

HikCentral Access Control V2.4.0

User Manual

Symbol Conventions

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

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

Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

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

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

Contents

Chapter 1 Introduction 1

Chapter 2 Recommended Running Environment for Server 2

Chapter 3 Getting Started 3

3.1 Login 3

3.2 Home Page Overview 5

3.3 Download Mobile Client 8

Chapter 4 Device and Server Management 10

4.1 Before You Start 10

4.2 Add Device(s) 10

4.2.1 Adding Modes Supported by Different Devices 10

4.2.2 Parameters on Add Device Pages 14

4.3 Add Server(s) 15

4.4 After Adding Devices/Servers: Operations on Device List Page 16

4.4.1 Configure Parameters for Access Control Devices 17

4.4.2 Upgrade Device Firmware 24

4.4.3 Create Password for Inactive Device(s) 27

4.4.4 Edit Online Device's Network Information 28

4.4.5 Restore/Reset Device Password 29

Chapter 5 Area Management 32

5.1 Add an Area Manually 32

5.2 Import Areas in a Batch 33

5.3 Add Element to Area 33

5.4 Edit Element in Area 34

5.4.1 Parameters on Edit Door Page 35

5.4.2 Edit Alarm Input/Output in an Area 37

5.5 Remove Element from Area 37

Chapter 6 Person Management 38
6.1 Add Departments 38
6.2 Basic Configuration Before Managing Persons 40
6.3 Add Person 40
6.3.1 Add a Single Person Manually 41
6.3.2 Batch Add Persons by Template 44
6.3.3 Import Domain Persons 46
6.3.4 Import Persons from Device 47
6.3.5 Operations Available on Person List 50
6.4 Person Self-Registration 53
6.4.1 Set Self-Registration Parameters 53
6.4.2 Scan QR Code for Self-Registration 55
6.4.3 Review Self-Registered Person Information 56
6.5 Resigned Persons Management 57
6.6 Credentials Management 58
6.6.1 Manage Credentials for a Single Person 58
6.6.2 Import Profile Pictures 61
6.6.3 Card Management 62
6.7 Position Management 70
Chapter 7 Access Control Management 71
7.1 Flow Chart of Door Access Control 72
7.2 Assign Access Level to Persons 73
7.2.1 Add Access Level 74
7.2.2 Manually Assign Access Level 75
7.2.3 Access Level Overview 79
7.2.4 Regularly Apply Access Level Settings to Devices 80
7.2.5 Clear Persons' Access Levels 81
7.2.6 Set Access Schedule Template 81

7.3 How to Open the Door by Your Smart Phone 82
7.4 Real Time Monitoring 86
7.5 Data Search 89
7.6 Advanced Functions 92
7.6.1 Add Remain Unlocked and Remain Locked Rule 92
7.6.2 Configure First Person In 92
7.6.3 Manage Multi-Factor Authentication 93
7.6.4 Configure Multi-Door Interlocking 95
7.6.5 Anti-Passback 95
7.6.6 Add a Batch Locking and Unlocking Group 98
7.6.7 Add a Final Authentication Counting Group 98
7.6.8 Configure Authentication Mode 99
7.6.9 Apply Advertisement to Access Control Devices 101
7.6.10 Add Audio Broadcast 102
7.6.11 Add an Authentication Password 104
7.7 Access Control Test 105
Chapter 8 Attendance 110
8.1 Flow Chart of Time and Attendance 112
8.2 Configure Attendance Mode 112
8.3 Add an Attendance Group 113
8.4 Basic Configuration 116
8.4.1 Specify Attendance Check Points 116
8.4.2 Add a Pay Code 120
8.4.3 Edit a Fixed Code 121
8.4.4 Add a Leave Rule 122
8.4.5 Configure Check-In/Check-Out via Mobile Client 125
8.4.6 Configure Storage Settings 127
8.5 Configure Attendance Rules for Global / Department / Attendance Group 127

8.5.1 Define Weekends 127
8.5.2 Configure Attendance Calculation Rule 128
8.5.3 Define Absence 128
8.5.4 Add Holidays Requiring Attendance 131
8.5.5 Calculation of Leaves 132
8.5.6 Configure Overtime Parameters 132
8.5.7 Configure Authentication Mode 135
8.6 Add Timetable 135
8.6.1 Add Break Timetables 135
8.6.2 Add Timetable for Normal Shift 137
8.6.3 Add Timetable for Flexible Shift 140
8.7 Add Shift 142
8.8 Manage Schedule 143
8.8.1 Schedule Overview 143
8.8.2 Assign Schedule in Quick Mode 144
8.8.3 Assign Schedule to Department 144
8.8.4 Assign Schedule to Attendance Groups 145
8.8.5 Assign Schedule to Person 147
8.8.6 Add Temporary Schedule 148
8.9 Configure Calculation Mode of Attendance Results 148
8.9.1 Manually Calculate Attendance Results 149
8.9.2 Set Auto-Calculation Time of Attendance Results 149
8.10 Approval Flow 149
8.10.1 Step 1: Add Approval Role 150
8.10.2 Step 2: Configure Approval Flow 150
8.10.3 Step 3: Add Leave Rule 151
8.10.4 Step 4: Employees Submit Applications 152
8.10.5 Step 5: Reviewers Review Applications 153

8.10.6 Step 6: Employees Check Application Status 155
8.11 Application Management for Admin 155
8.11.1 Apply for a Leave / Check-In/Out Correction / Overtime 156
8.11.2 Import Applications 156
8.11.3 Review or Undo Applications 157
8.12 Application Management for Employee 157
8.12.1 Login via Web Client (Employee) 157
8.12.2 Overview of Personal Attendance Data 158
8.12.3 Submit and View Applications 159
8.12.4 (Administrator) Review Employees' Applications 160
8.12.5 View and Export Attendance Records and Reports 161
8.13 View Attendance Records 161
8.13.1 Import Transactions 162
8.14 Manage Attendance Reports 163
8.14.1 Set Display Rules for Attendance Report 163
8.14.2 View Daily/Weekly/Monthly/Summary Attendance Reports 163
8.14.3 Send Attendance Report Regularly 165
8.14.4 Add a Custom Report 167
Chapter 9 Video Intercom Management 169
9.1 Flow Chart of Video Intercom 169
9.2 Add Video Intercom Device 171
9.3 Configure Device Parameters 171
9.4 Add a Call Schedule for a Door Station 172
9.5 Link Resources with Indoor Stations 173
9.5.1 Link Doorbell to Indoor Station 173
9.5.2 Link Persons to Indoor Station 174
9.6 Apply Data to Indoor Station 174
9.6.1 Add and Apply a Notice 174

9.6.2 Apply Software Package to Indoor Station 176
9.7 Make and Receive Calls on Platform 177
9.7.1 Add Call Schedule Template 178
9.7.2 Add Call Recipients 178
9.8 Apply Advertisements to Door Stations 178
Chapter 10 Skin-Surface Temperature Screening 180
10.1 Temperature Screening Configuration 180
10.1.1 Group Temperature Screening Points 180
10.1.2 Configure Temperature Screening Parameters 181
10.2 Real-Time Skin-Surface Temperature Monitoring 181
10.3 Search History Temperature Screening Data 183
10.4 Registration 183
10.4.1 Register Person Information 184
10.4.2 Customize Registration Template 185
10.4.3 View Registered Person Information 185
10.5 Search for Temperature Screening Records 186
10.6 Configure the Scheduled Report of Screening 187
10.7 Generate Skin-Surface Temperature Analysis Report 190
Chapter 11 Map Management 192
11.1 Configure Map 192
11.1.1 Select and Set GIS or E-map for an Area 193
11.1.2 Add Hot Spot to Map 194
11.1.3 Add Hot Region to Map 195
11.1.4 Add Tag to Map 196
11.1.5 Add Resource Group on Map 197
11.1.6 Add Event and Alarm to Map 198
11.1.7 Add Geographic Area to Map 198
11.2 Monitor on Map 199

11.2.1 View and Operate Hot Spot 199
11.2.2 Preview Hot Region 201
11.2.3 Operate Resources from Geographic Area 201
Chapter 12 Management of Platform Accounts and Security 202
12.1 Add a Role 202
12.2 User Management 204
12.2.1 Add a Normal User 204
12.2.2 Import Domain Users 205
12.2.3 Import Normal Users via an Excel File 207
12.2.4 Operations After Adding Users 208
12.2.5 Export Normal Users 208
12.3 System Security Settings 209
12.3.1 Set Basic Security Parameters 209
12.3.2 Configure Security Questions 210
12.3.3 Change Password of Current User 210
12.3.4 Forgot Password 212
12.4 Configure Permission Schedule 214
Chapter 13 System Configuration 215
13.1 Normal Settings 215
13.1.1 Set User Preference 215
13.1.2 Set Holiday 217
13.1.3 Set Printer 218
13.1.4 Set Card Template 219
13.2 Calling Settings 220
13.2.1 Add Call Recipients 220
13.2.2 Add a Receiving Schedule Template 220
13.2.3 Configure Call Parameters 221
13.3 Network Settings 222

13.3.1 Set NTP for Time Synchronization 222
13.3.2 Set Active Directory 223
13.3.3 Set Device Access Protocol 224
13.3.4 Set WAN Access 224
13.3.5 Set IP Address for Receiving Device Information 224
13.4 Storage Settings 225
13.4.1 Set Storage on System Server 225
13.4.2 Set Storage for Records 226
13.5 Email Settings 226
13.5.1 Configure Email Account 226
13.5.2 Add Email Template for Sending Report Regularly 227
13.5.3 Add Email Template for Event and Alarm Linkage 229
13.6 Security Settings 230
13.6.1 Set Transport Protocol 230
13.6.2 Set Database Password 231
13.6.3 Enable Export of Profile Pictures 231
13.6.4 Watermark Settings 231
13.7 Third-Party Integration Settings 232
13.7.1 Integrate via OpenAPI Gateway 232
13.7.2 Data Interchange 232
13.8 Advanced Settings 236
13.8.1 Diagnosis and Maintenance 236
13.8.2 Reset Device Network Information 237
13.9 Set Company Information 237
Chapter 14 Event and Alarm 239
14.1 Manage Event and Alarm 240
14.1.1 Supported Events and Alarms 240
14.1.2 Add Combined Alarm 240

14.1.3 Add Generic Event 245
14.1.4 Add User-Defined Event 248
14.2 Set Basic Event and Alarm Parameters 249
14.2.1 Configure Receiving Schedule Template 249
14.2.2 Custom Alarm Settings 251
14.2.3 Configure Alarm Receiving Settings 254
14.2.4 Send Event and Alarm Report Regularly 255
14.3 Event and Alarm Search 257
14.3.1 Event and Alarm Overview 257
14.3.2 Search for Event and Alarm Logs 258
Chapter 15 Maintenance 260
15.1 Real-Time Health Status Overview 260
15.2 Set Basic Maintenance Parameters 262
15.2.1 Set Warning Threshold for Streaming Media Usage 262
15.2.2 Set Network Timeout 263
15.2.3 Set Auto-Check Frequency 264
15.3 Resource Status 265
15.4 Log Search 266
15.4.1 Search for Server Logs 266
15.4.2 Search for Logs Stored on Device 266
15.5 Service Manager 267
15.6 Set System Data Backup 268
15.7 Restore System Data 269
15.8 Export Configuration Data 270
15.9 Import Configuration Files 270

Chapter 1 Introduction

The platform is developed for the management of security system and features flexibility, scalability high reliability, and powerful functions.

The platform provides features including information sharing, convenient connection, and multi-service cooperation. It is capable of adding devices for management, access control, time and attendance, alarm linkage, and so on.

The complete platform contains the following components. You can install the components according to actual needs.

Component	Introduction
System Management Service (SYS)	• Provides the unified authentication service for connecting with the clients and servers. • Provides the management for the users, roles, permissions, devices, and services. • Provides the configuration APIs for monitoring and management modules.
Built-in Streaming Service	Provides forwarding and distributing the audio and video data of live view.

The following table shows the provided clients for accessing or managing the platform.

Client	Introduction
Web Client	Web Client is a B/S client for managing system. It provides multiple functionalities, including device management, area management, event configuration, user management, and so on.
Mobile Client	Mobile Client is the software designed for getting access to the platform via Wi-Fi, 4G, and 5 G networks with mobile device. It fulfills the functions of the devices connected to the platform.

Chapter 2 Recommended Running Environment for Server

Operating System

- Microsoft® Windows 11 (64-bit) (including version 24H2)
- Microsoft® Windows 10 (64-bit)
- Microsoft® Windows Server 2025
- Microsoft® Windows Server 2019 (64-bit)
- Microsoft® Windows Server 2016 (64-bit)
- Microsoft® Windows Server 2012 R2 (64-bit)
- Microsoft® Windows Server 2012 (64-bit)
- Microsoft® Windows Server 2022

Note

For Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) updated in April, 2014.

CPU

Intel® Core™ i3-8100 and later

Memory

4 GB+

Web Browser

Firefox® 125+, Google Chrome® 125+, Microsoft® Edge 125+, and Safari® 16.6+.

HDD

SATA 7200 RPM Enterprise Class disk with 650 GB storage capacity. When running the SYS, there should be at least 1 GB free space.

Chapter 3 Getting Started

The following content describes the tasks typically involved in setting a working system.

On the lower left of the log-in page, click **Scan QR Code for Help**, and then scan the QR Code by your smart phone to view the how-to videos of the platform.

Before accessing the SYS, finish the following tasks.

- Set the transfer protocol. For details, refer to ***Set Transport Protocol*** .
- Set the SYS's IP address before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

3.1 Login

You can access and configure the platform via web browser directly, without installing any client on your computer.

Steps

Note

- If failed password attempt of current user is detected, you are required to input the verification code. The failed password attempts from current client, other client, and other address will all require the verification code.
- The failed password attempt and verification code attempt from current client and other address will all be accumulated. Your IP address will be locked for a specified period of time after specific number of failed password or verification code attempts detected.
- The account will be frozen for 30 minutes after 5 failed password attempts. The failed password attempts from current client and other addresses will all be accumulated. When the account is frozen after accumulated failed password attempts, you can still try login on another PC.
- The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required strength, you will be asked to change your password.
- If your password is expired, you will be asked to change your password when login.

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key to open the login page.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   - The Web Client transmits data via the HTTPS, using our self-developed HTTPS certificate, which is not issued by the Certificate Authority. So that a risk prompt will show when you

opening the Web Client. To avoid the prompt, you can apply for a certificate from the Certificate Authority.

- The login session of the Web Client will expire and a prompt with countdown will appear after the configured time period in which there is no action. For setting the time period, refer to ***Set Basic Security Parameters*** .

2. (For Administrator to login Web Client) On the login page, select the **Management** tab.
3. For first-time login for admin user:
   1) Enter a password and confirm the password for the admin user in the pop-up Create Password window, click **Next**, and select a method for password reset verification.

      Email

      Click **Verification Code → Next** and set the email address for receiving the password reset verification code.

      Security Question

      Click **Security Question → Next** , select security question(s) from the drop-down lists, and enter your answers accordingly.

   2) Click **Finish**.

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.

   The Home page of the Web Client will show.
4. For first-time login for normal users, or users whose passwords were reset:
   1) Enter the user name and password, and click **Log In**.

      You can contact the Administrator for the user name and initial password.

      The Change Password window shows.

   2) Set a new password and confirm the password.

   The Home page of the Web Client will show.
5. For all users (except employees, non-first time) Enter the user name and password, and click **Log In**.

   The Home page of the Web Client will show.

3.2 Home Page Overview

The default Home page of the Web Client provides a statistics overview of different application and configuration data.

Top Navigation Bar

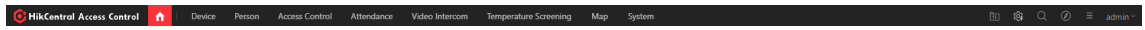


Figure 3-1 Top Navigation Bar of the Web Client

Home Page Icon

Click to enter the Home Page.

Module names beside shows the available modules. You can click to refresh data on the current page of the functionality module.

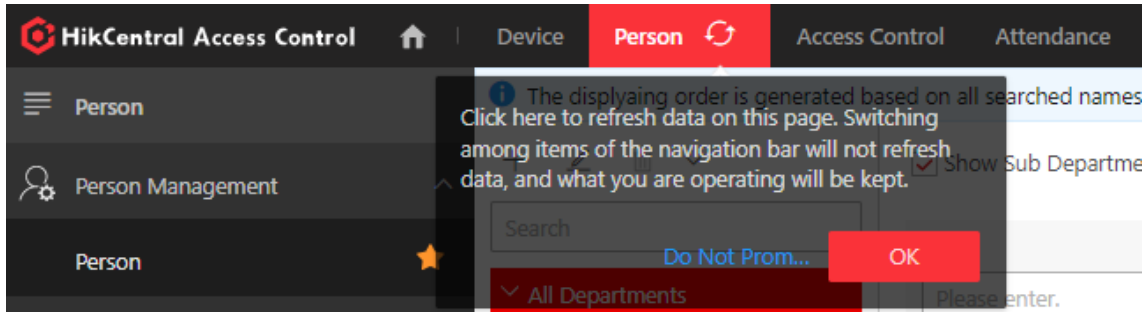


Figure 3-2 Refresh Module on Navigation Bar

Download Center

You can view all of the downloading tasks and completed tasks on the platform. You can start or stop downloading task(s), delete downloading and downloaded task(s). Click **Custom Download Location** on the top right and select a saving path in the PC, and the files will be automatically downloaded in the selected file folder.

Common Functions

Quickly find and use frequently-used functions of the System, Access Control, and Attendance modules.

Quick Function Search

Enter a keyword of a function and go to its page quickly.

Help Center

Access Control

A wizard which guides you through the basic configurations of Access Control. You can also view the flow chart which introduces the configurations and operations of access control in ***Flow Chart of Door Access Control*** .

Attendance

A wizard which guides you through the management and configurations of Attendance. You can also view the flow chart which introduces the management of devices, departments, and persons, basic attendance configuration, attendance rule configuration, and record search and handling in ***Flow Chart of Time and Attendance*** .

Web Client User Manual

A wizard which guides you through the user manual of Web Client.

Maintenance and Management

Back Up and Restore System Data

You can manually back up the data in the system, or configure a schedule to run the backup task regularly.

When an exception occurs, you can restore the database if you have backed up the database.

For more details, refer to ***Set System Data Backup*** and ***Restore System Data*** .

Export Configuration Data

You can export and save configuration data to your local PC.

For more details, refer to ***Export Configuration Data*** .

Download the Web Control

For accessing the Web Client via web browser, you must install a web control on the PC on which you access the Web Client when performing some functions. Web Client automatically asks you to install the web control when you want to access the corresponding functions, and you can follow the prompts to install it on the PC. Click **Web Control** to start downloading the web control, or click to view its details and download it.

About

Check the version information of the Web Client and the system ID.

Account

Change Password

Change the password of the current user.

For more details, refer to ***Change Password of Current User*** .

Logout

Log out of the system and back to the login page.

Quick Configuration

On the top right of Home Page, you can click **Expand Quick Configuration** to enter the management and configurations of Access Control or Attendance.

Quick Start

This section displays the quick start of menu items, which have been added to Favorites on the left of each module.

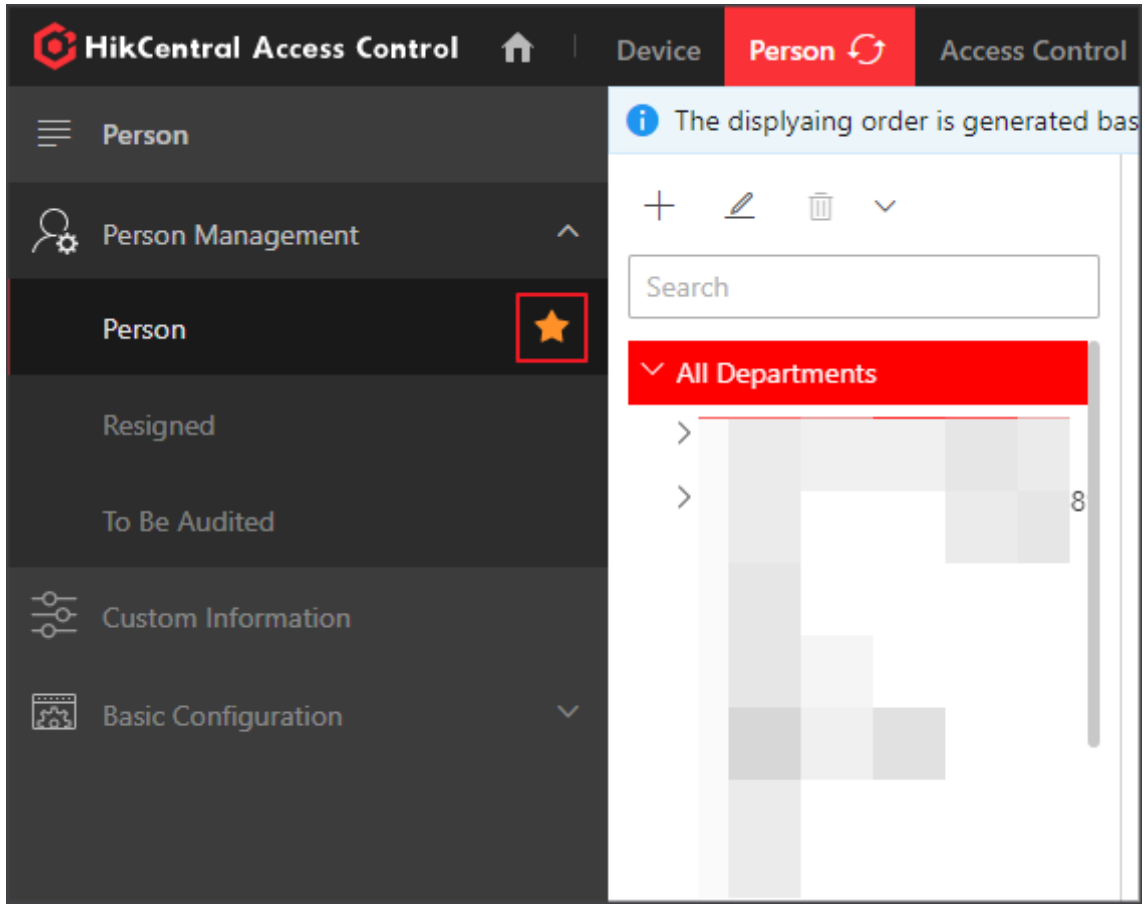


Figure 3-3 Add Menu Item to Favorites for Quick Start

You can drag the menu item to adjust the order, or click to remove the menu item from quick start.

Device Status

This section displays the device status, including the numbers of normal or exceptions devices, including total devices, access control device or video intercom device.
You can click to refresh to view the real-time status of results.

Attendance Report

This section displays attendance report of total persons in pie chart.

- You can select the time period (such as today, last week, and last 3 months) and departments to view the corresponding attendance report.
- You can click to export the attendance report in the format of PDF, PNG, or JPG.
- You can click to refresh to view the real-time status of results.

Attendance Status Statistics

This section displays the statistics of attendance status in line chart.

- You can select the time period (such as today, last week, and last 3 months) and departments to view the corresponding attendance status statistics.
- You can click to export the attendance status statistics in the format of PDF, PNG, or JPG.
- You can click to refresh to view the real-time status of results.

Alarm / Access Control Event

This section displays alarms and access control events

- Select **Alarm** tab.
  - Click › to view the alarm details. You can also acknowledge or unlock the alarm.
  - Click , enable the **Alarm Ringtone**, and select a default ringtone or custom ringtone. You can also check the **Real-Time Pop-Up Box When Alarm Occurs**.
- Select **Access Control Event** tab. You can click **Mark All As Read** to mark all messages as read.
- Click **View All** to view more alarms or events.

Pending Task

This section displays the pending task list, including the employees' attendance applications to be handled. Click **Handle** to approve/reject/undo the application. Click **View All** to view more attendance applications.

Person Credential Status

This section displays the person credential status, including the numbers of configured or not configured persons, cards, fingerprints, face pictures, and irises.
You can click to refresh to view the real-time status of results.

Overall Work Hours / Overtime

This section displays the overall work hours and overtime statistics in line chart.

- You can select the time period (such as today, last week, and last 3 months) and departments to view the corresponding statistics.
- You can click to export the attendance status statistics in the format of PDF, PNG, or JPG.
- You can click to refresh to view the real-time status of results.

3.3 Download Mobile Client

On the login page of Web Client, you can scan the QR code at the bottom to download the Mobile Client, or install it in the APP Store.

Scan the corresponding QR code on the Login page with your mobile terminal to download the Mobile Client.

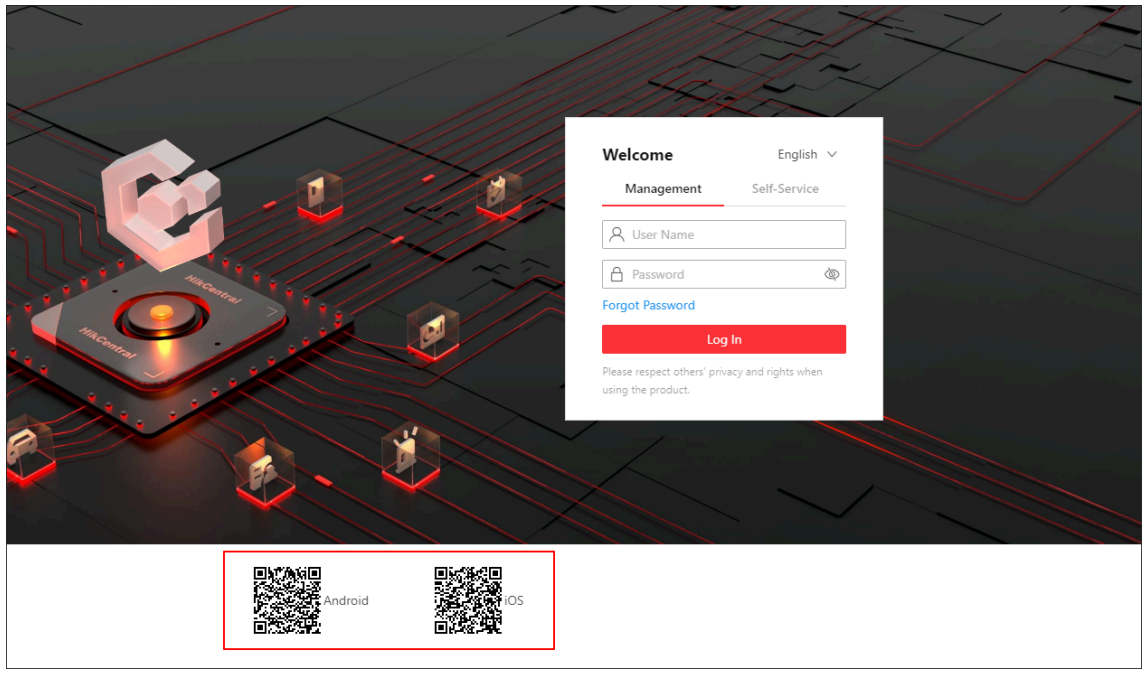


Figure 3-4 QR Code for Downloading Mobile Client

Chapter 4 Device and Server Management

On the top, select **Device → Device and Server** to enter the Device and Server Module.

4.1 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. Such initial configuration is required in order to be able to connect the devices to the platform via network.
- To add devices via ISUP or ONVIF, you need to go to → **Basic Management → System → Network → Device Access Protocol** , and enable **Allow ISUP Registration** or check **Access via ONVIF Protocol**.
- For accessing the Web Client via web browser, you must install a web control on the PC on which you access the Web Client when performing some functions. Web Client automatically asks you to install the web control when you want to access the corresponding functions, and you can follow the prompts to install it on the PC.

  You can also go to the top navigation bar, and click **Maintenance and Management → Web Control** to start downloading the web control, or click to view its details and download it.

4.2 Add Device(s)

This chapter introduces how to add online devices, add device manually, and batch import devices and explains parameters on Add Device pages.

4.2.1 Adding Modes Supported by Different Devices

You can

Add Online Devices

Table 4-1 Add Online Devices

Scenario	Description	Supported Device Types
The devices are on the same network as the Web Client.	1. In the Online Device area, select a network type. **Server Network** As the default selection, the detected online	• Access Control Device • Video Intercom Device

Scenario	Description	Supported Device Types
	devices in the same local subnet with the SYS server will be listed in the Online Device area. **Local Network** The detected online devices in the same local subnet with the Web Client will be listed in the Online Device area. 2. In the Online Device area, select **Hikvision Private Protocol**/ **Hikvision ISUP Protocol** to filter the detected online devices. **Note** Select **Hikvision Private Protocol** / **Hikvision ISUP Protocol** to add a Hikvision device. 3. In the Online Device area, select the active device(s) to be added, and click **Add to Device List** to open the Add Online Device window.	

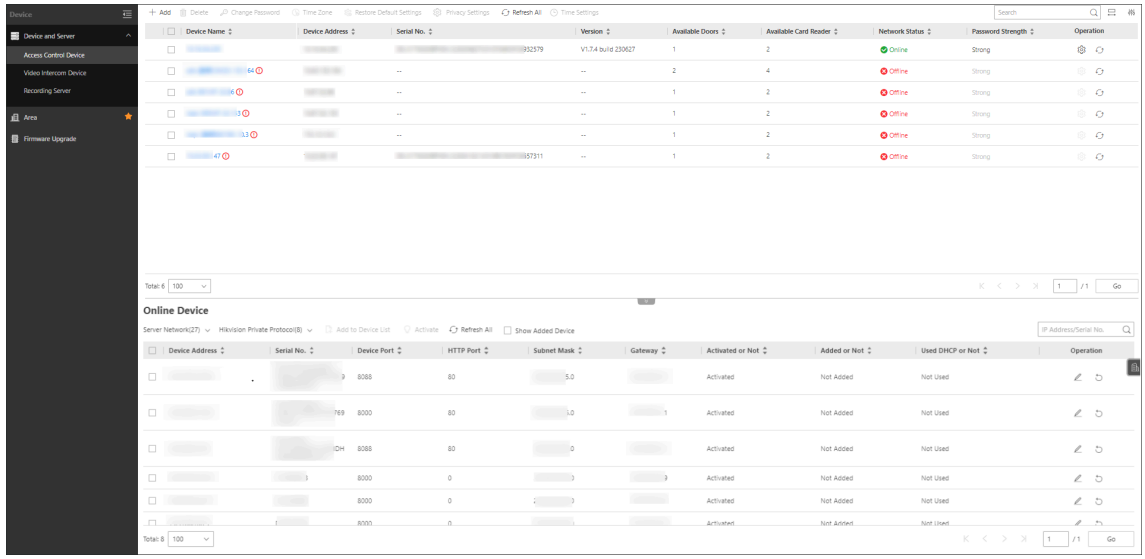


Figure 4-1 Online Device

Add Devices Manually

On the left, select the type of device, and then click **Add** on the top.

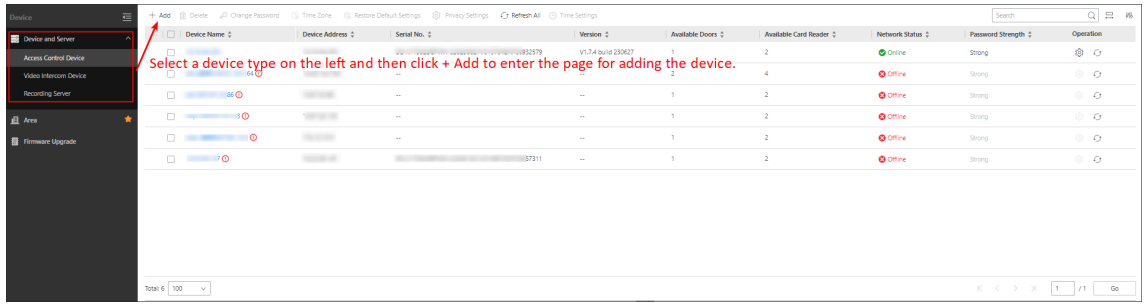


Figure 4-2 Entry for Adding Device

Table 4-2 Add Devices Manually

Adding Mode	Scenario	Description	Supported Device Types
Add device by IP address / domain	When you know the IP address or domain name of a device, you can add it to the platform by specifying the IP address (or	Select **Hikvision Private Protocol /** as the Access Protocol, and select **IP Address/ Domain**.	• Access Control Device • Video Intercom Device

Adding Mode	Scenario	Description	Supported Device Types
	domain name), user name, password, etc.		
Add devices by IP segment	When multiple devices to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some other related parameters.	Select **Hikvision Private Protocol /** as the Access Protocol, and select **IP Segment** as the adding mode.	• Access Control Device
Add device by device ID	For the devices supporting ISUP, you can add them by specifying a predefined device ID, key, etc.	Select **Hikvision ISUP Protocol** as the Access Protocol, and select **Device ID** as the adding mode.	• Access Control Device
Add devices by device ID segment	If you need to add multiple devices which have no fixed IP addresses and support ISUP to the platform, you can add them at a time after configuring device ID segment for the devices	Select **Hikvision ISUP Protocol** as the Access Protocol, and select **Device ID Segment** as the adding mode.	• Access Control Device

Batch Import Devices

Table 4-3 Batch Import Devices

Scenario	Description	Supported Device Types
When there are multiple devices to be added, you can edit the predefined template containing the required device information, and import the	1. Select an access protocol. 2. Click **Download Template** and save the predefined template (excel file) on your PC.	• Access Control Device • Video Intercom Device

Scenario	Description	Supported Device Types
template to the platform to add devices in a batch.	3. Open the exported template file and enter the required information of the devices to be added in the corresponding column. 4. Click and select the edited file.	

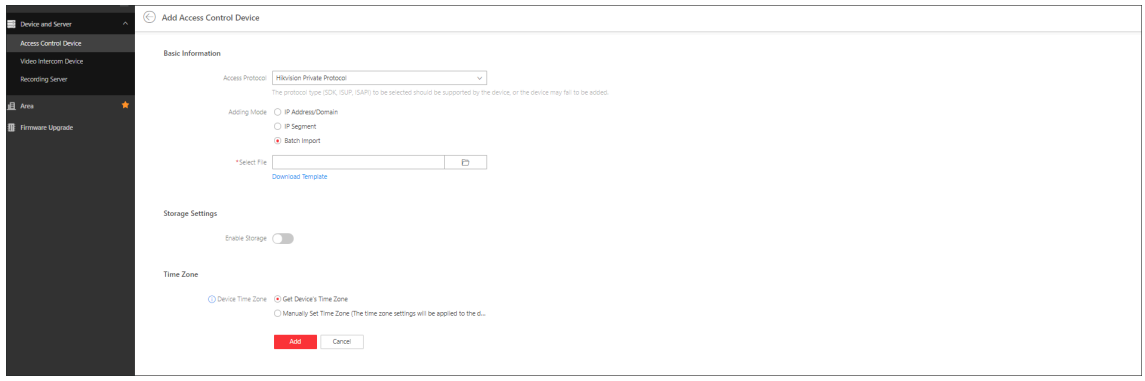


Figure 4-3 Batch Import Devices

4.2.2 Parameters on Add Device Pages

This chapter introduces parameters for adding devices.

Note

Parameters may vary by different access protocols.

Basic Information

Device Address / Start and End IP Address

The IP address of the device. For online devices, the address is shown automatically. For other modes, you should enter them manually.

Add by Encryption

If you add the device via this method, the SDK service port should be encrypted.

Device Port

The port number of the device, which is shown automatically. The default port number is 8000.

Picture Storage

If it is checked, the captured pictures will be automatically saved to the storage location you configured in picture storage settings for the access points.

Note

For details about configuring picture storage settings, see ***Edit Element in Area*** .

Time Zone

Click **Get Device's Time Zone** to get the device's time zone, or click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list..

Resource Information

Add Resource to Area

Import the resources of the added device(s) to an existing area or a new area.

If you do not import resources to an area, you cannot perform further operations.

4.3 Add Server(s)

This chapter introduces parameters on adding pages of different servers.

On the left, select a server type, and then click **Add** on the top.

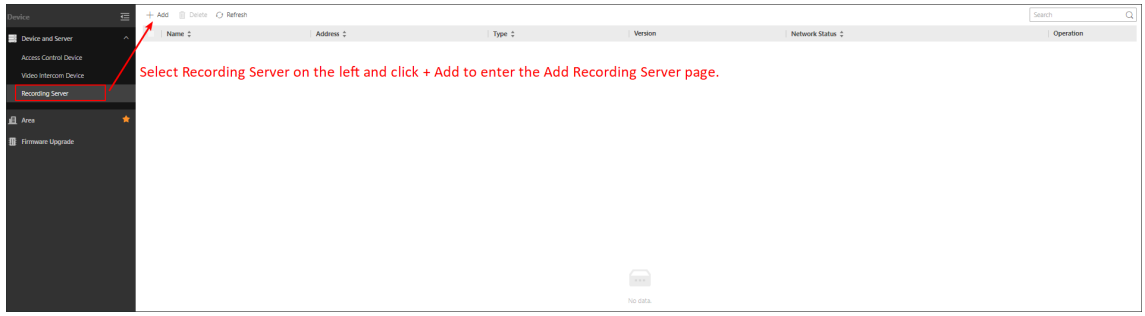


Figure 4-4 Entry for Adding Server(s)

Parameters on Add Recording Server Page

Note

The parameters vary by different types of recording server.

Address

The pStor server's IP address in LAN that can communicate with SYS.

ANR Function

You can check this field to enable the ANR function. This function is enabled default. If the network is disconnected between the pStor and the device, data can be stored on the pStor automatically.

Control Port

The control port No. of the pStor server. If it is not changed, use the default value.

Network Port

The network port No. of the pStor server. If it is not changed, use the default value.

Signaling Gateway Port

The signaling gateway port No. of the pStor server. If it is not changed, use the default value.

Enable Picture Storage

Switch on it for storing pictures in this server.

Access Secret Key and Secret Key

Enter the user's access secret key and secret key of the pStor server for downloading pictures.

For pStor servers and cluster storage servers, you can download these two keys on the pStor server's Web Client page, or contact our technical support.

4.4 After Adding Devices/Servers: Operations on Device List Page

After adding devices, you can perform further operations on the device list.

Table 4-4 Operations Supported on Added Device List

Operations	Descriptions
Edit a Device/Server	Click a device/server's name to enter the editing page.
Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online Hikvision devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Replace Device	When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform.

Operations	Descriptions
	In the **Operation** column, click to replace the old device with the new device on the platform.
Set Time Zone	Select one or more device(s), click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. To restore all the device parameters, check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Privacy Settings	To protect the person's private information including the person's name and profile picture, you can configure privacy settings for online access control devices.
Search for Device/Server(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search for the target device/server(s).
Delete Device/Server	Check device/server(s) in the list, and click **Delete** to delete the selected server(s).

4.4.1 Configure Parameters for Access Control Devices

You can configure parameters for access control devices, including device time, linkage settings (linked device actions), maintenance settings, etc.

On the left, select **Access Control Device**, and click in the Operation column to enter the configuration page of a device.

Configure device parameters according to the following topics.

Note

- Device support required. Parameters vary with different device types and models.
- The supported features and parameters are subject to the applications you installed.

Time

You can view the time zone where the device locates and set the following parameters.

Device Time

Click the **Device Time** field to customize time for the device.

Sync with Server Time

Synchronize the device time with the server of the platform.

Biometrics

You can enable facial recognition and fingerprint recognition of access control devices if the devices support biometrics recognition.

Facial Recognition

Set facial recognition function for the device, and select a facial recognition mode.

Single-Person Recognition

The device can recognize one person at a time.

Multiple-Person Recognition

The device can recognize multiple persons at a time.

Fingerprint Recognition

Set persons' fingerprint recognition for the device. Once enabled, the device can recognize persons by their fingerprints.

Skin-surface Temperature

Set **Temperature Measurement** to on to enable temperature screening function.

Threshold(℃)

Set the range of normal skin-surface temperature. The detected temperature that is not in this range is abnormal temperature. The maximum temperature should be higher than the minimum temperature.

Open Door When Temperature is Abnormal

If it is enabled, the door will open when person's skin-surface temperature is abnormal. By default, the door will not open for abnormal temperature.

Registration Device

If you enable this function, the information about added persons and credentials (including face pictures and fingerprints) added on the device will be automatically synchronized to the platform.

Mask Settings

Set **Mask Detection** to on to enable mask detection function. Once enabled, the device can detect persons without face masks.

Do Not Open Barrier when No Mask

If it is checked, the barrier will still open for persons without masks.

RS-485

RS-485 Communication Redundancy

You can check **RS-485 Communication Redundancy** to enable the function if you wire the RS-485 card to the device redundantly.

Working Mode

Select the working mode, including the card reader, door control unit, and access control host.

Turnstile Parameters

You can configure passing mode for the turnstile linked to the device.

Based on Lane Controller's DIP Mode

The device will follow the lane controller's DIP settings to control the turnstile. The settings on the main controller will be invalid.

Based on Main Controller's Settings

The device will follow the settings of main controller to control the turnstile. The DIP settings of the lane controller will be invalid.

Maintenance

You can reboot a device remotely and restore it to its default settings.

Reboot

Reboot the device.

Restore Default Settings

Restore the device to its default settings. The device needs to be activated after being restored.

Facial Recognition Mode

You can check **Deep Mode** to enable the function. Once enabled, all the face credentials applied to the device will be cleared. Go to **Access Control → Access Level** and click to apply the data in the platform to the device.

More

You can click **Configure** to open the remote configuration page of the device and configure more parameters. For details, refer to the user manual of the device.

Custom Wiegand Parameters

Based on the knowledge of uploading rule for the third-party Wiegand, you can configure Wiegand parameters to communicate between the device and the third-party card readers.

Note

- By default, the device disables the custom Wiegand function. If you enable the custom Wiegand function, all Wiegand ports in the device will use the customized Wiegand protocol.
- You can configure up to 5 custom Wiegand devices.

Switch on **Custom Wiegand** and configure the Wiegand parameters. You can select a device from the **Copy From** drop-down list to copy the settings of another device.

Total Length

Wiegand data length.

Parity Type

Set the valid parity for Wiegand data according to property of the third party card reader. You can select **Nothing**, **Odd Even Check**, or **XOR Parity**.

If you select **Odd Even Check**, you can configure the following:

Odd Start, Length

If the odd parity start bit is 1 and the length is 12, then the platform will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0 (Bit 0 is the first bit).

Even Start, Length

If the even parity start bit is 12, and the length is 12, then the platform will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

If you select **XOR Parity**, you can configure the following:

XOR Parity Start Bit, Length per Group, Length for Parity

Depending on the table displayed below, the start bit is 0, the length per group is 4, and the length for parity is 40. It means that the platform will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits (The result length is the same as the length per group).

Output Rule

Set the output rule.

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed below, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed below, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

Note

Take Wiegand 44 for example, the setting values in the Custom Wiegand are as follows:

Custom Wiegand Name	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Type	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Set Wiegand Parameters

You can set Wiegand parameters for access control devices to facilitate communications between card readers and access control devices.

Select a Wiegand protocol in the list, and click in the Operation column to pop up a window of Wiegand information. On the pop-up window, set Wiegand parameters and click **OK**.

Direction

Whether the device is used for inputting (receiving) or outputting (sending) data.

Check **Input** or **Output**.

Wiegand Mode

The signal transmitting mode. Whether the device transmits 26-bit, 34-bit, 27-bit, and 35-bit data.

Note

Wiegand mode can only be selected when the direction is **Output**.

Output Format

Whether to output the signal as employee No. or card No.

Note

Output format can only be selected when the direction is output.

Signal Sending Interval

The interval of sending data.

Linked Card Reader

The card reader No. to be linked.

Note

Linked card reader can only be selected when the device supports linking to a card reader.

Configure Device Actions

You can set the linkage actions of an access control device for different event sources, so that when the device detects a linkage source, the device can execute actions such as triggering alarm output, triggering buzzer, locking/unlocking access point, etc.

Click **Add** in the Linkage section. Set the event source, and then configure parameters of the linkage target.

Buzzing

Buzzer on Controller

ON

Turn on the buzzer on the access controller when the specified event is triggered.

OFF

Turn off the buzzer on the access controller when the specified event is triggered.

No Linkage

Disable the linkage action.

Buzzer on Reader

ON

Turn on the buzzer on the card reader when the specified event is triggered.

OFF

Turn off the buzzer on the card reader when the specified event is triggered.

No Linkage

Disable the linkage action.

Alarm Output

ON

Trigger the alarm output when the specified event is triggered.

OFF

Stop the alarm output when the specified event is triggered.

No Linkage

Disable the linkage action.

Zone

ON

Arm the zone when the specified event is triggered.

OFF

Disarm the zone when the specified event is triggered.

No Linkage

Disable the linkage action.

Access Point

Unlock

Unlock the door or barrier when the specified event is triggered.

Lock

Lock the door or barrier when the specified event is triggered.

Remain Unlocked

The door or barrier will remain unlocked when the specified event is triggered.

Remain Locked

The door or barrier will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

Card Swiping Parameters

You can configure card swiping parameters to allow authentication by entering card number on keypad, enable NFC clone card, enable M1 encryption, etc.

In Card Swiping section, configure card swiping parameters.

Reader Communication Protocol

Select the reader communication protocol.

Input Card Number On Keypad

If it is checked, users can enter card number on keypad for authentication.

Enable NFC Card

If it is enabled, users can use cloned cards for authentication.

M1 Encryption

If it is enabled, only the card with the same encrypted sector can be granted access, and you need to choose an encrypted sector.

Voice Prompt

If it is enabled, an audio prompt will be played when swiping cards.

Upload Picture after Linked Capture

Upload the pictures captured by devices to the platform automatically.

Picture Storage

If it is checked, the captured pictures will be automatically saved to the storage location you configured in picture storage settings for the access points.

Picture Size

Select a picture size from the drop-down list for the captured pictures saved to the storage location.

Picture Quality

Select a picture quality from the drop-down list for the captured pictures saved to the storage location.

Capture Times

Select the capture times from the drop-down list for the devices to capture face pictures for the times selected.

4.4.2 Upgrade Device Firmware

You can upgrade the devices with the firmware to be upgraded according to device type and upgrade mode.

Select **Firmware Upgrade** on the left navigation pane.

Select Device for Upgrade

You should first select the target device type for upgrade.

The following table shows devices types and their firmware upgrading methods accordingly.

Via Current Web Client	Via Hik-Connect
• Access Control Device • Card Reader • Indoor Station • Door Station	• Indoor Station • Door Station

Via Current Web Client	Via Hik-Connect
Note Upgrading the card reader linked to the door station is not supported. • Main Station	**Note** Upgrading the card reader linked to the door station is not supported. • Main Station

Select Upgrade Mode and Schedule

The upgrade mode is provided by the platform after you select the device, including via the current Web Client, via Hik-Connect (which is a cloud service), and via FTP.

Upgrade Method	Steps
Upgrade Device Firmware via Current Web Client	1. Select **Via Current Web Client**. 2. In the **Upgrade By** field, select the upgrade method. 3. In the **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade. 4. Select device(s). 5. Select an upgrade package from the local PC. 6. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.
Upgrade Device Firmware via Hik-Connect	1. Select **Via Hik-Connect**. 2. In the **Device Access Protocol** field, select the relevant protocol. 3. In the **Upgrade By** field, select the upgrade method. **Note** This field is not required if Hik-Partner Pro Protocol is selected as the device access protocol. 4. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade. 5. Install the required web plug-in. **Note** If you select Local PC as the upgrade method, you should install the required web plug-in if the prompt pops up.

Upgrade Method	Steps
	6. Select device(s). 7. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.
Upgrade Device Firmware via FTP	1. Select **Upgrade Firmware via FTP**. 2. Set the basic information. **FTP Server Address** The address of FTP server, where you have uploaded the firmware upgrade package. **Port No.** The port number of FTP server. **User Name** The user name of FTP server. **Password** The password of the FTP server. **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. **Path** If you save FTP firmware upgrade package in a non-root directory, enter the root directory name. If you saved FTP firmware upgrade package in a root directory, keep the field empty. 3. Select a device type and select a device from the device list.

Upgrade Method	Steps
	4. Select an upgrade package from the local PC. 5. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.

Note

In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

To view the devices with firmware upgraded, upgrading, to be upgraded, and not upgraded, you can click in the Upgrade Status column. In the upgrade task list, you can click in the Operation column to delete the upgrade task.

4.4.3 Create Password for Inactive Device(s)

The devices with simple default password may be accessed by the unauthorized user easily. For the security purpose, the default password is not provided for some devices. You are required to create the password to activate them before adding them to the platform. Besides activating the device one by one, you can also batch activate multiple devices which have the same password simultaneously.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Access Control via network.
- This function should be supported by the device. Make sure the devices you want to activate support this function.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, view the device status and select one or multiple inactive devices.
3. Click **Activate** to open the device activation window.
4. Create a password in the password field, 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.

5. Click **Save** to create the password for the device.

Note

If you have not set security questions, the window of setting security questions will pop up, and you should select the method of resetting password and set the security questions as needed.

An **Operation completed.** message is displayed when the password is set successfully.

6. Click in the Operation column to change the device's IP address, subnet mask, gateway, and so on if needed.

Note

For details, refer to ***Edit Online Device's Network Information*** .

4.4.4 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with SYS or Web Client, can be detected by HikCentral Access Control. For the detected online devices, you can edit their network information as desired via HikCentral Access Control remotely and conveniently. For example, you can change the device IP address due to the changes of the network.

Before You Start

For some devices, you should activate it before editing its network information. Refer to ***Create Password for Inactive Device(s)*** for details.

Perform this task when you need to edit the network information for the detected online devices.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS will be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
3. View the device status, and click in the Operation column of an active device.
4. Edit the device parameters, such as IP address, device port, subnet mask, and gateway.

Note

The parameters may vary for different device types.

5. Click .
6. Enter the device's password.
7. Click **Save**.

4.4.5 Restore/Reset Device Password

If you forgot the password of the detected online devices, you can restore the device's default password or reset the device's password through the system. Then you can access the device or add it to the system using the password.

Restore Device's Default Password

For some devices with old firmware version, if you forgot the password you use to access the online device, you can restore the device's default password through the platform and then you must change the default password to a stronger one for better security.
In the Online Device area, view the device status (shown on Security column) and click in the Operation column of an active device. Enter the security code in the pop-up window and restore the default password of the selected device.

Note

Contact our technical support to obtain a security code.

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.

Reset Device Password

If you forget the password you use to access the online device, you can request for a key file from the technical support and reset the device's password through the platform.

1. In the Online Device area, view the device status (shown on Security column) and click icon in the Operation column of an active device. The Reset Password window pops up.

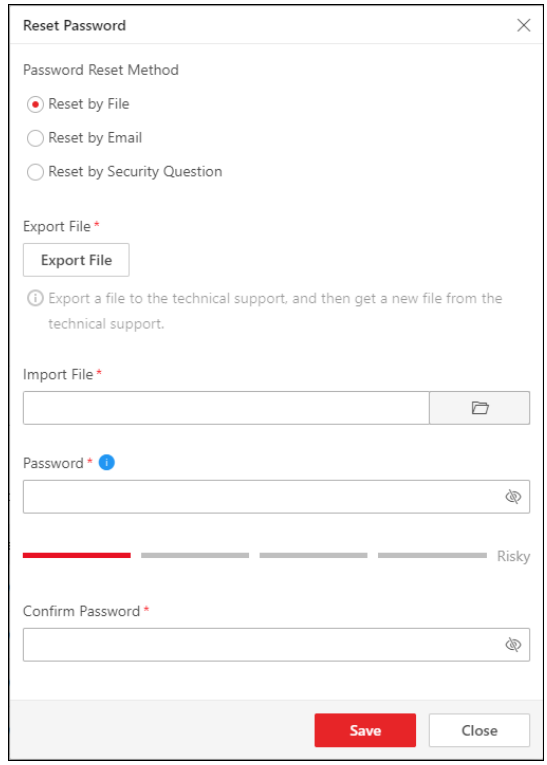


Figure 4-5 Reset Password

2. Select a password reset method and save the settings.
   - **Reset by File:** Click **Export File** to save the device file on your PC. Send the file to the technical support.

     Note

     For the following operations about resetting the password, contact the technical support.
   - **Reset by Email:** Export the QR code and sent it to the email displayed. You will receive the verification code in 5 minutes. Enter the code, new password, and confirm password.
   - **Reset by Security Question:** Enter the answer to the security question, new password, and confirm password.

     Note

     If you have not set security questions, the window of setting security questions will pop up, and you should set the security questions as needed.

     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.

Chapter 5 Area Management

HikCentral Access Control provides areas to manage the added resources in different groups. You can group the resources into different areas according to the resources' locations. For example, in a house, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named My House) for convenient management. You can do some other operations of the devices after managing the resources by areas.

In the top left corner of Home page, select → **Basic Management** → **Device** , and click **Area** on the left.

5.1 Add an Area Manually

You should add an area before managing the elements by areas.

Click + on the area list panel to open the Add Area panel, select a parent area to add a sub area, and create a name for the area.

After adding the area, you can perform the following operations on the area list.

Operation	Description
Edit Area	Hover the cursor on ··· and click **Edit** to edit the area.
Export Device Information in Area	Hover the cursor on ··· and click **Export Device Information in Area** to export all devices that you have permission to access in the current area.
Delete Area	Select an area and click 🗑 or hover the cursor on ··· and click **Delete** to delete the selected area. You can also press **Ctrl** on your keyboard, select multiple areas, and then click 🗑 to delete areas in a batch. After deleting the area, the resources in the area will be removed from the area.
Move Area	Drag the added area to another parent area as the sub area.
Stick on Top	Hover the cursor on ··· and click **Stick on Top** / **Cancel Stick Area On Top** to stick the area / cancel sticking the area to the top. **Note** The order of the parent area cannot be changed.

Operation	Description
Import/Export Areas	Click to import areas with predefined template file; click to export all areas to local PC.
Customize Additional Information	In the area list panel on the left, click to enter the Customize Additional Information page. Click **Add**, set the name and type, and click **Add** to customize the additional area information.

5.2 Import Areas in a Batch

You can batch add areas via importing a predefined template file.

Click . In the pop-up pane, click **Download Template** and enter the area related information in the downloaded template.

Area

Rule

1. Fields marked with asterisk (*) are required.
2. Please enter the area to be imported in Area Name and its upper-level area path in Area Path.
3. Area name: Required. 1 to 64 characters allowed. Special characters such as '/\:*?"<>| cannot be entered.
4. Area path: If the path is left blank, the area will be added to the root area by default.

Example

Area Name*	Area Path
Area 1	
Area 2	First-Level Area
Area 3	First-Level Area > Second-Level Area
Area 4	First-Level Area > Second-Level Area > Third-Level Area
Area 5	First-Level Area > Second-Level Area > Third-Level Area > Fourth-Level Area

Data Details

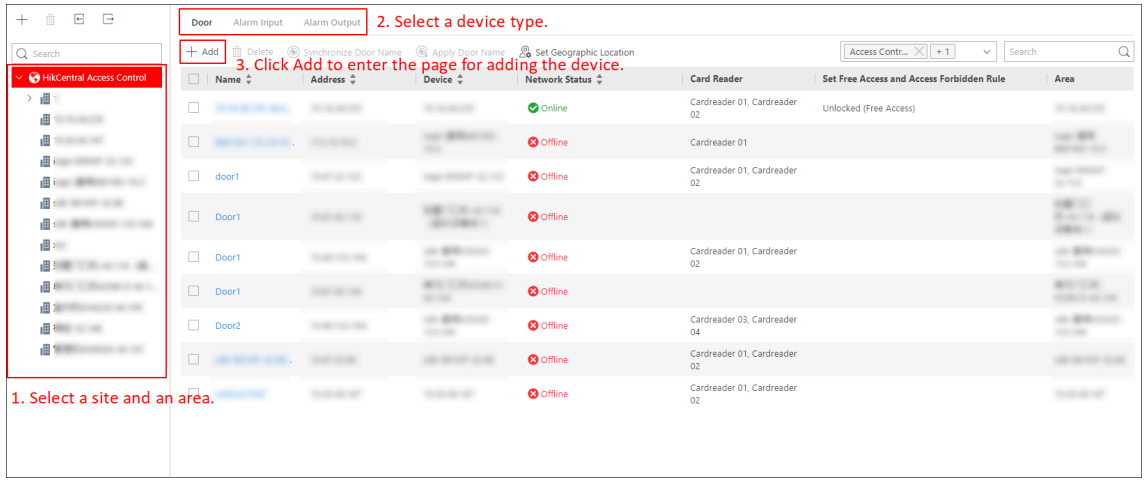
Area Name*	Area Path

Figure 5-1 Downloaded Template

5.3 Add Element to Area

Add Devices to Area

Select a site and an area on the left, select a device type on the top, and click **Add**.



Note

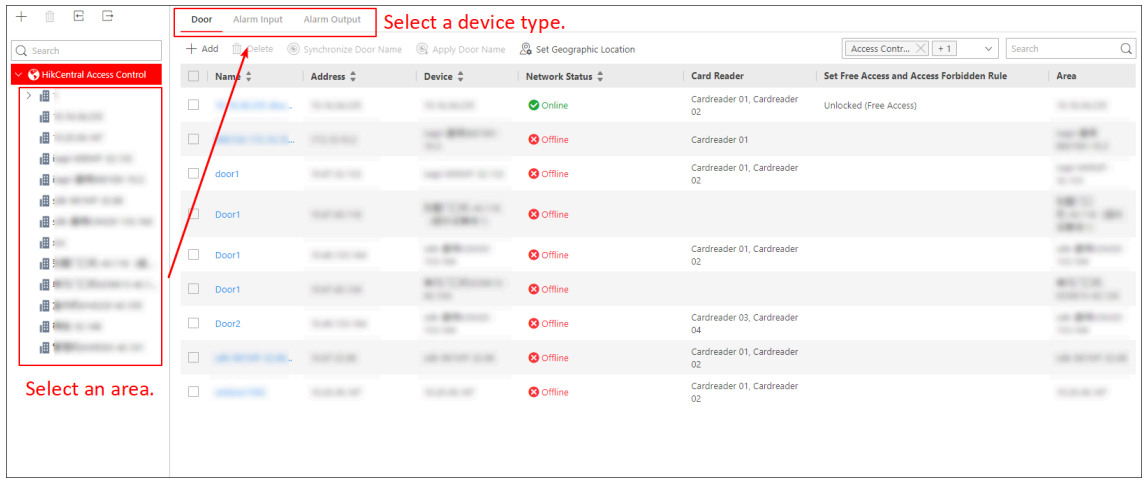
- For alarm output, when the alarm or event linked with the alarm output is detected, alarm devices (e.g., the siren, alarm lamp, etc.) connected with the alarm output will make actions. For example, when receiving the alarm out signal from the system, the alarm lamp will flash.

Figure 5-2 Entry for Adding Element

5.4 Edit Element in Area

You can edit the area's added elements, such as event settings, and map settings, application settings, hardware settings, and attendance settings for doors, and so on.

Select an area on the left and a device type on the top.



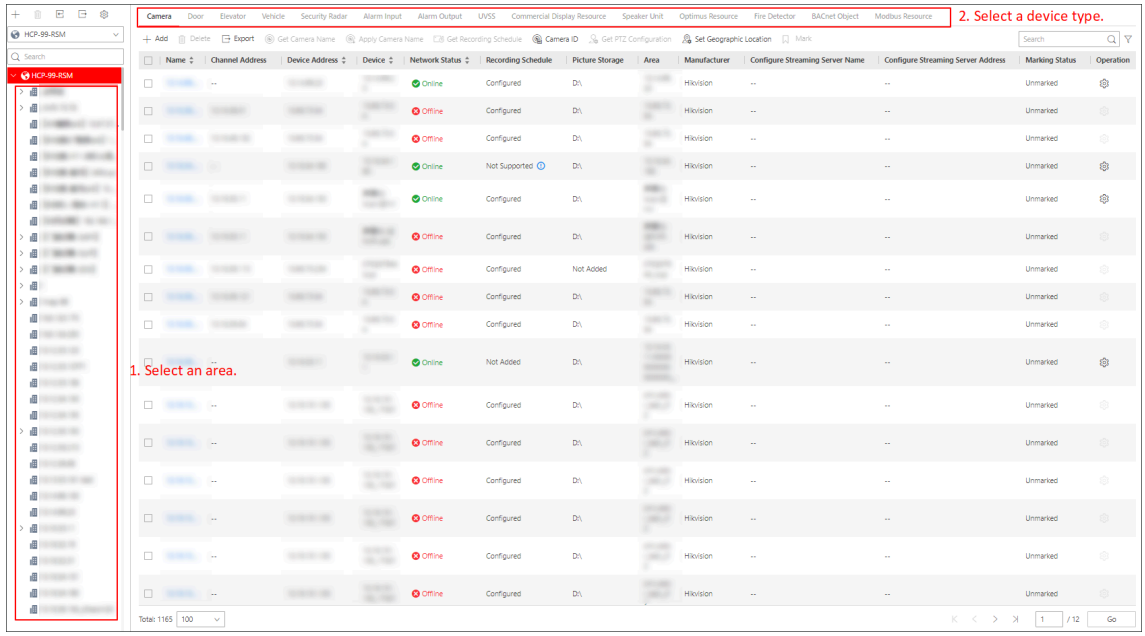


Figure 5-3 Select Area and Device Type

5.4.1 Parameters on Edit Door Page

Basic Information

Name

Edit the name for the door.

Note

If you change the name, you can click in the door list page to apply the new name to the device.

Door Contact

The door contact's connection mode.

Exit Button Type

The exit button connection mode.

Lock Door when Door Closed

If it is enabled, the door will be locked once the door magnetic is closed. If there is no door magnetic, the door will be locked after the extended open duration ends.

Note

This function should be supported by the device.

Open Duration

The time interval between the door is unlocked and locked again.

Extended Open Duration

The time interval between the door is unlocked and locked again for the person whose extended access function is enabled.

Door Open Timeout Alarm

After enabled, if the door has been configured with the event or alarm, when the door contact open duration has reached the limit, the event or alarm will be uploaded to the system.

Duress Code

If you enter this code on the card reader keypad, the Mobile Client will receive a duress event. It should be different from the super password and dismiss code.

Super Password

If you enter this password on the card reader keypad, you are exempted from all the remaining locked (Credential Failed), anti-passback, and first card authorization restrictions. It should be different from the duress code and dismiss code.

Dismiss Code

If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different from the duress code and supper password.

Picture Storage

Switch on and select a storage location from the drop-down list.

Note

If an error occurs during picture storage configuration, appears on the right of the door name.

Card Reader

Min. Card Swipe Interval

After it is enabled, you cannot swipe the same card again within the minimum card swiping interval.

Reset Entry on Keypad After(s)

Set the maximum time interval of pressing two keys on the keypad. If timed out, the first entry will be reset.

Failed Card Attempts Alarm

After it is enabled, if the door is configured with event or alarm, when the number of excessive failed card swiping attempts has reached the limit, the event or alarm will be uploaded to the system.

Tampering Detection

After it is enabled, if the door is configured with device tampered event or alarm, when the device body or panel is taken apart, the alarm will be triggered and sent to the system.

OK LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for OK core wire connection on the card reader mainboard.

Error LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for ERR core wire connection on the card reader mainboard.

Face 1:N Matching Threshold

Set the threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate. The maximum value is 100.

Face Recognition Interval

The time interval between continuous face recognition twice when authenticating.

Face Anti-spoofing

If it is enabled, the device can recognize the live face. Also, you can check **Protect Sensitivity of Face Anti-Proofing**, and set the face anti-spoofing security level.

Face Recognition Application Mode

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

Face Recognition Terminal

For a turnstile or an access controller of certain types, switch on **Face Recognition Terminal** and add face recognition terminals to link with the selected turnstile.

Copy To

Click **Copy To** in the upper right corner to apply the current settings of the door to other door(s).

5.4.2 Edit Alarm Input/Output in an Area

You can click an alarm input/output name in the **Name** column to enter the Edit Alarm Input page and edit the alarm input/output name.

5.5 Remove Element from Area

Select a device type tab to show the added elements. Then select the elements below and click to remove the elements from the area..

Chapter 6 Person Management

You can add person information to the platform for further operations such as access control (linking a person to an access level), time and attendance (assign a schedule to a person), etc. After adding the persons, you can edit and delete the person information if needed.

On the top, select **Person** to enter the Person module.

6.1 Add Departments

When there are a large number of persons managed in the platform, you can put the persons into different departments. For example, you can group employees of a company to different departments.

Steps

1. Select **Person Management → Person** on the left navigation bar of Person module.
2. Click + at the top of the department list to enter the Add Department page.
3. Set the department information, including the parent department, department name, and description.

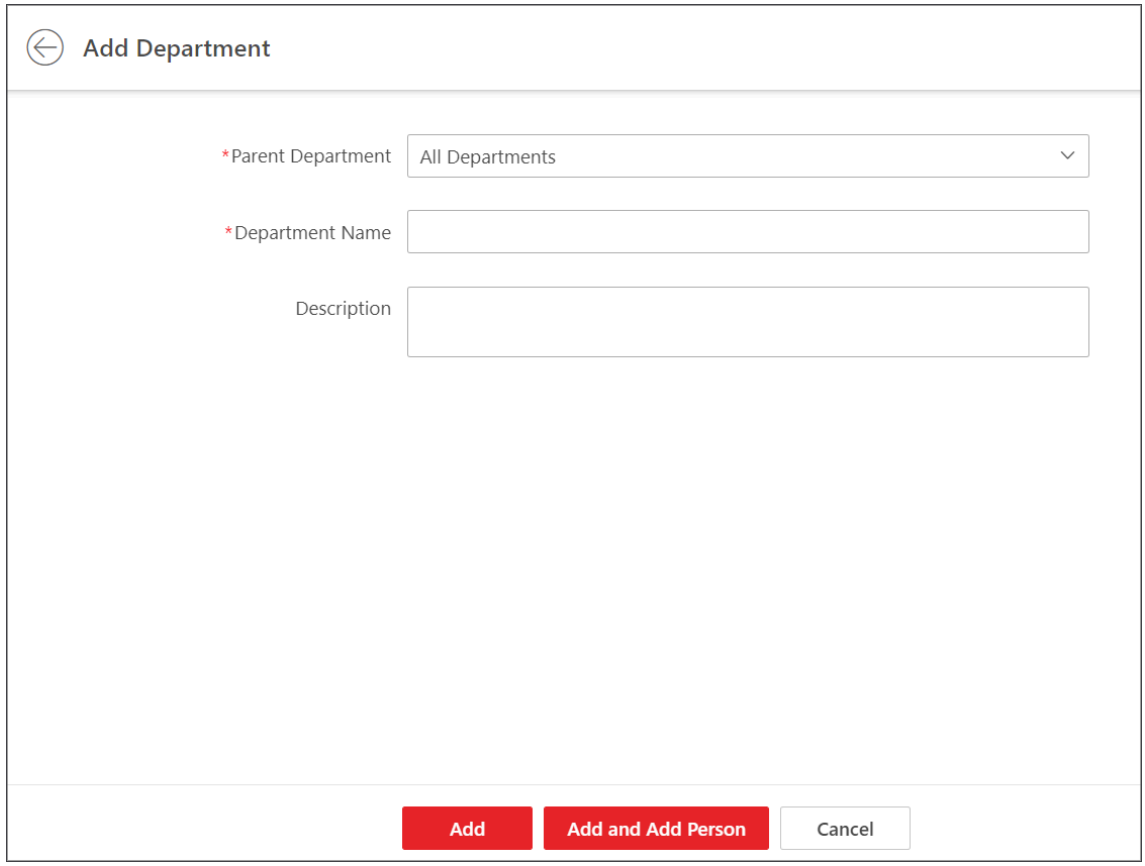


Figure 6-1 Add Department

4. Add department.
   - Click **Add** to add the department and go back to the person management page.
   - Click **Add and Add Person** to add the department and enter the Add Person page.
5. **Optional:** Perform the following operations after adding departments.

Edit Department	Select a department, and click at the top of the department list to edit the parent department, department name, or remarks.
Delete a Department	Select a department and click at the top of the department list to delete the selected one.
	Note The root department cannot be deleted.
Delete All Departments	Click beside at the top of the department list to delete all added departments.

6.2 Basic Configuration Before Managing Persons

The following configurations can be preparations before managing persons.

[Important] Set Person ID Rule

Note

Once a person is added to the platform, the ID rule will be **not configurable**, so we recommended that you should ensure the ID rule at the very beginning.

In the Person module, select **Basic Configuration → Person ID Rule** on the left. Set the total length, and select the ID generation mode, finally save the settings.

Customize Additional Information

Customize a person's basic information by adding additional items as either custom private or custom public information. The former refers to private information such as the person's salary. The latter refers to public information such as the person's department and occupation. When an additional information item is added, it will be displayed as an configuration option on the Basic Information tab of the Add Person page.
Select **Additional Information** on the left, and then click **Add**. In the pop-up window, enter the following parameters and save.

Type

Select the type to restrict the format of the contents of the item.

Sharing Property

Click **Private** or **Public** to set the sharing property of the contents of the item.

For example, if you select **General Text**, enter the text when adding a person. If you select **Date**, setting date as the content of the item is required when adding a person (see the figure below).

Manage Cause of Unauthorizing Persons or Disabling Person Cards

In the left navigation bar of the Person module, click **Basic Configuration → Person Settings → Cause of Disabling** . Click **Add** to add a custom cause. You will be required to select a cause when unauthorizing person(s).

6.3 Add Person

Multiple methods are provided for you to add persons to the platform. You can add a person manually. If you want to add multiple persons at a time, you can import persons by downloading and filling in a template or import persons from devices. In addition, you can batch import domain persons.

You can perform the following operations for adding persons.

If you have enabled the **Use This Device as Registration Device** function on the device's configuration page, the information about added persons and credentials, edited credentials on the device will be automatically synchronized to the platform.

6.3.1 Add a Single Person Manually

You can manually add a person to the platform by setting the person's basic information, credential information, and other information such as the person's access level. The above-mentioned person information constitutes the data basis for the applications related to identity authentication of the person, such as the access control application .

Note

Before adding persons to the platform, you should confirm and set the person ID rule. As once a person is added, the ID rule cannot be edited any more. For more about the ID rule settings, refer to ***Basic Configuration Before Managing Persons*** .
To quickly add a person without entering the Person module, you can click on the top right, and select **Add Person**. For parameter introduction, see the following content.

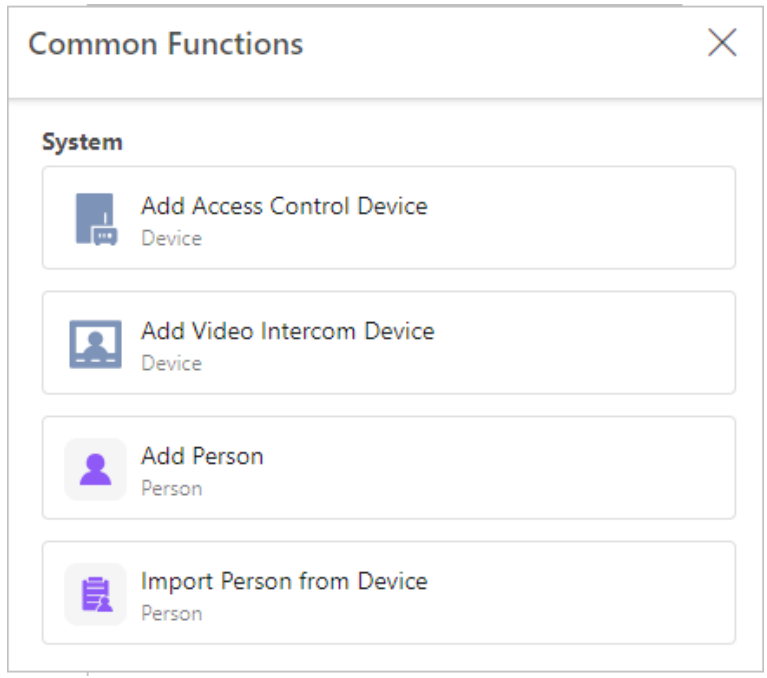


Figure 6-2 Common Functions

On the Person page, select a department from the department list on the left. Then click **Add** above the person list to enter the Add Person page.

Basic Information

Set the person's basic information, such as ID, department, first name, and last name.

ID (Required)

The default ID is generated by the platform. You can edit it if needed.

Profile Picture

See .

Effective Period (Required)

Set the effective period for the person in applications such as access control application, to determine the period when the person can access the specified access points with credentials.

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 ***2021/10/23 13:30:00*** to ***2022/01/20 14:10:00*** and the extended time is selected as **1 Month**, the end time of effective period will change to ***2022/02/20 14:10:00***.

Date of Employment

The start date of employment for the person.

Allow Login to Self-Service

Switch on **Allow Login to Self-Service** ans set a password to allow employees to log into the platform as an employee. On the Login page, employees select the **Self-Service** tab, and enter the employee ID and password to log in.

Credential Management

Add credential information for the person. See ***Manage Credentials for a Single Person*** for details.

Access Level

Click **Access Level** tab, and assign access levels to the person to define the access points where the person can access during the authorized period.

Super Access Permission

Persons with this permission will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first person authorization.

Extended Access

When the person accesses the door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

Note

The extended access and super user functions cannot be enabled concurrently.

Device Administrator

Determine if the person has the administrator permission of access control devices.

If the check-box is checked, when you synchronize person information from access control devices, the administrator permission for the person will be retained.

PIN Code

If you have enabled the function of automatically generating PIN for persons, the platform will generate a PIN automatically. You can click **Auto Generate PIN** to generate a new PIN. In most cases, the PIN code cannot be used as a credential alone: it must be used after card when accessing; It can be used alone only when **Authenticate via PIN Code** is enabled on the platform and the authentication mode of the card readers is also set to **Authenticate via PIN Code**.

- The PIN code should contain 4 to 8 characters.
- For details about enabling **Authenticate via PIN Code** on the platform, see ***Add Departments*** .

Assign Access Level

Assign the permission for specified access points. You can click to view information on access points and access schedules.

Schedule

Click **Schedule** tab, view and edit the schedule of the person in the table.

Allow Check-In/Out via Mobile Client

Switch on it to allow the person to check in/out via the Mobile Client.

Attendance Group

Select an attendance group from the drop-down list. For details, refer to ***Add an Attendance Group*** .

Leave Rule

Select a leave rule for the person. For details, refer to ***Add a Leave Rule*** .

Schedule Overview

View the schedule of the person. You can click **Set Schedule** to set a schedule for the person. For details, refer to ***Assign Schedule to Person*** .

Alarm Detection

On the **Alarm Detection** page, enable **Configure Operation Permission of Security Control Device**. Click **Add** to select device and configure operation permissions including **Arm**, **Disarm**, and **Auto Control** for selected device(s).

User Property

Lifetime

All permissions can be configured for the user.

One-Off

Expires after either a single arming or disarming action, or expires automatically after a 24-hour period. No duress code permission. No Keyfobs and tags permission.

Keypad Password

Only 4 to 6 digits are allowed.

Duress Password

Only 4 to 6 digits are allowed. One-Off users do not need to configure the duress password.

Resident Information

On the **Resident Information** page, set resident information to link the person with the indoor station and floor and room number.

Note

- Make sure you have added indoor stations to the platform.
- When you select an indoor station, the room number of the indoor station will be filled in automatically in **Room**. You can edit the room number.
- Up to 10 persons can be linked with one indoor station. And a person cannot be linked to multiple indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

Skin-Surface Temperature

Enter the person's skin-surface temperature and select the corresponding temperature status. For example, if a person's skin-surface temperature is 37 °C, then you can select her/his temperature status as normal.

Additional Information

On the Additional Information tab, enter additional information to be applied.

Platform User

Add New User

Create a new user and link it with the person.

Select Existing User

Link an existing user with the person.

6.3.2 Batch Add Persons by Template

You can batch add persons to the platform with the minimum effort by importing a template (an Excel file) which contains the person information such as the names of the department and the access levels.

Steps

1. Select **Person Management → Person** on the left.

2. Click **Import → Import Person Information via Excel** .

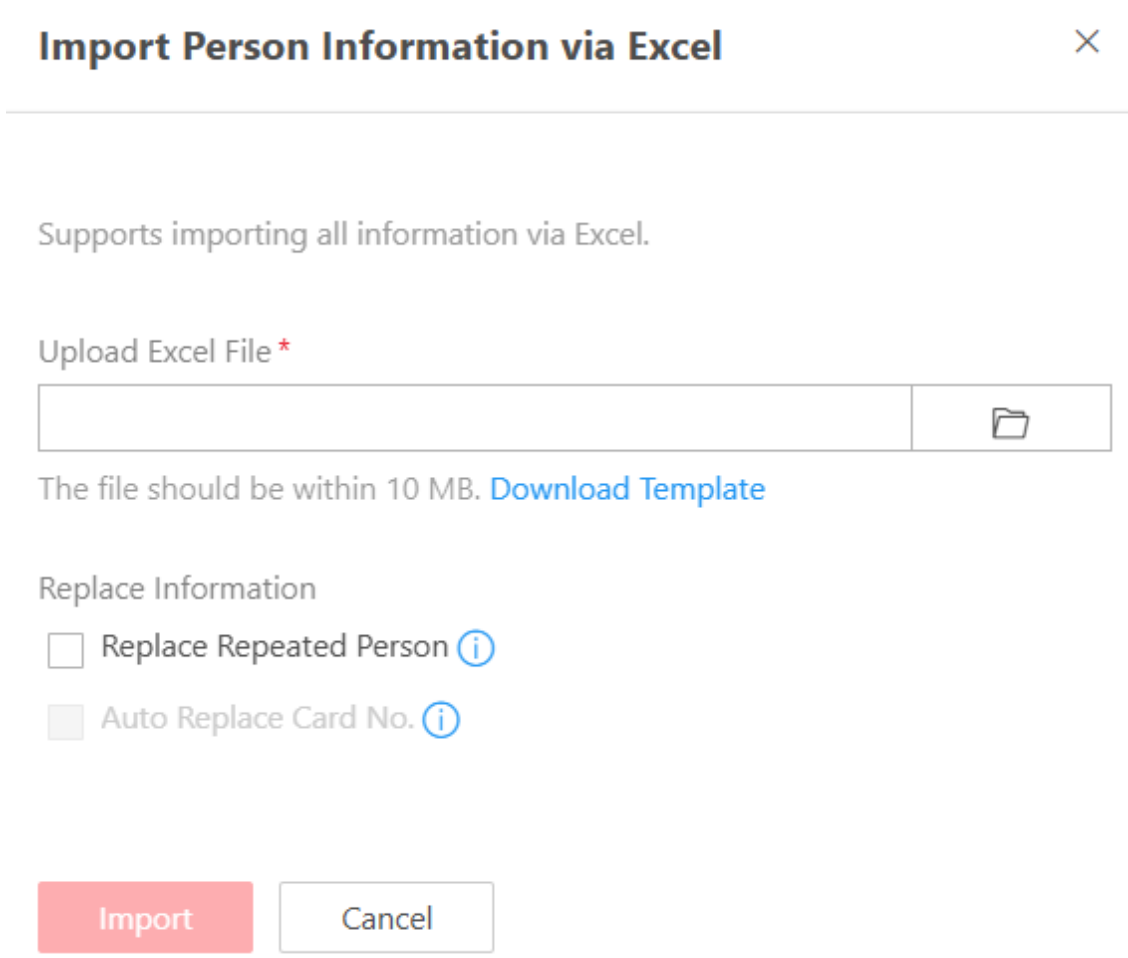


Figure 6-3 Batch Add Persons by Template

3. In the pop-up window, click **Download Template**.
4. Check the basic information items you want to include in the template, such as person type, card No., and email. You can also check custom additional information items.
5. Click **Download** to save the template to your PC.
6. In the downloaded template, enter the person information following the rules shown in the template.
7. Click , and then select the template (with person information) from your PC.
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 list.
9. **Optional:** Check **Auto Replace Card No.** to replace the card No. automatically if it already exists in the platform.
10. Click **Import** to start importing.

Note

- The importing process cannot be stopped once started.
- You can batch issue cards to the persons by importing the template with card No. information.

The importing progress shows and you can check the results.

Note

You can export the person information that failed to be imported, and try again after editing.

6.3.3 Import Domain Persons

You can import the users in the AD (Active Directory) domain to the platform as persons. After importing the person information (including person name and account name) in the AD domain, you can set other information for the persons, such as credentials.

Before You Start

Make sure you have configured the active directory settings. See ***Set Active Directory*** for details.

Steps

1. On the Person page, click **Import → Import Person Information via Domain Group** .
2. Select the importing mode.

   Import Domain Persons

   Import specified persons. Select the organization unit and select the persons under the organization unit which are displayed in the Domain Person list on the right. The person information will be synchronized based on each person.

   Import Domain Organization Unit and Person

   Import all the persons in the organization unit. The person information will be synchronized based on each group.

   Person in Security Group

   Import the selected security groups in the AD domain.
3. When selecting **Import Domain Persons** or **Person in Security Group** as the importing mode, select a department to which the selected items (persons or security groups) need to be imported.
4. Set the effective period for the persons as needed.
5. Click **Import**.

Note

- If the profile picture/email in the domain is linked to the profile picture/email in the platform, the persons' profile picture/email will be imported to the platform from the domain as well. You can view the profile picture/email on the person details page but you cannot edit it.
- If the profile picture/email in the domain is NOT linked to the profile picture/email in the platform, you can take a picture or upload a picture as the person's profile picture and enter the email address.

6.3.4 Import Persons from Device

Import persons information to the platform from devices, including access control devices, video intercom devices, or enrollment station.

To quickly add a person without entering the Person module, you can click on the top right, and select **Import Person From Device**. For parameter introduction, see the following content.

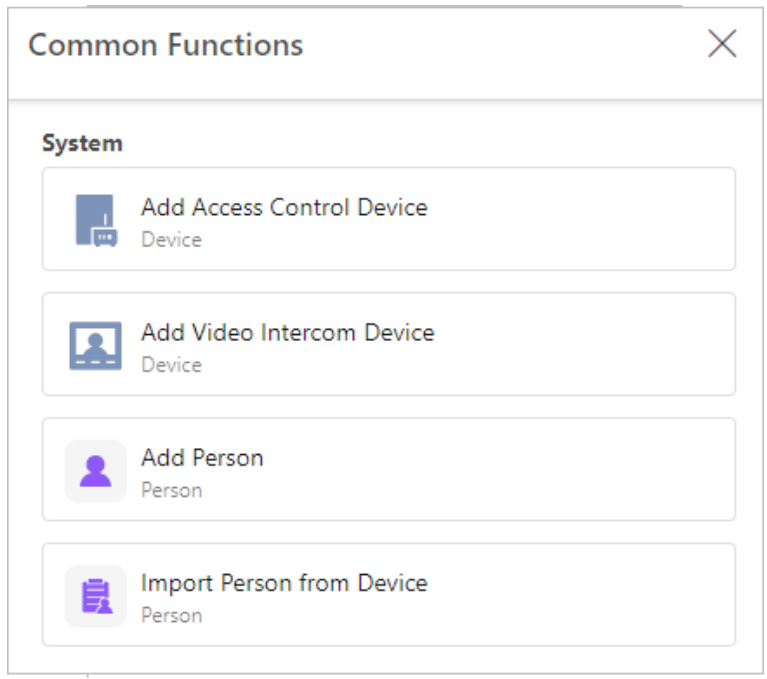


Figure 6-4 Common Functions

On the Person page, click **Import → Import Person Information from Device** to open the Import from Device pane. Select the **Device Type** as **Access Control Device** / **Video Intercom Device** / **Enrollment Station**.

Note

When importing, the platform will compare person information on the device with person information in the platform based on the person name. If the person name exists on the device but does not exist in the platform, the platform will create a new person. If a person name exists on both sides, the corresponding person information in the platform will be replaced by the one on the device.

Import Persons from Access Control Devices or Video Intercom Devices

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 platform. The person information that can be imported includes person names, profile pictures, credentials (PIN codes, cards, and fingerprints), effective periods, person roles, etc.

Importing Range

Import All Persons

Import all the persons stored in the selected devices.

Import Specified Persons

Specify the ID of up to 5 persons and import the persons to the platform.

Select Department

Select a department to which the persons will be imported.

Replace Profile Picture

Replace existed profile pictures with the new ones from the devices.

If the following window pops up, select a method to import the person information.

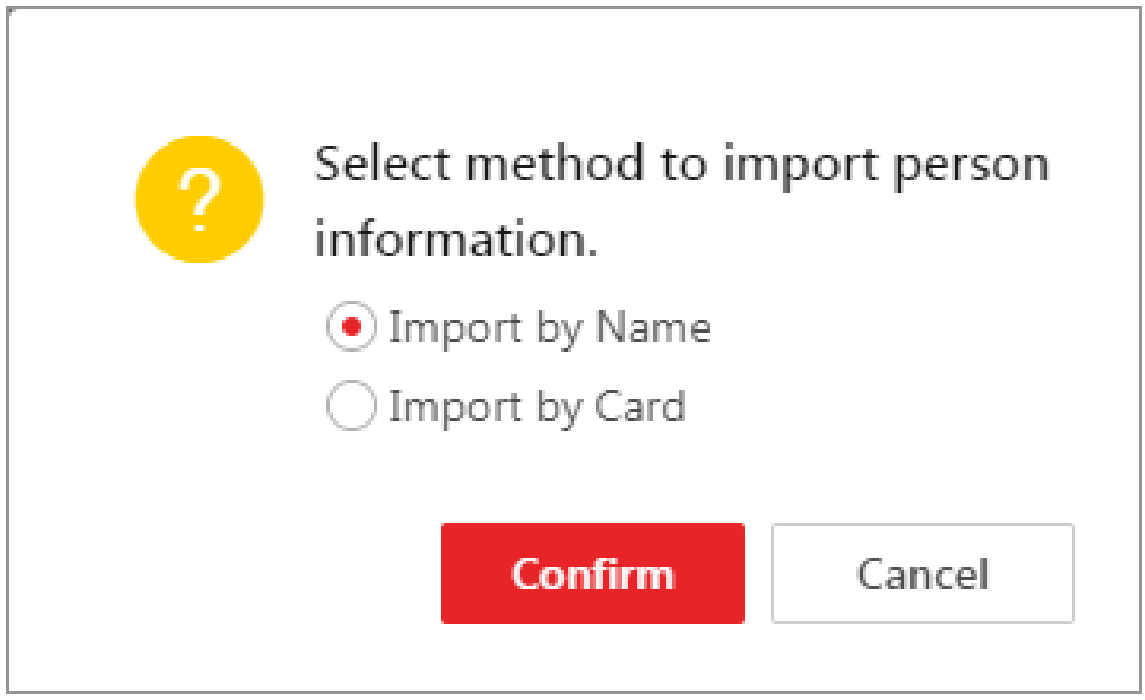


Figure 6-5 Select an Import Method

Import by Name

The person information directly linked to the access control devices will be imported.

Note

This method is usually used for the access control devices with facial recognition capability.

Import by Card

The person information linked to the cards of the access control devices will be imported

Note

This method is usually used for the access control devices which link person information via cards.

Import Persons from Enrollment Station

You can apply the required person information to an enrollment station via a template or the person list on the platform, and then enroll the persons' credentials via the enrollment station. Once you complete the enrollment, you can import the person and credential information from the enrollment station to the platform by specifying the IP address, port number, user name and password of the device to allow the platform to access it.

Before application or importing, configure access mode, access protocol, address, port No., user name, and password of the enrollment station to link the platform to it.

Then, select the Stage as **Apply Person Information**.

Import from Template

If the persons are not added to the platform, download the template from the enrollment station and then edit the template and apply it to the enrollment station for enrolling the persons' credentials.

Import from Person List

If the persons have been added to the platform, select the department to apply the persons to the enrollment station for enrolling the persons' credentials.

Enroll person credentials, and select the Stage as **Copy Back Person and Credential Information**. Select a department and click **Import**.

6.3.5 Operations Available on Person List

For added persons, you can perform the following operation(s).

Edit Person	Click the person name to edit the person details. **Note** When editing the person's effective period, if you have issued temporary card(s) to the person, make sure the expiry date(s) of the person's temporary card(s) are within the effective period.
Delete Persons	Check the person(s) and click **Delete** to delete the selected person(s). Hover the cursor onto beside **Delete**, and then click **Delete All** to delete all persons.
Clear All Profile Pictures	Hover the cursor onto beside **Delete**, and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.
Export Person Information	Click **Export → Export Person Information** , select the **Exporting Range**, and check information types you need to export person information to your PC. For information security, you need to enter your login password to authenticate.
Export Profile Pictures	Click **Export → Export Profile Picture** , select the **Exporting Range**, enter your login password

	and a password for decompressing the ZIP file, and click **Export**. **Note** Before using this function, you should activate this function first by going to **System → Security → Export Profile Pictures** page and checking the **Export Profile Pictures**.
Adjust Person	• Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed. 1. Select one or more persons, click **Adjust → Adjust Department** . 2. Select the target department to which the persons are about to be moved. 3. Click **Move**. • Adjust the effective period for the person in applications. 1. Select one or more persons, click → **Adjust Effective Period** . 2. Select the effective period from the drop-down list. 3. Click **OK**. • Adjust the person's status as resigned. 1. Select one or more persons, click → **Adjust Effective Period** . 2. Set the departure date, type, and reason.. 3. Click **OK**.
Manage Persons' Cards	See ***Card Management*** .
Synchronize Domain Persons	Select person(s) whose information has changed in the AD domain and click **More → Synchronize Domain Persons** at the top of person list to get the latest person information.
Link Persons to Indoor Stations	Select one or more persons, and click **More → Link to Indoor Station** , then select an indoor station for each person to apply the person information to the indoor station.

	Note • A pop-up window will appear after you click **Save**. Click **Yes** to save the indoor station's room number as the room number, or click **No** to keep the old room number (if there is not an old room number, the room number of the indoor station you select will be saved). • Make sure you have added indoor stations to the platform. • Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations. • Make sure the room number is consistent with the actual location information of the indoor station.
Clear Access Levels	Select one or more persons, click **More → Clear Access Levels of Person** to clear the access levels of the selected persons. **Note** The access levels of these persons cannot be restored once they are cleared.
Check Person Authorization	Select one or more persons, click **More → Check Access Levels of Person** to enter Check Person Authorization page. On the page, you can test whether the person's access levels and credentials are applied to the access control devices and video intercom devices. If failed to be applied, you can apply them again.
Enable/Disable Check-In/Out via Mobile Client	Select one or more persons, click **More → Enable/Disable Check-In/Out via Mobile Client** .
Unlock Users	For persons whose account is locked due to too many failed attempts for login, Administrators can unlock their accounts for login. On the top, click **More → Unlock for Login** , check persons, and click **Unlock**.

6.4 Person Self-Registration

If there are persons to be added to the system, you can generate a QR code for them to scan. After scanning the generated QR code by smart phone, the persons can enter their personal information (including profile) on Self-Registration page. If you have enabled Review Self-Registered Persons function, you need to review and approve their person information, otherwise they cannot be added to the system.

This function is applicable to circumstances like a company where there are a large amount of new employees to be added to the system. For example, you print the generated QR code for the new employees to scan. After scanning the QR code by smart phone, new employees will enter Self-Registration page to import their personal information.

Note

You should set self-registration parameters beforehand. See ***Set Self-Registration Parameters*** for details.

6.4.1 Set Self-Registration Parameters

Before starting self-registration, you need to set self-registration parameters. A QR code is necessary for the persons to register their information by themselves. Besides, you can configure face quality verification and person information review.

Select **Basic Configuration → Self-Registration Settings** on the left panel, or click **Person Management → To Be Reviewed → Self-Registration Settings** to enter the Self-Registration Settings page.

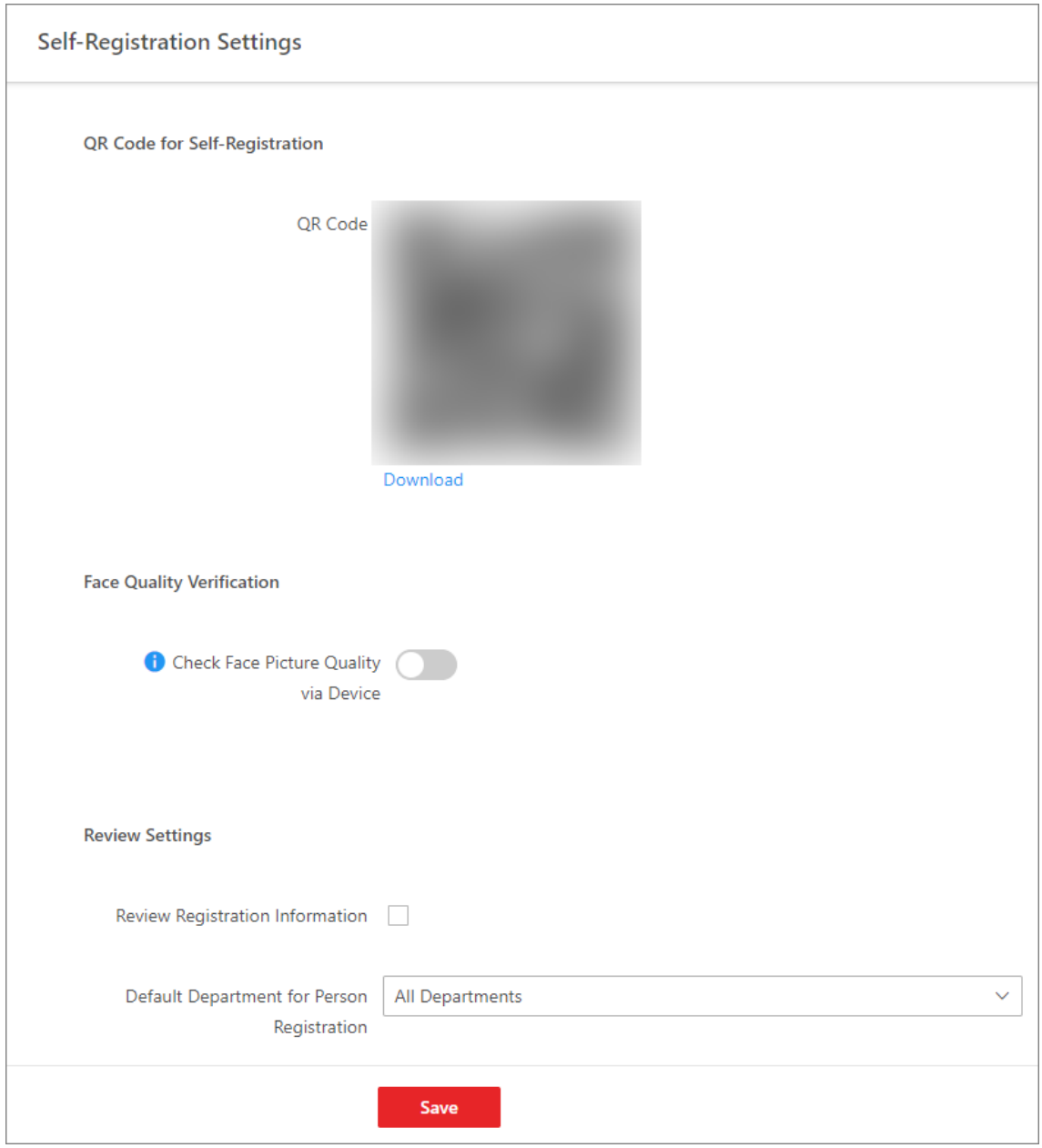


Figure 6-6 Self-Registration Settings

QR Code for Self-Registration

The platform will generate a QR code for you to download. After downloading the QR code, you can print it or send it to persons who are going to register.

Face Quality Verification

After the person uploads profile by a cellphone, the selected device will automatically start checking the profile's quality. If the profile picture is not qualified, the person will be notified.

Only when the uploaded profile is qualified can the person register successfully. Otherwise, the person's information cannot be uploaded to the platform.

Note

To use this function properly, make sure you have added an access control device or video intercom device to the platform beforehand.

Review Self-Registered Persons

Set a default department. Once the person information is registered, the person will be added to this group.

If you enable **Review Self-Registered Persons**, after registration, you need to review the person information on the Persons to be Reviewed page. After verification, the person will be added to the selected department. See ***Review Self-Registered Person Information*** for details about how to review.

6.4.2 Scan QR Code for Self-Registration

If a person needs to register by self-service, the person should use a smart phone to scan the self-registration QR code to enter the Self-Registration page and enter person information. After registration, the person details will be uploaded to the platform for review.

Before You Start

The administrator can print the QR code or send the QR code to persons to scan. See ***Set Self-Registration Parameters*** about how to generate a self-registration QR code.

Steps

1. Use your smart phone to scan the self-registration QR code to enter the Self-Registration page.
2. Tap the profile frame to upload a face picture.

Note

- You can select a picture from your phone album, or take a photo by phone.
- After uploading a profile, profile quality checking will automatically start. If the profile is not qualified, you will be notified. Only when the uploaded profile is qualified can you register successfully. Otherwise, your personal information cannot be uploaded to the platform. See ***Set Self-Registration Parameters*** for details about setting Face Quality Verification function.

3. Set your personal information, including name, ID, email, phone number, etc.
4. Enter the verification code.
5. Tap **Save**.
   - If **Review Self-Registered Persons** function is enabled, wait for the review. If you are approved, you will be added to the platform. See ***Review Self-Registered Person Information*** about how to review.
   - If **Review Self-Registered Persons** function is disabled, the person information will be uploaded to the platform.

6.4.3 Review Self-Registered Person Information

If you have enabled **Verify Registration Information** function when you set self-registration parameters, after the persons registered, their person information will be displayed on the Persons to be Reviewed page, and their status will be displayed as **To be Reviewed**. You should review their personal information to approve. After approving, they will be added to the target department.

Then select **Person Management → To Be Reviewed** on the left panel to enter the Persons to Be Reviewed page.

Review the displayed person information and verify them.

Table 6-1 Review Self-Registerd Persons

Operation	Description
Approve Self-Registered Person Information	If the self-registered person information is correct, approve the information to add the registered persons into the platform. • Select a registered person, and click to approve the person. • Check multiple registered persons, and click **Approve** to approve them all.
Reject Self-Registered Person Information	If there is something wrong or missing with the self-registered person information, reject the person and tell the person to register again with right information. • Select a registered person, and click to reject the person. • Check multiple registered persons, and click **Reject** to reject them in a batch.
Delete Self-Registered Person Information	• Select a registered person, and click to delete the person from the Persons to be Reviewed list. • Check multiple registered persons, and click **Delete** to delete them all from the Persons to be Reviewed list.

Approved persons will be added to the target department; rejected persons will not be added to the target department, but they will stay in the Persons to be Reviewed list.

6.5 Resigned Persons Management

You can manage resigned persons by adding, deleting, and editing resigned persons. You can also reinstate resigned persons and export resigned person information.

Manage Resignation Types

If the default resignation types do not meet your needs, you can add other resignation types.
Select **Basic Configuration → Resignation Type** on the left.

- Click **Add**, enter the departure type name, and click **Add** in the pop-up window to customize the type.
- Click in the Operation column to edit the added departure type.
- Click or **Delete** to delete the selected departure type(s).

Note

- The default types (dismiss, departure, redeployment, and suspension with pay) cannot be deleted or edited.
- Up to 100 departure types can be added.

Add Resigned Persons

You can add one or multiple resigned persons, delete and export the resigned person information.
Select **Person Management → Resigned** on the left, and then click **Add** to open the Add Resigned Person pane. Click to select one or multiple persons from the departments.

Departure Date

Last day of the current employment.

Disable Attendance

Check it, then the platform will not calculate attendance results generated during the period between applying for resigning and departure date.

You can also select persons on the person list, and click **Adjust → Resigned** to quickly add resigned persons.
For persons to be resigned, their permissions of access, and credentials such as the card, fingerprint, face picture, iris data will be deleted at the day of resignation.

Reinstate Persons

You can reinstate persons who are resigned and to be resigned.
Select **Person Management → Resigned** on the left. Select one or multiple persons and click **Reinstate**. On the pop-up, select the department to which the person(s) will be reinstated, and click **Reinstate**.
After the person reinstatement, you can view the related persons in the person list.

After the reinstatement, the resigned persons need to upload their credentials, such as face picture, fingerprint, and iris data. Their access levels will be accordance to that of their departments.

6.6 Credentials Management

Before credential management, you can perform the following preparations if needed.

- **Set QR Code Mode**: You can select static QR code or dynamic QR code for employees. If you select dynamic QR code, the platform will generate a dynamic QR code for persons on the platform. Every time the employee uses the QR code to authenticate, the platform will invalidate the current QR code in use. While static QR code will stay unchanged. The card in the personnel credential list does not display the QR code information.
  In the left navigation bar of the Person module, click **Basic Configuration → Credential Settings → QR Code Mode** . Select a QR code mode, and set the QR code validity period if you select **Dynamic QR Code**.
  QR code updates can occur in three ways:
  - Manually Update: The user actively updates the QR code.
  - Automatic Update: The QR code will be refreshed once it has reached its pre-set expiration time.
  - Update Upon App Re-entry: The QR code will be refreshed when the user re-enters the application.
- **Automatically Generate PIN for Persons**: Enable this function so that you do not have to manually set PINs for newly-added persons.
  In the left navigation bar of the Person module, click **Basic Configuration → PIN Configuration** . Check **Auto Generate PIN for Person** and save.

6.6.1 Manage Credentials for a Single Person

When adding a person, you can add the required credential information for the person. The supported credentials include normal cards, profile pictures, fingerprints, irises. These credentials can be used for the access authentication in applications such as access control .

You can add or change credentials on the Add/Edit Person page and the Person List.

- On the Add/Edit Person page, you can collect or add a profile picture, and click **Credential Management** to add other credentials such as cards, fingerprints, irises.
- On the Person List page, credentials (including cards, fingerprints, irises but profile pictures) are displayed in the Credential Information column. You can view numbers of them, or click their icons to view details or add one credential.

How to Add a Profile Picture

On the Add/Edit Person page, hover the cursor on , and select from three modes to add a profile picture.

From Device

This mode is suitable for non-face-to-face scenario when the person and the system administrator are on different locations.

Note

- For access control devices, only specific models of face recognition terminals are supported.
- For video intercom devices, door stations and outer door stations are supported.
- For enrollment stations, you need to set related parameters, including access mode, access protocol, device address, port, user name, password, face anti-spoofing, and security level.

Capture

Click **Capture** and then select one of the PC's webcams to take a picture.

Upload Picture

Click **Upload Picture** to select a picture from your PC. On top of the Upload Picture window, click **Detect Now** and select a device type and device to detect the face picture quality.

Note

- 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 or zoom in/out before cutting it.

Note

If you add a smart terminal to the platform, the smart terminal will automatically create models for the profile picture.

How to Generate a QR Code for a Person

The QR code of card is only displayed when you set the QR code mode to static QR code.
A QR code will be generated automatically after ***adding a card*** and the icon will appear in the top right corner of the card area when you enter the Add Credential page from the editing person page. You can click (also on the Credential Information column of the Person List) to view and scan the QR code or click **Download** to save it to the local storage for further operations.

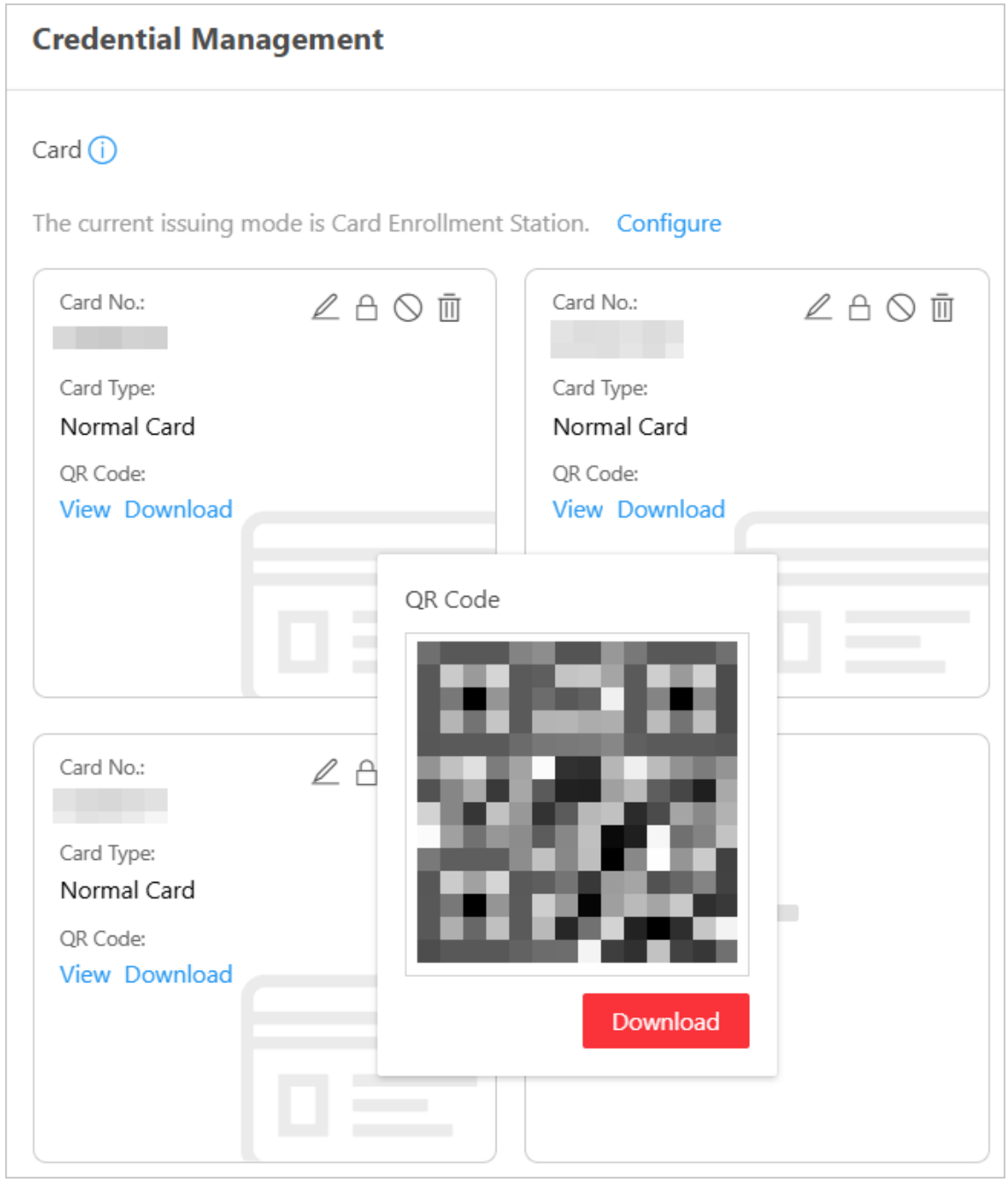


Figure 6-7 View QR Code of Card

How to Collect Irises

In the Iris area, collect irises of the person. Click **Configure** to select a device used for collecting the person's irises. Click + and then start collecting irises.

How to Collect Fingerprints

In the Fingerprint area, click **Configure** to set the method for collecting the person's fingerprint, and then collect the fingerprint.

USB Fingerprint Recorder

Plug the USB interface of the fingerprint recorder to the PC on which the Web Client runs and then collect the person's fingerprint via the device.

Fingerprint and Card Reader

Select a device type and then select a fingerprint and card reader to collect the person's fingerprint.

Enrollment Station

If you set network as the access mode, set other parameters of the enrollment station (e.g., access protocol, device IP address, and device port No.,) to allow the platform to access the device via network. And then collect the person's fingerprint via the device.

If you set USB as the access mode, plug the USB interface of the enrollment station to the PC on which the Web Client runs, and then collect the person's fingerprint via the device.

Switch on **Special Credential** and then add special cards and corresponding fingerprint information.

6.6.2 Import Profile Pictures

You can add multiple persons' profile pictures to the persons in a department. If you access the platform via the Web Client running on the SYS, you need to specify a path where the profile pictures are stored. If you access the platform via the Web Client running on other computers, you can import a ZIP file containing the profile pictures.

Steps

Note

If the ID in the name of the profile picture is duplicate with the person's ID that already exists in the platform, the former will replace the latter. If the ID in the name of the profile picture doesn't exist in the platform, or the name of the profile picture only contains the person name, the platform will create a new person.

1. Name the profile pictures according to the person name or person ID.

   Note

   - The naming rule of picture is: Person Name, Person ID, or Person Name ID. The person name should contain the first name and the last name, separated by a plus sign.

The naming rule for profile pictures: First Name+Last Name_ID. At least one of first name and last name is required, and the ID is optional. For example, Kate+Smith_123.jpg; Kate_123.jpg; Smith_123.jpg.

- Dimension recommendation for each picture: 295×412.
  Size recommendation for each picture: 60 KB to 100 KB.
- The pictures should be in JPG, JPEG, or PNG format.

2. **Optional:** If you access the platform via the Web Client running on the SYS, move these pictures into one folder and then compress the folder in ZIP format.

Note

The ZIP file should be smaller than 4 GB, or the uploading will fail.

3. On the top, select **Person**.
4. Select **Person Management → Person** on the left.
5. Click → **Import Profile Picture** .
6. Select the person pictures.
   - If you access the platform via the Web Client running on the SYS, select a path where the profile pictures are stored.
   - If you access the platform via the Web Client running on other computers, select ZIP files containing the profile pictures.

   Note

   You can hold CTRL key and select multiple ZIP files. Each ZIP file should be no larger than 4 GB.
7. Select a department from **Department**.
8. **Optional:** Switch on **Check Face Quality by Device** and then select a device type and a device for verifying the face quality.
9. Click **Import** to start importing.

   The importing progress shows and you can check the results.
10. **Optional:** After importing profile pictures, click **Export Failure Details** to export an Excel file to the local PC and view the failure details.

6.6.3 Card Management

How to Add a Card

In the ***Card*** area, click + , and then manually enter the card No. or swipe the card on devices (enrollment station, card enrollment station, or card reader) to add normal cards.

- For manually entering, digits, letters, and the combination of digits and letters can be entered.
- For swiping cards, you can read card information via the enrollment station, card enrollment station, or card reader. For details, see ***Batch Issue Cards to Persons*** .

Set Card Issuing Parameters

HikCentral Access Control provides multiple modes for issuing cards, including reading card numbers via devices (card enrollment stations or enrollment stations) and manually entering card numbers.

Steps

1. Select **Person Management → Person** on the left.
2. Open the card issuing settings window when managing credentials or batch issuing cards to persons.
   - Open the window when managing credentials.
   - Open the window when batch issuing cards to persons.
   - Open the window when filtering persons in the person list.

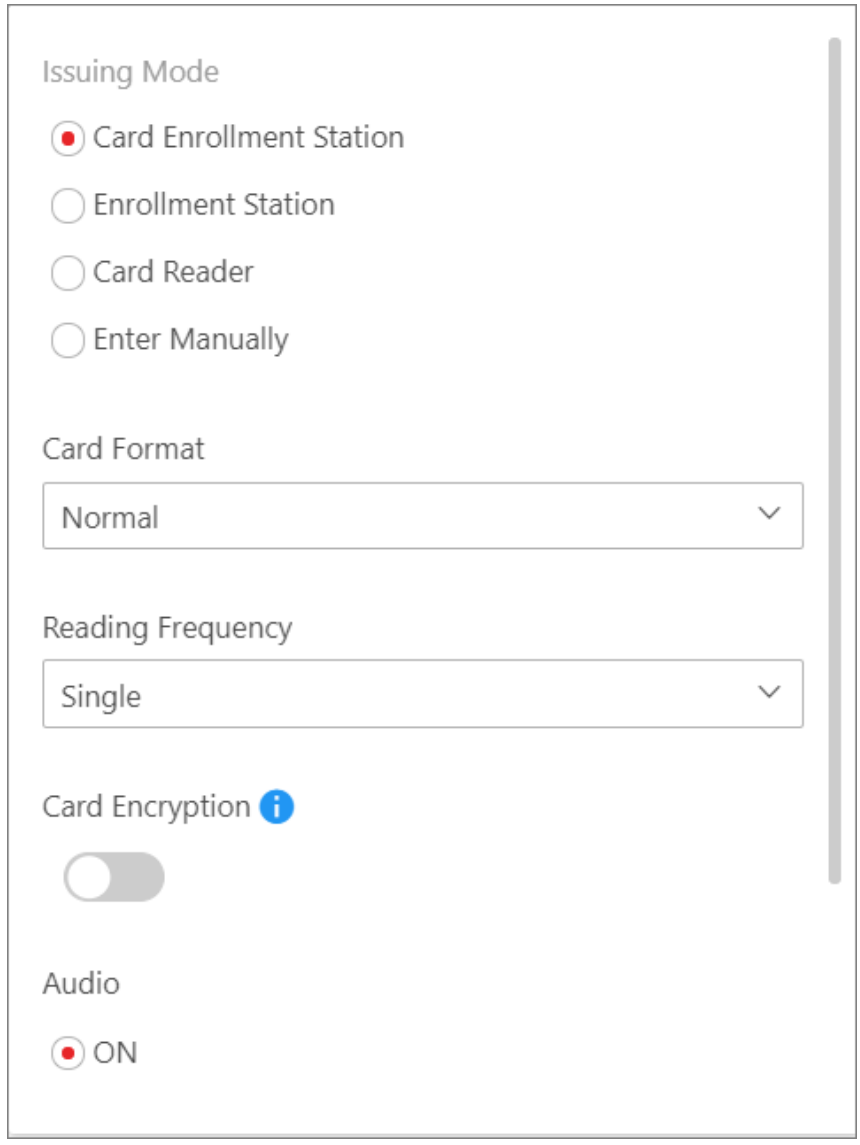


Figure 6-8 Card Issuing Settings Window Opened when Batch Issuing Cards to Persons

3. Select an issuing mode and set the related parameters.

Card Enrollment Station

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

If you select this mode, you should set the card format and card encryption function.

Card No. Type

If the card type is Wiegand card, select **Wiegand**. If not, select **Normal**.

Reading Frequency

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

Note

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

Card Encryption

If you set **Normal** as the card No. type, you can enable the card encryption function and select section(s) to be encrypted for security purpose. After enabled, you should enable the card encryption in the access control device's configuration page to make card encryption effective.

Audio

Turn on or turn off the audio.

Enrollment Station

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

If you select this mode, you should set the required parameters below.

Access Mode

The access mode of the enrollment station. Click **Network** or **USB** from the dropdown list.

Access Protocol

The access protocol of the enrollment station. By default, the access protocol is SDK.

Device Address

The IP address of the enrollment station.

Device Port

The port number of the enrollment station.

User Name

The user name used to log in to the enrollment station.

Password

The password used to log in to the enrollment station.

Card Format

If the card is Wiegand card, select **Wiegand**. If not, select **Normal**.

RF Card Type

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

Note

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

Card Reader

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

Note

- One card reader can be selected for issuing cards by only one user at the same time.
- If you set a third-party card reader to read the card number, you should set the custom Wiegand protocol for the device to configure the communication rule first.

Enter Manually

Note

This parameter is not available on the card issuing settings window opened when managing credentials and filtering persons in the person list.

If you select this mode, you need to 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

4. Click **Save** (for Credential Management) or **Start** (for Batch Issue Cards to Persons).

Batch Issue Cards to Persons

The platform provides a convenient way to batch issue cards to multiple persons.

Steps

Note

- Up to 5 cards can be issued to one person.
- You cannot issue cards to persons who have temporary cards.

1. Select **Person Management → Person** on the left.
2. Select persons to whom the cards will be issued.
3. Move the cursor onto **Card**, and then click **Batch Issue Cards to Persons**.
4. In the pop-up window, set the related parameters.

Note

For details about setting the card issuing mode and parameters, refer to ***Set Card Issuing Parameters*** .

5. Issue one card to one person according to the issuing mode you select.
   - If you set the issuing mode to **Card Enrollment Station**, place the card on the card enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you set the issuing mode to **Card Reader**, swipe the card on the card reader. The card number will be read automatically and the card will be issued to the first person in the list.

- If you set the issuing mode to **Enrollment Station**, place the card on the enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
- If you set the issuing mode to **Enter Manually**, enter the card number manually in the Card Number field. Press **Enter** key on the keyboard to issue the card to the person.

Note

You can check **Auto Increment Card Number** and enter a start card number to issue cards with incremental numbers to the selected persons in the list.

6. Click **Start** to start issuing cards.
7. Repeat step 5 to issue the cards to the persons in the list in sequence.

Note

You cannot change the card issuing mode once you issue one card to one person.

8. Click **Save**.

Print Cards

After adding persons to the platform, you can print their information onto blank physical cards. If you have set credential information (e.g., virtual card information) for the persons, the credential information will be linked to the physical cards once the physical cards are printed. For example, in the scenario of employee management, you can print physical cards as the employee ID badges, which can be used by your employees as the credentials for access authentication at the access points of your company.

Before You Start

- Make sure you have added the supported printers to the platform. For details, see ***Set Printer*** .
- Make sure you have added card templates to the platform. For details, see ***Set Card Template*** .

Steps

1. Select **Person Management → Person** on the left.
2. **Optional:** Set conditions to search for the target persons.
3. Select the persons for whom you need to print cards.
4. Click **Print Card** to open the Print Card window.

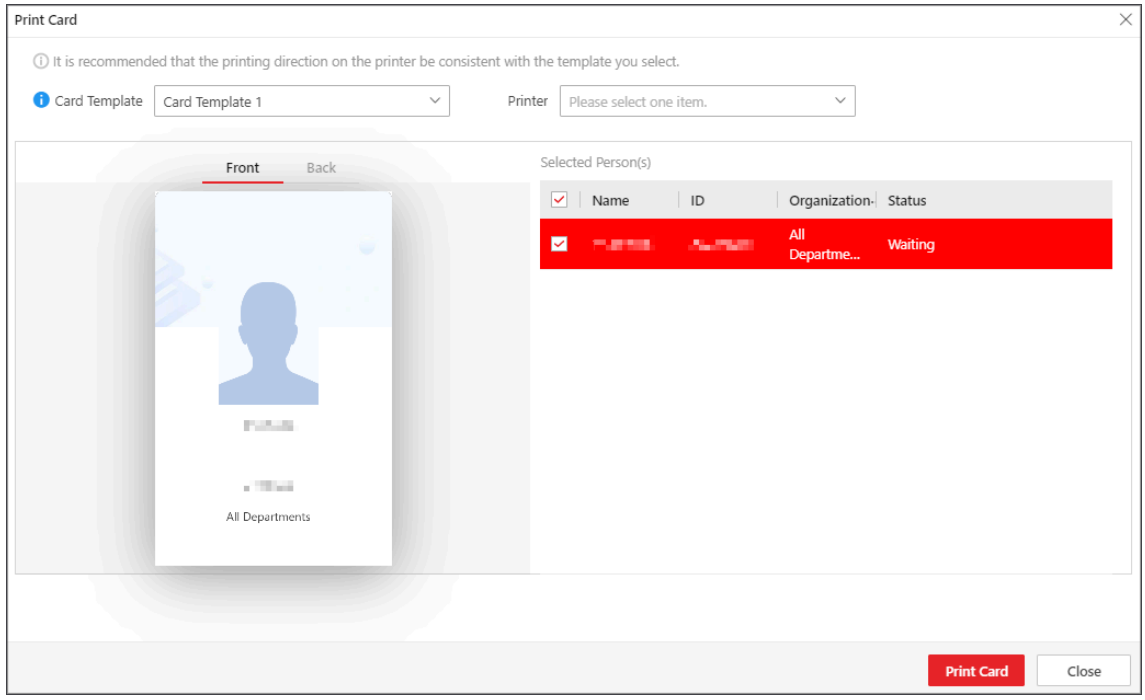


Figure 6-9 Print Card Window

5. Select a card template from **Card Template**.
6. Select a printer from **Printer**.
7. Select person(s) from the Selected Person list.
8. Click **Front** and **Back** to preview the information to be printed on the front and back of the physical cards.
9. Click **Print Card**.

What to do next

If you have not manually added card information for the persons, batch issue card information to them. Otherwise the persons cannot use the physical cards for access authentication. See ***Batch Issue Cards to Persons*** for details.

Card Loss

If a person cannot find her/his card, he/she should contact the card issuer as quickly as possible and the card issuer should report card loss via Web Client immediately to freeze the access level of the lost card. The card issuer can issue a temporary card with effective period and access level to the person. When the card is found, the card issuer need to take back the temporary card and cancel the card loss report, and then the found card will be active again.

Report Card Loss

Click the name of the person in the person list to enter the basic information page, and then click **Credential Management** to expand the Add Credential panel. In the Card area, move the cursor onto the lost card and then click . After you report card loss, the access levels of the lost card will be inactive.

You can also select the persons in the person list, move the cursor onto **Card** on the top, and then select **Report Loss** on the top to batch report loss.

Issue a Temporary Card to a Person

If a card is reported as loss, you can issue a temporary card to the person who loses the card. Once the temporary card is issued, other cards linked to this person will be inactive, and the biometric credentials linked to these inactive cards will be transferred to this temporary card.
On the page of a single person. click **Credential Management** under the profile picture to open the Credential Management pane. In the Card area, click .
The expiry date of a temporary card should be within the effective period of the person (card owner). In other words, the expiry date cannot be later than the effective period. For details about setting or editing the person's effective period, see ***Add a Single Person Manually*** .
You can delete the temporary card for the person. Once the temporary card is deleted, the inactive cards of the person will restore to the active status, and their previously linked person information will also restore.
Perform the following operation(s) if needed.

Table 6-2 Operations for Temporary Card

Operation	Description
Edit the Temporary Card	Move the cursor onto the temporary card, and then click to edit the temporary card.
Delete the Temporary Card	Move the cursor onto the temporary card, and then click .

Batch Cancel Card Loss

If the lost cards are found, you can batch cancel the card loss reports for multiple persons. After that, the cards' access levels will return to be active and the original biometric credentials (such as fingerprints and face information) will be linked to these cards again.

Select the persons in the person list, hover the cursor on **Card**, and then click **Cancel Card Loss**.

Disable/Restore Card

On the person list, check persons and click **Card → Disable Card** , select the card(s) to be disabled, select the cause of disabling, and click **Disable**.

If you want to restore cards, check persons and click **Card → Restore Card** , select the card(s) and click **Restore**.

6.7 Position Management

The platform allows you to add positions to define the hierarchical levels of your company. By assigning the positions to employees, you can quickly understand the number of active employees in each position and the number of employees who have resigned. You can manually add positions one by one or import multiple positions at once via a predefined template.

Select **Position Management** on the left to enter the Position Management page.

Add a Position Manually

Click + above the left position tree to open the Add Position pane. Enter the name of the position. From the drop-down list, select the upper-level position to which the position to be added is subordinate. You can click to select the persons that have been assigned to this position.

Import Positions

Click above the left position tree to open the Batch Import Positions pane.
Click **Download Template** to download the template to the local PC. Open the downloaded template file and fill in the required information, including the names of the positions and their upper-level positions. Click to select the edited template file from the local PC.
Check **Auto Replace Duplicated Position** to allow the platform to automatically replace existing positions if the file to be imported contains positions that are already added to the platform.

Note

If it is not checked and the file contains positions that are already added to the platform, the import may fail.

Chapter 7 Access Control Management

Access control is a security technique that can be used to regulate who can get access to the specified door.

On the top, select **Access Control**.

On the Web Client, the administrator can add access control devices and video intercom devices to the system, group resources (such as doors) into different areas, and define access permissions by creating an access level to group the doors and an access group to group the persons. After assigning the access level to the access group, the persons in the access group will be authorized to access the doors in the access level with their credentials during the authorized time period.

The following are high-frequency scenarios for your reference.

- ***Assign by Person*** : Assign access level to persons, so that the assignees can have the access to the access points in the access levels.
- ***Manage Multi-Factor Authentication*** : An access authentication scheme which requires all the predefined persons to be present and authenticate.
- ***Anti-Passback*** : Only one person can pass the access point after swiping the card.
- ***How to Open the Door by Your Smart Phone*** : Open the door quickly by the Mobile Client or by rotating their phone by the reader.

On top right of Home page, you can click **Expand Quick Configuration**, click **Quick Configure** in Access Control, and through the following steps, you can quickly set doors and time that allow persons to enter and exit, so as to control and manage person entrance and exit.

1. Add access control devices. For details, refer to ***Add Device(s)*** .
2. Add persons. For details, refer to ***Person Management*** .
3. Set time period that allows persons to enter and exit. For details, refer to ***Set Access Schedule Template*** .
4. Set door(s) that allow entrance and exit. For details, refer to ***Assign Access Level to Persons*** .
5. Assign access levels to persons. For details, refer to ***Assign Access Level to Persons*** .

Name	Description
Wizard	You can view the brief introduction of the Access Control function and the major steps of configuration. You can hover the mouse cursor over each step and click ↗ to go to the corresponding page; click **Quick Configure** to complete the configuration process step by step in the Access Control Wizard.
Health Status	In Health Status, click the number in a circle to view status of each resource type, or click the number on the right of **Exception** to go to the Maintenance page for details about alarm inputs.

Name	Description
	In the upper-right corner, click **Go to Maintenance** to enter the Maintenance module. For more about the Maintenance module, refer to ***Maintenance*** .
Person Credential Status	Click the number in the circle of each credential to go to the Person page. Click the number under the application items (including person information and credentials) to go to the corresponding pages for details.
Access Event Statistics	Click and select a period to view the statistics of this period. Hover over , select a file format, and click **Export** to export the data generated in the selected period.
Person Access Event Statistics	Click to show the details of the recognized person. Click **Auto Update Record** to automatically display the latest record. Click **More** to go to the Person Authentication Record page to search for more data.

7.1 Flow Chart of Door Access Control

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

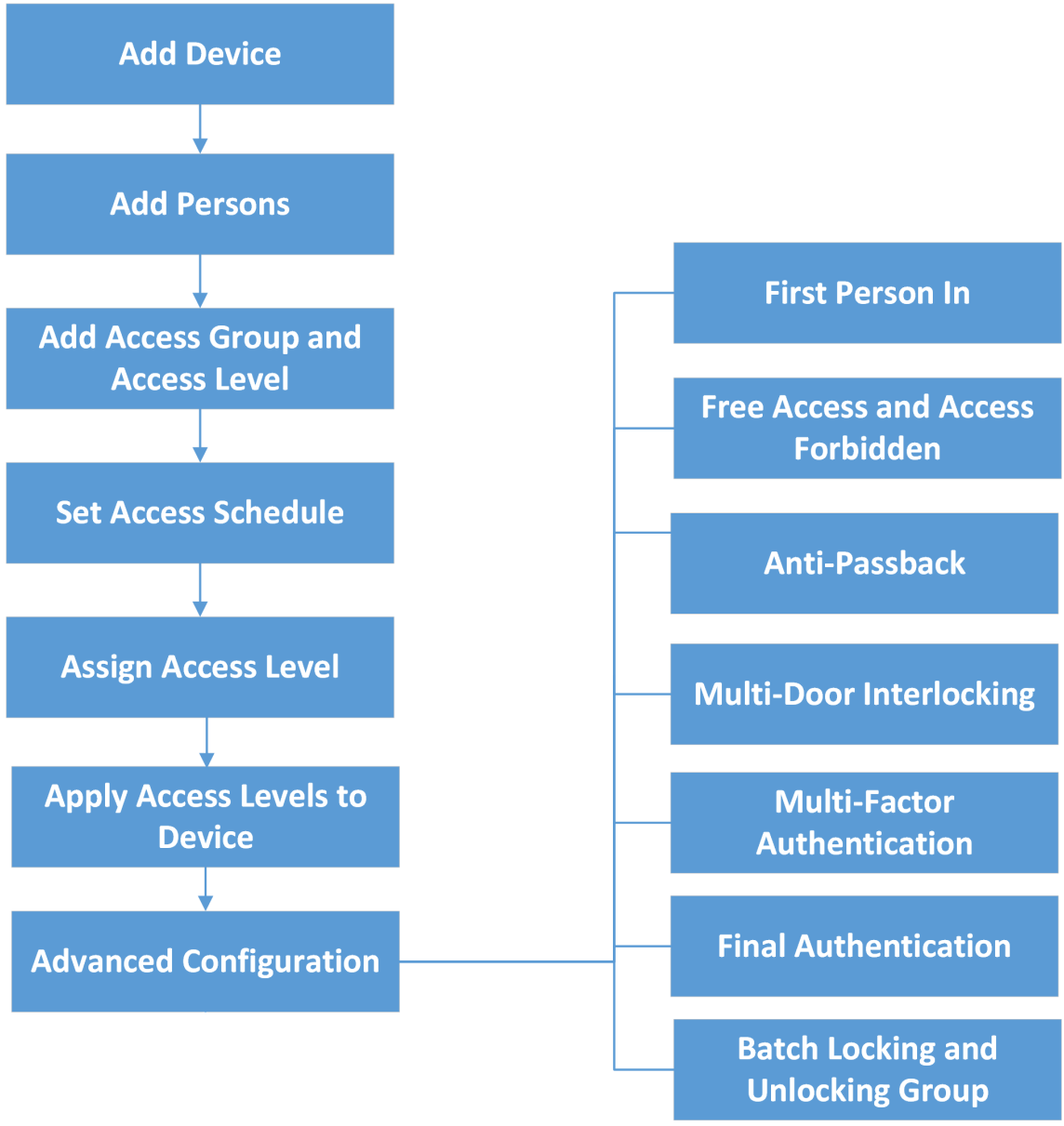


Figure 7-1 Flow Chart of Door Access Control

7.2 Assign Access Level to Persons

Assigning access level to persons can define which persons can get access to which access points during the authorized time period.

7.2.1 Add Access Level

Steps

1. On the top, select **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. **Optional:** Edit the description for the access level.
5. Select the access point type.
6. Select the access point(s).

   In the **Available** list, select the access point(s) and click . You can view your selection in the **Selected** list.

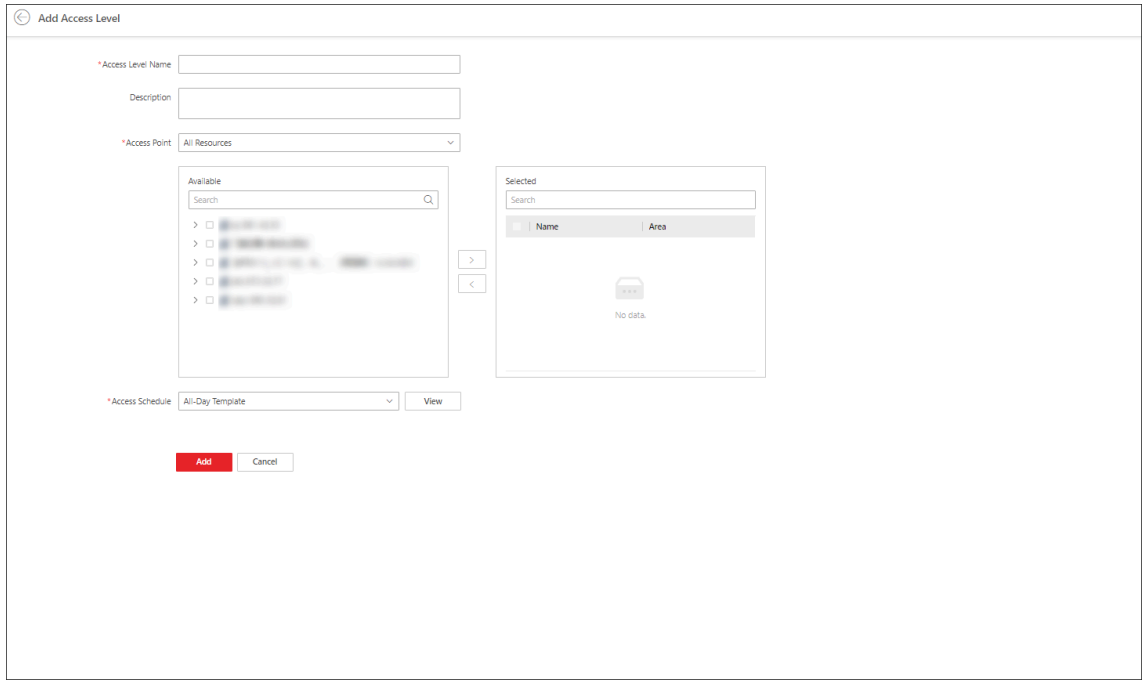


Figure 7-2 Select Access Points

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.

   Note

   All default and custom access schedules are shown in the **Access Schedule** drop-down list. You can click **New Access Schedule Template** to customize a schedule. Or you can predefine access schedule templates. For details, refer to .
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 or click → **Delete All** to delete all access levels..
View Details of Access Schedule or Access Point	Click to view details of access schedules or access points.

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 ***Manually Assign Access Level*** .

7.2.2 Manually 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, department, or access group.

For applying large-scale access levels, go to **Basic Configuration → General → Apply Large-Scale Access Level** . Once enabled, data will be applied to devices in the form of packaged files, which requires high server I/O performance (at least an SSD).

Assign Access Level in Quick Mode

If you need to assign the access level to person(s) quickly, you can use the quick access authorization function.

On the top navigation bar, click → **Quick Access Authorization** .

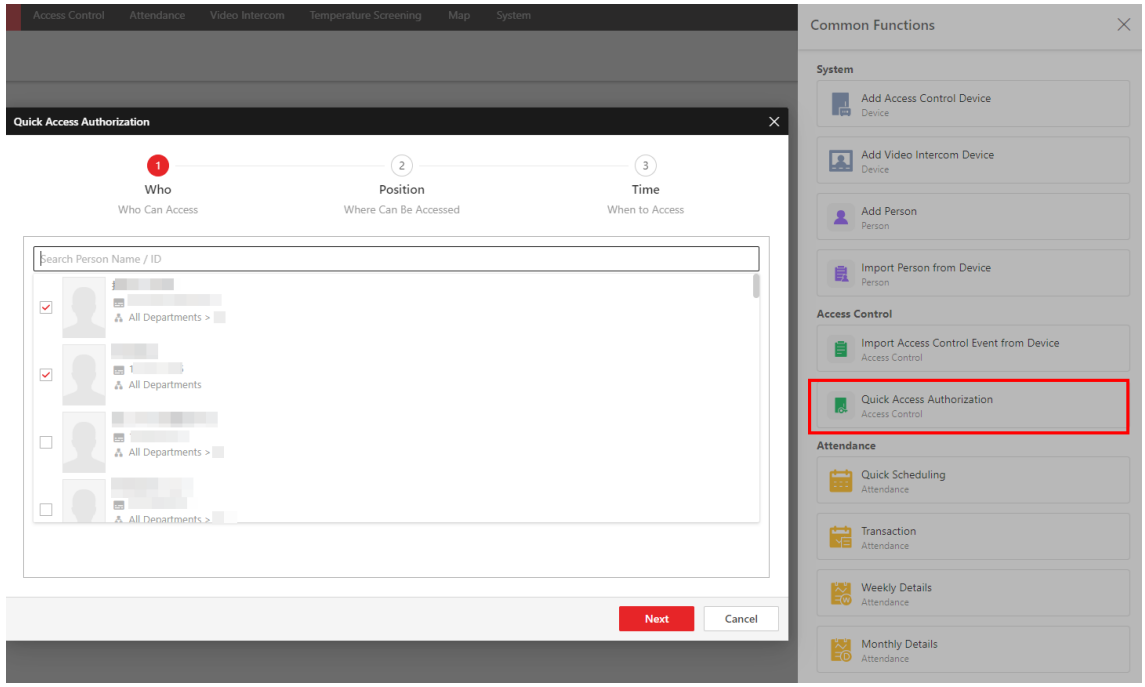


Figure 7-3 Quick Access Authentication

Select persons to assign access levels, doors of which the access level will be assigned, and the access schedule, and then save the settings.

Note

- If the access level is not created before, a new access level will be automatically created and displayed on the page of access level overview in the Access Control module.
- If you click **New Access Schedule Template** when selecting the access schedule, the created access schedule template will be displayed on the Access Schedule Template page.

Assign by Access Level

You can assign an access level to multiple persons so that the assigned persons can have the access to the access points in the access level.

Before You Start

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

Follow the steps to assign an access level to persons.

Steps

1. Select **Assign Access Level** on the left.
2. Click **Assign by Access Level** on the top.

Note

For the first time assignment, click **Add** at the center of the page to enter the assignment page.

3. Click on the access level that you want to assign to persons.
4. On the assignee pane, click **Assign To** to show person list.
5. Select the persons whom you want to assign the access level to and click **Add**.

Note

If you check **Select All**, all persons who matched the search conditions you set will be selected.

The access level settings will be applied to devices automatically.

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. Select **Assign Access Level** on the left.
2. Click **Assign by Person** on the top.
3. Check persons in the list, and click **Assign Access Level** to open the Assign Access Level pane.
4. **Optional:** In the Assign Access Level pane, click to add persons.
5. In the Access Level list, check the access levels that you want to assign to the selected persons.
6. Click **Assign**.

   The access level settings will be applied to devices automatically.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

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 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. Select **Assign Access Level** on the left.
2. **Optional:** For the first time assignment, click **Assign Now** in the center of the page to open the Batch Assign Access Level to Departments page, and then see the second choice in ***3*** .
3. 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 a department.
     b. Click **Assign Access Level** on the top.
     c. In the Assign Access Level pane, select the access levels you want to assign to the selected department.
     d. Click **Assign**.
   - Assign access levels to multiple departments at a time.
     a. Click **Batch Assign** on the upper left.
     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-Departments**.

     c. In access level list, select the access levels you want to assign to the departments.
     d. Click **Save**.

   The access level settings will be applied to devices automatically.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

Assign by Access Group

An access group is the group of persons who have the same access permissions (In a specified time period, they have the permission to access the specified access points). You can add the persons who have the same access permission to the same access group. For example, the employees in the same department should access the company gates during the working hours. The employees can be added to the same access group and be related to the access level which contains the access permission of the company gates. You can assign one or multiple access levels to the access group, and the persons in the access group will get the permission to access all the access points in the access level(s).

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 platform. For details, refer to ***Add Access Level*** .

Steps

1. Select **Assign Access Level** on the left.

2. Click **Assign by Access Group** on the top.

Note

For the first time assignment, click **Assign Access Level** at the center of the page to enter the assignment page.

3. **Optional:** Add access groups.
   1) Click + at the top of the access group list to open the Manage Access Group pane, and then click **Add** to enter the Add Access Group page.

   Note

   If no access group is added to the access group list, click **Add Access Group** in the access group list to enter the Add Access Group page.

   2) In the **Group Name** field, enter the name of the access group.
   3) In the **Group Member** area, click **Add** to open the person list, select the person(s) to be added to the access group.

   Note

   If you check **Select All**, all persons who matched the search conditions you set will be selected.

   4) Click **Add** to add the selected person(s) to the access group.
   5) Click **Add** at the bottom.
4. Check access group(s) to assign access levels to.
5. Click **Assign Access Level** on the top.
6. In the Assign Access Level page, select the access level(s) to be assigned to.
7. Click **Assign**.

   The access level settings will be applied to devices automatically.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

7.2.3 Access Level Overview

The platform provides an overview of all persons' access levels for access points. You can filter persons and perform some operations on their access levels.

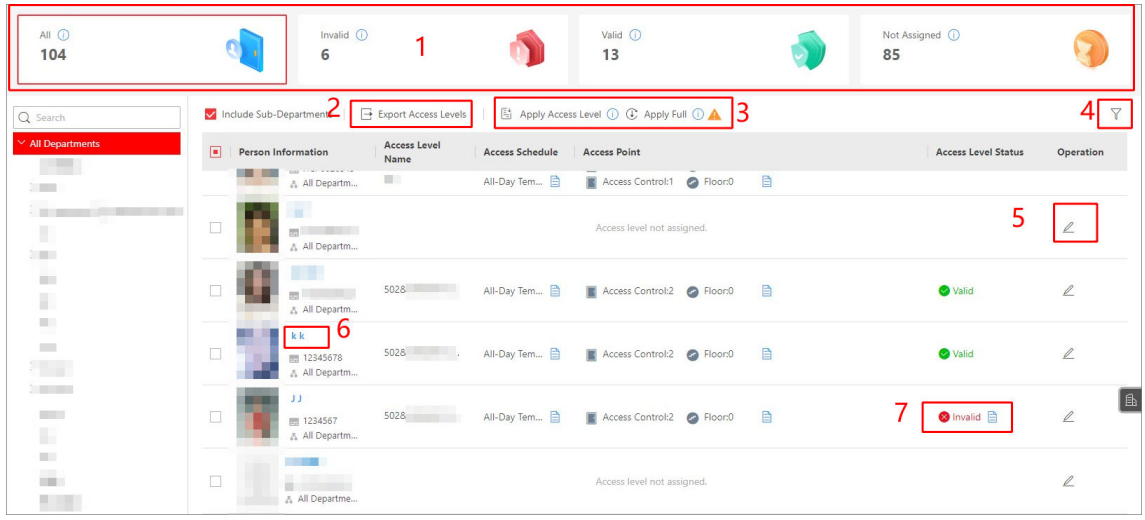


Figure 7-4 Access Level Overview

1	On the top, you can click the cards to display all persons, persons with invalid access levels, persons with valid access levels, or persons not assigned with access levels if needed.
2	Export a list of persons and their access levels in Excel or CSV format.
3	For persons whose access levels failed to be applied, persons with invalid access levels, or persons not assigned with access levels, you can apply access levels for them. You can select access points before applying.
4	Filter persons by different conditions such as person name, ID, access level.
5	Click to edit a persons access levels. You can add or delete access levels.
6	Click a person name to view the person information.
7	If a person's access level failed to be applied, "Invalid" will show in the Access Level Status column. You can click to view the details.

7.2.4 Regularly Apply Access Level Settings to Devices

You can set a schedule to apply the access level settings that failed to be automatically applied to devices.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Manually Assign Access Level*** .

Steps

1. Go to **Basic Configuration → General** .

2. Switch on **Apply to Device (Scheduled)**.
3. Select an applying mode.
   - **Apply at Fixed Time**: Apply the changed access level settings and the settings that failed to be applied last time to devices at a specific time (System Management Server time) on a daily basis. You can select a time in the **Auto-Apply At** drop-down list.
   - **Apply Every Certain Hours**: Apply the changed access level settings and the settings that failed to be applied last time to devices immediately and every certain hours afterward. You can select an interval in the **Time Interval** drop-down list.
4. Click **Save**.

7.2.5 Clear Persons' Access Levels

You can clear the access levels of persons so that they cannot access the access points in the access levels. For example, if there is no access record of certain persons entering or exiting for a long time, the administrator can clear their access levels to make sure the persons' credentials will not be misused.

On the left, select **Assign Access Level**, then select an access level assigning mode on the top.

The unassigning operations vary by different assigning modes.

- On the **Assign by Access Level / Assign By Person** page, select the target person, hover the cursor on ⌄ , and select **Unassign All Access levels** or **Unassign Specified Access Levels**.

Note

For the latter one, if you selected multiple persons, only the common access levels shared by the selected persons can be unassigned.

- On the **Assign by Department / Assign by Access Group** page, check access level(s) and click **Unassign**, or hover the cursor on ⌄ and select **Unassign All**.

Note

- Once cleared, the previous access level settings of the persons cannot be restored. You need to re-assign access levels for them again when needed.
- After the access level settings of the selected persons are cleared , these persons will be removed from the related access groups.
- After the access levels are unassigned, the changes will be automatically applied to devices, and the access level settings of the persons will be deleted from the devices.

7.2.6 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 three default access control schedule templates: All-day Template,

Workday Template, and Weekend Template. You can also add customized templates according to your needs.

Steps

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

   Copy From

   You can select to copy the settings from existing templates.

   Weekly Schedule Template

   Select or draw in the box to define the authorized time periods. After drawing, you can enter a time or adjust the time by clicking the arrows in the box popped up. You can set up to 8 separate time periods for each day.

   Click **Erase** and select or draw on the authorized time periods to clear the selection. If you want to define the authorized time periods again, click **Authorize**.

   Holiday Schedule

   Set a holiday schedule if you want different schedules for specific days. Holiday schedule has a higher priority than weekly schedule.

   a. Click **Add Holiday**.
   b. Select existing holiday templates, or click **Add** to create a new holiday template (see ***Set Holiday*** for details).
   c. Click **Add**.
   d. Set a schedule pattern for holidays.
4. Click **Add** to save the template.
5. **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.

7.3 How to Open the Door by Your Smart Phone

Users can open the door quickly by the Mobile Client or by rotating their phone by the reader. With a specific configuration, they can open the door without logging into the Mobile Client.

Step 1 Add Access Control Devices

First, you need to go to the Device module to add an access control device that supports Bluetooth. See details in ***Add Device(s)*** .
Then, go to the Maintenance page to check the device capability.

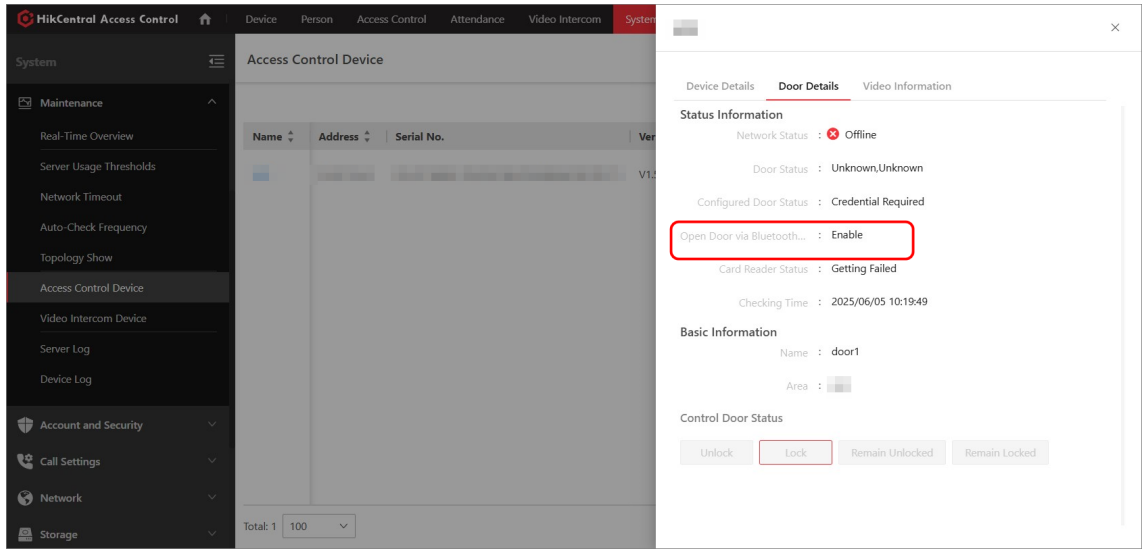


Figure 7-5 Check Device Capability

Step 2 Enable Self-Service Login for the Person

Go to the Person page, click a person name to enter the editing page, and then enable the **Allow Login to Self-Service** for the person. This allows the person to log into the Mobile Client and the Self-Service of Web Client.

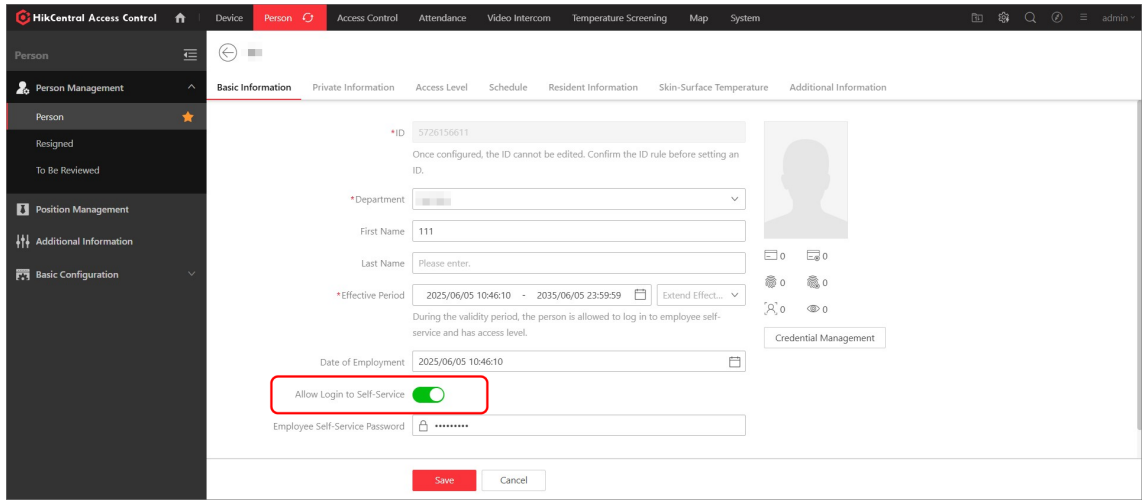


Figure 7-6 Enable Self-Service Login

Go to the Access Level tab, and enable **Open Door via Bluetooth on Mobile Client**.

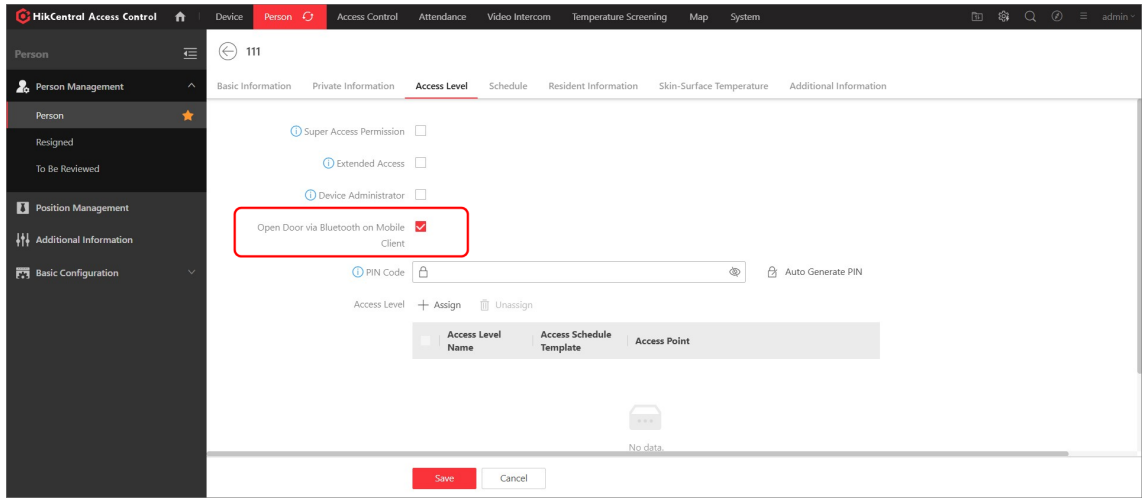


Figure 7-7 Access Level Tab on Person Page

Step 3 Basic Settings in Access Control Module

1. Go back to the Access Control page, create an access level for the door supporting Bluetooth.

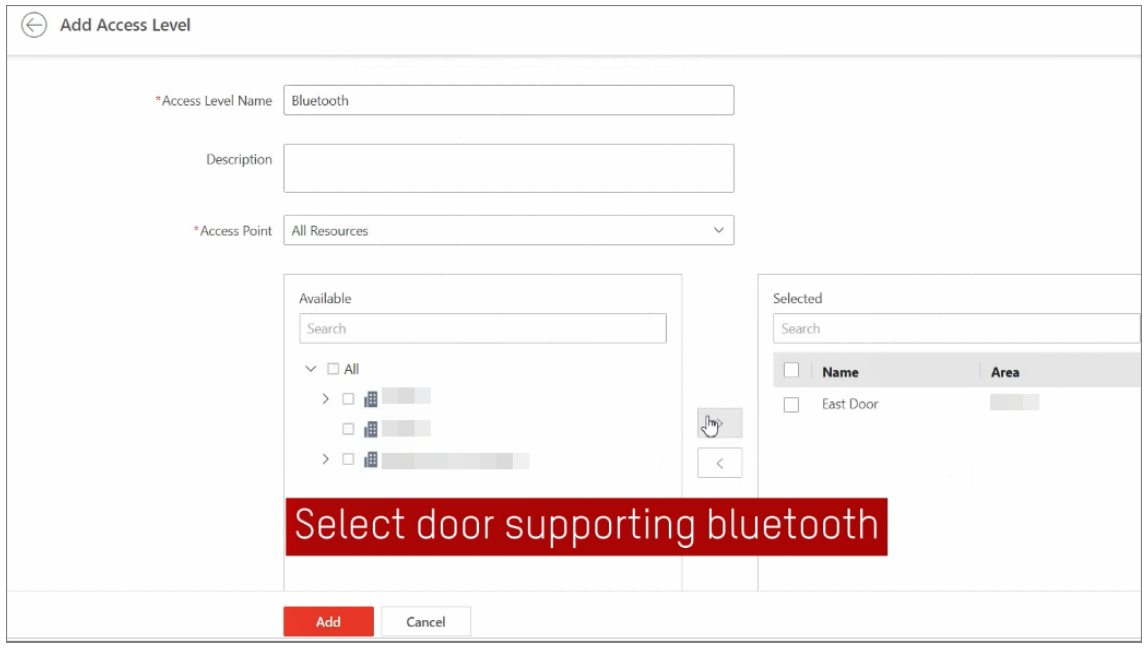


Figure 7-8 Create Access Level

2. Assign the added access level to person(s).

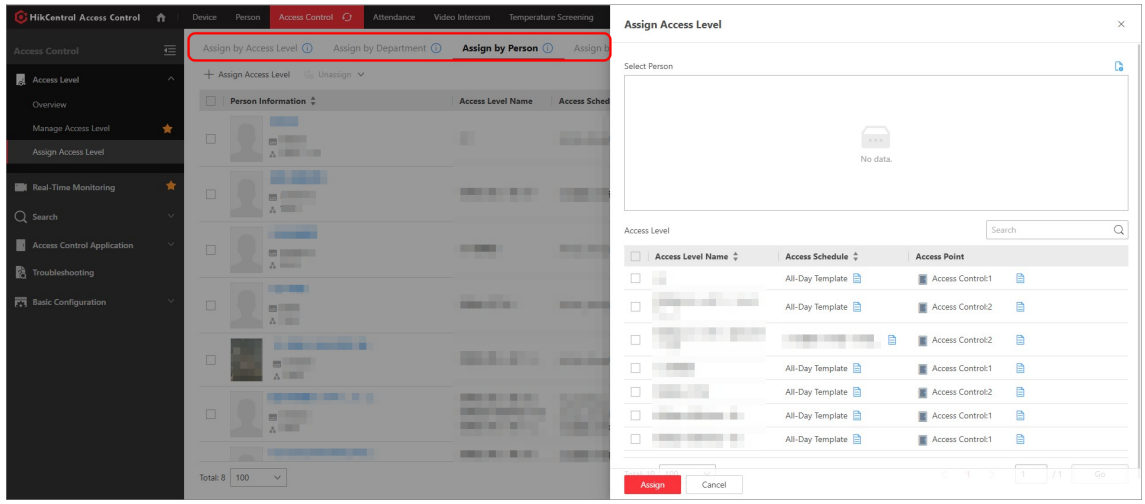


Figure 7-9 Assign Access Level to Person(s)

3. Select **Basic Configuration → General** on the left. In the **Open Door via Bluetooth** area, select the door opening mode.
   (Optional) In the Offline Unlocking area, select the validity of offline unlocking.

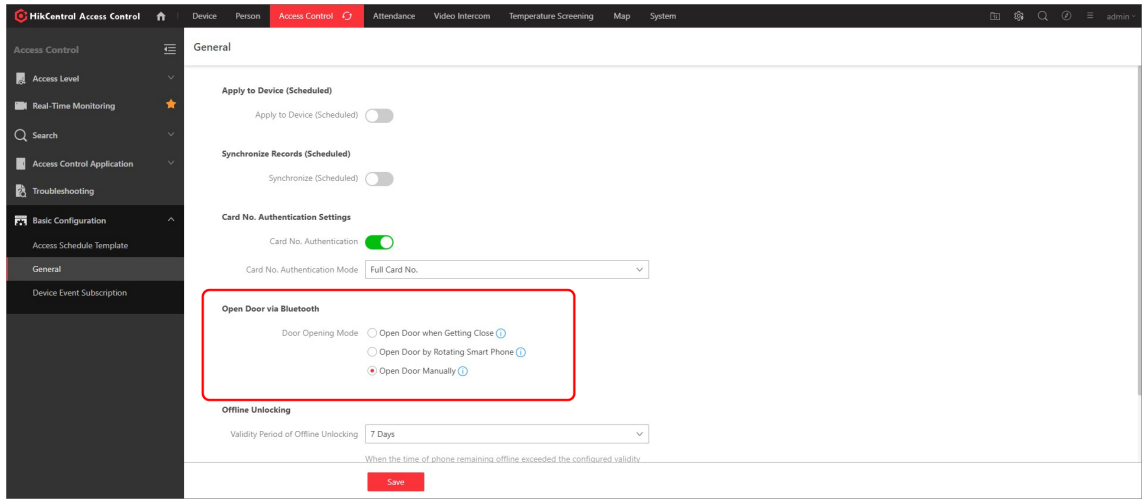


Figure 7-10 Open Door via Bluetooth Settings

Step 4 View Real-Time Events and Search History Access Records

The operation of opening door via smart phone may trigger configured events. You can find the access event in the Real-Time Event area on the Real-Time Monitoring page.
Or click to search for history access records stored on the device.

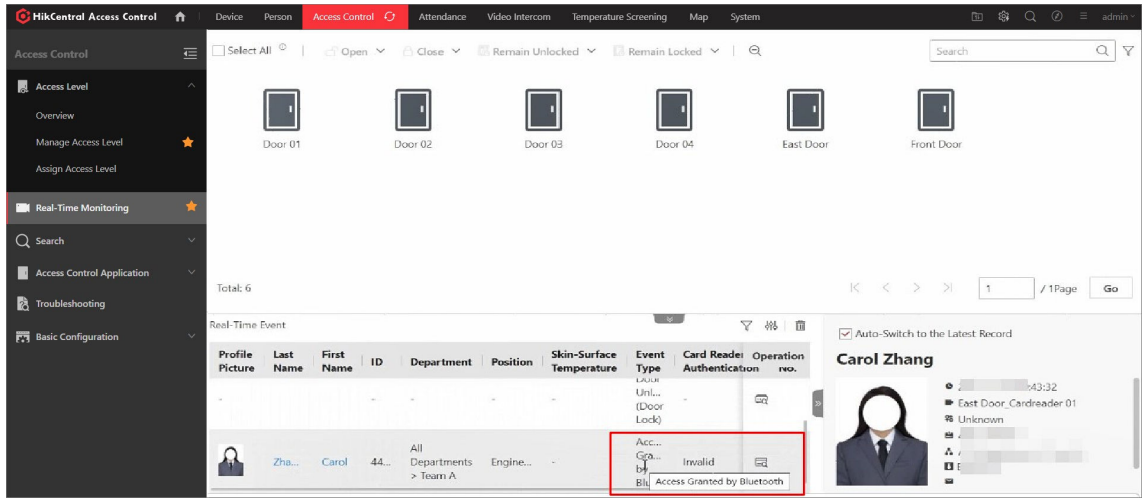


Figure 7-11 View Real-Time Events

7.4 Real Time Monitoring

You can control access point status in a batch when an emergency happens. For example, after grouping the access points of a school's main entrances and exits into one group, school's security personnel can lock down the access points in the group, so that no one can enter or leave the school except for maintenance and high-level admins. This function can also block out teachers, custodians, students, etc.

Note

- Make sure you have grouped access points that need to be batch locked or unlocked. See details in ***Add a Batch Locking and Unlocking Group*** .
- Only the users with Administrator or Operator role can control all access points in a batch.

On the left, select **Real-Time Monitoring**.

You can control all or part of the access points in the area according to your need. When the emergency is over, you can restore the status to Access with Credential.

Start Live View of Access Control Devices

For access control devices with cameras installed inside, you can start live view of these devices.

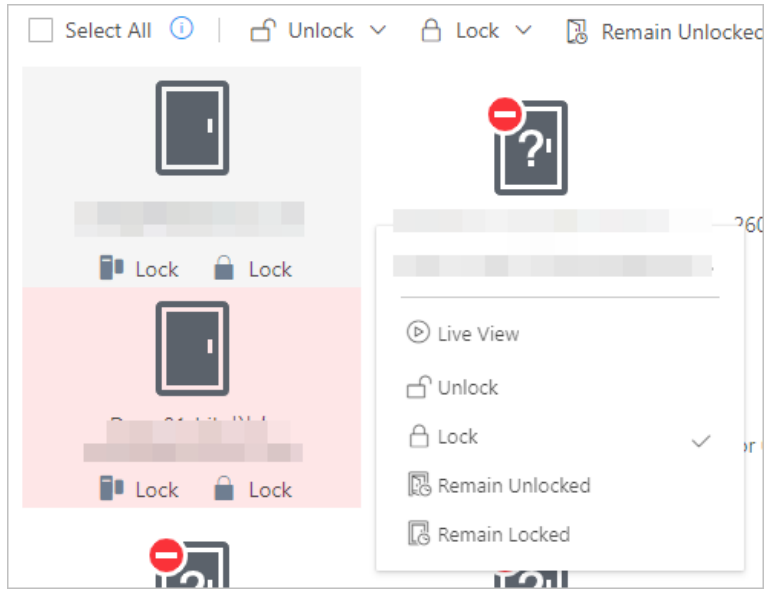


Figure 7-12 Real-Time Monitoring Page

View Real-Time Access Event

In the Access Control module, you can view events triggered by doors.
Make sure you have subscribed to device and access events. Go to **Basic Configuration → Device Event Subscription → Device Event / Normal Access Event / Abnormal Access Event** . Enable the event types you want to subscribe to and disable those you don't need. You can still search for device/access records via the Web Client. See ***Data Search*** .
Select the site and area that you want to view the access events. Real-time access events are displayed at the bottom of the page.

Search for Device Records	Click in the Operation column to go to the Device Recorded Data Retrieval page to search for records by customizing search conditions.
Filter Events	You can filter the real-time events by setting conditions according to record types and event source. Click to set conditions.
Custom Column	Click to customize the columns to be displayed.
Clear Events	Click to clear all events in the list.
View Details of Latest Access Record	On the lower-right corner of this page, check **Auto Update Record** to display the person information contained in the newest access record. If you uncheck the **Auto Update Record**,

	the platform will display the person information contained in the historical access records. The platform supports hiding the window.

Door Control

You can change the status of all doors to locked, unlocked, remaining locked, or remaining unlocked.
Control all or part of the doors.

Unlock

When a door is unlocked, persons can pass the door without any credentials for a certain time period. When open duration is over, the door will be closed and locked again automatically.

Select a door and click **Unlock** to unlock a door or click **Select all** to unlock all doors.

Click **Unlock → ⌄ Unlock Doors in Batch Locking and Unlocking Group** to unlock doors in the batch locking and unlocking group you have added.

Note

For details about setting the door's open duration, see ***Parameters on Edit Door Page*** .

Lock

When the door is locked, persons who has the access permission can access the door with credentials.

Select a door and click **Lock** to lock a door or click **Select all** to lock all doors.

Click **Lock → ⌄ Lock Doors in Batch Locking and Unlocking Group** to lock doors in the batch locking and unlocking group you have added.

Remain Unlocked

Doors will be unlocked. All persons can access the door with no credentials required. This function is used when an emergency happens and all people are required to leave as quickly as possible, such as in a fire escape.

Select a door and click **Remain Unlocked** and the door will remain unlocked. Click **Select all** and all the doors will remain unlocked.

Click **Remain Unlocked → ⌄ Remain Doors Unlocked in Batch Locking and Unlocking Group** and the doors in the batch locking and unlocking group you have added will remain unlocked.

Remain Locked

Door will be closed and locked. No person, except for the users with super access permission, can access the door even with authorized credentials. This function is applicable for situations such as preventing unwanted persons in the building from getting away.

Select a door and click **Remain Locked** and the door will remain locked. Click **Select all** and all the doors will remain locked.

Click **Remain Locked →** ⌄ **Remain Doors Locked in Batch Locking and Unlocking Group** and the doors in the batch locking and unlocking group you have added will remain locked.

7.5 Data Search

On the Search page, you can search for person authentication records, data recorded on devices, and perform final authentication counting.

On the left, select **Search**.

Note

You can go to **Basic Configuration → General → Apply to Device (Scheduled) / Synchronize Records (Scheduled)** to enable the feature of synchronizing access records and device logs to the platform on schedule.

Search Access Records

On the Person Authentication Record page, you can search for persons' authentication records triggered on specified access points by setting search conditions. For example, if you select specific access points and set the event type to access denied by card, you can get all access denied events (accessing by swiping a card) triggered on the access points.

Note

Make sure you have configured the access point event. For details, refer to .

You can import person authentication records to the system from devices or files. Go to **Import Event → Import From Device / Import From File** .

Import From Device

- If the device has uploaded records to the system before, switching on **Specified Time Range** is not required and records during the past 7 days of the selected device(s) will be imported by default if no time range is specified.
- If the device has never uploaded any record to the system before, you must switch on **Specified Time Range** for importing records from the selected device(s).

Import From File

Import from the file which is exported from the device. Only the encrypted file can be imported.

Table 7-1 More Operations

Operation	Description
View Record Details	Click the person name in the Full Name column to view the record details, such as person information, and access information.
Forgive Anti-Passback Violation	When a person attempts to use a card without following the anti-passback rule, the access will be denied. This is called "Anti-Passback Violation". When the anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven. You can click **Forgive Anti-Passback** on the top to forgive all the anti-passback violation events in the search results.
Export Single Record	Click in the Operation column to save a record as an Excel or CSV file on your PC, including the event details, the person information, person profile, recorded video file (if configured), etc.
Export All Searched Records	Click **Export** in the upper-right corner to save the searched record details in your PC. You can select the file format as an Excel, PDF or a CSV file, and select items to export.

Search Data Recorded on Device

The logs can be events/alarms triggered by abnormal events detected by devices and those triggered by devices (such as device faults). You can search for the logs in different dimensions according to your needs.

Access Point(s)

Access points include doors of access control devices and video intercom devices. The logs can be access records, operation records, and alarms triggered by human behaviors.

Device

Devices include access control devices and video intercom devices. The logs recorded in these devices can cover all events triggered by devices (such as device faults).

Alarm Input

The alarm inputs included in devices. The logs are arming status changes.

Table 7-2 More Operations

Operation	Description
View Record Details	Click the device name in the Source column to view the record details, such as the device name and record type.
Export Single Record	Click in the Operation column to save the record to the local PC as a CSV file.
Export All Searched Records	Click **Export** to save all the searched records to the local PC as an Excel, PDF, or a CSV file.

View Final Authentication Statistics

The system can count individuals in a region by grouping doors and using final authentication records. This allows you to see who has been granted access and how many people are still in the area. The function is applicable for certain emergency scene. For example, during a fire escape, all people are required to exit the region.
Make sure you have added final authentication counting groups to group the doors. See ***Add a Final Authentication Counting Group*** .

All Persons

All the entering and exiting access records in the last 24 hours will be listed.

People Stayed

Persons who are still staying in the region will be listed. The system filters the persons whose entering record is found but exiting record is not found.

People Exited

Persons who entered and exited the region afterward will be listed.

Table 7-3 More Operations

Operation	Description
View Event Details	Click the person name in the Name column to view the record details, including person information, and access information.
Export Single Record	Click in the Operation column to download the record, including the person information, person profile, phone number, location of last access, etc.
Export All Searched Records	Click **Export** in the upper-right corner to export the searched access control events details

Operation	Description
	(including the person information, person profile, phone number, location of last access, etc.).

Up to 100,000 records can be exported each time.

7.6 Advanced Functions

7.6.1 Add Remain Unlocked and Remain Locked Rule

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

Steps

Note

This function should be supported by the device.

1. On the left navigation bar, select **Remain Unlocked & Remain Locked**.
2. Click **Add** to enter the Add Remain Unlocked & Remain Locked Rule page.

   For the first-time configuration, click **Configure Now** in the center of the page.
3. Enter the rule name.
4. Select an access point from the following area list.
5. Select weekly schedule for the access point(s).
6. Click **Add**.

   The system will automatically apply the schedule(s) to devices.

7.6.2 Configure First Person In

First Person In refers to a rule where only after the first person is authorized to enter using their card, fingerprint, or face, can other people's permissions be activated. You can set the door opening rule to allow free access after the first person or require authorization by the first person, which is suitable for scenarios such as quick emergency response or personnel access control.

Steps

Note

This function should be supported by the device.

1. Go to **Access Control Application → First Person In → Add** .

For the first time configuration, click **Configure Now** in the center of the page to enter the Add First Person In Rule page.

2. Enter the rule name.
3. Select a door from the resource list.
4. Set **Rule of Opening Door**.
5. Set the consecutive authentication times and the interval of consecutive authentication.
6. **Optional:** Enable **First Person Authentication Time** to set a time when the rule takes effect and a fixed time period requiring first person authentication.
7. In the First Person area, click **Add** to select first person(s).

   If you check **Select All**, all persons who matched the search conditions you set will be selected.
8. Click **Add** to add the rule.

   After adding a rule, you can click the rule name to edit the rule.

7.6.3 Manage Multi-Factor Authentication

Multi-Factor Authentication is an access authentication scheme which requires all the predefined persons to be present and authenticate. It is generally used in places such as bank vault to ensure the security of important assets and data.

On the left, select **Access Control Application → Multi-Factor Authentication** . If any multi-factor authentication rule is added, the multi-factor authentication list will show. You can manage multi-factor groups and users to receive remote door open request. For the first time usage, click **Configure Now** to enter the Add Multi-Factor Authentication Rule page.

Multi-Factor Authentication Group

Persons in the group have the permission for multi-factor authentication of specific doors.

User to Receive Remote Door Open Request

Configure this when the access mode is Remotely Unlock After Granted.

Note

This function should be supported by the device.

Add a Multi-Factor Authentication Rule

Steps

1. On the Multi-Factor Authentication page, click **Add**.
2. Enter the rule name.
3. Select a door from the following area list.
4. In the Access Schedule area, set the time periods in which the persons are allowed to authenticate.

   You can click **Copy From** to copy the access schedule of another rule.

5. Click **Link to Group** to set the access group(s) to define who have the permission to access the door.

   For the first-time configuration, click **Add Group** to create a multi-factor authentication group by selecting persons as the group members.

   Card Swiping Order

   Click ↑ or ↓ in the **Operation** column to set the authentication order of different access groups.

   Number of Persons for Authentication

   Define how many persons should authenticate.

   For example, if you set 3 for access group Security Guard and 1 for access group Bank Manager, it means three security guards should swipe cards on the card reader (or other access mode), and one bank manager should swipe card on the card reader (or other access mode) for this multi-factor authentication.
6. Set the access mode of the door.

   Unlock After Access Granted

   The door will be unlocked automatically after the persons swipe their cards (or other type of credentials) on the card readers of the door and the access is granted.

   Remotely Unlock After Granted

   After the persons authenticate, a window will pop up for the operator. The operator should select whether to unlock the door.

   Unlock by Super Password When Offline

   If the user to receive remote door open request is offline, the persons in the multi-factor authentication group can enter the super password.

   Enter Super Password After Granted

   After the persons swipe their cards (or other type of credentials) on the card readers of the door and the access is granted, they should enter the super password on the card reader. After that, the door will be unlocked successfully.
7. Set the card swiping interval and make sure the interval between two authentications on the card reader is within this value.

   Example

   When you set the interval as 5s, if the interval between two authentications is longer than 5s, the authentications will be invalid, and you should authenticate again from the beginning.
8. Click **Add**.
9. **Optional:** If you select **Remotely Unlock After Granted** as the access mode, click **User to Receive Remote Door Open Request** above the multi-factor authentication list to add users who are going to receive the request.

7.6.4 Configure Multi-Door Interlocking

Multi-door interlocking is used to control the entry of persons to a secure area such as a clean room, where dust or small particles may cause a major issue. One multi-door interlocking group is composed of at least two doors and only one door can be opened simultaneously.

Before You Start

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. Go to **Access Control Application → Multi-Door Interlocking → Add** .

   For the first time configuration, click **Configure Now** in the center of the page.
2. Create a name for the group.
3. Select doors and click .
4. Click **Add**.

   After adding a group, you can click **Set Geographic Location** to view the real-time alarms triggered in the region. For details, see ***Add Geographic Area to Map*** .

7.6.5 Anti-Passback

The anti-passback is designed to minimize the misuse or fraudulent use of access credentials such as passing back the card to an unauthorized person, or tailed access. Only one person can pass the access point after authentication. This function is mainly used for enhanced access security of some important or specific places (e.g., laboratories, offices).

You can configure area anti-passback rules or route anti-passback rules for different scenarios. Go to **Access Control Application → Anti-Passback → Area Aniti-Passback / Route Anti-Passback** .

Area Anti-Passback

A person with an entry record must also have an exit record to re-enter or exit the area. The area anti-passback function creates a specific door group. For example, when a person enters the area by swiping a card, they must exit through a door in the same group. If they exit without swiping at a door in the group, they cannot re-enter through any door in the group.

Make sure you have added the access points to different areas. For details, refer to ***Add Element to Area*** .

Table 7-4 Key Parameter Description

Step	Description
1	**Control Anti-Passback by Device** Control anti-passback by selecting specific doors through which people are allowed to enter and exit.

Step	Description
	Suitable for general environments. For example, a small office building with a few entry and exit points, where the security system needs to ensure that employees enter and exit through designated doors. **Control Anti-Passback by Platform** Control anti-passback by the rules set by the platform. By setting a rule that requires specified personnel to enter and exit through the same door during fixed time periods, you can ensure that only authorized personnel access these areas during the specified times. For example, from 8 PM to 6 AM every day, only specific on-duty personnel can enter and exit the data center, and they must do so through the same door. If you select this option, check **Enable Rule Now**. In the **Rule Configuration** step, you can: • Select persons who should enter and exit through the same door. • Select doors through which people are allowed to enter and exit. • Specify the times during the week when people should follow the entry and exit order.
3	**Anti-Passback Violation** When a person attempts to use a card without following the rule, the access will be denied. When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven. **Forgive Anti-Passback Violation Regularly** Set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday. **Non Anti-Passback Period** Set a fixed time during which persons can access the area without following the rule. This function should be supported by the device.

Route Anti-Passback

Persons must authenticate through a configured sequence of doors in one direction. The route anti-passback depends on the card swiping route. Set up a card reader sequence for access control, defining initial and subsequent card readers to enforce anti-passback based on stored entry and exit data.

Table 7-5 Key Parameter Description

Step	Description
1	**Control Anti-Passback by Device** Control anti-passback by setting the card reading order people should follow for entry and exit. Suitable for general environments. For example, you need to ensure that employees enter and exit through designated route from Card Reader 1 to Card Reader 2. **Control Anti-Passback by Platform** Control anti-passback by the rules set by the platform. By setting a rule that requires specified personnel to enter and exit in a specific order during fixed time periods, you can ensure that only authorized personnel enter and exit these areas in the correct sequence during the specified times. For example, during an event, staff must enter and exit the event area through multiple doors in a specified order, ensuring the safety and order of the event. If you select this option, check **Enable Rule Now**. In the **Rule Configuration** step, you can: • Select persons who should enter and exit through the same door. • Set the order that people follow for entry and exit. • Specify the times during the week when people should follow the entry and exit order.
3	**First Card Reader** Set the first card reader in the route to the first card reader. If you violate the route anti-passback rule, you should swipe the card again from the first card reader. **Forgive Anti-Passback Violation Regularly** Set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday. **Non Anti-Passback Period** Set a fixed time during which persons can access the area without following the rule. This function should be supported by the device.

Perform the following operations after adding an anti-passback group to the area.

Edit Anti-Passback Group	Click the group name to edit the anti-passback group settings.

	You can edit the name of the group, add or delete doors in the group, change the settings of forgiving anti-passback violation regularly, and edit the locations of the group and doors on the map.
Set/Cancel Forgiving Anti-Passback Regularly	Select the group(s), click **Set Forgiving Anti-Passback Regularly**, and specify a fixed time so that the platform can automatically forgive the anti-passback violations occurred in the selected anti-passback group(s) at that time everyday. You can also select the group(s) and click **Cancel Forgiving Anti-Passback Regularly** to cancel the settings of the selected group(s).

7.6.6 Add a Batch Locking and Unlocking Group

The batch locking and unlocking group is a group for access points which need to be controlled in a batch. You can add doors of access control devices, doors of video intercom devices to the group.

Before You Start
Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

Steps
1. Go to **Access Control Application → Batch Locking and Unlocking Group → Add** .
   For the first time configuration, click **Configure Now** in the center of the page.
2. Create a name for the group.
3. In the Access Point area, select the access points and click › to add them to the group.
4. Click **Save**.

7.6.7 Add a Final Authentication Counting Group

The final authentication counting group is used to group the access points in a certain area. You can set certain access points as the region edge. Only the number of persons accessing these access points are counted. By grouping these access points, the platform provides counting functions based on the entry and exit records on these access points. With this function, you can know who enters/exits this region and how many persons still stay in this region. This is applicable for certain emergency scenes. For example, during a fire escape, the number of the remaining/ stayed-in persons and name list are required for rescue.

Before You Start
Add the access points into different areas. For details, refer to ***Add Element to Area*** .

Steps

1. Go to **Access Control Application → Final Authentication Counting Group → Add** .
   For the first time configuration, click **Configure Now** in the center of the page.
2. Create a name for the group.
3. Click **Add** and select doors from the area list.
4. Set the entering or exiting direction of the card readers of the selected access points.
5. Click **Save**.
   After adding a group, you can click **Set Geographic Location** to view the real-time number of people entered, exited or stayed in the region. For details, see ***Add Geographic Area to Map*** .

7.6.8 Configure Authentication Mode

The authentication mode is used to determine whether a person has the permission to pass the access point by using single or multiple authentication modes (e.g., employee ID, face, fingerprint, password, PIN code, or a combination of them). You can set the reader authentication mode for access points or set the private authentication mode for persons. If a device has been configured with different authentication modes by two methods, the person's private authentication mode has higher priority than the reader authentication mode.

Set Reader Authentication Mode

You can set the reader authentication mode to employee ID, password, face, fingerprint, PIN code, or a combination of them in normal time periods or custom time periods according to your actual need.

Before You Start

Make sure you have added doors to the area. See ***Add Element to Area*** for details.

Steps

Note

This function should be supported by the device.

1. Go to **Access Control Application → Authentication Mode → Card Reader Authentication Mode** .
2. Select an area from the area list, and doors in that area will be displayed on the right.
3. Click a door name on the right.
4. Select the Card Reader Authentication Mode Settings.

   Batch

   Set the same reader authentication mode for all the readers of a door.

   Single

If you want to set different reader authentication modes for different readers, select this mode.

5. Select the Card Reader Authentication Mode.

Reader Authentication Mode

Set the reader's authentication mode in normal time periods. For example, if you select **Card**, persons on the platform should open the door by swiping the card for authentication each time.

Reader Authentication Mode (Custom)

When you want persons on the platform to open the door via another authentication mode in some special time periods, you need to set the reader's authentication mode and select the custom time period. For example, if you select **Fingerprint** and **Weekend Template**, persons on the platform should open the door via fingerprint at weekends.

6. **Optional:** Click **Copy To** in the upper-right corner to apply the settings to other doors.
7. Click **Save**.

Set Person Private Authentication Mode

You can set private authentication methods (such as card, fingerprint, etc.) for different persons. The person's private authentication mode has higher priority than the existing authentication mode of the device. This is suitable for the following two scenarios, allowing for more flexible and secure personnel management: different persons can use different authentication modes for accessing the same access point and a person can use different authentication modes for accessing different access points.

Steps

1. Go to **Access Control Application → Authentication Mode → Private Authentication Mode** .
2. Select a department from the left list.

   All persons in the department will be listed on the right panel.
3. Click in the Operation column to open the Authentication Device pane.
4. Click **Add**, check the device(s) from the list, and select the authentication mode from the drop-down list for the selected device(s).
5. Click **OK** to add the device(s) for authentication for the person.
6. **Optional:** Perform one of the following operations to edit the authentication mode(s) for the device(s).
   - Select an authentication mode from the Authentication Mode drop-down list to configure the authentication mode for each device.
   - Click **Batch Configuration**, select an authentication mode from the drop-down list, and click **Save** to configure the same authentication mode for all added devices.
7. **Optional:** In the Private Authentication Mode page, click in the Operation column, select the person(s), and click **OK** to copy the person's private authentication mode settings to another person or other persons.

Result

The number of devices added for each person is displayed in the Device for Authentication column. You can click beside the number to view names and authentication modes of all devices.

7.6.9 Apply Advertisement to Access Control Devices

You can add picture(s), video(s), and text(s) in the advertisements, then apply the advertisements to access control devices. After applying advertisements, you can filter or delete them.

Steps

1. Go to **Access Control Application → Apply Advertisement → Apply Advertisement** .
2. Select the available door station in the left list and click to add it to the right list. You can click to remove it from the selected door station list on the left.
3. Add materials (picture, video, or text) for an advertisement to be applied to access control devices.

Note

- The material type (picture, video, or text) should be supported by devices.
- You can check two types of advertisement materials at the same. For example, you can check both picture and video at the same time, excluding text.
- You can add up to 8 videos and pictures, or 3 texts at one time.

- a. Click **Picture →** to add picture(s) for an advertisement.
  b. Set the duration for pictures switching interval.
  c. Set the time period to play the added picture(s).

  Note

  Up to 2 time periods are allowed. You can click **Add** to add the time period if needed.

- a. Click **Video →** to add a video for an advertisement.
  b. Set the duration for videos switching interval.
  c. Set the time period to play the added video.

  a. Click **Text →** to add a text for an advertisement.
  b. Set the advertisement texts, including uploading the background picture, setting the text title/font size/color, and selecting the layout style.
  c. Set the time period to play the added texts.

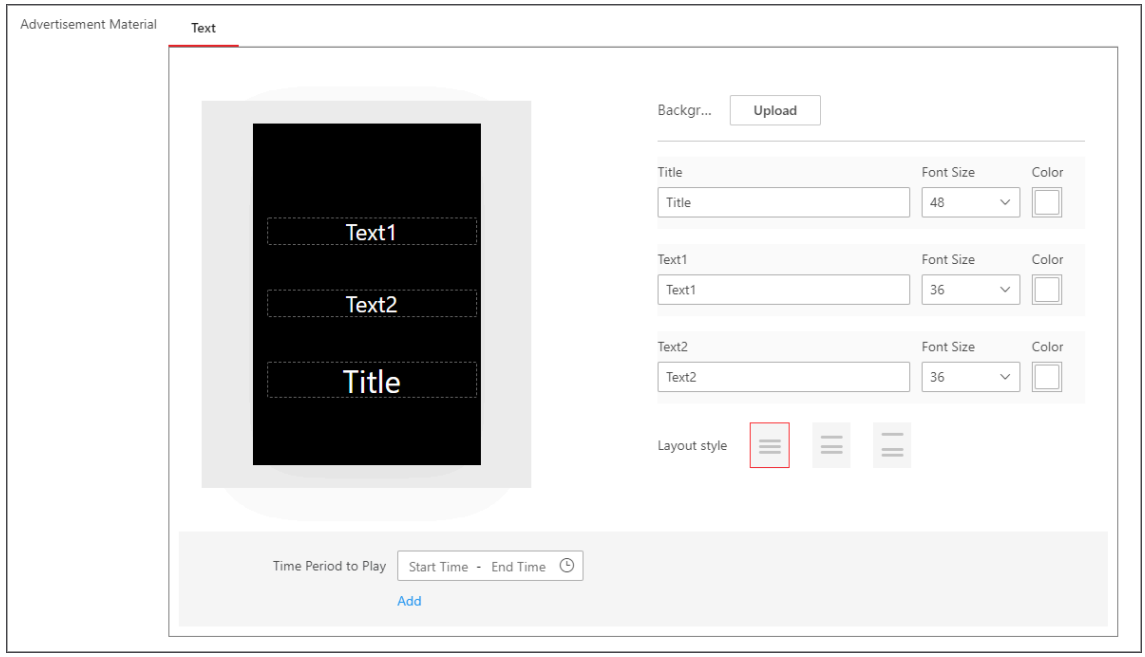


Figure 7-13 Add Text in Advertisement

4. The playing schedules set for the picture(s), video(s), and text(s) in the advertisement will be displayed by different color blocks.
5. Switch on **Sleep**, and set the sleep duration (from 20 to 60 seconds). For example, if you set the sleep duration to 20 seconds with three videos added, each video played will be followed by a 20-second pause.
6. Click **Apply**.
7. **Optional:** Perform the following operations.

Filter Advertisement	Click and set filter conditions such as device name, and then click **Filter** to filter the target advertisement.
Delete Advertisement	Select one or multiple advertisements in the list and click **Clear Advertisements** to delete the advertisements. Also, you can click **Delete All** to delete all of the advertisements.
Copy Advertisement	Select one advertisement in the list, click in the operation column to copy the current advertisement to other devices.
View Details	Select one advertisement in the list, click to view the details of applying progress.

7.6.10 Add Audio Broadcast

You can add daily audio broadcasts for regular use and particular broadcasts for holidays or special days after the authentication of persons. These broadcasts of the devices can be tailored to meet

providing routine, holiday, or special date announcements (e.g. broadcast **Access Granted** when the authentication result is **When Access Granted**. After creating the broadcasts, you can apply them to the selected devices.

Steps

1. Go to **Access Control Application → Audio Broadcast → Add Audio Broadcast** .
2. Select the broadcast device(s).
3. Enable the daily broadcast. Audio broadcasts will be played according to the specified timetable on days without particular broadcasts.

   Note

   For the two types of authentication result, 4 time periods in total can be added.

   1) **Optional:** Enable **Broadcast Address** to select the broadcast address type.
   2) Set the broadcast time and content.
      - Click **Add** to add new broadcast time and content.
      - Click to create a copy and set the time and content based on the existing one.
4. In the Particular Broadcast area, click **Add** to add particular broadcasts. Audio broadcasts will be played according to the specified timetable on holiday or specified dates.

   Note

   For the two types of authentication result, 4 time periods in total can be added.

   1) Select the particular day type.
   2) Select the holidays(s) or select the specified day(s).

      Note

      - If the specified days overlap the holidays, the broadcasts for specified days will be played.
      - Click **Add** to add new holidays. For details, refer to ***Set Holiday*** .

   3) **Optional:** Enable **Broadcast Address** to select the broadcast address type.
   4) Set the broadcast time and content.
      - Click **Add** to add new broadcast time and content.
      - Click to create a copy and set the time and content based on the existing one.
   5) Click **Save**.
5. Click **Add**.

   The settings will be applied to the selected device(s).
6. **Optional:** After applying, perform the following operations as needed.

View Device Details	Click the device name to view the broadcast details of the device. You can also edit the broadcast settings to apply for another time.
View Broadcast Details	Click to view broadcast details.

Copy Broadcast Settings to Other Devices	In the operation column, click to select the device(s) to copy to. Click **Copy** and the settings will be applied to the selected device(s).
Apply Failed Broadcast to Device	• At the top of the broadcast list page, click **Details** to view failure details or click **Apply Again**. • In the Operation column, click to apply again.
Delete Broadcast of Device	Check the device(s) and click **Delete** to delete the broadcast(s) of the selected device(s). You can also click → **Delete All** to delete the broadcasts of all devices.

7.6.11 Add an Authentication Password

You can set an authentication password for a person so that they can access the devices by entering the authentication password. This ensures that only authorized personnel can enter specific areas, such as offices and warehouses, or that strict access control is implemented for certain areas.

Before You Start

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. Go to **Access Control Application → Authentication Password → Add** .
2. If there are cards without PIN, select **Auto Generate** or **Enter Manually** to automatically generate or enter an authentication password manually.

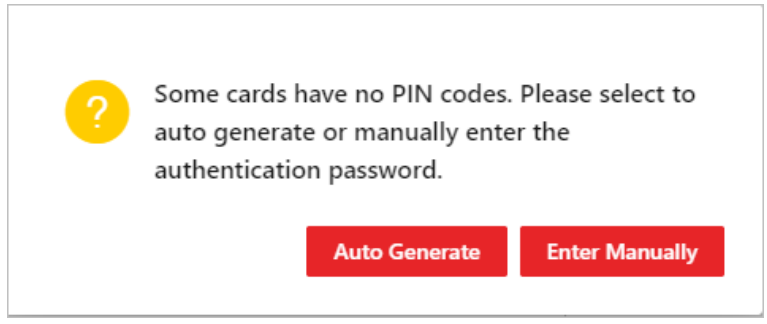


Figure 7-14 The Prompt

3. **Optional:** Enter the authentication password for persons whose authentication password is empty, or check persons and then click **Auto Generate Authentication Password**.
4. Select devices in the following list.

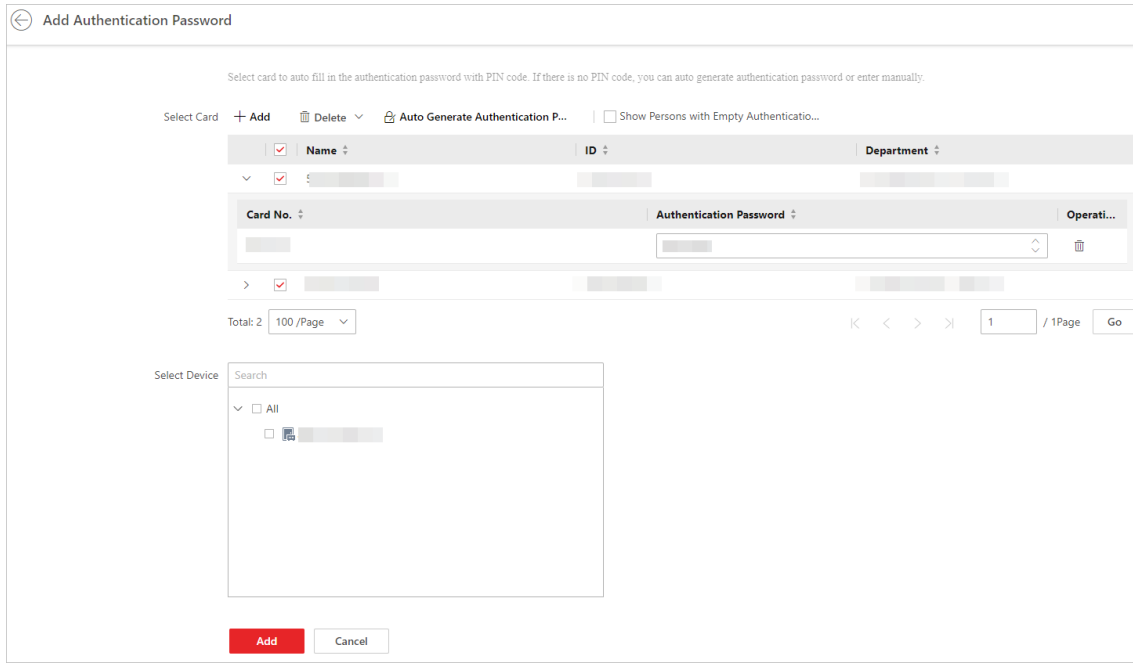


Figure 7-15 Add Authentication Password Page

5. Click **Add**.

   The platform will automatically apply the authentication passwords to the selected devices, and the applying progress will be displayed.
6. **Optional:** Check persons and click **Batch Edit Linked Devices** to batch add or delete devices they can access via authentication password.

7.7 Access Control Test

HikCentral Access Control provides **Access Control Test**. It is a tool through which you can test whether the configurations about access control (such as persons' credentials and access levels for access control and video intercom) are set correctly and completely and whether the devices are running properly.

On the top, select **Access Control**. Select **Troubleshooting** on the left.

Check Credential Status

Select the **Credential Status** tab to view the status of the added credentials.

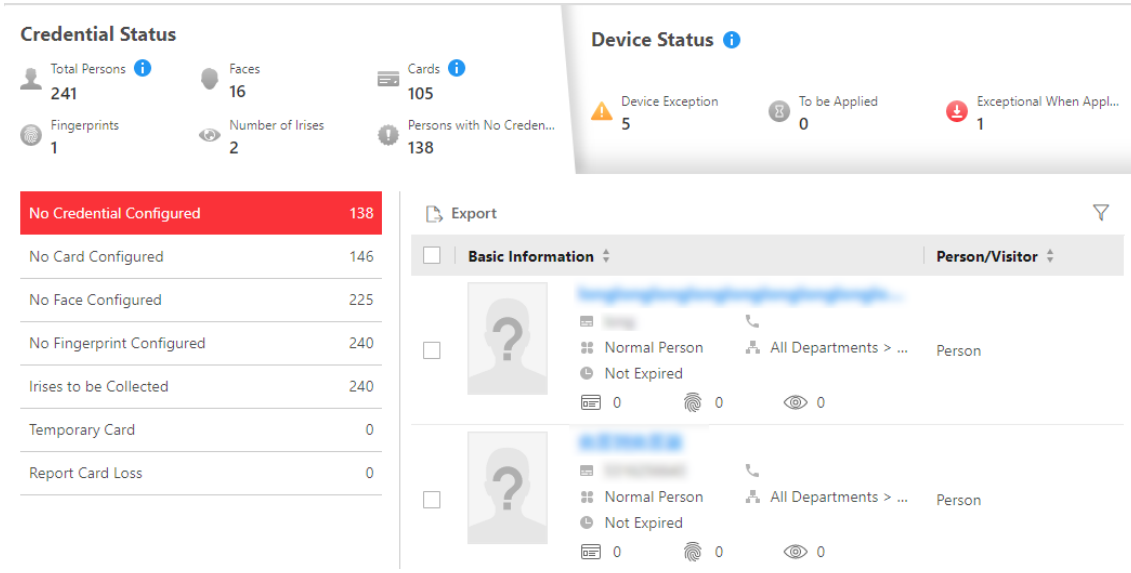


Figure 7-16 Credential Status

There are 6 types of exceptions on credential settings in the system. The number next to each exception type indicates the number of persons whose credential settings are abnormal.
Click each exception type to view the information about the persons with exceptions.
You can click the person's name to edit the credentials if necessary.

Check Device Status

Select the **Device Status** tab to view the status of the devices (including access control devices and video intercom devices). You can check person information and credential information that are already applied to the devices, configured in the system, fails to be applied, and check information of persons to be applied to the devices.

Note

Only the status of the devices which have been configured with access levels are shown.

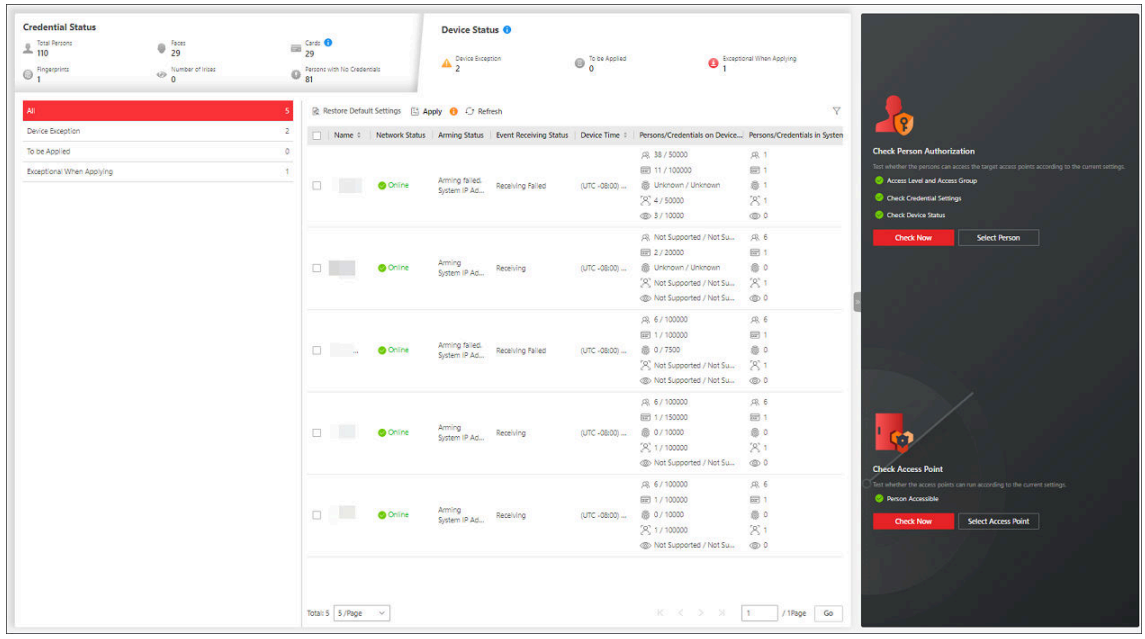


Figure 7-17 Device Status

Click each exception type to view the information about the persons with exceptions.
You can select the devices and click the following buttons to solve device issues.

Restore Default Settings	Restore the settings on the devices to the default value.
Apply	Apply person information and credential settings to these devices again.
Refresh	Refresh the list to get the latest device status.

Check Authorization Settings of Persons

You can check the authorization settings (such as access levels and access group settings, credential settings, and applying status) of specific persons in the system. This function helps you to test whether the persons can access the target access points according to the current settings.

Click  to expand the side panel.

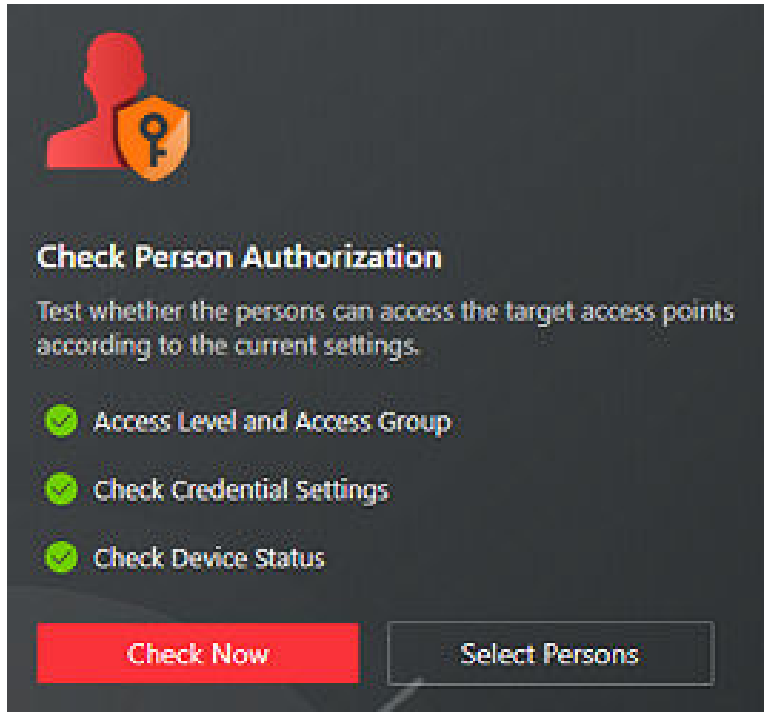


Figure 7-18 Check Authorization Settings

In the **Check Person Authorization** section, select the item(s) you want to check.
Click **Check Now** to test the authorization settings of all existing persons.
Or click **Select Persons** to select the persons you want to test and then click **Check Now** to test the authorization settings of the selected persons.

Note

When selecting persons, if you check **Select All Persons**, all persons will be selected.

Check Access Point Settings

You can test whether the persons can access the access points according to the settings in the system.

Click « to expand the side panel.

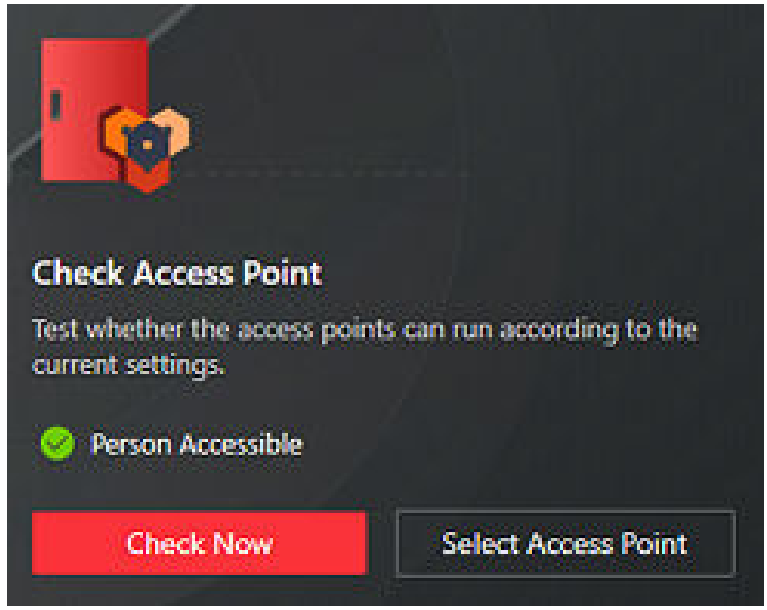


Figure 7-19 Check Access Point Settings

In the **Check Access Point** section, select the item(s) you want to check.
Click **Check Now** to test the settings of all existing access points in the system.
Or click **Select Access Points** to select the access points you want to test and then click **Check Now** to test the settings of the selected access points.

Note

The access points which are not added to any access levels will not be checked.

Chapter 8 Attendance

In the Attendance module, you can easily manage the time & attendance system of your department and check your employees' attendance.

On the top, select **Attendance** .

On the Home page, you can view the attendance report, attendance status statistics, and overall work hours / overtime.

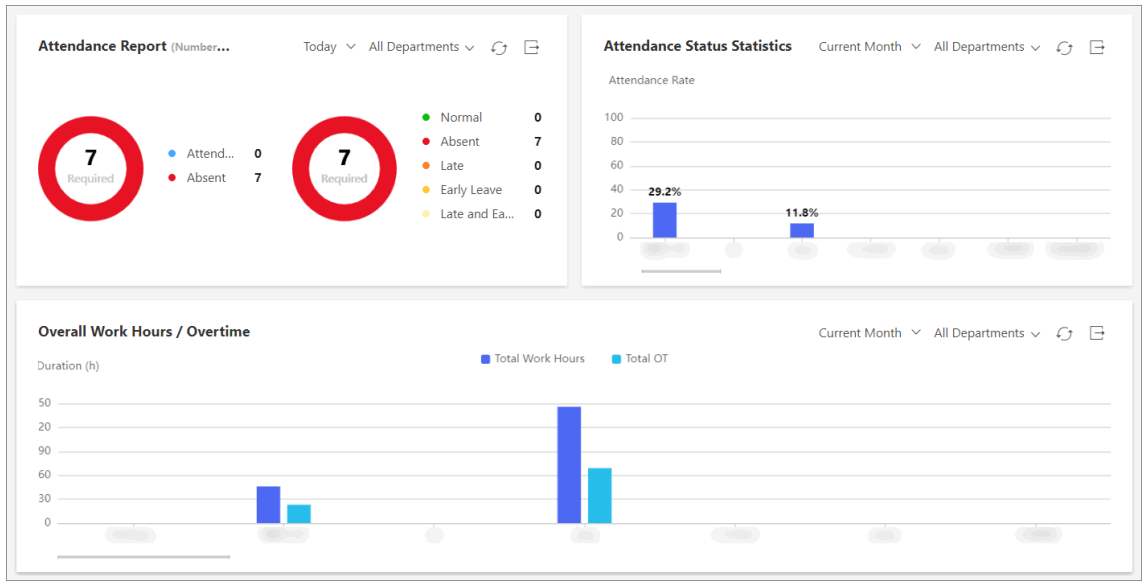


Figure 8-1 Attendance Charts

To set up a time & attendance system from the start, click **Expand Quick Configuration → Get Started** and follow the instructions on screen.

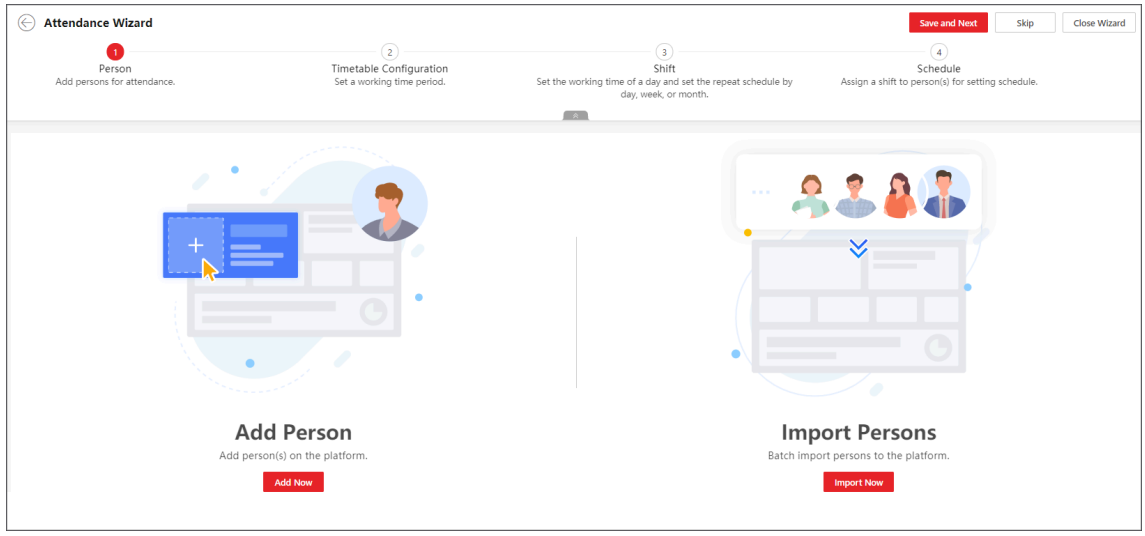


Figure 8-2 Attendance Wizard

1. **Person**: Add persons for attendance. For more details, refer to ***Add Departments*** and ***Add Person*** .
2. **Timetable Configuration**: Set a working time period. For more details, refer to ***Add Timetable*** .
3. **Shift**: Set the working time of a day and set the repeat schedule by day, week, or month. For more details, refer to ***Add Shift*** .
4. **Schedule**: Assign a shift to persons and set schedules. For more details, refer to ***Manage Schedule*** .

Note

You can click to on the right to browse through all steps.

8.1 Flow Chart of Time and Attendance

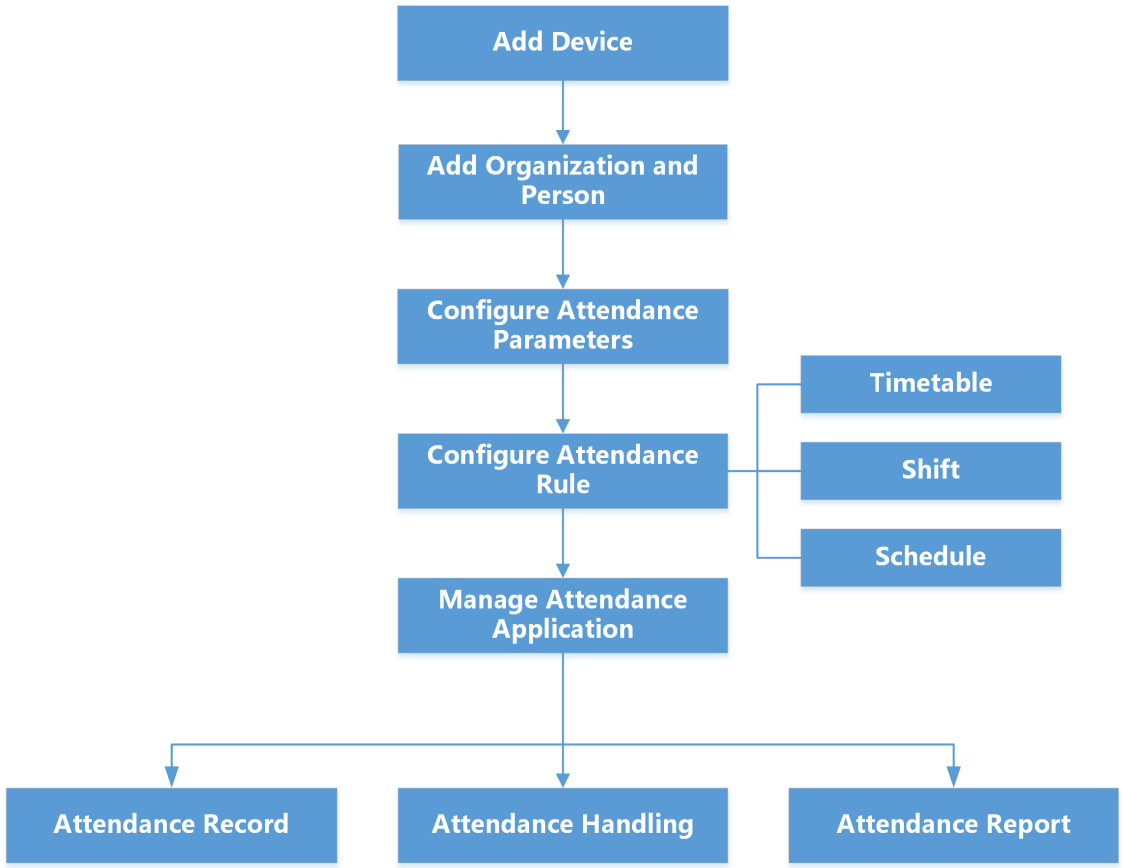


Figure 8-3 Flow Chart of Time & Attendance

8.2 Configure Attendance Mode

Professional Mode provides full functional modules, while Lite Mode offers a more streamlined set of features tailored for simplified scenarios. If Lite Mode meets your attendance check requirements, it is recommended for use. For new users, Lite Mode will be provided by default.

The differences between the two modes are as follows:

Table 8-1 Mode Differences

Function	Lite Mode	Professional Mode
Rule	Support global rule.	Support global rule, department rule, and attendance group rule.
Schedule	Support scheduling shift by department and person, and provide temporary schedule.	Support scheduling shift by department, person, and attendance group, and provide temporary schedule.
Check-In/Out via Mobile Client	/	Supported
Attendance Application	Submitted by admin.	Submitted by employee.
Application and Approval	Support automatic approval and allows the approval to be withdrawn.	Support approving or rejecting the application by reviewers.
Approval Flow	/	Support custom reviewers and review processes.
Attendance Report	Types: 9	Types: 32
Custom Attendance Report	/	Supported
Others	/	Support custom leave rules, report settings, attendance check points, and storage settings.

Note

- Only administrators are allowed to switch modes. Switching between modes won't affect existing data.
- When switching modes, all users logged in through management mode or self-service mode will be automatically logged out.
- Switching from professional mode to simple mode is not allowed when attendance approvals are in progress.

8.3 Add an Attendance Group

For situations where users need to set exclusive attendance rules for specified employees, users can add the employees to an attendance group configured with attendance rules different from and prior to that of a department.

Before You Start

Make sure you have added the employees to the platform.

Steps

1. On the top. select **Attendance → Attendance Group** .
2. Click **Add**.
3. On the Add Attendance Group pane, enter a name of the group.

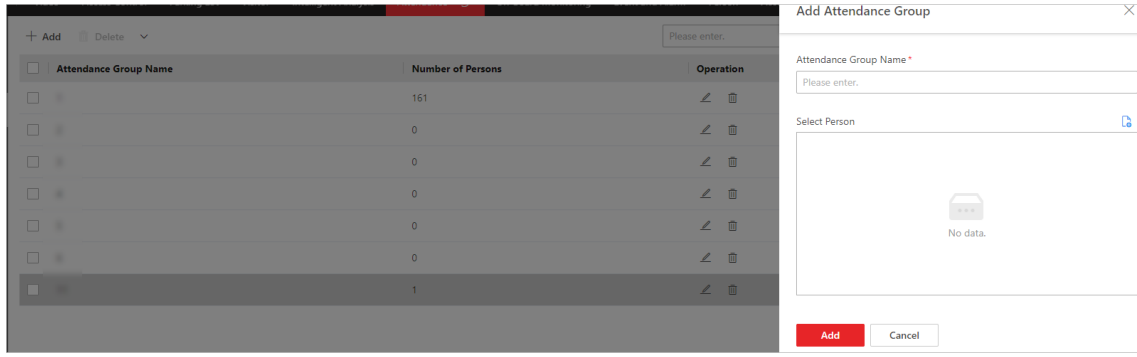


Figure 8-4 Add Attendance Group

4. Click and check persons in different departments, and click **Add** to save the selections.

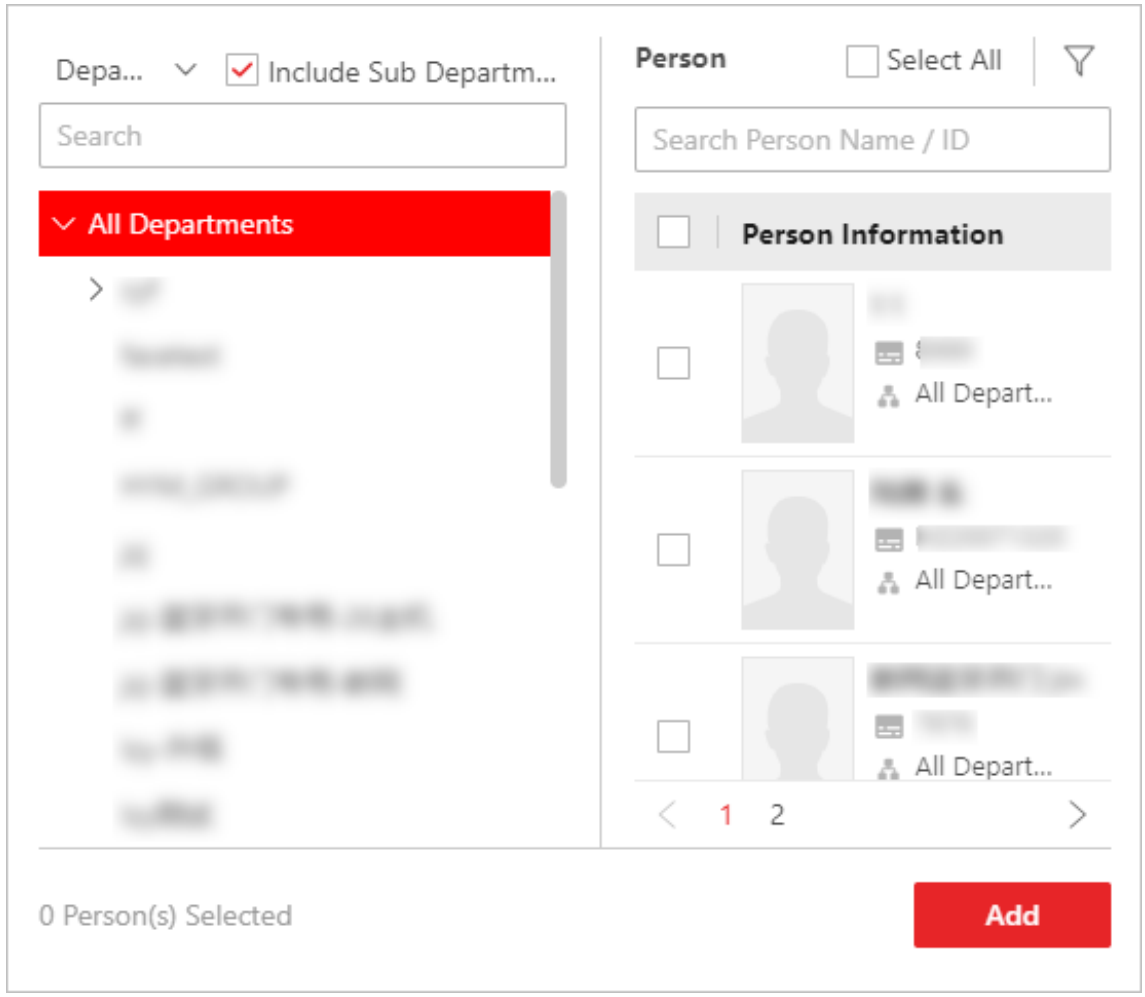


Figure 8-5 Add Persons to Attendance Group

Note

You can click on the top left to filter persons by additional information.

5. Perform the following operations.

Edit an Attendance Group	Click and then edit the group name or click to add persons to the group.
Add Persons to an Attendance Group	Click an added group to show persons on the right. Then click **Assign To** to add persons to the group.
Remove Persons from an Attendance Group	Click an added group to show persons on the right. Then check persons and click **Unassign** to remove the selected persons from the group. Or click → **Unassign All** to remove all persons from the group.

Set Display Mode of Each Column	Click ⇔ to display each column title completely/incompletely.

What to do next

Configure attendance rules for the group. See ***Configure Attendance Rules for Global / Department / Attendance Group*** .

8.4 Basic Configuration

You can set basic parameters for the attendance module, such as adding pay codes, editing the fixed codes, setting the storage location, and customizing attendance status.

8.4.1 Specify Attendance Check Points

By default, all devices are attendance check points. You can specify some access points for attendance check, so that the check-in/out by credentials (such as swiping card on the access point's card reader) will be valid.

Steps

1. Select **Basic Configuration → Attendance Check Point** on the left.

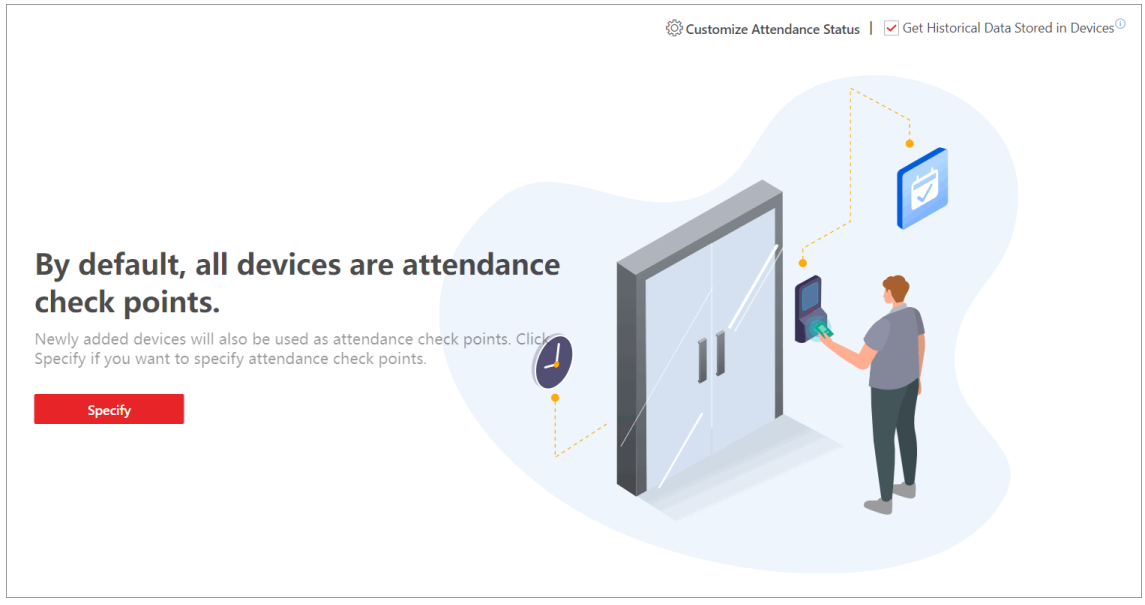


Figure 8-6 Default Mode

2. **Optional:** Click **Customize Attendance Status** to select attendance mode and custom attendance parameters. For details, see ***Customize Attendance Status on Device*** .
3. **Optional:** Check **Get Historical Data Stored in Devices** to synchronize the historical data generated by attendance check points to existing data. This will cause a recalculation of attendance results.

4. Click **Specify** to start customizing attendance check points.
5. Click **Add**.
6. Select the type of the attendance check point.

   Check-In & Out

   The attendance records of check-in or check-out on the attendance check point are both valid.

   Check-In Only

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-in. Persons cannot check out on this check point.

   Check-Out Only

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-out. Persons cannot check in on this check point.
7. Select the resource type (e.g., door) from the drop-down list.

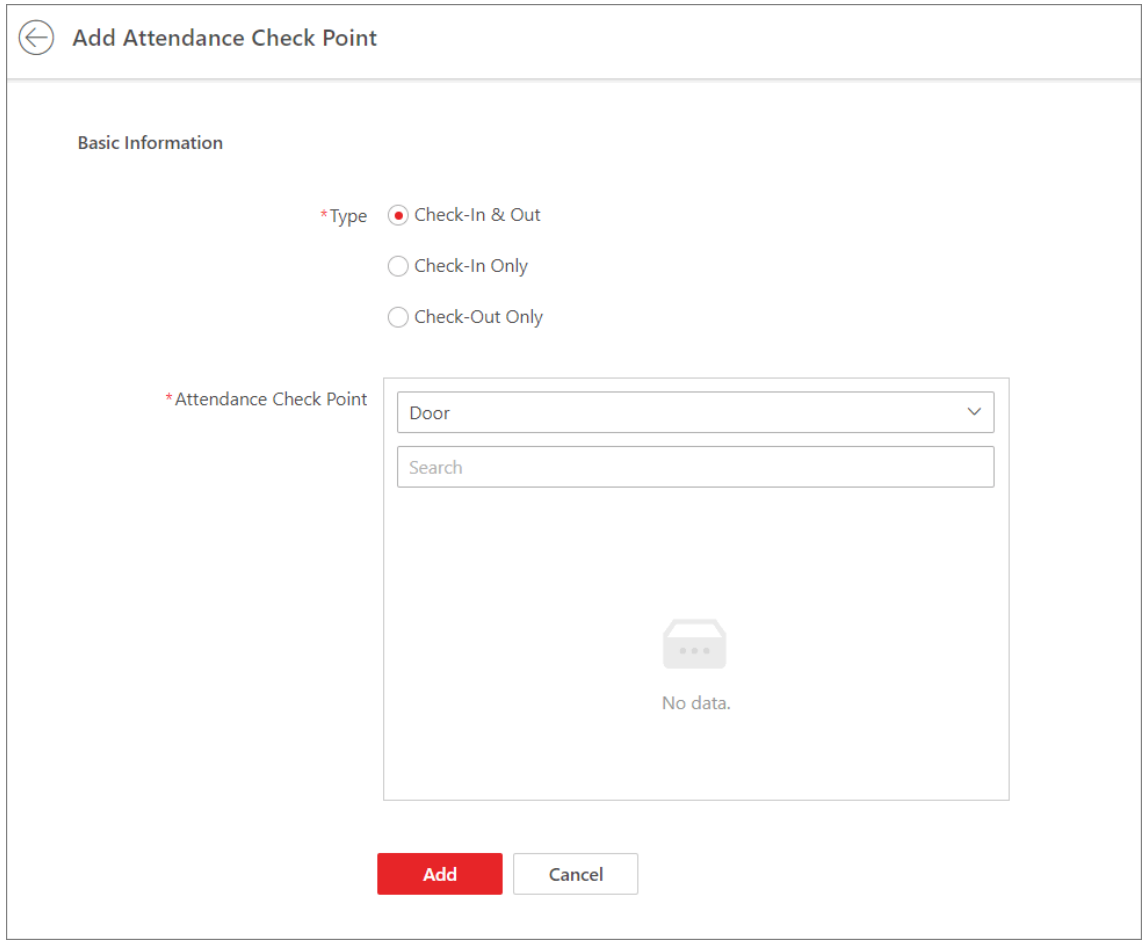


Figure 8-7 Add Attendance Check Point

All the resources which have not been set as attendance check point will be displayed.

8. Select the resources.
9. Click **Add**.

   The selected resources will be displayed in the attendance check point list.
10. **Optional:** Perform the following operations.

Change Check Point's Type	For the added attendance check points, you can select one or more items and click **Set as Check-In Only**, **Set as Check-Out Only**, or **Set as Check-In/Out** from drop-down list to change the current type to another.
Delete Check Point	To delete the added attendance check point, select the added attendance check point(s) and click **Delete**.

Note

If the attendance check point is deleted, the attendance records on this attendance check point will be deleted as well, and it will affect the persons' attendance results for the days on which the attendance data haven't been calculated.

Customize Attendance Status on Device

You can customize the rules of attendance status on device. After setting up Attendance Status on Device and applying the settings to the devices, you can choose to use the attendance status on the devices to calculate the attendance results.

Steps

1. In the left navigation pane of the Attendance module, select **Basic Configuration → Attendance Check Point** .
2. Click **Custom Attendance Status** on the top right.
3. Switch on **Enable Attendance Status on Device**.
4. Set the parameters.

   Attendance Mode

   Manual: No attendance schedule. Manual selection of attendance status is required when a person checks in or checks out on a device.

   Automatic: Specify an attendance schedule and the attendance status of a person is judged according to the schedule.

   Manual And Auto: Specify an attendance schedule and the attendance status of a person is judged according to the schedule. The person can also change the attendance status manually on device.

   Attendance Status Required

   On: Manual selection of attendance status is required for a valid check-in/out.

Off: Manual selection of attendance status is optional.

Note

Not available when in Manual mode, because manual selection of attendance status is always required.

Custom Name of Working

Customize the status name for check-in and check-out.

Custom Break Name

Customize the status name for the start and end of a break.

Custom Overtime Name

Customize the status name for the start and end of an overtime.

Time Template

Select a status and drag on the template to define the attendance status of a period of time.

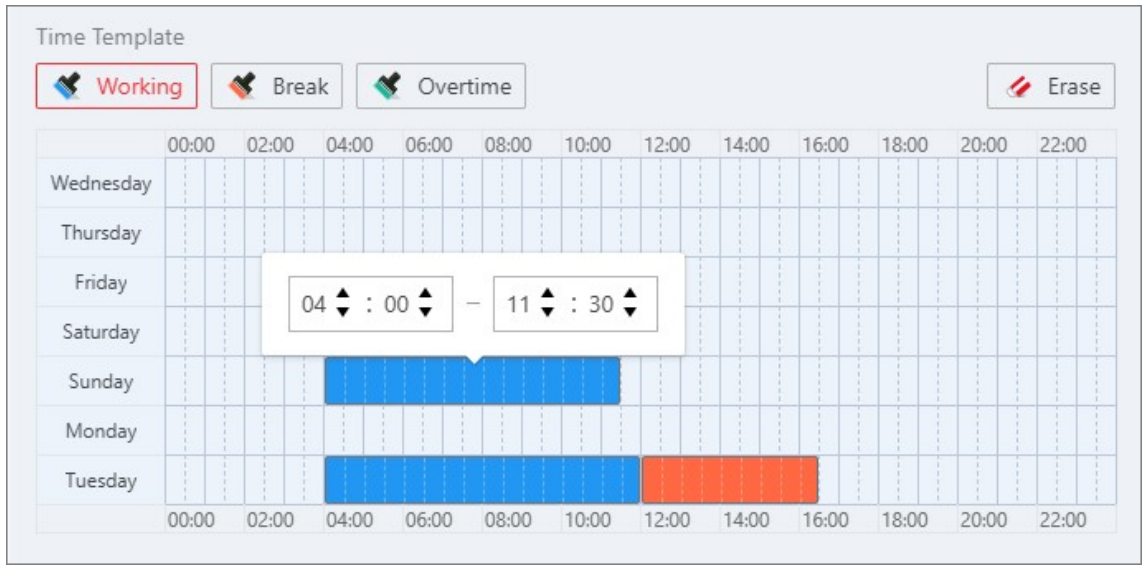


Figure 8-8 Time Template

Note

- Not available when in Manual mode. Because manual selection of attendance status is always required and no attendance schedule is needed.
- Work time and break time must be continuous.
- Overtime cannot be continuous with work and break time.
- Overtime must be before or after work or break time.

5. Click **Save** to save the settings and apply the settings to the attendance check points you added.

Note

- You can view the applying result on the Apply Custom Status window.
- See details about adding attendance check points in ***Specify Attendance Check Points*** .
- You can switch on **Enable T&A Status on Device** when configuring break timetables, timetables, or shifts to record the T&A status on devices, which will be used in attendance results calculation.

8.4.2 Add a Pay Code

Pay code defines the attendance status and calculation codes for calculating the attendance statistics on the third-party system. You can add, edit, and delete pay codes, filter the pay codes by conditions, set the column title, and custom column items.

Steps

1. Go to **Basic Configuration → Pay Code** .
2. Click **Add** to open the Add Pay Code pane.
3. Create the pay code name.
4. Set the pay code type and related parameters.

   Leave

   leave type which displays in reports and leave applications.

   Unit: Unit of pay code. Select from minute, hour, day, and HH:MM (time accurate to minute).

   Overtime

   Overtime type which displays in configuration of overtime rules, reports and overtime applications.

   Work Hour Rate

   Used for calculating the overtime period, e.g., the actual working time of overtime is 2 hours and the work hour rate is 1.5, then the overtime period is 3 hours.

   Color

   Used for making differences among pay codes.
5. Set the rounding rule.

   Round Up

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

   Round to Nearest

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

   Round Down

   Round the number of pay code down, e.g., if you make 0.5 go down, then 6.5 rounds down to 6.
6. Set the Min. Value for the rounding rule.

7. Set whether to display the pay code in report.
8. Click **Add**.
9. **Optional:** Perform the following operations.

Operation	Description
Edit Pay Code	Click in the Operation column to edit the pay code information.
Delete Single Pay Code	Click in the Operation column to edit the pay code information.
Batch Delete Pay Codes	Select one or multiple pay codes and click **Delete** to delete them. Or Select **Delete All** to delete all the pay codes.
Filter Pay Code	Click to expand the conditions, set the filter conditions and click **Filter** for filtering the pay codes.
Set Column Width	Click to select **Complete Display of Each Column Title/Incomplete Display of Each Column Title** to set the column title width.
Custom Column Item	Click and select the needed column items to display. You can also click **Reset** to reset to the default column items.

8.4.3 Edit a Fixed Code

Fixed code refers to the calculation rules of attendance types. You can set parameters of fixed codes such as the unit, symbol, and rounding rule.

Go to **Basic Configuration → Fixed Code** .

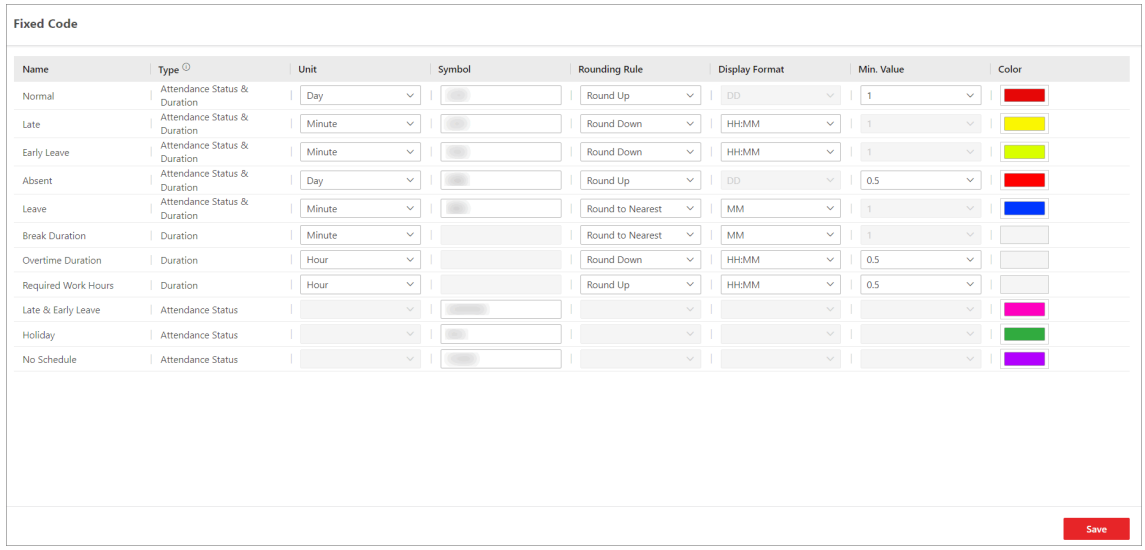


Figure 8-9 Edit Fixed Code

You can set the following parameters and click **Save** to finish editing.

Unit

Unit of pay code. Select from minute, hour, and day.

Symbol

Different symbols indicate different status respectively, including late, absent, no schedule, holiday, etc. You can customize these marks according to actual needs.

Rounding Rule

Rule for calculating the attendance.

Round Up

Round the number of pay code up, e.g., to make 0.5 go up, so 6.5 rounds up to 7.

Round to Nearest

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

Round Down

Round the number of pay code down, e.g., to make 0.5 go down, so 6.5 rounds down to 6.

Display Format

Time format of the fixed code, including HH:MM, DD, HH, and MM.

Min. Value

The minimum value of the fixed code. Select from 1 and 0.5.

Note

When the Unit is "hour", the min. value is 0.25.

Color

Used for making differences among fixed codes.

8.4.4 Add a Leave Rule

A leave rule refers to a group of leave types and persons, where the persons in the group enjoys certain leaves.

Steps

1. Go to **Basic Configuration → Leave Rule → Add Leave Rule** .

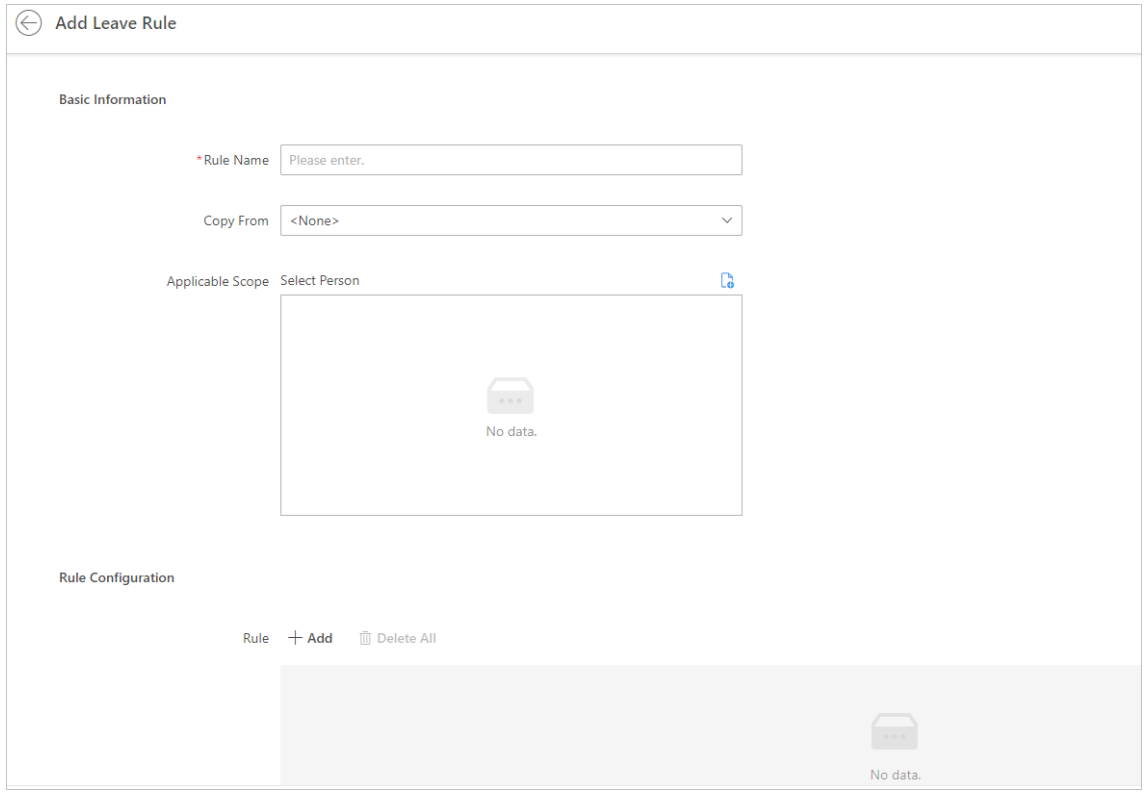


Figure 8-10 Add Leave Rule

2. Enter a rule name.
3. **Optional:** Select an existing leave rule from the drop-down list of **Copy From** to copy the persons using the selected leave rule here.
4. Click to select persons who are going to use the leave rule.
5. Add a rule.
   1) In the Rule Configuration area, click **Add** to open the Add Rule pane.
   2) Select a pay code from the drop-down list.
   3) Set the related parameters.

      Min. Days of Employment Allowed for Leave Application

      Only when the days of employment reaches this value, can the employee apply for a leave.

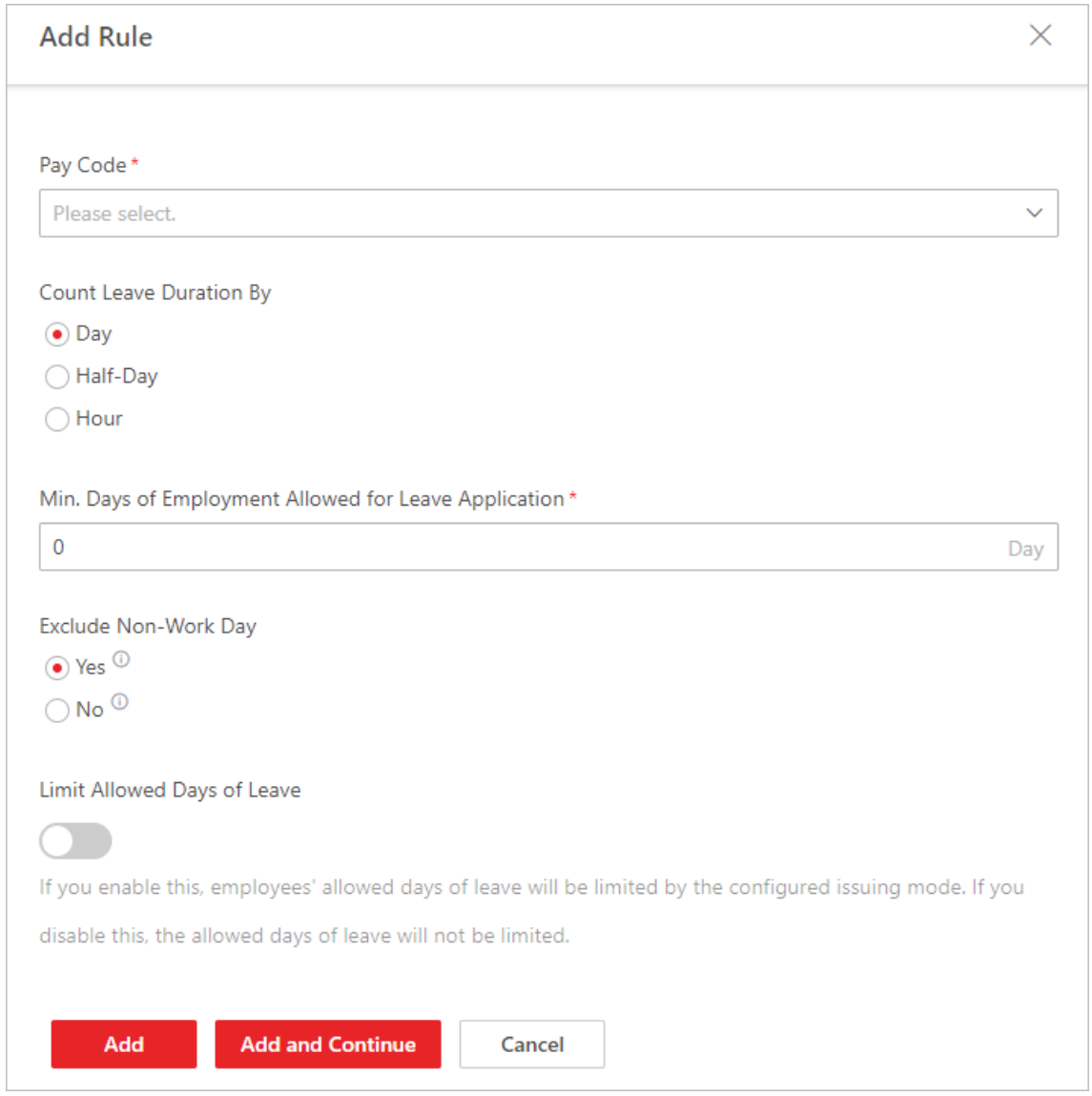


Figure 8-11 Add Rule

4) **Optional:** Enable **Limit Allowed Days of Leave** and set the related parameters.

Issuing Mode

Auto Issue Annually

The platform issues allowed days of leave to employees on a specified day each year. You need to select an issuing date and select an issuing rule.

Issuing Rule

Fixed Amount

The platform issues the same days of leave to employees each year.

Depends On Employment Years

The issued days of leave depend on the employment years.

Issue All Days of Leave Once

Issue all days of leave to employees once. You need to set the number of days and you can configure expiry date of the days if needed.

6. Save the settings.

8.4.5 Configure Check-In/Check-Out via Mobile Client

After configuring the function of check-in/check-out via mobile client, employees in the platform will be able to check in/out inside the valid geographic scope via the Mobile Client. And the platform will perform attendance calculation of check-in records collected by the Mobile Client.

Click **Check-In/Out Area via Mobile Client** on the left navigation bar.

For Configuration of the First Time

For configuration of the first time, you will enter the following page.

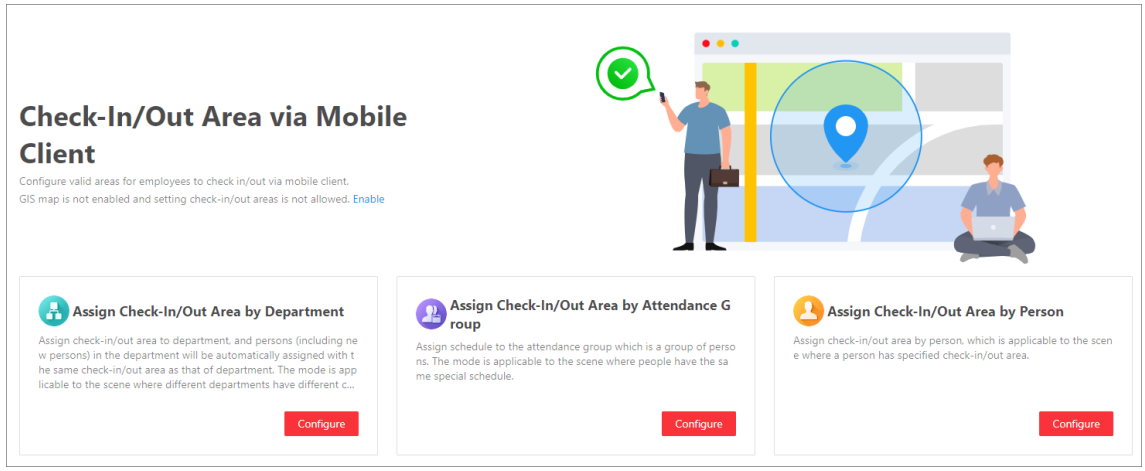


Figure 8-12 Page for Configuration of the First Time

Click **Enable** to enable GIS map, and then click **Configure** to start assigning check-in/out area by department / attendance group / person.

The following shows how to assign check-in/out area by department.

Click **Configure** to show the page of Assign Check-In/Out Area by Department. Select department(s) and click **Next** on the top left. Enter an area name, an draw the area in the radius mode or custom mode. Hover the cursor on the edge of the area and drag to change the scope.

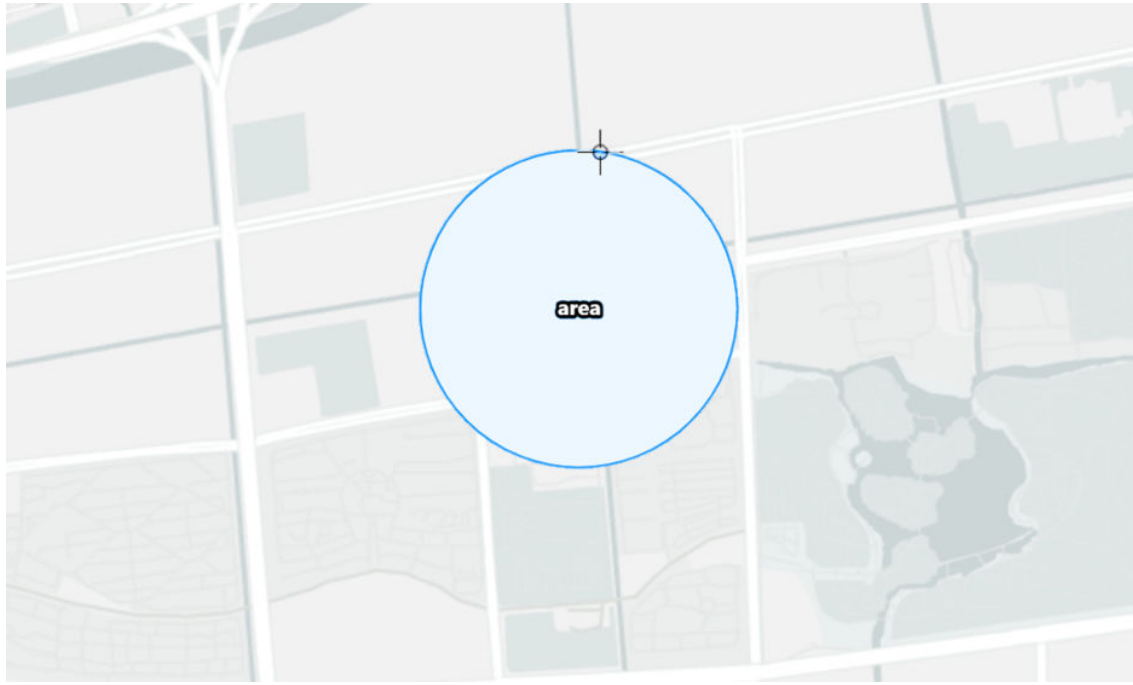


Figure 8-13 Draw Check-In/Out Area

For Configuration of Not the First Time

For configuration of the first time, you will enter the following page.

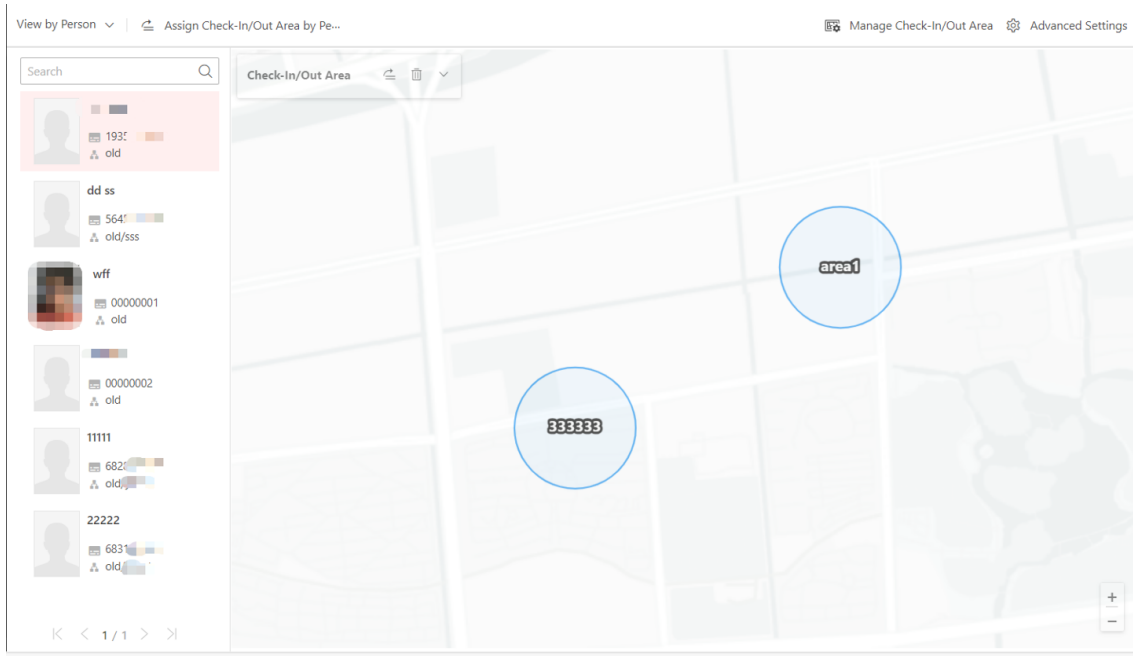


Figure 8-14 Page for Configuration of Not the First Time

Manage Check-In/Out Area

Add/edit/delete check-in/out area(s).

Advanced Settings

Set requirements for employees when checking in/out, approval method of check-in/out, and configure GIS map.

View by Department / Attendance Group / Person

Select the view mode of check-in/out.

You can also select a person /attendance group / department, and click to select check-in/out area(s).

8.4.6 Configure Storage Settings

You can set the storage location of the attachment in exception application.

1. Go to **Basic Configuration → Storage Settings** .
2. Select a backup file to be restored.
3. Click **Save**.

8.5 Configure Attendance Rules for Global / Department / Attendance Group

The attendance rule indicates a set of parameters about time and attendance, including the weekend settings, absence rule, overtime parameters, attendance calculation mode, holiday settings, the calculation of leaves, the authentication mode selection of attendance check, etc. It can be defined as a global / department / group attendance rule. You can configure an attendance group with a group attendance rule which has higher priority than the department rule. You can also configure a department with a department rule which has higher priority than the global rule used for the whole company or institution.

Go to **Attendance Rule → Global Rule / Department Rule / Group Rule** . For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.

8.5.1 Define Weekends

Different countries or regions adopt different weekend convention. HikCentral Access Control provides weekends definition function. You can select one or more days of week as the weekends according to actual situation.

In the Weekend Settings area, select the day(s) of week from Monday to Sunday. The attendance data of the selected date(s) will be calculated with the weekend rule.

8.5.2 Configure Attendance Calculation Rule

Calculated by

First In & Last Out: Only count and calculate the duration of the first and last check-in/out records within the valid check-in/out period.

Each Check-In/Out: Count each check-in/out record within the valid check-in/out period and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/out records.

Count Work Hours in Check-in/out Period Only

Only the working hours within the valid check-in and check-out time period are counted as valid working hours. This feature is only effective during normal shifts when using the **First In & Last Out** method. For example, if the valid check-in and check-out time period is from 9:00 to 18:00, and an employee checks in at 8:30 and checks out at 17:00, the valid working hours are from 9:00 to 17:00.

Enable T&A Status on Device

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

Note

- If a break timetable in the timetable is not enabled with T&A Status on Device, it will be enabled if you enable this function for the timetable.
  If a break timetable in the timetable is already enabled with T&A Status on Device, this setting will not change even if you disable the function for the timetable.
- To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

Day Change Time

Set a time to mark the change of a day. For example, if the day change time is set as 08:00:00, check-in before 08:00:00 will be calculated into the attendance of the previous day, and check-in after 08:00:00 will be calculated into the attendance of the current day.

8.5.3 Define Absence

You can define the absence rule in the global dimension or define an absence rule for a certain department or attendance group. When the employee's attendance conforms to the absence rule, the attendance record will be marked as absent or other status you define.

In the Absence Settings area, you can define the absence rules.

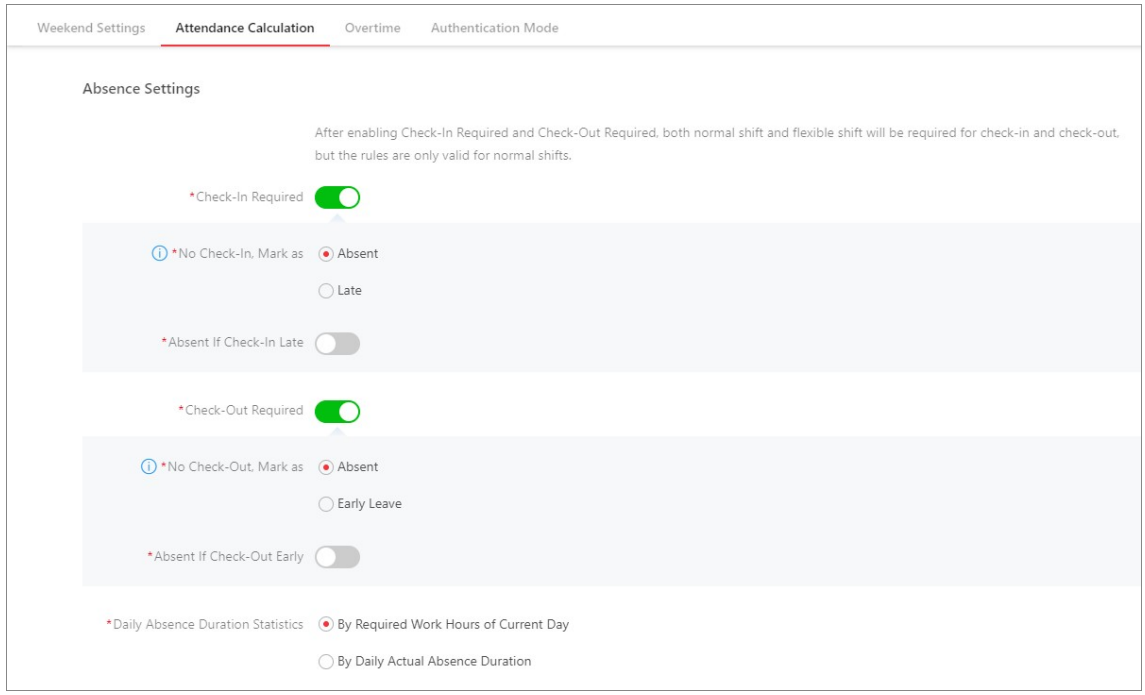


Figure 8-15 Absence Settings

Set Absence Rule for Check-In

Switch on **Check-In Required**. Once this function is disabled, employees will not be required to check in.

In **No Check-In, Mark as**, specify an attendance status when a person does not check in or fails to check in within the valid check-in period. If you select **Late**, you need to set a fixed late duration. For example, if the scheduled start work time is 9:00, valid check-in period is 6:00-12:00 (defined in Timetable - Attendance), **Late Duration** is set to 60 minutes, and **No Check-In, Mark as** is set to **Absent**, the attendance status of an employee will be:

- Normal, if the employee checks in between 6:00 and 9:00.

  Note

  You can set overtime rules to count the extra hours before scheduled start work time as overtime. See details in ***Configure Overtime Parameters*** .

- Late, if the employee checks in between 9:01 and 9:59.
- Absent, if the employee checks in after 10:00 or does not check in.

Switch on **Absent If Check-In Late** and set a tolerant threshold in **Late for**. When the employee's check-in time minus scheduled start work time is longer than the **Late for** value, the employee's attendance status on that day will be marked as Absent.

Set Absence Rule for Check-Out

Switch on **Check-Out Required**. Once this function is disabled, employees will not be required to check out.

In **No Check-Out, Mark as**, specify an attendance status when a person does not check out or fails to check out within the valid check-out period. If you select **Early Leave**, you need to set a fixed late duration.
For example, if the scheduled end work time is 18:00 and valid check-out period is 17:00-21:00 (defined in Timetable - Attendance), and **Early for** is set to 60 minutes, the attendance status of an employee will be:

- Absent, if the employee checks out before 17:00 or does not check out.
- Early Leave, if the employee checks out between 17:01 and 17:59.
- Normal, if the employee checks out between 18:00 and 21:00.

Note

You can set overtime rules to count the extra hours after scheduled end work time as overtime. See details in ***Configure Overtime Parameters*** .

Switch on **Absent If Check-Out Early** and set a tolerant threshold in **Early for**. When the scheduled end work time minus employee's check-out time is longer than the **Early for** value, the employee's attendance status on that day will be marked as Absent.

Daily Absence Duration Statistics

This feature records the specific absence duration of personnel on a daily basis. The duration will be displayed in both the total time card (daily report) and the person attendance summary (summary report). There are two methods for calculating daily absence duration:

- **By Required Work Hours of Current Day**: The required work hours for the current day will be counted as the absence duration and displayed in the **Absent** field of the total time card or the person attendance summary. For example, if the required work hours for the current day are 8 hours, but the actual work hours are 2 hours, the absence duration will be 8 hours.
- **By Daily Actual Absence Duration**: The actual absence duration for the day will be recorded and displayed in the **Absent** field of the total time card or the person attendance summary. For example, if the actual absence duration 2 hours, the absence duration will be 2 hours.

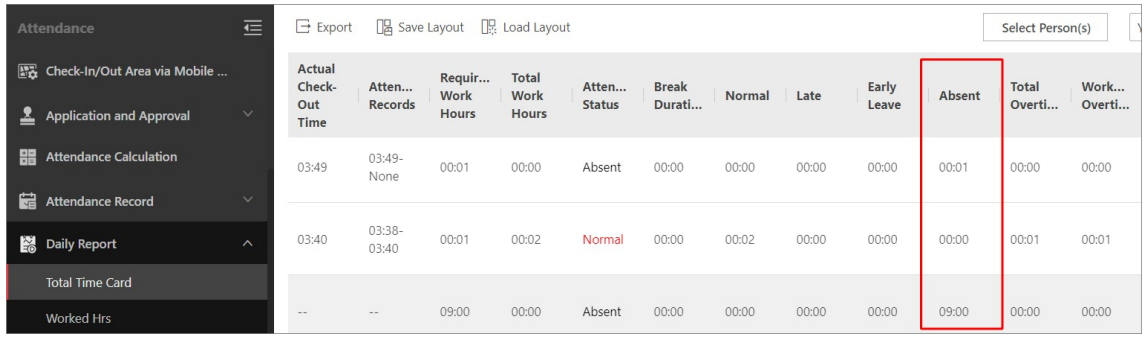


Figure 8-17 Absence Duration (Total Time Card)

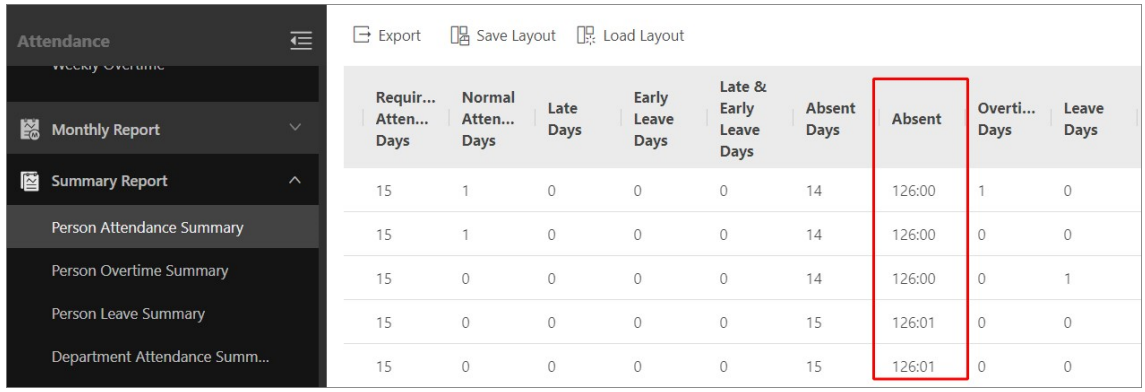


Figure 8-18 Absence Duration (Person Attendance Summary)

8.5.4 Add Holidays Requiring Attendance

You can set a holiday that requires normal attendance as in weekdays.

Steps

1. Select the **Attendance Calculation** tab.

   Note

   For details of adding a holiday, see ***Add a Holiday*** .

2. In **Holidays Requiring Attendance** area, select a holiday that requires attendance. You can click **Add** to add a holiday.

Add a Holiday

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 or an irregular holiday according to the actual scene.

Steps

1. Select **Basic Configuration → Holiday Settings** on the left. You can also access the Holiday Settings page in **System**.
2. Click **Add** to add a holiday.

   Regular Holiday

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

   You can set the **Start Time** and the number of daysfor the holiday, and choose whether to **Repeat Annually** in the system.

   Irregular Holiday

The irregular holiday is suitable for the holiday that is calculated by the day in a specific week, and the specified date might be different every year. For example, Mother's Day is on the second Sunday of each May.

For the **Start Time**, you can set the start day of the holiday. For example, select May, Second, and Sunday for Mother's Day. Then, you can set the number of days for the holiday, and choose whether to **Repeat Annually** in the system.

8.5.5 Calculation of Leaves

You can set the status of leaves as normal attendance, leave, or absent.

In the **Attendance Calculation → Leave Settings** area, you can choose to mark leave as **Normal**, **Leave**, or **Absent**. The leave status will be displayed in the attendance results.

8.5.6 Configure Overtime Parameters

Overtime is the amount of time a person works beyond scheduled work hours. You can configure parameters, including work hour rate, overtime level, and attendance status for overtime, for workdays, weekends, and holidays.

Overtime on Workday/Weekend

Calculation Mode

Select a calculation mode.

By Total Work Hours

Overtime is calculated according to the extra work hours that exceed the required work hours.

OT Duration Calculation Mode

Select a method for overtime duration calculation.

Fixed

Overtime duration is fixed regardless of the actual overtime. You need to set a fixed duration in the **Overtime Duration** field.

Actual

Count the actual duration of the overtime. You need to set a minimum threshold for a valid overtime.

For example, if you set the threshold to 60 minutes:

- Overtime duration is 0 if a person works for 59 minutes longer than the required work hours;
- Overtime duration is 61 if a person works for 61 minutes longer than the required work hours.

By Time Points

Overtime duration is calculated according to the extra work hours earlier than the start-work time or later than end-work time in one day.

You can enable **Count Early Check-In as OT** and **Count Late Check-Out as OT** to set the overtime duration calculation mode respectively.

OT Duration Calculation Mode

Select a method for overtime duration calculation.

Fixed

Overtime duration is fixed regardless of the actual overtime. You need to set a fixed duration in the **Overtime Duration** field.

Actual

Count the actual duration of the overtime. You need to set a minimum threshold for a valid overtime.

For example, if you set **Earlier than Check-In Time for Mark as Valid Overtime** to 30 minutes, and the start-work time is 9:00:

- Overtime duration is 0 if a person checks in at 8:31.
- Overtime duration is 31 if a person checks in at 8:29.

Overtime Level Settings

Click **Configure Rule** to open the Configure Overtime Rule window. Select an attendance data, and click **Add Rule** to set a total overtime duration and select an overtime mode. You can click **Copy** to copy another day's overtime rule. The total work hours will be calculated according to the work hour rate of each overtime level.

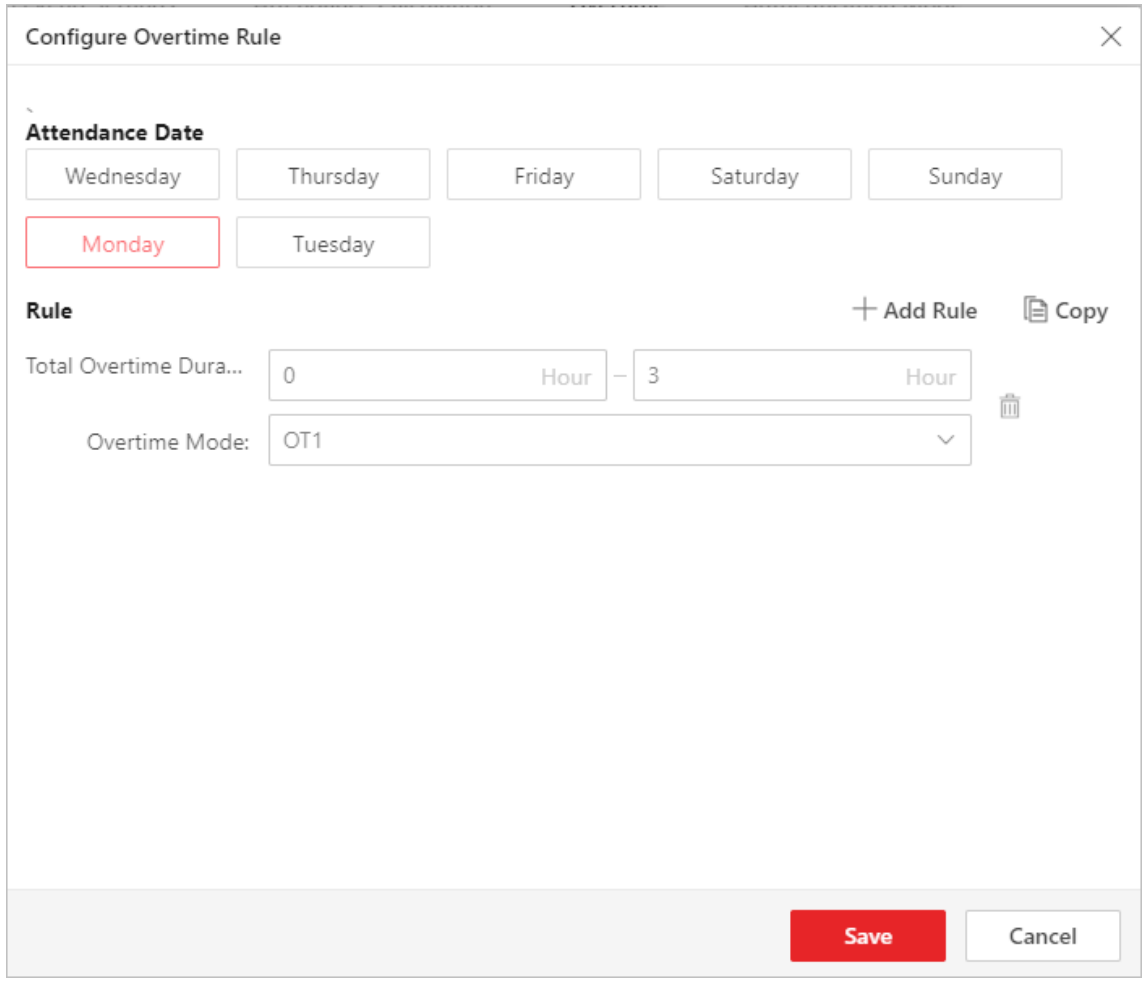


Figure 8-19 Configure Overtime Rule

Overtime on Weekends

You can switch on **Overtime on Weekends** and set the valid overtime threshold. Then when a person's work hours on weekends are less than the threshold, the overtime will be 0.

Overtime on Holidays

If Works Longer than Mark as Valid Overtime

Set a minimum threshold for a valid overtime.

Set Max. Overtime

Switch on to set an upper limit for the overtime duration in the **If Works Longer than Mark as Invalid Overtime** field. Exceeded work hours will not be counted as valid overtime.

Overtime Level on Holiday

Set the overtime level for each holiday.

You can select multiple holidays and click **Batch Set Overtime Level** to batch set the overtime level, or set the overtime level for each holiday separately.

Note

- To add a new holiday, click **Add Holiday**.
- To edit holidays, click **Holiday Settings**.

Overtime Not in Valid Attendance Check Period

Count the extra work time outside the valid check-in/out period as valid overtime.

8.5.7 Configure Authentication Mode

You can configure authentication modes, including card, fingerprint,, face, and iris. After setting authentication mode, you can get attendance records of the configured authentication mode and calculate attendance data of the configured authentication mode.

For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.

Select **Authentication Mode** on the right, switch on **Customize Authentication Mode**, and select card, fingerprint, iris, or/and face as the authentication mode.

Note

This function requires device capability.

8.6 Add Timetable

The timetable defines the detailed time rules for attendance, such as work time, break time, etc. According to the actual requirements, you can select normal shift or flexible shift as timetable type for further configuration and application, and then the employees need to follow the time rules to check in, check out, etc.

8.6.1 Add Break Timetables

Break timetables define the start/end time of breaks and the calculation method of break duration. You can create break timetables in advance and use them as templates when configuring break time in a timetable.

Steps

1. Select **Shift Settings → Break Timetable** on the left.
2. Click **Add**.
3. Set parameters for the break timetable.

   Name

Create a descriptive name for the break timetable, such as "Launch Break".

Start Time

Start time of the break.

Earliest Allowable Start Time

Flexible start time of the break. If a person checks out earlier than **Earliest Allowable Start Time**, the check-out will not be counted as the break start time and no break will be recorded.

End Time

End time of the break.

Latest Allowable End Time

Flexible end time of the break. If a person checks in later than **Latest Allowable End Time**, the check-in will not be counted as the break end time.

Break Duration Calculation Mode

Method for counting the duration of a break.

Period

Fixed duration. The actual break start/end time of persons will only be recorded but not be used to calculate the duration of breaks.

Break Duration

Set the duration of the break.

Must Check

Actual duration calculated by the check-out time and check-in time.

In **Count Early/Late Return**, you need to choose to count early or late return time **By Duration** or **By Time Point**.

By Duration

When the actual break duration (end time minus start time) is shorter than or longer than the specified duration, it will be counted as early or late return.

By Time Point

When the actual return time is earlier than or later than the specified end time, it will be counted as early or late return.

You also need to set the threshold and the attendance status for the early/late return time.

If early/late for

Threshold for counting the early/late return time.

Mark as

Choose to count the remaining time of a early return as overtime or the exceeded time of a late return as late, early leave, or absent.

If you do not want to count the early/late return time, set it to **Normal**.

Set Calculation Mode

Switch on to set the calculation method of break duration.

Calculated by

First In & Last Out: Only count and calculate the duration of the first and last check-in/out records during the start/end time of the break.

Each Check-In/Out: Count each check-in/out record during the start/end time of the break and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/outs.

Enable T&A Status on Device

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

Note

To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

4. Click **Add** to finish adding the timetable, or click **Add and Continue** to finish adding the timetable and add a new break timetable.
5. **Optional:** Perform further operations after adding the break timetable.

Edit Break Timetable	Click on the name of a break timetable to edit it.
Delete Break Timetable	Select the break timetables you want to delete and click **Delete** to delete them.

What to do next

Use the break timetable to set the break time in a timetable. See ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .

8.6.2 Add Timetable for Normal Shift

Normal shift is usually used for the attendance with fixed schedule. The employees should check in before the start-work time and check out after the end-work time. Otherwise, their attendance status will be late, early leave, or absent. You can add the timetable for normal shift to define the detailed rules (e.g., start-work time, end-work time, late rule, valid check-in/out time, break time, etc.), in order to monitor employees' working hours and attendance.

Steps

1. Select **Shift Settings → Timetable** on the left.
2. Click **Add**.
3. Configure the **Basic Settings**.
   1) On the top, create a timetable name.

2) Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Schedule in time bar.
3) Select **Normal Shift** as the time period type, and set the following parameters.

Scheduled Work Time

Range of the scheduled work time, including start-work time and end-work time.

Valid Check-In Period

If the employee does not check in during the valid check-in period, the check-in will not be recorded and the attendance status will be absent or late depending on the absence settings.

Note

It is allowed to set the valid check-in period crossing days, therefore the time period can be more than 24 hours. For example, you can set the start time to 08:00:00 on the previous day, set the end time to 10:00:00 on the current day.

Valid Check-Out Period

If the employee does not check out during the valid check-out period, the check-out will not be recorded and the attendance status will be absent or early leave depending on the absence settings.

Note

It is allowed to set the valid check-out period crossing days, therefore the time period can be more than 24 hours. For example, you can set the start time to 18:00:00 on the previous day, set the end time to 19:00:00 on the current day.

Min. Work Hours

Employees' work duration in one day must be longer than minimum work hours. Otherwise, the attendance status will be absent.

Flexible Mode

Allow Late/Early Leave

The employees are allowed to arrive late or leave early for a specific period of time. For this mode, you need to set the allowable time for late and early leave. If an employee checks in/out within the period after the start-work time or before the end-work time, the attendance status will be **Normal**. For example, if the start-work time is set to 09:00:00, and the late allowable duration is 30 minutes, and the employee checks in at 09:15:00, the attendance status will be **Normal**.

Flexible Period

Flexible period allows employees to extend their start-work time and end-work time. For this mode, you need to set the flexible duration, which defines the extended duration for both start-work time and end-work time. If the total late and early leave

time is within the flexible duration, the attendance status will be **Normal**. For example, if the scheduled work time is set to 09:00:00 to 18:00:00, and the flexible duration is 30 minutes, and the employee checks in at 09:15:00, and checks out at 18:15:00, the attendance status will be **Normal**.

4. In **Break Period**, set the following parameters.

Break Time

Click **Add** to select one or multiple break timetables. For adding timetables, see ***Add Break Timetables*** .

Exclude Break Duration from Work Hours

Enable the function and set the break duration which will not be counted into work hours.

5. In **Attendance Calculation**, set the following parameters.

Note

The attendance calculation rule has higher priority than the department, group, and global rules.

Set Calculation Rule

Switch on to set the calculation method of work duration. See details in ***Configure Attendance Calculation Rule*** .

Absence Settings

Set a different absence rule instead of using the general absence rule.

Note

See details about setting a general absence rule in ***Define Absence*** . You can also refer to this topic for explanations for the parameters in the absence rule.

6. In **Overtime**, switch on **Count Timetable as Overtime**, and set the following parameters.

Note

- The overtime timetable has higher priority than the department, group, and global rules.
- See details about setting an overtime timetable in ***Configure Overtime Parameters*** . You can also refer to this chapter for explanations of the parameters.

7. **Optional:** In **Timetable Overview**, view the timetable in a time line.



Figure 8-20 Timetable Overview

8. Click **Add** to save the timetable, or click **Add and Continue** to continue adding another timetable.

What to do next
Use the timetables to define the work schedule on each day in a shift. For more details, refer to ***Add Shift*** .

8.6.3 Add Timetable for Flexible Shift

Flexible shift is usually used for the attendance with flexible schedule. It does not require a strict check-in time and check-out time and only requires that the employees' work hours are longer than the minimum work hours.

Steps
1. Go to **Shift Settings → Timetable** .
2. Click **Add**.
3. Configure the **Basic Settings**.
   1) On the top, create a timetable name.
   2) Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Schedule in time bar.
   3) Select **Flexible Shift** as the time period type, and set the following parameters.

      Valid Check-In/Out Period

      If the employee does not check in/out within the valid check-in/out period, the check-in/out will not be recorded and the attendance status will be late or absent.

      Min. Work Hours

      Employees' work duration in one day must be longer than minimum work hours. Otherwise, the attendance status will be absent.

      Latest Check-In Time

      If the actual check-in time is later than this time, the attendance status will be marked as Late.
4. In **Break Period**, click **Add** to select the break timetables to define the break time in the timetable.

   Note
   - You can click **Add** to create a new break timetable. See details in ***Add Break Timetables*** .
   - Enable **Exclude Break Duration from Work Hours** and set the break duration which will not be counted into work hours.
5. In **Attendance Calculation**, switch on **Set Calculation Mode**, and set the following parameters.

   Note
   The attendance calculation rule has higher priority than the department and global rules.

   Calculation Rule

   Calculated by

First In & Last Out: Only count and calculate the duration of the first and last check-in/out records within the valid check-in/out period.

Each Check-In/Out: Count each check-in/out record within the valid check-in/out period and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/out records.

Enable T&A Status on Device

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

Note

- If a break timetable in the timetable is not enabled with T&A Status on Device, it will be enabled if you enable this function for the timetable.
  If a break timetable in the timetable is already enabled with T&A Status on Device, this setting will not change even if you disable the function for the timetable.
- To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

Day Change Settings

Switch on to set the day change time.

Absence Settings

Set a different absence rule instead of using the general absence rule.

Note

See details about setting a general absence rule in ***Define Absence*** . You can also refer to this topic for explanations for the parameters in the absence rule.

6. In **Overtime**, switch on **Count Timetable as Overtime**, and set the following parameters.

Note

- The overtime timetable has higher priority than the department and global rules.
- See details about setting a overtime timetables in ***Configure Overtime Parameters*** . You can also refer to this topic for explanations for the parameters.

7. **Optional:** In **Timetable Overview**, view the timetable in a timeline.



Figure 8-21 Timetable Overview

8. Click **Add** to save the timetable, or click **Add and Continue** to continue adding another timetable.

What to do next
Use the timetables to define the work schedule on each day in a shift. For more details, refer to ***Add Shift*** .

8.7 Add Shift

Shift is the time arrangement for employees. Shifts can be assigned to employees to regulate their duties. You can adopt one or multiple timetables in one shift.

Before You Start
Make sure you have added timetables. See details in ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .

Steps
1. Go to **Shift Settings → Shift**
2. Click **Add**.
3. Set the shift's basic information, including creating a descriptive name and editing its description.
4. **Optional:** Select another shift from the drop-down list of **Copy from** field to copy the shift information to the current shift.
5. Set the shift's repeating pattern.

   Week

   The shift will repeat every 1 to 52 weeks based on your selection.

   Day

   The shift will repeat every 1 to 31 days based on your selection.

   Month

   The shift will repeat every 1 to 12 months based on your selection.
6. Select a timetable and click on the table below to apply the timetable on each day.

   Note

   You can use up to 8 different timetables in one shift.
7. Switch on **Configure Attendance During Holidays**, and select the holidays. On holidays, the shift will not be effective.
8. Click **Add** to finish adding the shift.

What to do next
Assign shift to persons or departments. See details in ***Assign Schedule to Person*** or ***Assign Schedule to Department*** .

8.8 Manage Schedule

Schedule is used to specify the persons and effective periods during which the persons perform their duties following the attendance rule defined in the shift. After setting the shift, you need to assign it to the departments, attendance groups,persons, or add a temporary schedule, so that it will calculate the attendance records for persons according to this schedule.

8.8.1 Schedule Overview

The schedule overview shows the schedule information of each person in the department / attendance group. You can also view the detailed schedule of one person for each day in one month/week.

On the top, select **Attendance**.

Select **Schedule → Schedule Overview** on the left.

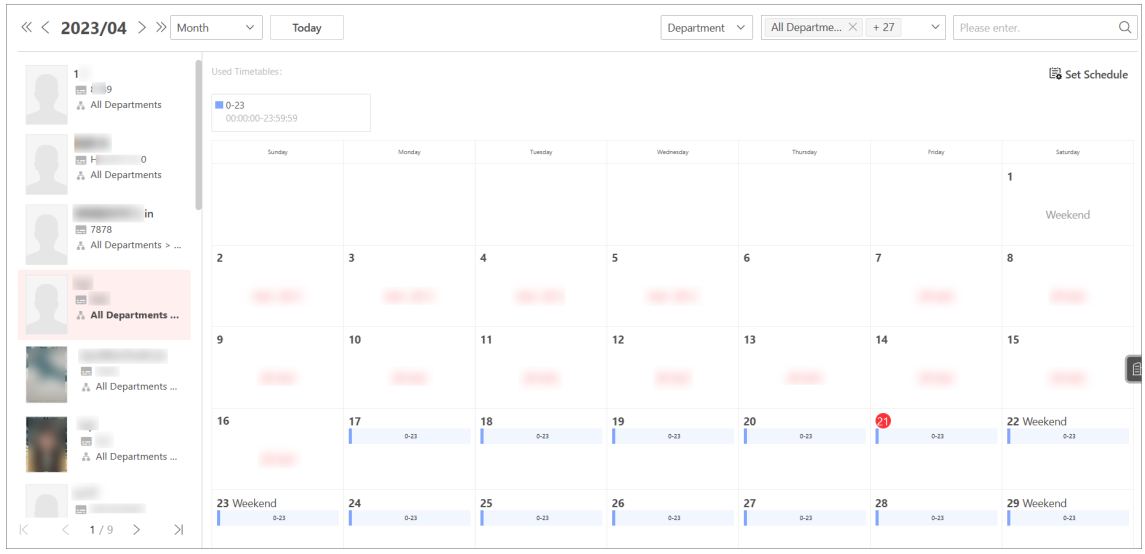


Figure 8-22 Schedule Overview

On the top, select **Department** / **Attendance Group** to view the schedule information by department or attendance group.

Select specific department / attendance group.

Note

- You can check **Include Sub-Department** to display the persons of sub-departments.
- You can enter keywords to search for specific departments / attendance groups.

On the left, you can view the schedule information about every person in the department / attendance group.

Click the person name to enter the detailed schedule of this person for each day in one month, such as effective period, schedule name, and so on.

You can perform the following operations.

- Select **Month**/**Week** to view the schedule by month or week.
- Click **Today** to locate today in the schedule.
- Click **Set Schedule** to edit the schedule. For details, see ***Assign Schedule to Person*** .
- On the upper-right corner, enter the keyword to search for specific persons to view schedules related to them.

8.8.2 Assign Schedule in Quick Mode

If you need to assign the schedule for person(s) quickly, you can use the quick scheduling function.

On the top navigation bar, click → **Quick Scheduling** .

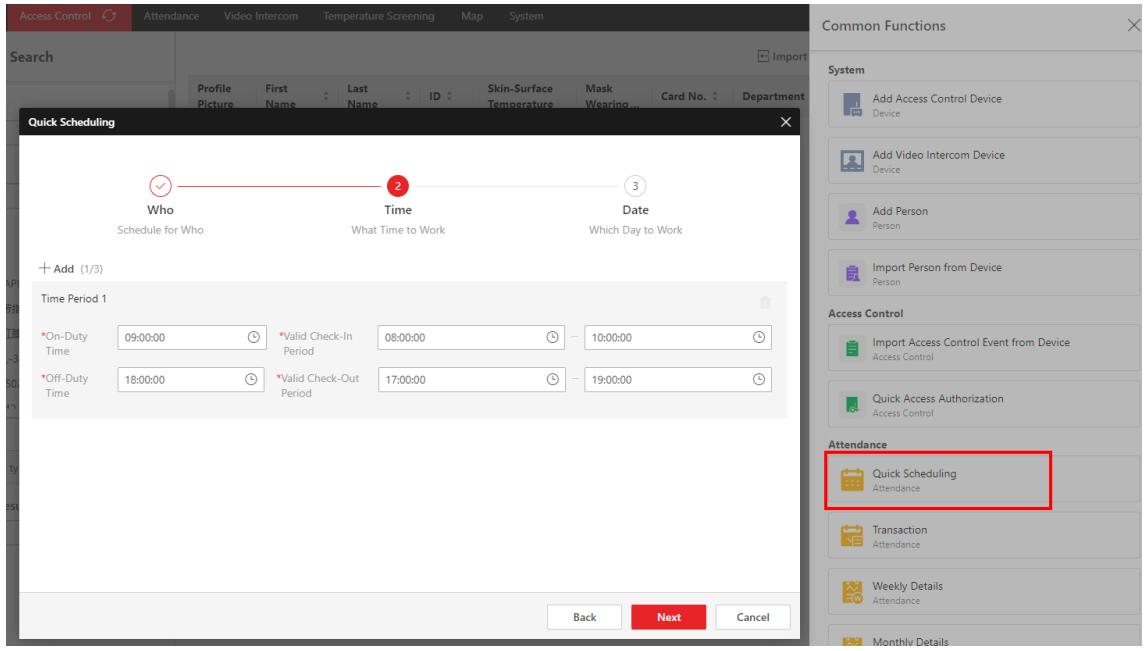


Figure 8-23 Quick Scheduling

Configure **Who**, **Time**, and **Date**, and then save the settings.

8.8.3 Assign Schedule to Department

After setting the shift, you need to assign it to the department so that it will calculate the attendance records for persons in the department according to this schedule.

Steps

1. On the top left, select **Schedule** → **Department Schedule** .

2. Open the add schedule page.
3. Set schedule parameters.

Effective Period

The shift is effective within the period you set.

Shift

Select a shift to be assigned, and you can click **View** to preview the schedule.

Note

You can click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .

4. **Optional:** Click to select attendance check points linked with the schedule.

Only authentications at the linked attendance check points will be counted.

5. **Optional:** Switch on **Configure Check In/Out Not Required**, check one of the following parameters if needed.

Check-In Not Required

Persons in the person group(s) in this schedule do not need to check in when they arrive.

Check-Out Not Required

Persons in the person group(s) in this schedule do not need to check out when they leave.

Effective for Overtime

The overtime of the persons in the person group(s) in this schedule will be recorded.

6. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.

8.8.4 Assign Schedule to Attendance Groups

After setting the shift, you need to assign it to an attendance group so that the platform will calculate the attendance records for persons in the group according to this schedule.

Steps

1. On the top left, select **Schedule → Group Schedule** .
2. Click **Add Schedule** to open the Add Schedule pane on the right.
3. In the Attendance Group area, check group(s) you want to assign a schedule to.

Note

You can click **Add Attendance Group** to add a new one.

4. Set schedule parameters.

Effective Period

The shift is effective within the period you set.

Shift

Select a shift to be assigned.

Note

- click **View** to preview the schedule.
- Click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .

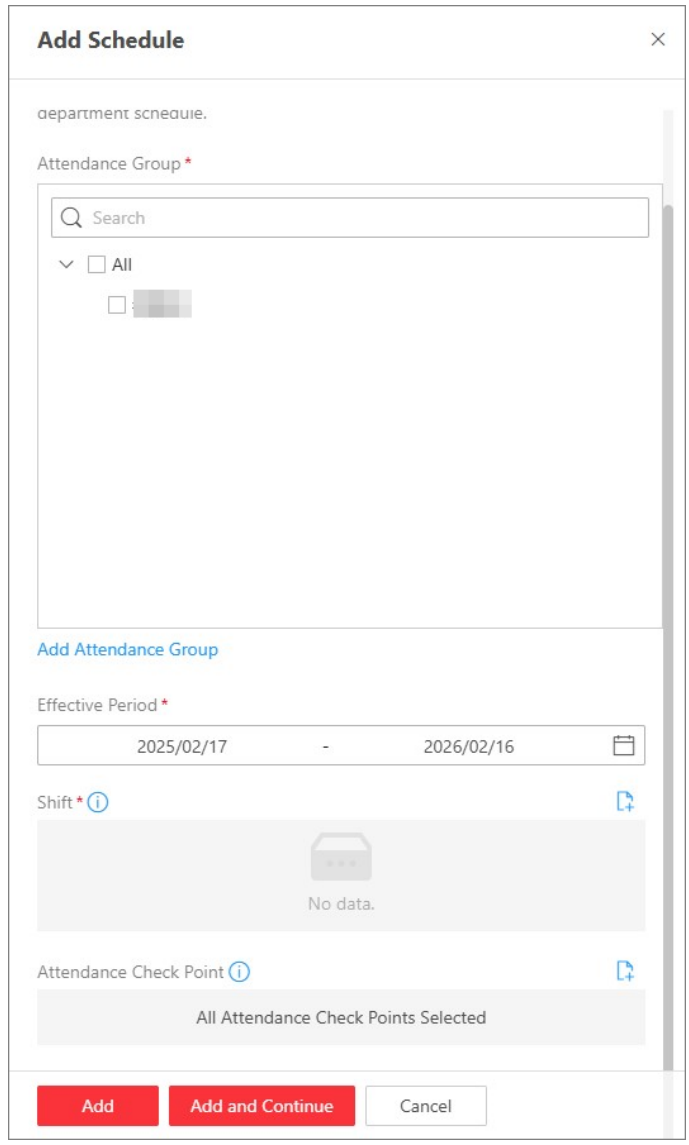


Figure 8-24 Add Schedule

5. **Optional:** Click to select attendance check point(s) linked with the schedule.
   Only authentications at the linked attendance check points will be counted.
6. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.

8.8.5 Assign Schedule to Person

You can add a person schedule and assign a shift to one or more persons, so that it will calculate the attendance records for the persons according to this schedule.

Steps

Note

The person schedule has the higher priority than department schedule.

1. On the top left, select **Schedule → Person Schedule** .
2. Click **Add Schedule** to enter the Add Schedule page.
3. On the Add Schedule pane, click to select person(s) you want to assign schedule to,
4. Set required parameters.

   Effective Period

   Within the period you set, the shift is effective.

   Shift

   Select a shift to be assigned, and you can click **View** to preview the schedule.

   Note

   You can click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .
5. **Optional:** Click to select attendance check points linked with the schedule.

   Only authentications at the linked attendance check points will be counted.
6. **Optional:** Switch on **Configure Check In/Out Not Required**, check one of the following parameters if needed.

   Check-In Not Required

   Persons in the person group(s) in this schedule do not need to check in when they arrive.

   Check-Out Not Required

   Persons in the person group(s) in this schedule do not need to check out when they leave.

   Effective for Overtime

   The overtime of the persons in the person group(s) in this schedule will be recorded.
7. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.
8. **Optional:** Perform the following operations.

Edit Schedule	Select a person in the list and click to edit the person's schedule.
Filter Schedule	Click and set filter conditions such as person name, and then click **Filter** to filter the target schedule.
Delete Schedule	Select one or multiple schedules in the list and click **Delete Schedule** to delete the schedules. Also, you can click **Delete All** to delete all of the schedules.

8.8.6 Add Temporary Schedule

You can add a temporary schedule for a person and the person will be assigned with the schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start

You should have added the person(s) and the shift. For details, refer to ***Add Shift*** .

Steps

Note

The temporary schedule has the higher priority than other schedules.

1. On the top left, select **Schedule → Temporary Schedule** .
2. Click **Add** to enter Add Temporary Schedule page.
3. In **Select Person** area, click and select the needed persons.
4. In **Select Timetable(s)** area, select the needed timetable.

   Note

   You can also click to add timetable if needed. For details, refer to ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .
5. Above the calendar, select the year and month.
6. In the calendar area, click one or multiple dates, then the selected timetable will be added to the selected date(s).
7. **Optional:** In the specific date of the calendar, click and select whether to perform the following operations.

   Clear Shifts

   Click to clear all schedules of the selected date.

   Restore to Initial Schedule

   Click to cancel the adding and restore to the initial schedule.

   Specify Attendance Check Points

   Click to select specific devices as the attendance check points. By default, all devices are attendance check points.
8. Click **Finish** on the top right.

8.9 Configure Calculation Mode of Attendance Results

You can set the attendance calculation mode as manual calculation or auto calculation. Go to **Attendance → Attendance Calculation → Manual Calculation / Auto Calculation** .

8.9.1 Manually Calculate Attendance Results

If department or schedule changes or abnormal attendance records are handled, you can recalculate the attendance results according to the latest data. After re-calculation, the original results will be replaced by new attendance results.

Steps

Note

HikCentral Access Control can calculate the attendance data automatically at a fixed time point (4 o'clock by default) every day. You can edit the time point in **Attendance → Attendance Calculation → Auto Calculation** .

1. Select **Manual Calculation**.
2. Set the start time and end time for attendance calculation.
3. Select target person(s) for attendance calculation.
   - **All Persons**: Calculate all persons' attendance records.
   - **Specified Attendance Group(s)**: Select one or multiple attendance groups for calculation.
   - **Specific Person(s)**: Click to select one or multiple persons for calculation.
4. Click **Calculate**.

   Note

   It can only calculate the attendance data recorded within three months.

8.9.2 Set Auto-Calculation Time of Attendance Results

Attendance results calculation refers to calculating the attendance status and duration according to persons' check-in/out records. You can set an auto-calculation time so that the platform will calculate the attendance results for all persons at a specific time every day.

Steps

1. Select **Auto Calculation**.
2. Select a time in **Calculate at**.
3. **Optional:** Enable **Recalculate Historical Data**.
4. Click **Save**.

8.10 Approval Flow

When employees submit attendance applications, including leave, overtime, attendance correction, and check-in/out via the Mobile Client, reviewers should process these applications. This entire process is the approval flow, which defines the steps of the approval process.

To complete an entire approval flow, follow these steps. Here, take applying for a leave as an example.

1. Add approval roles for an application and link persons to each role.
2. Configure the approval flow with the added approval roles to regulate the flow of reviewing applications.
3. Add leave rules for specific persons. When these persons apply for leave, they should follow the leave rules.
4. Employees submit applications via the Mobile Client or the Web Client (Self-Service).
5. Reviewers review applications from employees via the Mobile Client or the Web Client.
6. Employees check their application status via the Mobile Client or the Web Client (Self-Service).

8.10.1 Step 1: Add Approval Role

Add approval roles for an application and link persons to each role.

Go to **Attendance → Approval Management → Approval Role → Add Now / Add** .

For example, you can add approval roles as HR or Team Manager and link persons to each role.

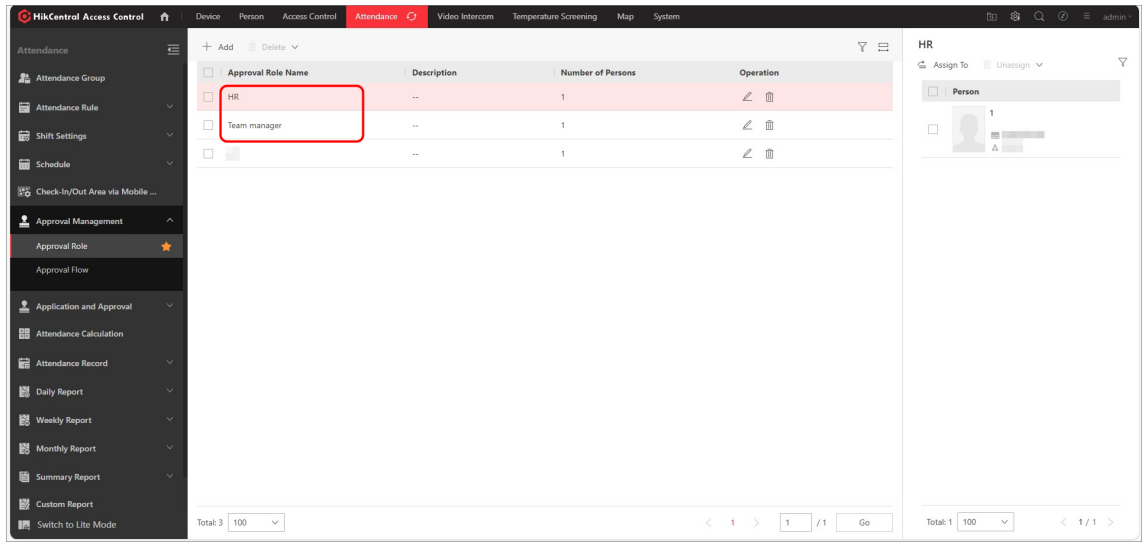


Figure 8-25 Approval Role

8.10.2 Step 2: Configure Approval Flow

Configure the approval flow with the added approval roles to regulate the flow of reviewing applications.

Go to **Attendance → Approval Management → Approval Role → Approval Flow → Add** .

Take adding a **Department Approval Flow** as an example, which defines the leave approval process of reviewing applications from a department. Employees in the Team A and B will follow the leave flow when they apply for leave.

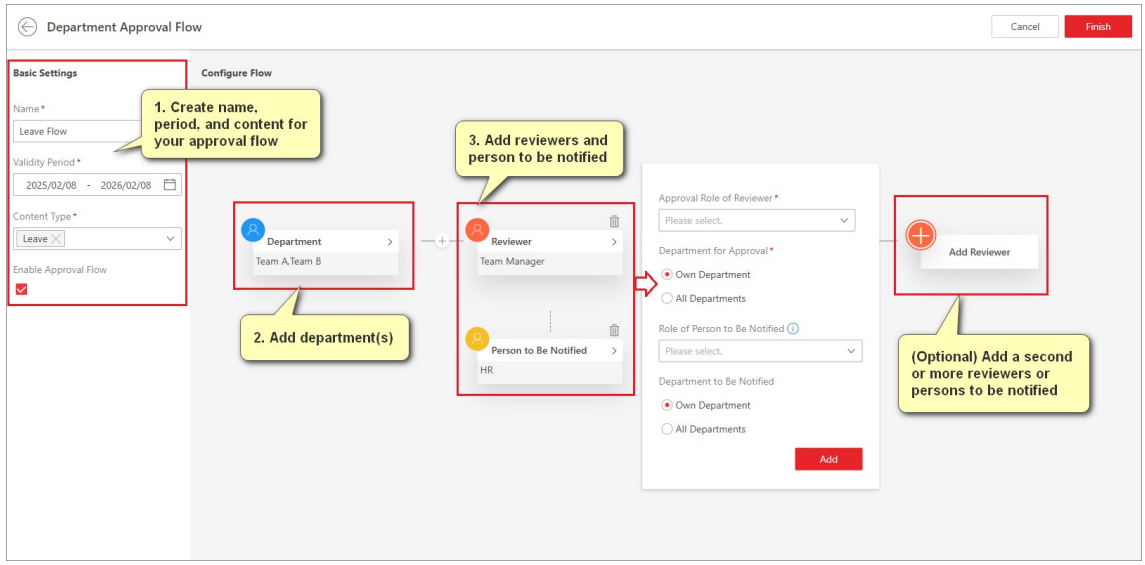


Figure 8-26 Approval Flow

8.10.3 Step 3: Add Leave Rule

Add leave rules for specific persons. When these persons apply for leave, they should follow the leave rules.

Go to **Attendance → Basic Configuration → Leave Rule → Add Leave Rule** .

For details, see ***Add a Leave Rule*** .

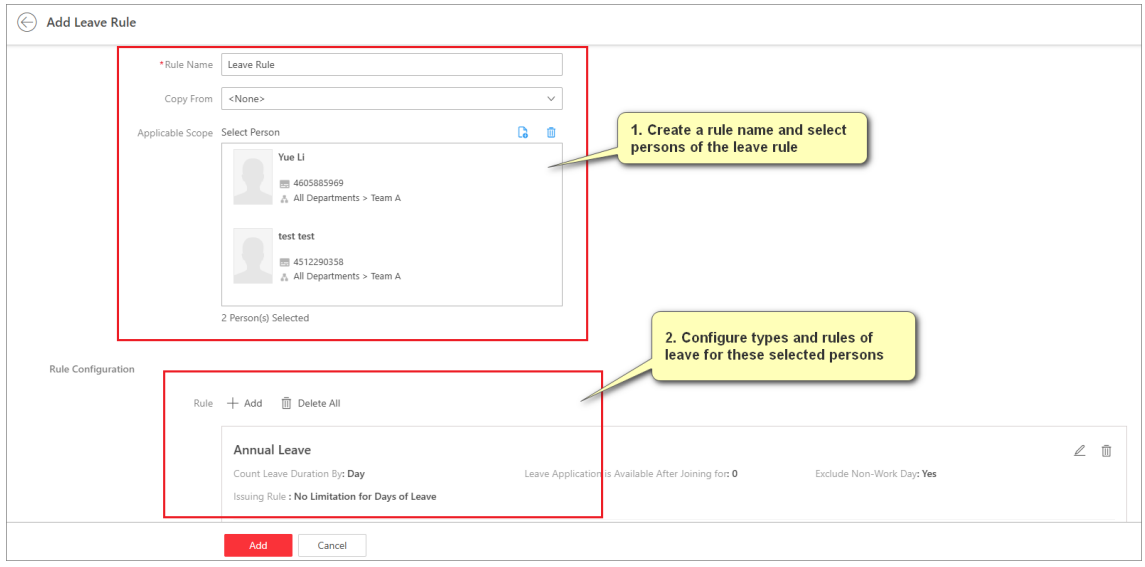


Figure 8-27 Leave Rule

8.10.4 Step 4: Employees Submit Applications

Employees submit applications via the Web Client or the Mobile Client (Self-Service).

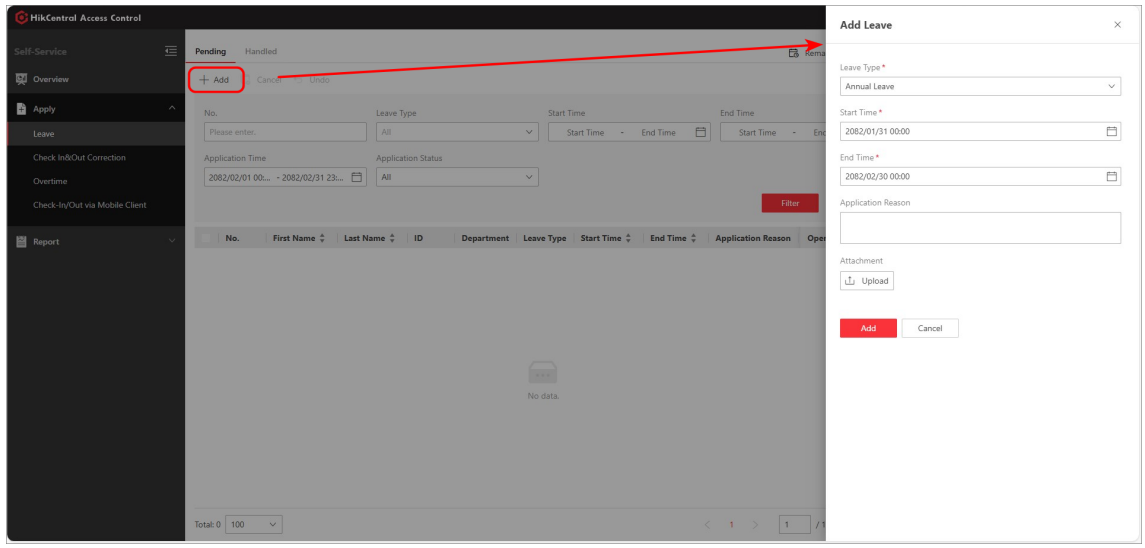


Figure 8-28 Via the Web Client

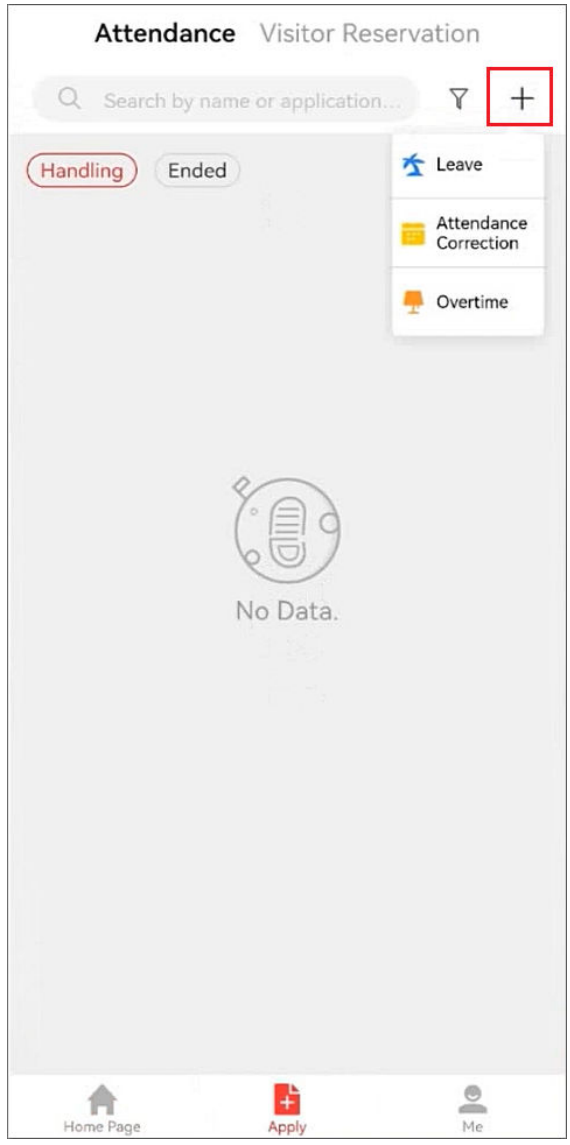


Figure 8-29 Via the Mobile Client

8.10.5 Step 5: Reviewers Review Applications

Reviewers review applications from employees via the Web Client or the Mobile Client. Persons to be notified (if any) can view the application flow.

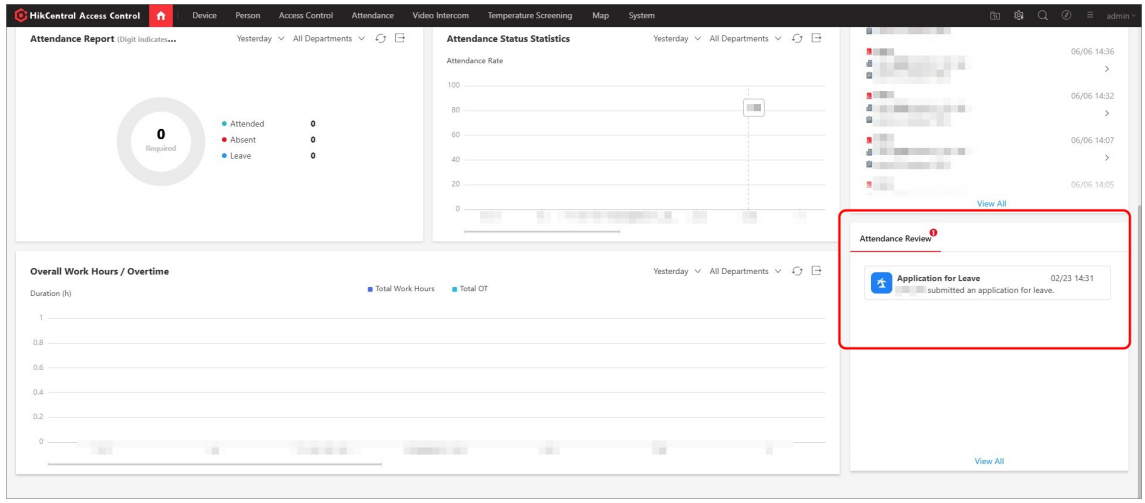


Figure 8-30 Via the Web Client

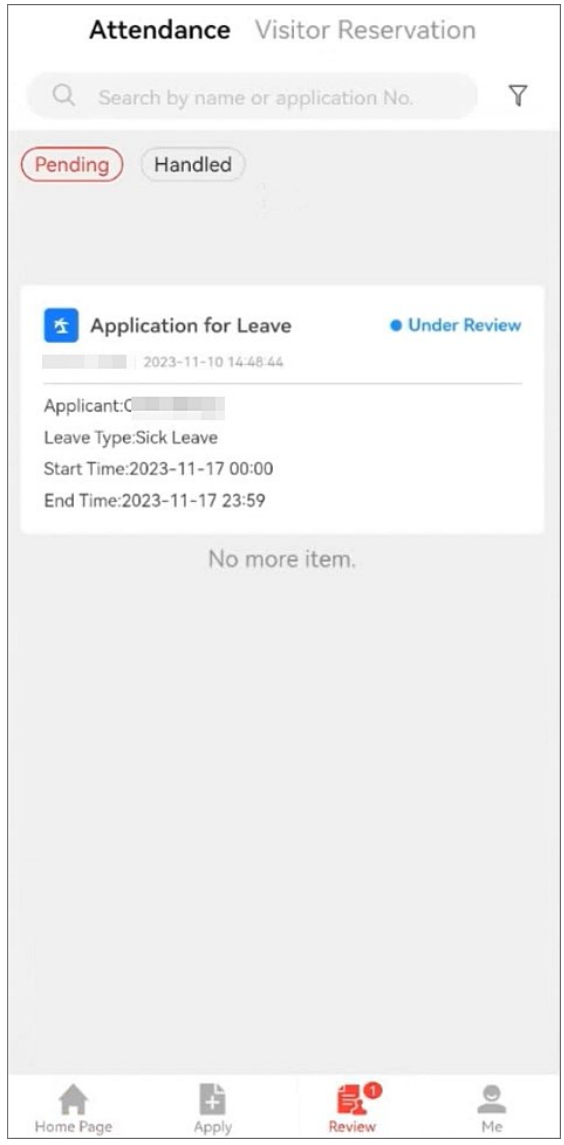


Figure 8-31 Via the Mobile Client

8.10.6 Step 6: Employees Check Application Status

After applications are reviewed, employees can check their application status on the page where they submit the application via the Web Client or the Mobile Client (Self-Service).

8.11 Application Management for Admin

The persons' attendance records will be recorded and stored in the system. As the administrator, you can search for the target persons and perform attendance applications for a single person or

multiple persons according to the actual need, including applying for leave, overtime, and attendance correction. After submitting applications, you can view the application details and status of each handling. You can also review (approve or reject) and undo applications.

Go to **Attendance → Application and Approval** .

8.11.1 Apply for a Leave / Check-In/Out Correction / Overtime

As the administrator, you can apply for leaves and working overtime, and correcting the check-in or check-out records for the employee(s).

Select **Leave / Check-In/Out Correction / Overtime** and click **Add** in the top left corner.

Select a person or multiple persons and set required parameters.

Leave Type / Correction Item / Overtime Type

- **Leave Type**: Sick leave, maternity leave, annual leave, etc.
- **Correction Item**: The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.
- **Overtime Type**: OT1, OT2, and OT3.

Application Reason (Optional)

The application reason for the leave / correction / overtime.

Attachment (Optional)

The attachment for the leave / correction / overtime application, such as the medical records for sick leave, the certificate of the right attendance time, attendance records, etc.

Auto Approve (Optional)

If the box is checked, the added application for the person will be approved automatically.

After applications, you can click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.

You can also review or undo the application. For details, refer to ***Review or Undo Applications*** .

8.11.2 Import Applications

As the administrator, you can batch apply for leave, overtime, or attendance correction for multiple employees.

Steps

1. Select **Application and Approval → Leave / Check-In&Out Correction / Overtime** on the left.
2. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
3. Click **Import**.
4. In the pop-up window, click **Download Template** and edit the related information in the downloaded template.

5. Click and import the template with the corrected attendance records.
6. Click **Import**.

What to do next
You can review or undo the imported applications. For details, refer to ***Review or Undo Applications*** .

8.11.3 Review or Undo Applications

As an administrator, after applying for employees' leave, overtime, attendance correction, or check in&out via Mobile Client, you can review (including approving or rejecting) or undoing the application.

1. On the left, select **Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client**.
2. (Optional) Click to filter the target employee by setting conditions (such as name, ID, department).
3. Select the target employee, the employee's application flow will be displayed on the right.
4. You can perform the following operations.
   - (Optional) Click to view the check in/out areas of the employee.
   - Check employee(s) and click **Approve** to approve the employee's attendance application.
   - Check employee(s) and click **Reject** to reject the employee's attendance application.
   - Check employee(s) and click **Undo** to undo the employee's attendance application.

8.12 Application Management for Employee

If you are an employee, you can log in to the Self-Service module where you can have an overview of your attendance records, review applications (if you are an administrator and assigned with the approval role as reviewer), and view your schedule. Besides, in this module, you can submit applications for leave, overtime, or attendance correction, and view the details and the handling status of applications. You can also view and export attendance records.

8.12.1 Login via Web Client (Employee)

Employees can access the system via web browser.

Before You Start
The administrator should enable self-service login and set the login password for employees.

Steps
1. In the address bar of the web browser, input the address of the PC running SYS service and press the **Enter** key.

Example

If the IP address of the PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

2. Select the **Self-Service** tab.
3. Enter the employee ID and password.
4. Click **Log In** to log in to the system.

Note

- Employees are required to change the password and set security questions for password retrieval upon the first login.
- If employees forget the password, they can retrieve the password in **Forgot Password** by answering security questions.
- If the password is expired, employees will be asked to change the password upon login.

Result

Web Client home page displays after employees successfully log in to the system.

8.12.2 Overview of Personal Attendance Data

You can have an overview of your attendance records in a specific time period, review applications, and view personal schedule.

When you log in to the Self-Service module, the overview page will be displayed, which shows the recent and history attendance statistics.

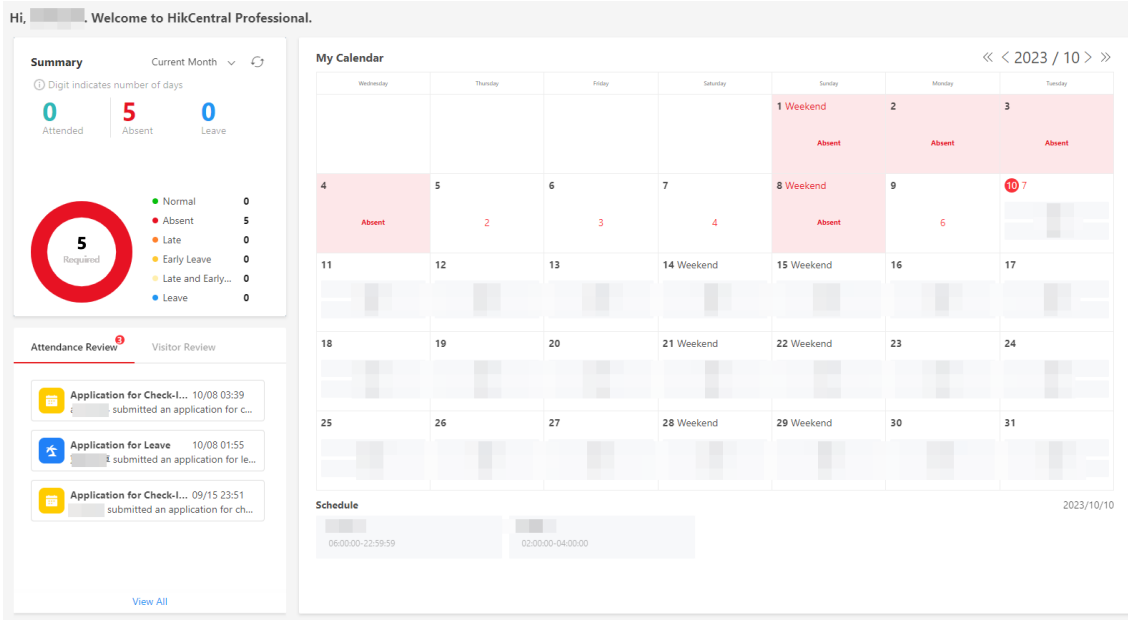


Figure 8-32 Overview of Personal Attendance Data

Summary	Click ⌄ to select a time period to view the attendance records in the time period.
My Calendar	You can have an overview of your attendance data and schedule in a month. Move the cursor to a day on the calendar and click ⚙, you can submit an application for the current day. For details about submitting applications, refer to ***Submit and View Applications*** .
Attendance/Visitor Review	You can select an application and click **Handle** to handle the application.
Schedule	View personal schedule.

8.12.3 Submit and View Applications

As an employee, you can submit attendance applications for leave, overtime, or attendance correction, and the applications will be reviewed by the administrator. Also, you can view the application details and the application flow to know the status of each handling.

On the lest, go to **Apply → Leave / Check-In/Out Correction / Overtime → Pending → Add** .

Leave Type / Correction Item / Overtime Type

- **Leave Type**: Sick leave, maternity leave, annual leave, etc.
- **Correction Item**: The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.
- **Overtime Type**: OT1, OT2, and OT3.

Application Reason (Optional)

The application reason for the leave / correction / overtime.

Attachment (Optional)

The attachment for the leave / correction / overtime application, such as the medical records for sick leave, the certificate of the right attendance time, attendance records, etc.

After applications, you can view and export them. For details, refer to ***View and Export Attendance Records and Reports*** .

(Employee) Review or Undo Submitted Applications

The employee can review or undo the submitted application(s) for attendance after logging into the self-service account.

Select **Review → Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client** on the left. Select the **Pending** or **Handled** tab.

You can perform the following operations in the Operation column after checking applications.

- Click to approve the employee's attendance application.
- Click to reject the employee's attendance application.

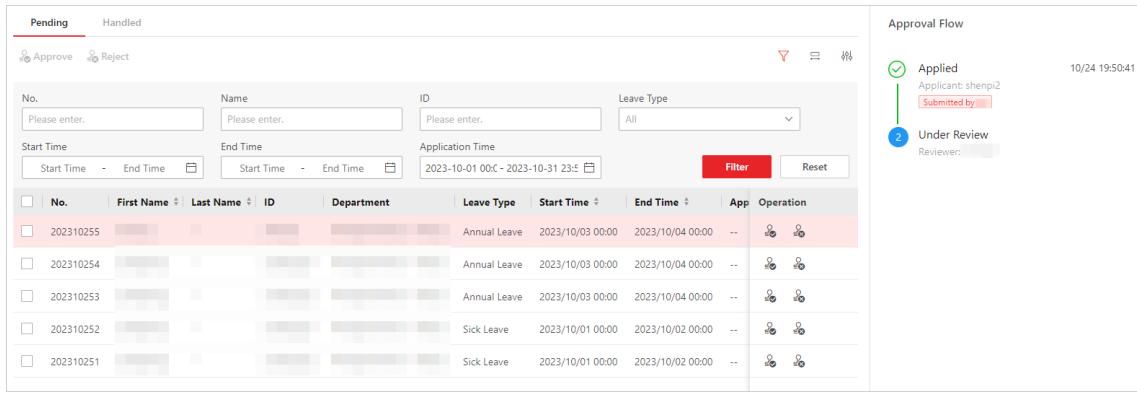


Figure 8-33 Review Employees' Applications

8.12.4 (Administrator) Review Employees' Applications

After employees submit the attendance applications for leave, overtime, attendance correction, and check-in/out via Mobile Client, the administrator should review (including approving or rejecting) or undo the employee's applications.

On the left, select **Review → Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client** .

Click to filter target employees by setting conditions (such as name, ID, department). Select the target employee, the employee's application flow will be displayed on the right.

You can perform the following operations in the Operation column for application review.

- Click to approve the employee's attendance application.
- Click to reject the employee's attendance application.
- Click to undo the employee's attendance application.

You can also select multiple employees to review or undo the employee's attendance applications in a batch.

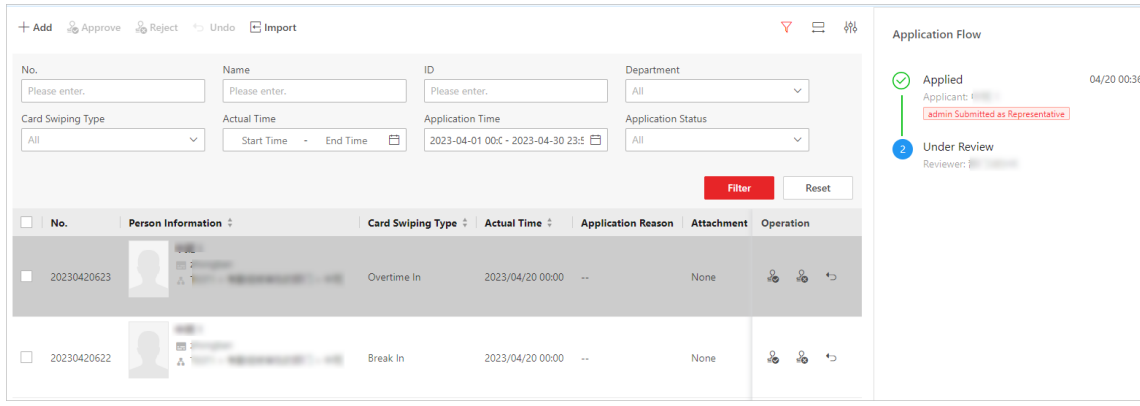


Figure 8-34 Review or Undo Employees' Applications

8.12.5 View and Export Attendance Records and Reports

As an employee, you can view the attendance records and reports. Also, you can export the records or reports in the file format of Excel, PDF, or CSV.

1. Select **Report** on the left.
2. Select the menu item as needed to view the records or report details.
3. You can perform the following operations in the Operation column for application review.
   - Click **Export** to export the records or reports in the file format of Excel, PDF, or CSV.
   - On the top-right corner, click to select the type of self-adaptive column width (complete or incomplete display of each column title).
   - On the top-right corner, click to select the items for custom display in the column.

8.13 View Attendance Records

Persons' attendance records will be recorded and stored in the system. You can view different types of attendance records.

On the top, select **Attendance**. Then select **Attendance Record** on the left.

Click **Transaction**, **Time Card**, **Check In&Out Record**, **First & Last Access Report**, **Leave Record**, **Check In&Out Correction Record**, and **Overtime Record** according to your need.

You can perform the following operations on the pages of attendance records.

- Click **Export** to export the report in Excel, PDF, or CSV format. You can also select the calculating dimension of the report.
- For transactions, click **Import** to import transactions recorded in files or devices to the system.
- Click to customize column items.
- After customizing column items, click **Save Layout** to save the current layout for later use.

  Exporting Allowed

After enabled, the layout can be exported in the report.

Sharing Allowed

After enabled, the layout will be shared among accounts.

Fixed Date

After enabled, you can set a specific time period for attendance data displayed the layout. Only attendance data generated during this time period will be displayed in the layout.

- Click **Load Layout** to display the report in a layout shared by other users. You can search for a layout before loading it. For layout saved by yourself, you can edit or delete them.
- Click ⇆ to display each column title completely/incompletely.

8.13.1 Import Transactions

Transactions on the attendance check devices could fail to be transmitted to HikCentral Access Control due to many causes, such as device offline and network connection failure. Or some of your attendance check devices are not added to the platform, but you still need to manage their transactions on the platform. You can use this function to get the latest transactions from the devices.

Select **Attendance Record → Transaction → Import → Import from Device / Import from File** .

Import from Device

Applicable to getting the latest transactions on the attendance check devices that are added to the platform.
Select the devices that store the transactions, and then select the time range to be imported. Click **OK** to import the transactions within the range on the selected devices.

Import from File

Applicable to attendance check devices added or not added to the platform.

Note

For devices that are not added to the platform, you need to make sure that the devices are supported by the platform. See *HikCentral Access Control Compatibility List* for reference.

Many attendance check devices have the ability to export a file that contains persons' transactions. You can import the file to the platform so that the transactions can be managed on the platform.

Note

- To export the data file on an attendance check device, please refer to the user manual of the device.
- Usually, you need to enter the back-stage management page of the device to export the event file to a connected external storage device via USB port, and then transfer the event file to the PC where the platform runs.

8.14 Manage Attendance Reports

Attendance report is the statistics of the attendance results of the specific department(s) or person(s) in a certain time period. For example, the employer or related persons can view the employees' attendance via attendance report and make it as the standard of performance evaluation or pay calculation. You can define the display rules on the report, set the rule of sending reports regularly, add a custom report, and manually export reports.

8.14.1 Set Display Rules for Attendance Report

You can configure the contents displayed in the attendance report, such as the company name, logo, date format, time format.

On the top, select **Attendance**.

Company Information

The company information (including company name and logo) will be displayed on the cover page of the attendance report. You can customize the company name. You can also upload a picture for the logo.

Note

Hover over your cursor on the uploaded logo picture, and you can click **Delete Logo** to delete the picture.

Format of Date and Time

The formats of date and time may vary for the persons in different countries or regions. You can set the date format and time format according to the actual needs.

8.14.2 View Daily/Weekly/Monthly/Summary Attendance Reports

You can view and export daily/weekly/monthly/summary attendance reports.

In the Attendance module, select **Daily Report**, **Weekly Report**, **Monthly Report**, or **Summary Report** on the left as needed.

Note

For the weekly/monthly report, you can also click on the top navigation bar, and then click **Total Time Card** / **Weekly Details** / **Monthly Details** to quickly go to the pages.

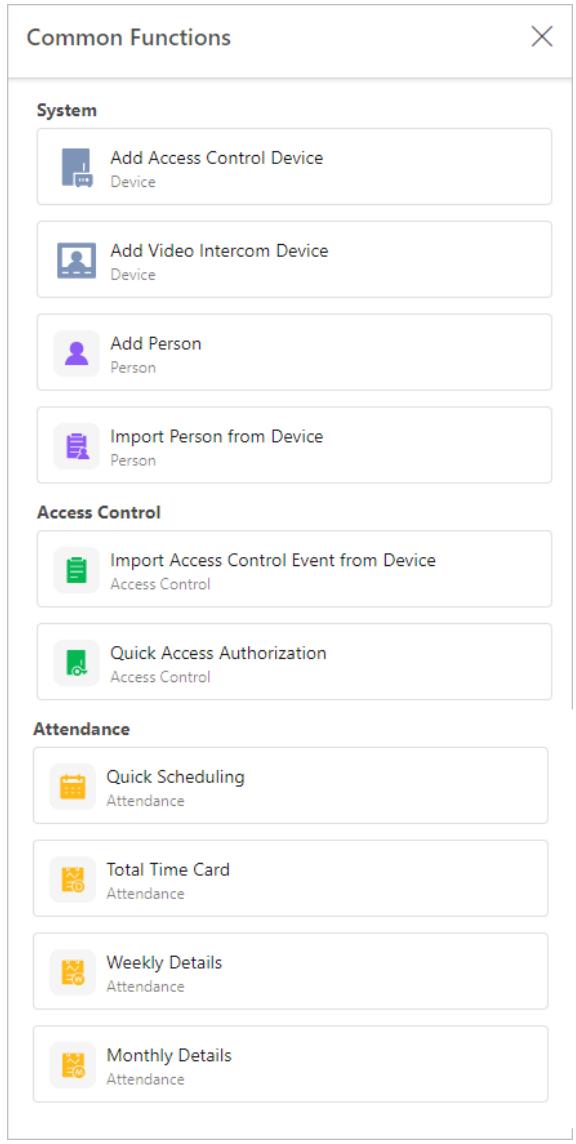


Figure 8-35 Common Functions

Report Type	Description
Daily Report	Daily report shows data on a daily basis. The report contains data recorded on the day prior to the current day.
Weekly Report	The report contains the persons' attendance results of the recent one week.

Report Type	Description
Monthly Report	The report contains the persons' attendance results of the current month.
Summary Report	The summary report provides an overview of the person's/ group's/department's attendance results.

Under these four types of reports, you can select a report as needed.

For some kinds of reports, you can perform the following operations as needed.

- Click **Export** to export the report in Excel, PDF, or CSV format. You can also select the calculating dimension of the report.
- Click **Select Person(s)** and select the desired persons to filter the attendance report by person.
- Click and select the desired time range to filter the attendance report by time range.
- Click and select the order to sort the attendance report.
- Click to customize column items. Custom person information added in **Person → Additional Information** will also be displayed in the items.
- After customizing column items, click **Save Layout** to save the current layout for later use.

  Exporting Allowed

  After enabled, the layout can be exported in the report.

  Sharing Allowed

  After enabled, the layout will be shared among accounts.

  Fixed Date

  After enabled, you can set a specific time period for attendance data displayed in the layout. Only attendance data generated during this time period will be displayed in the layout.
- Click **Load Layout** to display the layouts saved by you and the layouts shared by other users. After loading layouts, you can search for a specific layout, and edit or delete the layouts you saved.
- Click to display each column title completely/incompletely.

8.14.3 Send Attendance Report Regularly

You can set a regular report rule for specific departments, and the platform will send an emails attached with a report (an Excel file) to the recipients daily, weekly, or monthly, showing the attendance records of the persons in these departments during specific periods.

Before You Start

- Set the email template with recipient information, subject, and content.
- Set the email parameters such as sender address, SMTP server address and port, etc.

Steps

1. Select **Basic Configuration → Report Settings → Scheduled Report** on the left.

2. Click **Add** (for first time) or click + .
3. Create a report name.
4. Select a type and language for the scheduled report.
5. In **Statistics Content**, select the **Person Selection Method** as **Department** or **Attendance Group**.

Note

- For Department Attendance / Overtime Summary, you can only select departments. For Group Attendance / Overtime Summary, you can only select attendance groups.
- You can check **Include Sub-Department** to display the persons of sub-departments.
- You can click and filter persons by status (all, employed, or resigned).

6. **Optional:** For reports excluding Attendance/Overtime Summary and Attendance/Overtime Summary, click **Select Extra Person**, and click to include individual persons whose attendance data will be delivered in this report.
7. In the **Time Settings** section, set the statistical cycle to **By Day**, **By Week**, or **By Month** and set the report time range and sending time.

Report Time

Previous day

Daily report shows data on a daily basis. The platform will send one report at the sending time every day. The report contains data recorded on the day prior to the current day.

For example, if you set the sending time to 20:00, the system will send a report at 20:00 every day, containing the persons' attendance results between 00:00 and 24:00 prior to the current day.

Last 7 Days / Last 14 Days

The platform will send one report at the sending time every one or two week(s). The report contains the persons' attendance results of the recent one/two weeks.

For example, for weekly report, if you set the sending time to 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing persons' attendance results of the last week or recent two weeks based on your selection.

Current Month / Last Month

The platform will send one report at the sending time every month. The report contains the persons' attendance results of the current/last month of the sending date.

Note

To ensure the accuracy of the report, you are recommended to set the sending time at least one hour later than the auto-calculation time of the attendance results. By default, the platform will calculate the attendance results of the previous day at 4 A.M. every day. You can change the auto calculation time in General Rule. See details in ***Set Auto-Calculation Time of Attendance Results*** .

8. In the Export Settings, select a format for the report.

Note

If you select PDF, you can customize the paper size and direction of printing.

9. **Optional:** Select and enable the way of sending the report from **Send via Email**, **Upload to SFTP**, and **Save to Local Storage**.

Note

- If you enable **Send via Email**, you can click **Add** to add a new email template.
- To set up the SFTP or local storage, click > **SFTP Settings** or **Configure Local Storage**.

10. Click **Save** to save the report schedule.

The report will be generated and sent to the recipient at the specified sending time.

8.14.4 Add a Custom Report

You can create a fully-customized attendance report. After creating a custom report, you can export the report manually or set a schedule to send the report to your email regularly.

Steps

1. On the top, go to **Attendance → Custom Report** .
2. Click + to add a custom report.
3. Create a descriptive name for the report in the **Report Name** field.
4. Choose whether to merge the data of the same person/department/date.
5. Select a sorting rule for records from the **Table Display Rule** drop-down list.
6. Select the data items you want to include in the report from **Optional Fields**.
   - Custom fields will be displayed if you have added additional person information in **Person → Additional Information** . These fields can be exported in the report.
   - You can drag the items in **Selected Fields** to set the order of the items.
7. **Optional:** Click **Preview** to view the report to make sure the format and content are correct.
8. Click **Add** to save the custom report, or click **Add and Continue** to add another one.
9. **Optional:** Perform further operations.

Edit Report	Select a report and click to edit it.
Delete Report	Select a report and click to delete it, or click → **Delete All** to delete all reports.
Export Report	Click **Export** and specify the departments, target persons, time range, and report format to export the report to the PC. See ***Export a Custom Report*** .
Send Report Regularly	You can set a schedule to send the report regularly. See details in ***Send Attendance Report Regularly*** .

Export a Custom Report

You can specify the department / attendance group, time period, and format to export a custom report to your local PC.

Before You Start

Make sure you have ***added a custom report*** .

Steps

1. Select a custom report on the left pane, and click **Export** to open the Export Settings page.
2. On the Person Selection Method area, select **Department** / **Attendance Group**.
3. Check the desired departments / attendance groups.

   If you select **Department**, you can check **Include Sub-Department** to display the persons of sub-departments. You can also click to filter persons by status (all, employed, or resigned).
4. **Optional:** Click **Select Extra Persons**, and click to include individual persons whose attendance data will be delivered in this report.
   - You can check **Include Sub-Department** to display the persons of sub-departments.
   - You can click and select person status (all, employed, or resigned), or enable **Additional Information** and enter the keyword in the text field to search for matched persons.
5. Specify the time period by selecting the predefined time period, or clicking **Custom** to customize the start and end date.
6. Specify the report format.

   If you select PDF, you can customize the paper size and direction of printing.
7. Enter password and click **Export** to export the custom report to the local PC.

Chapter 9 Video Intercom Management

Video intercom is an audiovisual communication and security technique used in a building or a small collection of buildings. With microphones and cameras at both sides, it enables the intercommunication via video and audio signals and provides a safe and easy monitoring solution for apartment buildings and private houses.

On the Web Client, you can add video intercom devices to the system, group resources (e.g., doors) into different areas, configure call schedules, link resources (persons, and doorbells) with indoor station, manage notices, call indoor stations, and view recents.

On the top, select **Video Intercom**.

9.1 Flow Chart of Video Intercom

For the first time, you can follow the flow chart to perform configurations and operations.

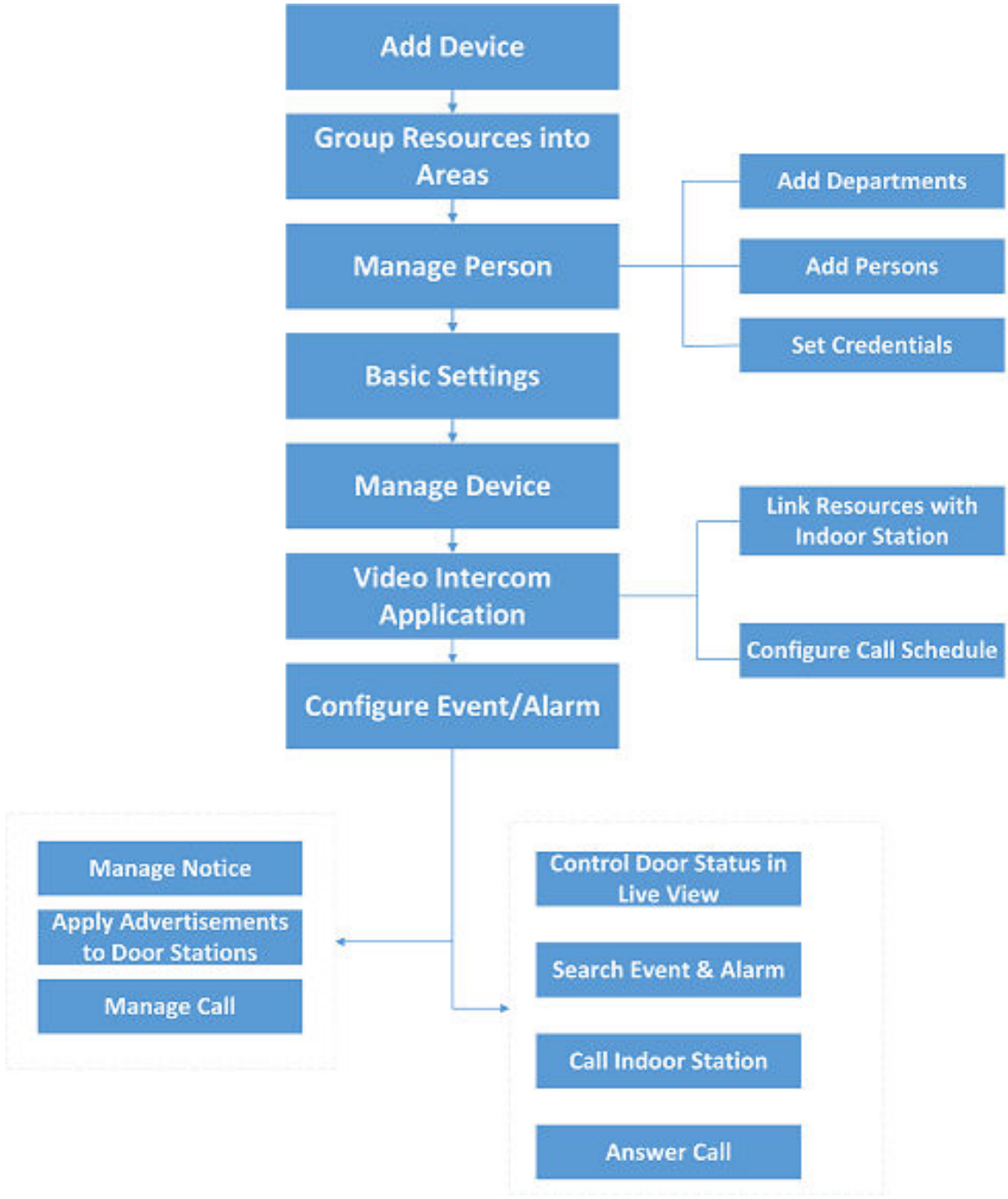


Figure 9-1 Flow Chart of Video Intercom

- **Add Device**: Add video intercom devices (such as main station, outer door station, indoor station, and door station) to HikCentral Access Control and configure device parameters remotely.
- **Group Resources into Areas**: After adding the devices to the system, you need to group the devices' resources (such as doors) into different areas according to the resources' locations.
- **Manage Person**: Add departments and persons to the system, and set credential information.

- **Basic Settings**: Add call recipients, add call schedule templates, add receiving schedule template, and configure call parameters.
- **Manage Device**: Set location information for video intercom devices and apply the settings to devices.
- **Video Intercom Application**: Add call schedules and apply them to devices, link resources (person, and doorbell) to indoor stations.
- **Configure Event / Alarm**: Configure event and alarm for video intercom resources.
- **Manage Notice**: Add notices and apply them to indoor stations.
- **Apply Advertisements to Door Stations**: Apply pictures or video to door stations as advertisements.
- **Manage Call**: Call indoor stations and view recents.

9.2 Add Video Intercom Device

Device Management

1. Select **Device Management** on the left.
2. Select **Add** to set the basic information and location information.
3. Select **Apply Settings**, select devices and the applying mode, and select **Apply** to apply the location information to devices.

9.3 Configure Device Parameters

After adding the video intercom devices, you can configure parameters for them remotely, including device time, maintenance settings, etc.

After adding a video intercom device, click ⚙ in the **Operation** column to configure the device.

Note

The parameters may vary with different models of devices.

Time

You can view the time zone where the device locates and set the following parameters.

Device Time

Click **Device Time** field to customize time for the device.

Sync with Server Time

Synchronize the device time with that of the SYS server of the system.

Call Management Center

For door station, you can set this function switch to on and select a shortcut button. When the configured button on the device is pressed, it will call management center. The default button is 1.

Note

This should be supported by the device.

Card Swiping

For outer door station and door station which supports M1 encryption, you can enable **M1 Encryption** and select the sector. Only the card with the same encrypted sector can be granted by swiping the card on the card reader.

Maintenance

You can reboot a device remotely, and restore it to its default settings.

Reboot

Reboot the device.

Restore Default

Restore the device to its default settings. The device should be activated after restoring.

More

For more configurations, you can click **Configure** to go to Remote Configuration page of the device.

9.4 Add a Call Schedule for a Door Station

You can add a call schedule for a door station to configure when door stations can call indoor stations or management centers.

Steps

1. On the top, select **Video Intercom Application → Door Station Call Schedule Settings** .
2. Select **Add** to add a door station call schedule.
3. Select a door station in the list.
4. Add a call schedule template. Click **Add Call Schedule Template** to set the template name, weekly schedule template, and holiday schedule, and select a room number for each button.
   1) Select **Add Call Schedule Template**.
   2) Set the template name.
   3) Select an existing template from the **Copy from** the drop-down list.
   4) Select **Indoor Station** if there is someone indoor who can answer the call from the door station and select **Management Center** if there is no one who can answer the call.
   5) Configure the weekly schedule.

Operations	How To
Draw Task Time	Click a grid or drag the cursor on the time line to draw a time period during which the task is activated.
Set Precise Time	Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as  .

6) **Optional:** Select **Add Holiday** to select an existing holiday template, or select **Add** to add a new template.

Note

If you configure a template for a management center, the Room cannot be selected.

5. Click **Add** to save the schedule.
6. Select **Apply Settings** to apply call schedules to devices.
7. **Optional:** To add call templates to devices in a batch, select **Batch Import Call Schedule → Download Template** , fill in the template, upload the template, and select **Import**.

9.5 Link Resources with Indoor Stations

After adding an indoor station to the plaform, you can link persons with an indoor station. You can also relate a doorbell with an indoor station. When the Call Management Center function of this doorbell is disabled, you can call the related indoor station by the doorbell.

9.5.1 Link Doorbell to Indoor Station

Steps

1. On the left pane, select **Video Intercom Application → Link Doorbell to Indoor Station** .
2. Select **Link** to enter the Link Doorbell with Indoor Station page.
3. From the drop-down list of **Device Name**, select a location. And then select the doorbell to be linked to the indoor station.
4. In the indoor station list, select the corresponding indoor station that the doorbell is to be linked to and click **Add**.

Note

The location information of the indoor station is the same as that of the doorbell.

9.5.2 Link Persons to Indoor Station

Steps

1. Select **Video Intercom Application → Link Person to Indoor Station** on the left.
2. Click **Link**.

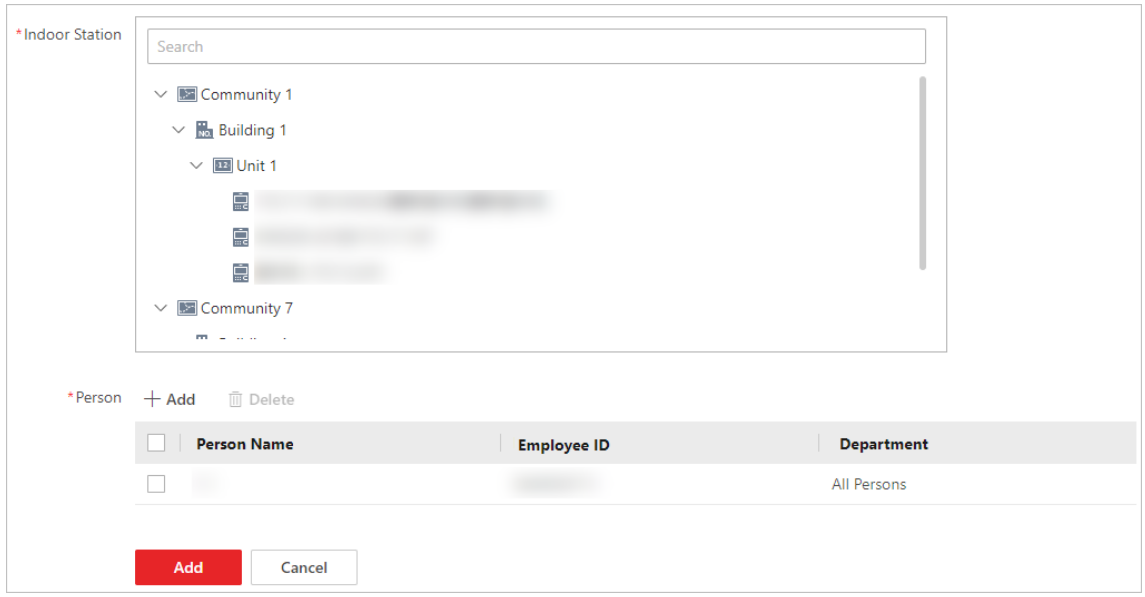


Figure 9-2 Add Linked Person

3. Select an indoor station.

Note

Up to 10 persons can be linked to an indoor station and the person cannot be linked to multiple indoor stations.

4. Click **Add** to select persons to be linked to the indoor station.
5. Click **Add**.

9.6 Apply Data to Indoor Station

You can apply notices to an indoor station to alert people in emergencies or install a software on indoor stations to expand their functions. After applying a software package to the indoor stations, the software will be installed automatically.

9.6.1 Add and Apply a Notice

There are four types of notice, including advertisement, property information, alarm, and notification. They are used for sending information to residents. You can add and apply notices to

indoor stations. For example, when an emergency occur, you can add and apply a notice to indoor stations to inform residents for timely actions. After adding and applying notices, you can delete, filter, and export them. You can also copy a notice and apply it to indoor stations conveniently.

1. On the top, select **Apply Data to Indoor Station → Manage Notice** .
2. Select the **Apply Notice** tab, and select **Add** to add a notice.
3. Configure the notice.
   a. Create a title of the notice and set the notice type.
   b. Select + to add pictures.

   Note

   Up to 6 JPG pictures can be added, and each picture should be no larger than 512 KB.

   c. Enter the content of the notice.
   d. Select indoor stations to receive the notice.
4. Select **Preview** to preview the notice.
5. Select **Apply** to apply the notice to indoor stations.
6. (Optional) Select the **Apply Notice** tab.
   - Select one or more notices, and select **Copy and Apply** to apply notices to indoor stations.
   - If you want to edit the notice content, select to copy the current notice and edit the notice as needed. Select **Apply** to apply the notice to indoor stations.

Add and Apply a Notice

You add and apply notices to indoor stations. After adding and applying notices, you can delete, filter, and export them.

Steps

1. On the top, select **Video Intercom → Apply Data to Indoor Station → Manage Notice** .
2. Select the **Apply Notice** tab, and click **Add** to add a notice.
3. Create a title of the notice.
4. Select a notice type.
5. **Optional:** Click + to add pictures.

   Note

   Up to 6 pictures can be added, and each picture should be no larger than 512 KB. The picture format should be JPG.

6. Enter the content of the notice.
7. Select indoor stations to receive the notice.
8. Click **Preview** to preview the notice.
9. Click **Apply** to apply the notice to indoor stations.
10. **Optional:** Perform the following operations.

Delete Notice	Check one or more notices and click **Delete**.

Export Notice	Check one or more notices and click **Export** to export notice information to the Excel/CVS file.
Filter Notices	In the upper-right corner, click to set filter conditions and click **Filter**.
View Notice Details	Click to view the basic information (title, notice type, etc.) and application status.

Note

On the Application Status page, you can also apply or search for notices.

Copy and Apply Notice to Indoor Stations

You can copy a notice and apply it to indoor stations conveniently. Before application, you can also edit the copied notice.

Note

Make sure you have added and applied a notice to indoor stations.

On the top, select **Video Intercom**. Then, select **Apply Data to Indoor Station → Manage Notice** on the left.

Select the **Apply Notice** tab.

The followings are two methods for copying and applying the notice(s).

1. If notice information needs no change, check one or more notices, and click **Copy and Apply**. The checked notice(s) will be copied and applied to indoor stations directly.
2. If notice information needs change, click to copy the current notice and edit the notice as needed. Click **Apply** to apply the notice to indoor stations.

9.6.2 Apply Software Package to Indoor Station

This function is only supported by certain models.

Steps

1. On the top, select **Apply Data to Indoor Station → Apply Software Package** .
2. Click **Apply Software Package**.
3. Select **All Indoor Stations** or **Specified Indoor Station(s)**.

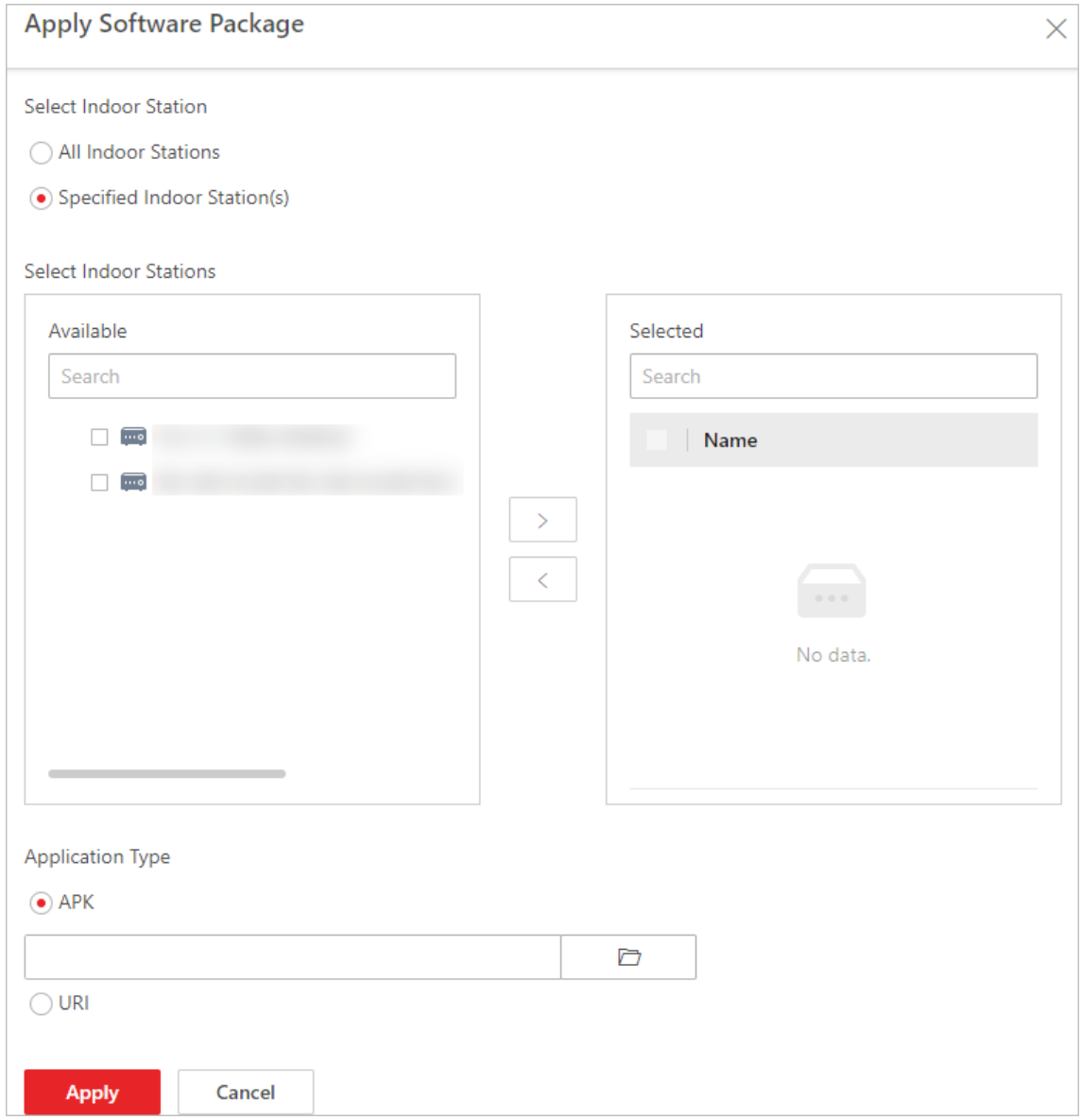


Figure 9-3 Apply Software Package

4. Select an application type.
5. Select **Apply**.

9.7 Make and Receive Calls on Platform

You can configure a receiving schedule template to define when the platform user can receive calls. After configuring receiving schedule templates, you can adding platform users as call recipients. When someone calls the platform, the added recipients can receive and answer the call.

9.7.1 Add Call Schedule Template

Steps

1. **Basic Configuration → Call Schedule Template** .
2. Select + to add a schedule template.

   You cannot edit or delete The two default templates, namely All-Day Call Schedule Template for Indoor Station and All-Day Call Schedule Template for Call Center.
3. Configure the template.
   1) Create a name for the template.
   2) **Optional:** Select an existing template from the **Copy from** drop-down list.
   3) Select **Indoor Station** if there is someone indoor who can answer the call from the door station and select **Management Center** if there is no one who can answer the call.
   4) Set the weekly schedule.

Operations	Description
Set Task Time	Click a grid or drag the cursor on the time line to draw a time period during which the task is activated.
Set Precise Time	Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as  .

   5) **Optional:** Select **Add Holiday** to select an existing holiday template, or click **Add** to add a new template.
4. Select **Add** to save the template.

9.7.2 Add Call Recipients

Go to **System → Call Settings → Call Recipient** .

9.8 Apply Advertisements to Door Stations

You can add pictures or videos in the advertisements, then apply the advertisements to door stations. After applying advertisements, you can filter or delete them. This function is only supported by this model: DS-KD9403-E6.

Steps

1. On the top, select **Video Intercom → Apply Advertisements to Door Stations** .
2. Click **Apply Advertisements to Door Stations** on the top.
3. Select the available door station in the left list and click › to add it to the right list.

4. Add picture(s) or a video for an advertisement to be applied to door stations.

Note

For the picture advertisement, you can add up to six pictures. For the video advertisement, you can add up to three videos.

- a. Click **Picture** → + to add picture(s) for an advertisement.
  b. Set the **Picture Switching Interval**.
  c. Set the time period to play the added picture(s).

  Note

  Click **Add** to add the time period if needed.
- a. Click **Video** → + to add a video for an advertisement.
  b. Set the time period to play the added video.

  Note

  Click **Add** to add the time period if needed.

5. The playing schedules set for the picture(s) and the video in the advertisement will be displayed by different color blocks.
6. Click **Apply**.

Chapter 10 Skin-Surface Temperature Screening

After adding the access control devices with temperature screening function to the system, you can view the temperature of the detected persons in the Skin-Surface Temperature module. The system also shows whether the detected person is wearing a mask or not. With skin-surface temperature screening and mask detection functions, the system provides an alert if an individual is running a fever or not wearing a mask.

In the Skin-Surface Temperature module, you can view the real-time and history temperature screening records and face mask detection records. You can also generate a report about these records to view the overall information.

Note

The mask detection function will show when the mask related function is turned on in the **System → Normal → User Preference** page.

10.1 Temperature Screening Configuration

Before temperature screening, you should set temperature screening point groups and add related temperature screening points to the added groups. Also, for the temperature screening points, you can configure their parameters including temperature screening threshold and alarm threshold.

10.1.1 Group Temperature Screening Points

You can group multiple temperature screening points for convenient management. For example, you can group all the temperature screening points on the same floor into a group.

Steps

1. On the top, select **Temperature**.
2. Select **Temperature Screening Configuration** on the left.
3. Create temperature screening point group(s).
   1) Click + on the upper left corner of the page.
   2) Enter the name for the temperature screening point group as desired.
   3) Click **Add**.
4. Add temperature screening point(s) for the added temperature screening point group.
   1) Click **Add**.
   2) In the pop-up device list, check temperature screening point(s) as desired.

      Note

      You can enter a key word (supports fuzzy search) in the search box to quickly search for the target device(s).

   3) Click **Add**.

5. **Optional:** After adding temperature screening point(s), perform following operations.

Delete	• Click to delete single temperature screening point. • Check multiple temperature screening points, and click **Delete** to batch delete the selected devices.
Configure Parameters	Check one or multiple temperature screening points, and click **Configuration** to configure related parameters for the selected device(s). **Note** For details, refer to ***Configure Temperature Screening Parameters*** .
Export	Click **Export** to export detailed information of temperature screening point(s) such as device type, serial No., and temperature screening threshold to the local PC.

10.1.2 Configure Temperature Screening Parameters

For the added temperature screening point(s), you can configure the related parameters including temperature screening threshold and alarm threshold.

Check one or more added temperature screening point(s), and click **Configuration** to configure temperature screening parameters.

Temperature Screening Threshold

Set the threshold for temperature screening. When the detected skin-surface temperature is higher than the threshold, a temperature screening event will be triggered.

Alarm Threshold

Set the threshold for alarm. When the detected skin-surface temperature is higher than the threshold, an alarm will be triggered.

Note

- The temperature screening threshold should be smaller than alarm threshold.
- For temperature screening points which are access control points, you should configure their temperature screening parameters on the device parameters configuration page.

10.2 Real-Time Skin-Surface Temperature Monitoring

You can view the latest skin-surface temperature information detected by screening points. If there are persons whose skin-surface temperatures are abnormal, you will know at the first time. Besides, you will be able to quickly locate the persons according to the displayed screening point name and screening group. For unregistered persons, you can quickly register for them.

On the top, select **Temperature**. Select **Skin-Surface Temperature** on the left. Select a temperature screening point group on the left. Red number indicates the number of skin-surface temperature screening points. Black number indicates the total number of devices in a temperature screening point group.

In the Picture area, the latest captured picture is displayed on the left. When new pictures are captured and displayed here, old captured pictures will be displayed on the right as thumbnails with faces, screening point name, person name, similarity, temperature, wearing mask or not, and detecting time.

Persons with different features will be marked by different colors. Orange means the captured person is not wearing a mask, but skin-surface temperature is normal; red means the captured person's skin-surface temperature is abnormal; green means the captured person's skin-surface temperature is normal and the person is wearing a mask. Click **More** to jump to the History page to view more captured pictures.

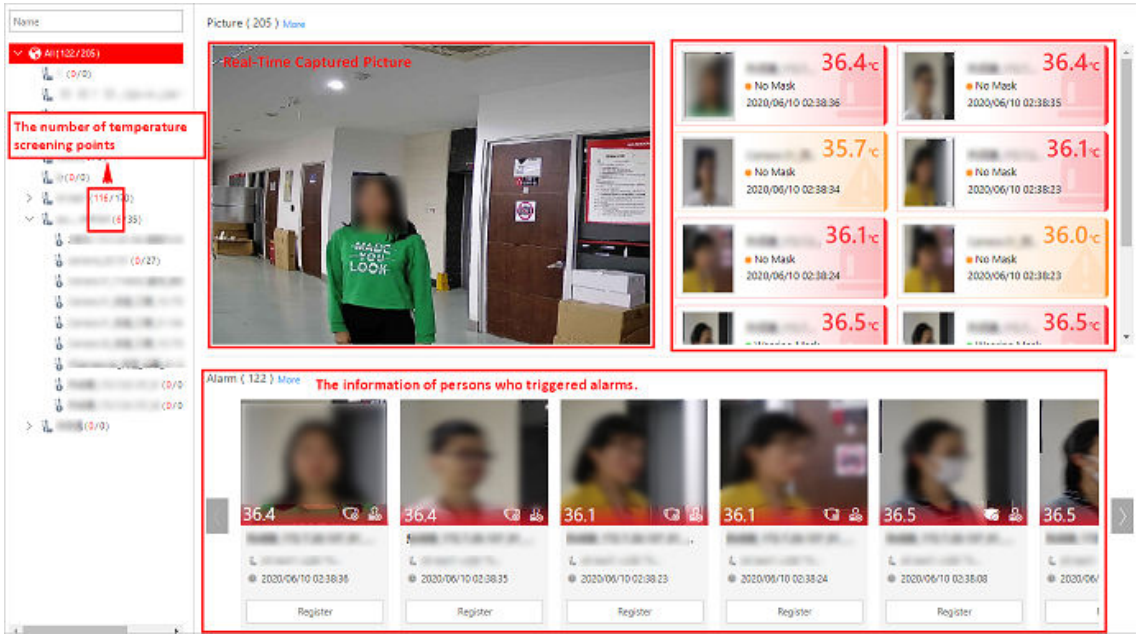


Figure 10-1 Real-Time Skin-Surface Temperature

When a person's skin-surface temperature exceeds the threshold you set, or the person is not wearing a mask, an alarm will be triggered. In the Alarm area, the pictures and information of persons who have triggered alarms are displayed. Following the title Alarm, the alarm amount is displayed. See *The User Manual of HikCentral Access Control Web Client* for details about how to set a temperature threshold.

The person information includes skin-surface temperature, wearing mask or not, registered or unregistered, temperature screening point name, temperature screening point group name, and detecting time. You can click **Register** to register for the person, or click **More** to go to the History page to view more alarm information.

10.3 Search History Temperature Screening Data

You can set search conditions such as start time, end time, and skin-surface temperature to search for history temperature screening data.

Before You Start
Make sure temperature screening data has been generated in real-time skin-surface temperature monitoring.

Steps
1. On the top, select **Temperature**.
2. Select **History** on the left.
3. Select a temperature screening point group or a temperature screening point from the list.
4. Click ▽ to unfold the Filter panel.
5. Set the search condition(s) including start time, end time, skin-surface temperature, etc.
6. Click **Filter**.

   History temperature screening data that meets the search condition(s) will be displayed below.
7. **Optional:** For the searched results, perform the following operations as desired.

View Result Details	You can view the detailed information of the searched results, including temperature screening group, temperature screening point, captured time, person's skin-surface temperature, whether wearing masks, etc. **Note**  represents that the person wears a mask, and  represents that the person doesn't wear a mask.
Edit/Register Person Information	You can edit or register person information based on the different icons. •  : The person is registered. For the registered person, click **Edit** to edit the person information. •  : The person is unregistered. For the unregistered person, click **Register** to enter person's registration information. For details, refer to ***Register Person Information*** .
Export	Click **Export** to export temperature screening data including temperature screening point, temperature screening point group, temperature status, etc., in excel file.

10.4 Registration

To manage the people who have been screened skin-surface temperature conveniently, you can register for them by entering their personal information. After registration, you can view and filter the registered persons' information.

10.4.1 Register Person Information

For unregistered persons displayed on real-time skin-surface temperature page or history page of skin-surface temperature, you can register for them.

Steps

1. On the top, select **Temperature**.
2. Select **Skin-Surface Temperature** or **History** on the left.

   The skin-surface temperature screening information will be displayed.
3. If a screened person is not registered, you can click **Register** to enter the Register page to register for the person.

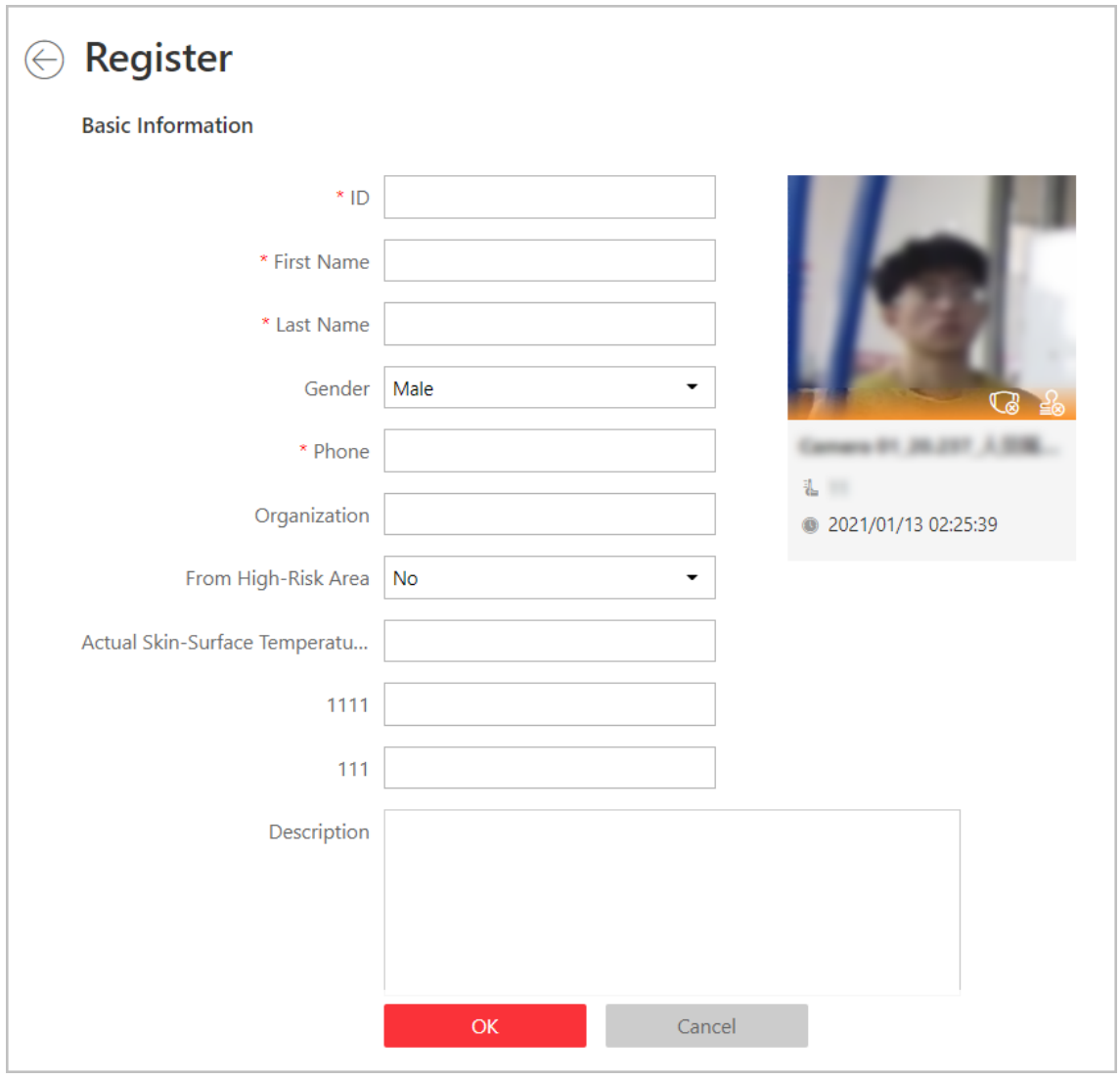


Figure 10-2 Register Page

4. Set personal information, including ID, name, phone number, whether from high-risk areas etc.

Note

You can custom the information displayed on this page according to your needs. See ***Customize Registration Template*** for details.

5. Click **OK** to finish the registration.

   Registered persons' information will be displayed on Registration page for a centralized management. See ***View Registered Person Information*** for details.

10.4.2 Customize Registration Template

You can set customized person information for registration which are not predefined in the system according to your actual needs.

Steps

Note

Up to 5 additional items can be added.

1. On the top, select **Temperature**.
2. Select **Registration** on the left.
3. Click **Registration Template** to enter the Registration Template page.
4. Click **Add**.
5. Create a name for the additional item.

   Note

   Up to 32 characters are allowed for the name.

6. Select the format type as general text, number, date or single selection for the additional item.

   Example

   For example, if you select general text, you need to enter words for this item when registering person information.

7. Click **Add**.
8. **Optional:** Perform one or more of the following operations.

Edit Name	Click to edit the name.
Delete	Click to delete the additional item.

10.4.3 View Registered Person Information

For the registered persons, you can view their detailed information including person name, ID, phone, skin-surface temperature, wearing mask or not, etc.

On the top, select **Temperature**. Select **Registration** on the left.

You can view person name, ID, phone, skin-surface temperature, wearing mask or not, registering time and other information in the list.

Click in the Operation column to edit person information as desired.

Click **Export** on the upper left corner of the page to export and view detailed registered person information in excel file.

10.5 Search for Temperature Screening Records

Skin-surface temperature screening records give you an overview of skin-surface temperature, mask-wearing detection results, and registered person information. Based on the temperature status and mask-wearing detection results, you will quickly learn how many person's skin-surface temperatures are abnormal and how many persons are not wearing masks. With registered person information, you can quickly filter persons with abnormal skin-surface temperature or with no mask on to learn their detailed information such as name, location, face picture, from high-risk area or not, etc.

On the top, select **Temperature**. Select **Report** on the left.

Select a temperature screening point group or temperature screening point, set the time range at the bottom and click **Generate Report**.

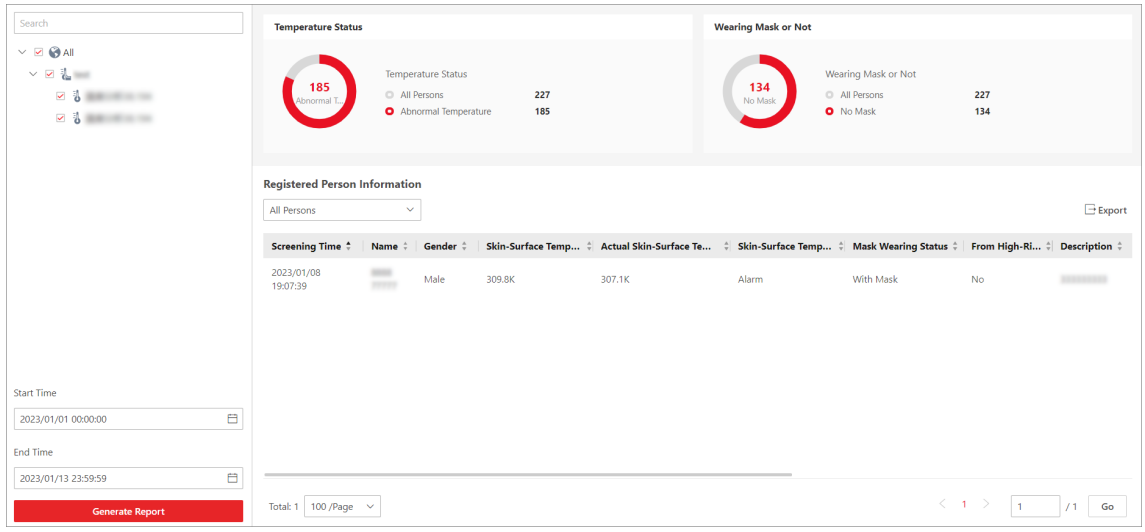


Figure 10-3 Skin-Surface Temperature Screening Records

Temperature Status

Temperature Status gives you the total number of persons whose skin-surface temperatures are screened and the number of persons with abnormal temperature.

Wearing Mask or Not

It gives you the total number of persons whose mask wearing status had been detected, and the number of persons with no mask on.

Registered Person Information

You can filter persons with abnormal skin-surface temperature or those not wearing any mask quickly to view their detailed information. For example, if a person with abnormal skin-surface temperature is not wearing a mask, you need to pay attention to him or her. Based on the temperature screening point name or temperature screening point group name, you can quickly locate the person.
Click to view a person's detailed information including an enlarged face picture, event details, and registered information.
Click **Export** to save the registered person information in your PC as an Excel file.

10.6 Configure the Scheduled Report of Screening

You can configure scheduled temperature screening analysis reports by specifying a statistical cycle, the analysis type, and the relevant statistical objects (i.e., temperature screening points or departments). Once set, the platform will send an email to the specified recipient(s) regularly with the report attached, which shows the variation trend of the number of people whose skin-surface temperatures are abnormal during the set time period.

Steps

Note

- A report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. On the top, select **Temperature Screening → Basic Configuration → Scheduled Report** .
2. Enter the Create Report page.
   - For configuring scheduled reports for the first time, click **Add** in the middle of the page.
   - If you have configured scheduled reports before, click + at the top of the left pane.

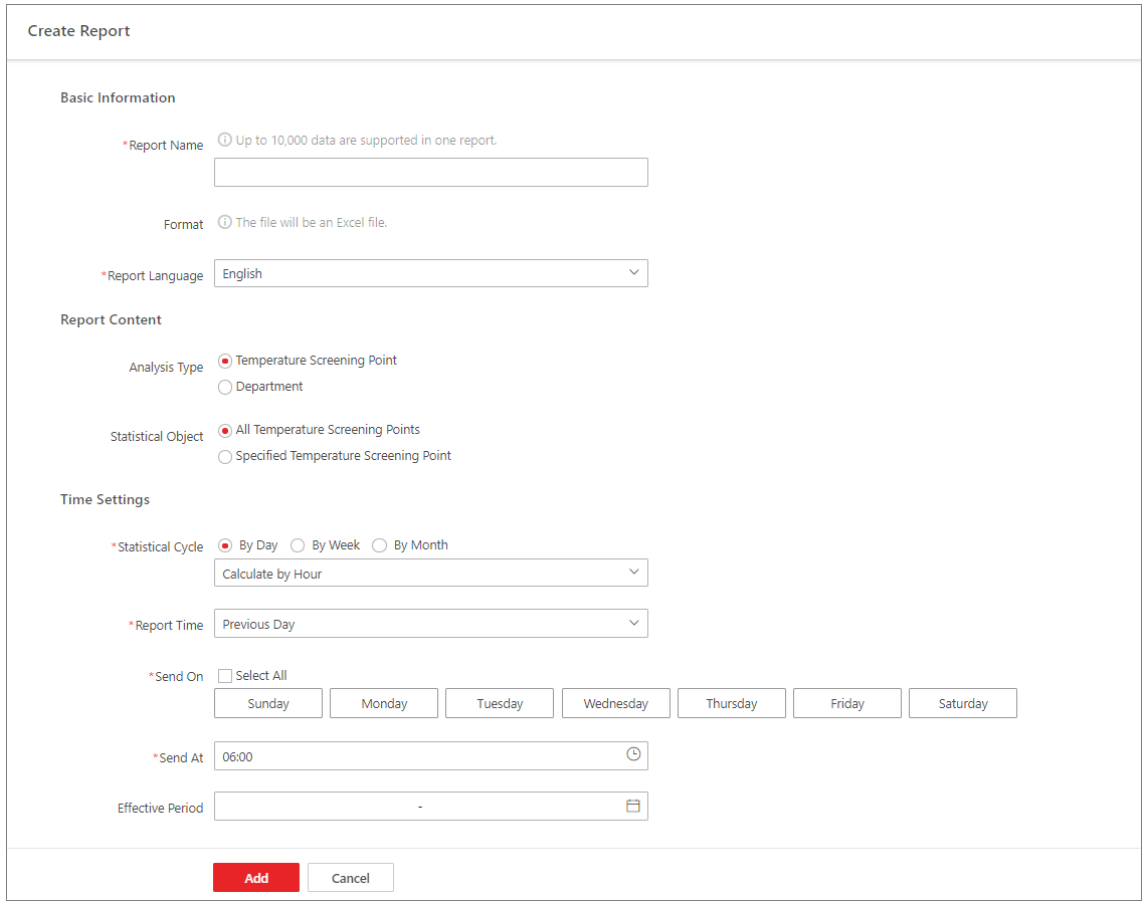


Figure 10-4 Configure Scheduled Report

3. Create a name for the report and select a report language from the drop-down list.
4. Set the report content.
   1) Select an analysis type from **Temperature Screening Point** and **Department**.
   2) Select the statistical objects accordingly. You can select all or specify specific temperature screening points / departments.

   Note

   If the analysis type is set to **Department**, you may also select the way you would like to export the report content from **By Department** and **By Person**.
5. Select a statistical cycle from **By Day**, **By Week**, and **By Month**, and set the statistical period and report sending time accordingly.

   By Day

   The daily report shows data on a daily basis. The platform will send one report at the set sending time on the specified day(s) with analysis results of the previous day.

For example, if you set the sending time as 20:00 and select all days of a week, the platform will send a report at 20:00 every day, containing the analysis results of the day before the current day between 00:00 and 24:00.

By Week or By Month

Compared with the daily report, the weekly/monthly report can be less time consuming, since they are not to be generated every day. The platform will send one report on the set day/date at the specified sending time every week/month with analysis results of the last 7/14 days or the current/last month respectively.

For example, for the weekly report, if you set the sending time as 6:00 on Monday and the statistical period as the last 7 days, the platform will send a report at 6:00 every Monday morning, containing the analysis results between last Monday and Sunday.

Note

If the analysis type is set to **Temperature Screening Point**, you may also set how the report will present the analysis results generated in the specified time period below the statistical cycle options. You can choose from **Calculate by Hour** and **Calculate by Day** accordingly.

6. **Optional:** Set an effective period (start time and end time) for the scheduled report.
7. **Optional:** Set the advanced parameters.

Send Report via Email

Select an email template from the drop-down list to define the recipient information and email format (subject and content), so that the report can be sent to the recipient(s) regularly via email.

Note

- You can select an existing email template or click **Add** to add a new one.

Upload to SFTP

Configure SFTP settings including the SFTP address, port No., user name, password, and the saving path for the report to be uploaded to the SFTP server regularly.

Note

You can also click → **SFTP Settings** at the top of the left pane to configure the corresponding parameters.

Save to Local Storage

Configure a saving path for the report to be saved to the local storage regularly.

Note

You can also click → **Configure Local Storage** at the top of the left pane to configure the saving path.

8. Click **Add** to finish setting the scheduled report rule.

10.7 Generate Skin-Surface Temperature Analysis Report

You can generate skin-surface temperature analysis reports to view the variation trend of the number of people with abnormal skin-surface temperature over a specified time period.

Before You Start

Make sure you have added device that supports temperature screening and have enabled temperature screening on the device. For details, see the user manual of the device.

Steps

1. On the left navigation bar of the Temperature Screening page, select **Statistics Analysis**.
2. Select a statistics type for the analysis report from **Temperature Screening Point** and **Department**.
3. Select temperature screening point(s) or department(s) for analysis.
   - For selecting temperature screening points:
     a. Click to open the resource list pane.
     b. Select an area in the area list to show the corresponding temperature screening points.
     c. Check the temperature screening point(s) of which the screening results are to be analyzed.
   - For selecting departments:

     Check the department(s) of which the persons' skin-surface temperature screening results are to be analyzed.

     Note

     You can check **Select Sub-Groups** to simultaneously select/deselect the sub department(s) of the department that you have selected/deselected.
4. Select a report type from **Daily Report**, **Weekly Report**, **Monthly Report**, and **Annual Report**, or a report with custom time interval.
5. In the Time field, select a predefined time period or customize a time period accordingly.
6. Click **Generate Report**.

   The statistics of the selected item(s) will be displayed.
7. **Optional:** Perform the following operations if required.

Show/Hide Certain Data	Click the legend to show or hide the screening results of the corresponding statistical object, such as certain temperature screening point or certain department.
View Abnormal Temperature or No Mask Statistics	In the top left corner of the chart, select Abnormal Temperature or No Mask from the first drop-down list to display the statistics of people with abnormal temperature or those not wearing any face masks respectively.
Switch Between Line Chart and Histogram	Click / to switch between line chart and histogram.

8. **Optional:** Export the report to the local PC.
   1) On the top right of the page, click **Export**.
   2) Select the dimension (time-related) of the report to be exported.

      Example

      For example, if you are exporting a daily report, you can select from **By Day** and **By Hour**, and you will be able to export 1 or 24 records respectively for each statistical object (i.e., temperature screening point or department).

      Note

      For reports of department(s), you may also choose the export content from **By Department** and **By Person**.

   3) Select the format of the exported file from **Excel**, **CSV**, and **PDF**.
   4) Click **Export**.

Chapter 11 Map Management

Two types of map are available: GIS map and E-map. On the GIS map, you can set and view the site and element's geographic location. On the e-map, which is a static map, you can set and view the geographic locations of the alarm inputs, and alarm outputs, etc.

With the 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 placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access devices at multiple locations around the world in a geographically correct way.

E-map is a static image (it does 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 placed on the map are called hot spots). You can see the physical locations of the alarm inputs, and alarm outputs, etc. With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

11.1 Configure Map

You need to configure GIS maps and e-maps before using them. You can add hot spots, hot regions, labels, resource groups, etc. to the maps.

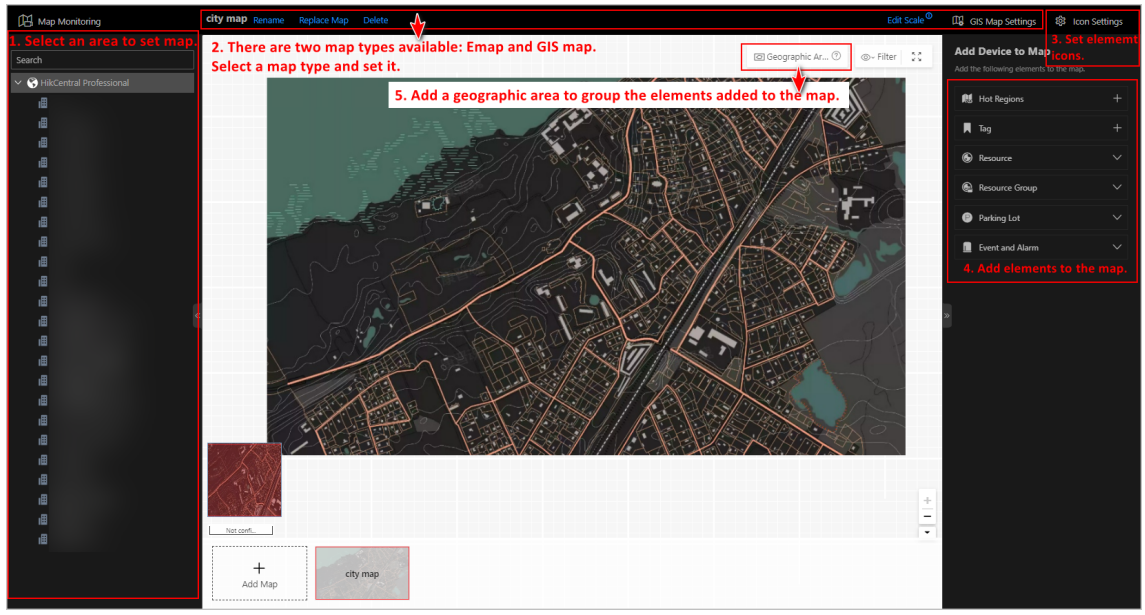


Figure 11-1 Main Interface of Configuring Map

11.1.1 Select and Set GIS or E-map for an Area

You can either set a GIS map for an area or upload an E-map for an area.

Steps

1. On the top, select **Map**.
2. Click **Map Settings** on the top right to enter the map settings page.

Add E-Map for Area

You can add and link e-maps to the area so that the elements assigned to the area can be added to e-map.

Steps

1. Select an area on the left.
2. Open the Add Map pane.
3. Select an adding mode.
4. Select a map.
   - If you select **Add E-Map** as the adding mode, select a map picture saved on the PC.
   - If you select **Link to Other Map**, select an area from the following list.
5. Click **Add**.
6. **Optional:** Set a map scale.

   Note

   The scale of a map is the ratio of a distance on the map to the corresponding distance on the ground. The client can calculate two locations' distance on the map according to the distance on the ground.

   1) Click **Edit Scale** on the top right of the map.
   2) Click two locations on the map to form a line.
   3) Enter the real distance between the two points in the Actual Length field.
   4) Click **OK** to finish setting the map scale.
7. **Optional:** Hover the mouse over the added e-map area to perform the following operations.

Edit Picture	Click and change a picture.
Edit Map Name	Click and set a custom name for the map.
Unlink Map	Click to remove the map or cancel the linkage between the map and area.

For the hot regions, hot spots, combined alarms, you can set different icons for them to recognize them quickly on the map.

Steps

1. Click **Icon Settings** to set the customized icons.
   1) Select a device type to enter the icon settings page.
   2) Set the icon size, including width (px) and height (px).

3) Click **Add** to select a picture file from the local PC.

Note

The icon picture format can only be PNG, JPG, or JPEG.

4) **Optional:** Click to constrain the aspect ratio.
5) Click **Save**.

Note

You can customize door icons for the five status, namely general, door open, door closed, remain open, remain closed, and unknown.

Result

You can view the GIS map on Map Monitoring page and perform the following operations in the map area.

Operations After Adding Maps

Result

Filter	Click and select the object type you want to show on the map.
Full Screen	Click to show the map in full-screen mode.
Zoom In/Out	Scroll the mouse wheel or click + / − to zoom in or zoom out the map.
Adjust Map Area	Click-and-drag the map to adjust the map area for view.
View Resource Latitude and Longitude (For GIS Map)	Hover over a resource, and you can view its latitude and longitude on the GIS map.

11.1.2 Add Hot Spot to Map

You can add elements (e.g., doors, alarm inputs, etc.) as the hot spot and place the hot spot on the e-map. Then you can view the elements on the map and perform further operations via Mobile Client.

Before You Start

A map should ***have been added*** .

Steps

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.

4. Click **Resource Group** on the right.
5. Select a device type and an area from the drop-down lists.
6. Select a device and drag it to the map.

   The hot spot is displayed on the map.
7. **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 locations.
Edit Hot Spot	Click the added hot spot icon on the map and click **Edit** to edit the detailed information (such as selecting icon style).
Delete Hot Spot	Click the hot spot icon on the map and click **Delete** to remove the hot spot from the map.

11.1.3 Add Hot Region to 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.

Steps

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Hot Region** icon on the right.
5. Click a position on the map to select it as the location of the hot region.
6. Select an area from the area list.
7. Click **Save** on dialog to add the hot region.

   The added hot region icon will be displayed on the parent map.
8. **Optional:** Perform the following operation(s) after adding the hot region.

Adjust Hot Region Location	Drag the added hot region on the parent map to the desired locations.
Edit Hot Region	Click the added hot region icon on the map to view and edit the detailed information, including hot region name, icon style, name color, and remarks on the appearing dialog.
Edit Hot Region Area	Drag the white point on the hot region's line to edit the hot region's size or shape as the following picture.
Delete Hot Region	Click the hot region icon on the map and click **Delete** on the appearing dialog to delete the hot region.

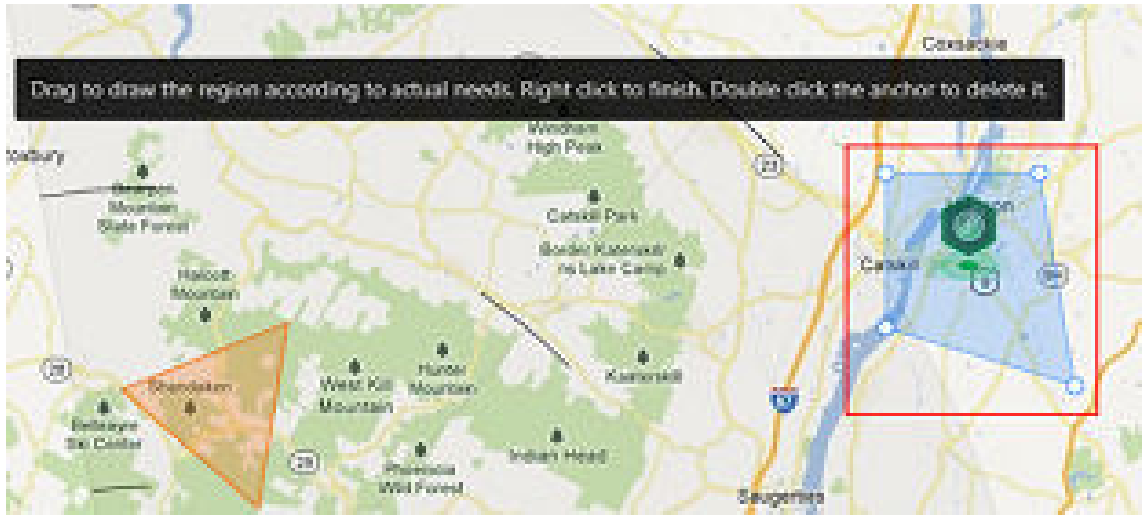


Figure 11-2 Edit Hot Region Area

11.1.4 Add Tag to Map

You can add tags with description on the map.

Steps

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Tag** icon on the right.
5. Click on the map where you want to place the tag.
6. Customize a name for the tag, and you can input content for the tag as desired.
7. Click **Save**.

   The added tag icon will be displayed on the map.
8. **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 content on the appearing dialog.
Delete Tag	Click the tag icon on the map and click **Delete** on the appearing dialog to delete the tag.

11.1.5 Add Resource Group on Map

You can also add the resource groups on the map by locating the resources in the group on the map and setting the edge of the region for detection.

Note

Before adding resource groups to a map, make sure that at least one map ***has been added*** .

Currently, the following resource groups can be added on the map for further operations:

Anti-Passback Group

After adding the anti-passback group on the map, when an anti-passback alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Mobile Client.

For details about how to add an anti-passback group on the map, refer to .

Multi-Door Interlocking Group

After adding the multi-door interlocking group on the map, when multi-door interlocking alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Mobile Client.

For details about how to add a multi-door interlocking group on the map, refer to ***Configure Multi-Door Interlocking***

Final Authentication Counting Group

After adding the entry &exit counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Mobile Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

For details about how to add an entry &exit counting group on the map, refer to ***Add a Final Authentication Counting Group*** .

Batch Locking and Unlocking Group

This function is mainly applicable for emergent situation. For example, the school's security personnel can lock down the doors in this group by quick operation on the Mobile Client, so that the school closes and no one can get into the school except for maintenance and high level admins. This function would block out teachers, custodians, students, etc.

For details about adding doors that need to be batch locked or unlocked, refer to ***Add a Batch Locking and Unlocking Group*** .

11.1.6 Add Event and Alarm to Map

You can add the combined alarms and generic alarms on map to locate the alarm for a visualized monitoring.

Steps

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Event and Alarm** on the right.
5. Drag a combined alarm or generic event to the map.
6. **Optional:** Perform the following operations after adding the combined alarm.

Adjust Event and Alarm Location	Drag the added element on the map to the desired locations.
Edit Event and Alarm	Click the added element icon on the map and click **Edit** to edit the detailed information and selecting icon style).
Delete Event and Alarm	Click the element icon on the map and click **Delete** to remove the element from the map.

11.1.7 Add Geographic Area to Map

Geographic areas refer to a customized map area with elements added to the map. Geographic areas are used to manage multiple elements added to the map. After adding a geographic area to the map, you can batch operate the elements within the area.

Click **Map Settings** in the top right corner of the map module to enter the map settings page.

Select an area on the left, and select an E-map or GIS map.

Click **Geographic Area**, left-click to draw a point, and right-click to finish.

Note

- When an alarm occurs from a camera in the area, the geographic area will blink in the color configured in the event and alarm module.
- A resource within the area will be highlighted to indicate that it has been successfully associated with the area. Resources can be dragged in and out so that you can add or remove resources to the region.

11.2 Monitor on Map

After configuring the maps via Web Client, you can view hot spots, hot regions, and resource groups etc., on the map. You can also zoom in/out to view the map and search locations on the map.

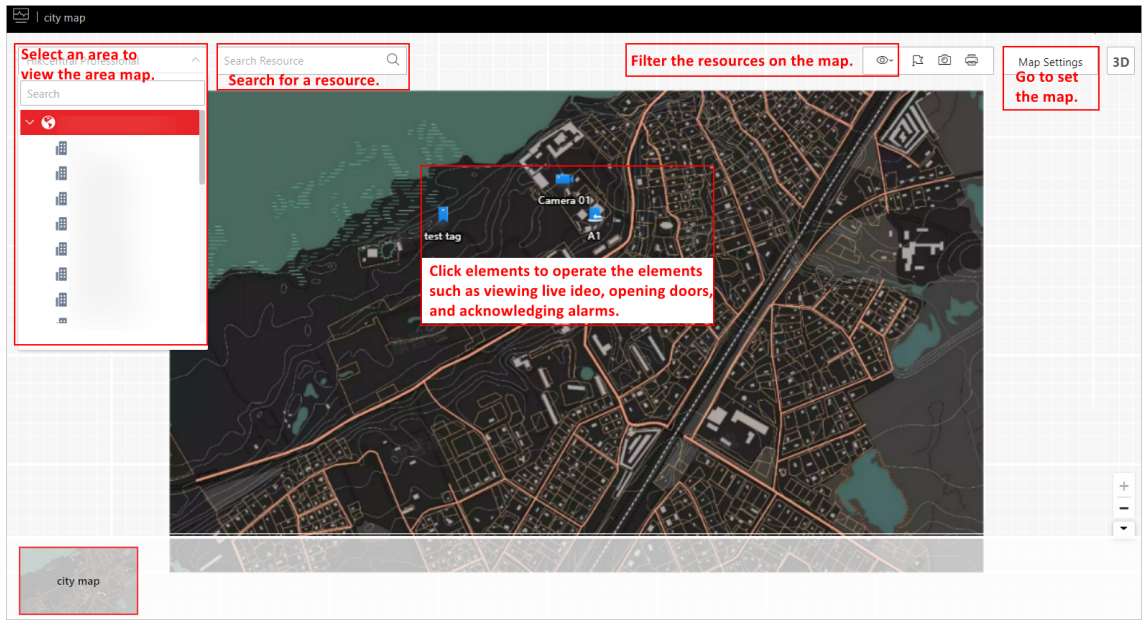


Figure 11-3 Map Monitoring

11.2.1 View and Operate Hot Spot

You can view locations of hot spots including alarm inputs, alarm outputs, access points, etc. on the map. Also, you can set the arming control and view history alarms of monitoring scenarios through the hot spots.

Before You Start

Configure the map settings via the Web Client. For details, see ***Map Management*** 。

Steps

1. On the top, select **Map**.
2. Select a map to enter the map.
3. **Optional:** Perform the following operations on the map.

Filter Resource on Map	Click and check resource type(s) as desired.
More Tools	: Add a label on map. **2D/3D**: Switch the displaying dimension of the map.

Search : Search hot spot or location on the map.

4. Click the hot spot to open the dialog which displays its related functions.
   - If there is an alarm triggered on the hot spot, the hot spot icon will turn into red alarm mode . Click the red icon, and you can view the detailed alarm information.
5. Operate in the dialog.

Arm or Disarm Hot Spot	You can arm or disarm the hot spots via the arming control function. After arming the device, the current Mobile Client can receive the triggered alarm information from the hot spot. Click a hot spot to open the dialog which displays its related functions. In the dialog, click **Arm**/**Disarm** to arm/disarm the hot spot.
View History Alarm	When an alarm is triggered, it will be recorded in the system. You can check the history log related to an alarm, including the alarm source details, alarm category, alarm triggered time, etc. Click a hot spot to open the dialog which displays its related functions. In the dialog, click to enter the event and alarm search page. Then you can search history alarms of the hot spot.



Figure 11-4 Arm Hot Spot / View History Alarm

11.2.2 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
Configure the map settings via the Web Client. For details, see ***Map Management*** .

Steps
1. Click **Map Monitoring** in the top left corner of the map module to enter the map monitoring page.
2. Click **Select Map** on the top left to display the map(s) of an area.
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.

Note

If you enter an area map from a particular map, the full path of the hot region map will be displayed in the upper-left corner. Each time you click **Back**, it only returns to the previous level of the map.

11.2.3 Operate Resources from Geographic Area

After you add a geographic area to a map, you can batch operate the resources within the area.

Click **Map Monitoring** in the top left corner of the map module to enter the map monitoring page..

Click **Select Map** on the top left to display the map(s) of an area.

Note

- When multiple geographic regions overlap, you can select the geographic region from the list first and then click the menu.
- Batch operation is not supported when there are more than 100 resources in a geographic area.

Click the geographic area to perform the following operations.

Block All Alarms	Click **Ignore All** to block all alarms in the area.
Broadcast	Click **Broadcast**, and all IP speakers in the area will start to broadcast and the device icon status will change.
Audio Alarm Control	Click **Audio Alarm Control** to start audible alarms.
Strobe Light Alarm Control	Click **Strobe Light Alarm Control** to start sound and light alarm of all devices in the area with the feature.

Chapter 12 Management of Platform Accounts and Security

You can manage roles and users, assign roles with varying permissions to different users, configure security parameters and questions, and configure permission schedules to enhance system security.

On the top, select **System → Account and Security** .

12.1 Add a Role

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

Steps

Note

The platform has predefined two default roles: Administrator and Operator, which cannot be edited or deleted.

Administrator

Role that has all permissions of the platform.

Operator

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

1. On the left navigation bar of System module, select **Account and Security → Roles** .
2. Click **Add** to enter Add Role page.
3. Set the basic information of the role, including role name, effective period, role status, permission schedule template, description, etc.

   Copy From

   Copy all settings from an existing role.

   Permission Schedule Template

   Set the authorized time period when the role's permission is valid. Select **All-day Template**/**Workday Template**/**Weekend Template** as the permission schedule of the role, or click **Add** to customize a new permission schedule template.

   - When a role expires or the role's permission is invalid after editing the permission schedule, users assigned with the role will be forced to log out and not able to log in.
   - The permission schedule's time zone is consistent with that of the platform.
   - By default, the role will be linked with All-day Template after updating the platform.
4. Configure permission settings for the role.

Area Display Rule

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

Resource Access

Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

Note

If you do not check the resources, the resource permission cannot be applied to the role.

User Permission

The role's permission for different operations on the platform. On the Custom tab, check permission items for the role and click **Save as a Template** so that the template can be applied to other roles. On the Use Template tab, select a permission template from the drop-down list for the role, and the permission details will show below.

5. Click **Add** to add the role and return to the role management page, or click **Add and Continue** to save the settings and continue to add another role.
6. **Optional:** After adding a role, you can perform the following operations on the Roles page.

Disable a Role	Check a role and click **Inactivate**. Inactivated roles cannot be assigned to any user.
Enable a Role	Check a role and click **Activate**.
Refresh Roles	If any changes has been made for roles on the Server, you can click **Refresh All** to synchronize the changes to the current client.
Filter Roles	On the upper right of the Roles page, click different buttons to filter roles. **Assigned** The role assigned to the current user. **Created by Me** Role(s) created by the current user. **Others** Roles except the role assigned to the current user and roles created by the current user.

12.2 User Management

12.2.1 Add a Normal User

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

Steps

1. Select **Users** on the left.
2. Click **Add** on the top.
3. Set basic information for the user.

   Password

   Create an initial password for the user. The user will be asked to change the password when logging in for first time.

   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.

   Email

   The email address of the admin user can be edited by the user assigned with the role of administrator.

   User Status

   Active is selected by default. If you select **Inactive**, the user account will be inactivated until you activate it.
4. Configure parameters related to login protection.

   Allow Remembering Password When Login

   Via Mobile Client / Control Client

   When you log in to the Mobile Client / Control Client, the password will be remembered by default. If the password does not need to be remembered, you can uncheck it.
5. Configure permission settings for the user.

   Set as Default Recipient

   It is not selected by default. If it is selected, the user will have the permissions to access the selected resources.

Assign Role

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

Note

If you want to add new roles, click **Add**. See ***Add a Role*** for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.

6. Click **Add** to add the user and return to the user management page, or click **Add and Continue** to save the settings and continue to add another user.

12.2.2 Import Domain Users

You can batch import the users (including the user name, real name, and email) in the AD domain to the platform and assign roles to the domain users.

Before You Start

Make sure you have configured active directory settings. See ***Set Active Directory*** for details.

Steps

1. In the left navigation bar of the System module, click **Account and Security → Users** .
2. Click **Import User → Via Domain Group** .

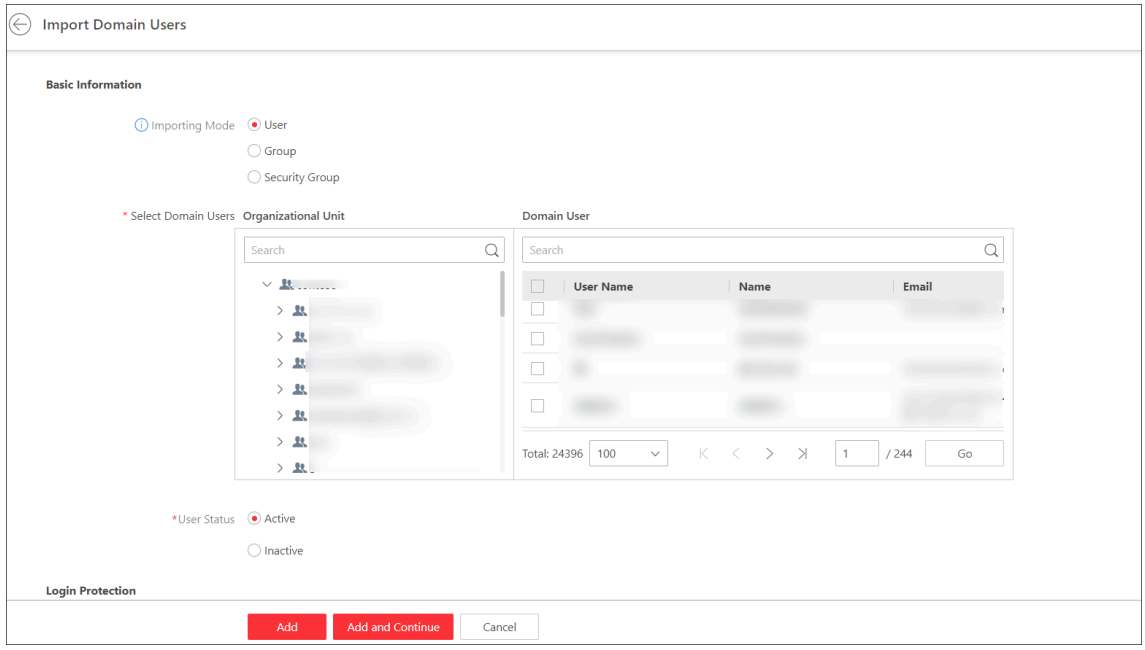


Figure 12-1 Import Domain Users

3. Select an importing mode.

User

Import individual users. Select an organization unit and select one or more domain users in this organization unit.

Group

Select an organization unit to import all the domain users in this organization unit.

Note

The platform does not support this function if the Azure domain is configured.

Security Group

Import all the domain users in the security group(s). Select an organization unit and select one or more security groups in this organization unit.

4. Select domain users from active directory.
5. Select the user status as **Active** or **Inactive**.
6. **Optional:** To limit the maximum IP addresses logged in to the platform using the user account, switch on **Restrict Concurrent Logins** and enter the maximum number of concurrent logins.
7. **Optional:** Configure parameters related to login protection.

Allow Remembering Password When Login

Via Mobile Client / Control Client

When you log in to the Mobile Client / Control Client, the password will be remembered by default. If the password does not need to be remembered, you can uncheck it.

8. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit. If the user with higher permission locks the PTZ, the user with lower permission level will not be able to control the PTZ unit.

Example

When two users control the PTZ unit at the same time, the user who has the higher PTZ control permission level takes control of the PTZ.

9. Select the roles that you want to assign to the domain users.
   - If no role has been added, two default roles are selectable: administrator and operator.

     Administrator

     The role that has all permissions of the HikCentral Access Control.

     Operator

     The role that has all permissions of the HikCentral Access Control Control Client.
   - If you want to add new roles, you can click **Add New Role**. See ***Add a Role*** for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.
10. Complete importing the domain users.
    - Click **Add** to import the domain users and return to the user management page.
    - Click **Add and Continue** to save the settings and continue to import other domain users.

Result

After successfully adding the domain users, the users can log in to the HikCentral Access Control via the Web Client and Mobile Client with their domain accounts and passwords.

12.2.3 Import Normal Users via an Excel File

You can import normal users via a template (an Excel file) to batch add normal users.

Select **Users** on the left.

Click **Import User → Via Excel** on the top.

Click **Download Template** to download the template file.

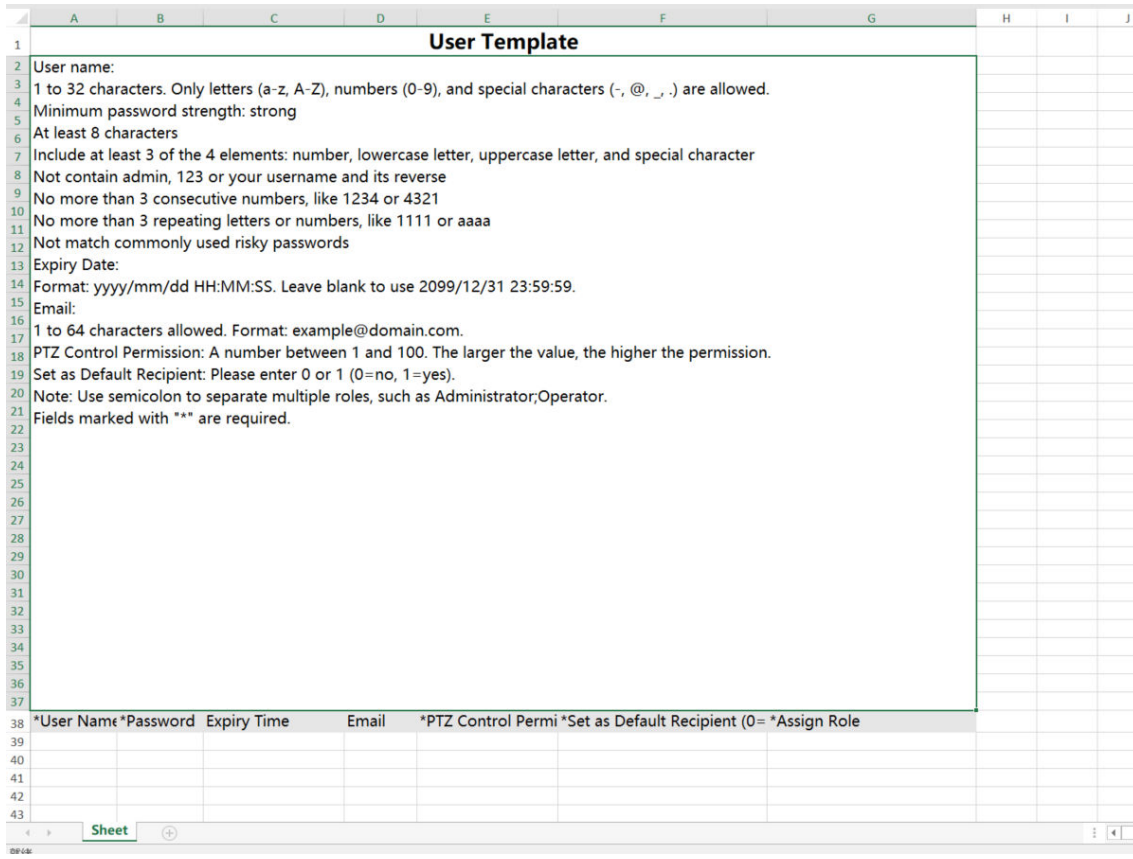


Figure 12-2 Template File

Enter user information in the downloaded template file and click to select the edited template file. You can also select an exported file with edited information of multiple users to modify user information. For details about exporting user information, see ***Export Normal Users*** .

You can check **Replace Repeated User Name** to replace the user name in the list which is duplicate with the imported user name.

12.2.4 Operations After Adding Users

On the Users page, you can perform the following operations if needed.

Table 12-1 Operations After Adding Users

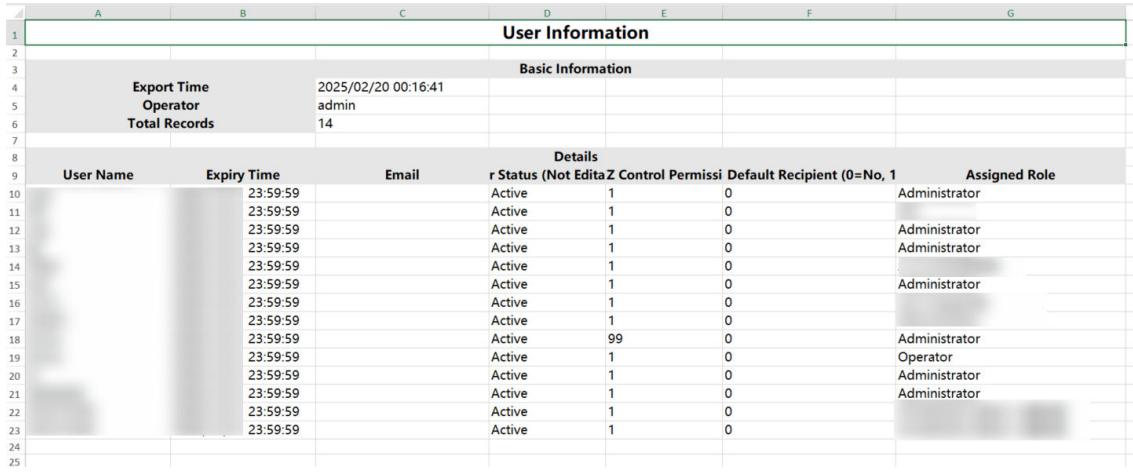
Operation	Description
Synchronize Domain Users	After importing the domain user information to the platform, if the user information in domain is changed, click **Synchronize Domain Users** to get the latest information of the users imported to the platform. If the users are imported by group, it will synchronize the latest user information from the domain group (including added users, deleted users, edited users, etc., in the group).
Force Logout a User	In the user list, select an online user and click **Force Logout** to log out the user.
Disable a User	Check a user and click **Inactivate**. Inactivated users cannot log into the platform.
Enable a User	Check a disabled user and click **Activate**.
Unlock a User	For users whose account is locked due to too many login failures, Administrators can unlock their accounts for login.
Refresh All	If any changes has been made for users on the Server, you can click **Refresh All** to synchronize the changes to the current client.

12.2.5 Export Normal Users

You can export the information of specific/all normal users to an Excel file to your PC.

Select **Users** on the left.

Select users in the list and click **Export User** on the top. Confirm your password and click **Export**.



User Information

Basic Information

Export Time	2025/02/20 00:16:41
Operator	admin
Total Records	14

Details

User Name	Expiry Time	Email	r Status (Not Edita	Z Control Permissi	Default Recipient (0=No, 1	Assigned Role
	23:59:59		Active	1	0	Administrator
	23:59:59		Active	1	0	
	23:59:59		Active	1	0	Administrator
	23:59:59		Active	1	0	Administrator
	23:59:59		Active	1	0	
	23:59:59		Active	1	0	Administrator
	23:59:59		Active	1	0	
	23:59:59		Active	1	0	
	23:59:59		Active	99	0	Administrator
	23:59:59		Active	1	0	Operator
	23:59:59		Active	1	0	Administrator
	23:59:59		Active	1	0	Administrator
	23:59:59		Active	1	0	
	23:59:59		Active	1	0	

Figure 12-3 Exported File

If you need to import the exported file after editing it to update the user information, see ***Import Normal Users via an Excel File*** for details.

12.3 System Security Settings

12.3.1 Set Basic Security Parameters

System security is crucial for your system and property. You can lock IP address to prevent malicious attacks and set other security settings to increase the system security.

Select **Account and Security → Basic Parameters** on the left.

Max. Failed Login Attempts

Select the maximum allowable login attempts for accessing HikCentral Access Control. Failed login attempts include failed password attempt and failed verification code attempt.

Lock Duration

Set the lock duration for this IP address. During the lock duration, the login attempt via this IP address is not allowed.

Minimum Password Strength

Define the minimum complexity requirements that the password should meet.

Enable Maximum Password Validity Period

Force user to change the password when the password expires.

Password Will Expire In

Set the maximum number of days that the password is valid. After the maximum number of days, you should change the password. You can select the predefined time length or customize the time length.

Days to Remind Before Password Expiration

Set days to remind you at each time you login or in the small hours of each day by sending an email notification before password expiration.

Web Login Expires If No Action Within

Set minutes after which the Web login will expire if there is no actions during the set minutes.

Auto Log Out Mobile App

The Mobile Client will be automatically logged out if there is no operation in a set time period. You can select the predefined time period or customize a time period.

Request Terms Agreement for Mobile Client Login

If it is checked, users should agree to the terms each time they log in to the Mobile Client.

12.3.2 Configure Security Questions

Security questions can be used to verify user identity when users want to reset the password. After setting the security questions, users needs to first answer the security questions correctly before they can reset the password, so as to ensure account security.

Select **Security Question** on the left.

Select a question from the drop-down list and set an answer to it.

Note

The answer is not case sensitive.

Click **Save** to save the settings.

12.3.3 Change Password of Current User

You can change the password of your currently logged-in user account via Web Client.

Steps

1. Move the cursor to the user name at the top-right corner of the Web Client.
2. In the drop-down list, click **Change Password** to open the Change Password panel.

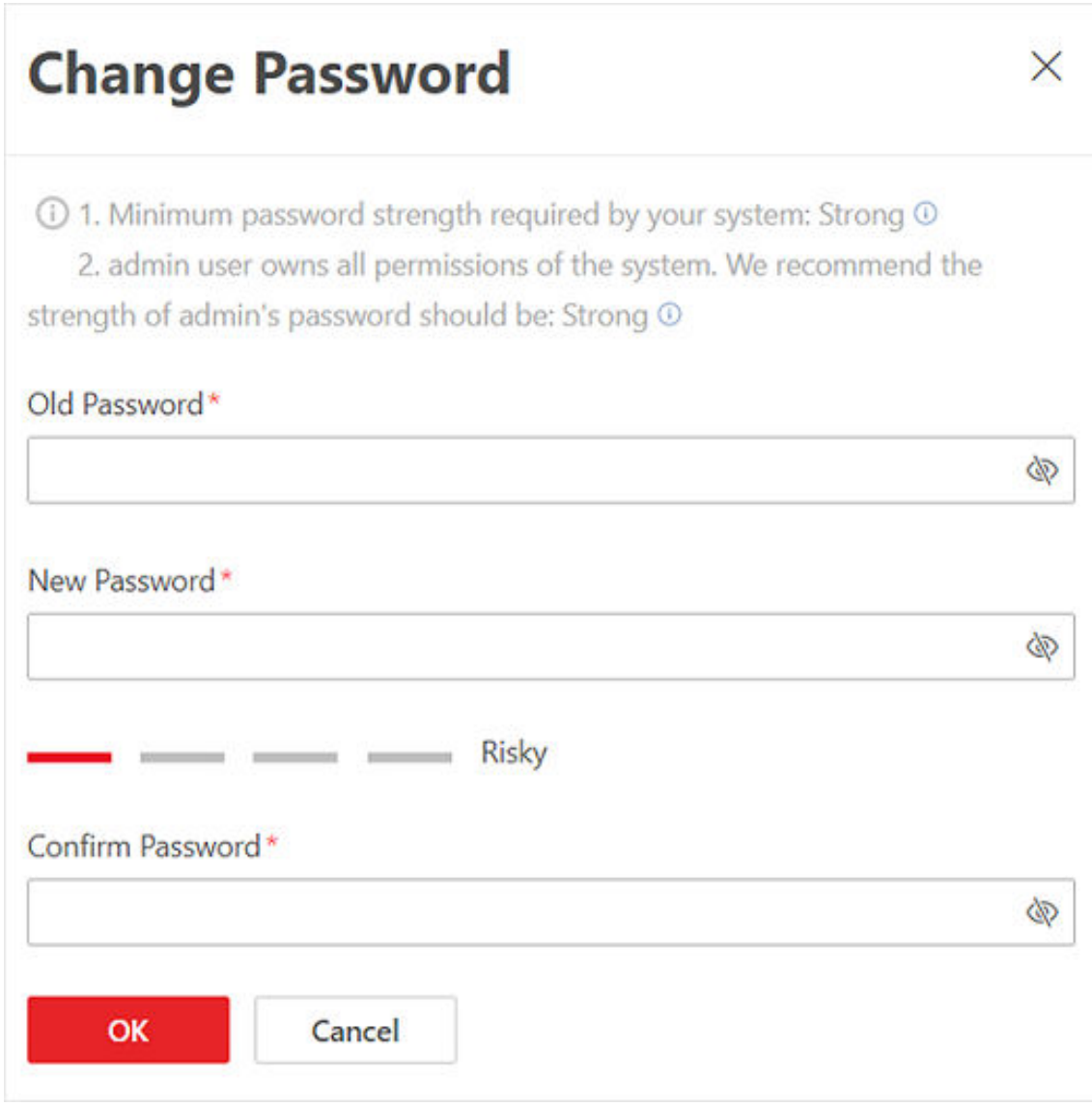


Figure 12-4 Change Password Panel

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 the change.

12.3.4 Forgot Password

If you forget the password of your account, you can reset the password.

Before You Start

- Make sure the normal user has been configured with an available email address.
- Make sure the email server is tested successfully.

Steps

1. On the login page, click **Forgot Password**.
2. Enter your user name and click **Next**.
3. Enter the required information on the Reset Password window.
   - If you are the admin user whose account is configured with security questions, you can answer the pre-configured questions, click **Next**, and set and confirm your new password.

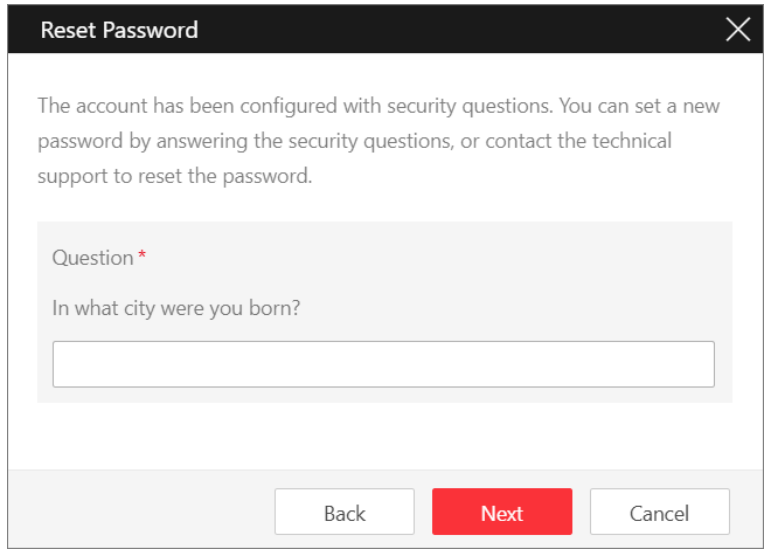


Figure 12-5 Reset Password for admin User via Security Questions

   - If you are the admin user or a normal user whose account is configured with an email address, you can click **Get Verification Code** and a verification code will be sent to your email address. Enter the verification code you received, set a new password, and confirm the password within 10 minutes.

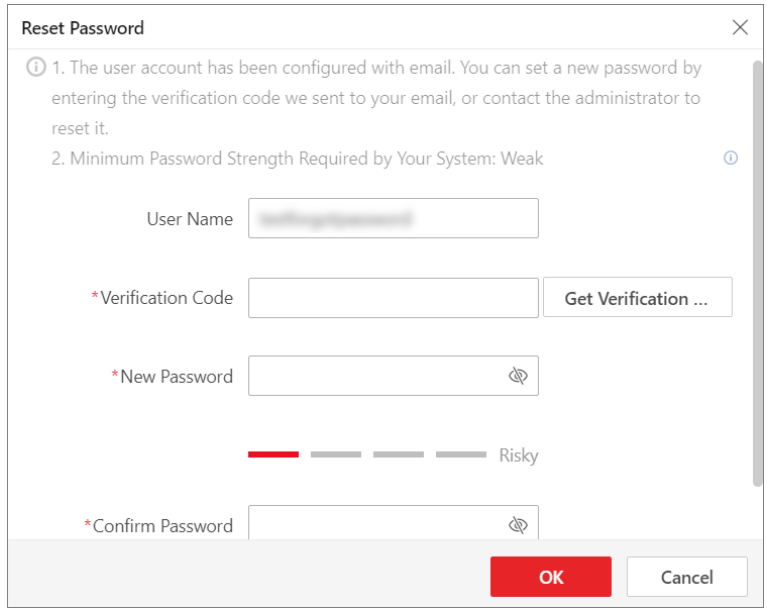


Figure 12-6 Reset Password via Verification Code

Note

If no email address is set for your normal user account, you need to contact the admin user to reset your password.

- If you are a domain user, you need to contact the admin user to reset your password.

Note

The password strength can be checked by the system and should meet the system requirements. If the password strength is lower than the required minimum strength, you will be asked to change your password. For setting the minimum password strength, refer to ***Set Basic Security Parameters*** .

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.
  The password should:
  - Not contain admin, 123 or your username
  - Have no more than 3 consecutive numbers, like 1234 or 4321

- Have no more than 3 repeating letters or numbers, like 1111 or aaaa
- Not match commonly used risky passwords

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

4. Click **OK**.

12.4 Configure Permission Schedule

Permission schedule defines the time when a role's permissions are valid. During unauthorized time periods, the user assigned with the role will be forced to log out and cannot log in. The platform provides 3 default permission schedule templates: All-day Template, Workday Template, and Weekend Template. You can add new templates according to actual needs.

Steps

1. On the top, select **System → Account and Security → Permission Schedule Template** .
2. Click + on the top left.
3. Set basic information.

   Copy From

   Copy the settings from another existing template.
4. In the **Weekly Schedule** area, click **Authorize** to select or draw in the box to define the authorized time periods.

   Note

   You can set up to 6 separate time periods for each day.
5. Click **Add** to add the permission schedule template.

Chapter 13 System Configuration

This module allows you to set different types (e.g., normal settings, network settings, storage settings, and so on) of parameters for the platform, such as defining a customized name for the site, setting NTP (Network Time Protocol) for synchronizing the time between the platform and the NTP server, and setting an IP address to allow the platform to access the WAN (Wide Area Network).

On the top, select **System** to enter this module.

13.1 Normal Settings

The normal settings menu provides entries of setting the user preference, holidays, printers, and card templates.

On the left navigation bar of the System page, select **Normal** to display the normal settings menu.

13.1.1 Set User Preference

For different countries, regions, cultures, and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, such as the site name, the first day of a week, and the calendar type.

Select **User Preference** on the left navigation bar to enter the following page.

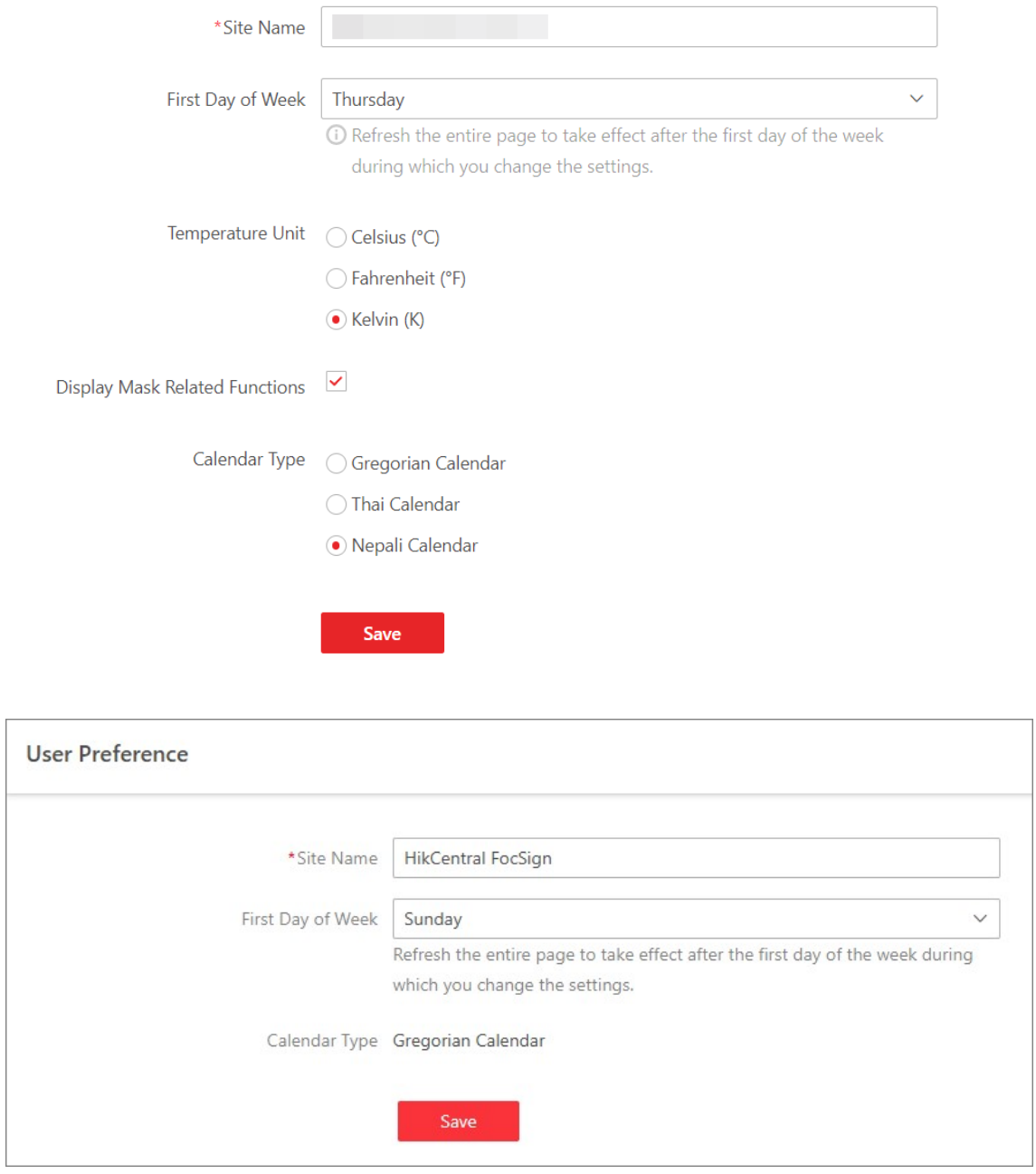


Figure 13-1 User Preference

Set the following parameters:

Site Name

Set the name of current site.

First Day of Week

Set the first day of a week as Sunday, Monday, Tuesday, etc., according to the custom of the actual scene.

Note

This parameter is used in the report generation, etc.

Temperature Unit

Set the temperature unit according to the custom of the actual scene.

Note

This parameter is used in the temperature analysis report generation, etc.

Display Mask Related Functions

Set whether to display mask related functions. Check the box to display the functions about masks on Web Client and Mobile Client. Otherwise these functions will be hidden.

Note

This parameter is mainly used in temperature screening module.

Calendar Type

Set the calendar type as Gregorian Calendar, Thai Calendar and Nepali Calendar according to the custom of the actual scene.

13.1.2 Set Holiday

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.

Select **Holiday Settings** on the left navigation bar to enter the Holiday Settings page.

Add 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.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Regular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

Start Time

The start date of the holiday.

Number of Days

The lasting days of the holiday.

Repeat Annually

If checked, the platform will generate the date of the holiday according to the date of SYS (System Server).

4. Click **Add**.

Add 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.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Irregular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

Start Time

The start date of the holiday.

For example, select **May**, **Second**, and **Sunday** for Mother's Day.

Number of Days

The lasting days of the holiday.

Repeat Annually

If checked, the system will generate the date of the holiday according to the date of SYS.

Note

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

4. Click **Add**.

13.1.3 Set Printer

You can set printers for the platform, which can be used to print the stranded person list in some urgent evacuation scenario, such as fire hazard.

Note

Make sure that the printers are installed on the same network with SYS.

Select **Printer Settings** on the left navigation bar to enter the Printer Settings page.

Click **Add** to select the printer(s) detected by the platform.

Note

After setting a printer for the platform, you can link the printer when configuring alarm/event whose source type is alarm input.

You can click in the Operation column to delete a printer or click **Delete All** to delete all added printers.

13.1.4 Set Card Template

The platform has provided two predefined card template for you. If they do not meet your requirements, you can set styles for card templates by yourself. After settings, the card will be applied in the format of the template.

Steps

1. Select **Card Template** to enter the Card Template page.
2. Click **Add**.
3. Create a name for the template.
4. **Optional:** Select the shape of the template.
5. Set the front style of the template.

Insert Picture	Click **Insert Picture** to select a picture for the template.
Insert Background Picture	Click **Insert Background Picture** to select a background picture for the template.
Insert Text	Click **Insert Text** to set the text for the template.
Customize Contents	Check the attribute(s) for the content of the template. You can also click **Additional Information** to customize the attributes for the template.
Configure Text Settings	• Select a text box and set the font type, font size, font color, and bold front for the text in the box. • Select one or multiple text boxes and click , , or in the Text Alignment field to adjust the alignment of the text in the box. • Select multiple pictures or text boxes and click , , or in the Content Alignment to adjust these elements. • Right-click a picture (except the background picture) or text box to show a drop-down menu and click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down** to adjust the layer of the picture or text box displayed on the template. • Right-click a picture (except the background picture) or text box to show a drop-down menu and click **Delete** to remove the picture or text box.

6. **Optional:** Refer to the previous step to set the back style of the template.
7. Click **Add** to add the template and go back to the card template list page.

The added card template will be listed on the Card Template page.

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

View Template	Click in the Operation column to view the template details.
Edit Template	Click in the Operation column to edit template details.
	Note The predefined card templates cannot be edited.
Delete Templates	Click in the Operation column of a template or click **Delete All** at the top to delete the template or delete all added templates.
	Note The predefined card templates cannot be deleted.

13.2 Calling Settings

You can add call recipients for receiving and answer calls, add receiving schedule templates defining when users can receive calls, and configure call parameters such as record storage.

13.2.1 Add Call Recipients

You can add users in the platform as call recipients. After adding call recipients, when someone calls the system, the added recipients can receive and answer the call.

Go to **Call Settings → Call Recipient** on the left.

Click **Add**, select users to receive calls, set devices for receiving calls from, select a receiving schedule template, and click **Add**.

13.2.2 Add a Receiving Schedule Template

Receiving schedule template defines when the user can receive calls. For example, if a resident is absent from home during workdays and is at home during weekends and holidays, the resident can customize a schedule template to receive calls from device during weekends and holidays.

Steps

1. Click + to add a schedule template.

   The default templates, namely All-Day Receiving Schedule Template, cannot be edited or deleted.
2. Create a name for the template.
3. **Optional:** Select an existing template from the **Copy from** drop-down list.

4. Draw the receiving time. Click a grid or drag the cursor on the time line to draw a time period during which the user can receive calls.

Note

- Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as .
- Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.

5. **Optional:** Click **Add Holiday** to select a holiday template.
   1) You can select an existed holiday template, or click **Add** below the template list to configure a new template in the pop-up window.
   2) Click **Add**.
   3) Click a grid or drag the cursor on the time line to draw the receiving time as shown in the previous step.

Note

See ***Set Holiday*** for detailed information of configure a holiday template.

6. Click **Add** to save the template.
7. **Optional:** Select a template from the template list, and then click to delete it.

Note

Schedule templates that has been linked cannot be deleted.

13.2.3 Configure Call Parameters

You can configure call parameters, including record storage, calling parameters of radar, access control or video intercom devices, and whether to receive calls from devices to the platform.

Go to **Call Settings → Call Parameter** on the left.

Configure the following parameters as needed, then click **Save** to save settings.

Records Storage

You can store the records generated in the operation of video intercom, such as the records of linking the video or audio files to call logs.

Select **Local Storage** or **pStor** from the drop-down list to store the records on the local PC or on the pStor server. After that, you can view and select the corresponding resource pool.

Note

For **Local Storage**, make sure you have enabled local storage and added the local resource pool. For details, refer to ***Set Storage on System Server*** .

Access Control or Video Intercom Devices Calling Parameters

Supports configuring calling parameters of access control or video intercom devices. You can select local ringtone files, valid only for calls received on the platform.

Receive Calls

Enable this to receive call from devices to the platform.

13.3 Network Settings

The network settings menu provides entries of setting NTP for time synchronization, selecting device access protocol, setting an IP address to allow the platform to access the WAN, and so on.

On the left navigation bar of the System page, select **Network** to display the network settings menu.

13.3.1 Set NTP for Time Synchronization

You can set NTP parameters for synchronizing the time between resources managed on the platform and the NTP server.

Steps

1. Select **NTP** on the left navigation bar.
2. Select the **Time Sync Mode**.

Note

For time synchronization via network and the local server, just set the synchronization interval and click **Save**. For time synchronization via the NTP server, follow steps below.

3. Set the NTP server address and port No.

Note

If the local NTP server has been configured, click **Detect Local NTP** to fill in the NTP server address and port No. automatically.

4. Enter the interval of the automatic time synchronization.
5. **Optional:** Click **Test** to test the communication between resources and the NTP server.
6. **Optional:** Switch on **Configure WAN Mapping** and enter the IP address and port No. for WAN mapping.

Note

If the NTP service is locally deployed, you can configure WAN mapping to synchronize the time for devices on the WAN. Otherwise, enabling mapping is not required.

7. Click **Save**.

13.3.2 Set Active Directory

If you have an AD (Active Directory) domain controller which contains the information (e.g., user data, computer information), you can configure the settings to get the related information. In this way, you can add the users that belong to an organization unit (OU) (e.g., a department of your company) to the platform conveniently.

Steps

1. Select **Active Directory** on the left navigation bar.
2. Configure the corresponding parameters for connecting the platform to the AD domain controller.
3. Set the time to automatically synchronize the users in the AD domain to the platform.
4. **Optional:** Link the person information you are concerned about in the domain to the person information on the platform.

   Note

   Once enabled, the corresponding person information on the platform will match the linked person information in the domain and cannot be edited.

   1) Switch on **Linked Person Information**.

      The basic and custom additional information items (see *Customize Additional Information*) are displayed by default. You can set the relationship for those or add new person information items as needed.

   2) **Optional:** Click **Add** to add a person information item you are concerned about.

      Note

      - You do not need to add the basic person information items (including ID, first name, last name, phone, and remark) manually, which have the default relationship with the information in the domain.
      - The person information item is case-sensitive.

   3) Click + to show the person information items stored in the domain and check checkboxes in the domain to link them to the custom person information item when importing the domain's persons.
   4) Click and drag one item to another to change the relationship between each other.
   5) **Optional:** Hover over the linked person information in the domain and click × to remove the relationship.
5. Click **Save**.

   After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on the **Account and Security → Users** page.

13.3.3 Set Device Access Protocol

Before adding devices supporting ISUP and ONVIF protocol to the platform, you need to set the related configuration to allow these devices to access the platform.

Select **Device Access Protocol** on the left navigation bar.

Switch on **Allow ISUP Registration** to allow devices to access the platform via the ONVIF protocol or ISUP.

Note

After **Allow ISUP Registration** is switched on, you can check **Allow ISUP of Earlier Version** to allow devices to access the platform via ISUP of version 2.6 or 4.0.

13.3.4 Set WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for the platform to access WAN (Wide Area Network).

Select **WAN Access** and enable the button. You can select one or more application scenario(s) and click **Export Ports** to export an Excel file about the port information for WAN configuration.

Port Information for WAN Configuration

Rule

1. Do not edit the contents in the first two columns.
2. If a port is marked in red, it means that its LAN port has changed from the previous exported result. You need to edit the port mapping configuration on the router accordingly.

Port Name	LAN Port	WAN Por	Protocol	Network Communication Direction	Port Function	Remark
Client Communication Port (HTTP)	80	80	TCP	From Client to Platform	Used for accessing the client via HTTP protocol.	After the port is edited, the client that is logged in via WAN will be logged out.
Client Communication Port (HTTPS)	443	443	TCP	From Client to Platform	Used for accessing the client via HTTPS protocol.	After the port is edited, the client that is logged in via WAN will be logged out.
Generic Event Receiving Port (TCP)	15300	15300	TCP	From Third-Party System to Platform	Used for receiving generic events via TCP.	
Generic Event Receiving Port (UDP)	15300	15300	UDP	From Third-Party System to Platform	Used for receiving generic events via UDP.	
Generic Event Receiving Port (HTTP)	15310	15310	TCP	From Third-Party System to Platform	Used for receiving generic events via HTTP.	
Generic Event Receiving Port (HTTPS)	15443	15443	TCP	From Third-Party System to Platform	Used for receiving generic events via HTTPS.	
ISUP Alarm Receiving Port (TCP)	7332	7332	TCP	From ISUP Device to Platform	Used for receiving alarm information from ISUP devices.	
ISUP Alarm Receiving Port (UDP)	7334	7334	UDP	From ISUP Device to Platform	Used for receiving alarm information from ISUP devices.	
ISUP Registration Port	7660	7660	TCP	From ISUP Device to Platform	Used for receiving registration information of ISUP devices.	
Server Local Picture Storage Port (HTTP)	6011	6011	TCP	From Client/Device to Platform	Used for storing pictures on the SYS server based on HTTP protocol.	
Server Local Picture Storage Port (HTTPS)	6111	6111	TCP	From Client/Device to Platform	Used for storing pictures on the SYS server based on HTTPS protocol.	
Server Local File Storage Port (HTTP)	6203	6203	TCP	From Client/Device to Platform	Used for storing files on the SYS server based on HTTP protocol.	
Server Local File Storage Port (HTTPS)	6204	6204	TCP	From Client/Device to Platform	Used for storing files on the SYS server based on HTTPS protocol.	
RTSP Streaming Port (TCP)	554	554	TCP	From Client to Platform	Used for getting real-time live stream from the streaming server.	After the port is edited, the client that is logged in via WAN will be logged out.

Figure 13-2 Exported Template

Send the template to your maintenance staff to enter the WAN port numbers, and get the completed template.

Click **Import Ports** to import the completed template.

Check the imported ports, and click **Save**.

13.3.5 Set IP Address for Receiving Device Information

You can select the NIC of the current SYS (System Server) so that the platform can receive the alarm information of the device connected via ONVIF protocol.

Before You Start

Make sure the server's ports ranging from 8087 to 8097 are available.

Steps

1. Select **Address for Receiving Device Info** on the left navigation bar.
2. Select **Get from NIC** or **Enter Manually**.

   Get from NIC

   Select the currently used NIC name of SYS in the drop-down list. The NIC information including description, MAC address, and IP address will be displayed.

   Enter Manually

   If you have configured hot spare for the SYS, you should manually enter the IP address.
3. Click **Save**.

13.4 Storage Settings

The storage settings menu provides entries of setting storage for pictures and files on SYS and specifying retention periods for different types of records.

On the left navigation bar of the System page, select **Storage** to display the storage settings menu.

13.4.1 Set Storage on System Server

The imported pictures (such as the static e-map pictures and the face pictures in the person list) can be stored on SYS. You can configure the storage locations and the corresponding quotas for them.

Steps

Note

This configuration is available only when the Web Client is running on SYS.

1. Select **Storage on SYS Server** on the left navigation bar.

   The disks of SYS are displayed with current free space and total capacity.
2. Switch on **Enable Local Storage**.
3. Configure the related parameters for storing pictures.
   1) Select the disk to store the imported pictures.

      Note

      The disk should have at least 1.25 GB of free space for picture storage.
   2) **Optional:** Switch on **Set Quota for Pictures** and set the storage quota for the pictures.
4. Click **Add** to add a resource pool for storing files.
   1) Enter the name of the resource pool.
   2) Select a disk to store the files.

Note

The disk should have at least 9 GB of free space for file storage.

3) **Optional:** Switch on **Restrict Quota for Pictures** and set the storage quota for the files.
4) Check **Overwrite When Storage Space is Insufficient**, and the newly imported files will overwrite the existing files when the disk space is insufficient.
5) Click **Add**.
6) **Optional:** Click **Delete** or in the Operation column to delete a resource pool.
7) **Optional:** Click a resource pool name to edit related settings.

5. Click **Save**.

13.4.2 Set Storage for Records

The data retention period specifies how long you can keep the events, logs, and some records on SYS.

Steps

1. Select **Records Storage** on the left navigation bar.
2. Select one language from the drop-down list to set the language of the sorting rule.
3. Set the data retention period from the drop-down list for the required data types.
4. Click **Save**.

13.5 Email Settings

The email settings menu provides entries of setting different email templates for scheduled reports, events and alarms, and pending tasks, and configuring the basic email parameters. The email template specifies the recipient, email subject, and content.

On the left navigation bar of the System page, select **Email** to display the email settings menu.

13.5.1 Configure Email Account

You should configure the parameters of the sender's email account before the system can send the message to the designated email account(s) as the email linkage.

Steps

1. Select **Email → Email Settings** on the left navigation bar.
2. Configure the parameters according to actual needs.

Server Authentication

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

Cryptographic Protocol

Select the cryptographic protocol of the email to protect the email content if required by the SMTP server.

Sender Email Address

Enter the email address of the sender to send the message.

Sender Name

Enter the sender name to send the message.

SMTP Server Address

The SMTP server's IP address or host name (e.g., smtp.263xmail.com).

SMTP Server Port

The default TCP/IP port used for SMTP is 25.

User Name (Optional)

User name for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

Password (Optional)

Password for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

Note

For users of Google email, you should log in to your Google account, enable the 2-step verification function, generate the APP password, and enter here.

3. Click **Email Test** to test whether the email settings work or not.

   The corresponding attention message box will pop up.
4. Click **Save**.

13.5.2 Add Email Template for Sending Report Regularly

You can set email templates (including specifying the recipient, email subject, and content) for sending the report regularly, so that the platform can send the report as an email attachment to the designated recipient regularly according to the predefined email template.

Before You Start

Make sure you have set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. Select **Scheduled Report Email Template** on the left navigation bar.
2. Click **Add** to enter the Add Email Template page.

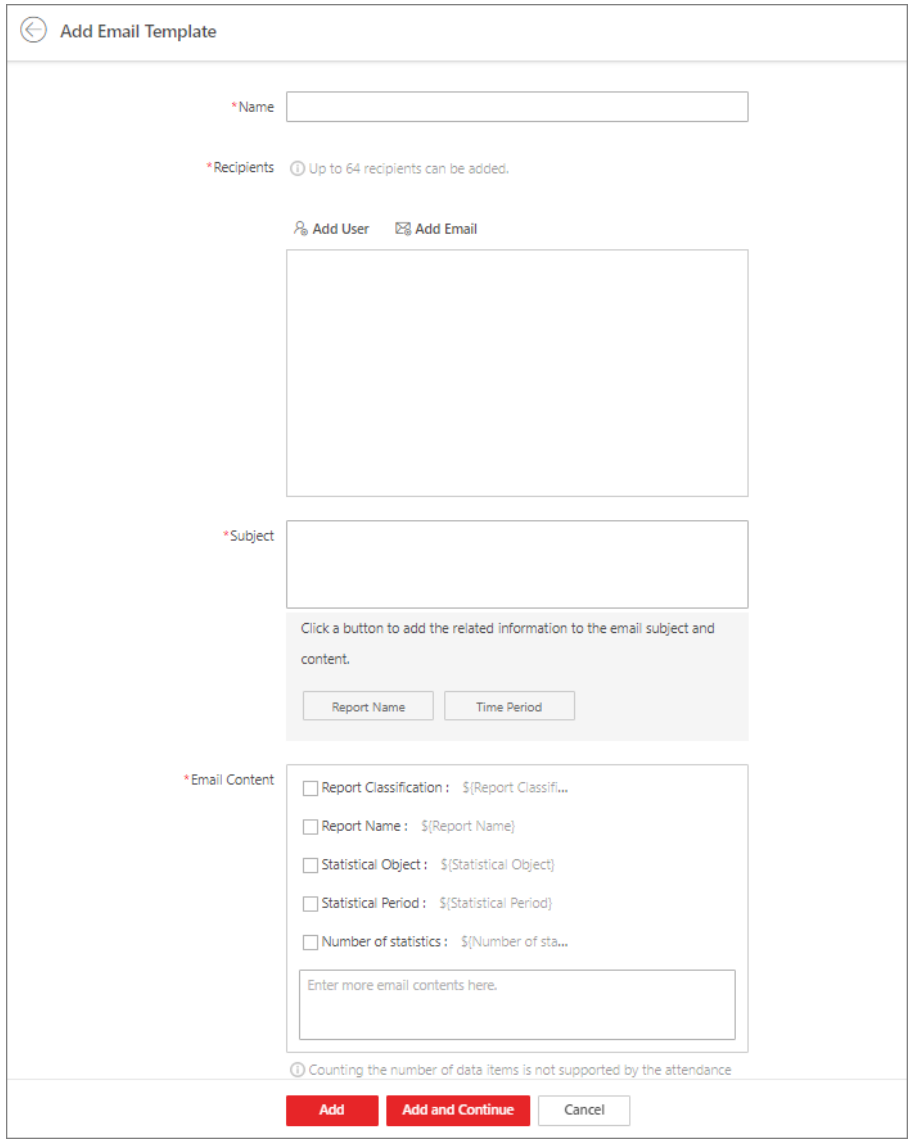


Figure 13-3 Add Email Template for Sending Reports Regularly

3. Enter the required parameters.

Recipients

- Click **Add User** and select the person's email, which is configured when adding the person.
- Click **Add Email** and enter the recipient email address to send the email to.

Note

You can enter multiple recipients and separate them by ";".

Subject

Enter the email subject as desired. You can also click buttons below to add the related information to the subject.

Email Content

Define report contents to be sent. In the Email Content field, check the content type(s) (i.e., Report Classification, Report Name, Statistical Object, Statistical Period, and Number of Statistics) to add the related information to the content and enter more detailed contents in the text box to complete the design of report contents.

Note

If you add the time period to the email subject or add the statistical period to the email content, and the email application (such as Outlook) and the platform are in different time zones, the displayed period may have some deviations.

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:** After adding email templates, perform the operations such as editing, deleting, and searching for templates.

13.5.3 Add Email Template for Event and Alarm Linkage

You can set email templates (including specifying the recipient, email subject, and content) for event and alarm linkage. When the event or alarm is triggered, the platform can send email as the linkage action to the designate recipient regularly according to the predefined email template.

Before You Start

Make sure you have set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. Select **Event and Alarm Email Template** on the left navigation bar.
2. Click **Add** to enter the Add Email Template page.
3. Enter the required parameters.

   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(s) email address to send the email to.

   Note

   You can enter multiple recipients and separate them by ";".

   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.

   Email Content

Define the event or alarm information to be sent. You can also click buttons below the **Email Content** parameter to add the related information to the content.

Note

If you add the event time to the email subject or content, and the email application (such as Outlook) and the platform are in different time zones, the displayed event time may have some deviations.

4. **Optional:** Check **Attach Captured Picture** and/or **Attach Linked Video**.
5. Select a content language to define the language of the sent content.
6. Click **Add** to add the template and go back to the email template list page. or click **Add and Continue** to add the template and continue to add other templates.

   The email template will be displayed on the email template list.

13.6 Security Settings

The security settings menu provides entries of setting the transfer protocol for SYS, exporting service component certificate, enabling export of profile pictures, enabling watermark in video or picture, and setting the database password.

On the left navigation bar of the System page, select **Security** to display the security settings menu.

13.6.1 Set Transport Protocol

You can set SYS's transport protocol to define the access mode for SYS via clients as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Steps

1. Select **Transport Protocol** on the left navigation bar.
2. In the **Transport Protocol Between Platform and Browser** field, select **HTTP** or **HTTPS** as the transport protocol between clients and SYS.

   Note

   For HTTPS, only the TLS 1.2 and later versions are supported. The browser must support and has enabled the TLS 1.2 or later version. You are recommended to use the browser supporting TLS 1.3.

3. **Optional:** If **HTTPS** is selected, perform the following steps to set the certificate.
   1) Select **Platform Provided Certificate**, or select **New Certificate** and click to select a new certificate file from your local PC.
   2) **Optional:** Click **Add** → → **Confirm** to add a upper-level certificate as needed.

Note

You can select the added certificate(s) and click **Delete** to delete them, or click ⤓ in the Operation column of a certificate to download the certificate.

4. Click **Save**.
   - The SYS will restart automatically after the transport protocol is changed.
   - All logged-in users will be forced to log out during the restarting, which takes about one minute and after that, the users can log in again.

13.6.2 Set Database Password

You can set the database password of the platform on the Web Client running on SYS.

Note

Setting database password is only available when you access the Web Client on SYS locally.

Select **Database Password** on the left navigation bar.

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

13.6.3 Enable Export of Profile Pictures

In the Person module, you can export the profile pictures of the added persons as a ZIP file to your PC . For information security, you can choose to convert these profile pictures into unreadable modeling data for saving.

On the left navigation bar, select **Profile Picture** and check **Export Profile Pictures**.

Switch on **Save Model Data of Profile Picture Only** and select a validity period for the profile pictures.

13.6.4 Watermark Settings

On the left navigation bar, click **Watermark Settings**. and then enable **Watermark**.

1. Configure the display content, text style, transparency, rotation angle, and size.
2. click **Background Settings** to set the watermark's background
3. click **Save**.

13.7 Third-Party Integration Settings

The third-party integration settings menu provides entries of integrating via Optimus, OpenAPI Gateway, SIA Gateway, BACnet Gateway, and Sur-gard Gateway, setting SIA event access, interchanging data, and setting a WhatsApp merchant account.

On the left navigation bar of the System page, select **Third-Party Integration** to display the third-party integration settings menu.

13.7.1 Integrate via OpenAPI Gateway

The platform provides the OpenAPI Gateway to integrate the third-party system. By the provided open APIs (Application Programming Interfaces), the third-party system can obtain some functions of HikCentral Access Control to develop more customized features.

Note

The gateway should be deployed on the same network with SYS.

Select **OpenAPI Gateway** on the left navigation bar, switch on **Open API**, and set the IP address and management port of the gateway, or select partner users to define resource and operation permissions in the integration.

(Optional) Click **Test** to test the service availability of the gateway.

Click **Save**.

13.7.2 Data Interchange

The access records in HikCentral Access Control can be used by third-party systems for pay calculation or other applications. You can synchronize the access records to a third-party database by entering the information of the database table in the required space. You can also dump the access records in CSV or TXT format, and then let the third-party database read the access records to get them.

Synchronize Access Records to Third-Party Database

You can enable synchronization function to apply the access records of specified resources from HikCentral Access Control to the third-party database automatically.

Steps

1. Select **Data Interchange** on the left navigation bar.
2. Switch on **Data Interchange**.
3. Click **Add** and select the resource(s) for access records synchronization.

Note

- For card readers, you should also select a direction when adding them. Or you can select the added card readers and click **Set Direction (In/Out) of Attendance Check Point** to batch select directions for them.
- Click in the Operation column to delete the resource or click **Delete All** to delete all added resources.
- Select the added resource(s) and click **Synchronize Event** and set the time range for events to be synchronized from devices.

4. Select the encoding format of data interchange.
5. **Optional:** Check **Do Not Push Failed Records**.

   The failed records will not be pushed to the third-party system.
6. Select **Database Synchronization**.
7. **Optional:** Switch on **Auto Push Failed Record** to select the push mode.

   Push at Fixed Time

   The failed record will be pushed at the time you set.

   Push at Fixed Interval

   The failed record will be pushed according to the interval you set.
8. **Optional:** Select a database type.
9. Set the required parameters of the third-party database, including server IP address or domain name, server port, database name, user name, and password.
10. Click **Test Connection** to test whether database can be connected.
11. Set table parameters of database table and table fields according to the actual configurations.
    1) Enter the table name of the third-party database.
    2) Enter the mode of the third-party database.
    3) Set the mapped table fields between the HikCentral Access Control and the third-party database.
    4) **Optional:** Click **Customize Items to Display** to select the items to be displayed in the table.
12. Click **Save**.

    A window will pop up and you can choose to push the test data now or later.
13. **Optional:** Click **Quick Diagnosis** in the top right corner to quickly diagnose the settings and the function.

    Note

    If there are errors found, you can export the failed data for checking.

Dump Access Records to Third-Party Database

The access records of specified resources can be dumped as a CSV file or TXT file and the third-party system will read the dumped file (instead of accessing the database and mapping the table fields) for further applications, such as attendance calculation and pay calculation. You can also

configure dump rules for dumping access records. After that, the access records will be dumped to the third-party database according to the added rules.

Steps

1. Select **Data Interchange** on the left navigation bar.
2. Switch on **Data Interchange**.
3. Click **Add** and select the resource(s) for access records synchronization.

Note

- For card readers, you should also select a direction when adding them. Or you can select the added card readers and click **Set Direction (In/Out) of Attendance Check Point** to batch select directions for them.
- Click in the Operation column to delete the resource or click **Delete All** to delete all added resources.
- Select the added resource(s) and click **Synchronize Event** and set the time range for events to be synchronized from devices.

4. Select the encoding format of data interchange.
5. **Optional:** Check **Do Not Push Failed Records**.

   The failure records will not be pushed to the third-party system.
6. Select **Access Record Dump**.
7. In the Dump Rule area, click **Add** and set the required parameters.

   Overwrite File

   If it not checked, you re recommended to regularly view the disk capacity in case the new files cannot be generated if the disk if full.

   File Name

   The name of the CSV file or TXT file which the access records are dumped as.

   Storage Location

   Local Storage

   The access records can be dumped as a file saved in the local disk of the SYS. Then you need to copy this file from the server to your PC with the third-party system installed to read the dumped file.

   Note

   - You need to log in to the Web Client running on the SYS to configure related settings of local storage.
   - You need to set **Saving Path**, which is the path where the CSV file or TXT file is saved.

   SFTP Storage

   You can access the SFTP server as the storage location for saving the dumped file by setting the SFTP address, port, user name, and password. And you can enter the path to

save the dumped file in the folder on the SFTP server or leave it empty to save the file in the root directory.

Note

The third-party system should be installed in the SFTP server to read the dumped file.

Content

The display items and data in the dumped file.

Department

The group of persons. You can select and search for departments in the list.

Min. Length of Person ID

For some scenarios, the person IDs need to be dumped as a certain fixed length.

You can switch it on and set the value of **Length**. If the length of the person ID is shorter than the value, zero(s) will be added before the ID to make it equal to the value. If the length is longer than the value, the person IDs will be dumped according to the actual length.

Designated Length of Card No.

For some scenarios, the card numbers need to be dumped as a certain fixed length.

You can switch it on and set the value of **Length**. If the length of the card number is shorter than the value, zero(s) will be added before the card number to make it equal to the value. If the length is longer than the value, the card number will be dumped according to the actual length.

Generate Table Header

When the card swiping records are dumped from the system to the local PC, the column names will be included in the dumped file and used as the table header.

File Format

Two formats are supported, including CSV and TXT.

Dump Frequency

The frequency for dumping access records.

Dump Time

The time when dumping card swiping records is started.

8. Click **Add** on the Add Dump Rule page.

The added rules will be listed in the Dump Rule area.

Note

You can click × in the Operation column to delete the rule or click **Delete All** to delete all added rules.

9. Click **Save**.
10. **Optional:** Click **Quick Diagnosis** in the top right corner to quickly diagnose the settings and the function.

Note

If there are errors found, you can export the failed data for checking.

13.8 Advanced Settings

The advanced settings menu provides entries of setting system hot spare, generating or debugging logs, downloading the event tracking information, and resetting the network information for devices.

On the left navigation bar of the System page, select **Advanced** to display the advanced settings menu.

13.8.1 Diagnosis and Maintenance

For the operation and maintenance personnel, they can generate and download logs of a specified time period for locating issues, debug logs, and view or download the event tracking information.

Select **Diagnosis & Maintenance** on the left navigation bar.

Generate Logs

1. Check the service log type(s).
2. Specify the start and end time of the time period in which the logs are to be generated.
3. Click **Generate** to start generating a log file.
   When completes, a zip file name will appear at the bottom of the Maintenance Data section and you can click to download the log file to the local PC.

Debug Logs

1. Click **Download Template** to download the template of log configuration file to the local PC.
2. Fill in the template with required information locally.
3. Click to upload the configured template to the platform and click **Start Debugging**.
   A 24-hour countdown will automatically start.

   Note

   When the countdown finishes, the on-going debugging will be canceled automatically. You can click **Extend Debugging** to extend the debugging duration.
4. (Optional) Click **Close Debugging** to stop the debugging.

View and Download Event Tracking Information

Click **Event Tracking Information** in the top right corner of the Diagnosis and Maintenance page to open the Event Tracking Information page.

On the Event Tracking Information page, you can view the exception and general information and click **Download Event Tracking Information** in the top right corner to download the event tracking information to the local PC. You can also click **Refresh** to refresh the event tracking information.

13.8.2 Reset Device Network Information

When the system network domain changes (such as server migration), you must reset the network information for the added device to adapt to the new network environment. Otherwise, some functions of the device will be affected.

Steps

1. Select **Reset Network Information** on the left navigation bar.
2. Click **Reset** to one-touch reset the device network information.

13.9 Set Company Information

You can configure and show the company information on the Web Client for customization requirements.

Select **Company Information** on the left navigation bar.

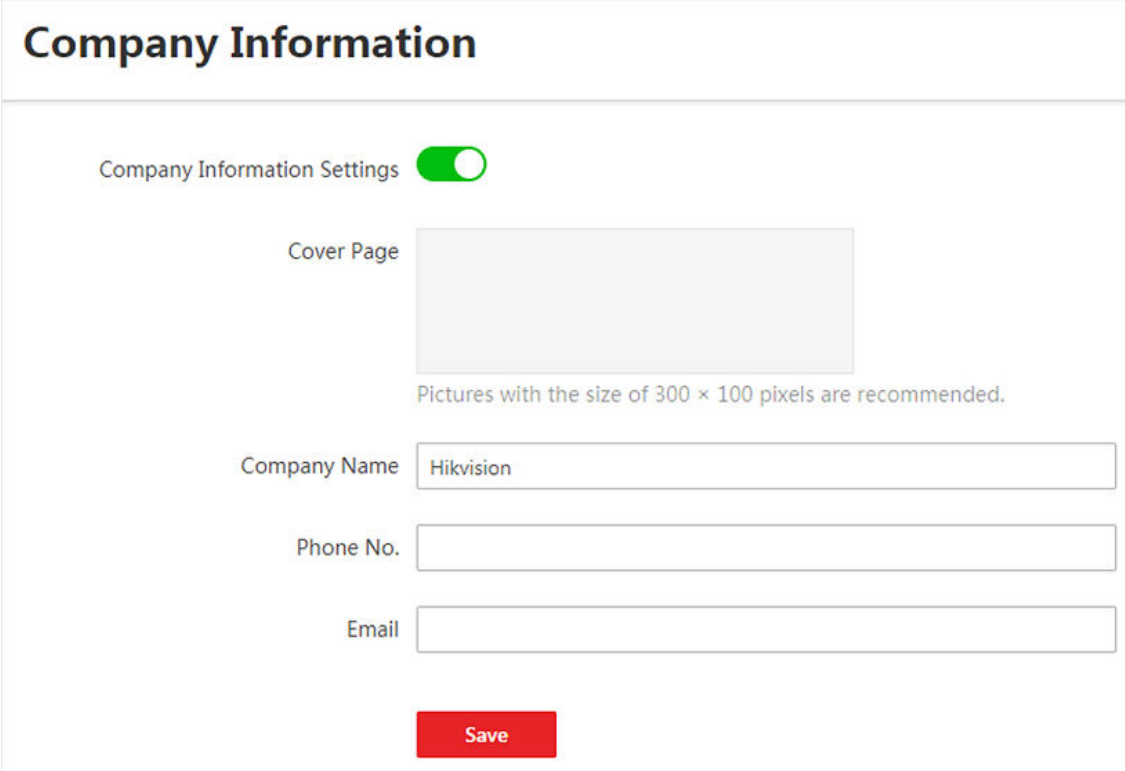


Figure 13-4 Company Information Settings

Switch on **Company Information Settings** to enable displaying company information on the Web Client. Then set the information (cover page, company name, etc.) as needed and click **Save**.

An icon appears at right of the Web Client and keeps displaying. You can click the icon to view the company information.

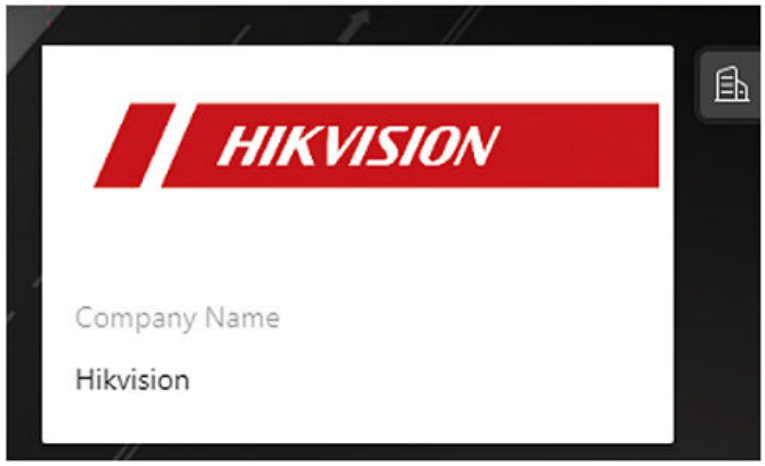


Figure 13-5 Company Information Displayed on Web Client

Chapter 14 Event and Alarm

On the Web Client, you can set rules to detect events and alarms, and set linkage actions for notification. The detailed information of the events and alarms can be received and checked via the Mobile Client.

On the top, select **System**.

Event

Event is the signal that resource (e.g., device, server) sends when something occurs. The platform can receive and record events for checking, and can also trigger a series of linkage actions for notification. The event can also trigger an alarm for further notification and linkage actions (such as alarm recipients and pop-up window). You can check the event related video and captured pictures if you set the recording and capturing as event linkages.

The rule of an event includes four elements, namely, "event source" (i.e., the device which detects the event), "triggering event" (the specified event type), "what to do" (linkage actions after this event is detected), and "when" (during the specified time period, the linkage actions can be triggered).

Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. Alarm can trigger a series of linkage actions (e.g., popping up window, showing the alarm details) for notification and alarm handling. You can check the received real-time alarm information and search for history alarms.

The rule of an alarm includes six elements, namely, "alarm source" (i.e., the device which detects the triggering event), "triggering event" (the specified event type occurred on the alarm source and triggers the alarm), "when" (during the specified time period, the alarm can be triggered), "recipient" (the user on the platform who can receive this alarm), "priority" (the importance or urgency of this alarm), and "what to do" (linkage actions after this alarm is triggered).

Linkage Action

An event's linkage actions (such as card swiping and user login) are used to record the event details and trigger basic actions (such as linking access point to lock or unlock, triggering alarm output, and sending email).

An alarm's linkage actions (such as sending emails to specific groups) are used to record the alarm details and provide recipients multiple ways to view the alarm information for alarm acknowledgment and handling.

14.1 Manage Event and Alarm

You can configure parameters for event types provided by the platform to detect normal events or trigger normal alarms, or add combined alarms, generic events, and user-defined events for a wider range of applications.

14.1.1 Supported Events and Alarms

Currently, the platform supports following events and alarms for different types of resources.

Access Control

Door

Events occurred on doors of access control devices and video intercom devices, such as access event and door status event.

Alarm Input

Events occurred on alarm inputs of access control devices on the platform.

Person

Events occurred during the process of authentication by person, such as card No. matched events and person matched events.

Maintenance

Operation exceptions occurred on the resources (e.g., access control devices) added to the platform, such as the device offline, server exception, and so on.

User

Events occurred during the user login and logout process.

Custom Event

User-Defined Event

Events defined by users themselves.

Generic Event

Events transferred in the form of TCP/UDP/HTTP/HTTPS data packages from resources (e.g., external systems and devices) if something occurred and matched the configured expression.

Device Application Event

Events uploaded by the added resources which contain HEOP or AIOP application.

14.1.2 Add Combined Alarm

For some complicated scenarios, the alarm should be triggered when multiple events or alarms are detected or triggered. For example, the platform detects intrusion in area B, then the arming of

area A starts. After that, if the platform detects intrusion in area A, then an alarm will be triggered to notify the security personnel.

Steps

1. On the left of the System module, click **Event and Alarm → Combined Alarm** .
2. Click **Add Combined Alarm** to open the Add Combined Alarm pane.

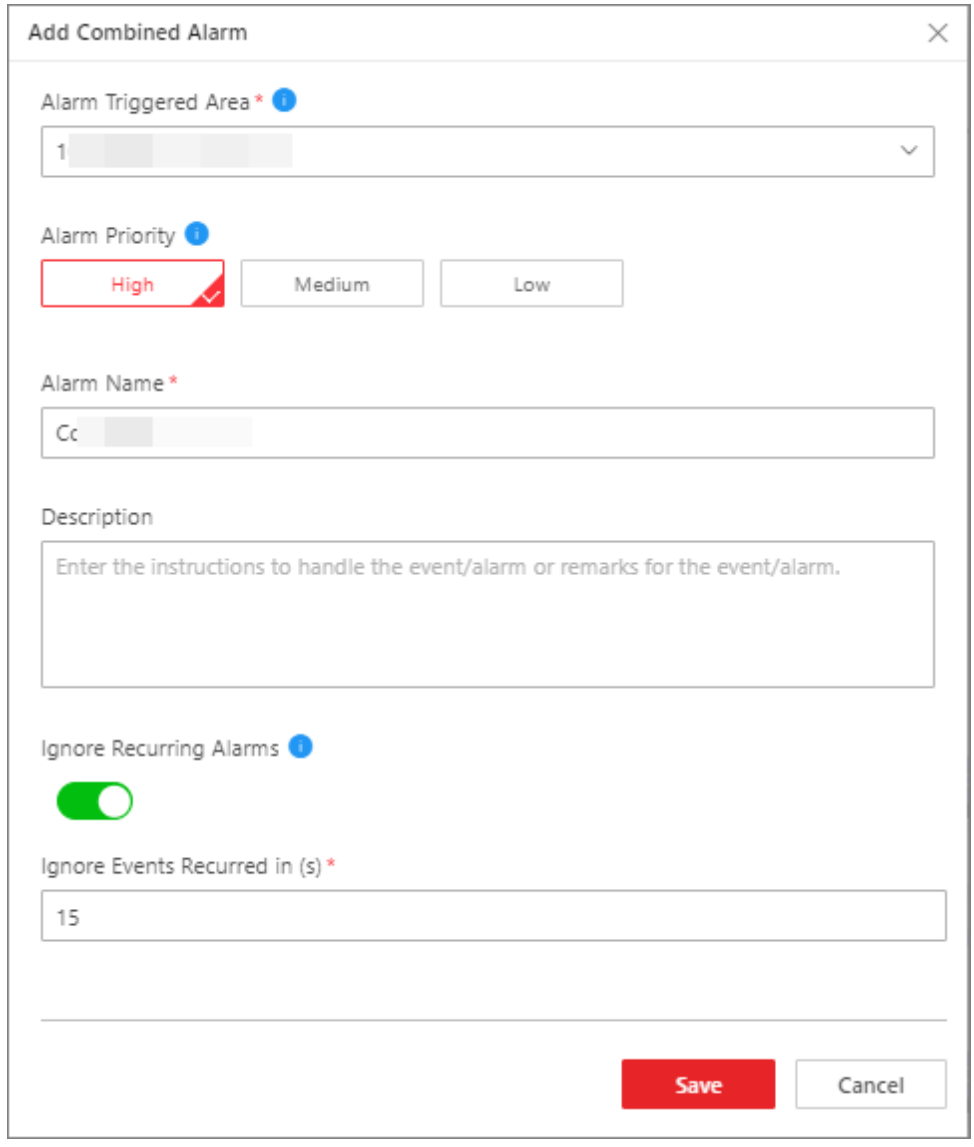


Figure 14-1 Add Combined Alarm

3. Set parameters on the page.

Alarm Triggered Area

Select the area where the combined alarm will be triggered.

Alarm Priority

The priority including low, medium, high, and custom level, which indicates the urgent degree of the combined alarm.

Alarm Name

Create a name for the combined alarm.

Description

Describe the combined alarm according to your requirements.

Ignore Repetitive Events/Alarms

Once it is enabled, the platform will ignore the combined alarm recurred within the configured time period.

4. Click **Save** to enter the configuration page.
5. Configure a receiving schedule for the combined alarm.
   1) Click ⊕ on the configuration page to open the Select Schedule Template pane.
   2) Select a schedule template as **All-Day Template**, **Weekday Template**, **Weekend Template**, or a custom template.

   Note

   For how to customize a schedule template, refer to ***Configure Receiving Schedule Template*** .

   3) Click **Save**.

   A Receiving Schedule card will appear on the page.

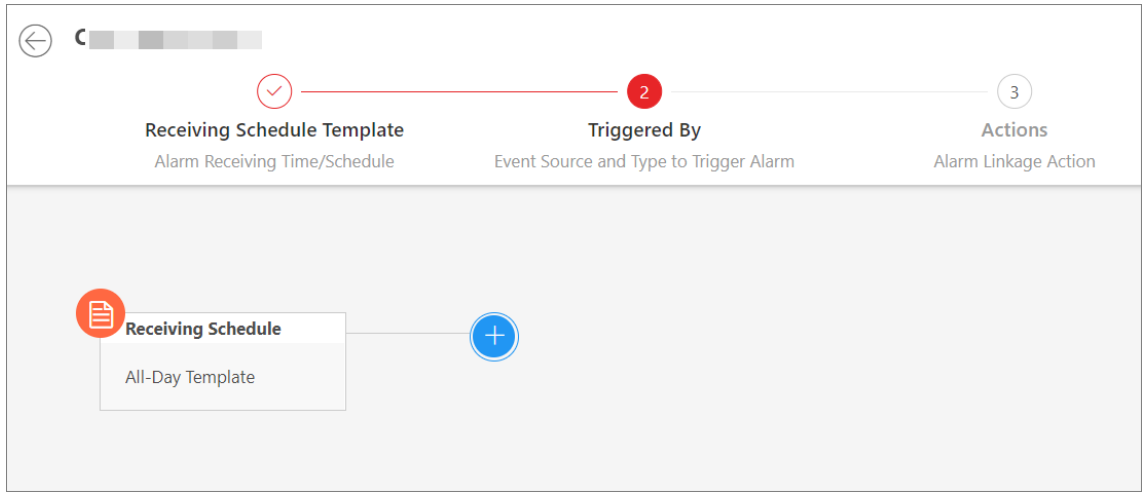


Figure 14-2 Receiving Schedule Card

6. Configure conditions for triggering the combined alarm.
   1) Click ⊕ at the right of the Receiving Schedule card to open the Select Alarm Triggering Logic pane.
   2) Select a triggering logic and click **Save**. The condition card will appear.

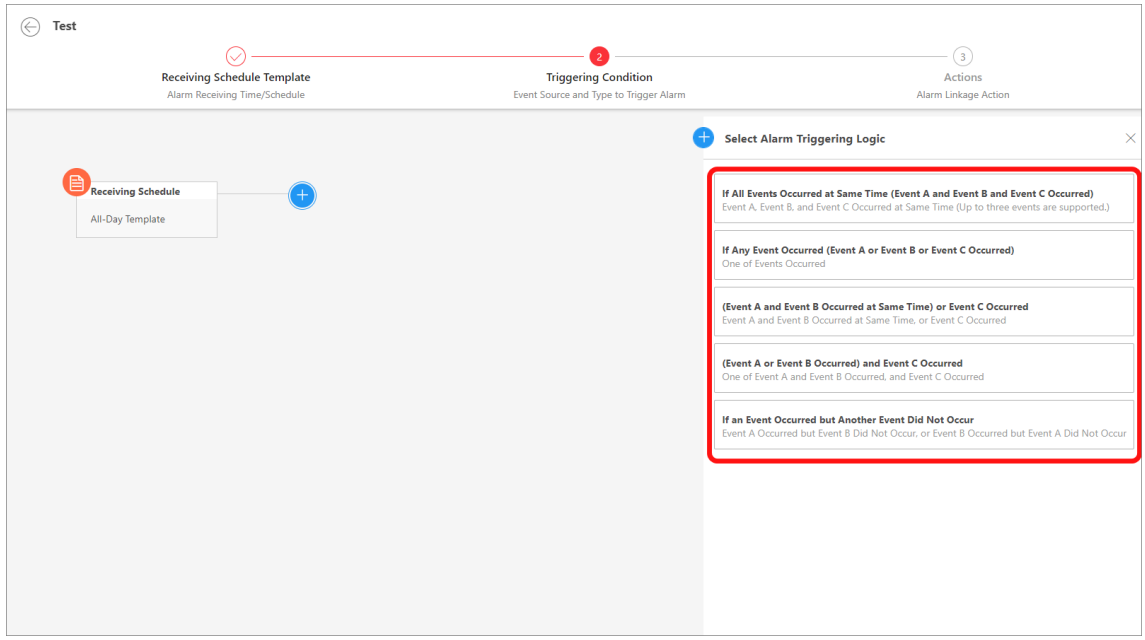


Figure 14-3 Alarm Triggering Logic

3) Click ⊕ on the condition card to open the Select Event Source and Event Type pane.
4) Select a triggering event and a source, and click **Save**.

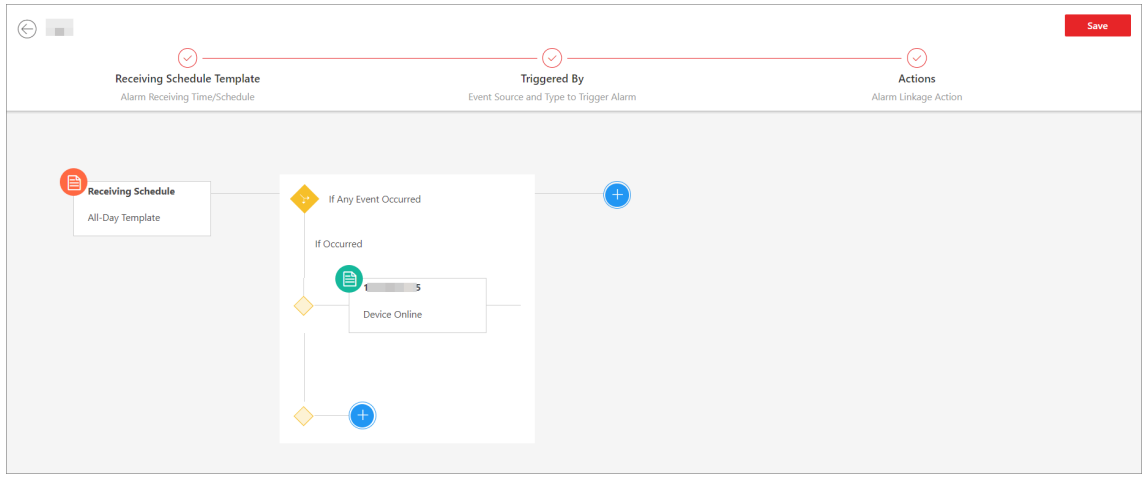


Figure 14-4 Condition Card

5) **Optional:** Click ⊕ below the newly added event source and type card to select more event sources and types.
6) **Optional:** Click ⚙ on the event source and type card to enter the remote configuration page of the event source. For details about remote configuration, refer to the user manual of the corresponding device.

7. Configure the alarm recipient(s) and linkage action(s) for the combined alarm.
1) Click ⊕ at the right of the triggering logic card to open the Select Alarm Linkage Action panel.

2) Click **Alarm Recipients** and select the recipient(s).

Note

If **Automatically Receive Alarm** is enabled for some users (refer to ***Add a Normal User*** for details), the Alarm Recipients card will be automatically generated after the event source and type is configured, and these users will be selected as recipients. You can click the generated card to edit the alarm recipients, but the selected users cannot be unselected.

3) Click **Save**.

4) Click ⊕ below the Alarm Recipients card to select a linkage action and set the corresponding parameters. For details, refer to .

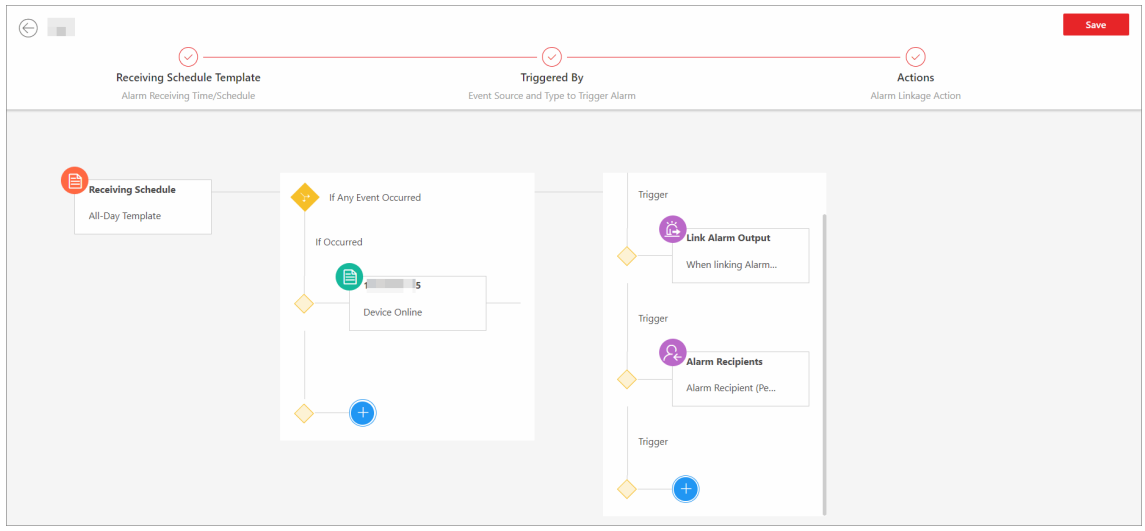


Figure 14-5 Action Card

5) **Optional:** Click ⊕ below the Alarm Recipients card to add more linkage actions.

8. **Optional:** Click the icon on the top left of each card to reselect the content.
9. **Optional:** Move the cursor on each card and click 🗑 appeared on the top right of the card to delete the card.

Note

If the card is deleted, the following cards or sub cards (if any) will also be deleted.

10. Click **Save** in the top right corner of the combined alarm configuration page to add the combined alarm to the platform.

Note

If the alarm recipients are not configured for this combined alarm, you cannot save the combined alarm.

11. **Optional:** Perform the following operations according to your requirements.

Copy Parameters to Existing Alarm	Click **Copy**, and select **Add Combined Alarm** to copy the current rule to other resources, or select **Copy Settings to Other Alarm** to copy selected settings (such as basic information, actions, receiving schedule, receiving mode) to the target.
Delete Alarm	Click **Delete** to delete this alarm.
Test	Click **Test** to trigger this alarm manually, and you can check whether the linkage actions take effect and whether the recipients can receive the notification.
Enable/Disable	Switch on the button beside **Status** to enable or disable this alarm. After the alarm is enabled, it can be received by the platform. If you disable this alarm, you will be required to set the start time and duration of disabling and the platform cannot receive the alarm in the duration.

14.1.3 Add Generic Event

A generic event is a signal transferred in the form of TCP/UDP/HTTP/HTTPS data package from the resource (e.g., external systems and devices) if something occurred and matched the configured expression. In this way, you can easily integrate the platform with a very wide range of external sources, such as access control systems and alarm systems.

Steps

1. On the top, select **System**.
2. Select **Event and Alarm → Generic Event** on the left.
3. Click **Add** to enter the Add Generic Event page.

Note

You can also click **Import** to batch import the events by the template.

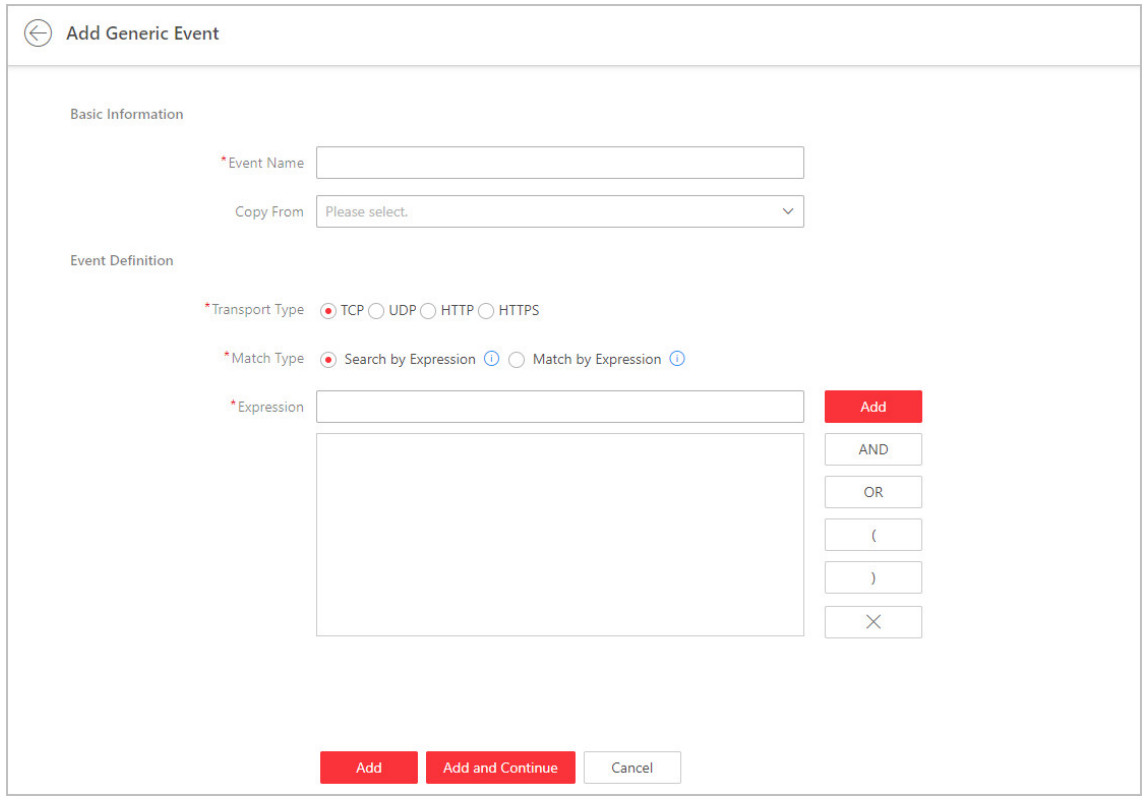


Figure 14-6 Add Generic Event Page

4. Set a name for the event.
5. **Optional:** Copy the settings from other generic events in the **Copy from** field.
6. Select **TCP**, **UDP**, **HTTP**, or **HTTPS** as the transport protocol.
7. Select the match type to define what received data packages can trigger events.

   Search by Expression

   The received package must contain the text defined by the expression or more. For example, if you have defined the expression as 'Motion' AND 'Line Crossing', the event can be detected when the received package contains "Motion", "Intrusion", and "Line Crossing".

   Match by Expression

   The text in the received package must be exactly the same as that defined by the expression.

   Search by Keyword

   The received package must contain the keywords.
8. Define the expression for analyzing the received package.
   1) Enter the term which should be contained in the expression in the text field.
   2) Click **Add** to add the term to the expression.
   3) Click the parenthesis or operator button to add it to the expression.
   4) **Optional:** Click ✕ to remove the item at the left of the cursor from the expression.

Note

You can position the cursor inside the expression in order to determine where a new item should be included or where an item should be removed.

The parenthesis or operator buttons are described in the following:

AND

You specify that the terms on both sides of the AND operator must be included.

For example, if you define the rule as 'Motion' AND 'Line Crossing' AND 'Intrusion', the term Motion, and Line Crossing as well as the term Intrusion must be all contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with AND, the fewer events will be detected.

OR

You specify that any term should be contained.

For example, if you define the rule as 'Motion' OR 'Line Crossing' OR 'Intrusion', any of the terms (Motion, Line Crossing, or Intrusion) must be contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with OR, the more events will be detected.

(

Add the left parenthesis to the rule. Parentheses can be used to ensure that related terms are processed together as a unit; in other words, they can be used to force a certain processing order in the analysis.

For example, if you define the rule as ('Motion' OR 'Line Crossing') AND 'Intrusion', the two terms inside the parentheses will be processed first, then the result will be combined with the last part of the rule. In other words, the system will first search any packages containing either of the terms Motion or Line Crossing, then it searches the results to look for the packages that contain the term Intrusion.

)

Add the right parenthesis to the rule.

9. Click **Add** to add the event and back to the event list page, or click **Add and Continue** to add the event and continue to add a new event.
10. **Optional:** Perform the following operations after adding the event.

Edit Event Settings	Click the name in the Event Name column to edit the corresponding event settings.

Receive Generic Event	Select the events, click **Receive Generic Event** to open the settings pane, and check the checkboxes to enable receiving the generic events via different protocols.
Import/Export Events	Select the events, and click **Import/Export**.

14.1.4 Add User-Defined Event

When you are viewing videos or checking the alarm information, if there is some information that needs to be paid attention to, you can manually define a new event type which is not in the provided event and alarm list or the defined generic events for triggering an alarm or being configured as a linkage action of alarms. This kind of event is called as the user-defined event.

Steps

1. On the top, select **System**.
2. Select **Event and Alarm → User-Defined Event** on the left.
3. Click **Add**.

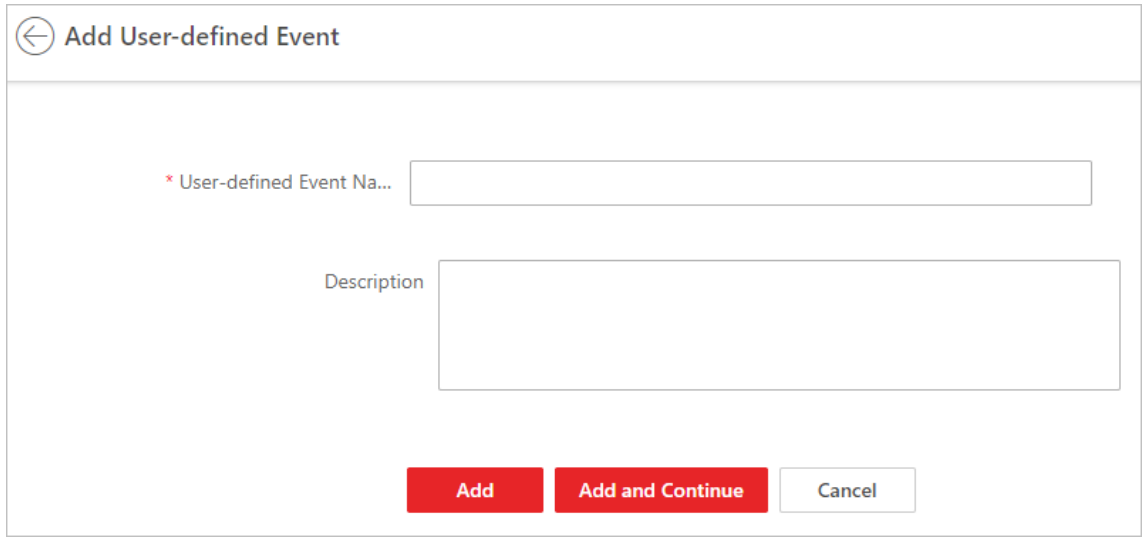


Figure 14-7 Add User-Defined Event

4. Create a name for the event.
5. **Optional:** Enter the information to describe the event.
6. Click **Add** to add the event and go back to the event list page, or click **Add and Continue** to add the event and continue to add a new one.

   With the customized user-defined event, the platform provides the following functions:

   - Integrate other third-party systems with HikCentral Access Control by using the data received from the third-party system. The user-defined events can be triggered as an alarm outside the HikCentral Access Control. For details, contact our technical support.

14.2 Set Basic Event and Alarm Parameters

After setting basic parameters for events and alarms, you can set receiving schedules, and recipient groups or specific recipients who can receive events and alarms in specific timeout period, and you can send events/alarms reports regularly via email to the recipients / recipient groups. You can also define alarm priorities, alarm categories, and alarm icons to meet the actual requirements.

14.2.1 Configure 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. The platform has predefined three default receiving schedule templates: All-Day Template, Weekday Template, and Weekend Template. You can also customize a template according to actual needs.

Steps

Note

Receiving schedule template defines the time when you can receive events or alarms. If the event schedule differs from the alarm receiving schedule, make sure the time of the event receiving schedule covers that of the alarm receiving schedule.

1. On the top, select **System**.
2. Select **Event and Alarm → Receiving Schedule Template** on the left.
3. Click + to enter the Add Receiving Schedule Template page.

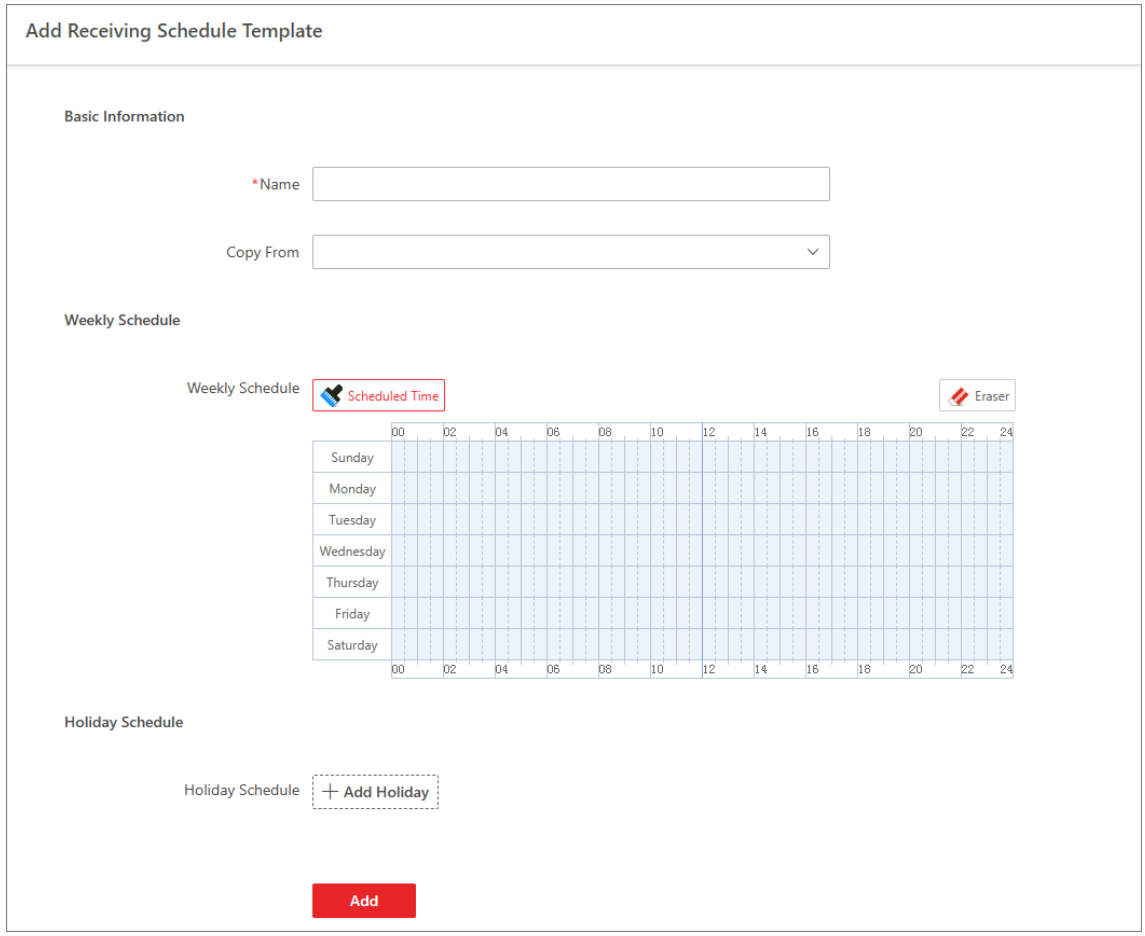


Figure 14-8 Add Receiving Schedule Template

4. Enter a name for the template.
5. **Optional:** Select another defined template to copy the settings to the current template.
6. Click **Scheduled Time** and drag on the time bar to set time periods during which the event can be triggered on the event source and notified the recipients.

Note

- Up to 4 time periods can be set for each day.
- On the schedule time table, you can click to set the specific time period which accurate to minute.

7. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
8. **Optional:** Set a holiday schedule if you want different schedules for specific days.
   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set the schedule for holidays.

9. Click **Add** to add the template.

The receiving schedule template will be displayed on the receiving schedule template list.

10. **Optional:** Perform the following operations after adding the receiving schedule template.

View Template Details	Click the template name to view its details.
Edit Template	Click the name of a custom template to edit template details. **Note** The predefined templates cannot be edited.
Delete Template	Select a template and click to delete the template. **Note** • The predefined templates cannot be edited. • If there are events/alarms configured with this template, you can replace the template with other receiving schedule. Or you can click **Delete Now** to delete the template, and this operation will cause exceptions of related events/alarms.

14.2.2 Custom Alarm Settings

The platform has predefined several alarm priorities, alarm categories, color template, and alarm icons for basic needs. You can edit the predefined alarm priority and alarm category, and customize alarm priority and alarm category according to actual needs.

Steps

Note

Alarm Priority

Define the importance or urgency of alarms for handling or acknowledgment.

Alarm Category

Used when the user acknowledges the alarm and categories what kind of alarm it is, e,g., false alarm, or alarm to be verified. You can search for alarms by the alarm category.

Alarm Icon When Alarm Occurs

The platform has predefined some icons of resources for several special alarms.

For example, it predefined the icon for the Door Opened Abnormally alarm. When this alarm is triggered, the door icon will turn to the icon displayed here to notify users.

1. On the top, select **System**.

2. Select **Event and Alarm → Alarm Custom Settings** on the left.
3. Customize alarm priorities according to actual needs. By default, three kinds of alarm priority exist.

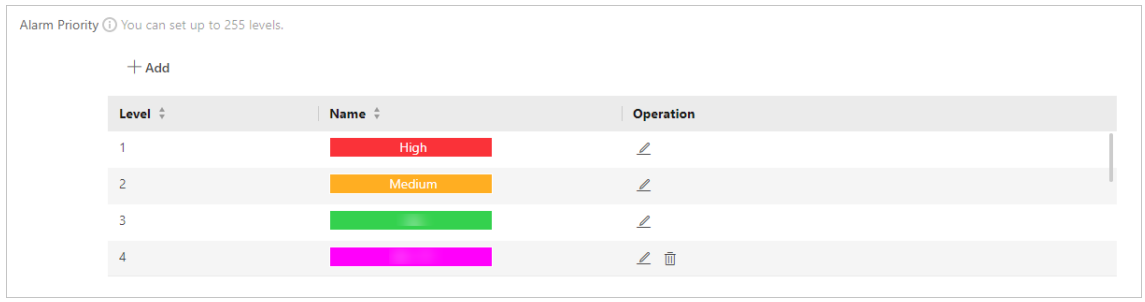


Figure 14-9 Alarm Priority

1) Click **Add** to open the adding alarm priority pane.

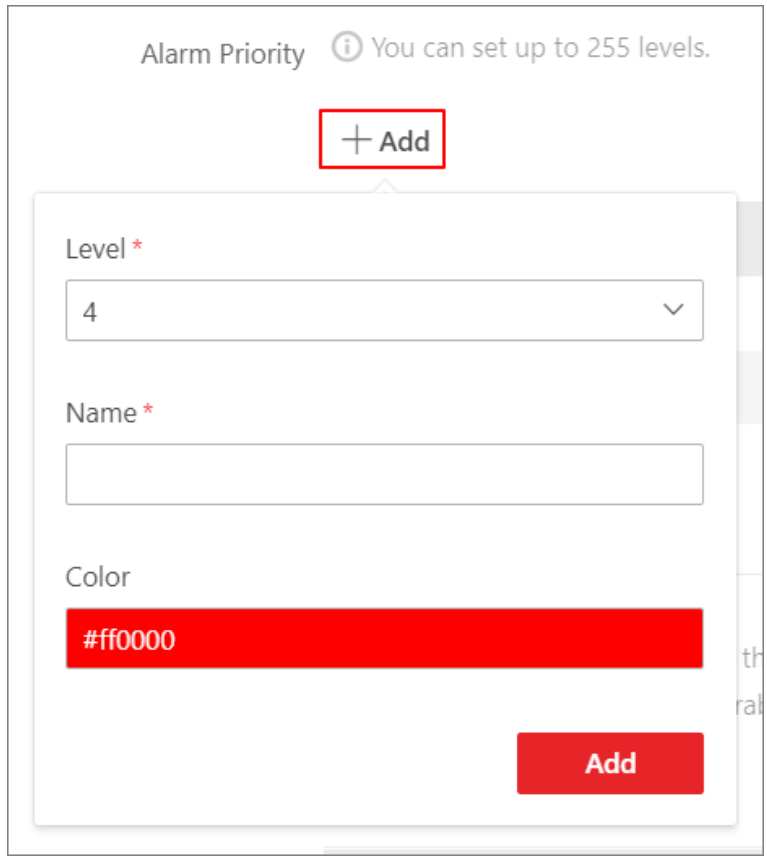


Figure 14-10 Add Alarm Priority

2) Select a level No. for the priority.
3) Enter a descriptive name for the priority.
4) Select the color for the priority.
5) Click **Add**.

The priority will be displayed on the alarm priority list.

4. Customize alarm categories according to actual needs. By default, four alarm categories exist.

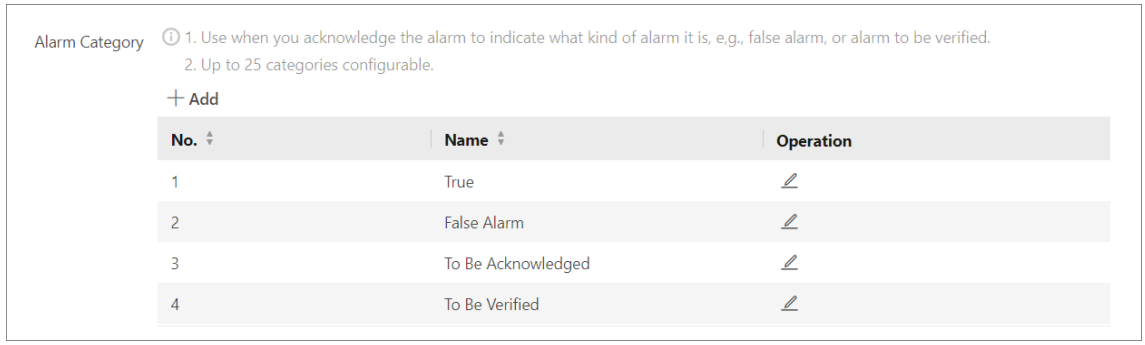


Figure 14-11 Alarm Category

1) Click **Add** to open the adding alarm category pane.

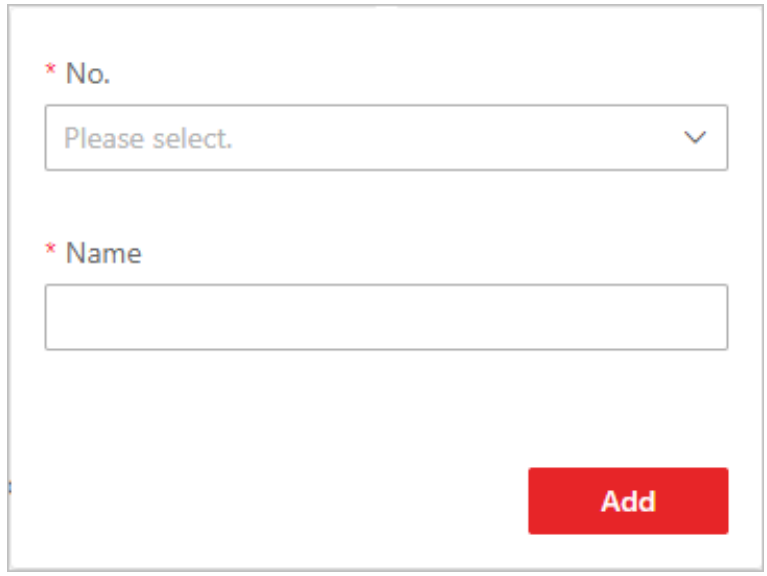


Figure 14-12 Add Alarm Category

2) Select a No. for the alarm category.
3) Enter a descriptive name for the alarm category.
4) Click **Add**.

The alarm category will be displayed on the alarm category list.

5. In the Alarm Icon When Alarm Occurs field, view the alarm icons provided by the platform which are used to notify the users that the alarm is triggered.

Note

These predefined alarm icons cannot be edited and deleted.

6. **Optional:** Perform the following operation(s) after adding alarm priority and category.

Edit Click to edit the alarm priority and category.

Note

You cannot edit the No. of predefined alarm priorities and categories.

Delete Click to delete the alarm priority and category.

Note

You cannot delete the predefined alarm priorities and categories.

14.2.3 Configure Alarm Receiving Settings

You can manage alarm recipients in groups to quickly set recipients for different categories of alarms, and set default alarm recipients who can receive all the alarms triggered by resources they have access permissions, so that you do not have to select recipients for each single alarm.

Steps

1. On the top, select **System**.
2. Select **Event and Alarm → Alarm Receiving Configuration** on the left.
3. In the Alarm Recipient Group field, click + above the group list to open the adding alarm recipient group pane.
4. Enter a name for the group and click **Add**.

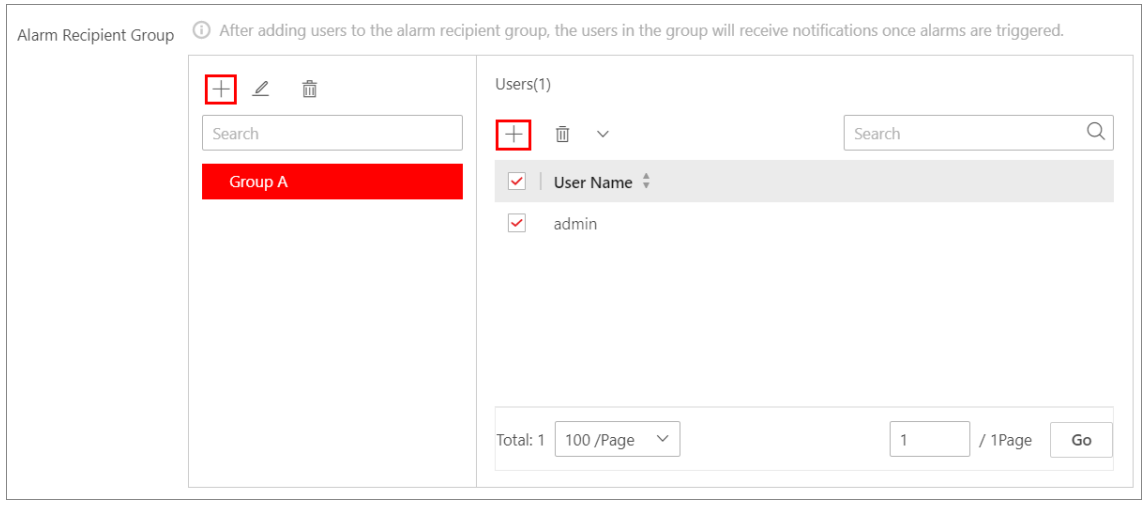


Figure 14-13 Alarm Recipient Group Field

5. Select an alarm recipient group and click + in the Users field to add user(s) to the group.
6. **Optional:** Check user(s) in the group and click to remove the selected user(s) from the group or click → **Delete All** to remove all the users from the group.
7. Check user(s) in the Recipient field as the default alarm recipient(s).

   The default alarm recipients will be automatically selected when setting recipients for alarms, and they cannot be deselected.

8. Click **Save**.

   The configured alarm recipient group(s) will appear on the Add Event and Alarm page and they can be selected when setting recipients for alarms.

14.2.4 Send Event and Alarm Report Regularly

You can set a scheduled report rule for specified events or alarms, and the platform can send an email with a report attached to the target recipients by day or week, showing the details of specified events or alarms triggered on the day or the week.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

One report can contain up to 10,000 event records in total.

1. On the top, select **System**.
2. Select **Event and Alarm → Scheduled Report** on the left.
3. Click **Add** if there is no scheduled report rule or click + above the rule list to enter the Create Report page.
4. Set the basic information.

   Report Name

   Create a name for the report.

   Format

   Select **Excel** or **PDF** as the report format and select a language for report contents.

   Note

   You can skip this step if you want to keep the default settings.

   Report Language

   Select the report language.
5. In the Report Content field, select **Event Alarm Rule** or **Area** as the statistics dimension, and click **Add** to select statistical objects to be contained in the report.

   Note

   Up to 32 events and alarms can be added in one report.
6. Set the report sending rule and time.

Statistical Cycle

By Day

If the statistics cycle is selected as **By Day**, the report shows data on a daily basis. The platform will send a report at the sending time on the selected day(s) of the week, which contains information of the events triggered on the day (24 hours) before the sending date.

For example, if you select **Monday**, **Tuesday**, and **Friday** in the Send On failed, and set the sending time as 18:00, the platform will send a report at 18:00 on every Monday, Tuesday, and Friday, containing details of all the events triggered between 00:00 and 24:00 on every Sunday, Monday, and Thursday.

By Week

If the statistics cycle is selected as **By Week**, the report shows data on a weekly basis, which may be less time-consuming. The platform will send a report at the sending time on the selected day of the week, which contains information of events and alarms triggered on the recent 7 days or recent 14 days before the sending date.

For example, if you set the sending time as 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing details of all the events triggered between last Monday and Sunday.

Report Time

Select the specific report time.

Send On

Select the date of a week for sending the report. You can click **Select All** to set all dates of a week.

Send At

Select the time of a day for sending the report.

Effective Period

Set an effective period for the report to improve the data security.

7. Set advanced parameters.

Send via Email

If it is enabled, you can select an email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add New** to add a new email template. For setting the email template, refer to ***Email Settings*** .

Upload to SETP

If it is enabled, the platform will automatically upload and save reports to the FTP server.

Save to Local Storage

If it is enabled, the platform will automatically upload and save reports to the local storage.

Note

You can click **Configure** or click → **SFTP Settings / Configure Local Storage** to log in to the SFTP server by entering the IP address, port, user name, and password, and set the saving path on the SFTP server or local storage for reports.

8. Click **Save** to add the report rule.

14.3 Event and Alarm Search

The platform provides the statistics and analysis results of historical events and alarms for you to have an overview and further applications. You can also search for historical events and alarms by setting different conditions to view the details as required.

14.3.1 Event and Alarm Overview

In the event and alarm overview module, it gives you an overview of the event or alarm distribution, top 5 event types or alarm categories, and top 5 event or alarm areas.

On the top, select **System**.

Select **Event and Alarm → Overview** on the left.

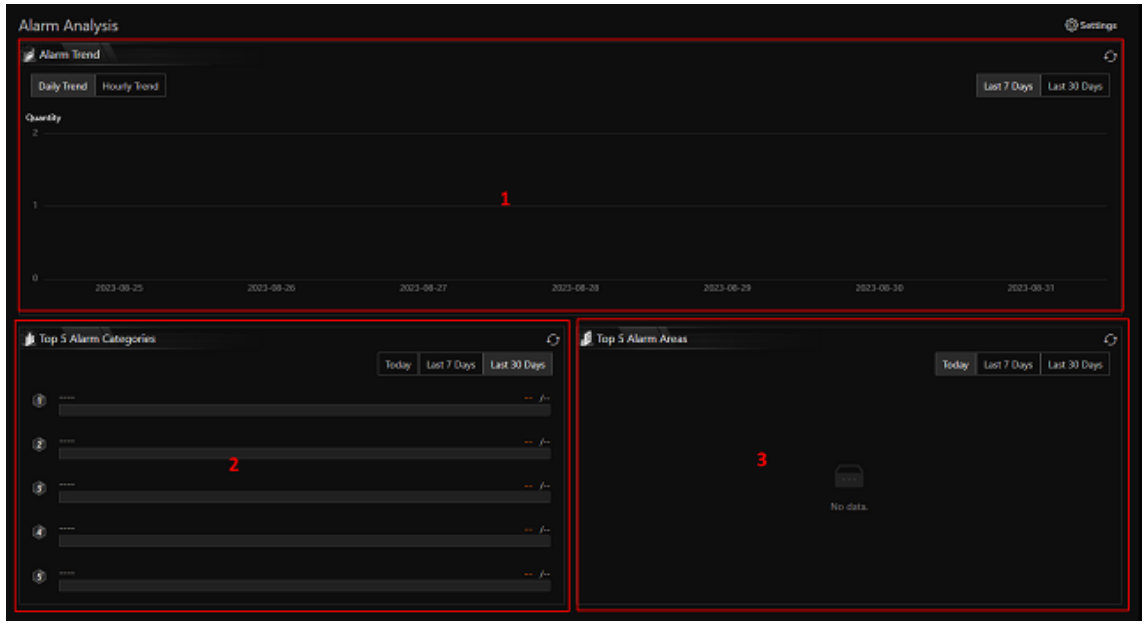


Figure 14-14 Event and Alarm Analysis

Module	Description
1	• Daily Trend: The numbers of events or alarms in the last 7 days or last 30 days are displayed in the vertical bar chart. • Hourly Trend: The numbers of events or alarms of 24 hours for the last 7 days, the last 30 days, or the custom period are displayed in the line chart.
2	The data of top 5 event types or alarm categories triggered in the current day, last 7 days or last 30 days are displayed in the horizontal bar chart. You can click the red number of an item to jump to the Event and Alarm Search page.
3	The data of the top 5 event or alarm areas in the current day, last 7 days or last 30 days are displayed in the horizontal bar chart.

You can click **Settings** in the upper-right corner to customize event types or alarm categories to be calculated on the overview page.

Note

The information displayed in each area will change according to the report target on the Settings pane. For example, if you select **Alarm** on the Settings pane as the report target, the upper area will only display the number of alarms, the lower-left area will only display the data of top 5 alarm categories, and the lower-right area will only display the data of top 5 alarm areas.

14.3.2 Search for Event and Alarm Logs

You can search for event and alarm log files of the added resource by setting different conditions.

Before You Start

Make sure you have configured events and alarms first. See for details.

Steps

1. On the top, select **System → Event and Alarm → Event and Alarm Search** .
2. Set the time range for search.
   - Select a predefined time period for search.
   - Select **Custom** and specify the start time and end time for search.
3. In the field of **Trigger Alarm**, select the event status (whether the event is triggered as the alarm).

   All

   Both events and alarms.

   Disabled

   The events happened but were not triggered as alarms.

   Enabled

The events happened and were triggered as alarms. If you select this, you can set conditions for filtering alarms by marking status, acknowledging status, alarm priority, or alarm category.

4. Switch **Area** on and then click to select the area of the event or alarm source.
5. Switch **Triggering Condition** on and then click to select the triggering events.

Note

- If you select triggering events in the Access Control category, enter the entered/exited person's name.
- If you select triggering events in the Third-Party Resource Integration category and have entered the additional information about the alarm on the third-party system, enter the additional information.

6. Switch **Event/Alarm Name** on to select the event/alarm name in the drop-down list.
7. Click **Search**.

   The matched event or alarm logs will be listed on the right page.
8. **Optional:** Click **Export** and select the format as **Excel** or **PDF** to save all searched events and alarms to the local PC.

Note

When exporting all events and alarms in Excel format, you can check **Include Picture Information** to export the related pictures.

Chapter 15 Maintenance

The system provides Service Manager to manage the installed services on the SYS server. You can check the service's running status, edit the service port, start/stop service via the Service Manager.

The system also provides backup of the database, so that your data can be well protected and recovered when an exception occurs.

You can also export the system's configuration data and save it to the local PC.

On the top, select **System → Maintenance** .

15.1 Real-Time Health Status Overview

In the Health Overview module, you can view the real-time health status of the devices, servers, and resources managed on the platform.

On the left of the System module, click **Maintenance → Real-Time Overview** .

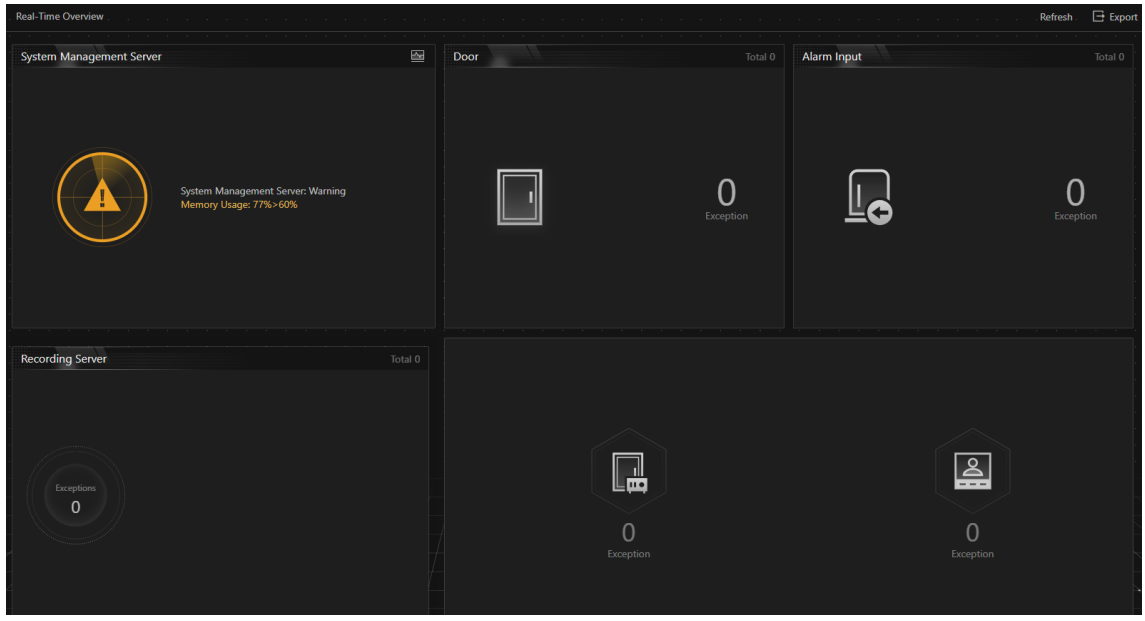
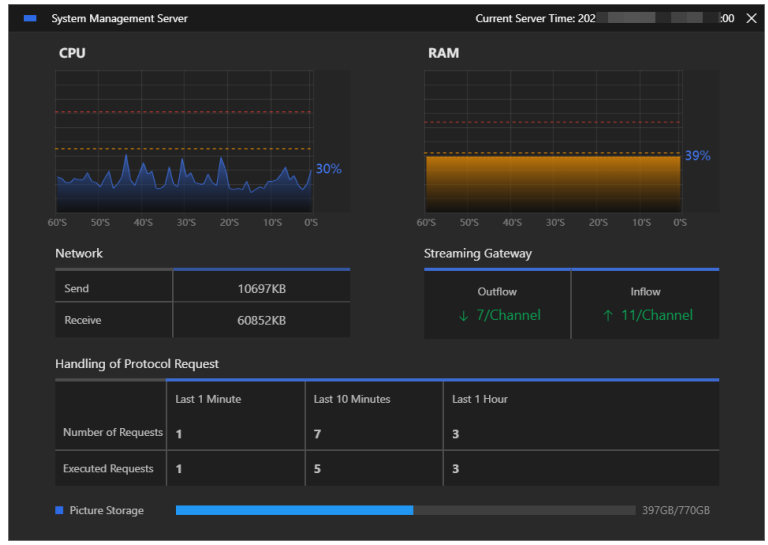
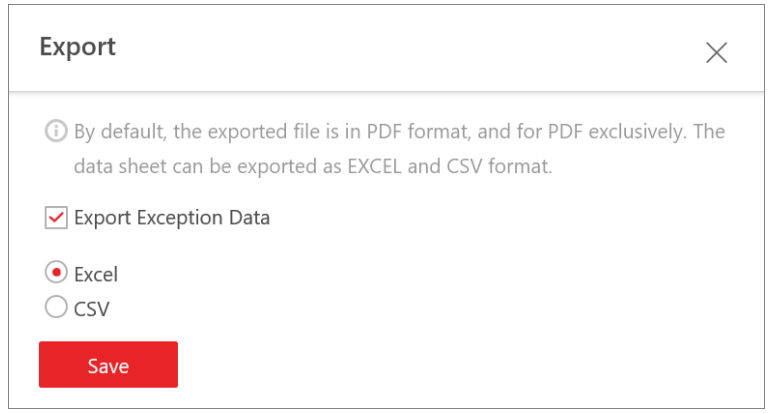


Figure 15-1 Real-Time Health Status Overview

Table 15-1 Real-Time Health Status Page

Section	Description
Display Resource Status by Site	Select a site from the drop-down list in the upper left corner to display the status of resources on the selected site.

Section	Description
	If an exception occurs on a site, the icon will appear beside the site name and you can move the cursor over it to view the exception details.
System Management Server Status	View the CPU and RAM usages of the site server in the top right corner of the overview page. Click **Details** to open the System Management Server window to view the detailed status, including the current server time, CPU usage, RAM usage, network status, streaming gateway status, handling status of protocol request, and picture storage.  **Figure 15-2 Status Details of System Management Server**
Resource Status	View the abnormal data of different resources added to the platform in the graphical way. You can move the cursor over the chart to display the exception types and the corresponding numbers of abnormal devices, and then click a type or the number on the chart to view the real-time status details of resources.
Device Exception Statistics	View the number of abnormal devices with different types added on the platform. You can click a number under the device picture to view the real-time status details of the device. If the icon appears at the top of device picture, it indicates that the device firmware should be upgraded. For upgrading the firmware, refer to ***Upgrade Device Firmware*** .

Section	Description
Refresh Overview Page	• Manually Refresh: Click **Refresh** in the upper right corner of Real-Time Overview page to manually refresh the resource status on the page. • Auto Refresh: Go to **Maintenance → Basic Configuration → Auto-Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Auto-Check Frequency*** .
Export Overview Page or Exception Data	Click **Export** in the upper right corner of Real-Time Overview page to export the page in PDF format. Or you can check **Export Exception Data** to export the exception data in Excel/CSV format.  **Figure 15-3 Export Overview Page or Exception Data**

15.2 Set Basic Maintenance Parameters

You can set parameters to regularly send device and resource log reports to specified users via email, set the warning threshold for SYS usage, configure the default response timeout of the interactions among the Web Client, SYS, and devices, and specify the health check frequency.

15.2.1 Set Warning Threshold for Streaming Media Usage

An alarm can be triggered if the Streaming Media's CPU usage and RAM usage reaches a predefined warning threshold and lasts for a predefined duration, or if the channel usage of Streaming Media reaches a predefined warning threshold.

Select **Maintenance → Server Usage Thresholds** on the left.

CPU/RAM Usage

Drag ⌂ to adjust the threshold value of CPU or RAM usage, and then define the duration in the **Notify if Value Exceeds for (s)** field.

Example

- If you set the Warning threshold value to 60%, and set 20 in the **Notify if Value Exceeds for (s)** field for the CPU usage, you can view the CPU usage reaching to the Waring threshold line in the status window of SYS on the Health Status Overview page when the CPU usage reaches 60% and lasts for 20 seconds.
- If you set the Warning threshold value to 60%, set 20 in the **Notify if Value Exceeds for (s)** field for the CPU Usage, and set an alarm for CPU Warning, the alarm will be triggered when the CPU usage reaches 60% and lasts for 20 seconds.

Streaming Server Usage

Drag ⌂ to adjust the threshold value of bandwidth usage (in and out). When the bandwidth usage (in or out) reaches a certain threshold value, the corresponding status (normal, warning, or abnormal) will be displayed in the list on the streaming server status page.

Streaming Channels of Streaming Media

Enter a specific value in the text field or click ∧ / ∨ to adjust the threshold value for the number of input or output channels of Streaming Media.

Example

If you set the Warning threshold value to 160 for the number of input channels of Streaming Media, you can view the number of used input channels reaching to the Waring threshold line in the status window of SYS on the Health Status Overview page when the number of used input channels reaches 160.

15.2.2 Set Network Timeout

Network timeout is a certain amount of time which is used to define whether the interaction among the Web Client, SYS, and devices is successful or not. To be specific, if one party fails to response after the configured timeout passes, the interaction between them is regarded as a failure.

Select **Maintenance → Network Timeout** on the left.

Select the network timeout and click **Save**.

Table 15-2 Minimum Response Timeout in Different Interactions

Interaction Relation	Minimum Response Timeout
Between Web Client and SYS	60 s
Between SYS and Device	5 s
Between Web Client and Device	60 s

Note

This parameter affects all Web Clients accessing the current SYS.

15.2.3 Set Auto-Check Frequency

The SYS will check the health of devices, resources, and servers managed on the platform. The platform will display the health check results in the Real-Time Overview module. You can set the frequency which controls how often the platform gets the latest status of the devices, servers, and resources.

Select **Maintenance → Auto Check Frequency** .

Device Health Status

You can set the health check frequency for different devices managed on the platform. It controls how often the platform pings these devices to determine whether they are online.
After disabled, the platform will not update the status of the managed devices. You need to refresh manually to get the latest status.

Note

You should adjust the check frequency according to the number of devices. The greater the number of devices, the lower the frequency of health checks. When the frequency set is too high, you will be prompted and recommended to set a lower frequency.

Server Health Status

You can set the health check frequency for the managed recording servers. It controls how often the platform pings these servers to determine whether they are online.
After disabled, the platform will not update the status of the managed servers. You need to refresh manually to get the latest status.

Others

- **Alarm/Event Enabled or Not:** Set how often the platform checks whether the event and alarm rules are enabled or not. After disabled, the platform will not update the configured event and alarm rule status.

15.3 Resource Status

You can monitor the status of the added resources, such as access control devices and Recording Servers, which helps you find out and maintain the abnormal resources in time, ensuring the smooth running of the platform to the greatest extent.

On the top, select **System → Maintenance** .

Select a resource type to perform the following operations.

Common Operations

Operation	Description
Filter Resource Status	Check the checkbox in the top right of status display page to select exception types from the drop-down list to filter the resource status.
View Device Status	Click the device name to view the status details and basic information of the device.
Configure Device	Click in the Operation column to go to the Area page to configure the parameters of the specified device.
Filter Device	Select the device type(s) from the first drop-down list on the top to filter the device status by device type.
Export Status Data	Click **Export** to export the status data as CSV or Excel to the local PC.
Refresh Resource Status	Click in the Operation column to refresh the status of the specified resource, or click **Refresh** to refresh the status of all resources displayed on the page. **Note** The resource status will be automatically refreshed in a specified interval ().
Edit Current Value	Click in the Current Value column to edit current value of the device.

15.4 Log Search

Two types of log files are provided: server logs and device logs. The server logs refer to the logs files stored in the SYS server; The device logs refer to the log files stored on the connected devices, such as security control device;

15.4.1 Search for Server Logs

You can search for server logs, which contain error logs, warning logs and information logs. Server logs contain historical user and server activities. You can search for the logs and then check the details.

Steps

1. Select **Maintenance → Server Log** on the left.
2. In the **Event** area, select one or multiple log types and sub types.

   Note

   Error logs record failures or errors. Information logs refer to other general logs which record successful or unknown operation results.
3. In the **Source** area, set the source of the logs that you want to search for.
4. **Optional:** In the **Resource Name** area, enter the name of a resource to search the logs of the resource.
5. Set the time range for search.

   Note

   You can select **Custom** to set a precise start time and end time.
6. Click **Search**.

   All matched logs are listed with details on the right.
7. **Optional:** Check all or specific logs, click **Export**, and then select a file format (i.e., Excel or CSV) to download the searched logs as a single file to your local PC.

15.4.2 Search for Logs Stored on Device

You can search for the logs stored on access control devices.

Steps

1. Select **Maintenance → Device Log** on the left.
2. On the left, select **System Log → Device Log** .
3. Select a device type and select the device you want to search.
4. Select the event(s) you want to search.
5. Specify the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

6. Click **Search**.

   All matched logs are listed with details on the right.

7. **Optional:** Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC.

15.5 Service Manager

After successfully installing the service module(s), you can run the Service Manager and perform related operations of service, such as starting, stopping, or restarting the service.

Steps

1. Right-click and select **Run as Administrator** to run the Service Manager.

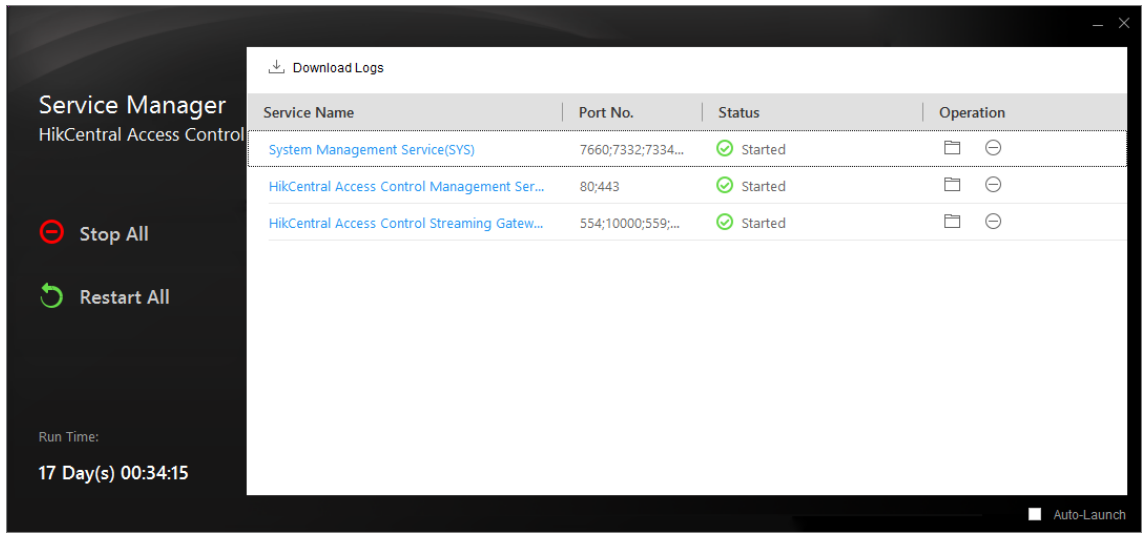


Figure 15-4 Service Manager Main Page

Note

The displayed items vary with the service modules you selected for installation.

2. **Optional:** Perform the following operation(s) after starting the Service Manager.

Stop All	Click **Stop All** to stop all the services.
Restart All	Click **Restart All** to run all the services again.
Stop Specific Service	Select one service and click to stop the service.
Edit Service	Click the service name to edit the port of the service.

Note

If the port number of the service is occupied by other service, the port No. will be shown in red. You should change the port number to other value before the service can work properly.

Open Service Location Select one service and click to go to the installation directory of the service.

3. **Optional:** Click **Auto Recover Database Exception** to recover database exception caused by accidents such as power-off and unexpected reboot.
   1) Enable **Auto Recover Database Exception**.

   Note

   The database service will restart after you enable this function.

   2) Click to set the archive path for recovering the database.

   Note

   - The remaining disk space of the archive path should be twice as the size of database data.
   - The archive path should be under a path in English.

   3) Click **OK** to finish setting.
4. **Optional:** Check **Auto-Launch** to enable launching the Service Manager automatically after the PC started up.
5. Click **Dual-Server Deployment** to deploy the database on another server.

15.6 Set System Data Backup

To restore the original system data after a data loss event or recovering data from an earlier time, you can manually back up system data, or configure a schedule to back up regularly. System data includes data configured in the system, pictures, received events and alarms, card swiping data, and maintenance data.

Steps

Note

The backups are stored in the SYS server. You can edit the saving path only on the Web Client running on the SYS server.

1. In the top right of the Home Page, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Back Up** tab.
3. In **Type**, select the data that you want to back up.
4. Set a backup schedule to run backup regularly.
   1) In **How Often**, select the frequency to back up the system data.

2) In **Which Day** and **When**, specify which time to back up.
3) In **Max. Number of Backups**, set the maximum number of backup files. Old backup files will be automatically deleted.

Note

The value ranges from 1 to 5.

5. Save the settings.
   - Click **Save** to save the backup schedule.
   - Click **Save and Back Up Now** to back up the system data immediately, and you can monitor the backup progress in the progress bar window.

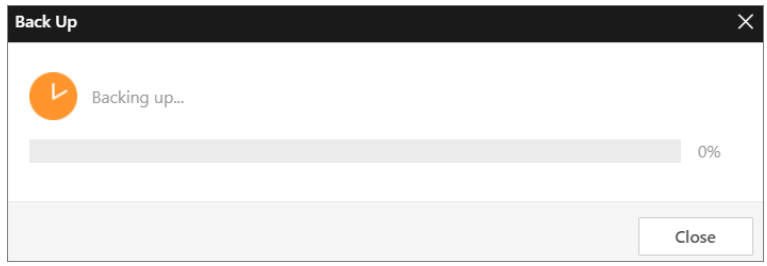


Figure 15-5 Backup Progress

15.7 Restore System Data

When an exception occurs, you can restore the system data if you have backed up system data before.

Before You Start

Make sure you have backed up system data. Refer to ***Set System Data Backup*** for details.

Steps

Note

System data recovery will restore the system to an earlier state, and thus the data added after backup date will be lost.

1. In the top right of the Home Page, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Restore** tab.
3. Select a backup file to be restored.

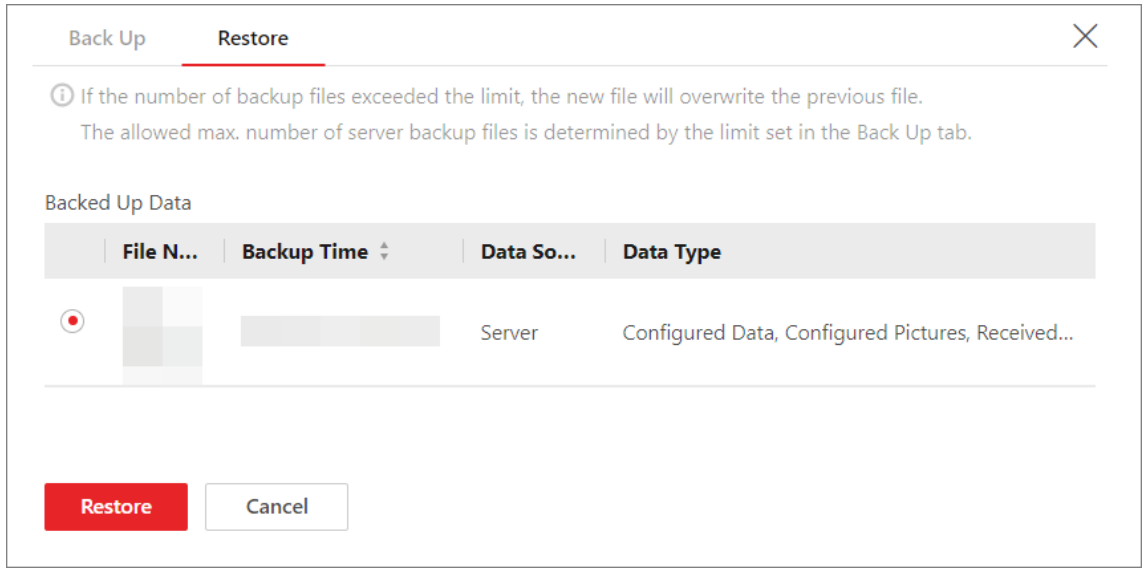


Figure 15-6 Restore System Data

4. Click **Restore** to confirm the system data recovery.

What to do next

After restoring the system data, you must reboot the SYS service via Service Manager and log in to Web Client again.

15.8 Export Configuration Data

You can export and save configuration data to local disk, including recording settings and resource configurations.

Steps

1. On the top navigation bar, click **Maintenance and Management → Export Configuration Data** .
2. Select the configuration data types that you want to export.
3. Click **Export** to download the data to the local PC.

Note

The configuration data file is in CSV format.

15.9 Import Configuration Files

If you have used applications on the iVMS-4200, you can get configuration files (including configurations of devices, persons, events, and access levels) of these applications and import

them to the system via the Web Client for quickly configuring the corresponding applications on the system.

Steps

1. In the top right of the Web Client, click **Maintenance and Management → Data Migration** .

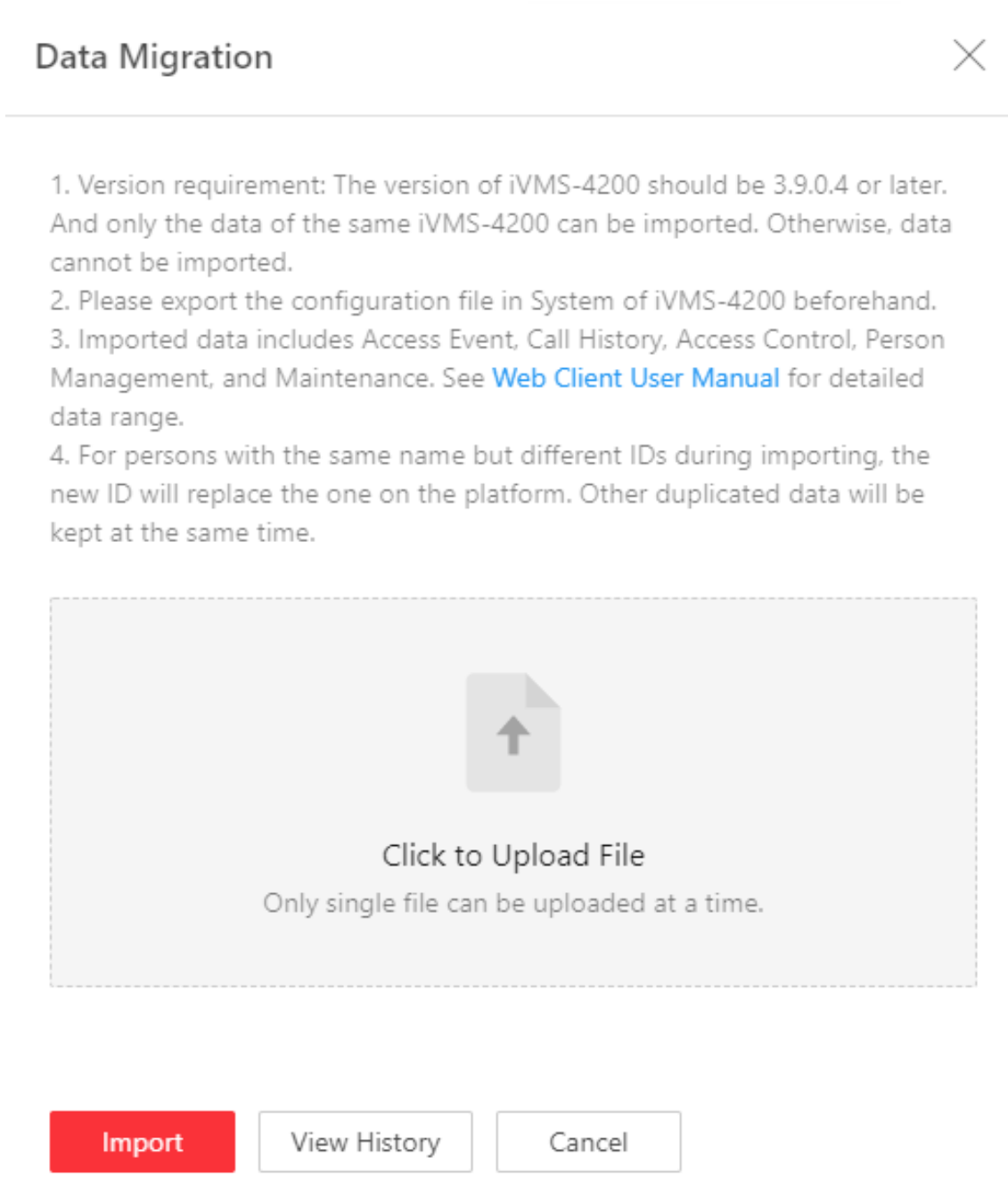


Figure 15-7 Data Migration

2. Click to select the configuration file(s) of iVMS-4200 from the local PC.
   - The data that can be imported include the followings.
     - Device: The information about access control devices, video intercom devices. The related area and channel resources will be added automatically according to devices.
     - Person: The basic information and credential information (i.e., card, fingerprint, face, and iris).
     - Event: Event types that are both supported by iVMS-4200 / iVMS-4200 AC Client Software and HikCentral Access Control.
     - Access Level: The settings of access levels, holidays, and schedule templates.
   - When importing device configurations, if the number of resources exceeds the limit, the excess resources cannot be imported.
3. Click **Import** to start importing the configuration file(s) to the platform.

Note

During the import, you can close the details window and normally use the platform.

A progress bar will pop up and display the import progress, import result, and error information (if failed).


See Far, Go Further