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.

Contents

Chapter 1 Introduction 1

1.1 Target Audience 1

1.2 Related Entities 2

1.3 Running Environment 2

Chapter 2 Hik Connect for Teams Portal Overview 4

Chapter 3 Account Management 8

3.1 About Licenses 8

3.2 Get Your Account Information 10

3.3 Login 13

3.4 Log In via an Azure Account 14

Chapter 4 Application Summary 15

4.1 Flow Chart of Door Access Control 16

4.2 Flow Chart of Video Intercom Management 17

4.3 Flow Chart of Time & Attendance 18

4.4 Flow Chart of On-Board Monitoring 19

Chapter 5 Resource Management 21

5.1 Manage Area 21

5.2 Manage Encoding Device in Area 23

5.2.1 Add Detected Online Encoding Devices 23

5.2.2 Add Encoding Device by Device Serial No. and Verification Code 26

5.3 Manage Access Control Devices in Area 29

5.3.1 Add Detected Online Access Control Devices 29

5.3.2 Add Access Control Device by Device Serial No. and Verification Code 31

5.3.3 Configure Access Control Device Parameters 34

5.4 Manage Video Intercom Devices in Area 35

5.4.1 Add Detected Online Video Intercom Devices 35

5.4.2 Add Video Intercom Device by Device Serial No. and Verification Code 38

5.4.3 Configure Video Intercom Device Parameters 41

5.5 Manage Hik-ProConnect Box in Area 42

5.5.1 Add Detected Online Hik-ProConnect Boxes 42

5.5.2 Add Hik-ProConnect Box by Device Serial No. and Verification Code 45

5.6 Manage On-Board Device in Area 48

5.6.1 Add Detected Online On-Board Devices 48

5.6.2 Add On-Board Device by Device Serial No. and Verification Code 51

5.7 General Device Operations 53

5.7.1 Import Devices via Template 53

5.7.2 Import Personal Devices to Hik Connect for Teams 54

5.7.3 Unbind a Device from Its Current Account 56

5.7.4 Create Password for Inactive Device(s) 57

5.7.5 Edit Online Device's Network Information 59

5.7.6 Reset Device Password 59

5.7.7 Upgrade Device Firmware 60

5.7.8 Export Device Information 61

5.8 Manage Cameras in Area 62

5.8.1 Add a Camera to Area 62

5.8.2 Edit a Camera in Area 63

5.9 Manage Vehicles in Area 64

5.10 Manage Doors in Area 65

5.10.1 Add a Door to Area 65

5.10.2 Edit a Door in Area 66

5.11 Manage Alarm Inputs in Area 68

5.12 Manage Alarm Outputs in Area 69

Chapter 6 Video Management 70

6.1 Configure Recording and Storage 70

6.1.1 Configure Recording for Cameras 71

6.1.2 Configure Recording Schedule Template 72

6.1.3 Configure Cloud Storage for Camera Linked to Hik-ProConnect Box 73

6.1.4 Configure Cloud Storage for Camera Linked to NVR 74

6.1.5 Batch Configure Cloud Storage for Cameras 75

6.2 Start Fast View 77

6.3 Manage Views 77

6.3.1 Add a View Group 77

6.3.2 Add a View 78

6.3.3 Perform View Auto-Switch 79

6.3.4 Perform Camera Auto-Switch in One Window 79

6.4 Live View 80

6.4.1 Start Live View in Area Mode 80

6.4.2 Start Live View in View Mode 82

6.4.3 PTZ Control 84

6.4.4 Acknowledge Alarms During Live View 86

6.4.5 View Dewarped Live View of Fisheye Camera 86

6.5 Playback 87

6.5.1 Start Playback in Area Mode 87

6.5.2 Start Playback in View Mode 90

6.5.3 Synchronous Playback 92

6.5.4 Play Back Videos Stored on the Cloud 92

6.6 Set Video Parameters 92

6.6.1 Set Network Parameters 92

6.6.2 Set File Parameters 93

6.6.3 Set Display Parameters 94

6.6.4 Set Audio Parameters 96

6.6.5 Set Shortcuts for USB Joysticks 96

6.7 Video Search 97

6.7.1 Search for Video Footage 97

6.7.2 Search for Vehicle/Person-Detected Videos 99

6.7.3 Search for Tagged Videos 101

6.8 Download Task Management 102

Chapter 7 Access Control Management 105

7.1 Configurations Before Access Control Management 105

7.1.1 Set Holidays for Schedule 105

7.1.2 Set Access Schedule Template 106

7.1.3 Set General Parameters 107

7.1.4 Subscribe to Device and Access Events 107

7.2 Manage Access Level 108

7.2.1 Access Level Overview 108

7.2.2 Add Access Level 109

7.2.3 Assign Access Level 110

7.2.4 Manually Apply Access Level Settings to Device 112

7.3 Real-Time Monitoring 113

7.3.1 View Real-Time Access Events 113

7.3.2 Control Door 114

7.4 Record Search 115

7.4.1 Search for Access Records 116

7.4.2 Search for Data Recorded on Device 117

Chapter 8 Time & Attendance 118

8.1 Basic Configuration 118

8.1.1 Select Shift Type 118

8.1.2 Define Weekend 119

8.1.3 Define Overtime 119

8.1.4 Configure Attendance Rule 120

8.1.5 Add Timetable 124

8.1.6 Add Holiday 127

8.1.7 Add Leave Type 129

8.1.8 Configure Report Settings 129

8.1.9 Configure Attendance Parameters for Person 130

8.1.10 Customize Export 132

8.2 Schedule Management 133

8.2.1 Assign Schedule to Persons 133

8.2.2 Schedule Overview 134

8.3 Application Management 136

8.3.1 Submit Leave Application 137

8.3.2 Submit Attendance Correction Application 138

8.3.3 Review Applications 140

8.4 View and Export Reports 141

Chapter 9 Video Intercom Management 144

9.1 Video Intercom Overview 144

9.2 Housing Management 144

9.2.1 Add Building 145

9.2.2 Add Room 146

9.2.3 Add Resident 147

9.3 Call Management 150

9.3.1 View Call History 150

9.3.2 Specify Users for Receiving Calls from Devices 150

9.4 Create Temporary Pass 151

Chapter 10 On-Board Monitoring 154

10.1 Dashboard Overview 154

10.2 Configurations Before On-Board Monitoring 155

10.2.1 Set Basic Parameters 155

10.2.2 Set Event Types to Be Received 156

10.3 Configure Driving Rule 156

10.3.1 Add a Driving Rule for Region 157

10.3.2 Add a Driving Rule for Route 159

10.3.3 Configure a Rule Schedule Template 163

10.4 Driving Monitoring 164

10.5 Search for Tracks 167

10.6 Search for Driving Events 168

10.7 Statistics and Reports 170

10.7.1 Generate a Driving Duration Report 170

10.7.2 Generate a Driving Distance Report 172

10.7.3 Generate a Speeding Report 173

10.7.4 Generate a Driving Event Report 174

Chapter 11 Analysis Report 177

11.1 Basic Configuration 177

11.1.1 Add Analysis Configuration 177

11.1.2 Configure the Source of People Counting Data 178

11.1.3 Configure Global Heat Map 180

11.1.4 Add Promotion 183

11.2 View General Report 183

11.3 View Promotion Report 187

Chapter 12 Map Management 191

12.1 Map Settings 191

12.1.1 Link Area with Map 191

12.1.2 Change Monitored Area on GIS Map 192

12.1.3 Add Static Map for Area 192

12.1.4 Add Hot Spot on Map 193

12.1.5 Add Hot Region on Map 194

12.1.6 Add Tag on Map 195

12.2 Map Monitoring 195

12.2.1 Operate Hot Spot 195

12.2.2 Preview Hot Region 196

12.2.3 Operate Map 196

Chapter 13 Alarm Management 198

13.1 Alarm Settings 198

13.1.1 Supported Alarms 198

13.1.2 Add an Alarm Rule 199

13.1.3 Configure a Receiving Schedule Template 203

13.1.4 Define Alarm Priority and Alarm Category 204

13.1.5 Add an Email Linkage Template 206

13.2 Search for Alarms 207

13.3 View Resources' Real-Time Alarms 209

13.4 View Pop-Up Window Triggered by Alarm 213

Chapter 14 Person Management 215

14.1 Add a Department 215

14.2 Add a Person 217

14.3 Import Persons from Device 223

14.4 Import Persons via Template 225

14.5 Batch Issue Cards to Persons 226

Chapter 15 Maintenance 231

15.1 Real-Time Status Overview 231

15.2 Health Monitoring 232

15.3 Log Search 234

15.3.1 Search for Logs Stored on Devices 234

15.3.2 Search for Operation Logs 236

Chapter 16 Team Management 237

16.1 Role and User Management 237

16.1.1 Add a Normal User 237

16.1.2 Add a Role 240

16.1.3 Import Users 243

16.1.4 Change Password of Current User 243

16.1.5 Delete the Super User 244

16.2 Archive Management 245

16.2.1 Archive Overview 245

16.2.2 Archive Settings 246

16.2.3 Archive Search 248

16.3 Service Details 253

16.3.1 Service Overview 254

16.3.2 Invite a Service Provider to Manage System 256

16.3.3 View Details of Cloud Storage Service 258

16.4 Configure Email Account 260

16.5 Team Configuration 261

Chapter 1 Introduction

Hik Connect for Teams (HCT) is a Video Security as a Service (VSaaS) platform for enterprise users. 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, 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.

HCT provides easy-to-use clients (a Portal and a Mobile Client) for users to access it.

Table 1-1 Portal and Mobile Client

Client	Description
Portal	For users to 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	For users to log in to HCT to use more lightweight features of the services, such as live view, playback, driving monitoring, remote door controls, person/resident management, etc. It is also for self-service users to use self-service features such as door opening via mobile credentials, call answering and management, temporary pass management, etc.

1.1 Target Audience

This manual provides the super user and normal users with the essential information and instructions about how to use the Portal to perform configurations and/or operations for video monitoring, on-board monitoring, video intercom management, and access control management. Specifically, it describes how to manage users, resources, alarms, etc., and perform operations such as live view, driving monitoring, housing management, and door controls.

1.2 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 the 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, 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 Running Environment

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)

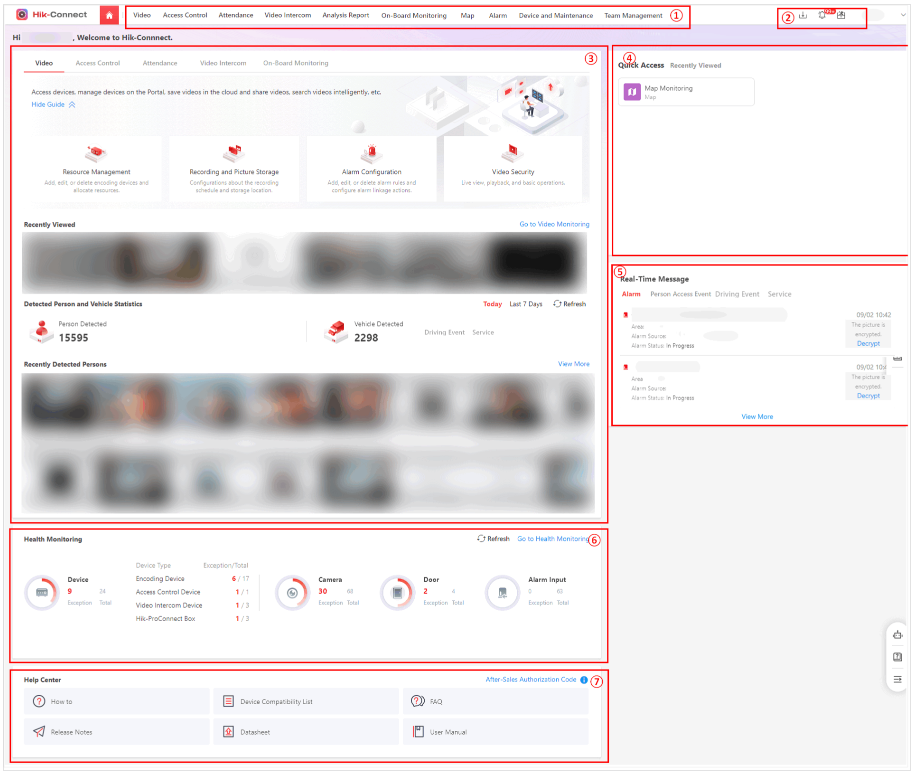
Web Browser Version

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

Chapter 2 Hik Connect for Teams Portal Overview

The home page of the Portal provides an intuitive user interface for you to access features and resources in the System.

The home page of the Portal is shown below.



Access devices, manage devices on the Portal, save videos in the cloud and share videos, search videos intelligently, etc.

Resource Management: Add, edit, or delete encoding devices and allocate resources.

Recording and Picture Storage: Configurations about the recording schedule and storage location.

Alarm Configuration: Add, edit, or delete alarm rules and configure alarm linkage actions.

Video Security: Live view, playback, and basic operations.

The picture is encrypted.

Figure 2-1 Home Page

Table 2-1 Home Page Description

No.	Description
1	The top navigation bar that provides access to the service modules and management modules such as Map, Alarm, Person, Device and Maintenance, and System Management. **Note** Which service modules' entries are displayed here depend on which services you are using (either on free/trial plans or full service plans), including video management, on-board monitoring, access control, video intercom, and analysis report.

No.	Description
	You can click 🏠 to go back to the home page at any time, and click ··· to find the hidden entries of the navigation bar.
2	The area from which you can access the Download Center (refer to ***Download Task Management*** for details) and the Message Center (refer to ***View Resources' Real-Time Alarms*** for details), download the VSPlayer and Web Control, view personal devices (if there are any, and refer to ***Import Personal Devices to Hik Connect for Teams***), view information about HCT (e.g., version, user agreement terms, legal information, etc.), and change the account password (refer to ***Change Password of Current User*** for details).
3	The area from which you can view configuration guides, the recently accessed resources/modules, and service-related statistics for each service. You can also go to the corresponding pages by clicking on the cards of the guides, clicking **View More** and **Go to ...** displayed for each section of the service overview, or clicking some of the service-related statistics. **Note** Which service modules' entries are displayed here depend on which services you are using (either on free/trial plans or full service plans), including video management, on-board monitoring, video intercom, and access control. • **Video Management**: You can check the recently viewed cameras, captures of videos with persons/vehicles recently detected, and the total number of captures with persons/ vehicles detected on the current day or over the past 7 days. • **Access Control**: You can view the overall statistics related to persons' access levels, the recently controlled doors, and the recent access records. You can also hover over a door to perform door controls as needed. Click **Quick Configure** below the service overview to complete the service-related configurations in order without manually jumping from module to module. • **Attendance**: You can view the total number of daily attendance results generated within the selected time range and the number for each specific attendance result. You can also export the result diagrams in PDF, PNG, and JPG format to your local PC.

No.	Description
	• **Video Intercom**: You can view the overall housing related statistics, the call history, and the temporary passes. You can also hover over a temporary pass to view and download the corresponding QR code. Click **Quick Configure** below the service overview to complete the service-related configurations in order without manually jumping from module to module. • **On-Board Monitoring**: You can view the current day's driving statistics, including the driving distance, driving duration, speeding times, and the number of driving events, as well as the recently located vehicles.
4	• **Quick Access**: The area that provides quick accesses to pages you have favorited by clicking ☆ on the menu of each module. You can hover over an item and drag it to adjust the display order, or click 🗑 to delete it from Quick Access. **Note** Upon first-time login, key modules corresponding to the services you are using will be provided in this field by default. • **Recently Viewed**: The area that displays your 10 most recently visited pages to provide you quick accesses to them.
5	The area that displays real-time messages received by the System in real time, including alarms, person access events, person access events, and service messages (e.g., service expiry reminder, and devices to be accepted). You can click a message to view its details and perform the corresponding operations, such as accepting the handed over devices.
6	The area from which you can view the overall health monitoring status of devices and resources added to the System. You can click **Refresh** to update the statistics displayed in this field, click **Go to Health Monitoring** to go to the Overview page of Device and Maintenance, or click a specific number to go to the health monitoring page of the corresponding device/ resource.
7	The area from which you can view/download support documents such as the user manual and the device compatibility list.

No.	Description
	You can also click **After-Sales Authorization Code** to create an authorization code that can be given to the maintenance personnel or your service provider for them to maintain your system.
8	The hover bar which provides access to the Help Center and an online service chatbot that provides Q&A services from any page. You can find instructions for how to use each service and support documents such as How-To guides and user manual in the Help Center.

Chapter 3 Account Management

For the super user, they can register an account by themselves or get their account information from invitation emails (invitations to join HCT) sent by their service provider; for normal users, they can get their account information from invitation emails or directly from the super user or other normal users who have the permission to create users. With the account information, the super user and normal users can log into the System for further configurations or operations.

3.1 About Licenses

Hik Connect for Teams provides both free features and subscription features, and the subscription features are controlled by various types of licenses, including those for using the video management, on-board monitoring, access control, video intercom, and analysis report services. You can purchase licenses from your service provider according to your needs.

Note

- If the licenses you have purchased are about to expire, please contact your service provider to renew them in time to ensure the proper use of the service features.
- If any of your licenses has expired and the number of resources allowed to be added exceeds the limit, your system will enter a "service limit exceeded" status and all service-related features will be unavailable. To continue using Hik Connect for Teams, you need to either contact your service provider to purchase more licenses, or you can go to Resource Management to delete some resources.

Table 3-1 License Description

License	Description
Video Management	• Controls the availability of features related to the video management service, such as live view, playback, video search, and other video related settings. Without the license, your use of service may be limited. • Determines the maximum number of video channels that can be added to areas. Without the license, you can only add a fixed number of video channels covered by the free plan. • Determines whether cloud storage can be enabled for channels and the maximum number of channels for which cloud storage can be enabled.

License	Description
	Note The cloud storage feature is only available in some countries/ regions. Please contact Hikvision for details.
On-Board Monitoring	• Controls the availability of features related to the on-board monitoring service, such as driving monitoring, vehicle locating, vehicle track search, driving event search, driving rule configuration, and other on-board monitoring related settings. Without the license, your use of service may be limited. • Determines the maximum number of vehicles that can be added to areas. Without the license, you can only add a fixed number of vehicles covered by the free plan.
Access Control & Attendance	• Access control devices control the availability of features related to the access control service, such as access level management, person management, access record search, remote door controls, door opening via mobile credentials, and other access control related settings. Without the license, your use of service may be limited. Determines the maximum number of doors that can be added to areas and the maximum number of persons that can be added to the system. Without the license, you can only add a fixed number of doors and persons covered by the free plan. • The attendance service provides company managers with attendance data of employees, including check-in time, check-out time, overtime, and leave, to help them improve management efficiency and make strategies based on the data.
Video Intercom	• Controls the availability of features related to the video intercom service, such as housing management, call answering and management, and temporary pass management. Without the license, the features will be unavailable. • Determines the maximum number of rooms that can be added to areas. Without the license, you can only add a fixed number of doors covered by the free plan.
Analysis Report	Controls the availability of features related to the analysis report service, such as monitoring the health status and data reporting status of the cameras with people counting / heat analysis capability, configuring the source of people counting data and

License	Description
	the global heat map, and checking reports of the regular days and reports for showing the effects of promotions. Without the license, the features will be unavailable.

3.2 Get Your Account Information

You can self-register a super user account or get your account information via an invitation email sent by your service provider when they hands over the HCT system to you. Normal users of your system can get their account information via invitation emails sent by you or other users with the permission to create normal user accounts, or you can create accounts for them by specifying the account name and password.

Refer to the following sections for the self-registration process, the overall system handover process, and sample invitation emails.

- ***Self-Register a Super User Account***
- ***Get Super User Account Information via Invitation Email***
- ***Create Normal User Accounts***

Self-Register a Super User Account

You can create your own HCT system by self-registering a super user account. A self-registered account can enjoy using HCT with free service plans for the video management service, access control service, and video intercom service. If you want to purchase/activate more service plans or use the analysis report service, invite a service provider to manage your system (for details, refer to ***Invite a Service Provider to Manage System***). The steps for registering a super user account on the Portal are as follows:

1. Visit ***https://www.hik-connect.com/*** to enter the overview page of Hik Connect for Teams, and click **Register Now** on the top right.
2. Enter **User Name**, **Password**, **Confirm Password**, **Country/Region**, **Email**, and CAPTCHA code, and check Terms of Service and Privacy Policy.

   Note

   We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
3. Click **Next** and a security code will be send to the email.
4. Enter the security code, click **OK**, and your account will be successfully registered.
5. Log in to the account, and tap **Me → Create Team** to create a team.
6. Set the required information such as team name, time zone, and scene type.

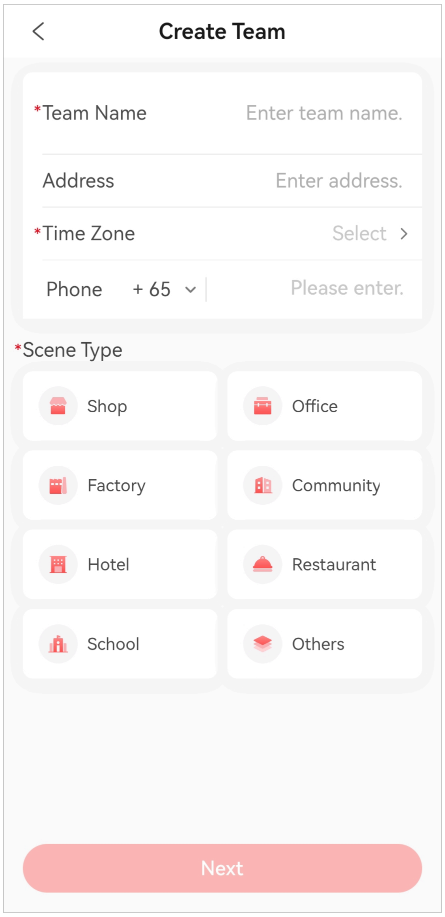


Figure 3-1 Create Team

7. Tap **Next** to enter the Activate Service page. Activate the desired services if needed.
8. Tap **Create Team** to finish the operation, and enter the home page of your team.

Get Super User Account Information via Invitation Email

If your service provider creates an HCT system for you on Hik-Partner Pro, an email will be sent to you when the system is being handed over. You can register an HCT account and log in to HCT. The diagram below shows the overall handover process of your system.

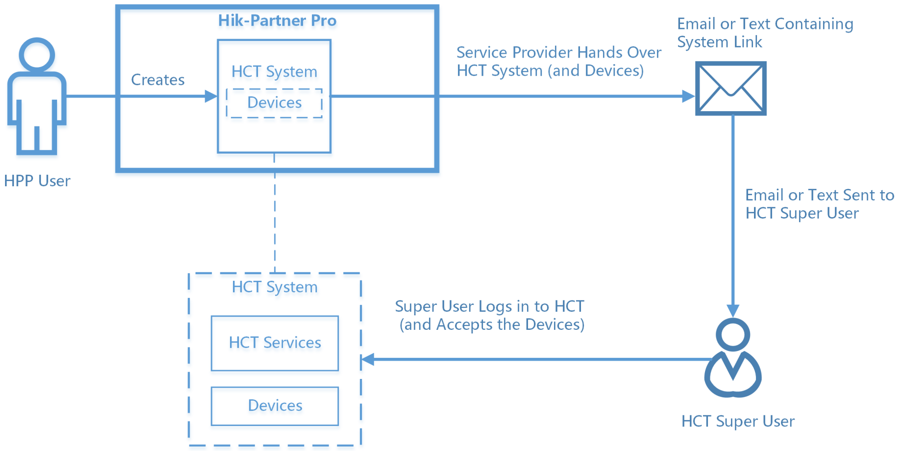

Hik-Partner Pro
HPP User
Creates
HCT System
Devices
Service Provider Hands Over HCT System (and Devices)
Email or Text Containing System Link
Email or Text Sent to HCT Super User
HCT System
HCT Services
Devices
Super User Logs in to HCT (and Accepts the Devices)
HCT Super User

Figure 3-2 How a System Is Created and Handed Over

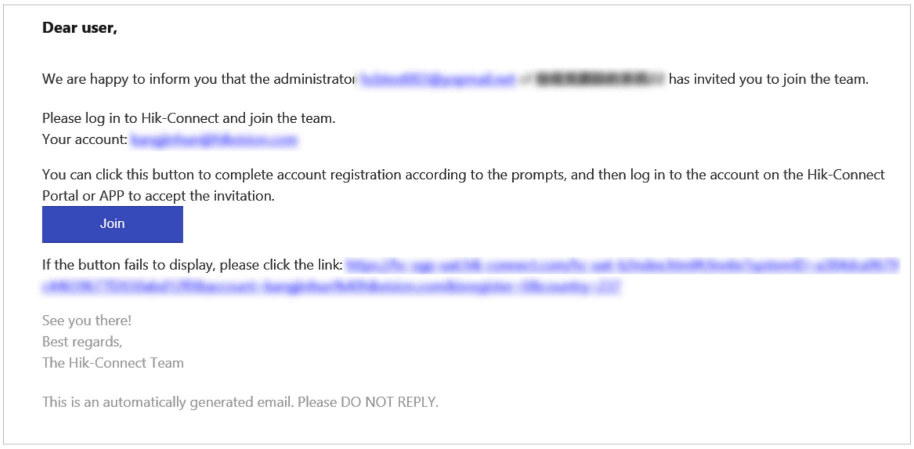
Note

If you need to switch to a new service provider due to a change of circumstances, invite a new service provider to manage your system. For details, refer to ***Invite a Service Provider to Manage System*** .

Create Normal User Accounts

After logging into the System, you can create normal user accounts with email address or phone number (see ***Add a Normal User*** for details). If an account is created with an email address, an invitation email that contains the necessary information for the normal user to log in to the System will be sent to the specified email address or phone number.

The figure below shows a sample invitation email sent to a normal user.



Dear user,

We are happy to inform you that the administrator [redacted] of [redacted] has invited you to join the team.

Please log in to Hik-Connect and join the team.
Your account: [redacted]

You can click this button to complete account registration according to the prompts, and then log in to the account on the Hik-Connect Portal or APP to accept the invitation.

Join

If the button fails to display, please click the link: [redacted]

See you there!
Best regards,
The Hik-Connect Team

This is an automatically generated email. Please DO NOT REPLY.

Figure 3-3 Sample Invitation Email for Normal Users

3.3 Login

Before you can manage resources and perform other operations such as playback and controlling doors (if you have the corresponding permissions), you need to log in to the System by an account.

Before You Start

Make sure you have gotten your account information. For details, refer to ***Get Your Account Information*** .

Steps

1. Visit ***https://www.hik-connect.com/*** to enter the overview page of Hik Connect for Teams.
2. Optional: Select a display language from the drop-down list in the upper-right corner.
3. On the top right, click **Log In**.
4. Select email account or phone number as the account type, and enter the account name.
5. Optional: Reset the password if you have forgotten the password.
   1) Click **Forgot Password** to open the Forgot Password window.
   2) Enter your account and CAPTCHA code, and then click **Next**.

      A security code will be sent to your email.
   3) Enter the security code you receive.
   4) Create a new password, and then confirm it.

      Note

      We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   5) Click **OK**.
6. Click **Login**.
- If you have gotten your account information from an invitation email and you are logging in to the System for the first time, the Change Password page will appear. In this case, you need to create a new password, agree to the service terms and privacy policy, and then click **Login** to log into the Portal.

  Note

  We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
- If you are logging in to the System as the super user for the first time, click **Agree** on the Welcome page to grant the required permissions shown on the page to your service provider before you can enter the Home page of the Portal.

Note

If you refuse to grant the permissions, you will be redirected back to the login page.

3.4 Log In via an Azure Account

After finishing required configuration on the Azure platform and HCT, you can log into HCT with Azure account.

Before You Start

- Finish the configuration on the Azure platform including HCT server address, and redirecting address.
- Finish the configuration on HCT. The configuration includes enabling Azure AD login, setting user permission, and enabling account sync.

Steps

Note

The feature is only available in certain countries or regions.

1. Visit ***https://www.hik-connect.com/*** to enter the overview page of Hik Connect for Teams.
2. **Optional:** Select a display language from the drop-down list in the upper-right corner.
3. On the top right, click **Log In**.
4. Click **Log in with Azure**.
5. Enter the email enterprise email, click **Next**, and click **Agree** to agree to the terms and policies.

   For the first time login, the login page of the Microsoft will be displayed.
6. **Optional:** On the login page of the Microsoft, enter your domain account and password, and log in to the account.

   Note

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

   The home page will be displayed after you successfully log in to the system.

Chapter 4 Application Summary

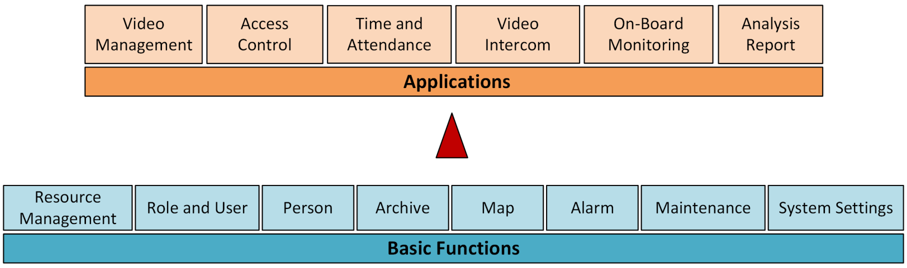


Figure 4-1 Functions and Applications in Hik Connect for Teams

Table 4-1 Applications in Hik Connect for Teams

Application	Description
Video Management	Refer to ***Video Management*** for details.
Access Control	Refer to ***Flow Chart of Door Access Control*** and ***Access Control Management*** for details.
Time and Attendance	Refer to ***Flow Chart of Time & Attendance*** and ***Time & Attendance*** for details.
Video Intercom	Refer to ***Flow Chart of Video Intercom Management*** and ***Video Intercom Management*** for details.
On-Board Monitoring	Refer to ***Flow Chart of On-Board Monitoring*** and ***On-Board Monitoring*** for details.
Analysis Report	Refer to ***Analysis Report*** for details.

Table 4-2 Basic Functions in Hik Connect for Teams

Basic Function	Description
Resource Management	Refer to ***Resource Management*** for details.
Role and User	Refer to ***Role and User Management*** for details.
Person	Refer to ***Person Management*** for details.
Archive	Refer to ***Archive Management*** for details.
Map	Refer to ***Map Management*** for details.
Alarm	Refer to ***Alarm Management*** for details.
Maintenance	Refer to ***Maintenance*** for details.
System Settings	Refer to ***Team Configuration*** for details.

4.1 Flow Chart of Door Access Control

The following flow chart shows the process of the configurations and operations of door access control.

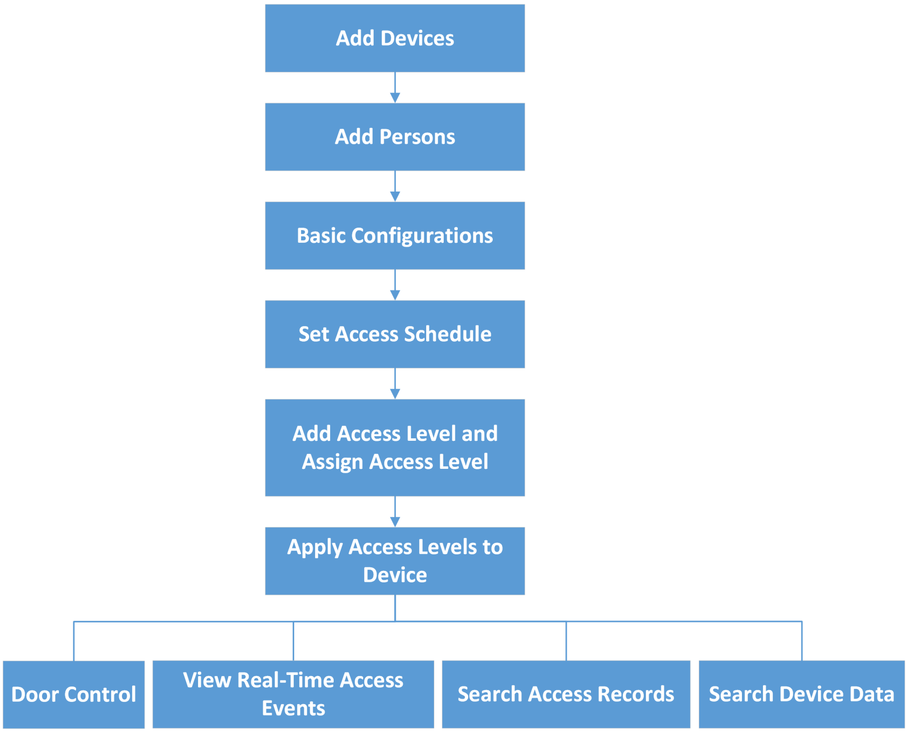


Figure 4-2 Flow Chart of Door Access Control

- **Add Device**: You need to add access control devices to the system first. For details, refer to ***Manage Access Control Devices in Area*** .
- **Add Persons**: Add person information and set person's credentials (such as PIN, card, and fingerprint). For details, refer to ***Person Management*** .
- **Set Access Schedule**: The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** .
- **Add Access Level**: An access level is a group of doors. After assigning access level, the assigned objects can get access to these doors during the authorized time period. For details, refer to ***Add Access Level*** .
- **Assign Access Level**: You need to assign access levels to persons, so that the assignees can access 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 a department. For details, refer to ***Assign Access Level*** .
- **Apply Access Levels to Device**: After setting the linkage between the persons and the access level, the access levels will be applied to devices automatically. But you can also manually apply the person's access level settings to the access control devices of the doors linked to the access level to take effect after changing access level settings. After that, the persons can access these

doors during the authorized time period defined by the related access level. For details, refer to ***Manually Apply Access Level Settings to Device*** .

- **Door Control**: After the above configurations on the Portal, you can control the doors status during live view, view real-time access events, search for history access records, etc. See ***Real-Time Monitoring*** and ***Record Search*** for details.

4.2 Flow Chart of Video Intercom Management

The following flow chart shows the process of configuring and managing video intercom.

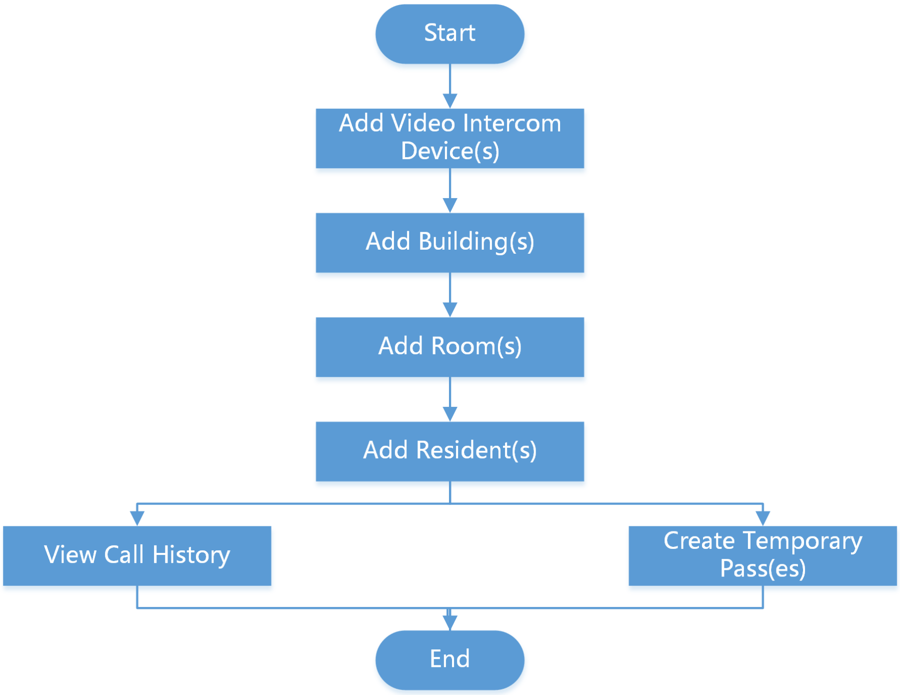


Figure 4-3 Flow Chart of Video Intercom Management

Add Video Intercom Device(s)	Add video intercom devices to areas to support video intercom management. See details in ***Manage Video Intercom Devices in Area*** .
Add Building(s), Room(s), and Resident(s)	Add buildings, rooms, and residents. Link video intercom devices (door stations) to buildings for security purposes when adding residents, and add residents to rooms in the buildings to allow them to access the corresponding buildings and receive video calls. See details in ***Add Building*** , ***Add Room*** , and ***Add Resident*** .

View Call History	View and export the call history. See details in ***View Call History*** .
Create Temporary Pass(es)	Create temporary passes which contain corresponding passwords and QR codes for persons with temporary access needs (e.g., delivery person) to unlock doors according to the set access levels. See details in ***Create Temporary Pass*** .

4.3 Flow Chart of Time & Attendance

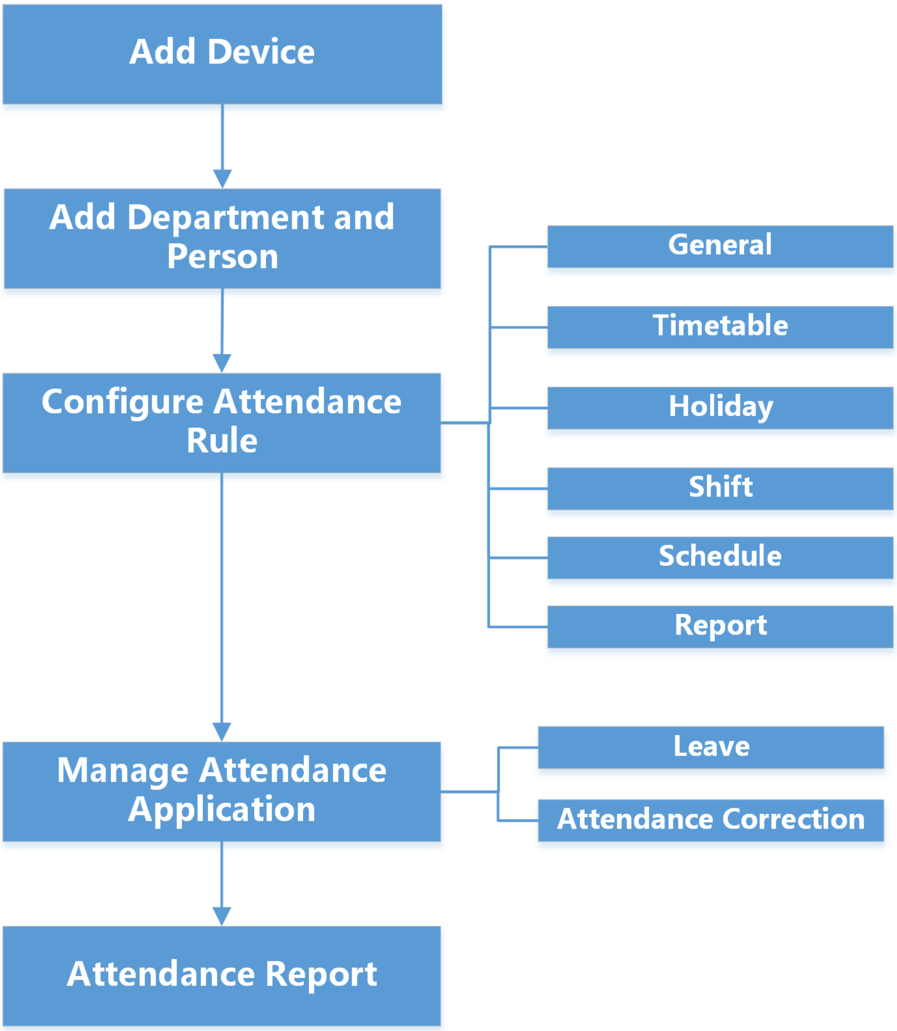


Figure 4-4 Flow Chart of Time & Attendance

- **Add Device**: Add access control devices to the System. For more details, refer to ***Manage Access Control Devices in Area*** .
- **Add Department and Person**: Add departments and persons to the System. For more details, refer to ***Person Management*** .
- **Configure Attendance Rule**: Select the shift type, define the weekend, configure overtime and regular attendance rules, add holidays and leave types, configure the report settings, add timetables, and assign schedules to persons. For more details, refer to ***Basic Configuration*** and ***Schedule Management*** .
- **Manage Attendance Application**: Apply for leave and the correction of attendance results for employees and review applications submitted by employees. For more details, refer to ***Application Management*** .
- **Attendance Report**: Export attendance reports to the local PC. For more details, refer to ***View and Export Reports*** .

4.4 Flow Chart of On-Board Monitoring

The following flow chart shows the process of configuring and managing on-board monitoring.

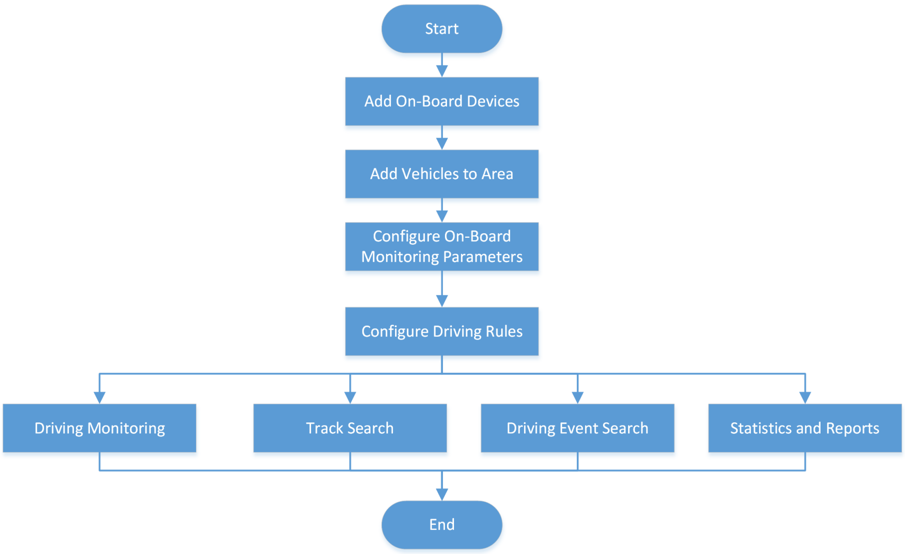


Figure 4-5 Flow Chart of On-Board Monitoring

Add On-Board Devices	See details in ***Manage On-Board Device in Area*** .
Add Vehicles to Area	See details in ***Manage Vehicles in Area*** .
Configure On-Board Monitoring Parameters	See details in ***Configurations Before On-Board Monitoring*** .

Configure Driving Rules	See details in ***Add a Driving Rule for Region*** , ***Add a Driving Rule for Route*** , and ***Configure a Rule Schedule Template*** .
Applications	See details in ***Driving Monitoring*** , ***Search for Tracks*** , ***Search for Driving Events*** , and ***Statistics and Reports*** .

Chapter 5 Resource Management

Hik Connect for Teams supports multiple device types, including encoding device, access control device, video intercom device, Hik-ProConnect box, on-board device, etc. You can add devices to areas for management. After adding devices, you can view/edit/delete/search for devices in areas, configure the required parameters, move devices to a new area and so on.

5.1 Manage Area

Hik Connect for Teams provides areas to manage the added resources in groups. You can add different areas to group different resources as needed. After adding an area, you can edit/search/delete it and link it with a map.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. **Optional:** Select a parent area from the area list to add a sub area.
3. Click + to open the Add Area panel.

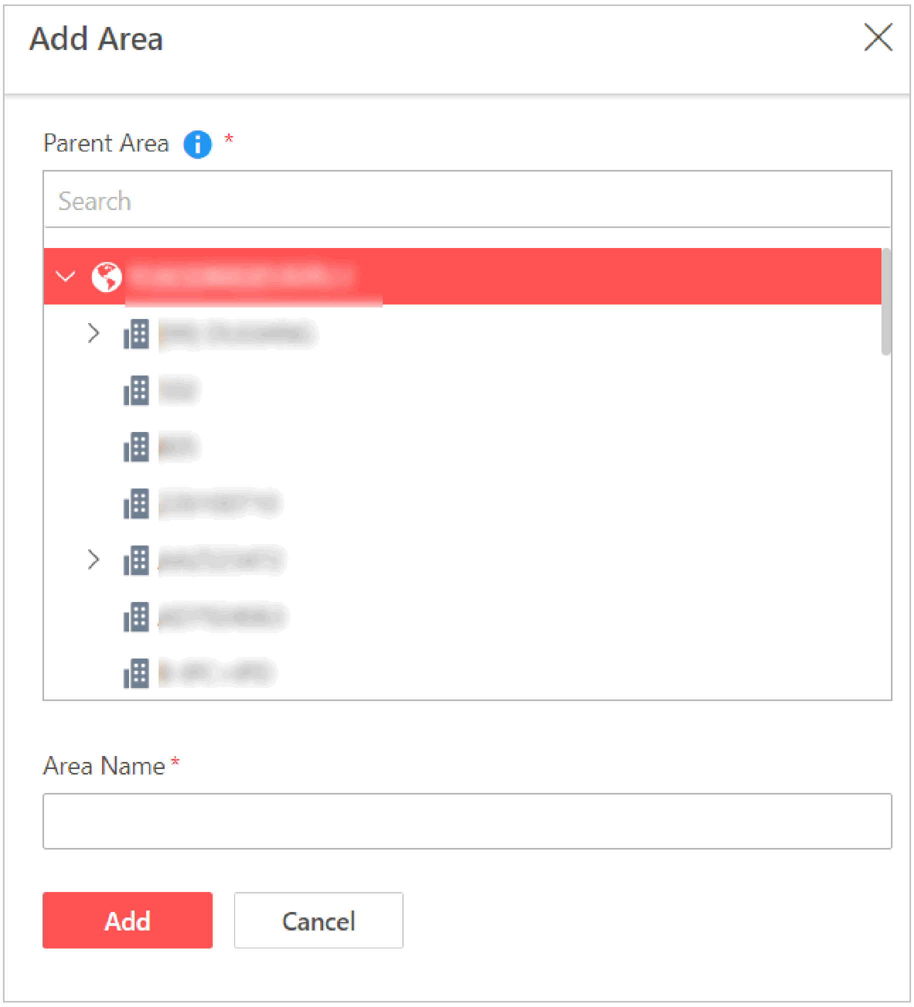


Figure 5-1 Add Area

4. Select a parent area to add a sub area.

5. Create a name for the area.

6. Click **Add**.

7. Optional: Perform the following operations.

Edit Area Select an area, and click ✎ to edit it.

Delete Area

- Select an area, and click 🗑 to delete it.
- Press **Ctrl** on your keyboard, select multiple areas, and then click 🗑 to batch delete the selected areas.

Note

The root area can not be deleted. If the area is deleted, all the resources in the area will be removed.

Link Area with Map Select an area, and click 🗺 to link the area with map(s). For details, refer to ***Add Static Map for Area*** .

Search Area Enter keyword(s) in the search box to search for the target area(s).

5.2 Manage Encoding Device in Area

You can add encoding devices to areas via three methods: adding detected online encoding devices, adding encoding devices by device serial No. and verification code, and batch importing encoding devices by a template. After devices are added, you can manage the added devices such as configuring devices remotely and setting the time zone for them.

5.2.1 Add Detected Online Encoding Devices

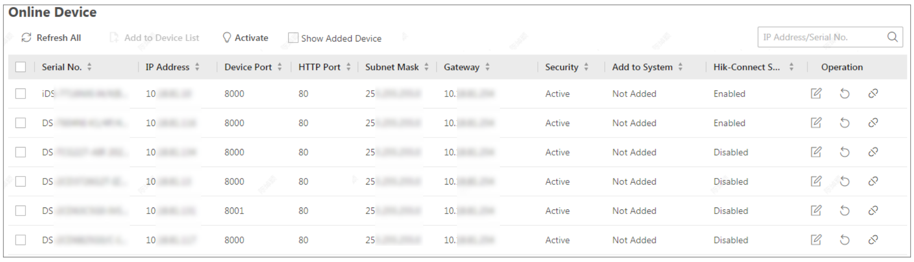
The encoding devices connected to the same network with the Portal can be detected, and the device information (e.g., IP address) will be recognized by the Portal. Based on the information, you can add the devices quickly.

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- Make sure the devices to be added are on the same LAN with the PC running the Portal.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Click **Device → Encoding Device** on the top.
3. In the Online Device area, check the device(s) to be added.



Online Device

☐	Serial No.	IP Address	Device Port	HTTP Port	Subnet Mask	Gateway	Security	Add to System	Hik-Connect S...	Operation
☐	iDS[redacted]	10[redacted]	8000	80	25[redacted]	10.[redacted]	Active	Not Added	Enabled	
☐	DS[redacted]	10[redacted]	8000	80	25[redacted]	10.[redacted]	Active	Not Added	Enabled	
☐	DS[redacted]	10[redacted]	8000	80	25[redacted]	10.[redacted]	Active	Not Added	Disabled	
☐	DS[redacted]	10[redacted]	8000	80	25[redacted]	10.[redacted]	Active	Not Added	Disabled	
☐	DS[redacted]	10[redacted]	8001	80	25[redacted]	10.[redacted]	Active	Not Added	Disabled	
☐	DS[redacted]	10[redacted]	8000	80	25[redacted]	10.[redacted]	Active	Not Added	Disabled	

Figure 5-2 Online Device List

4. Click **Add to Device List** to enter the Add Online Device page.
5. **Optional:** If there are inactive device(s) to be added, enter the password to activate them, and click **Next**.

Note

When you click **Next**, a prompt will pop up if activation failed. You can click **Enter Again** to activate the devices that failed to be activated. Devices failed to be activated cannot be added to the System.

6. Enter the device password, and click **Next**.

- If the devices to be added share the same password, enter their common password.
- If the devices to be added have different passwords, turn off **Enter a Common Password** switch, and enter the password respectively for each device.

Note

- After entering device admin passwords, the System will automatically start connecting the devices to the Hik-Connect service. Devices that failed to be connected to the Hik-Connect service cannot be added.
- When you click **Next**, a prompt will pop up if there is/are incorrect password(s). You can click **Enter Again** to correct the password. Devices with incorrect passwords cannot be added.

7. **Optional:** Enter the device verification code, and click **Next**.
   - If the devices to be added share the same verification code, enter their common verification code.
   - If the devices to be added have different verification codes, enter the verification code respectively for each device.

Note

When you click **Next**, a prompt will pop up if there is/are incorrect verification code(s). You can click **Enter Again** to correct the verification code. Devices with incorrect verification codes cannot be added.

8. Click **Next** after the System finishes testing the device compatibility automatically.
9. Configure device parameters, and click **Add**.

Basic Information

Verify Stream Encryption Key

If the switch is on, you should enter the stream encryption key on the device. Then during the live view and playback of the camera, the client will verify the key for security purposes.

Note

This function should be supported by the device. Refer to user manual of the device.

Time Zone

Select a time zone from the drop-down list for the device.

Note

You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System's, the System will apply the time zone settings to the device.

Area Information

Select an area in the list to add the device to.

Resource Information

Add the resource(s) of the device to an area.

Note

- You can import all the resources or the specified camera to the corresponding area. The device and the resource(s) of the device should be added to the same area.
- If you do not import resource(s) to the area, you cannot perform operations such as live view and playback.

Note

- You can view the adding process and the result. For devices failed to be added, you can view the failure reasons.
- If the failure reason is a low firmware version, you can upgrade the device if needed. If the failure reason is that the device has been added, you can click 🔗 to unbind the device. For details about unbinding a device from its current account, refer to ***Unbind a Device from Its Current Account*** .

The added device(s) will be displayed in the device list. You can click ⚙ on the top right corner to customize contents which will be displayed as column titles in the device list.

10. Optional: Perform the following operation(s) for the added devices.

Edit Device

Click the device name to view and edit the device basic information, time zone related information, etc.

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.

Upgrade 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.

Move the mouse cursor to the icon ⓘ beside the device name, and click **Upgrade** to upgrade the device.

Refresh Device

Click ⟳ on the Operation column to refresh the status of a device.

Click ⟳ **Refresh All** to refresh status of all the devices in the list.

Search for Device

Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

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).

5.2.2 Add Encoding Device by Device Serial No. and Verification Code

You can manually add encoding device(s) to the System by entering the device serial number and device verification code.

Before You Start

- 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 serial No. can be found on the device label or the device web configuration page, and the verification code is the stream encryption key you set on the device configuration page when enabling the Hik-Connect service.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. **Optional:** Select an area in the area list.
3. Click **Device → Encoding Device** on the top.
4. Click + Add⌄ → **Add Device** to enter the Add Device page.

Note

You can also click + Add⌄ → **Import via Excel** to batch add devices via the given template with device information.

5. Set the basic information for the device, including serial No., verification code, etc.

Device Serial No.

The serial No. of the device.

Device Verification Code

The stream encryption key you set on the device configuration page.

Device Name

Create a descriptive name for the device.

(Optional) User Name

Enter the user name.

(Optional) Password

Enter the device password.

⚠ **Caution**

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

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

6. **Optional:** Select a time zone from the drop-down list for the device.

Note

You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System, the System will apply the time zone settings to the device.

7. Select an area to add the device to.

Note

- If you have not selected an area previously, you can click **Create Area by Device Name** to create a new area by the device name, or click **Existing Area** and select an existing area from the list. When selecting **Existing Area**, you can also click **Add New Area** to add a new area. For details, refer to ***Manage Area*** .
- If you have selected an area (except the root area) previously, you can click **Create Area by Device Name** to create a new area by the device name, or click **Current Area** to add the device to the selected area.

8. **Optional:** Add the resource(s) of the device to an area.

Note

- You can import all the resources or the specified camera to the corresponding area. The device and the resource(s) of the device should be added to the same area.
- If you do not import resource(s) to the area, you cannot perform operations such as live view and playback.

9. Add the device.

- Click **Add** to add the current device and go back to the device list page.
- Click **Add and Continue** to add the current device and continue to add other devices.

Note

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. You can click ☰ to customize contents which will be displayed as column titles in the device list.

10. Optional: Perform the following operation(s) for the added devices.

Edit Device

Click the device name to view and edit the device basic information, time zone related information, etc.

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.

Upgrade Device

Move the mouse cursor to the icon ❗ beside the device name, and click **Upgrade** to upgrade the device.

Refresh Device

Click ↻ on the Operation column to refresh the status of a device.

Click ↻ **Refresh All** to refresh status of all the devices in the list.

Search for Device

Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

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).

5.3 Manage Access Control Devices in Area

You can add access control devices to areas via three methods: adding detected online access control devices, adding access control devices by device serial No. and verification code, and batch importing access control devices by a template. After devices are added, you can manage the added devices such as configuring devices remotely and setting the time zone.

5.3.1 Add Detected Online Access Control Devices

The access control devices connected to the same network as the Portal can be detected and their information (e.g., serial No., IP address, and device port) can be recognized by the Portal. Based on the information, you can add access control devices quickly.

Before You Start
Make sure the device you are going to use is correctly installed and connected to the same network as the Portal.

Steps

1. Go to the page for adding access control devices.
   - On the top navigation bar, click **Device and Maintenance → Resource Management → Device → Access Control Device** .
   - In the service overview section on the Home page, click **Access Control →** Door .

2. In the Online Device area, check the active device(s) to be added.

3. Click **Add to Device List** to enter the Add Online Device page.

4. Optional: If there are inactive device(s) to be added, enter the password to activate device(s), and click **Next**.

Note

When you click **Next**, a prompt will pop up if activation failed. You can click **Enter Again** to activate the devices that are failed to be activated. Devices failed to be activated cannot be added to the System.

5. Enter the device password, and click **Next**.
   - If the devices to be added share the same password, enter their common password.
   - If the devices to be added have different passwords, turn off **Enter a Common Password** switch, and enter the password respectively for each device.
6. **Optional:** Enter the device verification code, and click **Next**.
   - If the devices to be added share the same verification code, enter their common verification code.
   - If the devices to be added have different verification codes, enter the verification code respectively for each device.

Note

When you click **Next**, a prompt will pop up if there is/are incorrect verification codes. You can click **Enter Again** to correct the verification code. Devices with incorrect verification codes cannot be added to the System.

7. Click **Next** after the System finishes testing the device compatibility automatically.

   The device and its linked door resources will be added to the area. The devices added will be displayed in the device list. You can click ☰ to customize contents to be displayed in the device list.
8. Configure device parameters, and click **Next**.

   Time Zone

   Select a time zone from the drop-down list for the device.

   Note

   You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System's, the System will apply the time zone settings to the device.

   Area Information

   Select an area to add the device(s) to the area.
9. **Optional:** Perform the following operation(s) for the added devices.

   Edit Device

   Click the device name to view and edit the device basic information, time zone, etc.

   Upgrade Device

   Move the mouse cursor to the icon ❗ beside the device name, and click **Upgrade** to upgrade the device.

   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.

Refresh Device

Click ⟳ in the Operation column to refresh the status of a device.

Click ⟳ **Refresh All** above the device list to refresh status of all the devices in the list.

Search Device

Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

Delete Device

Select the added device(s) and click 🗑 **Delete** to delete the selected device(s).

Change Verification Code

Select the added device(s), click 🔑 **Change Verification Code**, and enter the device verification code.

Set Time Zone

Select the added device(s) and click 🕓 **Time Zone** to set the time zone for the device(s).

Set Device Parameters

Select the added device(s) and click ⚙ **Set Device Parameters** above the device list to set device parameters. For details, refer to ***Configure Access Control Device Parameters*** .

Move to Other Area

Select the added device(s), click ↗ **Move to Other Area**, select an area, and click **Move** to move the device(s) to the selected area.

5.3.2 Add Access Control Device by Device Serial No. and Verification Code

You can manually add access control device(s) to the System by entering the device serial number and device verification code.

Before You Start

- Make sure the device you are going to use is correctly installed and connected to the network as specified by the manufacturer.
- Make sure you have got the device serial No. and verification code. In general, the serial No. can be found on the device label or the device local configuration page, and the verification code can be found on the device configuration page as well.

Steps

1. Go to the page for adding access control devices.

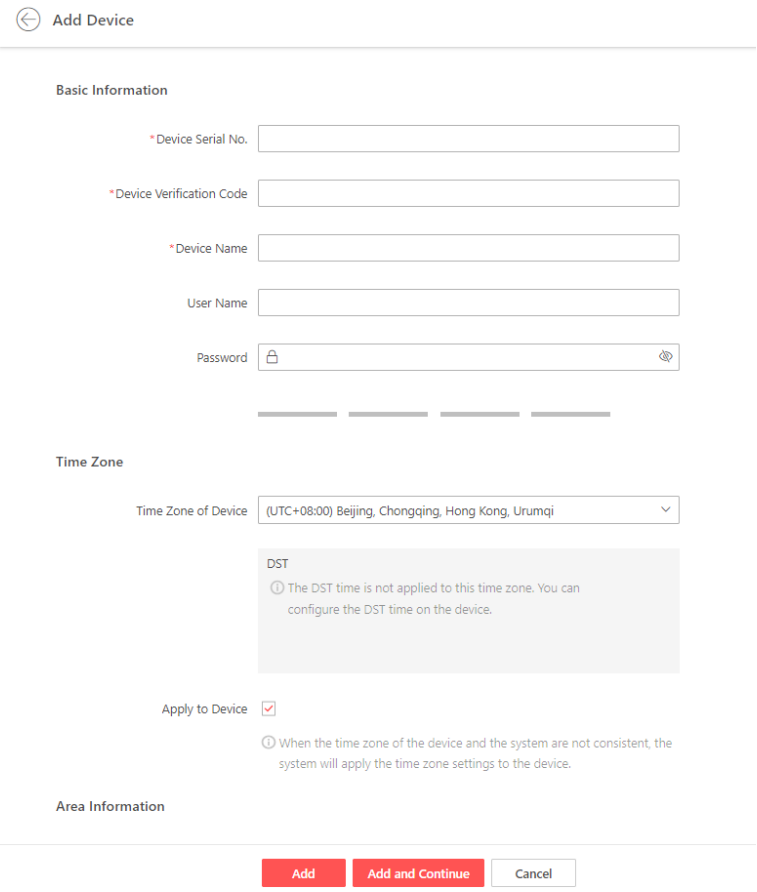
- On the top navigation bar, click **Device and Maintenance → Resource Management → Device → Access Control Device** .
- In the service overview section on the Home page, click **Access Control →** Door .

2. Optional: Select an area in the area list.

3. Click + Add → **Add Device** to enter the Add Device page.

Note

You can also click +∨ → **Import via Excel** to batch add devices via the given template with device information.



Add Device

Basic Information

*Device Serial No.

*Device Verification Code

*Device Name

User Name

Password

Time Zone

Time Zone of Device: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

DST

ⓘ The DST time is not applied to this time zone. You can configure the DST time on the device.

Apply to Device ☑

ⓘ When the time zone of the device and the system are not consistent, the system will apply the time zone settings to the device.

Area Information

Figure 5-3 Add Access Control Device

4. Set the basic information, including serial No., device verification code, device name, user name, and password.

Device Verification Code

The device verification code can be found on the device configuration page.

Password

Enter the device password.

Caution

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

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

5. **Optional:** Select a time zone from the drop-down list for the device.

Note

You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System's, the System will apply the time zone settings to the device.

6. Select an area to add the device to.

Note

- If an area is selected in the step 2, you can select **Create Area by Device Name** or **Current Area**.
- If no area is selected in the step 2 (the root area is selected by default), you can select **Create Area by Device Name** or **Existing Area**. If you select **Existing Area**, you can also click **Add New Area** to add a new area. For details, refer to ***Manage Area*** .

7. Click **Add** or **Add and Continue**.

The device and its linked door resources will be added to the area. The device will be displayed in the device list. You can click ⫶ on the top right corner to customize contents to be displayed in the device list.

8. **Optional:** Perform the following operation(s) for the added devices.

Edit Device

Click the device name to view and edit the device basic information, time zone, etc.

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.

Upgrade Device

Move the mouse cursor to the icon ❗ beside the device name, and click **Upgrade** to upgrade the device.

Refresh Device

Click ↻ in the Operation column to refresh the status of a device.

Click ↻ **Refresh All** above the device list to refresh status of all the devices in the list.

Search for Device

Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

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.

Delete Device

Select the added device(s) and click **Delete** to delete the selected device(s).

Set Time Zone

Select the added device(s) and click **Time Zone** to set the time zone for the device(s).

Set Device Parameters

Select the added device(s) and click **Set Device Parameters** above the device list to set device parameters. For details, refer to ***Configure Access Control Device Parameters*** .

Move to Other Area

Select the added device(s), click **Move to Other Area**, select an area, and click **Move** to move the device(s) to the selected area.

5.3.3 Configure Access Control Device Parameters

After adding access control devices, you can set the device parameters, including settings about privacy, skin-surface temperature, mask, and card swiping.

Note

Make sure the related features are supported by the devices.

Go to the video intercom device list by either of the following entrances.

- On the top navigation bar, click **Device and Maintenance → Resource Management → Device → Access Control Device** .
- In the service overview section on the Home page, click **Access Control →** Door .

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.

5.4 Manage Video Intercom Devices in Area

You can add video intercom devices to areas via three methods: adding detected online video intercom devices, adding video intercom devices by device serial No. and verification code, and batch importing video intercom devices by a template. After devices are added, you can configure the devices remotely, set the time zone, and configure other device parameters such as the public passwords.

5.4.1 Add Detected Online Video Intercom Devices

The video intercom devices connected to the same network with the Portal can be detected, and their information (e.g., IP address) can be recognized by the Portal. Based on the information, you can add the devices quickly.

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- Make sure the devices to be added are on the same LAN with the PC running the Portal.

Steps

1. Go to the page for adding video intercom devices.
   - On the top navigation bar, click **Device and Maintenance → Resource Management → Device → Video Intercom Device** .
   - In the service overview section on the Home page, click **Video Intercom → Device Management** .
2. In the Online Device area, check the active device(s) to be added.
3. Click **Add to Device List** to enter the Add Online Device page.
4. **Optional:** If there are inactive device(s) to be added, enter the password to activate device(s), and click **Next**.

Note

When you click **Next**, a prompt will pop up if activation failed. You can click **Enter Again** to activate the devices that are failed to be activated. Devices failed to be activated cannot be added to the System.

5. Enter the device password, and click **Next**.
   - If the devices to be added share the same password, enter their common password.
   - If the devices to be added have different passwords, turn off **Enter a Common Password** switch, and enter the password respectively for each device.
6. **Optional:** Enter the device verification code, and click **Next**.
   - If the devices to be added share the same verification code, enter their common verification code.
   - If the devices to be added have different verification codes, enter the verification code respectively for each device.

Note

When you click **Next**, a prompt will pop up if there is/are incorrect verification code(s). You can click **Enter Again** to correct the verification code(s). Devices with incorrect verification codes cannot be added to the System.

7. Click **Next** after the System finishes testing the device compatibility automatically.

Note

You will go back to the device list page. If connecting to the device failed, an icon ⓘ will appear on the right side of the device. Move the mouse cursor to the icon ⓘ , and click **Edit** to edit the device information or click **Refresh** to refresh the device status.

8. Configure device parameters, and click **Next**.

   Time Zone

Select a time zone from the drop-down list for the device.

> **Note**
>
> You can check **Apply to Device**, and then when the time zone of the device is inconsistent with that of the System's, the System will apply the time zone settings to the device.

Area Information

Select an area to add the device(s) to the area.

9. **Optional:** Perform the following operation(s) for the added devices.

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.

Set Time Zone

Select the added device(s) and click 🕓 to set the time zone for the device(s).

Refresh Device

Click ↻ in the Operation column to refresh the status of a device.

Click ↻ above the device list to refresh status of all the devices in the list.

Move to Other Area

Select the added device(s), click ⧉ , select an area, and click **Move** to move the device(s) to the selected area.

Edit Device

Click the device name to view and edit the device basic information, time zone, etc.

Search Device

Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

Delete Device

Select the added device(s) and click 🗑 to delete the selected device(s).

Change Verification Code

Select the added device(s), click 🔑 , and enter the device verification code.

Set Device Parameters

Select the added device(s) and click ⚙ above the device list to set/ disable the M1 card encryption for card swiping and set/disable the public password. For details, refer to ***Configure Video Intercom Device Parameters*** .

Set Displayed Items

Click ⫶ to set items which will be displayed on the device list.

5.4.2 Add Video Intercom Device by Device Serial No. and Verification Code

You can manually add video intercom device(s) to the System by entering the device serial number and device verification code.

Before You Start

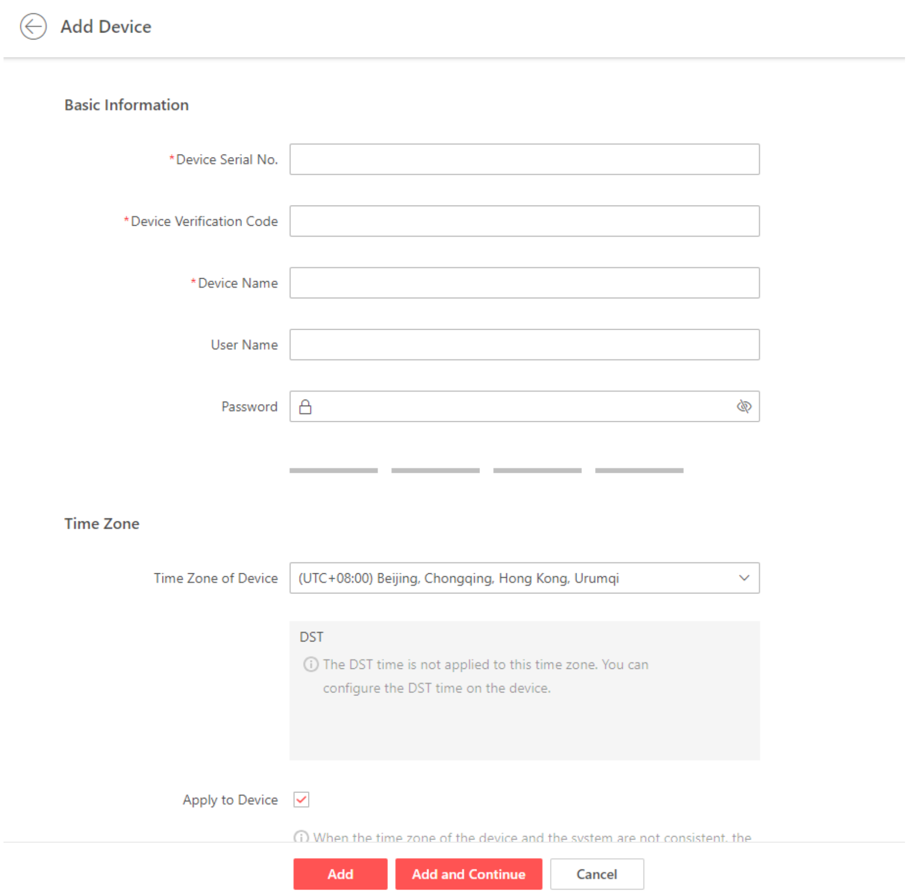
- Make sure the video intercom device you are going to use is correctly installed and connected to the network as specified by the manufacturer.
- Make sure you have got the device serial No. and verification code. In general, the serial No. can be found on the device web configuration page, and the verification code can be found on the device label.

Steps

1. Go to the page for adding video intercom devices.
   - On the top navigation bar, click **Device and Maintenance → Resource Management → Device → Video Intercom Device** .
   - In the service overview section on the Home page, click **Video Intercom → Device Management** .

2. Optional: Select an area in the area list.

3. Click + Add → **Add Device** to enter the Add Device page.



Add Device

Basic Information

*Device Serial No.

*Device Verification Code

*Device Name

User Name

Password

Time Zone

Time Zone of Device: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

DST

ⓘ The DST time is not applied to this time zone. You can configure the DST time on the device.

Apply to Device ☑

ⓘ When the time zone of the device and the system are not consistent, the

Figure 5-4 Add Video Intercom Device

4. Set the basic information for the device, including the device serial No., verification code, etc.

Device Serial No.

The serial No. of the device.

Note

You can get the serial No. on the device web configuration page.

Device Verification Code

The verification code of the device.

Note

You can get the verification code on the device label.

Device Name

Create a descriptive name for the device.

(Optional) User Name

Enter the user name.

(Optional) Password

Enter the device password.

Caution

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

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

5. **Optional:** Select a time zone from the drop-down list for the device.

Note

You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System's, the System will apply the time zone settings to the device.

6. Select an area to add the device to.

Note

- If an area is selected in the step 2, you can select **Create Area by Device Name** or **Current Area**.
- If no area is selected in the step 2 (the root area is selected by default), you can select **Create Area by Device Name** or **Existing Area**. If you select **Existing Area**, you can also click **Add New Area** to add a new area. For details, refer to ***Manage Area*** .

7. Click **Add** or **Add and Continue** to finish adding the device.

Note

You will go back to the device list page. If connecting to the device failed, an icon ❗ will appear on the right side of the device. Move the mouse cursor to the icon ❗ , and click **Edit** to edit the device information or click **Refresh** to refresh the device status.

8. **Optional:** Perform the following operation(s) for the added devices.

Edit Device

Click the device name to view and edit the device basic information, time zone, etc.

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.

Upgrade Device
Move the mouse cursor to the icon beside the device name, and click **Upgrade** to upgrade the device.

Refresh Device
Click in the Operation column to refresh the status of a device.

Click **Refresh All** above the device list to refresh status of all the devices in the list.

Search for Device
Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

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.

Set Time Zone
Select the added device(s) and click **Time Zone** to set the time zone for the device(s).

Move to Other Area
Select the added device(s), click **Move to Other Area**, select an area, and click **Move** to move the device(s) to the selected area.

Delete Device
Select the added device(s) and click **Delete** to delete the selected device(s).

Set Device Parameters
Select the added device(s) and click **Set Device Parameters** above the device list to set/disable the M1 card encryption for card swiping and set/disable the public password. For details, refer to ***Configure Video Intercom Device Parameters*** .

Set Displayed Items
Click to set items which will be displayed on the device list.

5.4.3 Configure Video Intercom Device Parameters

After adding video intercom devices, you can set the device parameters (e.g., card-swiping related parameters and public password).

Note

Make sure the related features are supported by the devices.

1. Go to the video intercom device list.
   - On the top navigation bar, click **Device and Maintenance → Resource Management → Device → Video Intercom Device** .
   - In the service overview section on the Home page, click **Video Intercom → Device Management** .
2. Select the added device(s) for configurations.
3. Click **Set Device Parameters**.

4. Set the parameters according to your needs.

   Card Swiping

   Enable the M1 card encryption for the device(s) and select the encrypted sector.

   For the device enabled with M1 card encryption, only the cards with the selected encrypted sector can be verified when you swipe the cards on the device's connected card reader.

   Public Password

   Enable and set the public password(s). Click **Add** to set more passwords.

   You can share the public passwords with residents and visitors for them to open the public door.

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

5.5 Manage Hik-ProConnect Box in Area

You can add Hik-ProConnect boxes to areas via three methods: adding detected online Hik-ProConnect boxes, adding Hik-ProConnect boxes by device serial No. and verification code, and importing Hik-ProConnect boxes using a template. After devices are added, you can manage the added Hik-ProConnect boxes such as configuring them remotely, performing network tests, and setting the time zone for them.

5.5.1 Add Detected Online Hik-ProConnect Boxes

The Hik-ProConnect boxes connected to the same network with the Portal can be detected, and the device information will be recognized by the Portal. Based on the information (e.g., IP address), you can add the Hik-ProConnect boxes quickly.

Before You Start

- Make sure the Hik-ProConnect boxes you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- Make sure the Hik-ProConnect boxes to be added are on the same LAN with the PC running the Portal.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Click **Device → Hik-ProConnect Box** on the top.
3. In the Online Device area, select the Hik-ProConnect box(es) to be added.
4. Click **Add to Device List** to enter the Add Online Device page.
5. **Optional:** If there are device(s) not activated, enter the password to activate them, and click **Next**.

ⓘ **Note**

When you click **Next**, a prompt will pop up if activation failed. You can click **Enter Again** to activate the device(s) that failed to be activated, otherwise the device(s) cannot be added to the System.

6. Enter the password of the device, and click **Next**.
   - If the devices to be added share the same password, enter their common password.
   - If the devices to be added have different passwords, turn off the **Enter a Common Password** switch, and enter the password respectively for each device.

ⓘ **Note**

- After entering the device passwords, the System will automatically start connecting the devices to the Hik-Connect service. Devices that failed to be connected to the Hik-Connect service cannot be added.
- When you click **Next**, a prompt will pop up if there is/are incorrect password(s). You can click **Enter Again** to correct the password(s). Devices with incorrect passwords cannot be added.

7. **Optional:** Enter the device verification code, and click **Next**.
   - If the devices to be added share the same verification code, enter their common verification code.
   - If the devices to be added have different verification codes, enter the verification code respectively for each device.

ⓘ **Note**

When you click **Next**, a prompt will pop up if there is/are incorrect verification code(s). You can click **Enter Again** to correct the verification code(s). Devices with incorrect verification codes cannot be added.

8. Click **Next** after the System finishes testing the device compatibility automatically.
9. Configure device parameters, and click **Add**.

Time Zone

Select a time zone from the drop-down list for the device.

ⓘ **Note**

You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System, the System will apply the time zone settings to the device.

Area Information

Select an area in the list to add the device to.

Note

- You can view the adding process and the result. For devices failed to be added, you can view the failure reasons.
- If the failure reason is a low firmware version, you can upgrade the device if needed. If the failure reason is that the device has been added, you can click 🔗 to unbind the device. For details about unbinding a device from its current account, refer to ***Unbind a Device from Its Current Account*** .

The added devices will be displayed in the device list. You can click ⚙ on the top right corner to customize contents which will be displayed as column titles in the device list.

10. Optional: Perform the following operation(s) for the added devices.

Edit Device
Click the device name to view and edit the device basic information, time zone related information, resource information, etc.

Remote Configurations
Click ⚙ in the Operation column to set the remote configurations of the corresponding device.

Note

For details about remote configurations, see the user manual of the device.

Upgrade 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.

Move the cursor to the icon ⓘ beside the device name, and click **Upgrade** to upgrade the device.

Refresh Device
Click ↻ in the Operation column to refresh the status of a device.

Click ↻ **Refresh All** to refresh status of all devices in the list.

Search for Device
Enter keyword(s) in the search box in the upper-right corner to search for the target device(s). You can search by device name, device serial No., and version No.

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.

Set Time Zone
Select the added device(s) and click 🕓 **Time Zone** to set the time zone for the device(s).

Perform Network Test
Click ◎ in the Operation column to start a network test for the corresponding device.

Delete Device
Select the added device(s) and click 🗑 **Delete** to delete the selected device(s).

5.5.2 Add Hik-ProConnect Box by Device Serial No. and Verification Code

You can manually add Hik-ProConnect box(es) to the System by entering the device serial No. and device verification code.

Before You Start

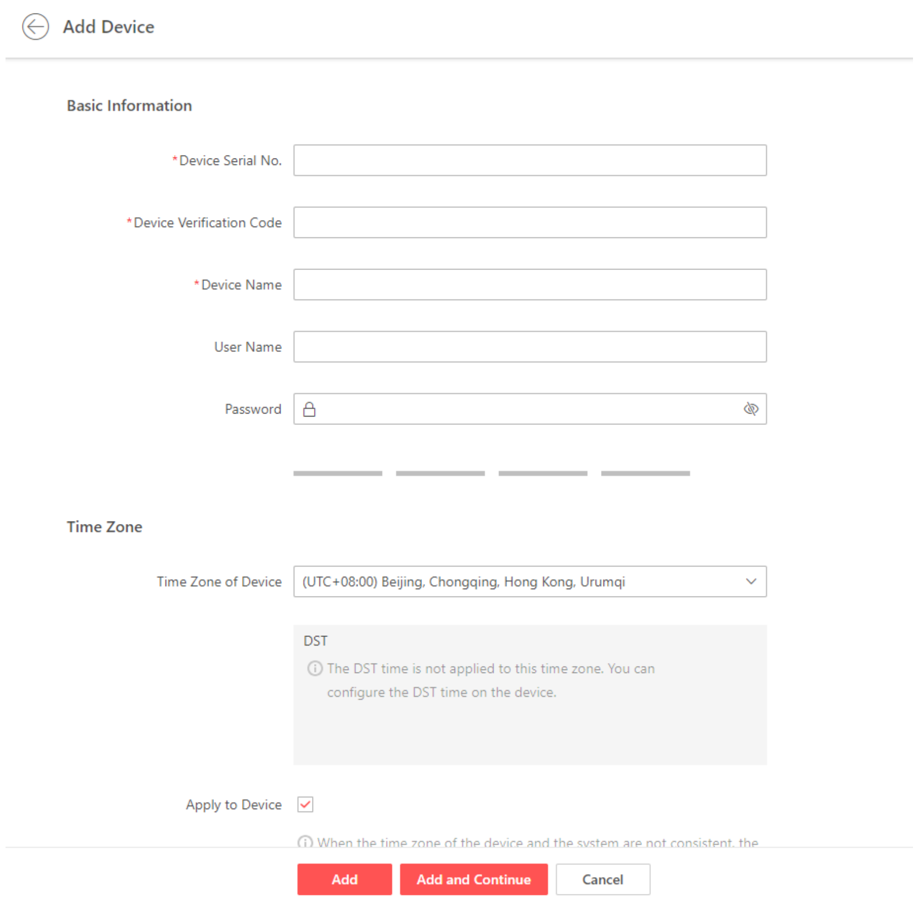
- Make sure the Hik-ProConnect box you are going to use is correctly installed and connected to the network as specified by the manufacturers.
- Make sure you have got the device serial No. and verification code. In general, the serial No. and the default verification code can be found on the device label. If no device verification code is found, use the verification code you set when enabling the Hik-Connect service.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. **Optional:** Select an area in the area list.
3. Click **Device → Hik-ProConnect Box** on the top.
4. Click + Add⌄ → **Add Device** to enter the Add Device page.

Note

You can also click + Add⌄ → **Import via Excel** to batch add devices via the given template with device information.



Add Device

Basic Information

*Device Serial No.

*Device Verification Code

*Device Name

User Name

Password

Time Zone

Time Zone of Device: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

DST

ⓘ The DST time is not applied to this time zone. You can configure the DST time on the device.

Apply to Device ☑

ⓘ When the time zone of the device and the system are not consistent, the

Figure 5-5 Add Hik-ProConnect Box

5. Enter the basic information of the device, including device serial No., device verification code, etc.

Note

The default device verification code is usually on the device label. If no device verification code is found, enter the verification code you created when enabling the Hik-Connect service.

Caution

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

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

6. Optional: Select a time zone from the drop-down list for the device.

Note

You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System, the System will apply the time zone settings to the device.

7. Select an area to add the device to.

Note

- If you have not selected an area previously, you can click **Create Area by Device Name** to create a new area by the device name, or click **Existing Area** and select an existing area from the list. When selecting **Existing Area**, you can also click **Add New Area** to add a new area. For details, refer to ***Manage Area*** .
- If you have selected an area (except the root area) previously, you can click **Create Area by Device Name** to create a new area by the device name, or click **Current Area** to add the device to the selected area.

8. Add the device.

- Click **Add** to add the current device and go back to the device list page.
- Click **Add and Continue** to add the current device and continue to add other devices.

Note

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.

You can click ☷ to customize contents which will be displayed as column titles in the device list.

9. Optional: Perform the following operation(s) for the added devices.

Edit Device

Click the device name to view and edit the device basic information, time zone related information, etc.

Remote Configurations

Click ⚙ in the Operation column to set the remote configurations of the corresponding device.

Note

For details about remote configurations, see the user manual of the device.

Upgrade Device

Move the cursor to the icon ⚠ beside the device name, and click **Upgrade** to upgrade the device.

Refresh Device

Click ↻ in the Operation column to refresh the status of a device.

Click ↻ **Refresh All** to refresh status of all devices in the list.

Search for Device

Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

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.

Set Time Zone
Select the added device(s) and click **Time Zone** to set the time zone for the device(s).

Perform Network Test
Click in the Operation column to start a network test for the corresponding device.

Delete Device
Select the added device(s) and click **Delete** to delete the selected device(s).

5.6 Manage On-Board Device in Area

You can add on-board devices to areas via two methods, namely, adding online on-board devices and importing on-board devices from your personal account. After adding devices, you can manage the added devices such as configuring devices remotely and setting the time zone for them.

5.6.1 Add Detected Online On-Board Devices

The on-board devices connected to the same network with the Portal can be detected, which makes the devices' information about themselves (e.g., IP address) recognized by the Portal. Based on the information, you can add the devices quickly.

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- Make sure the devices to be added are on the same LAN with the PC running the Portal.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Click **Device → On-Board Device** on the top.
3. In the Online Device area, check the active device(s) to be added.
4. Click **Add to Device List** to enter the Add Online Device page.
5. **Optional:** If there are inactive device(s) to be added, enter the password to activate device(s), and click **Next**.

   Note

   When you click **Next**, a prompt will pop up if activation failed. You can click **Enter Again** to activate the devices that are failed to be activated. Devices failed to be activated cannot be added to the System.

6. Enter the device password, and click **Next**.
   - If the devices to be added share the same password, enter their common password.

- If the devices to be added have different passwords, turn off **Enter a Common Password** switch, and enter the password respectively for each device.

Note

- After entering device admin passwords, the System will automatically start connecting the devices to the Hik-Connect service. Devices that are failed to be connected to the Hik-Connect service cannot be added.
- When you click **Next**, a prompt will pop up if there is/are incorrect passwords. You can click **Enter Again** to correct the password. Devices with incorrect passwords cannot be added.

7. **Optional:** Enter the device verification code, and click **Next**.
   - If the devices to be added share the same verification code, enter their common verification code.
   - If the devices to be added have different verification codes, enter the verification code respectively for each device.

Note

When you click **Next**, a prompt will pop up if there is/are incorrect verification codes. You can click **Enter Again** to correct the verification code. Devices with incorrect verification codes cannot be added to the System.

8. Click **Next** after the System finishes testing the device compatibility automatically.
9. Configure device parameters, and click **Add**.

Basic Information

Verify Stream Encryption Key

If the switch is enabled, you should enter the stream encryption key on the device. Then during the live view and playback of the camera, the client will verify the key for security purposes.

Note

This function should be supported by the device. Refer to user manual of the device.

Time Zone

Select a time zone from the drop-down list for the device.

Note

- You can click **View** to view the details of the selected time zone.
- You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System's, the System will apply the time zone settings to the device.

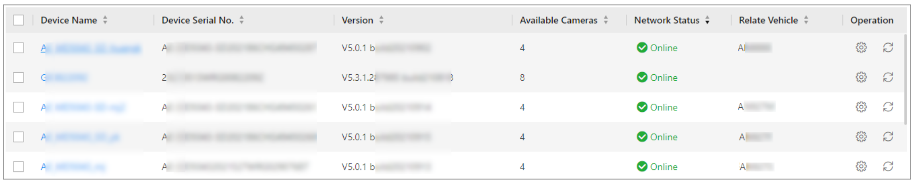
Area Information

Select an area in the list to add the device to.

Note

You can view the adding process and the result. You can click ⚙ to select the columns to be displayed in the device list.

The devices that are added will be displayed in the device list.



□	Device Name	Device Serial No.	Version	Available Cameras	Network Status	Relate Vehicle	Operation
□	A[redacted]	A[redacted]	V5.0.1 b[redacted]	4	✓ Online	A[redacted]	⚙ ↻
□	G[redacted]	2[redacted]	V5.3.1.2[redacted]	8	✓ Online		⚙ ↻
□	A[redacted]	A[redacted]	V5.0.1 b[redacted]	4	✓ Online	A[redacted]	⚙ ↻
□	A[redacted]	A[redacted]	V5.0.1 b[redacted]	4	✓ Online	A[redacted]	⚙ ↻
□	A[redacted]	A[redacted]	V5.0.1 b[redacted]	4	✓ Online	A[redacted]	⚙ ↻

Figure 5-6 Device List

10. **Optional:** Perform the following operation(s) for the added devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

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

Set Time Zone

Select the added device(s) and click **Time Zone** to set the time zone for the device(s).

Refresh Device

Click ↻ on the Operation column to refresh the status of a device.

Click **Refresh All** to refresh status of all the devices in the list.

Edit Device

Click the device name to view and edit the device basic information, time zone related information, etc.

Upgrade Device

Move the mouse cursor to the icon ⓘ beside the device name, and click **Upgrade** to upgrade the device.

Search Device

Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

Delete Device

Select the added device(s) and click **Delete** to delete the selected device(s).

Note

After deleting an on-board device, the vehicle(s) linked with the device will also be deleted from the System.

5.6.2 Add On-Board Device by Device Serial No. and Verification Code

You can manually add on-board device(s) to the System by entering the device serial number and device verification code.

Before You Start

- Make sure the on-board 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 serial No. can be found on the device label or the device web configuration page, and the verification code is the stream encryption key you set on the device configuration page when enabling the Hik-Connect service.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. **Optional:** Select an area in the area list.
3. Click **Device → On-Board Device** on the top.
4. Click + Add → **Add Device** to enter the Add Device page.

   Note

   You can also click + Add → **Import via Excel** to batch add devices via the given template with device information.

5. Set the basic information for the device, including serial No., verification code, etc.

   Device Serial No.

   The serial No. of the device.

   Device Verification Code

   The encryption key you set on the device configuration page.

   Device Name

   Create a descriptive name for the device.

   (Optional) User Name

   Enter the user name.

   (Optional) Password

   Enter the device password.

   Caution

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

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

6. **Optional:** Add the resource of the device (vehicle) to the area.
   - Select **New Vehicle**, and enter the license plate number of the vehicle.
   - Select **Existing Vehicles**, and select a vehicle from the area list.

Note

The device and the resource of the device should be added to the same area.

7. **Optional:** Select a time zone from the drop-down list for the device.

Note

You can check **Apply to Device**, then when the time zone of the device is inconsistent with that of the System's, the System will apply the time zone settings to the device.

8. Select an area to add the device to.

Note

- Skip this step if you have selected an area in the previous step.
- You can click **Add New Area** to add a new area. For details, refer to ***Manage Area*** .

9. Click **Add** to finish adding the device or click **Add and Continue** to save the settings and continue to add another device.

Note

On the device list page, if the device is offline, or the device's firmware version is too old, an icon ⓘ will appear on the right side of the device. You can click to select the columns to be displayed in the device list.

10. **Optional:** Perform the following operation(s) for the added devices.

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.
Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Refresh Device	Click ↻ on the Operation column to refresh the status of a device. Click ↻ **Refresh All** to refresh status of all the devices in the list.

Edit Device
Click the device name to view and edit the device basic information, time zone related information, etc.

Upgrade Device
Move the mouse cursor to the icon (!) beside the device name, and click **Upgrade** to upgrade the device.

Search for Device
Enter keyword(s) in the search box in the upper-right corner to search for the target device(s).

Delete Device
Select the added device(s) and click 🗑 **Delete** to delete the selected device(s).

> **Note**
>
> After deleting an on-board device, the vehicle(s) linked with the device will also be deleted from the System.

5.7 General Device Operations

There are some common operations for all types of devices before or after adding them to the System for management, such as unbinding a device from its current account, creating passwords to activate the inactive ones, editing the network information for online devices, resetting device password, and upgrading device firmware. Besides, you can import devices via a template, import devices from your personal account, export device information, and accept devices handed over by your service provider during the system handover.

5.7.1 Import Devices via Template

When there are multiple devices to be added, you can edit the predefined template containing the required device information, and import the template to the platform to batch add the devices.

Before You Start

- Make sure the devices you are going to use is correctly installed and connected to the network as specified by the manufacturers.
- Make sure the devices have been activated and connected to the Hik-Connect service.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Click **Device** on the top, and then select a device type.
3. Click **Import → Import via Excel** to pop up the Import window.
4. Click **Download Template** to download the template to the local PC.
5. Open the downloaded template file, and enter the required device information.
6. Click 📁 to select the edited template file.
7. Select the time zone from the drop-down list.

8. Click **Import** to import the devices to the platform.

Note

The devices added are displayed in the device list. You can click to select the columns to be displayed in the device list.

5.7.2 Import Personal Devices to Hik Connect for Teams

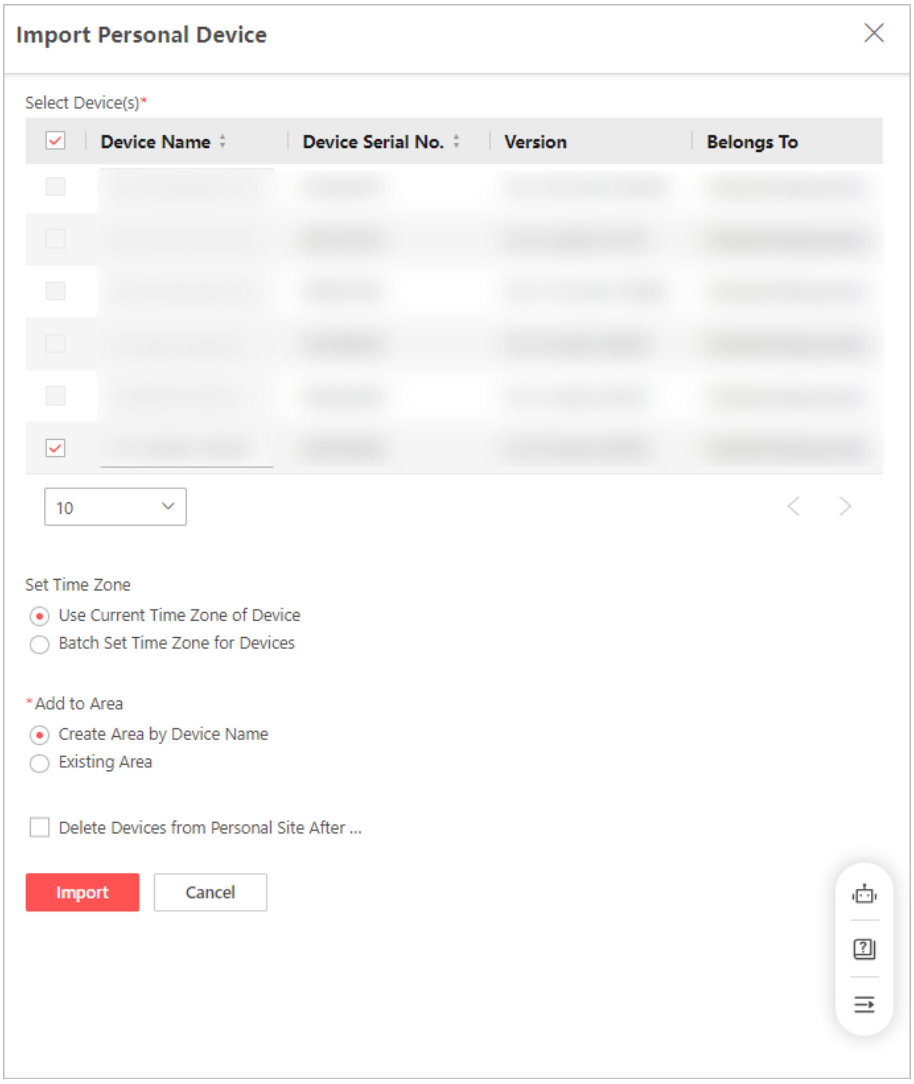
The Hik-Connect includes Hik-Connect Personal and Hik Connect for Teams. Installers or service providers like you may be managing devices centrally from a remote location through your own Hik-Connect account. With the device import feature, you can sync personal devices from your Hik-Connect account to Hik Connect for Teams for more efficient device management.

Steps

Note

For personal devices, you can 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 you devices, your shared devices, devices shared with you, and your account information.

1. On the top navigation bar, click **Device and Maintenance → Resource Management** .
2. Click **Device** on the top
3. Click to enter the Import Personal Device page.
4. Check the devices as needed.



Import Personal Device

Select Device(s)*

☑	Device Name	Device Serial No.	Version	Belongs To
□	[redacted]	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]	[redacted]
☑	[redacted]	[redacted]	[redacted]	[redacted]

10

Set Time Zone

● Use Current Time Zone of Device

○ Batch Set Time Zone for Devices

*Add to Area

● Create Area by Device Name

○ Existing Area

□ Delete Devices from Personal Site After ...

Figure 5-7 Import Devices

5. Set device time zones.

- Select **Use Current Time Zone of Device** and the platform will get device time zone settings and use them.
- Select **Batch Set Time Zone for Devices** and select a time zone for all the selected devices.

Note

Check **Apply to Device**, and the selected time zone will be applied to the selected devices.

6. Optional:

7. Create an area by device name or select an existing area.

8. Optional: Check **Delete Devices from Personal Site After They Are Imported**.

9. Click **Import**or click **Import More** to import more devices.

A window will pop up and show the importing result.

10. **Optional:** You can enable local recording, cloud recording, and set access control permissions on the Adding Results pane.

5.7.3 Unbind a Device from Its Current Account

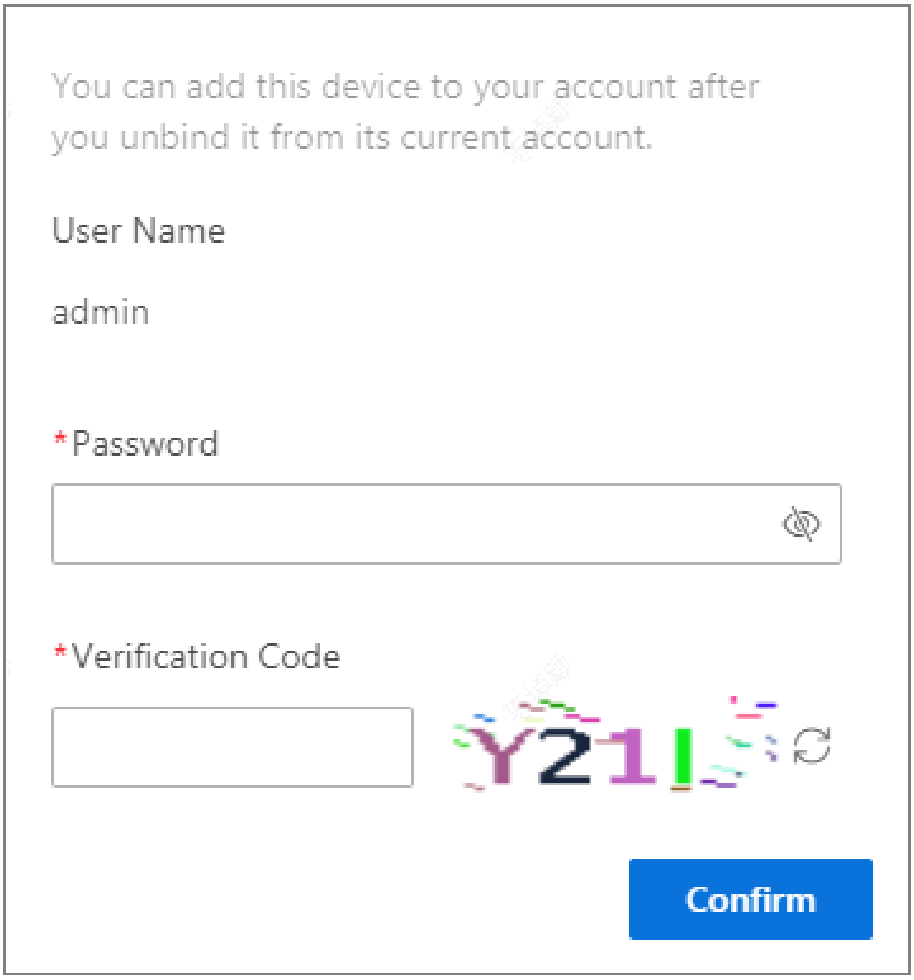
When you need to add a device which has already been added to an account, you should unbind it before you can add it to your account.

Before You Start

- Make sure the device is on the same LAN with the PC running the Portal.
- Make sure the device has been activated. Refer to ***Create Password for Inactive Device(s)*** for details.

Steps

1. On the top navigation bar, click **Device and Maintenance → Resource Management → Device** .
2. Below **Device**, select the device type (e.g., encoding device, access control device, video intercom device, Hik-ProConnect box, and on-board device).
3. In the Online Device area, click 🔗 in the Operation column of an active device.



You can add this device to your account after you unbind it from its current account.

User Name

admin

*Password

*Verification Code

Figure 5-8 Unbind a Device

4. In the pop-up window, enter the device password.
5. Enter the verification code.
6. Click **Confirm**.

5.7.4 Create Password for Inactive Device(s)

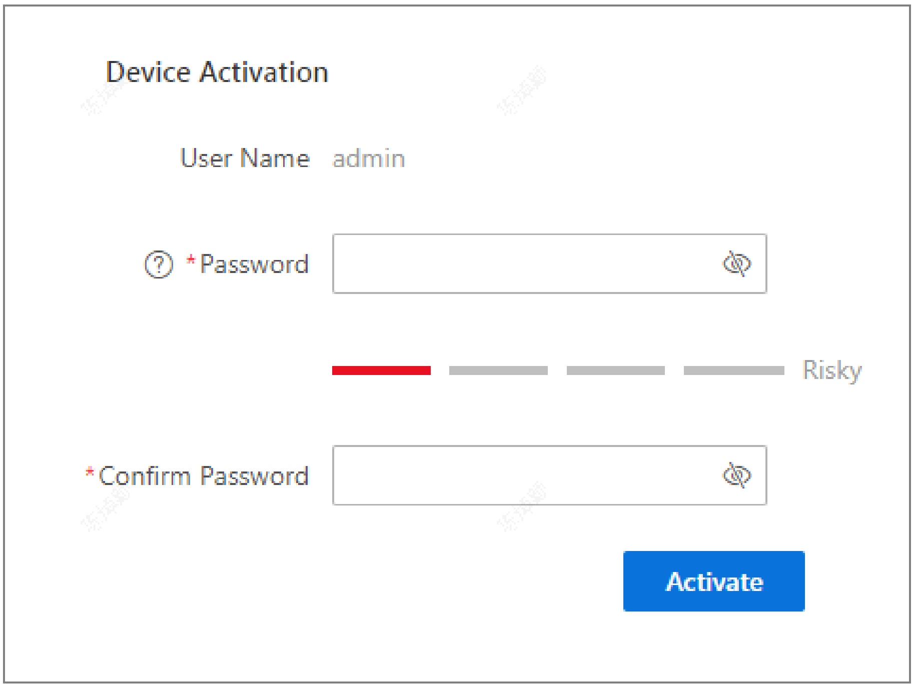
You should crincaeate password(s) to activate device(s) before adding them to the System and performing more operations. You can activate the device one by one, or batch activate devices which have the same password.

Before You Start
Make sure the devices to be activated are on the same LAN with the PC running the Portal.

Steps
1. On the top navigation bar, click **Device and Maintenance → Resource Management → Device** .
2. Below **Device**, select the device type (e.g., encoding device, access control device, video intercom device, Hik-ProConnect box, and on-board device).

3. In the Online Device area, select one or multiple inactive devices.

4. Click **Activate** to open the device activation window.



Device Activation

User Name admin

*Password

Risky

*Confirm Password

Figure 5-9 Device Activation Window

5. Create a password and confirm the password.

Caution

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

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

6. Click **Activate**.

7. Optional: Perform more operations after activating the device.

Edit Device Network Parameters	Click ✎ to edit the device network parameters. For details, refer to ***Edit Online Device's Network Information*** .
Reset Device Password	Click ↺ to reset the password of the device. For details, refer to ***Reset Device Password*** .
Unbind Device	Click 🔗 to unbind the device from its current account. For details, refer to ***Unbind a Device from Its Current Account*** .

5.7.5 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. via the Portal.

Before You Start

- Make sure the device has been activated. For details, refer to ***Create Password for Inactive Device(s)*** .
- Make sure the device to be edited is on the same LAN with the PC running the Portal.

Steps

1. On the top navigation bar, click **Device and Maintenance → Resource Management → Device** .
2. Below **Device**, select the device type (e.g., encoding device, access control device, video intercom device, Hik-ProConnect box, and on-board device).
3. In the Online Device area, click ✎ in the Operation column of an active device.
4. Edit the device parameters, including the IP address, device port, HTTP port, subnet mask, and gateway.

   Note

   The parameters may vary for different device types.
5. Click ✓ .
6. Enter the device password.
7. Click **Save**.

5.7.6 Reset Device Password

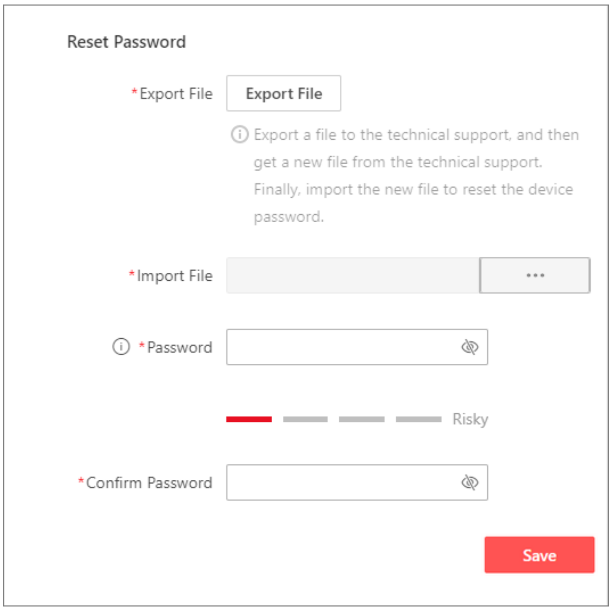
If you forget the device password, you can apply a key file from the technical support and then reset the device password.

Before You Start

- Make sure the device is on the same LAN with the PC running the Portal.
- Make sure the device has been activated. Refer to ***Create Password for Inactive Device(s)*** for details.

Steps

1. On the top navigation bar, click **Device and Maintenance → Resource Management → Device** .
2. Below **Device**, select the device type (e.g., encoding device, access control device, video intercom device, Hik-ProConnect box, and on-board device).
3. In the Online Device area, click ↺ on the Operation column of an active device.


Reset Password

*Export File: Export File

Export a file to the technical support, and then get a new file from the technical support. Finally, import the new file to reset the device password.

*Import File: ...

*Password:

Risky

*Confirm Password:

Save

Figure 5-10 Reset Password Window

The Reset Password window pops up.

4. Click **Export File** to save the file to your local PC.
5. Send the file to the technical support.
6. Click ... , and select the file you got from the technical support to import it to the System.
7. Create a new password for the device and confirm the password.

⚠ Caution

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

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

8. Click **Save**.

5.7.7 Upgrade Device Firmware

If there are devices to be upgraded, you can upgrade the firmware of the device via the platform.

Before You Start

Make sure the device to be upgraded has been connected to power supply properly.

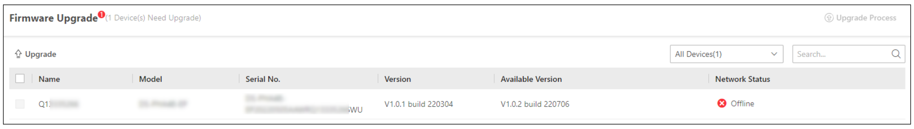
Steps

Note

Choose a proper time for upgrade since you do not have access to the device functions during upgrade.

1. On the top navigation bar, click **Device and Maintenance → Firmware Upgrade** .

You will enter the Firmware Upgrade page and can view the number of devices that need to be upgraded.



Firmware Upgrade (1 Device(s) Need Upgrade)

Upgrade Process

Upgrade

All Devices(1)

Search...

□	Name	Model	Serial No.	Version	Available Version	Network Status
□	Q1[redacted]	[redacted]	[redacted]WU	V1.0.1 build 220304	V1.0.2 build 220706	Offline

Figure 5-11 Firmware Upgrade

2. Optional: Filter the devices to be upgraded.

- Select **Encoding Device**, **On-Board Device**, **Access Control Device**, **Video Intercom Device**, or **Hik-ProConnect Box** as the device type from the drop-down list.

  Note

  The platform now supports upgrading firmwares of solar-powered cameras and card readers of access control devices.

- Enter keywords in the search box.

The devices that meet the condition(s) will be displayed in the list.

3. Select the device(s) to be upgraded.

4. Click **Upgrade**.

5. Read the Upgrade Confirmation and click **OK**.

Note

During the upgrade, you can click ⊖ in the upper-left corner to return to the Firmware Upgrade page, and then click **Upgrade Process** in the upper-right corner of the page to go back to the Upgrade Process page as needed.

Upgrade starts, and the upgrade results will be displayed when the upgrade is finished.

6. Optional: Upgrade device(s) failed to be upgraded again.

- Click ⇧ in the operation column to upgrade a single device.
- Click **Upgrade All Failed Tasks** to upgrade all the devices.

5.7.8 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, the technical support can locate and solve the problems more efficiently.

Steps

1. On the top navigation bar, click **Device and Maintenance → Resource Management** .

2. **Optional:** Select an area in the area list.
3. Click **Device**, and then select a device type.
4. Click → **Export** .

   You will view the exporting process, and then all devices of the selected type will be exported.

5.8 Manage Cameras in Area

You can add cameras to an area for management. For the added camera, you can also edit its basic information, local storage, etc.

5.8.1 Add a Camera to Area

You can add a camera to the area for management.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Select an area (except the root area) in the list.

   Note

   Make sure you have the permission to the selected area. For details about configuring the permission, refer to ***Add a Role*** .

3. Click **Camera** on the top.
4. Click **Add** to enter the Add Camera page.
5. Select **Encoding Device** or **On-Board Device** as the device type.
6. Select camera(s) to be added.
7. Click **Add** to add camera(s) to the area.

   The added camera(s) will be displayed in the list. You can check **Include Sub-Area** to display camera(s) in the sub-areas.

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

   View Live View Select camera(s), and click **Live View** to view the live view of the selected camera(s).

   Move Camera to Other Area Select camera(s), and click **Move to Other Area** to move the selected camera(s) to another area.

   Add Camera to Map Select camera(s), and click **Add Map Resources** to add selected camera(s) to the map. For details, refer to ***Add Hot Spot on Map*** .

   Configure Cloud Storage Select camera(s), and click **Configure Cloud Storage** to enter the Batch Configure Cloud Storage for Cameras page. For details, refer to ***Batch Configure Cloud Storage for Cameras*** .

Configure Local Storage
Select camera(s), and click **Configure Local Storage** to pop up the Configure Cloud Storage panel. For details, refer to ***Configure Recording for Cameras*** .

Configure Video Parameters
Select camera(s), and click **Configure Video Parameters** to configure video parameters for the camera(s) including stream type, video type, resolution, bit rate type, video quality, etc.

Get Device Recording Settings

- Get the Recording Settings of a Single Device: Click a camera name, and click **Get Device's Recording Settings**.
- Batch Sync Recording Schedules: Select camera(s), and click **Batch Sync Recording Schedules** to batch synchronizing recording schedules with devices.

Delete Camera
Select camera(s), and click **Delete** to delete the selected camera(s).

Filter Camera
Click ⌄ in the upper-right corner, and select a device type to filter cameras.

Search Camera
Enter keyword(s) in the search box in the upper-right corner to search for the target camera(s).

5.8.2 Edit a Camera in Area

You can edit the basic information such as the name of the camera added to the area.

Before You Start
Make sure you have added camera(s) to areas. For details, refer to ***Add a Camera to Area*** .

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. **Optional:** Select an area in the list.

   Note

   The root area is selected by default.
3. Click **Camera** on the top to show the cameras added to the selected area.
4. Click a camera's name in the **Name** column to enter the camera editing page.
5. **Optional:** Perform the following operations to edit the camera.

Basic Information
You can edit the camera's name.

You can click **Refresh** to get the latest captured image of the camera.

Local Storage
You can edit the local recording settings for the camera. See details in ***Configure Recording for Cameras*** .

Cloud Storage Server
You can edit the cloud storage settings for the camera. If the camera is linked to an NVR that supports cloud storage, refer to ***Configure Cloud***

Storage for Camera Linked to NVR for details; if not, refer to ***Configure Cloud Storage for Camera Linked to Hik-ProConnect Box*** for details.

Note

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

Copy to
You can click **Copy to** in the top right corner, and copy the configuration item(s) of this camera to other cameras.

Remote Configuration
Click **Remote Configuration** in the top right corner to enter the remote configuration page of the camera, and configure remotely for the camera.

6. Click **Save**.

5.9 Manage Vehicles in Area

You can add vehicles to areas for management.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Select an area (except the root area) in the list.

   Note

   Make sure you have the permission to the selected area. For details about configuring the permission, refer to ***Add a Role*** .
3. Click **Vehicle** on the top.
4. Click **Add** to enter the Add Vehicle page.
5. Set the vehicle information, including license plate number, driver's last name and first name, etc.
6. In the Device Information area, select a linked device from the drop-down list.
7. Add the vehicle.
   - Click **Add** to add the current vehicle and go back to the vehicle list page.
   - Click **Add and Continue** to add the current vehicle and continue to add other vehicle(s).

   After adding a vehicle, a sub area named as the license plate number of the vehicle will be created automatically. The resources of the linked device will be automatically imported to this sub area.
8. **Optional:** Perform the following operation(s).

   Move Vehicle to Other Area
   Select vehicle(s), and click **Move to Other Area** to move the selected vehicle(s) to another area.

Batch Set Speed Threshold for Vehicles
Select the vehicle(s), click **Speed Threshold Settings**, drag the slider or enter an integer in the text field, and click **OK**.

Delete Vehicle
Select vehicle(s), and click **Delete** to delete the selected vehicle(s).

> **Note**
>
> The sub area named as the license plate No. of the vehicle will also be deleted.

Search Vehicle
Enter keyword(s) in the search box in the upper-right corner to search for the target vehicle(s).

Edit Vehicle
Click a vehicle's name in the License Plate No. column, and edit the vehicle's basic information (license plate number, driver's last name and first name, etc.) and its linked device.

5.10 Manage Doors in Area

You can add doors to an area for management. For the added door, you can also edit its basic information, related cameras, etc.

5.10.1 Add a Door to Area

You can add a door to the area for management.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Select an area (except the root area) in the list.

   > **Note**
   >
   > Make sure you have the permission to the selected area. For details about configuring the permission, refer to ***Add a Role*** .

3. Click **Door** on the top.
4. Click **Add** to enter the Add Door page.
5. Select the device type as **Access Control Device** or **Video Intercom Device**.
6. Select door(s) in the area list.
7. Click **Add** to add door(s) to the area.

   The added door(s) will be displayed in the list. You can check **Include Sub-area** to display door(s) in the sub-areas.
8. **Optional:** Perform the following operation(s).

   Filter Doors
   Click ⌄ in the upper right corner to filter doors by device type.

Move Door to Other Area	Select door(s), and click **Move to Other Area** to move the selected door(s) to a new area.
Delete Door	Select door(s), and click **Delete** to delete the selected door(s).
Search Door	Enter keyword(s) in the search box in the upper-right corner to search for the target door(s).

5.10.2 Edit a Door in Area

You can edit a door added to the area such as its basic information and related camera.

Before You Start

Make sure you have added door(s) to areas. For details, refer to ***Add a Door to Area*** .

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. **Optional:** Select an area in the list.

   Note

   The root area is selected by default.
3. Click **Door** on the top to show the doors added to the selected area.
4. Click a door's name in the **Name** column to enter the door editing page.
5. **Optional:** Edit the door's basic information.

   Note

   The parameters may vary for different doors.

   Door Picture

   Upload or edit a picture for the door.

   Door-Open Duration

   Configure the time interval between the door is open and closed.

   Extended Open Duration (s)

   Configure the time interval between the door is open and closed for the person with extended access needs.

   Door Open Timeout Alarm

   Turn on the switch and configure the maximum open duration. If the door has been configured with event or alarm, when the door open duration reaches the maximum value, the event or alarm will be triggered and uploaded to the system.

   Duress Code

   Custom a duress code, and enter the duress code to open the door when duress happens.

Dismiss Code

Custom a dismiss code, and enter the dismiss code to stop the buzzer of the card reader if needed.

Note

The duress code and the dismiss code should be different.

6. **Optional:** Click **Add** to add related cameras to the door to view the cameras' live view, playback, etc.

Note

- Up to 2 cameras can be linked to one door.
- You can click 🗑 to delete a camera.

7. **Optional:** Switch on **Anti Tailing** to detect and record tailing events.

Note

- To use this function, make sure you have linked the door to at least one camera with the capability of people counting.
- You can click ⚙ to enter the remote configuration page of the camera, and view or edit the parameters related with person's direction.

8. **Optional:** In the Card Reader panel, switch on Card Reader 1 or Card Reader 2 and set the card reader related parameters.

Access Mode (Custom)

Select an access mode (e.g., Card, Card+Password, Card/Face, etc.,), and then draw on the table to define the time period(s) when this mode will take effect. You can select different access modes for different time periods in a day and different days in a week.

Failed Card Attempts Alarm

If the door is configured with event or alarm, when the number of failed card swiping attempts has reached the limit, the event or alarm will be triggered and uploaded to the system. You should set the maximum failed attempts.

Tampering Detection

If the door is configured with device tampered event or alarm, when the device body or panel is tampered, the alarm will be triggered and uploaded to the system.

Face 1:N Matching Threshold

Face 1:N Matching means comparing the captured face picture with all face pictures stored in the device. You can set the matching threshold for face 1:N matching. The larger the value, the smaller the false matching rate.

Face Anti-Spoofing

If checked, the device can detect whether the face is a live person's face or not. You should set the Face Anti-Spoofing Security Level as **Low**, **Medium**, or **High**.

Face 1:1 Matching Threshold

Face 1:1 Matching means comparing the captured face picture with the face picture stored in the device. You can set the matching threshold for face 1:1 matching. The larger the value, the smaller the false matching rate.

Face Recognition Application Mode

Select **Indoor** or **Others** according to actual environment.

Note

The parameters (including Access Mode, Failed Card Attempts Alarm, Tampering Detection,and Face 1:1 Matching Threshold) are only applicable to the access control device.

9. **Optional:** Click **Remote Configuration** in the top right corner to enter the remote configuration page of the door, and configure remotely for the door.
10. **Optional:** Click **Copy to** in the top right corner, and copy the configuration item(s) of this door to other doors.
11. Click **Save** to save the above settings.

5.11 Manage Alarm Inputs in Area

You can add alarm inputs to areas for management.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Select an area (except the root area) in the list.

Note

Make sure you have the permission to the selected area. For details about configuring the permission, refer to ***Add a Role*** .

3. Click **Alarm Input** on the top.
4. Click **Add** to enter the Add Alarm Input page.
5. Select **Encoding Device**, **On-Board Device**, **Access Control Device**, or **Video Intercom Device** as the device type.
6. Select the alarm input(s) to be added.
7. Click **Add**.

   The added alarm input(s) will be displayed in the list. You can check **Include Sub-area** to display alarm input(s) in the sub-areas.
8. **Optional:** Perform the following operation(s).

Move Alarm Input to Other Area	Select alarm input(s), and click **Move to Other Area** to move the selected alarm input(s) to the other area.
Add Alarm Input to Map	Select alarm input(s), and click **Add Map Resource** to add selected alarm input(s) to the map. For details, refer to ***Add Hot Spot on Map*** .
Edit Alarm Input	Click an alarm input in the Name column, and edit its name.

Delete Alarm Input Select alarm input(s), and click **Delete** to delete the selected alarm input(s).

Search Alarm Input Enter keyword(s) in the search box in the upper-right corner to search for the target alarm input(s).

5.12 Manage Alarm Outputs in Area

You can add alarm outputs to areas for management.

Steps

1. Click **Device and Maintenance** on the top navigation bar, and click **Resource Management** on the left panel.
2. Select an area (except the root area) in the list.

   Note

   Make sure you have the permission to the selected area. For details about configuring the permission, refer to ***Add a Role*** .
3. Click **Alarm Output** on the top.
4. Click **Add** to enter the Add Alarm Output page.
5. Select **Encoding Device**, **On-Board Device**, **Access Control Device**, or **Video Intercom Device** as the device type.
6. Select the alarm output(s) to be added.
7. Click **Add**.

   The added alarm output(s) will be displayed in the list. You can check **Include Sub-area** to display alarm output(s) in the sub-areas.
8. **Optional:** Perform the following operation(s).

   Move Alarm Output to Other Area Select alarm output(s), and click **Move to Other Area** to move the selected alarm output(s) to the other area.

   Add Alarm Output to Map Select alarm output(s), and click **Add Map Resource** to add selected alarm output(s) to the map. For details, refer to ***Add Hot Spot on Map*** .

   Edit Alarm Output Click an alarm output in the Name column, and edit its name.

   Delete Alarm Output Select alarm output(s), and click **Delete** to delete the selected alarm output(s).

   Search Alarm Output Enter keyword(s) in the search box in the upper-right corner to search for the target alarm output(s).

Chapter 6 Video Management

The Portal provides the following functionality: video security, video search, and recording schedule template settings.

Video Security	• See details in ***Start Fast View*** , ***Manage Views*** , ***Live View*** , ***Playback*** , and ***Set Video Parameters*** . • The Video Security module is divided into 2 tabs. ◦ Fast View: You can watch the live video in different areas directly and easily locate the target camera(s). ◦ Monitoring: You can watch live videos or playback in area/view mode. **Note** Your last-viewed tab will be remembered by the portal and your tab choice will be applied next time you enter the Video Security module.
Video Search	See details in ***Video Search*** .
Recording Schedule Template Settings	See details in ***Configure Recording and Storage*** .

Note

Without the Web Control plug-in, you can use basic functions of fast view and monitoring with limited channels; you can install the Web Control plug-in to unlock more video-related functions including view management, multi-channel main stream, multiple window divisions, cloud storage video playback, synchronous playback, multi-speed playback, etc.

6.1 Configure Recording and Storage

Before you can play back video files recorded by cameras, you need to configure recording schedules, recording methods, etc.

6.1.1 Configure Recording for Cameras

You can configure recording for cameras by selecting a recording schedule template and setting other parameters as needed, then video files of cameras can be stored according to the configured recording schedule.

Steps

1. On the top navigation bar, select **Device and Maintenance → Resource Management** .
2. Select the **Camera** tab.
3. Select an area on the left side to show its cameras.
4. Configure local storage for the camera(s).
   - Configure for a single camera: Select a camera and click its name to enter camera settings page, click **Local Storage** on the top, and switch on **Local Storage**.
   - Batch configure for cameras: Select cameras and click .

   Note

   To use this function, you should insert an SD card to the network camera, or install a disk inside the NVR.
5. Select a recording schedule template for the camera.

   All-Day Time-based Template

   Record the video for all the day continuously.

   All-Day Event-based Template

   Record the video when the alarm occurs.

   Add New

   Set the customized template. For details, refer to ***Configure Recording Schedule Template*** .

   View

   View the template details.
6. **Optional:** Set other parameters as needed.

   Stream Type

   Select a stream type.

   Pre-Record

   Record video from periods preceding detected events.

   Post-Record

   Record video from periods following detected events.

   Video Expiration

   Switch on **Video Expiration** and enter expiration day(s) to automatically delete the oldest videos after the specified retention period.

   Enable ANR

Check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network fails and transport the video to storage device when network recovers.

7. Click **OK**.

6.1.2 Configure Recording Schedule Template

Recording schedule is time arrangement for video recording. You can configure the recording schedules to record videos in a certain period. Two default recording schedules are available: All-day Time-based Template and All-day Event-based Template. All-day Time-based Template can be used for recording videos for all day continuously, and All-day Event-based Template is for recording videos when alarm is triggered. You can also customize the recording schedule.

Steps

1. On the top navigation bar, select **Video → Recording Schedule Template Settings** .

2. Click + on the left panel to add a new schedule template.

3. Set the required information.

Name

Required. Set a name for the template.

Copy From

Optional. Select a template from the drop-down list and copy its settings.

4. Select a schedule type and drag on the time bar to draw a time period.

Time-based

Continuously recording according to the time you arranged. The schedule time bar is marked in blue.

Event-based

Recording videos when alarm is triggered. The schedule time bar is marked in orange.

Note

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

5. Optional: Click **Erase** and click on the time bar to clear the drawn time period.

6. Click **Save** to add the template.

7. Optional: Perform the following operations.

Edit Template	Click a template and edit its name, recording type, etc. **Note** The two default templates cannot be edited.
Delete Template	Click 🗑 to delete a template.

Note

The two default templates cannot be deleted.

Search Template Enter one or more keywords in the search box to search for the template.

6.1.3 Configure Cloud Storage for Camera Linked to Hik-ProConnect Box

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.

Before You Start

- The cloud storage feature is only available in some countries/regions. Please contact Hikvision for details.
- Make sure you have added Hik-ProConnect boxes to the System. For details about adding Hik-ProConnect boxes, see ***Manage Hik-ProConnect Box in Area*** .
- Make sure the camera you are going to configure is already added to the System. For details about adding devices, see ***Manage Encoding Device in Area*** .

Steps

1. On the top navigation bar, select **Device and Maintenance → Resource Management** .
2. Select the **Camera** tab.
3. Click a camera name to enter the camera details page.
4. Switch on **Cloud Storage Server**.
5. Select a Hik-ProConnect box from the drop-down list as the storage location.

   Note

   - The storage location will be automatically set to Hik-ProConnect box if there is a Hik-ProConnect box added to the System and the device to which the camera belongs does not support cloud storage.
   - In general, the IP address and port No. of the camera will be automatically filled in below. If not, you can manually enter the IP address and port No. of the camera.
6. **Optional:** Click **Network Test** to start testing the network performance.

   Note

   It is recommended that you perform the test to configure the optimal number of cameras (channels) and set suitable stream types for them to better utilize the available network bandwidth.

   The latest test result will be displayed below **Storage Location**.
7. Select an unlinked channel of the Hik-ProConnect box to link with the camera.

Note

If the camera is already linked to a channel, a window will pop up if you select another unlinked channel. Click **OK** to switch to the selected channel, or click **Cancel** to stay linked to the current channel.

8. **Optional:** Change the **Stream Type** if needed.

Note

The default stream type is selected based on the recommended resolution of your network test result. You can select from **SD**, **HD**, and **Custom** based on your network conditions. After the cloud storage service is enabled, the actual resolution and bit rate will be displayed below your selection.

9. Enter the user name and password of the camera.
10. Select an available cloud storage plan from the drop-down list of **Cloud Storage Plan**.

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.
- If there is no cloud storage plans available, contact your service provider.

11. Click **Save**.

6.1.4 Configure Cloud Storage for Camera Linked to NVR

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.

Before You Start

- The cloud storage feature is only available in some countries/regions. Please contact Hikvision for details.
- Make sure you have added NVRs to the System. For details about adding devices, see ***Manage Encoding Device in Area*** .

Steps

1. On the top navigation bar, select **Device and Maintenance → Resource Management** .
2. Select the **Camera** tab.
3. Click a camera name to enter the camera details page.
4. Switch on **Cloud Storage Server**.

Note

The storage location will be automatically set to **Encoding Device**, which is the NVR to which the camera belongs. You can also switch the storage location to a Hik-ProConnect box. For details about configuring cloud storage for a camera by linking it to a Hik-ProConnect box channel, see ***Configure Cloud Storage for Camera Linked to Hik-ProConnect Box*** .

5. **Optional:** Click **Network Test** to start testing the network performance.

   Note

   It is recommended that you perform the test to configure the optimal number of cameras (channels) and set suitable stream types for them to better utilize the available network bandwidth.

   The latest test result will be displayed below **Storage Location**.
6. **Optional:** Change the **Stream Type** if needed.

   Note

   The default stream type is **HD**. You can choose to change it to **SD** based on your network conditions. After the cloud storage service is enabled, the actual resolution and bit rate will be displayed below your selection.
7. Select an available cloud storage plan from the drop-down list of **Cloud Storage Plan**.

   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.
   - If there are no cloud storage plans available, contact your service provider.
8. Click **Save**.

6.1.5 Batch Configure Cloud Storage for Cameras

You can configure cloud storage for multiple cameras at the same time. After cloud storage is enabled for the cameras, event-related videos of the cameras will be uploaded to the cloud.

Before You Start

- The cloud storage feature is only available in some countries/regions. Please contact Hikvision for details.
- Make sure the cameras you are going to configure are already added to the corresponding areas. For details about adding cameras to areas, refer to ***Add a Camera to Area*** .

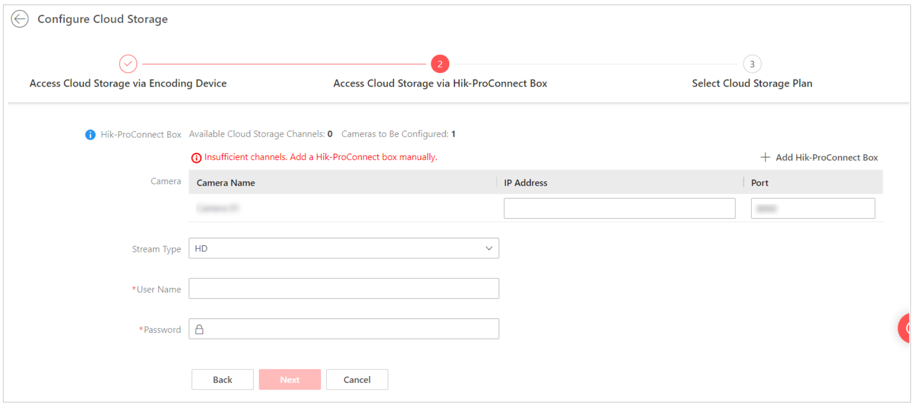
Steps

1. On the top navigation bar, select **Device and Maintenance → Resource Management** .
2. Select the **Camera** tab.

3. Optional: Select an area from the area list.

4. Select the cameras from the camera list, and click ☁ .

You will enter the Configure Cloud Storage process.



Configure Cloud Storage

✓ Access Cloud Storage via Encoding Device — 2 Access Cloud Storage via Hik-ProConnect Box — 3 Select Cloud Storage Plan

Hik-ProConnect Box Available Cloud Storage Channels: **0** Cameras to Be Configured: **1**

Insufficient channels. Add a Hik-ProConnect box manually.

Camera

Camera Name	IP Address	Port

Stream Type: HD

*User Name:

*Password:

Figure 6-1 Configure Cloud Storage for Cameras

5. On the Access Cloud Storage via Encoding Device page, check the cameras for which you want to configure cloud storage via the encoding devices the cameras are linked to, select a stream type based on your network conditions, and click **Next**.

Note

Only cameras that are linked to an encoding device that supports cloud storage will be shown on this page. If none of the cameras you selected meet this condition, you will be directed to the Access Cloud Storage via Hik-ProConnect Box page after clicking ☁ .

6. On the Access Cloud Storage via Hik-ProConnect Box page, configure cloud storage for cameras that are not linked to an encoding device that supports cloud storage by linking each of them to a Hik-ProConnect box channel.

Note

Skip this step if all the cameras you selected can access cloud storage via the encoding device they are linked to.

1) Click **Add Hik-ProConnect Box** to add a Hik-ProConnect box first. If the available Hik-ProConnect box channels are still insufficient, click again to add more.

Note

In general, the IP address and port No. of each camera will be automatically filled in the corresponding boxes when a Hik-ProConnect box is added. If not, you can manually enter the IP address and port No. of each camera.

2) **Optional:** Select a stream type based on your network conditions.

3) Enter your user name and password.

4) Click **Next**.

7. On the Select Cloud Storage Plan page, select a type of cloud storage plan from the drop-down list, and check which specific plans to use for the cameras you selected.

Note

- The number of plans you select here should be greater than or equal to that of the cameras to be configured.
- If the available cloud storage plans are insufficient, contact your service provider.

8. Click **Finish**.

6.2 Start Fast View

You can see thumbnails of the cameras' images in all areas. You can also operations such as starting batch live view of all cameras from an area.

Go to **Video → Video Security → Fast View** .

You can perform the following operations.

Start Batch Live View	In the upper-right corner of an area, click **Batch Live View** to start batch live view of the cameras from the area.
Start Live View of a Camera	Click the image of a camera to start live view.
Expand Window	In the upper-right corner of a window, click ⤢ to go to the Monitoring section.

6.3 Manage Views

A view is a window division with resource channels (cameras) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows as the default so that you can quickly access these cameras later. For example, you can link camera 1, camera 2, and camera 3 located in your office to the certain windows and save them as a view called "office". Then, you can access the view "office" and these cameras will display in the linked windows quickly.

6.3.1 Add a View Group

You can add view groups to group the related views together for viewing and management.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Go to **Monitoring → View** .
3. Select **Public View** or **Private View** to add the view group.

Note

Other users cannot view the view groups and views in the private view group.

4. Click **Add View Group**.
5. Create a name for the group or use the default name.
6. Click **Add** to add this view group.
7. **Optional:** Perform the following operations after adding view groups.

Delete View Group	Hover on a view group, and click ··· → **Delete** to delete the custom view group.
Edit View Group	Hover on a view group, and click ··· → **Edit** to edit the view group name.
View Group Auto-Switch	Hover on a view group, and click ··· → **Play** to start view group auto-switch. For details,refer to ***Perform View Auto-Switch*** .

6.3.2 Add a View

View defines the window division and resource channels (cameras) linked to each window. You can add a view by dragging specific camera(s) to the corresponding window(s). In the live view window, digital zoom, rotated image, created zooming area, camera ID, stream type, position, preset No., and fisheye dewarping status can be saved in a view. In the playback window, digital zoom, rotated image, created zooming area, camera ID, position, and fisheye dewarping status can be saved in a view.

Before You Start

Make sure you have added cameras to areas. Refer to ***Add a Camera to Area*** for details.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Go to **Monitoring → Camera** .
3. Select one or multiple cameras, double click or drag them to the live view or playback window.
4. **Optional:** If you drag multiple cameras to the window, click **Batch Play** in the pop-up menu.
5. Click 🖫 to save the current cameras and window division as a view.
6. Edit the name of the view to be added or use the default name.
7. Select a view group to add the view.
8. Click **Save**.

   The view is added to the view list in **View** tab.
9. **Optional:** Perform more operations after adding a view.

Edit View	Hover on a view, and click ··· → **Edit** to edit the name and/or view group of the selected view.
Delete View	Hover on a view, and click ··· → **Delete** to delete the selected view.
Start Live View in View Mode	Select the **Live View** tab, hover on a view, and click ··· → **Play** to start live view in view mode. For details, refer to ***Start Live View in View Mode*** .

Start Playback in View Mode
Select the **Playback** tab, hover on a view, and click ⋯ → **Play** to start playback in view mode. For details, refer to ***Start Playback in View Mode*** .

6.3.3 Perform View Auto-Switch

For view groups with multiple views, you can start view group auto-switch to display views of a view group one after the other.

Before You Start
Make sure you have added at least two views into one view group. See ***Add a View*** for details.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Go to **Monitoring → View** .
3. Click **Live View** tab.
4. Double click a view group, or hover on a view group and click ⋯ → **View Group Auto-Switch** to start auto-switch of views in the view group.
5. Optional: Perform the following operations during view auto-switch.

Switch Views
Switch the added views from the drop-down list above the live view window.

Set Auto-Switch Interval
Click « or » in the bottom toolbar to set the auto-switch interval to 1 second, 10 seconds, 30 seconds, 1 minute, 2 minutes or 5 minutes.

View Previous or Next View
Click < or > in the bottom toolbar to view the previous or next view.

Pause Auto-Switch
Click ⏸ in the bottom toolbar to pause the auto-switch.

6.3.4 Perform Camera Auto-Switch in One Window

You can view videos of cameras in the same or different areas one after another in a single window. You can also specify the interval of camera auto-switch.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Go to **Monitoring → Camera** .
3. Click **Live View** tab.
4. Start camera auto-switch.
   - Drag an area on the left panel to the live view window.

Note

Make sure at least two cameras have been added to the area. Refer to ***Add a Camera to Area*** for details.

- Hold the Ctrl key and select multiple cameras in an area or different areas, and then drag them to the live view window.

5. Click **Single-Screen Auto-Switch** in the pop-up menu to display the videos of the cameras in one window.
6. **Optional:** Perform more operations after starting camera auto-switch.

Set Auto-Switch Interval
Click « or » in the lower-left corner of the live view window to set the auto-switch interval to 5 seconds, 10 seconds, 20 seconds, 40 seconds, 1 minute, 3 minutes or 5 minutes.

View Previous or Next Camera
Click < or > in the lower-left corner of the live view window to go to the previous or next camera.

Pause Auto-Switch
Click ⏸ in the lower-left corner of the live view window to pause the auto-switch.

6.4 Live View

In the Live View module of Portal Client, you can view the live video of the added cameras and do some basic operations, including picture capturing, recording, PTZ control, and so on.

6.4.1 Start Live View in Area Mode

You can play the live video streamed from the added cameras. During live view, you can record the live video manually or take a quick snapshot of the live video via the Portal.

Before You Start

Make sure you have grouped cameras into areas. Refer to ***Add a Camera to Area*** for details.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Go to **Monitoring → Camera** .

   The areas and resources which the current user has permission to access are listed.
3. Click **Live View** to enter the live view page.
4. **Optional:** Click ⊞ in the upper-right corner to change the live view window division.

   Average

   All the divided windows are distributed evenly.

   Highlighted

   The highlighted window is used to display the live video from the critical camera.

   Horizontal

The divided windows are distributed horizontally in the window.

Vertical

The divided windows are distributed vertically in the window.

Others

Other types of window division besides the types above.

5. Start live view.
   - Drag a camera to the display window to play the live video streamed from the camera, or double-click the camera to start the live view in a free display window.
   - Drag an area to a display window, and click **Batch Play**, or double-click the area to play the live videos streamed from all cameras in the area.

Note

The display windows automatically adapt to the number of cameras in the area.

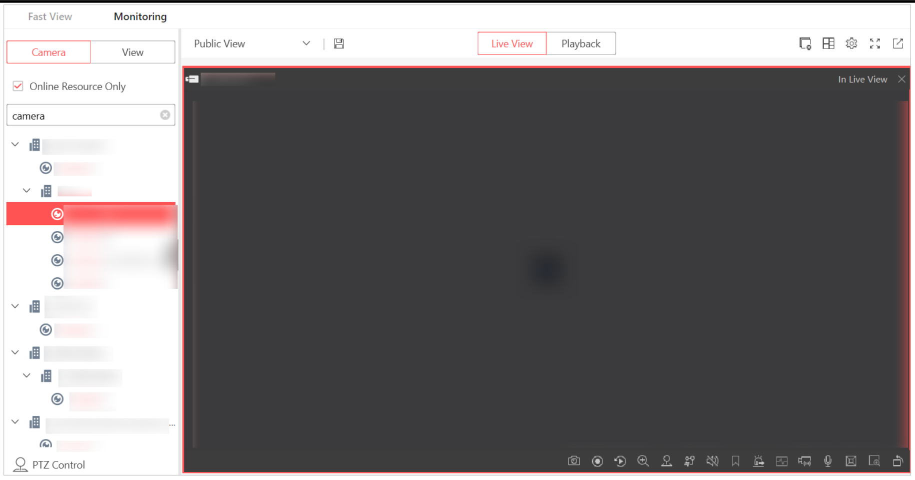


Figure 6-2 Start Live View

6. **Optional:** Click in the top right corner of the live view page to open an auxiliary screen.

Note

No more than 3 auxiliary screens can be opened at the same time.

7. **Optional:** Perform the following operations on the live view toolbar.

Capture Picture

Click to capture a picture. After capturing, you can click **Edit → Save and Archive** to save the picture as an archive.

Start Recording

Click to start the manual recording. After recording, you can click **Archive** to save the recorded file as an archive.

Instant Playback

Click to switch to the instant playback mode. Hover over the playback image and click to exit instant playback mode.

Digital Zoom

Click to enlarge the image.

Switch Stream Type

Click to switch the live view stream to main stream or sub stream.

Turn On/Off Audio
Click 🔇 to turn on the audio and click 🔊 to turn it off.

Add Tag
Click 🔖 to add a tag for the video footage in a selected time range during live view.

Alarm Output
Click to display the Alarm Output Control page and turn on/off the alarm outputs of the connected camera.

Camera Status
Click to show the camera's recording status, signal status, connection number, etc.

Video Enhancement
Click to adjust the video image including brightness, saturation, etc.

Two-Way Audio
Click 🎤 to start two-way audio with the camera to get the real-time audio from the device to realize voice talk with the person at the device.

> **Note**
>
> To perform two-way audio with the camera, you can also click the camera in the camera list, and click 🎤 .

Fisheye Expansion
Click to enter the fisheye dewarping mode. In this mode, the video image is corrected and the geometric distortion caused by the fisheye camera lens is reversed.

> **Note**
>
> This function is available for fisheye cameras. For details, refer to ***View Dewarped Live View of Fisheye Camera*** .

Create Zooming Area
Click and draw a rectangle area in the live video image. The area created will be displayed in a new window.

Rotate Image
Click to rotate the video image.

6.4.2 Start Live View in View Mode

You can quickly start the live view of the cameras managed in a view.

Before You Start
Make sure you have added at least a view. Refer to ***Add a View*** for details.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Go to **Monitoring → View** .
3. Start live view of the cameras related to the view.
   - Double-click a view.
   - Move the mouse cursor to a view, and click ··· → **Play** beside the view name.

Note

You can switch the added views from the drop-down list in the upper-left corner above the live view window.

4. **Optional:** Click in the top right corner of the live view page to open an auxiliary screen.

Note

No more than 3 auxiliary screens can be opened at the same time.

5. **Optional:** Perform the following operations on the toolbar of the live view window.

Capture Picture
Click to capture a picture. After capturing, you can click **Edit → Save and Archive** to save the picture as an archive.

Start Recording
Click to start the manual recording. After recording, you can click **Archive** to save the recorded file as an archive.

Instant Playback
Click to switch to the instant playback mode. Hover over the playback image and click to exit instant playback mode.

Digital Zoom
Click to enlarge the image.

Switch Stream Type
Click to switch the live view stream to main stream or sub stream.

Turn On/Off Audio
Click to turn on the audio and click to turn it off.

Add Tag
Click to add a tag for the video footage in a selected time range during live view.

Alarm Output
Click to display the Alarm Output Control page and turn on/off the alarm outputs of the connected camera.

Camera Status
Click to show the camera's recording status, signal status, connection number, etc.

Video Enhancement
Click to adjust the video image including brightness, saturation, etc.

Two-Way Audio
Click to start two-way audio with the camera to get the real-time audio from the device to realize voice talk with the person at the device.

Note

To perform two-way audio with the camera, you can also click the camera in the camera list, and click .

Fisheye Expansion
Click to enter the fisheye dewarping mode. In this mode, the video image is corrected and the geometric distortion caused by the fisheye camera lens is reversed.

Note

This function is available for fisheye cameras. For details, refer to ***View Dewarped Live View of Fisheye Camera*** .

Rotate Image Click to rotate the video image.

6.4.3 PTZ Control

With the PTZ Control functionality provided by the Portal, you can make cameras pan and tilt to required positions, zoom in or out live images, etc.

Note

Make sure the camera supports PTZ control.

On the top navigation bar, select **Video → Video Security** to enter the Video Security page.

Click **PTZ Control** in the bottom left corner.

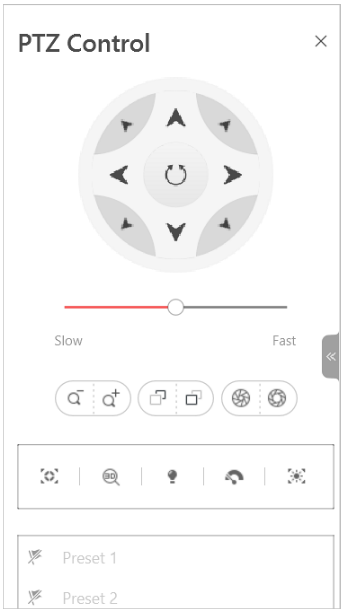


Figure 6-3 PTZ Control

The following buttons are available on the PTZ control panel:

	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.

⧉ ◻	Click **Focus +** move the focal point forward, and click **Focus -** to move the focal point backward.
⊛ ⊛	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.
Call the Preset	If you have configured a preset, hover the cursor on the preset and click ▷ to call it.

Configure a Preset

A preset is a predefined camera position which contains configurations for pan, tilt, zoom, focus, and other parameters. You can also set a virtual preset after enabling digital zoom.

Steps

1. On the top navigation bar, select **Video → Video Security** .

2. Start live view.

> **Note**
>
> Refer to ***Start Live View in Area Mode*** for details.

3. Click **PTZ Control** on the left to open the PTZ control panel.

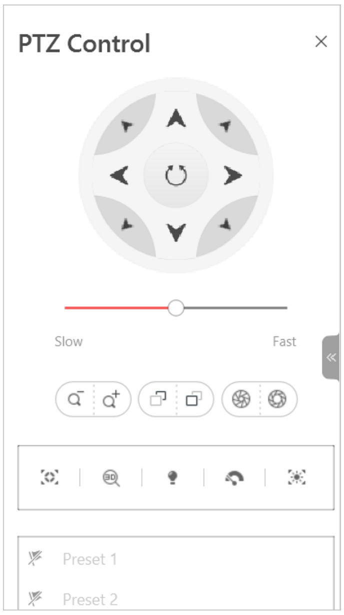


Figure 6-4 PTZ Control Panel

4. Use PTZ control to adjust the camera image to the desired direction and adjust other parameters such as zoom, focus, and iris to optimize the image.

5. Select a PTZ preset number from the preset list and click ✎ .

6. Create a name for the preset in the pop-up window.

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

Note

An unconfigured preset is gray, while a configured preset is highlighted.

8. **Optional:** After adding the preset, you can do one or more of the followings:

Call Preset	Double-click the preset, or select the preset and click ⊙ .
Edit Preset	Select the preset from the list and click ✎ .
Delete Preset	Select the preset from the list and click 🗑 .

6.4.4 Acknowledge Alarms During Live View

You can view and acknowledge alarms during live view.

1. On the top navigation bar, select **Video → Video Security** .
2. Click **Monitoring → Live View** .
3. When an alarm is triggered, the title bar of the live view window will turn red. Click the red title bar to view the alarm information and acknowledge the alarm.

6.4.5 View Dewarped Live View of Fisheye Camera

You can set center calibration and view dewarped live view of a fisheye camera. Dewarping refers to the process of perspective correction of an image, to reverse the effects of geometric distortion caused by the fisheye camera lens. It allows you to cover a wide area with a single device and get a "normal" view of an otherwise distorted or reversed image. Also, during live view, you can perform more operations such as adjusting view angle and zooming in/out.

Steps

1. Start live view of a fisheye camera.

Note

For details, refer to ***Start Live View in Area Mode*** .

2. On the toolbar of display window, click ⊠ to enter the fisheye dewarping mode and view live view.

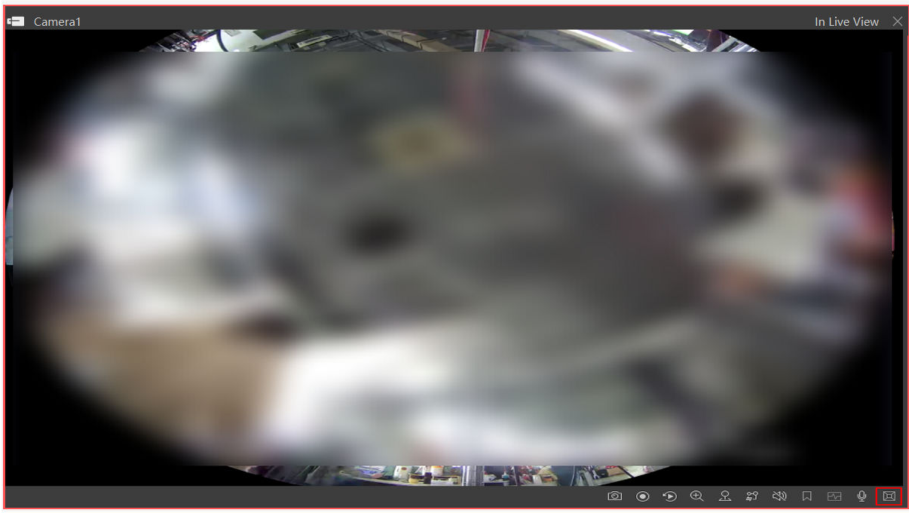


Figure 6-5 Fisheye Dewarping

3. **Optional:** Click ⊠ → ⊠ to set the mounting type and the expanding mode of the fisheye camera as needed.
4. **Optional:** Perform the following operations.

Adjust View Angle	Click on a point, and drag the video to adjust the view angle.
Zoom in/out View	Hover the cursor over the live video, and scroll the mouse wheel to zoom in or out the view.
Perform PTZ Control	Use the PTZ panel on the left side to perform PTZ control of the camera. **Note** Setting pattern is not supported by fisheye cameras.
Configure a Preset	You can configure a preset on the PTZ control panel. For details, refer to ***Configure a Preset*** .

6.5 Playback

The video files stored on the local storage devices and on the cloud can be searched and played back remotely through via web browser.

6.5.1 Start Playback in Area Mode

You can search for and play back the videos stored on the local storage devices and on the cloud remotely via the Portal.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Click **Monitoring → Camera** on the top.
3. Click **Playback** to enter the playback page.
4. Drag an area or a camera to the display window, or double-click the camera or area to play the recorded videos of the specified camera(s) in the selected window.

   Note

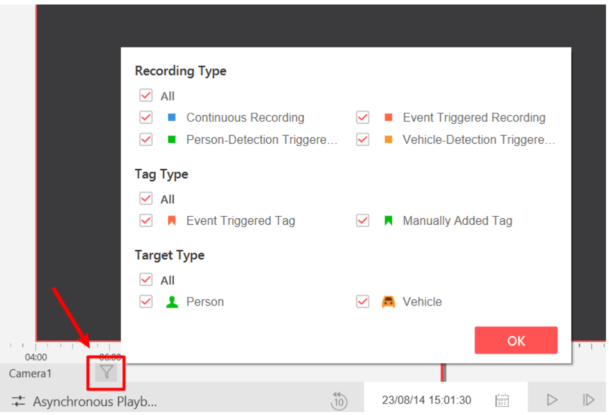
   The playback window supports up to 16 channels.

   Today's recorded video files of the selected camera(s) will be played.
5. Click on the toolbar to set the date and time.

   After selecting the date and time, the matched video files will be played automatically in the display window.
6. **Optional:** Click on the toolbar to filter videos for playback.

   Note

   - You can filter videos by recording type (continuous recording, event triggered recording, person-detection triggered recording, and vehicle-detection triggered recording), tag type, target type, and storage location. The filtered color tags will be displayed on the timeline.
   - For person-detection triggered recordings and vehicle-detection triggered recordings, you can view the captured pictures of the recordings.



Recording Type

☑ All

☑ Continuous Recording ☑ Event Triggered Recording

☑ Person-Detection Triggere... ☑ Vehicle-Detection Triggere...

Tag Type

☑ All

☑ Event Triggered Tag ☑ Manually Added Tag

Target Type

☑ All

☑ Person ☑ Vehicle

Figure 6-6 Filter Videos for Playback

7. Play back videos in the specified time period by timeline or thumbnail.
   - Drag the timeline forward or backward to the position of the desired video segment.
   - Move the cursor over the timeline to take a quick view of video thumbnails (if supported by the device) and click a video thumbnail to play the specific video segment.

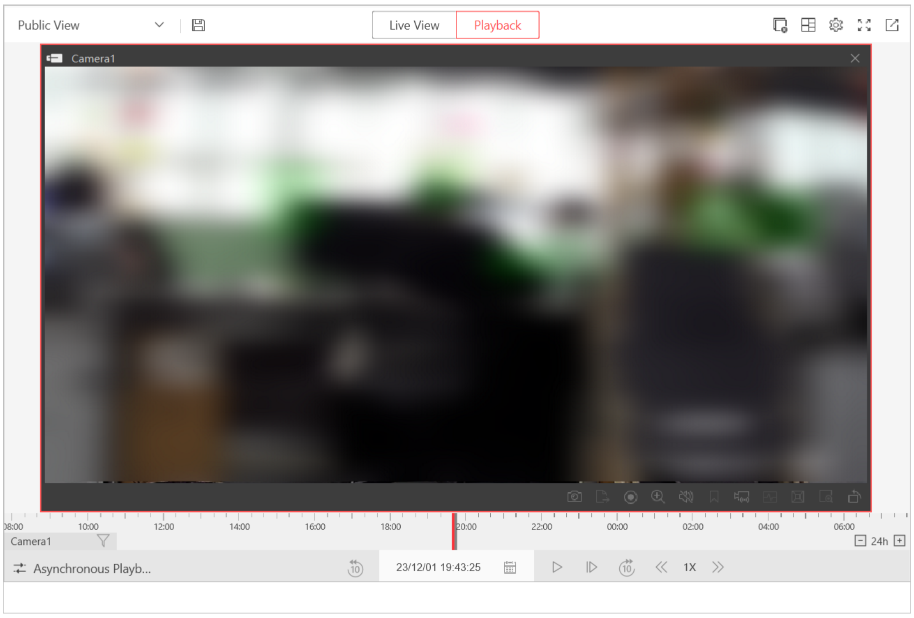


Figure 6-7 Playback

Note

You can click » or « to fast forward or fast reverse the video.

8. **Optional:** Click in the top right corner of the playback page to open an auxiliary screen.

Note

No more than 3 auxiliary screens can be opened at the same time.

9. **Optional:** Perform the following operations on the playback toolbar.

Capture a Picture

Click to capture a picture.

Export Video

Click to open the Export pane. Select the footage to be exported, and then set the **Download Time**, **File Type**, and text label to export the video footage.

Note

If the failure happened or no video exported, a window will pop up to remind you of stopping playback before exporting. After the playback is stopped, the window will display the image of the last frame.

Start Recording

Click to start the manual recording. After recording, you can click **Archive** to save the recorded file as an archive.

Digital Zoom

Click to enlarge the image.

Enable/Disable Audio

Click to enable audio of the video. Click again to disable.

Add Tag
Click to open the Add Tag pane. Select the video footage and tag time and click **Save** to add a tag for the selected footage.

Video Enhancement
Click to adjust the video image including brightness, saturation, etc.

View Camera Status
Click to view key parameters, status details, and basic introduction of the camera.

Fisheye Expansion
Click to enter the fisheye dewarping mode. In this mode, the video image is corrected and the geometric distortion caused by the fisheye camera lens is reversed.

Note

This function is available for fisheye cameras.

Create Zooming Area
Click and draw a rectangle area in the live video image. The area created will be displayed in a new window.

Rotate Image
Click to rotate the video image.

Archive Captured Picture or Clipped Video
Click **Archive** or **Edit → Save and Archive** on the pop-up window after capturing a picture or clipping the video to open the Archive window. Set the archive name, archive tag, archive level, etc., and click **Save** to archive the captured picture or clipped video.

6.5.2 Start Playback in View Mode

You can quickly start the playback of the cameras managed in a view.

Before You Start
Make sure you have added at least a view. Refer to ***Add a View*** for details.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Click **Monitoring → View** to enter the view page.
3. Click **Playback** to enter the playback window.
4. Start playback of the cameras related to the view.
   - Double click a view.
   - Move the mouse cursor to a view, and click ··· → **Play** beside the view name.

   Note

   You can switch the added views from the drop-down list in the upper-left corner above the playback window.
5. **Optional:** Click in the top right corner of the playback page to open an auxiliary screen.

Note

No more than 3 auxiliary screens can be opened at the same time.

6. **Optional:** Perform the following operations on the toolbar of the playback window.

Capture Picture
Click to capture a picture.

Export Video
Click to open the Export pane. Select the footage to be exported, and then set the **Download Time**, **File Type**, and text label to export the video footage.

Note

If the failure happened or no video exported, a window will pop up to remind you of stopping playback before exporting. After the playback is stopped, the window will display the image of the last frame.

Start Recording
Click to start the manual recording. After recording, you can click **Archive** to save the recorded file as an archive.

Digital Zoom
Click to enlarge the image.

Enable/Disable Audio
Click to enable audio of the video. Click again to disable.

Add Tag
Click to open the Add Tag pane. Select the video footage and tag time and click **Save** to add a tag for the selected footage.

Video Enhancement
Click to adjust the video image including brightness, saturation, etc.

View Camera Status
Click to view key parameters, status details, and basic introduction of the camera.

Fisheye Expansion
Click to enter the fisheye dewarping mode. In this mode, the video image is corrected and the geometric distortion caused by the fisheye camera lens is reversed.

Note

This function is available for fisheye cameras. For details, refer to ***View Dewarped Live View of Fisheye Camera*** .

Create Zooming Area
Click and draw a rectangle area in the live video image. The area created will be displayed in a new window.

Rotate Image
Click to rotate the video image.

Archive Captured Picture or Clipped Video
Click **Archive** or **Edit → Save and Archive** on the pop-up window after capturing a picture or clipping the video to open the Archive window. Set the archive name, archive tag, archive level, etc., and click **Save** to archive the captured picture or clipped video.

6.5.3 Synchronous Playback

You can play the video files of different cameras synchronously.

Steps

1. On the top navigation bar, select **Video → Video Security** .

2. Click **Monitoring → Playback** to enter the playback page.

3. Start normal playback of at least two cameras.

4. Click **Synchronous Playback** on the lower left to enable the synchronous playback.

The cameras displayed in Playback will start synchronous playback.

5. Optional: Click **Asynchronous Playback** on the lower left to disable synchronous playback.

6. Optional: Click ▷ or ◁ to perform normal or reverse playback.

7. Optional: Click |▷ or ◁| to perform single-frame normal or reverse playback.

Note

- No more than 16 cameras are allowed in single-frame normal and reverse playback.
- If you pause the play for one camera, others will be paused in the synchronous playback mode.

6.5.4 Play Back Videos Stored on the Cloud

You can play back the videos stored on the cloud, which are uploaded to the cloud by Hik-ProConnect boxes from their linked channels or by NVRs from their linked channels for which cloud storage has been enabled.

Note

- Make sure that you have the permission to play back videos.
- The cloud storage feature is only available in some countries/regions. Please contact Hikvision for details.

For detailed steps for playback, refer to ***Start Playback in Area Mode*** .

6.6 Set Video Parameters

You can set network parameters, picture file format, file saving path, and display parameters.

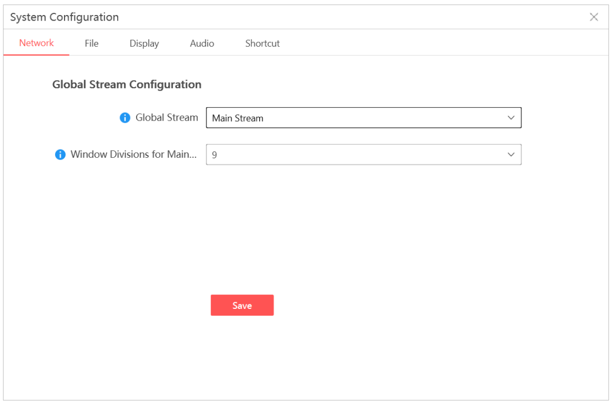
6.6.1 Set Network Parameters

You can set a global stream type for live view and window divisions for main stream.

Steps

1. On the top navigation bar, select **Video → Video Security** .

2. Click **Monitoring** on the top.
3. Click ⚙ in the top right corner of the Live View or Playback page to open the System Configuration window.



System Configuration

Global Stream Configuration

Global Stream: Main Stream

Window Divisions for Main...: 9

Figure 6-8 Set Network Parameters

4. Configure network parameters.

   Global Stream

   Select the default stream type for live view for global usage. If the network is in good condition, select main stream or sub-stream. If the network is in poor condition, select smooth stream.

   If the device doesn't support smooth stream, it will use sub-stream. If the device doesn't support sub-stream, it will use main stream.

   Window Divisions for Main Stream

   When the number of divided windows is smaller than the number you set, the live video will be displayed by main stream.

Note

The above parameters are valid for live view only.

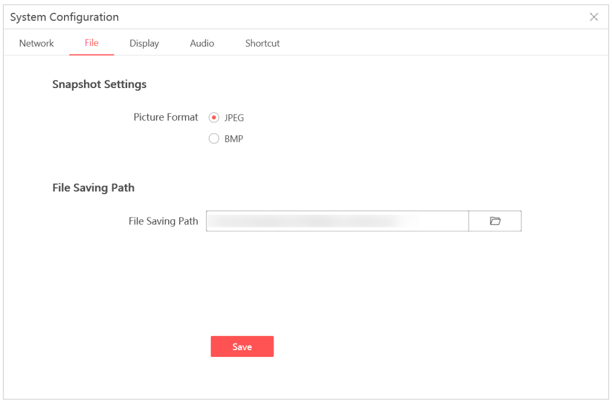
5. Click **Save**.

6.6.2 Set File Parameters

You can set the file format of pictures captured during live view or playback, and set a path for saving files.

Steps

1. On the top navigation bar, select **Video → Video Security** .
2. Click **Monitoring** on the top.
3. Click ⚙ in the top right corner of the Live View or Playback page to open the System Configuration window.
4. Click **File** to enter the file settings page.



System Configuration

Snapshot Settings

Picture Format ● JPEG ○ BMP

File Saving Path

File Saving Path

Figure 6-9 Set File Parameters

5. Configure file parameters.

Snapshot Settings

Select **JPEG** or **BMP** as the file format for the captured pictures.

File Saving Path

Set the saving path for files you will download to your computer (such as manually recorded video files and captured pictures).

6. Click **Save**.

6.6.3 Set Display Parameters

You can set display parameters, including the view scale, window scale, status of GPU hardware decoding, and whether to overlay VCA rule frames and highlight detected motions on the videos.

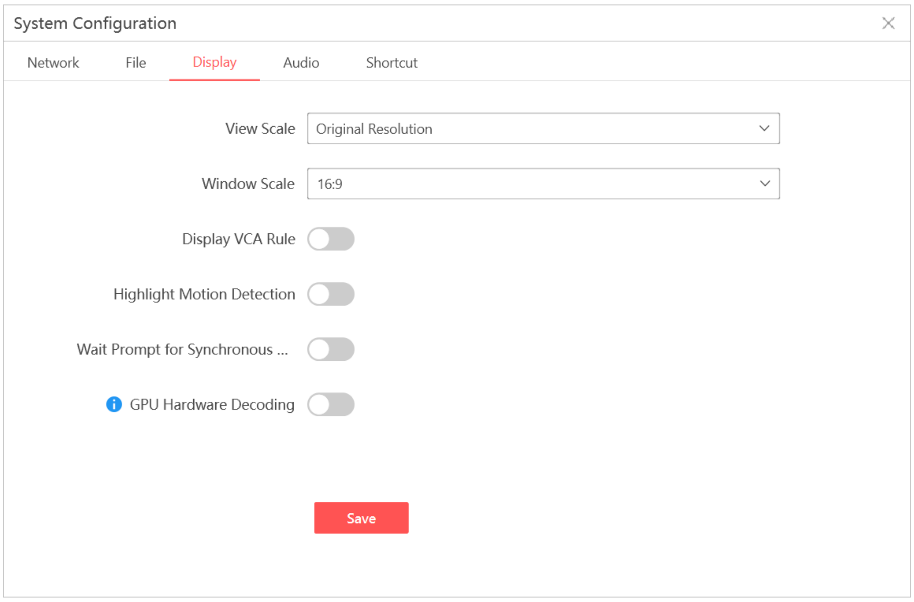
Steps

1. On the top navigation bar, select **Video → Video Security** .

2. Click **Monitoring** on the top.

3. Click ⚙ in the top right corner of the Live View or Playback page to open the System Configuration window.

4. Click the **Display** tab.



View Scale: Original Resolution

Window Scale: 16:9

Display VCA Rule

Highlight Motion Detection

Wait Prompt for Synchronous ...

GPU Hardware Decoding

Figure 6-10 Set Display Parameters

5. Configure the display parameters.

View Scale

Set the scale of the video. You can set it to **Original Resolution** or **Full Screen**.

Window Scale

Set the scale of the window. You can set it to **4:3**, **16:9**, or **Full Screen**.

Note

For smooth operation, dragging a window will be disabled after you set it to **Full Screen**.

Display VCA Rule

When switched on, frames of VCA (Video Content Analysis) rules configured on the devices will be overlaid on the videos. Based on the frames, you can quickly recognize the targets that trigger alarms and improve the efficiency of alarm reviewing.

Highlight Motion Detection

When switched on, detected motions will be highlighted on the videos. Based on the highlights, you can quickly recognize the targets that trigger alarms and improve the efficiency of alarm reviewing.

Wait Prompt for Synchronous Playback

When switched on, a wait-for-play prompt will be displayed for cameras with recordings at a time later than the time indicated by the current time pointer in synchronous playback mode.

GPU Hardware Decoding

When switched on, GPU decoding is enabled for live view and playback to save CPU resources. When the performance of the graphic card is good, you can enable GPU decoding to lower the computer's performance consumption. It is not recommended to enable this function if the graphic card's performance is poor.

Note

- Your computer must support GPU decoding.
- After enabling GPU decoding, restart live view and playback for GPU decoding to take effect.
- If the client shows a blurred screen after enabling GPU decoding, disable GPU decoding.
- If GPU decoding is enabled, overlaying transaction information on live view and playback image is not supported.

6. Click **Save**.

6.6.4 Set Audio Parameters

You can enable auto turning on audio, then the audio will automatically turn on when you start live view or playback.

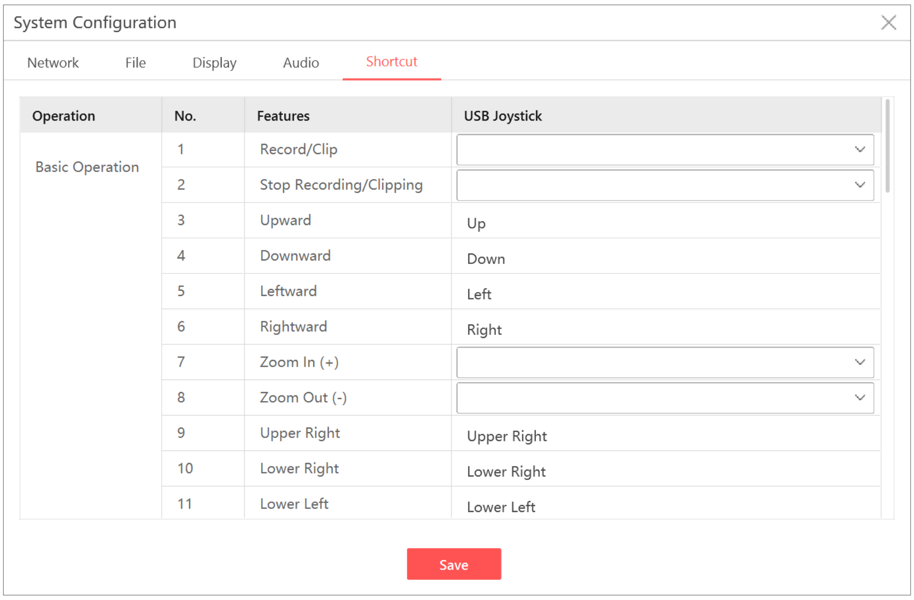
1. On the top navigation bar, select **Video → Video Security** .
2. Click **Monitoring** on the top.
3. Click ⚙ in the top right corner of the Live View or Playback page to open the System Configuration window.
4. Click **Audio** to enter the audio settings page.
   You can check **Enable** to auto turn on audio. If enabled, the audio will be automatically turned on when you start live view or playback.
5. Click **Save** to save the settings.

6.6.5 Set Shortcuts for USB Joysticks

You can connect a USB joysticks to the computer that runs the Portal to do controls and operations quickly and conveniently via the configured shortcuts during live view and playback.

Steps

1. On the top navigation bar, click **Video → Video Security → Monitoring** .
2. Click ⚙ in the top right corner of the Live View or Playback page to open the System Configuration window.
3. Click **Shortcut** to enter the shortcut settings page.



Operation	No.	Features	USB Joystick
Basic Operation	1	Record/Clip	
	2	Stop Recording/Clipping	
	3	Upward	Up
	4	Downward	Down
	5	Leftward	Left
	6	Rightward	Right
	7	Zoom In (+)	
	8	Zoom Out (-)	
	9	Upper Right	Upper Right
	10	Lower Right	Lower Right
	11	Lower Left	Lower Left

Figure 6-11 Set Shortcuts for USB Joysticks

4. Select a feature and select a compound key number from the drop-down list as the shortcut for the feature.

Example

If you select **1** as the shortcut for starting recording or clipping, you can press the **1** key on the USB joystick connected to the computer that runs the Portal to quickly start recording or clipping.

5. Optional: Repeat the previous step to set different shortcut keys for different features.

6. Click **Save**.

6.7 Video Search

In this module, you can search for videos stored in the local storage and on the cloud storage server by time, camera (no more than 16 selected), and content (history video footage, video with person/vehicle detected, tag). You can also export the searched video(s) to the local PC or save them as archives.

Note

Cloud storage is only available in some countries/regions. Please contact Hikvision for details.

6.7.1 Search for Video Footage

You can search for video footage by time and camera.

Steps

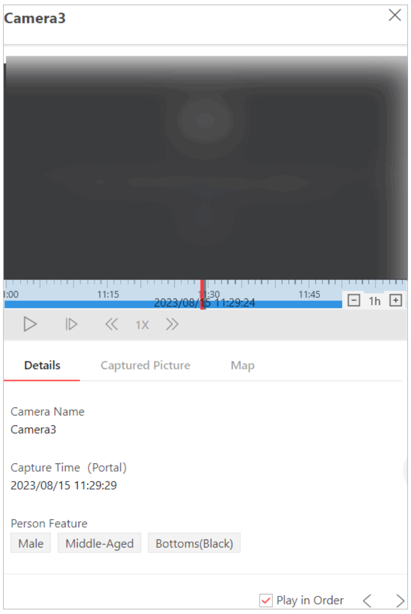
1. On the top navigation bar, select **Video → Video Search** to enter the Intelligent Video Search page.
2. Set the time range.
3. Select **Video Footage** as the content.
4. Check cameras of interest.

   Note

   No more than 16 cameras can be selected.
5. Click **Search**.

   The matched videos are displayed on the right.
6. **Optional:** Perform the following operations on the matched results as needed.

Operation	Description
Switch Display Mode	Click ≡ / ▦ to switch between thumbnail mode and list mode for display of matched videos. **Note** In thumbnail mode: You can adjust the thumbnail size in the bottom right corner.
View Result Statistics	The result statistics of matched results are displayed at the bottom. • In the top right corner of the result statistics, click ⊟ / ⊞ to reduce/ increase the displayed time range. • You can also double-click a bar on the timeline to display the list of videos within a specific time period. • Click **Video Footage**, **Person Detected**, **Vehicle Detected**, and **Tag** to filter tags.
Filter Results	You can further filter the matched results by footage length and storage type.
View Video Details	Click a video and the video details pane will be displayed on the right. • You can play back the video by single frame. Speed playback by 1/16X to 16X is supported. • You can view the video details including the camera name, start time and end time, and video length; you can also view the camera location on the map. See details in ***Add Hot Spot on Map*** for map configuration.



Camera Name
Camera3

Capture Time (Portal)
2023/08/15 11:29:29

Person Feature
Male | Middle-Aged | Bottoms(Black)

Figure 6-12 Details for Video Footage

Export Video Select the video(s) and click **Export** to export the video(s) to the local PC.

Note

You can select up to 10 videos at a time.

Archive Video Select one or multiple videos and click **Archive** to save the video(s) as one archive. After they are archived, you can manage them in Archive Management. See details in ***Archive Management*** .

Note

You can select up to 10 videos at a time.

6.7.2 Search for Vehicle/Person-Detected Videos

You can search for vehicle/person-detected videos by time and camera.

1. On the top navigation bar, select **Video → Video Search** to enter the Video Search page.
2. Set the time range.
3. Select **Person and Vehicle Detected** as the content.
4. Select **All Cameras** or **Specified Camera**.
5. Click **Search**.
6. Perform the following operations on the matched results as needed.

Operation	Description
Switch Display Mode	Click ≡ / ▦ to switch between thumbnail mode and list mode for display of matched results. **Note** In thumbnail mode, you can adjust the thumbnail size in the bottom right corner.
View Result Statistics	The result statistics of matched results are displayed at the bottom. - In the top left corner of the result statistics, you can view the max. number of captured pictures within a time period. - In the top right corner of the result statistics, you can reduce/increase the displayed time range by clicking ⊟ / ⊞ . - You can hover over each bar in the bar chart to view the number of captured pictures within a specific time period. - You can double-click each bar (30-second range) in the bar chart to display the list of captured pictures within a specific time period.
Filter Results	- Person detected: You can further filter the matched results by top color, bottom color, whether wearing glasses/hat/mask/ backpack, etc. - Vehicle detected: You can further filter the matched results by brand, vehicle type, country/region, color, and license plate number.
View Video Details	Click a captured picture and the video details pane will be displayed on the right. - You can watch the video and the video will automatically jump to 5 seconds before the picture captured. You can play back the video by single frame. Speed playback by 1/16X to 16X is supported. - You can view the video details including the camera name, captured time, license plate

Operation	Description
	No., and vehicle attributes / person feature; you can also view the camera location on the map. See details in ***Add Hot Spot on Map*** for map configuration.
Export Video	Select the captured picture(s) and click **Export** to export the 1-minute video(s) (from 5 seconds before the capture to 55 seconds after the capture by default) in which the picture is captured to the local PC. **Note** You can select up to 10 pictures at a time.
Archive Video	Select one or multiple captured pictures and click **Archive** to save the 1-minute video(s) (from 5 seconds before the capture to 55 seconds after the capture by default) in which the picture is captured as one archive. After videos are archived, you can manage them in Archive Management. See details in ***Archive Management*** . **Note** You can select up to 10 pictures at a time.

6.7.3 Search for Tagged Videos

If you have added tags to videos, you can search for videos by tag.

Before You Start

Make sure you have added tags to videos.

Steps

1. On the top navigation bar, select **Video → Video Search** to enter the Video Search page.
2. Set the time range.
3. Select **Tag** as the content.
4. Select **All Cameras** or **Specified Camera**.
5. Click **Search**.

   The matched videos are displayed on the right.
6. **Optional:** Perform the following operations on the matched results as needed.

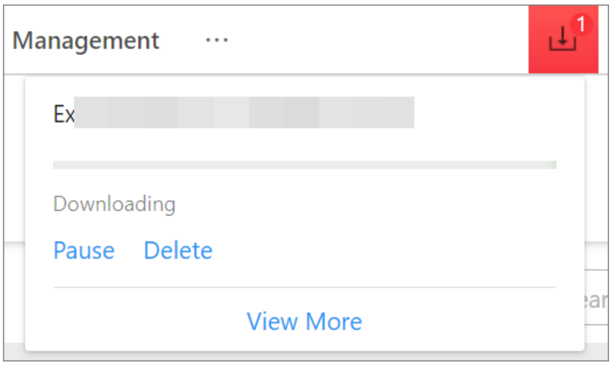
Operation	Description
View Result Statistics	The result statistics of matched results are displayed at the bottom. • In the top left corner of the result statistics, you can view the max. number of tags within a time period. • In the top right corner of the result statistics, you can reduce/increase the displayed time range by clicking ⊟ / ⊞ . • You can hover over each bar in the bar chart to view the number of tags within specific time period. • You can double-click each bar (30-second range) in the bar chart to display the list of tags within a specific time period.
Filter Results	You can further filter the matched results by tag type, storage type, and tag name/description.
View Tag Details	Click a tag name and the tag details pane will be displayed on the right. • You can play back the tagged video by single frame. Speed playback by 1/16X to 16X is supported. • You can view the tag details including the tag name, tag description, tag time, tag type, camera name and storage type; you can view the camera location on the map. See details in ***Add Hot Spot on Map*** for map configuration.
Edit/Delete Tag	On the top of the tag details pane, click **Edit**/**Delete** to edit or delete the tag.
Export Tagged Video	Select the video(s) and click **Export** to export the video(s) to the local PC. **Note** You can select up to 10 videos at a time.
Archive Tagged Video	Select one or multiple videos and click **Archive** to save the video(s) as one archive. After they are archived, you can manage them in Archive Management. See details in ***Archive Management*** . **Note** You can select up to 10 videos at a time.

6.8 Download Task Management

You can view the ongoing or completed download task information and manage all the tasks (e.g., video downloading, archive downloading), such as stopping, resuming, and deleting in the Download Center.

The Entry of Download Center

In the top right corner of the Portal, hover the cursor over ⤓ to show a floating window, which will display the latest 5 tasks. The displayed information vary with different task types. Refer to the table below for details.



Management ···

Ex[redacted]

Downloading

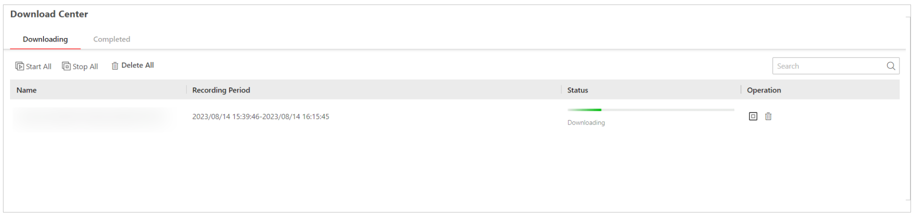
Figure 6-13 Floating Window on the Download Center Entry

Table 6-1 Task Types and Displayed Information

Task Type	Displayed Information
Downloading Task	File name, downloading status, downloading progress, downloading speed, remaining time, and operations (**Stop**/ **Delete**).
Paused Task	File name, downloading status, downloading progress, and operations (**Start**/**Delete**).
Waiting Task	File name, downloading status, and operations (**Stop**/**Delete**).
Failed Task	File name, downloading status, and operations (**Retry**/**Delete**).
Completed Task	File name, completion time, and operations (**Open File** / **Delete**).

Downloading Task

Click ⤓ to enter the Download Center page, and click **Downloading Task** to enter the corresponding page.



Download Center

Name	Recording Period	Status	Operation
[redacted]	2023/08/14 15:39:46-2023/08/14 16:15:45	Downloading	⊡ 🗑

Figure 6-14 Downloading Task Page

On the Downloading page, you can:

- View the downloading tasks, including the saving path, the file size, and the start time and end time of the video footage to be downloaded.

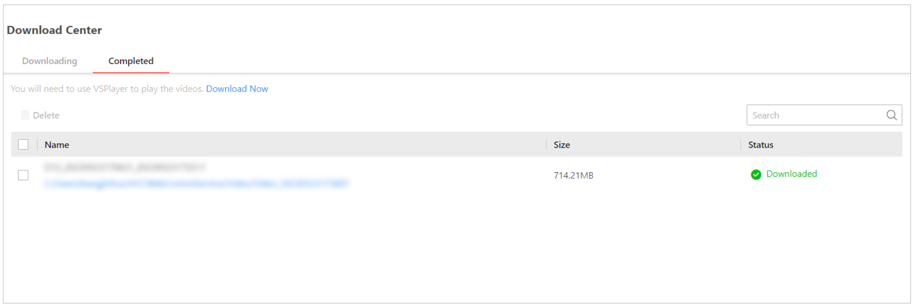
Note

If the file to be downloaded is not a video, no content will be displayed in the Recording Period column.

- Click ⊡ in the Operation column to stop a downloading task or click **Stop All** at the top of the task list to stop all downloading tasks.
- Click ▷ in the Operation column to start a downloading task or click **Start All** at the top of the task list to start all downloading tasks.
- Click 🗑 in the Operation column to delete a downloading task or click **Delete All** at the top of the task list to delete all downloading tasks.
- Enter a keyword in the Search field of the top right corner to search for downloading tasks.

Completed Task

Click ⤓ to enter the Download Center page, and click **Completed Task** to enter the corresponding page.



You will need to use VSPlayer to play the videos. Download Now

□ Name	Size	Status
□ [redacted]	714.21MB	✓ Downloaded

Figure 6-15 Completed Task Page

On the Completed page, you can:

- View the completed tasks.
- Click the saving path under the task name to view the downloaded files in the folder.
- Click **Download Now** on the top of the list to download the VSPlayer.
- Check the completed task(s) and click **Delete** at the top of the task list to delete the selected tasks.
- Enter a keyword in the Search field of the top right corner to search for completed tasks.

Chapter 7 Access Control Management

On the Portal, the Administrator can add access control devices to the System, group resources into different areas, and define access permission by creating an access level to group doors. After assigning access levels to persons, persons will be authorized to access doors in the access levels with their credentials during the authorized time period. Moreover, you can create temporary passes for people (e.g., visitors) with temporary access needs.

Note

The entry of creating temporary passes in the Access Control module is **Access Control → Temporary Pass Management** . For the detailed operations, refer to ***Create Temporary Pass*** .

7.1 Configurations Before Access Control Management

Before using the access control, users should configure some related parameters, including holidays, access schedule templates, general parameters, and subscribing to device and access events.

7.1.1 Set Holidays for Schedule

You can add the holiday to define the special days that can adopt a different schedule or access schedule. You can set a regular holiday and an irregular holiday according to the actual scene.

Steps

1. On the top navigation bar, click **Access Control → Access Control Configuration → Holiday Settings** .
2. Click **Add**.
3. Enter a holiday name.
4. Select a holiday type, and set the following parameters.

   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**.

5. Click **Add**.
6. **Optional:** Perform the following operations.

Edit a Holiday	In the holiday list, click ✎ to edit the settings of a holiday.
Delete a Holiday	In the holiday list, click 🗑 to remove it from the holiday list.

7.1.2 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.

Steps

1. On the top navigation bar, click **Access Control → Access Control Configuration → Access Schedule Template** .
2. Click + to create a blank template.
3. Configure the template in the template information panel on the right.

   Name

   Create a name for the template.

   Copy from

   Optionally, you can select to copy the settings from existing templates.
4. In the **Weekly Schedule Template** box, set a schedule pattern for each day.
   1) Click **Authorize** and select or draw in the box to define the authorized time periods.
   2) **Optional:** 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. **Optional:** Set a holiday schedule if you want different schedules for specific days.

   Note

   Holiday schedule has a higher priority than weekly schedule.

1) Click **Add Holiday**.
2) Select existing holiday templates, or click **Add New** to create a new holiday template (see ***Set Holidays for Schedule*** for details).
3) Click **Add**.
4) Set a schedule pattern for holidays.

6. Click **Add** to save the template.

7. Optional: Perform further operations on added templates.

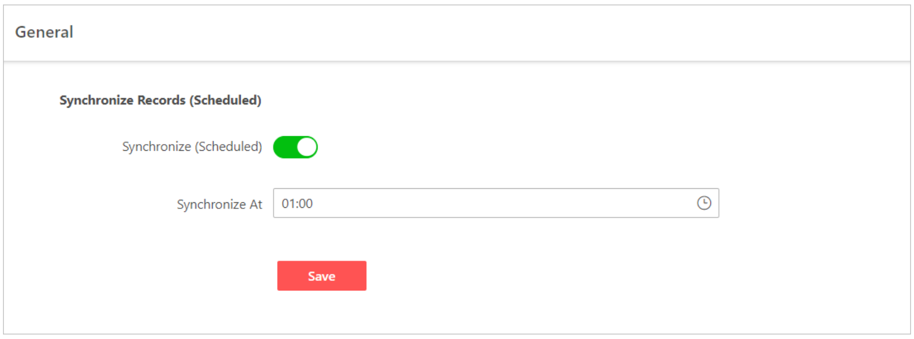
View and Edit Template Details	Click a template item to view and edit its configurations.
Delete Template	Click a template item and click 🗑 to delete it.

7.1.3 Set General Parameters

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.

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

In the Synchronize Records (Scheduled) area, switch on **Synchronize (Scheduled)**, set a fixed time, and click **Save** to synchronize access records from the devices to the system regularly.



General

Synchronize Records (Scheduled)

Synchronize (Scheduled) ●

Synchronize At 01:00

Figure 7-1 General Parameters

7.1.4 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.

Follow the steps to enable the subscription for device and access events.

Steps

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. **Optional:** 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. For details, see ***Search for Access Records*** and ***Search for Data Recorded on Device*** .

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

What to do next

View the real-time event records of the device and access events that you subscribe to. For details, see ***View Real-Time Access Events*** .

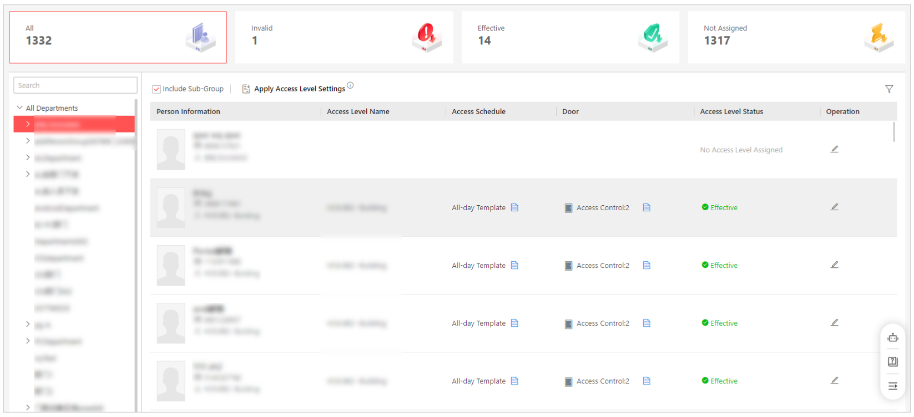
7.2 Manage Access Level

In access control, access level is a group of access points. Assigning access level to persons, departments, or access groups can define the access permission that which persons can get access to which access points during the authorized time period.

7.2.1 Access Level Overview

The Access Level Overview page displays access level status statistics and persons' access level details. You can filter persons by different conditions or edit an access level.

On the top navigation bar, click **Access Control → Access Level → Access Level Overview** .



All 1332

Invalid 1

Effective 14

Not Assigned 1317

Search

All Departments

[redacted]

☑ Include Sub-Group | Apply Access Level Settings

Person Information	Access Level Name	Access Schedule	Door	Access Level Status	Operation
[redacted]				No Access Level Assigned	
[redacted]	[redacted]	All-day Template	Access Control:2	✓ Effective	
[redacted]	[redacted]	All-day Template	Access Control:2	✓ Effective	
[redacted]	[redacted]	All-day Template	Access Control:2	✓ Effective	
[redacted]	[redacted]	All-day Template	Access Control:2	✓ Effective	

Figure 7-2 Access Level Overview

- On the top, you can learn the access level status.

  Invalid

  Includes access levels failed to be applied and access levels not applied yet.

Not Assigned

Access levels not assigned to persons or departments.

- Click ▽ to filter persons by different conditions.
- Click 🗎 in the Access Schedule column to view the details of access schedule.
- Click 🗎 in the Door column to view details of a door.
- Click 🗎 in the Access Level Status column to view the applying failure details of access level.
- Click ✎ to edit an access level.
- Click **Apply Access Level Settings** to apply access levels to devices manually. See ***Manually Apply Access Level Settings to Device*** .

7.2.2 Add Access Level

To define the access permission, you need to add an access level to group the access points.

Steps

1. On the top navigation bar, click **Access Control → Access Level → Manage Access Level** .

2. Click **Add** to enter the Add Access Level page.

3. Create a name for the access level.

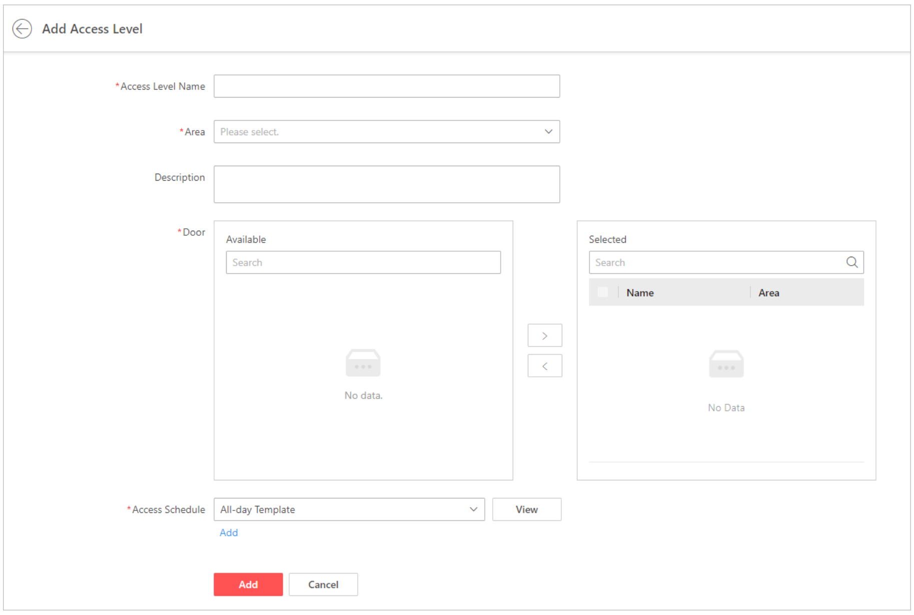
4. Select an area.

5. Optional: Edit the description for the access level.

6. Select the door(s) to add to the access level.

1) In the **Available** list, select the access point(s) you want to add to the system and click > . You can view your selection in the **Selected** list.

2) **Optional:** In the **Selected** list, select the access point(s) that you no longer want to add to the system, and click < to undo selection.



*Access Schedule: All-day Template

Figure 7-3 Add Access Level

7. Select an access schedule to define in which time period, persons are authorized to access the access points you select in the previous step.
8. Click **Add** to add the access level and return to the access level management page.
9. Optional: Perform further operations on the added access level(s).

Edit Access Level	Click the name of an access level to view and edit its configurations.
Delete Access Level	Select an access level and click **Delete** to delete it.
Delete All Access Levels	Click ⌄ → **Delete All** to delete all access levels.

Note

The access levels with the tag of "System" cannot be deleted here because these access levels are automatically generated for buildings in the Video Intercom module.

What to do next

You need to assign the access level to persons, so that the assignees can have the access to the access points in the access level according to the access schedule. For details, refer to ***Assign Access Level*** .

7.2.3 Assign Access Level

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.

Assign by Department

You can assign access levels to departments, so that the persons in the department can have the access to the access points in the access levels.

Before You Start

- Make sure you have added departments and persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific departments.

Steps

1. On the navigation bar, select **Access Control → Access Level → Assign by Department** .
2. Do one of the following to assign access levels to departments.
   - Assign access levels to each department one by one.
      a. In the department list, click on a department.
      b. In the assigned access level pane on the right, click **Assign**.

c. In the Assign Access Level pane, select the access levels you want to assign to the selected department.
d. Click **Save**.

- Assign access levels to multiple departments at a time.
  a. Click **Batch Assign**.
  b. 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**.

  c. In access level list, select the access levels you want to assign to the departments.
  d. 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. For details, refer to ***Assign by Person*** .

The access level settings will be applied to devices automatically.

3. **Optional:** You can also apply access level settings to devices manually or regularly.

Note

For details, refer to ***Manually Apply Access Level Settings to Device*** and ***Set General Parameters*** .

4. **Optional:** To unassign an access level from the department, select the access level and click **Unassign**. To unassign all access levels, click → **Unassign All** .

Assign by Person

You can assign access levels to persons, so that the assignees can have the access to the access points in the access levels.

Before You Start

- Make sure you have added persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific persons.

Steps

1. On the top navigation bar, click **Access Control → Access Level → Assign by Person** .
2. Click **Assign Access Level** on the top.
3. On the Assign Access Level pane, click , select the persons, and click **Add**.

Note

To apply the access level settings of all persons, check **Select All Persons**.

4. Check access levels to assign.
5. Click **Save**.

   The access level settings will be applied to devices automatically.
6. **Optional:** You can also apply access level settings to devices manually or regularly.

   Note

   For details, refer to ***Manually Apply Access Level Settings to Device*** and ***Set General Parameters*** .
7. **Optional:** To unassign a person's access levels, select the person and click **Unassign**, then choose **Unassign All Access levels** or **Unassign Specified Access Levels**.

7.2.4 Manually Apply Access Level Settings to Device

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.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Assign Access Level*** .

Steps

1. On the top navigation bar, click **Access Control → Access Level → Access Level Overview** .
2. Click **Apply Access Level Settings**.
3. 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.
4. 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**.

7.3 Real-Time Monitoring

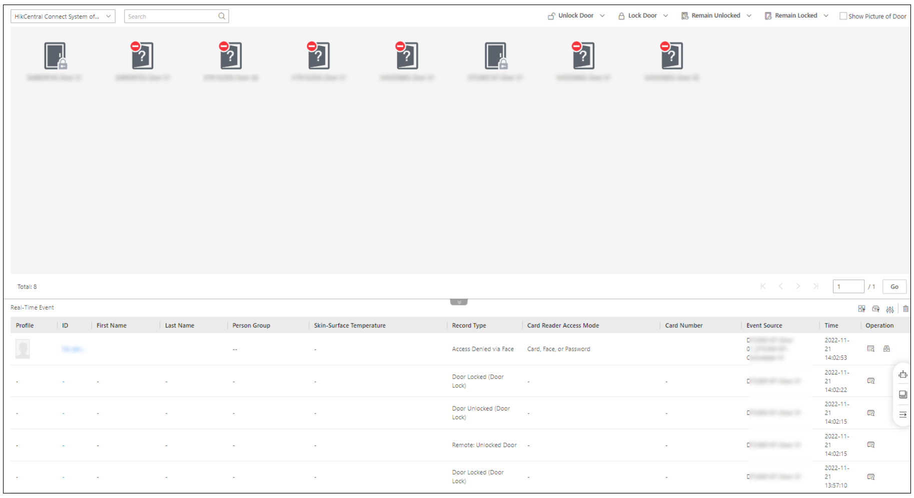
In this module, you can view the real-time events triggered by doors and control doors based on their status.

7.3.1 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** .



Profile	ID	First Name	Last Name	Person Group	Skin-Surface Temperature	Record Type	Card Reader Access Mode	Card Number	Event Source	Time	Operation
	[redacted]			--	-	Access Denied via Face	Card, Face, or Password		[redacted]	2022-11-21 14:02:53	
-	-	-	-	-	-	Door Locked (Door Lock)	-	-	[redacted]	2022-11-21 14:02:22	
-	-	-	-	-	-	Door Unlocked (Door Lock)	-	-	[redacted]	2022-11-21 14:02:15	
-	-	-	-	-	-	Remote: Unlocked Door	-	-	[redacted]	2022-11-21 14:02:15	
-	-	-	-	-	-	Door Locked (Door Lock)	-	-	[redacted]	2022-11-21 13:57:10	

Figure 7-4 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.

7.3.2 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. See details in ***Manage Access Control Devices in Area*** .

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** .

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. For details about setting the period, see ***Edit a Door in Area*** . • 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. For details about super users' permission, view ***Role and User Management*** . • 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.

7.4 Record Search

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.

7.4.1 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.

Steps

1. On the top navigation bar, click **Access Control → Search → Access Record Retrieval** .

2. Optional: Import access records from devices to the System.

1) Click **Import Events**.
2) Select the devices from the list.
3) (Optional) Specify the time range.
4) Click **OK**.

3. Set conditions as needed.

Time

Specify the time range for record search.

Person

Select **Select Person** and click to select one or multiple persons, or select **Search by Person Name** / **Search Card No.** to enter a person name / card No. for record search.

Door

Select one or multiple doors, or you can select an area to select all doors in the selected area.

Record Type

Click to select one or multiple event types.

Authentication Result

Select **All**, **Access Granted**, or **Authentication Failed** as the search condition.

Skin-Surface Temperature Status

Switch on **Skin-Surface Temperature Status** and select **Normal** or **Abnormal** as the search condition.

Wearing Mask or Not

Switch on **Wearing Mask or Not** and select **Wearing Mask** or **No Mask** as the search condition.

4. Click **Search**.

The matched records are displayed.

5. Optional: Perform further operations.

Customize Columns to be Displayed	Click to customize the columns to be displayed.
View Record Details	Click the person name to view the record details.

Export a Single Record Click ⇥ in the Operation column to export the record to your local PC.

Export All Matched Records Click **Export** to export all matched records to your local PC.

7.4.2 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.

Steps

1. On the top navigation bar, click **Access Control → Search → Device Recorded Data Retrieval** .

2. Set conditions as needed.

Time

Specify the time range for record search.

Door

Switch on **Door**. Select one or multiple doors, or you can select an area to select all doors in the selected area.

In the Record Type area, click ⊕ to select one or multiple event types.

Device

Switch on **Device**. Select one or multiple devices, or you can select an area to select all devices in the selected area.

In the Record Type area, click ⊕ to select one or multiple event types.

Alarm Input

Switch on **Device**. Select one or multiple alarm inputs, or you can select an area to select all alarm inputs in the selected area.

In the Record Type area, click ⊕ to select one or multiple event types.

3. Click **Search**.

The matched records are displayed.

4. Optional: Perform further operations.

Customize Columns to be Displayed Click ⚙ to customize the columns to be displayed.

Export a Single Record Click ⇥ in the Operation column to export the record to your local PC.

Export All Matched Records Click **Export** to export all matched records to your local PC.

Chapter 8 Time & Attendance

In the Attendance module, you can easily manage the time & attendance system of departments and check employees' attendance.

After completing the basic configuration (see ***Basic Configuration***), administrators of the company can view & assign schedules to persons (see ***Schedule Management*** , manage leave applications and attendance correction applications of employees (see ***Application Management***), and view & export various types of attendance reports (see ***View and Export Reports***).

Note

If you have upgraded the time and attendance service, the what's new of the upgraded version will pop up when you enter the module for the first time.

8.1 Basic Configuration

You can set basic parameters for the Attendance module, including selecting shift types and adding timetables for the corresponding shift types, configuring overtime rules and attendance rules, as well as configuring weekends, holidays, leave types, and report settings.

8.1.1 Select Shift Type

The platform provides two shift types: normal shift and flexible shift. You can select shift type(s) according to actual needs.

For entering the Attendance module for the first time, you should select at least one shift type. Refer to the following for the explanations of the two shift types.

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. That is, 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).

You can go to **Attendance → Basic Configuration → General** , and click **Edit** on the top of the page to edit the shift type if needed.

8.1.2 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.

Steps

1. On the top navigation bar, click **Attendance → Basic Configuration → General → Weekend** to define weekend.
2. Click the day(s) of interest to set it/them as a weekend.
3. Click **Save**.

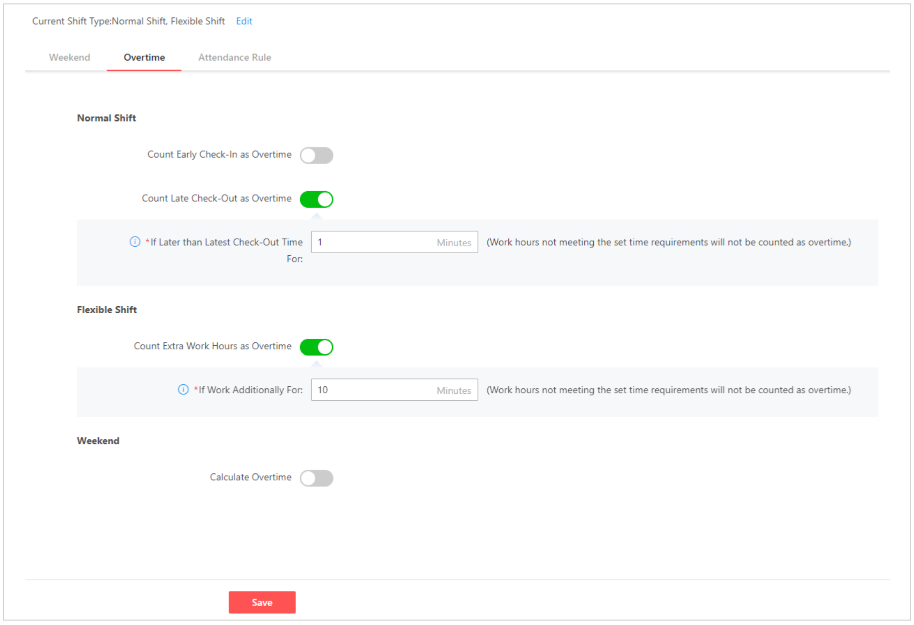
8.1.3 Define Overtime

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** .

Note

The contents displayed on the page may vary with the shift type you selected, so make sure you have selected the shift type you need. For details, refer to ***Select Shift Type*** .



Current Shift Type:Normal Shift, Flexible Shift

Normal Shift

Count Early Check-In as Overtime: off

Count Late Check-Out as Overtime: on

*If Later than Latest Check-Out Time For: 1 Minutes (Work hours not meeting the set time requirements will not be counted as overtime.)

Flexible Shift

Count Extra Work Hours as Overtime: on

*If Work Additionally For: 10 Minutes (Work hours not meeting the set time requirements will not be counted as overtime.)

Weekend

Calculate Overtime: off

Figure 8-1 Define Overtime

Normal Shift

Count Early Check-In as Overtime

For normal shifts, you may enable the parameter and specify how early is considered as working overtime. For example, if you enter 30 here, and a person checks in 40 minutes earlier than the earliest check-in time, the overtime duration will be 40 minutes.

Count Late Check-Out as Overtime

For normal shifts, you may enable the parameter and specify how late is considered as working overtime. For example, if you enter 30 here, and a person checks out 40 minutes later than the latest check-in time, the overtime duration will be 40 minutes.

Flexible Shift

Count Extra Work Hours as Overtime

For flexible shifts, you may enable the parameter and specify how many extra minutes are considered as overtime. For example, if you enter 30 here, and a person works 40 minutes longer than the required work period, the overtime duration will be 40 minutes.

Weekend

Calculate Overtime

For weekends, you may enable the parameter and specify how many minutes are considered as overtime. For the definition of the weekend, refer to ***Define Weekend*** .

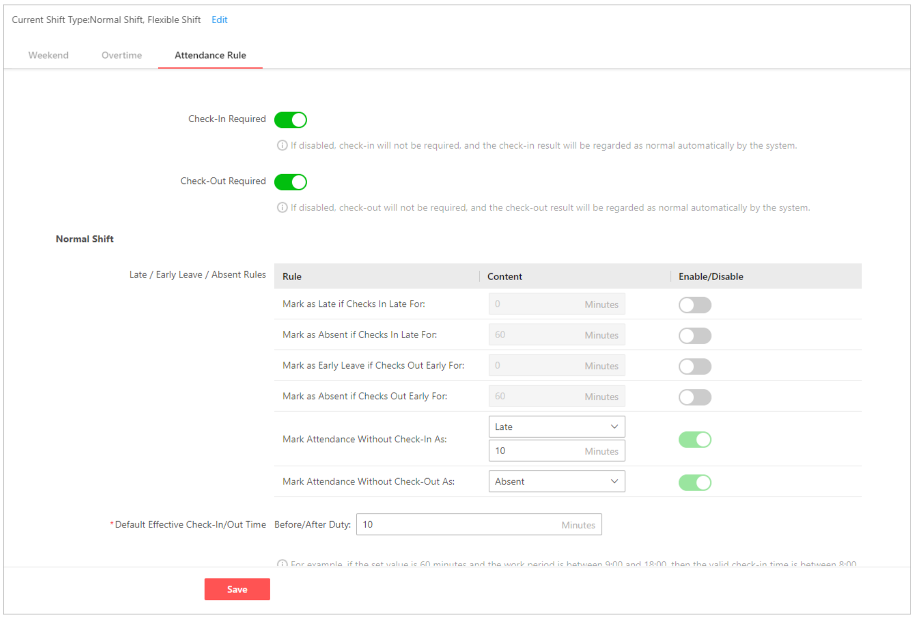
8.1.4 Configure Attendance Rule

Attendance rules define how attendance results will be marked for the employees based on whether they checked in/out and the specific time recorded for each check-in/out.

On the top navigation bar, click **Attendance → Basic Configuration → General → Attendance Rule** .

Note

The contents displayed on the page may vary with the shift type you selected, so make sure you have selected the shift type you need. For details, refer to ***Select Shift Type*** .



Current Shift Type:Normal Shift, Flexible Shift Edit

Check-In Required ●

ⓘ If disabled, check-in will not be required, and the check-in result will be regarded as normal automatically by the system.

Check-Out Required ●

ⓘ If disabled, check-out will not be required, and the check-out result will be regarded as normal automatically by the system.

Normal Shift

Late / Early Leave / Absent Rules

Rule	Content	Enable/Disable
Mark as Late if Checks In Late For:	0 Minutes	○
Mark as Absent if Checks In Late For:	60 Minutes	○
Mark as Early Leave if Checks Out Early For:	0 Minutes	○
Mark as Absent if Checks Out Early For:	60 Minutes	○
Mark Attendance Without Check-In As:	Late 10 Minutes	●
Mark Attendance Without Check-Out As:	Absent	●

*Default Effective Check-In/Out Time Before/After Duty: 10 Minutes

ⓘ For example, if the set value is 60 minutes and the work period is between 9:00 and 18:00, then the valid check-in time is between 8:00

Figure 8-2 Attendance Rule Configuration Page

Check-In Required

An employee is required to check in only if **Check-In Required** is switched on. If it is switched off, check-in is not mandatory and the attendance result of an employee will be marked as **Normal** even if there is no check-in record.

Check-Out Required

An employee is required to check out only if **Check-Out Required** is switched on. If it is switched off, check-out is not mandatory and the attendance result of an employee will be marked as **Normal** even if there is no check-out record.

Normal Shift

Late / Early Leave / Absent Rules

For normal shifts, you can define how attendance results that are not normal (i.e., late, early leave, and absent) are marked for the employees.

Table 8-1 Rule Configuration Explanation

Rule	Option	Description
Mark as Late if Checks In Late For	An integer no greater than 1440. Unit: min. **Note** The value you set for this rule should be less than that	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**.

Rule	Option	Description
	for marking late check-in as **Absent**.	
Mark as Absent if Checks In Late For	An integer no greater than 1440. Unit: min. **Note** The value you set for this rule should be greater than that for marking late check-in as **Late**.	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**.
Mark as Early Leave if Checks Out Early For	An integer no greater than 1440. Unit: min. **Note** The value you set for this rule should be less than that for marking early check-out as **Absent**.	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**.
Mark as Absent if Checks Out Early For	An integer no greater than 1440. Unit: min. **Note** The value you set for this rule should be greater than that for marking early check-out as **Early Leave**.	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 **Absent**.
Mark Attendance Without Check-In As	Absent/Late	• 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

Rule	Option	Description
		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. **Note** The rule is enabled by default and cannot be disabled if **Check-In Required** is enabled.
Mark Attendance Without Check-Out As	Absent / Early Leave	• 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. **Note** The rule is enabled by default and cannot be disabled if **Check-Out Required** is enabled.

Note

If checking in is not required, rules related to check-in will not be displayed. Likewise, rules related to check-out will not be displayed if checking out is not required.

Default Effective Check-In/Out Time

For normal shifts, you can set the default tolerance time for marking check-in/out as **Normal**. The value you enter here will be reflected on the Add Timetable pane when you add a timetable for a normal shift.

For example, if the value set for **Before/After Duty** is 60 minutes and the work period of a timetable is set to 9:00 to 18:00, then the default valid check-in time is between 8:00 and 10:00, and the default valid check-out time is between 17:00 and 19:00.

Flexible Shift

Default Effective Check-In/Out Time

For flexible shifts, you can specify the default effective time period for check-in/out. The time period you set here will be reflected on the Add Timetable pane when you add a timetable for a flexible shift.

8.1.5 Add Timetable

The timetable defines the detailed time rules for attendance, such as work time and break time. According to the actual requirements, you can add a timetable for normal or flexible shift, and then the employees need to follow the time rules to check in, check out, etc.

Add Timetable for Normal Shift

For normal shift, there is strict check-in/out time for the employees, and they should check in before the start-work time and check out after the end-work time. You can add a timetable for the normal shift to define the detailed rules such as work period and break time.

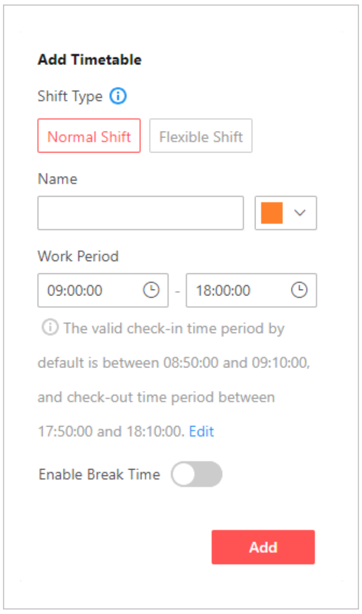
Before You Start

Make sure you have selected normal shift as the shift type. For details, refer to ***Select Shift Type*** .

Steps

1. Go to **Attendance → Basic Configuration → Timetable** .

2. Click **Add**.



Add Timetable

Shift Type ⓘ

Normal Shift | Flexible Shift

Name

Work Period

09:00:00 - 18:00:00

ⓘ The valid check-in time period by default is between 08:50:00 and 09:10:00, and check-out time period between 17:50:00 and 18:10:00. Edit

Enable Break Time

Add

Figure 8-3 Add Timetable

3. Optional: If you have selected two shift types, only select **Normal Shift** as the shift type here.

4. Enter the timetable name, and select a color from the drop-down list if needed.

5. Set the work period.

6. Optional: Click **Edit** to edit the effective check-in/out time.

Note

The default effective check-in/out time is set in **Attendance → Basic Configuration → General → Attendance Rule** . For details, refer to ***Configure Attendance Rule*** .

7. Optional: Enable **Enable Break Time**, and select a break type.

Fixed Duration

The break duration is fixed, and you should set the break duration. The actual break start/end time of employees will not be calculated as the break duration.

Actual Duration

The break duration is calculated by the actual check-out and check-in time of employees.

Note

You can check **Count Break Time in Work Hours** to include the break time into work hours.

8. Click **Add**.

9. Optional: Perform more operations after adding timetables.

Edit Timetable Click the name of the timetable to edit it as needed.

Delete Timetable Check the timetable(s) to be deleted, and click **Delete** to delete it/them.

Filter Timetable Click ▽ in the upper-right corner, and filter timetables according to the name and type.

Add Timetable for Flexible Shift

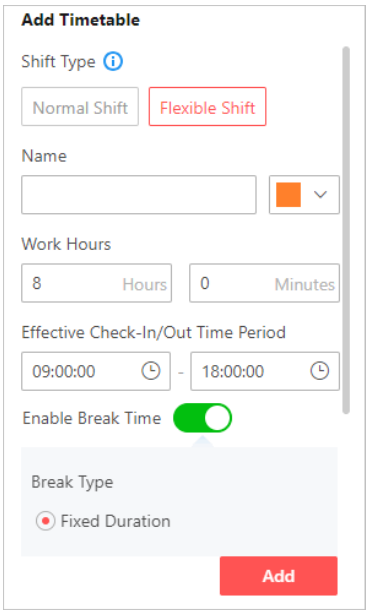
For flexible shift, there is no strict check-in/out time for the employees, and they only need to work longer than the minimum work hours. You can add a timetable for the flexible shift to define the detailed rules such as work hours and break time.

Before You Start

Make sure you have selected flexible shift as the shift type. For details, refer to ***Select Shift Type*** .

Steps

1. Go to **Attendance → Basic Configuration → Timetable** .
2. Click **Add**.



Add Timetable

Shift Type

Normal Shift ● Flexible Shift

Name

Work Hours: 8 Hours 0 Minutes

Effective Check-In/Out Time Period: 09:00:00 - 18:00:00

Enable Break Time: on

Break Type: ● Fixed Duration

Add

Figure 8-4 Add Timetable

3. **Optional:** If you have selected two shift types, only select **Flexible Shift** as the shift type here.
4. Enter the timetable name, and select a color from the drop-down list if needed.
5. Set the work hours.
6. **Optional:** Edit the effective check-in/out time.

Note

The default effective check-in/out time is set in **Attendance → Basic Configuration → General → Attendance Rule** . For details, refer to ***Configure Attendance Rule*** .

7. **Optional:** Enable **Enable Break Time**, and select a break type.

Fixed Duration

The break duration is fixed, and you should set the break duration. The actual break start/end time of employees will not be calculated as the break duration.

Actual Duration

The break duration is calculated by the actual check-out and check-in time of employees.

Note

You can check **Count Break Time in Work Hours** to include the break time into work hours.

8. Click **Add** to add the timetable for the flexible shift.
9. **Optional:** Perform more operations after adding timetables.

Edit Timetable Click the name of the timetable to edit it as needed.

Delete Timetable Check the timetable(s) to be deleted, and click **Delete** to delete it/them.

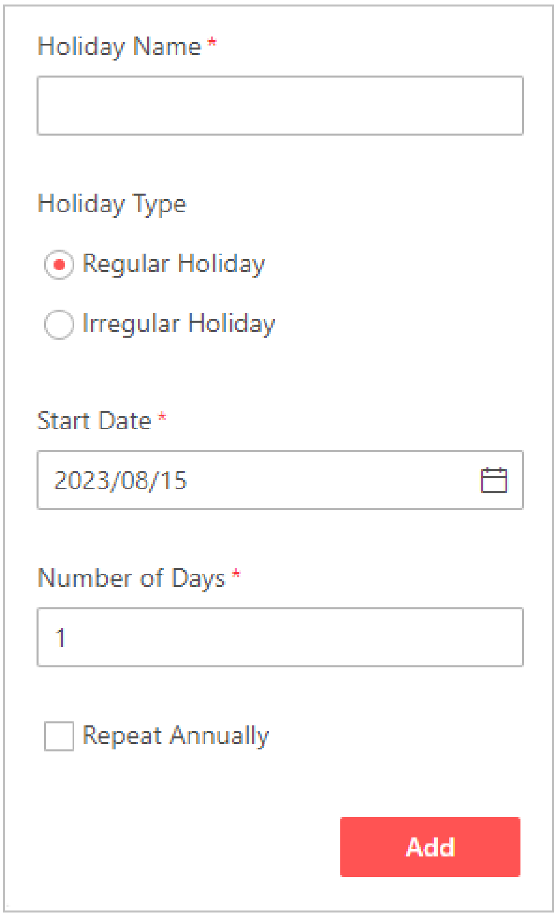
Filter Timetable Click ▽ in the upper-right corner, and filter timetables according to the name and type.

8.1.6 Add Holiday

You can add holidays to define the special days on which shift schedules cannot be assigned to persons. You can set a regular holiday or an irregular holiday depending on the actual scenario.

Steps

1. On the top navigation bar, click **Attendance → Basic Configuration → Holiday** to go to the holiday management page.
2. Click **Add**.



Holiday Name *

Holiday Type

● Regular Holiday

○ Irregular Holiday

Start Date *

2023/08/15

Number of Days *

1

□ Repeat Annually

Figure 8-5 Add Holiday Pane

3. Enter a name for the holiday.

4. Select **Regular Holiday** or **Irregular Holiday** as the holiday type.

5. Set parameters accordingly.

- For a regular holiday, select a start date and enter the number of days for the holiday.
- For an irregular holiday, select a year, a month, and a day, and set the number of days. For example, if you select **2024**, **March**, **Third**, and **Saturday** and enter 3 for the number of days, it means the holiday will start on the third Saturday in March of 2024, and it will last for 3 days.

6. Optional: Check **Repeat Annually** to make this holiday setting effective every year.

7. Click **Add**.

The added holiday will be displayed in the holiday list.

8. Optional: After adding holidays, perform the following operations.

Edit Holiday	Click ✎ in the Operation column of a holiday to edit its information.
Delete Holiday	Click 🗑 in the Operation column of a holiday to delete it from the holiday list, or click **Delete All** at the top to delete all holidays.

Note

Up to 200 holidays can be added, and holidays are not allowed to overlap with each other.

8.1.7 Add Leave Type

Customizing leave types can help you manage employee time-off requests in a more efficient way.

Steps

1. On the top navigation bar, click **Attendance → Basic Configuration → Leave Type** to go to the leave type management page.
2. Click **Add** in the top left corner.
3. Enter a name for the leave type and click **Add**.

Note

Up to 128 leave types can be added.

4. **Optional:** After adding leave types, perform the following operations.

Edit Leave Type
Click ✎ in the Operation column of a leave type to edit its name.

Delete Leave Type
Select one or multiple leave types, and click **Delete** to delete the selected leave type(s).

Search for Leave Type
Enter a keyword in the search box, and click 🔍 to search for a leave type.

What to do next

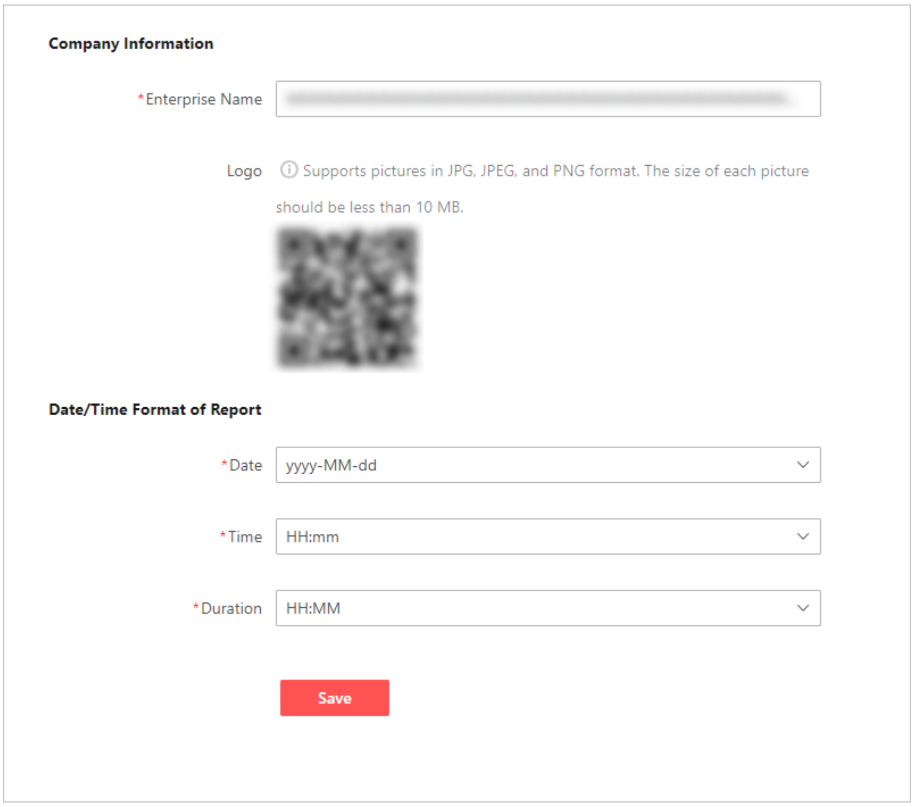
An added leave type can be selected when you or the employees submit leave applications. For details, refer to ***Submit Leave Application*** .

8.1.8 Configure Report Settings

You can configure your company name, company logo, and the time format to be displayed on the attendance reports as needed.

Steps

1. On the top navigation bar, click **Attendance → Basic Configuration → Report** .



Company Information

*Enterprise Name

Logo ⓘ Supports pictures in JPG, JPEG, and PNG format. The size of each picture should be less than 10 MB.

Date/Time Format of Report

*Date: yyyy-MM-dd

*Time: HH:mm

*Duration: HH:MM

Figure 8-6 Configure Report Settings

2. Enter the name of your company.

3. Upload a logo picture.

1) Hover your mouse over the square area of the logo and click **Upload Logo**.

2) Select the logo picture of your company from the local PC.

3) (Optional) Click ↺ ↻ 🔍 in the lower-right corner of the Upload Logo pane to rotate the logo picture and adjust its size.

4) Click **Save**.

4. In the Date/Time Format of Report area, select the format of date, time, and duration respectively.

5. Click **Save**.

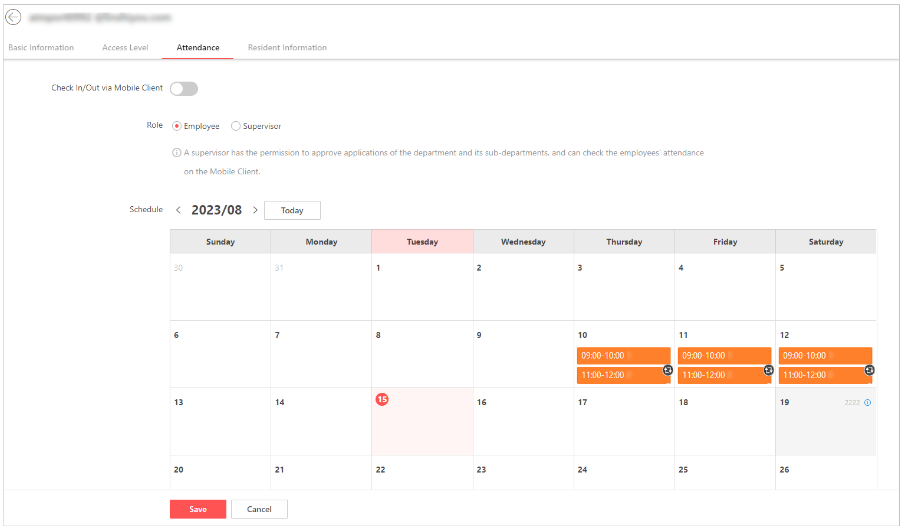
8.1.9 Configure Attendance Parameters for Person

To track and manage employee attendance, you need to add the corresponding employees to the System as persons. Besides the regular access control related parameters such as credentials and access levels, you can also configure parameters that are specific to the time and attendance module, such as the person's role in the department and whether the person can check in/out remotely via the Mobile Client.

Note

For details about adding employees to the System, see ***Add a Person*** .

Go to the person management page by clicking **Person** on the top navigation bar. Click the ID of the employee for which you want to configure the attendance related parameters to enter the person details page, and then select the **Attendance** tab at the top.



[redacted]

Check In/Out via Mobile Client

Role ● Employee ○ Supervisor

ⓘ 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 ‹ 2023/08 › Today

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
30	31	1	2	3	4	5
6	7	8	9	10 09:00-10:00 11:00-12:00	11 09:00-10:00 11:00-12:00	12 09:00-10:00 11:00-12:00
13	14	15	16	17	18	19 2222 ⓘ
20	21	22	23	24	25	26

Figure 8-7 Attendance Related Parameters

Check In/Out via Mobile Client

Switch on **Check In/Out via Mobile Client** to allow the person to check in or out via the Mobile Client. If you check **Must Upload Picture** below, the person must take an instant photo to submit as the proof of attendance while checking in/out. See the *Hik Connect for Teams Mobile Client User Manual* for details about how remote check-in/out works.

Role

Select whether the person is an employee or a supervisor of the department.

Note

The role of a person is set to employee by default. A supervisor is a higher-ranking employee who has additional permission to review applications and check attendance data of the employees in the same department on the Mobile Client.

Schedule

If shifts are scheduled for the person, you can view the person's schedule in the monthly calendar and switch to other months by clicking ‹ or › . You can click **Today** to quickly go to the current day in the calendar.

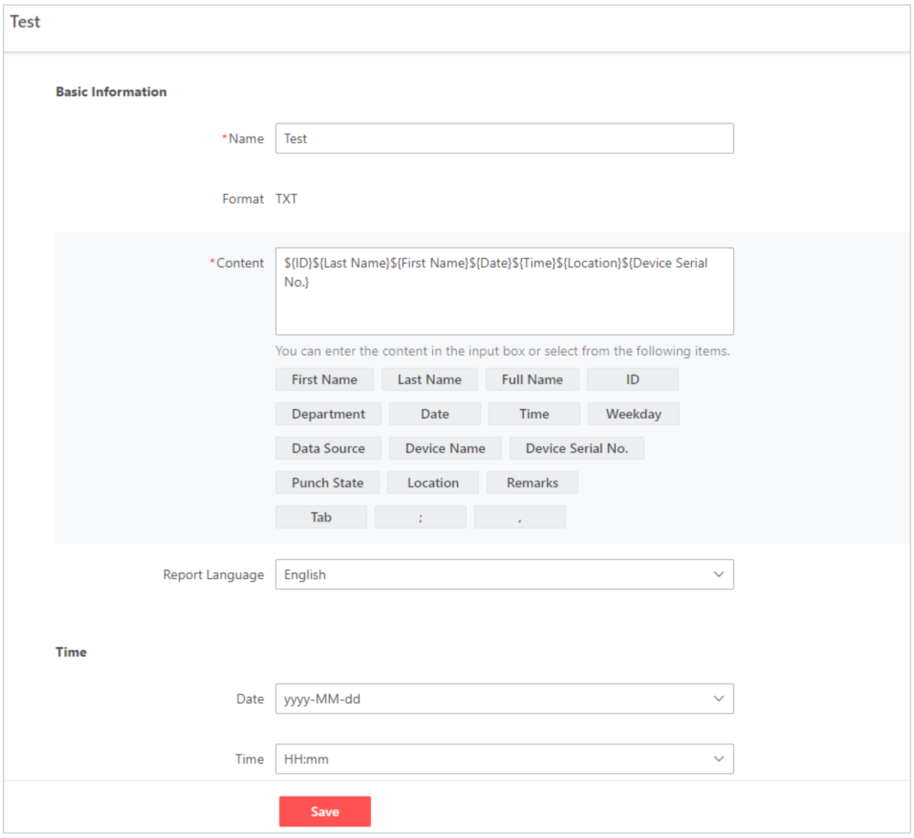
8.1.10 Customize Export

To integrate with third-party salary statistics software, you can customize attendance data and export them as you need.

Steps

1. On the top navigation bar, click **Attendance → Basic Configuration → Custom Export** .

2. Click ＋ to set the customized export.



Test

Basic Information

*Name: Test

Format: TXT

*Content: ${ID}${Last Name}${First Name}${Date}${Time}${Location}${Device Serial No.}

You can enter the content in the input box or select from the following items.

Report Language: English

Time

Date: yyyy-MM-dd

Time: HH:mm

Figure 8-8 Custom Export

3. Set a name for the export.

4. Click a content tab to add an item to the content box or you can enter the contents.

5. Set the report language, and set the format of date, time, and duration.

6. Select departments between **All Departments** and **Designated Department**.

7. Click **Save**.

8. Click ⇥ , select the time period for the report, and click **Export**.

The report will be downloaded by the browser.

8.2 Schedule Management

The platform provides a schedule overview page for users to filter the selected persons' schedules by different time dimensions and export the displayed schedules in different formats. Users can also assign a schedule to a single person or multiple persons in a batch.

8.2.1 Assign Schedule to Persons

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

Before You Start

Make sure you have added persons to the platform. See ***Person Management*** .

Steps

1. On the top, select **Attendance**, and then select **Schedule** on the left.

2. Hover the cursor over a box of a person and click + to open the Schedule pane.

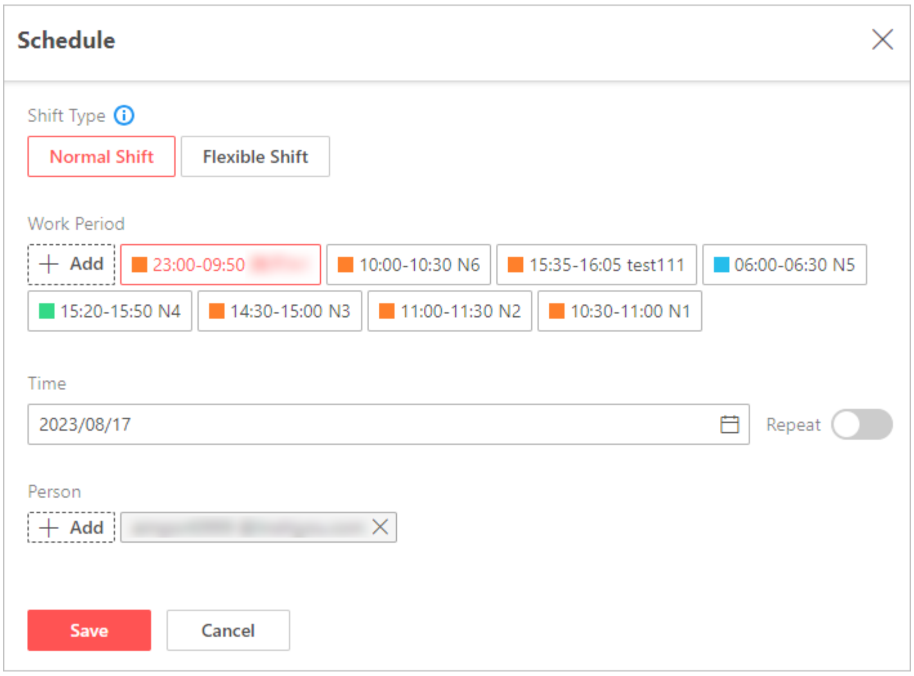
3. Optional: Select a shift type.

Note

You need to select a shift type only when the two shift types are configured.

4. Select a work period, or click **Add** to add one. See ***Add Timetable*** .

5. In the Time field, select a time period during which the schedule works.



Schedule

Shift Type

Normal Shift | Flexible Shift

Work Period

+ Add | 23:00-09:50 [redacted] | 10:00-10:30 N6 | 15:35-16:05 test111 | 06:00-06:30 N5 | 15:20-15:50 N4 | 14:30-15:00 N3 | 11:00-11:30 N2 | 10:30-11:00 N1

Time

2023/08/17

Repeat

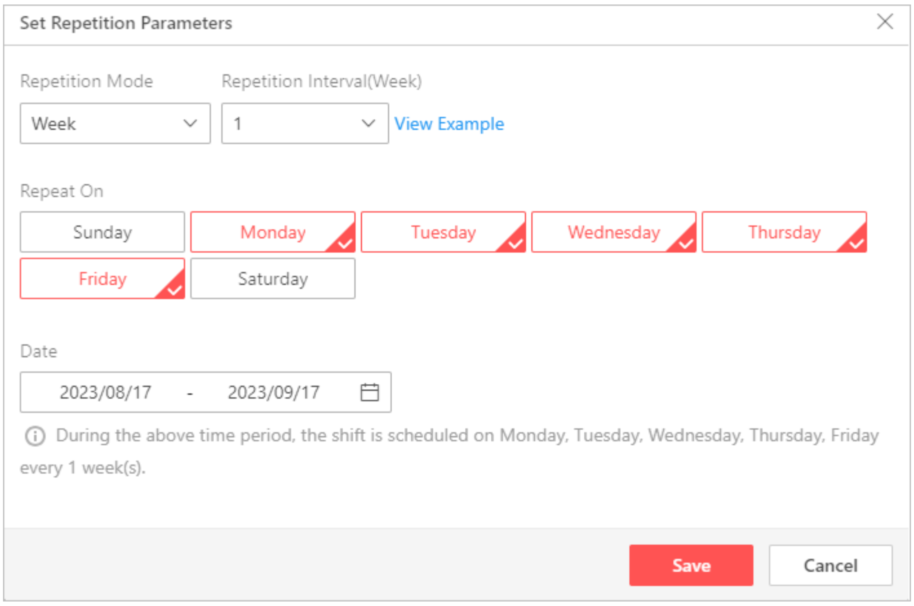
Person

+ Add [redacted]

Save | Cancel

Figure 8-9 Schedule Pane

6. **Optional:** Enable **Repeat** to open the Set Repetition Parameters window and set related parameters.



Set Repetition Parameters

Repetition Mode: Week

Repetition Interval(Week): 1

Repeat On: ☐ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☐ Saturday

Date: 2023/08/17 - 2023/09/17

During the above time period, the shift is scheduled on Monday, Tuesday, Wednesday, Thursday, Friday every 1 week(s).

Figure 8-10 Set Repetition Parameters Window

Note

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. **Optional:** In the Person field, click **Add** to check other persons to assign the work period to.
8. Click **Save**.
9. **Optional:** Select a person, click a work period for details or deleting the work period.

Note

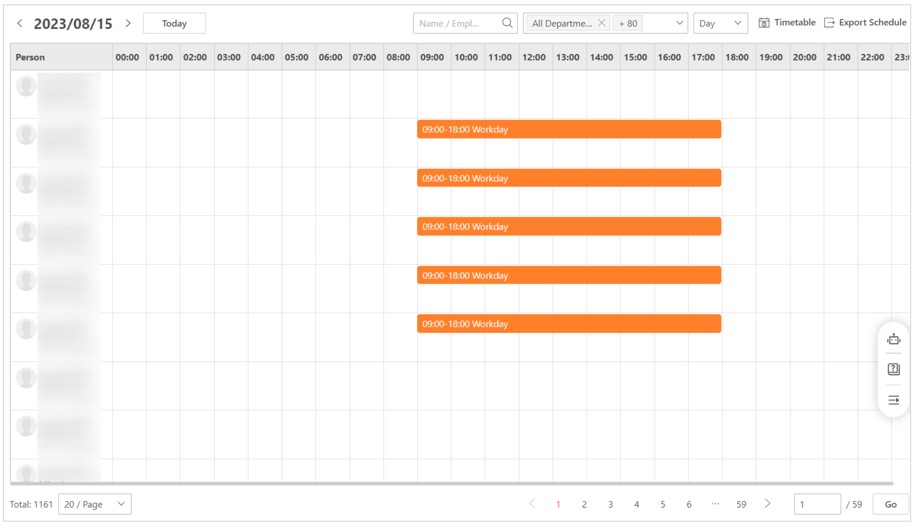
For other options, see ***Schedule Overview*** .

8.2.2 Schedule Overview

The schedule overview shows the schedule information of each person in the departments. You can also view the detailed schedule of one person on each day.

On the top navigation bar, click **Attendance → Schedule** to enter the schedule overview page.

On the schedule overview page, you can select departments, click **Today**, select **Day**/**Week**/**Month**, or enter person name/ID to filter and display the schedule information of each person by different dimensions.



09:00-18:00 Workday

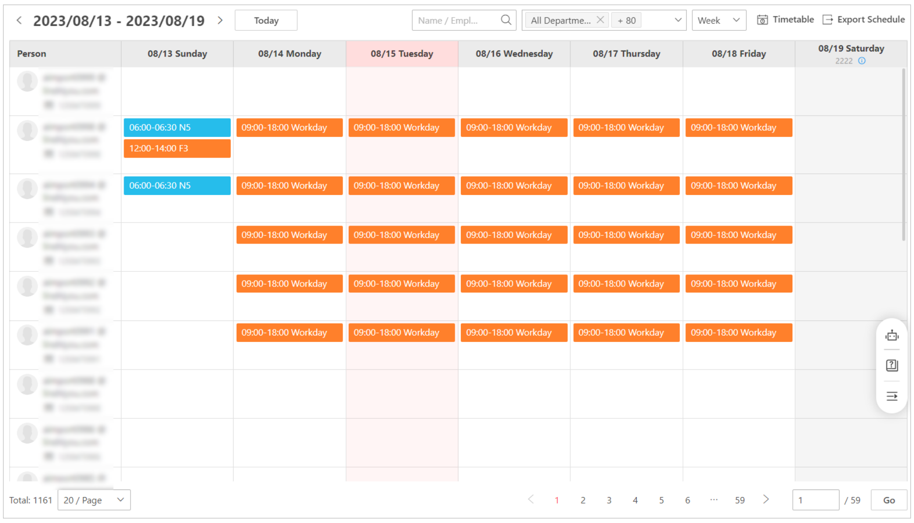
09:00-18:00 Workday

09:00-18:00 Workday

09:00-18:00 Workday

09:00-18:00 Workday

Figure 8-11 Display Schedule by Day



Person	08/13 Sunday	08/14 Monday	08/15 Tuesday	08/16 Wednesday	08/17 Thursday	08/18 Friday	08/19 Saturday 2222
	06:00-06:30 N5 12:00-14:00 F3	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	
	06:00-06:30 N5	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	
		09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	
		09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	
		09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	09:00-18:00 Workday	

Figure 8-12 Display Schedule by Week

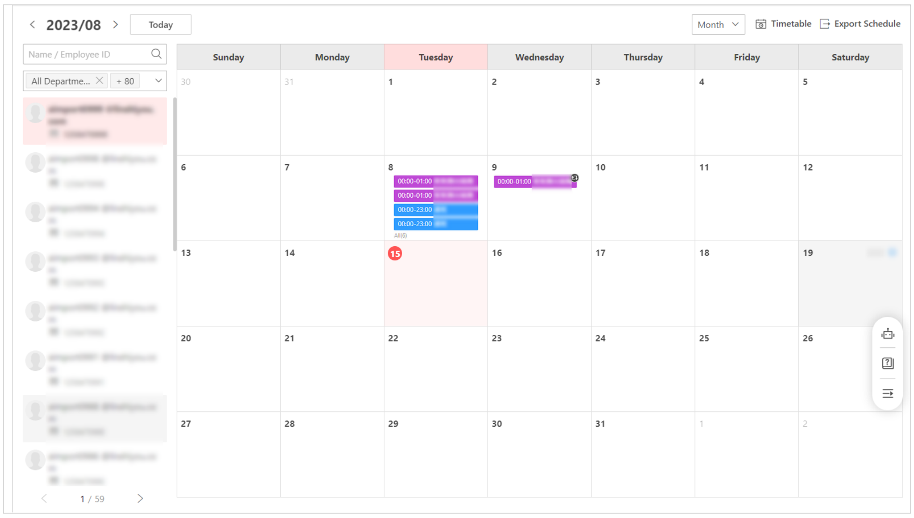


Figure 8-13 Display Schedule by Month

After filtering and displaying the schedule, you can perform the following operations.

- Hover the cursor over a box of a person and click + to open the Schedule pane to add a work period for the person. See ***Assign Schedule to Persons*** for details.

  Note

  Adding a work period to a holiday is not allowed.
- Click a work period for details or deleting the work period.
- When displaying the schedule by month, click a person listed on the left to display the detailed schedule of this person.
- When displaying the schedule by week or month, drag a work period to another date or person.
- Click **Export Schedule** on the top right to export the schedule displayed on the current page in the PDF/PNG/JPG format.
- Click **Timetable** on the top right to go to the **Timetable** page for timetable management. See ***Add Timetable*** for details.

8.3 Application Management

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.

8.3.1 Submit Leave Application

On the Portal, the administrator can submit a leave application for an employee upon the employee's request.

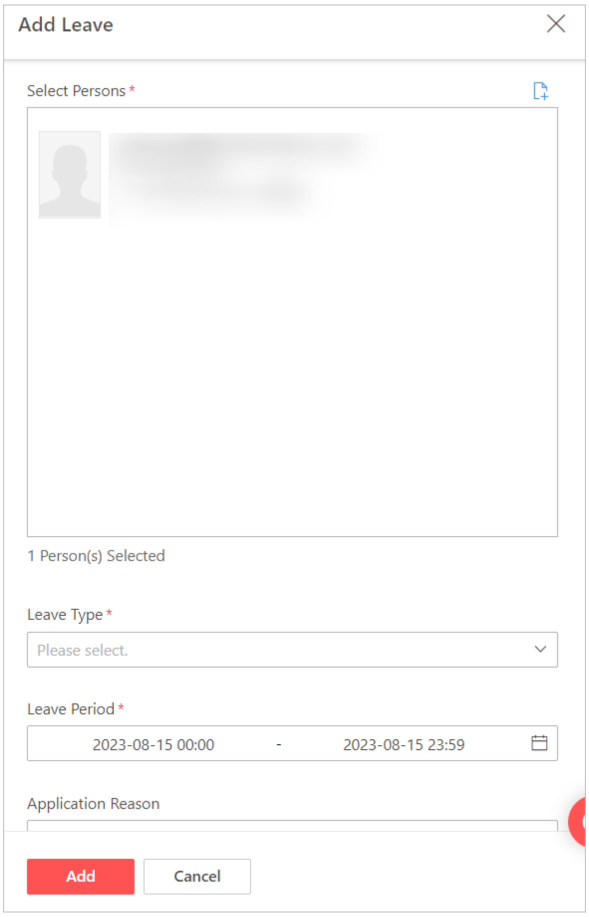
Before You Start

Make sure you have added leave types. See details in ***Add Leave Type*** .

Steps

1. On the top navigation bar, click **Attendance → Review → Leave** .

2. Click **Add** to display the Add Leave pane.



Add Leave

Select Persons *

1 Person(s) Selected

Leave Type *

Please select.

Leave Period *

2023-08-15 00:00 - 2023-08-15 23:59

Application Reason

Add

Cancel

Figure 8-14 Submit Leave Application

3. In the Select Persons area, click , select one or multiple persons, and click **Add**.

4. Select a leave type from the drop-down list.

5. Specify the leave period.

6. Optional: Enter the reason for applying and upload attachments.

7. Optional: Check **Auto Approve**.

Note

If checked, the application takes effect immediately after being submitted with no approval required.

8. Click **Add**.

9. Optional: Perform further operations.

Filter Leave Applications
Click ▽ in the upper-right corner, set the conditions, and click **Filter** to view the matched applications.

Enable/Disable Self-Adaptive Column Width
Click ☰ in the upper-right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title**.

Customize Columns to Be Displayed
Click ⚙ in the upper-right corner and select the columns to be displayed as needed.

Handle Leave Applications
You can view the application flow of an added application, view and download the attachments, and approve/reject/withdraw applications. For details, refer to ***Review Applications*** .

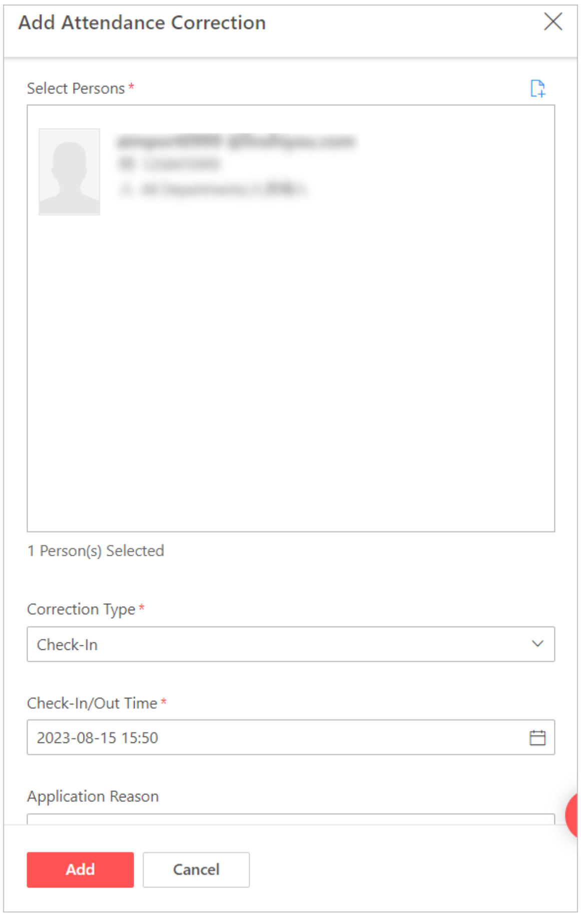
8.3.2 Submit Attendance Correction Application

On the Portal, the administrator can submit an attendance correction application for an employee upon the employee's request.

Steps

1. On the top navigation bar, click **Attendance → Review → Attendance Correction** .

2. Click **Add** to display the Add Attendance Correction pane.



Select Persons *

[redacted]

1 Person(s) Selected

Correction Type *
Check-In

Check-In/Out Time *
2023-08-15 15:50

Application Reason

Figure 8-15 Submit Attendance Correction Application

3. In the Select Persons area, click 🗋, select one or multiple persons, and click **Add**.

4. Select **Check-In** or **Check-Out** as the correction type.

5. Specify the check-in/out time.

6. Optional: Enter the reason for applying and upload attachments.

7. Optional: Check **Auto Approve**.

Note

If checked, the application takes effect immediately after being submitted with no approval required.

8. Click **Add**.

9. Optional: Perform further operations.

Filter Attendance Correction Applications	Click ▽ in the upper-right corner, set the conditions, and click **Filter** to view the matched applications.
Enable/Disable Self-Adaptive Column Width	Click ☰ in the upper-right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title**.
Customize Columns to Be Displayed	Click ⚙ in the upper-right corner and select the columns to be displayed as needed.

Handle Attendance Correction Applications	You can view the application flow of an added application, view and download the attachments, and approve/reject/withdraw applications. For details, refer to ***Review Applications*** .

8.3.3 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 8-2 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.
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.

Operation	Description
	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.

8.4 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.

Note

You can configure parameters for the reports, including the company name, company logo, and time format. See details in ***Configure Report Settings*** .

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 8-3 Report Contents

Report Type	Description
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 Report	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.

Report Type	Description
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.
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.
Transaction Report	Original check-in/out records for attendance calculation are displayed, including the employee information, date, time, weekday, data source, device name, punch state, and remarks.
Mobile Transaction Report	Records of employees checking in/out via the Mobile Client are displayed, including the employee information, date, time, weekday, remarks, location, and attachment. Each attachment can be downloaded to your local PC independently for viewing.

You can perform the following operations:

Table 8-4 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.

Note

Transaction page and Mobile Transaction page do not support recalculating attendance.

Chapter 9 Video Intercom Management

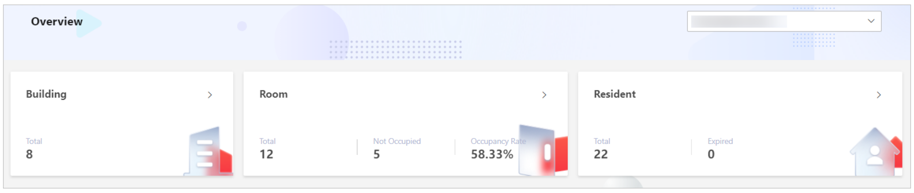
You can configure and manage video intercom for areas for which you have permission. After you add video intercom devices, add buildings, rooms, and residents, and link the devices to buildings, video calls can be placed from the video intercom devices to the Mobile Clients of the corresponding residents. Moreover, you can view the call history and create temporary passes for people (e.g, visitors) with temporary access needs.

9.1 Video Intercom Overview

The video intercom overview page provides the housing statistics, including the total number of buildings, the total number of rooms, the number of not-occupied rooms (rooms without residents), the occupancy rate of all rooms, the total number of residents, and the number expired residents.

Go to the Overview page.

- On the top navigation bar, click **Video Intercom → Overview** .
- In the service overview section on the Home page, click **Video Intercom → Go to Overview** .



Overview

[redacted]

Building
Total 8

Room
Total 12
Not Occupied 5
Occupancy Rate 58.33%

Resident
Total 22
Expired 0

Figure 9-1 Overview

Select an area from the drop-down list on the top right of the page to show the housing statistics of the selected area.

Click › or the total number in the building/room/resident section to switch to the building/room/resident list of the selected area.

Click the number of not-occupied rooms to switch to the list of rooms without residents of the selected area.

Click the number of expired residents to switch to the list of expired residents of the selected area.

9.2 Housing Management

You can manage buildings, rooms in the buildings, and residents in the rooms by operations such as adding, deleting, and editing. You can link door stations to buildings for security purposes and you can add residents to rooms in the buildings to allow them to access the corresponding buildings.

9.2.1 Add Building

You can add a building to an area. When adding, you can also batch create rooms for the building and link door stations to the building.

Before You Start

- Make sure you have added an area. For details, refer to ***Manage Area*** .
- Make sure you have the permission for housing management.

Steps

1. Go to the Building page.
   - On the top navigation bar, select **Video Intercom → Building** .
   - In the service overview section on the Home page, click **Video Intercom**, and then click the number of buildings in the overview section.
2. **Optional:** Select an area from the area list on the left to add a building to it.
3. Click **Add** to enter the Add Building page.
4. Select an area from the drop-down list or add a new area to add a building to it.

   Note

   If you have selected an area with no sub areas in Step 2, you can skip this step.
5. Enter the building No. and name for the building.
6. **Optional:** Enable **Batch Room Creation** and complete related settings to batch creating rooms.

   Room Numbering Rule

   Select a rule for numbering the rooms.

   You can number the rooms with respect to the floor level (e.g., 101 is the first room on the first floor) or with incremental numbering (independent of the floor level).

   Number of Floors

   Enter the total number of floors for the building.

   Number of Households Per Floor

   Enter the total number of households (rooms) on each floor.

   Note

   You can click **Preview Room Info** to view how the rooms are distributed in the building.
7. **Optional:** Click **Add** and select devices (i.e., door stations) in the area of the building to link them to the building.

   Note

   - One door station can be linked to only one building.
   - Once the door station is linked to the building, permission to access the building for all residents added to rooms of the building will be automatically applied to the device door station.
8. Click **Add** to add the building.

9. Optional: Perform the following operations according to your needs after adding buildings.

Link Door Station(s)
Click in the Operation column and select door stations to link to the corresponding building.

> **Note**
>
> - One door station can be linked to only one building.
> - Once the door station is linked to the building, permission to access the building for all residents added to rooms of the building will be automatically applied to the device door station.

View Linked Door Station(s)
Click in the Door Station column to view the door station(s) linked to the corresponding building.

Delete Building(s)
Select the added building(s) and click **Delete** to delete the building(s).

Display Building(s) Added to Sub Area(s)
Check **Display Sub Areas** to also display the building(s) added to the sub area(s) when you select an area on the left.

Search for Building(s)
Enter the building name in the search box on the top right to search for the building(s).

9.2.2 Add Room

After adding a building to an area, you can add a room or batch add rooms to the added building.

Before You Start

- Make sure you have added a building. For details, refer to ***Add Building*** .
- Make sure you have the permission for housing management.

Steps

1. Go to the Room page.
   - On the top navigation bar, select **Video Intercom → Room** .
   - In the service overview section on the Home page, click **Video Intercom**, and then click the number of rooms in the overview section.

2. Optional: Select an area with buildings or select a building from the left list.

3. Click **Add** to add a room or click ⌄ **→ Batch Add** to batch add rooms.

4. Select an area from the drop-down list.

> **Note**
>
> If you have selected an area with buildings and with no sub areas or have selected a building in Step 2, you can skip this step.

5. Select a building from the drop-down list.

If you have selected a building in Step 2, you can skip this step.

6. Enter the room number(s) and room name(s).

Note

- The room No. is required and the room name is optional.
- If you are on the Batch Add Rooms page, you can click **Add Room** or **Batch Add Rooms** to add more rooms, or click 🗑 to delete a room.

7. Click **Add** to finish adding the room or click **Save and Add Resident** to save and continue adding resident(s) to the building.

Note

- **Save and Add Resident** is not available on the Batch Add Rooms page.
- Refer to ***Add Resident*** for details about adding residents.

8. Optional: Perform the following operations according to your needs after adding rooms.

Add a Resident

Click in the Operation column to add a resident to the corresponding room.

Note

Refer to ***Add Resident*** for details about adding residents.

Delete Room(s)

Select the added room(s) and click **Delete** to delete the room(s).

Display Room(s) Added to Sub Areas

Check **Display Sub Areas** to also display the room(s) added to the sub areas when you select an area on the left.

Filter Rooms

Click ▽ to filter rooms by the room No., room name, number of residents, householder, and email.

Set Displayed Columns

Click and check/uncheck the items to determine which items are displayed on the page and drag the items to adjust the order.

9.2.3 Add Resident

After adding buildings and rooms, you can add residents to rooms for them to log in to the Mobile Client to use functions including managing family members (only available to householders), opening doors via Bluetooth and QR code, remote door control, generating temporary passes, receiving video calls, view call history, and muting calls.

Before You Start

- Make sure you have added a building and added a room to the building. Refer to ***Add Building*** and ***Add Room*** for details.
- Make sure you have the permission to manage residents.

Steps

1. Go to the Resident page.

- On the top navigation bar, select **Video Intercom → Resident** .

- In the service overview section on the Home page, click **Video Intercom**, and then click the number of residents in the overview section.

2. **Optional:** Select a building with room(s) on the left.
3. Click **Add** to enter the Add Resident page.
4. Set resident information.
   - Select **Create New Resident** as the adding mode, and set the name, effective period, account, email, phone number, credentials, etc.
   - Select **Select from Existing Persons** as the adding mode, select a person, and edit the person (resident) information if needed.

Note

- For details about how to set the information, refer to ***Add a Person*** .
- The account is required because a resident has to log in to the Mobile Client using this email/ phone number (the self-service login is enabled for a resident automatically).

5. Select the area where the room to which you are to add the resident is located.

Note

If you have selected a building in Step 2, you can skip this step.

6. Click **Add** in the Housing Information section to select room(s).

Note

One resident can be added to multiple rooms.

7. **Optional:** Click ⌄ on the room card(s) and set the resident type(s).

Note

- Only one householder can be added to a room.
- If a person is the first resident added to a room, the resident type is set to the householder by default and can be changed to the family member.
- If a person is not the first resident added to a room, the resident type is set to the family member by default and can be changed to the householder. The original householder (if any) will be changed to the family member.

8. **Optional:** Check **Open Door via PIN Code** to generate the PIN code with 4 to 8 digits automatically and edit the code if needed.

Note

Once 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.

9. **Optional:** Click **Add** in the Access Level section and select access level(s) to assign to the resident.

Note

Once a resident is added to a room, permission to access the corresponding building will be automatically assigned to the resident. If there are other access levels needed, you can add and assign to the resident in this step.

10. Click **Add** to finish adding the resident or click **Add and Continue** to finish adding this resident and also start adding another.

    Note

    - The added residents will be synchronized to the Person page automatically.
    - No more than 6 residents can be added to one room.

11. **Optional:** Perform the following operations according to your needs after adding residents.

Edit a Resident

Click ✎ to edit the information for a corresponding resident.

Note

- If you change the resident type from the householder to the family member, a window for changing the householder will pop up and you can select another resident (if any) as the householder or check **No Householder**.
- If you change the resident type from the family member to the householder, the original householder (if any) will be changed to a family member automatically.

Delete Resident(s)

Select the added resident(s) and click **Delete** to delete the resident(s).

Note

- Once the householder of a room is deleted, a window for changing the householder will pop up and you can select another resident (if any) as the householder or check **No Householder**.
- Deleting residents will not delete the corresponding persons from the Person page.

Display Resident(s) Added to Sub Area(s)

Check **Display Sub Areas** to also display the resident(s) added to the sub area(s) when you select an area on the left.

Filter Residents

Click ▽ to filter residents by the name, room No., email, phone, resident type, and status.

Set Displayed Columns

Click ⚙ and check/uncheck the items to determine which items are displayed on the page and drag the items to adjust the order.

9.3 Call Management

You can set up which users can receive calls from which devices by adding specific users as call managers. Also, as a call manager or resident, you can view and export all your calls in Call History.

9.3.1 View Call History

You can view and export the call history which contains details such as the capture, device name, device model, building, and visiting purpose.

Note

- Residents can view the call history only on the Mobile Client. For details, refer to the *Hik Connect for Teams Mobile Client User Manual*.
- Make sure you have permission to manage calls.

Go to the Call History page.

- On the top navigation bar, select **Video Intercom → Call Management → Call History** .
- In the service overview section on the Home page, click **Video Intercom**, and then click **View More** in the call history section.

Supported operations are as follows.

Operation	Description
Export Call History	Check one or more call records and click **Export** to export the call records.
Filter Call History	Click ▽ , set conditions, and click **Filter** to filter call history.
Set Displayed Columns	Click ⚙ and check/uncheck the items to determine which items are displayed on the page and drag the items to adjust the order.

9.3.2 Specify Users for Receiving Calls from Devices

You can 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.

Steps

1. On the top navigation bar, select **Video Intercom → Call Management → Call Manager** .
2. Click **Add** to enter the Add Call Manager page.
3. Select a user to add them as the call manager.
4. 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.

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

6. Optional: Perform the following operations according to your needs after adding call managers.

Edit a Call Manager	Click ✎ in the Operation column to reselect the devices for receiving calls from for the corresponding call manager.
View Device(s) for Receiving Calls From	Click 🗎 in the Device for Receiving Calls From column to view the device list of the corresponding call manager.
Delete Selected/All Call Manager(s)	Select the added call manager(s) and click **Delete** to delete the call manager(s). Click ⌄ → **Delete All** to delete all call managers.
Search for Call Manager(s)	Enter the call manager name in the search box on the top right to search for the call manager(s).

9.4 Create Temporary Pass

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.

Before You Start

Make sure you have permission to manage temporary passes.

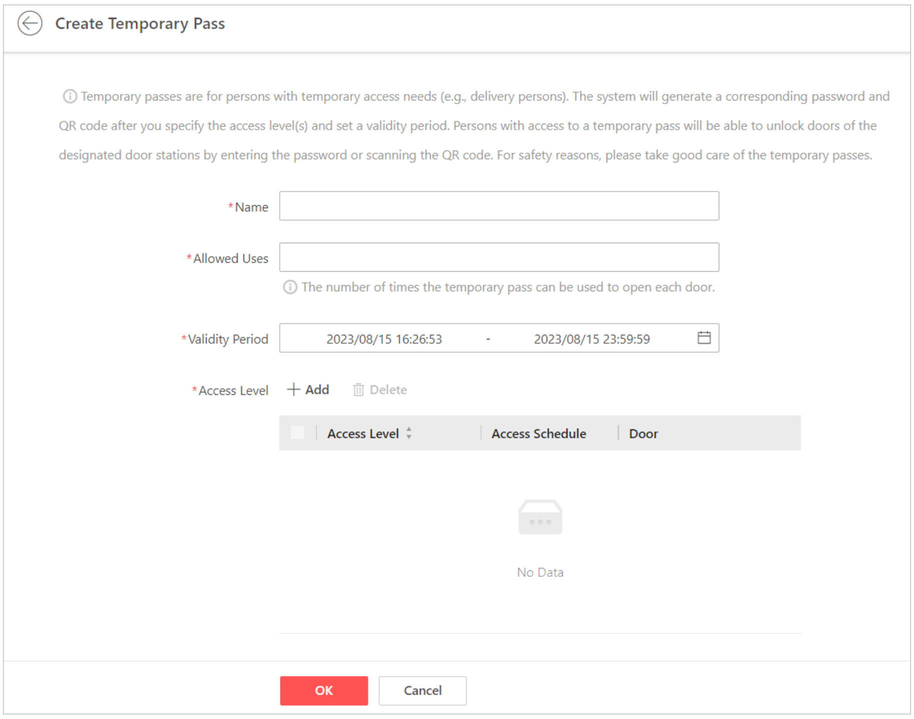
Steps

Note

Residents can create temporary passes only on the Mobile Client. For details, refer to the *Hik Connect for Teams Mobile Client User Manual*.

1. Go to the Temporary Pass Management page.
- On the top navigation bar, select **Video Intercom → Temporary Pass Management** .
- In the service overview section on the Home page, click **Video Intercom**, and then click **View More** in the temporary pass section.

2. Click **Add**.



Create Temporary Pass

ⓘ Temporary passes are for persons with temporary access needs (e.g., delivery persons). The system will generate a corresponding password and QR code after you specify the access level(s) and set a validity period. Persons with access to a temporary pass will be able to unlock doors of the designated door stations by entering the password or scanning the QR code. For safety reasons, please take good care of the temporary passes.

*Name

*Allowed Uses

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

*Validity Period 2023/08/15 16:26:53 - 2023/08/15 23:59:59

*Access Level + Add Delete

□	Access Level	Access Schedule	Door

No Data

Figure 9-2 Create Temporary Pass

3. 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.

4. Click **OK**.

5. Optional: Perform the following operations according to your needs after creating temporary passes.

Display and Download the QR Code
Move your cursor to ▦ and click **Download**.

View Door Unlock Record
Click ▤ in the Operation column to view the door unlock records of the temporary pass.

Delete Temporary Pass(es)
Select the added temporary pass(es) and click **Delete** to delete the temporary pass(es).

Search for Temporary Pass(es)

Enter the name of the temporary pass or creator in the search box on the top right to search for the temporary pass(es).

Chapter 10 On-Board Monitoring

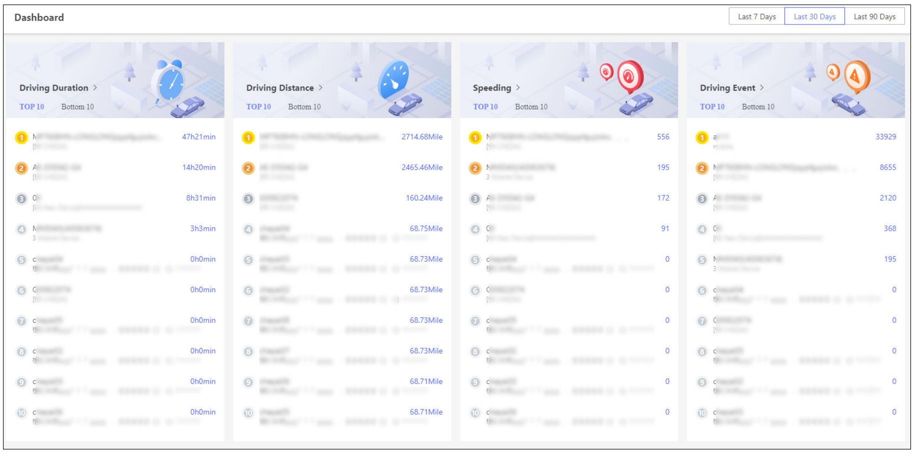
The On-Board Monitoring module is for users to monitor vehicles. It provides various information about vehicles, including the vehicle picture, driving status, driver information, speed, location, and so on. The main features are locating vehicles to get their real-time GPS information and driving speed, configuring driving rules, talking to drivers via two-way audio, playing videos streamed from the vehicle-mounted cameras, searching for and playing back the tracks vehicles have traveled along, viewing and acknowledging alarms, and generating on-board monitoring reports. In addition, you can search for driving events occurred during driving monitoring to know what happens to vehicles.

10.1 Dashboard Overview

The On-Board Monitoring Dashboard provides an at-a-glance view of different rankings, including the top/bottom 10 vehicles in driving duration, driving distance, speeding, and number of driving events during the past 7 days, 30 days, or 90 days.

Go to the Dashboard page by either of the following entrances.

- On the top navigation bar, click **On-Board Monitoring → Dashboard** .
- In the service overview section on the Home page, click **On-Board Monitoring → Go to Dashboard** .



	Driving Duration >	Driving Distance >	Speeding >	Driving Event >
1	47h21min	2714.68Mile	556	33929
2	14h20min	2465.46Mile	195	8655
3	8h31min	160.24Mile	172	2120
4	3h3min	68.75Mile	91	368
5	0h0min	68.73Mile	0	195
6	0h0min	68.73Mile	0	0
7	0h0min	68.73Mile	0	0
8	0h0min	68.73Mile	0	0
9	0h0min	68.71Mile	0	0
10	0h0min	68.71Mile	0	0

Figure 10-1 On-Board Monitoring Dashboard

Perform the following operations as needed.

Select Time Period for Calculation	Click **Last 7 Days**, **Last 30 Days**, or **Last 90 Days** in the top right corner of the page to display the statistics of the corresponding period.
Switch Between Top 10 and Bottom 10	Click **TOP 10** or **Bottom 10** to display the corresponding statistics.
Generate Report	Click > beside **Driving Duration**, **Driving Distance**, **Speeding**, or **Driving Event** to jump to the Statistics and Reports module to view and generate corresponding reports. See details in ***Statistics and Reports*** .

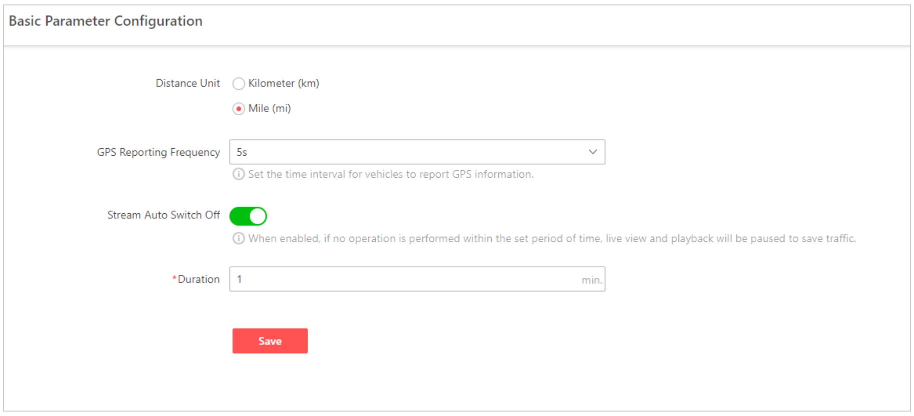
10.2 Configurations Before On-Board Monitoring

You can set the basic parameters, such as the distance unit and GPS reporting frequency, and select the event types to be received and calculated by the Portal.

10.2.1 Set Basic Parameters

You can configure the basic parameters including the distance unit, GPS reporting frequency, etc.

On the top navigation bar, click **On-Board Monitoring → Basic Configuration → Basic Parameter Configuration** to set the basic parameters.



Basic Parameter Configuration

Distance Unit ○ Kilometer (km)
● Mile (mi)

GPS Reporting Frequency 5s

ⓘ Set the time interval for vehicles to report GPS information.

Stream Auto Switch Off (on)

ⓘ When enabled, if no operation is performed within the set period of time, live view and playback will be paused to save traffic.

*Duration 1 min.

Figure 10-2 Basic Parameter Configuration

Distance Unit

Select **Kilometer (km)** or **Mile (mi)** as the distance unit.

GPS Reporting Frequency

Set the interval for vehicles to report GPS information.

Stream Auto Switch Off

You can switch on **Stream Auto Switch Off** and set the duration. If no operation is performed within the set duration, live view and playback will be paused to save traffic.

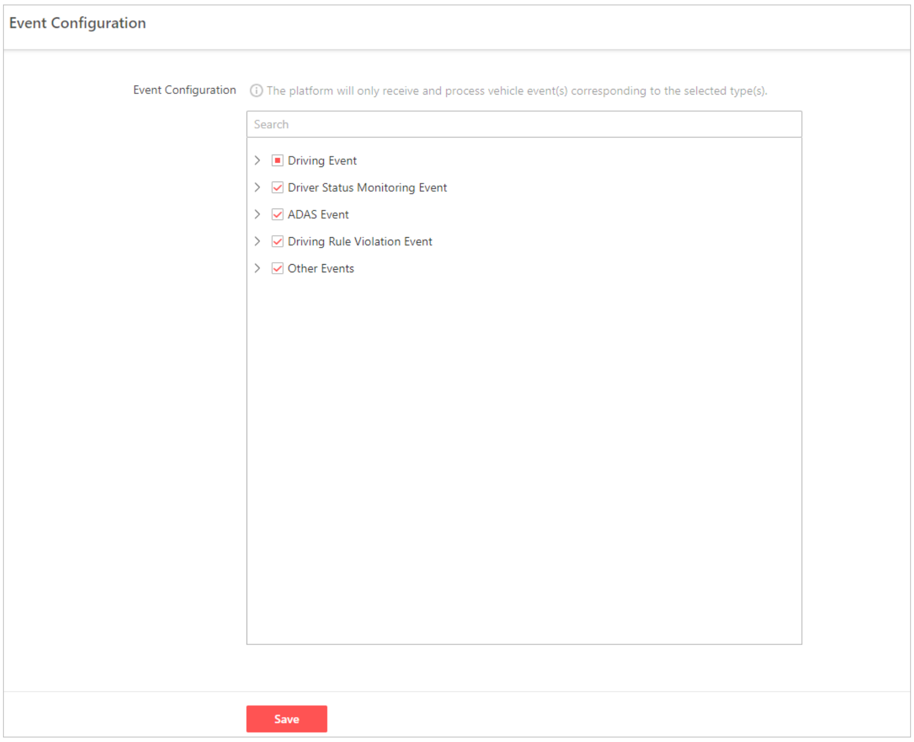
10.2.2 Set Event Types to Be Received

You can set the event types to be received and calculated by the Portal for the current user account.

On the top navigation bar, click **On-Board Monitoring → Basic Configuration → Event Receiving Configuration** to select the even types as needed.

Note

All the event types are selected by default.



Event Configuration

Event Configuration ⓘ The platform will only receive and process vehicle event(s) corresponding to the selected type(s).

Search
> ■ Driving Event
> ☑ Driver Status Monitoring Event
> ☑ ADAS Event
> ☑ Driving Rule Violation Event
> ☑ Other Events
Save

Figure 10-3 Event Configuration Page

10.3 Configure Driving Rule

There are two types of driving rule: driving rule for region and driving rule for route. A driving rule for region specifies the region where vehicles are allowed or not allowed to drive, and a driving rule for route specifies the route which vehicles should drive along or should not enter. Besides, you can configure rule schedule templates to define when the rules should take effect. As a result, if a vehicle breaks an effective rule, an event will be triggered and uploaded to the platform.

10.3.1 Add a Driving Rule for Region

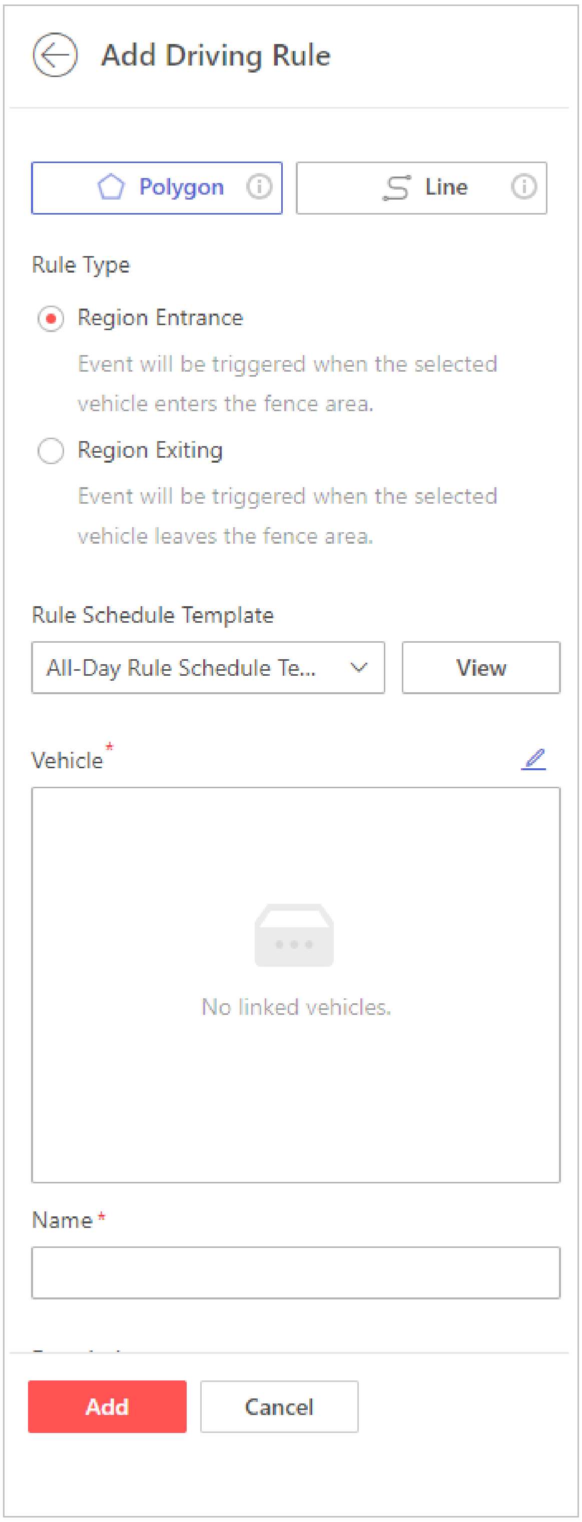
You can add a driving rule to specify the region where vehicles are allowed or not allowed to drive.

Steps

1. Go to the driving rule configuration page.

- On the top navigation bar, click **On-Board Monitoring → Driving Rule Configuration → Driving Rule Configuration** .
- In the service overview section on the Home page, click **On-Board Monitoring → Driving Monitoring Configuration** .

2. Click + to enter the Add Driving Rule page.



Add Driving Rule

Polygon | Line

Rule Type

● Region Entrance

Event will be triggered when the selected vehicle enters the fence area.

○ Region Exiting

Event will be triggered when the selected vehicle leaves the fence area.

Rule Schedule Template

All-Day Rule Schedule Te...

Vehicle*

No linked vehicles.

Name*

Figure 10-4 Add Driving Rule (Region)

3. Select **Polygon** which is suitable for configuring rules of entering or leaving a region.

4. Draw a region on the map for setting the rule.

Note

Click to start drawing and right-click to finish. After forming a region, drag a point to move it or double-click to delete it.

5. Select the rule type.

Region Entrance

Events will be triggered when the selected vehicles enter the region.

Region Exit

Events will be triggered when the selected vehicles leave the region.

6. Set other rule information.

1) Select a rule schedule template.

Note

You can click **View** to view the scheduled time of the selected template. If you have not configured any rule schedule template, you can see ***Configure a Rule Schedule Template*** for how to configure one.

2) Click ✎ to select vehicle(s) that the rule will be applied to.

3) Set a name for the rule.

4) **Optional:** Enter the rule description.

7. Click **Add**.

8. Optional: Perform the following operations after configuring the driving rules.

Manage the Map

- Click ⛶ to display the map in full-screen mode.
- Enter keywords on the top right of the map to search for a location.
- Click the thumbnail for map on the bottom right and change the map type (default, topographic map, or satellite map).
- Click + / − to zoom in/out.

Edit a Driving Rule

Move your cursor to the rule to be edited on the rule list and click ✎ to enter the editing page.

Copy a Driving Rule

Move your cursor to the rule to be copied on the rule list and click 🗐 to enter the Add Driving Rule page with the same rule settings.

Filter Driving Rules

On the rule list, click ▽ on the upper right, set filtering conditions, and click **OK** to filter rules.

Delete Driving Rules

On the rule list, select one or multiple rules and click 🗑 to delete them, or move your cursor to the rule to be deleted on the rule list and click 🗑 to delete it.

10.3.2 Add a Driving Rule for Route

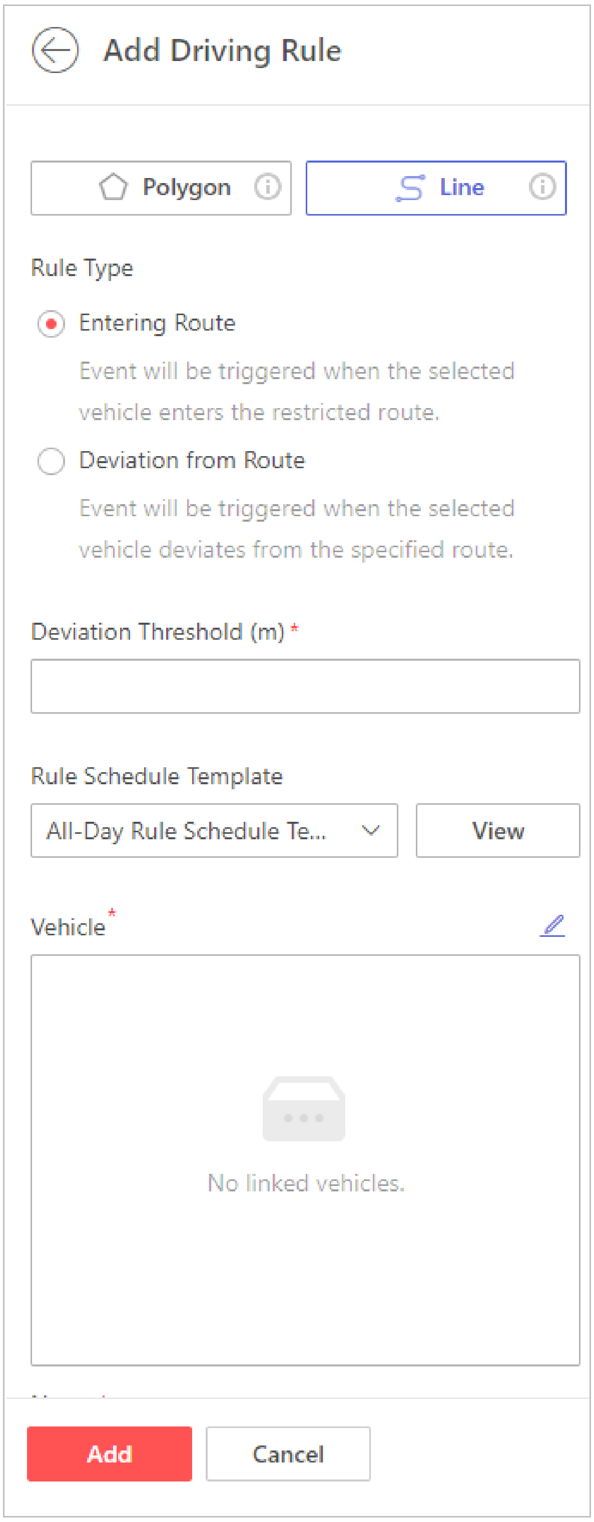
You can add a driving rule to specify the route which vehicles should drive along or should not enter.

Steps

1. Go to the driving rule configuration page.

- On the top navigation bar, click **On-Board Monitoring → Driving Rule Configuration → Driving Rule Configuration** .
- In the service overview section on the Home page, click **On-Board Monitoring → Driving Monitoring Configuration** .

2. Click + to enter the Add Driving Rule page.



Add Driving Rule

Rule Type

● Entering Route

Event will be triggered when the selected vehicle enters the restricted route.

○ Deviation from Route

Event will be triggered when the selected vehicle deviates from the specified route.

Deviation Threshold (m) *

Rule Schedule Template

All-Day Rule Schedule Te...

Vehicle*

No linked vehicles.

Figure 10-5 Add Driving Rule (Route)

3. Select **Line** which is suitable for configuring rules of deviating from a route or entering a restricted route.

4. Draw a route on the map for setting the rule.

Note

Click to start drawing and right-click to finish. After forming a region, drag a point to move it.

5. Select the rule type.

Entering Route

Events will be triggered when the selected vehicles enter the restricted route.

Deviation from Route

Events will be triggered when the selected vehicles deviate from the specified route.

6. Set other rule information.

1) Set the deviation threshold (m).

2) Select a rule schedule template.

Note

You can click **View** to view the scheduled time of the selected template. If you have not configured any rule schedule template, you can see ***Configure a Rule Schedule Template*** for how to configure one.

3) Click ✎ to select vehicle(s) that the rule will be applied to.

4) Set a name for the rule.

5) **Optional:** Enter the rule description.

7. Click **Add**.

8. Optional: Perform the following operations after configuring the driving rules.

Manage the Map

- Click ⛶ to display the map in full-screen mode.
- Enter keywords on the top right of the map to search for a location.
- Click the thumbnail for map on the bottom right and change the map type (default, topographic map, or satellite map).
- Click + / – to zoom in/out.

Edit a Driving Rule

Move your cursor to the rule to be edited on the rule list and click ✎ to enter the editing page.

Copy a Driving Rule

Move your cursor to the rule to be copied on the rule list and click ⎘ to enter the Add Driving Rule page with the same rule settings.

Filter Driving Rules

On the rule list, click ▽ on the upper right, set filtering conditions, and click **OK** to filter rules.

Delete Driving Rules

On the rule list, select one or multiple rules and click 🗑 to delete them, or move your cursor to the rule to be deleted on the rule list and click 🗑 to delete it.

10.3.3 Configure a Rule Schedule Template

You can add a rule schedule template to define the time when the related driving rules are effective in a week.

Steps

1. Go to the rule schedule template page.
   - On the top navigation bar, click **On-Board Monitoring → Driving Rule Configuration → Rule Schedule Template** .
   - In the service overview section on the Home page, click **On-Board Monitoring → Driving Monitoring Configuration → Rule Schedule Template** .
2. Click ＋ to enter the Add Rule Schedule Template page.

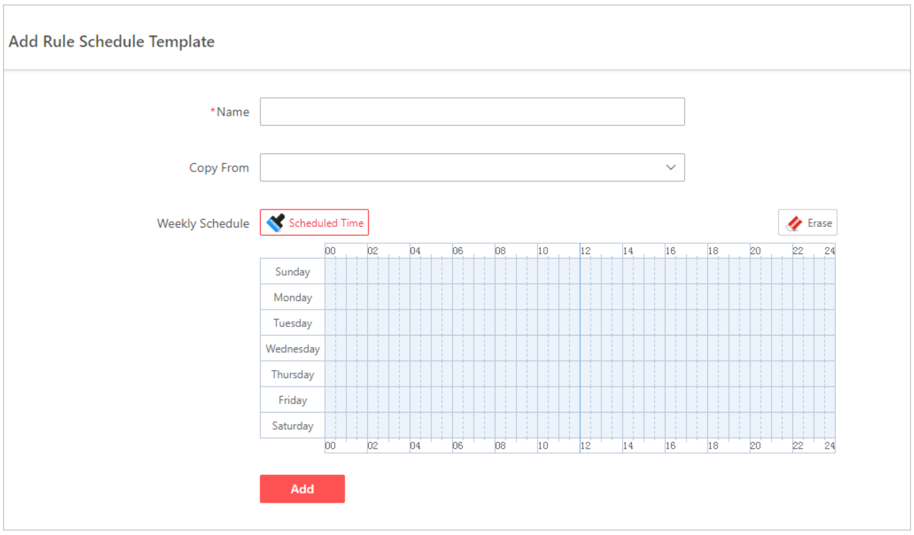


Figure 10-6 Add Rule Schedule Template

3. Create a name for the rule schedule template.
4. **Optional:** 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. **Optional:** Click **Erase** and click or drag on the formerly selected rectangle(s) to remove them from the scheduled time.
7. Click **Add**.
8. **Optional:** Perform the following operations.

Edit a Rule Schedule Template	On the template list, click a rule schedule template to edit it.

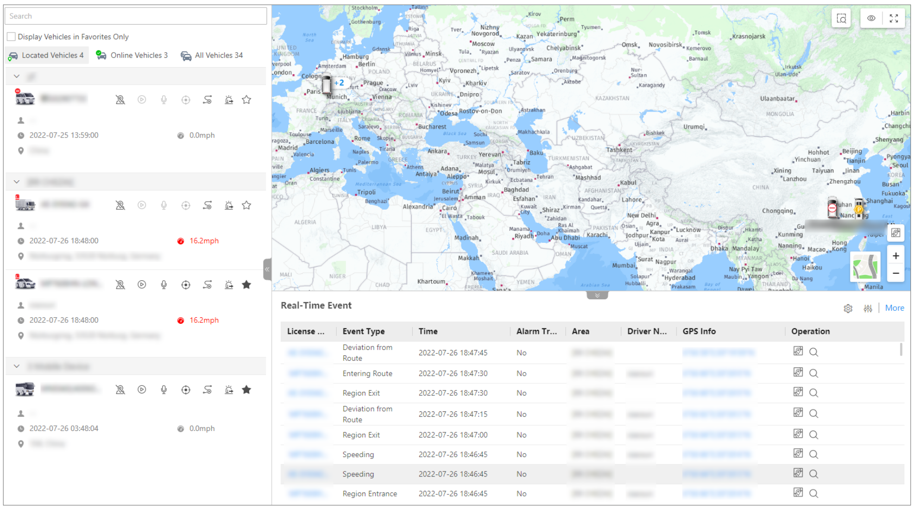
Delete a Rule Schedule Template	On the template list, select a rule schedule template and click 🗑 to delete it.

10.4 Driving Monitoring

The Driving Monitoring functionality is for monitoring vehicles. It provides various information such as the location, status, and speed of a vehicle, and also provides a range of applications including live view, two-way audio, vehicle tracking, and track playback.

Go to the Driving Monitoring page by either of the following entrances.

- On the top navigation bar, click **On-Board Monitoring → Driving Monitoring** .
- In the service overview section on the Home page, click **On-Board Monitoring → Driving Monitoring** .



Search

□ Display Vehicles in Favorites Only

Located Vehicles 4 · Online Vehicles 3 · All Vehicles 34

[redacted]

[redacted] ☆
2022-07-25 13:59:00 · 0.0mph

[redacted]

[redacted] ☆
2022-07-26 18:48:00 · 16.2mph

[redacted] ★
2022-07-26 18:48:00 · 16.2mph

[redacted]

[redacted] ★
2022-07-26 03:48:04 · 0.0mph

Real-Time Event · More

License ...	Event Type	Time	Alarm Tr...	Area	Driver N...	GPS Info	Operation
[redacted]	Deviation from Route	2022-07-26 18:47:45	No	[redacted]		[redacted]	
[redacted]	Entering Route	2022-07-26 18:47:30	No	[redacted]	[redacted]	[redacted]	
[redacted]	Region Exit	2022-07-26 18:47:30	No	[redacted]		[redacted]	
[redacted]	Deviation from Route	2022-07-26 18:47:15	No	[redacted]	[redacted]	[redacted]	
[redacted]	Region Exit	2022-07-26 18:47:00	No	[redacted]	[redacted]	[redacted]	
[redacted]	Speeding	2022-07-26 18:46:45	No	[redacted]	[redacted]	[redacted]	
[redacted]	Speeding	2022-07-26 18:46:45	No	[redacted]		[redacted]	
[redacted]	Region Entrance	2022-07-26 18:46:45	No	[redacted]	[redacted]	[redacted]	

Figure 10-7 Driving Monitoring Page

This functionality is introduced in sections as follows.

- ***Vehicle List Pane***
- ***Map***
- ***Real-Time Event***

Vehicle List Pane

On the vehicle list pane, you can perform operations as follows.

Operation	Description
Search for Vehicles	Enter the license plate number in the search box to search for the target vehicle.
Display Vehicles in Favorites Only	Check **Display Vehicles in Favorites Only** to only show the vehicles added to Favorites.

Operation	Description
Switch the Vehicle List	Click **All Vehicles**, **Online Vehicles**, or **Located Vehicles** to display the corresponding vehicle list.
Center a Vehicle	Click a vehicle to center the vehicle on the map.
Show the Vehicle Pane	Hover on a vehicle to show the vehicle pane. You can view the vehicle information, driver information, and camera information. By clicking a camera, you can start playing the live/ recorded video.
Locate a Vehicle / Cancel Locating a Vehicle	Click 📍 or 🚫 beside the vehicle name to locate a vehicle or cancel locating a vehicle.
Batch Locate Vehicles / Cancel Locating Vehicles	Click 📍 or 🚫 beside the area name to batch locate vehicles in an area or cancel locating the vehicles in an area.
Live View & Playback	Click ▶ to start playing the live/recorded video.
Two-Way Audio	Click 🎙 to start the two-way audio.
Track a Vehicle	Click ⌖ to track the real-time movement of the vehicle.
Play Back Track	Click ↺ , select a time period, select cameras for playback, and click **Start Playback** to play back the track the vehicle has traveled along during that period.
Control Alarm Outputs	Click 🔔 to open the Alarm Output Control pane, and then click **Disable** or **Enable** to control an alarm output.
Add a Vehicle to Favorites / Remove a Vehicle from Favorites	Click ☆ or ★ to add the vehicle to Favorites or remove it from Favorites.

Map

On the Map section, you can perform operations as follows.

Operation	Description
Specify an Area	Click ⬚ , and click and drag on the map to specify an area for vehicle search. You can batch

Operation	Description
	locate the searched vehicles. Right-click to exit the search.
Display the Driving Rule on Map	Click , and check **Driving Rule** and/or **Driving Rule Name**.
Switch to Full Screen Mode	Click to switch to full screen mode.
Switch the Map Type	Click and select **Default**, **Topographic Map**, or **Satellite Map**.
Center Vehicles	Click to center vehicles of the selected vehicle list on the map.
Zoom In/Out	Click + or − to zoom in or zoom out.
View Alarm Details	Click to view the alarm details. • Select the alarm priority and alarm category, enter the remark, and click **Acknowledge**/ **Acknowledge and Archive** to acknowledge / acknowledge and archive the alarm. • Click **Alarm Output Control** to enable/disable alarm outputs. • Click **Two-Way Audio** to start talk to the driver. • Click **Send Email** to send an email containing the alarm details to specified recipients. • Click **Track Playback** to play back the track. • Click **Live View** to start real-time tracking. • Check **Enable Pop-up Window** to pop up a window when an alarm is triggered.

Real-Time Event

You can view details about real-time events, including the license plate number, event type, time, alarm status, area, driver name, and GPS information. You can also perform operations as follows.

Operation	Description
View Event Details	Click the license plate number to view details. • Click **Alarm Output Control** to disable/enable alarm outputs. • Click **Two-Way Audio** to start two-way audio. • Click **Archive** to archive the event.

Operation	Description
	• Click **Track Playback** to play back the track. • Click **Live View** to start real-time tracking.
Locate the Event	Click the GPS info to locate the position where the event occurred on the map.
Center the Vehicle	Click to center the vehicle on the map.
View the Event on the Driving Event Search Page	Click to go to the Driving Event Search page to view the event. For details, refer to ***Search for Driving Events*** .
Set Event Types	Click to set the event types that will be received by the current account.
Custom Column Item	Click to set the displayed column items.
Go to the Driving Event Search Page for More Events	Click **More** to go to the Driving Event Search page and search for more events. For details, refer to ***Search for Driving Events*** .

10.5 Search for Tracks

You can search for the tracks that vehicles have traveled along in the specified period, view detailed information of each record, play back tracks, and export records to the PC.

Steps

1. On the top navigation bar, click **On-Board Monitoring → Track Search** .

2. Set search conditions.

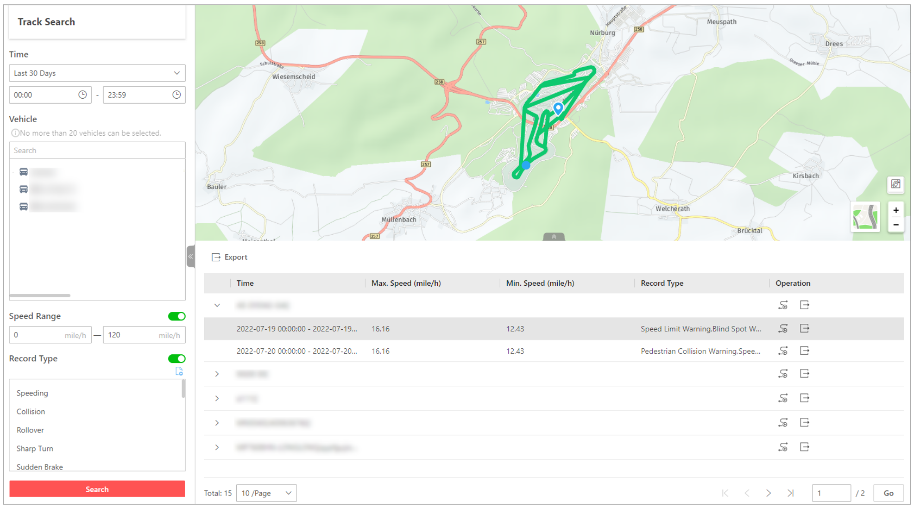
1) Specify the time period in which you want to search for vehicle tracks.

2) Select vehicle(s).

3) **Optional:** Switch on **Speed Range** and set a speed range.

4) **Optional:** Switch on **Event Type** and click to select event type(s).

3. Click **Search**.


Track Search

Time

Last 30 Days

00:00 - 23:59

Vehicle

ⓘNo more than 20 vehicles can be selected.

Search

[redacted]

Speed Range

0 mile/h — 120 mile/h

Record Type

Speeding

Collision

Rollover

Sharp Turn

Sudden Brake

Search

Export

	Time	Max. Speed (mile/h)	Min. Speed (mile/h)	Record Type	Operation
⌄	[redacted]				
	2022-07-19 00:00:00 - 2022-07-19...	16.16	12.43	Speed Limit Warning,Blind Spot W...	
	2022-07-20 00:00:00 - 2022-07-20...	16.16	12.43	Pedestrian Collision Warning,Spee...	
›	[redacted]				
›	[redacted]				
›	[redacted]				
›	[redacted]				

Total: 15 10 /Page 1 / 2 Go

Figure 10-8 Track Search

4. Optional: Perform the following operations.

Play Back a Track Click in the Operation column to play back a track.

You can select cameras for playback.

Export Records Click in the Operation column to export a single record to the PC.

Click **Export** on the upper left of the record list to export all records to the PC.

Center Vehicles Click to center vehicles on the map.

Switch the Map Type Click and select **Default**, **Topographic Map**, or **Satellite Map**.

Zoom In/Out Click + or − to zoom in or zoom out the map.

Other Click › to display more records.

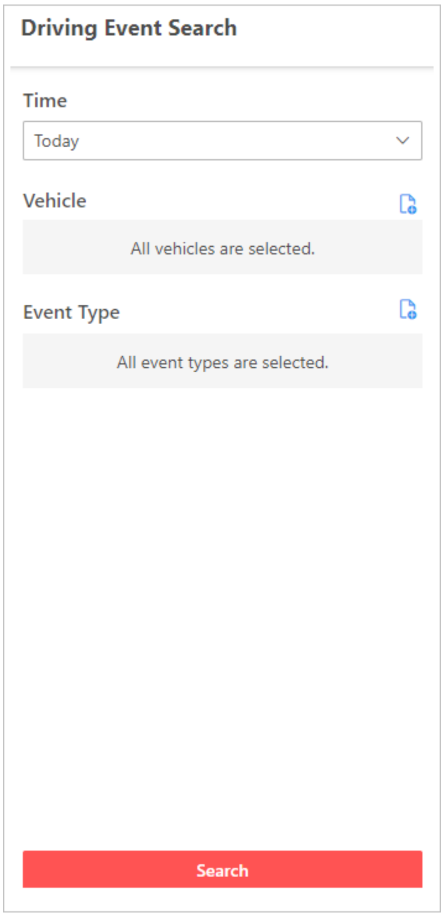
10.6 Search for Driving Events

You can search for the events triggered by vehicles, view detailed information of each record, and export records to the PC.

Steps

1. On the top navigation bar, click **On-Board Monitoring → Driving Event Search** .

2. Set search conditions.



Driving Event Search

Time

Today

Vehicle

All vehicles are selected.

Event Type

All event types are selected.

Figure 10-9 Driving Event Search Page

1) Specify the period you want to search for driving events in.
2) Select vehicles.
3) Select event types.

3. Click **Search**.

4. Optional: Perform the following operations.

Play Back a Track	Click to play back a track. You can select cameras for playback.
Export Records	Click in the Operation column to export a single record to the PC. Click **Export** on the upper left of the record list to export all matched records to the local PC.
Archive a Record	Click in the Operation column to archive the record.
View Event Details	Click the license plate number to view details. • Click **Alarm Output Control** to disable/enable alarm outputs. • Click **Two-Way Audio** to start two-way audio. • Click **Archive** to archive the event.

- Click **Track Playback** to play back the track.
- Click **Live View** to start real-time tracking.

Locate the Event
Click the GPS information to locate the position where the event occurred on the map.

Specify an Area
Click , and click and drag on the map to specify an area for vehicle search. You can batch locate the searched vehicles. Right-click to exit the search.

Switch the Map Type
Click and select **Default**, **Topographic Map**, or **Satellite Map**.

Center Vehicles
Click to center vehicles of the selected vehicle list on the map.

Zoom In/Out
Click + or – to zoom in or zoom out the map.

10.7 Statistics and Reports

Hik Connect for Teams provides multiple types of reports for you to get insight into the variation trend of the driving data related to the vehicles in your company/organization. These reports, which can be exported to your local PC, demonstrate data through tables, helping you make better business decisions, operation strategies, etc.

10.7.1 Generate a Driving Duration Report

You can generate a driving duration report to view the driving duration of specific vehicle at a certain speed in a certain period.

Steps

1. On the top navigation bar, click **On-Board Monitoring → Statistics and Reports → Driving Duration Report** .
2. Set search conditions.

   Vehicle

   Select one or multiple vehicles.

   Note

   Up to 20 vehicles can be selected.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the data of the selected vehicle in one calendar day.

   Weekly Report

The report to be generated will show the data of the selected vehicle in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicle in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicle in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

Driving Speed Exceeds

Set the speed threshold (0 mile/h, 20mile/h, 40 mile/h, 60 mile/h, or 80 mile/h) for calculating the driving duration. For example, if you select **20 mile/h**, the driving duration with vehicle speed over 20 mile/h will be calculated.

3. Click **Generate Report**.

The data will be shown on the right side of the page.

4. **Optional:** Perform the following operations.

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.
View Data in Table	View the data in a table that shows the license plate number, area, start time, end time, driving duration, maximum speed, minimum speed, start location, and end location. You can click in the Start Location column or End Location column to view the location on the map. You can select a vehicle from the drop-down list and set a period to further filter the data.
Export Report	Click **Export** to open the Export pane, and then set parameters including Vehicle, Time, Export By, and Export In. For the **Export By** parameter, you can set the content (brief or detailed) of the report to be exported.

For **Export In**, you can set the format of the report.

10.7.2 Generate a Driving Distance Report

You can generate a driving distance report to view the driving distance of specific vehicles in a certain period.

Steps

1. On the top navigation bar, click **On-Board Monitoring → Statistics and Reports → Driving Distance Report** .
2. Set search conditions.

   Vehicle

   Select one or multiple vehicles.

   Note

   Up to 20 vehicles can be selected.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the driving distance of the selected vehicles in one calendar day.

   Weekly Report

   The report to be generated will show the driving distance of the selected vehicles in one calendar week.

   Monthly Report

   The report to be generated will show the driving distance of the selected vehicles in one calendar month.

   Custom Time Interval

   The report to be generated will show the driving distance of the selected vehicles in a custom period of no more than 31 days.

   Time

   The driving distance in the selected period will be shown in the report.

   - For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
   - For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
   - For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
   - For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

The data will be shown on the right side of the page.

4. Optional: Perform the following operations if needed.

View Detailed Data
: Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.

View Data in Table
: View the data in a table that shows the license plate number, area, time, and driving distance.

  You can select a vehicle from the drop-down list and set a period to further filter the data.

Export Report
: Click **Export** to open the Export pane, and then set parameters including Vehicle, Time, and Export In.

  For Export In, you can set the format of the report.

10.7.3 Generate a Speeding Report

You can generate a speeding report to view the times that specific vehicles overspeed in a specific period.

Steps

1. On the top navigation bar, click **On-Board Monitoring → Statistics and Reports → Speeding Report** .

2. Set search conditions.

Vehicle

Select one or multiple vehicles.

Note

Up to 20 vehicles can be selected.

Report Type

Select a report type.

Daily Report

The report to be generated will show the data of the selected vehicles in one calendar day.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

   The data will be shown on the right side of the page.

4. **Optional:** Perform the following operations if needed.

View Detailed Data

Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.

View Data in Table

View the data in a table that shows the license plate number, area, time, data, direction, and speed.

You can click in the GPS Info column to view the location on the map.

You can select a vehicle from the drop-down list and set a period to further filter the data.

Export Report

Click **Export** to open the Export pane, and then set parameters including Vehicle, Time, Export By, and Export In.

For the Export By parameter, you can set the content (brief or detailed) of the report to be exported.

For Export In, you can set the format of the report.

10.7.4 Generate a Driving Event Report

You can generate a driving event report to view the number of events and event details related to specific vehicles in a specific period.

Steps

1. On the top navigation bar, click **On-Board Monitoring → Statistics and Reports → Driving Event Report** .
2. Set search conditions.

   Vehicle

Select one or multiple vehicles.

Note

Up to 20 vehicles can be selected.

Report Type

Select a report type.

Daily Report

The report to be generated will show the data of the selected vehicles in one calendar day.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

Event Type

By default, all event types are selected.

You can click to select the events to be calculated.

3. Click **Generate Report**.

The data will be shown in a line chart on which the Y-axis represents the number of events and the X-axis the time.

4. **Optional:** Perform the following operations.

View Detailed Data

Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.

View Data in Table

View the data in a table that shows the license plate number, record type, time, area, driver, GPS Info, and direction.

You can click in the GPS Info column to view the location on the map.

You can select a vehicle from the drop-down list and set a period to further filter the data.

Export Report

Click **Export** to open the Export pane, and then set parameters including Vehicle, Time, Record Type, Export By, and Export In.

For the Export By parameter, you can set the content (brief or detailed) of the report to be exported.

For Export In, you can set the format of the report.

Chapter 11 Analysis Report

By subscribing to the analysis report service, users 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.

11.1 Basic Configuration

In order to check the statistics (e.g., customer traffic, walk-in rate, etc.) of a site and the impact a promotion had on your site, you should create an analysis configuration for the corresponding area, specify which cameras are used for people counting at the entrances & exits, configure a global heat map as needed, and add the corresponding promotion period. You can also monitor the health status of the cameras with people counting / heat analysis capability which are added to the corresponding area.

11.1.1 Add Analysis Configuration

You can create an analysis configuration for the corresponding area of the site whose statistics you want to check.

Steps

1. On the top navigation bar, select **Analysis Report → Configuration → Analysis Configuration** .
2. Click + **Analysis Configuration**.

   The Analysis Configuration pane will show on the right.
3. Select an area from the resource tree.

   Note

   The root area and an area whose child area is already configured with an analysis configuration cannot be selected.
4. Specify the opening hours of your site.
5. **Optional:** Hover the cursor over the GIS map and click to place the site icon on the map. You can locate the site location quickly on the map by entering the site address in the search box.

Note

- After placing the icon on the map, the corresponding address will show in the text box above the map. You can edit the address if needed.
- If you need to adjust where you place the icon, click and drag it to a new location. The location above the map will also be adjusted accordingly.

6. Optional: Enter the name of the person in charge, a phone number for contact purposes, and the relevant notes.

7. Click **Save**.

8. Optional: Perform the following operations as needed.

Edit Site Information

You can edit the information of the site, such as the opening hours, geographic location, the person in charge, phone number, etc.

- Select an area that is configured with an analysis configuration from the left tree to enter its details page, and click **Edit** on the top right. Such an area is marked with 🏢 .
- Select a parent area from the left tree to view its child areas that have configured with analysis configurations on the right. Click a name to enter its details page, and click **Edit** on the top right.

Delete Analysis Configuration(s)

- On the left tree, hover the cursor over an area that is configured with an analysis configuration and click 🗑 . Such an area is marked with 🏢 .
- Select a parent area from the left tree to view its child areas that have configured with analysis configurations on the right. Select the area(s) and click **Delete**.

Batch Configure Opening Hours

Select a parent area from the left tree to view its child areas that have configured with analysis configurations on the right. Select the area(s) and click **Configure Opening Hours**.

Search for Analysis Configuration(s)

Enter the name of an area configured with an analysis configuration in the search box above the left tree to search in the root area, and in the search box on the top right to search in the parent area selected. Supports fuzzy search.

What to do next

Go to a site details page to specify which cameras are used for people counting at each entrance & exit and configure a global heat map as needed. Refer to ***Configure the Source of People Counting Data*** and ***Configure Global Heat Map*** respectively for details.

11.1.2 Configure the Source of People Counting Data

In order to view statistics such as the number of people walking in or passing by, you need to specify which cameras are used for people counting at each entrance & exit. You can also enable real-time people counting and set a threshold each for triggering overcapacity alarms and pre-alarms.

Before You Start

Make sure you have added an analysis configuration for the corresponding area of the site whose statistics you want to check. Refer to ***Add Analysis Configuration*** for details.

Steps

1. On the top navigation bar, select **Analysis Report → Configuration → Analysis Configuration** .

2. Enter the site details page.

- Locate or search for the target area in the left area tree. An area that is configured with an analysis configuration is marked with . Click the name of the target area to enter its details page.
- Select the parent area to which the target area belongs from the left area tree to view all its child areas that have configured with analysis configurations on the right. Click the name of the target area to enter its details page.

3. Click **Configure** below the People Counting field.

Note

If the area already has the global heat map configured, select the **People Counting** tab first and then click **Configure**.

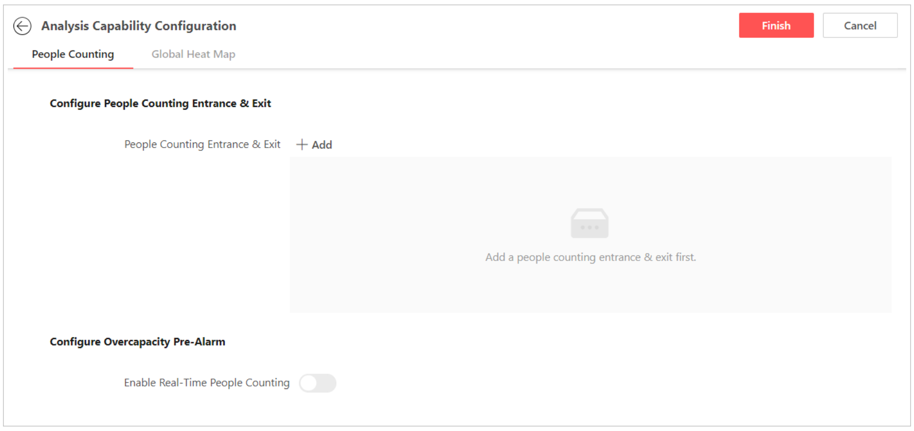

Analysis Capability Configuration
Finish
Cancel
People Counting
Global Heat Map
Configure People Counting Entrance & Exit
People Counting Entrance & Exit
+ Add
Add a people counting entrance & exit first.
Configure Overcapacity Pre-Alarm
Enable Real-Time People Counting

Figure 11-1 People Counting Configuration Page

4. Configure the entrances and exits according to the actual situation of the site.

1) Click **Add** to open the Add People Counting Entrance & Exit pane.

2) Create a name for the entrance & exit.

3) Select which cameras of this area are to be used for counting the people walking in (required) and the people passing by (optional) at this entrance & exit.

Note

No more than 10 cameras are allowed to be selected for each type of use.

4) **Optional:** Select whether to use the data collected at this entrance & exit as the source of the people counting statistics of this area.

Note

It is enabled by default.

5) Click **Save**.

Note

Repeat the above steps to create more entrances & exits as needed.

5. Optional: Switch on **Enable Real-Time People Counting** to configure the overcapacity rules.

1) Select a time from the drop-down list to set a fixed time for clearing the people counting data. You can also switch off **Regularly Clear All** if you do not need the regular data clearing function.
2) Select whether to create rules for triggering overcapacity alarms and pre-alarms by ticking/ unticking the corresponding boxes and setting the corresponding people counting threshold.

Note

- You have to configure at least one overcapacity rule.
- The people counting threshold you enter for overcapacity pre-alarms cannot be greater than that for overcapacity alarms.
- If you have not configured any alarm rules for overcapacity before, an alarm rule will be created for you in the Alarm module by default (with no alarm linkage or notification settings configured) with the area as the source of the alarm.
- If you have configured an alarm rule for overcapacity before, you can click **Configure Alarm Rule** to go to the Alarm Configuration page to edit the rule as needed.

6. Click **Finish** on the top right.

7. Perform the following operations.

Edit Configuration	On the People Counting tab of the site details page, click **Edit Configuration** to edit the people counting configurations.
Check Device Health Status	On the Health Status tab of the site details page, you can check the status of the people counting cameras. You can click **Refresh** to retrieve the latest camera status, search for the cameras by name, and filter the cameras by status. You can also click 🗎 in the Operation column of a camera to view the recent data reported by the camera or click ⚙ to enter its remote configuration page.

11.1.3 Configure Global Heat Map

In order to have a grasp on the overall heat analysis data of a site, you need to configure a global heat map and specify the locations of the heat analysis cameras. If there is no global heat map configured for the site, you can only view the individual heat analysis data of each camera, i.e., partial heat analysis data of the site.

Before You Start

Make sure you have added an analysis configuration for the corresponding area of the site whose heat analysis data you want to check. Refer to ***Add Analysis Configuration*** for details.

Steps

1. On the top navigation bar, select **Analysis Report → Configuration → Analysis Configuration** .
2. Enter the site details page.
   - Locate or search for the target area in the left area tree. An area that is configured with an analysis configuration is marked with . Click the name of the target area to enter its details page.
   - Select the parent area to which the target area belongs from the left area tree to view all its child areas that have configured with analysis configurations on the right. Click the name of the target area to enter its details page.
3. Click **Configure** below the Global Heat Map field.

   Note

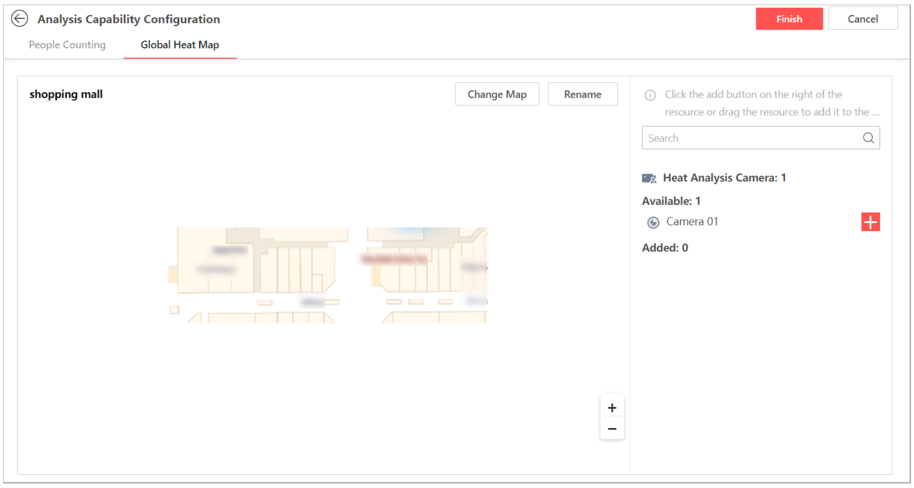
   If the area already has the people counting parameters configured, select the **Global Heat Map** tab first and then click **Configure**.

4. Click **Add Map**, click and then select the map image to be uploaded from your local PC, enter/edit the name of the map, and click **Save**.

   Note

   You can click **Add Map** to upload more static maps if needed.

5. Click the map to be used as the global heat map of the site and then click **Select Map** on the top right corner of the map.



Click the add button on the right of the resource or drag the resource to add it to the ...

Heat Analysis Camera: 1

Available: 1

Camera 01

Added: 0

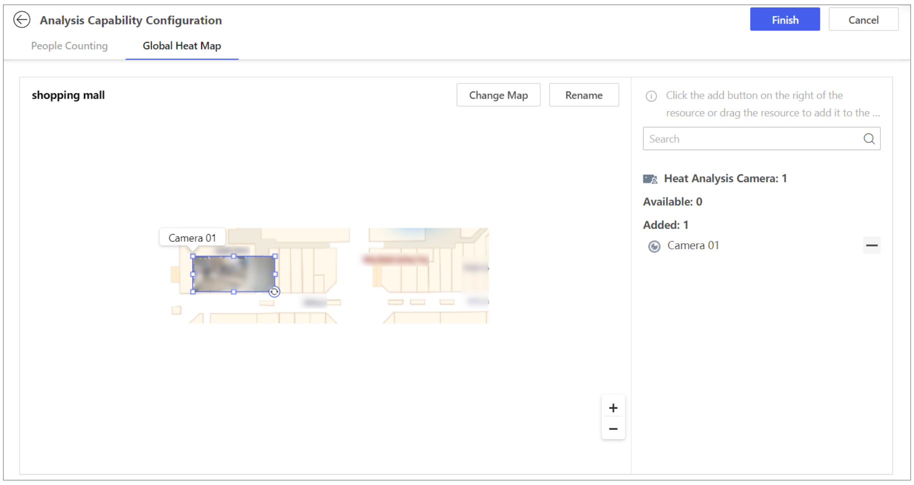
Figure 11-2 Configure Global Heat Map Page

6. Configure the locations of the heat analysis cameras on the map.
   1) Click ⊞ next to an available camera in the camera list or drag the camera to add it to the map. You can search for cameras by camera name.

Note

You can click – next to an added camera in the camera list to remove it from the map if needed.

2) Click a camera image and drag it on the map to adjust the camera location according to its actual position at the site.
3) Click a camera image and rescale the region covered by the camera by dragging the handle on each side or corner. You can also rotate the region if needed by dragging the handle located on the lower right corner of the camera image.



Click the add button on the right of the resource or drag the resource to add it to the ...

Heat Analysis Camera: 1

Available: 0

Added: 1

Camera 01

Figure 11-3 Handles for Rescaling and Rotating Camera Image

7. Click **Finish** on the top right.

8. Perform the following operations.

Edit Configuration

On the Global Heat Map tab of the site details page, click **Edit Configuration** to edit the map details. You can rename the map, change to another static map, add cameras to or remove cameras from the map, and edit the corresponding camera locations.

Clear Map Configurations

On the Global Heat Map tab of the site details page, click **Clear Configurations** to clear all configurations of the current map. The global heat map will not be displayed in the reports any more until you configure a new one.

Check Device Health Status

On the Health Status tab of the site details page, you can check the status of the heat analysis cameras.

You can click **Refresh** to retrieve the latest camera status, search for the cameras by name, and filter the cameras by status. You can also click 🗎 in the Operation column of a camera to view the recent data reported by the camera or click ⚙ to enter its remote configuration page.

11.1.4 Add Promotion

You can add promotions that are globally effective to check the impact a promotion had on a site, such as how many more customers a promotion brought in than the days without a promotion.

Steps

1. On the top navigation bar, select **Analysis Report → Configuration → Promotion Configuration** .
2. Click **Add** at the top.
3. Enter a name for the promotion and specify the promotion period.
4. Click **Save** to add the promotion.
5. Optional: Perform the following operations as needed.

Edit Promotion	Click the name of an added promotion to edit its name and the promotion period.
Delete Promotion(s)	Select the added promotion(s) and click **Delete**.
Search for Promotion(s)	Enter the promotion name in the search box on the top right to search for the promotion(s). Supports fuzzy search.

What to do next

Check the impact of the added promotion on a site. Refer to ***View Promotion Report*** for details.

11.2 View General Report

By checking the general report, you can get the 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 see the comparison results between the current cycle and the previous cycle.

Note

Make sure you have created an analysis configuration for the site for which you want to check the statistics. Refer to ***Add Analysis Configuration*** for details.

Go to the General Report page by clicking **Analysis Report** on the top navigation bar and select **Report → General Report** .

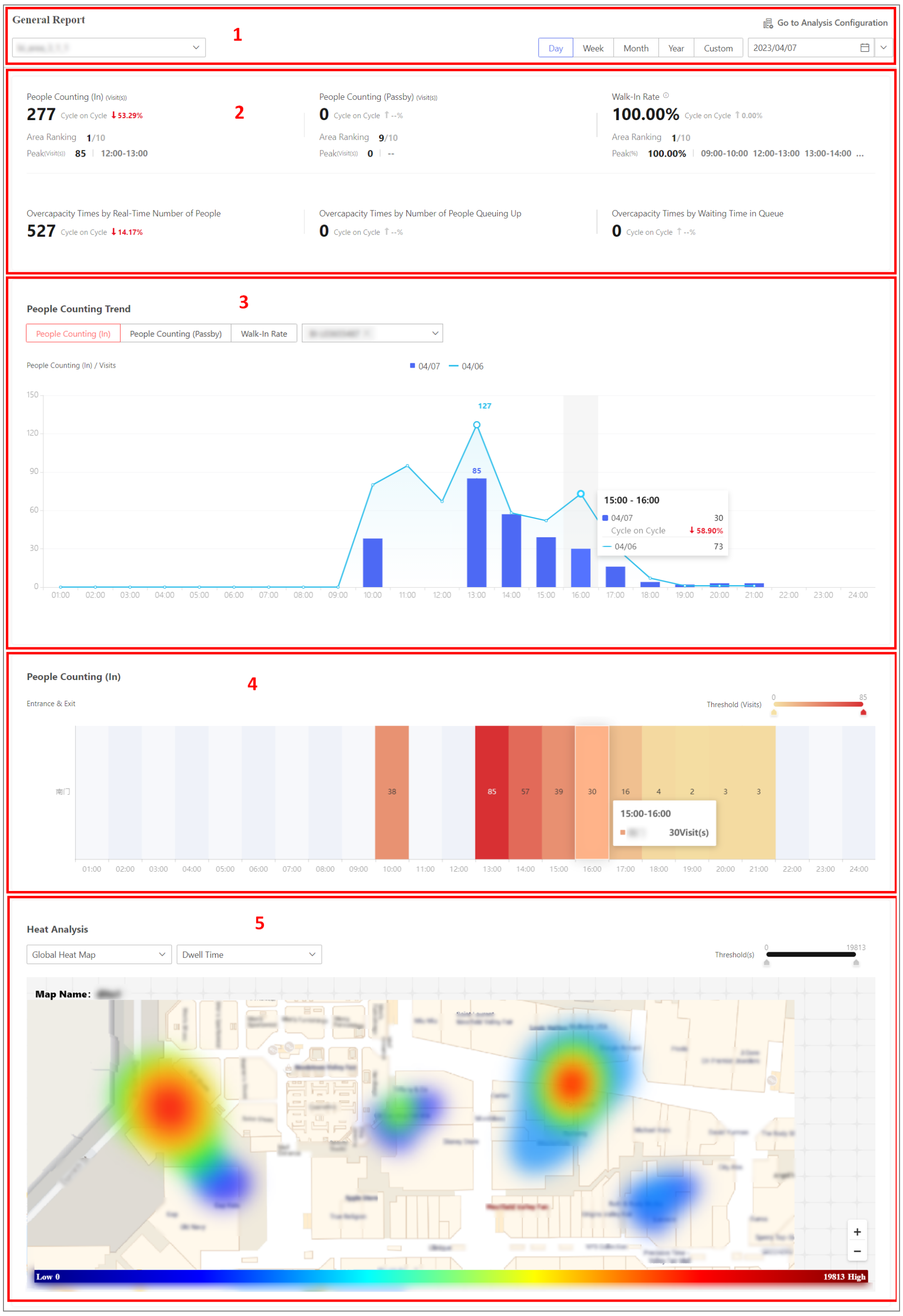


Figure 11-4 Sample General Report (Daily Report)

Table 11-1 General Report Section Introduction

Section No.	Description
1	The section where you can switch between sites and change the report type. You can choose to generate a daily/weekly/ monthly/annual report or a report of a custom time range (up to

Section No.	Description
	31 days). After you select a report type, you can specify the detailed report cycle via the right drop-down list. **Note** Upon you enter the General Report page, a weekly report of the current week (which starts on Sunday and ends on Saturday) for the site that you last viewed is displayed by default. You can click **Go to Analysis Configuration** on the top right to go to the site details page and edit the analysis configuration of the site as needed.
2	The section where you can check the site's overall people counting statistics of the specified time period, which include the followings: • The number of people that walked in, the number of people that passed by, and the walk-in rate. • The area ranking for each of the above-mentioned types of data, as well as the peak value and the specific time interval(s) of the peak value. • The overcapacity times by the real-time number of people, the number of people queuing up, and waiting time in a queue. • The cycle-on-cycle result (in the form of a percentage) between the specified cycle and the previous cycle for all six types of data. **Note** These statistics will only be available if you have configured the source of people counting data. Refer to ***Configure the Source of People Counting Data*** for details.
3	The section where you can view the trends of each type of the people counting data of the specified time period. The horizontal axis represents the time interval and the vertical axis represents the type of data selected in the top left of this section. Data of the current cycle are displayed in bars whereas those of the previous cycle are displayed in lines. You can filter the data by entrance & exit and hover the cursor over the graph to view the detailed statistics of a specific interval.

Section No.	Description
	Note If there is a promotion during the specified time period, the background of the corresponding day(s) will be marked in red shade.
4	The section where you can view the heat map of the people counting data of the specified time period. The horizontal axis represents the time interval and the vertical axis represents the entrances & exits (each entrance & exit takes up an individual row). You can drag the endpoints of the threshold bar located on the top right of this section to adjust the range of the data displayed on the heat map. You can also hover the cursor over a cell to view the detailed statistics of a specific interval and a specific entrance & exit. **Note** If there is a promotion during the specified time period, the background of the corresponding day(s) on the timeline will be marked in red shade.
5	The section where you can view the heat analysis results on a global heat map or the live image of each heat analysis camera. You can switch between the global heat map and the live images of cameras via the leftmost drop-down list. You can also select whether to show the heat analysis results by the number of people staying in an area or by the dwell time via the other drop-down list. **Note** If there is no global heat map configured for the site, you can only view the heat analysis data of each heat analysis camera added to this area. Refer to ***Configure Global Heat Map*** for how to configure a global heat map. The heat analysis data displayed in this section are cumulative. You can click a time interval on the horizontal axis to view data for a specific interval. You can also drag the endpoints of the threshold bar located on the top right of this section to adjust the range of the heat analysis results.

11.3 View Promotion Report

By checking the promotion report, you can have a grasp on the effect of a promotion by comparing the statistics collected in the promotion period with those of 7 days before and after the promotion.

Note

- Make sure you have created an analysis configuration for the site for which you want to check the statistics. Refer to ***Add Analysis Configuration*** for details.
- Make sure you have added the promotion. Refer to ***Add Promotion*** for details.

Go to the Promotion Report page by clicking **Analysis Report** on the top navigation bar and select **Report → Promotion Report** .

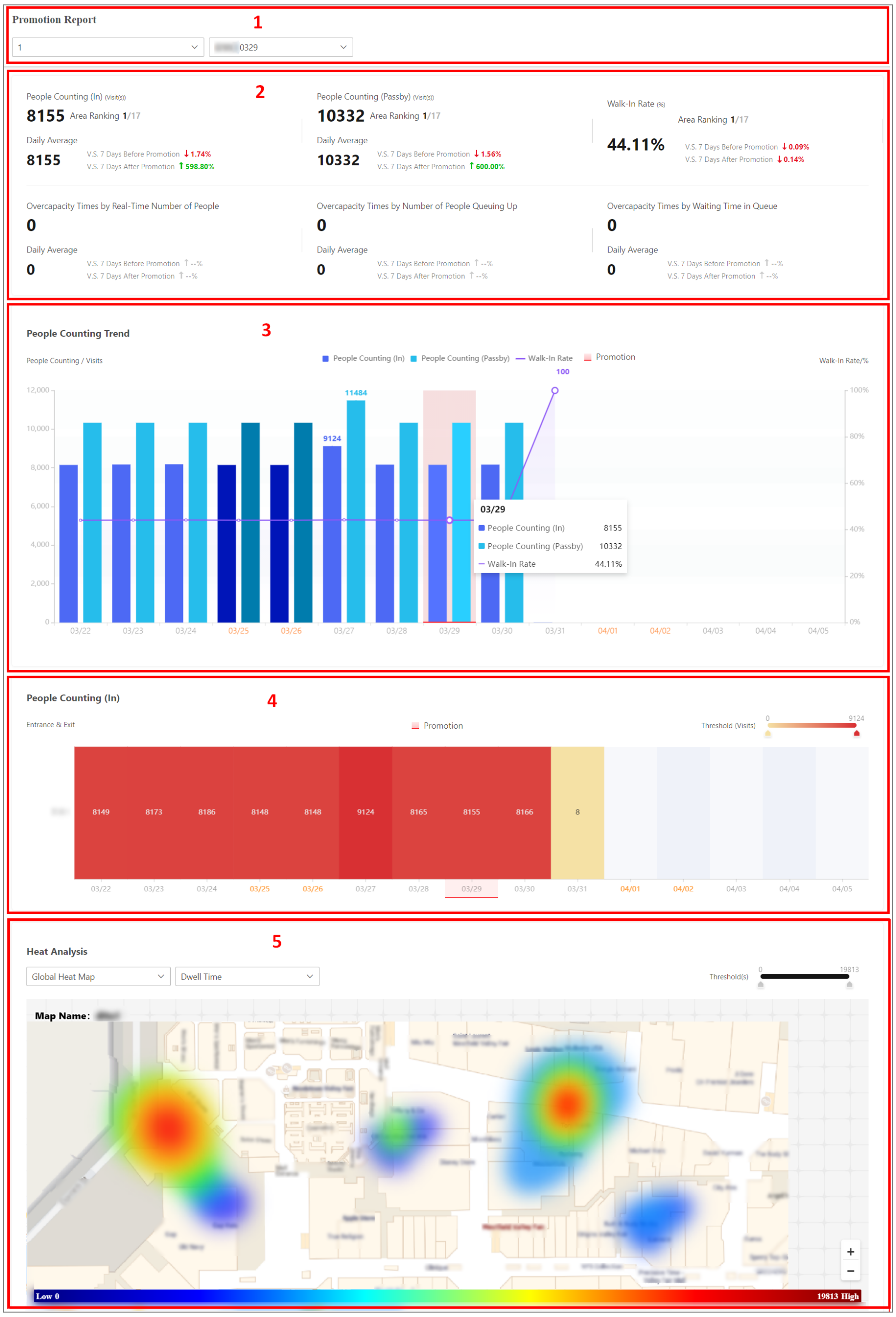


Figure 11-5 Sample Promotion Report

Table 11-2 Promotion Report Section Introduction

Section No.	Description
1	The section where you can switch between sites and select a promotion period.

Section No.	Description
	Note Upon you enter the Promotion Report page, the report of the closest promotion date for the site that you last viewed is displayed by default.
2	The section where you can check the site's overall people counting statistics during the promotion period, which include the followings: • The number of people that walked in, the number of people that passed by, the walk-in rate, and the area ranking for each of the above-mentioned types of data. • The overcapacity times by the real-time number of people, the number of people queuing up, and waiting time in a queue. • The daily average for all six types of data. • The comparison result (in the form of a percentage) between the data of the promotion period and those of 7 days before/ after the promotion for all six types of data. **Note** These statistics will only be available if you have configured the source of people counting data. Refer to ***Configure the Source of People Counting Data*** for details.
3	The section where you can compare the people counting data of the promotion period with those of 7 days before and after the promotion in a line/bar graph. The horizontal axis represents the date, the vertical axis on the left represents the number of visits, and the vertical axis on the right represents the walk-in rate (%). You can click a data type on the legend to hide the corresponding data on the graph. You can also hover the cursor over the graph to view the detailed statistics of a specific day.
4	The section where you can compare the people counting data of the promotion period with those of 7 days before and after the promotion in a heat map. The horizontal axis represents the date and the vertical axis represents the entrances & exits (each entrance & exit takes up an individual row). You can drag the endpoints of the threshold bar located on the top right of this section to adjust the range of the data displayed on the heat map. You can also hover the cursor over a cell to

Section No.	Description
	view the detailed statistics of a specific day and a specific entrance & exit.
5	The section where you can view the heat analysis results of the promotion period on a global heat map or the live image of each heat analysis camera. You can switch between the global heat map and the live images of cameras via the leftmost drop-down list. You can also select whether to show the heat analysis results by the number of people staying in an area or by the dwell time via the other drop-down list. **Note** If there is no global heat map configured for the site, you can only view the heat analysis data of each heat analysis camera added to this area. Refer to ***Configure Global Heat Map*** for how to configure a global heat map. The heat analysis data displayed in this section are cumulative. You can click a date on the horizontal axis to view data for a specific day. You can also drag the endpoints of the threshold bar located on the top right of this section to adjust the range of the heat analysis results.

Chapter 12 Map Management

Two types of map are available: GIS map and static map. You can add cameras, alarm outputs / zones, alarm inputs, and partitions (areas) to both maps. GIS maps are generally suitable for large-scale monitoring. For example, if you want to manage the traffic system of a city, you would need to use GIS maps; but if you want to monitor relatively small areas like a certain mall or company with a few floors, you would need to upload static maps for monitoring.

With GIS map, you can see the geographic locations of your security system. This type of map uses a geographic information system to accurately show all the hot spots' (resources (e.g., camera, alarm input) placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access cameras at multiple locations around the world in a geographically correct way. If the resources locate in multiple locations (e.g., different cities, different countries), GIS map can give you a single view to show them all and help you quickly go to each location to view video from the cameras. With the hot region, you can link to static maps to view the detailed monitoring scenario, for example, the monitoring scenario of a building.

Static maps do not have to be geographical maps, although they often are. Depending on your organization's needs, photos and other kinds of image files can also be used as e-maps which gives you a visual overview of the locations and distributions of the hot spots (resources (e.g., camera, alarm input) placed on the map are called hot spots). You can see the physical locations of the cameras, alarm inputs, and alarm outputs, etc., and in what direction the cameras are pointing.

After adding maps and resources to an area, you can monitor the area on map.

12.1 Map Settings

For a GIS map, you can set a monitored area on it. For a static map, you can directly add it to an area. After adding a map to an area, you can add hot spots, hot regions, and labels to the map.

12.1.1 Link Area with Map

You can link an area with map(s).

Steps

1. On the top navigation bar, click **Device and Maintenance → Resource Management** to go to the Resource Management page.
2. Select an area from the list.
3. Click 🗺 to enter the Map module and the Add static Map panel will pop up.
4. **Optional:** Select an area from the list.

Note

By default, the area you have selected previously will be displayed.

5. Add a map or link existing map(s).
   - Select **Add a Static Map** as the adding mode, and click 🗀 to select a static map from local PC.
   - Select **Select an Existing Map** as the adding mode, and select one or more maps from the map list below.

   Note

   You can enter keywords in the search box to search for target map(s).
6. **Optional:** If you have selected only one map in the previous step, check **Set as Default Static Map** to set the selected map as the default map.
7. Click **Add**.

   The area and the selected map(s) will be linked.

12.1.2 Change Monitored Area on GIS Map

There is a default GIS map added for areas. Adding, deleting, or editing the GIS map are not allowed. You can set a monitored area as needed.

Steps

1. On the top navigation bar, click **Map → Map Settings** .
2. Select an area in the top left corner.
3. Drag the map to set a monitored area for the selected area.
4. Click **Save**.
5. **Optional:** Click **Edit Map → Edit** to change to a new monitored area.
6. **Optional:** Click **Edit Map → Switch to Static Map** to switch to a static map.

12.1.3 Add Static Map for Area

You can select a static image from the local PC or add an existing static map to an area. For small-scale areas which can not be found on a GIS map, you can upload a customized map to an area. For example, if you want to monitor a mall with multiple floors, you can add static maps.

Steps

1. On the top navigation bar, click **Map → Map Settings** .
2. Select an area in the top left corner.
3. Click **Add Static Map**.
4. Select an adding mode.
   - Select **Add Static Map** and choose a map or multiple maps from local PC.
   - Select **Select Existing Map** and choose one or multiple existing maps.
5. **Optional:** Check **Set as Default Static Map** and the map will be set as the default map for the selected area.

Note

If you select multiple maps, the parameter will be unavailable.

6. Click **Add**.

7. Click **Edit Map** and perform the following operations after the map is added.

Rename Map	Click **Rename** to edit the map name.
Change Map	Click **Replace** to upload a new static map to replace the current one.
Set as Default Static Map	Click **Set as Default** to set the static map as the default map for the area.
Delete Map	Click **Delete** to delete the current map and all resources on it.
Switch to GIS Map	Click **Switch to GIS Map** to use the GIS map to monitor the area.

12.1.4 Add Hot Spot on Map

You can add elements (e.g., cameras, alarm inputs, etc.) as the hot spot and place the hot spot on the static map or GIS map. Then you can view the elements on the map and perform further operations. For example, you can start live view, view alarm information on the map.

Before You Start

- If you use the GIS map, make sure you have set a monitored area. For details, refer to ***Change Monitored Area on GIS Map*** .
- If you use a static map, make sure you have added a map to the area. For details, refer to ***Add Static Map for Area*** .

Steps

1. On the top navigation bar, click **Map → Map Settings** .

2. Select an area in the top left corner.

3. Select a map.

4. Click **Add Object** on the right pane.

5. Click **Add** in the **Resource** pane.

6. Select **Camera**, **Alarm Input / Zone**, **Alarm Output**,, or **Door** as the resource type.

Note

When adding resources to the map for the first time, there will be a tutorial.

7. Add resources to the map.

- Hover the mouse over the resource and click + to add a resource to the map.
- You can also drag resources to add them to the map or click **Add All to Map** to add all resources in an area to the map.

8. Optional: Perform the following operations after adding the hot spot.

Adjust Hot Spot Location	Drag the added hot spot on the map to the desired location.

Edit Hot Spot

Click the added hot spot icon on the map and click **Edit** to edit the detailed information (such as setting GIS address, and selecting icon color).

For camera hot spots, you can also edit the detection area, including radius, direction, and angle, or drag the displayed sector on the map to directly adjust the detection area.

Delete Hot Spot

Click the hot spot icon on the map and click **Delete** to remove the hot spot from the map.

12.1.5 Add Hot Region on 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.

Before You Start

- If you use the GIS map, make sure you have set a monitored area. For details, refer to ***Change Monitored Area on GIS Map*** .
- If you use a static map, make sure you have added two maps to the area. For details, refer to ***Add Static Map for Area*** .

Steps

1. On the top navigation toolbar, click **Map → Map Settings** .
2. Select an area in the top left corner.
3. Select a map.
4. Click **Add Object** on the right pane.
5. Click **Add** in the **Hot Regions** pane.
6. Select a map for the hot region, and click **Next**.
7. Enter the required information such as name and name color.
8. Click **OK**.
9. Drag to draw an area and right click to save it.
10. Optional: Perform the following operation(s) after adding the hot region.

View Hot Region Map

Click a hot region icon, click **View Hot Region Map** to view the map of the hot region. If there are multiple maps for a hot region, click **View Hot Region Map** and click a map to view the hot region map.

Edit Hot Region

Click **Edit Hot Region** and drag the white point on the hot region's line to edit the hot region's size or shape.

Edit Hot Region Information

Click the added hot region icon on the map to view and edit the detailed information, including GPS location (only available when parent map is GIS map), hot region name, name color, and descriptions. You can also edit the maps linked to the hot region.

Delete Hot Region	Click the hot region icon on the map and click **Delete** on the appearing dialog to delete the hot region.

12.1.6 Add Tag on Map

You can add tags with description on the map.

Before You Start

- If you use the GIS map, make sure you have set a monitored area. For details, refer to ***Change Monitored Area on GIS Map*** .
- If you use a static map, make sure you have added two maps to the area. For details, refer to ***Add Static Map for Area*** .

Steps

1. On the top navigation bar, click **Map → Map Settings** .
2. Select an area in the top left corner.
3. Select a map.
4. Click **Add Object** on the right pane.
5. Click **Add** in the **Tag** pane.
6. Click on the map to place the tag.
7. Customize a name and description for the tag.
8. Click **Save**.

The added tag icon will be displayed on the map.

9. Optional: Perform the following operation(s) after adding the tag.

Adjust Tag Location	Drag the added tag on the map to the desired locations.
Edit Tag	Click the added tag icon on the map to view and edit the detailed information, including name and description.
Delete Tag	Click the tag icon on the map and click **Delete** on the appearing dialog to delete the tag.

12.2 Map Monitoring

After maps and objects are added, you can operate hot spots, preview hot regions, and operate maps.

12.2.1 Operate Hot Spot

The resources (including cameras, alarm inputs, alarm outputs, partitions (areas), and doors) added on the map are called the hot spots. The hot spots show the locations of the resources. You can operate the hot spot, such as acknowledging alarms, viewing history alarms, and arming or disarming the resources.

Note

Make sure you have configured hot spot settings. For details, see ***Add Hot Spot on Map*** .

On the top navigation bar, click **Map → Map Monitoring** to enter the Map Monitoring page.

Click a hot spot to open the dialog which displays the available operations.

- For 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.
- For 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.
- For alarm output hot spots: Turn on or off the linked alarm output.
- For partition (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.
- For 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.

  Note

  - Some hot spot operations are not supported by offline resources whose icons are gray.
  - Setting doors of video intercom devices as normally closed is not supported.

12.2.2 Preview Hot Region

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

Before You Start

Make sure you configured hot region settings. For details, see ***Add Hot Region on Map*** .

Steps

1. On the top navigation bar, click **Map → Map Monitoring** to enter the Map Monitoring page.

2. Select an area in the top left corner.

3. Optional: If an area has multiple maps, click a map to select it.

4. Click a hot region on the map to enter the map of the hot region.

12.2.3 Operate Map

After opening map, you can perform one or more operations of the followings, such as zooming in or out map, adding label, printing map, and filtering resources.

Zoom in/Zoom out Map

Use the mouse wheel or click + or - to zoom in or zoom out on the map.

Filter

Click **Filter** and select the resource type you want to show on the map.

Add Tag

Click ⚐ to add a label with description to the map.

Screenshot

Click 📷 , and select an area. on the map You can save this area as a picture to local PC.

Print Map

Click 🖶 to print the map.

Locate Resource on Map

Click 📍 → **Resource** to search for a resource on the map. The located resources can be displayed in the center of the map.

Note

Only when the resource is added to the map, you can locate the resource on map.
Locating resources on map is only available when you use GIS map.

Search for Location

Click 📍 → **Geographic Location** to search for a location on the map. You can search locations on GIS map and hot spot/hot region on the e-map by entering keyword(s).

Note

Searching for locations is only available when you use GIS map.

Chapter 13 Alarm Management

An alarm is used to notify the security personnel of a particular situation which needs to be handled promptly. You can set linkage actions for alarms to record the alarm details and view the alarm information for alarm acknowledgment and handling. The alarm logs can be searched via the Portal and the real-time alarm details can be received and checked in the Alarm Center.

Alarm

The rule of an alarm includes six elements, namely, "**alarm source**" (i.e., the device which detects the abnormal situation), "**alarm**" (a specific type of alarm occurred on the alarm source), "**when**" (a specified period during which the alarm can be triggered), "**priority**" (the priority of this alarm), and "**what to do**" (linkage actions after this alarm is triggered). Besides these six elements, you can also set other properties for this alarm such as alarm description, etc.

Example

An alarm can be defined as an intrusion (**alarm source**) which happens in the bank vault and is detected by cameras mounted in the bank vault (**alarm**) on weekend (**when**), and then the camera start recording (**what to do**) once it happened. This alarm is marked as High priority (**priority**), and users including admin and operators can receive this alarm notification and check the alarm details.

13.1 Alarm Settings

13.1.1 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.

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.

13.1.2 Add an Alarm Rule

On the top navigation bar, click **Alarm → Basic Alarm Settings → Alarm Configuration** to enter the Alarm Configuration page.

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 and you can refer to ***Define Alarm Priority and Alarm Category*** for defining the alarm priority.

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

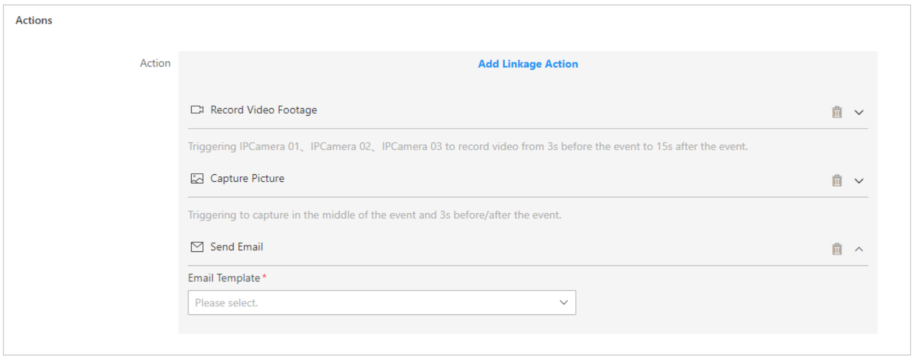
Select cameras to capture pictures during the alarm, and you can view the captured pictures when checking the event or alarm on the Alarm Search page.

- **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



Actions

Action

Add Linkage Action

Record Video Footage

Triggering IPCamera 01、IPCamera 02、IPCamera 03 to record video from 3s before the event to 15s after the event.

Capture Picture

Triggering to capture in the middle of the event and 3s before/after the event.

Send Email

Email Template*

Please select.

Figure 13-1 Set Linkage Action as Sending Email

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

Note

For details about how to set an email template, refer to ***Add an Email Linkage Template*** .

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

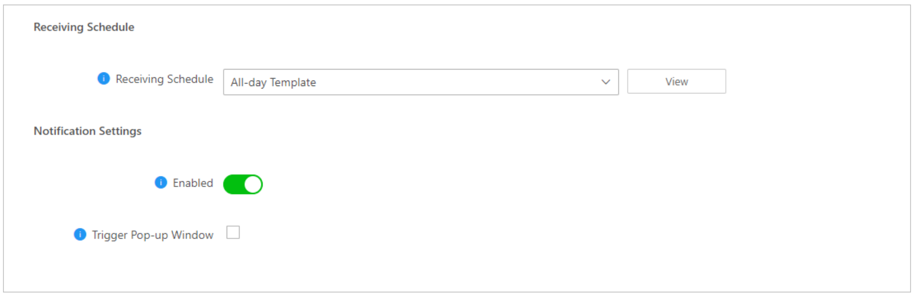
This field defines the time period when an alarm can be triggered.

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.



Receiving Schedule

Receiving Schedule: All-day Template

Notification Settings

Enabled: ●

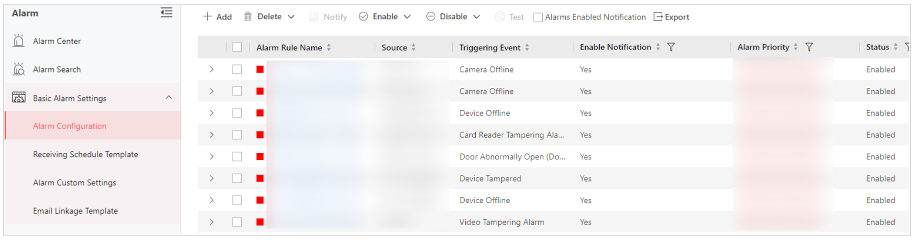
Trigger Pop-up Window: □

Figure 13-2 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.



	☐	Alarm Rule Name	Source	Triggering Event	Enable Notification	Alarm Priority	Status
>	☐	🟥 [redacted]	[redacted]	Camera Offline	Yes	[redacted]	Enabled
>	☐	🟥 [redacted]	[redacted]	Camera Offline	Yes	[redacted]	Enabled
>	☐	🟥 [redacted]	[redacted]	Device Offline	Yes	[redacted]	Enabled
>	☐	🟥 [redacted]	[redacted]	Card Reader Tampering Ala...	Yes	[redacted]	Enabled
>	☐	🟥 [redacted]	[redacted]	Door Abnormally Open (Do...	Yes	[redacted]	Enabled
>	☐	🟥 [redacted]	[redacted]	Device Tampered	Yes	[redacted]	Enabled
>	☐	🟥 [redacted]	[redacted]	Device Offline	Yes	[redacted]	Enabled
>	☐	🟥 [redacted]	[redacted]	Video Tampering Alarm	Yes	[redacted]	Enabled

Figure 13-3 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 13-1 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.

Operation	Description
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.

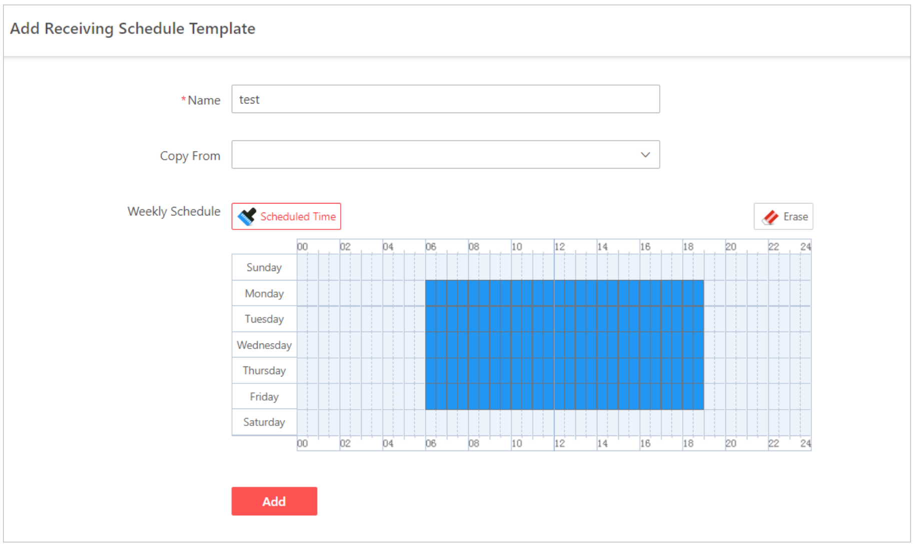
13.1.3 Configure a Receiving Schedule Template

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.

Steps

1. On the top navigation bar, click **Alarm → Basic Alarm Settings → Receiving Schedule Template** .

2. Click + to enter the Add Receiving Schedule Template page.



Add Receiving Schedule Template

*Name: test

Figure 13-4 Add Receiving Schedule Template

3. Create a name for the schedule template.

4. **Optional:** 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. **Optional:** Click **Erase** and click or drag on the formerly selected rectangle(s) to remove them from the scheduled time.
7. Click **Add**.
8. **Optional:** Perform the following operations.

Edit Receiving Schedule Template	On the template list, click a schedule template to edit it.
Delete Receiving Schedule Template	On the template list, select a schedule template and click 🗑 to delete it.

13.1.4 Define Alarm Priority and Alarm Category

The System predefines several alarm priorities and alarm categories for basic needs. You can edit them according to actual needs.

Steps

Note

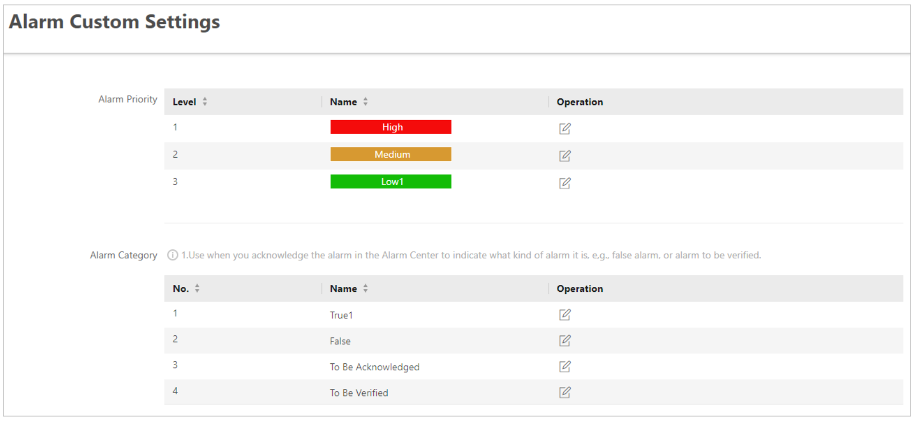
Alarm Priority

Define the priority for an alarm when adding the alarm and filtering the alarm in the Alarm Center.

Alarm Category

Alarm category is used when the user acknowledges the alarm in the Alarm Center and categorizes what kind of alarm it is, e,g., false alarm, or alarm to be acknowledged. You can search for alarms by category in the Alarm Center.

1. On the top navigation bar, click **Alarm → Basic Alarm Settings → Alarm Custom Settings** to enter the Alarm Configuration page.



Alarm Custom Settings

Alarm Priority

Level	Name	Operation
1	High	✎
2	Medium	✎
3	Low1	✎

Alarm Category

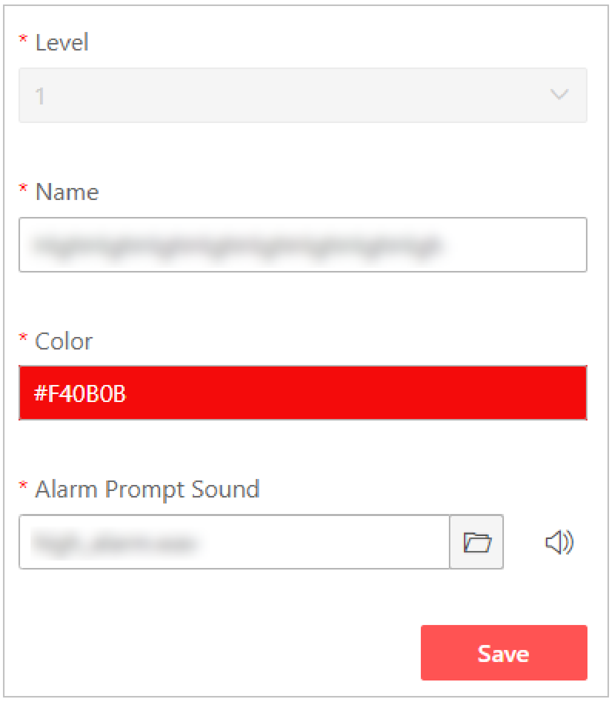
ⓘ 1.Use when you acknowledge the alarm in the Alarm Center to indicate what kind of alarm it is, e.g., false alarm, or alarm to be verified.

No.	Name	Operation
1	True1	✎
2	False	✎
3	To Be Acknowledged	✎
4	To Be Verified	✎

Figure 13-5 Defined Alarm Priority and Alarm Category

2. Edit a predefined alarm priority. By default, three kinds of alarm priority are displayed.

1) Select a predefined alarm priority and click ✎ in the Operation column.



* Level

1

* Name

* Color

#F40B0B

* Alarm Prompt Sound

Figure 13-6 Edit a Predefined Alarm Priority

2) Enter a descriptive name for the alarm priority.

3) Select a color for the alarm priority.

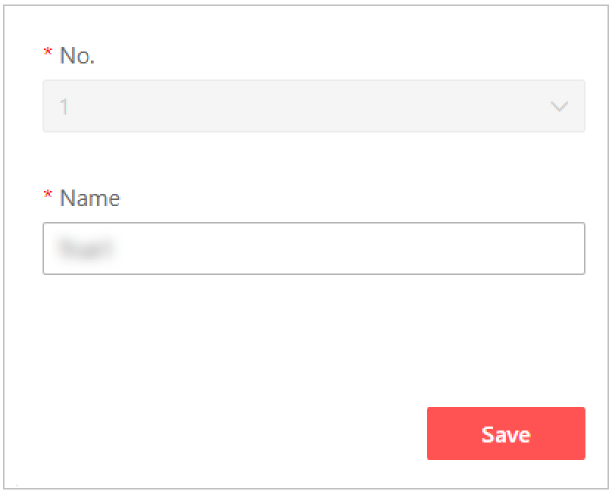
4) Click 🗀 to select an alarm audio file from the local storage as the prompt sound for the alarm priority.

5) **Optional:** Click 🔊 to play the selected audio.

6) Click **Save**.

3. Edit a predefined alarm category. By default, four alarm categories are displayed.

1) Select a predefined alarm category and click ✎ in the Operation column.



* No.

1

* Name

Figure 13-7 Edit a Predefined Alarm Category

2) Enter a descriptive name for the alarm category.

3) Click **Save**.

13.1.5 Add an Email Linkage Template

You can set email templates (including specifying the recipient, email subject, and content) for sending alarms regularly, so that the System can send alarms as the email attachments to the designated recipients regularly according to the predefined email templates.

Before You Start

Before adding the email template, you should set the sender's email account. See ***Configure Email Account*** for details.

Steps

1. On the top navigation bar, click **Alarm → Basic Alarm Settings → Email Linkage Template** .

2. Click **Add** to enter the Add Email Template page.

Note

For adding template for the first time, click **Add Template** in the center of the page.

3. Enter the required parameters.

Name

Create a name for the template.

Recipients

Click **Add User** and select the person's email as the recipient, which is configured when adding the person.

Click **Add Email** and enter the recipient email address.

Subject

Enter the email subject as desired. You can also click the button in the lower part of the window to add the related information to the subject.

Content

Define the report content to be sent. You can also click buttons below the **Content** parameter to add the related information to the content.

Note

If you add the time period to the email subject or email content, and the email application (such as Outlook) and the System are in different time zones, the displayed time period may have some deviations.

(Optional) Content Language

Select a relevant language from the drop-down list for the content.

4. Finish adding the email template.
   - Click **Add** to add the template and go back to the email template list page.
   - Click **Add and Continue** to add the template and continue to add other templates.

   The email template will be displayed in the email template list.
5. **Optional:** Perform the following operation(s) after adding the email template.

Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click 🗑 in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

13.2 Search for Alarms

The triggered alarms will be recorded in the System, you can set different conditions to search for alarms.

Before You Start

Make sure that alarms have been configured and triggered.

Steps

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

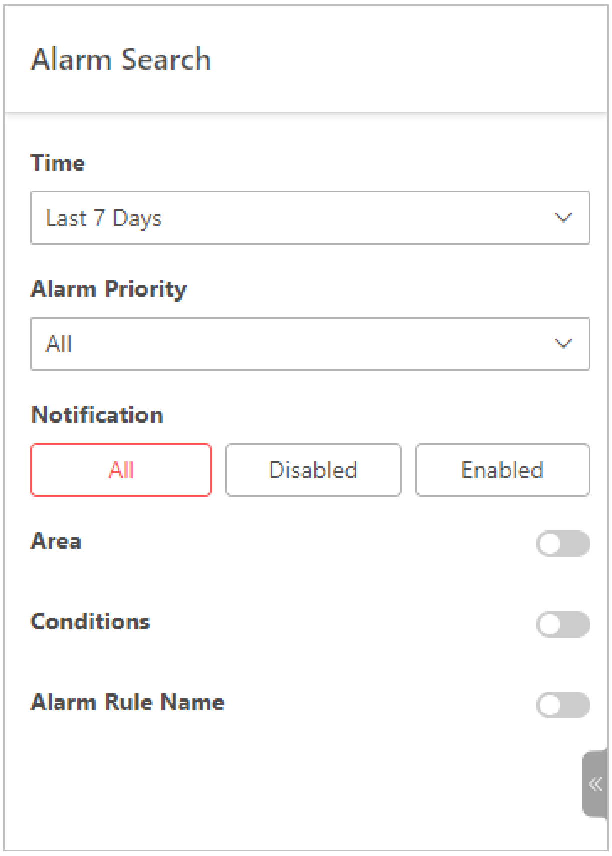


Figure 13-8 Alarm Search

2. Set the time range for search.
   - Select a predefined time period for search.
   - Select **Custom Time Interval** and specify the start time and end time 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.

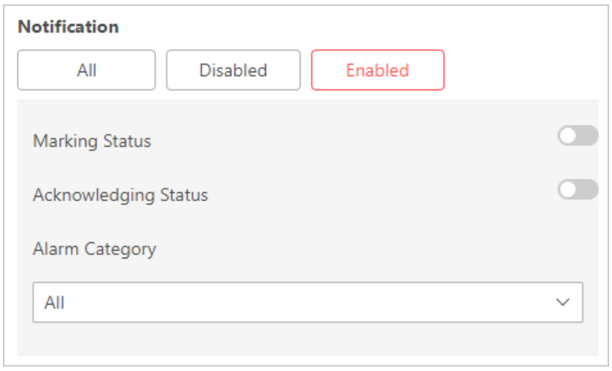
   Disabled

   Alarms with notification not enabled.

   Enabled

   Alarms with notification enabled.

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



Notification

All | Disabled | Enabled

Marking Status

Acknowledging Status

Alarm Category

All

Figure 13-9 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 **Area** and then click to select the area 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**.

   Matched alarms will be listed on the right.
10. **Optional:** Perform the following operation(s) after searching for alarms.

    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.

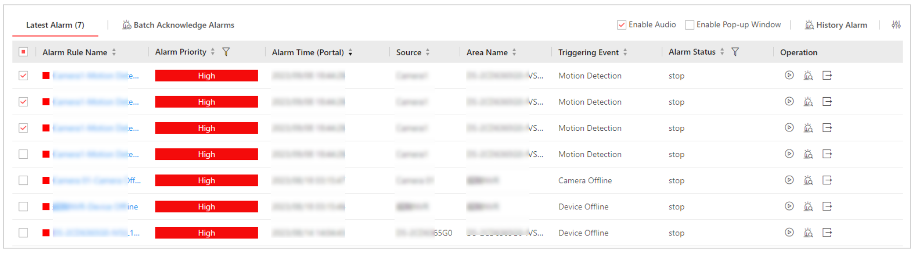
13.3 View Resources' Real-Time Alarms

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.



Latest Alarm (7) | Batch Acknowledge Alarms | ☑ Enable Audio | □ Enable Pop-up Window | History Alarm

■	Alarm Rule Name	Alarm Priority	Alarm Time (Portal)	Source	Area Name	Triggering Event	Alarm Status	Operation
☑	[redacted]e...	High	[redacted]	[redacted]	[redacted]VS...	Motion Detection	stop	
☑	[redacted]e...	High	[redacted]	[redacted]	[redacted]VS...	Motion Detection	stop	
☑	[redacted]e...	High	[redacted]	[redacted]	[redacted]VS...	Motion Detection	stop	
□	[redacted]e...	High	[redacted]	[redacted]	[redacted]VS...	Motion Detection	stop	
□	[redacted]ff...	High	[redacted]	[redacted]	[redacted]	Camera Offline	stop	
□	[redacted]ine	High	[redacted]	[redacted]	[redacted]	Device Offline	stop	
□	[redacted]1...	High	[redacted]	[redacted]65G0	[redacted]VS...	Device Offline	stop	

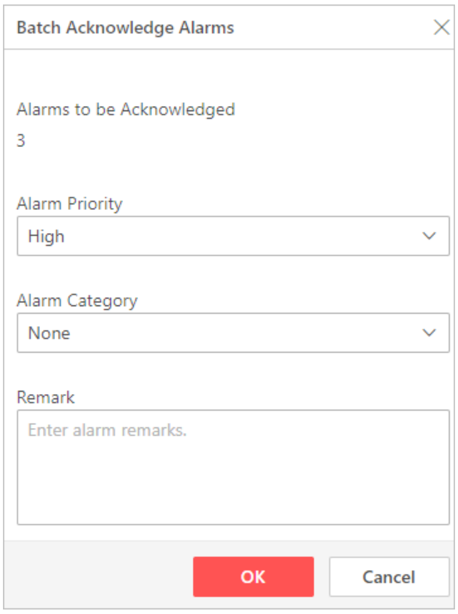
Figure 13-10 Alarm Center

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

Table 13-2 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 (Portal)** The time of the Portal when the alarm starts. **Alarm Time (Device)** The time of the device when the alarm starts. **Source** 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.

Operation	Description
	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** 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.

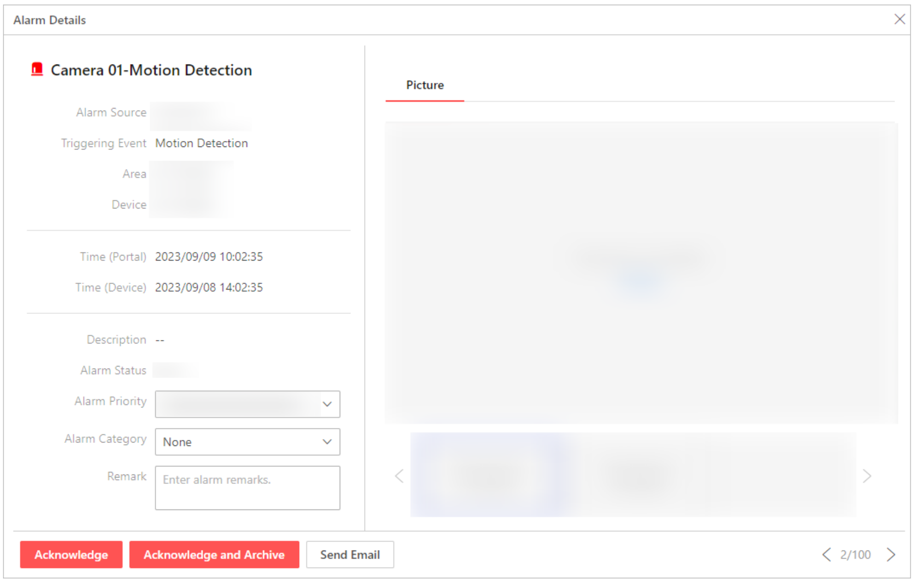
Operation	Description
	 Batch Acknowledge Alarms Alarms to be Acknowledged: 3 Alarm Priority: High Alarm Category: None Remark: Enter alarm remarks. **Figure 13-11 Batch Acknowledge Alarms** 2. (Optional) Set the alarm priority and alarm category. 3. (Optional) Enter remarks about the alarm acknowledgment. 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 ***Search for Alarms*** for details.
Enable Audio	Check alarms and check **Enable Audio**, so that once the alarms are triggered, audio notification will be played.
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.

13.4 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.



Alarm Details

Camera 01-Motion Detection

Alarm Source

Triggering Event Motion Detection

Area

Device

Time (Portal) 2023/09/09 10:02:35

Time (Device) 2023/09/08 14:02:35

Description --

Alarm Status

Alarm Priority

Alarm Category None

Remark Enter alarm remarks.

Figure 13-12 Alarm Triggered Pop-Up Window

Table 13-3 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

Function	Operation
	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.
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 14 Person Management

The person information is required when you use applications provided by the access control service, time and attendance service, and video intercom service. You can add the person information to the platform for further operations such as assigning access levels to a person, scheduling a person's shifts, linking a person to a room as the resident, etc. After adding the persons, you can edit and delete the person information if needed.

14.1 Add a 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.

Steps

1. On the top navigation bar of the Portal, 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.

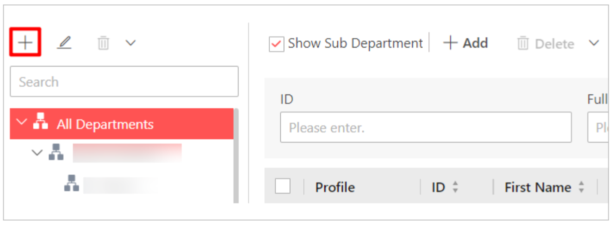
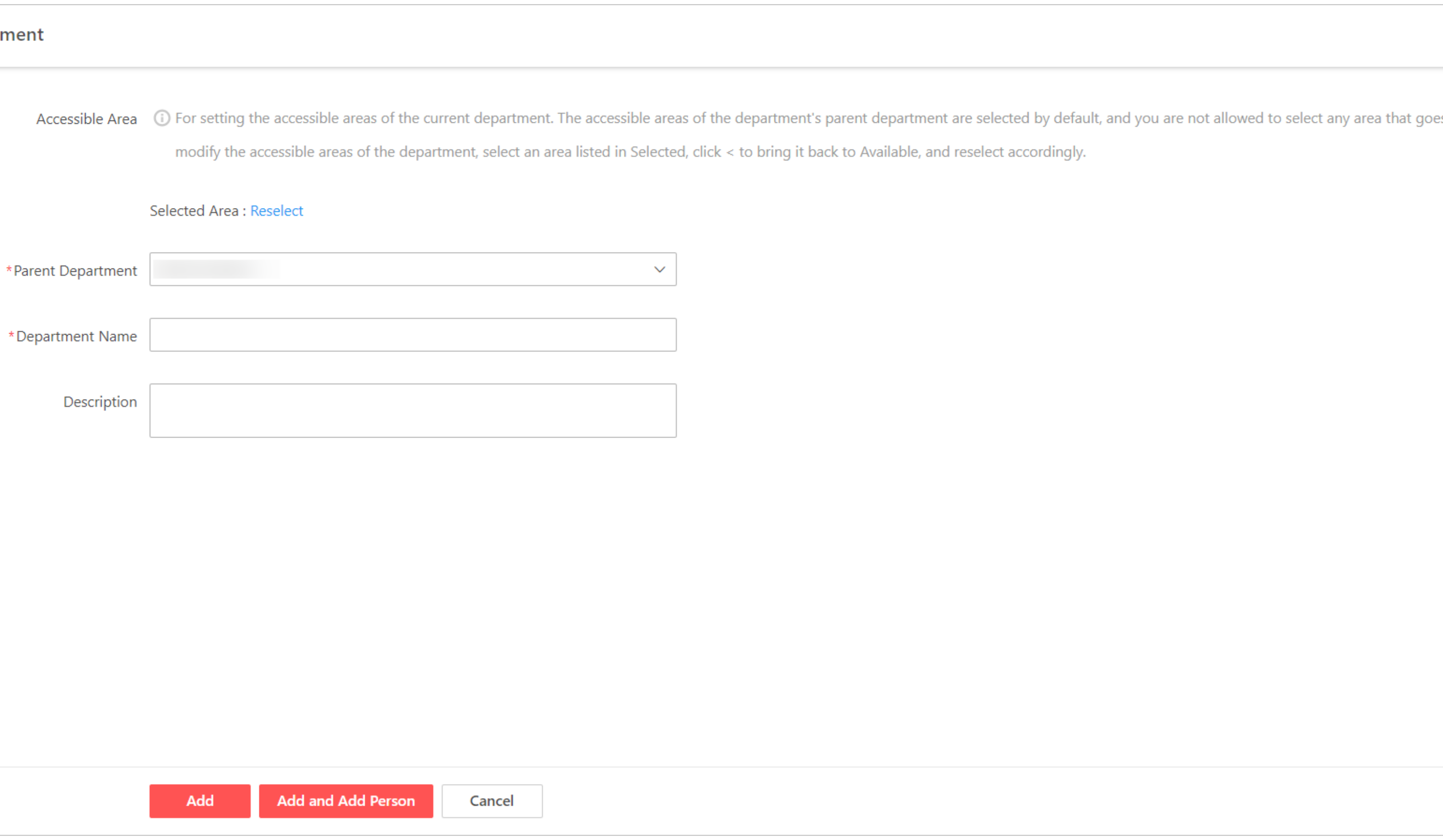


Figure 14-1 Enter the Add Department Page



ment

Accessible Area ⓘ For setting the accessible areas of the current department. The accessible areas of the department's parent department are selected by default, and you are not allowed to select any area that goes modify the accessible areas of the department, select an area listed in Selected, click < to bring it back to Available, and reselect accordingly.

Selected Area : Reselect

*Parent Department [redacted]

*Department Name

Description

Figure 14-2 Add Department Page

3. Optional: Reselect the area(s) to change the default accessible area(s) for the new department.

Note

- By default, the accessible areas of the parent department are selected. If the selected area of the parent department is the root area, you can click **Reselect** to open the area selection panel. If not, you can directly reselect the area(s) on the area selection panel.
- The unavailable areas are controlled by permissions assigned to the current user. For how to assign permissions to users, refer to ***Add a Normal User*** .

4. Optional: Change a parent department.

Note

You can only select parent departments that are linked to areas whose display permissions are assigned to you.

5. Enter a name for the department.

6. Optional: Enter the department description.

7. Add the department.

- Click **Add** to finish adding the department and go back to the person management page.
- Click **Add and Add Person** to finish adding the department and enter the Add Person page.

8. Optional: Perform the following operations after adding departments.

Edit a Department

Select a department and click ✎ at the top of the department list to edit the area, department name, and description.

Note

You cannot edit the unavailable departments and the area of the root department.

Delete a Department

Select a department and click 🗑 at the top of the department list to delete the selected department.

Once you delete a department, the sub departments (if any) and linked persons will also be deleted.

Note

The root department and unavailable departments cannot be deleted.

Delete All Added Departments

At the top of the department list, click ⌄ → **Delete All** to delete all the departments you added.

Once you delete all added departments, the sub departments (if any) and linked persons will also be deleted.

Note

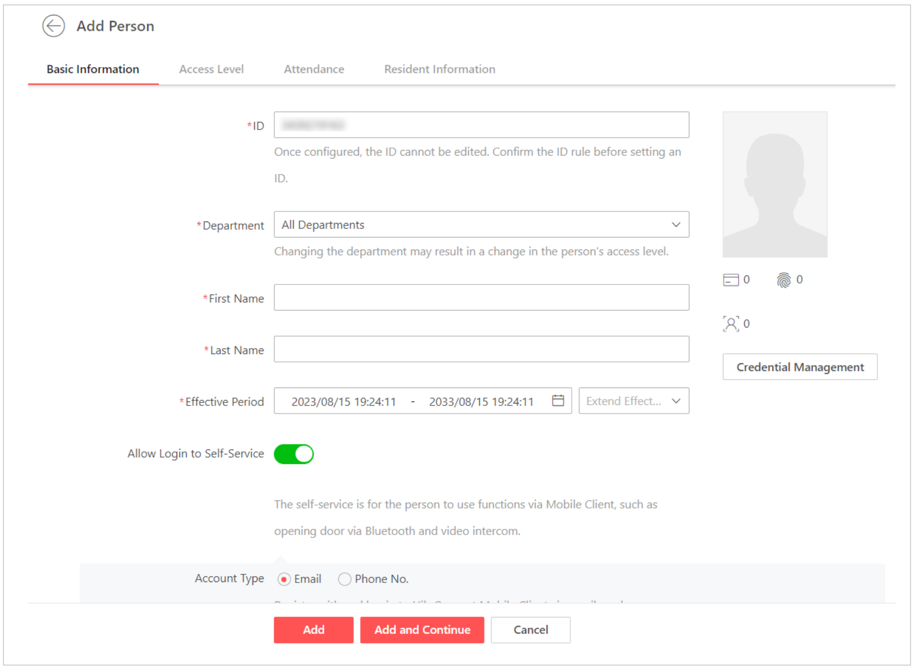
The root department and unavailable departments cannot be deleted.

14.2 Add a Person

To add a person, you should set the person's basic information, credential information, private information, and other information such as the person's access level. The above-mentioned person information contributes the data basis for the applications related to identity authentication of the person, such as the access control application, the time and attendance application, and the video intercom application.

Steps

1. On the top navigation bar of the Portal, click **Person** to enter the person management page.
2. Select a department from the department list on the left, and click **Add** at the top of the person list to open the Add Person page.



Add Person

*ID [redacted]

Once configured, the ID cannot be edited. Confirm the ID rule before setting an ID.

*Department: All Departments

Changing the department may result in a change in the person's access level.

*First Name

*Last Name

*Effective Period: 2023/08/15 19:24:11 - 2033/08/15 19:24:11 Extend Effect...

Allow Login to Self-Service: on

The self-service is for the person to use functions via Mobile Client, such as opening door via Bluetooth and video intercom.

Account Type: ● Email ○ Phone No.

Figure 14-3 Add Person Page

Note

All persons in the selected department will be displayed on the right. You can check **Show Sub Department** to display the persons in sub departments (if any).

3. Set the person's basic information.

ID (Required)

The default ID is generated by the platform. You can edit it if needed.

Note

The ID cannot be edited after you finish adding a person, so you should ensure its correctness at the beginning.

Department (Required)

Change the department for the person. You can only select parent departments under the areas whose display permissions are assigned to you. For how to add a department, refer to ***Add a Department*** .

Effective Period (Required)

Set the effective period for the person in the access control application, time and attendance application, and video intercom application to determine the period when the person can access the specified doors with credential or during which the person can participate in the attendance.

Click **Extend Effective Period** to show a drop-down list and select **1 Month / 3 Months / 6 Months / 1 Year** to quickly extend the effective period based on the configured end time. For example, if the period is from 2022/10/15 13:30:00 to 2022/11/15 14:00:00 and the extended time is selected as **1 Month**, the end time of effective period will change to 2022/12/15 14:00:00.

Allow Login to Self-Service

Switch on **Allow Login to Self-Service** to allow the person to log in to the Mobile Client as a self-service user and perform some operations related to the access control service and/or video intercom service.

You can enter an email address or click **Account** below the Email field to enter an account name and a password if you do not have an email for registering a self-service user account.

Note

- The operation related to the access control service includes authentication via bluetooth on the Mobile Client.
- Operations related to the video intercom service include authentication via QR code or bluetooth, calling and talking, temporary pass management, real-time monitoring via door stations, viewing the call history, and adding other residents to the room (for householder) on the Mobile Client.
- If you use the email to log in to the Mobile Client, a temporary password will be automatically sent to the entered email address. For the first time login, the person should change the password.

Account Type

Select **Email** or **Phone No.** as the account type. Optionally, you can click **More** to enter more information such as phone number or email, and remark.

Profile Photo

Hover the cursor onto 👤, and you can select from three modes to add a profile photo.

From Device

Collect the face picture via an enrollment station as the profile photo. This mode is suitable for non-face-to-face scenario when the person and the user who has the person management permissions are on different locations.

You can switch on **Face Anti-Spoofing** and set the security level (the higher security level, the higher reliability of face anti-spoofing detection) to make sure the face picture is collected from a live person instead of an image.

Take a Picture

Select one of the PC's webcams to take a picture as the profile photo.

Upload Picture

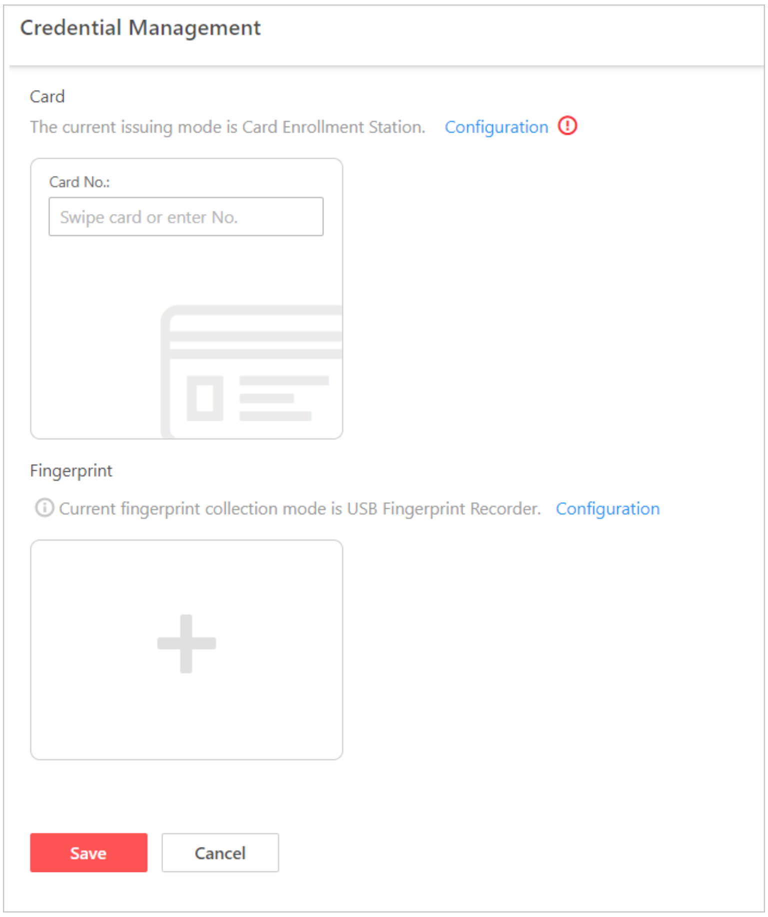
Select a picture from the PC as the profile photo.

It is recommended that the face in the picture be in the full-face view directly facing the camera, without a hat or head covering.

You can drag the picture to change its position, rotate, or zoom in/out before cutting and saving it.

Credential

The supported credentials include cards and fingerprints. These credential can be used for the access authentication in access control application and video intercom application.



Credential Management

Card

The current issuing mode is Card Enrollment Station. Configuration

Card No.: Swipe card or enter No.

Fingerprint

Current fingerprint collection mode is USB Fingerprint Recorder. Configuration

Figure 14-4 Credential Management Page

Card Credential

On the Credential Management page, click **Configuration** in the Card field to open the card issuing settings pane, select an issuing mode, and set the corresponding parameters (see ***Batch Issue Cards to Persons*** for details). And then swipe the card on the device (i.e., card enrollment station, enrollment station, and access control / video intercom device) according to the configured issuing mode to add a card.

Or you can directly click + in the Card field and manually enter the card No. (includes digits and letters) to add a card.

Fingerprint Credential

On the Credential Management page, click **Configuration** in the Fingerprint field to select a collection mode, and then click + to start collecting fingerprints.

You can select **USB Fingerprint Recorder**, **Enrollment Station**, or **Access Control / Video Intercom Device** as the collection mode, and then plug the USB interface of the fingerprint recorder or connect the enrollment station / access control device / video intercom device to the PC on which the Portal runs, and then collect the person's fingerprints via the device.

Note

After adding the card or fingerprint credential, you can hover the cursor onto an added credential and click ✎ or 🗑 to edit or delete them.

4. **Optional:** Configure the private information for the person, such as the phone No. and remarks.
5. **Optional:** Configure access level settings for the person.

Open Door via Bluetooth on Mobile Client

Once checked, if the bluetooth of the mobile phone on which the Mobile Client is running is enabled, the person can open doors by using the mobile phone.

Open Door via PIN Code

Check **Open Door via PIN Code** to automatically generate a PIN code (which can also be customized if needed) for access authentication. That is, the person is allowed to use the PIN code to open doors of which the access levels are assigned to him/her.

Note

In most cases, the PIN code must be used after the card or fingerprint authentication. It can be used as a credential alone only when **Open Door via PIN Code** is enabled both on the platform and card readers.

Assign Access Level

Click **Add** and select access level(s) to assign the selected access level(s) to the person for defining the doors which the person can access during the authorized period.

You can click 🗎 view details of doors and access schedules on the Add Access Level pane.

6. **Optional:** Configure the time and attendance parameters for the person.

Check In/Out via Mobile Client

Switch on **Check In/Out via Mobile Client** to allow the person to check in or out via the Mobile Client. If you check **Must Upload Picture**, the person must take a photo and upload it to the System for checking in or out.

Role

Select whether the person is an employee or a supervisor of the department.

Note

The role of a person is set to employee by default. A supervisor is a higher-ranking employee who has additional permission to review applications and check attendance data of the employees in the same department on the Mobile Client.

View Person's Schedule by Month

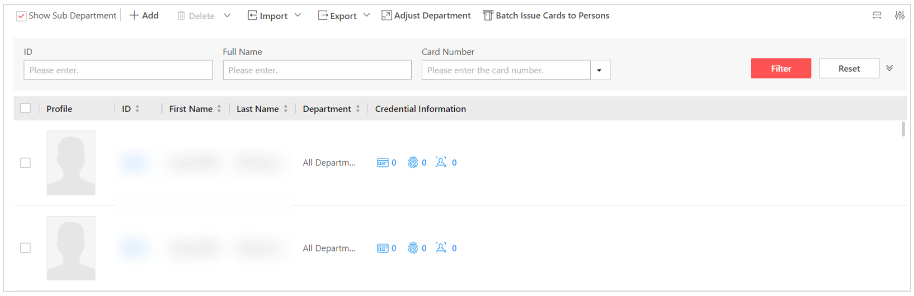
If shifts are scheduled for the person, you can click ‹ and › to switch between months for viewing the person's schedule in different months. Click **Today** to quickly locate the current day in the calendar and view the shift details.

7. **Optional:** Select an area and room(s) in the area to link the person to the selected room(s).

Note

No more than 6 residents can be linked to each room.

8. Finish adding a person.
   - Click **Add** to finish adding a person and go back to the person management page.
   - Click **Add and Continue** to finish adding a person and continue to add another person.



ID	Full Name	Card Number
Please enter.	Please enter.	Please enter the card number.

□	Profile	ID	First Name	Last Name	Department	Credential Information
□					All Departm...	0 0 0
□					All Departm...	0 0 0

Figure 14-5 Person List

9. **Optional:** Perform the following operation(s) after adding persons.

Edit a Person
Click a person name to edit the person information.

Delete Selected Person(s)
Check the person(s) and click **Delete** at the top of the person list to delete the selected person(s).

Delete All Persons
Click ⌄ → **Delete All** to delete all persons.

Adjust Persons' Department
Check the person(s), click **Adjust Department** at the top of the person list, select a target department, and click **Move** to move the person(s) to the selected department.

Note

Once moved, the access levels of the selected person(s) will be changed.

Batch Issue Cards to Persons
To conveniently manage card credentials for a large number of persons, you can batch issue cards to multiple persons. For how to issue cards to persons, refer to ***Batch Issue Cards to Persons*** .

Set Display Parameters of Person List

Click ⇄ → **Complete Display of Each Column Title / Incomplete Display of Each Column Title** to switch modes of self-adaptive column width for the person list.

Click 🎚 and check the column names to only display the selected columns in the person list.

Filter Displayed Persons

Set conditions including **ID**, **Full Name**, **Card Number**, **Effective Period**, **Credential Status**, **Phone No.**, or **Email**, and then click **Filter** to filter the displayed persons as required.

Note

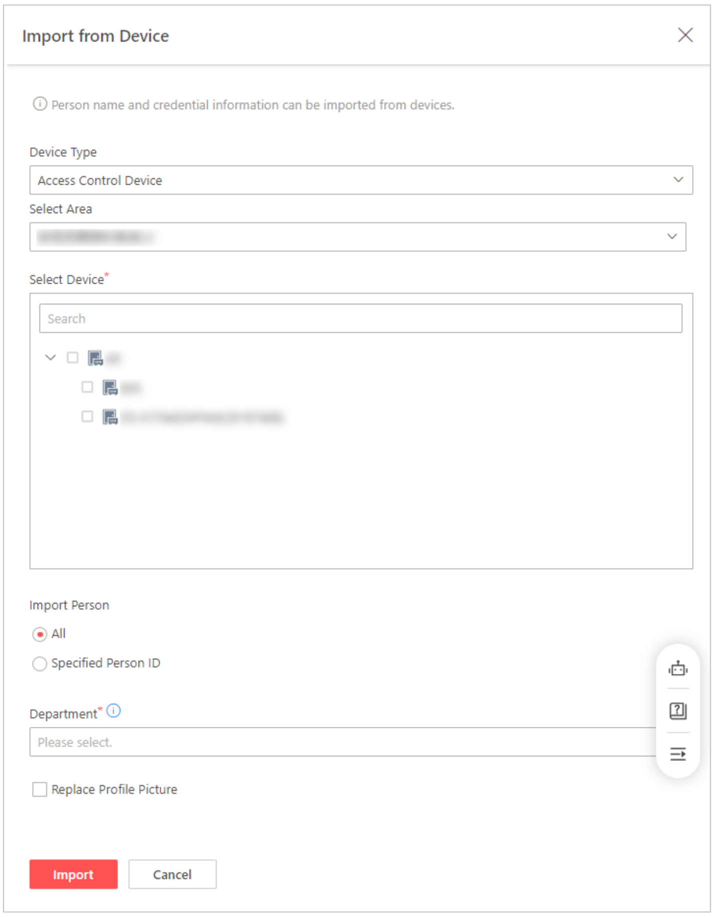
- The **Effective Period**, **Credential Status**, **Phone No.**, or **Email** conditions will be displayed after you click ⌄ to unfold the filter pane.
- If you do not want to enter the card No. manually, you can select **Read Card Number by Device** and click ⚙ to select issuing mode (see ***Batch Issue Cards to Persons*** for details) for automatically reading the card No.

14.3 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.

Steps

1. On the top navigation bar of the Portal, click **Person** to enter the person management page.
2. 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.



Import from Device

ⓘ Person name and credential information can be imported from devices.

Device Type

Access Control Device

Select Area

[redacted]

Select Device*

Search

- □ [redacted]
  - □ [redacted]
  - □ [redacted]

Import Person

● All

○ Specified Person ID

Department* ⓘ

Please select.

□ Replace Profile Picture

Import Cancel

Figure 14-6 Import Persons from Device Pane

3. Specify the device type and area to select the device(s) from which the person information is imported.

Note

You can enter a keyword (fuzzy search supported) in the search box to search for the target device(s) quickly.

4. Select the person(s) to 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.

5. Select a department to which persons will be imported.
6. **Optional:** Check **Replace Profile Picture** to replace existing persons' profile pictures by new ones from devices.
7. 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.

8. **Optional:** Refer to the last step in ***Add a Person*** for details about the available operations after importing persons from devices.

14.4 Import Persons via Template

If there are multiple persons to be added to the System, you can import them with the minimum effort via an Excel template that contains the person information such as person names, departments, and effective periods.

Steps

1. On the top navigation bar of the Portal, click **Person** to enter the person management page.
2. 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.

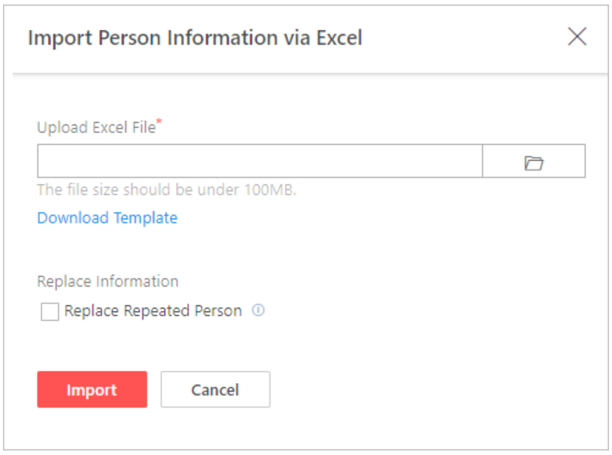
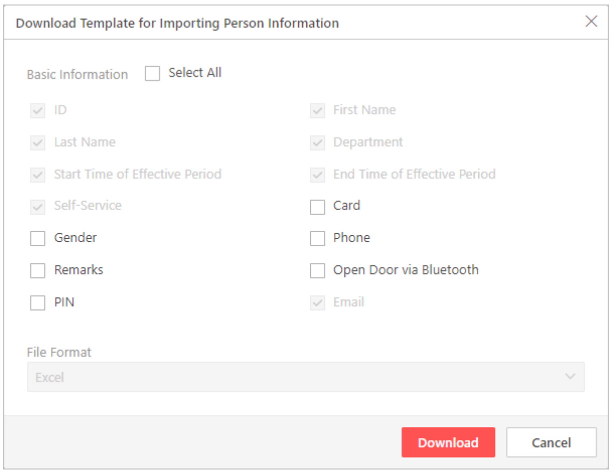

Import Person Information via Excel
Upload Excel File*
The file size should be under 100MB.
Download Template
Replace Information
□ Replace Repeated Person
Import
Cancel

Figure 14-7 Import Person Information via Excel

3. 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.



Download Template for Importing Person Information

Basic Information □ Select All

☑ ID	☑ First Name
☑ Last Name	☑ Department
☑ Start Time of Effective Period	☑ End Time of Effective Period
☑ Self-Service	□ Card
□ Gender	□ Phone
□ Remarks	□ Open Door via Bluetooth
□ PIN	☑ Email

File Format

Excel

Figure 14-8 Download Template for Importing Person Information Window

4. Check the basic information items to be included in the template, such as card No., phone number, and remarks.

Note

You can batch issue cards to persons by importing the template with the card No. item.

5. Click **Download** to save the template to the local PC.
6. In the downloaded template file, enter the person information by following rules shown in the template.
7. Click 🗁 and select the template (with person information) from the local PC to upload.
8. **Optional:** 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.
9. Click **Import** to start importing.

Note

- The importing process cannot be stopped once started.
- You can export the person information that failed to be imported, and try again after editing.

The importing progress will be displayed and then you can check the importing results.

10. **Optional:** Refer to the last step in ***Add a Person*** for details about the available operations after importing persons via a template.

14.5 Batch Issue Cards to Persons

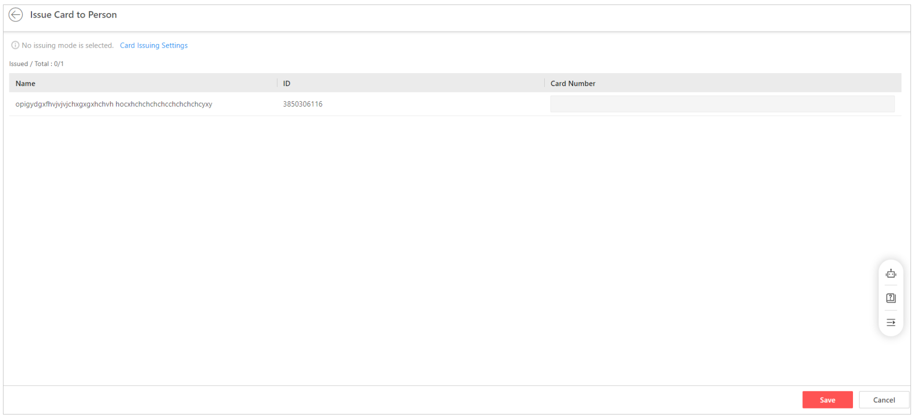
To conveniently manage card credentials for a large number of persons, the System provides a way to batch issue cards to multiple persons.

Steps

Note

Up to two cards can be issued to one person.

1. On the top navigation bar of the Portal, click **Person** to enter the person management page.
2. In the person list, check the person(s) to whom cards will be issued.
3. At the top of the person list, click **Batch Issue Cards to Persons** to enter the Issue Card to Person page.



Issue Card to Person

No issuing mode is selected. Card Issuing Settings

Issued / Total : 0/1

Name	ID	Card Number
opigydgxfhvjvjvjchxgxgxhchvh hocxhchchchchcchchchchcyxy	3850306116	

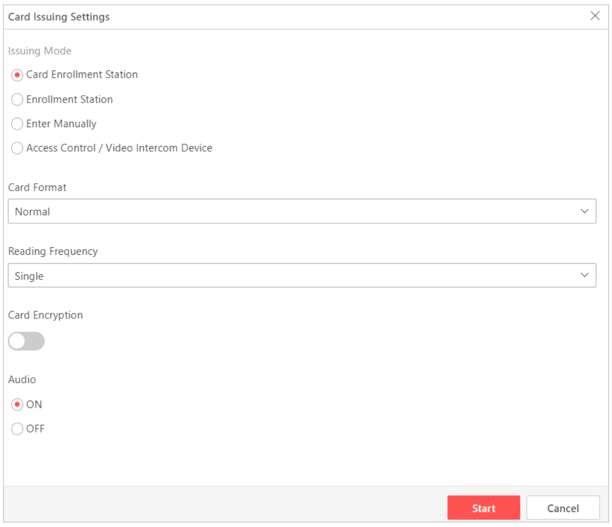
Figure 14-9 Issue Card to Person Page

4. Click **Card Issuing Settings** to open the Card Issuing Settings window, and select an issuing mode and set the related parameters on the pane.

Note

The Card Issuing Settings window will also be opened automatically when you enter the Issue Card to Person page.

Card Enrollment Station



Card Issuing Settings

Issuing Mode

● Card Enrollment Station

○ Enrollment Station

○ Enter Manually

○ Access Control / Video Intercom Device

Card Format

Normal

Reading Frequency

Single

Card Encryption

Audio

● ON

○ OFF

Figure 14-10 Issuing Mode: Card Enrollment Station

Connect a card enrollment station to the PC on which the Portal runs and set the following parameters to get the card number by place the card on the card enrollment station.

Card Format

Select a card format according to the actual card feature. For Wiegand cards, the card encryption is not supported.

Reading Frequency

If your card supports dual frequency (both IC and ID), select **Dual**. For dual frequency cards, the card encryption is not supported.

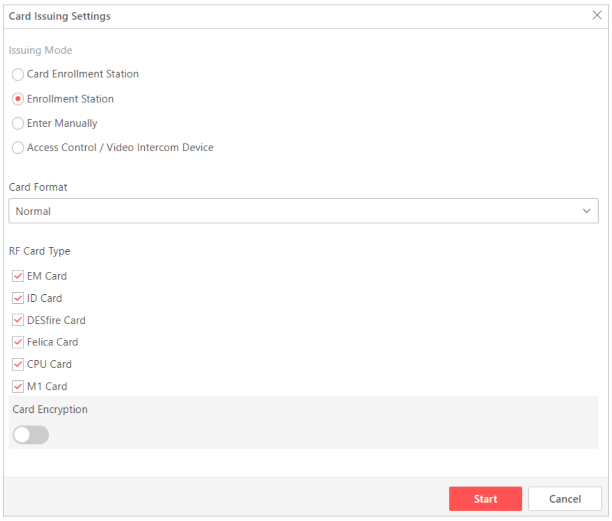
Card Encryption

Enable the card encryption and select sector(s) to be encrypted for security purpose. The settings will take effect after the card encryption function is also enabled on the card enrollment station.

Audio

Turn on or turn off the audio of the device when issuing cards.

Enrollment Station



Card Issuing Settings

Issuing Mode

○ Card Enrollment Station

● Enrollment Station

○ Enter Manually

○ Access Control / Video Intercom Device

Card Format

Normal

RF Card Type

☑ EM Card

☑ ID Card

☑ DESfire Card

☑ Felica Card

☑ CPU Card

☑ M1 Card

Card Encryption

Figure 14-11 Issuing Mode: Enrollment Station

Set the following parameters to enroll the card number remotely via the enrollment station and copy back to the System.

Card Format

Select a card format according to the actual card feature. For Wiegand cards, the card encryption is not supported.

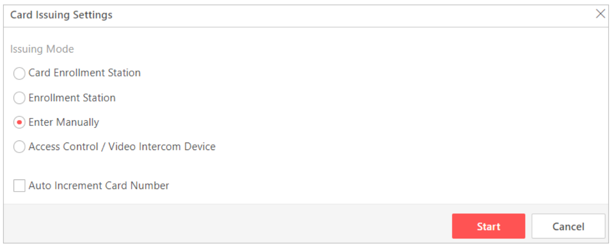
RF Card Type

Select the needed card type(s), including EM card, M1 card, etc. Only the M1 card supports the card encryption function.

Card Encryption

Enable the card encryption for the M1 card and select sector(s) to be encrypted for security purpose. The settings will take effect after the card encryption function is also enabled on the enrollment station.

Enter Manually



Card Issuing Settings

Issuing Mode

○ Card Enrollment Station

○ Enrollment Station

● Enter Manually

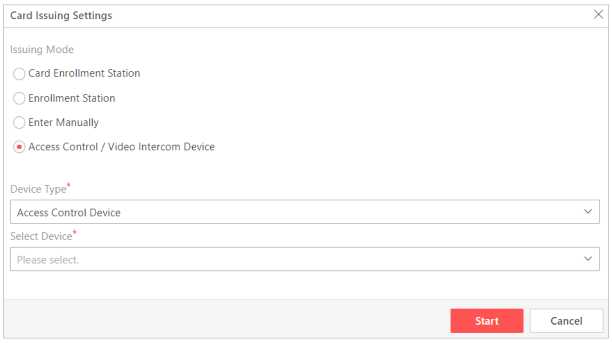
○ Access Control / Video Intercom Device

□ Auto Increment Card Number

Figure 14-12 Issuing Mode: Enter Manually

Manually enter the card number. You can check **Auto Increment Card Number** to enter a start card number to issue cards with incremental numbers to the selected persons in the list.

Access Control / Video Intercom Device



Card Issuing Settings

Issuing Mode

○ Card Enrollment Station

○ Enrollment Station

○ Enter Manually

● Access Control / Video Intercom Device

Device Type*

Access Control Device

Select Device*

Please select.

Figure 14-13 Issuing Mode: Access Control / Video Intercom Device

Select **Access Control Device** or **Video Intercom Device** as the device type, and select a device connected to the System to enroll the card numbers remotely via the selected device.

5. On the issuing settings pane, click **Start** to save the settings and start issuing cards to persons on the Issue Card to Person page.

- If you set the issuing mode to **Card Enrollment Station**, **Enrollment Station**, or **Access Control / Video Intercom Device**, place a card on the device, and the card number will be read automatically and be displayed in the Card Number column of the first person in the list.
- If you set the issuing mode to **Enter Manually**, enter a card number manually in the Card Number column of each person.

Note

- For the **Card Enrollment Station**, **Enrollment Station**, and **Access Control / Video Intercom Device** modes, you can repeat the operation of placing cards on the device to automatically read card numbers one by one, and cards will be issued to persons in the list in sequence.
- You cannot change the card issuing mode once you issue one card to one person.

6. Click **Save** to finish issuing cards to persons.

Chapter 15 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.

15.1 Real-Time Status Overview

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, and Hik-ProConnect boxes managed on the Portal.

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

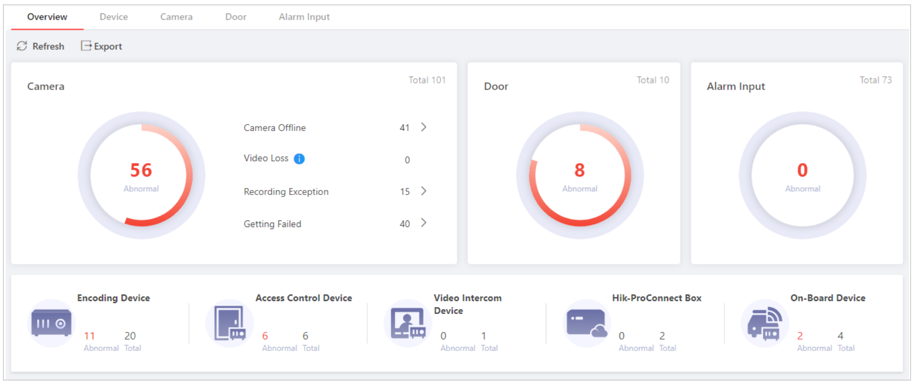


Figure 15-1 Real-Time Status Overview

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. For details, refer to ***Health Monitoring*** .

15.2 Health Monitoring

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, 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.

- ***Camera Status***
- ***Door Status***
- ***Alarm Input Status***
- ***Encoding Device Status***
- ***Access Control Device Status***
- ***Video Intercom Device Status***
- ***Hik-ProConnect Box Status***
- ***On-Board Device Status***
- ***Common Operations***

On the top navigation bar, click **Device and 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.
- 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.
- 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.

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.

15.3 Log Search

Two types of log files are provided: operation logs and device logs. Operation logs refer to the operation records that were performed on the Portal and Mobile Client. Device logs refer to the log files stored on the connected devices, including encoding device, on-board device, and access control device. You can search for the log files and view the log details.

15.3.1 Search for Logs Stored on Devices

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

Steps

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

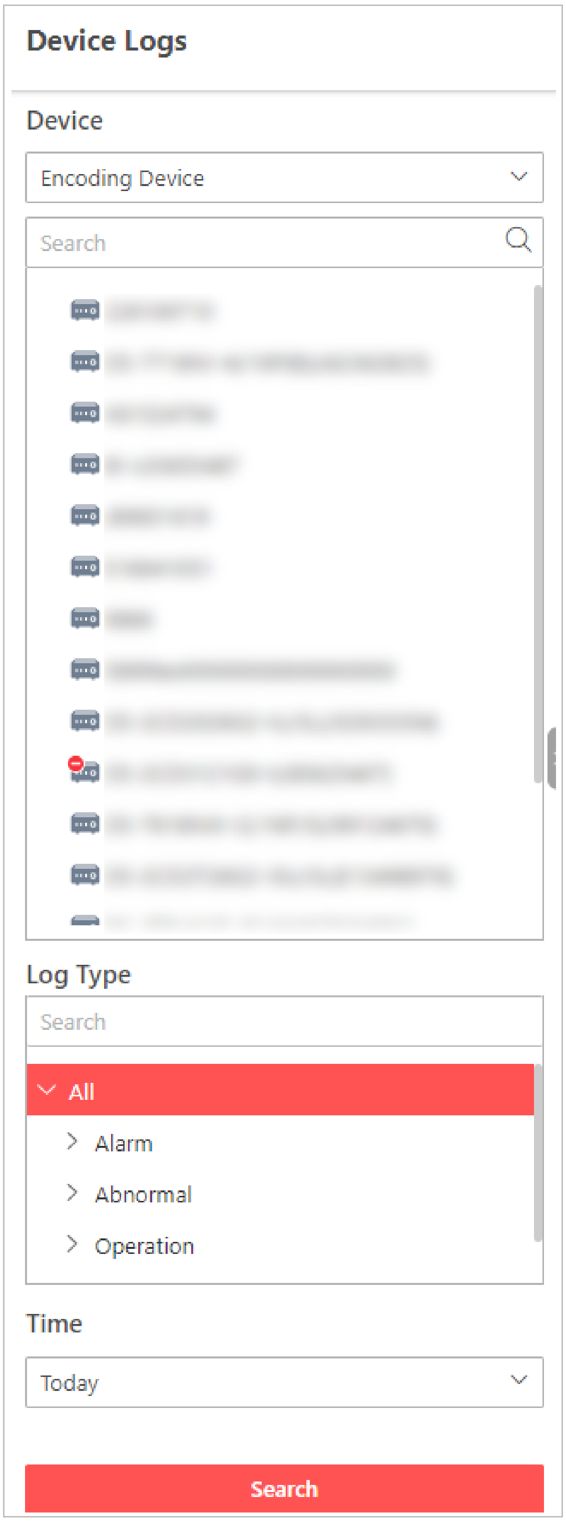


Figure 15-2 Search for Device Logs

2. In **Device**, select a device type (encoding device, on-board 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**.

   All matched logs are listed with details on the right.

15.3.2 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.

Steps

1. On the top navigation bar, click **Device and 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. **Optional:** 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**.

   All matched logs are listed with details on the right.

Chapter 16 Team Management

The Team Management module allows you to manage roles and users, manage archives, view service details, configure the sender's email account, set the time zone for global use, display the time difference, enable GDPR, and set battery threshold of solar-powered cameras.

16.1 Role and User Management

The System allows you to add users and assign user's permissions for accessing and managing the System. Before adding users to the System, you should create roles to define a user's operation or configuration permissions to services or modules, and then assign role(s) to a user for granting the permissions to the user. A user can have many different roles.

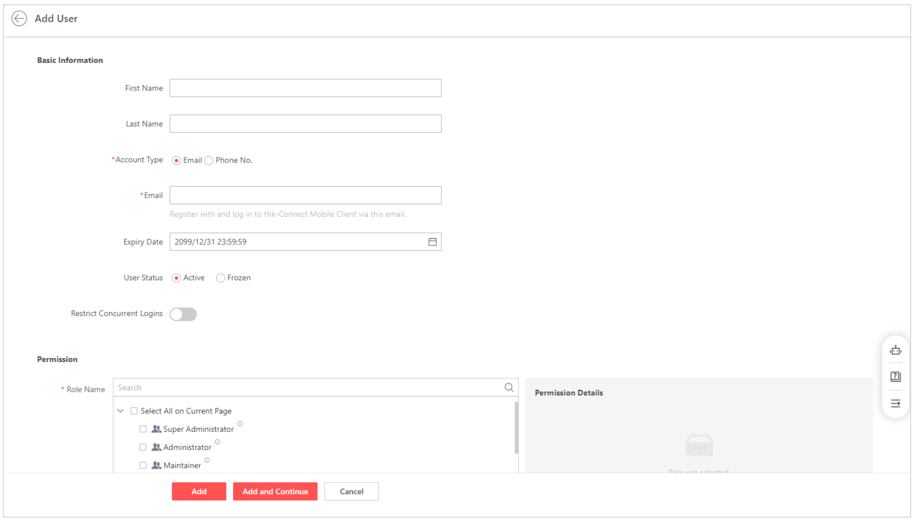
16.1.1 Add a Normal User

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

Before You Start
Make sure you are the super user or the user assigned with a role that has the User Management permission.

Steps

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**.



Add User

Basic Information

First Name

Last Name

*Account Type ● Email ○ Phone No.

*Email

Register with and log in to Hik-Connect Mobile Client via this email.

Expiry Date 2099/12/31 23:59:59

User Status ● Active ○ Frozen

Restrict Concurrent Logins

Permission

* Role Name Search

□ Select All on Current Page

□ Super Administrator

□ Administrator

□ Maintainer

Permission Details

Figure 16-1 Add a Normal User

3. Set basic information for the user.

First Name / Last Name

Enter the first name and last name of the user.

Note

The first name and last name of the normal user can be edited by the users assigned with the role of administrator.

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 to the email address.

Expiry Date

The date when the user account becomes invalid.

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. Select the role(s) that you want to assign to the user.

When you check the role(s), the permission details of all the selected role(s) will be displayed on the right.

5. 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.

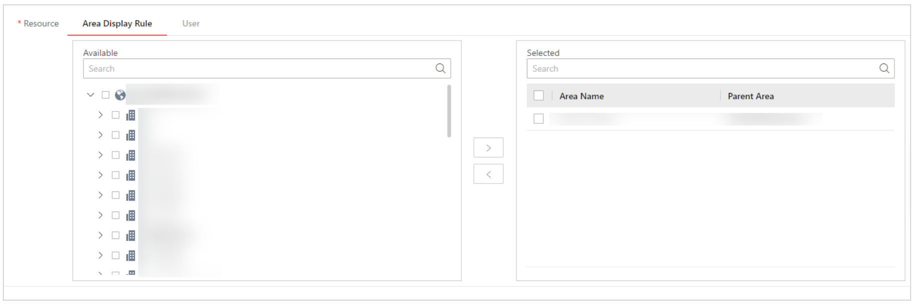


Figure 16-2 Area Display Rule

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.

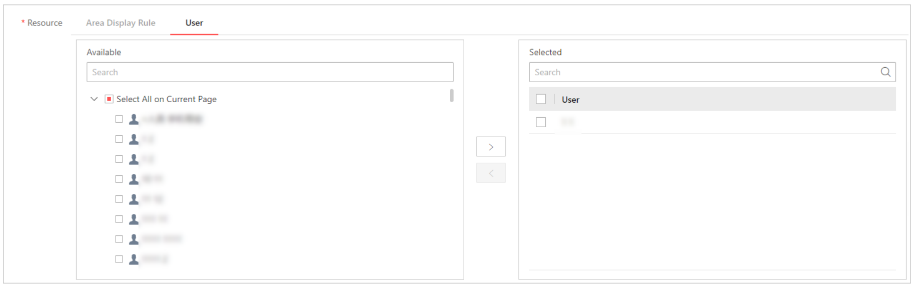


Figure 16-3 User

6. Do one of the following to complete adding the user.

- Click **Add** to add the user and return to the user management page.
- Click **Add and Continue** to save the settings and continue to add another user.

The initial password will automatically be sent to the email address configured above for the user. The user will be asked to change the password when logging in for the first time,

Note

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

7. Optional: Perform further operations after adding normal users.

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.

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).

Refresh User Status

Click **Refresh All** to get the latest status of all users.

Filter Users

Click ▽ to set conditions and filter users.

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.

Note

The above operations are only available on users you added or are assigned to you for management.

16.1.2 Add a Role

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

Before You Start

Make sure you are the super user or the user assigned with a role that has the Role Management permission.

Steps

Note

The System has predefined the following default roles: Super Administrator, Administrator, Operator, Maintainer, and Self-Service. 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 that has all permissions (including operation and configuration permissions) and access to all resources.

Administrator

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

Operator

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

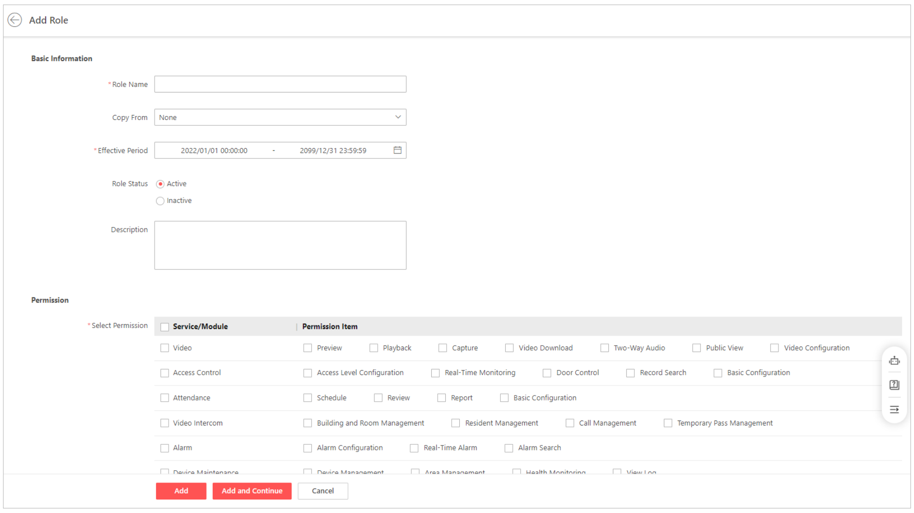
Maintainer

By default, the role 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 permissions, person management permissions, and operation permissions of the access control service and video intercom service.

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



Add Role

Basic Information

*Role Name

Copy From: None

*Effective Period: 2022/01/01 00:00:00 - 2099/12/31 23:59:59

Role Status: ● Active ○ Inactive

Description

Permission

*Select Permission

□ Service/Module	Permission Item
□ Video	□ Preview □ Playback □ Capture □ Video Download □ Two-Way Audio □ Public View □ Video Configuration
□ Access Control	□ Access Level Configuration □ Real-Time Monitoring □ Door Control □ Record Search □ Basic Configuration
□ Attendance	□ Schedule □ Review □ Report □ Basic Configuration
□ Video Intercom	□ Building and Room Management □ Resident Management □ Call Management □ Temporary Pass Management
□ Alarm	□ Alarm Configuration □ Real-Time Alarm □ Alarm Search
□ Device Maintenance	□ Device Management □ Area Management □ Health Monitoring □ View Log

Figure 16-4 Add a Role

3. Set the basic information for the role, including the role name, effective period, role status, description, and so on.

   Copy From

   Copy all settings from an existing role.

   Effective Period

   Set the time range within which the role takes effect. The role is inactive outside the effective period.

   Role Status

   Set the role status to **Active** or **Inactive**. For active roles, you can assign them to users.

4. Check the service(s)/module(s) or check the operation and configuration permission(s) of a service/module to assign the selected permission(s) to the role.

   Note

   The mobile credential permissions are not available when assigning permissions to a new role.

5. Complete adding the role.
   - Click **Add** to add the role and return to the role management page.
   - Click **Add and Continue** to save the settings and continue to add another role.

6. **Optional:** Perform further operations after adding roles.

   Edit a Role

   Click a role name to view and edit the role's settings, such as the role name, role status, effective period, and permissions.

   Note

   The default roles cannot be edited, except for the Maintainer role, whose permissions can be edited.

   Delete a Role

   Check a role and click **Delete** to delete the role.

Note

The default roles cannot be deleted.

Refresh Role Status Click **Refresh All** to get the latest status of roles.

Filter Roles Click ▽ and set the condition(s) (i.e., role status, name, and expiry date) to filter roles.

16.1.3 Import Users

When you need to add a large number of users, you can enter the user information in the predefined template and batch import to the platform.

Before You Start

Make sure you are the super user or the user assigned with a role that has the User Management permission.

Steps

1. On the top navigation bar of the Portal, click **Team Management → 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.
7. **Optional:** Refer to the last step in ***Add a Normal User*** for details about the available operations on users you added or that are assigned to you for management.

16.1.4 Change Password of Current User

You can change the password of your currently logged-in user account via the System.

Steps

1. Move the cursor to the user name in the top-right corner of the Portal.
2. In the drop-down list, click **Change Password** to open the Change Password pane.

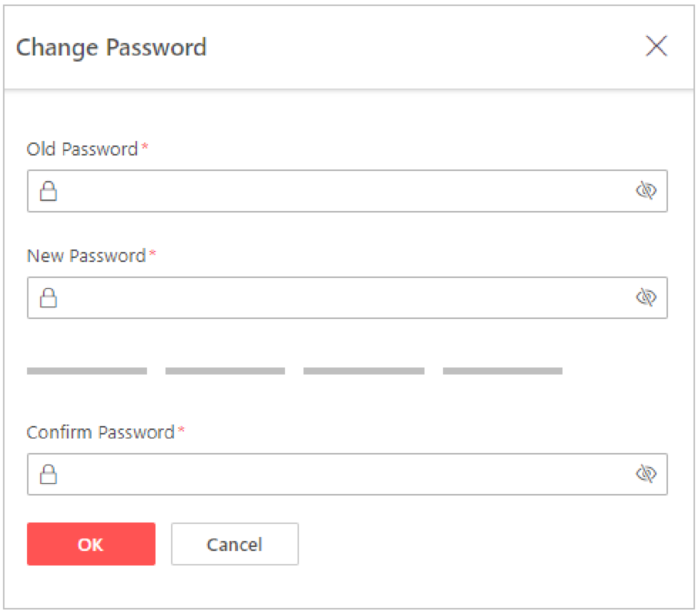


Figure 16-5 Change Password

3. Enter the old password and new password, and confirm the new password.

Caution

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

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

4. Click **OK** to save changes.

16.1.5 Delete the Super User

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

Before You Start

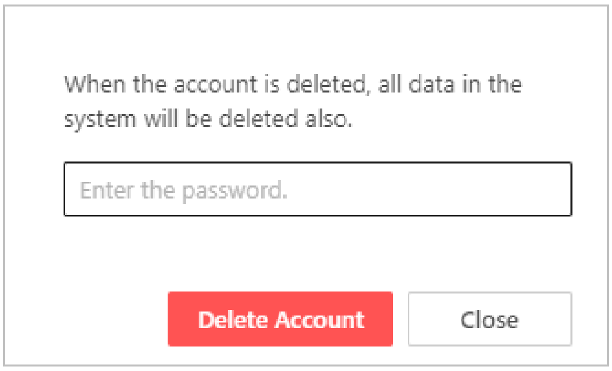
- Make sure you have logged in to the System by the super user.
- Make sure you have deleted all devices added to the System.

Steps

1. On the top navigation bar of the Portal, click **Team Management → 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.



When the account is deleted, all data in the system will be deleted also.

Enter the password.

Figure 16-6 Delete Super User

A window will pop up to let you confirm the deletion.

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.

All data in the System will be deleted if the super user is deleted.

16.2 Archive Management

You can archive the pictures captured and videos recorded and clipped during live view and playback. After they are archived, you can manage them (archives) in the Archive Management, including searching, editing, deleting, sharing, and exporting the archives, and adding, editing, and deleting archive tags and levels.

16.2.1 Archive Overview

On the Archive Overview page, you can view archives in recent 7 days, top 5 archive tags, and top 5 alarm triggered areas.

On the top navigation bar of the Portal, click **Team Management → Archive Management → Archive Overview** to enter the Archive Overview page.

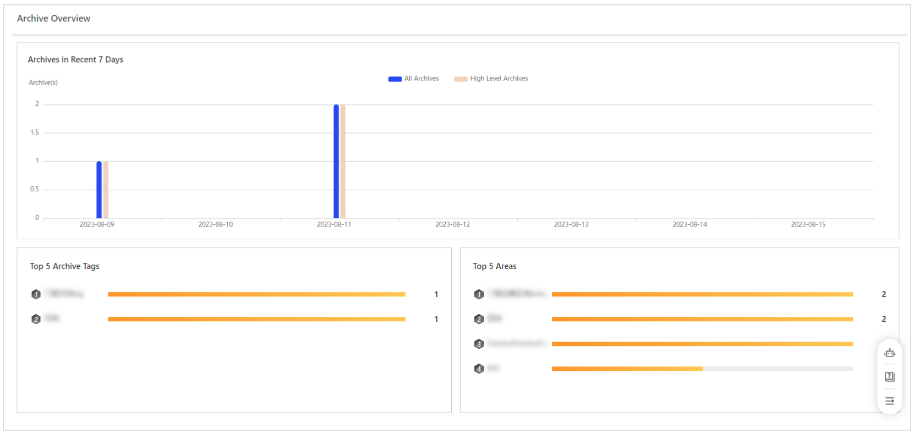


Figure 16-7 Archive Overview Page

Table 16-1 Archive Overview Page Description

Section	Description
Archives in Recent 7 Days	Displays numbers of all archives and high level archives each day for the recent 7 days. Click **All Archives** or **High Level Archives** to show or not to show the numbers of all archives or high level archives.
Top 5 Archive Tags	Displays the top 5 archive tags and the number of archives which use the tags during the archive retention period.
Top 5 Areas	Displays the top 5 alarm triggered areas and the number of archives during the archive retention period.

16.2.2 Archive Settings

You can define tags and levels to mark archives for fast search and handling reference.

Add an Archive Tag

You can define some tags to mark archives for fast search.

Steps

1. On the top navigation bar of the Portal, click **Team Management → Archive Management → Basic Archive Configuration → Archive Tag** to enter the Archive Tag page.

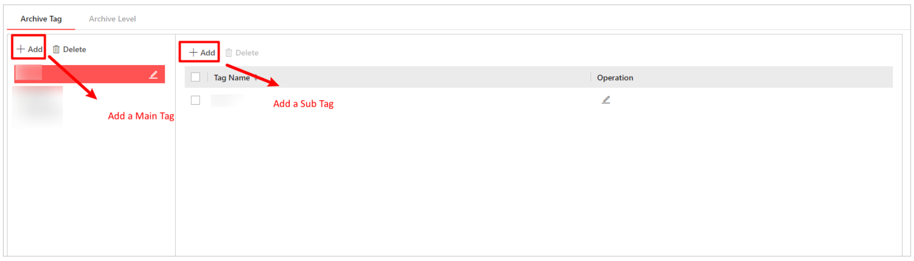


Figure 16-8 Archive Tag Page

2. On the Archive Tag page, click **Add** at the top of the left pane to add a main tag, or click **Add** in the center of the page to add a main tag if the tag is the first main tag.
3. Enter a main tag name and click **OK**.

Note

No more than 100 main tags can be added.

4. Select a main archive tag on the left pane, click **Add** at the top of the right list, and enter a name to add a sub tag for the selected main tag.

Note

No more than 100 sub tags can be added to one main tag.

5. **Optional:** After adding tags, perform the following operations.

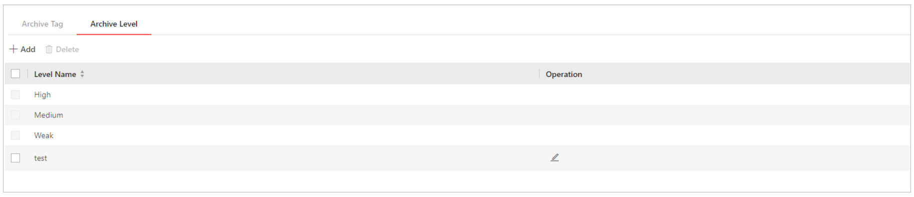
Edit Tag Name	• To edit the name of a main tag, select a main tag on the left pane and click ✎ . • To edit the name of a sub tag, select a sub tag in the right list and click ✎ in the Operation column.
Delete Tag	• To delete a main tag, select a main tag on the left pane and click **Delete** at the top of the left pane. • To delete the sub tag(s), check the sub tag(s) in the right list, and click **Delete** at the top of the right list.

Add an Archive Level

You can define some levels for marking the archive priorities. The System provides three predefined archive levels, including High, Medium, and Low.

Steps

1. On the top navigation bar of the Portal, click **Team Management → Archive Management → Basic Archive Configuration → Archive Level** to enter the Archive Level page.



☐	Level Name	Operation
☐	High	
☐	Medium	
☐	Weak	
☐	test	✎

Figure 16-9 Archive Level Page

2. Click **Add**.

3. Enter a name for the archive level and click **OK**.

Note

No more than 50 archive levels can be added.

4. Optional: After adding levels, perform the following operations.

Edit Level Name	Click ✎ in the Operation column of a level, and edit the level name.
Delete Levels	Check the level(s) and click **Delete** to delete the selected level(s).

Note

The predefined levels cannot be deleted or edited.

16.2.3 Archive Search

The Archive Search page displays archives in archived status and archiving status. You can search for archives by specifying the filtering condition(s). You can also perform certain operations on the archives according to their status, such as viewing the archived content, editing their information, deleting, sharing, and exporting the archives.

Filter Archives

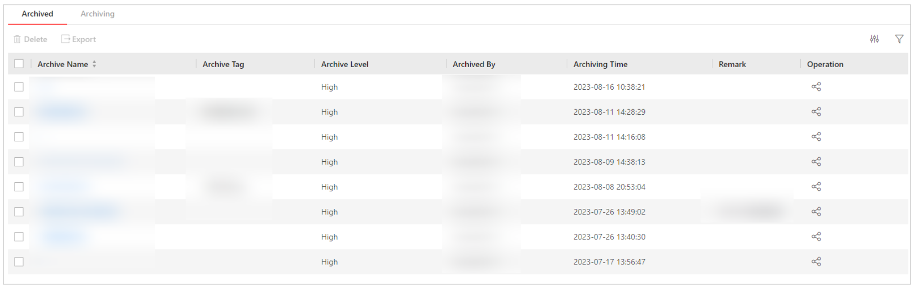
You can filter archives in archiving status and archived status by archive name, linked resource, archive tag, archive level, area where the archived content is located, account who created the archive, and archiving time interval within which the archive is created.

Steps

1. On the top navigation bar of the Portal, click **Team Management → Archive Management → Archive Search** to enter the Archive Search page.

2. Click **Archived** or **Archiving** to enter the page of archives with the corresponding status.

3. Click ▽ in the top right corner of the page to display the filter pane.



Archived | Archiving

Delete | Export

□	Archive Name	Archive Tag	Archive Level	Archived By	Archiving Time	Remark	Operation
□	[redacted]		High	[redacted]	2023-08-16 10:38:21		⋖
□	[redacted]	[redacted]	High	[redacted]	2023-08-11 14:28:29		⋖
□	[redacted]		High	[redacted]	2023-08-11 14:16:08		⋖
□	[redacted]		High	[redacted]	2023-08-09 14:38:13		⋖
□	[redacted]	[redacted]	High	[redacted]	2023-08-08 20:53:04		⋖
□	[redacted]		High	[redacted]	2023-07-26 13:49:02	[redacted]	⋖
□	[redacted]		High	[redacted]	2023-07-26 13:40:30		⋖
□	[redacted]		High	[redacted]	2023-07-17 13:56:47		⋖

Figure 16-10 Filter Pane of Archive Search Page

4. Set the condition(s) according to your needs.

5. Click **Filter** to filter archives that meet the configured conditions.

6. Optional: Perform the following operations.

Customize Column Displays

Click ⚙ in the top right corner and select/deselect the item(s) to customize the displayed column(s) of the list. Click **OK** to apply the custom settings.

View and Edit Archive

Click a specific archive name to view the archived content and basic information. You can edit the archive information if needed. For details, see ***View and Edit Archives*** .

Note

This operation is only for archives with the archived status.

Delete Archives

Check the archive(s), and click **Delete** to delete the selected archive(s).

Note

Archives cannot be restored after deletion. A pop-up window will ask you to confirm the operation before deleting the archive(s).

Share Archive

Click ⋖ in the Operation column of an archive to generate a link and create an extraction code for sharing the archive. For details, see ***Share Archives*** .

Note

This operation is only for archives with the archived status.

Retry Archiving

On the Archiving page, click ↻ in the Operation column of an archive to retry archiving it.

Export Archives

Check the archive(s), and click **Export** to export the selected archive(s) to your local PC. For details, see ***Export Archives*** .

Note

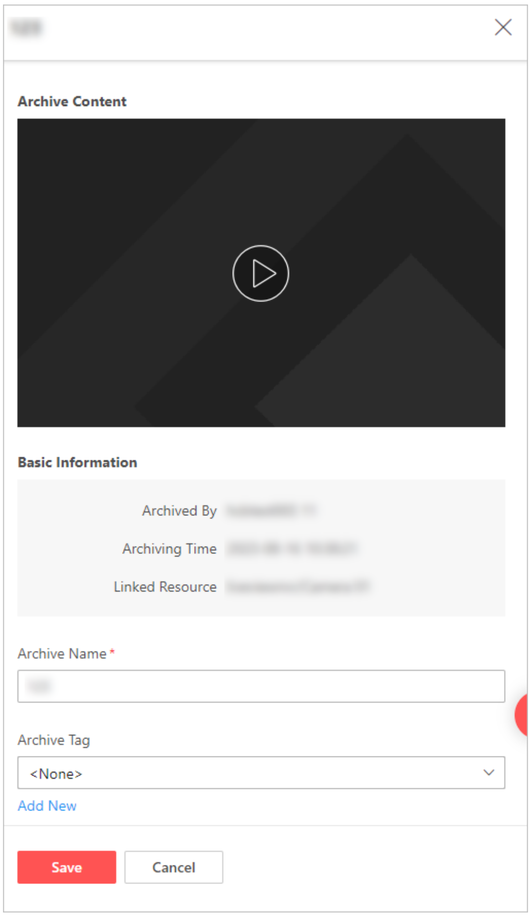
This operation is only for archives with the archived status.

View and Edit Archives

For archives with the archived status, you can view their archived content and basic information. You can also edit some of the information for the archives, including their name, tag, level, and remarks.

Steps

1. On the top navigation bar of the Portal, click **Team Management → Archive Management → Archive Search → Archived** to enter the Archived page.
2. **Optional:** Filter archives you want to view or edit. For details, see ***Filter Archives*** .
3. Click a specific archive name to open the details pane.



[redacted]

Archive Content

Basic Information

Archived By [redacted]

Archiving Time [redacted]

Linked Resource [redacted]

Archive Name*

[redacted]

Archive Tag

<None>

Add New

Save

Cancel

Figure 16-11 Archive Details Pane

Note

- The archived content could be in the form of a captured picture, a video footage, or alarm records.
- For archives of alarm records, you can view the alarm-related pictures, videos, and map screenshots.

4. Edit the archive name, tag, level, or remarks if needed.

Note

For the archive tag and level, you can click **Add New** to go to the Archive Tag or Archive Level page to create a new one. For details, refer to ***Add an Archive Tag*** and ***Add an Archive Level***

5. Click **Save** to update the archive information.

Share Archives

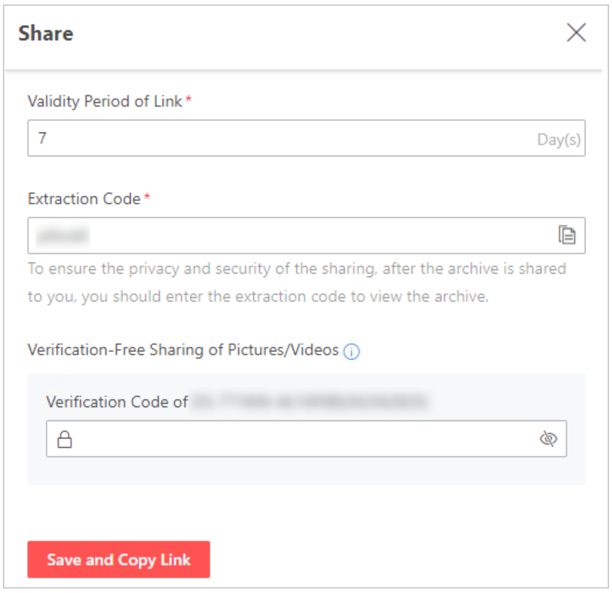
For archives with the archived status, you can generate a link to share an archive with other persons. To ensure a private and secure sharing, an extraction code is required to view the shared archive.

Steps

1. On the top navigation bar of the Portal, click **Team Management → Archive Management → Archive Search → Archived** to enter the Archived page.

2. Optional: Filter archives you want to view or edit. For details, see ***Filter Archives*** .

3. Click < in the Operation column of the archive to be shared to open the sharing settings pane.



Share

Validity Period of Link *

7 Day(s)

Extraction Code *

[redacted]

To ensure the privacy and security of the sharing, after the archive is shared to you, you should enter the extraction code to view the archive.

Verification-Free Sharing of Pictures/Videos ⓘ

Verification Code of [redacted]

Figure 16-12 Sharing Settings Pane

4. Set a validity period for the link.

Note

The shared archive will not be available after the link expires.

5. Set the extraction code for extracting the shared archive.

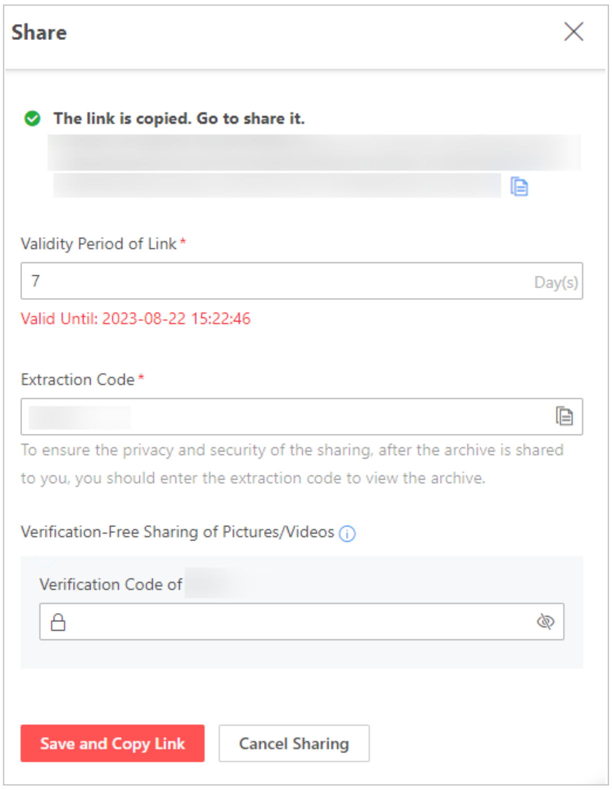
Note

The System automatically generates an extraction code for you. You can also create a custom extraction code by typing in the text box.

6. **Optional:** If the archive to be shared contains pictures captured or videos recorded by a device with stream encryption enabled, enter the verification code of the device when sharing so that the persons to be shared with can view the corresponding pictures or videos without entering the verification code.
7. Click **Save and Copy Link** to generate a link for sharing the archive and copy the link.

Note

You can click 🗎 beside the generated link to copy it again or click 🗎 to copy the extraction code only.



Share

The link is copied. Go to share it.

Validity Period of Link *

7 Day(s)

Valid Until: 2023-08-22 15:22:46

Extraction Code *

To ensure the privacy and security of the sharing, after the archive is shared to you, you should enter the extraction code to view the archive.

Verification-Free Sharing of Pictures/Videos

Verification Code of

Figure 16-13 Generated Link

8. Send the link and extraction code to the person(s) you want to share the archive with.

Note

- When you paste the link, the extraction code will be pasted under the link together.
- The link can be opened in browsers on a PC or a mobile phone. Enter the extraction code to view the content and information of the shared archive. Repeatedly entering an incorrect extraction code 6 times will cause the link to be invalid, so a new link needs to be generated in order to continue sharing the archive.
- To ensure the security of the content being viewed, archived content in the form of a video footage require the installation of the newest version of web control before viewing.

9. **Optional:** Click **Cancel Sharing** to invalidate the share link and stop sharing the archive if needed.

Export Archives

For archives with the archived status, you can export the content and basic information of the archives to your local PC.

Steps

1. On the top navigation bar of the Portal, click **Team Management → Archive Management → Archive Search Archived** to enter the Archived page.
2. **Optional:** Filter archives you want to view or edit. For details, see ***Filter Archives*** .
3. Check the archive(s) that you want to export.
4. Click **Export** at the top of the archive list on the Archived page to start exporting the selected archive(s) to your local PC.

Note

- If the archive(s) being exported contain any encrypted pictures or videos, you need to enter the verification code(s) of the device(s) by which the picture is captured or the video is recorded to download the archive(s).
- The exported files contain an XLSX file listing out the basic information of the archive(s) being exported, including a hyperlink for each archived content. Click on a hyperlink to open the folder containing the archived content, which could be in the form of a captured picture or a video footage. For archived content in the form of alarm records, each alarm record has its own folder containing the alarm-related pictures, videos, and map screenshots.

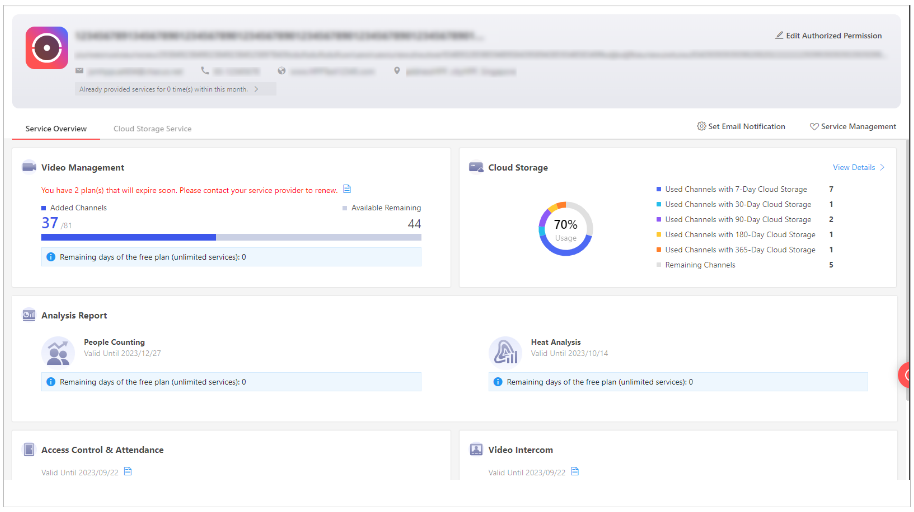
The export progress and result are displayed in the Download Center. For details, see ***Download Task Management*** .

16.3 Service Details

The Service Details module provides an overview of all services activated for the System, the detailed introduction of cloud storage service (if you have activated the service), an entry for starting/stopping using the service(s) for free, and the email configuration of service expiration notifications.

Note

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



[redacted]

Already provided services for 0 time(s) within this month.

You have 2 plan(s) that will expire soon. Please contact your service provider to renew.

Remaining days of the free plan (unlimited services): 0

Used Channels with 7-Day Cloud Storage	7
Used Channels with 30-Day Cloud Storage	1
Used Channels with 90-Day Cloud Storage	2
Used Channels with 180-Day Cloud Storage	1
Used Channels with 365-Day Cloud Storage	1
Remaining Channels	5

People Counting: Valid Until 2023/12/27

Remaining days of the free plan (unlimited services): 0

Heat Analysis: Valid Until 2023/10/14

Remaining days of the free plan (unlimited services): 0

Access Control & Attendance: Valid Until 2023/09/22

Video Intercom: Valid Until 2023/09/22

Figure 16-14 Service Details

- View your service provider's contact information (phone No. and email) and contact the service provider to enable the co-branding function for you to display the logo of your system.
- Click the gray area below the service provider information to open the Service Provider Operations pane for viewing the operation logs of your service provider, or you can click **View Detailed Operation Logs** to enter the Operation Log page to view details.
- Click **Edit Authorized Permission** in the top right corner of the page to open the Edit Authorized Permission pane, and then check/uncheck **System Access Permission** to authorize / cancel authorizing the system access permission to your service provider and set the corresponding validity period, or click **Discard Authorization** to cancel authorizing the service management permission.
- Click **Service Management** in the top right corner of the page and select/deselect the service(s) to start/stop using the service(s) if need. The deselected service(s) will not be displayed on the Service Overview page.

Note

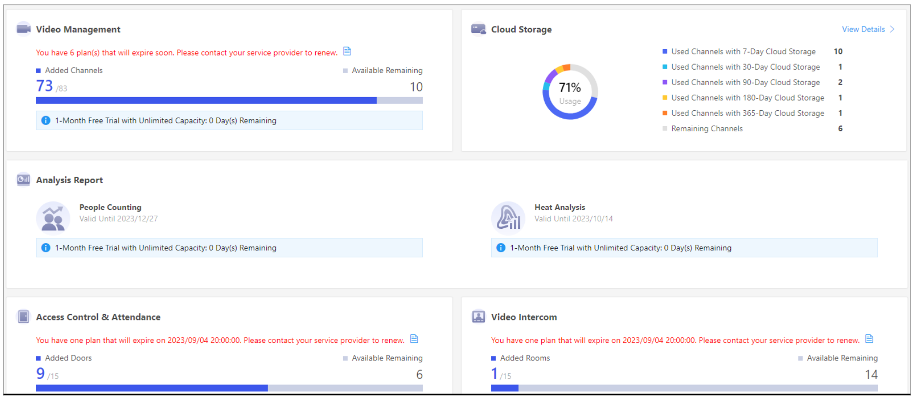
You cannot deselect all services at the same time.

- Click **Set Email Notification** to set the content language for the email notification which will be sent to you when the service plan is going to expire in 14/7/3/1 day(s) or has expired.
- Click **Service Overview** or **Cloud Storage Service** to view the information about services activated for the System or view details of the cloud storage service. See ***Service Overview*** and ***View Details of Cloud Storage Service*** for details.

16.3.1 Service Overview

On the Service Overview page, you can view the information about the service(s) activated for the System, such as the expiry time, the plan details, the used capacity, and the remaining capability.

On the top navigation bar of the Portal, click **Team Management → Service Details → Service Overview** to enter the Service Overview page.



You have 6 plan(s) that will expire soon. Please contact your service provider to renew.

1-Month Free Trial with Unlimited Capacity: 0 Day(s) Remaining

Used Channels with 7-Day Cloud Storage	10
Used Channels with 30-Day Cloud Storage	1
Used Channels with 90-Day Cloud Storage	2
Used Channels with 180-Day Cloud Storage	1
Used Channels with 365-Day Cloud Storage	1
Remaining Channels	6

People Counting Valid Until 2023/12/27

1-Month Free Trial with Unlimited Capacity: 0 Day(s) Remaining

Heat Analysis Valid Until 2023/10/14

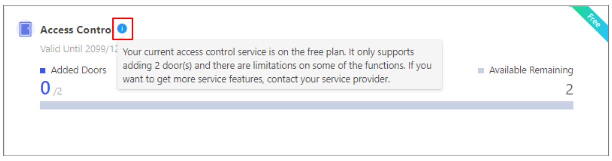
1-Month Free Trial with Unlimited Capacity: 0 Day(s) Remaining

You have one plan that will expire on 2023/09/04 20:00:00. Please contact your service provider to renew.

You have one plan that will expire on 2023/09/04 20:00:00. Please contact your service provider to renew.

Figure 16-15 Service Overview

- View the expiry time and the total/used/remaining capacity of the service(s) activated for the System.
- For the service(s) used for free or with trial plan, move the cursor on ⓘ to show the description about the plan details.

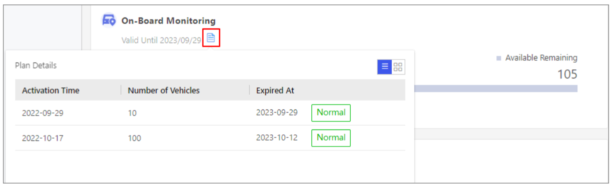


Valid Until 2099/12

Your current access control service is on the free plan. It only supports adding 2 door(s) and there are limitations on some of the functions. If you want to get more service features, contact your service provider.

Figure 16-16 Description About Free Plan

- For the service(s) with the plan(s) activated or with both the free plan and trial plan, click 🗎 to view the plan details (such as activation time, capacity, and expiry time) in different display mode.

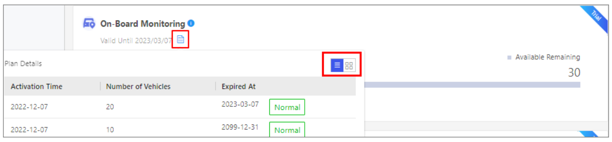


Valid Until 2023/09/29

Plan Details

Activation Time	Number of Vehicles	Expired At	
2022-09-29	10	2023-09-29	Normal
2022-10-17	100	2023-10-12	Normal

Figure 16-17 Activated Plan Details



Valid Until 2023/03/07

Plan Details

Activation Time	Number of Vehicles	Expired At	
2022-12-07	20	2023-03-07	Normal
2022-12-07	10	2099-12-31	Normal

Figure 16-18 Free and Trial Plans Details

Note

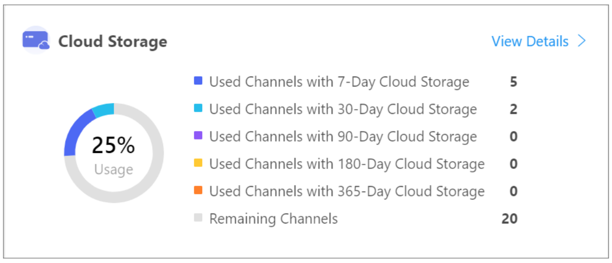
- If the service plans cannot meet your requirements or a plan is about to expire / has expired, contact your service provider.
- If your service provider changes the service plan, the super user will be notified of the changed service information including the new capacity and expiry time.

- For the cloud storage service with the service package(s) purchased, you can view the number of remaining channels, the number of used channels with 7-day / 30-day / 90-day / 180-day / 365-day cloud storage, and the usage percentage in a pie chart.

  You can also click **View Details** to enter the details page of cloud storage service. Refer to ***View Details of Cloud Storage Service*** for details.

Note

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



Cloud Storage

View Details >

25%
Usage

Used Channels with 7-Day Cloud Storage	5
Used Channels with 30-Day Cloud Storage	2
Used Channels with 90-Day Cloud Storage	0
Used Channels with 180-Day Cloud Storage	0
Used Channels with 365-Day Cloud Storage	0
Remaining Channels	20

Figure 16-19 Cloud Storage Service Overview

16.3.2 Invite a Service Provider to Manage System

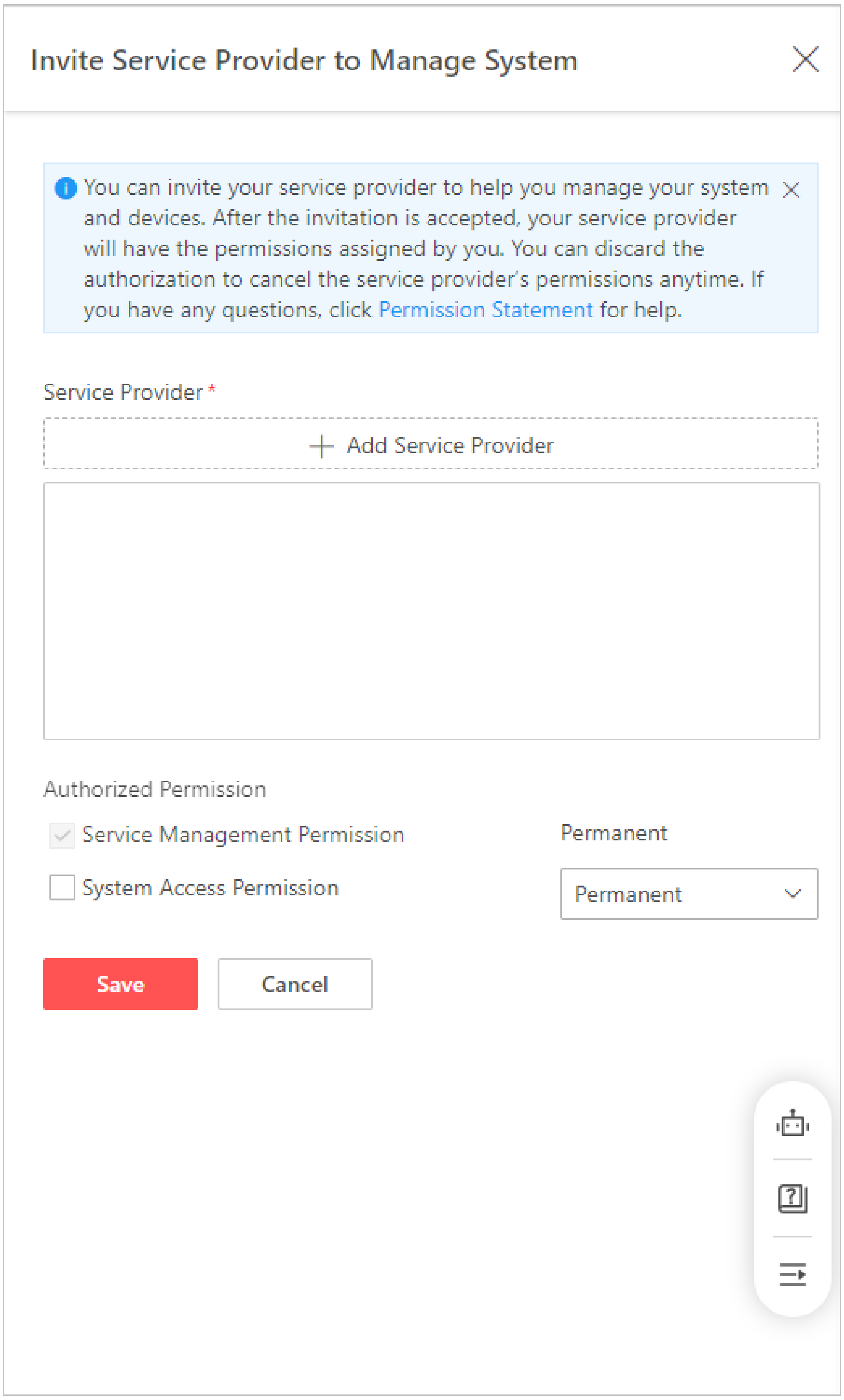
If your account is self-registered rather than handed over by a service provider, you can invite a service provider to link with your account, so that your service provider can provide you with value-added services. After the invitation is accepted, your service provider will have the permissions assigned by you. You can discard the authorization to cancel the service provider's permissions anytime.

Before You Start

Make sure your role is admin.

Steps

1. Go to **Team Management → Service Details → Authorize Now** to open the pane of inviting a service provider.



Invite Service Provider to Manage System

You can invite your service provider to help you manage your system and devices. After the invitation is accepted, your service provider will have the permissions assigned by you. You can discard the authorization to cancel the service provider's permissions anytime. If you have any questions, click Permission Statement for help.

Service Provider *

+ Add Service Provider

Authorized Permission

☑ Service Management Permission

□ System Access Permission

Permanent: Permanent

Figure 16-20 Invite Service Provider to Manage System

2. Select a service provider.

- Click **Add Service Provider**, and enter the service provider's email in the pop-up window.

- Previously added service providers are displayed in the list if there are any, and you can select an existing service provider from the list.

3. Select the desired authorized permission.

Service Management Permission

The service management permission is selected and set as **Permanent** by default and can not be changed.

System Access Permission

The system access permission can be set to **1 Hour**, **2 Hours**, **4 Hours**, **8 Hours**, **Permanent**, and **Custom Days**, and the maintenance personnel or service provider can only log in to the platform within the validity period.

4. Click **Save**.

- The authorization status will become **Invitation Is Sent, Wait...**.
- In the Message Center, you will see a service message that shows an invitation is sent to the service provider.

Note

During the period when the invitation has not yet been processed by the service provider, or the invitation has not expired, you are not allowed to invite a new service provider.

5. You can perform the following operations.

Edit Authorized Permission	Click **Edit Authorized Permission** to edit service access permission.
Discard Authorized Permission	If you want to change your service provider, click **Edit Authorized Permission → Discard Authorization** first, and then invite a new service provider. If you discard the authorized permission, your service provider will receive a notification about it.
View Service Provider Information	After a service provider accepts the invitation, you can view the service provider's information including email, phone number, account name, and location on the Service Details page.
Activate License to Expand Capacity or Renew Services	a. Click **Activate License**, enter the license code, and click **Verify**. b. Select **Expand Capacity** or **Renew**. After a license is activated, click **Activate License → View License Activation Records** to view the activation details.

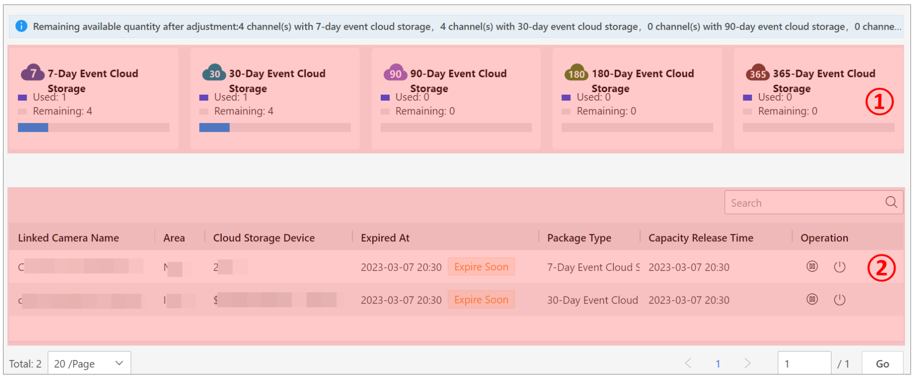
16.3.3 View Details of Cloud Storage Service

For the cloud storage service, you can view the number and expiry time of used or remaining channels with different service package types, and enable/pause/disable the cloud storage service for cameras linked to cloud storage devices.

Note

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

On the top navigation bar of the Portal, click **Team Management → Service Details → Cloud Storage Service** to enter the Cloud Storage Service page.



Remaining available quantity after adjustment:4 channel(s) with 7-day event cloud storage, 4 channel(s) with 30-day event cloud storage, 0 channel(s) with 90-day event cloud storage, 0 channe...

7-Day Event Cloud Storage
Used: 1
Remaining: 4

30-Day Event Cloud Storage
Used: 1
Remaining: 4

90-Day Event Cloud Storage
Used: 0
Remaining: 0

180-Day Event Cloud Storage
Used: 0
Remaining: 0

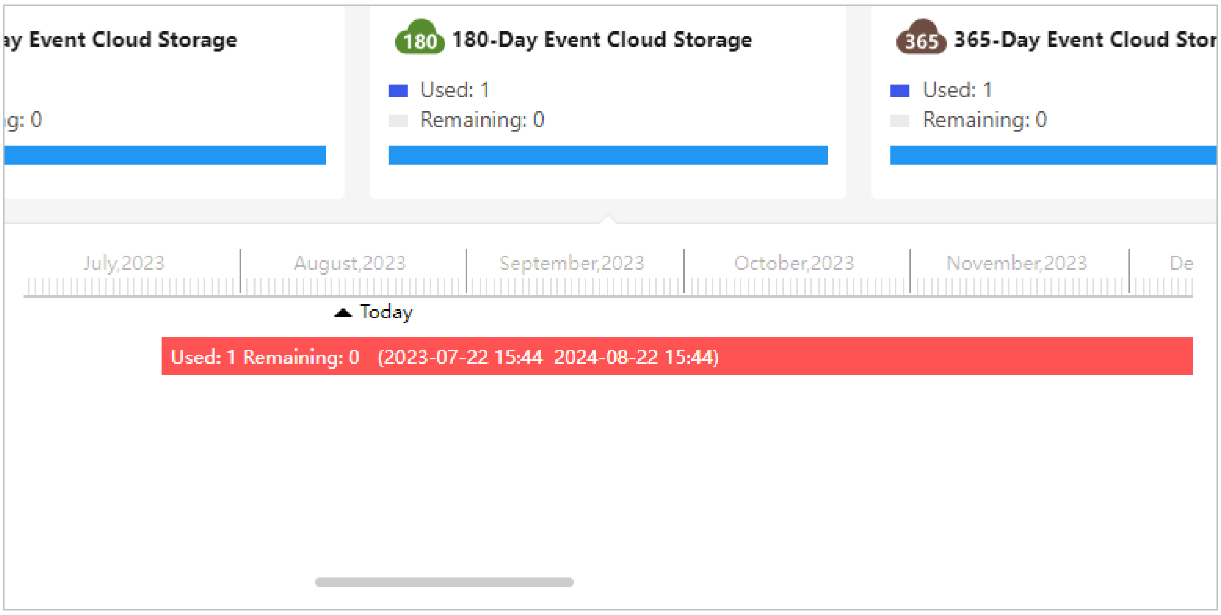
365-Day Event Cloud Storage
Used: 0
Remaining: 0

Search

Linked Camera Name	Area	Cloud Storage Device	Expired At	Package Type	Capacity Release Time	Operation
C[redacted]	N[redacted]	2[redacted]	2023-03-07 20:30 Expire Soon	7-Day Event Cloud S	2023-03-07 20:30	
c[redacted]	I[redacted]	$[redacted]	2023-03-07 20:30 Expire Soon	30-Day Event Cloud	2023-03-07 20:30	

Total: 2 20 /Page 1 1 /1 Go

Figure 16-21 Details Page of Cloud Storage Service



ay Event Cloud Storage
g: 0

180-Day Event Cloud Storage
Used: 1
Remaining: 0

365-Day Event Cloud Stor
Used: 1
Remaining: 0

Used: 1 Remaining: 0 (2023-07-22 15:44 2024-08-22 15:44)

Figure 16-22 View Expiry Time of Plans Activated for Channels

Table 16-2 Description of the Details Page

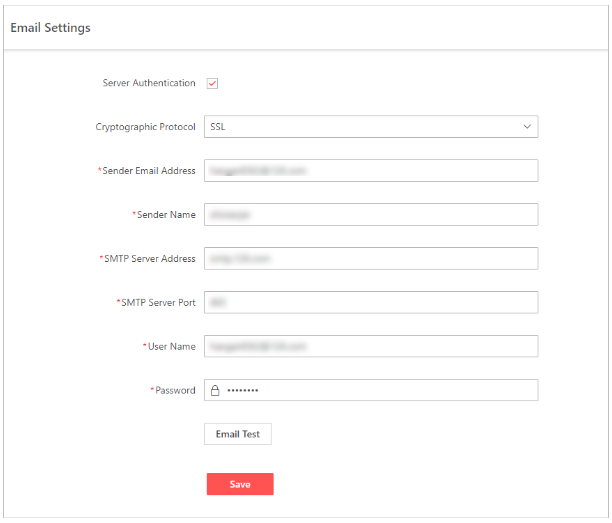
Area No.	Description
①	• View the number of used or remaining channels with the 7/30/90/180/365-day (which indicates the retention period of the event video footage on the cloud) event cloud storage. • Move the cursor on the 7/30/90/180/365-Day Event Cloud Storage area and a window will appear. You can view the expiry time of plans activated for channels in the window.
②	• View the cloud storage service details (such as expiry details, status, package type, and capacity release time) of cameras linked to NVRs or Hik-ProConnect boxes. • Click ⏸ / 🕓 / ⏻ in the Operation column of a linked camera to pause/enable/disable the cloud storage service for it.

16.4 Configure Email Account

You should configure the parameters of the sender's email account before the System can send the report to the designated email account(s) as the email linkage.

Steps

1. On the top navigation bar of the Portal, click **Team Management → Email Settings** to enter the Email Settings page.



Email Settings

Server Authentication ☑

Cryptographic Protocol: SSL

*Sender Email Address: [redacted]

*Sender Name: [redacted]

*SMTP Server Address: [redacted]

*SMTP Server Port: [redacted]

*User Name: [redacted]

*Password: ••••••••

Figure 16-23 Email Settings

2. Configure the parameters according to actual needs.

Server Authentication

If you check **Server Authentication**, you should complete the authentication before you log in to the mail server.

Cryptographic Protocol

Select the cryptographic protocol of the email to protect the email content if it is required by the SMTP server.

Sender Email Address

Enter the email address of the sender to receive messages.

Sender Name

Enter the sender name to receive messages.

SMTP Server Address

Set the IP address or host name of the SMTP Server.

SMTP Server Port

Set the TCP/IP port used for the SMTP server.

3. Click **Email Test** to test whether the email settings work or not.

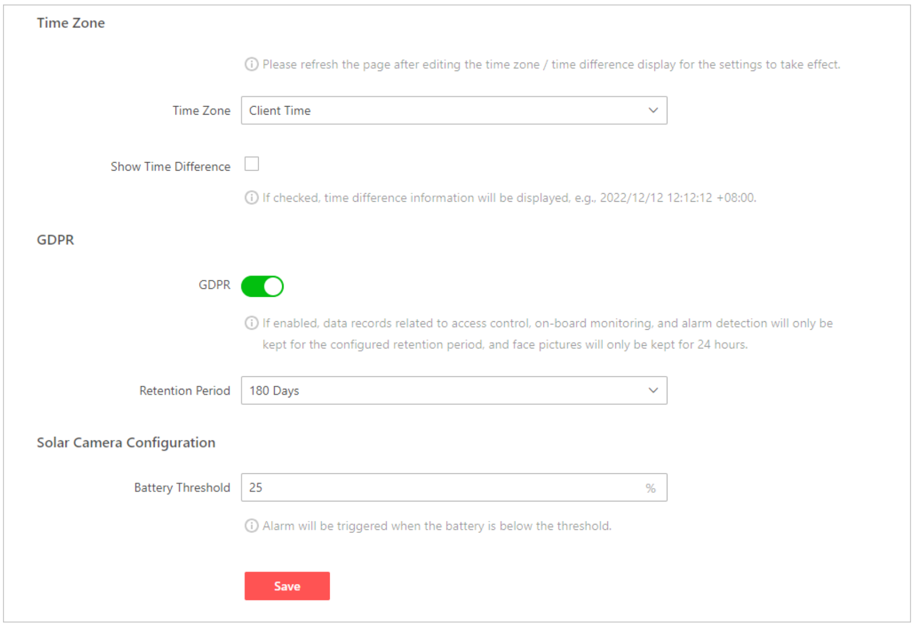
The corresponding attention message box will pop up.

4. Click **Save**.

16.5 Team Configuration

On the Team Configuration page, you can select which time (client time or device time) to use globally, choose whether to display the time difference, enable GDPR (General Data Protection Regulation) and set the retention period of data records, and set the battery threshold for solar-powered camera alarms.

On the top navigation bar, click **Team Management → Team Configuration → Team Configuration** to enter the Team Configuration page.



Time Zone

Please refresh the page after editing the time zone / time difference display for the settings to take effect.

Time Zone: Client Time

Show Time Difference □

If checked, time difference information will be displayed, e.g., 2022/12/12 12:12:12 +08:00.

GDPR

GDPR: ●

If enabled, data records related to access control, on-board monitoring, and alarm detection will only be kept for the configured retention period, and face pictures will only be kept for 24 hours.

Retention Period: 180 Days

Solar Camera Configuration

Battery Threshold: 25 %

Alarm will be triggered when the battery is below the threshold.

Figure 16-24 System Configuration

Time Zone

Select **Client Time** (default) or **Device Time** for video / data records / log search, playback, and expiration detection.

You can check **Show Time Difference** to display the time difference between UTC (Universal Time Coordinated) and the local time (the client time or device time). For example, "2022/11/01 10:00:00 +8:00".

Note

- **Client Time** refers to the time of the country or region where the user is located, while **Device Time** refers to the time of the country or region where the device is located.
- The time zone settings is only valid for the current logged-in user.

GDPR

When enabled, data records related to access control, and attendance, will only be kept for the configured retention period, but face pictures will only be kept for 24 hours. You can select a retention period from the drop-down list. The longest retention period is 180 days.

Solar-Powered Camera Configuration

Set a battery threshold for the Battery Low alarm of solar-powered cameras. When the battery of a solar-powered camera is lower than the configured threshold, an alarm will be triggered (if the Battery Low alarm rule is configured).

For how to configure a Battery Low alarm, refer to ***Add an Alarm Rule*** .

See Far, Go Further