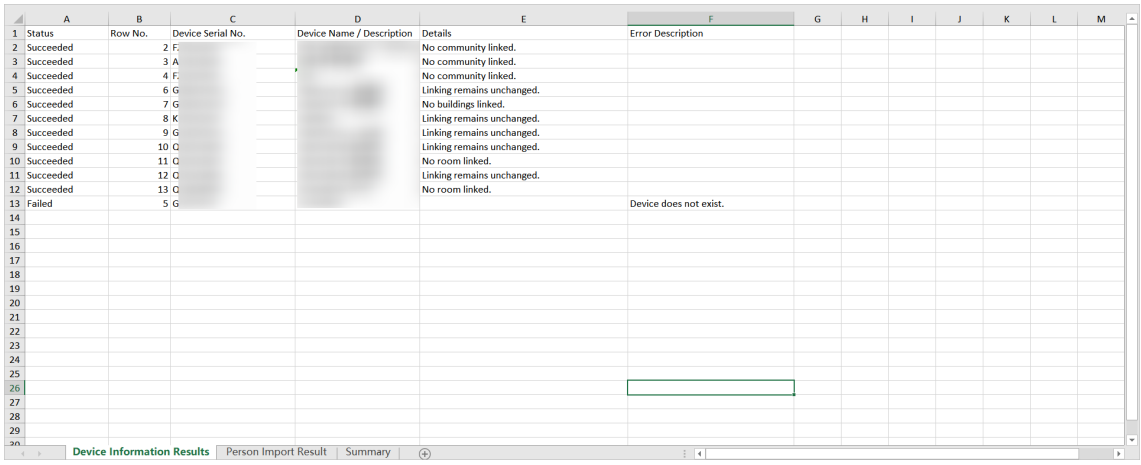
Note

You cannot cancel an import once it has started. Concurrent batch imports by multiple users are not supported.

6.3.4 Step 4: Check the Import Results

1. Once the import is complete, a summary will appear on the screen, showing:
   - The number of successfully and unsuccessfully bound devices.
   - The number of newly created or updated communities and buildings.
   - The number of successfully and unsuccessfully imported residents.
2. Click **Cause** to get a detailed Excel report.
3. The report contains three sheets:

- **Device Information Results:** Shows the processing status of each device, with reasons for any failures.
- **Person Import Results:** Shows the import status of each resident, with reasons for any failures.
- **Summary:** Provides an overall statistical overview.



Status	Row No.	Device Serial No.	Device Name / Description	Details	Error Description
Succeeded	2	F		No community linked.	
Succeeded	3	A		No community linked.	
Succeeded	4	F		No community linked.	
Succeeded	6	G		Linking remains unchanged.	
Succeeded	7	G		No buildings linked.	
Succeeded	8	K		Linking remains unchanged.	
Succeeded	9	G		Linking remains unchanged.	
Succeeded	10	C		Linking remains unchanged.	
Succeeded	11	C		No room linked.	
Succeeded	12	C		Linking remains unchanged.	
Succeeded	13	C		No room linked.	
Failed	5	G			Device does not exist.

Device Information Results | Person Import Result | Summary

Figure 6-3 Import Results

4. If there are any failures, you can use the information in the report to correct the data in your original template and re-upload the file.

6.4 How to add communities, units, buildings, rooms, and residents?

6.4.1 How to add communities?

The Community Management feature introduces a five-level hierarchy (Group, Community, Building, Unit, and Room) to help you organize large residential complexes or campuses more effectively.

Add a Community

1. Log in to the Portal, and go to ⁝⁝ → **Video Intercom** → **Community** to open the Community Management page.

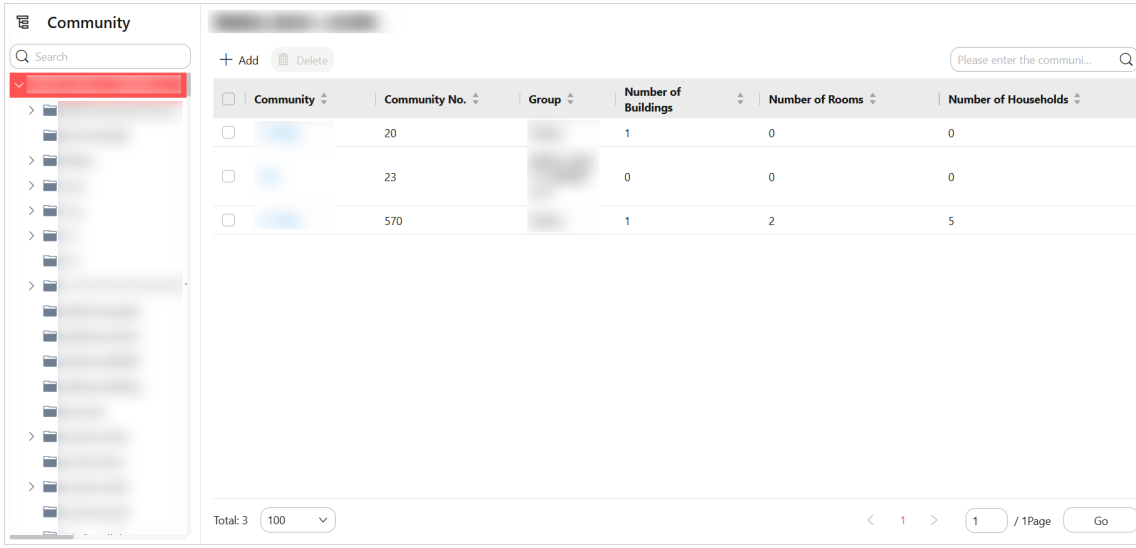


Figure 6-4 Add Community

2. The page displays a list of existing communities, including their name, No., parent group, and the number of buildings, rooms, and households.
3. Click **Add**.

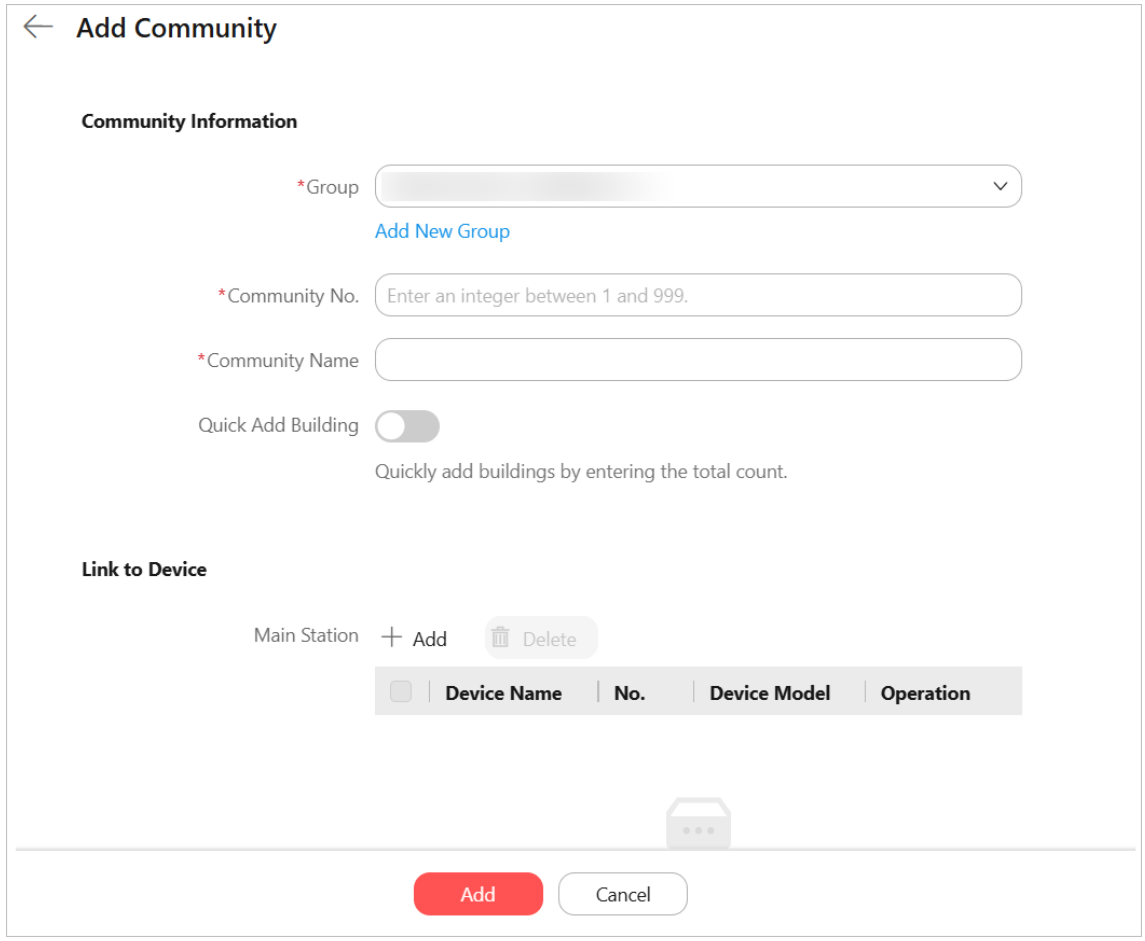


Figure 6-5 Add Community

4. In the pane that appears, fill in the following:
   - **Group**: Select where this community sits in the organization tree. It can be placed at the root level or nested under a specific group.
   - **Community No.**: Enter an integer between 1 and 999.
   - **Community Name**: Enter a clear, descriptive name.
5. (Optional) Enable **Quick Add Buildings**.
   - **Room Numbering Rule**: Select **Increment by 1 from the Start Number**.
   - **Number of Buildings**: Enter how many buildings you want to create, for example, 10. The system will generate Building 1 through Building 10.
   - **Start With**: Enter the starting number for the buildings, for example, 2.

Note

Deleting a Community Is Permanent: This action cannot be undone. All buildings, units, and rooms under the community will be permanently deleted, and associated devices will be unbound.

Link Main Stations

1. In the Main Station section, click **Add** tab and select a main station.

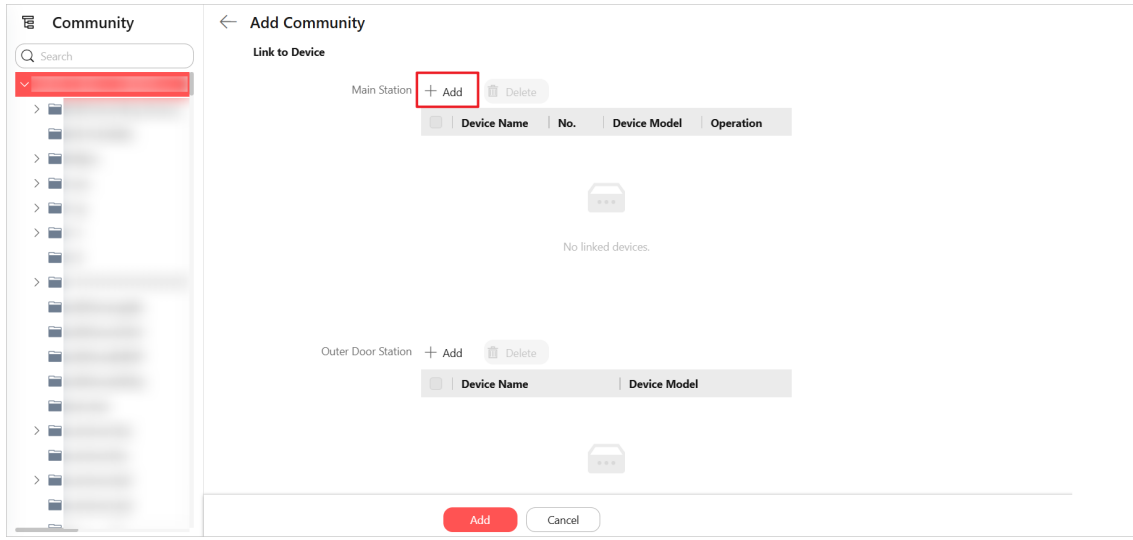


Figure 6-6 Link to Main Station

2. Select an available online device from the list, and click **Add**.
3. Click **Configure** in the Operation column to display the configuration pane.
4. Enter a unique number from 51 to 99.
5. Click **Add** to link buildings with the main station, so the door stations and indoor stations within the building can communicate with the main station.

Note

You may use the feature in the following scenarios:

- Property service calls are made from residents to security/property manager through the indoor station or app, which communicates with the main station via the cloud server.
- Property service calls are made from security/property manager to residents through the main station, which communicates with the indoor station or app via the cloud server.

'

6. Click **Add** in the Link to Device section to link cameras with the main station, so you can view live view of the linked cameras on the main station.

Configure Outer Door Stations

1. In the Outer Door Station section, click **Add**.

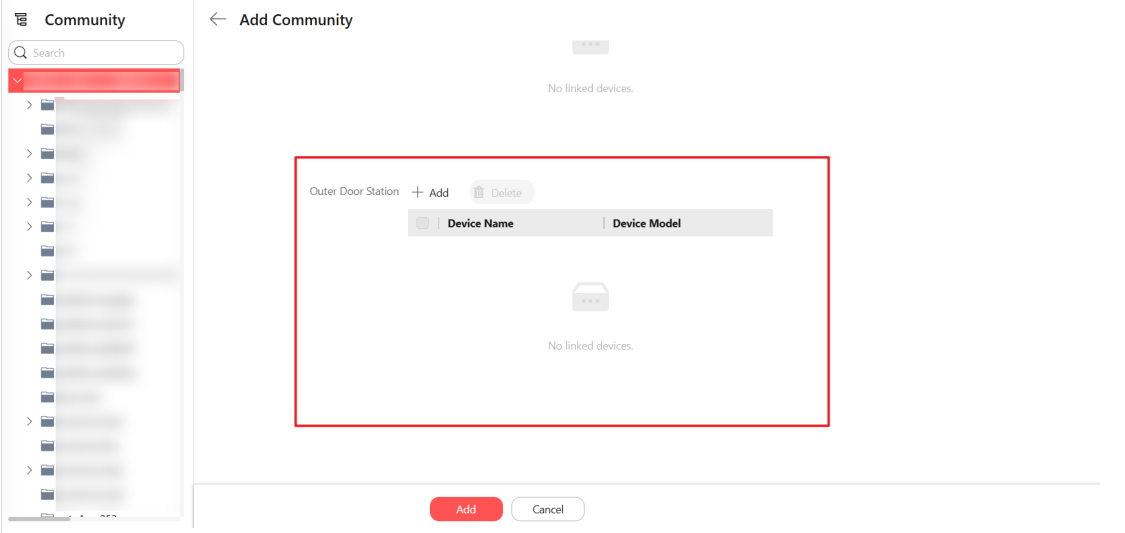


Figure 6-7 Link to Outer Door Station

2. Select an available online device.

Note

Device Already in Use: A device can only belong to one community. If a device is already assigned to another community, it will not appear in the selection list.

3. Click **Add**. The device will appear in the outer door station list.

Switch Between Communities on the Overview Page

1. Go to the → **Intercom** → **Overview** page.
2. At the top of the page, you will see a dropdown to switch communities. The default selection is the root group, which displays aggregated data for the entire platform.

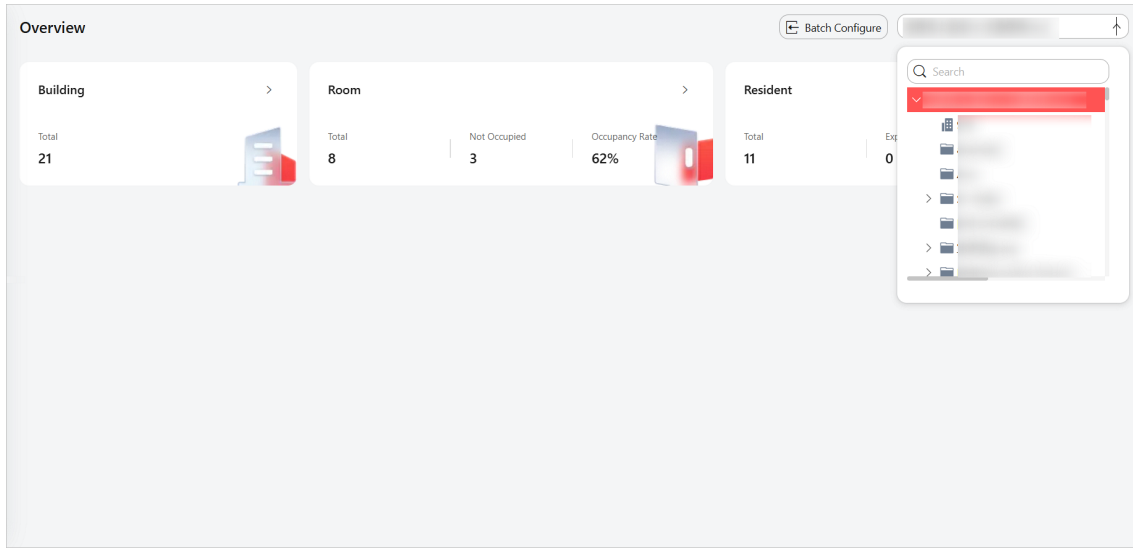


Figure 6-8 Switch Communities

3. Select a specific community from the dropdown menu.
4. The dashboard will refresh immediately, showing statistics such as the number of buildings, rooms, and residents for the chosen community.
5. Switching to a different community updates the displayed data in real time.

6.4.2 How to add buildings, units, and rooms?

1. Go to → **Video Intercom → Building → Add** to add a building.
2. Select the Group to which the building belongs to, and enter the building name.

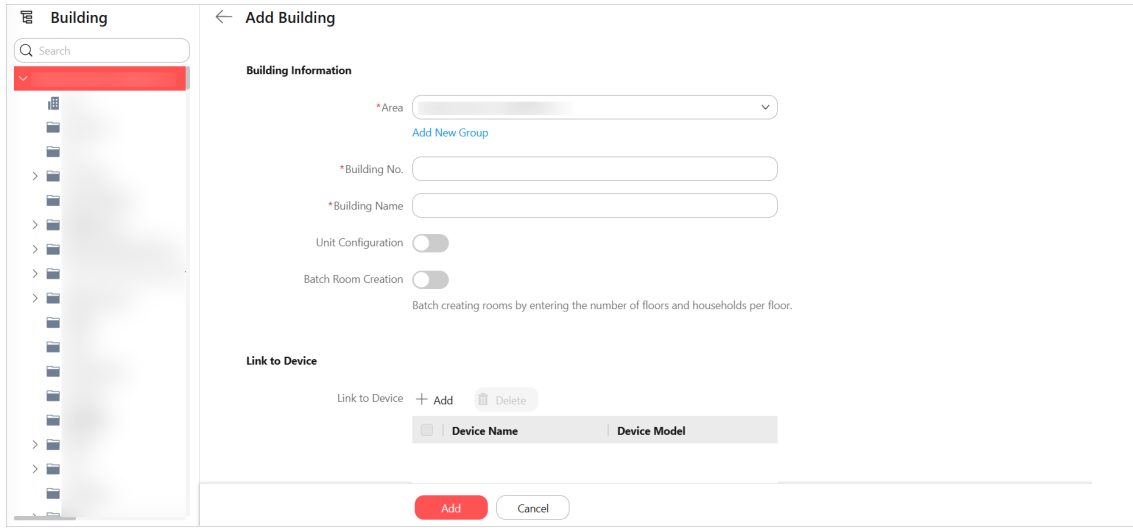


Figure 6-9 Add Building Page

3. Enable **Unit Configuration** to create units inside each new building.

4. Enable **Batch Room Creation** and enter the number of floors and the number of rooms per floor.
5. Link a camera and click **Add** at the bottom of the page.
6. You can view the added building on the Building page and the added rooms on the Room page.

How to add resident?

1. Go to → **Video Intercom** → **Resident** and click **Add**.

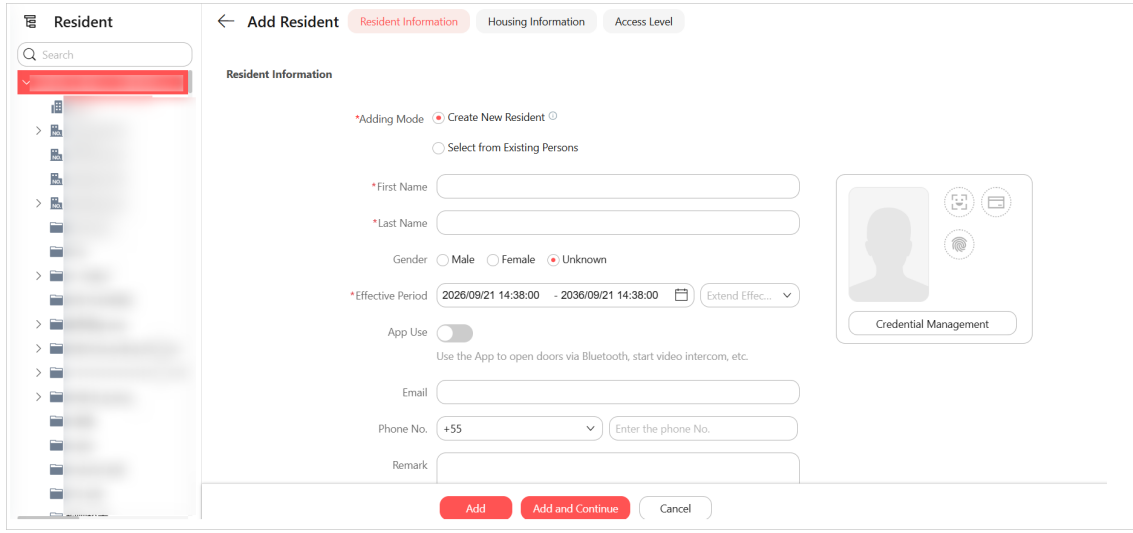


Figure 6-10 Add Resident

2. If the resident has been added to the Person list, select **Select from Existing Persons**, otherwise select **Create New Resident**.
   After you select **Create New Resident**, set the resident name, effective period, email, etc.
3. Enable **App Use** to allow the resident to log in to the Hik Connect for Teams Mobile Client with the email / phone No. to use the video intercom features.
4. Click the profile photo to upload the face picture of the resident.

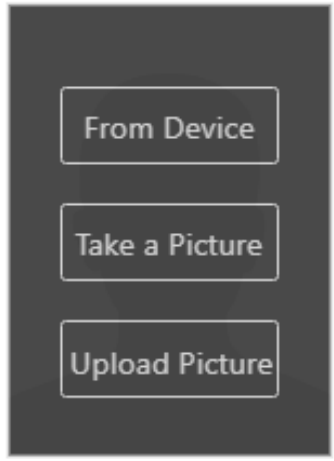


Figure 6-11 Upload Face Picture

5. Click **Credential Management** to add a card and/or a fingerprint for the resident.
6. Select an area/community where the resident is located.
   Click **Add** to add the resident to the corresponding room.

Note

After the resident is added to a room, the face picture will be applied to the video intercom device linked to the corresponding building, and the resident can access the building via face recognition.

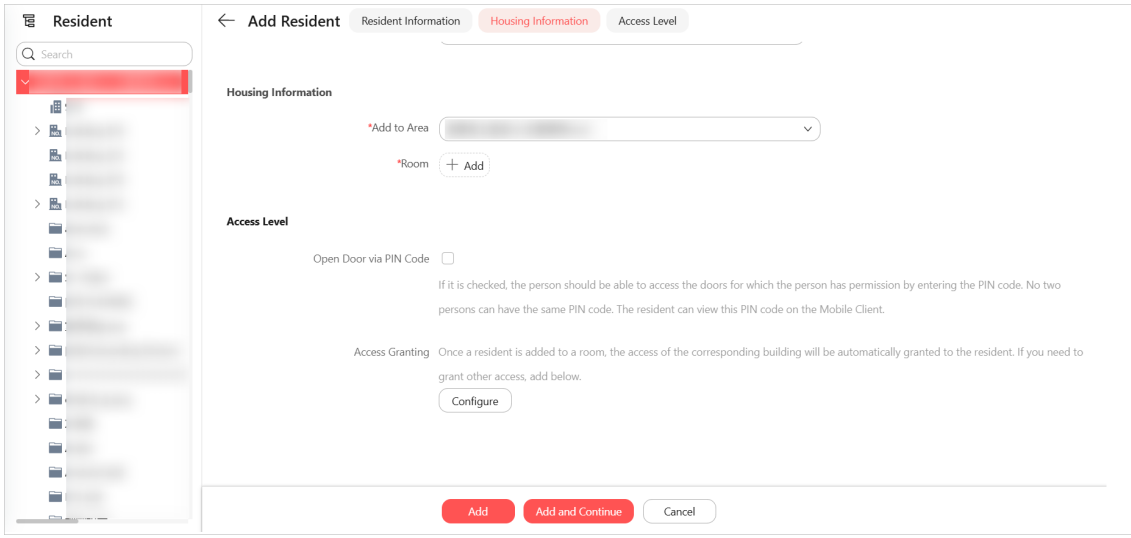


Figure 6-12 Housing Info and Access Level

7. **Open Door via PIN Code**: If it is checked, the person should be able to access the doors for which the person has permission by entering the PIN code. No two persons can have the same PIN code. The resident can view this PIN code on the Mobile Client.
8. **Access Granting**: Once a resident is added to a room, the access of the corresponding building will be automatically granted to the resident. If you need to grant other access, click **Configure**.
   - Click **Access Point** and select access points to grant the person 24/7 access to certain doors or floors.
   - Click **Access Level** to grant batch access to doors or floors for a set period.
9. Click **Add**.

6.5 How to manage notices?

In the Notice Management module, property managers can send regular and emergency notices directly to the resident app.

Go to → **Video Intercom → Management Center → Notice Management → Add** .

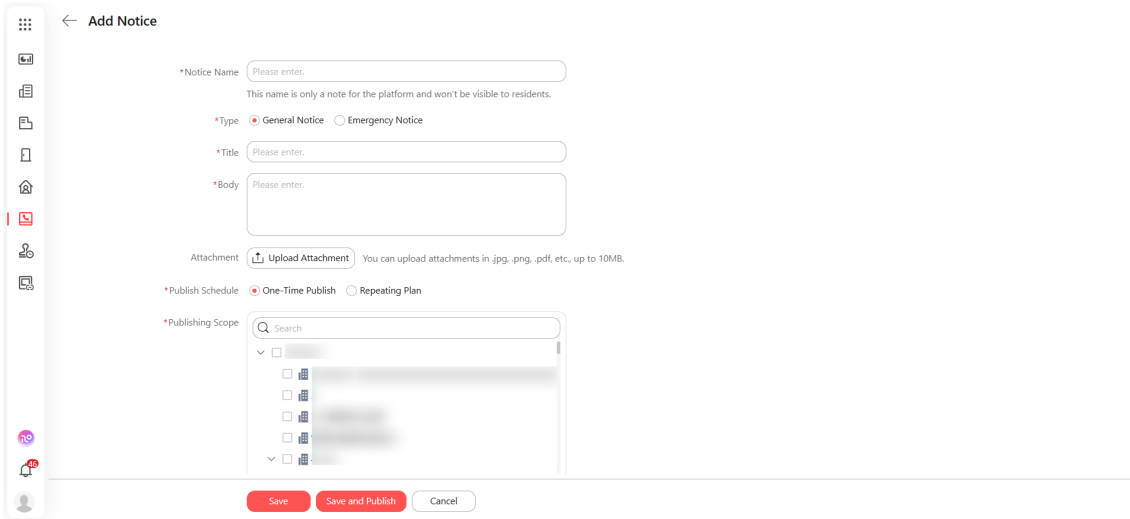


Figure 6-13 Add Notice

Property managers can now deliver notices to residents through the Portal, replacing traditional paper bulletins. Two notice types are supported: General Notices for daily updates with image and PDF attachments, and Emergency Notices that trigger an immediate pop-up with an alert sound on the resident app.

Managers can select recipients by unit, building, or the entire community, and set one-time or repeating schedules. Publishing records can be managed, exported, and deleted in batch.

On the resident app, a new "Notices" category has been added to Notification. Emergency notices are text-only, and attachments are limited to jpg, png, and pdf formats.

6.6 How to view call history?

Go to → **Video Intercom → Management Center → Call History** to view and export the call history.

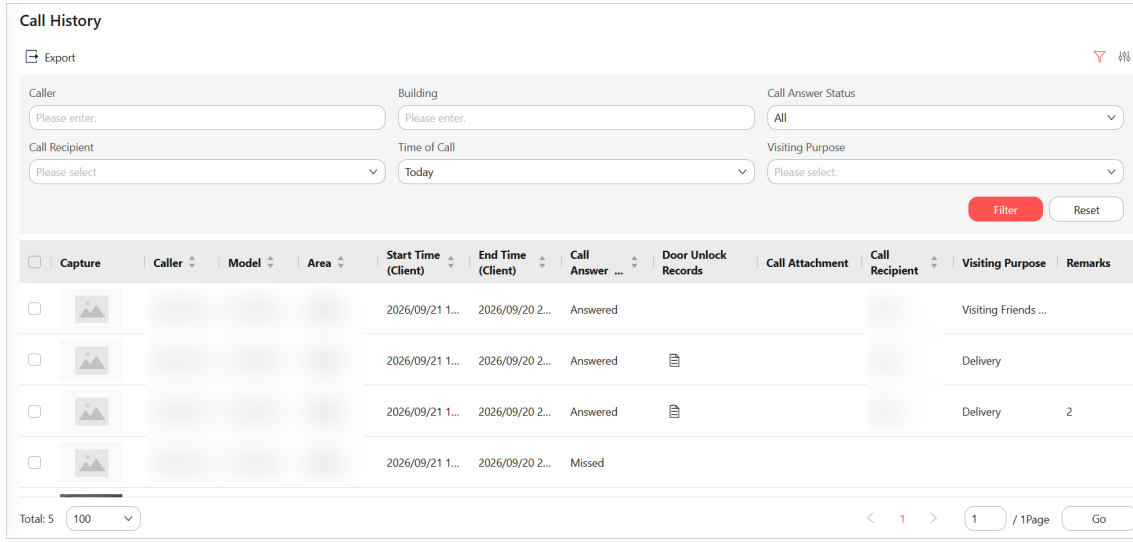


Figure 6-14 Call History

The three call answer status are as follows.

- Missed: Someone calls from the video intercom device and the resident does not receive or answer.
- Answered: Someone calls from the video intercom device and the resident receives and answers.
- Missed (Blocked):Set a blocklist in the App or on Indoor Stations to block calls from specific rooms, with syncing across platforms. Blocked calls show as "blocked" in call records.

6.7 How to add call manager?

1. Go to → **Video Intercom → Management Center → Call Manager** to add a call manager.
2. Click **Add** to enter the Add Call Manager page.
3. Set the devices from which the call manager receive calls.
   - Select **All Devices** for the call manager to receive calls from all the devices for which they have permissions.
   - Select **Specified Device(s)**, select device(s) on the Available list, and click **>** to move the selected device(s) to the Selected list for the call manager to receive calls from the selected device(s).
     Select device(s) on the Selected list and click **<** to remove the device(s) from the Selected list.

Note

The call manager will only receive calls from the selected devices.

4. Click **Save** to finish adding the call manager.

6.8 How to create temporary passes?

1. Go to → **Video Intercom** → **Temporary Pass Management** and click **Add**.

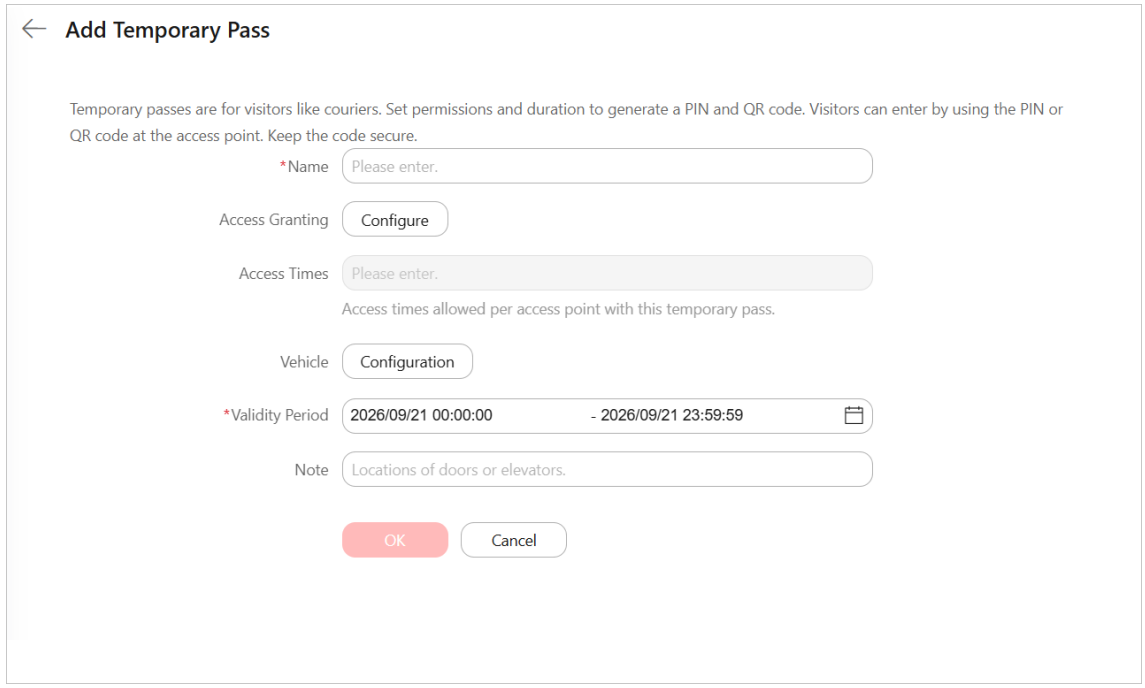


Figure 6-15 Create Temporary Pass

2. Set the name, access granting, access times, vehicle, and validity, and click **Add**.
3. After creating a temporary pass, you can download the QR code on the temporary pass list and provide it to the visitor.

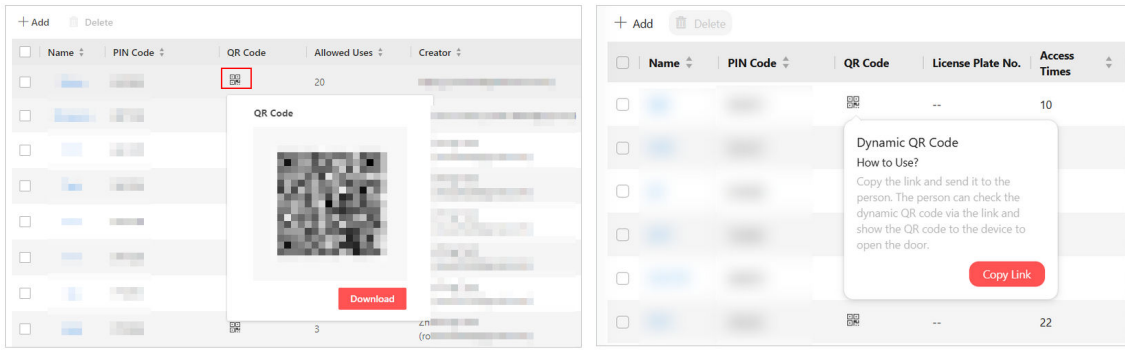


Figure 6-16 Download QR Code

4. Click the icon on the temporary pass list to view the door unlock records.

Chapter 7 On-board Monitoring

This guide provides comprehensive instructions for setting up and configuring on-board monitoring systems, including device addition, parameter configuration, and application usage.

7.1 Example Scenario

This guide provides a step-by-step configuration process for managing a fleet of vehicles traveling between City A and City B, including vehicle and driver setup, route planning, monitoring, and reporting. It covers scenarios for 5 drivers with examples for efficient fleet operations.

1. ***Add On-Board Devices***
   - Install and configure on-board monitoring devices on each vehicle. Ensure devices are connected to the network and integrated with the system.
   - **Example:** For a fleet traveling between City A and City B, install GPS devices on all 5 vehicles to track location and speed. Use cameras for driver behavior monitoring and safety compliance.
   - Path: ⁞⁞ → **Device → On-Board Device**
2. ***Configure Basic Fleet Parameters***
   - Set up basic parameters such as distance units (e.g., kilometers), GPS reporting frequency, and event thresholds to align with fleet operations.
   - **Example:** For the City A to B route, set GPS reporting every 30 seconds for real-time tracking. Use kilometers for distance calculations and enable speed alerts with a threshold of 100 km/h for highway sections.
   - Path: ⁞⁞ → **On-Board Monitoring → Basic Configuration → Basic Parameters**
3. ***Add and Manage Drivers***
   - Create driver profiles, assign them to vehicles, and configure license information. Group drivers for easier management based on shifts or routes.
   - **Example:** Add 5 drivers (e.g., John, Alice, Bob, Carol, David) for the City A-B route. Assign each driver to a specific vehicle and create groups for day and night shifts to streamline scheduling.
   - Path: ⁞⁞ → **On-Board Monitoring → Driver Management**
4. ***Define Route and Driving Rules***
   - Set up the route from City A to City B, including geofences, speed limits, and restricted areas. Configure rules for deviations or alerts to ensure compliance.
   - **Example:** Draw the route on a map with a speed limit of 80 km/h in urban areas and 100 km/h on highways. Set geofences at depots in City A and B to trigger arrival/departure alerts for all 5 vehicles.
   - Path: ⁞⁞ → **On-Board Monitoring → Driving Rule Configuration**
5. ***Configure Event Monitoring***

- Enable event types such as speeding, harsh braking, or route deviations. Set thresholds and notification methods for real-time alerts to improve safety.
- **Example:** Configure speeding alerts to trigger if vehicles exceed 100 km/h. Enable harsh braking detection with a threshold of 0.5g to monitor driver behavior and reduce accident risks on the City A-B route.
- Path: ⁞⁞ → **On-Board Monitoring → Basic Configuration → Event Receiving Configuration**

6. ***Assign Vehicles to Drivers***
   - Link drivers to specific vehicles and schedules. Ensure assignments match route requirements and shift patterns for optimal efficiency.
   - **Example:** Assign Driver John to Vehicle 1 for morning shifts on the City A-B route, and Driver Alice to Vehicle 2 for evening shifts. Use bulk assignment to quickly link all 5 drivers to their respective vehicles.
   - Path: ⁞⁞ → **On-Board Monitoring → Driver Management**
7. ***Set Up Real-Time Monitoring***
   - Enable live tracking, video streaming, and two-way audio for real-time fleet supervision. Configure alerts for immediate response to incidents.
   - **Example:** Use real-time tracking to monitor the 5 vehicles on the City A-B route. Enable live video from on-board cameras to check driver fatigue and road conditions, with two-way audio for communication.
   - Path: ⁞⁞ → **On-Board Monitoring → Driving Monitoring**
8. ***Generate Reports and Analytics***
   - Create reports on driving duration, distance, events, and compliance. Export data for analysis, payroll, or maintenance scheduling.
   - **Example:** Generate weekly reports for the 5 drivers, highlighting speeding incidents and fuel efficiency on the City A-B route. Export data in CSV format for integration with payroll systems.
   - Path: ⁞⁞ → **On-Board Monitoring → Statistics and Reports**

7.2 How to add on-board monitoring devices?

How to add on-board devices?

Refer to ***Device Management*** .

How to configure on-board monitoring device remotely?

After successfully adding the device, you can remotely configure the device's event upload function and other parameters on the platform, mainly including basic events and VCA events. VCA mainly includes driver behavior monitoring and ADAS.

1. Enter the device addition page, drag the scroll bar below, and click the **Remote Configuration** button.
2. Enter the remote configuration page requires the use of a plugin. If the plugin is not downloaded, the platform will remind you to download it when you click Settings. Follow the instructions to download, and refresh after success.
3. Click **Event → Basic Event → Channel No.** , then enable **Motion Detection**, select **Notify Surveillance Center**, set **Trigger Channel**, and click **Save**. After saving, if an event is triggered, you will receive push notification information using the HCT App.

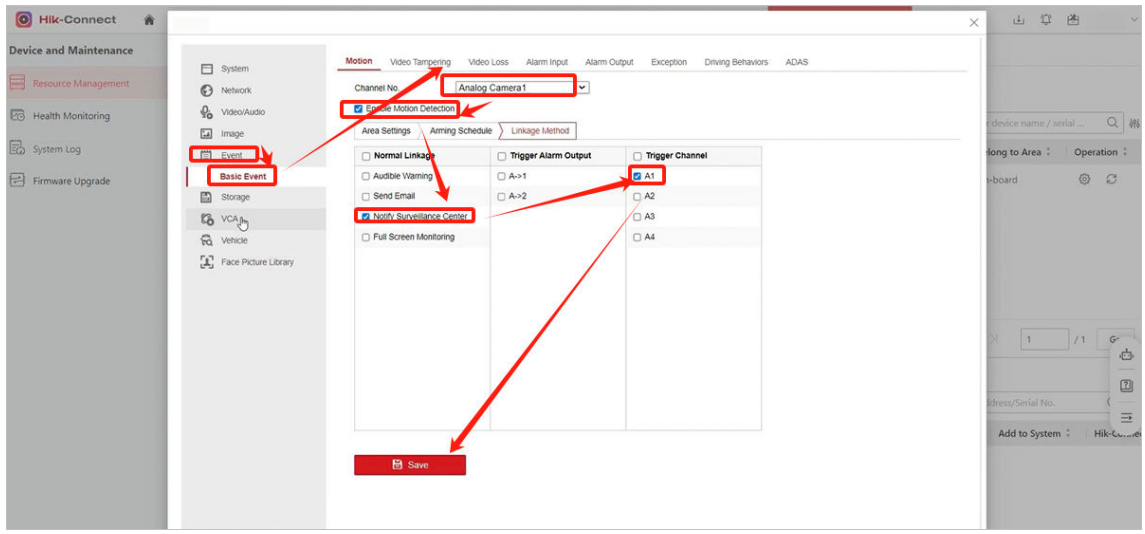


Figure 7-1 Configure Basic Event

4. Click **VCA → Driving Behaviors → Channel No.** , then enable **Platform** and click **Save**. After saving, if any driver behavior events in the list are triggered, the device will upload 7-second short videos and snapshots to the platform. You can view the details of driver violations in event alarms.

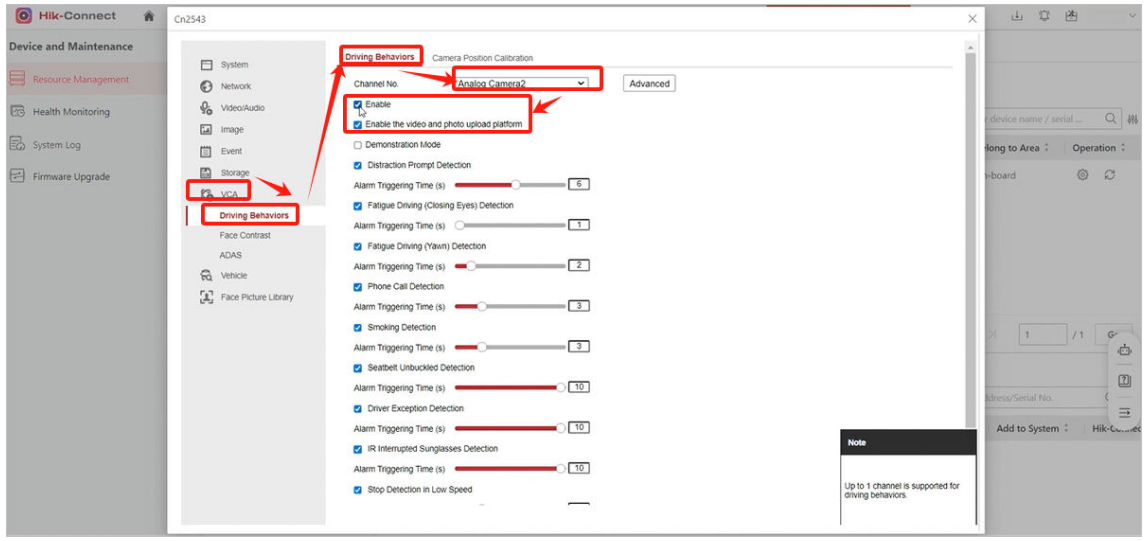


Figure 7-2 Configure VCA Event

7.3 How to configure parameters for on-board monitoring?

How to configure basic parameters?

Go to ⁝⁝ → **On-Board Monitoring** → **Basic Configuration** → **Basic Parameter Configuration** to configure the basic parameters for on-board monitoring, including the distance unit, the GPS reporting frequency, and the duration threshold for auto switching off stream.

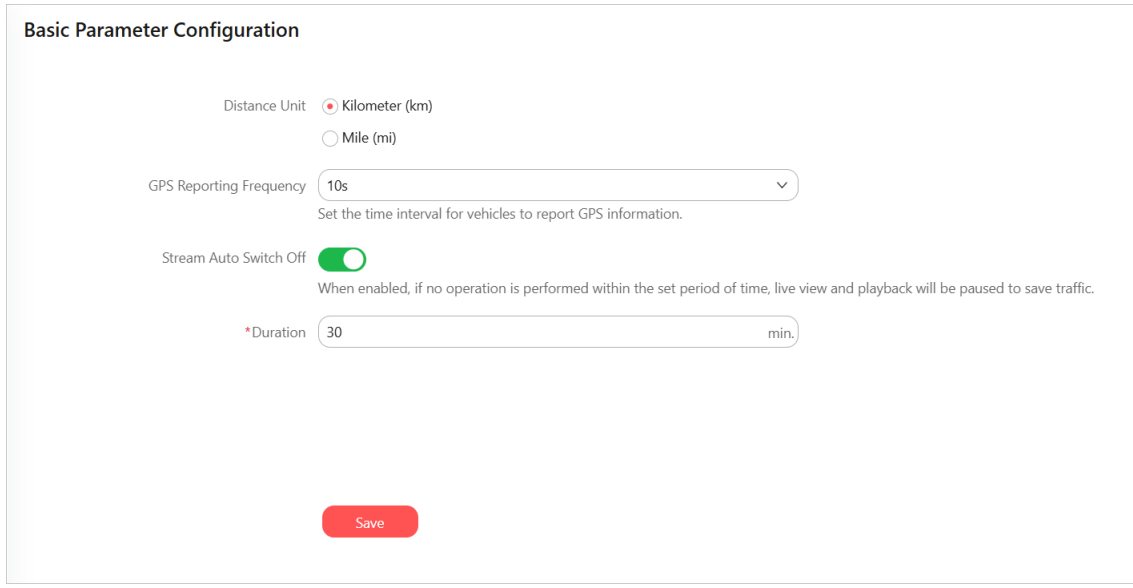


Figure 7-3 Basic Configuration

How to configure event receiving?

Go to ⁞⁞ → **On-Board Monitoring** → **Basic Configuration** → **Event Receiving Configuration** to set the types of events to be received by your system.

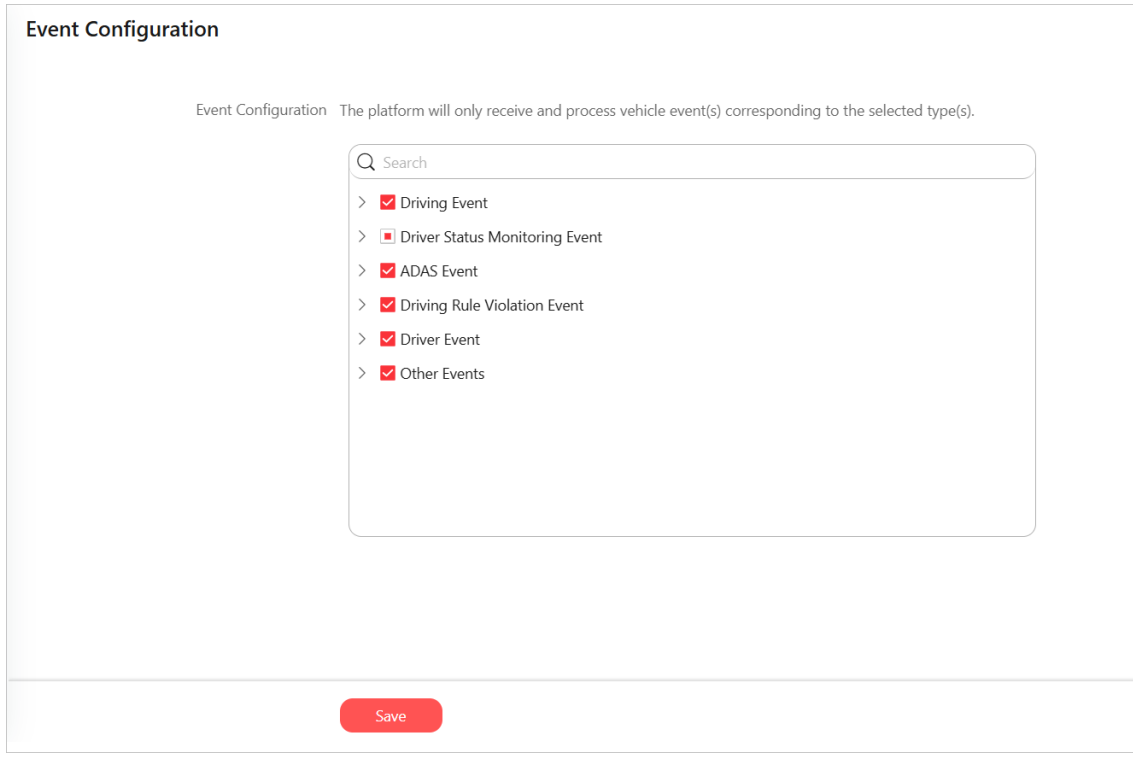


Figure 7-4 Event Receiving Configuration

Note

If an event type is not selected here, the system will not be able to receive the corresponding vehicle event reported by your device.

How to configure driving rules?

1. Go to ⁞⁞ → **On-Board Monitoring** → **Driving Rule Configuration** , and click **Add**.

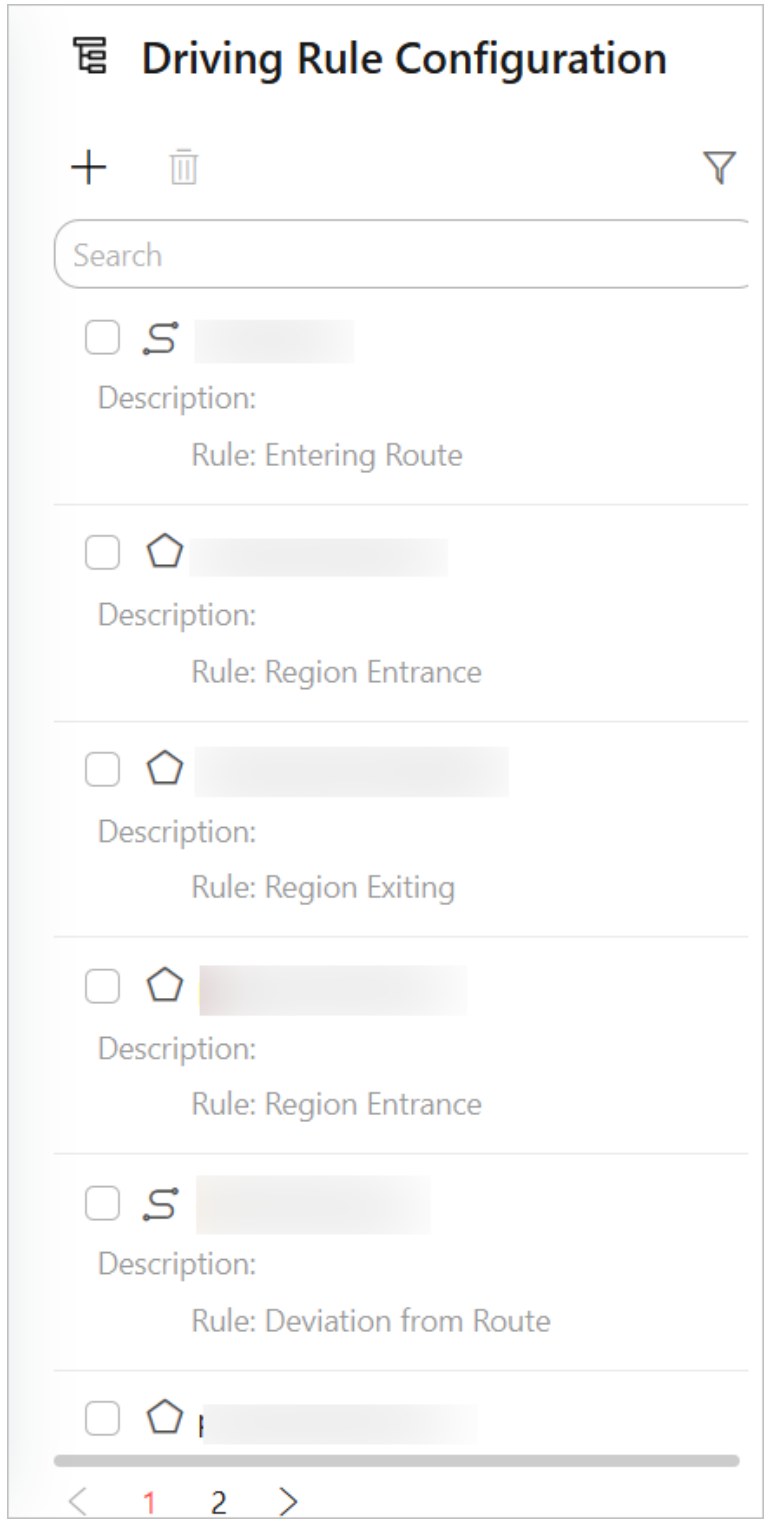


Figure 7-5 Add Driving Rule

2. Select **Polygon** or **Line** to add a driving rule for region/route respectively, and select a rule type.

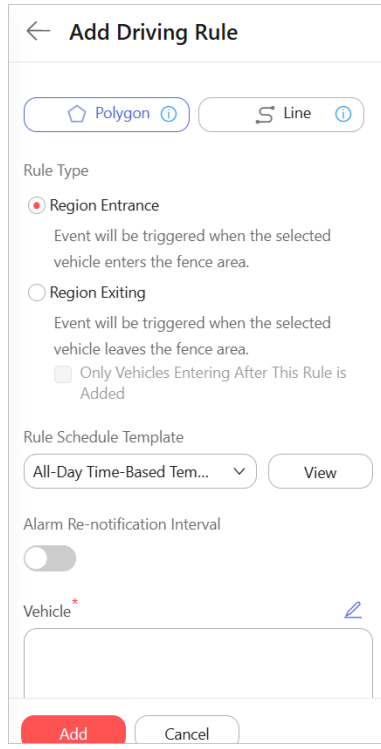


Figure 7-6 Add Driving Rule for Region/Route

3. Click on the map to start drawing a region/route for the driving rule, and right-click to finish drawing.
4. Set the other information (e.g., rule schedule template, vehicles, rule name) and click **Add**.

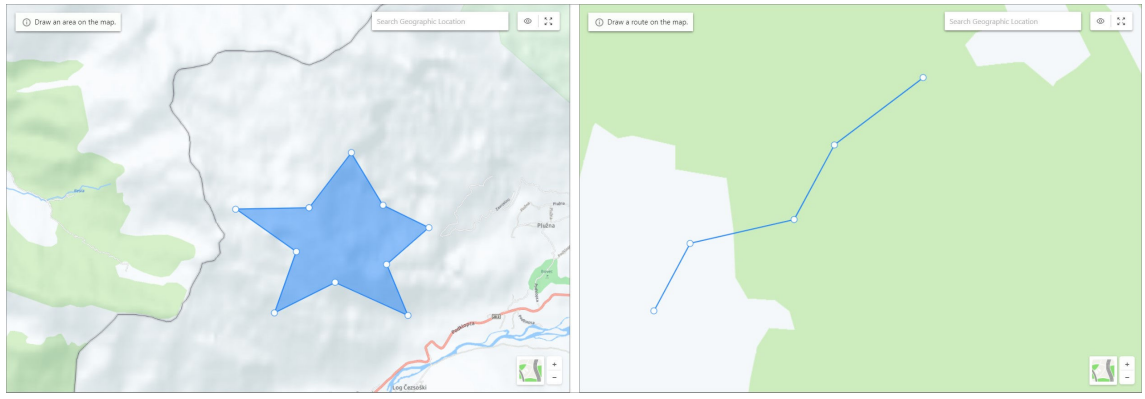


Figure 7-7 Draw Region/Route for Driving Rule on the Map

How to manage drivers?

1. Go to → **On-Board Monitoring** → **Driver Management** , click + , set the required parameters, and click **Add** to create a driver group.

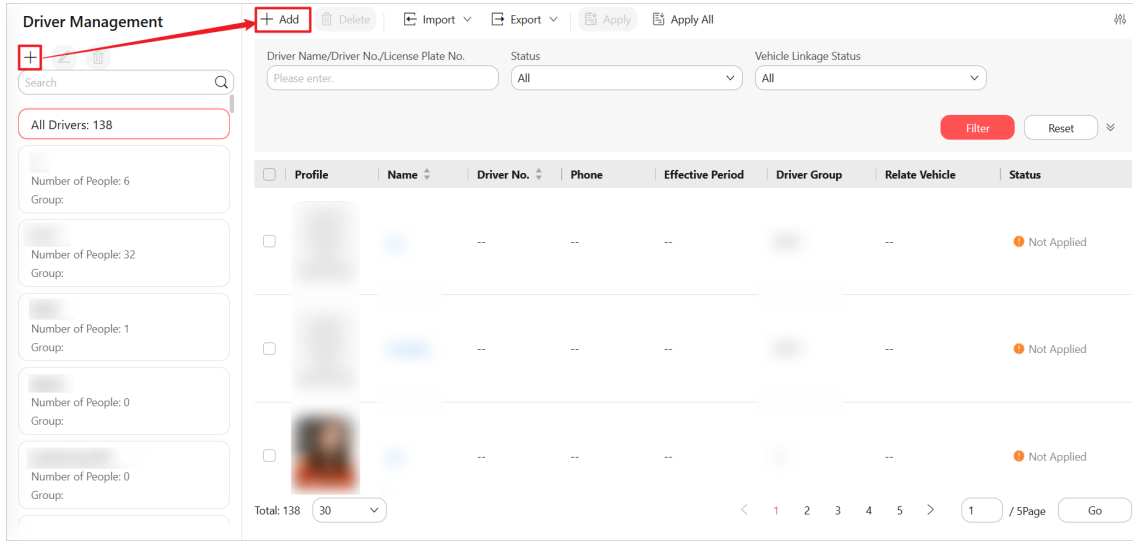


Figure 7-8 Add Driver Group

2. Select the created driver group and click **Add** to open the Add Driver page. Edit basic information, link vehicles, and edit driver's license information.

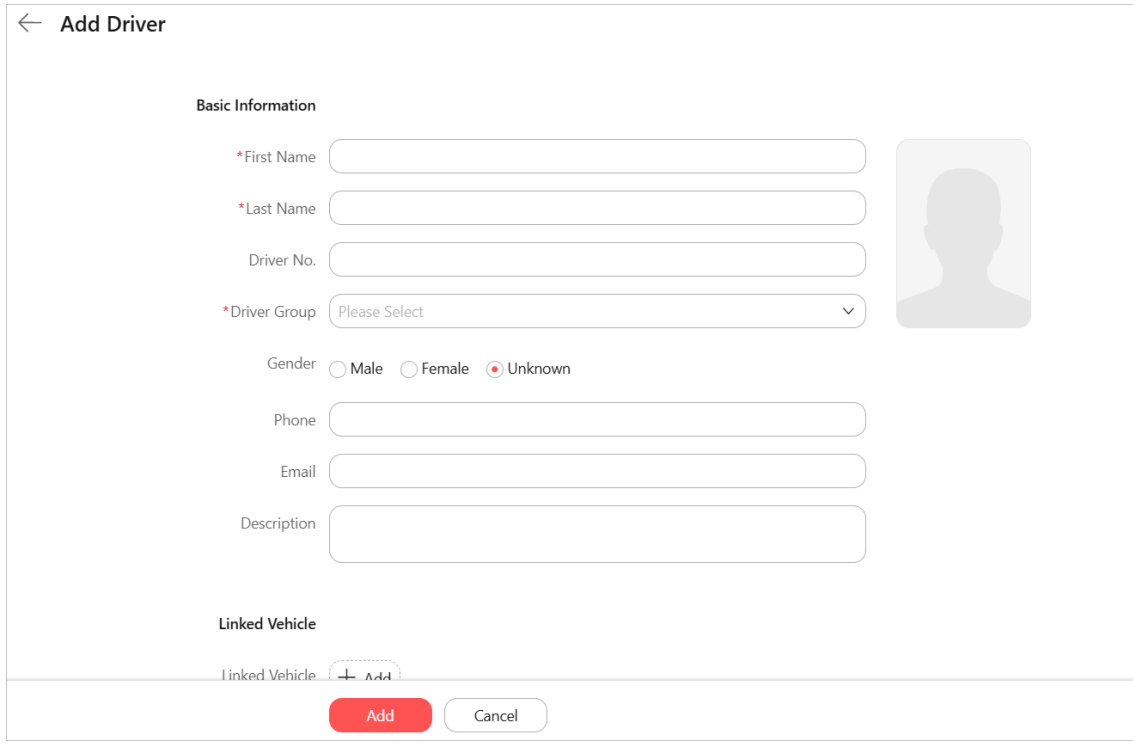


Figure 7-9 Edit Driver Information

3. Select the driver and click **Apply** to apply driver information to devices. The status will change from "Not Applied" to "Applied" if the information is successfully applied.

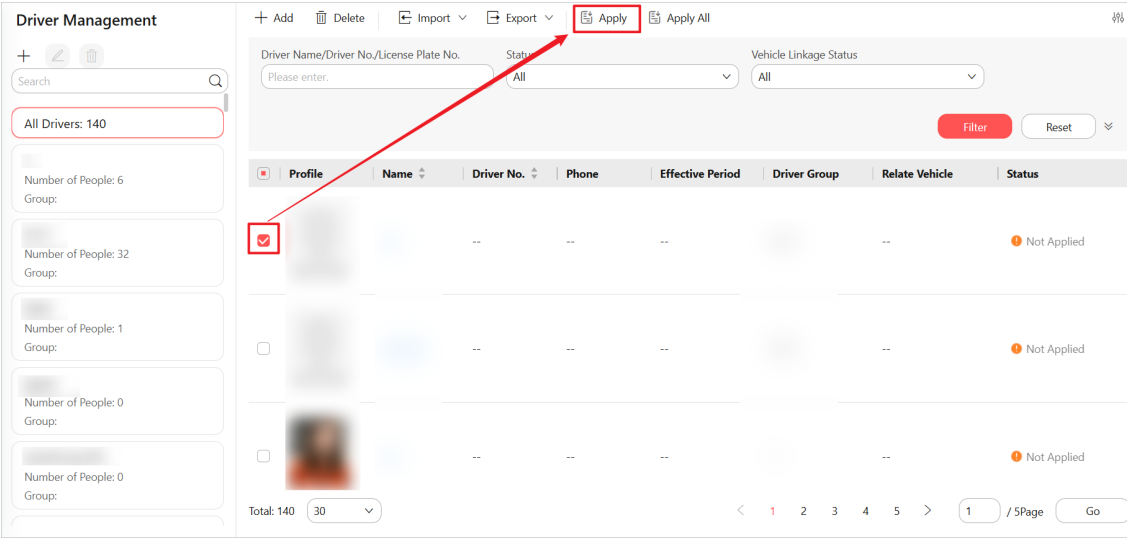


Figure 7-10 Apply Driver Information

7.4 How to use related applications?

How to use the dashboard?

1. In the Dashboard, you can see four different types of reports sorted by vehicle basis, including Driving Duration, Driving Distance, Speeding, and Driving Events. You can also select different times to view the ranking order. By clicking the name, you can jump to the detailed report module.

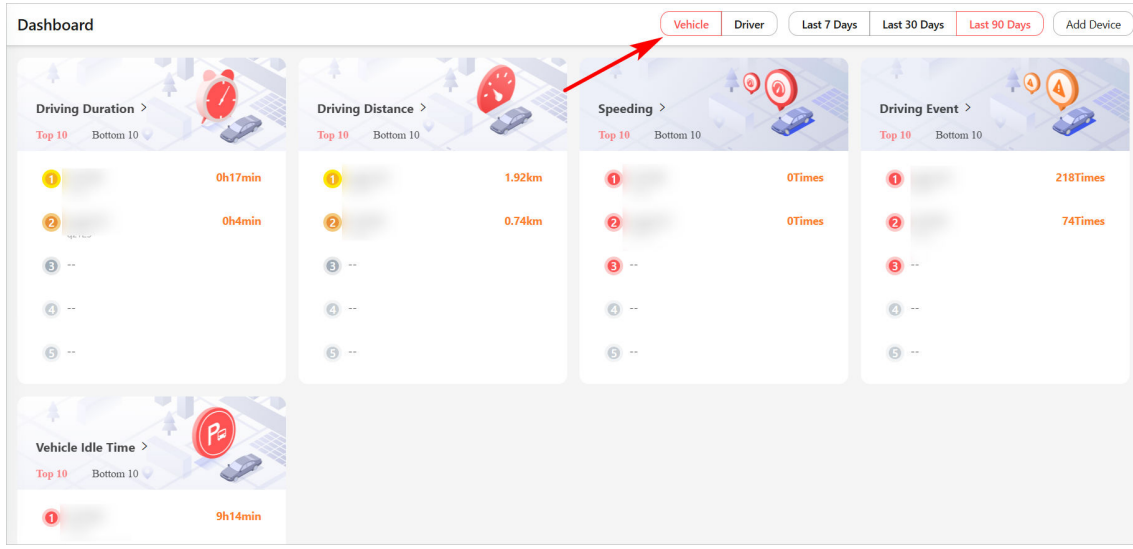


Figure 7-11 Vehicle Report Table

2. You can also select drivers to view the driving report ranking table. In addition, you can choose different sorting methods, including Top 10 and Bottom 10.

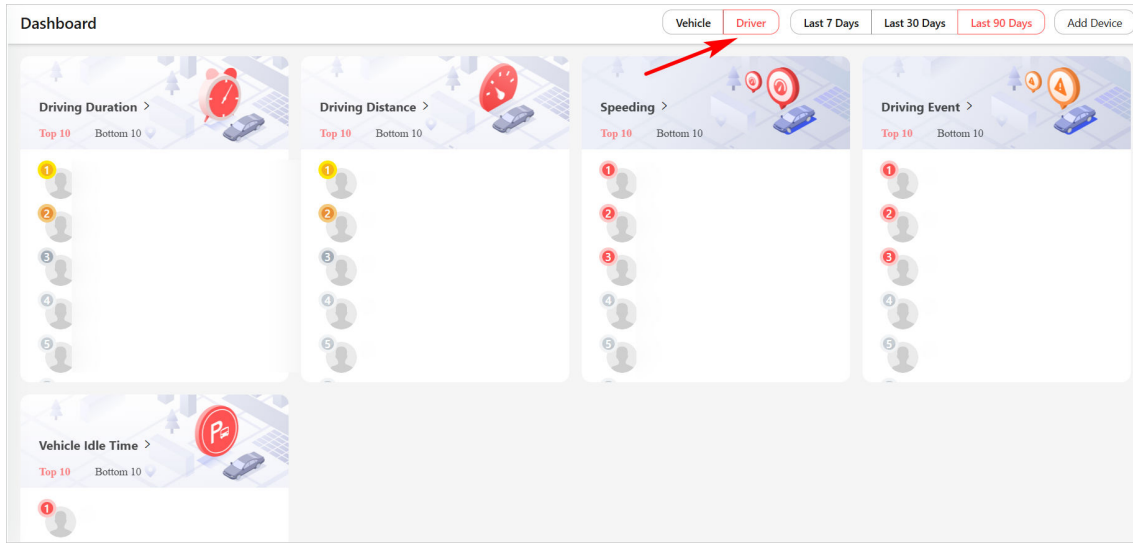


Figure 7-12 Driver Report Table

How to use driving monitoring?

Vehicle Locating: On the vehicle list pane, hover over a vehicle name, and click the location icon to locate the vehicle on the map.



Figure 7-13 Locate Vehicle on Map

Live View & Playback:

For playing the live/recorded videos of all channels: On the vehicle list pane, click ▷ beside a vehicle name. For vehicles being located, you can also click a vehicle on the map and select the play option.

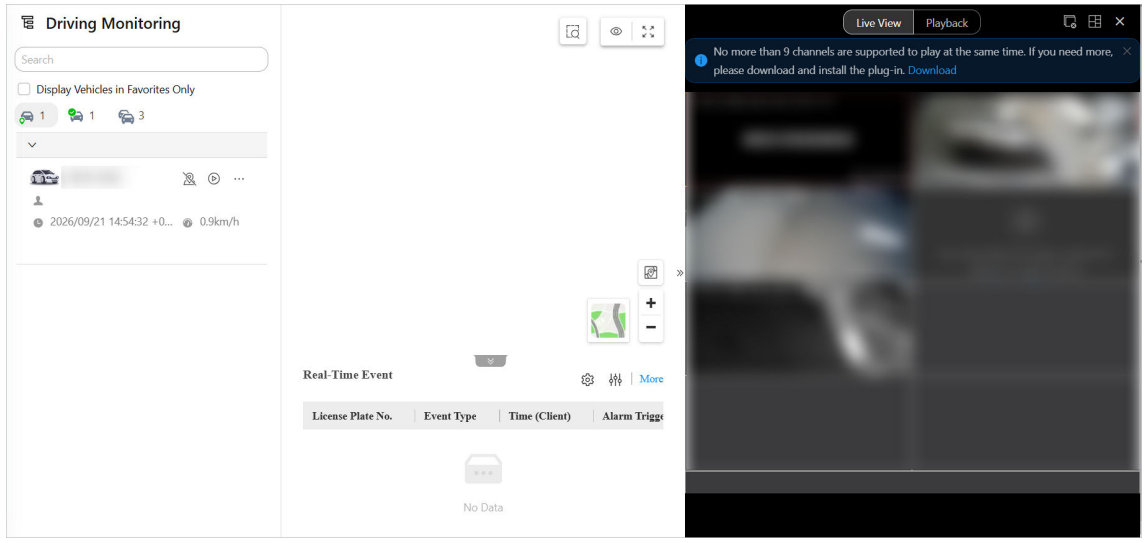


Figure 7-14 Play Video of All Channels

For playing the live/recorded videos of a specific channel: On the vehicle list pane, hover over a vehicle and select a camera/channel from the vehicle information pane.

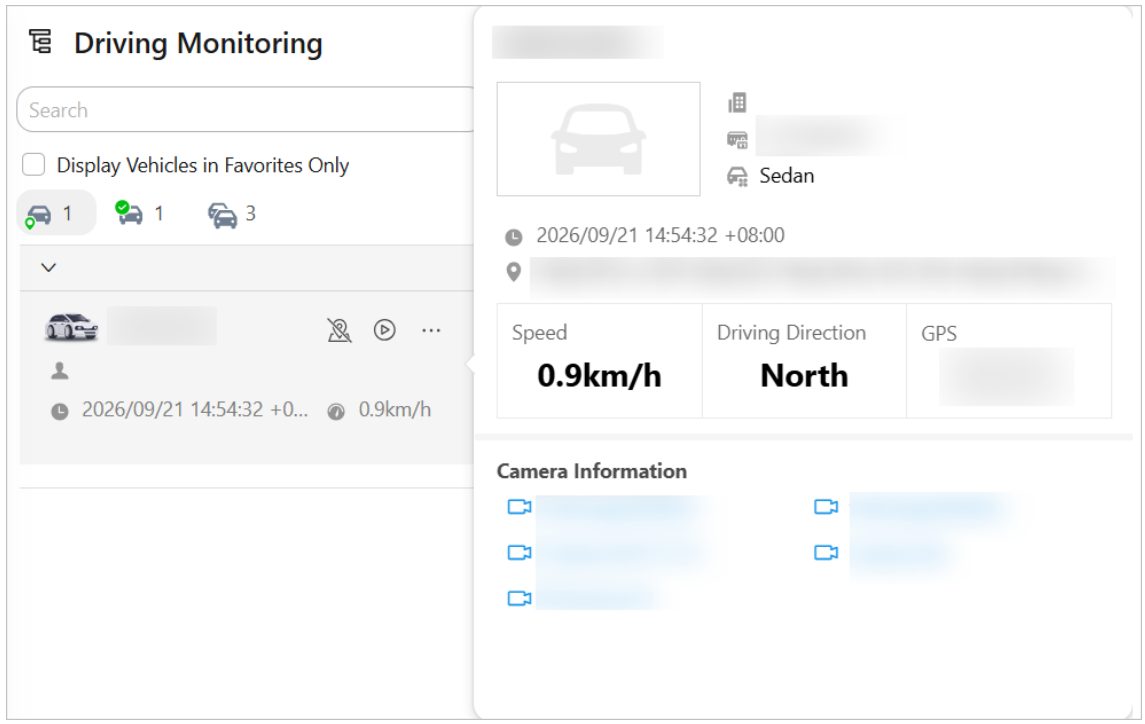


Figure 7-15 Select Camera for Live View / Playback

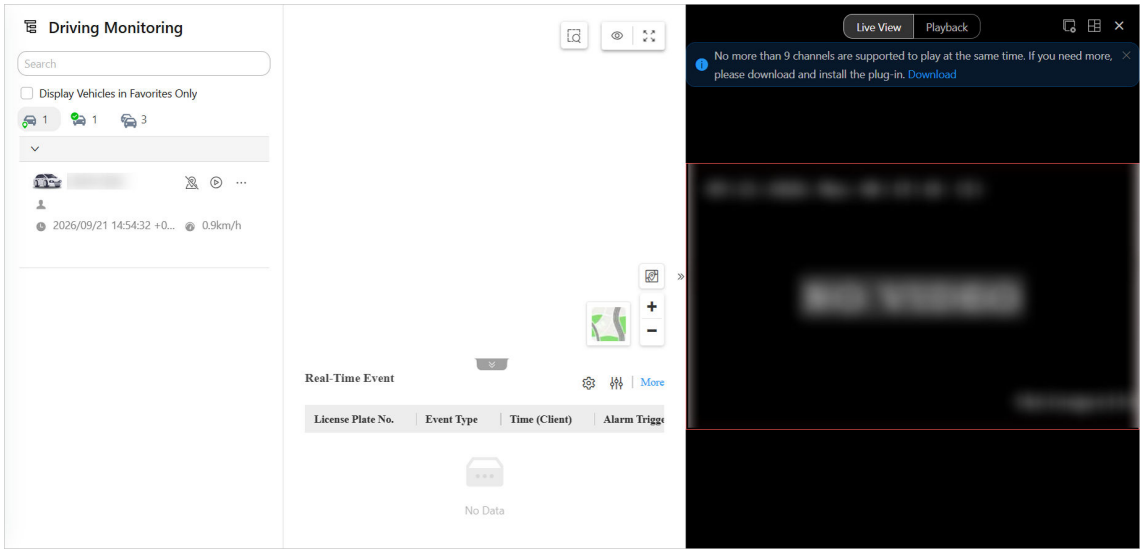


Figure 7-16 Play Video of a Specific Channel

Two-Way Audio: On the vehicle list pane, click ••• → **Two-Way Audio** , and click Start/Stop to start/stop the two-way audio respectively. For vehicles being located, you can also click a vehicle on the map and select the audio icon to start the two-way audio.

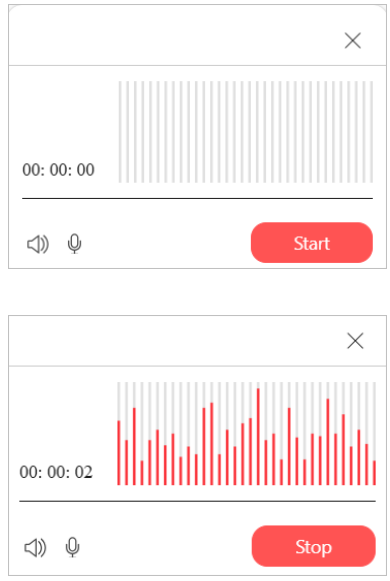


Figure 7-17 Two-Way Audio

Real-Time Tracking: On the vehicle list pane, click ••• → **Real-Time Tracking** to track the real-time movement of the vehicle. You can also choose whether to view live videos of cameras while tracking.

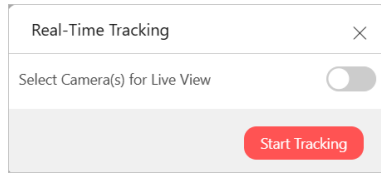


Figure 7-18 Select Cameras for Live View During Real-Time Tracking

For vehicles being located, you can also click a vehicle on the map and select the tracking icon to start the real-time tracking.

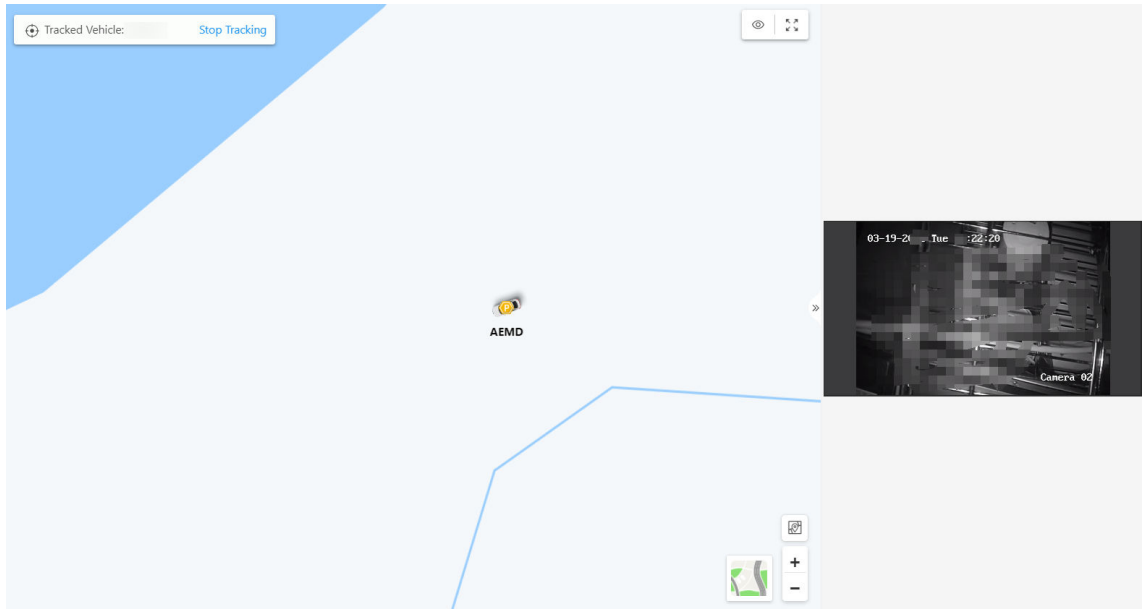


Figure 7-19 Real-Time Tracking

Track Playback: On the vehicle list pane, click the playback icon beside a vehicle name to play back the track the vehicle has traveled along during the selected time period. You can also choose whether to view recordings of cameras while playing back the vehicle's track.

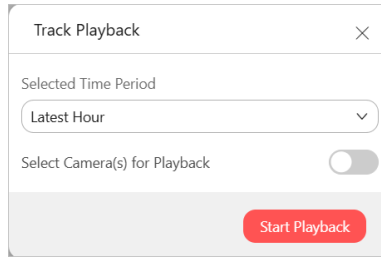


Figure 7-20 Select Cameras for Playback During Track Playback

For vehicles being located, you can also click a vehicle on the map and select the playback icon to play back the vehicle's track. During track playback, you can perform operations via the bottom tool bar, such as adjusting the playback speed, skipping the parts with no recordings, and setting a speed threshold.



Figure 7-21 Track Playback

Track Search: On the Track Search page, you can search for vehicle tracks by specifying a time period, selecting vehicle(s), setting a speed range, and selecting event type(s).

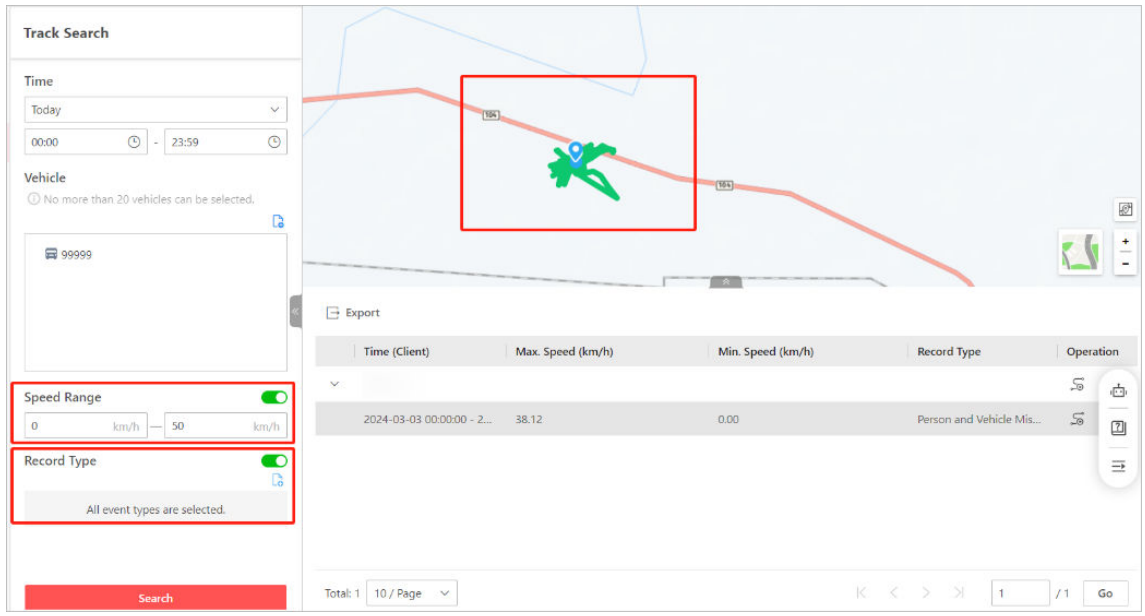


Figure 7-22 Track Search

How to search for driving events?

1. On the Driving Event Search page, you can search for the vehicle-triggered events by specifying a time period, selecting vehicle(s), and selecting event type(s).

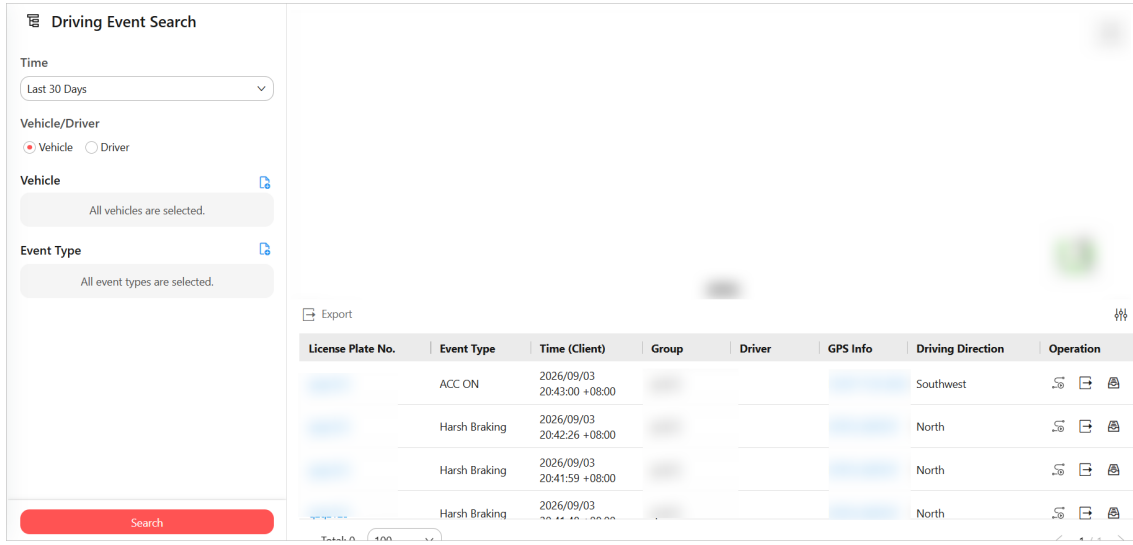
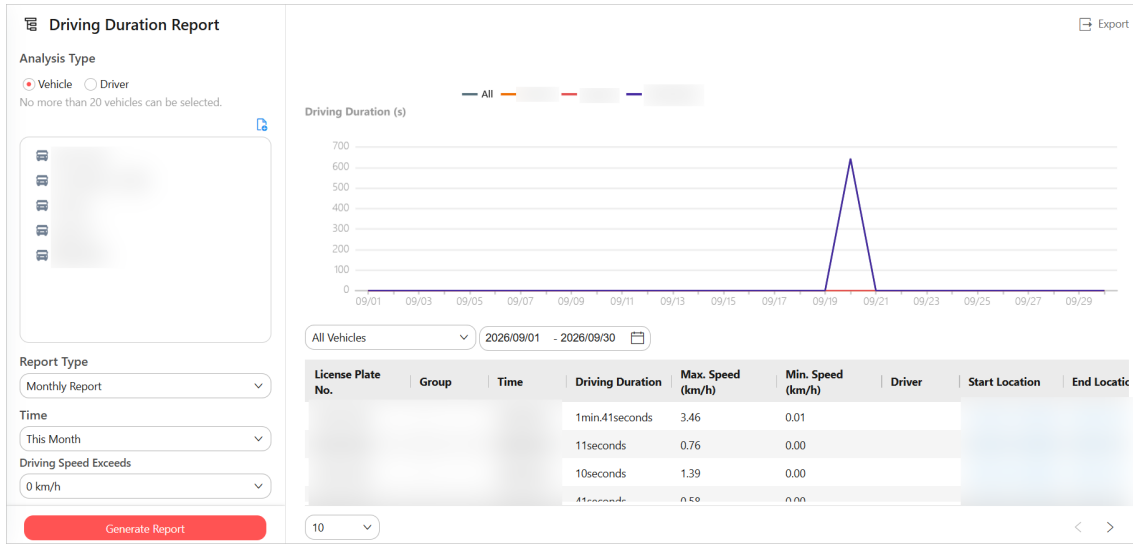


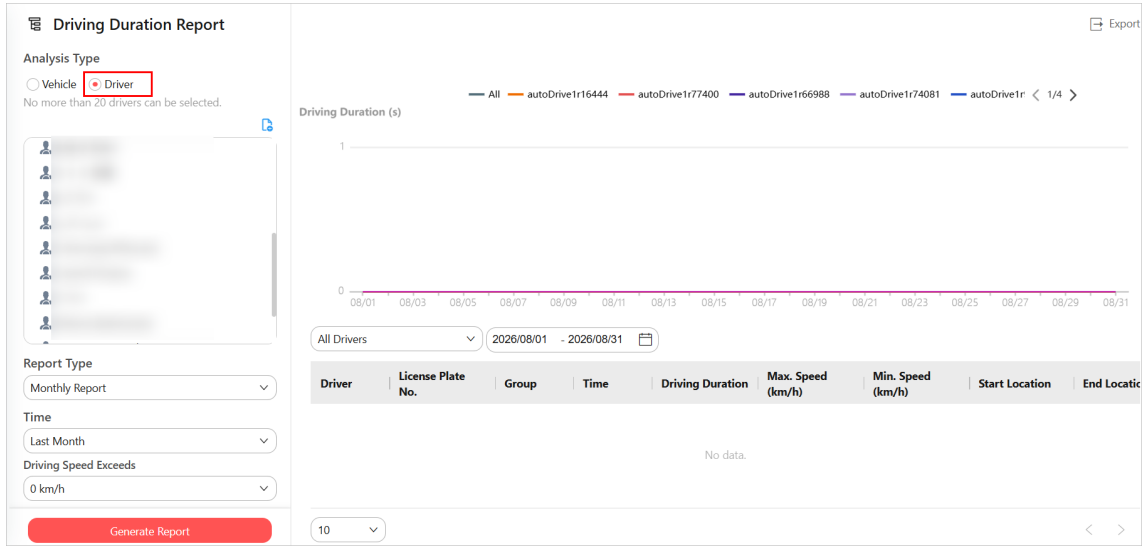
Figure 7-23 Driving Event Search

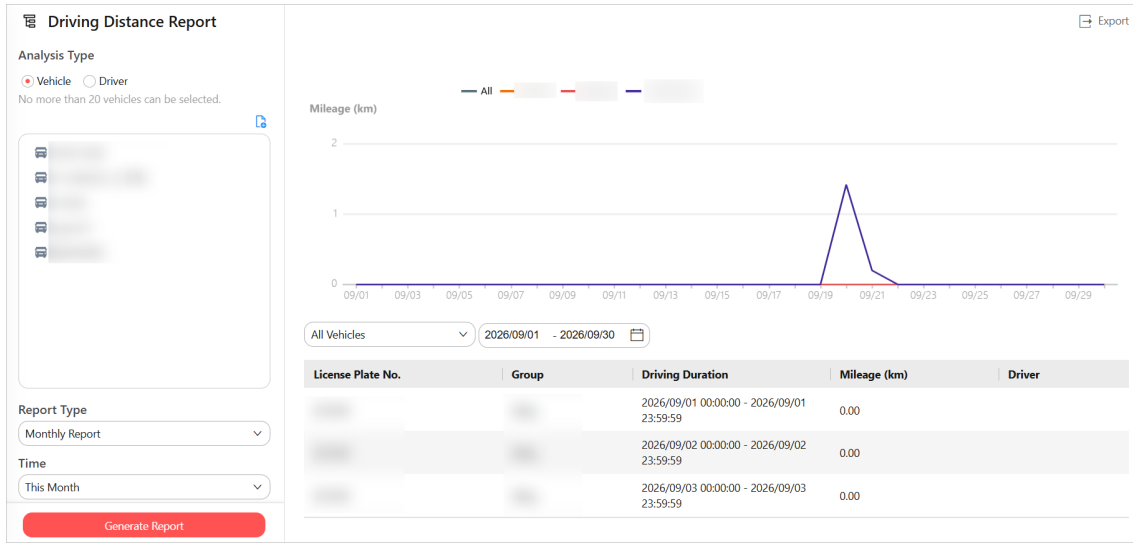
2. You can also search for vehicle-triggered events by specifying a time period, selecting drivers, and selecting event types.

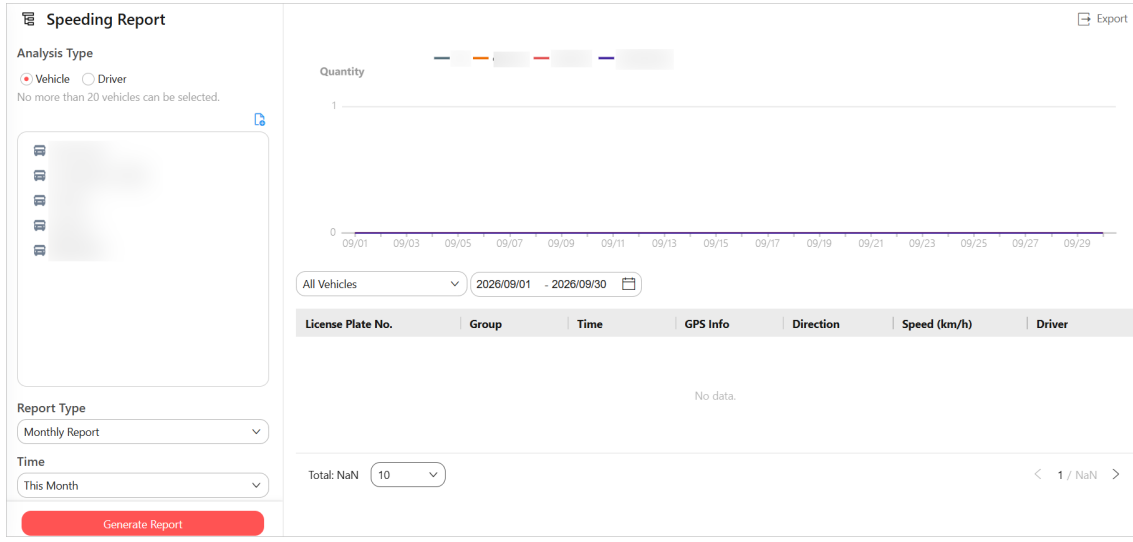
How to generate statistics and reports?

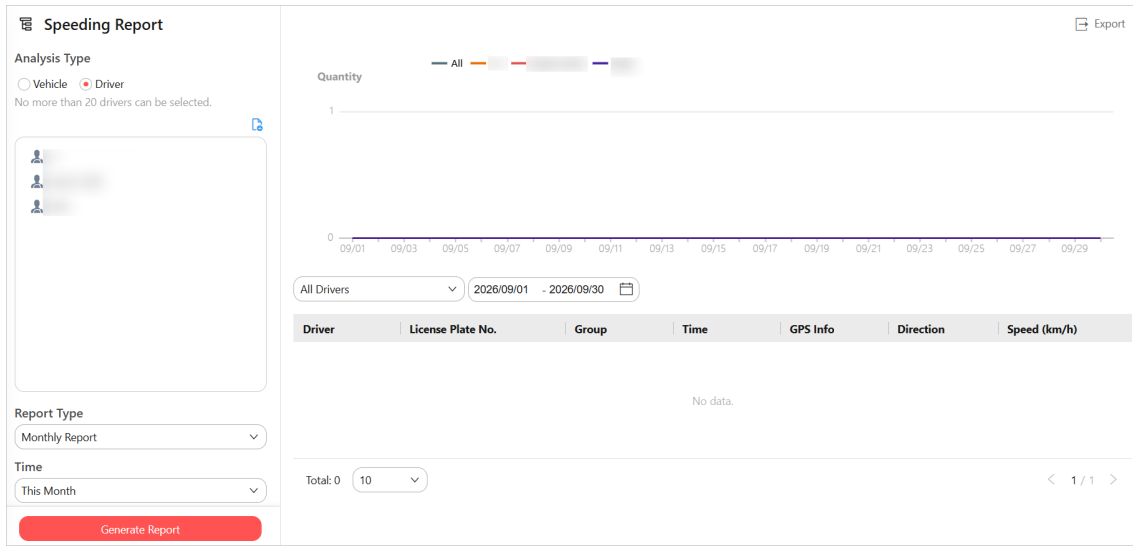
Go to → **On-Board Monitoring → Statistics and Reports** .
You can generate various types of driving data reports by selecting vehicles or drivers, including driving time reports, driving distance reports, speeding reports, and driving event reports. Supports exporting reports in CSV or XLSX format.

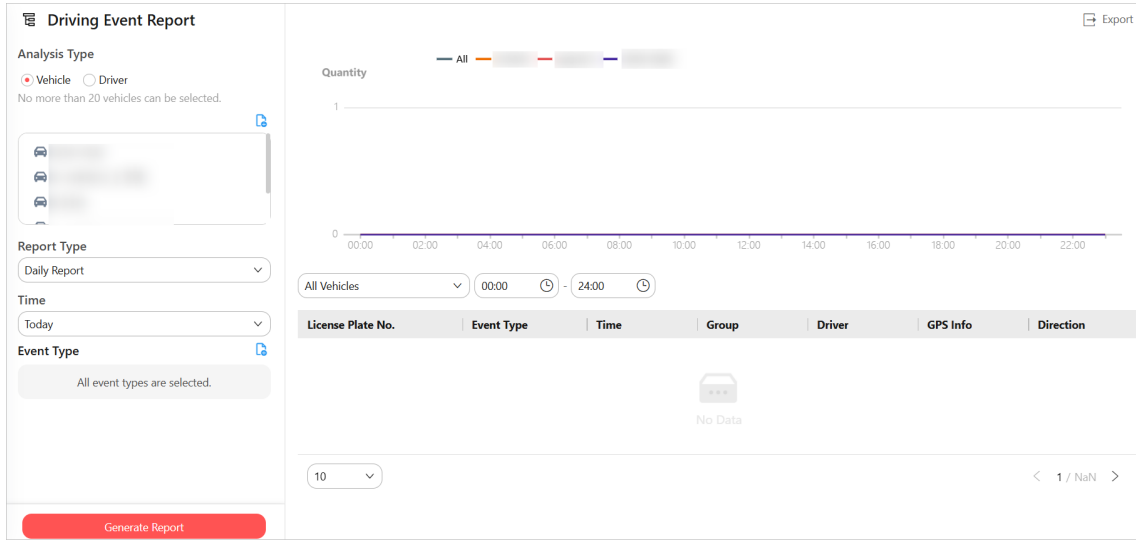


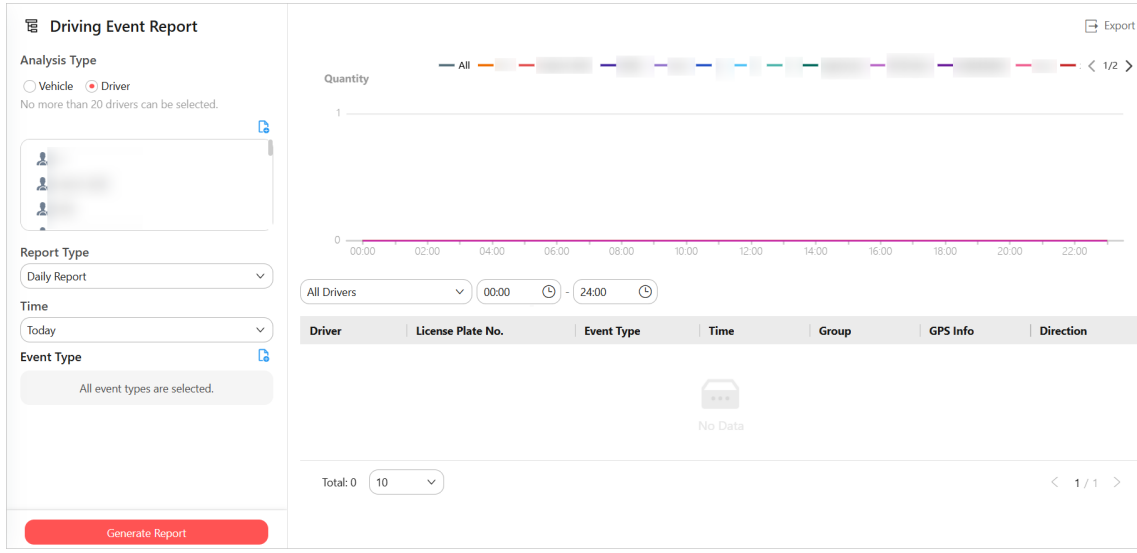

Driving Duration Report
Analysis Type
Vehicle
Driver
No more than 20 drivers can be selected.
Report Type
Monthly Report
Time
Last Month
Driving Speed Exceeds
0 km/h
Generate Report
Export
All
autoDrive1r16444
autoDrive1r77400
autoDrive1r66988
autoDrive1r74081
autoDrive1r
1/4
Driving Duration (s)
All Drivers
2026/08/01 - 2026/08/31
Driver
License Plate No.
Group
Time
Driving Duration
Max. Speed (km/h)
Min. Speed (km/h)
Start Location
End Locatic
No data.
10

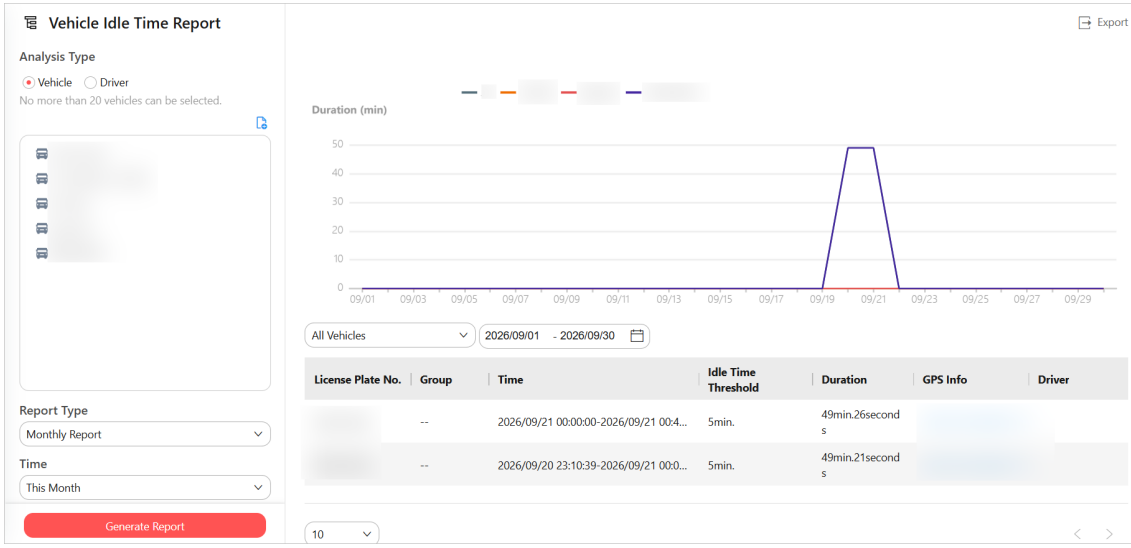

Driving Distance Report
Analysis Type
Vehicle
Driver
No more than 20 vehicles can be selected.
Report Type
Monthly Report
Time
This Month
Generate Report
Export
All
Mileage (km)
All Vehicles
2026/09/01 - 2026/09/30
License Plate No.
Group
Driving Duration
Mileage (km)
Driver
2026/09/01 00:00:00 - 2026/09/01 23:59:59
0.00
2026/09/02 00:00:00 - 2026/09/02 23:59:59
0.00
2026/09/03 00:00:00 - 2026/09/03 23:59:59
0.00


Speeding Report
Analysis Type
Vehicle
Driver
No more than 20 vehicles can be selected.
Report Type
Monthly Report
Time
This Month
Generate Report
Export
Quantity
1
0
09/01 09/03 09/05 09/07 09/09 09/11 09/13 09/15 09/17 09/19 09/21 09/23 09/25 09/27 09/29
All Vehicles
2026/09/01 - 2026/09/30
License Plate No.
Group
Time
GPS Info
Direction
Speed (km/h)
Driver
No data.
Total: NaN
10
1 / NaN


Speeding Report
Analysis Type
Vehicle
Driver
No more than 20 drivers can be selected.
Report Type
Monthly Report
Time
This Month
Generate Report
Export
All
Quantity
1
0
09/01 09/03 09/05 09/07 09/09 09/11 09/13 09/15 09/17 09/19 09/21 09/23 09/25 09/27 09/29
All Drivers
2026/09/01 - 2026/09/30
Driver
License Plate No.
Group
Time
GPS Info
Direction
Speed (km/h)
No data.
Total: 0
10
1 / 1


Driving Event Report
Analysis Type
Vehicle
Driver
No more than 20 vehicles can be selected.
Report Type
Daily Report
Time
Today
Event Type
All event types are selected.
Generate Report
Export
All
Quantity
1
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
All Vehicles
00:00
24:00
License Plate No.
Event Type
Time
Group
Driver
GPS Info
Direction
No Data
10
1 / NaN


Driving Event Report
Analysis Type
Vehicle
Driver
No more than 20 drivers can be selected.
Report Type
Daily Report
Time
Today
Event Type
All event types are selected.
Generate Report
Export
All
1/2
Quantity
1
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
All Drivers
00:00
24:00
Driver
License Plate No.
Event Type
Time
Group
GPS Info
Direction
No Data
Total: 0
10
1 / 1



How to perform remote upgrade?

Go to → **Device** → **Firmware Upgrade** . If the device has a new version push, you can upgrade remotely on the platform without needing to be at the local end of the vehicle device, which is more convenient.

7.5 How to set alarms for on-board devices?

Refer to ***Alarms*** for details.

Chapter 8 Intrusion Protection

After adding an alarm device to the Portal, you need to group the device's alarm inputs into areas for management. You also need to set an arming schedule for the alarm inputs in a security control area which defines when and how to arm the alarm inputs in this area. When alarms are triggered, the alarm information will be uploaded to the System to remind the security personnel to handle related issues.

8.1 Add Alarm Devices and Import Areas

Table 8-1 Add Alarm Devices and Import Areas

Type	Step
Add Alarm Devices	***Device Management***
Import Areas from Device	Click → **Intrusion** → **Area Management** to go to the Area Management page. Select a device from the list on the left and Click + to display the Add Area pane.

8.2 Perform Arming Control for Resources

After importing the areas configured on the device to the System, you can perform further operations, including configuring arming schedules for the areas, arming/disarming areas, bypassing zones, clearing alarms, etc.

Operations	Descriptions
Edit Security Control Area	Click the name of an area to display its details and then edit its name or set the arming schedule for it. **Note** For the area of AX security control panel, you cannot edit the arming schedule via the System. Only editing the schedule on the device is supported.
Delete Security Control Area	Select one or multiple areas and click .
Bypass/Restore Zone	Click › to expand the area details, and click **Bypass** / **Bypass Restored** to bypass/restore the zone.

Operations	Descriptions
	Note When some exceptions occur in one zone while other zones can work normally, you can bypass the zone with exceptions to turn off the protection of it. Otherwise, you cannot arm the security control area which the zone belongs to. You can also recover the zone that is bypassed to make it work normally.
Arm/Disarm Security Control Area	Select one or multiple areas and click / to arm the areas in Stay Arming / Away Arming mode, or click to disarm them. **Note** • After arming the areas, the System can receive the alarms triggered in the areas. • **Away Arming**: If all people in the detection area are going to leave, turn on this mode to arm all zones in the area after the defined dwell time. • **Stay Arming**: It is used when people stay inside the detection area. Turn on this mode to turn on all the perimeter burglary detectors (such as perimeter detectors, magnetic contacts, curtain detectors in the balcony). Meanwhile, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarms will not be triggered.
Clear Alarms	Select one or multiple areas and click to clear the triggered alarms.
Add Area on Map	Select an area and click to add it on the map.

Chapter 9 Analysis Report

By subscribing to the analysis report service, you can check reports that contain informational and analytical data about a site (e.g., retail store, shopping mall, museum, etc.), which can be used as the basis for making decisions, addressing problems, and developing better operational strategies. A general report contains people counting and heat analysis related statistics of the specified time period (e.g., a day/week/month/year or a custom time range), and a promotion report can be used to check the effect of a promotion by comparing the statistics collected in the promotion period with those of 7 days before and after the promotion.

9.1 How to configure analysis report service?

This guide provides a step-by-step configuration process for setting up the Analysis Report service, which enables users to generate comprehensive reports containing people counting and heat analysis data for sites like retail stores, shopping malls, and museums. The table below outlines the configuration steps in logical order, with references to the corresponding concepts and menu paths for easy navigation.

1. ***Activate Analysis Report Service***
   - Activate the Analysis Report service through Hik-Partner Pro or Hik Connect for Teams portal to receive a three-month free trial for People Counting and Heat Analysis services.
   - Path: ⁞⁞ → **Service**
2. ***Configure Device Local Functions***
   - Configure People Counting and Heat Analysis functions on the device web interface before adding to Hik Connect for Teams. Note that both functions cannot be enabled on the same camera simultaneously.
   - **Example:** For camera model iDS-2CD7186G0, enable Multi-Dimensional People Counting and configure counting rules through the device's web configuration interface.
   - Path: **Device Web → Configuration**
3. ***Add Encoding Devices***
   - Configure platform access parameters on devices and add them to Hik Connect for Teams using the device serial number and verification code.
   - **Example:** Configure platform access settings on the device web interface, then add the device to Hik Connect for Teams using the 9-character serial number found on the device label.
   - Path: ⁞⁞ → **Device → Encoding Device**
4. ***Configure Analysis Settings***

- Set up basic analysis configuration including area selection, operating hours, geographic location, and contact information. Configure People Counting entrances/exits and Global Heat Map capabilities.
- **Example:** Create People Counting Entrance & Exit configurations, enable overcapacity pre-alarm, and link resource cameras to floor maps for heat analysis visualization.
- Path: ⁞⁞ → **Analysis Report → Configuration → Analysis Configuration**

5. ***Add Employee Face Picture Libraries***
   - Create employee face libraries to exclude staff from customer people counting statistics. Add employee faces to libraries and apply them in batches to target stores with compatible cameras.
   - **Example:** Set up face libraries for retail stores to accurately count only customer traffic by excluding recognized employee faces from the statistics.
   - Path: ⁞⁞ → **Analysis Report → Configuration → Employee Face Library**
6. ***Generate and View Reports***
   - Access comprehensive analysis reports including People Counting trends, entrance statistics, and Heat Analysis data for general periods or specific promotions.
   - **Example:** Generate weekly reports showing customer traffic patterns, peak hours, and heat distribution maps to optimize store layout and staffing.
   - Path: ⁞⁞ → **Analysis Report → Report**

9.2 How to activate analysis report service?

Activate the service through Hik-Partner Pro or Hik Connect for Teams.

- When creating a new Teams mode site on Hik-Partner Pro portal, select the Analysis Report service to receive a three-month free trial for People Counting and Heat Analysis services.
- Enable the Analysis Report on Hik Connect for Teams Portal. The initial activation includes a three-month trial period. After expiration, contact your service provider or purchase a license to continue using the service.

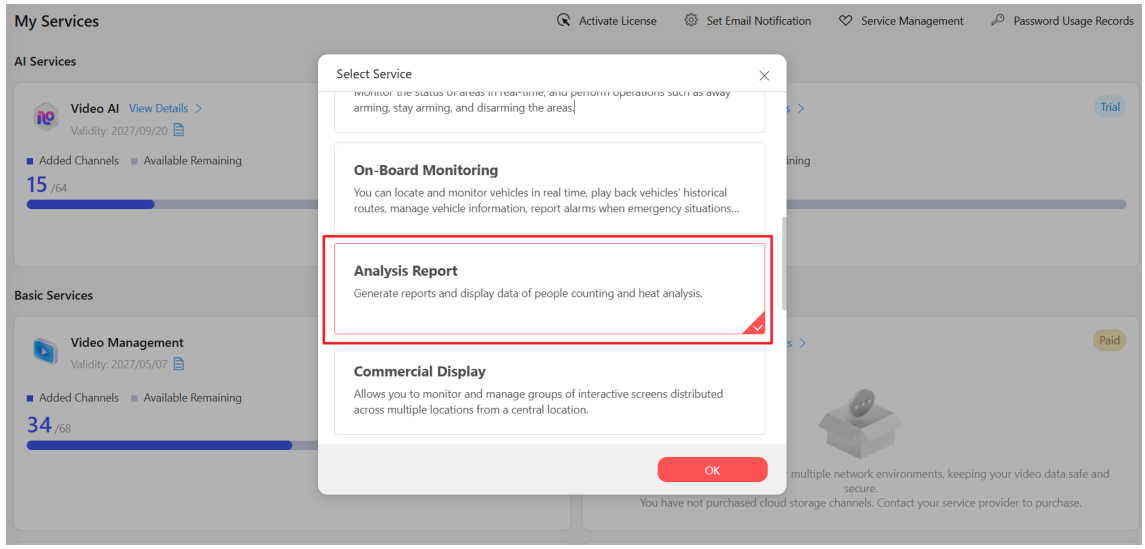


Figure 9-1 Activate Analysis Report from Hik-Partner Pro

9.3 How to configure devices for analysis report?

Configure devices locally and add them to Hik Connect for Teams.

9.3.1 How to configure device on web page?

Set up People Counting and Heat Analysis functions on device web interface.

How to configure people counting?

Configure People Counting and Heat Analysis functions on the device web interface before adding to Hik Connect for Teams.

Note

People Counting and Heat Analysis functions cannot be enabled on the same camera simultaneously. You need at least two cameras to use both services.

Configuration example for camera model iDS-2CD7186G0:

1. Enable Multi-Dimensional People Counting.

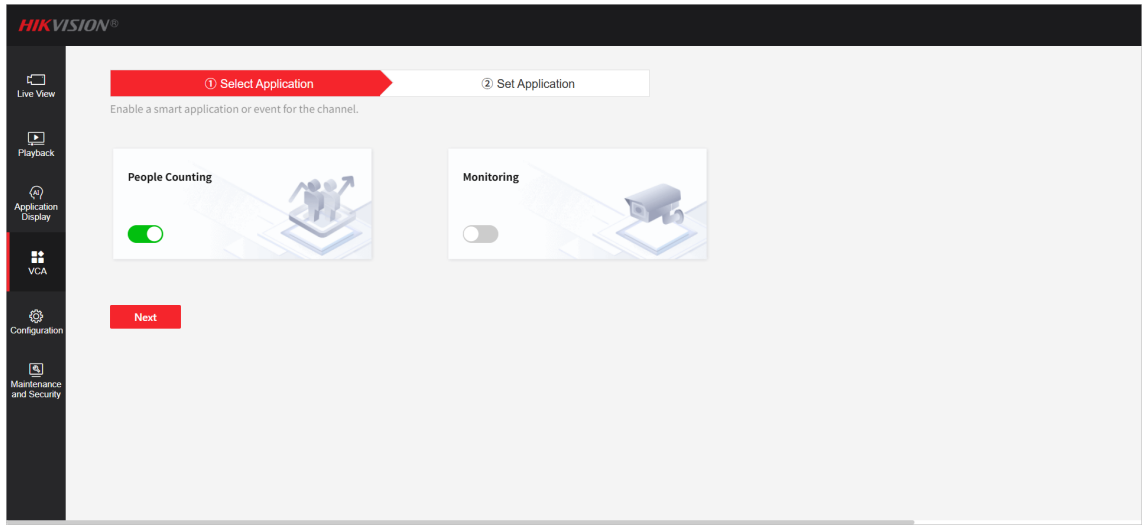
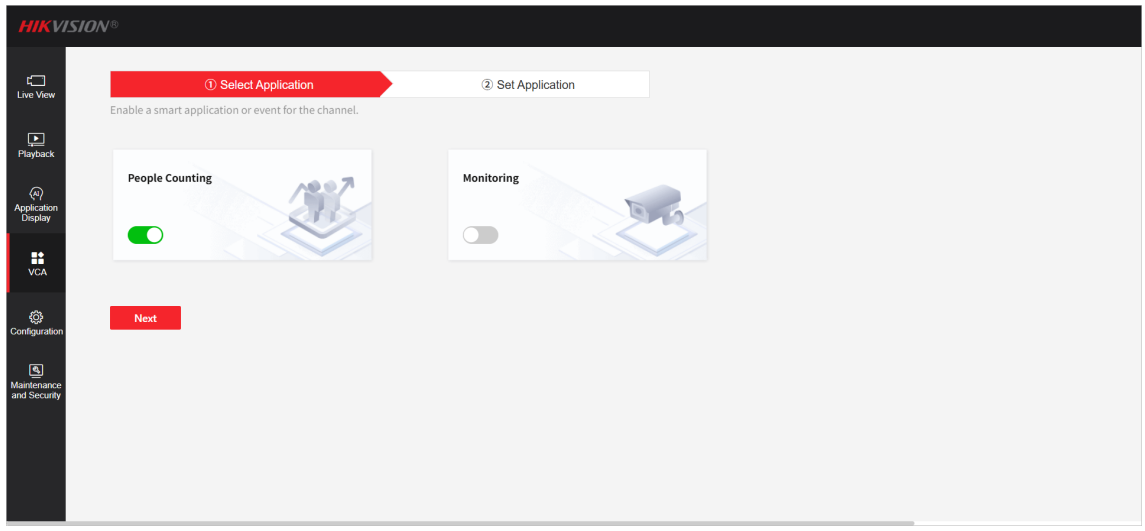
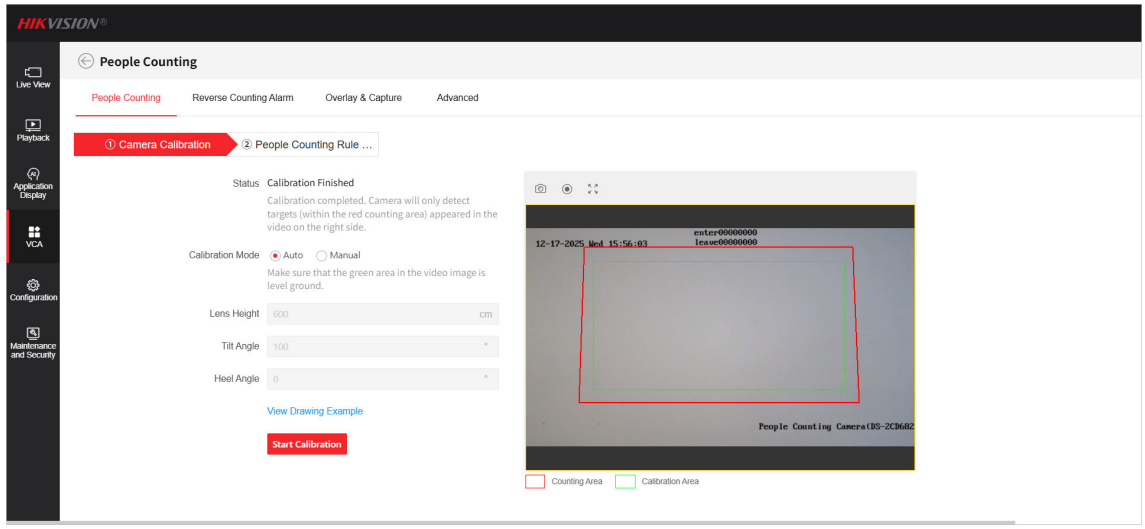


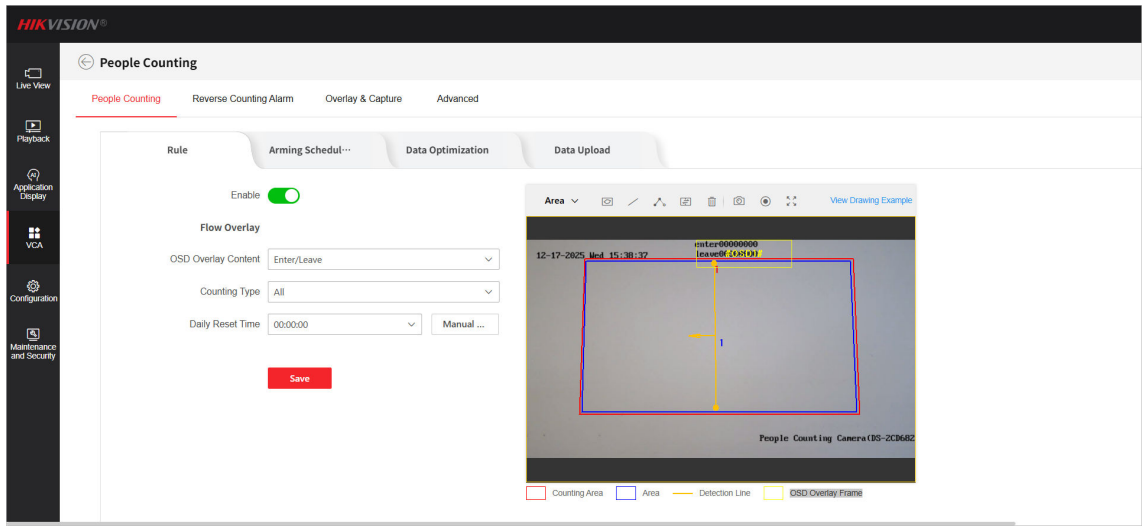
Figure 9-2 Enable People Counting Function

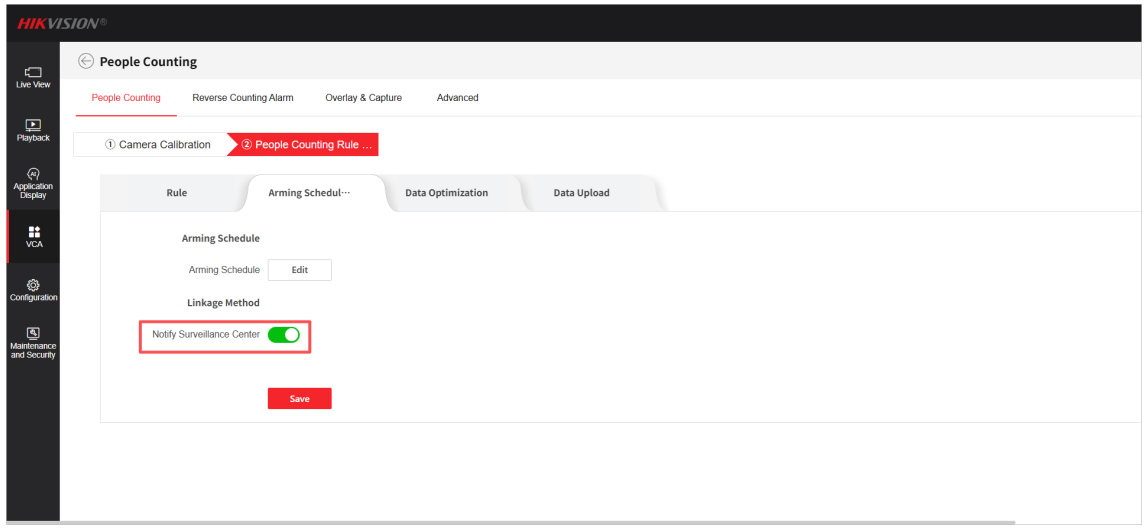
2. Configure the People Counting rules.

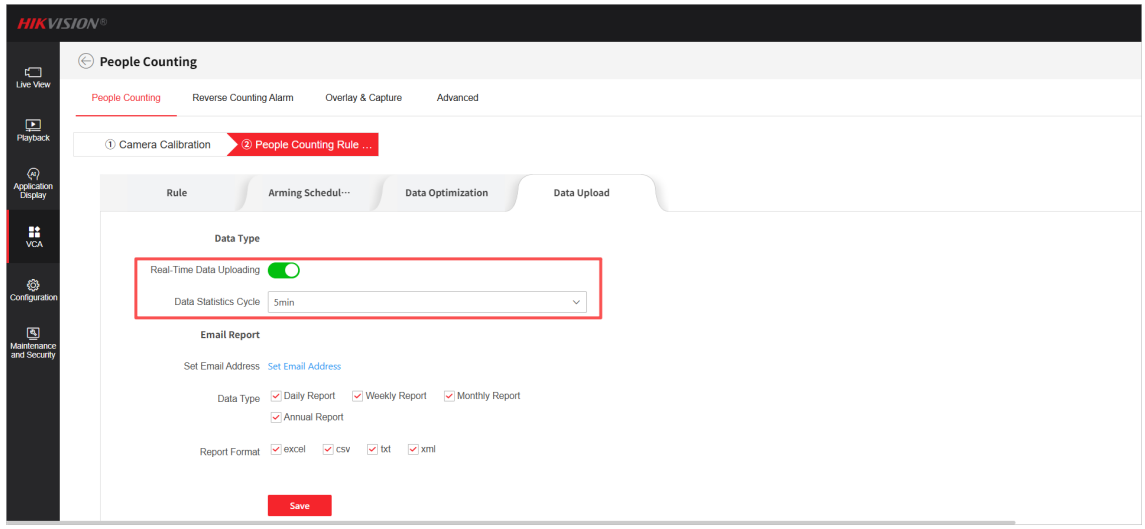




3. Set People Counting rules.







How to configure heat analysis?

1. Enter VCA and enable the People Management application.

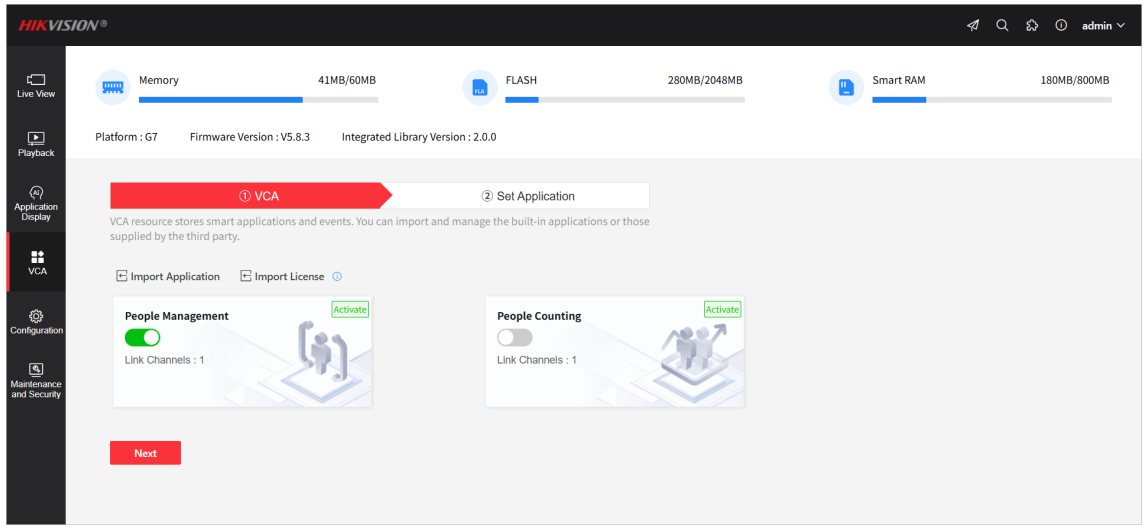
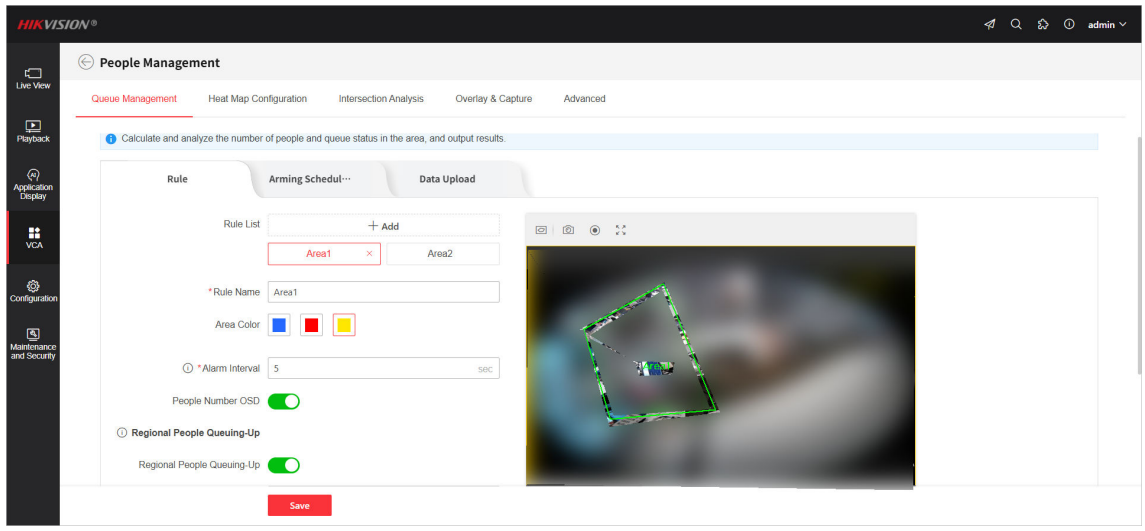
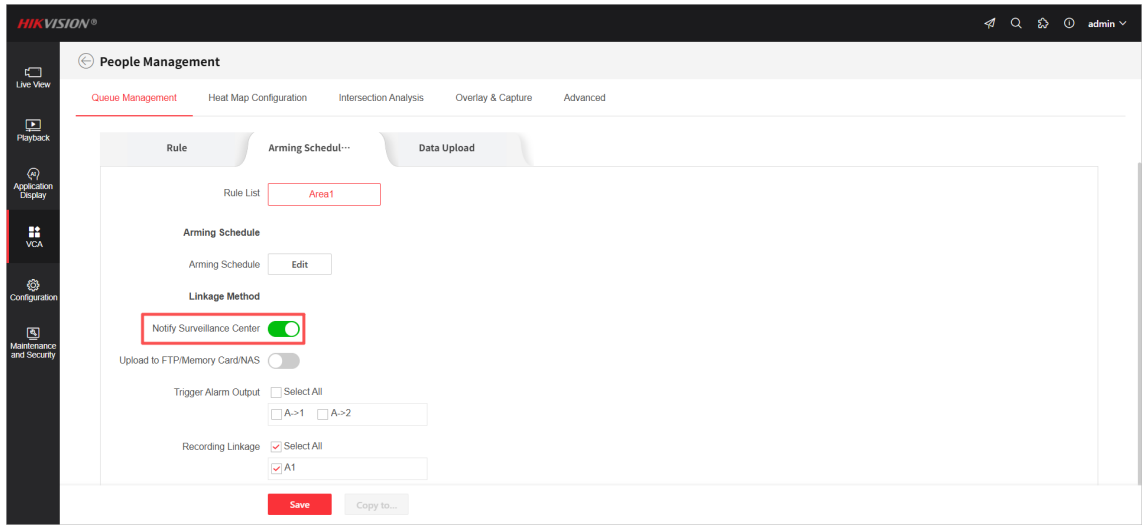
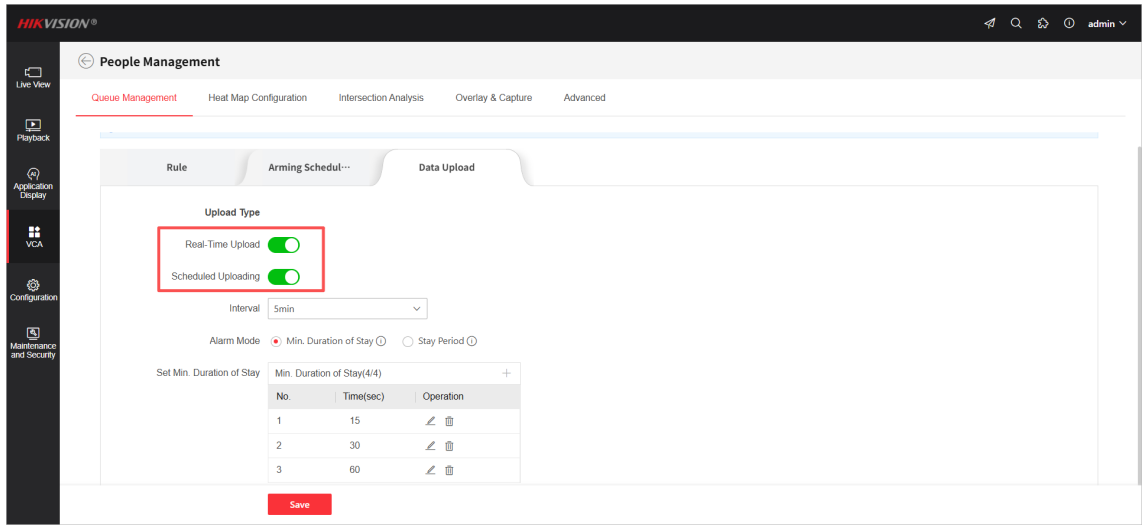


Figure 9-3 Enable Heat Analysis Application

2. Configure Queue Management.



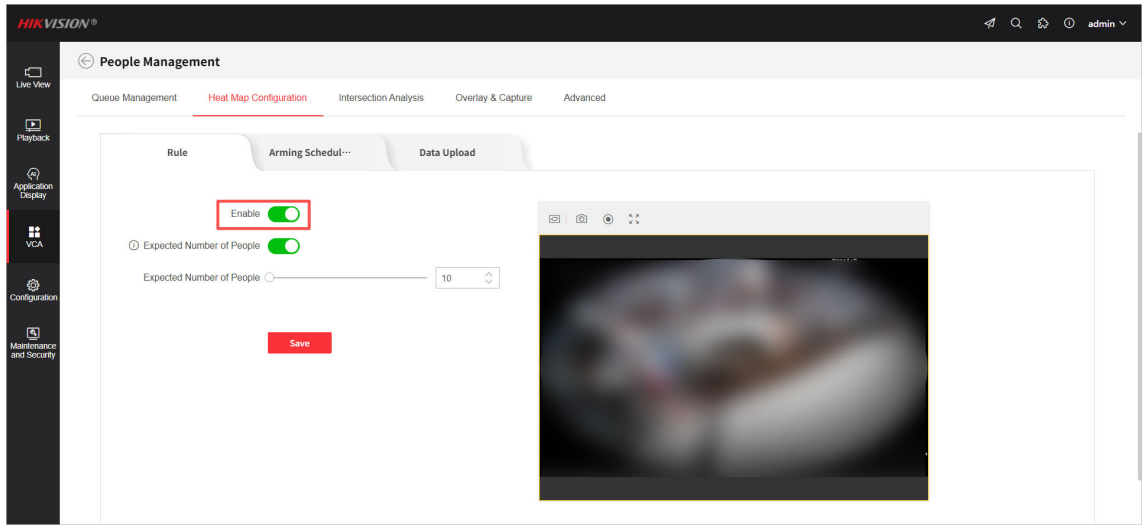


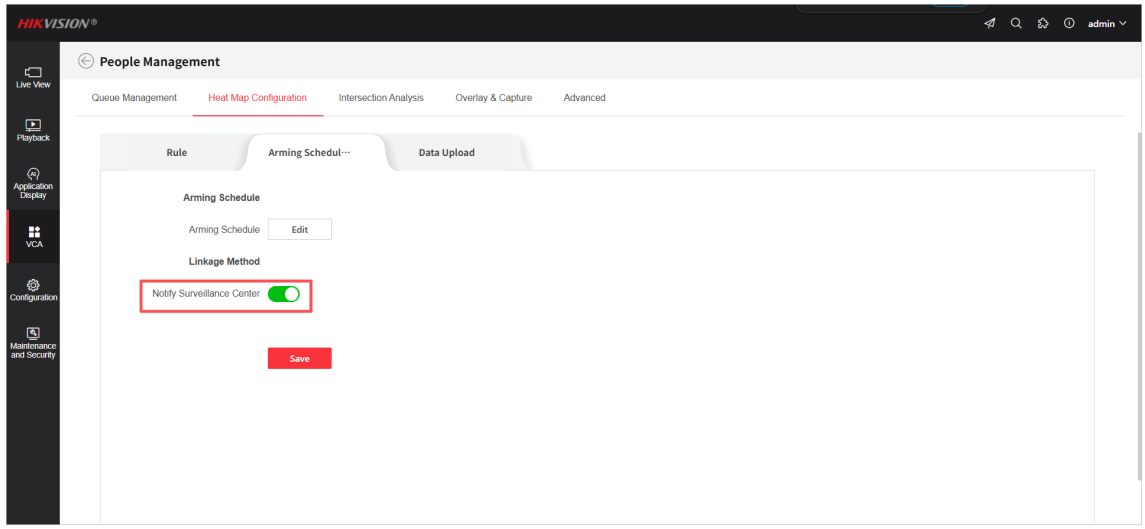


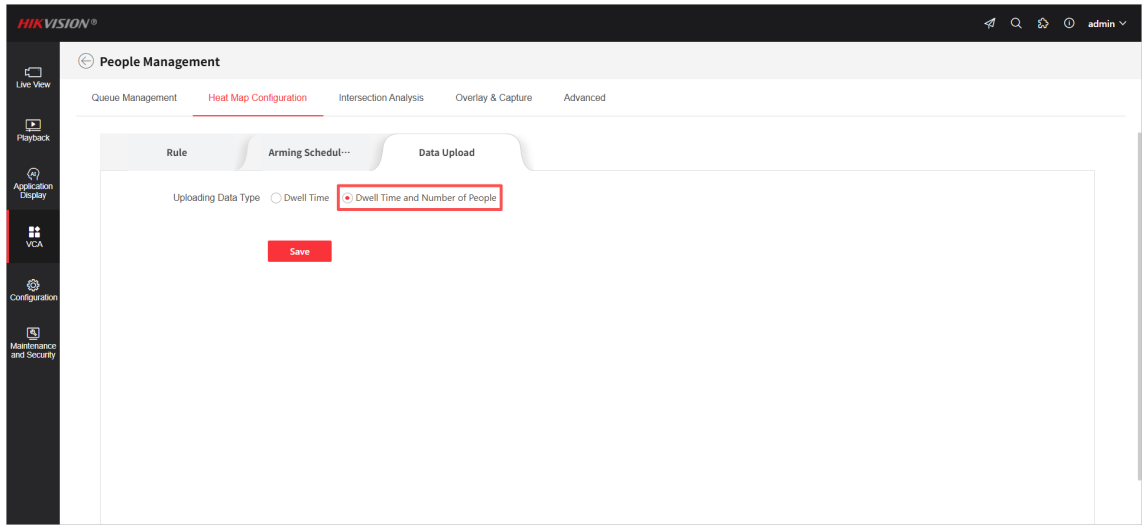
Note

- You can set zones for cameras to measure the total number of dwell people within a zone, dwell rate, and average dwell duration, etc.
- Each camera can add up to 8 zones.

3. Configure Heat Map Configuration.


HIKVISION
admin
Live View
Playback
Application Display
VCA
Configuration
Maintenance and Security
People Management
Queue Management
Heat Map Configuration
Intersection Analysis
Overlay & Capture
Advanced
Rule
Arming Schedul···
Data Upload
Enable
Expected Number of People
Expected Number of People
10
Save


HIKVISION
admin
Live View
Playback
Application Display
VCA
Configuration
Maintenance and Security
People Management
Queue Management
Heat Map Configuration
Intersection Analysis
Overlay & Capture
Advanced
Rule
Arming Schedul···
Data Upload
Arming Schedule
Arming Schedule
Edit
Linkage Method
Notify Surveillance Center
Save

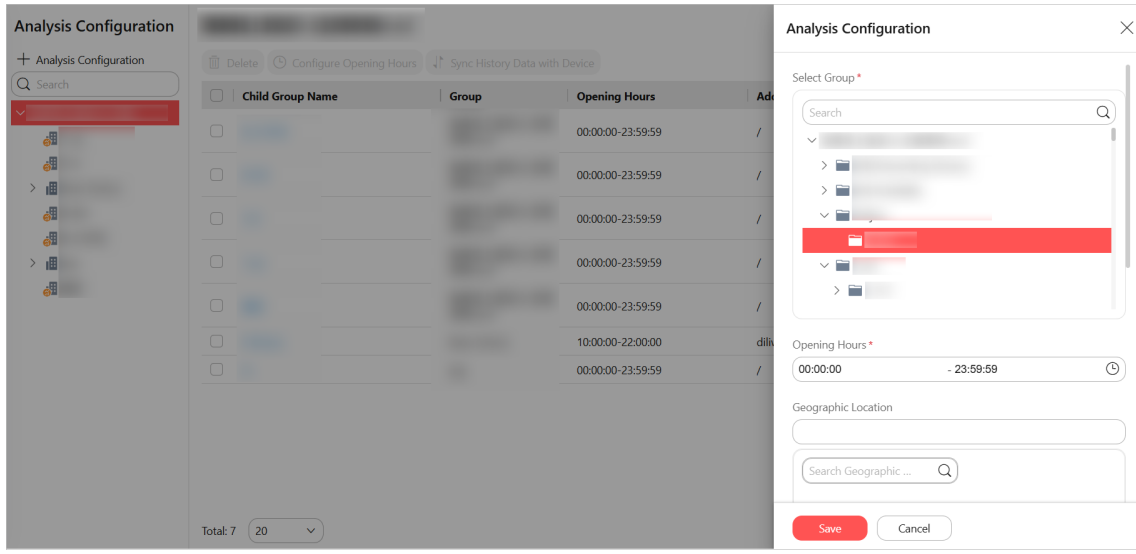


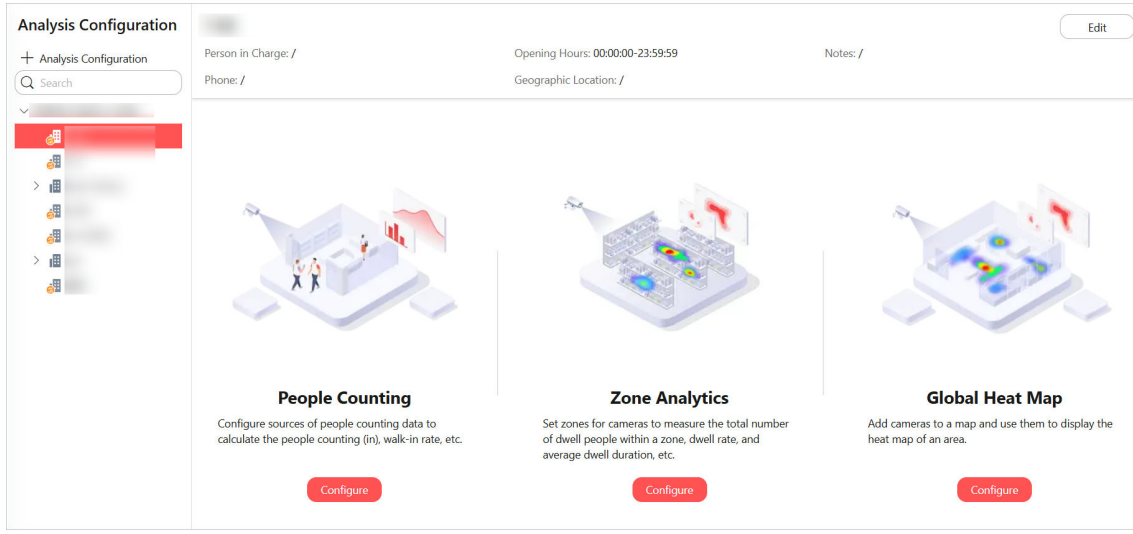
9.4 How to add encoding devices to Hik Connect for Teams?

Refer to ***Device Management*** .

9.5 How to add analysis configuration?

Add Analysis Configuration: Select area, set opening hour, set the geographic location, set person in charge, set phone, and enter notes.





How to configure people counting analysis capability?

1. Click **Configure** under the People Counting page to enter the Analysis Capability Configuration page of People Counting.
2. Click **Add** to add People Counting Entrance & Exit, enter the Entry & Exit Name, and select camera resources as People Counting Camera(In) and People Counting Camera (Passby).

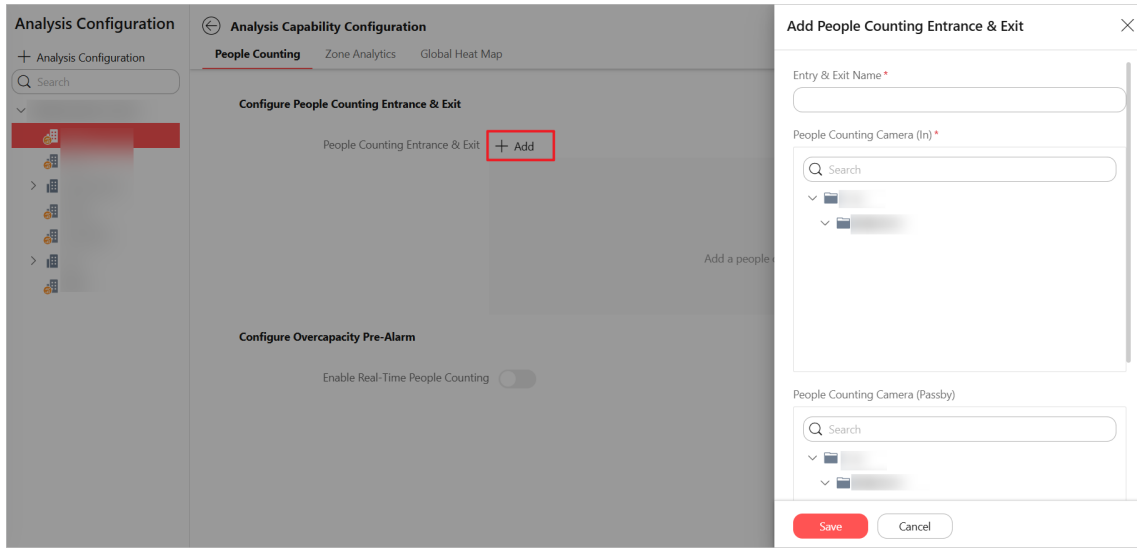


Figure 9-4 Configure People Counting Entrance & Exit

3. Enable **Used as Source of Regional People Counting Data**, and click **Save**.
4. You can also Configure Overcapacity Pre-Alarm after enabling Real-Time People Counting.

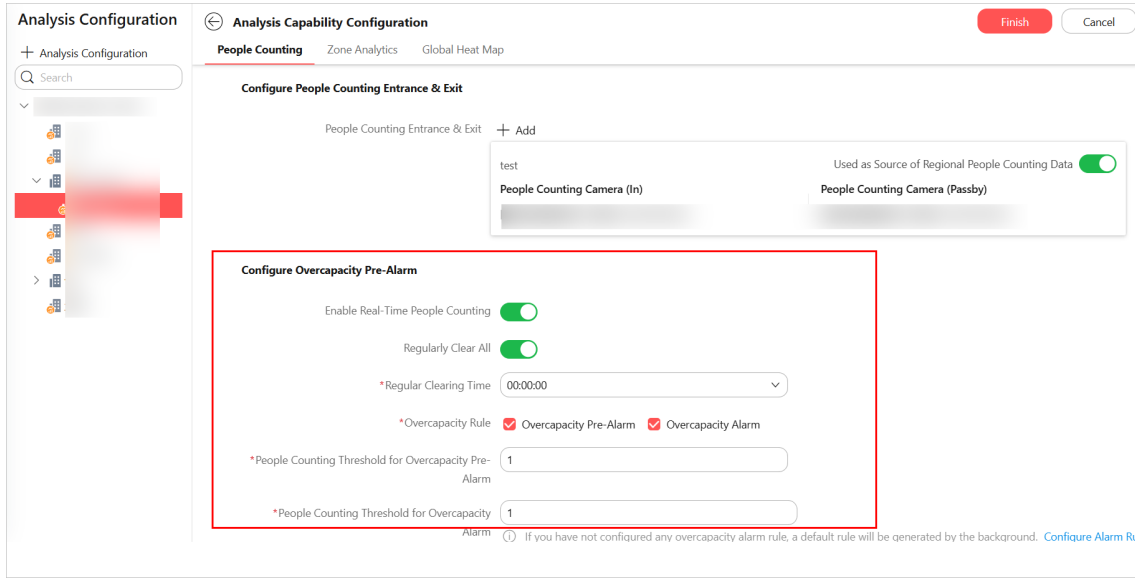
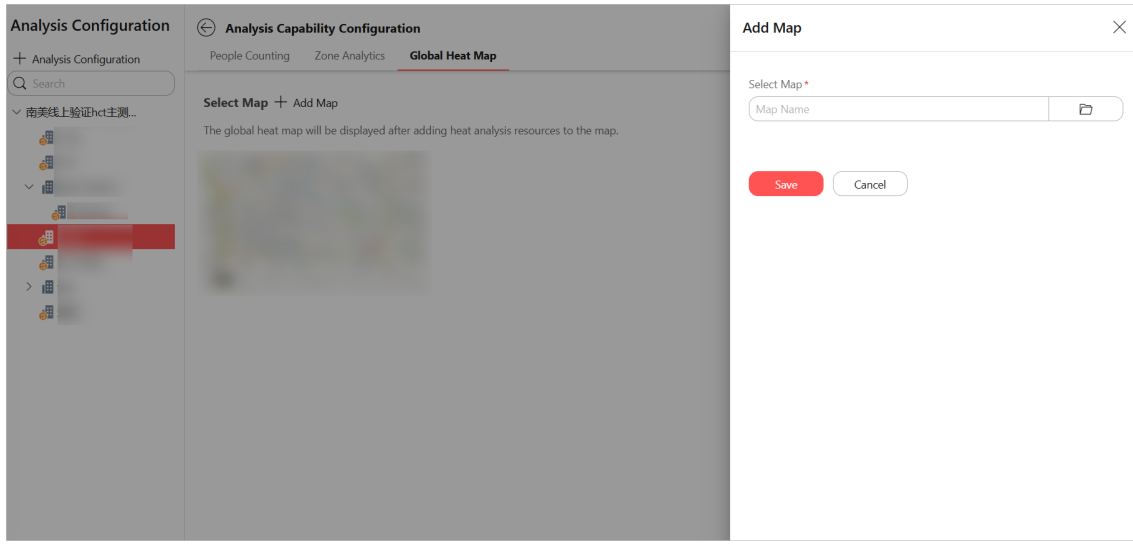


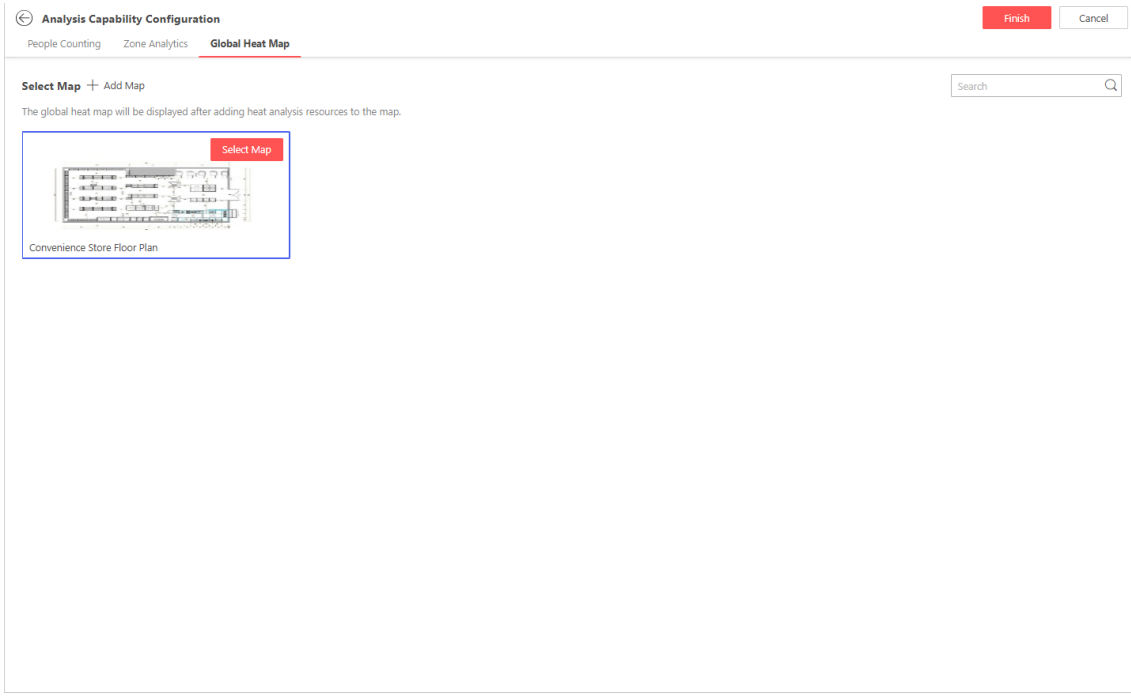
Figure 9-5 Configure Overcapacity Pre-Alarm

5. Click **Finish** to save the configuration.

How to configure global heat map analysis capability?

1. Click **Configure** under the Global Heat Map to enter the Analysis Capability Configuration page of Global Heat Map.





2. You can add a Map from the local folder on your computer.

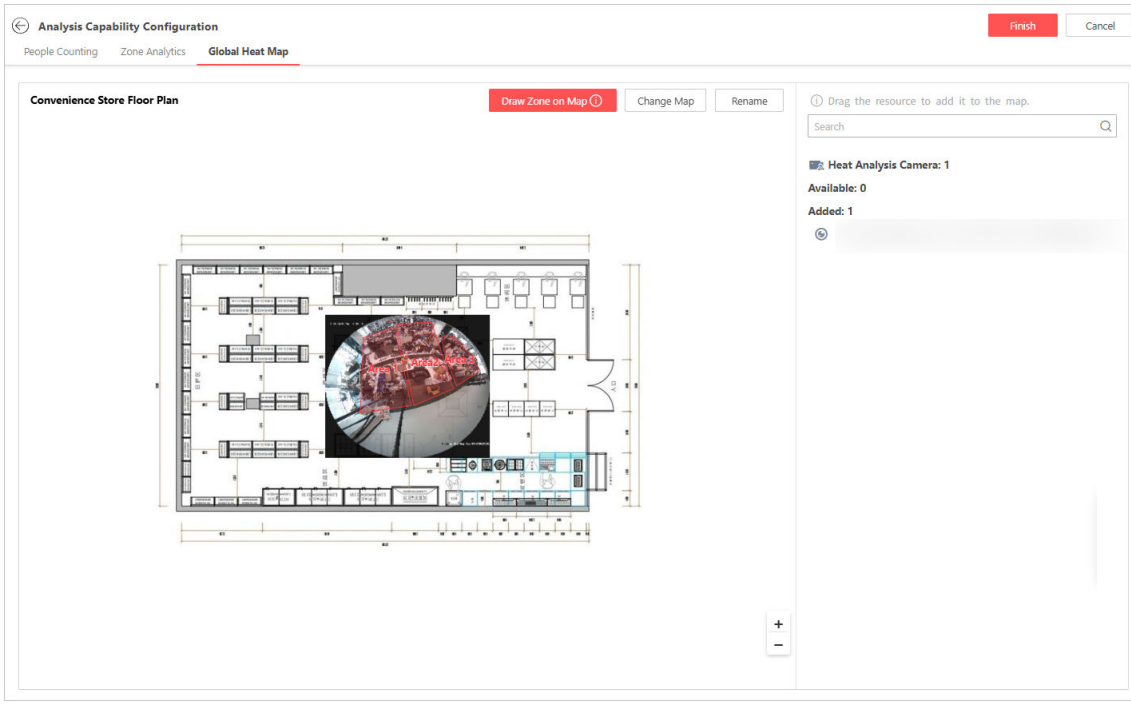


Figure 9-6 Add the Cameras on the Map

3. After adding a map, you can select the added map to link the cameras and add them to the map.

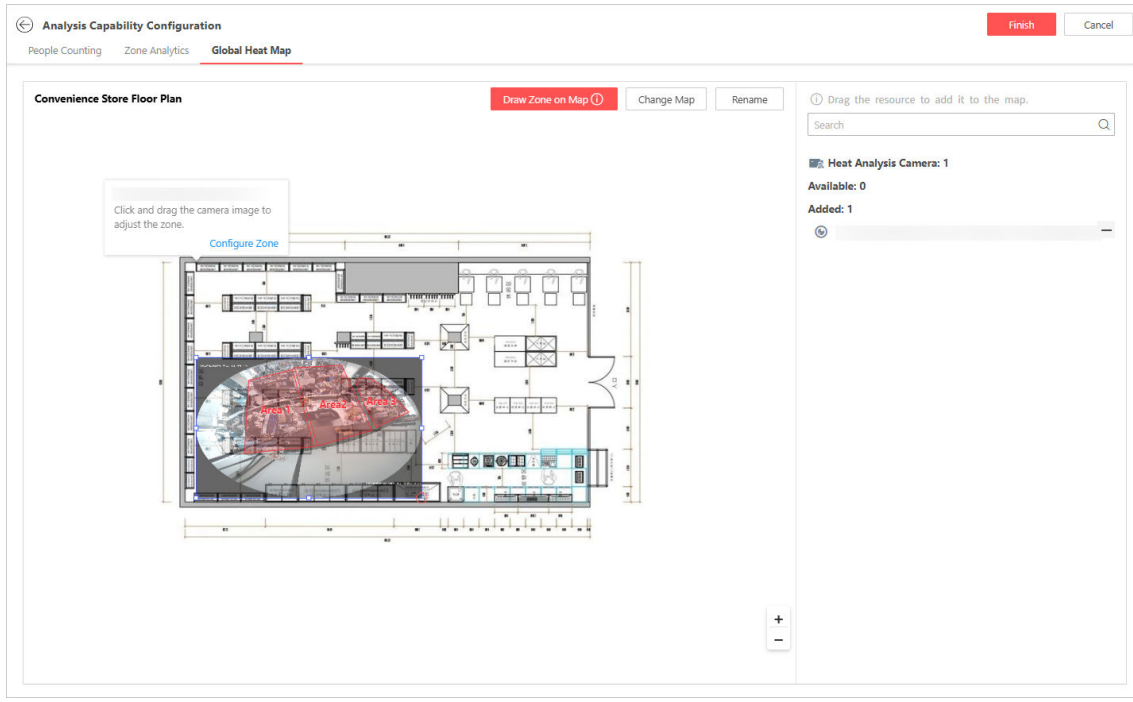


Figure 9-7 Configure Zone on the map

4. You can click and drag the camera image to adjust the zone.
5. You can also draw zone directly on the map and adjust its location and shape.

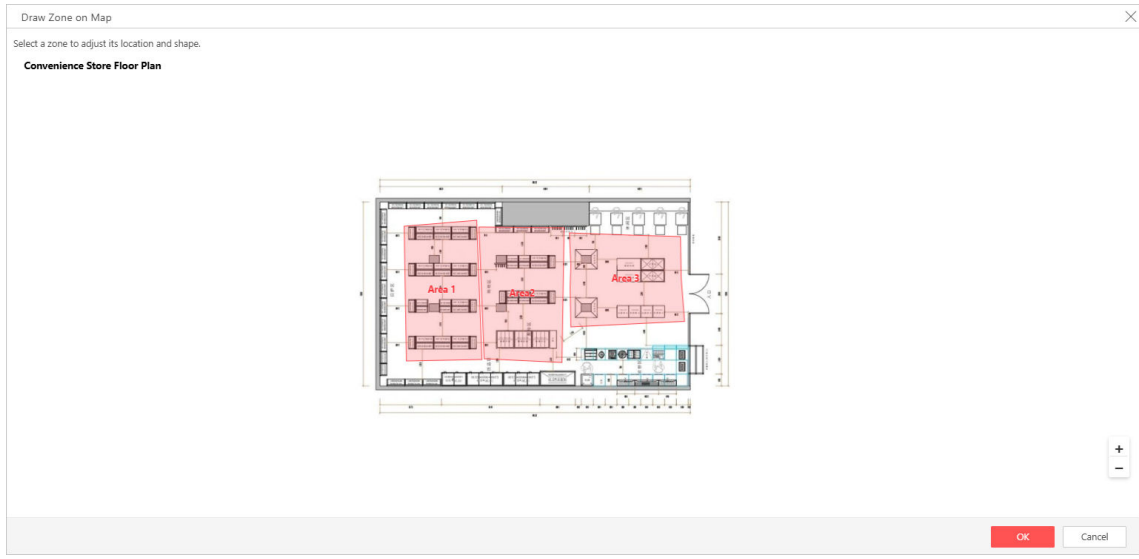


Figure 9-8 Adjust Zone on the map

6. You can check the Health Status after configuring Analysis Configuration.

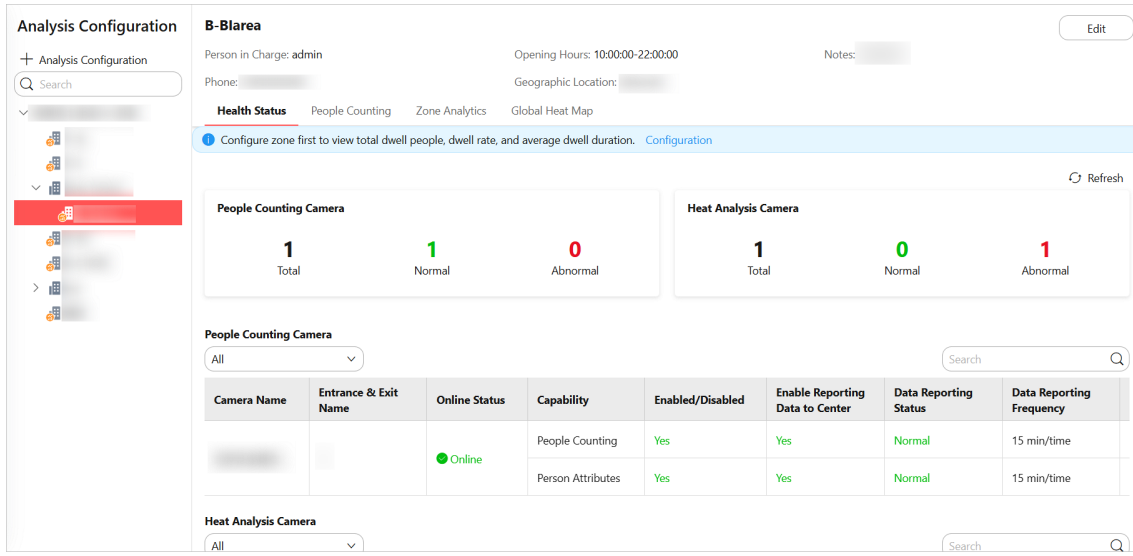
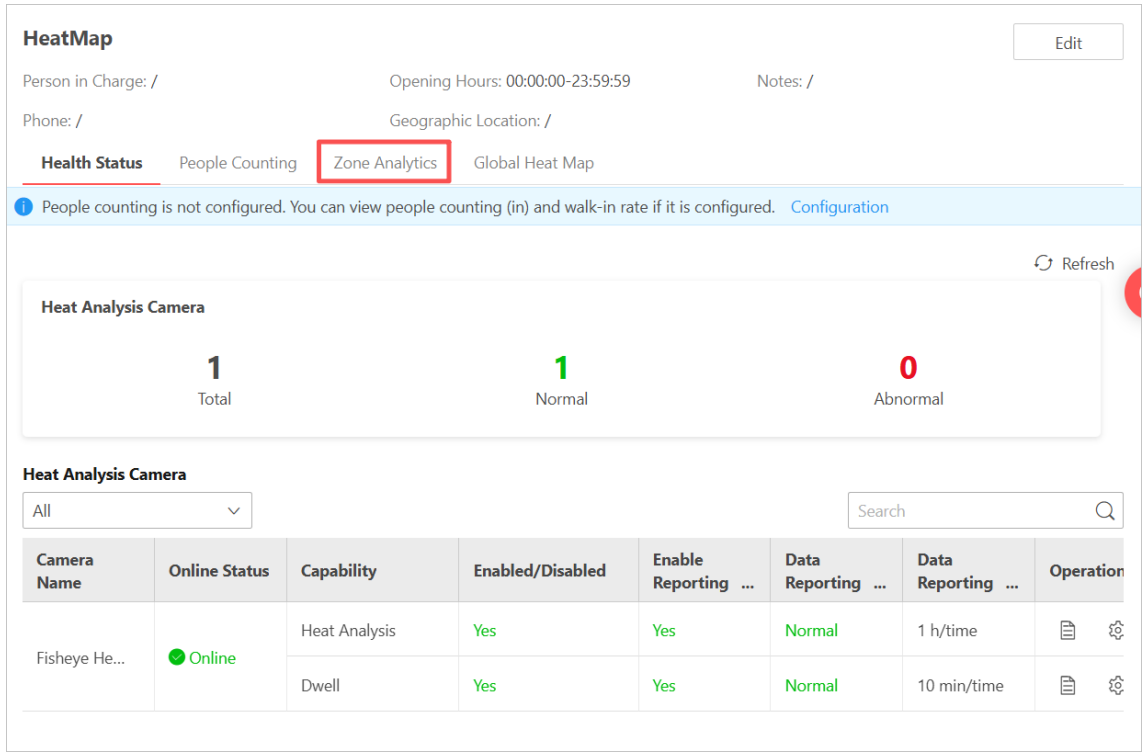
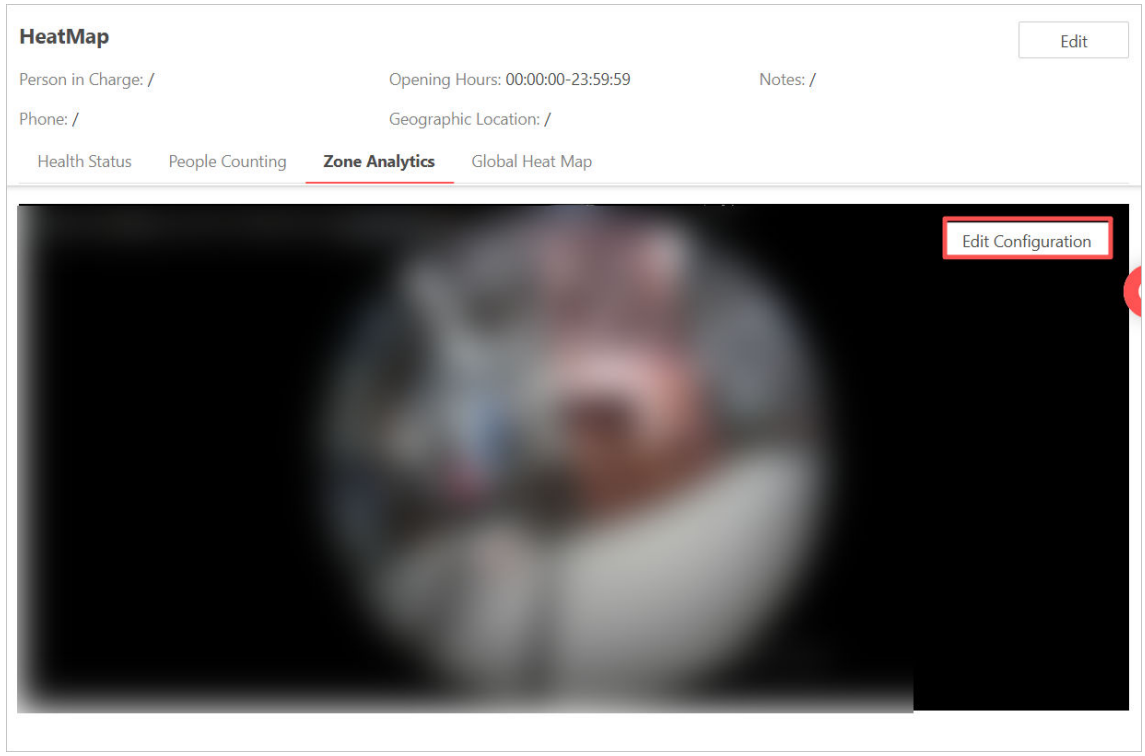


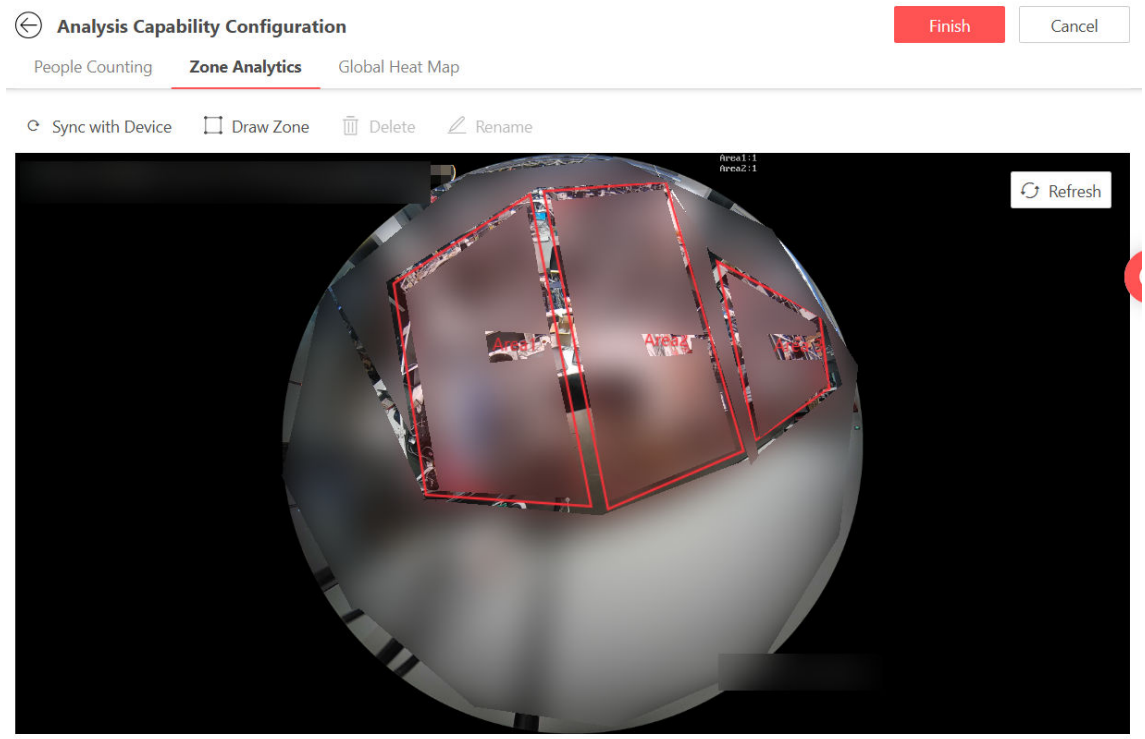
Figure 9-9 Check the Health Status

How to configure zone analytics analysis capability?

1. Click **Configure** under Zone Analytics page to enter the Zone Analytics Configuration page.
2. Click **Edit Configuration** to edit the Zone Analytics, you can **Sync with Device** or **Draw Zone** directly on the picture.
3. Click **Finish** to save the configuration.


HeatMap
Edit
Person in Charge: /
Opening Hours: 00:00:00-23:59:59
Notes: /
Phone: /
Geographic Location: /
Health Status
People Counting
Zone Analytics
Global Heat Map
People counting is not configured. You can view people counting (in) and walk-in rate if it is configured. Configuration
Refresh
Heat Analysis Camera
1
Total
1
Normal
0
Abnormal
Heat Analysis Camera
All
Search
Camera Name
Online Status
Capability
Enabled/Disabled
Enable Reporting ...
Data Reporting ...
Data Reporting ...
Operation
Fisheye He...
Online
Heat Analysis
Yes
Yes
Normal
1 h/time
Dwell
Yes
Yes
Normal
10 min/time


HeatMap
Edit
Person in Charge: /
Opening Hours: 00:00:00-23:59:59
Notes: /
Phone: /
Geographic Location: /
Health Status
People Counting
Zone Analytics
Global Heat Map
Edit Configuration



Note

Please note that each camera can draw a maximum of 8 zones, and each zone can draw a maximum of 10 edges. If more than 10 edges are drawn, clicking Finish will result in an error.

How to configure promotion settings?

Click **Add** under the Promotion Configuration page to add a promotion. Enter the Promotion Name and select Promotion Period to finish configuration.

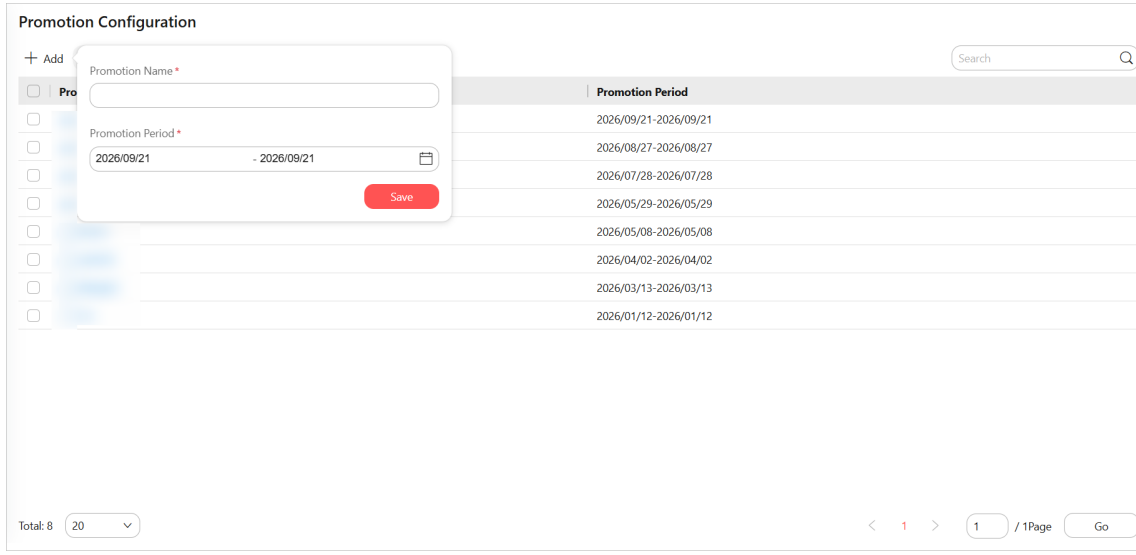


Figure 9-10 Promotion Configuration

How to configure scheduled reports?

After configuring the analysis configuration and promotion configuration, you can also set up scheduled report, customize the report name, language, select the stores, and set the report schedule. The reports can be sent according to specific time dimensions such as daily, weekly, and monthly. You can also add up to 10 recipients in the Email Settings.

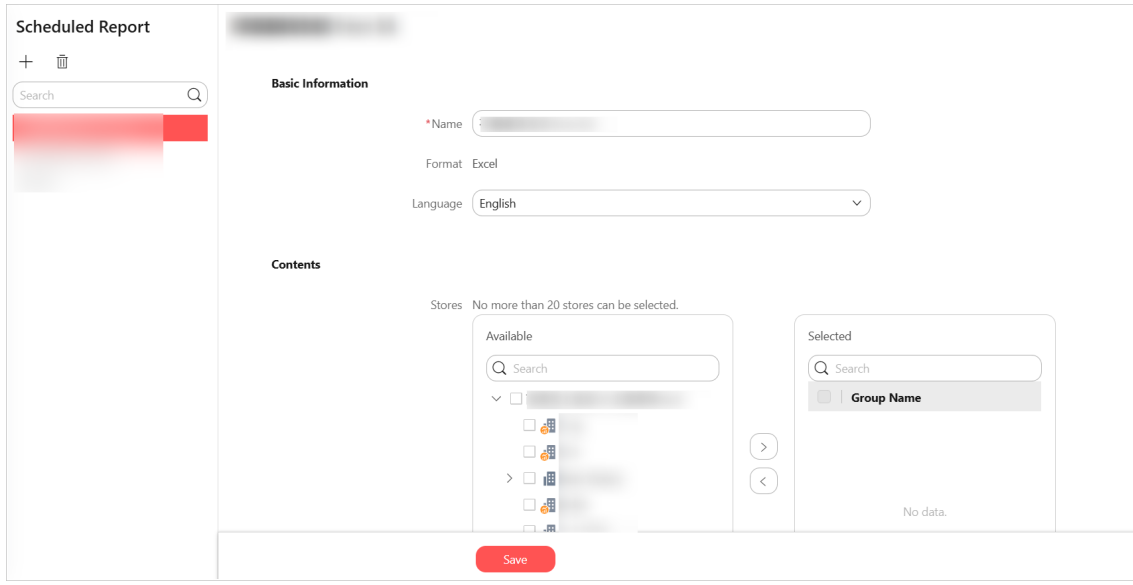


Figure 9-11 Configure Schedule Report

Note

- The schedule report supports up to 40 languages.
- The schedule report format currently only supports Excel.

9.6 How to add employee face picture libraries?

1. Go to **Analysis Report → Configuration → Employee Face Library** .
2. You can add employee face libraries to exclude staff from customer people counting statistics, and add employee faces to the employee face libraries.
3. Select target stores with compatible cameras, and apply faces in batches.
4. The system automatically retries failed applying (3 attempts) and you can manually retry for specific stores.

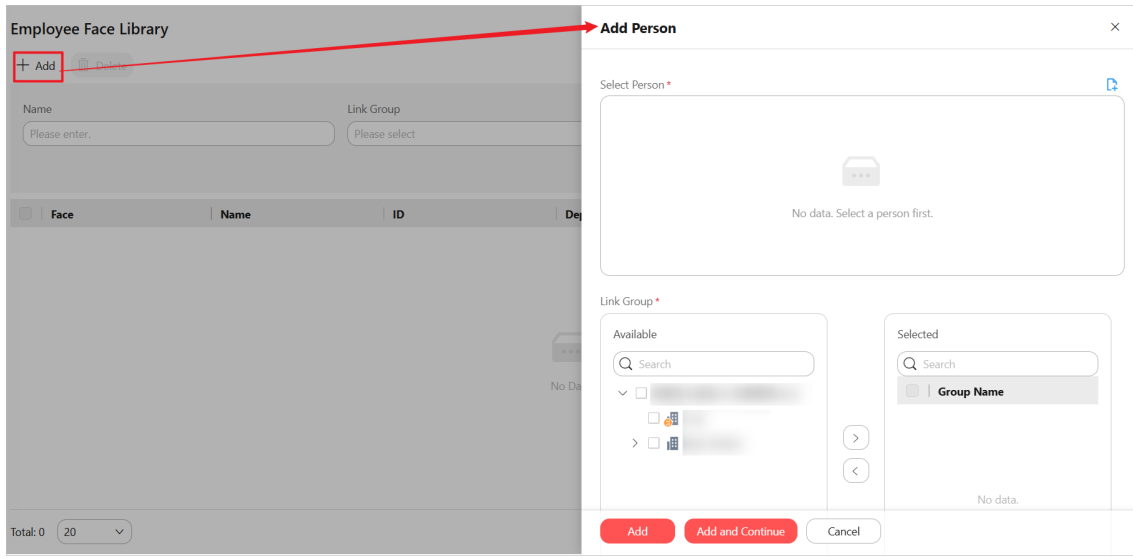
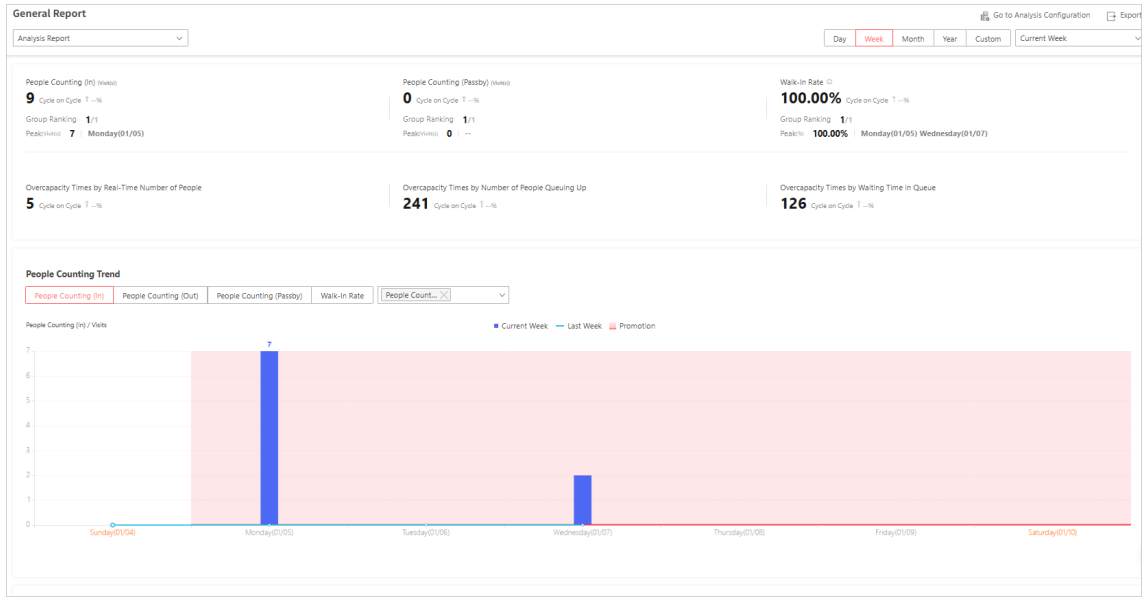
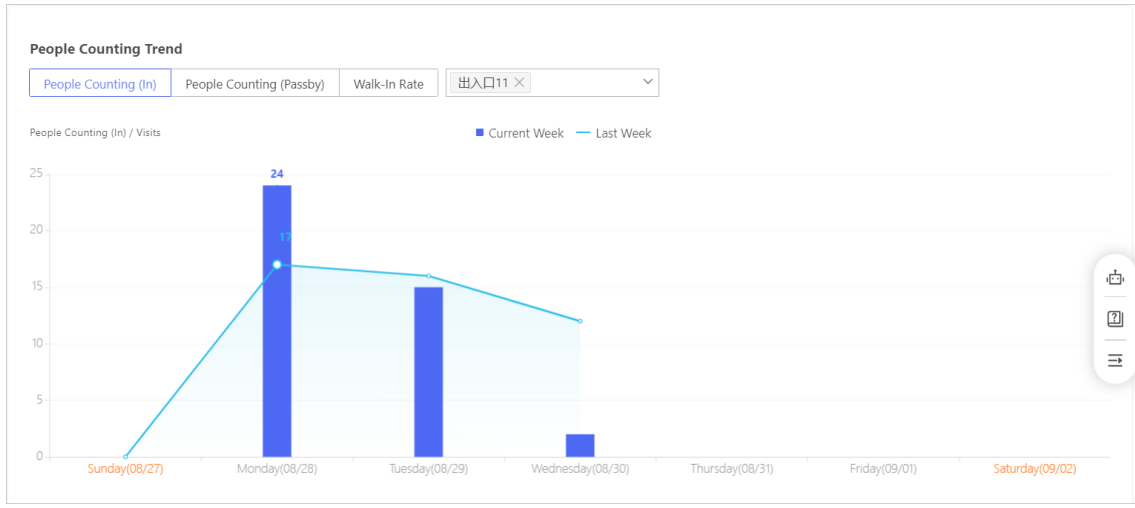


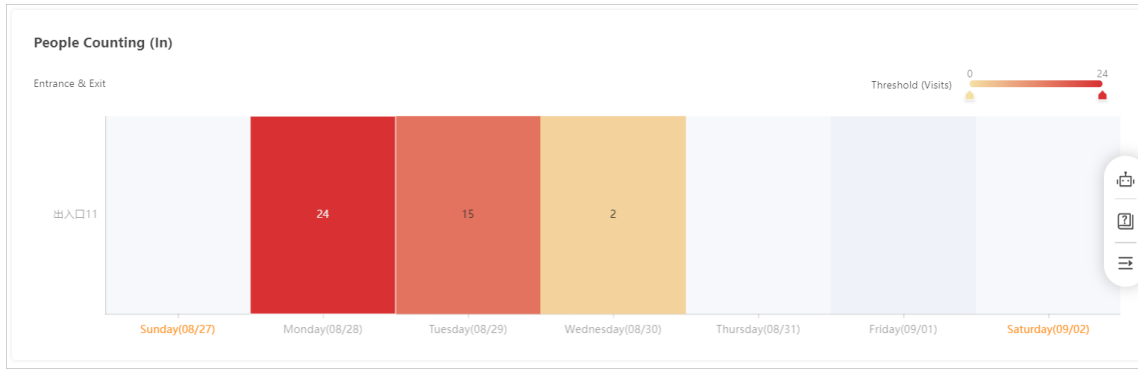
Figure 9-12 Employee Face Picture Library

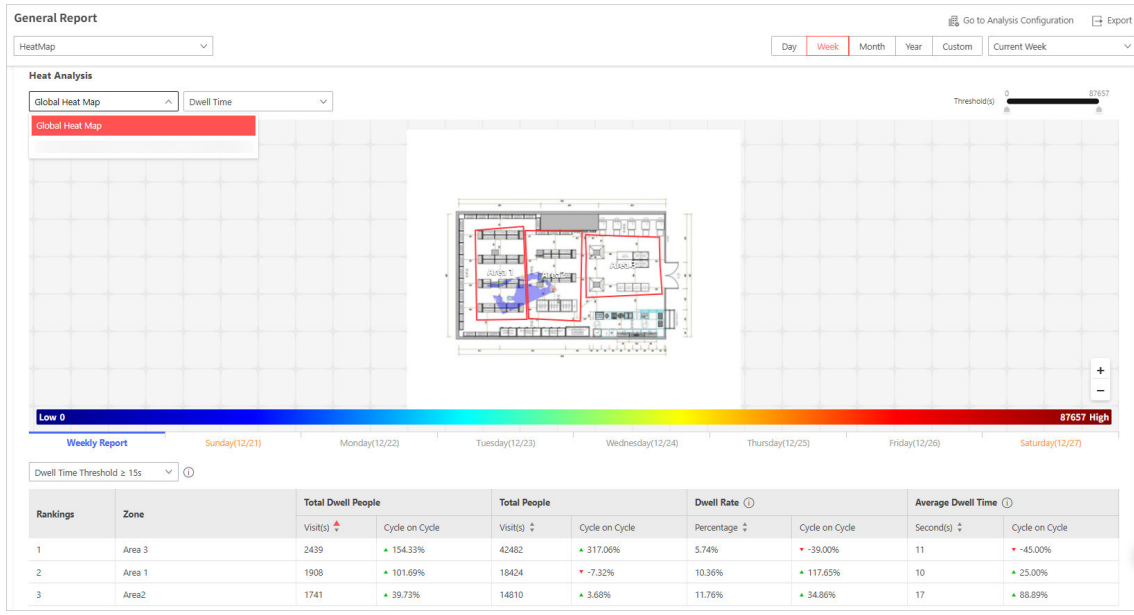
9.7 How to view analysis reports?

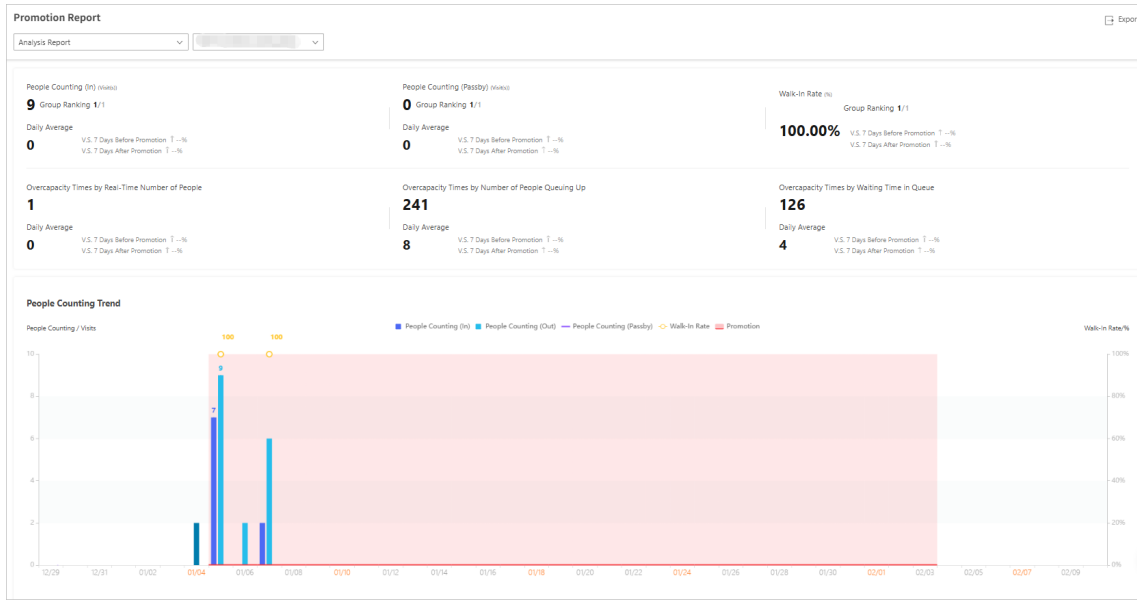
You can check general reports by day, week, month, year, and a custom period on the General Report page. Check the People Counting Trend, People Counting (In), and Heat Analysis. You can also check the Promotion Report on the General Report page.


General Report
Go to Analysis Configuration
Export
Analysis Report
Day
Week
Month
Year
Custom
Current Week
People Counting (In)
9
Cycle on Cycle
Group Ranking 1/1
Peak 7 Monday(01/05)
People Counting (Passby)
0
Group Ranking 1/1
Walk-In Rate
100.00%
Group Ranking 1/1
Peak 100.00% Monday(01/05) Wednesday(01/07)
Overcapacity Times by Real-Time Number of People
5
Overcapacity Times by Number of People Queuing Up
241
Overcapacity Times by Waiting Time in Queue
126
People Counting Trend
People Counting (In)
People Counting (Out)
People Counting (Passby)
Walk-In Rate
People Count...
People Counting (In) / Visits
Current Week
Last Week
Promotion
Sunday(01/04)
Monday(01/05)
Tuesday(01/06)
Wednesday(01/07)
Thursday(01/08)
Friday(01/09)
Saturday(01/10)


People Counting Trend
People Counting (In)
People Counting (Passby)
Walk-In Rate
出入口11
People Counting (In) / Visits
Current Week
Last Week
24
17
Sunday(08/27)
Monday(08/28)
Tuesday(08/29)
Wednesday(08/30)
Thursday(08/31)
Friday(09/01)
Saturday(09/02)


People Counting (In)
Entrance & Exit
Threshold (Visits)
0
24
出入口11
24
15
2
Sunday(08/27)
Monday(08/28)
Tuesday(08/29)
Wednesday(08/30)
Thursday(08/31)
Friday(09/01)
Saturday(09/02)


General Report
Go to Analysis Configuration
Export
HeatMap
Day
Week
Month
Year
Custom
Current Week
Heat Analysis
Global Heat Map
Dwell Time
Threshold(s)
Low 0
87657 High
Weekly Report
Sunday(12/21)
Monday(12/22)
Tuesday(12/23)
Wednesday(12/24)
Thursday(12/25)
Friday(12/26)
Saturday(12/27)
Dwell Time Threshold ≥ 15s
Rankings
Zone
Total Dwell People
Visit(s)
Cycle on Cycle
Total People
Visit(s)
Cycle on Cycle
Dwell Rate
Percentage
Cycle on Cycle
Average Dwell Time
Second(s)
Cycle on Cycle
1 Area 3 2439 154.33% 42482 317.06% 5.74% -39.00% 11 -45.00%
2 Area 1 1908 101.69% 18424 -7.32% 10.36% 117.65% 10 25.00%
3 Area2 1741 39.73% 14810 3.68% 11.76% 34.86% 17 88.89%


Promotion Report
Export
Analysis Report
People Counting (In)
9
Group Ranking 1/1
Daily Average
0
People Counting (Passby)
0
Group Ranking 1/1
Daily Average
0
Walk-In Rate
Group Ranking 1/1
100.00%
Overcapacity Times by Real-Time Number of People
1
Daily Average
0
Overcapacity Times by Number of People Queuing Up
241
Daily Average
8
Overcapacity Times by Waiting Time in Queue
126
Daily Average
4
People Counting Trend
People Counting / Visits
People Counting (In)
People Counting (Out)
People Counting (Passby)
Walk-In Rate
Promotion
Walk-In Rate/%

Chapter 10 Commercial Display

This concept describes how to set up and manage Commercial Display devices on Hik Connect for Teams, including compatibility checks, device configuration, and service settings.

10.1 Example Scenario

This guide provides a step-by-step configuration process for setting up commercial display devices in a school environment, including classrooms, libraries, and common areas.

1. ***Configure Commercial Display Devices***
   - Add devices to the system after configuring network parameters and entering serial numbers and verification codes.
   - **Example:** Install commercial displays in school classrooms and common areas. Configure network settings and ensure devices are online for centralized management.
   - Path: → **Device → Commercial Display Device**
2. ***Control Devices***
   - Manage device operations including screen on/off, restart, shutdown, and scheduled startup/shutdown.
   - **Example:** Set scheduled operations for classroom displays to automatically turn on during school hours and shut down after classes. Use scheduled startup for morning announcements.
   - Path: → **Commercial Display → Device Control**
3. ***Manage Applications***
   - Upload and manage applications on the devices, including educational software and display applications.
   - **Example:** Deploy educational applications to classroom displays for interactive learning. Manage application updates and monitor deployment status across multiple devices.
   - Path: → **Commercial Display → Application Management**
4. ***Generate Usage Reports***
   - Generate and export usage reports based on daily, weekly, monthly, or custom periods.
   - **Example:** Monitor display usage in different school areas. Generate monthly reports for library displays to track usage patterns and optimize content scheduling.
   - Path: → **Commercial Display → Flat Panel Usage Reports**

10.2 How to verify device compatibility?

Verify device compatibility before adding devices to the system.

Go to → → **Device Compatibility List** to make sure the device is supported.

Note

- If the device firmware version is lower than listed in the document, upgrade the version; otherwise, some functions may not be supported.
- Devices not listed may be added via Hik-Connect (P2P), but some Hik-Connect for Teams functions may be inaccessible.

10.3 How to configure commercial display devices?

Step-by-step process to add Commercial Display devices to Hik-Connect for Teams.

To use the Commercial Display service, first add devices to the system by following these steps:

1. Configure local parameters for the Commercial Display device:
   a. Turn on the large screen, navigate to **Settings → Network** , and select the connection method (wired, wireless, or hotspot).

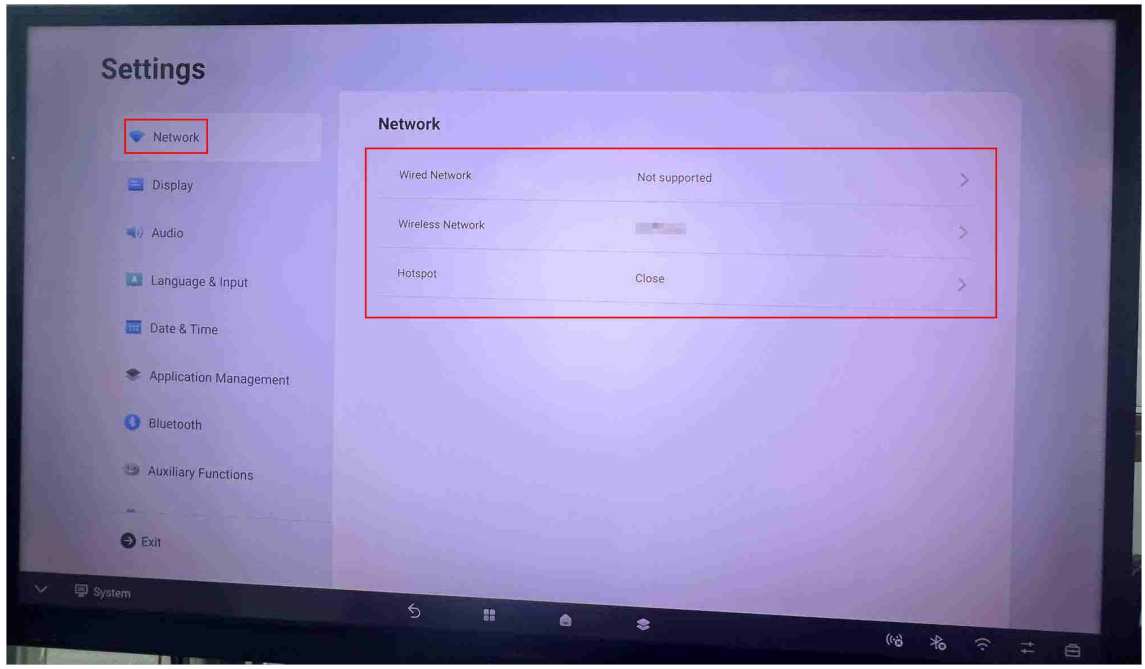


Figure 10-1 Network Settings

   b. Return to the home page, go to **Ark → Online** , and confirm the connection status shows online.

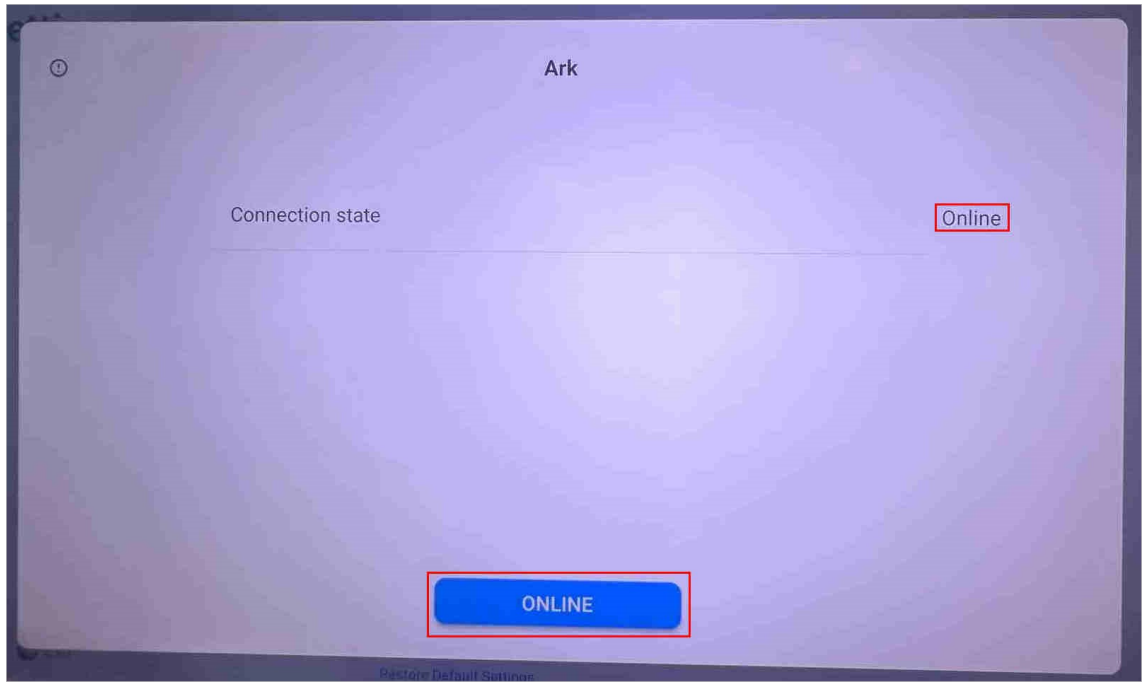


Figure 10-2 Ark Settings

2. Add the device to Hik-Connect for Teams on the Portal:
   a. Go to → **Device** → **Commercial Display Device** and click **Add**.
   b. Enter the device serial number and verification code, set the device name, and select the group.

Note

- After turning on the large screen, find the serial number in **Settings** → **About** .

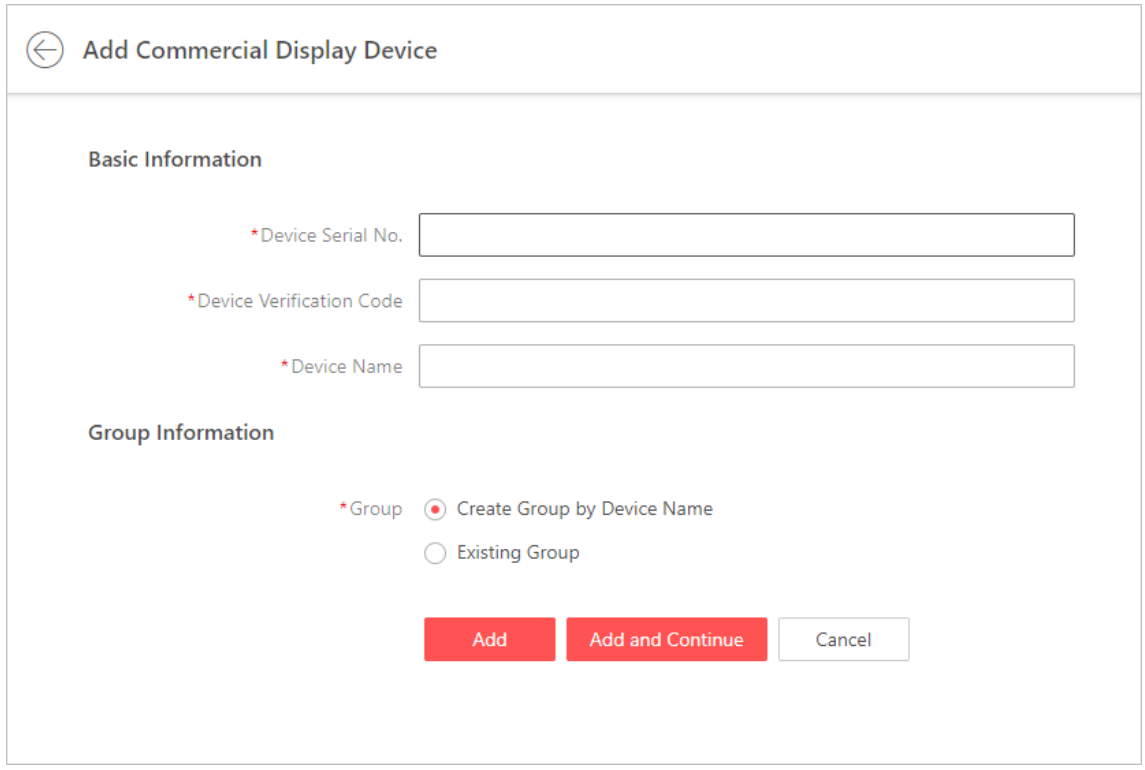


Figure 10-4 Getting Device Serial Number

- After turning on the large screen, go to **Home → Ark** and long-press the **Ark** button to get the verification code.

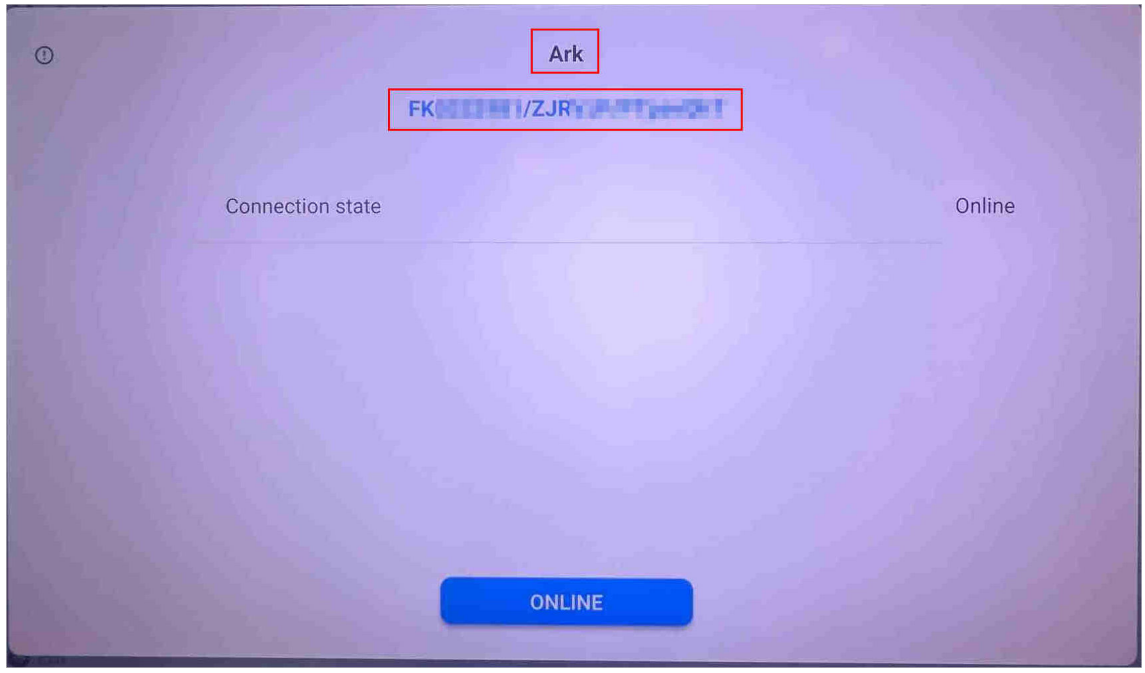


Figure 10-5 Getting Device Verification Code

c. Click **Add** to add the device to the system.

10.4 How to control devices?

1. Go to **Commercial Display → Device Control** .
2. Select a device to control actions such as **Screen On**, **Screen Off**, **Restart**, **Shutdown**, or **Scheduled Startup/Shutdown**.

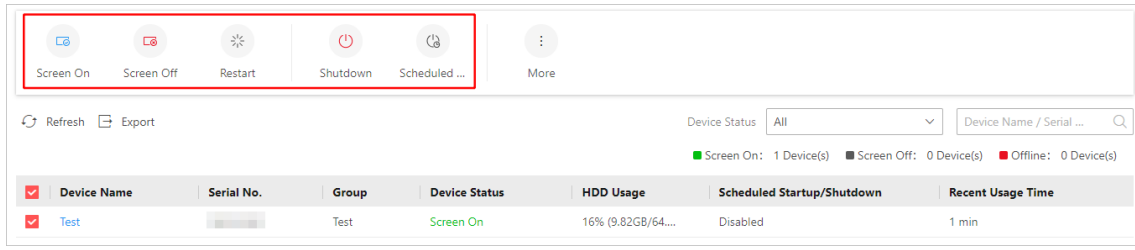


Figure 10-6 Device Control

3. For **Scheduled Startup/Shutdown**, set the time to control device power cycles and apply the schedule from Monday to Sunday.

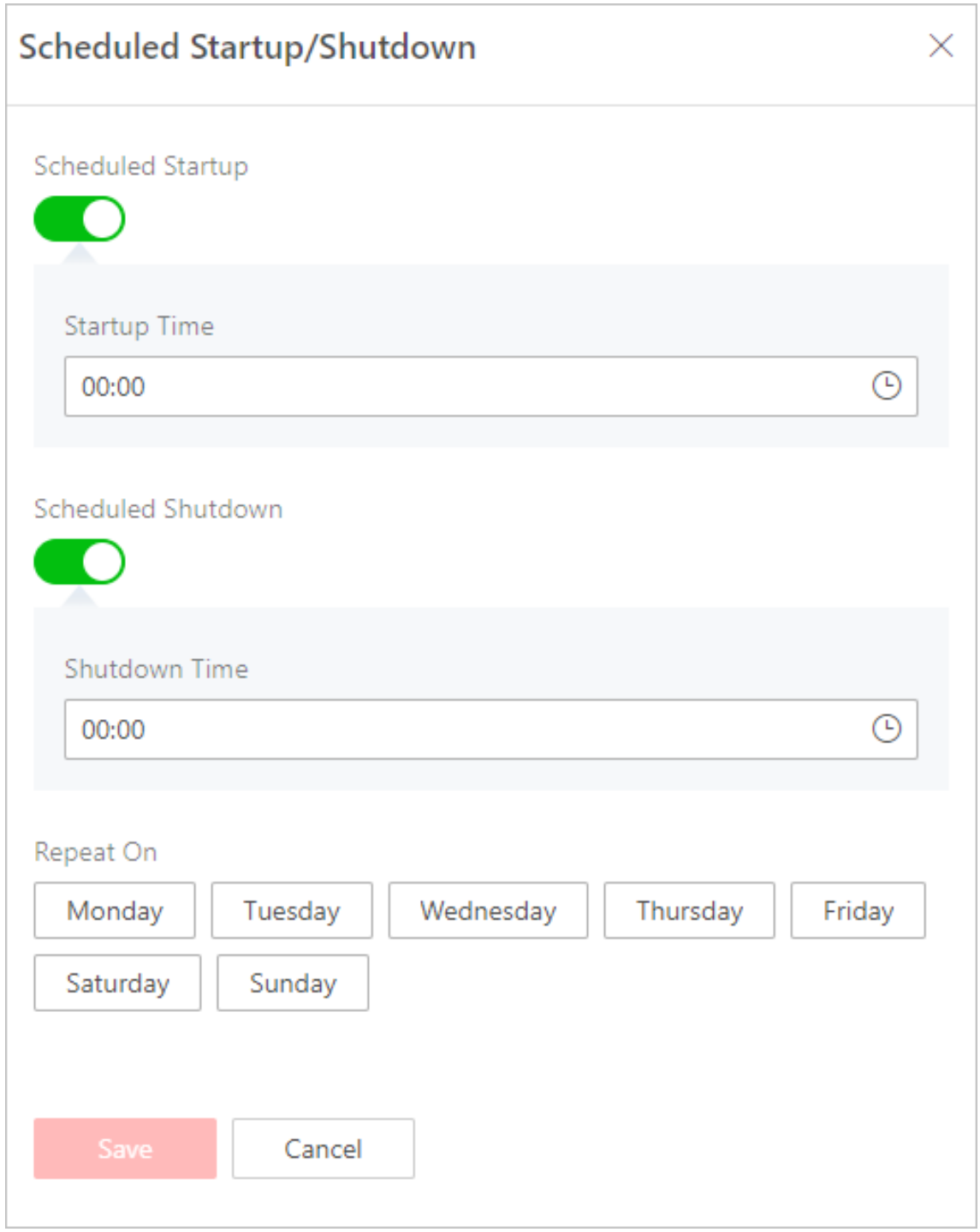


Figure 10-7 Scheduled Startup/Shutdown

4. Click **More** for additional operations like **Restore to Factory**, **Reset Device Password**, **Disable APK**, or **Enable APK**.

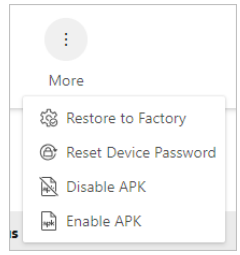


Figure 10-8 More

5. Click **Export** to download device details.

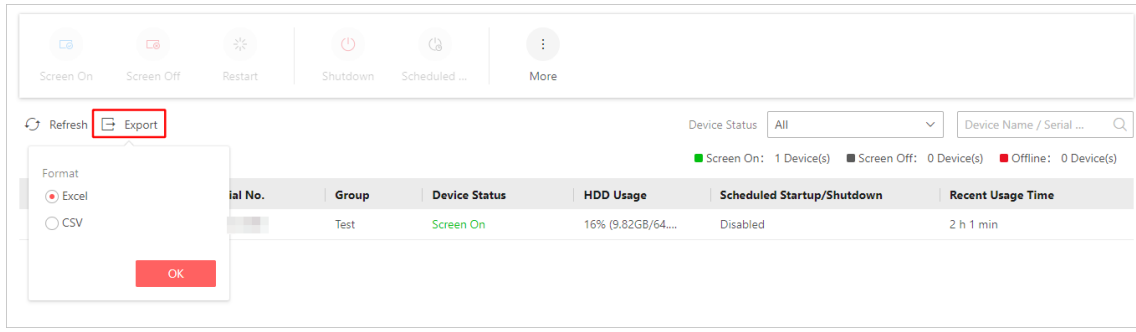


Figure 10-9 Export

10.5 How to manage applications?

1. Go to **Application Management** to manage applications on the device.

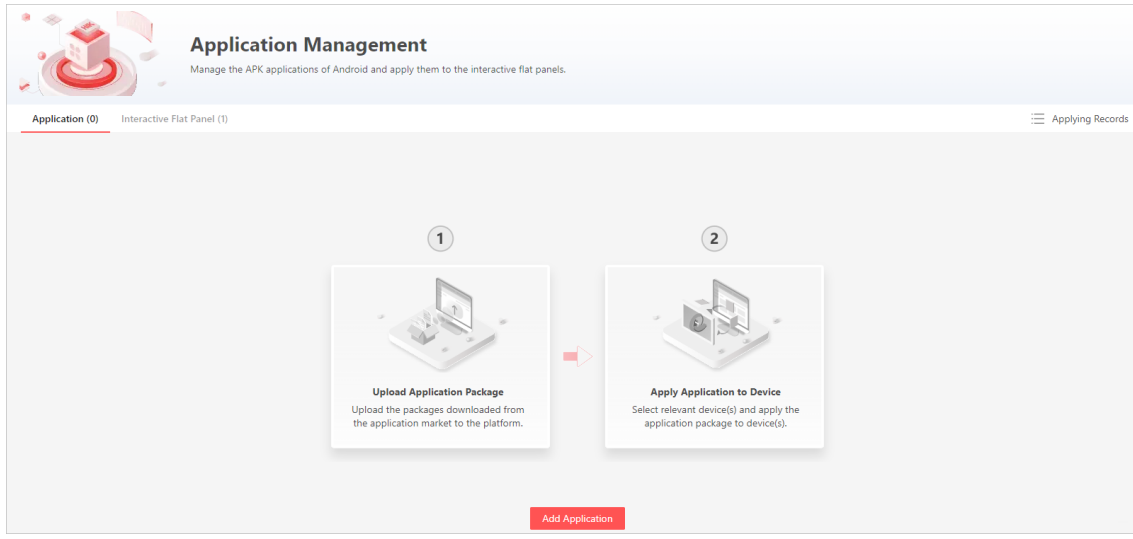


Figure 10-10 Application Management

2. Select **Add Application**, upload the application package, and click **Next**.

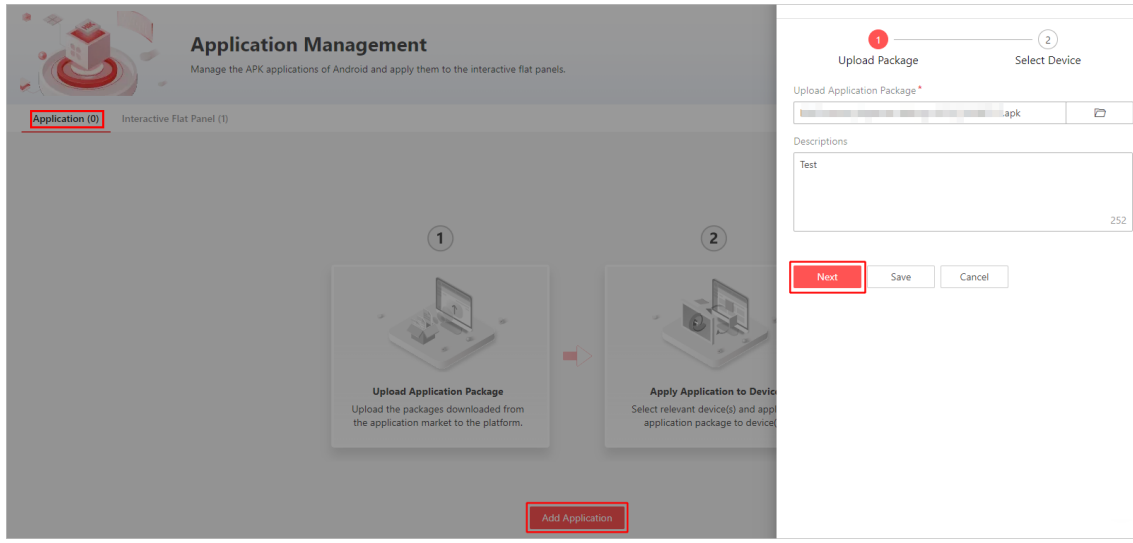


Figure 10-11 Add Application and Upload Package

Select the target devices and click **Apply**.

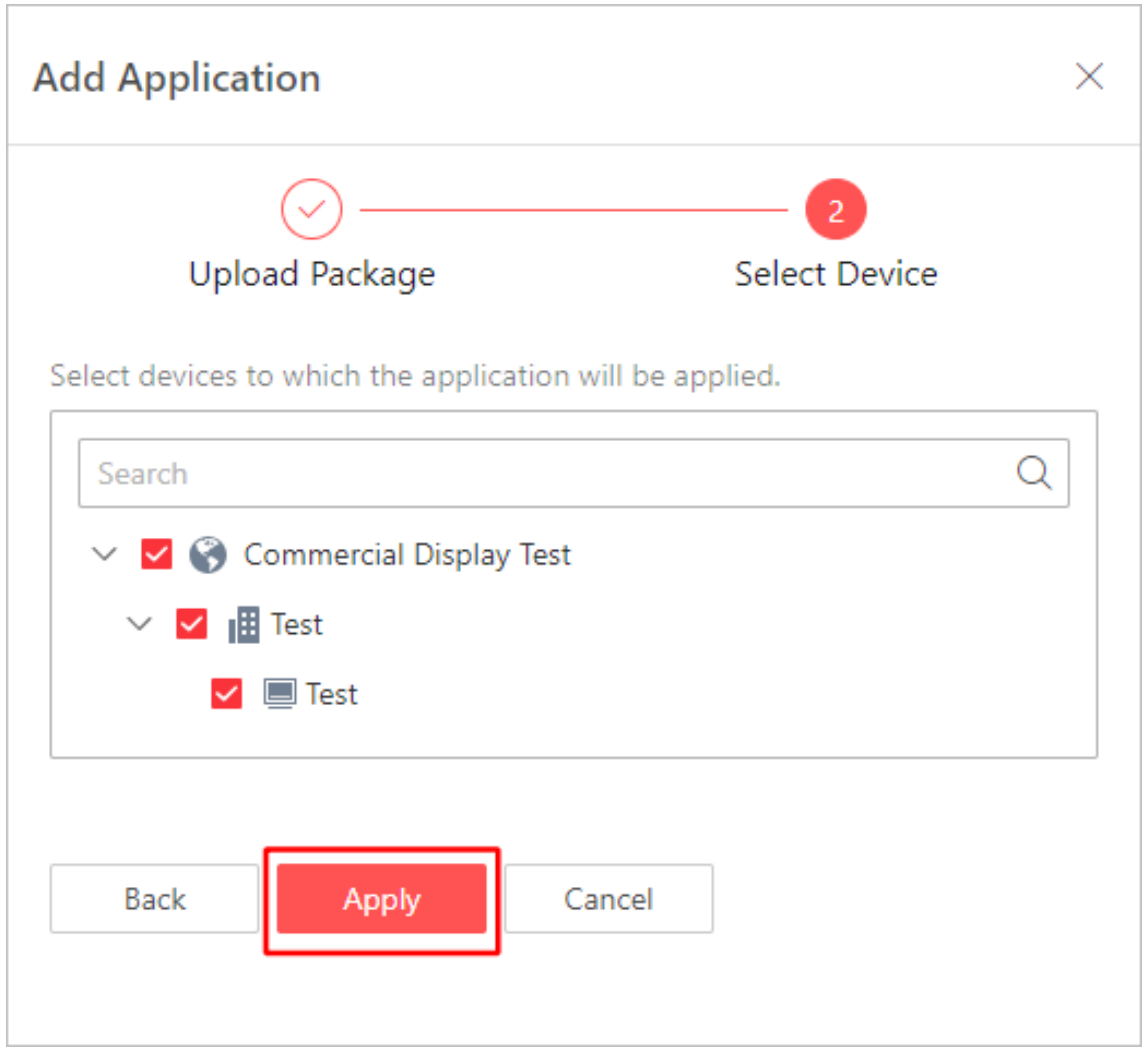


Figure 10-12 Select Devices

Wait for uploading to complete, click **Close**, then wait for applying and click **Close** again.



Figure 10-13 Application Applied

3. After successful deployment, view the APK list, check application records via **Applying Records**, or use **Delete** or **Add** for management.

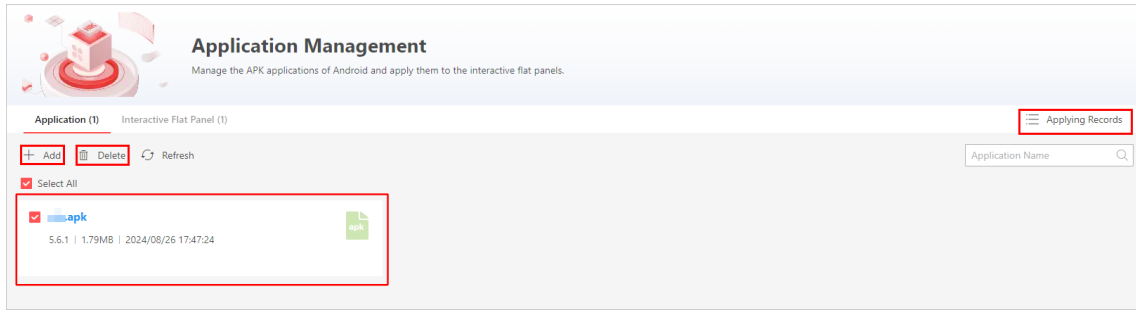


Figure 10-14 Application Management

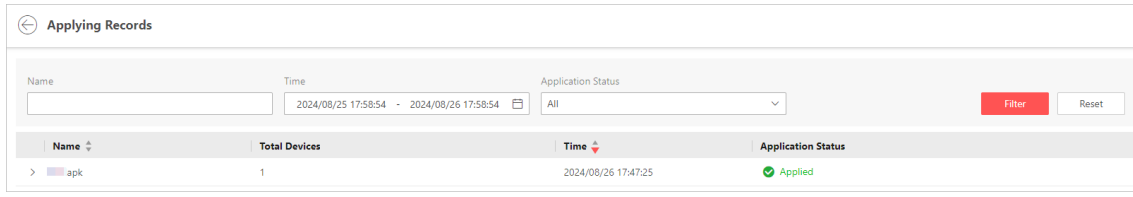


Figure 10-15 Apply Records

4. In the **Interactive Flat Panel** interface, view installed applications, and add or uninstall applications.

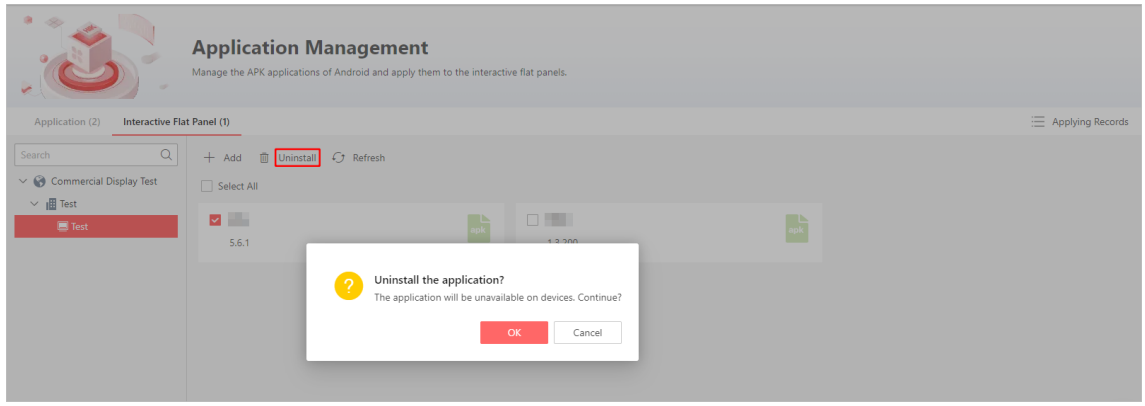


Figure 10-16 Uninstall Application

10.6 How to generate usage reports?

Generate and export usage reports for display devices based on daily, weekly, monthly, or custom periods.

In **Commercial Display → Flat Panel Usage Reports** , select a device and generate reports by duration (Daily, Weekly, Monthly, or Custom).
View device usage time and export the reports.

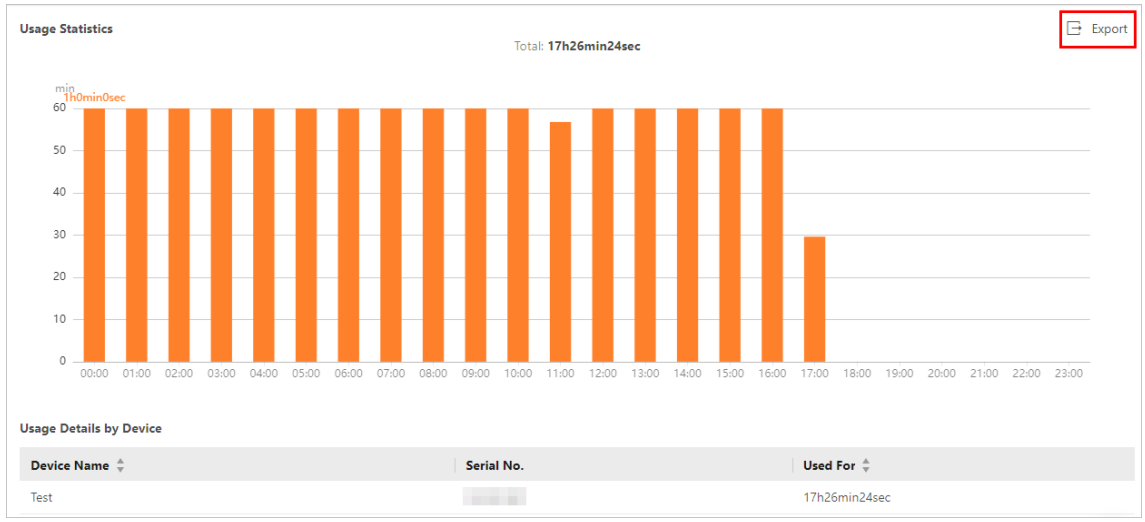


Figure 10-17 Daily Report

Chapter 11 ANPR

ANPR stands for Automatic Number Plate Recognition, a system that uses cameras and AI to automatically identify and record vehicle license plates. It is used for managing vehicle lists, searching for vehicle reports, and generating detailed reports. ANPR is particularly useful in scenarios like parking lots, toll roads, and security checkpoints, enhancing traffic management, security, and law enforcement.

11.1 Example Scenario

This guide provides a step-by-step configuration process for setting up the Automatic Number Plate Recognition (ANPR) system, which uses cameras and AI to automatically identify and record vehicle license plates for traffic management, security, and access control applications. The table below outlines the configuration steps in logical order, with references to the corresponding concepts and menu paths for easy navigation.

1. ***Activate ANPR Service***
   Enable the ANPR service in Service Management before use. If the service is unavailable, contact your authorized service provider for activation.
   → **Service**
2. ***Add ANPR Cameras***
   Add cameras with ANPR capability and configure them as ANPR cameras through the device management interface. Ensure cameras are properly positioned for optimal license plate recognition.
   Example: Add compatible cameras to the system, then navigate to the device list page to set them as ANPR cameras for license plate recognition functionality.
   → **Device → Encoding Device → Set as ANPR Camera**
3. ***Create Vehicle Lists***
   Create and manage vehicle lists for access control by defining list names, types, and associating ANPR cameras. Lists can be customized with colors and descriptions for better organization.
   Example: Create a "Authorized Vehicles" list for parking lot access, associating it with entrance and exit ANPR cameras for automated gate control.
   → **ANPR → List Management → Add List**
4. ***Add Vehicles to Lists***
   Populate vehicle lists using three methods: through person records, via on-board monitoring devices, or by creating new vehicle entries directly in the ANPR module.
   Example: Link vehicles to existing person records for employee parking, or create new vehicle entries for visitor management with specified validity periods.
   - → **Person → Link Vehicle**
   - → **ANPR → List Management → Add Vehicle**
5. ***Configure LED Display***

Configure LED display settings including display text with templates for plate number, date, time, font size, color, row number, and scroll mode. View real-time preview of visual effects.
Example: Set up LED displays at parking entrances to show recognized license plates and entry status with customized colors and scrolling effects.
⁞⁞ **→ ANPR → Configuration → LED Display Configuration**

6. ***Configure Broadcast***
   Set up broadcast configurations for four announcement types: allowlist, temporary plates, blocklist, and expiring allowlist. Upload custom audio files and set volume levels.
   Example: Configure audio announcements for different vehicle scenarios - welcoming authorized vehicles and warning about unauthorized access attempts.
   ⁞⁞ **→ ANPR → Configuration → Broadcast Configuration**
7. ***Configure Barrier Gate Control***
   Set up manual and automatic barrier gate control for vehicles. Enable barrier gate control on device details page and configure actions as Open Barrier Gate, Close Barrier Gate, or Empty.
   Example: Configure automatic gate opening for vehicles in authorized lists during business hours, with manual override capability for security personnel.
   ⁞⁞ **→ Video → Video Security → Live View**
8. ***Search Passing Vehicle Records***
   Search and review vehicle passing records captured by ANPR cameras with advanced filtering options including license plate, vehicle owner, list type, and time period. Export results with optional pictures.
   Example: Search for specific vehicle movements during security incidents, filtering by license plate and time range, then export the records for investigation purposes.
   ⁞⁞ **→ ANPR → Passing Vehicle Search**
9. ***Generate Vehicle Reports***
   Create comprehensive passing vehicle reports with daily, weekly, monthly, or custom period options. Filter reports by vehicle type, brand, and list membership status for detailed analytics.
   Example: Generate monthly traffic analysis reports showing vehicle distribution by type and brand, highlighting peak hours and traffic patterns for parking optimization.
   ⁞⁞ **→ ANPR → Passing Vehicle Report**

11.2 How to activate the ANPR service?

Go to ⁞⁞ **→ Service** .

Enable the ANPR service in Service Management before use. If the service is unavailable, contact your authorized service provider for activation.

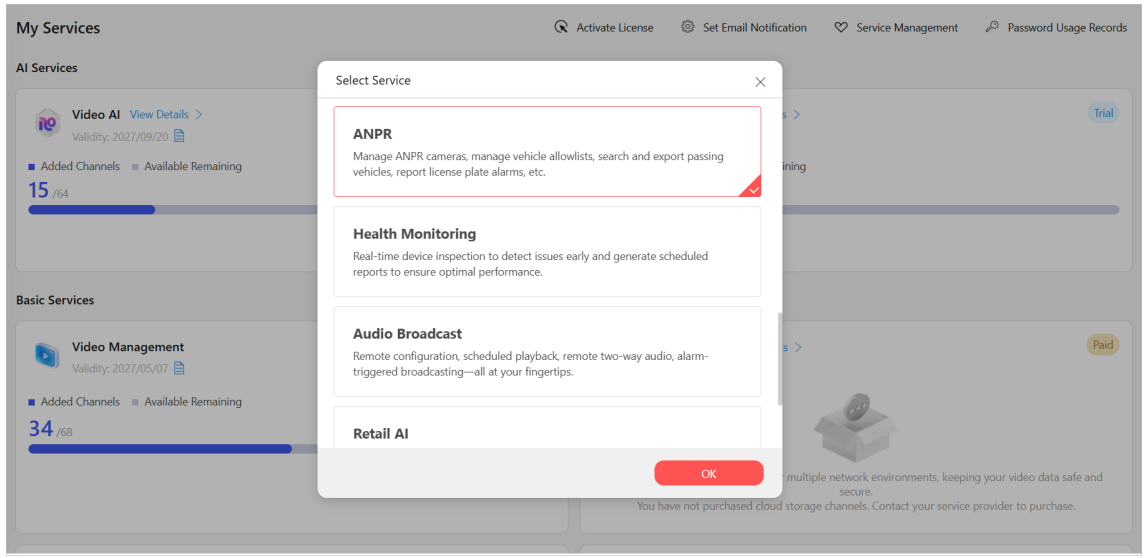


Figure 11-1 Enable ANPR Service

Note

- If your Hik-Connect account isn't authorized with an HPP service provider, select ANPR service when creating your system.
- ANPR service is billed per video channel and includes full video management capabilities.

After activation, you can configure vehicle lists, search vehicle records, generate reports, and control barrier gates.

11.3 How to add lists and add vehicles to lists?

You can create and manage vehicle lists for access control.

1. Go to → **ANPR** → **List Management** → **Add List** .

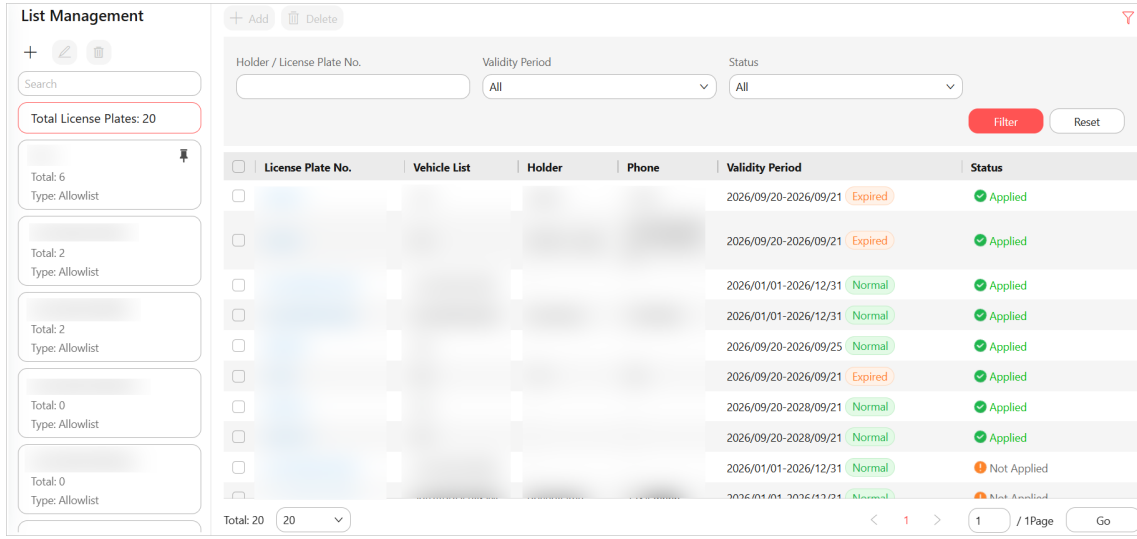


Figure 11-2 Add List

2. Enter a list name, select the list type, and link with ANPR cameras.

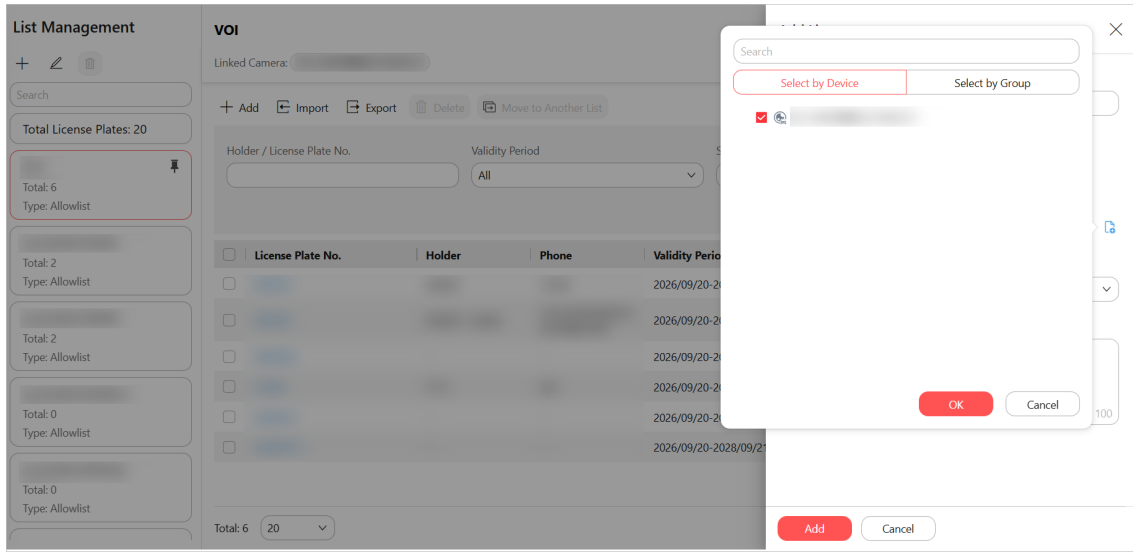
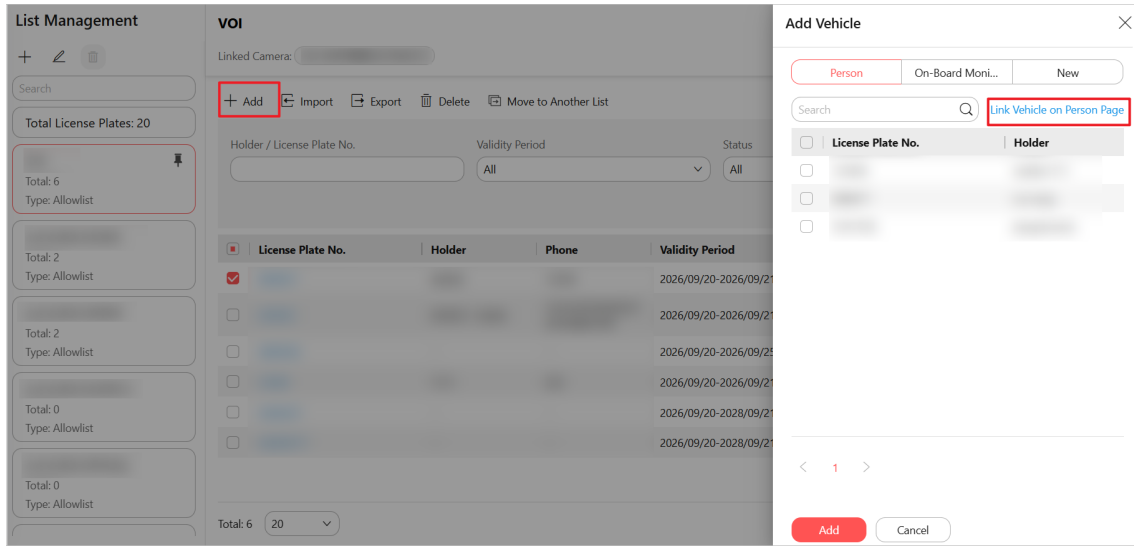
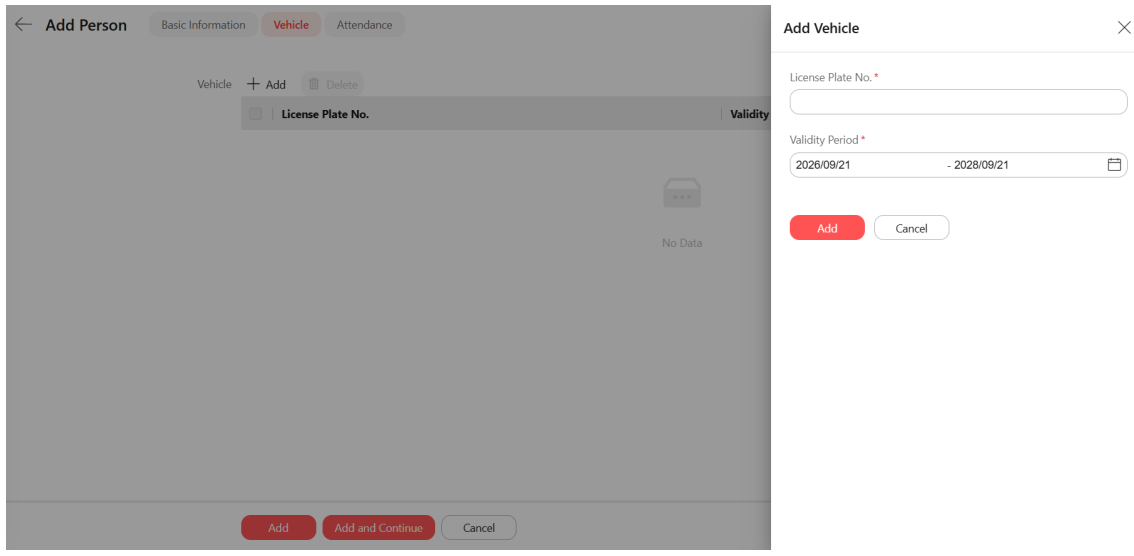


Figure 11-3 Add ANPR Camera

3. (Optional) You can bind remote control numbers when adding license plates.
4. Select the newly created list and click Add. You can choose to add vehicle from Person or On-Board Monitoring or select **New** to create new vehicle information.
   - When selecting add vehicle from Person, you can choose to enter vehicle information on the person details page. Click **Link Vehicle on Person Page**, select one person and enter the person details page. In the person details page, click vehicle tab, you can add the license plate No. and set validity period.





- When selecting add vehicle from On-Board Monitoring, you can select the On-Board Device and set validity period.

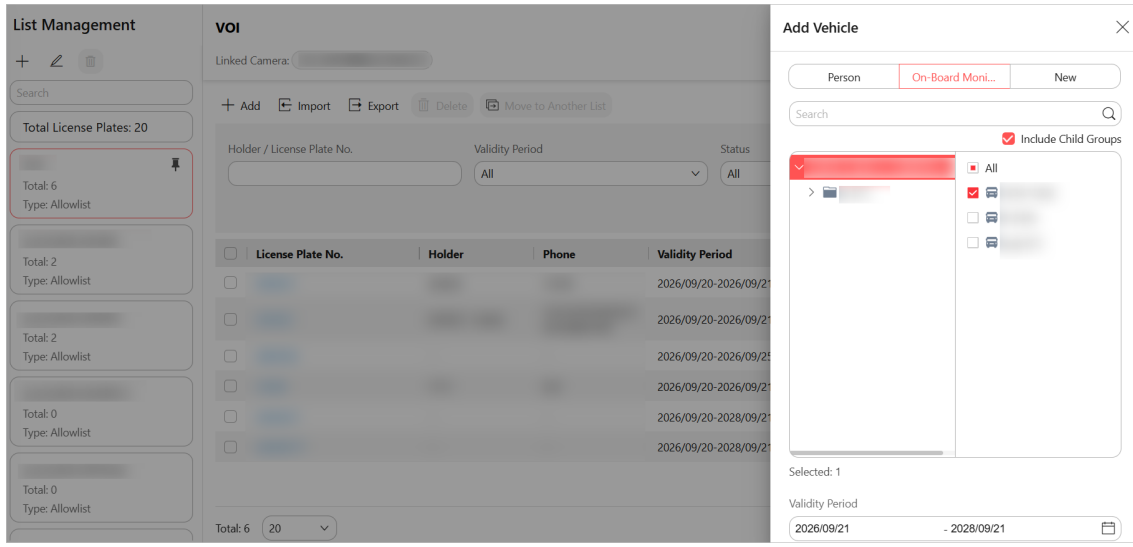


Figure 11-4 Add Vehicle from On-Board Monitoring

- When selecting New to create a new vehicle, you need to enter the license plate No., set the validity period and the owner's name and phone number.

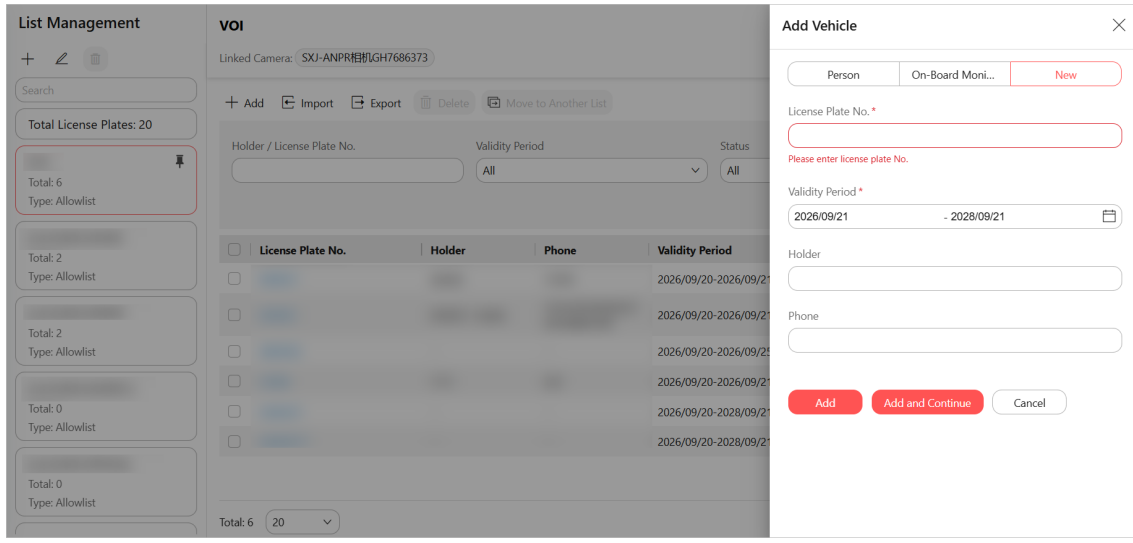


Figure 11-5 Create New Vehicle

11.4 How to set cameras as ANPR cameras and configure barrier gate control?

1. Go to ⁝⁝⁝ → **Device → Encoding Device**
   Set the device as the ANPR camera.

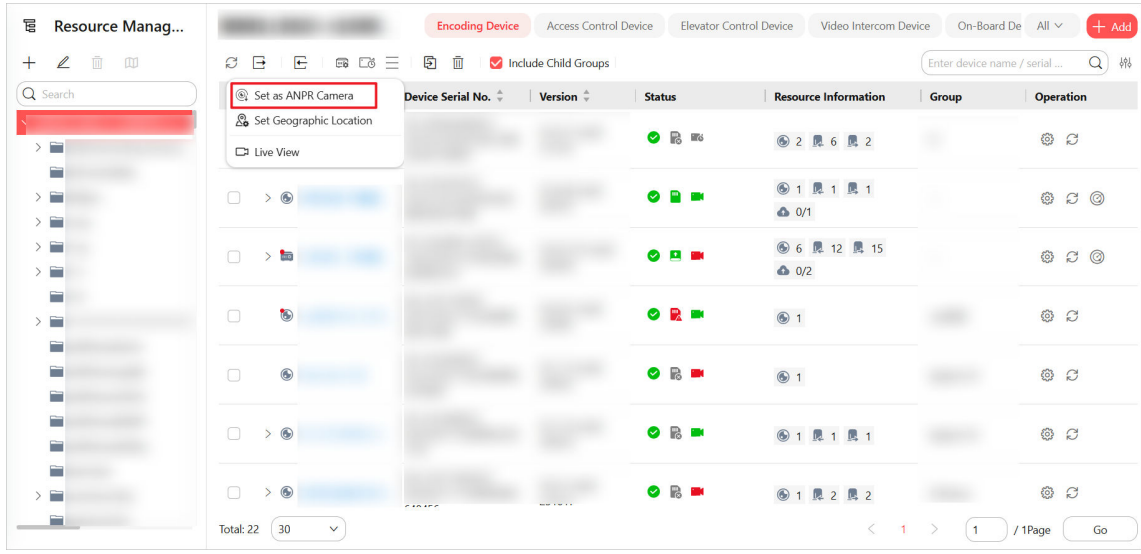


Figure 11-6 Set as ANPR Camera

2. On the Portal device details page, you can enable barrier gate control and set the barrier gate action as **Open Barrier Gate**, **Close Barrier Gate** or **Empty**.

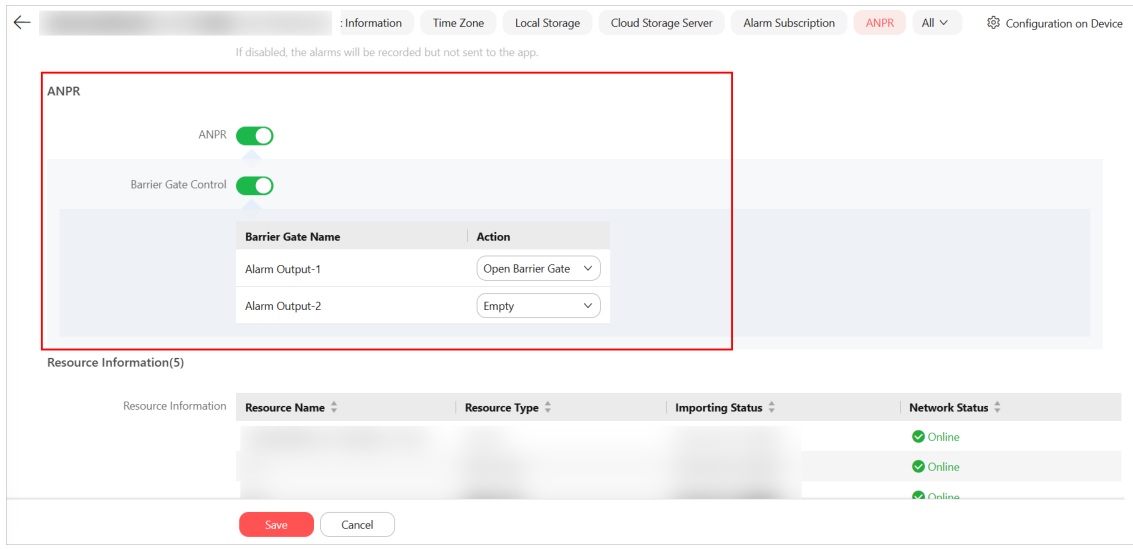


Figure 11-7 Set Barrier Gate Control

3. After completing the configuration of Barrier Gate Control, you can manually control the barrier gate.

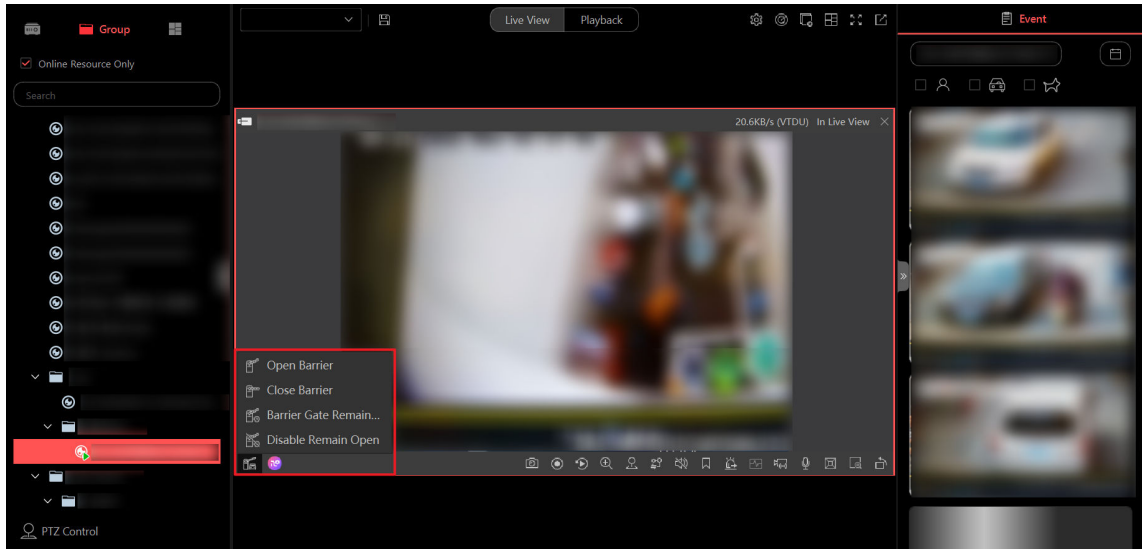


Figure 11-8 Barrier Gate Control on the Portal

11.5 How to retrieve passing vehicle records?

You can view vehicle passing records captured by one or multiple cameras. Also, you can further refine the results by specifying license plates, vehicle owner name, vehicle list, etc.

1. Go to → **ANPR** → **Passing Vehicle Search** .
2. Select ANPR cameras and set the time period.
3. Click **More** to filter by license plate number, vehicle owner, list type, vehicle type, brand, color, speed, country/region, and driving direction.

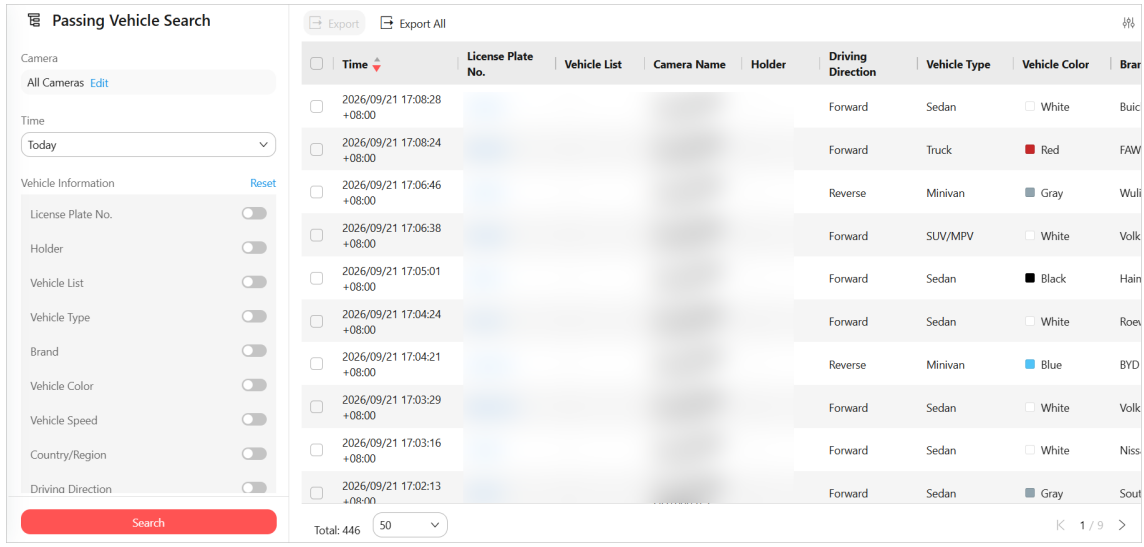


Figure 11-9 Search for Passing Vehicles

4. Export results to Excel, including records by default and optional pictures.

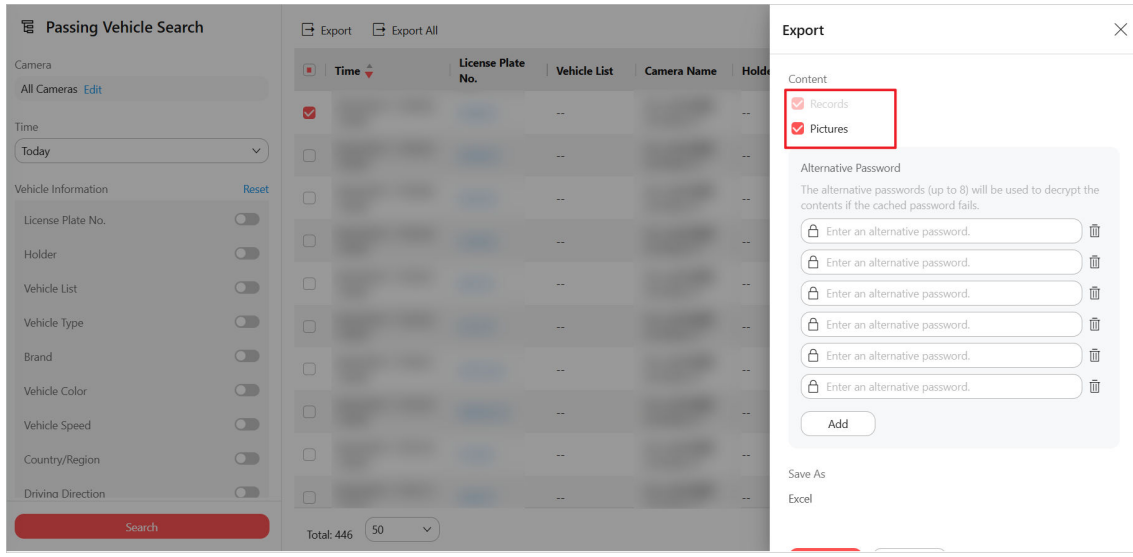


Figure 11-10 Export Records

5. Set alternative passwords for picture decryption if the cached password fails.

11.6 How to view passing vehicle reports?

You can view vehicle passing reports captured by specified cameras or cameras from specified groups. Also, you can further refine the reports by brand, vehicle type, vehicle and list.

1. Go to → **ANPR** → **Passing Vehicle Report** .
2. Select Camera or Group as the data source for reporting.
3. Choose one or multiple cameras for the report.
4. Select the report type: Daily, Weekly, Monthly, or Custom period.
5. Apply filters by vehicle type, brand, and list status (In list/Not in list).
6. Generate and export the report.

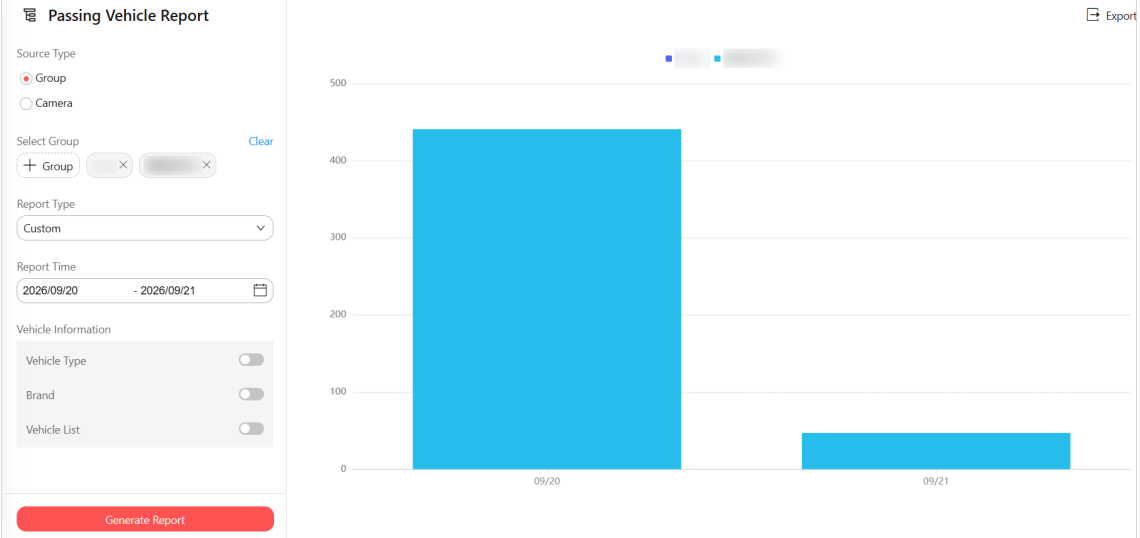


Figure 11-11 Passing Vehicle Report

11.7 How to configure LED Display?

(Portal) Adds → **ANPR → Configuration → LED Display Configuration** menu.

- You can configure display text (with templates for plate number, date, time, etc.), font size (16/32), color (red/green/yellow), row number, scroll mode, etc.
- You can view real-time preview of visual effects; configurations are applied to associated devices with status tracking (success/failure/in progress).

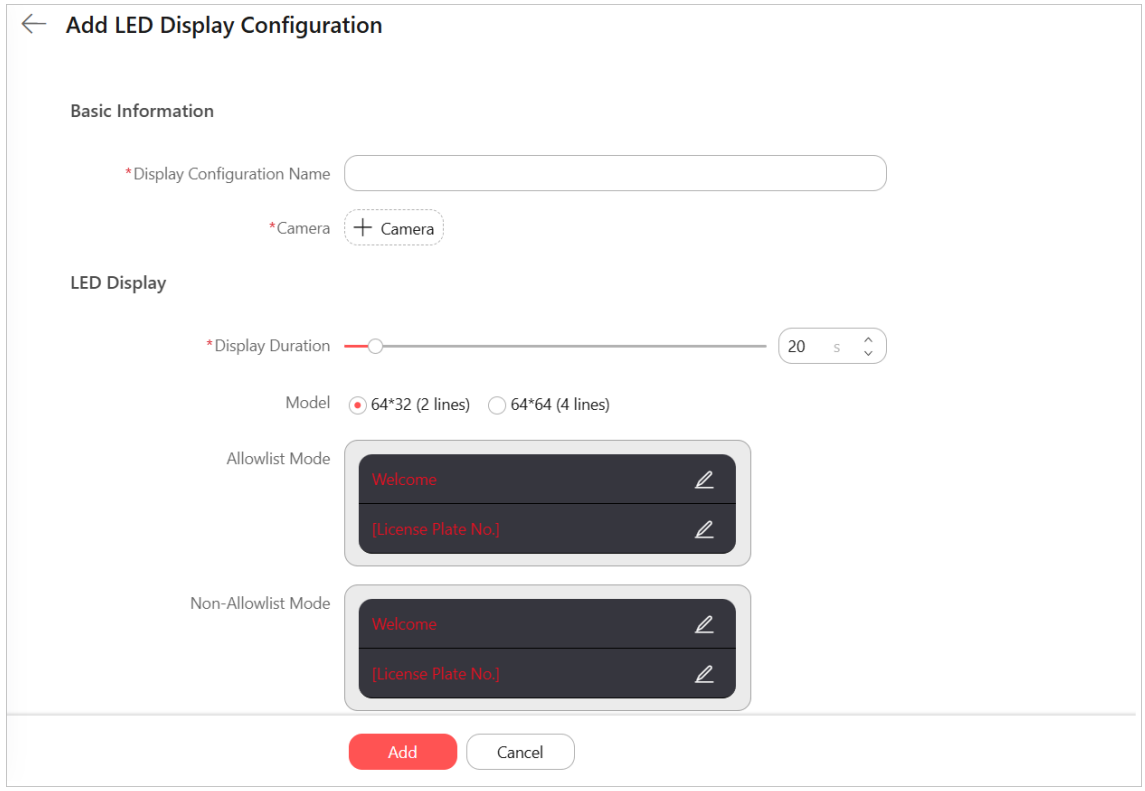


Figure 11-12 LED Configuration

Note

- Each device supports up to 4 LED configurations per scenario.
- Text limited to 40 characters; date/time must occupy separate rows.

11.8 How to configure broadcast?

Go to → **ANPR → Configuration → Broadcast Configuration** menu, supporting four announcement types: allowlist, temporary plates, blocklist, and expiring allowlist.

You can upload custom audio files (.wav format, ≤400KB), set volume (0-10), and apply to devices.

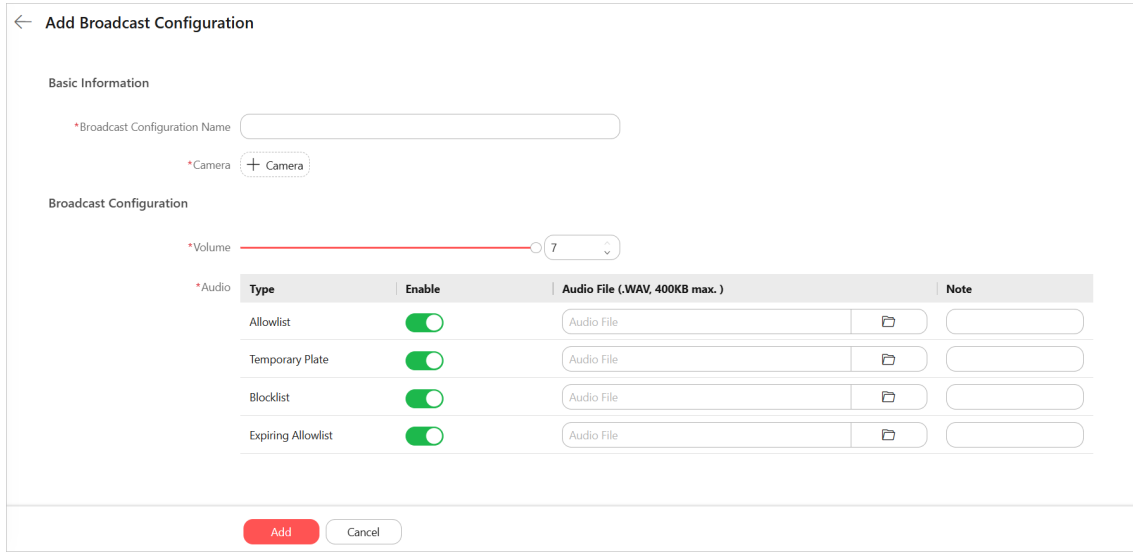


Figure 11-13 Broadcast Configuration

Note

- Each device can only be associated with one broadcast configuration.
- Audio names and content must be unique, with a character limit of 127.

Chapter 12 Audio Broadcast

In this module, you can upload audio files, schedule timed broadcasts, and set audio linkage of events. This system is used for efficient delivery of news, music, alerts, and live announcements. Common scenarios include radio stations, security systems, school notifications, and commercial broadcasting.

This feature is only available in certain countries or regions.

12.1 Add Network Speakers

Refer to ***Device Management*** to add network speakers (currently only the two models are supported: DS-QAZ1325G1T and DS-QAZ1206G1-BE).

You can link your network speakers with cameras so you can speak on the Live View page of the cameras or on the device list page on the Mobile Client.

12.2 Speak via a Single or Multiple Speakers

There are three ways to use the broadcast feature in Hik-Connect Teams: speaking to an individual device, broadcasting to multiple devices at once, or addressing the camera linked to the broadcast device.

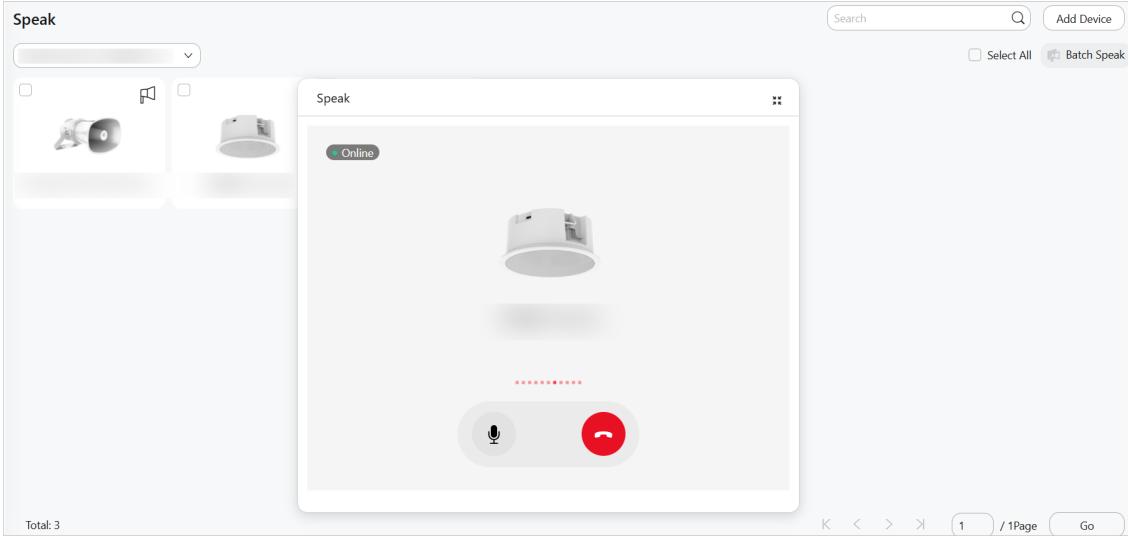
Go to **Audio Broadcast → Broadcast** .

- You can speak via a speaker.

Click the button in the upper-right corner of the a speaker.

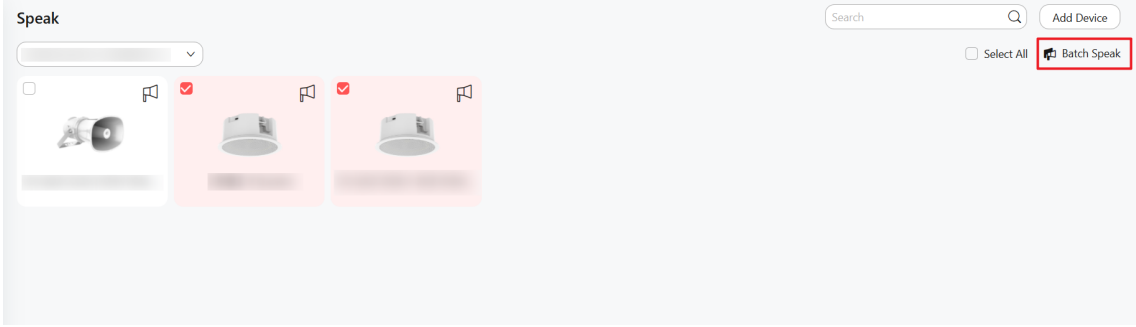


Speak via the speaker.

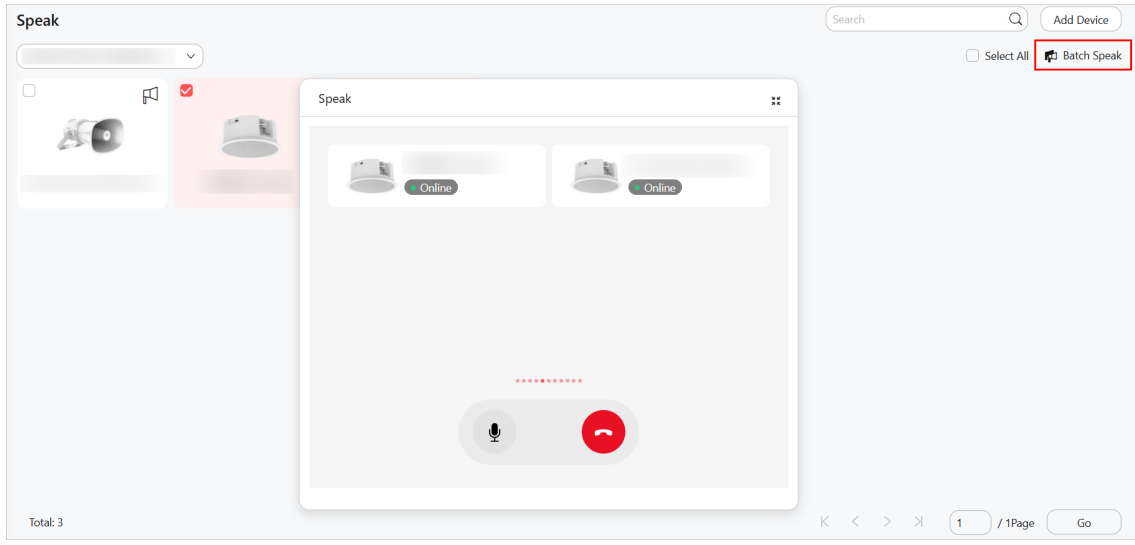


- Select multiple speakers and start batch speaking.

Select multiple speakers and click **Batch Speak** in the upper-right corner.

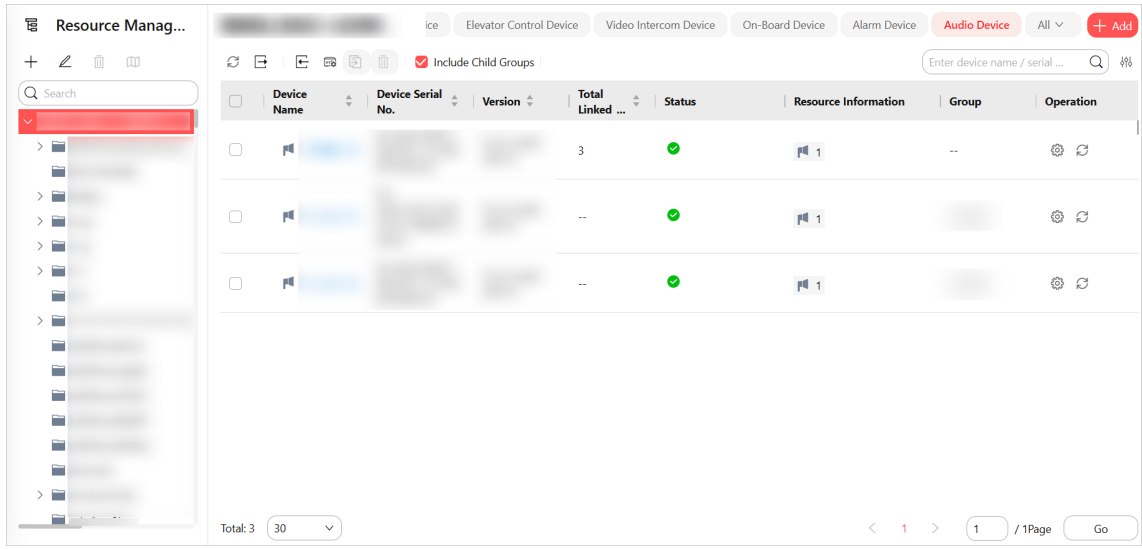


Speak to the selected speakers.

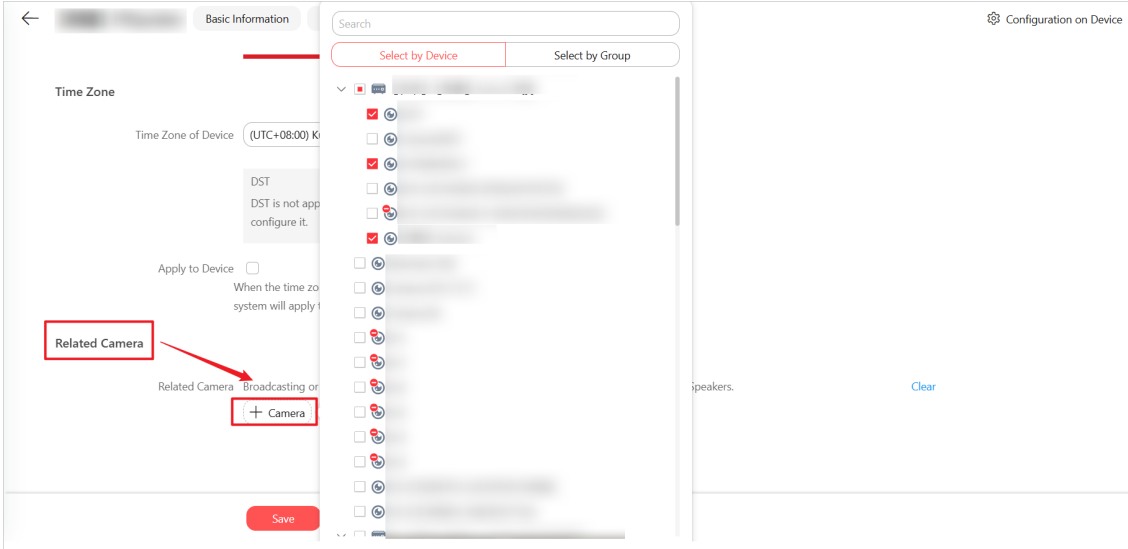


- Link a speaker with a camera and speak on the live view page.

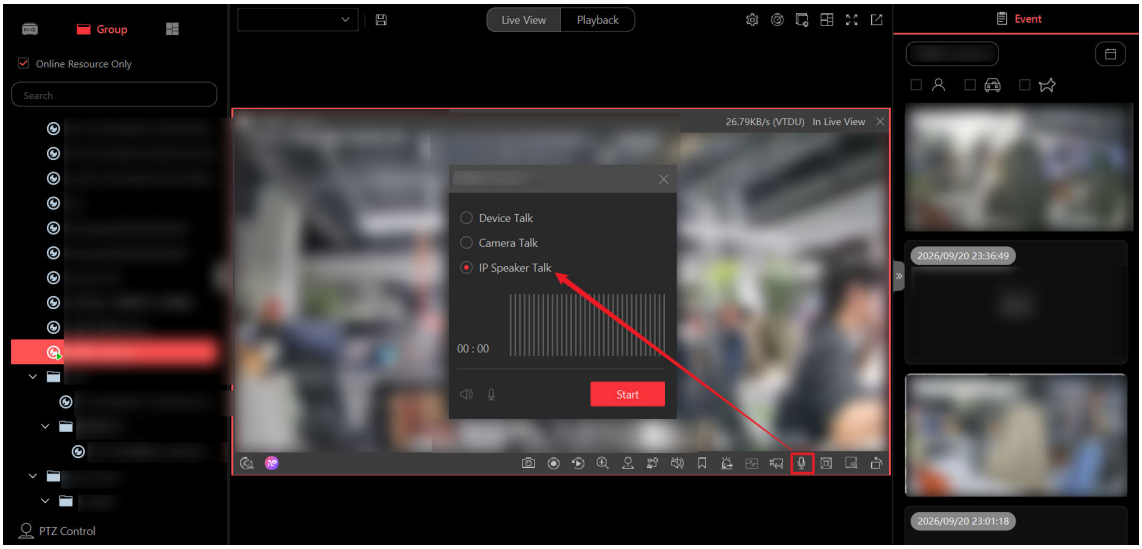
On the Device Configuration page, go to **Device → Audio Device →** and click a speaker name.



Click **Related Camera → + Camera** to link a camera with the speaker.



Click the speak icon on the toolbar to start speaking.

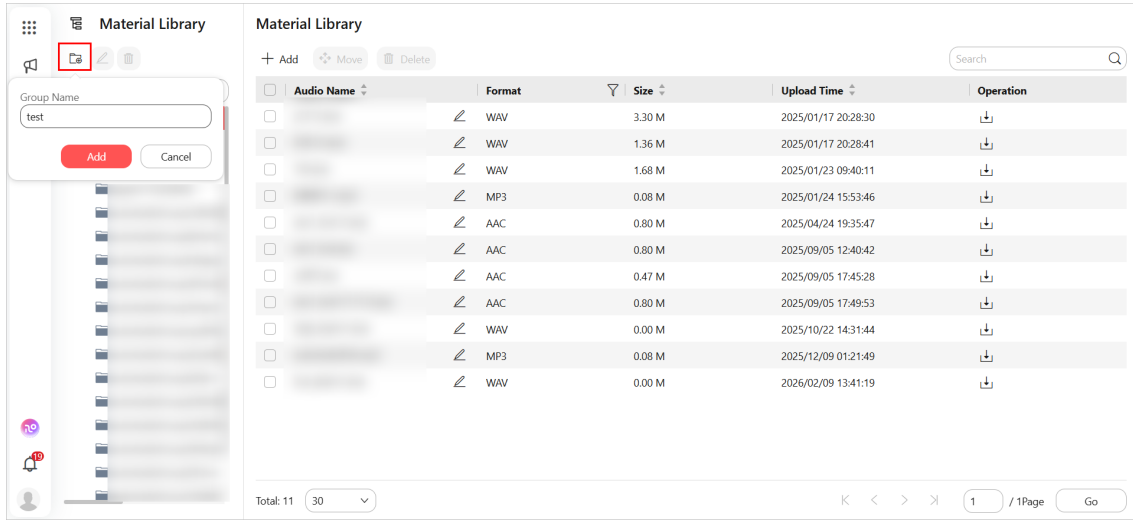


12.3 Upload Audio File

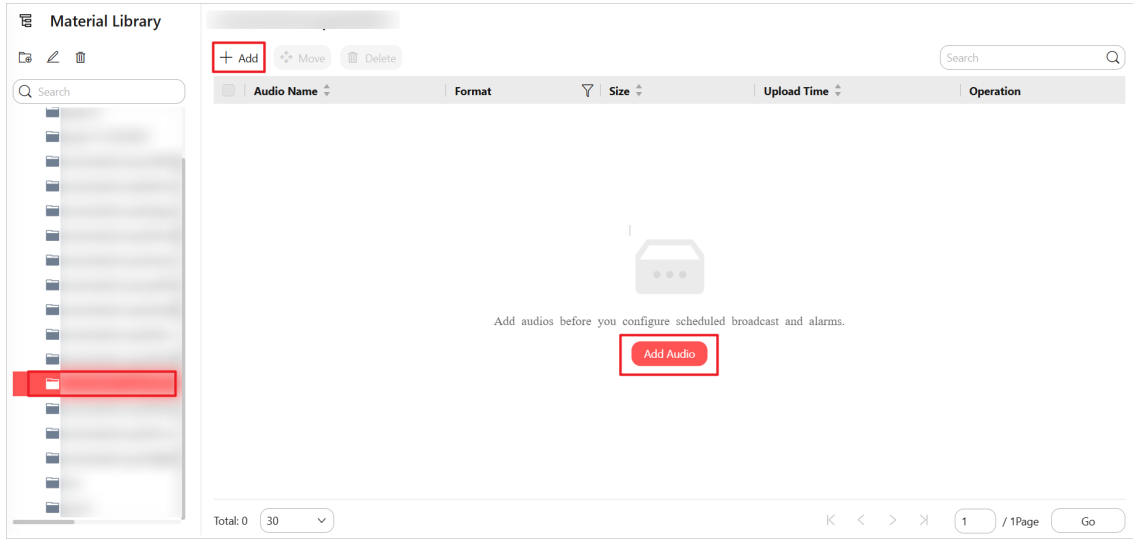
Uploading audio files is required before you add a scheduled broadcast task. You can upload audio files from your local computer, then add them to a scheduled broadcast task to play them at specific times.

Go to **Audio Broadcast → Material Library** .

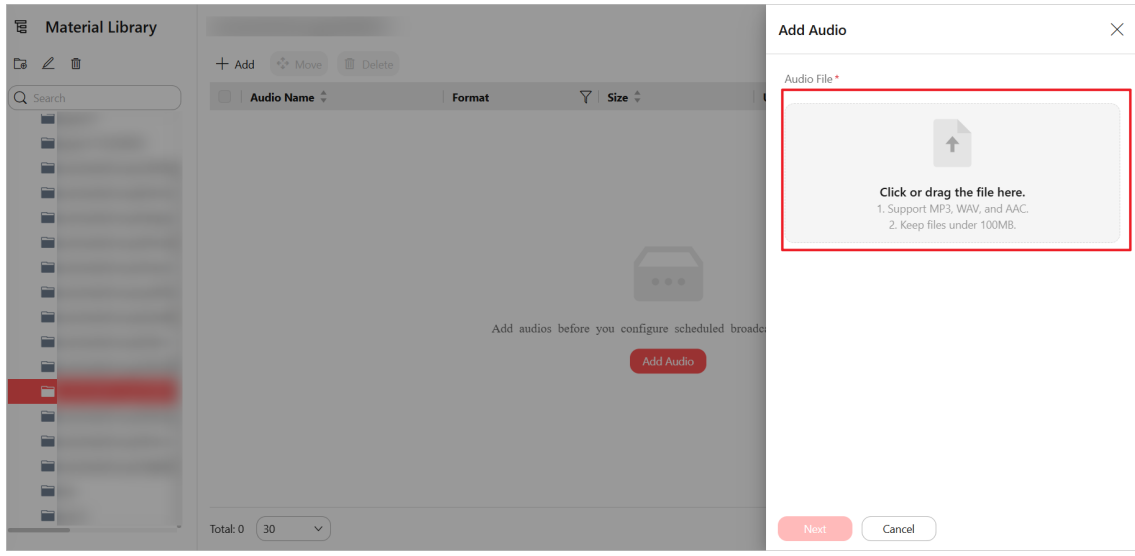
Click the icon to add an audio group.



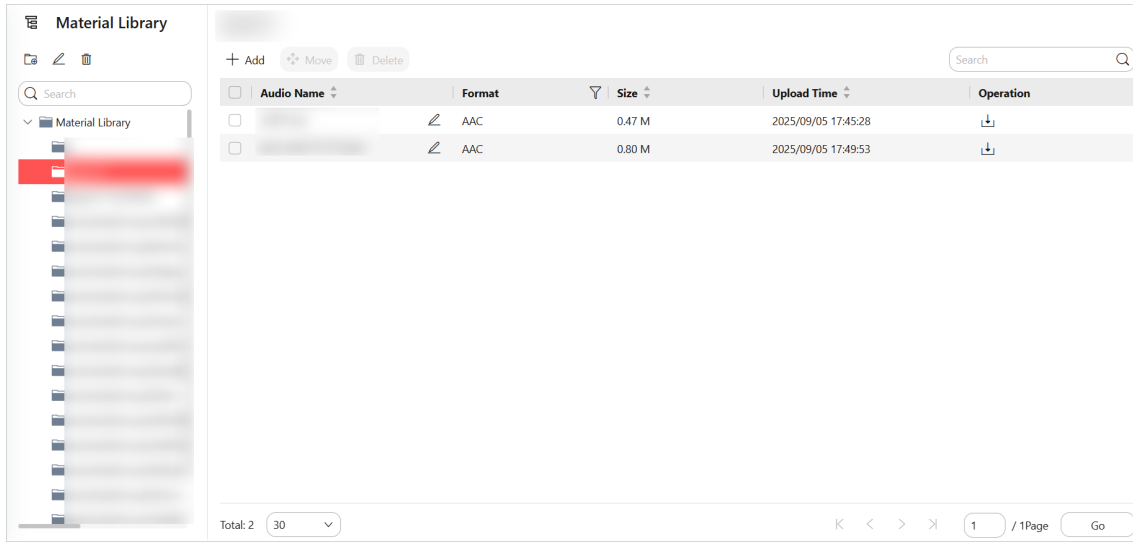
Click **Add** to add audios to the audio group.



Click the section to upload files or drag the files here and click **Next**.



You will see the audio files on the page.

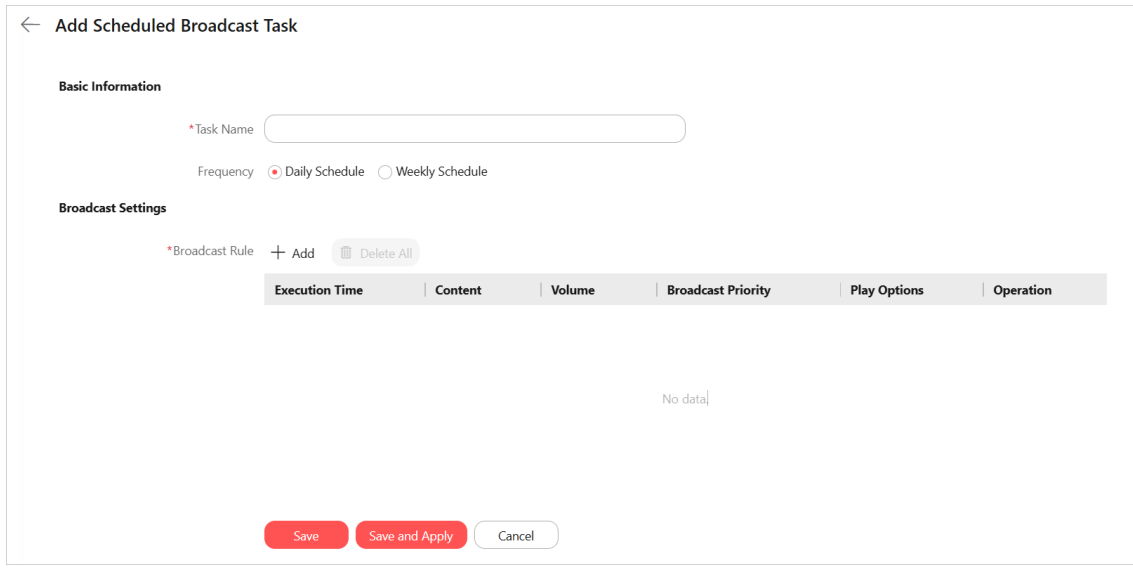


12.4 Add a Scheduled Broadcast Task

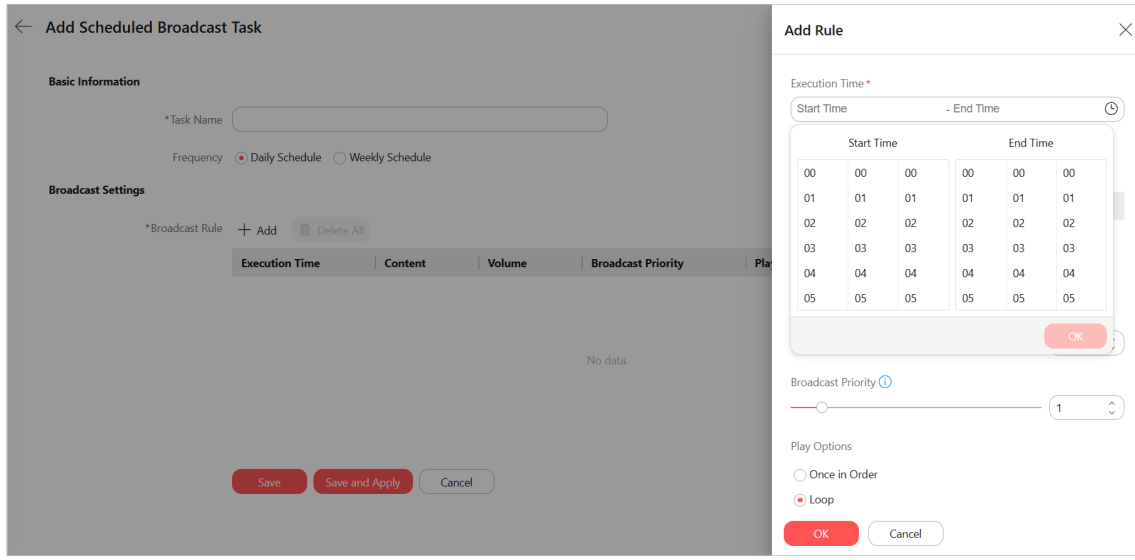
Scheduled broadcast tasks enable the device to play your uploaded audio files at fixed times through network speakers. Common use cases include corporate announcements (broadcasting company news, important notices, or emergency information to employees), school notifications (playing interval music, class schedule reminders, or emergency evacuation instructions), hotel services (timely broadcasting of welcome messages, room service introductions, or event arrangements), public spaces (playing background music, safety tips, or missing person announcements in malls and stations), and community announcements (regularly broadcasting weather forecasts, event notifications, or emergency alerts).

Go to **Audio Broadcast → Scheduled Broadcast Task** .

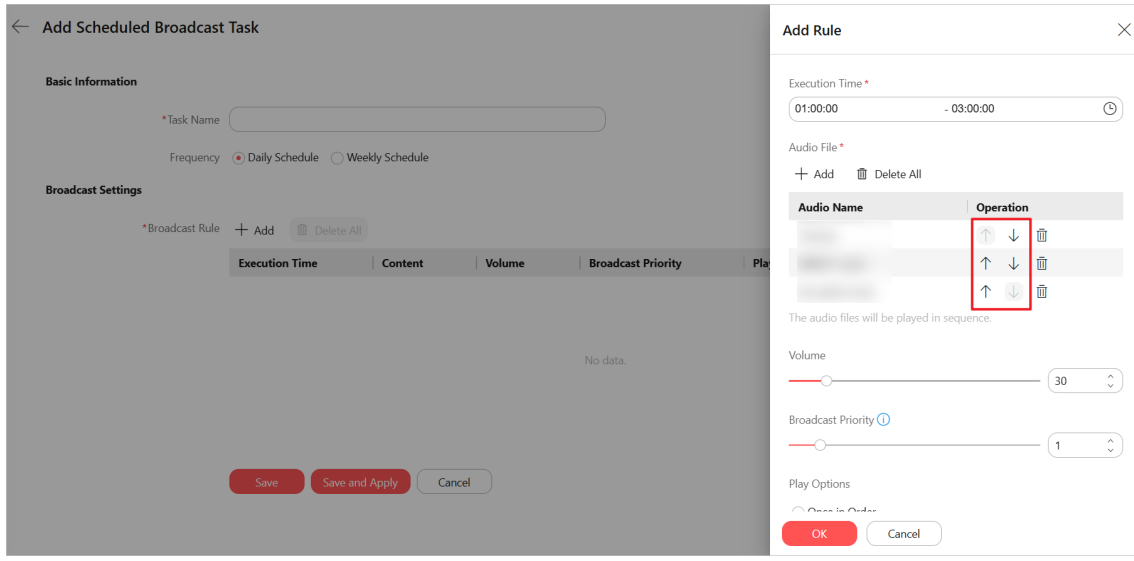
Enter a task name, and select daily or weekly schedule. For a weekly schedule, you can select days of a week such as Monday to Friday.



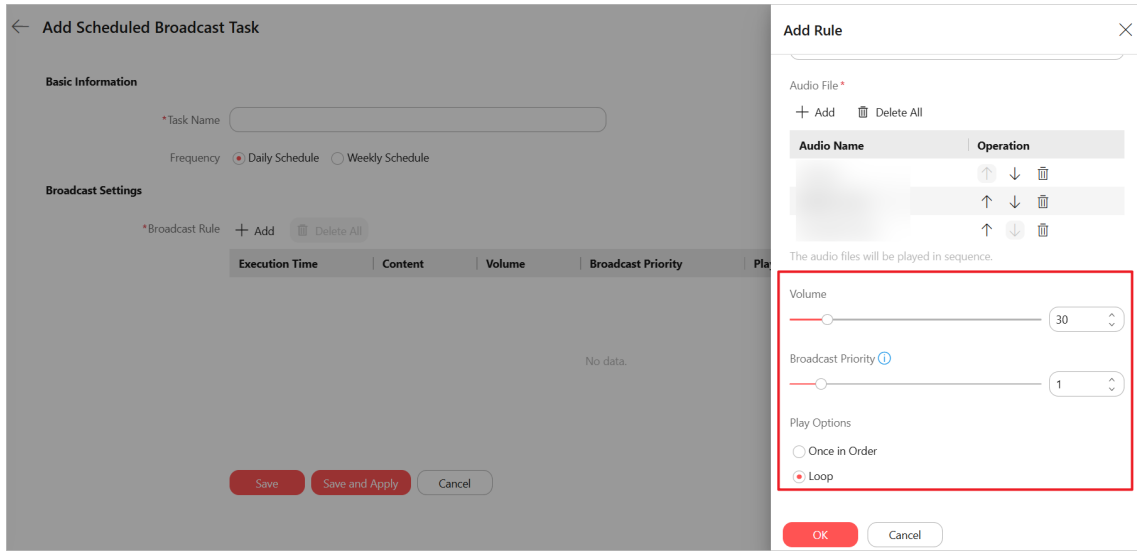
Click **Add** to open the Add Rule pane, and select the time when the task takes effect.



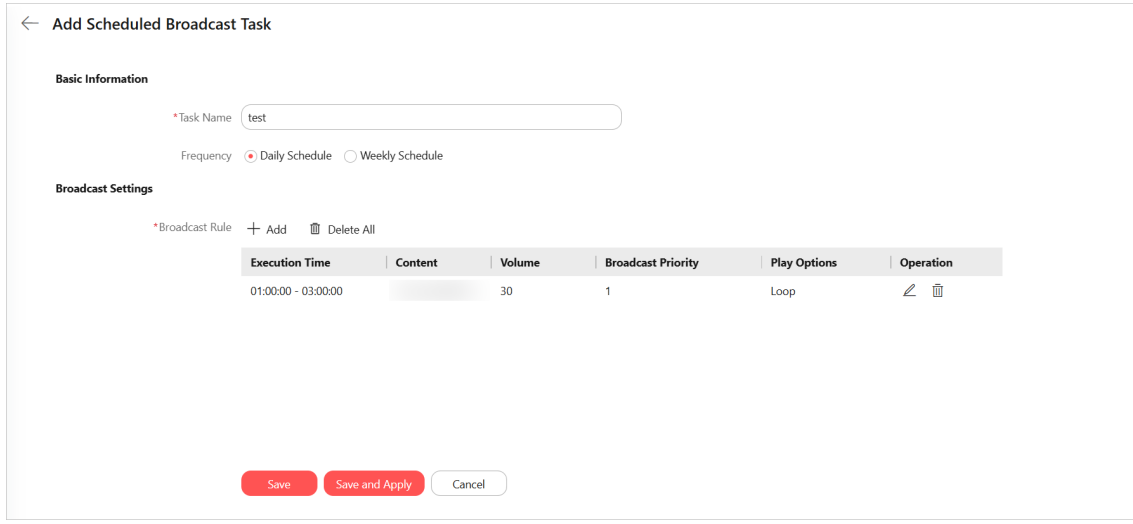
Click **Add** to upload audio files and edit the order of the files.



Set other parameters. Once in order means the audio files will be played once in order; loop means when the last audio is over, the first audio file will be played again.



Clock **Save and Apply** to apply the settings to the speakers.


Add Scheduled Broadcast Task
Basic Information
*Task Name
test
Frequency
Daily Schedule
Weekly Schedule
Broadcast Settings
*Broadcast Rule
Add
Delete All
Execution Time
Content
Volume
Broadcast Priority
Play Options
Operation
01:00:00 - 03:00:00
30
1
Loop
Save
Save and Apply
Cancel

Chapter 13 Network Device

You can set up the captive portal to control access to the network. When users access your network through a captive portal, they are required to authenticate using credentials and/or agree to certain terms and conditions. You can set authentication policies, customize portal pages, set authentication network segments, set authentication credentials (accounts, vouchers) and other information.

13.1 Set Up Captive Portal

You can set up a captive portal by customizing a portal page (portal template) first, and then adding an authentication policy and linking to a portal page.

On the Device page, check an AC router, and click **Captive Portal**.

1.

Parameter	Description
Template Name	The name of a portal page template.
Authentication Mode	The login options for users to access the network. **One-Click** Login without the user name and password. You can set the **Access Duration**. Users need to log in again when the duration is up. **Voucher** Login with a random 8-digit passcode. **Account** Login with the account and password.
Post-Login URL	The URL to which users are redirected to after successful authentication.
Terms & Conditions	The privacy policy to which users' consent is required.
Logo	Set whether to display the logo, upload the logo image, and set the logo size and position.
Background	Upload the background image.
Welcome Text	Enter the welcome texts, and set the color and size.
Copyright	Enter the copyright, and set the color and size.

2. Click **Policy → Add** . Set the required parameters and click **Save**.

Parameter	Description
Policy Name	The name of a captive portal.
Seamless Online	When enabled, after a successful authentication, subsequent connections to the Wi-Fi network will be auto authenticated within the set period of time.
Seamless Online Period	The period within which connections are auto authenticated after a successful authentication.
VLAN	The VLANs of AC routers that require authentication.
Portal Template	The portal page that is displayed for authentication.

13.2 Mange Users

Add Accounts

For account authentication, users can access the specified Wi-Fi network using the valid accounts.

1. Click **Account → Add** . Set the user name and password, select the user group, and tap **Save**.

Parameter	Description
User Name	The user name for authentication.
Password	The password for authentication.
User Group	Defines the number of concurrent devices, and access duration.

Add Vouchers

For voucher authentication, users can access the specified Wi-Fi network using the valid vouchers.

1. Access the captive portal settings of the AC router.
2. Click **Voucher → Batch Add** . Set the quantity of vouchers to generate, select the user group, and click **Save**.

Parameter	Description
Quantity	The number of vouchers to generate.
User Group	Defines the number of concurrent devices and access duration.

Add User Group

Add a user group to specify the access duration and number of concurrent clients. When you add accounts/vouchers, select a user group to apply the settings.

1. Go to the captive portal settings of the AC router.
2. Click **User Group → Add** . Set the number of concurrent clients and access duration, and click **Save**.

Parameter	Description
Group Name	The user group name.
Concurrent Clients	The number of concurrent devices for one account/voucher.
Access Duration	Clients will be auto disconnected after the access duration, and authentication will be required for reconnection to the Wi-Fi.

Chapter 14 Device Management

14.1 How to set parameters on the device local page before adding devices to the system?

1. Go to → → **Device Compatibility List** to make sure the device is supported by the platform.

   Note

   - If the firmware version of your device is lower than that listed in the document, a version upgrade is required, otherwise some of the functions may not be supported.
   - Devices NOT listed in the document may also be added to Hik Connect for Teamst, but if added, some of the Hik Connect for Teams functions may be inaccessible. The service is available only when devices are added via Hik-Connect (P2P).

2. Before adding on-board devices to your Hik Connect for Teams system, you should enable Hik-Connect access.
   a. Enter the device IP address in the browser address bar to open the device local page and go to **Configuration → Network → Platform Access** .
   b. Check **Enable** and select **Hik-Connect** in the Platform Access Mode field. For on-board devices, select **Guarding Vision** as the Platform Access Mode.
   c. Enter the device serial No. / encryption password (they are the same by default).
   Find the serial number of the device in one of the following ways:
      - Open the device web page and go to **Configuration → System → System Settings → Basic Information** . Usually, the serial number is the last 8 digits plus the previous letter or the last 9 digits of the character string displayed in the Serial No. field.
      - Check the label on the device itself or on its packaging. The serial number is the string of 9 characters (letters/digits) that follows "SN".

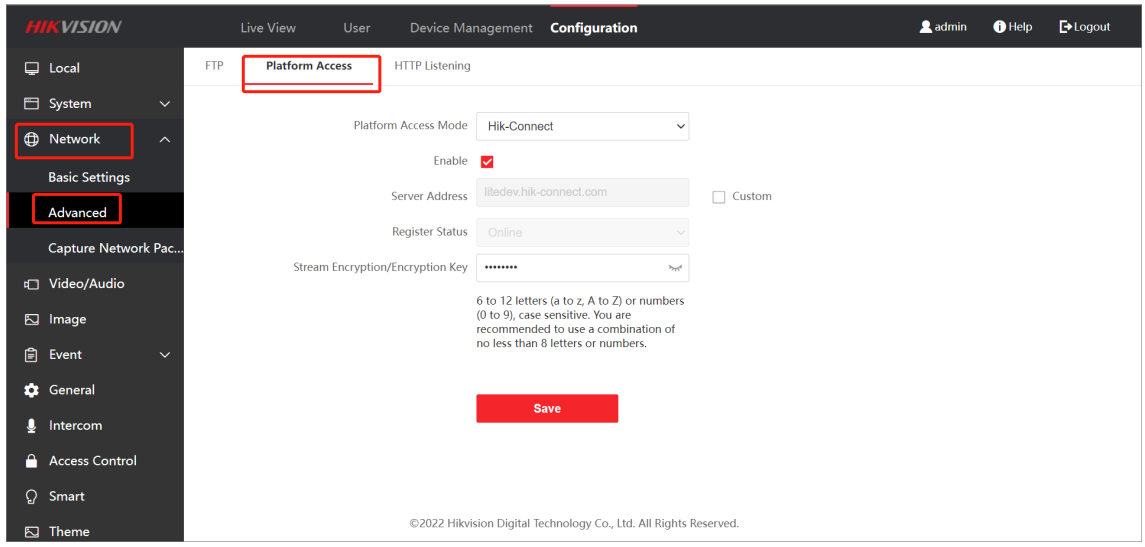


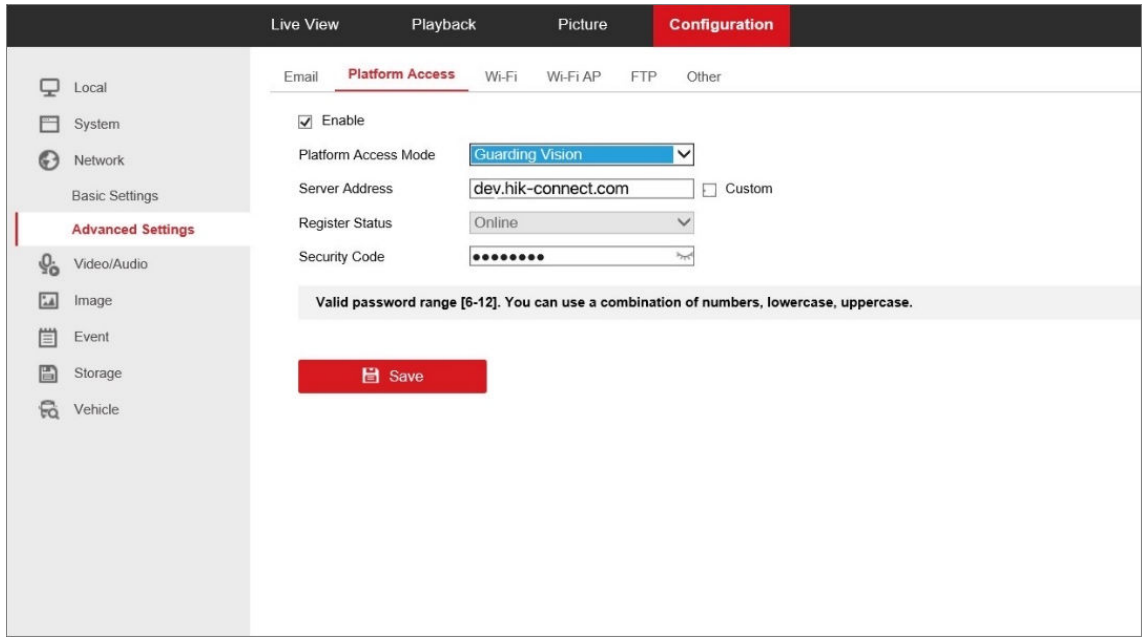
Figure 14-1 Find Serial Number on Device Label



Figure 14-2 Find Serial Number on Device Packaging

d. Make sure the register status is online, and click **Save**.





14.2 How to add devices to Hik Connect for Teams?

(Required) How to add groups?

Go to **Device**.
On the left pane, click + to add a group.

How to add devices?

1. Add Groups to Manage Devices: Click → **Device** → + on the left pane to add a group first.
2. Add devices to groups.

Table 14-1 Add Devices

User Intention	Method
Add Detected LAN Devices: The devices connected to the same network with the Portal can be detected, and the device information (e.g., IP address) will be recognized by the Portal. Based on the information, you can add the devices quickly.	Make sure the devices to be added are correctly installed and connected to the same LAN with the PC running the Portal. a. In **Online Device** section at the bottom of the Device page, select the detected devices, click **Activate**, and enter the password to activate them. b. Check the device(s) to be added, and click **Add to Device List** to enter the Add Online Device page. c. Enter the device verification code, and click **Next**. The verification code is the stream encryption key you set on the device configuration page when enabling the Hik-Connect service.
Add Devices through Device Serial No. and Verification Code	- Make sure the encoding device you are going to use is correctly installed and connected to the network as specified by the manufacturers. - Make sure ***you have got the device serial No.*** and verification code. In general, the verification code is the stream encryption key you set on the device configuration page when enabling the Hik-Connect service. Click + Add → **Add Device** to enter the Add Device page.
Import Devices via Excel	You can also click + Add → **Import via Excel** to batch add devices via the given template with device information.
Import Personal Devices	The Hik-Connect has the Hik-Connect Personal mode and the Hik Connect for Teams mode. Hover over the account name on the top right corner and select **View Personal Devices** to go to Hik-Connect Personal page in portal mode and view your devices. a. On the top navigation bar, click **Device** → to enter the Import Personal Device page. b. Set the parameters, and click **Import** or **Import More**.

What are the operations after devices are added?

Table 14-2 General Device Operations

User Intention	Descriptions
Unbind a Device from Its Current Account	In the Online Device area, click in the Operation column of an active device, enter password and verification code, and click **Confirm**.
Remote Configurations	Click in the Operation column to set the remote configurations of the corresponding device. **Note** For details about the remote configuration, see the user manual of the device.
Edit Device	Click the device name to view and edit the device basic information, time zone related information, etc.
Create Password for Inactive Device(s)	In the Online Device area, select one or multiple inactive devices, and click **Activate** to open the device activation window. Enter the password, and click **Activate**.
Edit Online Device's Network Information	For a detected online device, you can remotely edit its network information such as the IP address and port No. on the Portal. In the Online Device area, click in the Operation column of an active device.
Reset Device Password	In the Online Device area, click on the Operation column of an active device to reset its password.
Upgrade Device Firmware	On the device list page, if the device is offline, or the device firmware version is too old, an icon will appear on the right side of the device. On the device list page, if the device is offline, or the device firmware version is too old, an icon will appear on the right side of the device.
Export Device Information	You can batch export the information of a certain device type and view the information in an Excel file. In this way, our technical support can locate and solve the problems more efficiently. On the top navigation bar, click **Device and Maintenance → Resource Management** . Select a group in the area list, and select a device type on the right pane. Click **→ Export** .

User Intention	Descriptions
Change Verification Code	Device verification code can be used for device adding, as well as picture and video encryption. You can set or change the device verification code. Select the added device(s), click **Change Verification Code**, and set or edit the verification code as needed.
Enable/Disable Stream Encryption	Select the added device(s), and click **Enable Stream Encryption** or **Disable Stream Encryption** to enable or disable stream encryption. If enabled, you should enter the device verification code to view pictures and videos of the camera.
Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Move Device	Select the added device(s), click **Move to Other Area**, select a new area in the list, and click **Move** to move the selected device(s) to the new area.
Wake Up Solar-Powered Camera	Click to wake up the solar-powered camera whose status is asleep. You can also click the device name to enter the editing device page, and click **Wake Up** to wake up the device.
Test Network	Click in the Operation column to see the average upstream rate of a device.
Delete Device	Select the added device(s) and click **Delete** to delete the selected device(s).

How to set access control parameters?

Select one or multiple devices in the device list and click **Set Device Parameters** to set device parameters.

Privacy Settings	**Storage Mode** Set the event storage mode. Select **Overwrite**, **Delete Old Events Regularly** (and set a period), or **Delete Old Events by Specified Time** (and specify a time). **Result Display** Check the items to be displayed in authentication results. **Picture Uploading and Storage**

	Check items as needed.
Skin-Surface Temperature	Enable **Temperature Measurement** to set parameters. **Temperature Measurement Mode** Select **Authentication + Temperature Screening** or **Temperature Screening** as the mode. **Threshold(℃)** Set the range of normal skin-surface temperature. The detected temperature that is not in this range is abnormal temperature. The maximum temperature must be higher than the minimum temperature. **Open Door When Temperature is Abnormal** If enabled, the door will open when person's skin-surface temperature is abnormal. By default, it is disabled.
Mask Settings	Enable **Mask Settings** to set parameters. **No Entry Without Mask** If checked, the barrier will not open for persons without masks.
Card Swiping	**Voice Prompt** If enabled, an audio prompt will be played when a person swipes a card. **M1 Card Encryption** Enable **M1 Card Encryption** and select encrypt sector as needed. Only the cards with the same encrypted sector can be granted.

Chapter 15 Services

15.1 How to invite a service provider to manage your system?

You have two ways of purchasing services. One is to invite a service provider and ask the service provider to purchase and activate services for you. The other is to ask your service provider to purchase licenses and hand over license codes to you and you activate services by yourself. Either way a service provider is required for purchasing services.

1. Go to ⁞⁞ → **Service** → **Service Provider** to invite a service provider (a Hik-Partner Pro user) to manage your system.
2. After the service provider accepts your invitation, the service provider can purchase and activate services for your account.

15.2 How to activate services and purchase services?

- Activate Services:
  Go to ⁞⁞ → **Service** → **Service Market** → **AI Services** to activate AI services.
  Go to ⁞⁞ → **Service** → **Service Market** → **Basic Services** → **Activate** to activate a basic service.

  Note

  The AI features are only available in certain countries or regions.
- Purchase Services by Activating License Code by Yourself:
  1. Ask a service provider to buy licenses for you and get the license codes, or buy a license from our sales team.
  2. Go to ⁞⁞ → **Service** → **My Services** → **Activate License** to expand your package capacity or renew a service.
- Ask Service Provider to Purchase Service:
  After the service provider accepts your invitation, the service provider can purchase and activate services for your account.

15.3 How to transfer cloud storage?

Go to ⁞⁞ → **Service** → **My Services** → **Cloud Storage Service** → **View Details** .

You can transfer active cloud storage licenses between channels in the same system. When deleting devices with active licenses, the system provides transfer guidance to prevent accidental loss.

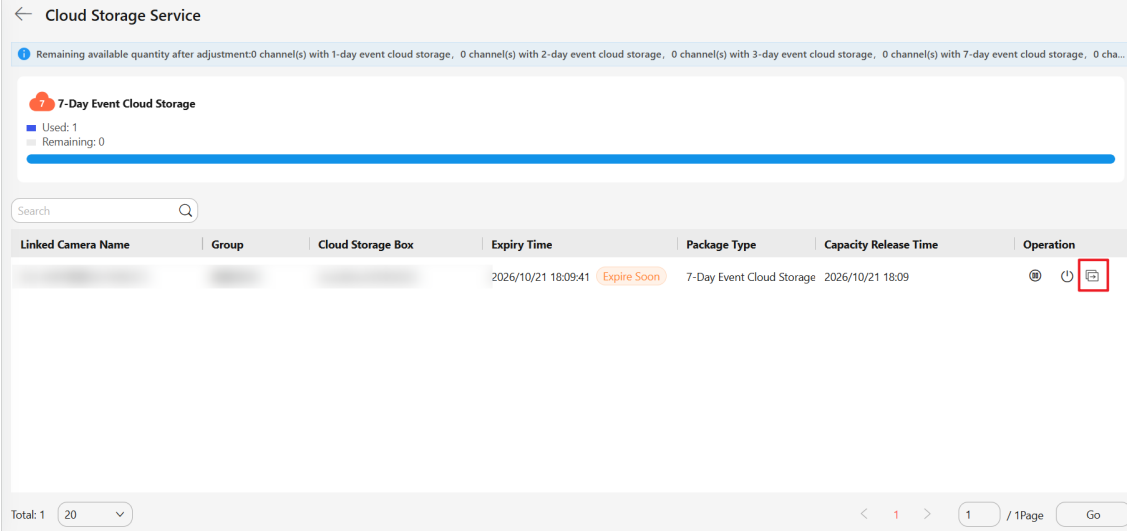


Figure 15-1 Transfer Cloud Storage Service

15.4 How to view password usage records?

Go to → **Service** → **My Services** → **Password Usage Records** .

You can view the device, channel, time, and purpose of password usage.

15.5 What are the AI services and how to use them?

- For the Video AI service, you can activate a maximum of 64 channels for each system. For the gun detection service, you can activate a maximum of 16 channels.
- The video AI service is an independent service with the video service. Make sure to activate the video service before activating the Video AI service for your channels.
- The AI features are only available in certain countries or regions.

15.5.1 Focus

Follow specific people, vehicles, unknown targets, or describe what you're looking for in natural language. Matching events are automatically delivered to you.

Go to **Video** → **Focus** .

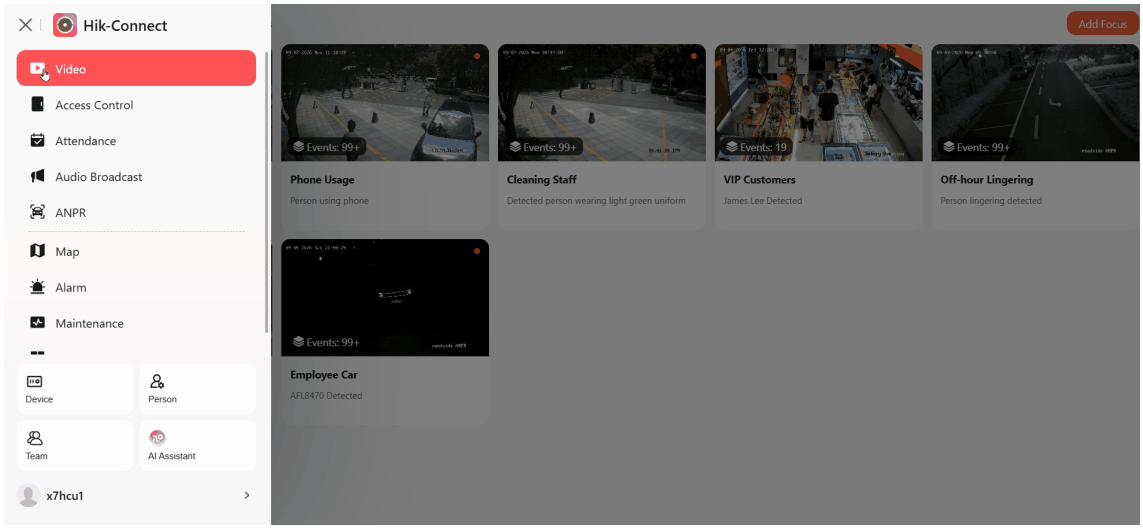


Figure 15-2 Focus

Background & Purpose

Security systems generate a flood of alerts daily, most of which are irrelevant to you. Important events get buried. Focus lets you zero in on what truly matters—specific people, specific vehicles, or custom scenarios target behaviors described in plain language. The system continuously monitors these subjects and delivers precise alerts, freeing you from notification noise.

Key Features

- **Focus on Specific People:** Select known individuals (family, employees) from your cloud person library, or choose "Unknown Person" to monitor strangers.
- **Focus on Specific Vehicles:** Select vehicles from your license plate library to track their entry, exit, or lingering behavior (requires ANPR camera).
- **AI Custom Focus:** Describe a scenario in everyday language, e.g., "Detecte person carrying handbag" The system monitors accordingly.
- **Real-Time Push & Refresh:** Receive a push notification on App when a focused subject triggers an event.

Example

- Scenario 1: Select a vendor vehicle's plate from your waste & recycling library. Get notified the moment it enters the premises, and tap to view its full entry/exit trajectory.
- Scenario 2: Choose a VIP customer from the VIP Lost. Receive alerts for the customers when they enter your store.

Limitations

- You can add a maximum of 64 focus rules per user.
- You can add up to 16 people and 16 vehicles per focus configuration.

15.5.2 AI Notification

Go to **Alarm → AI Notification Configuration** .

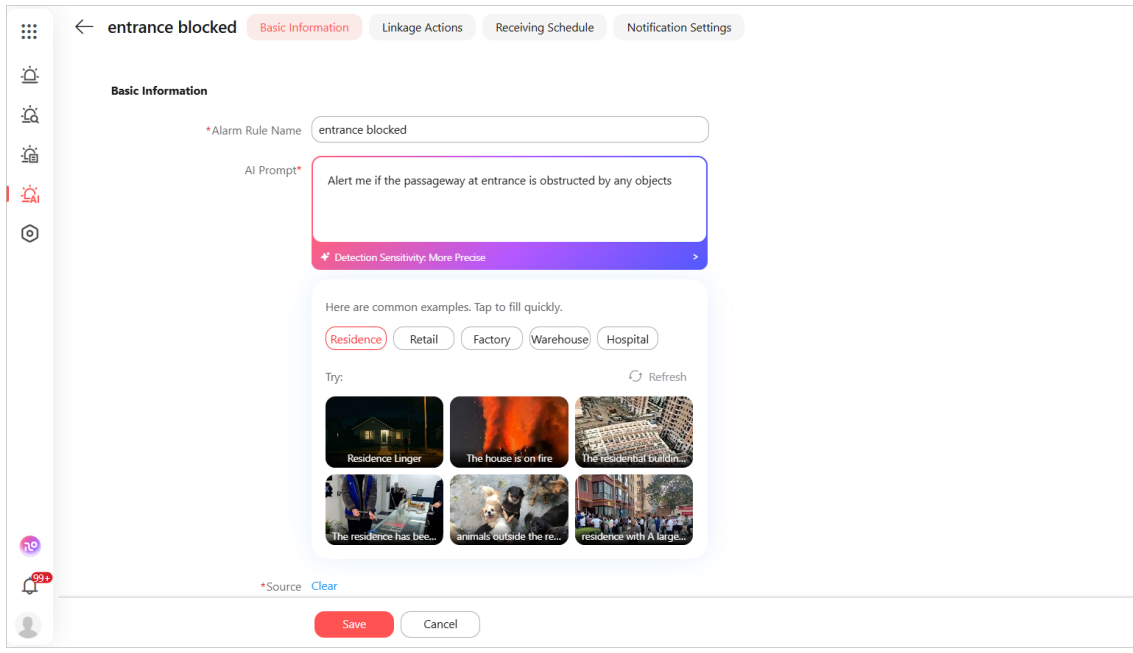


Figure 15-3 AI Notification

Background & Purpose

Leveraging AI's natural language understanding, the system turns your everyday descriptions into custom alert rules—so you'll get timely notifications for the events you care about.
For non-customized motion detection events with AI service enabled, notifications now include a description like "A man in black placed a package at the door."

Key Features

Natural Language Input: Describe an alert scenario in plain text, e.g., "Alert me if the passageway at entrance is obstructed by any objects".
Effect Preview: After configuration, the system instantly check matching results from the past 24 hours to verify accuracy, and then presents a structured rule for your review and fine-tuning.
AI Processing: The system automatically identifies targets (person/vehicle), behaviors (appear/linger/loiter).
Dedicated Event List: A new **AI Notification Configuration** tab consolidates all AI notifications, with support for deletion, and type filtering.

Example

- Alert me if a person wearing uniform appeared.
- Alert me if the passageway at entrance is obstructed by any objects.

Limitations

- Supports a maximum of 16 rules per channel.
- Only available for channels with the Video AI service enabled.

15.5.3 AI Deterrence

AI Deterrence detects intrusions in real time and instantly responds with AI-generated, targeted voice warnings, like calling out "the person in the blue shirt, please leave." to maximize deterrence.

Go to **Alarm → General Alarm Configuration** , add an alarm rule, set intrusion as the triggering event, and set AI Deterrence as the linkage action.

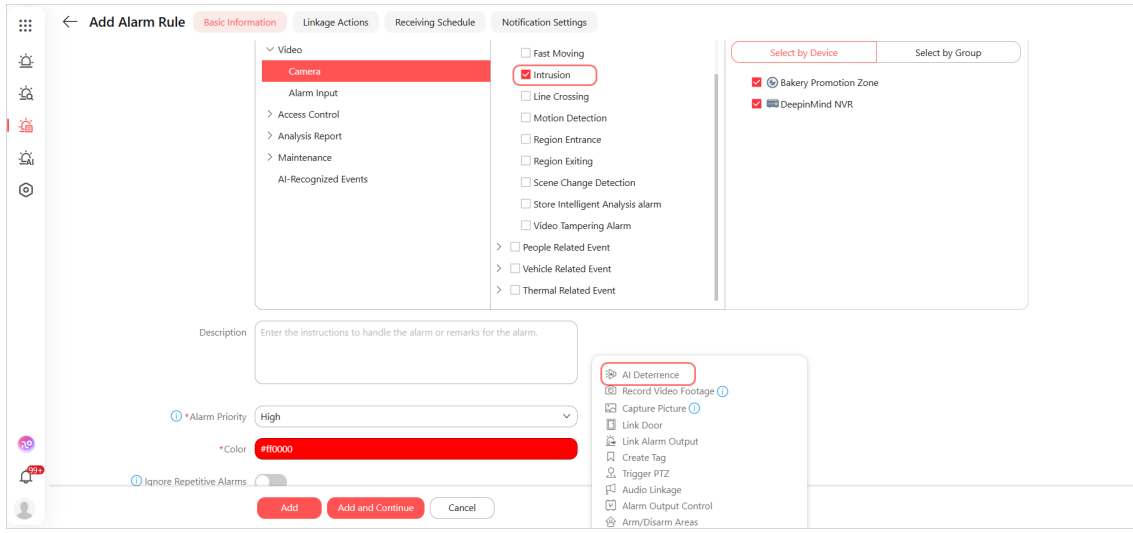


Figure 15-4 AI Deterrence

Background & Purpose

AI automatically triggers active intervention such as voice warnings the moment abnormal event is detected. This transforms security from "after-the-fact recording" to "preemptive deterrence," stopping threats before losses occur and significantly reducing the need for constant human monitoring.

Key Features

- **Three-Tier Escalation**:
  - Level 1: Initial warning (customized text, no AI)
  - Level 2: AI-detected attributes + warning (please leave)
  - Level 3: AI-detected attributes + escalated warning (security has been notified)
- **AI-Powered Voice Alerts:** With the video AI service, the system analyzes specific target features (clothing color, behavior) in real time and generates targeted verbal warnings, delivering a far stronger deterrent than fixed audio.

- **Device Integration:** Compatible with IP Speakers for custom audio broadcasting and IPC strobe lights for visual alarm.
- **Auto-Reset:** The deterrence level automatically resets if the alarm is interrupted for more than 2 minutes, preventing false escalation.

Example

Nighttime Store Protection: A person enters the doorway after 11 PM → L1 plays "You are in a monitored area, please leave immediately" → The person lingers for over 2 minutes, triggering L2: "Man in black jacket, please leave" with lights on → They still do not leave, triggering L3: "security has been notified".

Limitations

- An IP Speaker or a camera with strobe light capability is required for voice and visual alarm functions.
- The deterrence level automatically resets if the alarm is interrupted for more than 2 minutes.

15.5.4 Daily Summary

The feature analyzes 24 hours of video and events of a camera, automatically generating a daily overview with counts of people, vehicles, animals, suspicious events, and AI alarms—all in one place for quick review.

Go to **Video → Camera → Daily Summary** .

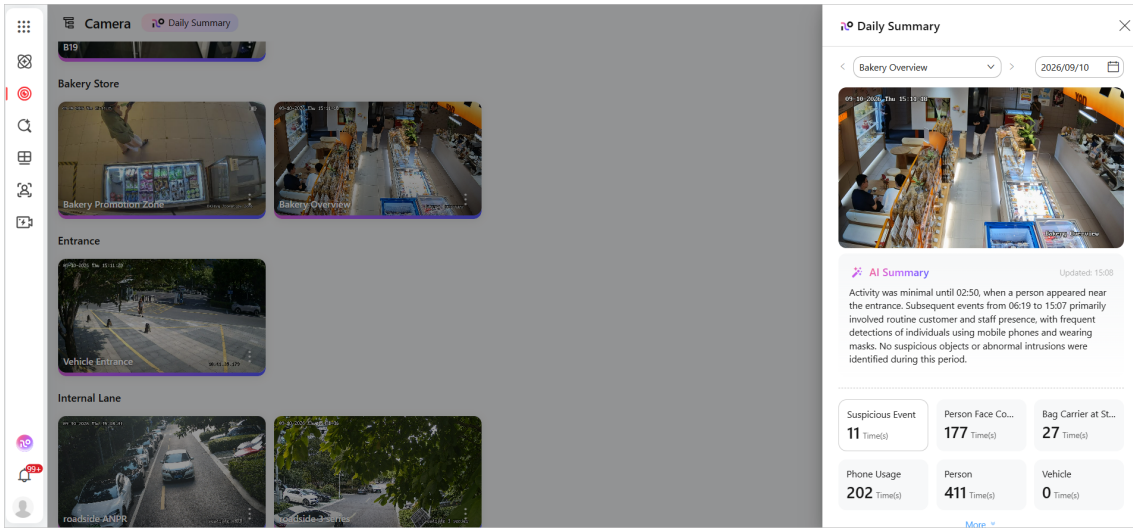


Figure 15-5 Daily Summary

Background & Purpose

Reviewing numerous daily events one by one is time-consuming and makes it easy to miss critical issues. The "Daily Summary" feature solves this by intelligently analyzing 24-hour events in your

space. It automatically generates a summary report and highlights events that need your attention, helping you quickly grasp the overall security situation.

Key Features

1. **AI Summary**: Generates a daily overview, counting events involving people, vehicles, and animals.
2. **Key Event Collection**: Categorizes abnormal events (e.g., suspicious events, AI alarms, focus, etc.) for quick review. Playback of event footage is available with one click.
3. **One-Click Alarm from Suspicious Events**: You can instantly convert a "Suspicious Event" found in the report into an AI notification, enhancing your security setup rapidly.

Example

Activity was minimal until 02:50, when a person appeared near the entrance. Subsequent events from 06:19 to 15:07 primarily involved routine customer and staff presence, with frequent detections of individuals using mobile phones and wearing masks. No suspicious objects or abnormal intrusions were identified during this period.

Limitations

- The report is based on event data from 00:00 to 24:00 of the selected day.
- You can view daily reports for the last 7 days.

15.5.5 Fusion Search

Enter a name, license plate, etc. and the AI assistant can search for access control, vehicle, and other records of the target, and display all results on a chronological timeline with time, location, and snapshot for each record.

Click to open AI Assistant.

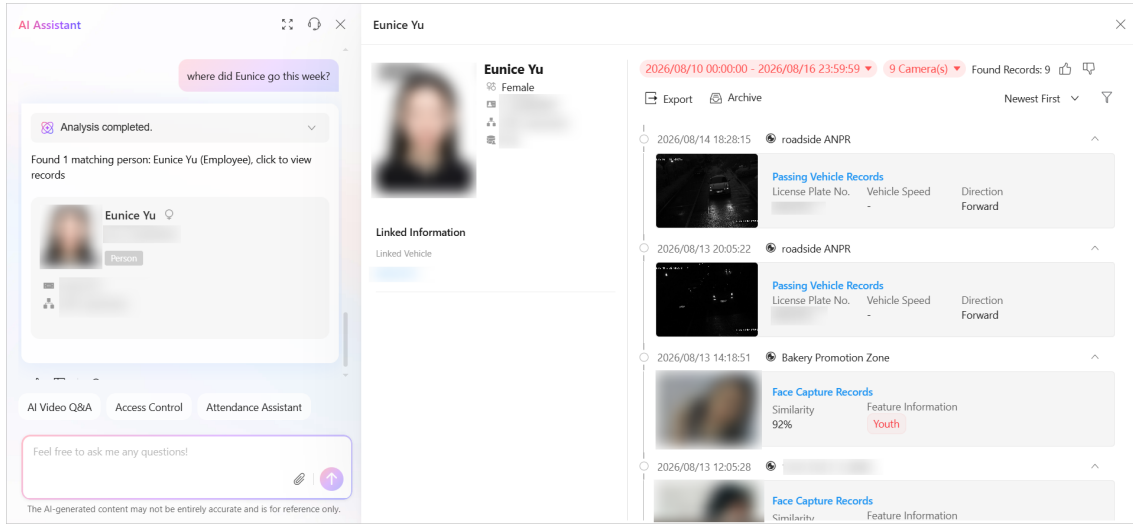


Figure 15-6 Fusion Search

Background & Purpose

During security operations, a target's information is scattered across multiple systems such as person records, access records, face captures, and vehicle data. Traditionally, you'd search each module separately. With Fusion Search, just type a query like "Find all records for John," and the system automatically searches across all systems, consolidating everything into one clear timeline, dramatically improving efficiency.

Key Features

- **Natural Language Search**: Enter names, license plates, phone numbers, or employee IDs in everyday language such as "Find John's access records" or "Find license plate xxx's passage records," to focus on exactly what you need.
- **Cross-System Aggregation**: Automatically searches personnel database, visitor database, face library, access control logs, and vehicle passage records, consolidating all records for the same target.
- **Timeline Display**: Results are displayed in chronological order on a timeline, mixing access control records, face captures, and vehicle passage records. Each entry includes time, location, and snapshot.
- **Export & Archive**: Export search results as files or save them as evidence for easy preservation and sharing.

Example

- **Person Search**: "Find Tom" → Displays Tom's basic info + a timeline of all today's access, capture, and vehicle records.
- **Vehicle Search**: "Find license plate ZA12345" → Displays vehicle info + owner info + all today's passage records.

Limitations

Default search range is today's data; time range can be adjusted via filters or natural language query.

15.5.6 AI Timeline

Pause the video during playback, select a target, and the system will automatically retrieve all appearances of that target across relevant channels, presenting them on a unified timeline for playback.

Start playback, pause the video, select a target, and the system will automatically retrieve all appearances of that target across relevant channels.



Figure 15-7 AI Timeline

Background & Purpose

During security reviews, tracking a target across cameras used to require manually opening multiple recordings and jumping between timestamps. Now, simply pause the video, select a target, and the system automatically retrieves all appearances across cameras on a unified timeline for synchronized playback, making cross-camera tracking simpler.

Key Features

1. **Pause to Detect**: Pause at any moment during playback, and the system will automatically identify people in the frame with bounding boxes. Click to select your tracking target.
2. **Unified Timeline Playback**: Once a target is selected, the system retrieves all appearances of that target across all channels for the day, generating a timeline for synchronized multi-channel playback.
3. **Dynamic Target Addition**: While the timeline is playing, you can pause at any time, select a newly appearing target, and add it to the current tracking list for parallel multi-target tracking.
4. **Map Integration**: If an e-map is configured, you can view the target's movement trajectory on the map during playback for clear spatial context.
5. **Flexible Parameter Adjustment**: Modify the time range (up to 24 hours), filter cameras, adjust playback speed, and disable/enable specific segments on the timeline at any time.
6. **One-Click Export & Archive**: After tracking, package the entire timeline and associated video clips into an HTML report for offline playback without plugins—ideal for evidence preservation and sharing.

Example

Scenario: Items are missing from a warehouse, and a suspect is believed to have moved from Area A to Area B.
Operation: Pause the Area A video during playback, select the suspicious person → The system automatically generates a timeline of that person's appearances across all channels for the day → The timeline shows the complete trajectory from Area A, through the corridor, to Area B → Export the report with one click as evidence.

Limitations

- The timeline only supports video channels; access control events are not currently supported.
- A maximum of 2 persons or one person and one vehicle can be tracked simultaneously.
- The maximum time range span is 24 hours.
- Export functionality is available via the Portal, supporting both plugin-free and plugin-based methods.

15.5.7 Gun Detection

1. Go to **Alarm → General Alarm Configuration** .
2. Add an alarm rule and set **Gun Detection** as a triggering event.

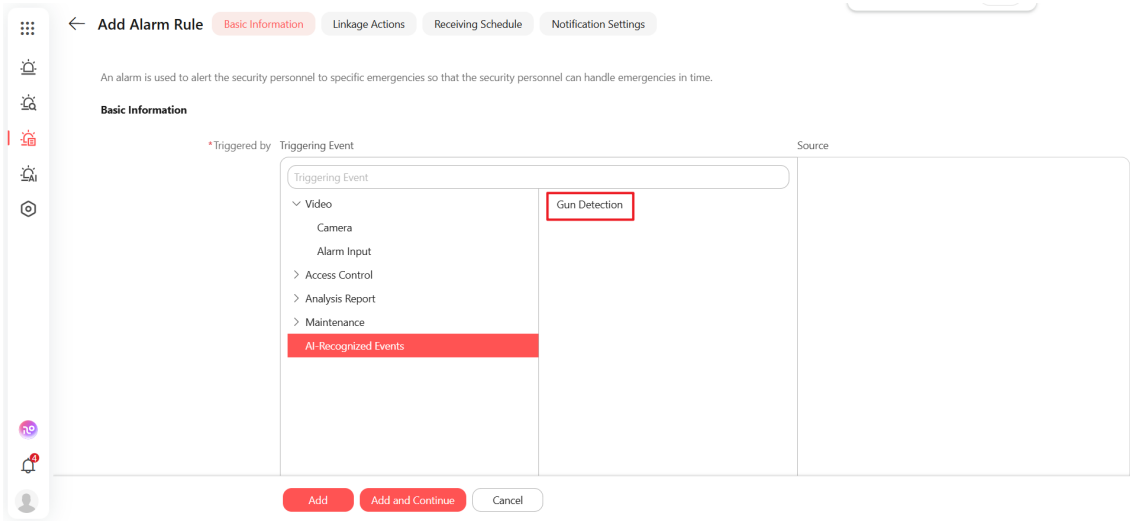


Figure 15-8 Gun Detection

Background & Purpose

In high-risk places like schools, malls, and business parks, manual monitoring often misses firearms in real time, delaying responses. The Gun Detection feature uses AI vision to analyze live surveillance footage. When a suspected firearm is detected, an alarm is instantly triggered and pushed to you, shifting security from post-incident response to pre-incident intervention and saving valuable time.

Key Features

1. **Real-Time Automatic Detection**: When motion detection is triggered, the platform automatically analyzes captured images for firearms—no manual intervention required.
2. **Detail View & Export**: View alarm details and snapshots containing firearms. Export or save as evidence.

Example

A weapon appears in a crowded area, and the system pushes a real-time notification to you.

Limitations

Gun detection is based on motion-triggered snapshots; scenarios without motion detection cannot be analyzed.

15.5.8 AI Assistant (Video)

Click to open AI Assistant.

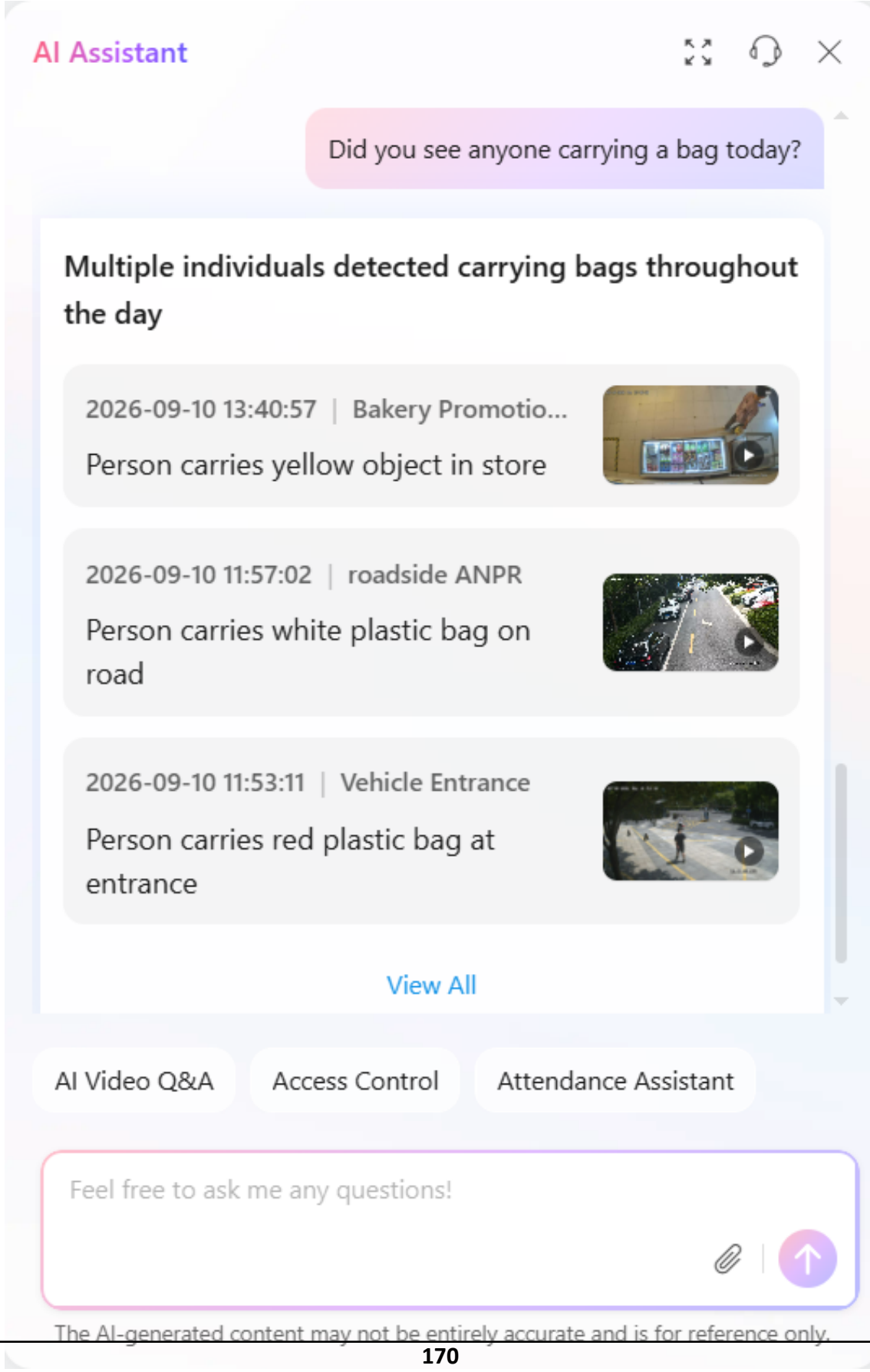


Figure 15-9 Video Q&A

Background & Purpose

To help you quickly find critical information in massive video data and avoid tedious manual searches, this version introduces the AI Video Agent. It unifies video AI capabilities through natural language understanding, making tasks like footage retrieval and video analysis as simple as chatting.

Key Features

1. **Natural Language Queries**: Ask questions like "Did anyone enter the warehouse last night?" or "How many cars came in today?".
2. **Smart Answers with Evidence**: The system provides a direct text answer along with relevant video clips. Click to play and verify instantly.
3. **Multi-Turn Conversation**: Supports follow-up questions within context. For example, ask "Did John appeared in these clips?", and the system understands the context automatically.
4. **Multi-Channel Q&A**: In Team mode, you can ask questions across multiple cameras simultaneously, with results summarized by channel.

Example

Q: Did you see anyone carrying a bag today?
A: Multiple individuals detected carrying bags throughout the day.

- 2026-09-10 13:40:57 | Bakery Promotion
  Person carries yellow object in store.
- 2026-09-10 11:57:02 | roadside ANPR
  Person carries white plastic bag on road.
- 2026-09-10 11:53:11 | Vehicle Entrance
  Person carries red plastic bag at entrance.

Limitations

- Supported question types: occurrence (yes/no), count/frequency, time/period, behavior description, and target attributes.
- When no time range is specified, the system defaults to searching the last 24 hours.
- Supports up to 3 turns of contextual conversation.

15.5.9 AI Assistant (Access Control & Attendance)

Click to open AI Assistant.

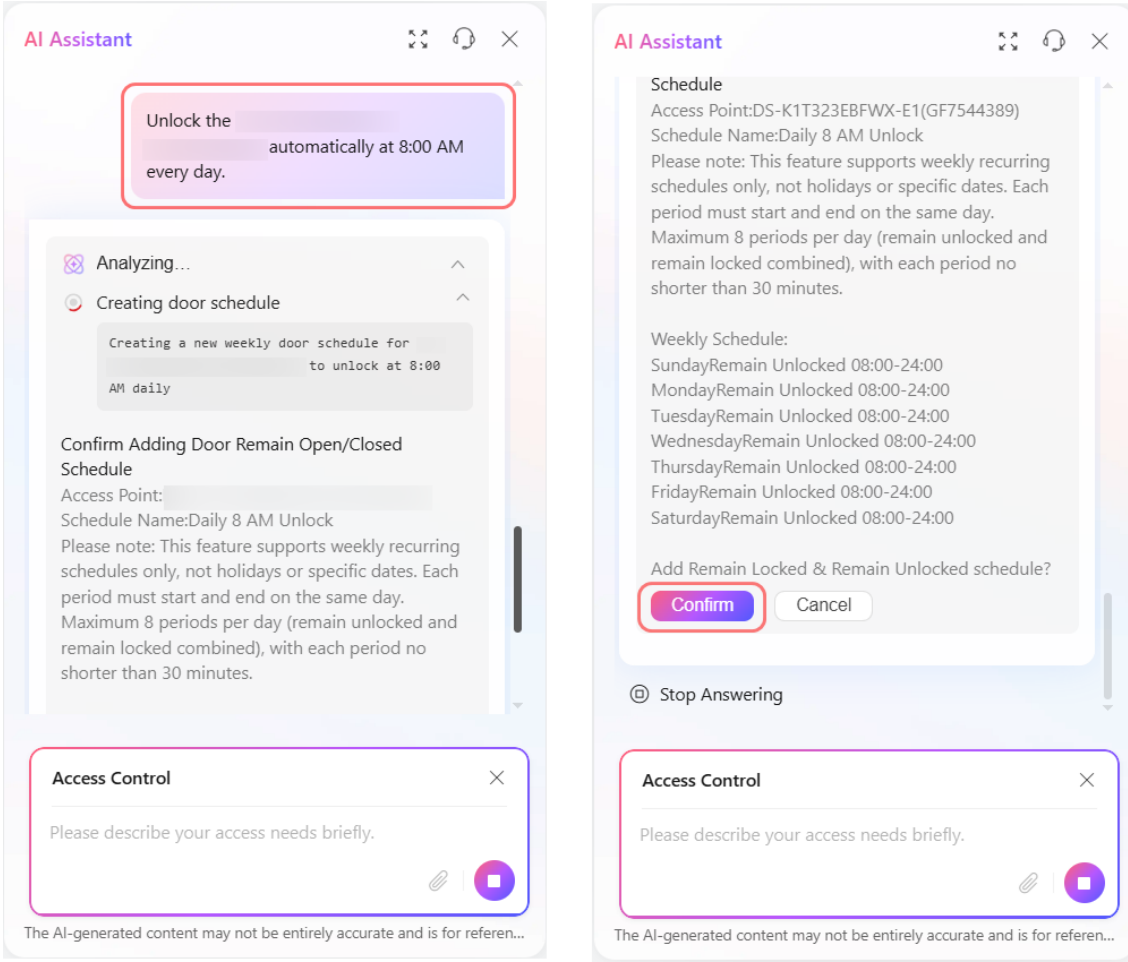


Figure 15-10 Access Control Q&A

Background & Purpose

Traditional access control systems are hard to use because they have many menus and pages. Tasks like checking attendance, setting up new employee access, or handling unusual events take a lot of time. To help non-technical users such as security guards, HR staff, and business owners, this version introduces Access Control Assistant. Just tell it what you need in simple words, and it will understand and do the task for you.

Key Features

1. **Conversational Query & Insights**
   Quickly retrieve personnel swipe records, attendance status, and abnormal events via text or voice. Results are presented clearly with summaries and structured cards.
   - Example: "Who was late today?"
   - Example: "Which users with expired credentials still tried to enter the company in the last three days?"
2. **One-Click Execution & Configuration**

Supports remote door unlocking, revoking user access, and locking down door groups for specific areas. All execution commands require secondary confirmation from the admin to ensure safety.
   - Example: "Unlock the lobby front door."
   - Example: "Lock down all doors in the warehouse group."
3. **Complex Task Automation**
   Automates multi-step workflows and provides clear step-by-step progress feedback.
   - Example: "Generate a temporary pass for visitor Jorge, valid for 10 uses today.
   - Example: "Export the attendance records for all employees from the past month."
4. **Proactive Monitoring & Scheduled Tasks**
   Create scheduled tasks and receive proactive notifications upon completion, with a one-click option to cancel the plan.
   - Example: "Tell me who has arrived at the company every day at 10:00 AM."
   - Example: "Send me a summary of all abnormal door events today at 8:00 PM, with images and short video clips."
   - Example: "Unlock the south gate automatically at 8:00 AM every day."

Limitations

- **Permissions**: This feature is only available to accounts with according privileges. Not available to self-service users.
- **Execution Confirmation**: All non-query actions (e.g., unlocking doors, deleting permissions) require secondary confirmation from you.
- **Data Privacy**: Your conversation history and feedback will be collected for service optimization. You must agree to the relevant terms before use. Sensitive information such as passwords will not be stored persistently.

Chapter 16 Alarms

16.1 How to set alarms?

16.1.1 How to add a general alarm?

Click → **Alarm** → **General Alarm Configuration** .

Click **Add**.

Triggering Event and Source

The following fields indicate two elements in the rule: "triggering event" and "alarm source".

Triggering Event

The specific event type detected by the event source will trigger an event or alarm.

Source

This field refers to the specific entity (such as cameras, doors) which can trigger this alarm.

Description

Enter the description or remarks for the alarm.

Alarm Priority

The field defines the priority for the alarm. Priority can be used for filtering alarms.

Color

Click the color to select a color to indicate this alarm, which will be displayed in the Alarm Center. You can set the color according to the urgency of this alarm. For example, you can set red color for an urgent alarm and set green color for a prompt alarm.

Ignore Repetitive Alarms

This function is used to avoid the same alarm that occurs frequently in a short time. You need to set the **Time Period for Ignoring Alarms (s)** which is the threshold of the recurring alarms.

For example, if you set **Time Period for Ignoring Alarms (s)** to ***30***, alarms of the same type occurring on the same camera within 30 s will be regarded as one alarm.

Note

The **Time Period for Ignoring Alarms (s)** is 15 s by default. You can set it from 15 s to 1800 s.

What to Do

The fields define what actions the System will take to record the alarm details and notify the security personnel.

Record Video Footage

Select the related camera to record the video when the event occurs or alarm is triggered. You can view the live video and play back the video in the Alarm Center.

- **View Pre-Event Video:** You can view the video recorded from periods preceding the alarm. Before the alarm starts, specify the number of seconds in which you want to view the recorded video.
- **Post-record:** Record video from periods following detected events. Specify the number of seconds which you want to record video after the alarm occurred.
- **Display Video by Default:** Set the video to be displayed by default in the Portal when receiving the triggered alarm information. You can select the recorded video or the live video to be displayed.

Note

- Make sure the related camera(s) have been configured with the recording schedule.
- Up to 16 cameras can be set as the related cameras.

Capture Picture

Select cameras to capture pictures during the alarm, and you can view the captured pictures when checking the event or alarm on the Alarm Search page.

- **Capture Picture Upon and After Event Detection**: Specify the number of seconds to define when the camera will capture pictures for the alarm. After you set the number of seconds for post-event (here the event refers to the triggering event), the camera will capture one picture at two time points respectively: at the configured seconds after the event ends and when the event is happening.

Link Access Point

Select between **All Access Points** and **Specified Access Points**. Then set linkage actions such as lock and unlock for the selected access points.

Send Email

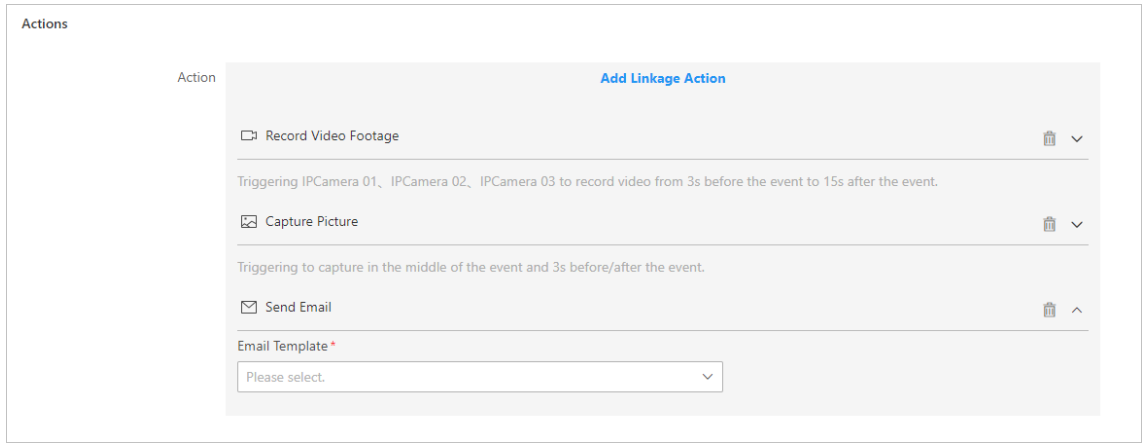


Figure 16-1 Set Linkage Action as Sending Email

Select an email template to send the alarm information according to the defined email settings.

Link Alarm Output

Select alarm output (if available) and the external device connected can be activated when the alarm occurs.

Create Tag

Select camera(s) to record the video when the alarm occurs and set the storage location for storing video files. The platform will add a tag to the alarm triggered video footage for convenient search.

- If the event source is a camera, to relate the source camera itself for tagged recording, select **Source Camera** and select the storage location (i.e., **Local Storage** and **Cloud Storage**) for storing the video files.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged length of the video footage. For example, you can set to record the tagged video started from 5 seconds before the alarm and lasted until 10 seconds after the alarm. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Trigger PTZ

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

When

This field defines the time period when an alarm can be triggered.

Receiving Schedule

The source is armed during the receiving schedule and when the triggering event is detected, an alarm will be triggered and link the configured linkage actions. The System predefines three default receiving schedule templates: All-day Template, Weekday Template, and Weekend Template. You can click **View** beside the selected template to view details.

Notification Settings

Switch on the **Notification** to show configurable alarm parameters.

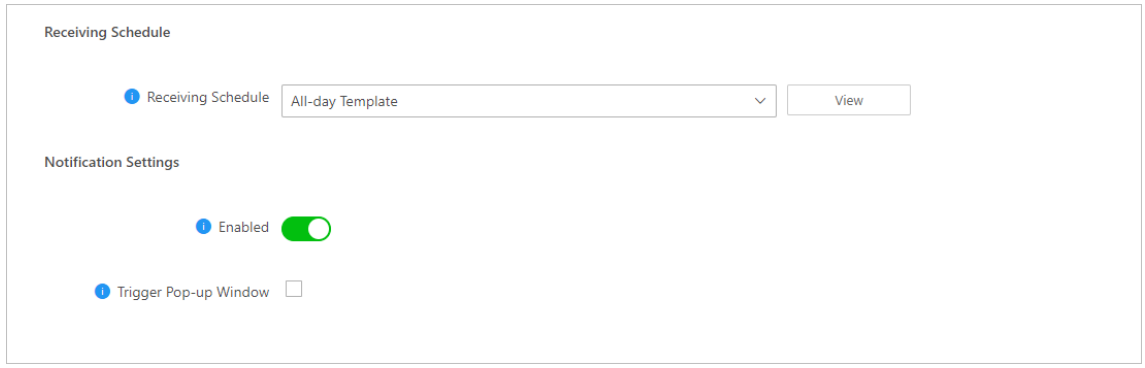


Figure 16-2 Alarm Settings

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

After setting alarm parameters, click **Add** to add the alarm and return to the alarm settings page, or click **Add and Continue** to save settings and add another alarm.

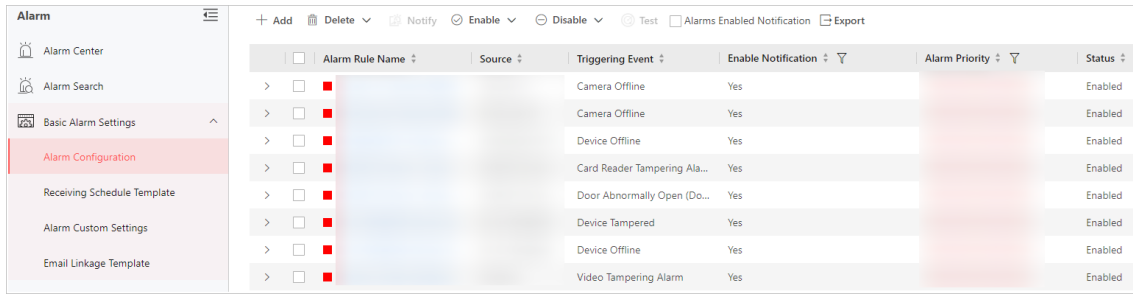


Figure 16-3 Alarm Configuration Page

Note

After adding the alarm, the alarm name which consists of the source name and triggering event type will be generated automatically.

Other Operations After Adding an Event or Alarm

Table 16-1 Other Operations

Operation	Description
Edit Alarms	Click the alarm name to enter the details page and edit the settings.
Copy to Other Alarms for Batch Configuration	1. Click the alarm name to enter the details page and click **Copy to** in the top right corner. 2. Specify settings of the alarm, select the target alarm(s), and click **OK**.
Delete Alarms	Select alarm(s) and click **Delete**.
Enable Alarm Notification	Select alarm(s) and click **Notification** so that you will be notified when the selected alarms are triggered.
Enable Alarms	Select an alarm and click **Enable** to enable the alarm, or click **Enable → Enable All** to enable all added alarms.
Disable Alarms	Select an alarm and click **Disable** to disable the alarm, or click **Disable → Disable All** to disable all added alarms.
Receive Alarms	Check alarms and click **Receive** on the top to accept the alarms, so the current Control Client can receive these alarms when it is triggered. You can click ⌄ **→ Receive All** to accept all the alarms via the current Control Client.
Ignore Alarms	Check alarms and click **Ignore** on the top to ignore the alarms, so the current Control Client will not receive these alarms during the ignorance duration even though it is triggered. You can click ⌄ **→ Ignore All** to ignore all the alarms via the current Control Client.
Test Alarms	Click **Test** to trigger the selected alarm(s) automatically. You can test if the linkage actions work properly.
Filter Alarms	Check **Alarms with Notification Enabled** to filter triggered alarms in the event and alarm list.

How to view supported alarms?

Currently, the System supports alarms triggered by the following types of resources:

Video

The video exceptions detected in the monitoring areas of cameras, such as motion detection and line crossing; and the alarms triggered by alarm inputs of video devices in the System.

Access Control

Access control events including door (e.g., card swiping events), alarm input (e.g., device armed, disarmed, restored, and triggered events), and person events (e.g., card number matched events).

Driving Monitoring

The driving monitoring alarms (e.g., speeding) or vehicle exceptions detected by on-board devices in the System.

Alarm Detection

Zone

Events occurred in zones in the platform, such as alarm input restored, bypass, and so on.

Partition (Area)

Events occurred in partitions (areas) of security control panels in the platform, such as away arming events, stay arming events, and so on.

Maintenance

The operating exceptions of the resources (i.e., cameras, Hik-ProConnect boxes, etc.) added to the System, such as camera offline and camera online.

16.1.2 How to add an AI notification?

1. Click → **Alarm → AI Notification Configuration → Add** .
2. Describe an alert scenario in plain text, e.g., "Alert me if the passageway at entrance is obstructed by any objects".
3. After configuration, the system instantly check matching results from the past 24 hours to verify accuracy, and then presents a structured rule for your review and fine-tuning.
4. The system automatically identifies targets (person/vehicle), behaviors (appear/linger/loiter).

Other Operations After Adding an Event or Alarm

Table 16-2 Other Operations

Operation	Description
Edit Alarms	Click the alarm name to enter the details page and edit the settings.
Copy to Other Alarms for Batch Configuration	1. Click the alarm name to enter the details page and click **Copy to** in the top right corner. 2. Specify settings of the alarm, select the target alarm(s), and click **OK**.

Operation	Description
Delete Alarms	Select alarm(s) and click **Delete**.
Enable Alarm Notification	Select alarm(s) and click **Notification** so that you will be notified when the selected alarms are triggered.
Enable Alarms	Select an alarm and click **Enable** to enable the alarm, or click **Enable → Enable All** to enable all added alarms.
Disable Alarms	Select an alarm and click **Disable** to disable the alarm, or click **Disable → Disable All** to disable all added alarms.
Receive Alarms	Check alarms and click **Receive** on the top to accept the alarms, so the current Control Client can receive these alarms when it is triggered. You can click ⌄ **→ Receive All** to accept all the alarms via the current Control Client.
Ignore Alarms	Check alarms and click **Ignore** on the top to ignore the alarms, so the current Control Client will not receive these alarms during the ignorance duration even though it is triggered. You can click ⌄ **→ Ignore All** to ignore all the alarms via the current Control Client.
Test Alarms	Click **Test** to trigger the selected alarm(s) automatically. You can test if the linkage actions work properly.
Filter Alarms	Check **Alarms with Notification Enabled** to filter triggered alarms in the event and alarm list.

16.1.3 How to configure a receiving schedule template?

When adding events and alarms, you can select the predefined receiving schedule template to define when the event and alarm can be triggered and notifying the recipients. You can also customize a template according to actual needs.

1. On the top navigation bar, click **Alarm → Basic Alarm Settings → Receiving Schedule Template** .
2. Click + to enter the Add Receiving Schedule Template page.

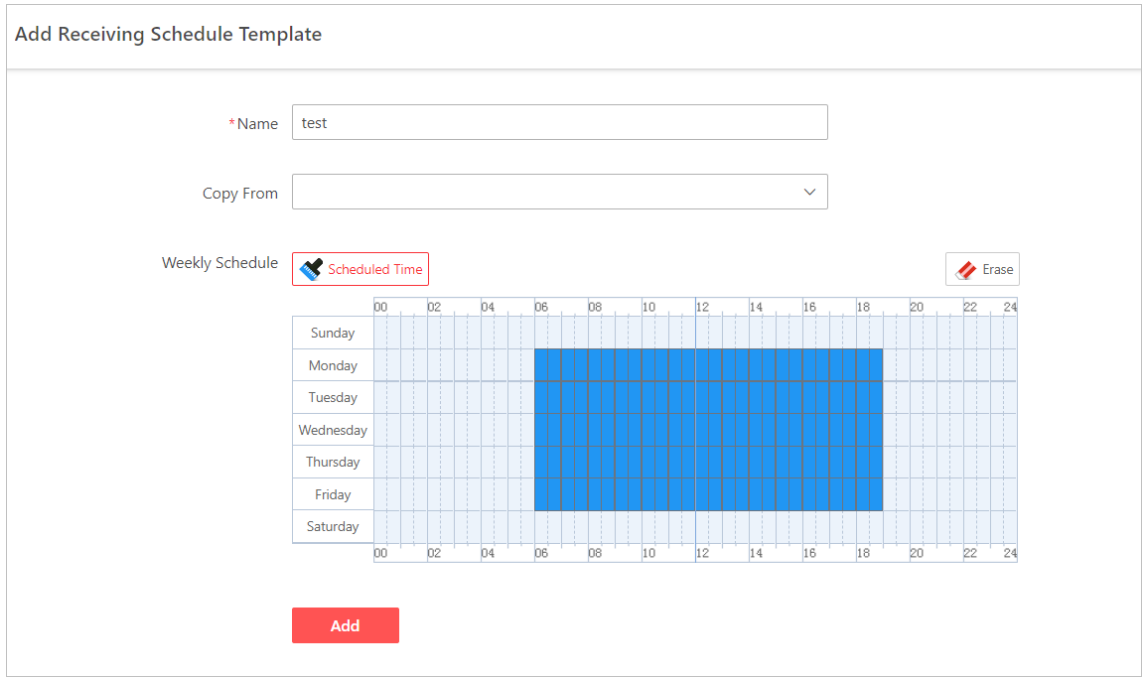


Figure 16-4 Add Receiving Schedule Template

3. Create a name for the schedule template.
4. In the **Copy From** field, select an existing template to copy its weekly schedule to the current one.
5. Click **Scheduled Time** and click or drag on the timetable to define the period.

Note

- A rectangle represents half an hour.
- You can click a selected rectangle to set a more accurate time period.

6. Click **Erase** and click or drag on the formerly selected rectangle(s) to remove them from the scheduled time.

16.2 How to search for alarms?

1. On the top navigation bar, click **Alarm → Alarm Search** to enter the Alarm Search page.
2. Set the time range for search.
3. Select the alarm priority.
4. Select the event type as **All**, **Disabled**, or **Enabled**.

All

Both alarms with and without notification enabled.

Disabled

Alarms with notification not enabled.

Enabled

Alarms with notification enabled.

5. If you select **Enabled**, you can set the following filter conditions.

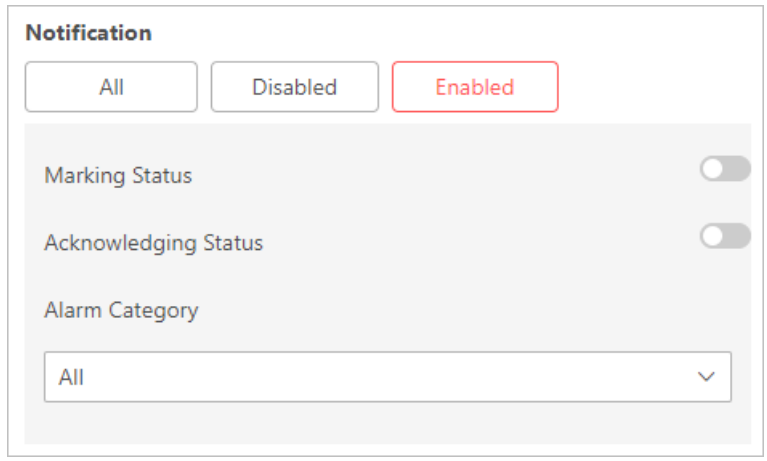


Figure 16-5 Notification Enabled

Marking Status

Switch on **Marking Status** and select **Marked** or **Unmarked** to filter marked or unmarked alarms.

Acknowledging Status

Switch on **Acknowledging Status** and select **Acknowledged** or **Unacknowledged** to filter acknowledged or unacknowledged alarms.

Alarm Category

Select a category to filter alarms by category.

6. Switch on **Group** and then click to select the group of the source.
7. Switch on **Conditions** and then click to select triggering events and the source.
8. Switch on **Alarm Rule Name** to select the alarm rule name from the drop-down list.
9. Click **Search**.
10. Perform the following operations.

Table 16-3 Further Operations

User intention	Description
View Alarm Details	Click the name of an alarm to view details and the linked video or picture.
Export Alarms	Click **Export Data on Current Page** to export all searched alarms in XLSX format to the local storage.
Archive Alarms	Check alarms and click **Archive** to save the selected alarms as archives.

16.3 How to view resources' real-time alarms?

The Alarm Center will display the real-time alarm information from the managed resources, such as motion detection, video loss, and video tampering. You can check the alarm details and perform different operations if configured.

Note

Before receiving alarms from resources, the alarm settings should be configured and alarms should be triggered.

On the top navigation bar, click **Alarm → Alarm Center** to enter the Alarm Center page.

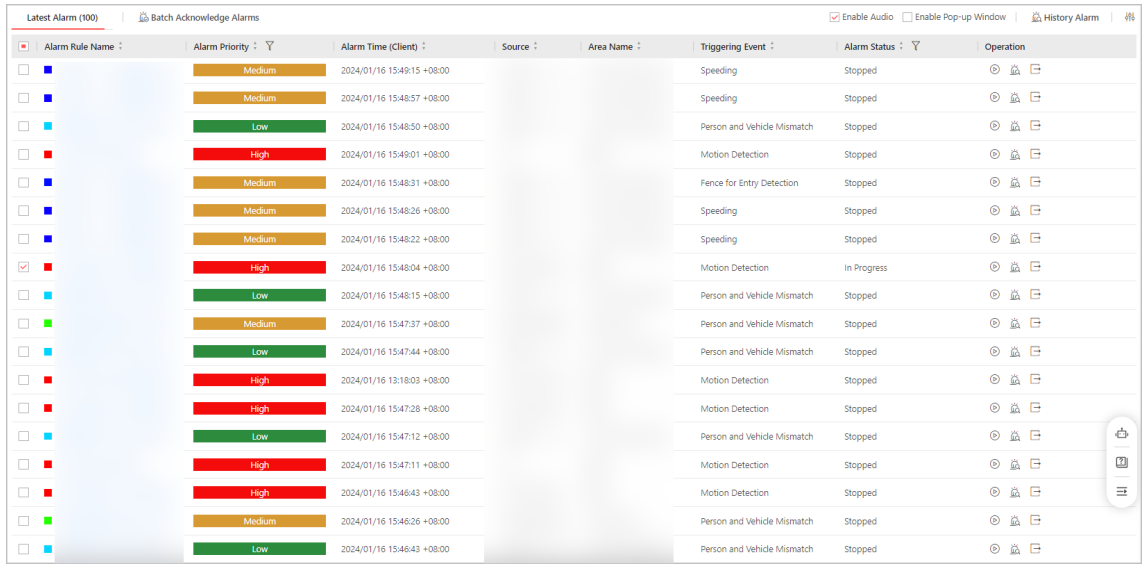


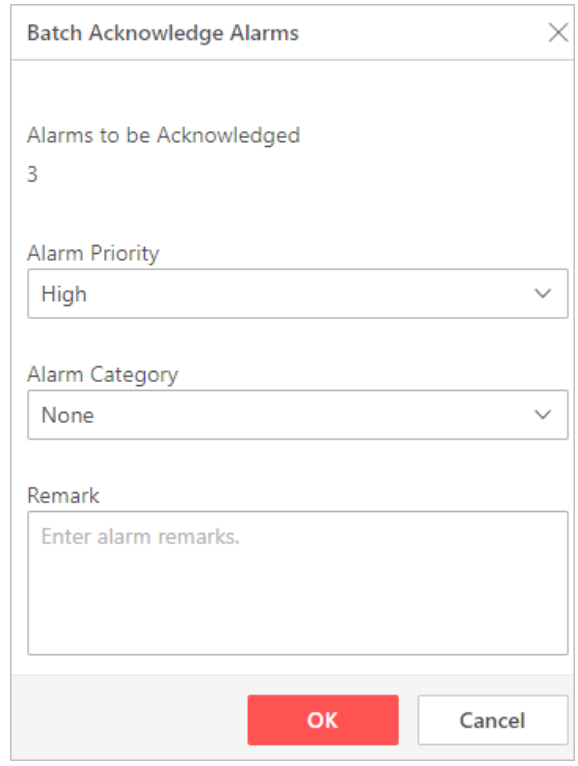
Figure 16-6 Alarm Center

You can view the latest received alarms in **Latest Alarm**.

Table 16-4 Operations in Alarm Center

Operation	Description
View Alarm Details	Click an alarm name to view the details. **Alarm Priority** The priority for the alarm according to the priority settings when adding the alarm on the Portal. **Alarm Time (Client)** The time of the Portal when the alarm starts. **Source**

Operation	Description
	The source that triggers the alarm. **Triggering Event** The type of event that triggers the alarm. **Alarm Status** The current status of the alarm, including stopped, started, and abnormal.
Operations of an Alarm	**Go to Alarm Search**: Click in the Operation column to go to the Event and Alarm Search page to search for the current alarm by setting conditions.
	View Linked Content: Click in the Operation column to start live view or playback of the related cameras that upload the alarm and view the captured pictures.
	Export: Click in the Operation column to download the alarm details.
	Acknowledge Alarm: Click an alarm name to open the alarm details window, set parameters (e.g., alarm priority, alarm category, and remark), and click **Acknowledge** to acknowledge the alarm.
	Acknowledge and Archive Alarm: Click an alarm name to open the alarm details window and click **Acknowledge and Archive** to acknowledge the alarm and save the alarm as an archive. You can set a name, tag, and level for the archive.
	Send Email: Click an alarm name to open the alarm details window and click **Send Email** to open the pop-up window for sending an email. You can select an email template, enter the recipient(s), and enter remarks as needed.
	Alarm Output Control: In the pop-up alarm window, click **Alarm Output Control** to enable or disable the linked alarm outputs if you have set linked alarm outputs in the alarm rule.
Filter Alarms	Set filter conditions to display the required alarms only. **Alarm Priority** The priority can be low, medium, high, and custom level, which indicates the urgency level of the alarm. **Alarm Status**

Operation	Description
	The alarm status can be **Start**, **Stop**, and **In Progress**. **Start** indicates the alarm has not stopped yet; **Stop** indicates the alarm has stopped; and **In Progress** indicates the alarm has started but not stopped.
Batch Acknowledge Alarms	1. Check alarms in the alarm list, and then click **Batch Acknowledge Alarms** to open the Batch Acknowledge Alarm window.  **Figure 16-7 Batch Acknowledge Alarms** 2. (Optional) Set the alarm priority and alarm category. 3. (Optional) Enter remarks about the alarm acknowledgment. 4. Click **OK**. **Note** Up to 100 alarms can be acknowledged at a time.
View Historical Alarms	Click **History Alarm** to enter the Event and Alarm Search page to search for historical alarms. See for details.
Enable Audio	Check alarms and check **Enable Audio**, so that once the alarms are triggered, audio notification will be played.

Operation	Description
Enable Pop-up Window	Check alarms and check **Enable Pop-up Window**, so that the Alarm Details window will pop up when the alarms are triggered.
Custom Column Items	On the top right, click to select column items to be displayed. You can click **Reset** to select again.

Note

- For access control events including person matched events and card number matched events, person information shall be displayed when you view alarm details.
- For solar-powered camera alarms, the battery information shall be included in the alarm information.

16.4 How to view pop-up window triggered by alarm?

After you enable the alarm linkage of Trigger Pop-up Window on the Portal and enable the pop-up window function, the alarm window will open when the corresponding alarm is triggered. You can view the alarm time, the source device which triggered the alarm, the triggering event, and alarm status, etc.

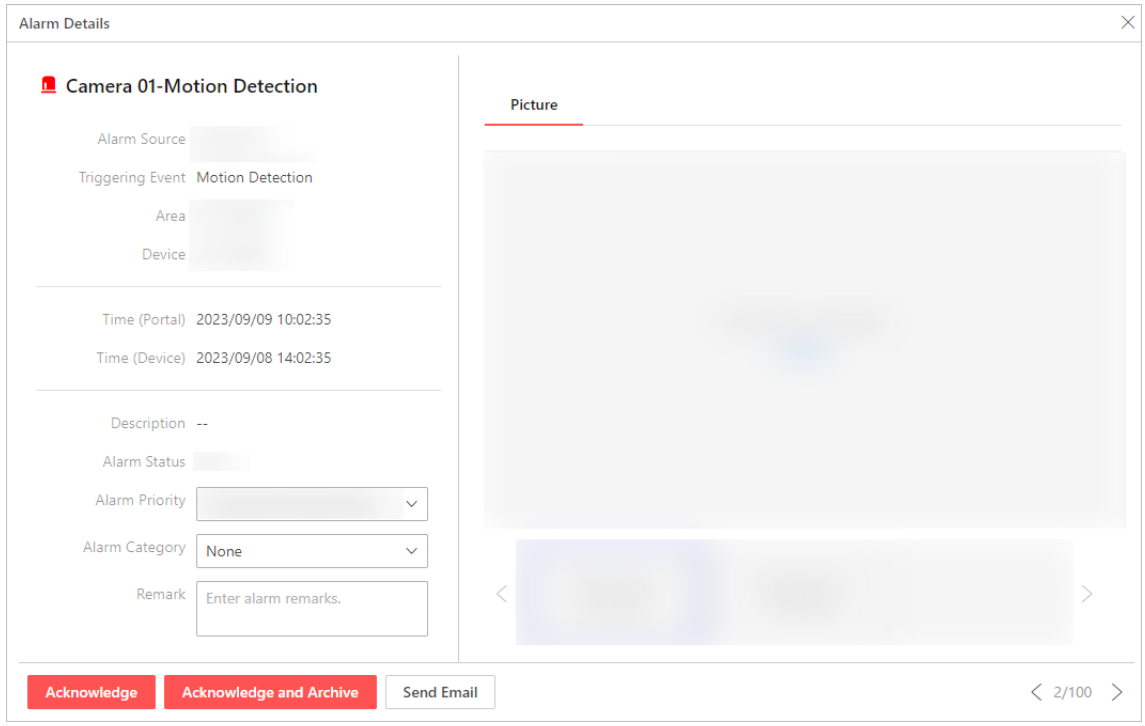


Figure 16-8 Alarm Triggered Pop-Up Window

Table 16-5 Functions and Operations Supported by Pop-Up Alarm Window

Function	Operation
Edit Alarm	Set the alarm priority, the alarm category, and remarks (e.g., enter "false alarm triggered by leaves" when you have checked the alarm details and found that it is a false alarm) according to the detailed alarm information.
View Alarm-Related Picture, Video, and Map	Click **Picture**/**Video**/**Map** to view the alarm-related cameras' captured pictures, the playback or live view when the alarm occurred, and view the camera/alarm input location on the map (if configured). **Note** • When viewing the recorded video files of the related camera, you can click **Go to Alarm Time** to play the video from the alarm time. You can also click **Live View** to view the live video of the related cameras. • During playback, you can click on the time bar to play back video files stored in the main storage or auxiliary storage.
Acknowledge Alarm	Click **Acknowledge** to acknowledge the alarm.
Acknowledge Alarm and Archive	Click **Acknowledge and Archive** to acknowledge and archive the alarm.
Send Alarm Email	Click **Send Email**, select an email template, and enter the recipient(s) of the alarm and remarks to send an email containing the information about this alarm to the selected recipients.
Control Alarm Output	Click **Alarm Output Control** to enable or disable the linked alarm outputs if you have linked alarm outputs to the alarm. For example, if a sounder is linked to the alarm, when the alarm is triggered, you can turn on or off the sounder.
View Previous or Next Alarm	Click < > to view the previous or next alarm information.
Enable Pop-Up Window	Uncheck **Enable Pop-up Window** to disable pop-up window when a new alarm is triggered. **Note** When the pop-up window remains open, the later alarm, if the alarm priority is higher, will be displayed in the pop-up window, and replace the earlier one.

Function	Operation
Start Two-Way Audio	For on-board related alarms, click **Two-Way Audio** to start two-way audio.
Perform Track Playback	For on-board related alarms, click **Track Playback** to view the driving track of the vehicle.
Start Live View	For on-board related alarms, click **Live View** to view the live video of the camera.
Control Doors	For alarms linked with door actions, you can lock or unlock doors. You can also set the door as remaining locked or remaining unlocked.

Chapter 17 Map Management

Add a Map

Click → **Map** and select a group in the upper-left corner.

Table 17-1 Map Type

Map Types	Operations
Online Map	Select **Switch to Online Map**Drag and zoom in/out on the map to select a monitoring area for the current group.
Static Map	Select **Add Static Map** to upload a map picture from the local PC to the Portal.

Add Resources to Maps

Go to → **Map** → **Map Settings** → **Add Object** .
You can add resources (Camera, Alarm Input / Zone, Alarm Output, Area, or Door), hot regions, and labels to the map.
The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Monitor on Map

Table 17-2 Monitor on Map

Resource	Operations
Camera Hot Spots	Check the live view of the camera, view its status, view the history alarms, etc. You can also acknowledge or ignore alarms.
Alarm Input / Zone Hot Spots	View its status, area, and remark, set the arming control, and view the history alarms. You can also acknowledge or ignore alarms.
Alarm Output Hot Spots	Turn on or off the linked alarm output.
Area Hot Spots	View each zone's status, area, and remark, set the arming control, and view the history alarms. You can also bypass any zone to turn off alarms or ignore all alarms.

Resource	Operations
Doors	View live view or captured pictures if a door has a camera or it is linked with a camera. Moreover, you can lock or unlock doors and set doors as normally open or normally closed. You can also ignore door alarms, view history door alarms, and view access records.
Hot Regions	Click a hot region on the map to enter the map of the hot region.

Chapter 18 Maintenance

You can check device status, view device basic information, view live view and playback of cameras, set remote configuration of devices, etc. You can also search for operation logs of users by setting conditions, and view log details.

18.1 How to view real-time status?

You can view the real-time health status of all resources or resources of a specified area so as to handle abnormal situations timely. The resources include cameras, alarm inputs, encoding devices, access control devices, video intercom devices, on-board devices, security control devices, and cloud storage boxes managed on the Portal.

On the top navigation bar, click → **Maintenance → Health Monitoring** .

Note

If there are any sub-areas under an area, you can view the status of devices from the sub-areas.

You can perform the following operations.

Refresh	In the upper right corner of the **All** page, click **Refresh** to refresh the resource status on the page.
Export Real-Time Status Data	In the upper right corner of the **All** page, click **Export** to export the data. **Note** Only the data on the current page will be exported by default.
View Resource Status	Click the numbers in red to enter the corresponding page to view exception details of resources.

18.2 How to monitor device health?

The health monitoring module provides near-real-time information about the status of added resources (including camera, alarm input, encoding device, access control device, video intercom device, on-board device, security control device, Hik-ProConnect box, and doors), which is important for operation and maintenance. When a device exception occurs, you can enter this module to check the device status by finding out the abnormal device(s) and viewing the exception details.

On the top navigation bar, click → **Maintenance** → **Health Monitoring** .

Select an area, and then select a resource type on the navigation pane on the top.

Camera Status

Note

Only cameras that have been added to areas will be monitored.

On the Camera page, you can view area information, network status, last inspection time, etc.
The following operations are available.

- Click to view the live view of the camera.
- Click to view the playback of the camera.
- Click the camera name to view its status and basic information.
- In the Device column, click the device name to check cameras of alarm inputs, on-board devices, or security control devices.
- In the top right corner, enter the keyword in the Search field to search for specific cameras.
- In the top left corner, enter the keyword in the Search field to search for specific areas.

Door Status

On the Door page, you can view information including network status, door status, card reader status, etc.
The following operations are available.

- Click **On**/**Off** in the Operation column to set the door as open or closed.
- Click **Open** / **Closed** in the Operation column to set the door as normally unlocked or normally locked.

Alarm Input Status

On the Alarm Input page, you can view the network status, device version, area, last inspection time, etc.
The following operations are available.

- In the Device column, click the device name to check cameras of alarm inputs, on-board devices, or security control devices.
- Click the device name to view device details and partition (area) details.

Encoding Device Status

On the Encoding Device page, you can view the network status, storage status, HDD usage, last inspection time, etc.
The following operations are available.

- Click the device name to view its status, basic information, and camera information.
- Hover the cursor over the bar in the HDD Usage column to view usage details.
- Click to reboot the encoding device.

Note

- If the device is an NVR that supports cloud storage, you can view the pieces of queuing footage.
- For solar-powered cameras, you can view remaining battery. You can also view and export battery and data usage reports.

Access Control Device Status

On the Access Control Device page, you can view the network performance, tampering status, last inspection time, etc.
Click the device name to view its status, basic information, etc.

Video Intercom Device Status

On the Video Intercom Device page, you can view the network performance, last inspection time, etc.
Click the device name to view its status, basic information, etc.

On-Board Device Status

On the On-Board Device page, you can view the network status, storage status, HDD usage, GPS status, GPS signal, last inspection time, etc.
The following operations are available.

- Click the device name to view its status, basic information, and camera information.
- Hover the cursor over the bar in the HDD Usage column to view usage details.
- Click ↻ to reboot the on-board device.

Hik-ProConnect Box Status

On the Hik-ProConnect box status page, you can view network status, device serial No., last inspection time, etc.
Click the device name to view its status, basic information, etc.

Security Control Device Status

On the Security Control Device page, you can view the model, firmware version, network status, device version, abnormal partitions (areas), battery status, last inspection time, etc.
The following operations are available.

- Click the device name to view device details and partition (area) details.
- Click ↻ to reboot the security control device.

Common Operations

Perform the following operations for different device types.

- In the top right corner, check the box besides the Search field and select a type in the drop-down list to view specific exceptions.
- In the top right corner, click **Refresh** to inspect all devices.
- In the top right corner, click **Export** to export the device monitoring information.

- Click in the Operation column to inspect the device.
- Click in the Operation column to set remote configurations of the device.

Note

For details about the remote configuration, refer to the user manual of the device.

18.3 How to search for logs stored on devices?

You can search for device logs by setting conditions, and view the log details.

1. On the top navigation bar, click → **Maintenance** → **System Log** → **Device Log** .

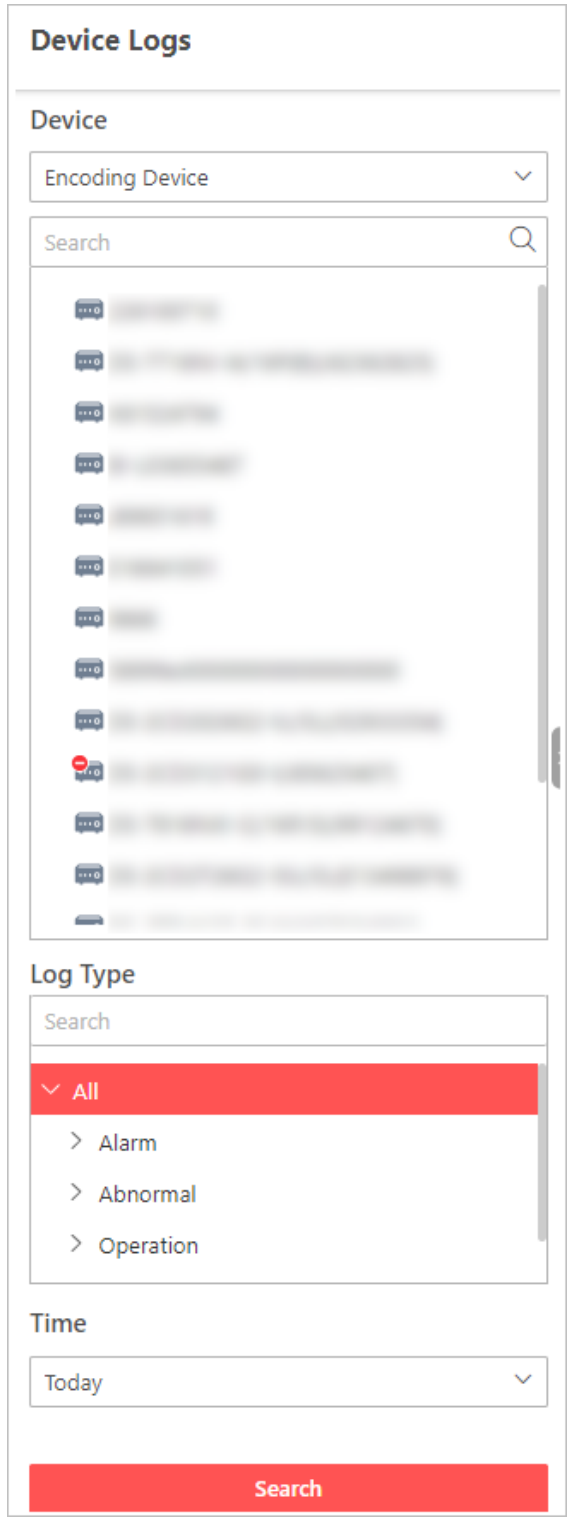


Figure 18-1 Search for Device Logs

2. In **Device**, select a device type (encoding device, on-board device, security control device, intercom device, or access control device).

3. In the search field, enter the device name to search for target devices.
4. In **Log Type**, select one or log types.
5. In **Time**, select the time range of this search.

   Note

   You can select **Custom Time Interval** to set the start time and the end time.
6. Click **Search**.

18.4 How to search for operation logs?

Operation logs refer to the operation records that were performed on the Portal and Mobile Client. You can search for operation logs of users by setting conditions, and view the log details.

1. On the top navigation bar, click → **Maintenance → System Log → Operation Log** .
2. In the Type field, select one or multiple log types and sub types.
3. In the User field, select users by whom the operation logs are generated.

   Note

   All users are selected by default.
4. In the Area field, select areas in which the operation logs happened.

   Note

   All areas are selected by default.
5. In the Resource Name field, enter the resource name to search for the logs of the resource.
6. In the Time field, select the time range of this search.

   Note

   You can select **Custom Time Interval** to set the start time and the end time.
7. Click **Search**.

18.5 How to view user login reports?

Administrators can monitor user login data through the new **User Login Report** under → **Maintenance → System Log** .

You can filter by time range (up to 90 days), client type (APP/Portal), and specific users to view login counts, online durations, and averages.

Chapter 19 Accounts

19.1 How to get accounts, log in, and create accounts?

How to register a super Admin account and log in?

1. Register a personal account first: Go to ***https://www.hik-connect.com/*** , click **Register Now**, and enter required information to register a person account.
2. Log in to Hik-Connect using the registered personal account, and click **Create Team** to enable more service.

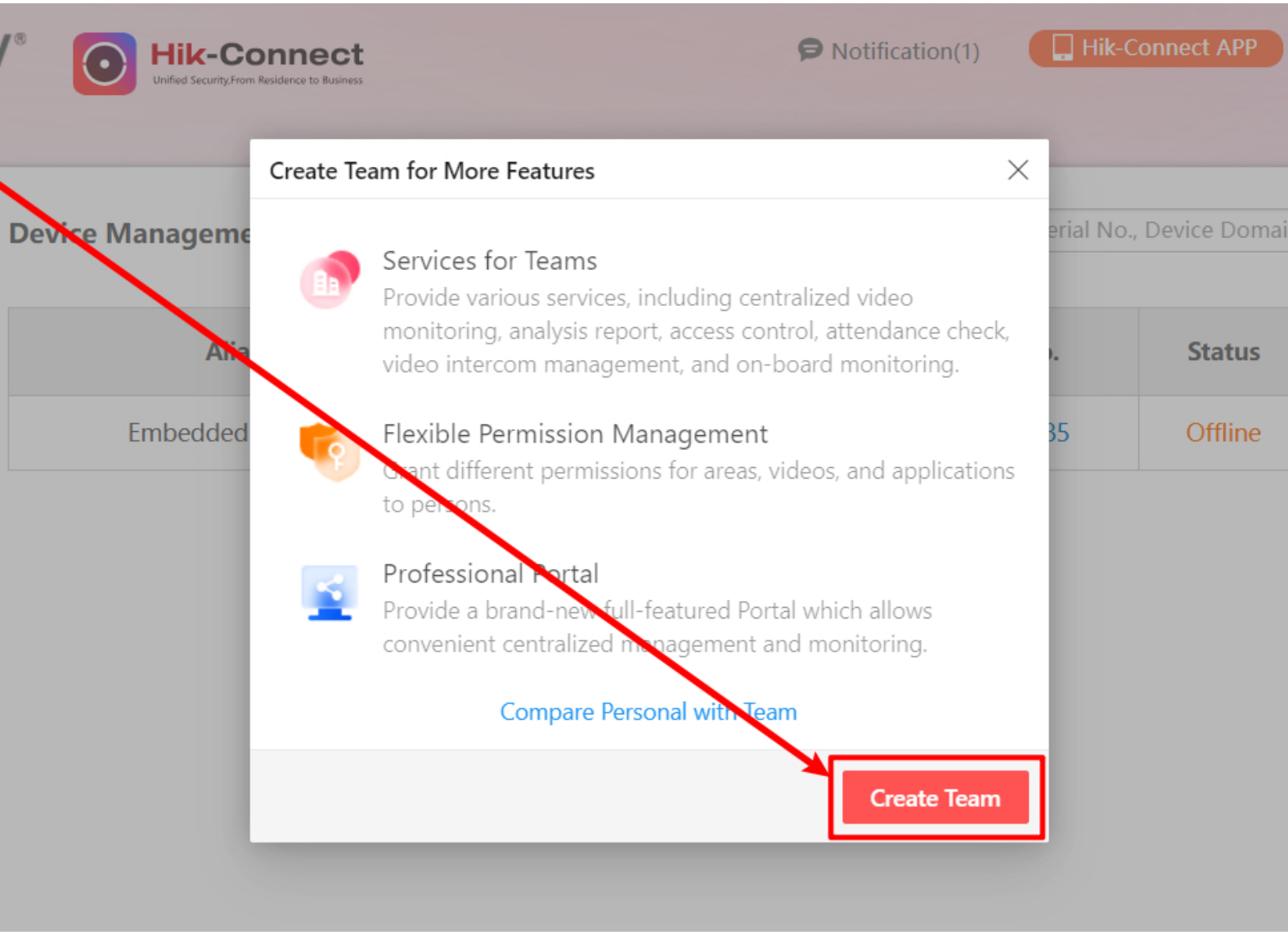


Figure 19-1 Create Team

How to accept system handed over by your service provider?

A service provider can hand over a system to you by sharing.

- The ownership of the system and its devices belongs to the service provider, who reserves the right to revoke the account and devices at any time. To protect your legal rights, please reach an agreement with the service provider before accepting the system, specifying the service details and validity.
- If the service provider shares the system with a third party, the third party will have access to the system's history data. If such data involves personal information or business secrets, please contact the service provider to change the encryption password promptly after the system sharing is canceled to prevent data leakage.

- If the service provider stops sharing the system with you, sub-accounts will be retained, and you may choose whether the sub-accounts will exit the team. Sub-accounts cannot join multiple teams; to join a new team account, you must first exit the current team.
- Please note that the ownership of the system and its devices always belongs to the service provider. You are not authorized to delete devices added to the system.
- The service provider reserves the right to access the device data under the system at any time, including but not limited to device configuration, live view, playback, intercom, PTZ (pan-tilt-zoom), PIRCAM GIFs, and video clips. These permissions may involve your personal information or privacy.

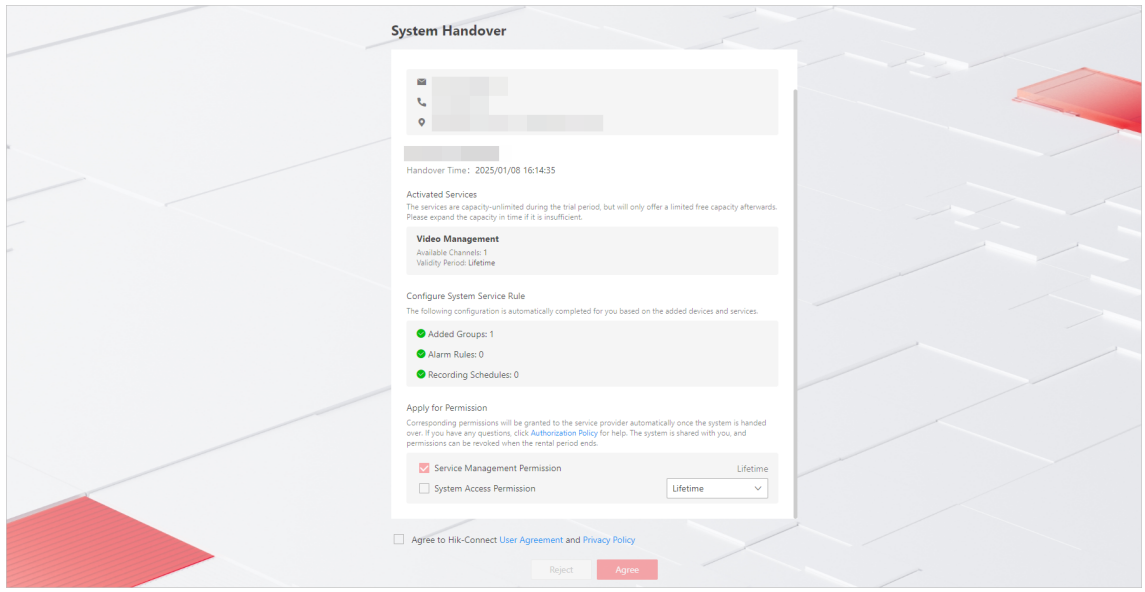


Figure 19-2 Hand Over by Sharing

How to create accounts for your team members?

Go to ⁞⁞ → **Team** → **User Management** → **Add** to add a user.

Account Type

The added user can log into Hik Connect for Teams through the email or phone number.

User Status

Freezing an account will prevent the user from log in to the system and revoke them the granted resource and operation permissions.

Role Name

A role has specific operation permissions, and assign a role to a user will grant them the operation permissions of the role.

19.2 How to configure Azure AD settings and log in to Hik Connect for Teams via Azure AD?

This guide provides step-by-step instructions for configuring Azure AD integration with Hik Connect for Teams.

How to create enterprise application on Azure AD?

Before you begin, make sure:

- Microsoft has renamed Azure AD to Microsoft Entra ID.
- This feature is only available in some regions and countries. If this feature is not visible to you, please contact our Hikvision team.

1. Log in to Azure AD, and select **Microsoft Entra ID**.

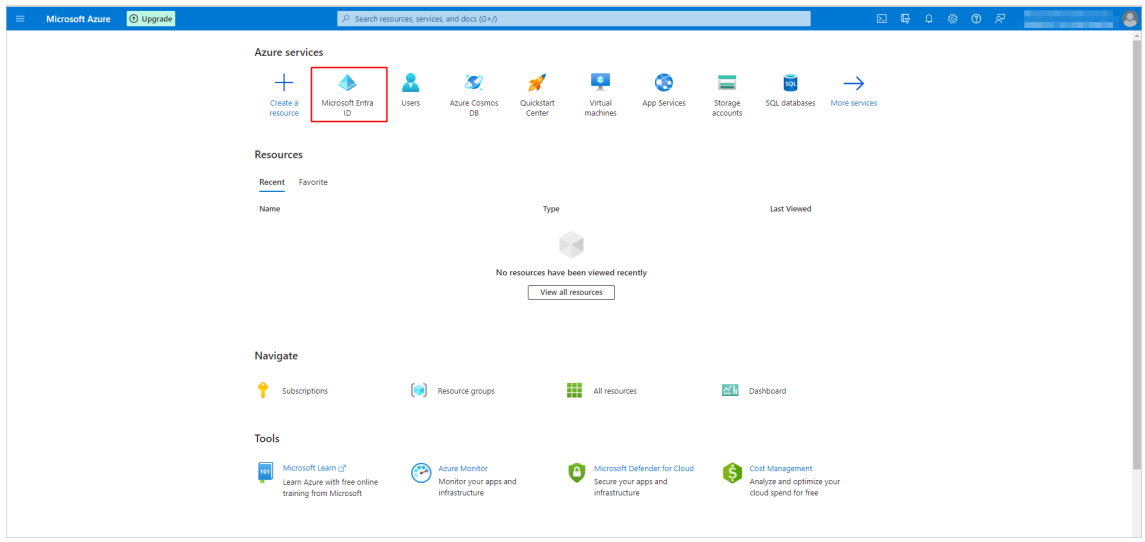


Figure 19-3 Microsoft Entra ID

2. Select **Enterprise applications**.

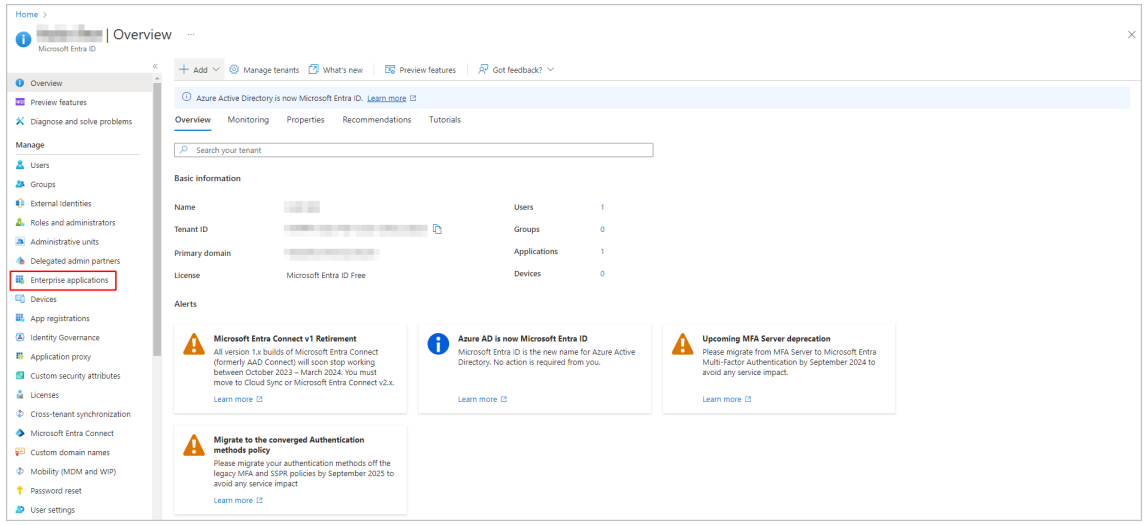


Figure 19-4 Enterprise Application

3. Select **New application**.

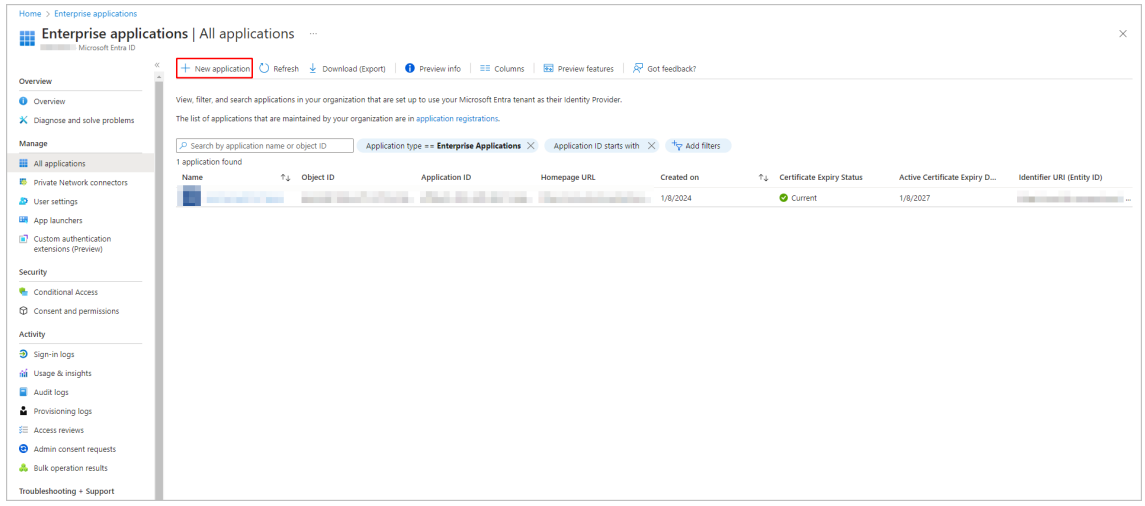


Figure 19-5 New Application

4. Select **Create your own application**.

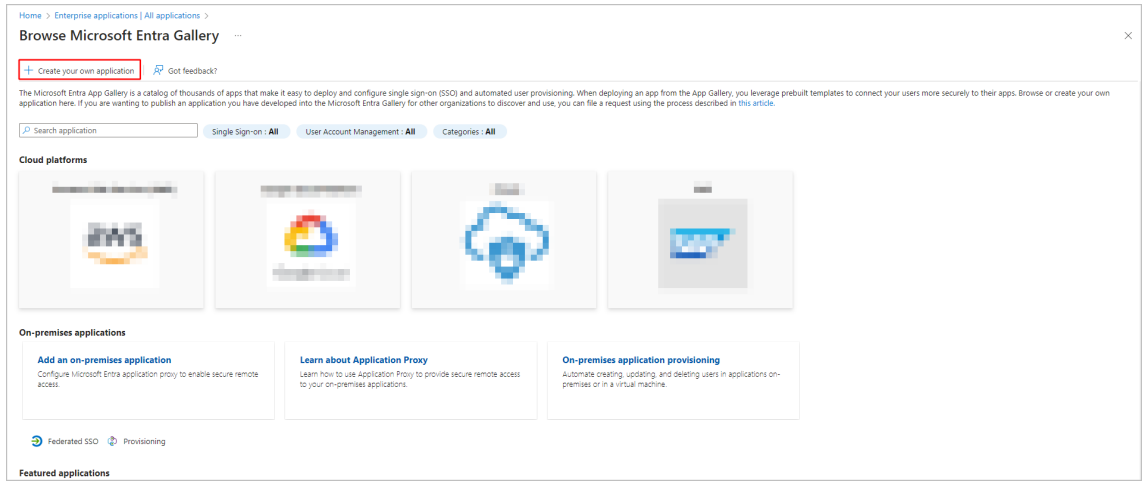


Figure 19-6 Create Your Own Application

5. Select an application that is not in the gallery and name it.

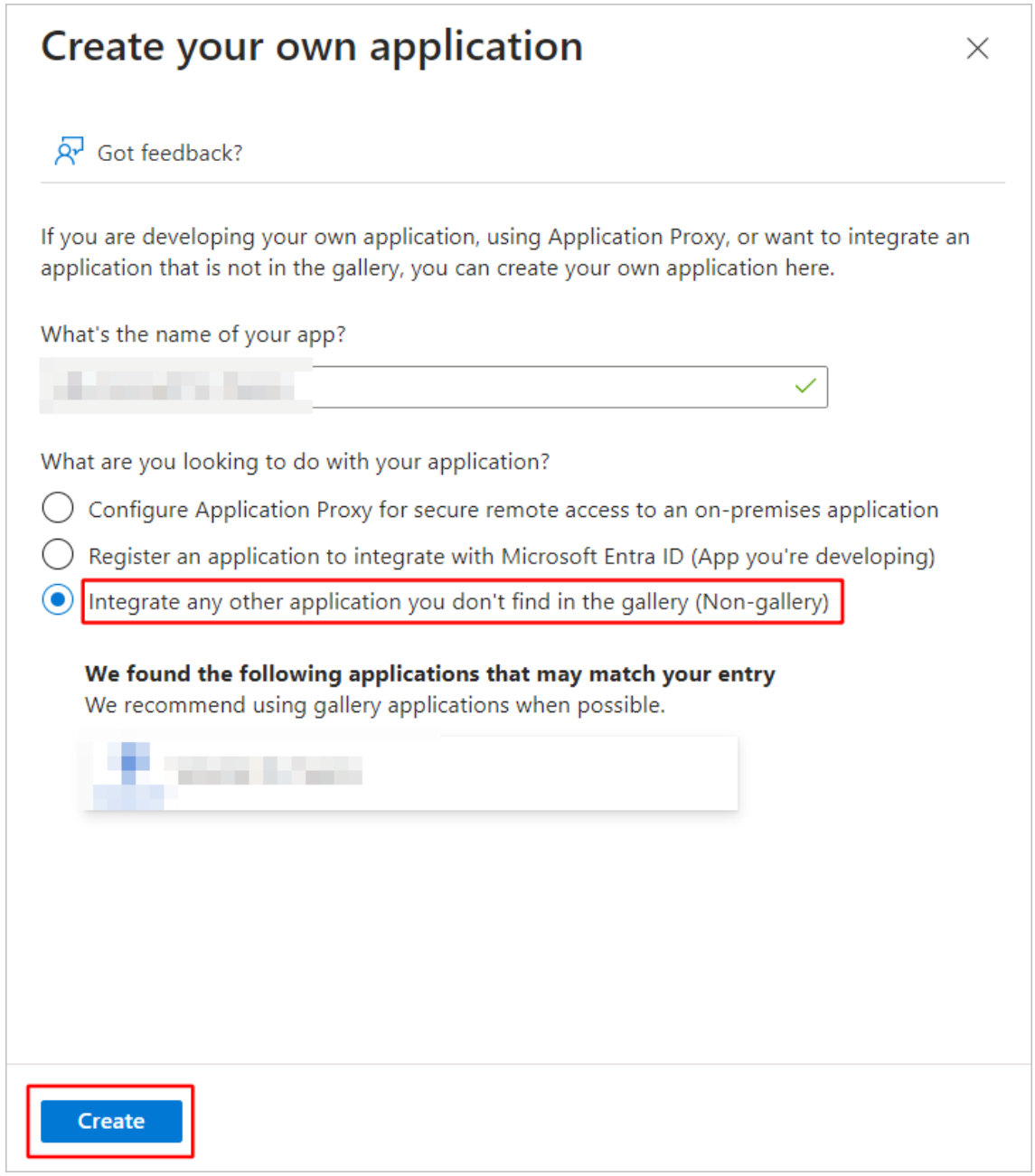


Figure 19-7 Select Application

How to configure SAML SSO single sign on?

1. Go to the enterprise application you just created and select **Set up single sign on**.

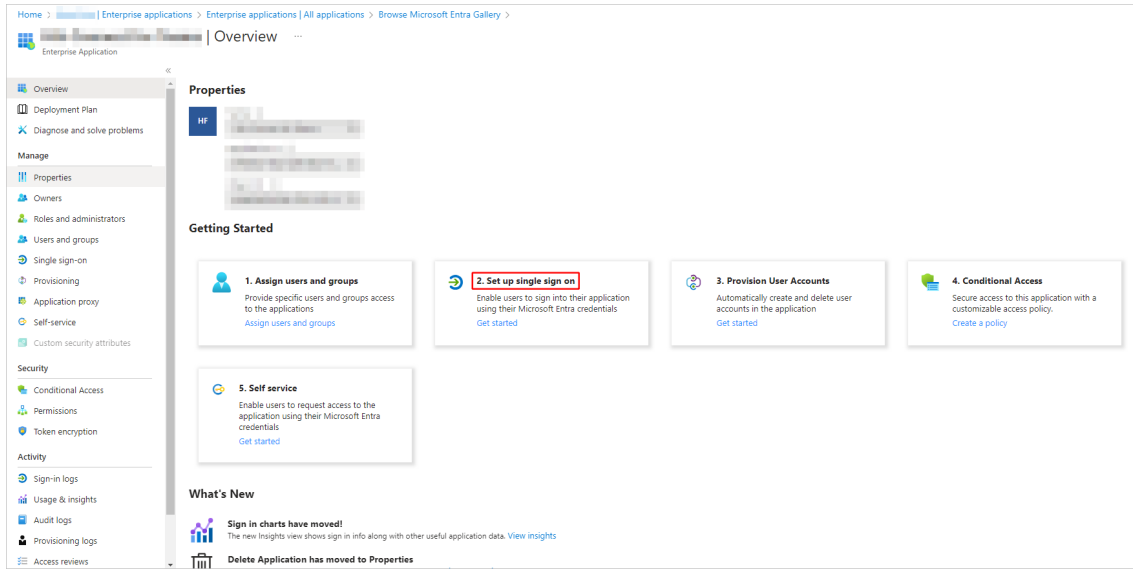


Figure 19-8 Set up Single Sign On

2. Select **SAML**.

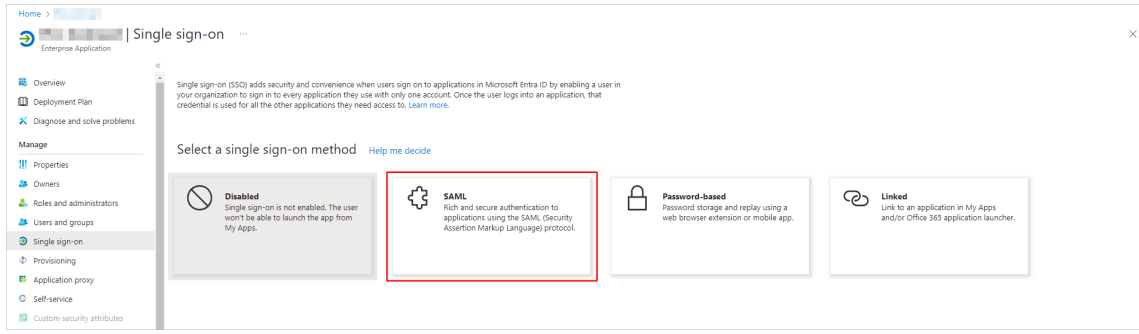


Figure 19-9 SAML

3. Configure the information required for SAML login authentication in Azure AD. You can find the required information in Hik Connect for Teams: ⁞⁞ → **Team** → **Team Configuration** → **Log in via Azure AD** . Click **Configure** to start the configuration.
4. In step ①, you need to copy the Entity ID and Reply URL to Azure AD.

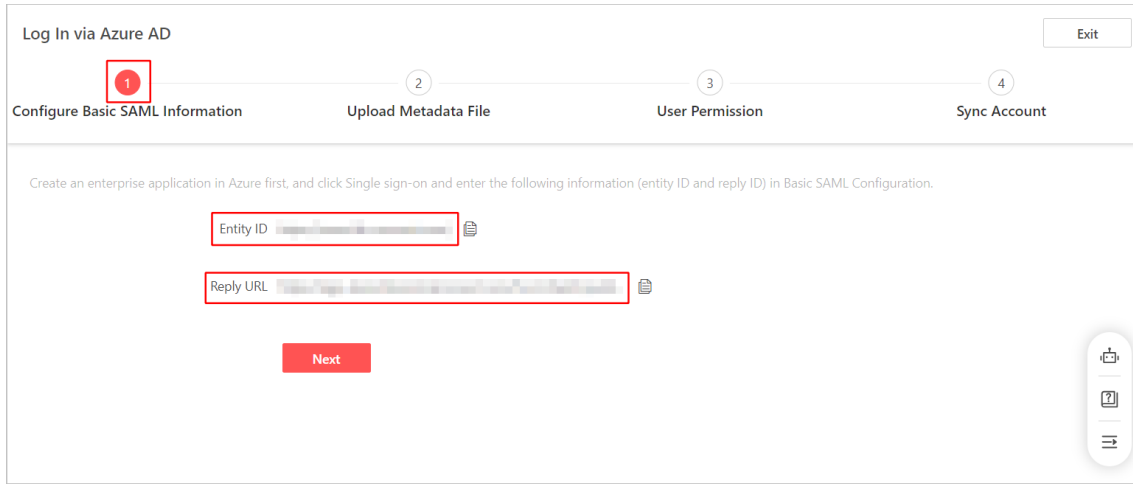


Figure 19-10 Copy Information

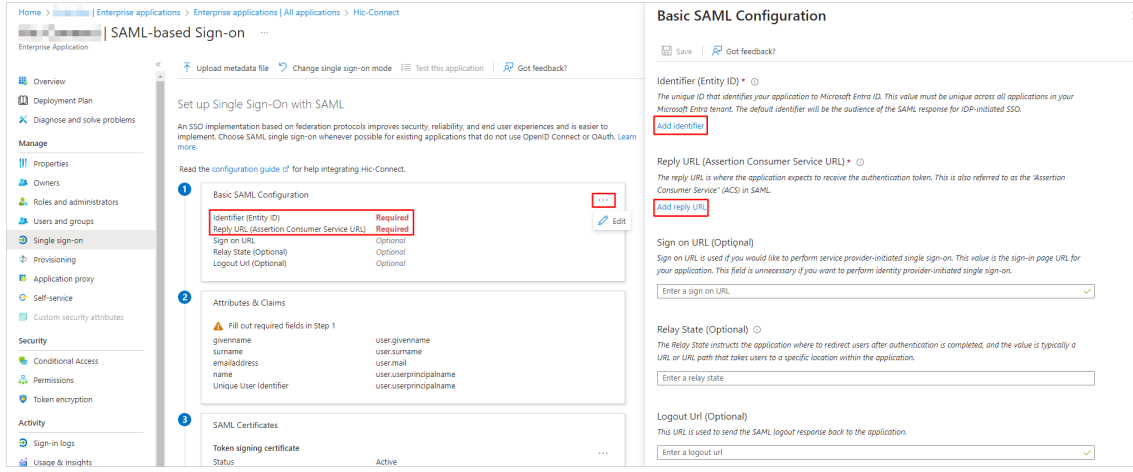


Figure 19-11 Copy to Azure

5. Save the Azure AD configuration and click **Next** on the Hik Connect for Teams configuration page. In step ② of the guide, you need to download the Metadata file from the Azure AD and upload it to Hik Connect for Teams.

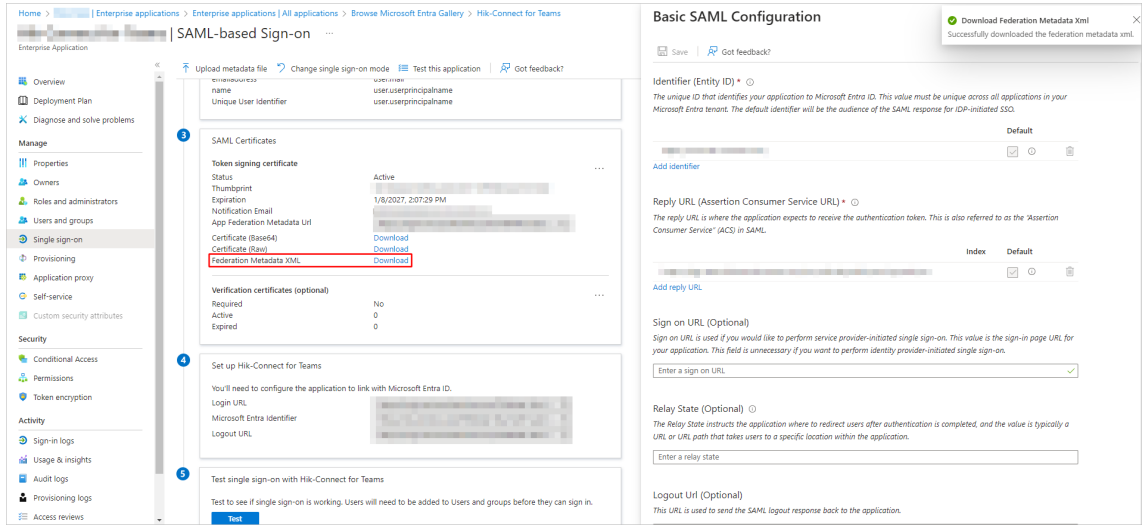


Figure 19-12 Download Metadata File

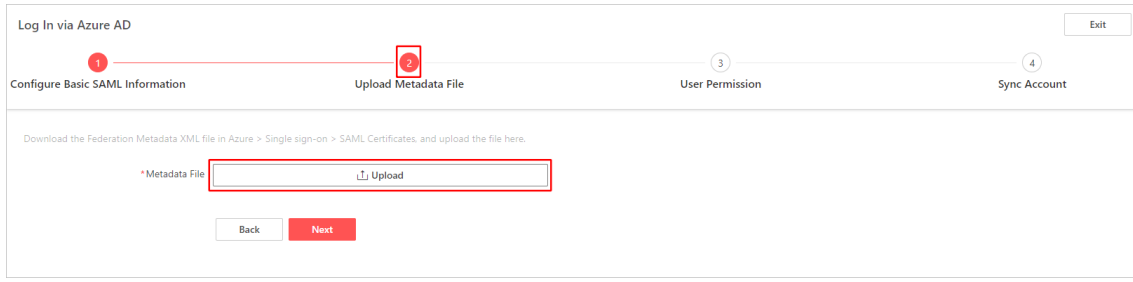


Figure 19-13 Upload to Hik-Connect

6. When the file is being uploaded to Hik Connect for Teams, HCT will test on the contents. If successful, there will be a prompt as follows.

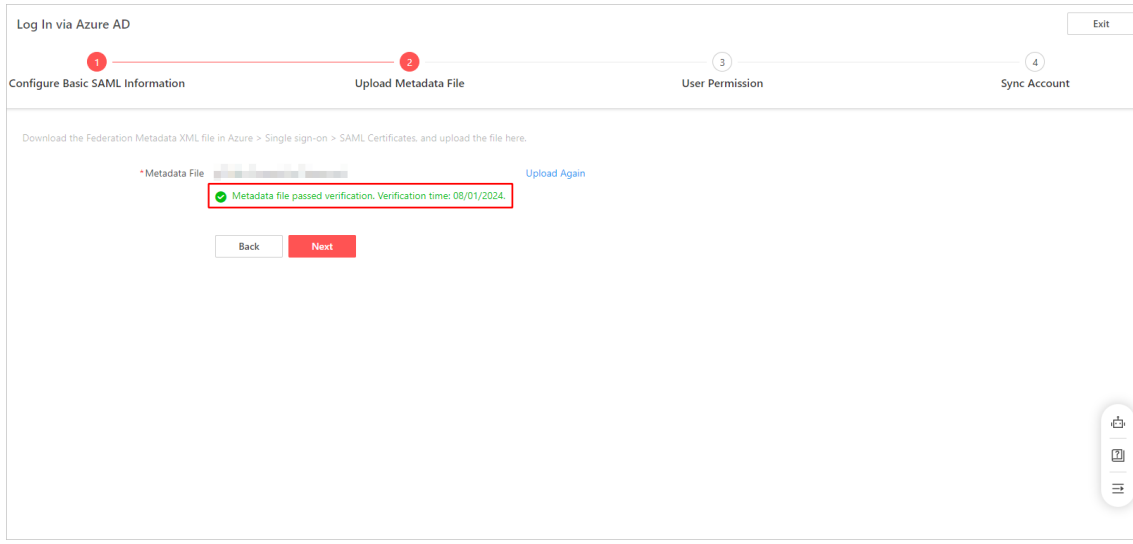


Figure 19-14 Prompt

7. You can select **Users and groups Add user/group** to add the accounts that need to log in to Hik Connect for Teams to the enterprise application in Azure AD according to your needs. These accounts come from your existing Azure AD tenant.

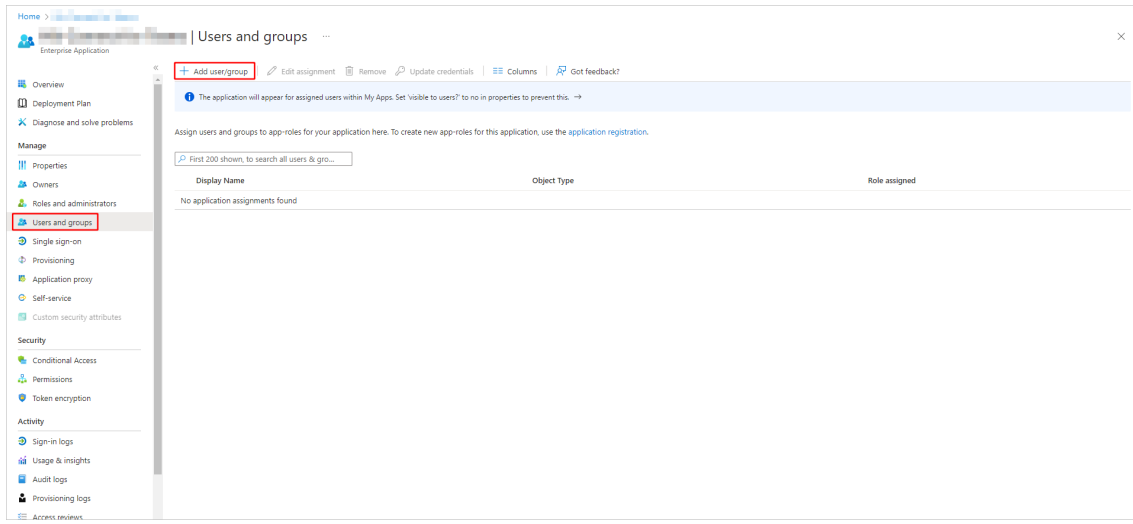


Figure 19-15 Add User

Note

If you have added user groups in your Azure, to sync the users successfully.

- Select **Attribute mapping (Preview)**, and disable Provision Microsoft Entra ID Groups. (Make sure the Enabled column is No.)

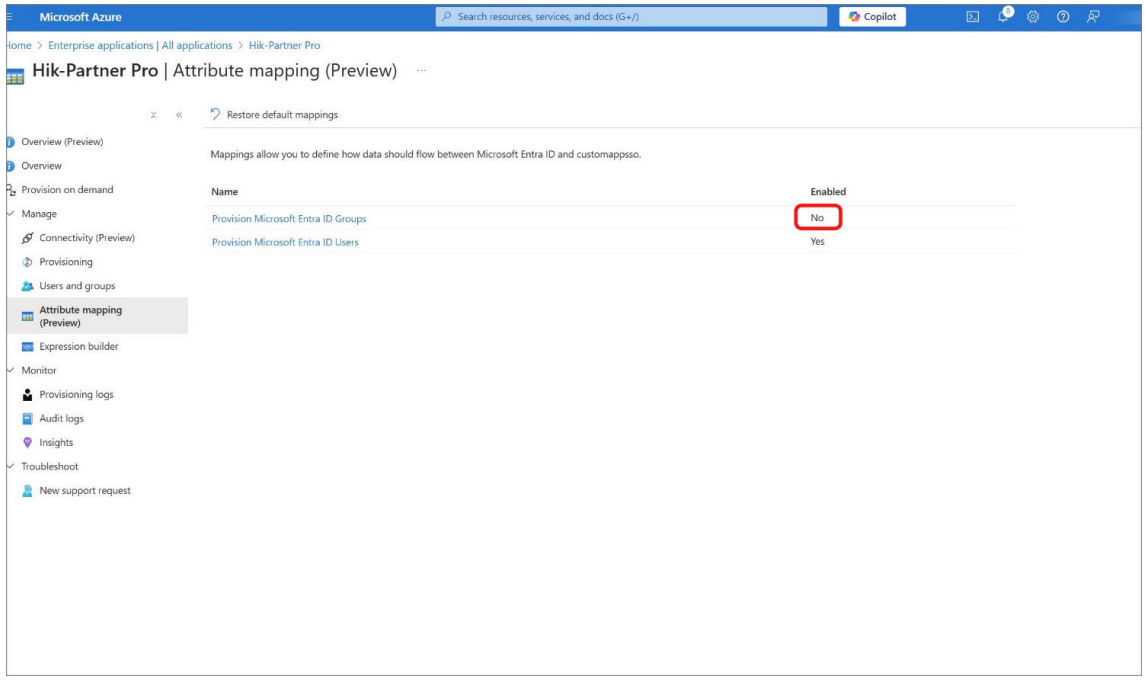


Figure 19-16 Disable Provision

- Select **Provisioning**, and click **Restart provisioning**.

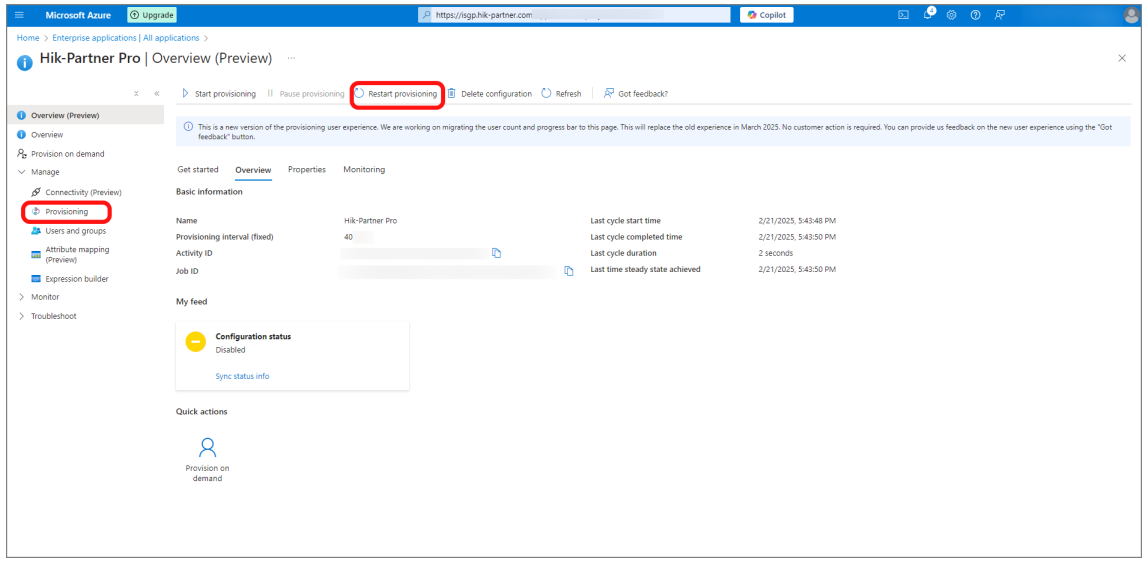


Figure 19-17 Restart Provision

Once you have finished selecting users, return to single sign-on of the enterprise application and perform the login test.

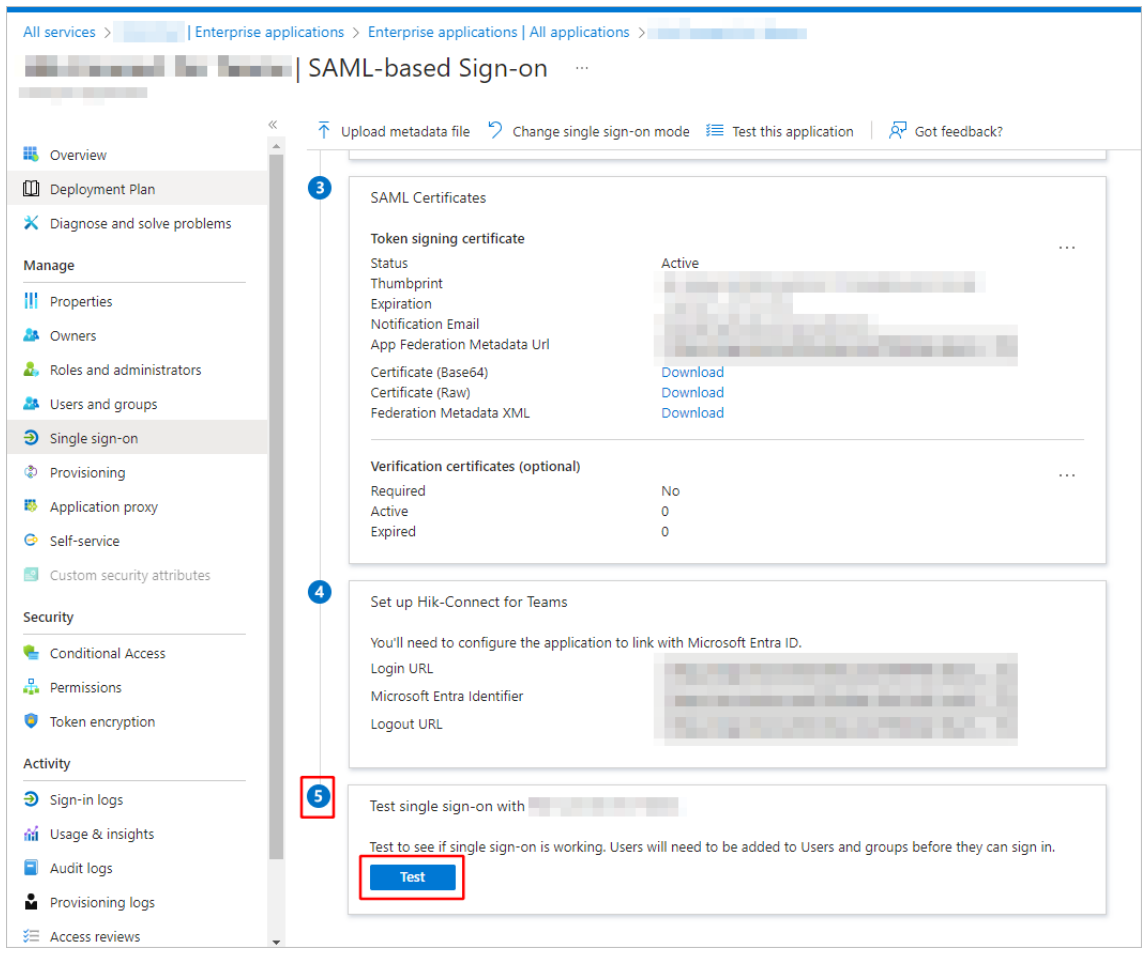


Figure 19-18 Test

If the following prompt pops up, it means that your login link in Hik Connect for Teams using the account in Azure AD has been established. Next, you need to import accounts in your Azure AD into Hik Connect for Teams, so that the corporate accounts in Azure AD to can be used to log in to Hik Connect for Teams. (If there is a prompt of cookies on the current page, click **Accept All**, otherwise there will be exceptions about using the feature.

How to configure Azure AD account synchronization (SCIM)?

1. On Hik Connect for Teams, click **Next** to enter step ③ to configure the default role and area permissions of the Azure AD account.
   Once the configuration is completed, accounts synced in for the first time from Azure AD will be assigned according to these permission settings.

Note

If the current available roles do not meet the actual demand, you can go to the Account and Security module to create roles first, and then return to the current page after the roles are

created. The configuration in steps ① and ② is automatically saved, you can click **Next** to enter step ③).

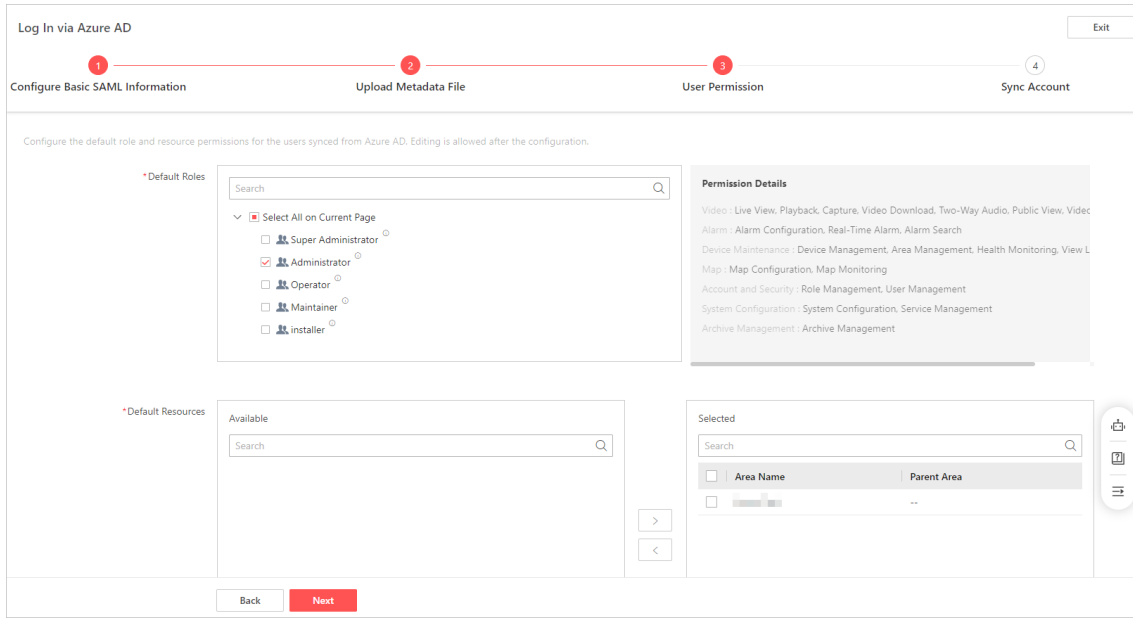


Figure 19-19 Continue

2. After the configuration is completed, click **Next** and go to step ④. At this point, you need to go back to Azure AD enterprise application to configure SCIM account synchronization.
   a. On the Azure AD enterprise application page, select **Provisioning → Get Started** .

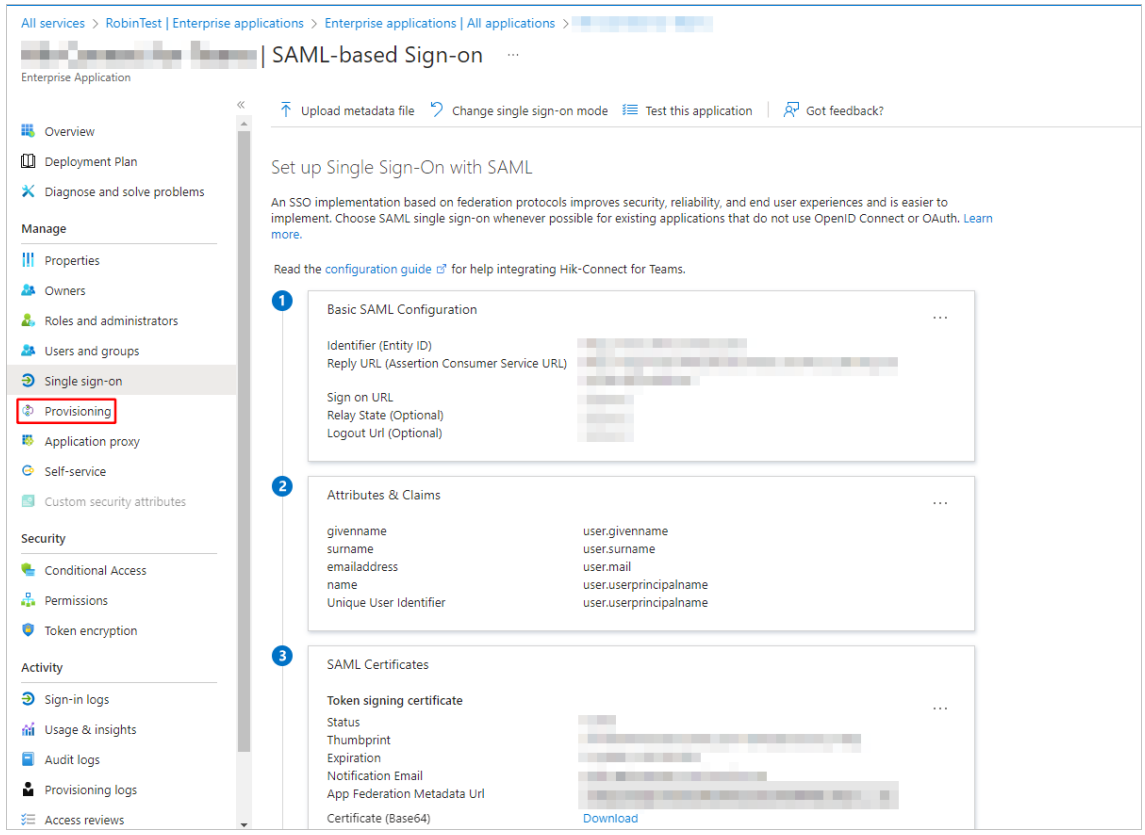


Figure 19-20 Provision

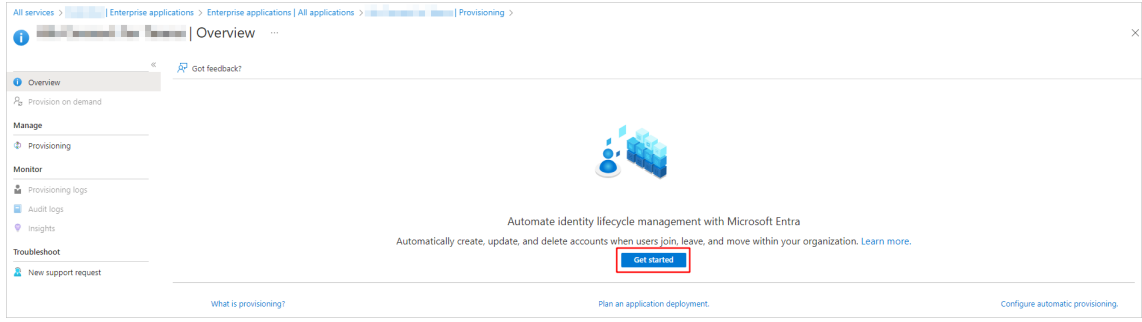


Figure 19-21 Get Started

b. Select Mode as Automatic and fill in the information from Hik Connect for Teams into the Admin Credentials field.

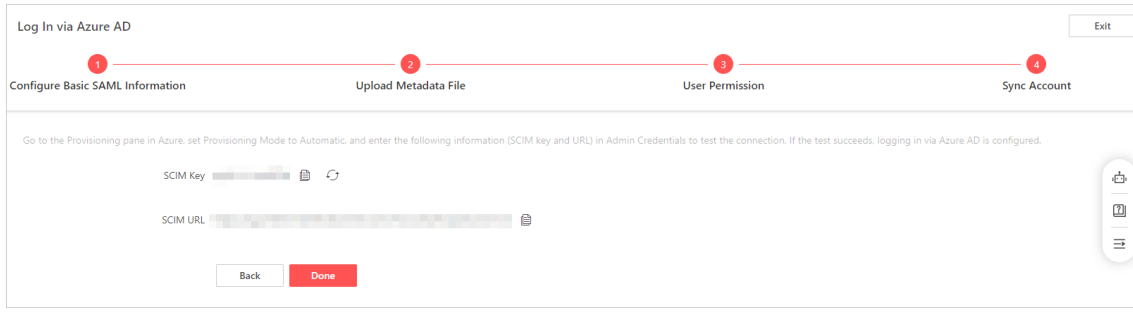


Figure 19-22 Information on Hik-Connect

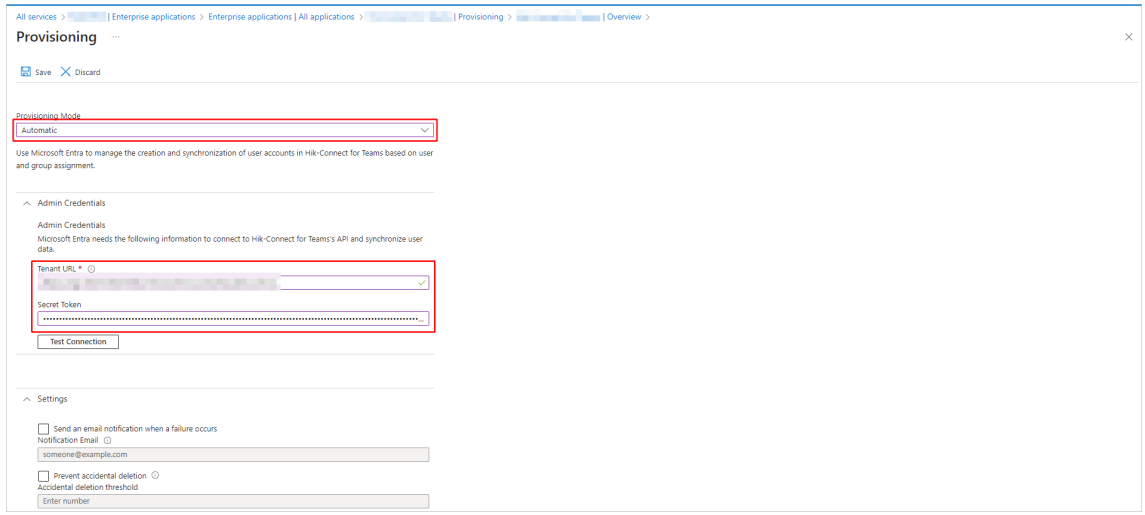


Figure 19-23 Select Mode and Fill in Information

c. Click **Test**, wait for a while, and there will be prompt saying that the connection is successfully. Click **Save**.

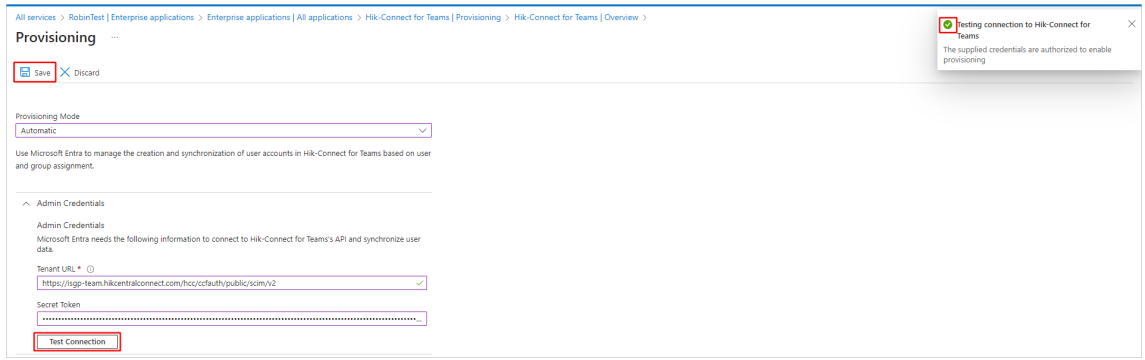


Figure 19-24 Test Connection

d. On the Provisioning page, click **Start provisioning**.

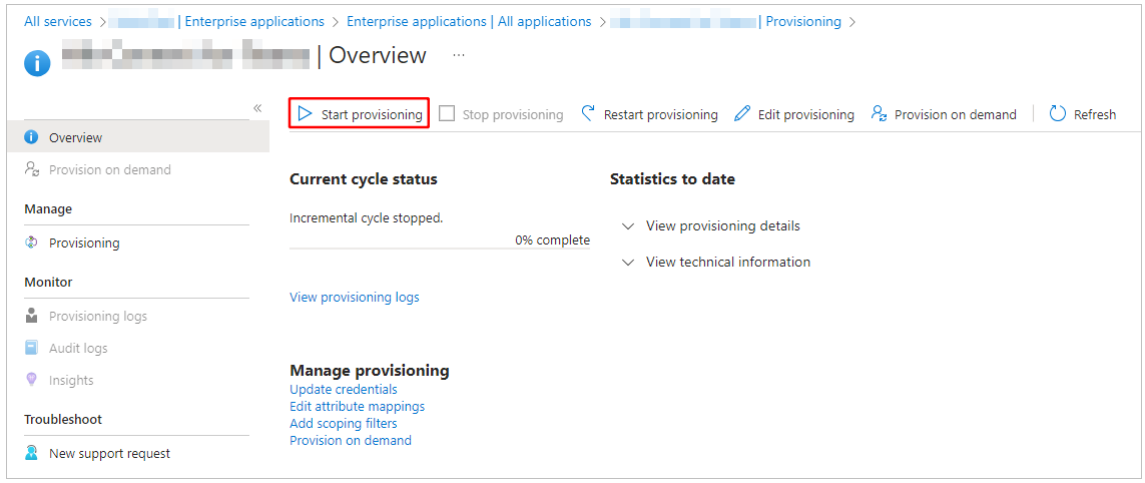


Figure 19-25 Start Provision

e. On the Hik-Connect page, click **Done** to complete the provisioning.

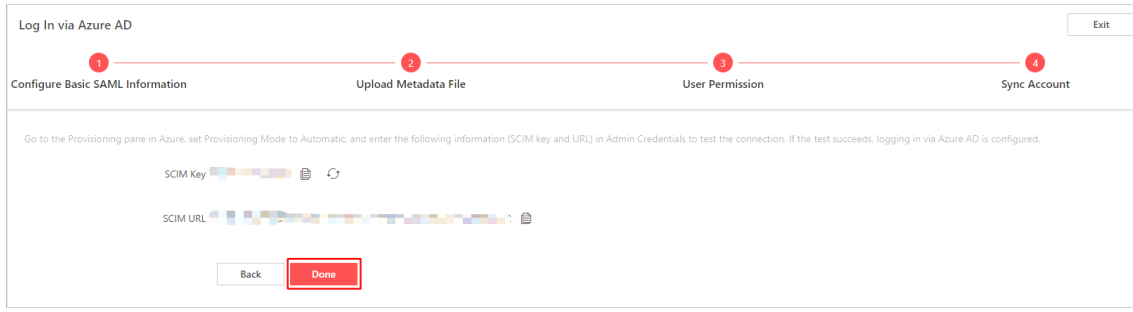


Figure 19-26 Done

Now your configuration is nearly completed, and next you can add the accounts that can log in to Hik Connect for Teams to your Azure AD enterprise application according to your needs. Generally, Azure AD will synchronize these newly added accounts to Hik Connect for Teams within 40 minutes. You can see more detailed synchronization information in Azure AD's **Provisioning** **View provisioning logs**. The accounts that are synchronized into Hik Connect for Teams are differentiated by a special marker.

How to log in via Azure AD?

Once the previous steps have been completed and the Azure AD account has been synchronized to Hik Connect for Teams, you can log in to the Portal or App with the account.

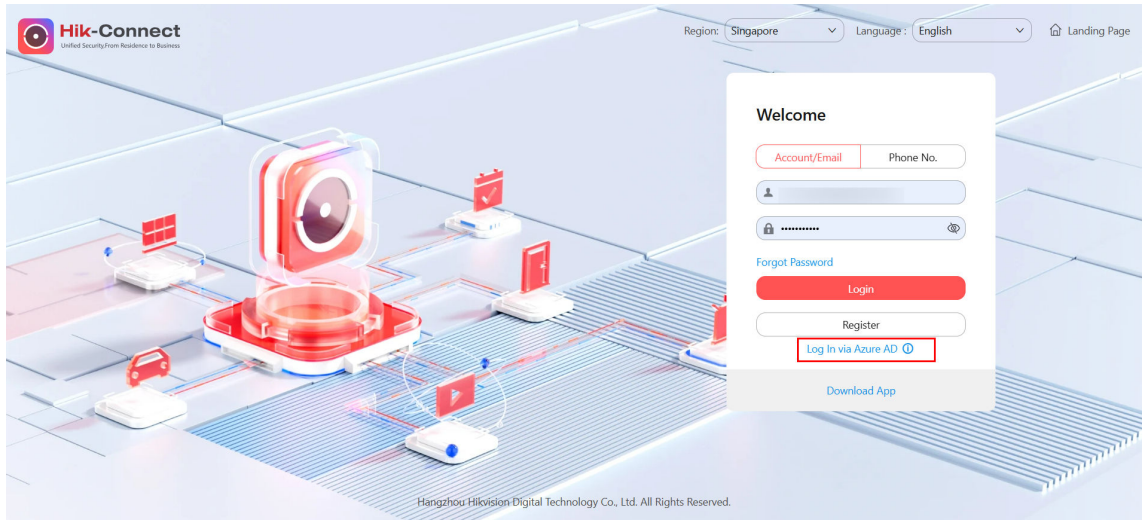


Figure 19-27 Log In

After clicking **Log in via Azure AD**, you will be prompted to enter your Azure AD account email address. If the account exists, Hik Connect for Teams will automatically jump to the Azure AD login page and you will be required to enter the password for authentication, and then you will automatically enter Hik Connect for Teams.

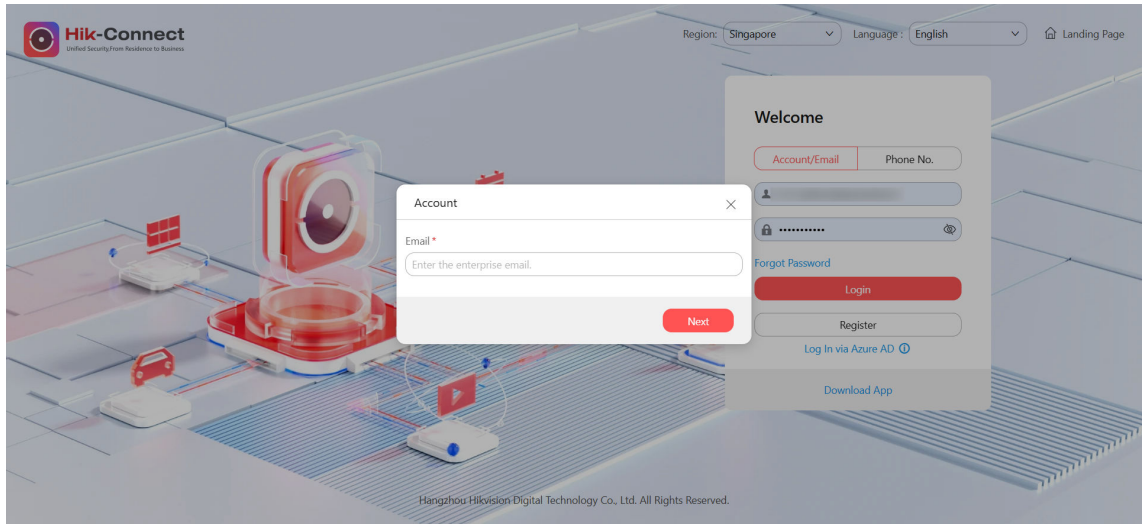


Figure 19-28 Enter Azure AD Email

- An Azure AD user account can only be uniquely bound to a Hik Connect for Teams account.
- Currently, only work/school accounts in Azure AD are supported for synchronization to Hik Connect for Teams. Guest/personal accounts are not supported for logging in to Hik Connect for Teams.

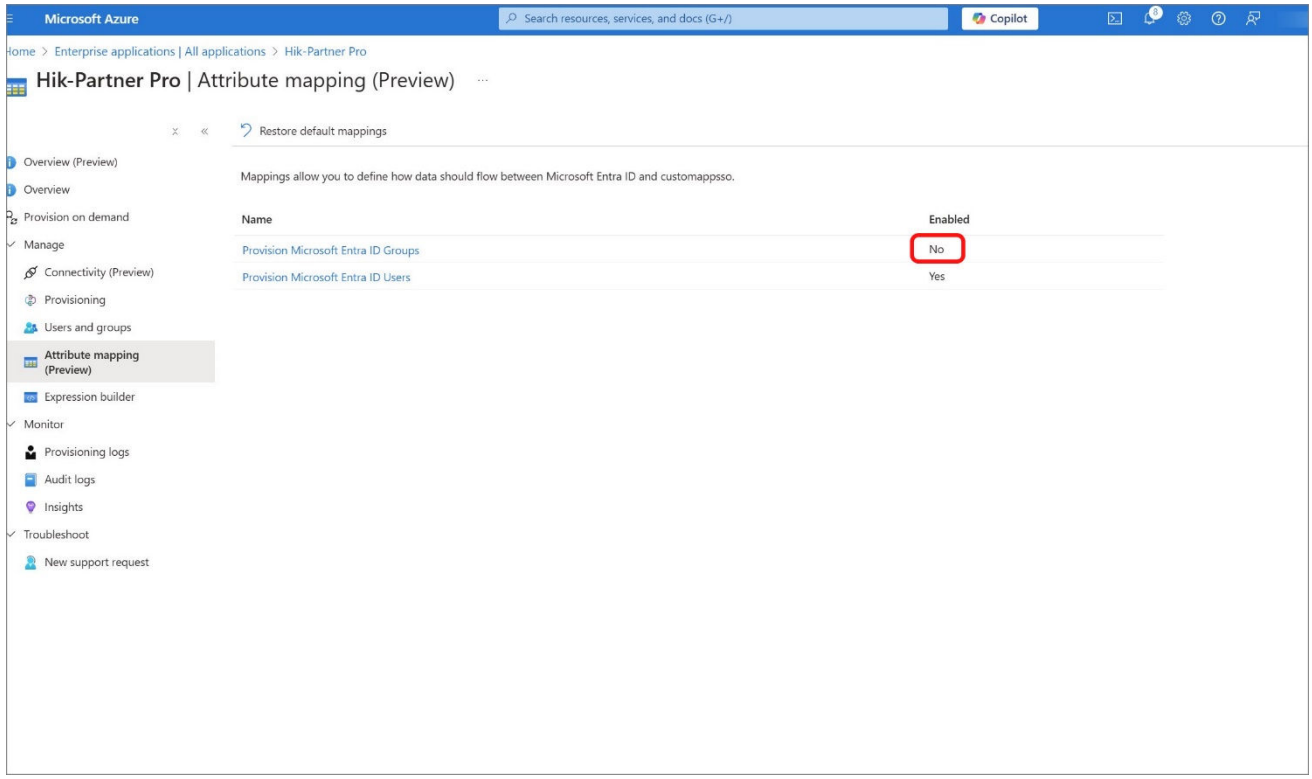
FAQ

Q: Why are my Azure AD accounts not synced to Hik Connect for Teams?

A:

Possible Causes:

1. You have added user groups in your Azure, which causes failure when you sync accounts to Hik-Partner Pro.



2. It generally takes about 40 minutes for Azure AD to sync the newly added accounts.

Troubleshooting Steps:

1. If you have added user groups in your Azure, to sync the users successfully:
   a. Select **Attribute mapping (Preview)**, and disable **Provision Microsoft Entra ID Groups** (Make sure the Enabled column is No.).

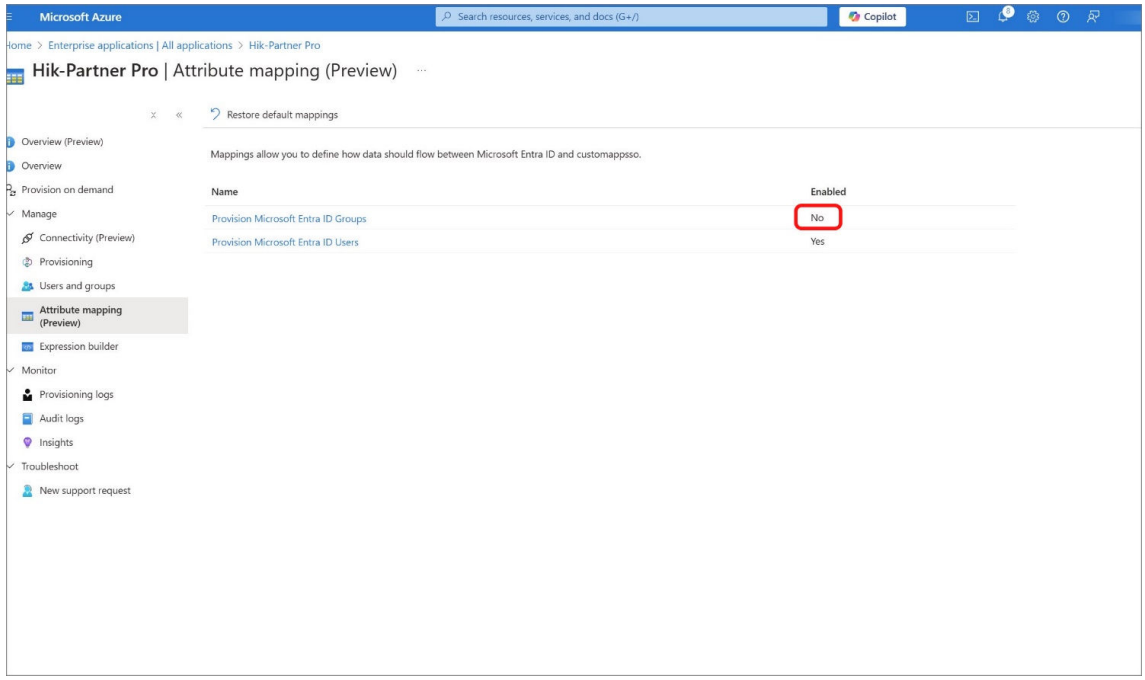


Figure 19-29 Make Sure the Column is No

b. Select **Provisioning**, and click **Restart provisioning**.

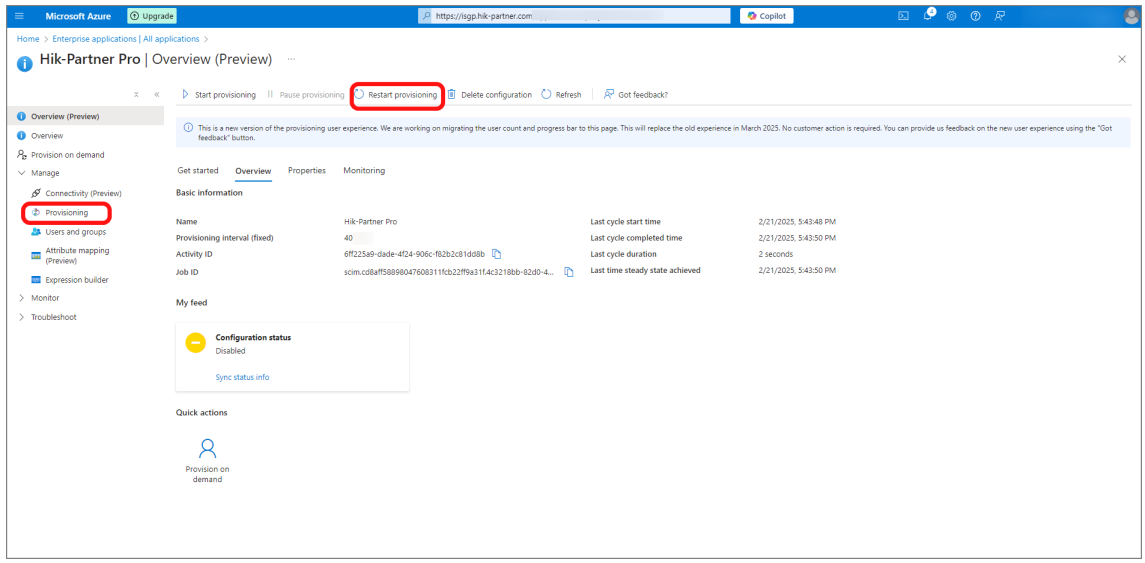


Figure 19-30 Restart Provision

2. Azure AD will generally sync the newly added accounts to Hik Connect for Teams in 40 minutes. Wait for 40 minutes, and to check the sync details, go to **Provisioning View provisioning logs**.

Q: What type of Azure AD accounts can be synced?

A: Currently, only work/school accounts in Azure AD are supported for synchronization to Hik-Connect. Guest/personal accounts are not supported for logging in to Hik Connect for Teams.

19.3 How to 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.

1. On the top navigation bar of the Portal, click **Team Management → Account and Security → Users** to enter the user management page.
2. Click **Add**.

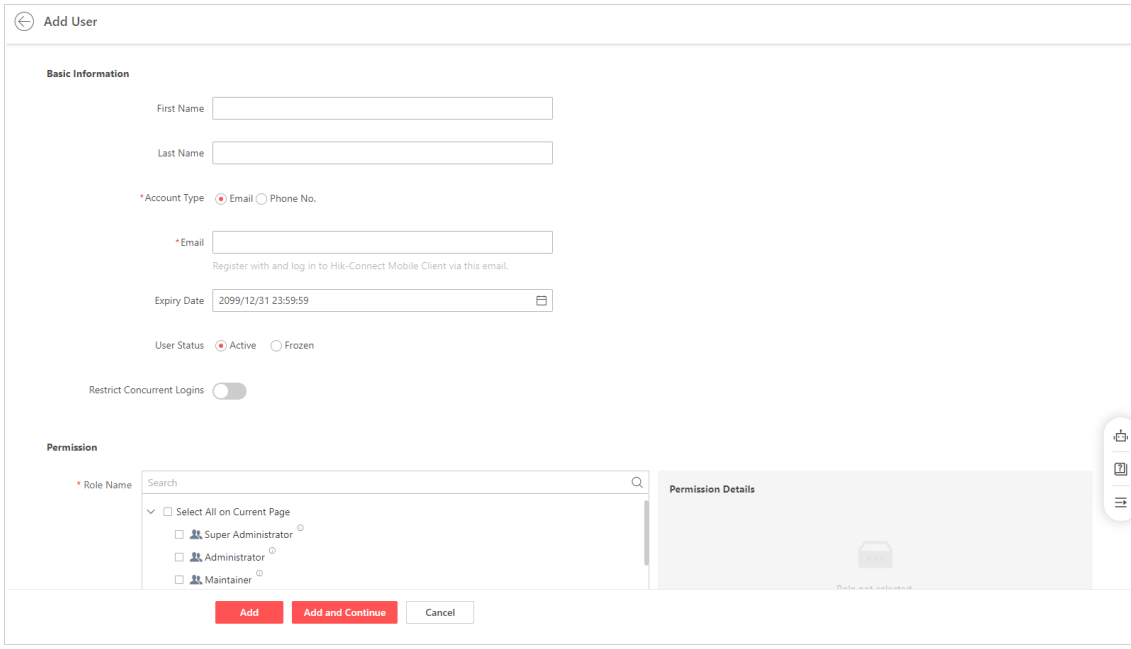


Figure 19-31 Add a Normal User

3. Set basic information for the user.

Account Type

Select **Email** or **Phone No.** as the account type, and the user can log in to the System via the email address or phone number. In this way, the System will automatically notify the user of the initial password by sending an email or a message to the email address or phone number.

User Status

Active is selected by default. If you select **Frozen**, this user account cannot log in to the System until you unfreeze it.

Restrict Concurrent Logins

To limit the maximum IP addresses logged in to the System using the user account, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.

4. Configure resource permissions for the user.
5. Perform further operations after adding normal users.

19.4 How to import users?

1. On the top navigation bar of the Portal, click → **Team → Account and Security → Users** to enter the user management page.
2. Click **Import** at the top of user list.
3. In the pop-up window, click **Download Template** to save the template to your PC.
4. In the downloaded template, enter the user information following the rules shown in the template.
5. In the pop-up window, click , and then select the template from your PC.
6. Click **Import** to batch import users to the System.

Table 19-1 Further Operations

User Intention	Description
Role Management	Click **Role Management** to add, edit, and delete roles.
Edit a User	Click the name of a user to view and edit the user's settings, such as the first name, the last name, user status, and permissions.
Reset Password for a Normal User	On the editing page of a user, click **Reset** in the Password field to set a new password for the user. For normal users who log in to the System via email addresses, you can enter the current admin password to send emails to them for changing passwords, or check **Set New Password for User Manually** to directly reset passwords for them. For normal users who log in to the System via their account names, you can enter the current admin password and new passwords to reset the password for them. **Note** - The super user or users assigned with the role of administrator can reset passwords of all normal users. - Normal users with the User Management permission can reset passwords of users without the User Management permission.
Delete Users	Check one or multiple users and click **Delete** to delete the selected users.

User Intention	Description
	Note If the users to be deleted is online, after they are deleted, the users will be forced to log out.
Batch Freeze/ Unfreeze Users	Check the existing users and click **Freeze** or **Unfreeze** to batch freeze or unfreeze the selected users. **Note** For a frozen user, the user account cannot log in to the System until you unfreeze it.
Import Users	Click **Import** and select a file from the PC to import users.
Export User Information	Select the user(s) and click **Export** to export the information about the selected user(s).
Invite User to Join Team	In the User Status column, hover over , and click **Send SMS Invitation** to invite a user to join your team.

19.5 How to assign roles to users?

Configure resource permissions for the user.

Area Display Rule

Show or hide specific area(s) for the user. If an area is hidden, the user cannot see and access the area and its resources.

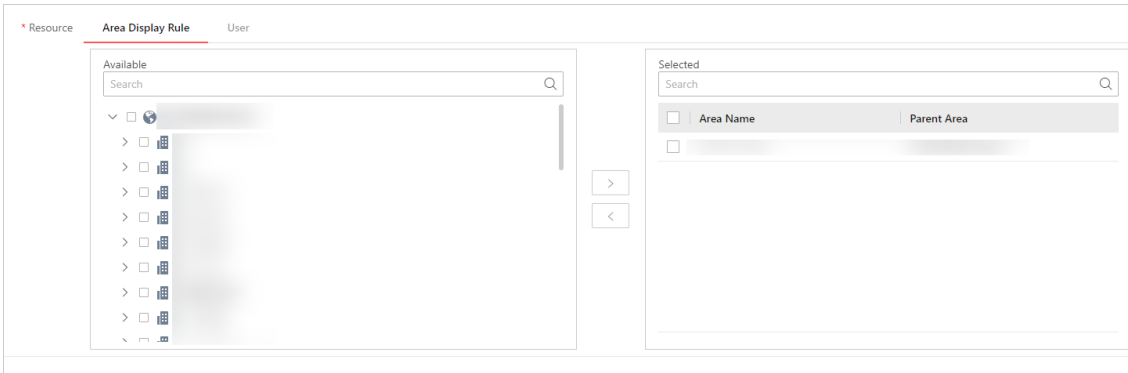


Figure 19-32 Area Display Rule

User

Assign all users or specified users to this user for management, such as viewing and editing the information, resetting passwords, deactivating/activating, deleting, and so on.

Note

Only users assigned with the role of super administrator can assign all users to other users for management. Once users have the management permission of all users, the subsequently added users can also be managed by them.

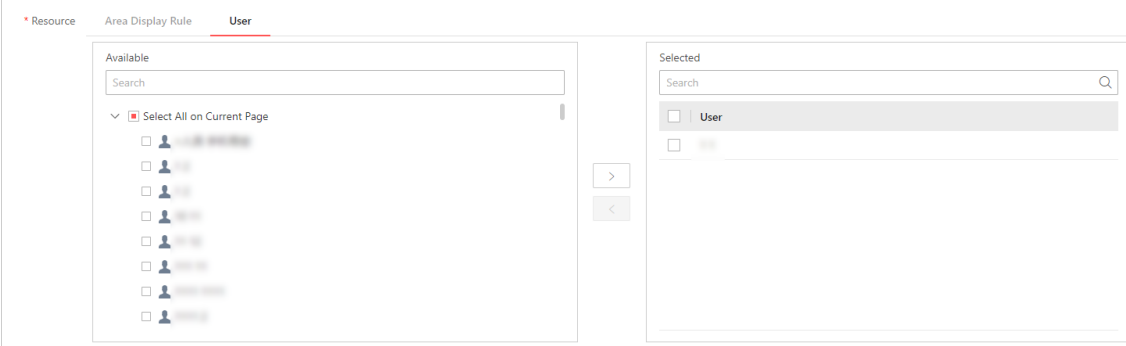


Figure 19-33 User

To batch manage permissions, click **Select Role** to select the role(s) that you want to assign to the user.

- Select a predefined role.

Note

The System has predefined the following default roles: Super Administrator, Administrator, Operator, and Maintainer. You can click the role name to view details. These default roles cannot be edited or deleted, except for the Maintainer role, whose permissions can be edited.

Super Administrator

The role has all permissions (including operation and configuration permissions) and access all resources.

Administrator

The role has all operation and configuration permissions (except for mobile credential permissions) of all services or modules on the System.

Operator

The role has operation permissions (e.g., live view, playback, door control, driving monitoring) of services or modules on the System.

Maintainer

By default, has the same permissions with the Operator role, but its permissions can be edited according to the actual needs. This role is used for installers or technical supports (who have to log in to the System via the URL and verification code) to confirm system faults.

Self-Service

The role that has the mobile credential permission, person management permissions, and operation permissions of the access control service and video intercom service.

- Click **Add Role** to add a new role.

Note

Only active roles can be assigned to users.

19.6 How to change password of the current user?

On the editing page of a user, click **Reset** in the Password field to set a new password for the user.

For normal users who log in to the System via email addresses, you can enter the current admin password to send emails to them for changing passwords, or check **Set New Password for User Manually** to directly reset passwords for them.

For normal users who log in to the System via their account names, you can enter the current admin password and new passwords to reset the password for them.

Note

- The super user or users assigned with the role of administrator can reset passwords of all normal users.
- Normal users with the User Management permission can reset passwords of users without the User Management permission.

19.7 How to delete a super user?

If you want to change the System's owner, you can delete the created super user.

1. On the top navigation bar of the Portal, click → **Team** → **Account and Security** → **Users** to enter the user management page.
2. Click a user name to enter the super user details page.
3. Click **Delete Account** in the top right corner.

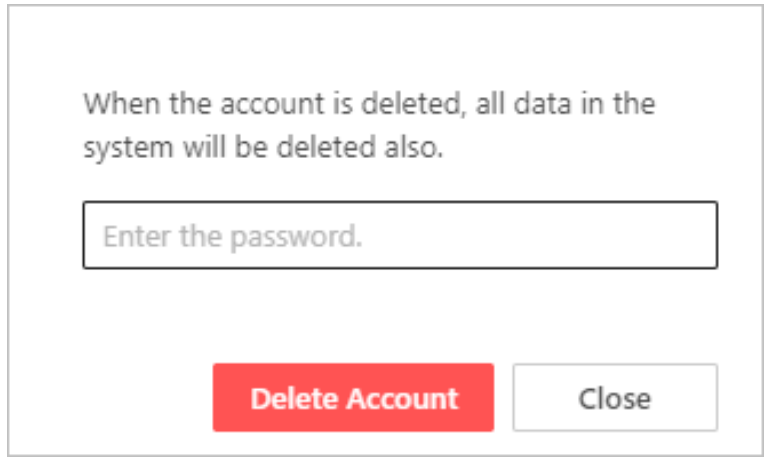


Figure 19-34 Delete Super User

4. In the pop-up window, enter the password of super user and click **Delete Account**.

Note

The super user cannot be deleted if the System still contains some devices.

19.8 How to enable Two-Factor Authentication (2FA)?

You can enable Two-Factor Authentication for your account. Once enabled, logging in will require not only your password but also a verification code sent to your email or mobile phone via SMS, or a push notification to a trusted device, adding an extra layer of security.

1. a. Log in to the Portal, navigate to the → **Team** → **Team Configuration** → **Account Security** .
   b. Enable **Two-Factor Authentication** and the system will send a verification code to your email for security confirmation.

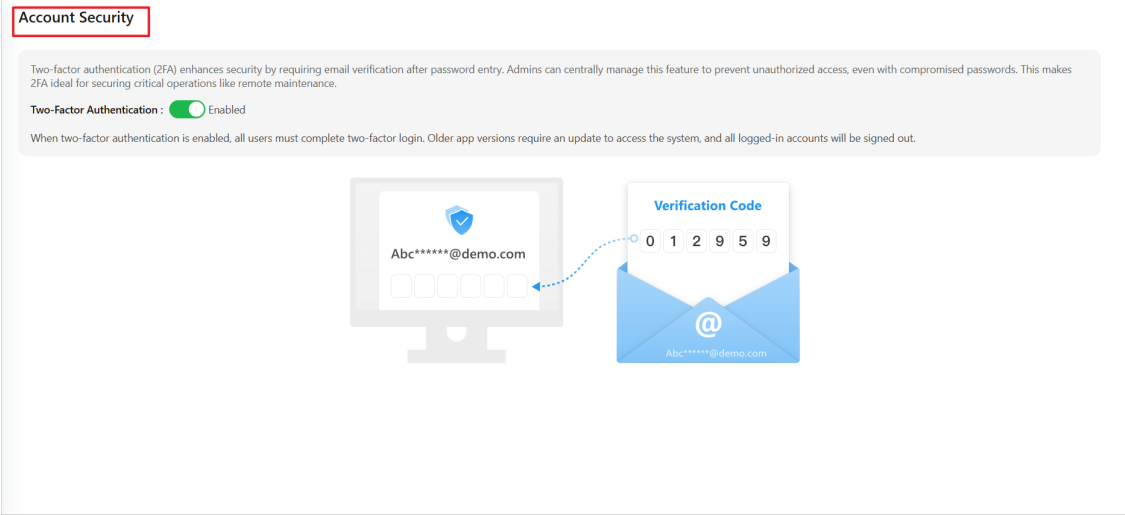


Figure 19-35 Enable 2FA

2. **Login Process:** When logging into an account with MFA enabled from a new, untrusted device:
   a. After entering the correct username and password, the system will require a second verification step.

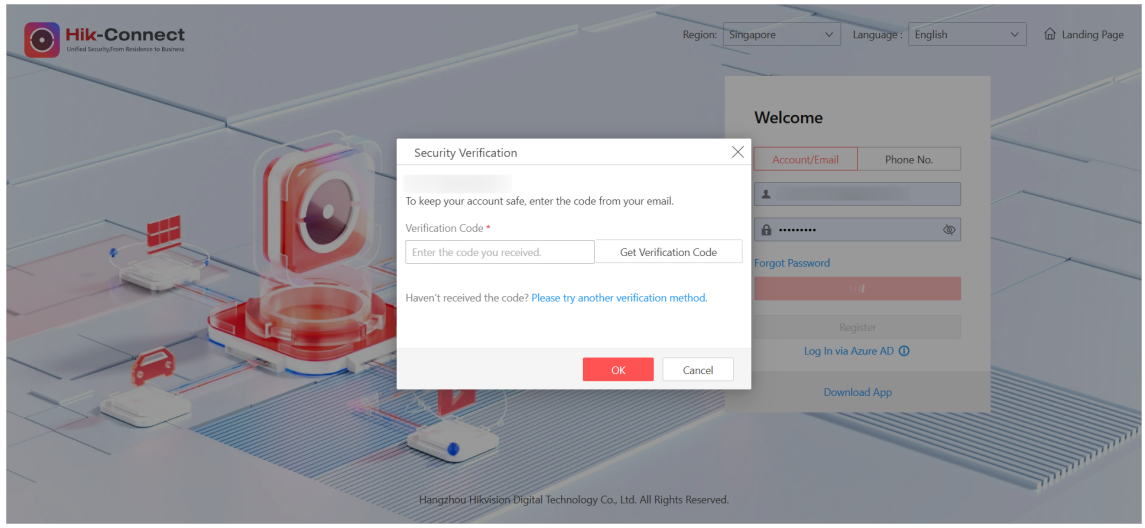


Figure 19-36 Verification Required

   b. A verification code will be sent by default to your registered email (or phone number). You may also have the option to receive a push notification on another trusted app device.
   c. Enter the correct code to log in successfully. You can choose to add the current device to your list of trusted devices, so future logins from this device won't require the second step.
3. **Managing Trusted Devices:** After logging in, you can view and manage your list of trusted devices within the "Me" or account settings. You can see device info, login location and time, and remove devices you no longer use (you cannot remove the device you are currently using).

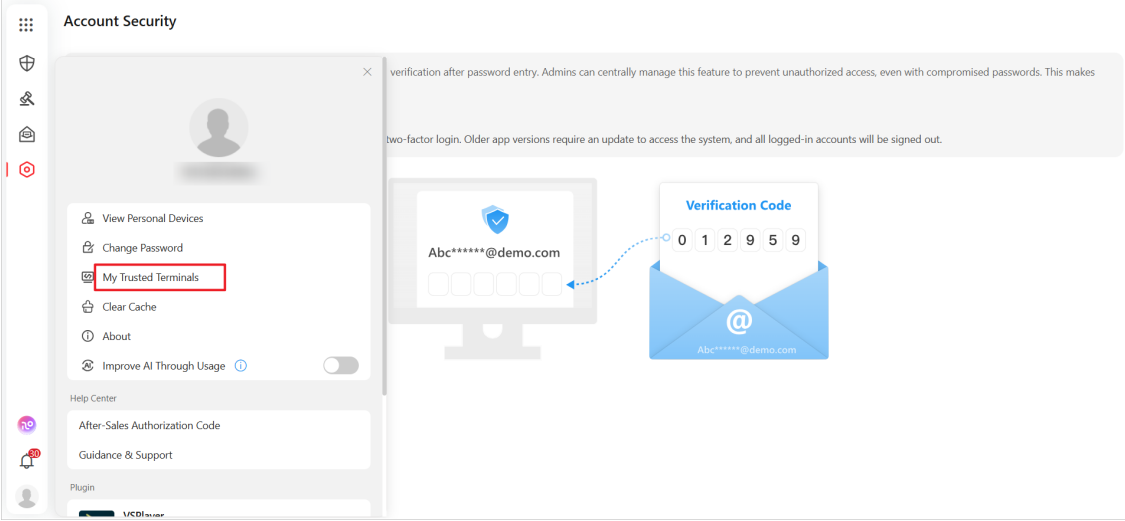


Figure 19-37 View Trusted Terminals


See Far, Go Further