HikCentral Access Control Web Client

User Manual

Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Contents

Chapter 1 How to Customize My Manual 1

Chapter 2 About This Document 4

2.1 Introduction 4

2.2 Recommended Running Environment 5

2.3 Symbol Conventions 5

Chapter 3 Login 6

3.1 First Time Login 6

3.1.1 Login for First Time for Admin User 6

3.1.2 First Time Login for Normal User 7

3.2 Login via Web Client (Administrator) 8

3.3 Login via Web Client (Employee) 9

3.4 Change Password for Reset User 10

3.5 Forgot Password 11

Chapter 4 Download Mobile Client 14

Chapter 5 Web Control 15

Chapter 6 Home Page Overview 16

Chapter 7 Getting Started 20

Chapter 8 License Management 21

8.1 Activate License - Online 21

8.2 Activate License - Offline 22

8.3 Update License - Online 24

8.4 Update License - Offline 24

8.5 Deactivate License - Online 26

8.6 Deactivate License - Offline 27

8.7 View License Details 28

8.8 Set SSP Expiration Prompt 29

Chapter 9 Role and User Management 31
9.1 Add Role 31
9.2 Add Normal User 34
9.3 Import Domain Users 36
9.4 Change Password of Current User 38
9.5 Configure Permission Schedule 39
Chapter 10 Application Summary 41
10.1 Flow Chart of Door Access Control 42
10.2 Flow Chart of Floor Access Control 44
10.3 Flow Chart of Time and Attendance 46
10.4 Flow Chart of Video Intercom 47
Chapter 11 Resource Management 49
11.1 Create Password for Inactive Device(s) 49
11.2 Edit Online Device's Network Information 50
11.3 Manage Access Control Device 51
11.3.1 Add Detected Online Access Control Devices 51
11.3.2 Add an Access Control Device by IP Address/Domain 57
11.3.3 Add Access Control Devices by IP Segment 59
11.3.4 Add an Access Control Device by Device ID 61
11.3.5 Add Access Control Devices by Device ID Segment 63
11.3.6 Add Access Control Devices in a Batch 66
11.3.7 Configure Device Parameters 68
11.3.8 Privacy Settings 82
11.4 Manage Elevator Control Device 83
11.4.1 Add Detected Online Elevator Control Devices 83
11.4.2 Add an Elevator Control Device by IP Address 88
11.4.3 Add Elevator Control Devices by IP Segment 90
11.4.4 Add Elevator Control Devices in a Batch 92

11.5 Manage Video Intercom Device 93
11.5.1 Add a Detected Online Video Intercom Device 94
11.5.2 Add a Video Intercom Device by IP Address 97
11.5.3 Add Video Intercom Devices in a Batch 100
11.6 Network Transmission Device Management 101
11.6.1 Add Detected Online Network Transmission Devices 102
11.6.2 Add Network Transmission Device by IP Address 106
11.6.3 Import Network Transmission Devices in a Batch 108
11.7 Add pStor 109
11.8 Upgrade Device Firmware 110
11.8.1 Upgrade Device Firmware via Current Web Client 111
11.8.2 Upgrade Device Firmware via Hik-Connect 112
11.8.3 Upgrade Device Firmware via FTP 112
11.9 Restore/Reset Device Password 114
11.9.1 Reset Device Password 114
11.9.2 Restore Device's Default Password 116
Chapter 12 Area Management 118
12.1 Add an Area 118
12.2 Add Element to Area 119
12.2.1 Add Door to Area 119
12.2.2 Add Elevator to Area 120
12.2.3 Add Alarm Input to Area 121
12.2.4 Add Alarm Output to Area 122
12.3 Edit Element in Area 123
12.3.1 Edit Door 124
12.3.2 Edit Elevator 126
12.3.3 Edit Alarm Input 128
12.3.4 Edit Alarm Output 128

12.4 Remove Element from Area 128
Chapter 13 Person Management 130
13.1 Add Departments 130
13.2 Add Person 131
13.2.1 Add a Person Manually 132
13.2.2 Batch Add Persons by Template 140
13.2.3 Import Domain Persons 143
13.2.4 Import Profile Pictures 146
13.2.5 Import Persons from Access Control Devices or Video Intercom Devices 147
13.2.6 Import Persons from Enrollment Station 151
13.3 Person Self-Registration 154
13.3.1 Set Self-Registration Parameters 155
13.3.2 Scan QR Code for Self-Registration 156
13.3.3 Review Self-Registered Person Information 157
13.4 Person Information Export 158
13.4.1 Export Person Information 158
13.4.2 Export Profile Pictures 158
13.5 Set Person ID Rule 158
13.6 Customize Additional Information 159
13.7 Batch Issue Cards to Persons 161
13.7.1 Set Card Issuing Parameters 162
13.8 Print Cards 164
13.9 Report Card Loss 165
13.9.1 Report Card Loss 165
13.9.2 Issue a Temporary Card to a Person 166
13.9.3 Batch Cancel Card Loss 167
13.10 Set Authentication via PIN Code 167
13.11 Manage Resigned Persons 168

13.11.1 Add Resigned Persons 168
13.11.2 Reinstate Persons 170
13.11.3 Manage Resignation Types 170
Chapter 14 Access Control Management 171
14.1 Manage Access Level 171
14.1.1 Add Access Level 171
14.1.2 Assign Access Level 172
14.1.3 Apply Persons' Access Levels to Device 176
14.1.4 Clear Persons' Access Levels 178
14.1.5 Set Access Schedule Template 179
14.1.6 Enable Authentication via Password 180
14.2 Access Control Test 180
14.3 Advanced Functions 183
14.3.1 Configure Free Access and Access Forbidden Rules 183
14.3.2 Configure First Person In Rule 184
14.3.3 Manage Multi-Factor Authentication 186
14.3.4 Configure Multi-Door Interlocking 189
14.3.5 Configure Anti-Passback Rules 189
14.3.6 Add Emergency Operation Group 192
14.3.7 Add Entry and Exit Counting Group 193
14.3.8 Configure Authentication Mode 193
14.3.9 Apply Advertisement to Access Control Devices 195
14.3.10 Add Audio Broadcast 197
14.3.11 Set Card Authentication Parameters 198
14.4 Door and Elevator Control 198
14.4.1 Start Live View of Access Control / Elevator Control Devices 199
14.4.2 Door Control 200
14.4.3 Elevator Control 201

14.4.4 View Real-Time Access Event 202
14.5 Subscribe to Device and Access Events 203
14.6 Synchronize Access Records to System Regularly 203
14.7 Enable Open Door via Bluetooth 203
14.8 Search Access Records 204
14.9 Search Data Recorded on Access Control Devices and Elevator Control Devices 207
14.10 Perform Entry & Exit Counting 208
Chapter 15 Time & Attendance 210
15.1 Basic Configuration 211
15.1.1 Specify Attendance Check Points 211
15.1.2 Add a Pay Code 214
15.1.3 Edit a Fixed Code 216
15.1.4 Configure Storage Settings 217
15.2 Configure Global/Department Attendance Rules 217
15.2.1 Define Weekends 217
15.2.2 Configure Overtime Parameters 218
15.2.3 Configure Attendance Calculation Mode 220
15.2.4 Define Absence 221
15.2.5 Add Holidays Requiring Attendance 222
15.2.6 Calculation of Leaves 223
15.2.7 Configure Authentication Mode 224
15.3 Add Timetable 224
15.3.1 Add Break Timetables 224
15.3.2 Add Timetable for Normal Shift 226
15.3.3 Add Timetable for Flexible Shift 229
15.4 Add Shift 231
15.5 Manage Schedule 232
15.5.1 Schedule Overview 232

15.5.2 Assign Schedule to Department 233
15.5.3 Assign Schedule to Person 234
15.5.4 Add Temporary Schedule 235
15.6 Configure Calculation Mode of Attendance Results 236
15.6.1 Manually Calculate Attendance Results 237
15.6.2 Set Auto-Calculation Time of Attendance Results 237
15.7 Application Flow Management 237
15.7.1 Add a Approval Role of Application Flow 238
15.7.2 Add a Department Application Flow 239
15.7.3 Add a Personal Application Flow 240
15.8 Application Management for Employee 242
15.8.1 Overview of Personal Attendance Data 242
15.8.2 Submit and View Applications 243
15.8.3 Review Employees' Applications 246
15.8.4 View and Export Attendance Records and Reports 246
15.9 Application Management for Admin 247
15.9.1 Apply for a Leave 247
15.9.2 Apply for a Check-In/Out Correction 248
15.9.3 Apply for Overtime 248
15.9.4 Import Applications 249
15.9.5 Review or Undo Applications 249
15.10 View Attendance Records 250
15.10.1 Import Transactions 251
15.11 Manage Attendance Reports 252
15.11.1 Set Display Rules for Attendance Report 252
15.11.2 View Daily/Weekly/Monthly/Summary Attendance Reports 252
15.11.3 Send Attendance Report Regularly 253
15.11.4 Add a Custom Report 255

Chapter 16 Video Intercom Management 256
16.1 Basic Settings of the Platform 256
16.1.1 Add Call Recipients 256
16.1.2 Add Call Schedule Template 257
16.1.3 Configure General Parameters 257
16.2 Configure Device Parameters 258
16.3 Manage Video Intercom Device 259
16.3.1 Set Locations for Video Intercom Devices 260
16.3.2 Apply Location to Video Intercom Devices 261
16.4 Video Intercom Application 261
16.4.1 Start Live View of Video Intercom Devices 262
16.4.2 Add Call Schedule for Door Stations 262
16.4.3 Apply Call Schedule to Door Stations 263
16.4.4 Link Resources with Indoor Stations 263
16.4.5 View Event/Alarm Related Notices 265
16.4.6 Apply Data to Indoor Station 266
16.4.7 Apply Advertisements to Door Stations 269
16.4.8 Search Data Recorded on Video Intercom Devices 270
16.5 Call & Talk 272
16.5.1 Call an Indoor Stations 272
16.5.2 View Recents 272
Chapter 17 Skin-Surface Temperature Screening 273
17.1 Temperature Screening Configuration 273
17.1.1 Group Temperature Screening Points 273
17.1.2 Configure Temperature Screening Parameters 274
17.2 Real-Time Skin-Surface Temperature Monitoring 274
17.3 Search History Temperature Screening Data 276
17.4 Registration 276

17.4.1 Register Person Information 277
17.4.2 Customize Registration Template 278
17.4.3 View Registered Person Information 278
17.5 Search for Temperature Screening Records 279
Chapter 18 Map Management 281
18.1 Set Icons for Elements on the Map 281
18.2 Add E-Map for Area 282
18.3 Add Hot Spot on Map 283
18.4 Add Hot Region on Map 283
18.5 Add Label on Map 284
18.6 Add Resource Group on Map 285
18.7 Add Combined Alarm on Map 286
18.8 Operate Hot Spot 286
18.8.1 Preview Hot Spot 287
18.8.2 Arm or Disarm Hot Spot 288
18.8.3 View History Alarm 288
18.9 Preview Hot Region 289
18.10 Preview Resource Group 289
18.11 Operate Map 290
Chapter 19 Emergency Mustering 291
19.1 Emergency Solution Settings 291
19.2 Start a Roll Call 293
Chapter 20 System Configuration 296
20.1 Set User Preference 296
20.2 Set Holiday 297
20.3 Set Printer 298
20.4 Set Card Template 299
20.5 Set NTP 300

20.6 Set Active Directory 301
20.7 Device Access Protocol 303
20.8 Set WAN Access 303
20.9 Set IP Address for Receiving Device Information 305
20.10 Configure Storage for Imported Pictures and Files 305
20.11 Set Records Storage Information 306
20.12 Set Email Template 307
20.12.1 Configure Email Account 308
20.12.2 Add Email Template for Sending Report Regularly 309
20.12.3 Add Email Template for Event and Alarm Linkage 311
20.13 Set Transfer Protocol 313
20.14 Set Database Password 314
20.15 Set Third-Party Integration 314
20.16 Data Interchange 315
20.16.1 Synchronize Card Swiping Records to Third-Party Database 315
20.16.2 Dump Access Records to Third-Party Database 316
20.17 Diagnose Remote Fault 318
20.18 View Event Tracking Information 319
20.19 Reset Device Network Information 319
20.20 Set Company Information 320
Chapter 21 System Security Settings 321
Chapter 22 Event and Alarm 323
22.1 Manage Event and Alarm 324
22.1.1 Supported Events and Alarms 324
22.1.2 Define Alarm Priority, Alarm Category, and Alarm Icon 325
22.1.3 Add Normal Event and Alarm 327
22.1.4 Add Combined Alarm 333
22.2 Add Generic Event 337

22.3 Add User-Defined Event 340
22.4 Configure Receiving Schedule Template 341
22.5 View Pop-Up Window Triggered by Alarm 342
22.6 Event and Alarm Search 344
22.6.1 Event and Alarm Overview 344
22.6.2 Search for Event and Alarm Logs 345
22.7 Send Event and Alarm Report Regularly 346
Chapter 23 Maintenance 349
23.1 Health Monitoring 349
23.1.1 Real-Time Health Status Overview 349
23.1.2 Real-Time Health Status Overview (Topology) 351
23.2 Set Basic Maintenance Parameters 357
23.2.1 Set Warning Threshold for Streaming Media Usage 358
23.2.2 Set Network Timeout 359
23.2.3 Set Health Check Frequency 359
23.2.4 Set Topology Show Parameters 360
23.3 Resource Status 361
23.3.1 Door Status 361
23.3.2 Floor Status 362
23.3.3 Alarm Input Status 362
23.3.4 Recording Server Status 363
23.3.5 Access Control Device Status 363
23.3.6 Elevator Control Device Status 363
23.3.7 Video Intercom Device Status 364
23.3.8 Network Transmission Device 364
23.4 Log Search 365
23.4.1 Search for Server Logs 365
23.4.2 Search for Logs Stored on Device 365

23.5 Service Manager 366
23.6 Set System Data Backup 367
23.7 Restore System Data 368
23.8 Export Configuration File 369

Chapter 1 How to Customize My Manual

This document provides the content customization function to help you quickly get the information that you need. On the Customize User Manual pane, you can select or check option(s) to filter contents and customize your own manual by different categories, including the product model, function, application, and scene.

Note

- This function is only available when you view the online documentation. If you have downloaded the PDF documentation for viewing, please ignore this chapter.
- Options and contents in videos and pictures below are for examples only, please subject to the actual information.

Customize Manual by Product Model

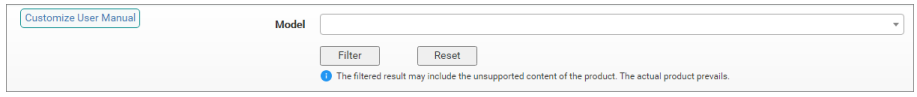


Figure 1-1 Customize User Manual Pane (by Product Model)

On the Customize User Manual pane, click the input field of the Model category to unfold the drop-down list, select a model from the list, and then click **Filter**. The result is shown below.

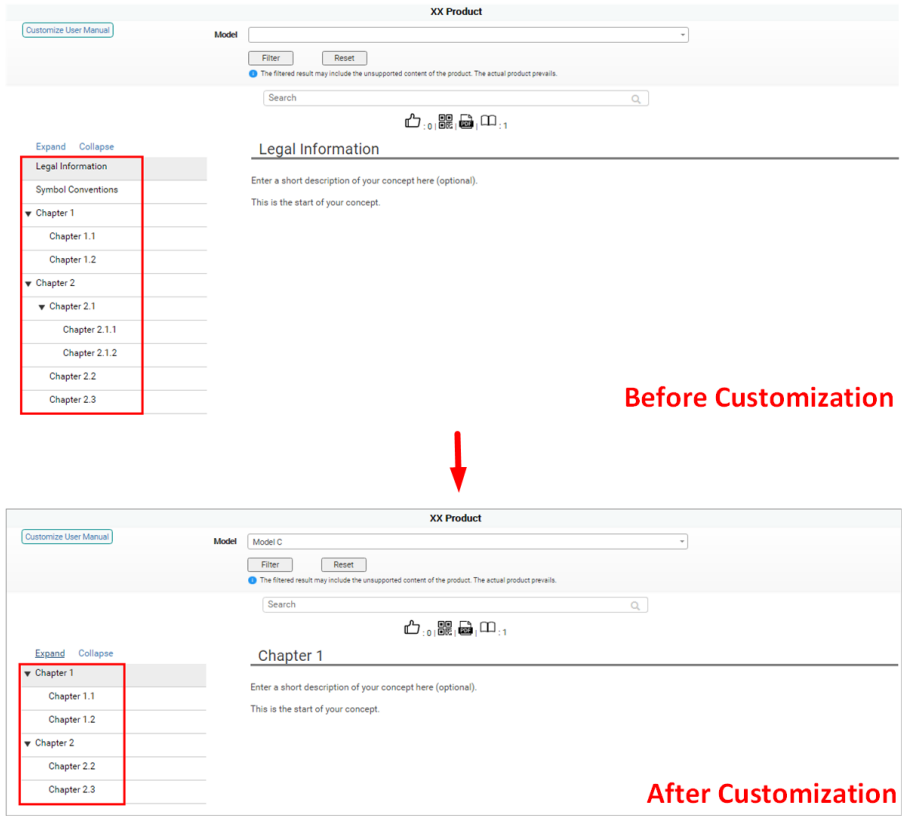


Figure 1-2 Result of Customizing Manual by Product Model

You can view the video below to get more details about the customization process.

Customize Manual by Application

Note

Due to the similarity among processes of customizing by Function, Application, and Scene categories, here we only take the process of customizing by application as an example.

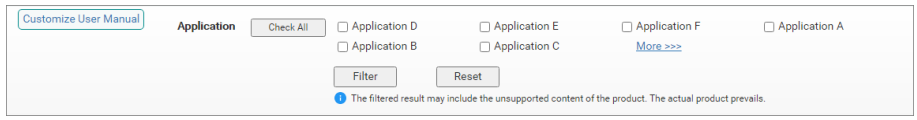


Figure 1-3 Customize User Manual Pane (by Application)

On the Customize User Manual pane, check one or multiple options under the Application category, and then click **Filter**. The result is shown below.

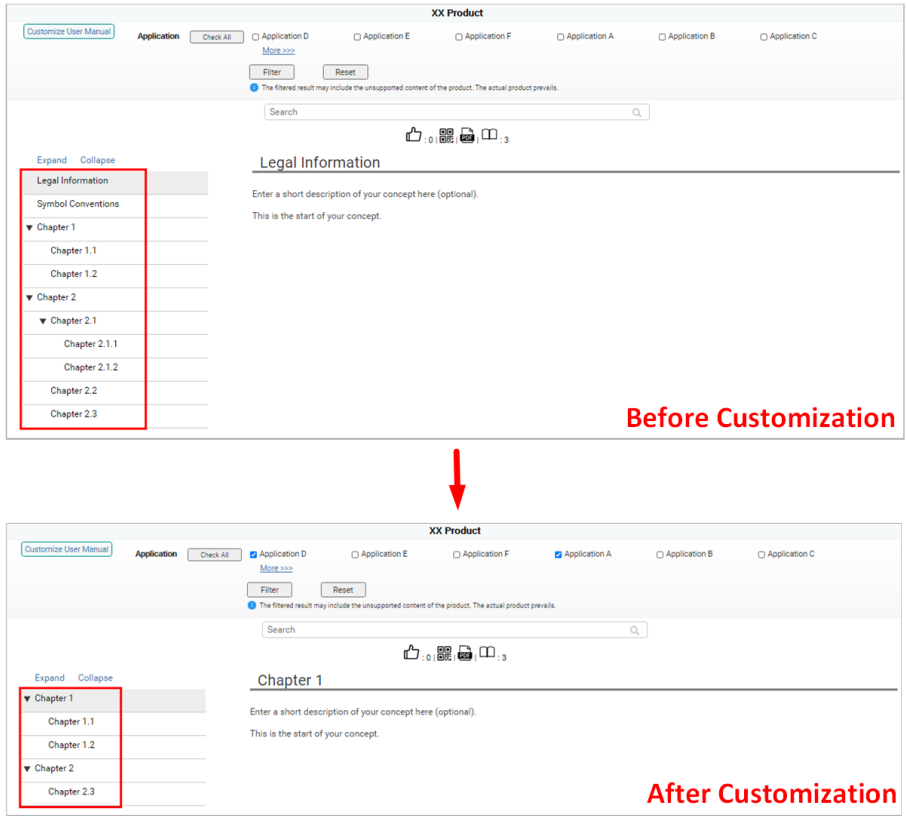


Figure 1-4 Result of Customizing Manual by Application

You can view the video below to get more details about the customization process.

Chapter 2 About This Document

This user manual is intended for the administrator of the system.

The manual guides you to establish and configure the security system. Follow this manual to perform system activation, access of the system, and configuration of the monitoring task via the provided Web Client, etc. To ensure the properness of usage and stability of the system, refer to the contents below and read the manual carefully before installation and operation.

2.1 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.

Note

The modules on the platform vary with the License you purchased. For detailed information, contact our technical support.

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.
Streaming Service (Optional)	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, recording schedule settings, 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.

2.2 Recommended Running Environment

The following is recommended system requirement for running the Web Client.

CPU

Intel® Core™ I3 and above

Memory

4 GB and above

Web Browser

Internet Explorer® 11 and above, Firefox® 90 and above, Google Chrome® 90 and above, Safari® 11 and above, Microsoft® Edge 89 and above.

Note

Upgrading from V1.x to V2.x requires double available disk spaces than usual.

2.3 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.

Chapter 3 Login

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

Note

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 ***System Security Settings*** .

3.1 First Time Login

If this is the first time for you to login, you can choose to login as admin or normal user according to your user role.

3.1.1 Login for First Time for Admin User

By default, the system predefined the administrator user named admin. When you login via the Web Client for the first time, you are required to create a password for the admin user before you can properly configure and operate the system.

Steps

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

   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.

   Note

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

2. Enter the password and confirm password for the admin user in the pop-up Create Password window.

Note

The password strength can be checked by the system and should meet the system requirements. The default minimum password strength should be **Medium**. For setting minimum password strength, refer to ***System Security Settings*** .

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 installer and/or end-user.

3. Click **OK**.

Web Client home page displays after you successfully creating the admin password.

3.1.2 First Time Login for Normal User

When you log in to the system as normal user via Web Client for the first time, you should change the initial password and set a new password for login.

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 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.

Note

You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.

Note

Contact the administrator for the user name and initial password.

3. Click **Log In** and the **Change Password** window opens.

4. Set a new password and confirm the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***System Security Settings*** .

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.

5. Click **OK** to change the password.

Result

Web Client home page displays after you successfully logging in.

3.2 Login via Web Client (Administrator)

You can access the system via web browser and configure the system.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press **Enter** key.

   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.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Select the **Management** tab.
3. Enter the user name and password.
4. Click **Log In** to log in to the system.

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. For setting failed login attempts and locking duration, refer to ***System Security Settings*** .
- 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.
- The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***System Security Settings*** .
- If your password is expired, you will be asked to change your password when login. For setting maximum password age, refer to ***System Security Settings*** .

Result

Web Client home page displays after you successfully logging in to the system.

3.3 Login via Web Client (Employee)

Employees can access the system via web browser.

Before You Start

The administrator should enable self-service login (enabled by default) and set the login password (employee ID by default) for employees.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press **Enter** key.

   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.

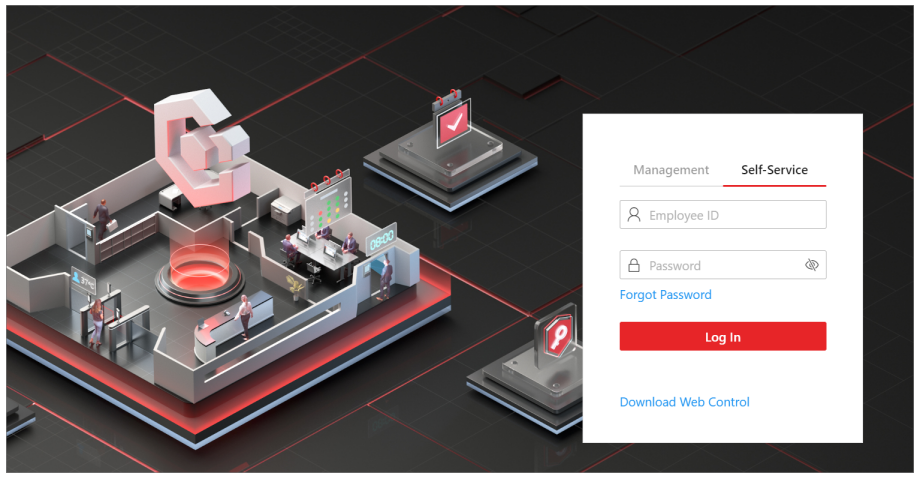


Figure 3-1 Login Page

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 upon the first login.
- If employees forget the password, they can reset new password in **Forgot Password**.
- If the password is expired, employees will be asked to change the password upon login. For setting maximum password age, refer to ***System Security Settings*** .

Result

Web Client home page displays after employees successfully log in to the system.

3.4 Change Password for Reset User

When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Access Control via the Web Client.

Steps

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

   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.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and initial password set by the administrator.
3. Click **Log In** and a **Change Password** window opens.
4. Set a new password and confirm the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***System Security Settings*** .

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.

5. Click **OK**.

Result

Web Client home page displays after you successfully changing the password.

3.5 Forgot Password

If you forgot the your account's password, you can reset the password and set a new 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, enter a user name in the User Name field.
2. Click **Forgot Password**.

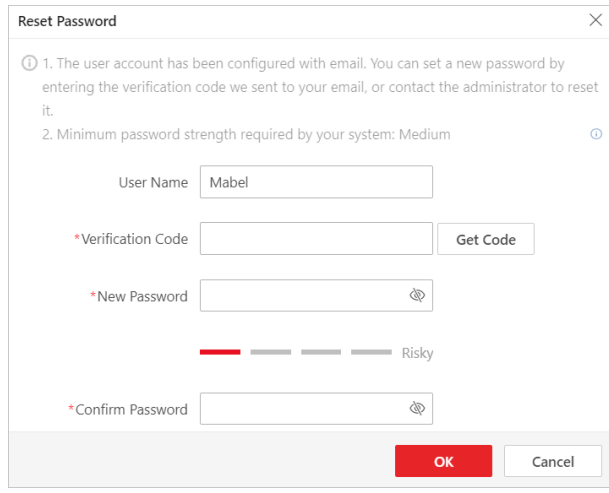


Figure 3-2 Reset Password for Normal User

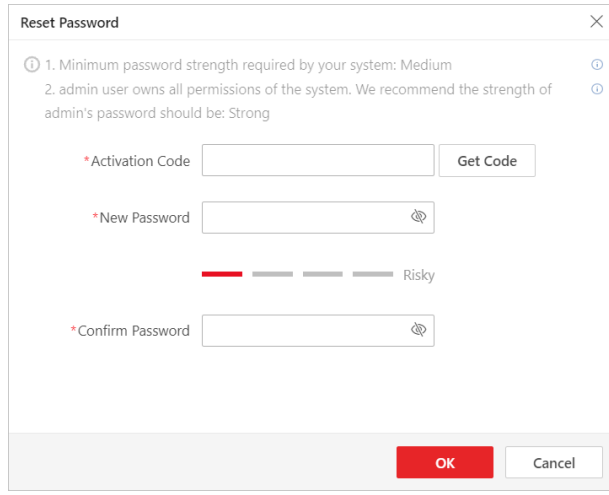


Figure 3-3 Reset Password for admin User

3. Enter the required information on the Reset Password pane.

- For the admin user, enter the License activation code, new password, and confirm password.

  Note

  If you forget the License activation code, you can click **Get Code** to send the activation code to the email address configured when activating the License in online mode. For setting an email for the admin user, refer to ***Activate License - Online*** .

- For normal users, click **Get Code** to send the verification code to the email address configured when adding the user. And then enter the received verification code, new password, and confirm password within 10 minutes.

  Note

  If the email address is not set for the normal user, contact the admin user to reset the password and change the password when login.

- For domain user, contact the admin user to reset the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***System Security Settings*** .

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 installer and/or end-user.

4. Click **OK**.

Chapter 4 Download Mobile Client

On the login page of Web Client, you can scan the QR code to download the Mobile Client that is used for accessing the system via mobile terminal (e.g., mobile phone).

Perform this task when you need to download the Mobile Client.

Note

You can also search and download the Mobile Client in the App Store.

Steps

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

   Example

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

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Scan the corresponding QR code with your mobile terminal to download the Mobile Client.

Chapter 5 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.

Chapter 6 Home Page Overview

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

Top Navigation Bar

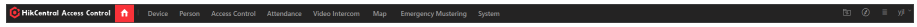


Figure 6-1 Top Navigation Bar of the Web Client

Home Page Icon

Click to enter the Home Page.

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

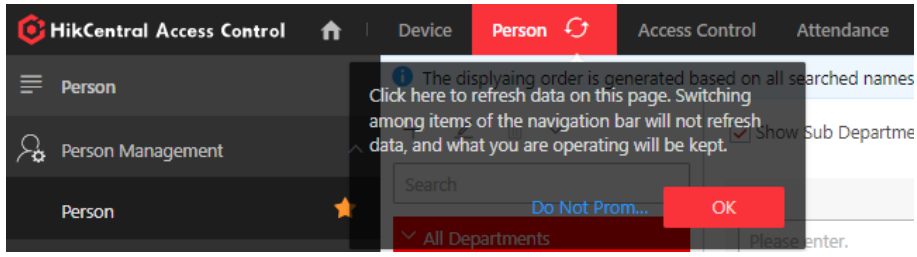


Figure 6-2 Refresh Module on Navigation Bar

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)

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 and elevator 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

License Details

You can view the License details, activate, upgrade, and deactivate the License if needed.

For more details, refer to ***License 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 File*** .

About

Check the version information of the Web Client.

View the License Agreement and Open-Source License Agreement.

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 of Home Page, you can click **Expand Quick Configuration** to enter the management and configurations of Access Control or Attendance.
Click **Fold Quick Configuration** or **Expand Quick Configuration** to fold or expand the window of quick configuration entry.

Quick Start

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

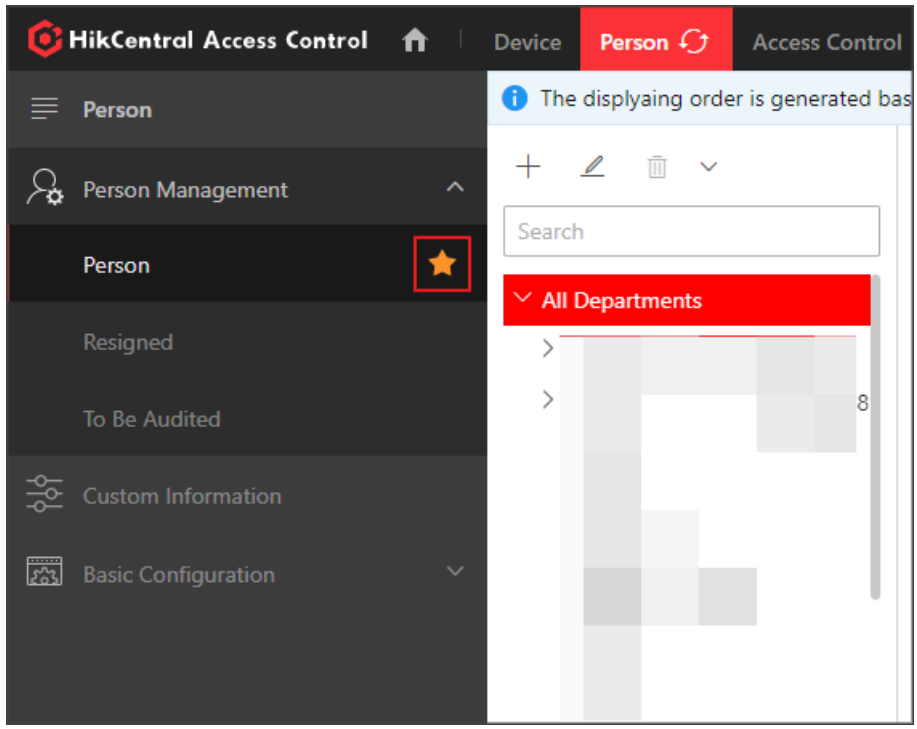


Figure 6-3 Add Menu Item to Favorites for Quick Start

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

Pending Task

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

Alarm / Access Control Event

This section displays alarms and access control events

- Select **Alarm** tab on the lower-right corner. Click › to view the alarm details, you can also acknowledge or unlock the alarm.
- Select **Access Control Event** tab. You can click **Mark All As Read** to mark all messages as read.
- You can click **View All** to view more alarms or events.

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.

Device Status

This section displays the device status, including the numbers of normal or exceptions devices, including total devices, access control device, elevator 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.

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.

Chapter 7 Getting Started

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

Verify Initial Configuration of Devices and Other Servers

Before doing anything on the platform, make sure the devices (encoding devices, access control devices, recording server, and so on) you are going to use are correctly mounted and connected to the network as specified by the manufacturers. Such initial configurations are required in order to connect the devices to the platform via network.

Log In to Web Client

Refer to ***Login for First Time for Admin User*** .

Activate License

Refer to ***Activate License - Online*** or ***Activate License - Offline*** .

Add Devices to Platform and Configure Area

The platform can quickly scan your network for relevant devices, and add them. Or you can add the devices by inputting the required information manually. The devices added should be organized into areas for convenient management. Refer to ***Resource Management*** and ***Area Management*** .

Configure Event and Alarm

The camera exception, device exception, server exception, alarm input, and so on, can trigger linkage actions in the platform. Refer to ***Event and Alarm*** .

Configure Users

Specify who should be able to access the platform, and how. You can set different permissions for the users to limit their operations. Refer to ***Role and User Management*** .

View How-to Videos

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.

Chapter 8 License Management

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

Two types of License are available for HikCentral Access Control:

- **Base:** You need to purchase at least one basic License to activate the HikCentral Access Control.
- **Expansion:** If you want to increase the capability of your system, you can purchase an expanded License to get additional features.

Note

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

8.1 Activate License - Online

If the SYS server to be activated can properly connect to the Internet, you can activate the SYS server in online mode.

Steps

1. Log in to HikCentral Access Control via the Web Client. Refer to ***Login via Web Client (Administrator)*** .
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Online Activation** to activate the License in online mode.
4. Enter the activation code received when you purchased your License.

   Note

   - If you have purchased more than one Licenses, you can click + and enter other activation codes.
   - The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. Click **Activate**.

   The email settings pane will appear after you activated the License.
7. Enter an email address for the admin user.

   Note

   This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.

8. Set the email server parameters. See details in ***Configure Email Account*** .
9. Click **OK** to save the email settings.

8.2 Activate License - Offline

If the SYS to be activated cannot connect to the Internet, you can activate the License in offline mode.

Steps
1. Log in to HikCentral Access Control via the Web Client.
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Offline Activation** to activate the License in offline mode.

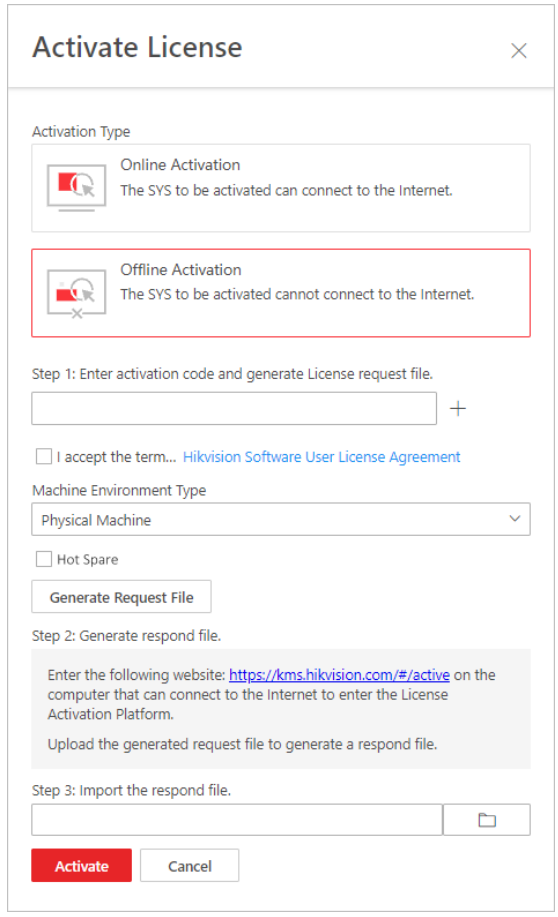


Figure 8-1 Activate License in Offline Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
7. Copy the request file to the computer that can connect to the Internet.
8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
9. Click and then select the downloaded request file.

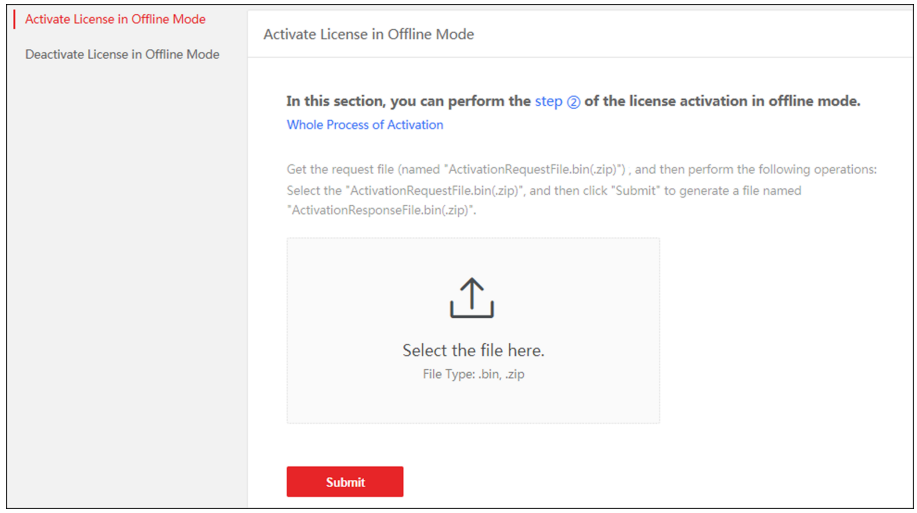


Figure 8-2 Select Request File

10. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral Access Control via the Web Client.
12. In the Offline Activation panel, click and select the downloaded respond file.
13. Click **Activate**.

    The email settings pane will appear after you activated the License.
14. Enter an email address for the admin user.

    Note

    This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.
15. Set the email server parameters. See details in ***Configure Email Account*** .
16. Click **OK** to save the email settings.

8.3 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., devices) for your HikCentral Access Control. If the SYS to be updated can properly connect to the Internet, you can update the License in online mode.

Before You Start
Contact your dealer or our sales team to purchase a License for additional features.

Steps
1. Log in to HikCentral Access Control via the Web Client. Refer to ***Login via Web Client (Administrator)*** for details.
2. On the top, move the cursor to ≡ **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Online Update** to update the License in online mode.
5. Enter the activation code received when you purchase your License.

Note
- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Update**.

8.4 Update License - Offline

As your project grows, you may need to increase the connectable number of devices for your HikCentral Access Control. If the SYS to be updated cannot connect to the Internet, you can update the system in offline mode.

Before You Start
Contact your dealer or our sales team to purchase a License for additional features.

Steps
1. Log in to HikCentral Access Control via the Web Client.
2. On the top, move the cursor to ≡ **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Offline Update** to update the License in the offline mode.

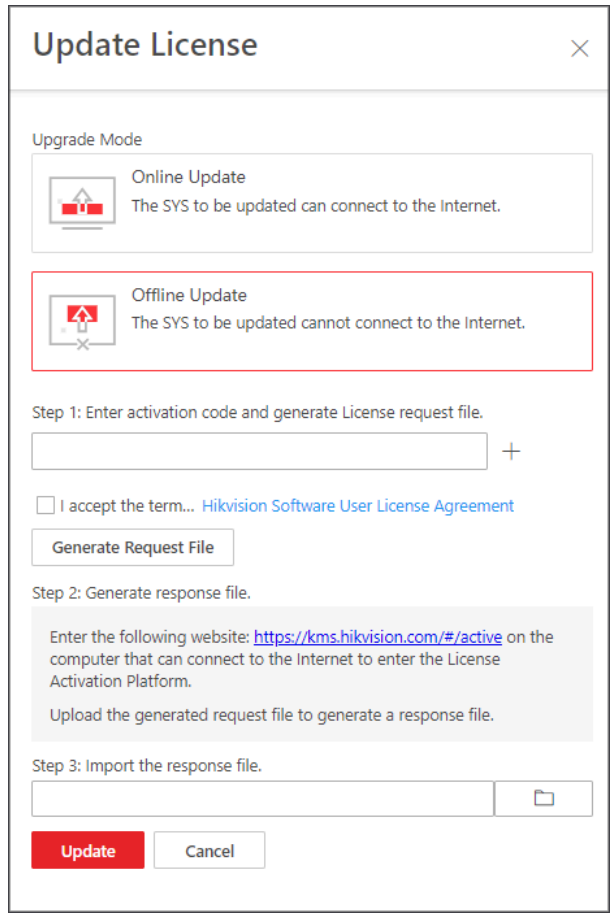


Figure 8-3 Update License in Offline Mode

5. Enter the activation code of your additional License.

Note

- If you have purchased more than one License, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.

7. Click **Generate Request File**.

A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

8. Copy the request file to the computer that can connect to the Internet.

9. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .

10. Click ↑ and then select the downloaded request file.

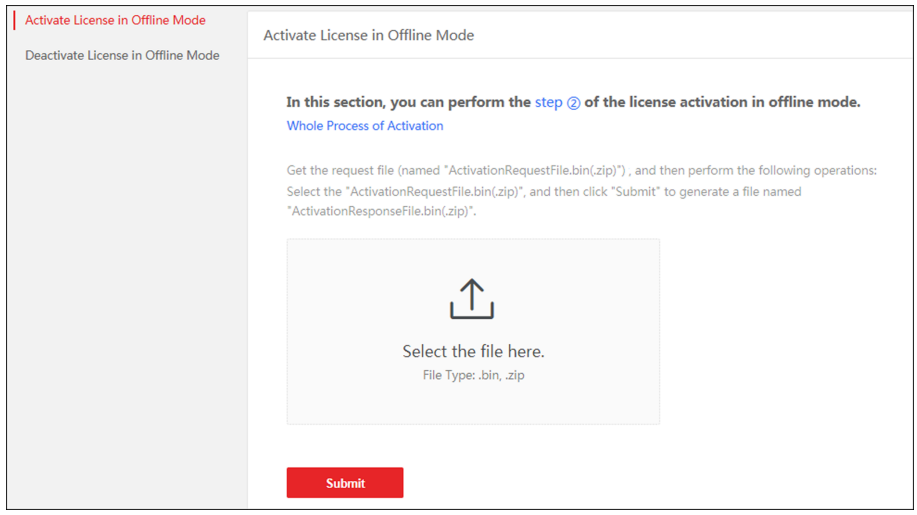


Figure 8-4 Select Request File

11. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
12. Copy the respond file to the proper directory of the computer that accesses HikCentral Access Control via the Web Client.
13. In the offline update panel, click 🗀 and select the downloaded respond file.
14. Click **Update**.

8.5 Deactivate License - Online

If you want to run the SYS on another PC or server, you should deactivate the SYS first and then activate it again. If the computer or server on which the SYSrunning can properly connect to the Internet, you can deactivate the License in online mode.

Steps

1. Log in to HikCentral Access Control via the Web Client. Refer to ***Login via Web Client (Administrator)*** .
2. On the top, move the cursor to ☰ **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License panel.
4. Click **Online Deactivation** to deactivate the License in online mode.
5. Check the activation code(s) to be deactivated.
6. Click **Deactivate**.

8.6 Deactivate License - Offline

If you want to run the SYS on another computer or server, you should deactivate the SYS first and then activate the SYS again. If the SYS to be deactivated cannot connect to the Internet, you can deactivate the License in offline mode.

Steps

1. Log in to the HikCentral Access Control via Web Client.
2. On the top, move the cursor to ☰ **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License pane.
4. Click **Offline Deactivation** to deactivate the License in offline mode.

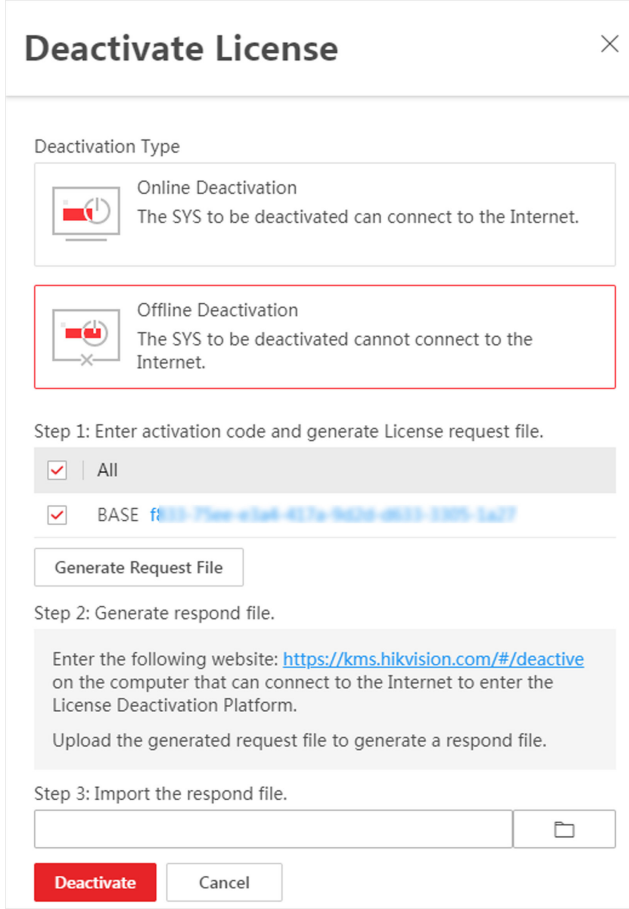


Figure 8-5 Deactivate License in Offline Mode

5. Check the activation code(s) to be deactivated.
6. Click **Generate Request File**.

Note

After the request file is generated, the selected activation code(s) will be unavailable.

A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

7. Copy the request file to the computer that can connect to the Internet.
8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/deactive*** .
9. Click and then select the downloaded request file.

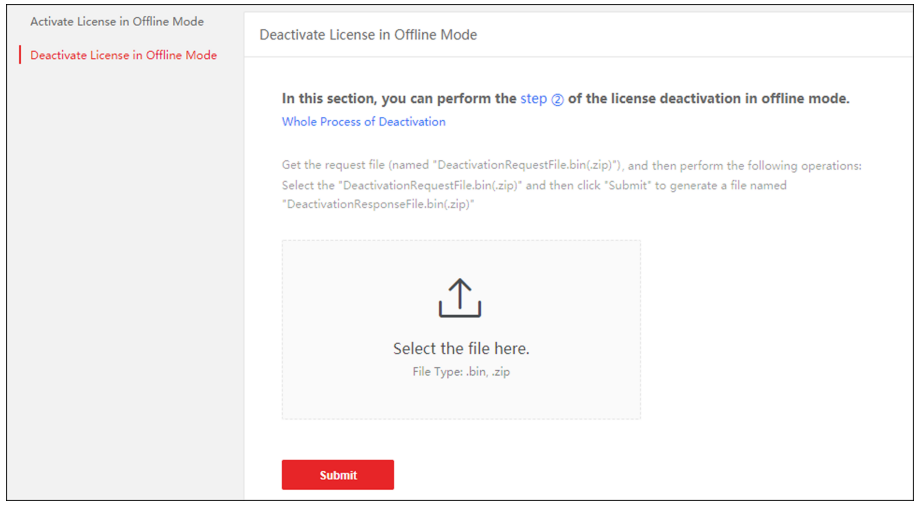


Figure 8-6 Select Request File

10. Click **Submit**.

    A respond file named "DectivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral Access Control via the Web Client.
12. In the Offline Deactivation pane, click and select the downloaded respond file.
13. Click **Deactivate**.

8.7 View License Details

You can check the authorization details of the License you purchased and view the number of manageable devices and function of your platform. If the License is not activated, you can also view the trial period.

Steps

1. Log in to the HikCentral Access Control via Web Client. See ***Login via Web Client (Administrator)*** for details.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **License Details** in the drop-down menu to open the License Details pane.

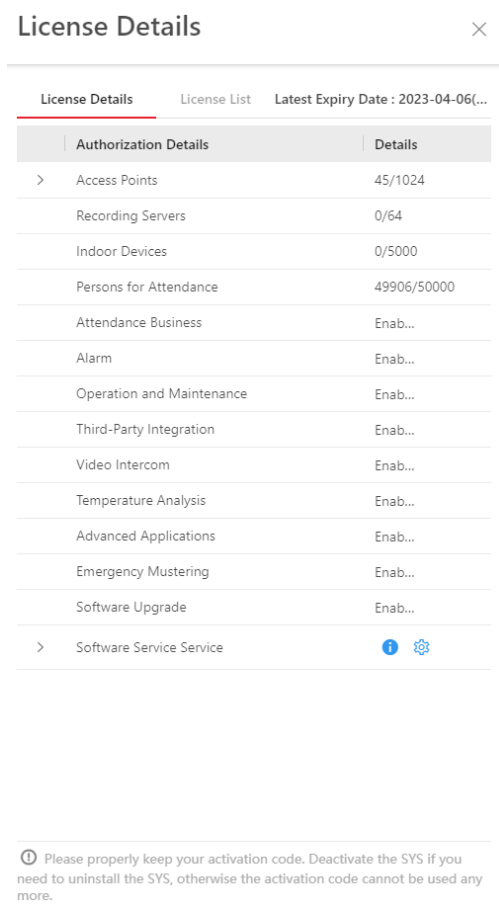


Figure 8-7 License Details Page

You can view the authorization details and check the expiry date of the trial License or the License you purchased.

4. **Optional:** Click **License List** to check all the activated License(s) of your platform and click an activation code to view the related authorization details.

8.8 Set SSP Expiration Prompt

SSP (Software Service Program) refers to the platform's maintenance service, which has an expire date and needs to be upgraded before expiration. You can set SSP expiration prompt on the platform. After that, when the SSP is going to expire, you can receive an email reminding the expiration every day during the configured period.

Steps

1. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
2. Click **License Details** in the drop-down menu to open the License Details pane.
3. Go to the bottom of details list and click to enter the SSP Expiration Prompt Settings pane.
4. Set the **Overdue Reminder** switch to ON.

5. Set the days when you will receive the prompt email before expiration.

Note

- You should enter an integer between 1 to 365.
- By default, the platform will send a prompt email 30 days before expiration.

6. Click **Add User** to add user(s) who can receive upgrade prompt.

Note

- You should configure the users' email addresses before adding them as recipients. The added users can receive upgrade prompt via the bound email addresses.
- Up to 64 recipients can be added.
- You can click × to delete the added user(s).

7. Click **Add Email** to add email address(es).

Note

You can add email of both the platform user(s) and other user(s). The platform will send expiration prompt to the added email address(es).

8. Click **Save**.

Chapter 9 Role and User Management

The system allows you to add users and assign user's permissions for accessing and managing the system. Before adding users to the system, you should create roles to define the user's access rights to system resources and then assign the role to the user for granting the permissions to the user. A user can have many different roles.

9.1 Add Role

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. You can click the role name to view details. The two default roles cannot be edited or deleted.

Administrator

Role that has all permissions of the platform.

Operator

Role that has all permissions for accessing resources and operating the Applications on the Web Client.

1. On the top, select **System**.
2. Select **Account and Security → Roles** on the left.
3. Click **Add** to enter Add Role page.
4. 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.

   Effective Period

   Set the time range within which the role takes effect. The role is inactive outside the effective period.

   Role Status

   Active is selected by default. If you select **Inactive**, the user account will be inactivated until you activate it.

   Permission Schedule Template

Set the authorized time period when the role's permission is valid. Select **All-day Template/ Weekday Template/Weekend Template** as the permission schedule of the role, or click **Add** to customize a new permission schedule template.

Note

- When 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.

5. 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.

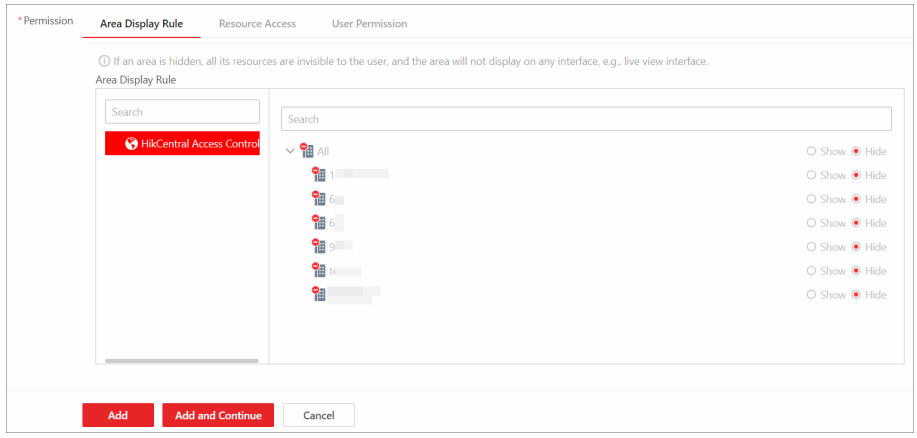


Figure 9-1 Area Display Rule

Resource Access

Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

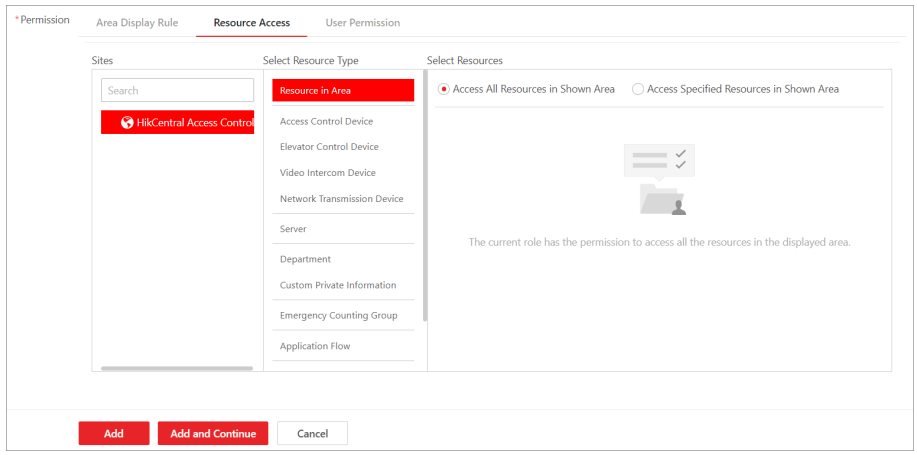


Figure 9-2 Resource Access

Note

If you do not check the resources, the resource permission cannot be applied to the role.

User Permission

Assign resource permissions, configuration permissions, and operation permissions to the role.

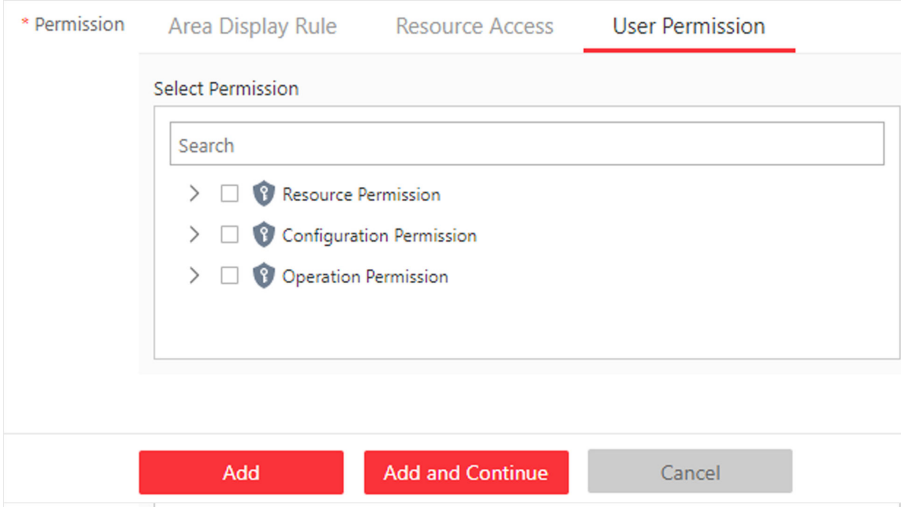


Figure 9-3 User Permission

6. Complete adding the role.
- Click **Add** to add the role and return to the role management page.
- Click **Add and Continue** to save the settings and continue to add another role.

7. Optional: Perform further operations on added roles.

Edit Role	Click a role name to view and edit role settings.

Note

The two default roles cannot be edited.

Delete Role Check a role and click **Delete** to delete the role.

Note

The two default roles cannot be deleted.

Inactivate Role Check a role and click **Inactivate** to set the role status to **Inactive**.

Activate Role Check an inactive role and click **Activate** to set the role status to **Active**.

Refresh Role Click **Refresh All** to get the latest status of the roles.

Filter Role Click to expand the filter conditions. Set the conditions and click **Filter** to filter the roles according to the set conditions.

9.2 Add 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. On the top, select **System**.
2. Select **Account and Security → Users** on the left.
3. Click **Add**.
4. Set basic information for the user.

User Name

Only letters (a-z, A-Z), digits (0-9), and "-" are allowed.

Password

Create an initial password for the user. The user will be asked to change the password when logging in for first time. See ***First Time Login for Normal User*** for details.

Note

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

Expiry Date

The date when the user account becomes invalid.

Email

The system can notify user by sending an email to the email address. The user can also reset the password via email.

Note

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.

Restrict Concurrent Logins

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

5. Configure permission settings for the user.

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 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. Do one of the following to complete adding the user.

- Click **Add** to add the user and return to the user management page.
- Click **Add and Continue** to save the settings and continue to add another user.

7. Optional: Perform further operations on the added normal users.

Edit User	Click user name to view and edit user settings.
Reset Password	Click user name and click **Reset** to set a new password for the user. Enter a new password and click **Reset**. **Note** The admin user can reset the passwords of all the other users (except domain user). Other users with Security permission (in Configuration and Control Permission) can reset the passwords of the users without Security permission. When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Access Control via the Web Client.
Delete User	Select a users and click **Delete** to delete the selected user.
Force Logout	Select an online user and click **Force Logout** to log out the online user.

Inactivate/ Activate User	• The admin user or user with administrator permission can inactivate or activate a user. • Select an active users and click **Inactivate/Activate** to inactivate/activate the user.
Refresh User	Click **Refresh All** to get the latest status of all users.
Filter User	Click ▽ to set conditions and filter the users.

9.3 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. On the top, select **System**.

2. Select **Account and Security → Users** on the left.

3. Click **Import Domain Users**.

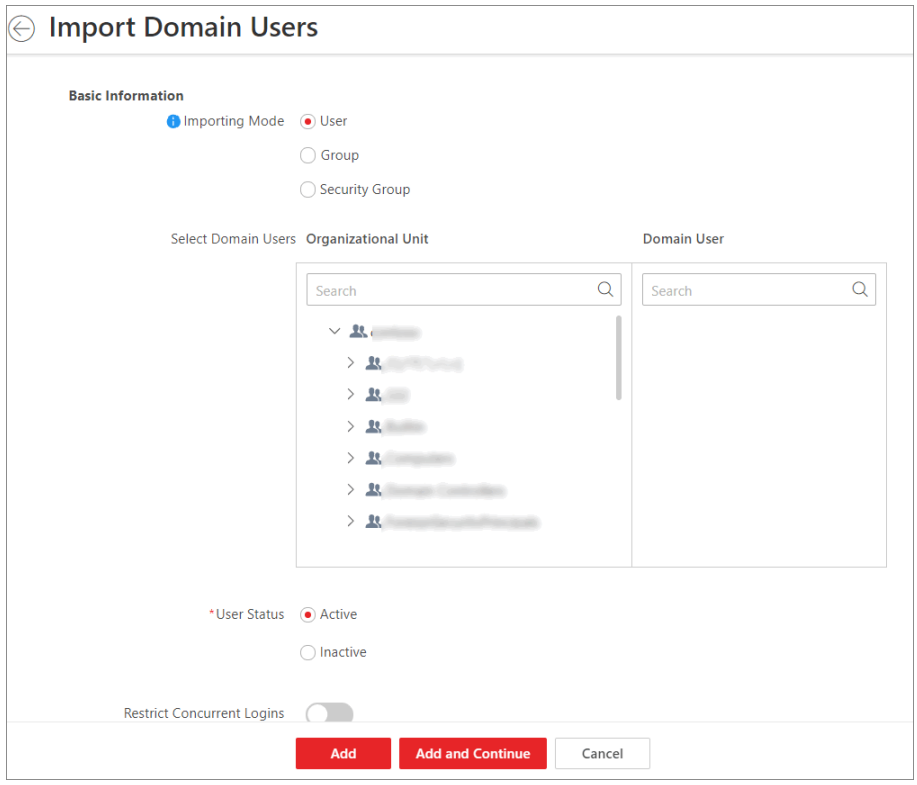


Figure 9-4 Import Domain Users

4. 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.

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.

5. Select domain users from active directory.
6. Select the user status as **Active** or **Inactive**.
7. **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.
8. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

Note

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.

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.

Note

- 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**. See ***Add 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.
11. **Optional:** 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).

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.

9.4 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.

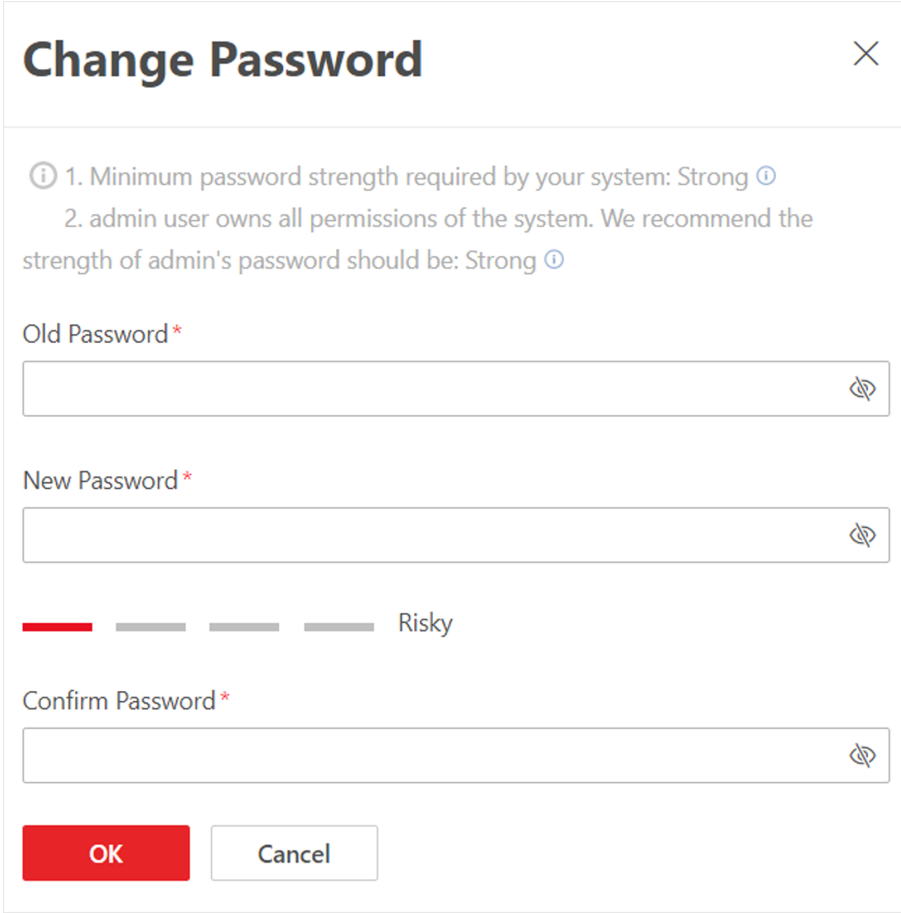


Figure 9-5 Change Password Panel

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.

9.5 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, Weekday Template, and Weekend Template. You can add new templates according to actual needs.

Steps

1. On the top, go to **System → Account and Security → Permission Schedule Template** .

2. Click + .

3. Set the basic information.

Name

Create a name for the template.

Copy From

Select the template from the drop-down list to copy the settings from another existing template.

4. In the **Weekly Schedule** area, set the weekly schedule as needed.

1) Click **Authorize**, and select or draw in the box to define the authorized time periods.
2) **Optional:** Click **Eraser**, and select or draw on the authorized time periods to clear the selection.

Note

You can set up to 6 separate time periods for each day.

5. **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.

Note

The holiday schedule has a higher priority than the weekly schedule.

6. Click **Add** to add the permission schedule template.
7. **Optional:** Perform further operations for the added templates.

View and Edit Template Details	Click the template to view and edit its configuration. **Note** Default templates cannot be edited.
Delete Template	Click a template, and click 🗑 to delete it. **Note** Default templates cannot be deleted.

What to do next

Set permission schedules for roles to define in which period the permissions for the roles are valid. For details, refer to ***Add Role*** .

Chapter 10 Application Summary

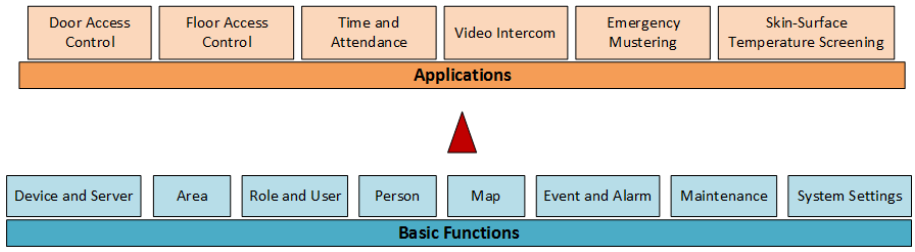


Figure 10-1 Functions and Applications in HikCentral Access Control

Table 10-1 Applications in HikCentral Access Control

Applications	Description
Door Access Control	Refer to ***Flow Chart of Door Access Control*** and ***Access Control Management*** for details.
Floor Access Control	Refer to ***Flow Chart of Floor Access Control*** and ***Access Control Management*** for details.
Time and Attendance	Refer to ***Flow Chart of Time and Attendance*** and ***Time & Attendance*** for details.
Video Intercom	Refer to ***Flow Chart of Video Intercom*** and ***Video Intercom Management*** for details.
Emergency Mustering	Refer to ***Emergency Mustering*** for details.
Skin-Surface Temperature Screening	Refer to ***Skin-Surface Temperature Screening*** for details.

Table 10-2 Basic Functions in HikCentral Access Control

Basic Functions	Description
Device and Server	Refer to ***Resource Management*** for details.
Area	Refer to ***Area Management*** for details.
Role and User	Refer to ***Role and User Management*** for details.
Person	Refer to ***Person Management*** for details.
Map	Refer to ***Map Management*** for details.
Event and Alarm	Refer to ***Event and Alarm*** for details.

Basic Functions	Description
Maintenance	Refer to ***Maintenance*** for details.
System Settings	Refer to ***System Configuration*** and ***System Security Settings*** for details.

10.1 Flow Chart of Door Access Control

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

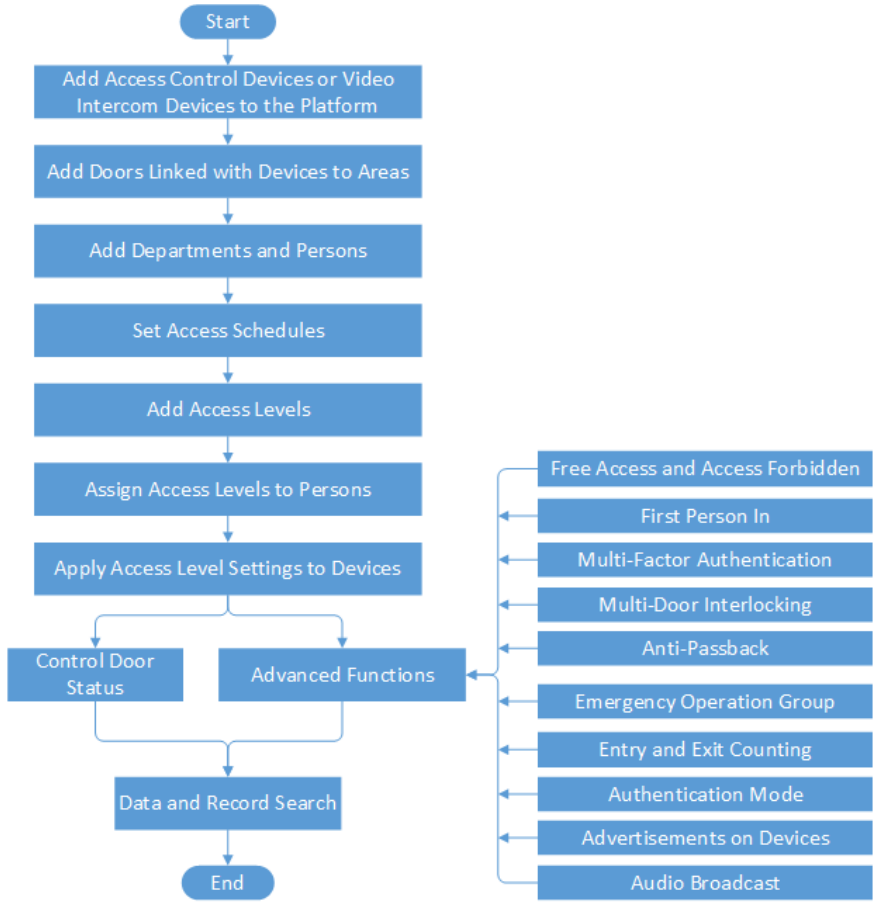


Figure 10-2 Flow Chart of Door Access Control

Note

Some functions in this flow chart need the License. For details about License, refer to ***License Management*** .

Table 10-3 Procedures of Door Access Control

Procedure	Description
Add Access Control Devices or Video Intercom Devices to the Platform	You need to add access control devices and video intercom devices to the system. For details, refer to ***Manage Access Control Device*** and ***Manage Video Intercom Device*** .
Add Doors Linked with Devices to Areas	Group doors linked with added devices for management. Refer to ***Add Door to Area*** for details.
Add Departments and Persons	Add person information and set person's credentials (such as PIN, card, and fingerprint). For details, refer to ***Person Management*** .
Set Access Schedules	The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** .
Add Access Levels	An access level is a group of doors. After assigning access level, the assigned objects can get access to these doors during the authorized time period. For details, refer to ***Manage Access Level*** .
Assign Access Levels to Persons	You need to assign access levels to persons, so that the assignees can access the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person or a department. For details, refer to ***Assign Access Level*** .
Apply Access Level Settings to Devices	After setting the linkage between the persons and the access level, you need to apply the person's access level settings to the access control device of the doors linked to the access level to take effect. After that, the persons can access these doors during the authorized time period defined by the related access level. For details, refer to ***Apply Persons' Access Levels to Device*** .
Control Door Status	You can manually change the door status to locked, unlocked, remaining locked, or remaining unlocked. Refer to ***Door Control*** for details.
Advanced Functions	Refer to ***Configure Free Access and Access Forbidden Rules*** , ***Configure First Person In Rule*** , ***Configure Multi-Factor Authentication Rule*** , ***Configure Multi-Door Interlocking*** , ***Configure Area Anti-Passback Rules*** , ***Add Emergency Operation Group*** , ***Add Entry and Exit Counting Group*** ,

Procedure	Description
	Configure Authentication Mode , ***Apply Advertisement to Access Control Devices*** , and ***Add Audio Broadcast*** for details.
Data and Record Search	Refer to ***Search Access Records*** and ***Search Data Recorded on Access Control Devices and Elevator Control Devices*** for details.

10.2 Flow Chart of Floor Access Control

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

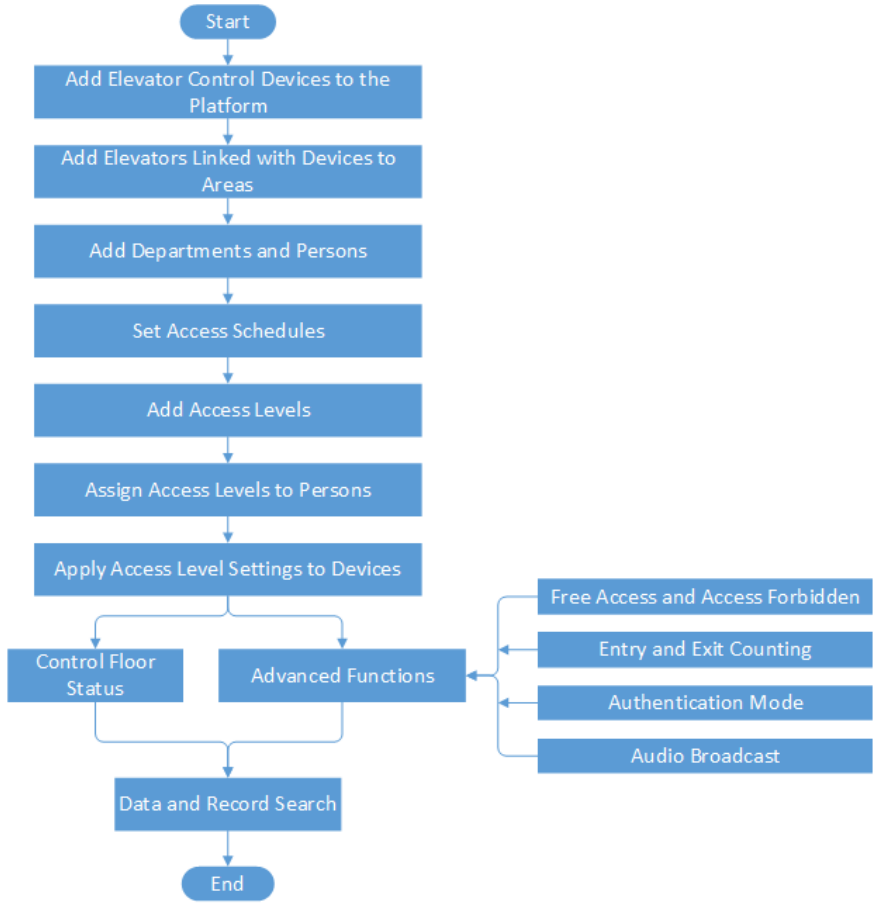


Figure 10-3 Flow Chart of Floor Access Control

Note

Some functions in this flow chart need the License. For details about License, refer to ***License Management*** .

Table 10-4 Procedures of Floor Access Control

Procedure	Description
Add Elevator Control Devices to the Platform	You need to add elevator control devices to the system. For details, refer to ***Manage Elevator Control Device*** .
Add Elevators Linked with Devices to Areas	Group elevators linked with added devices for management. Refer to ***Add Elevator to Area*** for details.
Add Departments and Persons	Add person information and set person's credentials (such as PIN, card, and fingerprint). For details, refer to ***Person Management*** .
Set Access Schedules	The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** .
Add Access Levels	An access level is a group of floors. After assigning access level, the assigned objects can get access to these floors during the authorized time period. For details, refer to ***Manage Access Level*** .
Assign Access Levels to Persons	You need to assign access levels to persons, so that the assignees can access the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person or a department. For details, refer to ***Assign Access Level*** .
Apply Access Level Settings to Devices	After setting the linkage between the persons and the access level, you need to apply the person's access level settings to the elevator control device of the elevators linked to the access level to take effect. After that, the persons can access these floors during the authorized time period defined by the related access level. For details, refer to ***Apply Persons' Access Levels to Device*** .
Control Floor Status	You can manually change the floor status to temporary access, access with credential, free access, or access forbidden. Refer to ***Elevator Control*** for details.
Advanced Functions	Refer to ***Configure Free Access and Access Forbidden Rules*** , ***Add Entry and Exit Counting Group*** , ***Configure Authentication Mode*** , and ***Add Audio Broadcast*** for details.
Data and Record Search	Refer to ***Search Access Records*** and ***Search Data Recorded on Access Control Devices and Elevator Control Devices*** for details.

10.3 Flow Chart of Time and Attendance

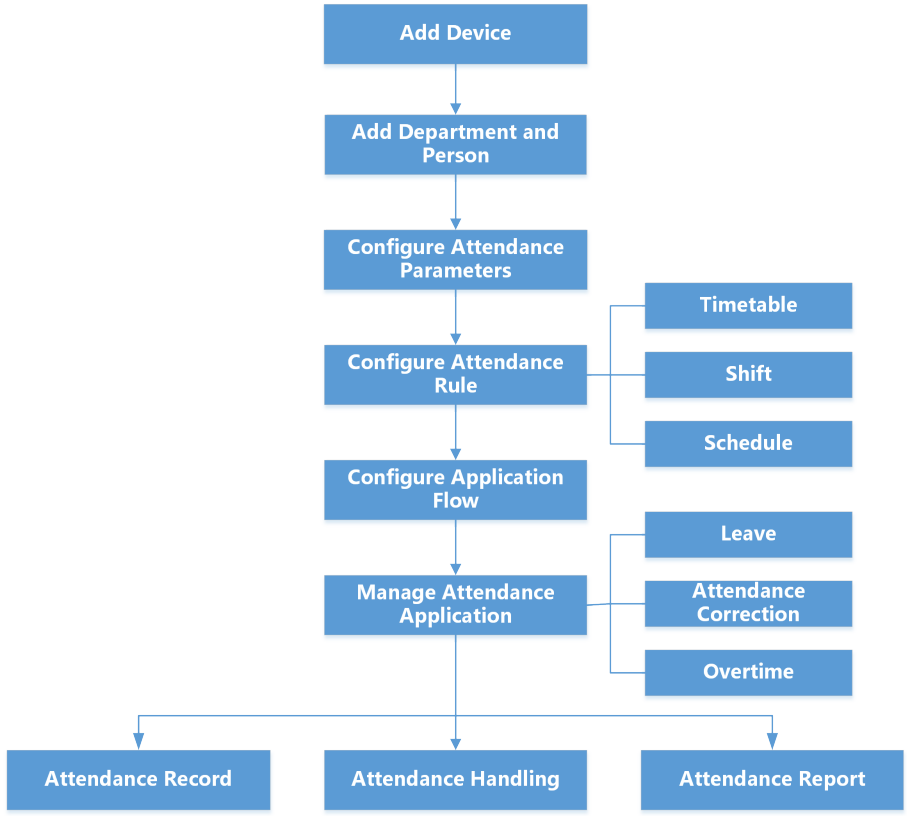


Figure 10-4 Flow Chart of Time & Attendance

- **Add Device**: Add devices (e.g., access control devices) to the platform. For more details, refer to ***Resource Management*** .
- **Add Department and Person**: Add departments and persons. For more details, refer to ***Add Departments*** and ***Add Person*** .
- **Configure Attendance Parameters**: Configure attendance check points, general rule, overtime rule, leave types, display rule for report, third-party database, etc. For more details, refer to ***Configure Global/Department Attendance Rules*** , ***Set Display Rules for Attendance Report*** and ***Synchronize Card Swiping Records to Third-Party Database*** .
- **Configure Attendance Rule**: Add timetable (including break timetable and work timetable), shift, and schedule. For more details, refer to ***Add Timetable*** , ***Add Shift*** and ***Manage Schedule*** .
- **Configure Application Flow**: Configure approval roles and application flows for departments/ persons. For more details, refer to ***Application Flow Management*** .
- **Manage Attendance Application**: Manage applications for employees and admins. For more details, refer to ***Application Management for Employee*** and ***Application Management for Admin*** .

- **Attendance Record**, **Attendance Handling**: Search and correct attendance records, apply for leave, get devices' attendance records, manually calculate attendance results, etc. For more details, refer to ***View Attendance Records*** .
- **Attendance Report**: Export attendance report to local PC or send it via email regularly. For more details, refer to ***Manage Attendance Reports*** .

10.4 Flow Chart of Video Intercom

For the first time, you can follow the flow chart to perform configurations and operations.

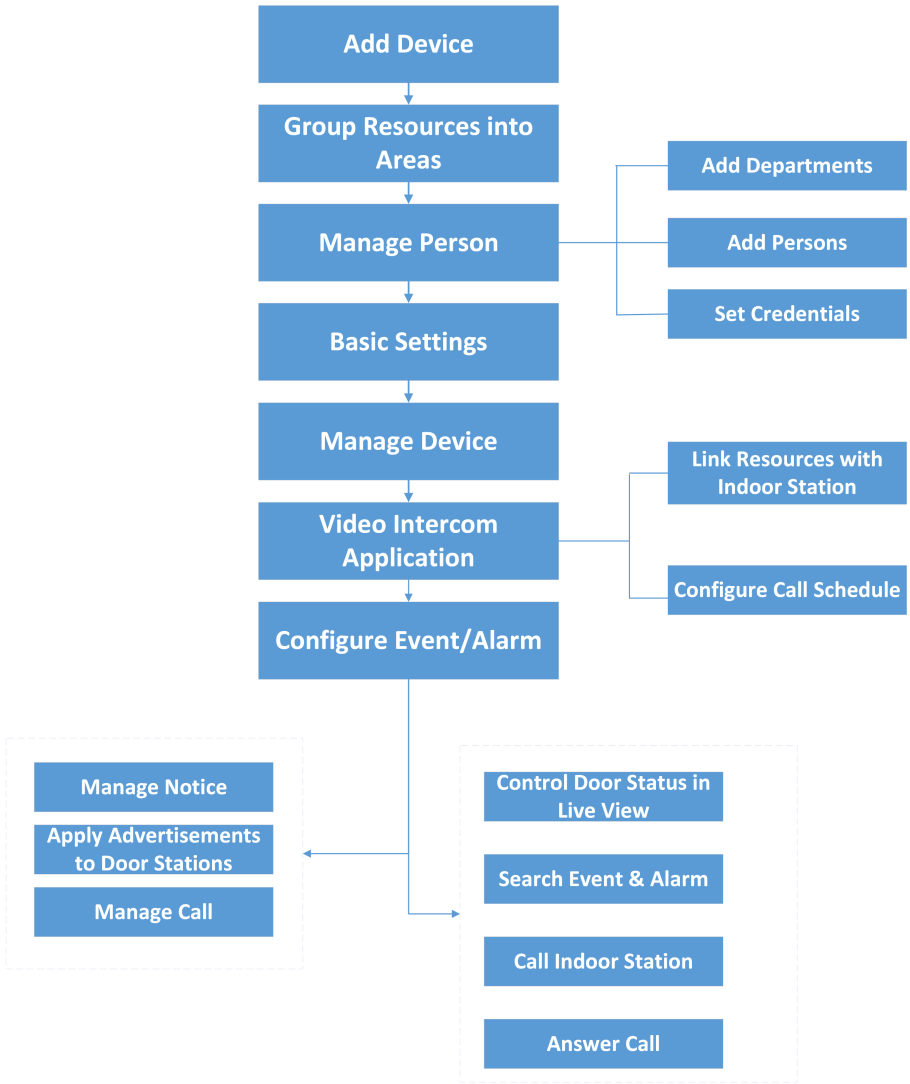


Figure 10-5 Flow Chart of Video Intercom

- **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. For more details, refer to ***Manage Video Intercom Device*** and ***Configure Device Parameters*** .

- **Group Resources into Areas**: After adding the devices to the system, you need to group the devices' resources (such as doors and cameras) into different areas according to the resources' locations. For details, refer to ***Area Management*** .
- **Manage Person**: Add departments and persons to the system, and set credential information. For details, refer to ***Person Management*** .
- **Basic Settings**: Add call recipients and call schedule templates, and configure call parameters. For details, refer to ***Basic Settings of the Platform*** .
- **Manage Device**: Set location information for video intercom devices and apply the settings to devices. For details, refer to ***Manage Video Intercom Device*** .
- **Video Intercom Application**: Add call schedules and apply them to devices, link resources (camera, person, and doorbell) to indoor stations. For details, refer to ***Video Intercom Application*** .
- **Configure Event / Alarm**: Configure event and alarm for video intercom resources. For more details, refer to ***Event and Alarm*** .
- **Manage Notice**: Add notices and apply them to indoor stations. For details, refer to ***Manage Notices*** .
- **Apply Advertisements to Door Stations**: Apply pictures or video to door stations as advertisements. See ***Apply Advertisements to Door Stations*** .
- **Manage Call**: Call indoor stations and view recents. Fore details, refer to ***Call & Talk*** .

Chapter 11 Resource Management

HikCentral Access Control supports multiple resource types, such as access control device, . After adding them to the system, you can manage them, configure required settings and perform further operations. For example, you can add access control devices for access control, time and attendance management, etc., .

11.1 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 top, select **Device**.
2. Select **Device and Server** on the left.
3. Select the device to be activated.
4. In the Online Device area, view the device status and select one or multiple inactive devices.
5. Click **Activate** to open the device activation window.
6. 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 installer and/or end-user.

7. 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.

8. 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*** .

11.2 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with SYS server 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 top, select **Device**.
2. Select **Device and Server** on the left.
3. Select the device type from **Access Control Device**, **Elevator Control Device**, **Video Intercom Device**, **Network Transmission Device**, and **Recording Server**.
4. 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.
5. View the device status, and click in the Operation column of an active device.
6. Edit the device parameters, such as IP address, device port, HTTP port, subnet mask, and gateway.

   Note

   - If you have switched on **Used DHCP**, you can only edit the device port No.
   - The parameters may vary for different device types.
7. Click .
8. Enter the device's password.

9. Click **Save**.

11.3 Manage Access Control Device

You can add the access control devices to the system for access permission configuration, time and attendance management, etc.

11.3.1 Add Detected Online Access Control Devices

The active online access control devices in the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add one online device one by one, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Access Control Device

The platform automatically detects online access control devices on the same local subnet with the client or SYS server. You can add the detected access control devices to the platform one by one if they have different user account.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Follow the steps to add a detected online access control device to the platform.

Steps

1. On the top, select **Device**.

2. Select **Device and Server → Access Control Device** on the left.

3. In the Online Device area, select a network type.

Server Network

All detected online devices on the same local subnet with the SYS server.

Local Network

All detected online devices on the same local subnet with the current Web Client.

4. Select **Hikvision Private Protocol** and **Hikvision ISUP Protocol** to filter the detected devices by protocol types.

Note

Make sure you have enabled the ISUP protocol registration to allow the devices to access the system, otherwise the online devices will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.

5. Select an active device that you want to add to the platform.
6. Click **Add to Device List**.

Note

For devices whose device port No. is 8000 and HTTP port No. is 80, the **Hikvision Private Protocol** is selected as the access protocol by default. For devices whose device port No. is 0 but the HTTP port No. is 80, the **ISAPI Protocol** is selected as the access protocol.

7. Configure the basic information for the device, including access protocol, device address, device port, device name, user name, and 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 installer and/or end-user.

Note

The access protocol will not show in the following situations:

- You check more than one device in the Online Device area.
- You check only one device in the Online Device area.
  - You can select **Hikvision ISUP Protocol** in the Online Device area.
  - You can select **Hikvision Private Protocol** in the Online Device area, and device port is 0.

8. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.

10. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

11. Click **Add**.
12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.
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. In the **Operation** column, click to replace the old device with the new device on the platform.
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.

Note

If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter key words in the search box and click to search for a specific device.

Add Detected Online Access Control Devices in a Batch

If the detected online access control devices share the same user name and password, you can add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select **Hikvision Private Protocol** and **Hikvision ISUP Protocol** to filter the detected devices by protocol types.

   Note

   Make sure you have enabled the ISUP protocol registration to allow the devices to access the system, otherwise the online devices will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**.

Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.

5. Select the active devices that you want to add to the platform.
6. Click **Add to Device List**.

Note

For devices whose device port No. is 8000 and HTTP port No. is 80, the **Hikvision Private Protocol** is selected as the access protocol by default. For devices whose device port No. is 0 but the HTTP port No. is 80, the **ISAPI Protocol** is selected as the access protocol.

7. Set parameters for the devices.

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 installer and/or end-user.

8. **Optional:** Set the time zone for the device.
   - **Get Device's Time Zone**

     The time zone of the device will be automatically chosen according to the region of the device.
   - **Manually Set Time Zone (The settings will be applied to the device automatically)**

     You can select a time zone of the device. The settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.

10. Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

11. Click **Add**.
12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Replace Device	In the **Operation** column, click to replace the device with a new device. If the serial No. of the new device is different from that of the old one, you need to confirm the replacement.
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 share the same password, you can select multiple devices to change the password together.
Privacy Settings	You can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter key words in the search box and click 🔍 to search for a specific device.

11.3.2 Add an Access Control Device by IP Address/Domain

If you know the IP address/domain of the access control device you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol**, or **Hikvision ISAPI Protocol** as the access protocol.
5. Select **IP Address/Domain** as the adding mode.
6. Enter the required parameters.

Note

By default, the device port number is 8000 when the access protocol is **Hikvision Private Protocol**, while the device port number is 80 when the access protocol is **Hikvision ISAPI Protocol**.

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 installer and/or end-user.

7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.

9. Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
Replace Device	If the original device malfunctions, you can replace it with a new device using the same IP address. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

11.3.3 Add Access Control Devices by IP Segment

If the access control devices you want to add to the platform share the same user account, and they are in the same IP segment, you can add them to the platform by specifying the start/end IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol** or **Hikvision ISAPI Protocol** as the access protocol.
5. Select **IP Segment** as the adding mode.
6. Enter the required information.

Note

By default, the device port number is 8000 when the access protocol is **Hikvision Private Protocol**, while the device port number is 80 when the access protocol is **Hikvision ISAPI Protocol**.

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 installer and/or end-user.

7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.

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.

Note

If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

11.3.4 Add an Access Control Device by Device ID

For access control devices supporting ISUP 4.0 or later protocol, you can add them by specifying a predefined device ID and key. This is a cost-effective choice when you need to manage access control devices that do not have fixed IP addresses.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.

2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.

Note

Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.

5. Select **Device ID** as the adding mode.
6. Enter the required the information.
7. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

     Note

     This configuration only affects the facial recognition device which supports face comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configure** to enable **Local Storage** and set the storage locations for pictures and files as needed.
8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device,

	restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

11.3.5 Add Access Control Devices by Device ID Segment

If you need to add multiple access control devices which support ISUP 5.0 protocol and have no fixed IP addresses to the platform, you can add them all at once after configuring a device ID segment for the devices.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.

Note

Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.

5. Select **Device ID Segment** as the adding mode.
6. Enter the required parameters.
7. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

     Note

     This configuration only affects the facial recognition device which supports face comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configuration** to enable **Local Storage** and set the storage locations for pictures and files as needed.
8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.

- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
- Click **Add** to add the device(s) and return to the device management page.
- Click **Add and Continue** to add the device(s) and continue to add other devices.

11. Optional: Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.
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. In the **Operation** column, click to replace the old device with the new device on the platform.
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. **Note** If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click 🔍 to search for a specific device.

11.3.6 Add Access Control Devices in a Batch

You can download and enter access control device information in the predefined spreadsheet to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol**, or **Hikvision ISAPI Protocol** as the access protocol.

   Note

   Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined spreadsheet (XLSX format) to local disk.
7. Open the spreadsheet and edit the required device information.
8. Click and select the edited spreadsheet.
9. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

     Note

     This configuration only affects the facial recognition device which supports face comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configure** to enable **Local Storage** and set the storage locations for pictures and files as needed.

   Setting picture storage location is not required for devices added via **Hikvision ISAPI Protocol**.
10. **Optional:** Set the time zone for the device.

    Get Device's Time Zone

    The time zone of the device will be automatically chosen according to the region of the device.

    Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

11. Finish adding the device(s).
- Click **Add** to add the device(s) and return to the device management page.
- Click **Add and Continue** to add the device(s) and continue to add other devices.

12. Optional: Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.
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. For details, refer to ***Privacy Settings*** .
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click 🔍 to search for a specific device.

11.3.7 Configure Device Parameters

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

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.

Before You Start

Make sure you have wired the third-party card readers to the access control device or elevator control device.

Steps

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.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** or **Device and Server → Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Switch on **Custom Wiegand**.
5. Configure the Wiegand parameters.

   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

Configure Device Actions for Access Event

You can set the linkage actions of an access control device or elevator control device for the device's events, so that when a specific event occurs, the device can execute actions such as triggering alarm output, triggering buzzer, arming/disarming zones, locking/unlocking access points, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** or **Device and Server → Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Event Linkage** as the linkage type.
   2) Select an event type from the **Event Type** drop-down list and then select a specific event.

   Note

   - If you select **Alarm Input Event**, you need to select an alarm input.
   - If you select **Door Event**, you need to select an access point.
   - If you select **Card Reader Event**, you need to select a card reader.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

Floor

Temporary Access

Grant access to the floor for a limited time when the specified event is triggered.

Access with Credential

Grant access to the floor if the user presents valid credentials when the specified event is triggered.

Free Access

Grant access to the floor indefinitely when the specified event is triggered.

Access Forbidden

Deny access to the floor indefinitely when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.

8. Optional: Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for Card Swiping

You can set the linkage actions of an access control device or elevator control device for card swiping, so that when the device detects a specific card, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the card holder.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.

2. Select **Device and Server → Access Control Device** on the left.

3. Click ⚙ in the Operation column to enter the configuration page of a device.

4. Click **Add** in the Linkage section.

5. Configure event source.

1) Select **Card Linkage** as the linkage type.
2) Select a card from the **Card No.** drop-down list.
3) Select a card reader from the **Card Reader** drop-down list.

6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

Floor

Temporary Access

Grant access to the floor for a limited time when the specified event is triggered.

Access with Credential

Grant access to the floor if the user presents valid credentials when the specified event is triggered.

Free Access

Grant access to the floor indefinitely when the specified event is triggered.

Access Forbidden

Deny access to the floor indefinitely when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.
8. Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for Person ID

You can set the linkage actions of an access control device or elevator control device for person ID, so that when the device detects the credentials of the person, it can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the person.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** or **Device and Server → Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.

5. Configure event source.
1) Select **Person Linkage** as the linkage type.
2) Select a person ID from the **Person** drop-down list.
3) Select a card reader from the **Card Reader** drop-down list.

6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

Floor

Temporary Access

Grant access to the floor for a limited time when the specified event is triggered.

Access with Credential

Grant access to the floor if the user presents valid credentials when the specified event is triggered.

Free Access

Grant access to the floor indefinitely when the specified event is triggered.

Access Forbidden

Deny access to the floor indefinitely when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.

8. Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for MAC Address

You can set access control device's linkage actions for MAC address of mobile devices, so that when the device detects a specific MAC address, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Select **MAC Linkage** as the linkage type, and then edit the MAC address.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

Floor

Temporary Access

Grant access to the floor for a limited time when the specified event is triggered.

Access with Credential

Grant access to the floor if the user presents valid credentials when the specified event is triggered.

Free Access

Grant access to the floor indefinitely when the specified event is triggered.

Access Forbidden

Deny access to the floor indefinitely when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.

8. Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure 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.

Steps

1. On the top, select **Device → Device and Server → Access Control Device** , or **Device and Server → Elevator Control Device** .
2. Click ⚙ on the Operation column to enter the configuration page of a device.
3. In Card Swiping section, configure card swiping parameters.

Note

Parameters vary with different device types and models.

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 the linked camera(s) to the platform automatically.

Note

For details about linking a camera to an access point, see ***Edit Door*** or ***Edit Elevator*** .

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 Door*** or ***Edit Elevator*** .

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.

Configure Other Parameters

You can configure other parameters for an access control device, such as device time and facial recognition mode.

Note

- Device support required. Parameters vary with different device types and models.
- For more remote configurations, click **Configuration** at the end of the device configuration page. For detailed instructions, refer to the user manual of the device.

Time

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

Device Time

Click the **Device Time** field to custom 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 enable, the device can recognize persons by their fingerprint.

Skin-surface Temperature

Set **Temperature Screening** 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 must be higher than the minimum temperature.

Open Door When Temperature is Abnormal

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

Linked Thermal Camera

Enter the device IP address of the linked thermal camera for temperature screening.

Note

It is used for the access control devices that do not support temperature screening.

Mask Settings

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

Do Not Open Barrier when No Mask

If checked, the barrier will still open for persons without a mask.

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 restoring.

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 **Configuration** to open the remote configuration page of the device and configure more parameters.

11.3.8 Privacy Settings

You can configure the settings for event storage, authentication, and picture uploading and storage, and clear the pictures on the access control devices to protect the person's private information, including name, profile picture, etc.

On the top, select **Device**. Then select **Device and Server → Access Control Device** on the left.

Select one or more devices and click **Privacy Settings**.

Note

Make sure the selected device is online.

Set the following parameters as needed and click **Save**.

Event Storage

Select the mode of event storage.

Overwrite

The events stored on the device will be overwritten automatically. For example, if a device can store up to 200 events. When this limit is reached, the first event will be overwritten by the newest one, and then the second will be overwritten.

Delete Old Events Regularly

Set a time period. The events stored on the device during the period will be automatically deleted at intervals of the period.

Delete Old Events by Specified Time

Set a specific time. The events stored on the device before the specific time will be automatically deleted.

Authentication

Check the items to be displayed in authentication results.

Picture Uploading and Storage

Check the items as needed.

Upload Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be uploaded to the system.

Save Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be saved to the devices.

Save Profile Pictures

If it is checked, the profile pictures will be saved to the devices.

Upload Event and Alarm Pictures

If it is checked, the event and alarm pictures will be uploaded to the system.

Save Event and Alarm Pictures

If it is checked, the event and alarm pictures will be saved to the devices.

Upload Thermal Pictures

If it is checked, the thermal pictures will be uploaded to the system.

Save Thermal Pictures

If it is checked, the thermal pictures will be saved to the devices.

Clear Pictures Stored on Device

Clear Face Pictures

Click **Clear** to clear all face pictures.

Clear Recognized or Captured Pictures

Click **Clear** to clear all recognized pictures or captured pictures.

11.4 Manage Elevator Control Device

You can add the elevator control device to the system to control the elevator(s), such as assign the access authority of specified floors to person, control the elevator status on the Mobile Client.

11.4.1 Add Detected Online Elevator Control Devices

The active online elevator control devices on the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add an online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function will be available.

Add a Detected Online Elevator Control Device

The Web Client automatically searches for online elevator control devices on the same local subnet with the client or SYS server. You can add the detected elevator control devices to the platform one by one if the devices do not share the same user account.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Elevator Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select an active device that you want to add to the platform.
5. Click **Add** to open the Add Elevator Control Device window.
6. Configure the basic information for the device, including device address, device port, device name, user name, and 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 installer and/or end-user.
7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

Note

- You can create a new area by device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the resources.
- Enter the range of floor number according to your application scenario.

9. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Click **Add**.
11. **Optional:** Perform further operations on added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.
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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

Add Detected Online Elevator Control Devices in a Batch

If the detected online elevator control devices share the same user account, you can add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Elevator Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select the active devices that you want to add to the platform.
5. Click **Add to Device List** to open the Add Elevator Control Device window.
6. Set parameters for the devices.

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 installer and/or end-user.

7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

   Note

   - You can create a new area by device name or select an existing area.
   - If you do not import resources to an area, you cannot perform further operations for the resources.
   - Enter the range of floor number according to your application scenario.

9. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

   Note

   - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
   - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.

11. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.

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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

11.4.2 Add an Elevator Control Device by IP Address

If you know the IP address of the elevator control device you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **IP Address** as the adding mode.
5. Enter the required parameters.

Note

By default, the device port number is 8000.

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 installer and/or end-user.

6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

Note

- You can create a new area by device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the resources.
- Enter the range of floor number according to your application scenario.

8. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

Note

Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.

9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.

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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

11.4.3 Add Elevator Control Devices by IP Segment

If the elevator control devices you want to add to the platform share the same user account, and they are in the same IP segment, you can add them to the platform by specifying the start/end IP address, user name, and password.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **IP Segment** as the adding mode.
5. Enter the required parameters.

Note

By default, the device port number is 8000.

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 installer and/or end-user.

6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

Note

- You can create a new area by device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the resources.
- Enter the range of floor number according to your application scenario.

8. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
9. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.

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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

11.4.4 Add Elevator Control Devices in a Batch

You can download and enter elevator control device information in the predefined spreadsheet to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined spreadsheet (XSLX file) to the local disk.
6. Open the spreadsheet and edit the required device information.
7. Click and select the edited spreadsheet.
8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
9. Finish adding the device(s).

- Click **Add** to add the device(s) and return to the device management page.
- Click **Add and Continue** to add the device(s) and continue to add other devices.

10. Optional: Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
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 share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click 🔍 to search for a specific device.

11.5 Manage Video Intercom Device

You can add video intercom devices (indoor station, door station, outer door station, and main station) to the system for management, including editing and deleting the devices, remote configuration, changing online devices' password, etc. You can also perform further operations such as video intercom, unlocking door remotely, etc. based on the added devices.

- **Indoor Station:** The indoor station is an intelligent terminal which can provide two-way audio, network transmission, data storage, remote unlocking, etc. It is mainly applied in the community.
- **Door Station:** The door station can send call to indoor station (residents) and main station. It is mainly applied in the community and office buildings.

- **Outer Door Station:** The outer door station can send call to indoor station (residents) and main station. It is mainly applied in the community and office buildings.
- **Main Station:** The main station is an intelligent terminal, which can be used to unlock door remotely, send call to residents and respond to residents' call. It is mainly applied in large community.

11.5.1 Add a Detected Online Video Intercom Device

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed in the list, and you can add the detected indoor station to the system one by one.

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.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Video Intercom Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the current Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active device to be added.
5. Click in the Online Device area to enter the Add Video Intercom Device page.

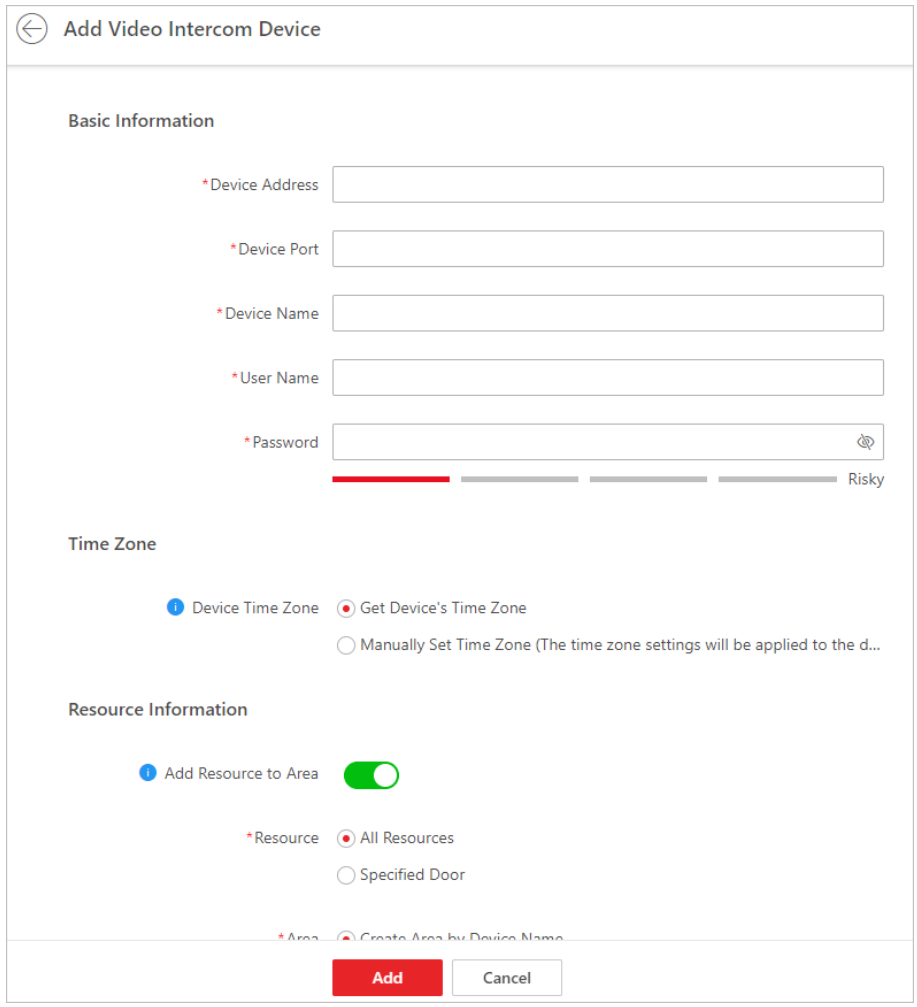


Figure 11-1 Add a Detected Online Video Intercom Device

6. Configure the basic information for the device, including device address, device port, device name, user name, and 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 installer and/or end-user.

7. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

Note

You can click **View** to view the details of the current time zone.

- Click **Get Device's Time Zone** to get the device's time zone.

8. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the alarm inputs or the specified alarm input to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further operations for the alarm inputs.

9. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Click **Add**.
11. **Optional:** Perform the following operation(s) after adding the online device.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click 🔑 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.
Restore Default Settings	Select the added device(s), and click ⚙ to restore the configured device parameters. **Note** If you want to restore all the device parameters, you can check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

11.5.2 Add a Video Intercom Device by IP Address

When you know the IP address of a video intercom device, you can add it to the system by specifying the IP address, user name, password, etc. for management and further video intercom applications.

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.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Video Intercom Device** on the left.
3. Click **Add** to enter Add Video Intercom Device page.
4. Select **IP Address** as the adding mode.

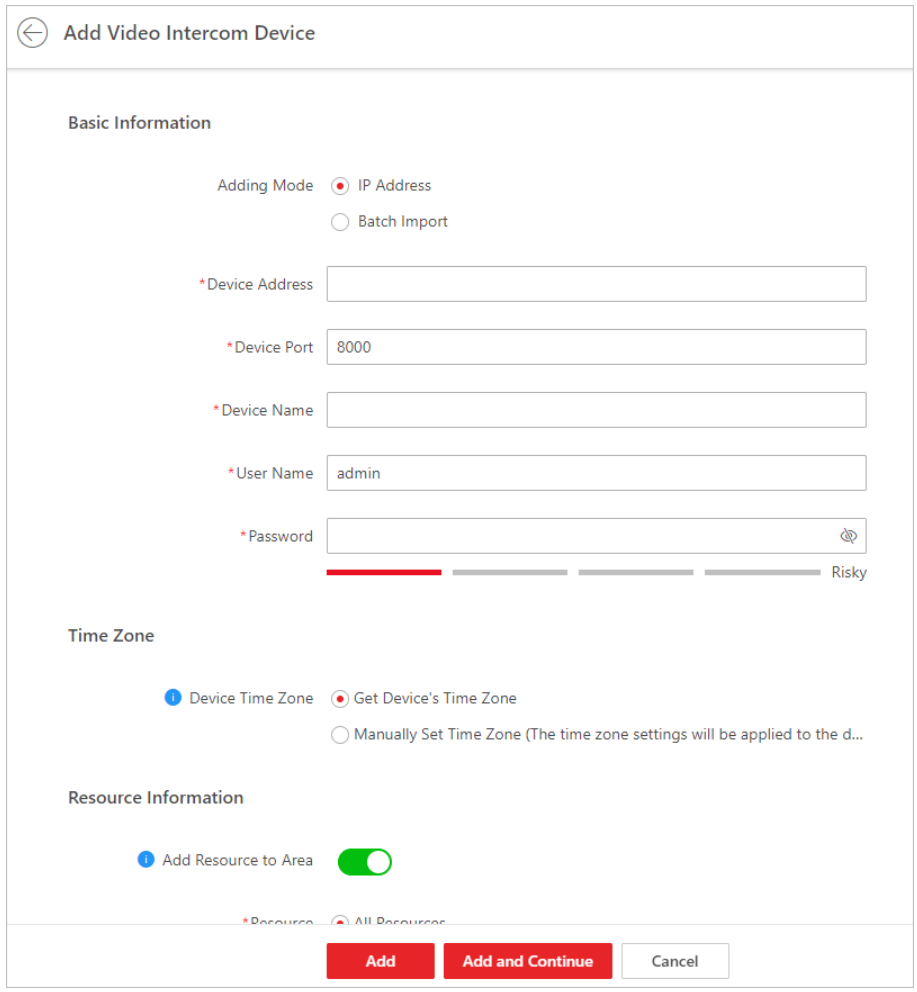


Figure 11-2 Add Video Intercom Device Page

5. Enter the required information.

Device Address

The IP address of the device.

Device Port

By default, the device port No. is 8000.

Device Name

Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

Password

The password required to access the account.

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 installer and/or end-user.

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

   Note

   You can click **View** to view the details of the current time zone.
7. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

   Note

   - You can import all the alarm inputs or the specified alarm input to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform further operations for the alarm inputs.
8. **Optional:** Check **Restore Default Settings** to restore all the parameters of the device configured on the system to default settings.
9. Finish adding the device.
   - Click **Add** to add the device and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add the next device.
10. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click 🔑 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.

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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

11.5.3 Add Video Intercom Devices in a Batch

You can add video intercom devices in a batch to the system by entering the device information to the predefined template and importing the template to the system.

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.

Steps
1. On the top, select **Device**.
2. Select **Device and Server → Video Intercom Device** on the left.
3. Click **Add** to enter Add Video Intercom Device page.
4. Click **Batch Import** as the adding mode.
5. Click **Download Template** to save the predefined template (Excel file) on your PC.
6. Open the exported template file and enter the required information of the devices to be added.
7. Click and select the template file.
8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

     Note
     You can click **View** to view the details of the current time zone.
9. Finish adding the devices.
   - Click **Add** to add the video intercom devices in a batch, and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add other video intercom devices.

10. Optional: Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 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.
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click 🔍 to search for a specific device.

11.6 Network Transmission Device Management

Network transmission devices (switch, network bridge and fiber converter) can be added to the system for management, to help the system monitor the network status of the managed devices.

After the network transmission devices are added to the system, the Web Client will automatically draw a network topology according to the location of the added devices, and display the information (IP address, port No., port status and stream rate) and network link status (fluent, busy, congested, disconnected).

11.6.1 Add Detected Online Network Transmission Devices

The system can perform an automated detection for available network transmission device s in the network where the Web Client or server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

You can add one online devices at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Network Transmission Device

When you want to add one of the detected online devices or add some of these devices with different user names and passwords, you need to select only one device every time to add it to HikCentral Access Control. The IP address, port number and user name will be recognized automatically, which can reduce some manual operations in a way.

Before You Start

Make sure the network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Access Control via network.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Network Transmission Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

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

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
4. In the Online Device area, select the active device to be added.
5. Click **Add to Device List** to open the Add Network Transmission Device window.
6. Set the required information.

   Device Address

   The IP address of the device, which is filled in automatically.

   Device Port

   The port number of the device, which is filled in automatically.

Device Name

Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Access Control using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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 installer and/or end-user.

Country Code

The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- You cannot edit the country code of the added device on its details page.

7. Click **Add**.
8. **Optional:** Perform the following operations after adding the device.

Remote Configuration	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the 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.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

Add Detected Online Network Transmission Devices in a Batch

For the detected online transmission network devices, if they have the same user name and password, you can add multiple devices to HikCentral Access Control at a time.

Before You Start

Make sure the network devices (switches, bridges or fiber converters) 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.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Network Transmission Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

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

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
4. In the Online Device area, select the devices to be added.
5. Click **Add to Device List** to enter the Add Online Device window.
6. Enter the user name, password, and country code.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Access Control using the non-admin account, your permissions may restrict your access to certain features.

   Password

The password required to access the account.

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 installer and/or end-user.

Country Code

The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- For the added device, its country code cannot be edited on the device details page.

7. Click **Add**.

8. Optional: Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the 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.
Set the System Connected Device	Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

11.6.2 Add Network Transmission Device by IP Address

When you know the IP address of a device, you can add it to the system by specifying the IP address, user name, password, etc.

Before You Start

Make sure the network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Access Control via network.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Network Transmission Device** on the left.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

Device Address

IP address of the device.

Device Port

The default device port number is 8000.

Device Name

Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

User Name

The administrator account which is created when activating the device, or the non-administrator account, such as operator. When adding device by non-administrator, the permission might be limited.

Password

The password required to access the account.

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 installer and/or end-user.

Country Code

The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- Once the device is added, its country code cannot be edited on the device details page.

6. Finish adding the device.
- Click **Add** to add the current device and back to the device list page.
- Click **Add and Continue** to finish adding the current device and continue adding other devices.

7. Optional: Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the 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.
Set the System Connected Device	Select the device, click **System Connected Switch** to set the switch as the system connected device. **Note** System connected switch is the switch that is directly connected with the SYS server.

11.6.3 Import Network Transmission Devices in a Batch

If there are a large number of devices to be added, you can enter the device information in the pre-defined template and upload the template to add the network transmission devices in a batch.

Before You Start

Make sure the network devices (switches, bridges or fiber converters) 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.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Network Transmission Device** on the left.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select the adding mode as **Batch Import**.
5. Click **Download Template** to download the template to the local PC.
6. Open the downloaded template file, and enter the required device information.
7. Click to select the edited template file.
8. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.
   - Click **Add and Continue** to finish adding the current device and continue adding other devices.
9. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the 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.
Set the System Connected Device	Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

11.7 Add pStor

You can add a pStor server as a recording server to the HikCentral Access Control for storing the videos and pictures.

Before You Start

- Make sure the pStor servers 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.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Recording Server** on the left.
3. Click **Add** to enter the Add Recording Server page.

   Note

   If the NTP server is not configured, a prompt message will appear on the top of the page. You can click **Configure** to set the time synchronization.
4. Select **pStor**.
5. Enter the network parameters.

   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 encoding 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.
6. **Optional:** Check **ANR Function** or not.

Note

This function is enabled default. If the network is disconnected between the pStor and the encoding device, data can be stored on the pStor automatically.

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

Note

You can download these two keys on the pStor server's Web Client page.

8. **Optional:** Switch on **Enable Picture Storage** for storing pictures in this pStor.

Note

You should set picture downloading port No..

9. Enter the name, user name, and password of the pStor 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 installer and/or end-user.

10. Finish adding the server.
    - Click **Add** to add the server and back to the server list page.
    - Click **Add and Continue** to save the settings and continue to add other servers.
11. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server and you can edit the information of the server and view its storage and camera information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click ⚙ in the Operation column to enter the login page of the pStor server. You can log in and configure the pStor server.
Search for Server	Enter keyword(s) in the search box in the top right corner to search for the target server(s).

11.8 Upgrade Device Firmware

You can upgrade the firmwares of the devices added to the system via the current Web Client or Hik-Connect.

Via Current Web Client

The following devices are supported to be upgraded the firmwares via the current Web Client:

- Access Control Device
- Card Reader
- Indoor Station
- Door Station

Note

Upgrading the card reader linked to the door station is not supported.

- Main Station

Via Hik-Connect

The following devices are supported to be upgraded the firmwares via Hik-Connect:

- Indoor Station
- Door Station

Note

Upgrading the card reader linked to the door station is not supported.

- Main Station

11.8.1 Upgrade Device Firmware via Current Web Client

You can upgrade device firmware via the current Web Client.

Steps

1. On the top, select **Device**.
2. Select **Firmware Upgrade** on the left.
3. Select the **Via Current Web Client** tab.
4. In the **Upgrade By** field, select the upgrade method.
5. In the **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
6. Select an upgrade package from the local computer and then click **Next**.

   The upgradable devices will be displayed.
7. **Optional:** Filter devices by device type, device firmware version, or device model.
8. Select device(s) and then click **Next**.
9. Select an upgrade schedule to upgrade the selected device(s).
   - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
   - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).

10. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be displayed.
11. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

11.8.2 Upgrade Device Firmware via Hik-Connect

You can upgrade device firmware via Hik-Connect, which is a cloud service.

Steps

1. On the top, select **Device**.
2. Select **Firmware Upgrade** on the left.
3. Select the **Via Hik-Connect** tab.
4. In the **Device Access Protocol** field, select the relevant protocol.
5. 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.
6. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
7. Click **Next**.
8. 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.

   The upgradable devices will be displayed.
9. Select device(s) and click **Next** to enter the upgrade schedule page.
10. Select an upgrade schedule to upgrade the selected device(s).
    - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
    - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).
11. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be open.
12. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

11.8.3 Upgrade Device Firmware via FTP

You can upgrade device firmware via FTP.

Steps

1. On the top, select **Device**.
2. Select **Firmware Upgrade** on the left.
3. Select the **Upgrade Firmware via FTP** tab.
4. 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 installer and/or end-user.

   Path

   If you saved 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.
5. Click **Next**.
6. Select an upgrade package from the local PC and then click **Next**.

   The upgradable device list will be displayed.
7. **Optional:** Filter devices by device type, device firmware version, or device model.
8. Select a device type and select a device from the device list.
9. **Optional:** If you select Dock Station as the device type, you need to select an upgrade object from the drop-down list.
10. Select **Upgrade Now** or **Custom** as the upgrading schedule.
11. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be displayed.
12. **Optional:** In the upper-right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.
13. **Optional:** In the upgrade task list, click × in the Operation column to delete the upgrade task.

11.9 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.

For detailed operations of restoring device's default password, refer to ***Restore Device's Default Password*** .

For detailed operations of resetting device's password, refer to ***Reset Device Password*** .

11.9.1 Reset Device Password

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

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.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to reset the device's password.

Steps

1. On the top, select **Device**.
2. Select **Device and Server** on the left, and then select a device type.
3. 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.

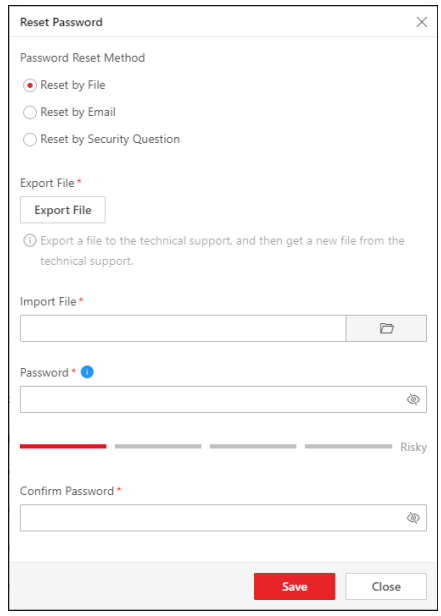


Figure 11-3 Reset Password

4. Select a password reset method:

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 installer and/or end-user.

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

11.9.2 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.

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.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operations about activating devices.

Perform this task when you need to restore the device's default password.

Steps

1. On the top, select **Device**.
2. Select **Device and Server** on the left, and then select a device type.
3. In the Online Device area, view the device status (shown on Security column) and click in the Operation column of an active device.

   A dialog with security code pops up.
4. Enter the security code and restore the default password of the selected device.

Note

Contact our technical support to obtain a security code.

What to do next

You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

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 installer and/or end-user.

Chapter 12 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, on the 1st floor, there mounted 64 cameras, 16 access points, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named 1st Floor) for convenient management. You can get the live view, play back the video files, and do some other operations of the devices after managing the resources by areas.

12.1 Add an Area

You can add an area to manage the devices.

Steps

1. On the top, select **Device**.
2. Click **Area** on the left.
3. Optional: Select the parent area in the area list panel to add a sub area.
4. Click + on the area list panel to open the Add Area panel.

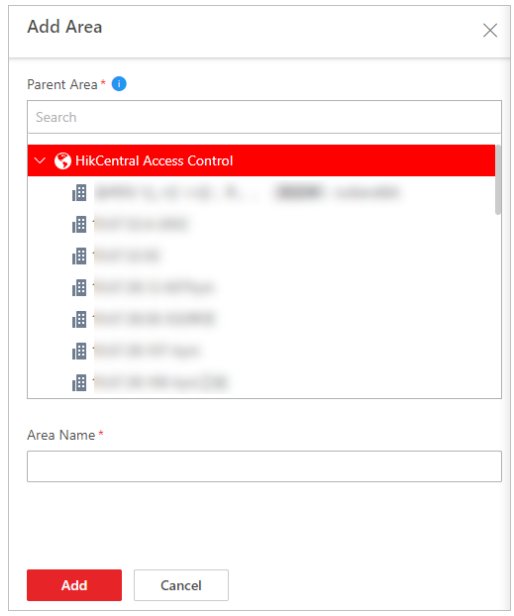


Figure 12-1 Add Area

5. Select the parent area to add a sub area.
6. Create a name for the area.
7. Click **Add**.
8. Optional: After adding the area, you can do one or more of the following:

Edit Area	Hover the cursor on a specific area and click ··· → **Edit** to edit the area.

Delete Area Select an area and click 🗑 or hover the cursor on an area 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.

Note

After deleting the area, the resources in the area will be removed from the area.

Search Area Enter a keyword in the search field of the area list panel to search for the area.

Move Area Drag the added area to another parent area as the sub area.

Stick on Top Hover the cursor on a specific area and click ··· → **Stick on Top** → to stick the area to the top.

Note

The order of the parent area will not be changed.

Remove from Top Hover the cursor on a specific area and click ··· → **Remove from Top** to restore the area order to the default (name order).

12.2 Add Element to Area

You can add elements to areas for management, including doors, elevators, alarm inputs, and alarm outputs.

12.2.1 Add Door to Area

You can add doors to areas for management.

Before You Start

The access control devices need to be added to the HikCentral Access Control for area management. Refer to ***Manage Access Control Device*** for details.

Steps

Note

One door can only belong to one area. You cannot add one door to multiple areas.

1. On the top, select **Device**.
2. Select **Area** on the left.
3. **Optional:** Select an area for adding doors to the area list panel.
4. Select the **Door** tab.
5. Click + on the element page to enter the Add Door page.

6. Select the device type.
7. Select the door(s) to be added.
8. Optional: Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.

The added door(s) will be displayed in the list.

10. Optional: After adding the doors, you can do one or more of the following.

Synchronize Door Name	Select the doors and click ↑↓ to synchronize the doors' names from the device in a batch. **Note** You can only synchronize the door name of online HIKVISION device.
Apply Door Name	Select the doors and click to apply the doors' names to the device in a batch.
Move to Other Area	Select the doors and click . Then select the target area to move the selected doors to and click **Move**.
Set Geographic Location	Click to enter Map Settings page and drag the door to the map. See ***Add Hot Spot on Map*** for details.
Display Doors of Sub Areas	Check **Include Sub-area** to display the doors in sub areas.
Filter by Device Type	Click and check the device type in the drop-down list to filter the doors.
Search for Doors	Enter the keywords in the Search field to search for doors.

12.2.2 Add Elevator to Area

You should add elevator to areas for further management.

Before You Start

The elevator control devices need to be added to the HikCentral Access Control for area management. Refer to ***Manage Elevator Control Device*** for details.

Steps

Note

One elevator can only belong to one area. You cannot add an elevator to multiple areas.

1. On the top, select **Device**.
2. Click **Area** on the left.
3. **Optional:** Select an area for adding elevators to in the area list panel.
4. Select the **Elevator** tab.
5. Click + to enter the Add Elevator page.
6. In the **Elevator Control Device** field, all the added elevator control devices are displayed. Select the device to add the elevator to.
7. In the **Range of Floor No.** field, enter the start No. and end No. of the floors that you want to import to the area.

   The floors between the start No. and end No. will be imported to the area. After imported, you can manage the floors in the system, such as adding to access levels, controlling status, etc.
8. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
9. Click **Add**.
10. **Optional:** After adding the elevator, you can do one or more of the followings.

Get Floor Name	Select the elevator and click ↑↓ to get the floors' names of the elevator from the device in a batch.
Apply Floor Name	Select the elevator and click to apply the elevator's floors names to the device in a batch.
Move to Other Area	Select the elevators and click . Then select the target area to move the selected elevators to and click **Move**.
Set Geographic Location	Click to enter the Map Settings page and drag the elevator to the map. See ***Add Hot Spot on Map*** for details.
Display Elevators of Sub Areas	Check **Include Sub-Area** to display the elevators of sub areas.
Search for Elevators	Enter the keywords in the Search field to search for elevators.

12.2.3 Add Alarm Input to Area

You can add alarm inputs to areas for management.

Before You Start

The devices need to be added to the HikCentral Access Control for area management. Refer to ***Resource Management*** for details.

Steps

Note

One alarm input can only belong to one area. You cannot add an alarm input to multiple areas.

1. On the top, select **Device**.
2. Click **Area** on the left.
3. **Optional:** Select an area for adding alarm inputs to.
4. Select the **Alarm Input** tab.
5. Click + to enter the Add Alarm Input page.
6. Select the device type.
7. Select the alarm inputs to add.
8. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.
10. **Optional:** After adding the alarm inputs, you can do one or more of the followings.

Delete Alarm Input	Select the alarm input(s) and click **Delete**.
Move to Other Area	Select the alarm input(s) and click . Then select the target area to move the selected alarm inputs to and click **Move**.
Add Alarm Input to Map	Click to enter Map Settings page and drag the alarm input to the map. See ***Add Hot Spot on Map*** for details.
Display Alarm Inputs of Sub Areas	Check **Include Sub-Area** to display the alarm inputs of sub areas.
Filter Alarm Inputs by Device Type	Select the device type(s) to be displayed in the list from the drop-down list to the left of the search box.
Search for Alarm Inputs	Enter the keywords in the Search field to search for alarm inputs.

12.2.4 Add Alarm Output to Area

You can add alarm outputs to areas for management. 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.

Before You Start

The devices need to be added to the HikCentral Access Control for area management. Refer to ***Resource Management*** for details.

Steps

Note

One alarm output can only belong to one area. You cannot add an alarm output to multiple areas.

1. On the top, select **Device**.
2. Click **Area** on the left.
3. **Optional:** Select an area for adding alarm outputs to.
4. Select the **Alarm Output** tab.
5. Click + to enter the Add Alarm Output page.
6. Select the device type.
7. Select the alarm outputs to add.
8. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.
10. **Optional:** After adding the alarm outputs, you can do one or more of the followings.

Delete Alarm Output	Select the alarm output(s) and click **Delete**.
Move to Other Area	Select the alarm outputs and click . Then select the target area to move the selected alarm outputs to and click **Move**.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page and drag the alarm output to the map. See ***Add Hot Spot on Map*** for details.
Display Alarm Outputs of Sub Areas	Check **Include Sub-Area** to display the alarm outputs of sub areas.
Search for Alarm Outputs	Enter the keywords in the Search field to search for alarm outputs.

12.3 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.

12.3.1 Edit Door

You can edit the basic information, related cameras, image storage settings, card reader settings, and face recognition terminal settings of a door.

Steps

1. On the top, select **Device**.
2. Click **Area** on the left.
3. In the area list panel, select one area.
4. Select the **Door** tab to show the added doors in this area.
5. Click a door's name in the **Name** column to enter the door editing page.
6. Edit the door's 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

After 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 ended.

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 configured with 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 with 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 with 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 with the duress code and supper password.

7. **Optional:** Switch on **Picture Storage** and select a storage location from the drop-down list.

Note

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

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

Min. Card Swipe Interval

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

Reset Entry on Keypad after

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 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 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.

Iris Recognition Interval

The time interval between two continuous face recognitions when authenticating.

Iris 1:N Security Level (Single-Eye)

Set the matching threshold when authenticating via 1:N matching single-eye mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Iris 1:N Security Level (Dual-Eye)

Set the matching threshold when authenticating via 1:N matching dual-eye mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Mask Detection

After being switched on, you can choose whether to enable **Not Allowed Without Mask** to restrict the passage of those not wearing masks.

Note

The parameters displayed vary according to the model of the access control device. For details about the parameters, refer to the user manual of the device.

9. **Optional:** For a turnstile or an access controller of certain types, set the **Face Recognition Terminal** switch to on and add face recognition terminals to link with the selected turnstile.
   1) Click **Add** to enter the Add Face Recognition Terminal page.
   2) Select **IP Address**, **Online Devices**, or **Device ID** as the adding mode, and set the required parameters, which may vary according to different terminals.
   3) Click **Add** to link the terminal to the turnstile or access controller.
10. **Optional:** Click **Copy To** in the upper right corner to apply the current settings of the door to other door(s).
11. Click **Save**.

12.3.2 Edit Elevator

You can edit basic information, floor information, related cameras, card reader settings of the elevator.

Steps

1. On the top, select **Device**.
2. Click **Area** on the left.
3. In the area list panel, select one area.
4. Select the **Elevator** tab to show the added elevators in this area.
5. Click an elevator's name in the **Name** column to enter the elevator editing page.
6. Edit the elevator's basic information.

   Name

   Edit the name for the elevator.

   Note

   If you changes the name, you can click in the elevator list page to apply the new name to the device.
7. In the Floor panel, all the imported floors will be displayed in the list. You can edit the floor's name or reset the imported floor No.

Edit Floor Name

You can edit the floor name if needed.

Note

If you changes the name, you can click **Apply Floor Name** in the elevator list page to apply the new name to the device.

Reset Imported Floor No.

You can click **Reset Imported Floor No.** and enter the range of the floor No. to reset the settings of the floors, such as schedule settings, name, access level settings, etc.

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

Min. Card Swipe Interval

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

Reset Entry on Keypad after

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 enabled, if the door has 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 enabled, if the door has 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.

Buzzer Polarity

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

Fingerprint Security Level

Select the fingerprint security level. The higher is the security level, the lower is the face acceptance rate (FAR). The higher is the security level, the higher is the false rejection rate (FRR).

Note

The parameters displayed vary according to the model of the access control device. For details about the parameters, refer to the user manual of the device.

9. **Optional:** Click **Copy to** in the upper right corner to apply the current settings of the elevator to other elevator(s).
10. Click **Save**.

12.3.3 Edit Alarm Input

You can edit the basic information of alarm input and relate detector to the security control panel's alarm input.

Steps

1. On the top, select **Device**.
2. Click **Area** on the left.
3. In the area list panel, select one area.
4. Select the **Alarm Input** tab to show the added alarm inputs.
5. Click an alarm input name in the **Name** column to enter the Edit Alarm Input page.
6. Edit the alarm input name.
7. Click **Save**.

12.3.4 Edit Alarm Output

You can edit the alarm output name.

Steps

1. On the top, select **Device**.
2. Click **Area** on the left.
3. In the area list panel, select one area.
4. Select the **Alarm Output** tab to show the added alarm outputs.
5. Click an alarm output name in the **Name** column.
6. Edit the alarm output name in the pop-up window.
7. Click **Save**.

12.4 Remove Element from Area

You can remove the added doors, elevators, alarm inputs, alarm outputs, from the area.

Steps

1. On the top, select **Device**.
2. Click **Area** on the left.
3. **Optional:** Select an area in the area list panel to show its added elements.

4. Select the , **Door**, **Elevator**, , **Security Radar**, **Alarm Input**, or **Alarm Output** tab to show the added elements.
5. Select the elements.
6. Click 🗑 to remove the elements from the area.

Chapter 13 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.

13.1 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. On the top, select **Person**.

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

3. Click + at the top of the department list to enter the Add Department page.

4. Set the department information, including the parent group, group name, and description.

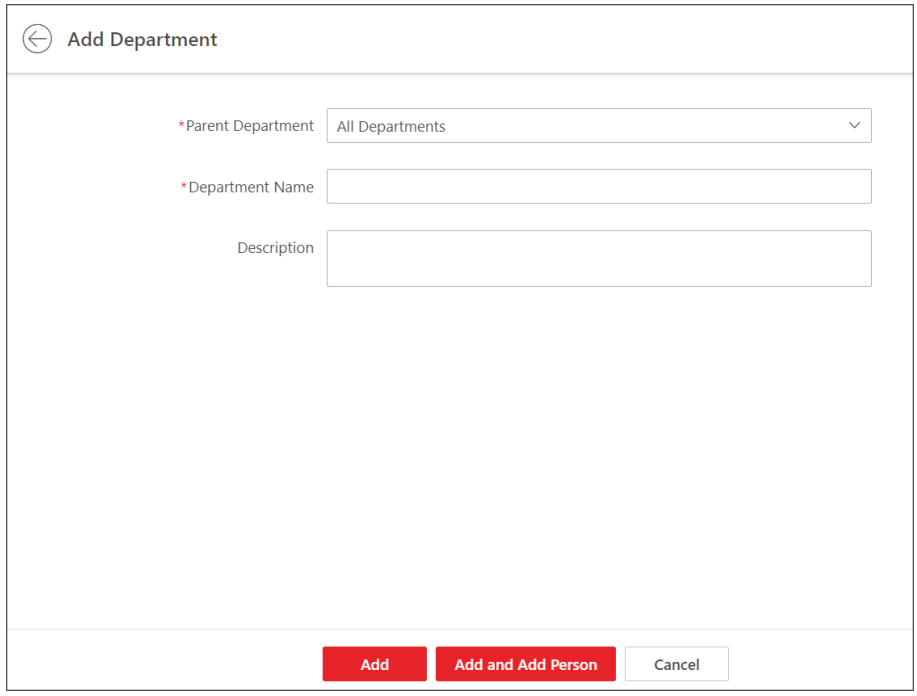


Figure 13-1 Add Department

5. 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.

6. 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 group, group 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.

13.2 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 access control devices/video intercom devices/ enrollment stations. In addition, you can batch add profile pictures for persons, and import domain persons.

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 ***Set Person ID Rule*** .

You can perform the following operations for adding person.

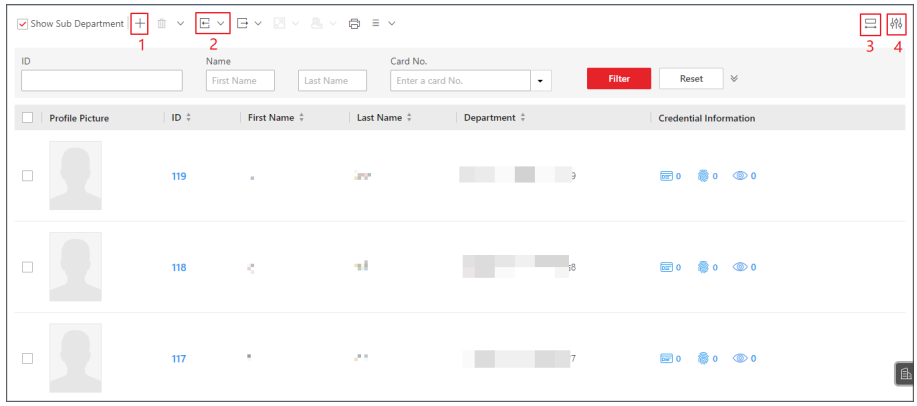


Figure 13-2 Introduction to Adding Person

1. You can click + to add a single person. For details, refer to ***Add a Person Manually*** .
2. You can click to perform the following operations.

- Batch import persons by template. For details, refer to ***Batch Add Persons by Template***
- Import users in the AD (Active Directory) domain to the platform as persons. For details, refer to ***Import Domain Persons*** .
- Import person pictures. For details, refer to ***Import Profile Pictures*** .
- Import persons information to the platform from devices, including access control devices, video intercom devices, or enrollment station. For details, refer to ***Import Persons from Access Control Devices or Video Intercom Devices*** or ***Import Persons from Enrollment Station*** .

3. On the top-right corner, click ⇔ to select the type of self-adaptive column width (complete or incomplete display of each column title).
4. On the top-right corner, click ⚙ to select the items for custom display in the column.

13.2.1 Add a 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, the elevator control application, the attendance management application, and the video intercom application.

Steps

1. On the top, select **Person**.

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

3. Select a department from the department list on the left.

All persons in the selected department will be displayed on the right. You can check **Show Sub-Group** to display the persons in sub departments (if any).

4. Click + at the top of person list to enter the Add Person page.

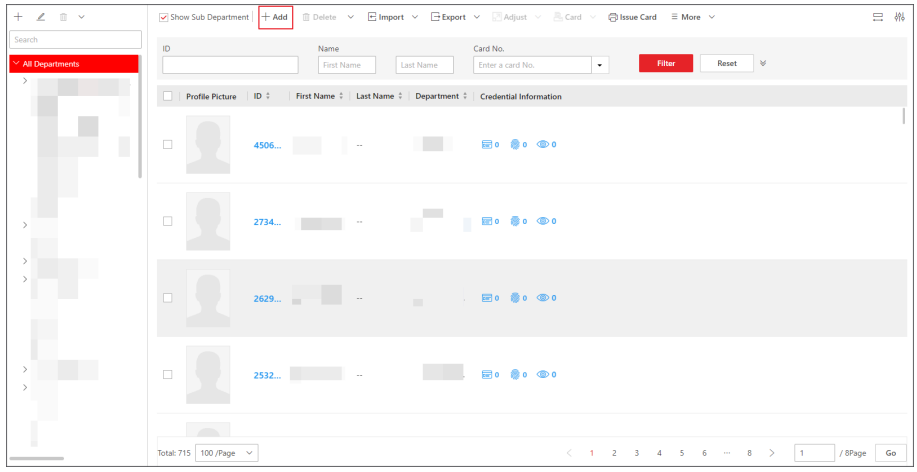


Figure 13-3 The Entry for Adding a Person

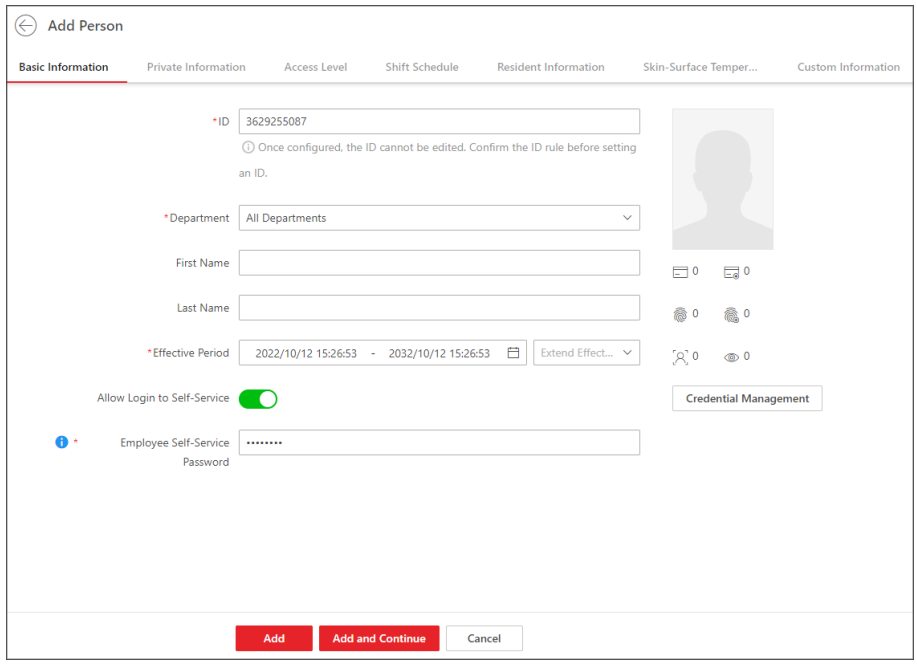


Figure 13-4 Add Person Page

5. 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.

Note

The ID cannot be edited after finishing adding a person, so you should ensure its correctness at the beginning.

Department (Required)

Select a department for the person.

Note

See ***Add Departments*** for details about how to add a department.

Profile Picture

Hover the cursor onto , and you can select from three modes to add a picture.

From Device

You can select **Access Control Device**, **Video Intercom Device**, or **Enrollment Station** and set parameters (if required) to connect the device to the platform, and then collect the face picture via the 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.

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.

Effective Period (Required)

Set the effective period for the person in applications such as access control application and time & attendance 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***.

Allow Login to Self-Service

Switch on **Allow Login to Self-Service** to allow employee to log in to self-service on the platform. For details, refer to ***Login via Web Client (Employee)*** .

Employee Self-Service Password

After enabling **Allow Login to Self-Service** for the employee self-service, set the password.

Note

By default, the password is the employee ID if the password has not been set. Once the password is modified, the new password should be set according to the password verification rule.

6. Add credential information for the person. See ***Manage Credentials*** for details.

Note

- You can click in the Credential Information column to add or edit the card information.
- You can click in the Credential Information column to add or edit the fingerprint information.
- You can click in the Credential Information column to add or edit the iris information.
- If you have added the QR code(s) for the person, you can click in the Credential Information column to download the QR code.

7. Set the person's private information, such as email, and phone No.
8. Assign access levels to the person to define the access points where the person can access during the authorized period.

Super User

If the person is set as a super user, the person 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.

Open Door via Bluetooth on Mobile Client

Check the box to open enable opening door via bluetooth on the Mobile Client.

PIN Code

Set the PIN code for access authentication. 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**.

Note

- 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

a. Click **Assign**.
b. Select one or more access levels for the person.
c. Click **Assign** to add the person to the selected access level(s).

Note

You can click to view information on access points and access schedules.

9. **Optional:** View schedule of the person in the table.

Note

You can click ‹ or › to switch the time (month).

10. **Optional:** Set resident information to link the person with the indoor station and room number.

Note

- Make sure you have added indoor stations to the platform.
- 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.

11. 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.

12. In Custom Public Information area, select custom information to be applied.

Note

Make sure you have set the custom public information. See ***Customize Additional Information*** for details.

13. Finish adding the person.
- Click **Add**.
- Click **Add and Continue** to finish adding the person and continue to add other persons.

The person will be displayed in the person list and you can view the details.

14. **Optional:** After adding persons, 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 to delete the selected person(s).
Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.

Clear Profile Pictures

Hover the cursor onto ⌄ beside 🗑 , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Export Person Information

Click ⇥ → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.

Export Profile Pictures

Click ⇥ → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to **System** → **Security** → **Export Profile Pictures** page to check 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.
  a. Select one or more persons, click ⤢ → **Adjust Department** .
  b. Select the target department to which the persons are about to be moved.
  c. Click **Move**.
- Adjust the effective period for the person in applications.
  a. Select one or more persons, click ⤢ → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click ⤢ → **Adjust Effective Period** .
  b. Set the departure date, type, and reason..
  c. Click **OK**.

Synchronize Domain Persons

Select person(s) whose information has changed in the AD domain and click ≡ → **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, click ≡ → **Link to Indoor Station** and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- 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 ≡ → **Clear Access Level to Person** to clear the access levels of the selected persons.

Note

The access levels of these persons cannot be restored once they are cleared.

Monitor Access Levels

Select one or more persons, click ≡ → **Monitor Access Level to Person** to monitor the access levels of the selected persons.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

Manage Credentials

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

Steps

1. On the top, select **Person**.
2. Select **Person Management** → **Person** on the left.
3. On the adding or editing person page, click **Credential Management** under the profile picture to open the Add Credential pane.
4. 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.

Note

- 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*** .

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 to view and scan the QR code or click **Download** to download the QR code picture to the local storage for further operations.

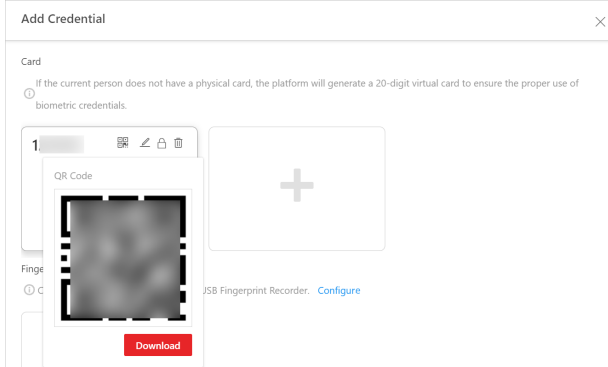


Figure 13-5 View QR Code of Card

5. 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.
6. **Optional:** In the Iris area, collect irises of the person.
   1) Click **Configure** to select a device used for collecting the person's irises.
   2) Click and then start collecting irises.
7. **Optional:** Switch on **Special Credential** and then add special cards and corresponding fingerprint information.
8. **Optional:** Perform the following operation(s).

Edit Card / Fingerprint / Iris Information	Hover the cursor onto an added card, fingerprint, or iris, and then click .
View and Download QR Code of Card	Hover the cursor onto an added card, and then click .
Delete Card / Fingerprint / Iris	Hover the cursor onto an added card, fingerprint, or iris, and then click .

9. Click **Save**.

13.2.2 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. On the top, select **Person**.
2. Select **Person Management → Person** on the left.
3. Click **→ Import Person Information via Excel** .

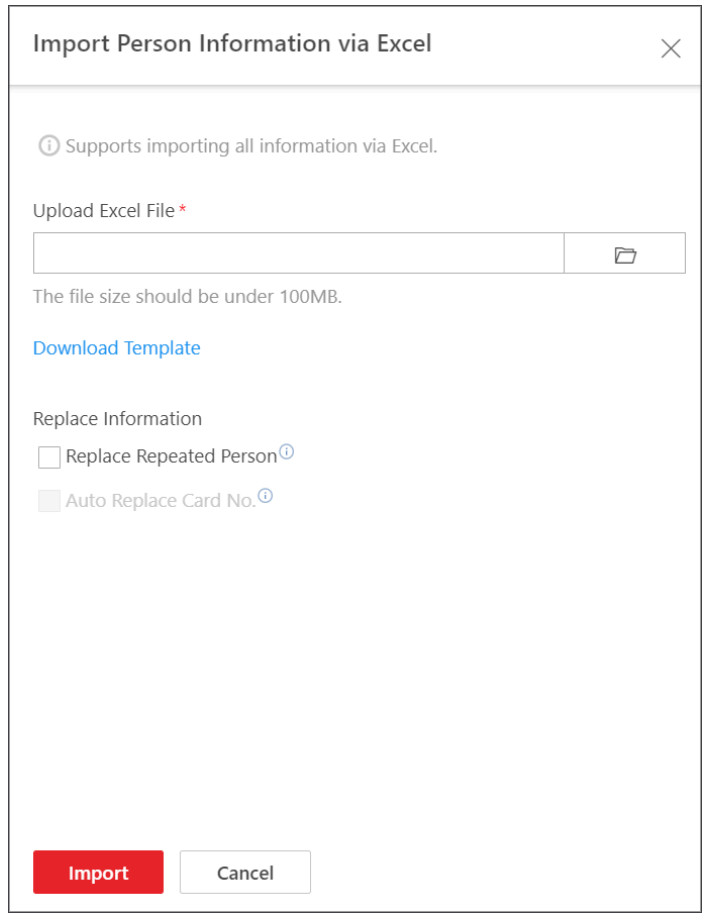


Figure 13-6 Batch Add Persons by Template

4. In the pop-up window, click **Download Template**.
5. 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. See ***Customize Additional Information*** for how to add custom additional information for persons.
6. Click **Download** to save the template to your PC.
7. In the downloaded template, enter the person information following the rules shown in the template.
8. Click , and then select the template from your PC.
9. **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.
10. **Optional:** Check **Auto Replace Card No.** to replace the card No. automatically if it already exists in the platform.
11. 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.

12. **Optional:** After adding persons, 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 to delete the selected person(s).
Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.
Clear Profile Pictures	Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.
Export Person Information	Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.
Export Profile Pictures	Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** To activate this function, you should go to **System** → **Security** → **Export Profile Pictures** page to check 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.

a. Select one or more persons, click → **Adjust Department** .
b. Select the target department to which the persons are about to be moved.
c. Click **Move**.

- Adjust the effective period for the person in applications.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click → **Resigned** .
  b. Set the departure date, type, and reason.
  c. Click **OK**.

Synchronize Domain Persons

Select person(s) whose information has changed in the AD domain and click → **Synchronize Domain Persons** at the top of person list to get the latest person information.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

13.2.3 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 top, select **Person**.
2. Click → **Import Person Information via Domain Group** to enter the Import Person Information via Domain Group page.
3. Select the importing mode.

   Import Domain Persons

   Import the 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.

Note

Make sure you have set security groups.

4. 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.
5. Set the effective period for the persons as needed.
6. Click **Import**.
7. **Optional:** Click the person name shown in the person list to view and edit the person information.

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. For linking the person information in the domain to the person information in the platform, refer to ***Set Active Directory*** .
- 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. For linking the person information in the domain to the person information in the platform, refer to ***Set Active Directory*** .

8. **Optional:** After adding persons, 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 to delete the selected person(s).
Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.
Clear Profile Pictures	Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Export Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to page to check 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.
  a. Select one or more persons, click → **Adjust Department** .
  b. Select the target department to which the persons are about to be moved.
  c. Click **Move**.
- Adjust the effective period for the person in applications.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Set the departure date, type, and reason..
  c. Click **OK**.

Synchronize Domain Persons

Select person(s) whose information has changed in the AD domain and click → **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, click → **Link to Indoor Station** and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- 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 ≡ → **Clear Access Levels to Person** to clear the access levels of the selected persons.

Note

The access levels of these persons cannot be restored once they are cleared.

Monitor Access Levels

Select one or more persons, click ≡ → **Monitor Access Levels to Person** to monitor the access levels of the selected persons.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

13.2.4 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.

13.2.5 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.

Steps

1. On the top, select **Person**.

2. Select **Person Management → To Be Reviewed** on the left.
3. Click → **Import Person Information from Device** .
4. Select **Access Control Device** or **Video Intercom Device** as the device type.
5. Select one or more devices from the device list.

Note

You can enter a key word (fuzzy search supported) in the search box to search the target device(s) quickly.

6. Select the importing mode.

All

Import all the persons stored in the selected devices.

Specified Employee No.

Specify the employee No. of up to five persons and import the persons to the platform.

7. Select a department to which the persons will be imported.
8. **Optional:** Check **Replace Profile Picture** to replace the existed person profile pictures with the new ones from the devices.
9. Click **Import** to start importing.

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.

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

Note

If not, skip this step.

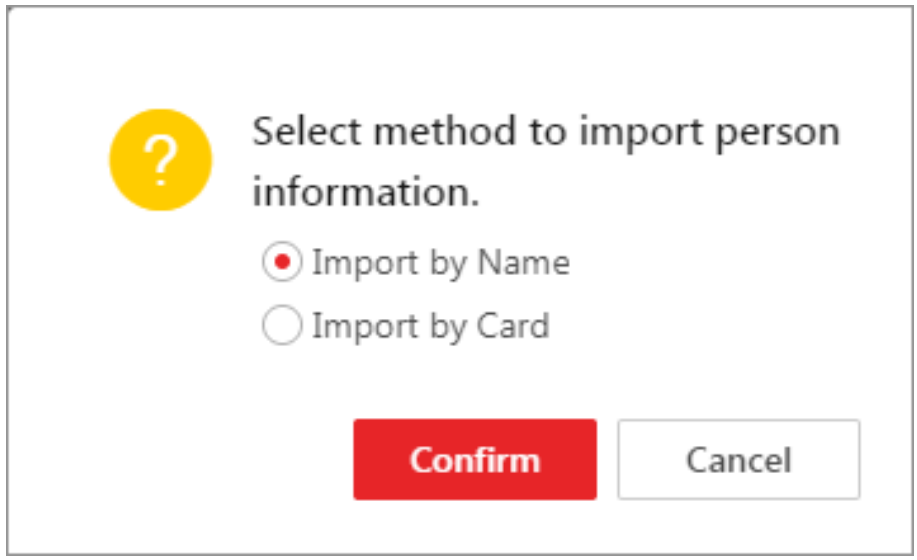


Figure 13-7 Select an Import Method

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.

11. **Optional:** 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 🗑 to delete the selected person(s).
Delete All Persons	Hover the cursor onto ⌄ beside 🗑 , and then click **Delete All** to delete all persons.
Clear Profile Pictures	Hover the cursor onto ⌄ beside 🗑 , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Export Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to page to check 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.
  a. Select one or more persons, click → **Adjust Department** .
  b. Select the target department to which the persons are about to be moved.
  c. Click **Move**.
- Adjust the effective period for the person in applications.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Set the departure date, type, and reason.
  c. Click **OK**.

Synchronize Domain Persons

Select person(s) whose information has changed in the AD domain and click → **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, click → **Link to Indoor Station** and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- 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 ☰ → **Clear Access Levels to Person** to clear the access levels of the selected persons.

Note

The access levels of these persons cannot be restored once they are cleared.

Monitor Access Levels

Select one or more persons, click ☰ → **Monitor Access Levels to Person** to monitor the access levels of the selected persons.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

13.2.6 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 You Start

Make sure you have enroll the persons' credentials via the enrollment station. For details, see ***Manage Credentials*** .

Steps

1. On the top, select **Person**.
2. Select **Person Management → To be Reviewed** on the left.
3. Click ⇦ → **Import Person Information from Device** .
4. Select **Enrollment Station** as the device type.

5. Set other parameters, such as access mode, device address, device port, and stage.

Device Address

Enter the IP address of the enrollment station from which the person information needs to be imported.

Device Port

Enter the port No. of the enrollment station from which the person information needs to be imported.

User Name

Enter the user name of the enrollment station from which the person information needs to be imported.

Password

Enter the password of the enrollment station from the person information needs to be imported.

6. Set importing stage and method.

Apply Person Information

The persons whose credentials need to be enrolled will be applied to the enrollment station.

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.

Copy Back Person and Credential Information

When the persons' credentials are enrolled, select the department to which the person and credential information will be imported to.

7. Click **Import** to start importing.

8. Optional: 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 to delete the selected person(s).
Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.

Clear Profile Pictures

Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Export Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to page to check 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.
  a. Select one or more persons, click → **Adjust Department** .
  b. Select the target department to which the persons are about to be moved.
  c. Click **Move**.
- Adjust the effective period for the person in applications.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Set the departure date, type, and reason..
  c. Click **OK**.

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, click **More → Link to Indoor Station** and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- 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 to Person** to clear the access levels of the selected persons.

Note

The access levels of these persons cannot be restored once they are cleared.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

13.3 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.
- The self-registration function is available when you purchase and activate any License.

13.3.1 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.

On the top, select **Person**. Select **Basic Configuration → Self-Registration Settings** on the left.

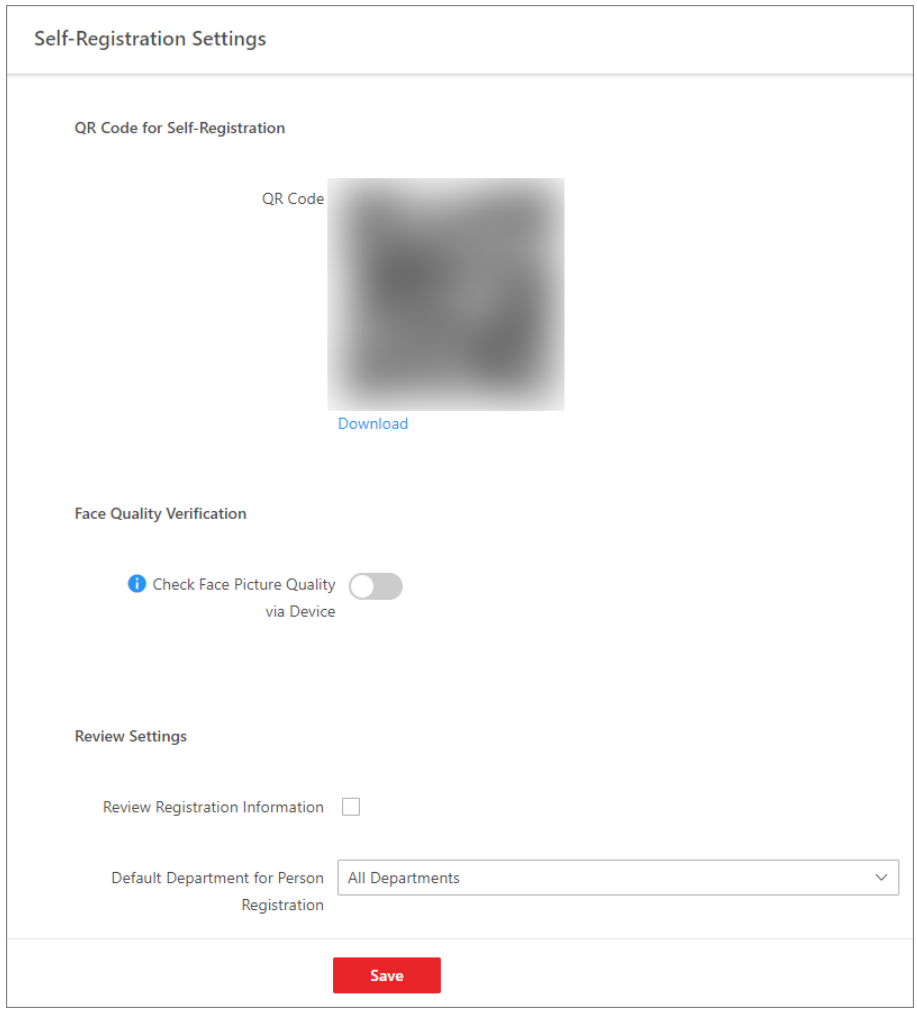


Figure 13-8 Self-Registration Settings

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.

13.3.2 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.

13.3.3 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.

Steps

1. On the top, select **Person**.
2. Select **Person Management → To be Reviewed** on the left.
3. **Optional:** Click to filter registered persons by name, ID, or status to quickly find your wanted persons.
4. Review the displayed person information and verify them.

Operations	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.
Self-Registration Settings	Click **Self-Registration Settings**, jumping to enter the Self-Registration Settings page to set self-registration parameters. **Note** For details, refer to ***Set Self-Registration Parameters*** .

Note

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.

13.4 Person Information Export

13.4.1 Export Person Information

Select person information and download it to the PC.

Steps

1. On the top, select **Person → Person Management → Person → Export → Export Person Information** .
2. Select the **Basic Information**, **Custom Additional Information**, **Access Level Information**, or **Schedule Information**, and click **Export**.

   The downloading task will be displayed in the Downloading Center.

13.4.2 Export Profile Pictures

Select persons and download their profile pictures to the PC if you need.

Note

Make sure you have enabled the Export Profile Pictures function on the **System → Security → Export Profile Pictures** .

On the top, select **Person → Person Management → Person → Export → Export Profile Picture** .

Enter the account's password, set a package password and confirm it. Click **Export**. The downloading task will be displayed in the Downloading Center.

13.5 Set Person ID Rule

Before adding persons, you should configure a rule to define the prefix No., total length, and whether using random digits for the person ID.

Steps

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.

1. On the top, select **Person**.
2. Select **Basic Configuration → Person ID Rule** on the left.
3. Enter a prefix No. and set the total length.
4. **Optional:** Check **Random ID** to generate the ID (excepts the fixed prefix No.) with random digits.

Example

If you enter ***10*** as the prefix No. and set the total length to 8, all the person IDs will start from "10", such as "10125454" (when **Random ID** is checked) and "10000001" (when **Random ID** is unchecked).

5. Click **Save**.

13.6 Customize Additional Information

You can add additional information items as the options for configuring a person's basic information. The platform allows you to customize two types of additional information items: custom private information items and custom public information items. 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.

The following figure shows the custom private information items (marked in red rectangles) on the Add Person page. See ***Add a Person Manually*** for details about how to add a person.

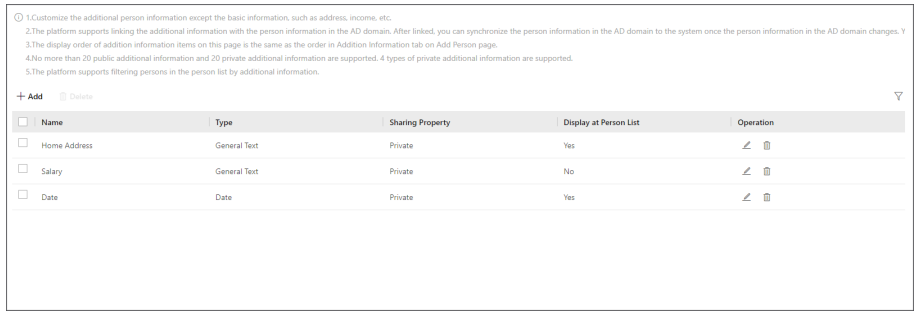


Figure 13-9 Custom Private Information Item as Configuration Option

Steps

Note

- You can customize up to 20 private information items and 20 public information items.
- The system administrator can define whether a user has the permission to view the custom private information when setting permissions for a user (see ***Add Role***). For information security, the system administrator needs to make sure the custom private information is only viewable to specific users.

1. On the top, select **Person**.

2. Select **Additional Information** on the left.

3. Click **Add**.

4. In the pop-up window, enter the following parameters.

Name

Create a name for the item. You can enter up to 32 characters.

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.

Example

For example, if you select **General Text**, entering text information as the content of the item is required 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).

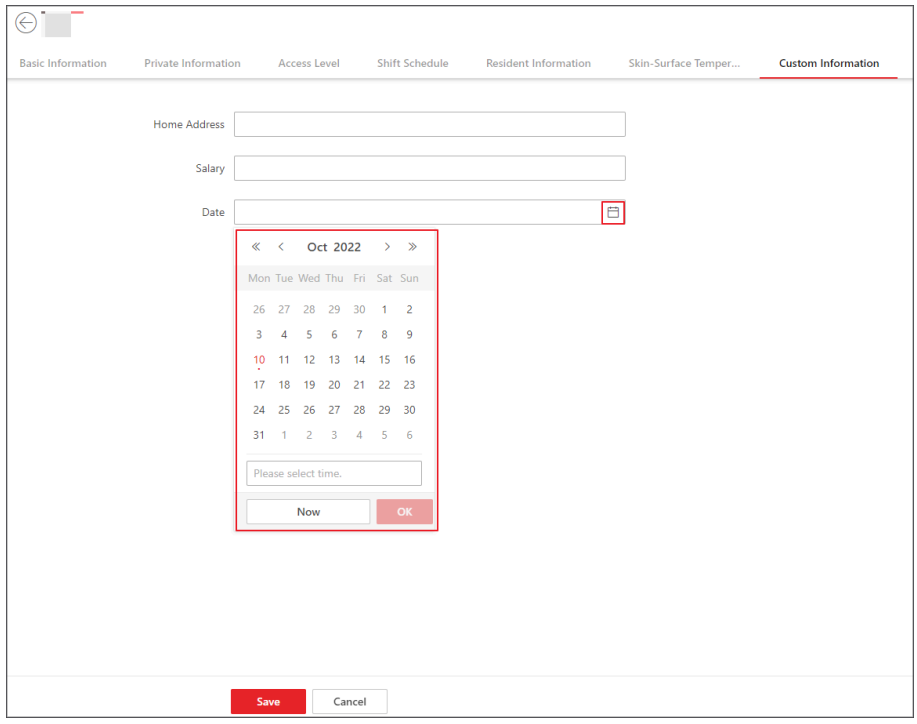


Figure 13-10 If You Select Date as the Type

Display at Person List

Click **Yes** or **No** to display or not display the custom additional information at the person list.

5. Click **Add**.
6. **Optional:** Perform the following operation(s) if needed.

Edit Name Click to edit the name of the additional information item.

Delete Click to delete the additional information item.

Note

You cannot delete the additional information item linked with person information in the domain.

13.7 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. On the top, select **Person**.
2. Select **Person Management → Person** on the left.
3. Select persons to whom the cards will be issued.
4. Move the cursor onto , and then click **Batch Issue Cards to Persons**.
5. 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*** .

6. 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 **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.

7. Click **Start** to start issuing cards.
8. 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.

9. Click **Save**.

13.7.1 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. On the top, select **Person**.
2. Select **Person Management → Person** on the left.
3. 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.

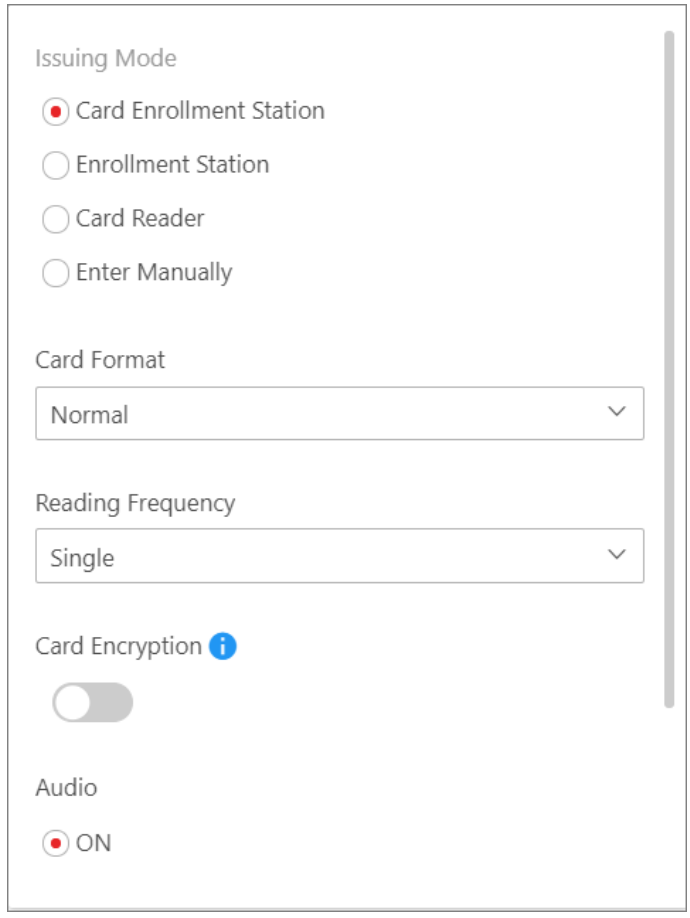


Figure 13-11 Card Issuing Settings Window Opened when Batch Issuing Cards to Persons

4. 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 Format

If the card 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 format, 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

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

13.8 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. On the top, select **Person**.
2. Select **Person Management → Person** on the left.
3. Optional: Set conditions to search for the target persons.
4. Select the persons for whom you need to print cards.

5. Click to open the Print Card window.

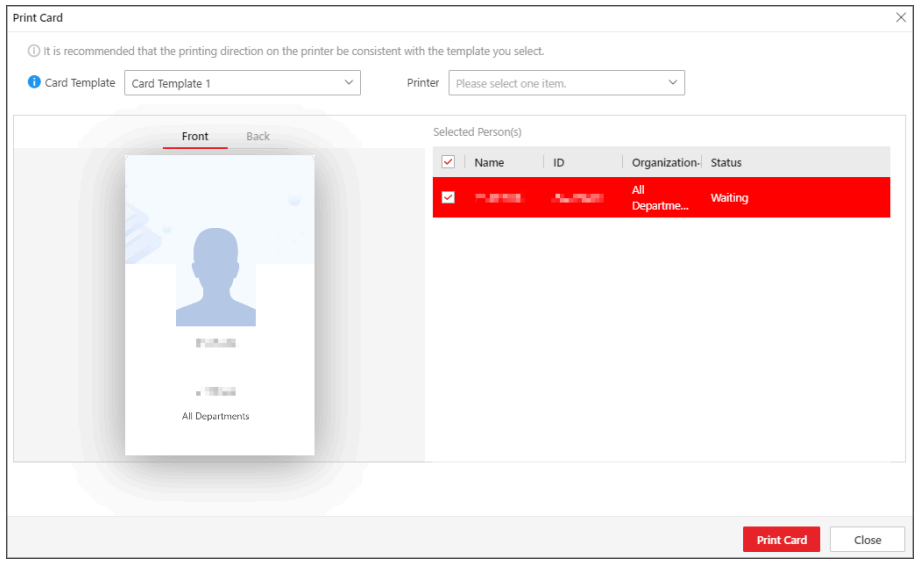


Figure 13-12 Print Card Window

6. Select a card template from **Card Template**.
7. Select a printer from **Printer**.
8. Select person(s) from the Selected Person list.
9. Click **Front** and **Back** to preview the information to be printed on the front and back of the physical cards.
10. 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.

Related Information Add a Person Manually

13.9 Report 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.

13.9.1 Report Card Loss

If a person cannot find her/his card, you can report card loss via the platform to freeze the access levels related to the card.

Steps

1. On the top, select **Person**.
2. Select **Person Management → Person** on the left.
3. **Optional:** On the Filter pane, click and set more conditions to search for persons for whom you want to report card loss.
4. 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.
5. In the Card area, move the cursor onto the lost card and then click .
6. Click **OK** to confirm the operation.
7. Click **Save**.

   After you report card loss, the access levels of the lost card will be inactive.
8. **Optional:** Move the cursor onto the lost card and then click to cancel the card loss report.

   Note

   You need to delete all the temporary cards before you can cancel the card loss report.

   The card's access level will be active and the original biometric credentials will be linked to this card again.
9. **Optional:** Select the persons in the person list, move the cursor onto on the top, and then click **Report Loss** on the top to batch report loss of multiple cards.

13.9.2 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.

Steps

1. On the top, select **Person**.
2. Select **Person Management → Person** on the left.
3. **Optional:** On the Filter pane, click and set more conditions to search for the person to whom you want to issue the temporary card.
4. Click the name of the person in the person list to enter the basic information page.
5. Click **Credential Management** to open the Credential Management pane.
6. In the Card area, click .
7. Click **OK** to confirm the operation.
8. Enter the card number.
9. Set the expiry date to define the time when the temporary card becomes invalid.

Note

The expiry date of the 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 Person Manually*** .

10. Click **Save**.

Note

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.

11. Perform the following operation(s) if needed.

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 .

13.9.3 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 will be linked to these cards again.

Steps

1. On the top, select **Person**.
2. Select **Person Management → Person** on the left.
3. Optional: On the Filter pane, click and set more conditions to search for the persons for whom you want to cancel card loss reports.
4. Select the persons in the person list.
5. Move the cursor onto , and then click **Cancel Card Loss**.

The persons' temporary cards will be deleted.

13.10 Set Authentication via PIN Code

You can enable this function for allowing persons to access via PIN code.

On the top, select **Person**, and then select **Basic Configuration → Authentication via PIN Code** on the left. Switch on **Authenticate via PIN Code**.

Note

- When enabled, if the authentication mode of the card readers at the access points is also set to **Authenticate via PIN Code**, all the added persons are allowed to use their PIN codes alone as the credential for access authentication.
- When enabled, no duplicated PIN code is allowed.
- You can set a PIN code for a person when setting basic information for the person. For details, see ***Add a Person Manually*** .

Manual

The system administrator needs to manually filter out persons who have no PIN code or have duplicated PIN codes, change their PIN codes and then notify them of the updated PIN codes.

Note

The system administrator needs to notify relevant persons of the updated PIN codes in time. Otherwise these persons' access authentication and attendance results will be affected.

Auto

The platform will automatically reset all persons' PIN codes and apply the reset PIN codes to the access control devices. The system administrator needs to notify all users of the updated PIN codes.

Click **Save**.

13.11 Manage Resigned Persons

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

13.11.1 Add Resigned Persons

You can add one or multiple resigned persons, delete and export the resigned person information.

Steps

1. On the top, select **Person**.
2. Select **Person Management → Resigned** on the left.
3. Click **Add** to open the Add Resigned Person pane.
4. Click to select one or multiple persons from the departments.

Note

- You can enter specific person name, department, or person ID click **Search** to filter the person information.
- You can check **Include Sub Department** for displaying the person in sub departments.
- You can check **Select All Persons** to select all matched persons.

5. Specify the following parameters.

Departure Date

Last day of the current employment.

Departure Type

Cause of the departure.

Note

You can click **Add Departure Type**, enter the departure type and click **Add** to customize the type. For details, see ***Manage Resignation Types*** .

6. Optional: Check **Disable Attendance**, then the platform will not calculate attendance results generated during the period between applying for resigning and departure date.

7. Optional: Specify the departure reason.

8. Click **OK**.

Note

You can also adjust the person's status as resigned in Person Management module. See details in ***Add a Person Manually*** and ***Batch Add Persons by Template*** .

For persons to be resigned, their permissions of access and vehicles, and credentials such as the card, fingerprint, face picture, iris data will be deleted at the day of resignation.

9. Perform the following operations.

Operation	Description
Edit Resigned Person	Select a person and click in the Operation column to edit the resignation information.
Filter Resigned Person	Click to expand the conditions, set the filter conditions and click **Filter** for filtering the resigned persons.
Export Resigned Person	Click **Export** to export the resigned person information in the current page according to the filter conditions.
Disable Attendance	Select one or multiple persons whose attendance status is "enable", and click **Disable Attendance** to batch disable the function.
Delete Resigned Person	Select one or multiple persons and click **Delete** to delete them.
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.

13.11.2 Reinstate Persons

You can reinstate persons who are resigned and to be resigned.

Steps

1. On the top, select **Person**.
2. Select **Person Management → Resigned** on the left.
3. Select one or multiple persons and click **Reinstate**.
4. 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 permissions and attendance schedule will be accordance to that of their departments.

13.11.3 Manage Resignation Types

If the default resignation types do not meet your needs, you can add other resignation types.

On the top, select **Person**.

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.

Chapter 14 Access Control Management

Access control is a security technique that can be used to regulate who can get access to the specified door and floor control can be used to regulate who can get access to the specified floors by taking the elevator.

On the Web Client, the administrator can add access control devices, elevator 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/floors 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 and floors in the access level with their credentials during the authorized time period.

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 access points 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 ***Manage Access Control Device*** .
2. Add persons for access control. 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 access point(s) that allow entrance and exit. For details, refer to ***Manage Access Level*** .
5. Assign access levels to persons. For details, refer to ***Manage Access Level*** .

14.1 Manage Access Level

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

14.1.1 Add Access Level

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

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

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

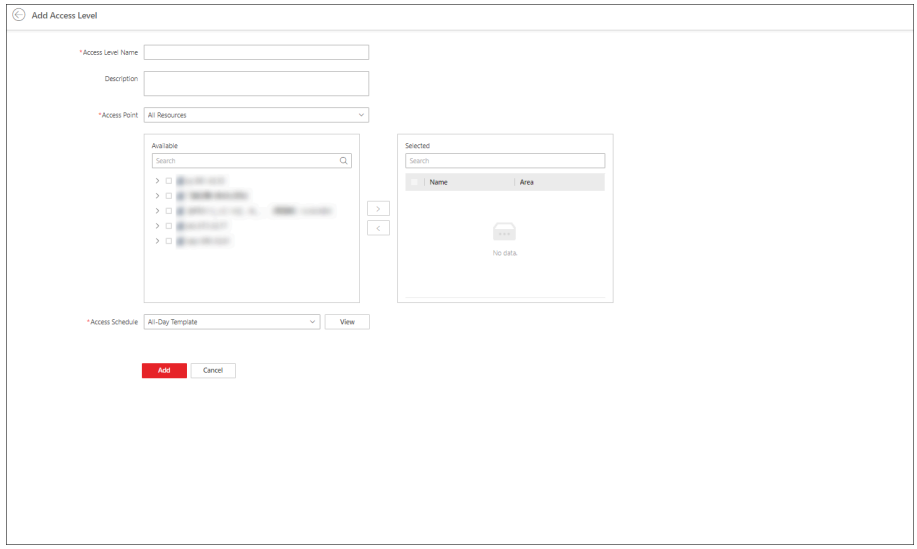


Figure 14-1 Select Access Points

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.
Delete All Access Levels	Click ∨ → **Delete All** to delete all access levels.

What to do next

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

14.1.2 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.

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. On the top, select **Access Control → Access Level → Assign by Access Level** .

2. Click on the access level that you want to assign to persons.

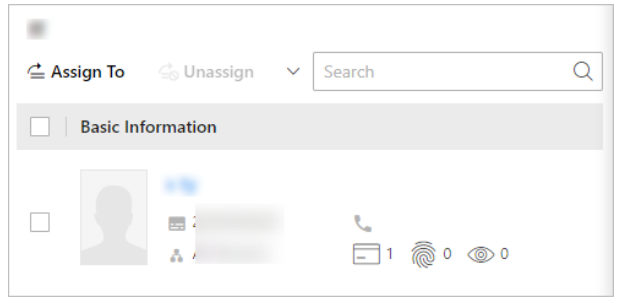


Figure 14-2 Assignee Panel

3. On the assignee panel, click **Assign To** to show person list.

4. Select the persons whom you want to assign the access level to and click **Add**.

Note

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

The access level settings will be applied to devices automatically.

5. Optional: To unassign a person from the access level, select the person and click **Unassign**. To unassign all, click → **Unassign All** .

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 Person

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

Before You Start

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

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

Steps

1. On the top, select **Access Control → Access Level → Assign by Person** .
2. In the department list, select a department.
3. In the person information panel on the right, select the persons to whom you want to assign access levels.

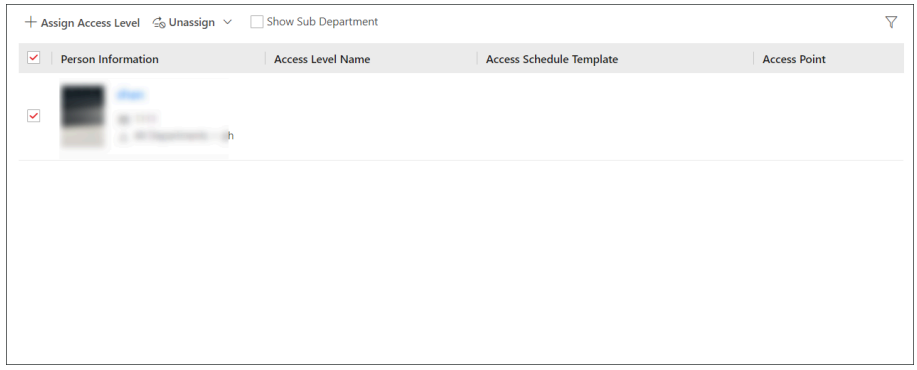


Figure 14-3 Person Information Panel

Note

You can click on person's name to view the details about the person.

4. Click **Assign Access Level**.
5. In the Assign Access Level panel, select 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.
7. **Optional:** To unassign a person's access levels, select the person and choose **Unassign All Access levels** or **Unassign Specified Access Levels**.

Note

For details, refer to ***Clear Persons' Access Levels*** .

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. On the top, select **Access Control → Access Level → Assign by Department** .
2. Do one of the following to assign access levels to departments.
   - Assign access levels to each department one by one.
     a. In the department list, click on a department.
     b. In the assigned access level panel on the right, click **Assign Access Level**.
     c. In the Assign Access Level panel, 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**.
     b. In the department list, select the departments where you want to assign access levels.

     Note

     Sub-groups are excluded from selection by default. To include all sub-groups of each department, check **Select Sub-Groups**.

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

   Note

   After assigning access levels to a department, you can still modify the access levels for each person in the group, and it will not affect the settings for the department. For details, refer to ***Assign by Person*** .

   The access level settings will be applied to devices automatically.
3. **Optional:** To unassign an access level from the department, select the access level and click **Unassign**. To unassign all access levels, click ∨ **→ Unassign All** .

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 permission (In the 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. One or multiple access levels can be assigned 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. On the top, select **Access Control → Access Level → Assign by Access Group** .
2. Perform one of the following operations to enter the Add Access Group page.
   - Click at the top of the access group list to enter the Manage Access Group page, and then click **Add** to enter the Add Access Group page.
   - 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.
3. In the **Group Name** field, enter the name of the access group.
4. 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 Persons**, all persons who matched the search conditions you set will be selected.
5. Click **Add** to add the selected person(s) to the access group.
6. After configuration, click **Add** at the bottom.
7. Select an access group to assign access levels to.
8. Click **Assign Access Level** on the right.
9. In the Assign Access Level page, select the access level(s) to be assigned to.
10. Click **Assign**.

    The access level settings will be applied to devices automatically.
11. **Optional:** Unassign access level(s) from the access group.
    - In the assigned access level list, select the access level(s) and click **Dissociate** to unassign the access level(s) from the access group.
    - In the assigned access level list, click → **Unassign All** to unassign all access levels from the access group.

What to do next

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

14.1.3 Apply Persons' Access Levels to Device

After setting or modifying the linkage between persons and access levels, you need to apply the access level settings to the access control devices or elevator control devices to take effect. After

that, the persons can access these access points during the authorized time period defined by the related access level.

Manually Apply Access Level Settings to Device

After setting access levels and assigning access levels to persons, departments, or access groups, you need to apply the relations between persons and access points to the devices.

Before You Start

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

Steps

1. On the top, select **Access Control**.
2. Select **Access Level**, and then select **Assign by Access Level**, **Assign by Person**, **Assign by Department**, or **Assign by Access Group** on the left.
3. Click **Apply Access Level Settings**.
4. On the Apply Access Level Settings panel, select the persons to apply the access level settings.
   - To apply the access level settings of all persons, select **All Persons**.
   - To apply the access level settings of specific persons, select **Specified Persons**, click , select the persons, and click **Add**.
5. Select the access points to apply the persons' access level settings.
   - To apply the access level settings of all access points, switch off **Specified Access Point**.
   - To apply the access level settings of specific access points, switch on **Specified Access Point** and select the access points.
6. Apply access level settings to devices.
   - To clear all persons' access level configurations on the devices first and then apply the configurations in the platform to the devices, check **Apply (Initial)** and click **Apply**.

     Note

     - Only available when you select **All Persons** previously.
     - During the initialization process, the devices will be offline, and persons cannot access these access points.
   - To apply changed (newly added, edited, deleted) access level settings to the devices, uncheck **Apply (Initial)** and click **Apply**.
7. **Optional:** If persons' access level settings (such as linked access levels, person credentials, etc.) are changed or the applying process failed, will appear next to , indicating some access level settings are pending to be applied to the devices. You can hover the cursor over to view the details.

   Note

   For troubleshooting the applying process, refer to ***Access Control Test*** .

Regularly Apply Access Level Settings to Devices

You can set a schedule to apply the access level settings in the system to devices automatically.

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

Steps
1. On the top, select **Access Control → 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**.

14.1.4 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 top, select **Access Control → Access Level → Assign by Person** .

Select a department to show all persons in the group. You can filter the target persons by setting search conditions.

Select the target person and click **Unassign** to choose **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.
After clearing, the previous access level settings of the persons cannot be restored. You need to re-assign access levels for them again when needed.

After clearing the access level settings of the selected persons, these persons will be removed from the related access groups. You need to apply the access level settings of these persons to the devices to take effect. For details, refer to ***Manually Apply Access Level Settings to Device*** for details. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .

After applying to the devices, the access level settings of the persons will be deleted from the devices.

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

Steps

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

Name

Create a name for the template.

Copy from

Optionally, you can select to copy the settings from existing templates.

6. In the **Weekly Schedule Template** box, set a schedule pattern for each day.
1) Click **Authorize** and select or draw in the box to define the authorized time periods.
2) **Optional:** Click **Erase** and select or draw on the authorized time periods to clear the selection.

Note

You can set up to 8 separate time periods for each day.

7. Optional: Set a holiday schedule if you want different schedules for specific days.

Note

Holiday schedule has a higher priority than weekly schedule.

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

8. Click **Add** to save the template.
9. 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.

What to do next

Set access schedule for access level to define in which time period persons are authorized to access the access points in the access level. For details, refer to ***Add Access Level*** .

14.1.6 Enable Authentication via Password

Authentication via password allows you to authenticate only via your password. After this function is enabled, all the passwords in the platform should be different from each other. You can update the password manually or automatically.

Steps

1. On the top, select **Access Control → Basic Configuration → General** .
2. Switch on **Authenticate via PIN Code**.
3. Select **Manual** or **Auto** as the PIN code update mode.

   Manual Mode

   You need to export users whose passwords are duplicated or not configured from the Person module, and then notify these users to update the passwords by themselves. A password should consist of 4 to 8 characters.

   Auto Mode

   The platform will change the duplicate password to a unique one or customize a unique password for each user whose password is not configured, and then notify these users.
4. Click **Save**.

14.2 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.

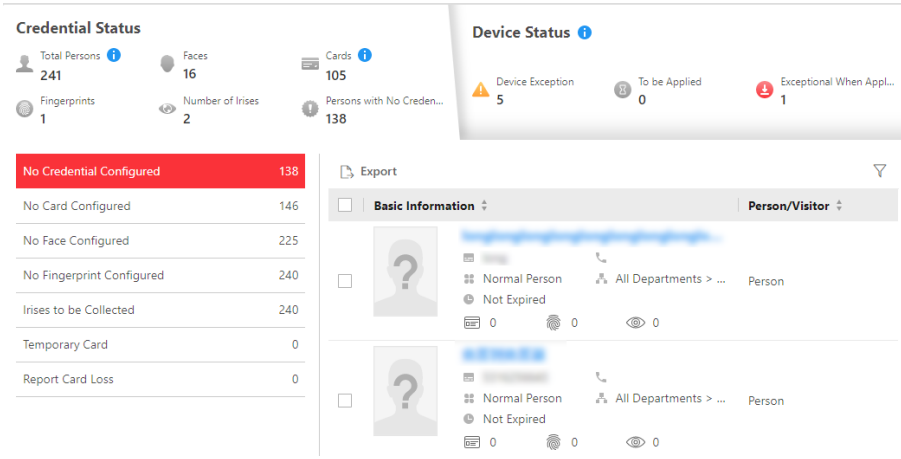


Figure 14-4 Credential Status

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, elevator 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.

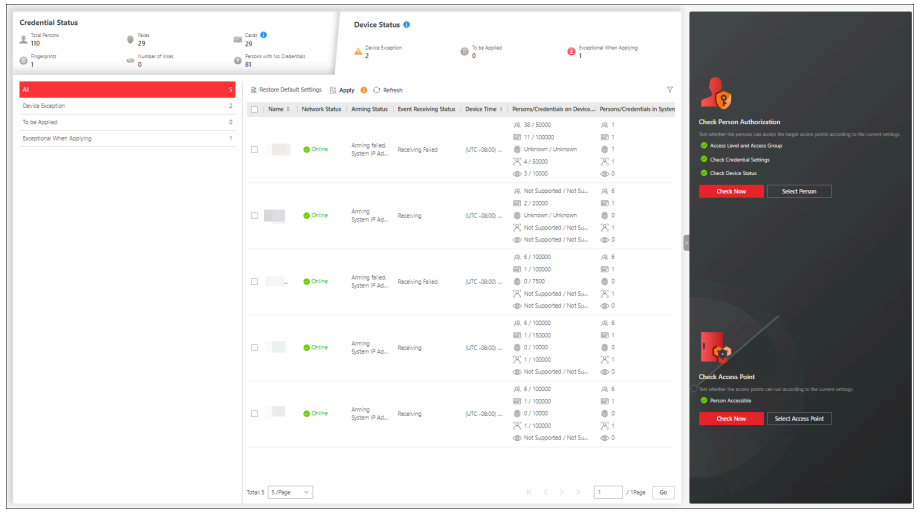


Figure 14-5 Device Status

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.

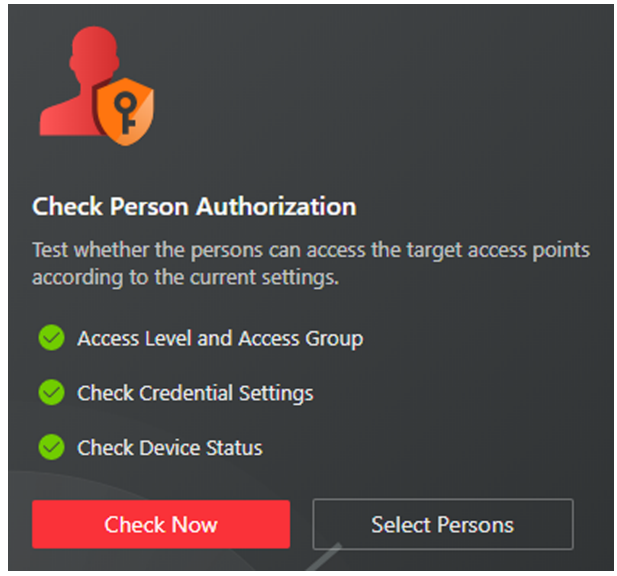


Figure 14-6 Check Authorization Settings

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.

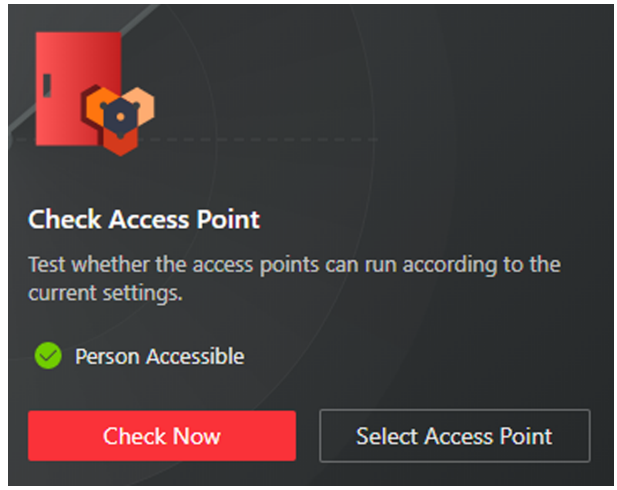


Figure 14-7 Check Access Point Settings

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.

14.3 Advanced Functions

14.3.1 Configure Free Access and Access Forbidden Rules

You may need to set access points accessible or inaccessible during certain periods. To perform this function, you need to configure free access and access forbidden rule for certain access points.

Steps

Note

This function should be supported by the device.

1. On the top, select **Access Control → Access Control Application → Free Access & Access Forbidden** .
2. Click **Add** to enter the Add Free Access and Access Forbidden Rule page.
3. Enter the rule name.
4. Select an access point from the following area list.
5. Select free access schedule or access forbidden schedule.

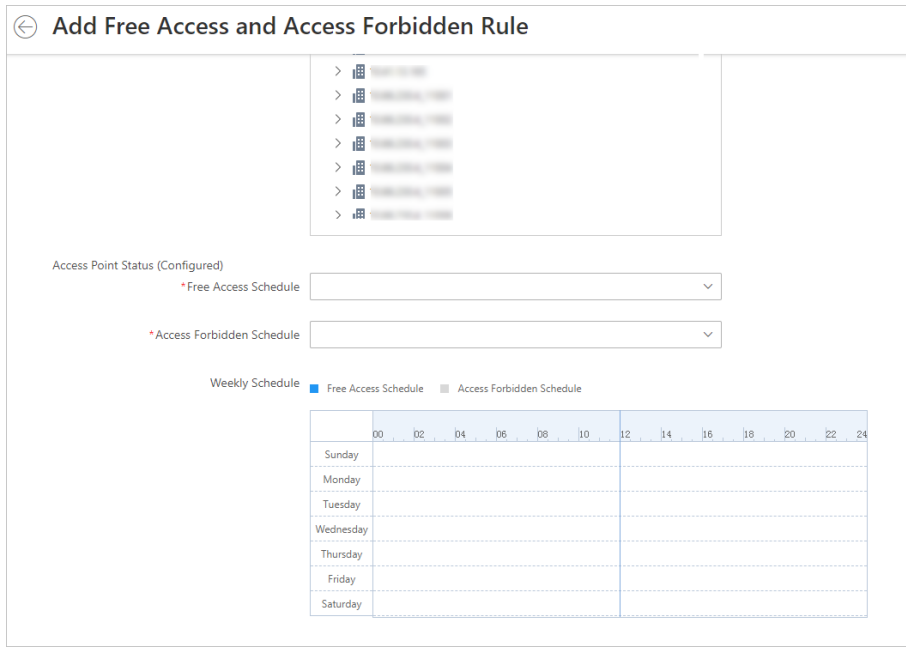


Figure 14-8 Add Free Access and Access Forbidden Rule Page

Free Access Schedule

During free access period, all persons can access the selected access points without credentials required.

Access Forbidden Schedule

During access forbidden period, no persons can access the selected access points even if he/she has the authorized credentials, except the super users.

Note

- You can click **Add** to add a custom access schedule or holiday schedule. See ***Set Access Schedule Template*** for details.

6. Click **Add**.

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

7. **Optional:** Perform the following operations.

View Schedule Details	Click to show the schedule details.
Copy Schedule to Other Access Point	Click a rule name to enter the rule page. Click **Copy To** on the top right to copy the schedule to other access points.

14.3.2 Configure First Person In Rule

First Person In refers to a rule that only after the first person is authorized to enter with his or her card, fingerprint, or face, can other people's permission be activated. There are two modes for First Person In, the Remaining Open after First Person and the Authorization by First Person.

Steps

Note

This function should be supported by the device.

1. On the top, select **Access Control** .
2. Select **Access Control Application → First Person In** on the left.
3. Click **Add** to enter the Add First Person In Rules page.
4. Enter the rule name.
5. Select a door from the area list.
6. Set **Rule of Opening Door**.

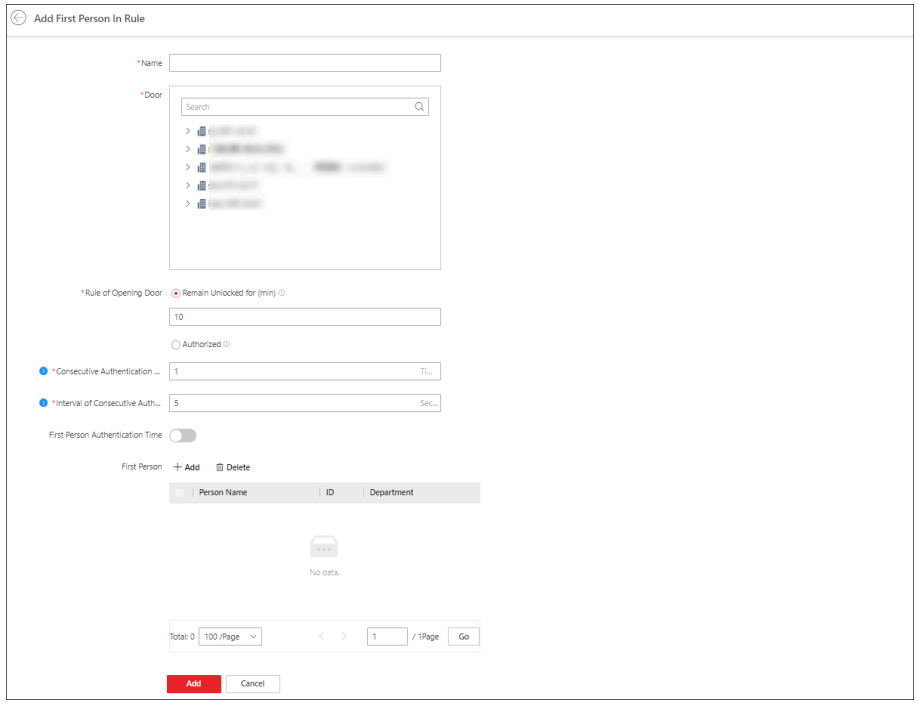


Figure 14-9 Add First Person In Rule Page

Remain Unlocked for (min)

When the door is locked, if the first person swipes card, the door will remain unlocked during the configured period.

Authorized

The door is locked and access is denied with any credentials (except during the free access schedule) until you swipe the first card. After the first person swipes card, the door is authorized and the persons with corresponding access level are granted to access. The authorization will be invalid at 00:00 a.m. every day.

7. Set the consecutive authentication times and the interval of consecutive authentication.
8. **Optional:** Enable **First Authentication Time** to set a fixed time period requiring first person authentication.
9. Click **Add** to select first person(s).

Note

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

10. Click **Add** to add the rule.

14.3.3 Manage Multi-Factor Authentication

Multi-Factor Authentication is an access authentication scheme which requires all the predefined persons to be present and get authentication. Multi-Factor Authentication is generally used in places such as bank vault to ensure the security of important assets and data. To perform this function, you need to configure multi-factor authentication rule and add multi-factor authentication group first. Besides, you can add persons to receive remote door open request.

Configure Multi-Factor Authentication Rule

In access control, multi-factor authentication is an authentication method in which the door will unlock only after multiple persons present authenticating multiple credentials in turn. This method is mainly used for locations with high security requirements, such as bank vault. With the mutual supervision of the persons, multi-factor authentication provides higher security for the assets in these locations.

Steps

Note

This function should be supported by the device.

1. On the top, select **Access Control → Access Control Application → Multi-Factor Authentication** .
2. Click **Add**.
3. Enter the rule name.
4. Select a door from the following area list.
5. Set the access mode of the door.

   Unlock After Access Granted

   The door will be unlocked automatically after the persons swiping 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 swiping their cards (or other type of credentials) on the card readers of the door and the access is granted, a window will pop up. The operator should confirm to unlock the door remotely and then the door will be unlocked successfully.

   Enter Super Password After Granted

After the persons swiping 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.

6. Set the access schedule to define in which time period, the persons are authorized to access the door.

Note

The default and customized access schedules are displayed in the drop-down list. You can click **Add** to customize a new schedule. For details, refer to ***Set Access Schedule Template*** .

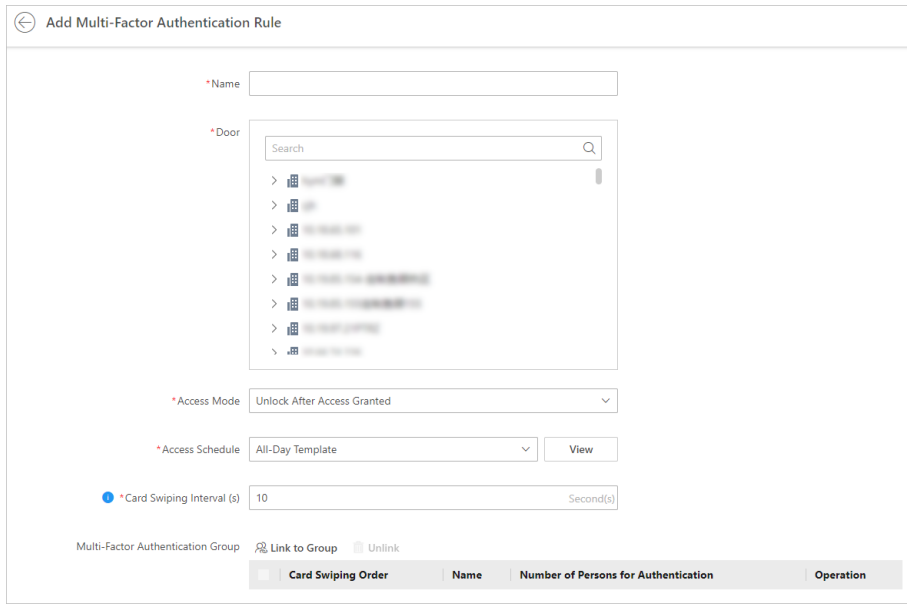


Figure 14-10 Add Multi-Factor Authentication Rule

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

Note

When adding groups, if you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

Card Swiping Order

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

Number of Persons for Authentications

Define how many persons should authenticate on the card reader.

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.

Note

This value should be no larger than the number of persons in the access group.

9. Click **Add**.

Add Multi-Factor Authentication Group

To perform the multi-factor authentication function, you need to create a multi-factor authentication group and appoint persons as the member of the group first. Persons in the group have the permission for multi-factor authentication of specific doors.

Steps

1. On the top, select **Access Control → Access Control Application** .
2. Click **Multi-Factor Authentication** on the left.
3. Click **Multi-Factor Authentication Group Management** on the top.
4. Click **Add** to open the Add Multi-Factor Authentication Group panel.
5. Enter the multi-factor authentication group name.
6. Click **Add** to select group members from the person list.

Note

When adding groups, if you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

7. Click **Add**.

Add User to Receive Remote Door Open Request

To handle remote door open requests, you need to appoint persons to receive these requests beforehand.

Steps

1. On the top, select **Access Control → Access Control Application → Multi-Factor Authentication** .
2. Click **User to Receive Remote Door Open Request** on the top.
3. Click **Add** to open the User to Receive Remote Door Open Request pane.
4. Select users from the list.

Note

If you check **All**, all persons will be selected.

5. Click **Add**.

14.3.4 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. On the top, select **Access Control → Access Control Application → Multi-Door Interlocking** .
2. Click **Add**.
3. Create a name for the group.
4. Select doors and click › .
5. Click **Add**.

14.3.5 Configure Anti-Passback Rules

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 swiping the card. You can configure area anti-passback rules or route anti-passback rules for different scenarios. This function is mainly used to enhance the access security of some important or specific places (e.g., laboratories, offices).

Configure Area Anti-Passback Rules

The area anti-passback function establishes a specific door group for an area. When a person accesses the area by swiping card, he/she should exit the area via the door in the anti-passback group if he/she enters the area via the door in the group, and he/she cannot enter the area via the door in the anti-passback group if he/she exited the area not by swiping card at the door in the group before.

Before You Start

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

Steps

1. On the top, select **Access Control → Access Control Application → Anti-Passback → Area Anti-Passback** .
2. Click **Add**.

3. Create a name for the door group.
4. Select doors in the Available list and click › to add them to the Selected list.
5. **Optional:** Switch on **Forgive Anti-Passback** and set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday.
   Anti-Passback Violation
   When a person attempts to use a card without following the rule, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven.
6. **Optional:** Switch on **Non Anti-Passback Period** to set a fixed time during which persons can access the area without following the rule.
7. Click **Add**.
8. **Optional:** Perform the following operations after adding the 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	When a person attempts to use a card without following the rule, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven. 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).
Delete Anti-Passback Group	Select the group(s) and click **Delete** to delete the anti-passback group(s).

Configure Route Anti-Passback Rules

The route anti-passback depends on the card swiping route. This function establishes a specific card reader sequence in which cards must be used in order to grant access. You should set the first card reader and the subsequent ones. It will authenticate the anti-passback according to the entrance and exit information stored in the card reader.

Steps

1. On the top, select **Access Control → Access Control Application → Anti-Passback → Route Anti-Passback** .
2. Click **Add** to enter the Add Route Anti-Passback page.

3. Create a name for the route anti-passback rule in the **Name** field.

4. Set the card reader order in the Card Reader Order area.

1) Click **Add**, select a card reader in the list, and click **Add** to add a card reader.
2) Hover the cursor on the added card reader and click ⊕ to add another card reader.

Note

You can repeat this step to add card readers according to a specific sequence as needed.

3) **Optional:** Click the card reader and click **Change Card Reader** to select another card reader to replace it.
4) **Optional:** Click the card reader and click **Delete** to delete the card reader and its subsequent card reader(s).

5. Optional: Switch on **First Card Reader** and select a card reader from the drop-down list to set it as the first card reader.

Note

If you violate the route anti-passback rule, you should swipe the card again from the first card reader.

6. Optional: Switch on **Forgive Anti-Passback** to set a fixed time so that the platform can forgive the anti-passback violations automatically everyday.

Anti-Passback Violation

When a person attempts to use a card out of the route anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven.

7. Optional: Switch on **Non Anti-Passback Period** to set a fixed time during which persons can access the area without following the rule.

8. Click **Add**.

9. Optional: Perform the following operations after adding the route anti-passback rule.

View Card Reader Order	Click 👁 in the Operation column to view the card reader order of the rule.
Edit Anti-Passback Rule	Click the rule name to edit the anti-passback rule settings. You can edit the name of the rule, add, change, or delete card readers in the order, change the first card reader, or change the settings of forgiving anti-passback violation regularly.
Set/Cancel Forgiving Anti-Passback Regularly	When a person attempts to use a card out of the route anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven. Select the rule(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 rule(s) at that time everyday.

	You can also select the rule(s) and click **Cancel Forgiving Anti-Passback Regularly** to cancel the settings of the selected rule(s).
Delete Anti-Passback Rule	Select the rule(s) and click **Delete** to delete the route anti-passback rule(s).

14.3.6 Add Emergency Operation Group

An emergency operation group is a group for access points which need to be operated (remaining locked/unlocked) in a batch. This function is mainly applicable for emergent situation.

Before You Start

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

Steps

1. On the top, select **Access Control → Access Control Application → Emergency Operation Group** .
2. Click **Add**.

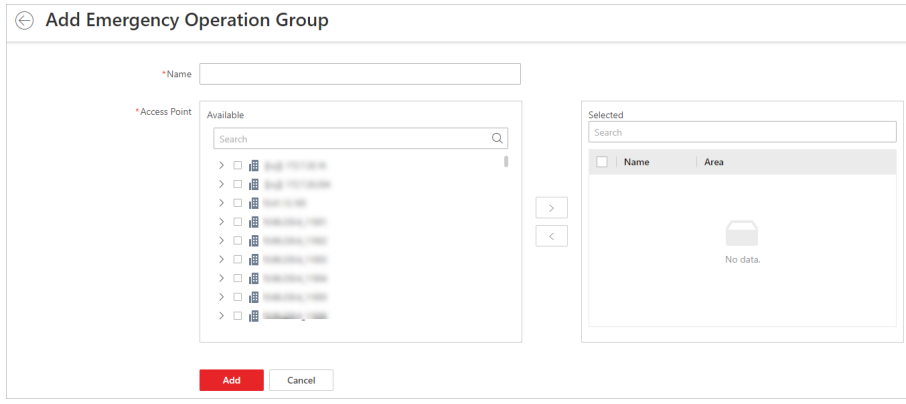


Figure 14-11 Add Emergency Operation Group Page

3. Create a name for the group.
4. Select the access points and click > to add them to the group.

Note

You can add doors of access control devices, doors of video intercom devices, and floors of elevator control devices to the emergency operation group.

5. Click **Save**.

   The emergency operation group is added in the table and you can view the access points in the group.

14.3.7 Add Entry and Exit Counting Group

The entry and exit counting group is used to group the access points in a certain region. You can set certain access points as the region border. Only the persons accessing these access points are counted, and other access points inside the region are ignored. 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. On the top, select **Access Control → Access Control Application → Entry & Exit Counting Group** .
2. Click **Add**.
3. Create a name for the group.
4. Click **Add** and select doors from the area list.
5. Set the entering or exiting direction of the card readers of the selected access points.

   The access records on the entering card reader will be counted as a person enters this region while the access records on the exiting one will be counted as a person exits this region.
6. Click **Save**.

   The entry & exit counting group is added to the table and you can view the access points in the group.

14.3.8 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. On the top, select **Access Control → Access Control Application → Authentication Mode** .
2. Select the **Card Reader Authentication Mode** tab.
3. Select an area from the area list.
4. Click a door name on the right.
5. 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.
6. 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.
7. **Optional:** Click **Copy To** in the upper-right corner to apply the settings to other doors.
8. Click **Save**.

Set Person Private Authentication Mode

In some situations, different persons need to use different authentication modes for accessing the same access point, and a person may need to use different authentication modes for accessing different access points. Setting the private authentication modes for different persons can provide an easy way for them to authenticate by less credentials or enhance the security of some important places by forcing them to use more credentials.

Steps

Note

The person's private authentication mode has higher priority than the existing authentication mode of the device.

1. On the top, select **Access Control → Access Control Application → Authentication Mode** .
2. Select the **Private Authentication Mode** tab.
3. Select a department from the left list.

   All persons in the department will be listed on the right panel.
4. Click in the Operation column to open the Authentication Device pane.
5. Click **Add**, check the device(s) from the list, and select the authentication mode from the drop-down list for the selected device(s).
6. Click **OK** to add the device(s) for authentication for the person.
7. **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.
8. **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.

14.3.9 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. On the top of Home page, select **Access Control → Access Control Application → Apply Advertisement** .
2. Select **Access Control Application → Apply Advertisement** on the left.
3. 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.
4. 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 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.

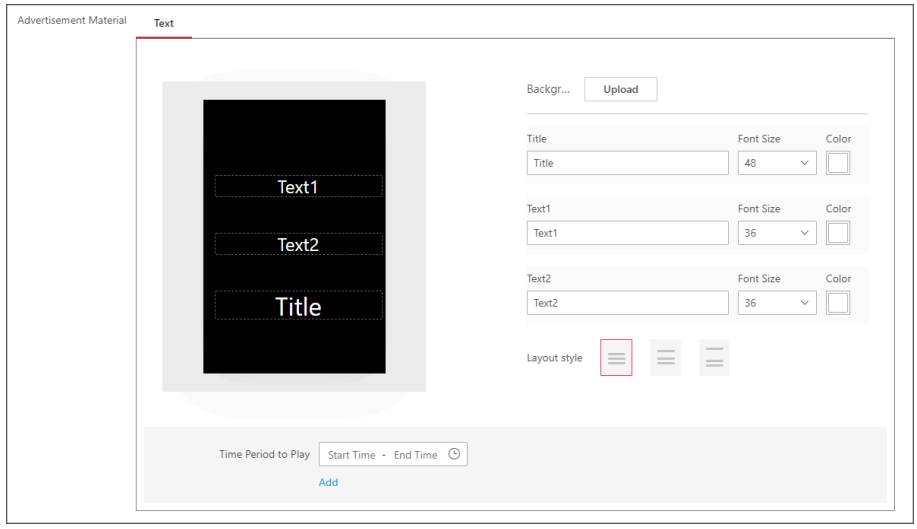


Figure 14-12 Add Text in Advertisement

5. The playing schedules set for the picture(s), video(s), and text(s) in the advertisement will be displayed by different color blocks.
6. Switch on **Sleep**, and set the sleep duration (from 20 to 60 seconds).
7. Click **Apply**.
8. **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.

14.3.10 Add Audio Broadcast

You can add daily audio broadcasts for daily use and add particular broadcasts for holidays or specific days. After adding broadcasts, you can apply them to devices.

Steps

1. On the top, select **Access Control → Access Control Application → Audio Broadcast** .

2. Click **Add Audio Broadcast**.

3. Select the broadcast device(s).

4. Enable the daily broadcast.

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.

5. In the Particular Broadcast area, click **Add** to add particular broadcasts.

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

- On the days without particular broadcasts, daily broadcasts will be played. 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**.

6. Click **Add**.

The settings will be applied to the selected device(s).

7. 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.

14.3.11 Set Card Authentication Parameters

Set the card reading content when authenticate via card on the device.

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

Select **Basic Configuration** → **General** on the left.

Enable **Card No. Authentication** and select a card authentication mode.

Full Card No.

All card No. will be read.

Wiegand 26 (3 Byte)

The device will read card via Wiegand 26 protocol (read 3 bytes).

Wiegand 26 (4 Byte)

The device will read card via Wiegand 26 protocol (read 4 bytes).

14.4 Door and Elevator Control

With emergency operation group, you can control door and elevator status in a batch when an emergency happens. For example, after grouping the doors of a school's main entrances and exits into one emergency operation group, school's security personnel can lock down the doors 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

Only the users with Administrator or Operator role can control all doors/floors in a batch.

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

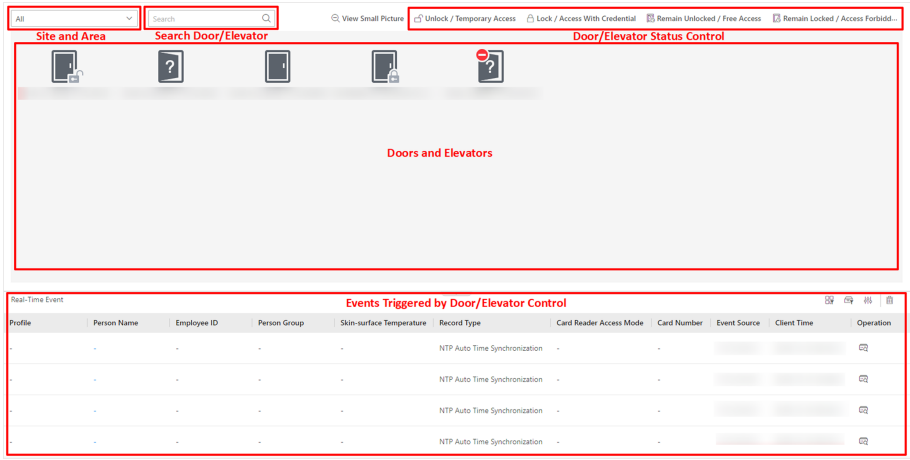


Figure 14-13 Access Control Real-time Monitoring

14.4.1 Start Live View of Access Control / Elevator Control Devices

For access control devices with cameras installed inside or linked outside, and elevator control devices linked with cameras, you can start live view of these devices.

Before You Start

Make sure you have added the devices to the platform.

Steps

1. On the top, select **Access Control → Real-Time Monitoring** .
2. Click a device and select **Live View**.

   The live view window of the device will be displayed on the right.

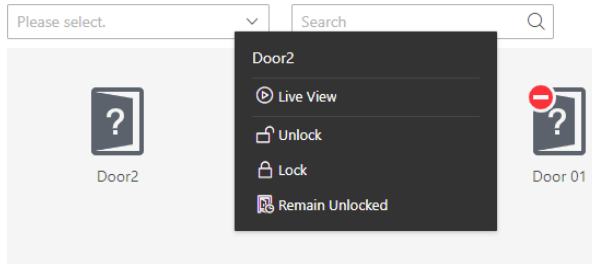


Figure 14-14 Start Live View

3. Hover the cursor on the live view window to show the tool bar at the bottom. You can click different buttons according to your need.

Example

You can click to start two-way audio with persons by the device.

14.4.2 Door Control

You can change the status of all doors in a site or doors in specific emergency operation groups to locked, unlocked, remaining locked, or remaining unlocked.

Note

Make sure you have grouped doors into an emergency operation group. See details in ***Add Emergency Operation Group*** .

On the top of the Home page, select **Access Control → Real-Time Monitoring** .

Control all or part of the doors.

Unlock

When a door is locked, if you unlock the door, it will be unlocked. When open duration is over, the door will be locked again automatically.

Click **Unlock / Temporary Access → All** to unlock all doors in the current site.

Click **Unlock / Temporary Access → Part** and select the emergency operation groups you want to unlock. Click **OK** to unlock the doors in the selected emergency operation groups.

Note

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

Lock

When the door is unlocked, if you lock the door, it will be closed and locked. The person who has the access permission can access the door with credentials.

Click **Lock / Access with Credential → All** to lock all doors in the current site.

Click **Lock / Access with Credential → Part** and select the emergency operation groups that you want to lock. Click **OK** to lock the doors in the selected emergency operation groups.

Remain Unlocked

Doors will be unlocked. All persons can access the door with no credentials required (free access). 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.

Click **Remain Unlocked / Free Access → All** and all doors in the current site will remain unlocked.

Click **Remain Unlocked / Free Access → Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain unlocked.

Remain Locked

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

Click **Remain Locked / Access Forbidden → All** to lock down all the doors in the site.

Click **Remain Locked / Access Forbidden → Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain locked.

Note

For setting person's super user permission, refer to ***Role and User Management*** .

14.4.3 Elevator Control

You can change the status of all floors in floors in specific emergency operation groups to temporary access, access with credential, free access, or access forbidden.

Note

Make sure you have grouped floors into an emergency operation group. See details in ***Add Emergency Operation Group*** .

On the top of the Home page, select **Access Control → Real-Time Monitoring** .

Control all or part of floors in the current area.

Temporary Access

During the temporary access time, the persons can access this floor with no credentials required. After the access time, the floor will recover to Access with Credential status.

Click **Unlock / Temporary Access → All** to set all the floors in the current area to Temporary Access.

Click **Unlock / Temporary Access → Part** and select one or more emergency operation groups to set all floors in the group(s) to Temporary Access.

For details about setting the temporary access duration, see ***Edit Elevator*** .

Access with Credential

Person who has the access permission can access this floor with credentials.

Click **Lock / Access with Credential → All** to set all the floors in the current area to Access with Credential.

Click **Lock / Access with Credential → Part** and select one or more emergency operation groups to set all the floors in the group(s) to Access with Credential.

Free Access

All persons can access this floor with no credentials required.

Click **Remain Unlocked / Free Access → All** to set all floors in the current area to Free Access.

Click **Remain Unlocked / Free Access → Part** and select one or more emergency operation groups to set all floors in the group(s) to Free Access.

Access Forbidden

No person, except the super users, can access this floor even with authorized credentials. This function is applicable for situations such as preventing a thief in the building from getting away.

Click **Remain Locked / Access Forbidden → All** to set all floors in the current area to Access Forbidden.

Click **Remain Locked / Access Forbidden → Part** and select one or more emergency operation groups to set all floors in the group(s) to Access Forbidden.

Note

For setting person's super user privilege, refer to ***Role and User Management*** .

14.4.4 View Real-Time Access Event

In the Access Control module, you can view events triggered by doors and elevators. You can also control door and elevator status according to the event details, search for more event information, and so on.

On the top, select **Access Control → Real-Time Monitoring** .

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 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-switch to the Latest Record** to display the person information contained in the newest access record. If you uncheck the **Auto-switch to the Latest Record**, the platform will display the person information contained in the historical access records. The platform supports hiding the window.

14.5 Subscribe to Device and Access Events

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

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

Steps

1. On the top, select **Access Control → Basic Configuration → Device Event Subscription** .
2. Select an event category from **Device Event**, **Normal Access Event**, and **Abnormal Access Event**.
3. Switch on the event types to subscribe to these events.
4. **Optional:** Switch off the event types whose real-time event records you do not want to receive.

   Note

   If you switch off an event type, the Web Client and Mobile Client will no longer receive real-time event records of the event. However, you can still search for the device/access records via the Web Client. For details, see ***Search Access Records*** and ***Search Data Recorded on Access Control Devices and Elevator Control Devices*** .

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

What to do next

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

14.6 Synchronize Access Records to System Regularly

Access records stored in devices can be synchronized to the system for central management. You can specify a fixed time in order to automatically synchronize access records from devices to the system at the specified time every day.

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

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

14.7 Enable Open Door via Bluetooth

You can enable open door via bluetooth and select a door opening mode.

Note

You can enable persons to open door via bluetooth in **Person Management → Person** .

On the top, select **Access Control**. Then, select **Basic Configuration → General** on the left. On **Open Door via Bluetooth**, choose from **Auto Open Door** and **Open Door Manually**.

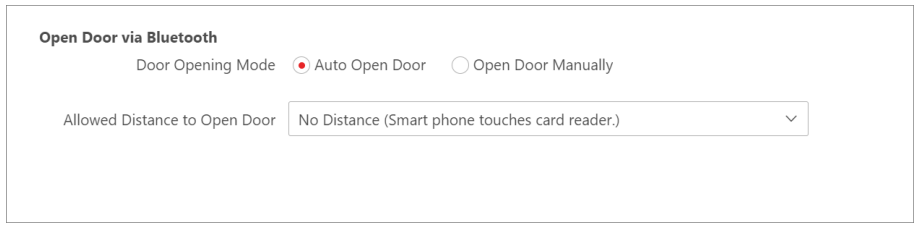


Figure 14-15 Open Door via Bluetooth

Auto Open Door

The door will open automatically when you get close to the door in a specific distance.

Allowed Distance to Open Door

You can select an allowed distance to open the door. You can choose from **No Distance (Smart phone touches the card reader)**, **Near (The distance between smart phone and card reader is about 20 cm)**, **Far (The distance between smart phone and card reader is about 50 cm)**, and **Customize (Enter a custom RSSI value)**.

Customize RSSI Value

You can set an RSSI value (a negative integer ranging from -1000 to -1). If the RSSI value of a nearby door is higher than or equal to the value you entered, the door will open automatically. It is recommended that you set this value according to the actual RSSI value displayed on the Mobile Client.

Open Door Manually

You can manually open a specific door on the Mobile Client.

14.8 Search Access Records

You can search for persons' access records triggered on specified access points (including doors and elevators) via the Client 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.

Before You Start

Make sure you have configured the access point event. For details, refer to ***Add Normal Event and Alarm*** .

Steps

1. On the top, click **Access Control → Search → Identity Access Search** .

2. Optional: Import access records to the system.

- Import access records from the device(s).
  a. Click **Import Event → Import from Device** to enter the Import from Device page.
  b. Select the device(s) from the device list.
  c. Optional: Switch on **Specified Time Range** and set the start time and end time to import access records generated in the specified time period.

Note

- If the device has uploaded access record(s) to the system before, switching on **Specified Time Range** is not required and access 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 access record to the system before, you must switch on **Specified Time Range** for importing access records from the selected device(s).

d. Click **OK** to start importing.

A window will pop up to display the importing progress and the failure details.

- Import access records from the file which is exported from the device.

a. Click **Import Event → Import from File** to enter the Import from File page.

b. Click to select the file to be imported.

Note

Only the encrypted file can be imported.

c. Enter the password in the **Password** field.

d. Click **OK**.

3. In the **Time** drop-down list, select the time during which the access records are generated.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

4. Optional: In the **Access Point** area, click and select door(s) and elevator(s) from the resource list.

5. Optional: In the **Record Type** area, click to select record type(s).

6. In the **Authentication Result** drop-down list, select an access result type to quickly filter access granted records or access denied records.

7. Set the searching mode.

- a. Select **Person** as the searching mode.

b. Select **Select Person** or **Fuzzy Matching** as the searching mode.

Select Person

Click to select the person(s)

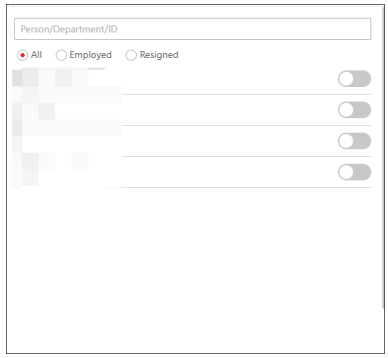
Note

- You can click **More** to enable custom information items and enter the keyword in the text filed to search for matched persons.

Note

Make sure you have customized additional information of persons. For details about customizing additional information, refer to ***Customize Additional Information*** .

- If you check **Select All Persons**, all persons who matched the search conditions you set will be selected.
- You can check **Include Sub Department** to display the persons of sub-departments.
- You can click **More** to select **Employed**/**Resigned** to select the employed/resigned person(s).



Fuzzy Matching

Enter a keyword to search for persons whose name contains the keyword.

c. Click **Add** to select the person(s), or enter the keywords of the person name for fuzzy matching.

- a. Select **Card No.** as the searching mode.
  b. Enter the card number.

8. Optional: Switch on **Temperature Status** and select **Normal** or **Abnormal**.

9. Optional: Switch on **Mask Wearing Status** and select **Wearing Mask** or **No Mask**.

10. Click **Search**.

Matched access records are listed on the right.

11. Optional: Perform the following operations after searching for access records.

Custom Column Items	On the top right, click to select column items to be displayed. You can click **Reset** to select again.
View Record Details	Click the person name in the Full Name column to view the record details, such as person information, and access information.
Filter Search Results by Person Type	Click next to the column name **Person** and select persons to filter the search results.
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 file in 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 access record details in your PC. You can select the file format as an Excel or a CSV file, and select items to export. If you select **Excel**, you can check **Profile Picture** to save the captured pictures and person profile photos.

Note

Up to 500 records can be exported each time.

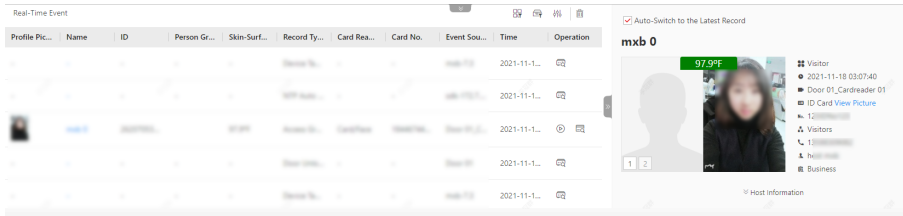


Figure 14-16 Real-Time Events

14.9 Search Data Recorded on Access Control Devices and Elevator Control Devices

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

Steps

1. On the top, select **Access Control → Search → Device Recorded Data Retrieval** .
2. In the Time drop-down list, select a time range for searching.

   Note

   You can select **Custom Time Interval** to set a precise start time and end time.

3. Switch on the resource types where you want to search for records.

   Access Point(s)

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

   Device

Devices include access control devices, elevator control devices, and video intercom devices. The data recorded in these devices covers all events triggered by devices (such as device faults).

Alarm Input

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

4. Select the record source(s) and record type(s).

5. Click **Search**.

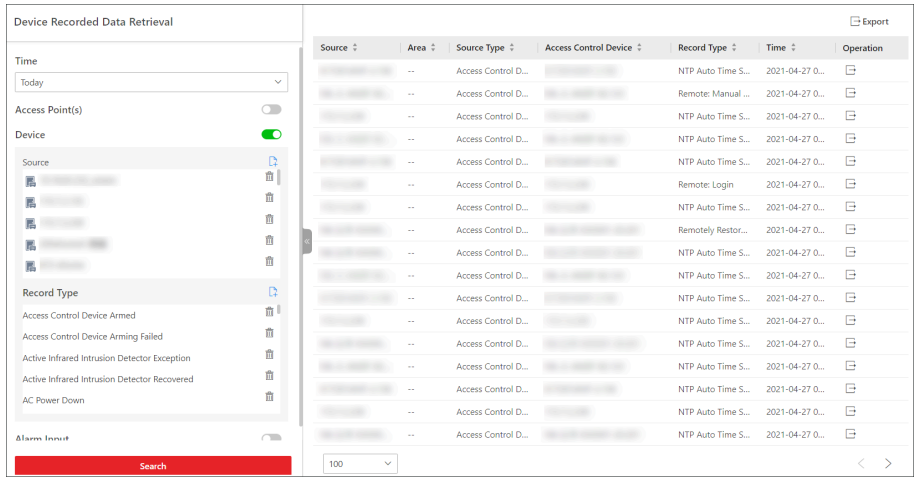


Figure 14-17 Device Recorded Data Retrieval

6. Optional: Perform further operations on the searched records.

View Record Details	Click the device name in the Source column to view the record details, such as 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 or a CSV file.

14.10 Perform Entry & Exit Counting

By grouping the doors (adding entry & exit counting group), the system provides counting functions based on the entry and exit records on these doors. With this function, you can check who enters/exits this region and how many persons still stay in this region. The function is applicable for certain emergency scene. For example, during a fire escape, all people are required to exit the region.

Before You Start

Make sure you have added entry & exit counting groups to group the doors. See ***Add Entry and Exit Counting Group*** .

Steps

Note

Currently, the platform only supports searching persons with access records in the last 24 hours.

1. On the top, select **Access Control → Search → Entry & Exit Counting** .
2. In the **Source** list, select an entry & exit counting group.
3. In the **Entry & Exit Counting Type** drop-down list, select the type of persons you want to search.

   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.
4. Click **Search**.

   All matched access records will be listed, showing information such as person details, location of last access, etc.
5. **Optional:** Perform further operations after searching.

View Event Details	Click the person name in the Name column to view the record details, including the recorded video of the access point's related camera (if configured), 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 (including the person information, person profile, phone number, location of last access, etc.). **Note** Up to 100,000 records can be exported each time.

Chapter 15 Time & Attendance

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

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

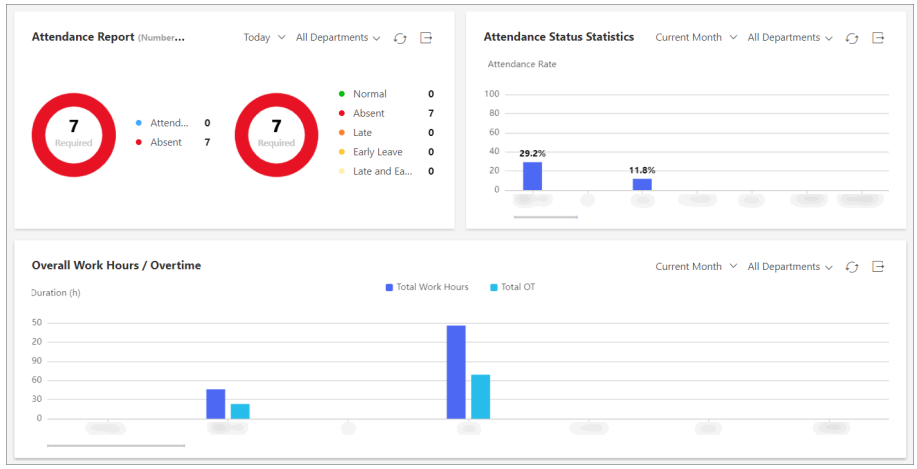


Figure 15-1 Attendance Charts

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

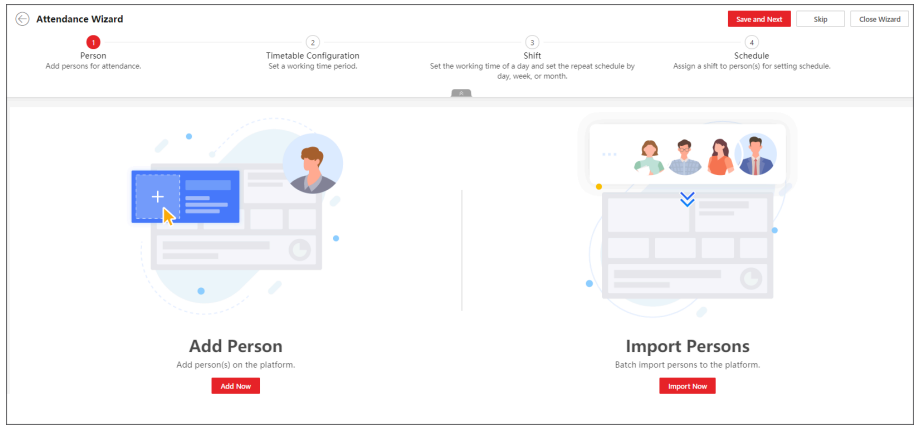


Figure 15-2 Attendance Wizard

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.

15.1 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.

15.1.1 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. On the top, select **Attendance**.

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

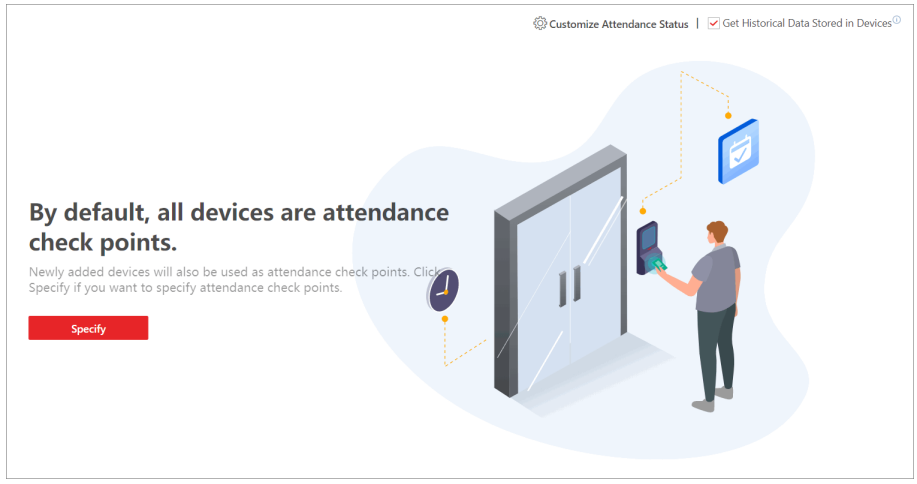


Figure 15-3 Default Mode

3. Optional: Click **Customize Attendance Status** to select attendance mode and custom attendance parameters. For details, see ***Customize Attendance Status on Device*** .

4. 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.

5. Click **Specify** to start customizing attendance check points.

6. Click **Add**.

7. 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.

8. Select the resource type (e.g., door) from the drop-down list.

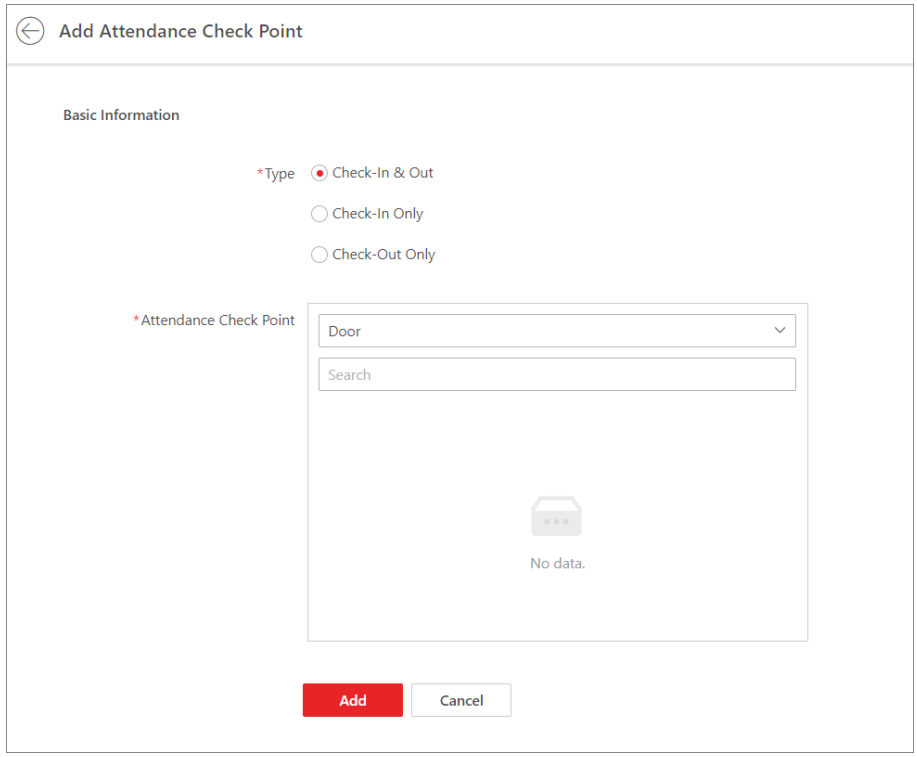


Figure 15-4 Add Attendance Check Point

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

9. Select the resources.

10. Click **Add**.

The selected resources will be displayed in the attendance check point list.

11. 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.

Before You Start

Make sure the devices support this feature.

Steps

1. On the top, select **Attendance → Basic Configuration → Attendance Check Point** .
2. Click **Customize Attendance Status on Device** on the upper-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.

Schedule Template

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

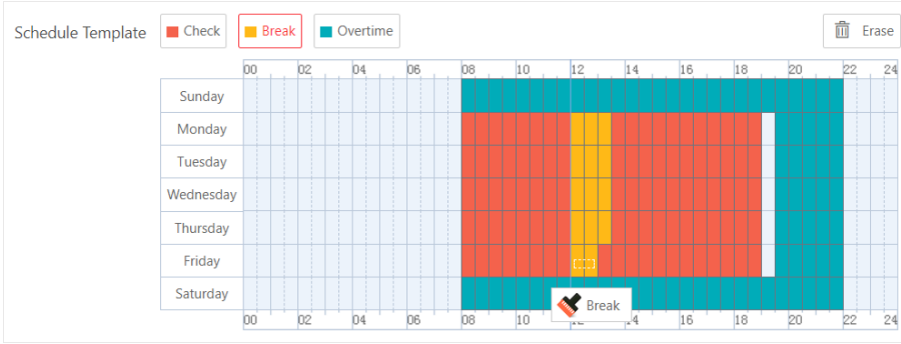


Figure 15-5 Schedule Template

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.

15.1.2 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. On the top, select **Attendance**.

2. Select **Basic Configuration → Pay Code** on the left.

3. Click **Add** to open the Add Pay Code pane.
4. Create the pay code name.
5. 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.

6. 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.

7. Set the Min. Value for the rounding rule.
8. Set whether to display the pay code in report.
9. Click **Add**.
10. 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.

15.1.3 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.

On the top, select **Attendance**.

Select **Basic Configuration → Fixed Code** on the left.

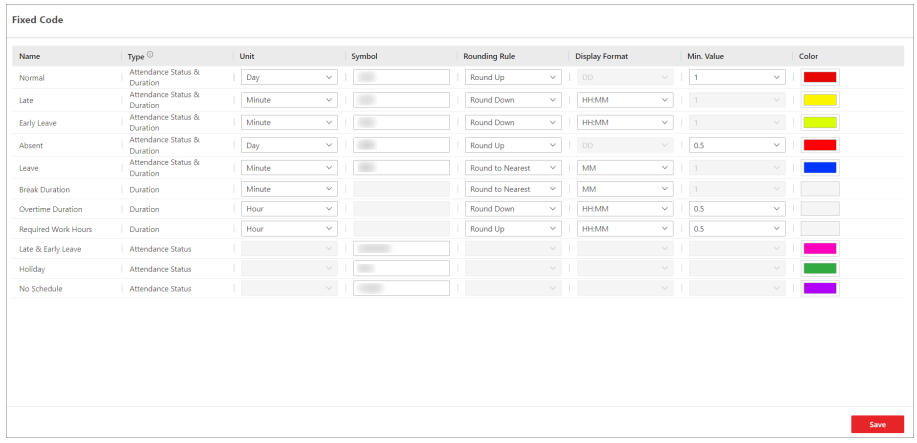


Figure 15-6 Edit Fixed Code

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.

Color

Used for making differences among fixed codes.

15.1.4 Configure Storage Settings

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

1. On the top, select **Attendance**.
2. Select **Basic Configuration → Storage Settings** on the left.
3. Select a backup file to be restored.
4. Click **Save**.

15.2 Configure Global/Department Attendance Rules

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 rule or a department rule. You can configure a department with a department rule which has higher priority than the global rule used for the whole company or institution.

15.2.1 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.

On the top, select **Attendance**. Select **Attendance Rule → Global Rule / Department Rule** on the left. For department rules, you need to click **Add** on the Department Rule page, and then check departments.

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.

15.2.2 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.

Steps

1. On the top, select **Attendance**.
2. Select **Attendance Rule → Global Rule / Department Rule** on the left.
3. **Optional:** For department rules, you need to click **Add** on the Department Rule page, and then check departments.
4. Select **Overtime** on the right to enter the overtime settings page.
5. In the Overtime Workday/Weekend area, switch on **Calculate Overtime** to set the calculation mode of overtime duration on workdays and weekends.

   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 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

Select the overtime levels and drag on the time slot to set the range of the selected overtime levels. The total work hours will be calculated according to the work hour rate of each overtime level.

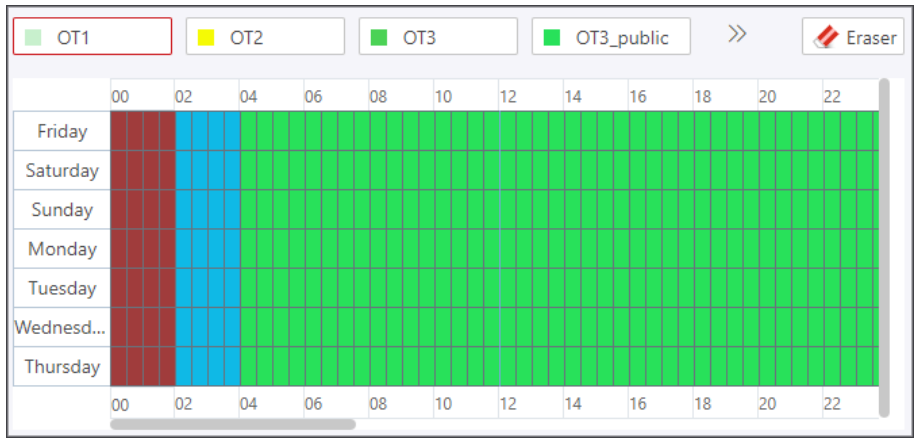


Figure 15-7 Overtime Level Settings

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.

6. In the Overtime on Holidays area, switch on **Calculate Overtime**, and then set the overtime rule for 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**.

7. **Optional:** Switch on **Calculate Overtime** in the Overtime Not in Valid Attendance Check Period area to count the extra work time outside the valid check-in/out period as valid overtime. And then select an overtime level from the drop-down list.
8. For global rule, click **Save**; for department rule, click **Add** on the top right.

15.2.3 Configure Attendance Calculation Mode

You can set the mode of attendance calculation.

Choose a calculation mode of work duration.

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 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.

15.2.4 Define Absence

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

On the top, select **Attendance**. Select **Attendance Rule → Global Rule / Department Rule** on the left. For department rules, you need to click **Add** on the Department Rule page, and then check departments. Click **Attendance Calculation** on the right.

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

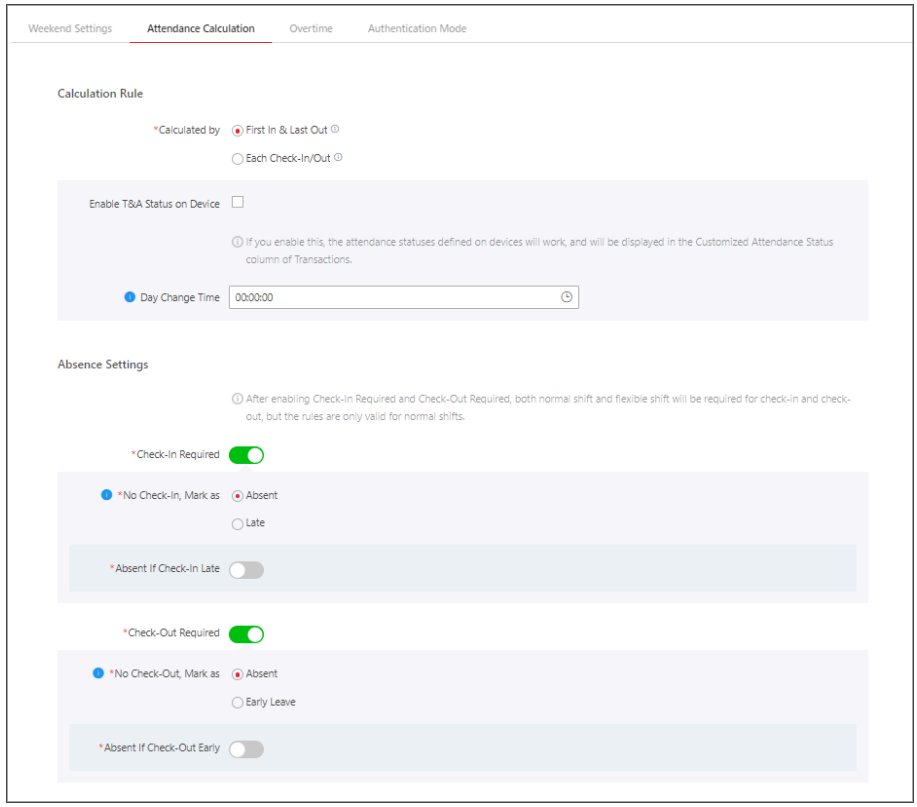


Figure 15-8 Absence Settings

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.

15.2.5 Add Holidays Requiring Attendance

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

Steps

1. On the top, select **Attendance**.
2. Select **Attendance Rule → Global Rule / Department Rule** on the left.
3. **Optional:** For department rules, you need to click **Add** on the Department Rule page, and then check departments.
4. Select the **Attendance Calculation** tab.

Note

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

5. 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. On the top, select **Attendance**.
2. Select **Basic Configuration → Holiday Settings** on the left. You can also access the Holiday Settings page in **System** on the top.
3. 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.

15.2.6 Calculation of Leaves

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

On the top, select **Attendance**. Then, select **Attendance Rule → Global Rule / Department Rule** on the left.

Note

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

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

15.2.7 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.

On the top, select **Attendance**. Select **Attendance Rule → Global Rule / Department Rule** on the left. Select **Authentication Mode** on the right.

Note

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

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

Note

This function requires device capability.

15.3 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.

15.3.1 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. On the top, select **Attendance**.
2. Select **Shift → Break Timetable** on the left.
3. Click **Add**.
4. 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.

5. Click **Add** to finish adding the timetable, or click **Add and Continue** to finish adding the timetable and add a new break timetable.
6. **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*** .

15.3.2 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. On the top, select **Attendance**. Select **Shift → Timetable** on the left.
2. Click **Add**.
3. In **Basic Settings**, create a timetable name.
4. 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.
5. 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**.

6. 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*** .

Count Break Time in Work Hours

Check the function to include the break time into work hours. It is checked by default.

7. In **Attendance Calculation**, switch on **Attendance Required During Time Period**, and set the following parameters.

Note

The attendance calculation rule has higher priority than the department and global rules.

Set Calculation Rule

Switch on to set the calculation method of work duration.

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.

8. 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 an overtime timetable in ***Configure Overtime Parameters*** . You can also refer to this chapter for explanations of the parameters.

9. **Optional:** In **Timetable Overview**, view the timetable in a time line.

Figure 15-9 Timetable Overview

Note

You can drag the time line to the left or right.

10. 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*** .

15.3.3 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. On the top, select **Attendance**.
2. Select **Shift → Timetable** on the left.
3. Click **Add**.
4. In **Basic Settings**, create a timetable name.
5. 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.
6. 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.

7. 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*** .
- Check **Count Break Time in Work Hours** to include the break time into work hours.

8. 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.

9. 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.

10. **Optional:** In **Timetable Overview**, view the timetable in a timeline.

Figure 15-10 Timetable Overview

Note

You can drag the timeline to the left or right.

11. 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*** .

15.4 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. On the top, select **Attendance**.
2. Select **Shift → Shift** on the left.
3. Click **Add**.
4. Set the shift's basic information, including creating a descriptive name and editing its description.
5. **Optional:** Select another shift from the drop-down list of **Copy from** field to copy the shift information to the current shift.
6. 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.

7. Select **Normal Shift** or **Flexible Shift** as the shift type.

   The corresponding timetables of normal shift or flexible shift will be displayed.

8. Select a timetable and click on the table below to apply the timetable on each day.

   Note

   - For **Normal**, you can apply more than one timetable in one day which requires the employees to check in and check out according to each timetable. The start and end work time and the valid check-in and out time in different timetables can not be overlapped.
   - You can use up to 8 different timetables in one shift.

9. Switch on **Configure Attendance During Holidays**, and select the holidays. On holidays, the shift will not be effective.

   Note

   For setting the holiday, refer to ***Set Holiday*** .

10. 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*** .

15.5 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 department or persons, or add a temporary schedule, so that it will calculate the attendance records for persons according to this schedule.

15.5.1 Schedule Overview

The schedule overview shows the schedule information of each person in the department. You can also view the detailed schedule of one person for each day in one month.

On the top, select **Attendance**.

Select **Schedule → Schedule Overview** on the left.

Select a department on the left, you can view the schedule information about every person in the department.

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 click **Edit** or **Delete** to edit the schedule or delete the schedule.

Note

If any schedule is not assigned to the person, you can click **Set Schedule** to assign a schedule to him/her.

15.5.2 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.

Before You Start

Make sure you have added departments and persons. For details, refer to ***Add Departments*** and ***Add Person*** .

Steps

1. On the top, select **Attendance**. Select **Schedule → Department Schedule** on the left.
2. Perform one of the following to set the schedule.

Assign One by One	On the left, select a department you want to assign shift to, and click **Add Schedule**.
Batch Assign	Click to open the panel. Select the departments.

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.

   Note

   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.
7. **Optional:** Perform the following operations.

Edit Schedule	Select a department in the list and click to edit the department's 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.

15.5.3 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.

Before You Start

Make sure you have added the person(s). For details, refer to ***Add Person*** .

Steps

Note

The person schedule has the higher priority than department schedule.

1. On the top, select **Attendance**. Select **Schedule → Person Schedule** on the left.
2. **Optional:** Select a department on the left, enter keywords in text field, or check **Show Sub Department** to filter the persons.
3. Select the persons you want to assign the shift to.
4. Click **Add Schedule** to enter the Add Schedule page.
5. 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*** .
6. **Optional:** Click to select attendance check points linked with the schedule.

   Note

   Only authentications at the linked attendance check points will be counted.
7. **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.

8. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.
9. **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.

15.5.4 Add Temporary Schedule

You can add a temporary schedule for the 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 Person*** and ***Add Shift*** .

Steps

Note

The temporary schedule has the higher priority than other schedules.

1. On the top, select **Attendance**. Select **Schedule → Temporary Schedule** on the left.
2. Click **Add** to enter Add Temporary Schedule page.
3. In **Select Person(s)** 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. In the top of the timetable, 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).

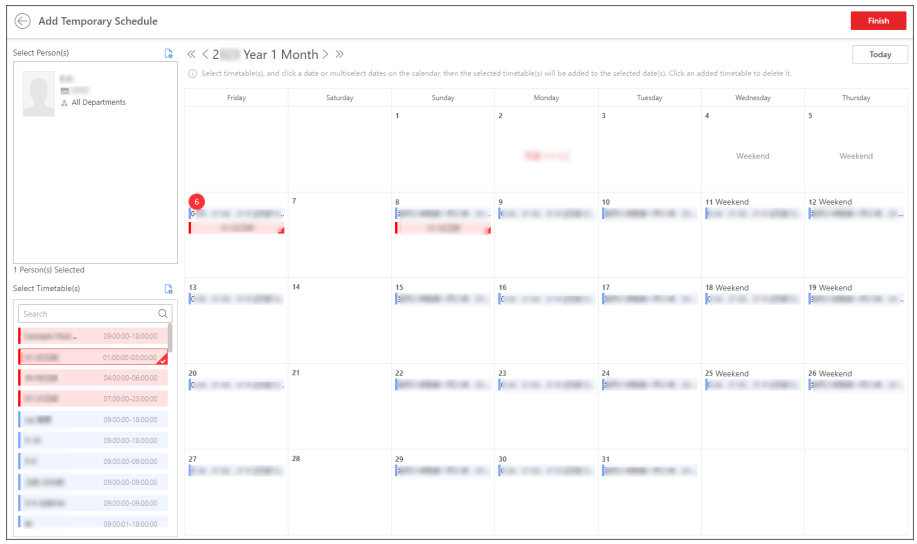


Figure 15-11 Add Temporary Schedule

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**.
9. After adding temporary schedules, you can perform the following operations.

Edit Temporary Schedule	Select a schedule in the list and click **Edit** to edit the schedule.
Delete Temporary Schedule	Select a schedule in the list and click **Delete Schedule** to delete the schedule. Also, you can click **Delete All** to delete all of the schedules.

15.6 Configure Calculation Mode of Attendance Results

You can set the attendance calculation mode as manual calculation or auto calculation.

15.6.1 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. On the top, select **Attendance**.
2. Select **Attendance Calculation** on the left, and then select **Manual Calculation** on the right.
3. Set the start time and end time for attendance calculation.
4. Select **All Persons** or **Specific Person(s)** for attendance calculation.
5. Click **Calculate**.

   Note

   It can only calculate the attendance data recorded within three months.

15.6.2 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. On the top, select **Attendance**.
2. Select **Attendance Calculation** on the left, and then select **Auto Calculation** on the right.
3. Select a time in **Calculate at**.
4. **Optional:** Enable **Recalculate Historical Data**.
5. Click **Save**.

15.7 Application Flow Management

The platform supports configuring department application flows and personal application flows. Application flow defines the approval process of department applications and personal applications. When configuring application flows, you can specify application departments, applicants, reviewers and persons to be notified of the review results via configuring approval roles. Applications from specified departments/persons need to be reviewed according to the configured application flow.

15.7.1 Add a Approval Role of Application Flow

Approval roles of application flow are for specifying reviewers and persons to be notified of review results. You can add and assign approval roles to persons. The persons assigned with the approval role as reviewer has the permission to approve/reject applications of specified departments/persons, and the person assigned with the role to be notified has the permission to receive and view review results. For example, you can add an approval role as Manager, and assign this role to specified persons. When configuring the personal application flow, you can select the reviewer's approval role as Manager, and the persons assigned with the Manager approval role has the permission to review the applicant's application.

Before You Start

Make sure the current admin user has the permissions for configuring approval roles. For details about user permissions, refer to ***Role and User Management*** .

Steps

1. On the top, select **Attendance**.
2. Select **Application Flow → Approval Role** on the left.
3. Click **Add** to add a new approval role.
4. Create a name for the approval role.
5. Click to select the person(s) to assign the approval role to.

Note

- You can click **More** to enable custom information items and enter the keyword in the text filed to search for matched persons.

  Note

  Make sure you have customized additional information of persons. For details about customizing additional information, refer to ***Customize Additional Information*** .
- You can check **Include Sub Department** to display the persons of sub-departments.

6. Click **Add** to finish adding the approval role.
7. Optional: Perform the following operations as needed.

Edit Approval Role	Select an approval role in the list and click to edit it.
Delete Approval Role	• Select one or multiple approval roles in the list and click **Delete** to delete the approval roles. Also, you can click **Delete All** to delete all approval roles. • Select an approval role from the list, and click to delete it.
Assign Approval Role to More Persons	Select an approval role in the list, and on the right pane, click **Assign To** to select persons to assign the approval role to.

Unassign Approval Role	Select an approval role in the list, and on the right pane, select the person(s) and click **Unassign** to unassign the approval role for the selected person(s). Also, you can **Unassign All** to unassign the approval role for all persons.

15.7.2 Add a Department Application Flow

Department application flow defines the approval process of reviewing applications from a department. Applications of the persons in the specified application department should be reviewed according to the department application flow.

Before You Start

- Make sure the current admin user has the permissions for configuring the application flow. For details about user permissions, refer to ***Role and User Management*** .
- Make sure you have added roles of the application flow. For details about adding roles, refer to ***Add a Approval Role of Application Flow*** .

Steps

1. On the top, select **Attendance**.
2. Select **Application Flow → Application Flow** on the left.
3. Click **Department Application Flow**.
4. On the left, set the basic information of the application flow.

The application is enabled by default. You can switch off **Enable Application Flow** to disable the application flow.

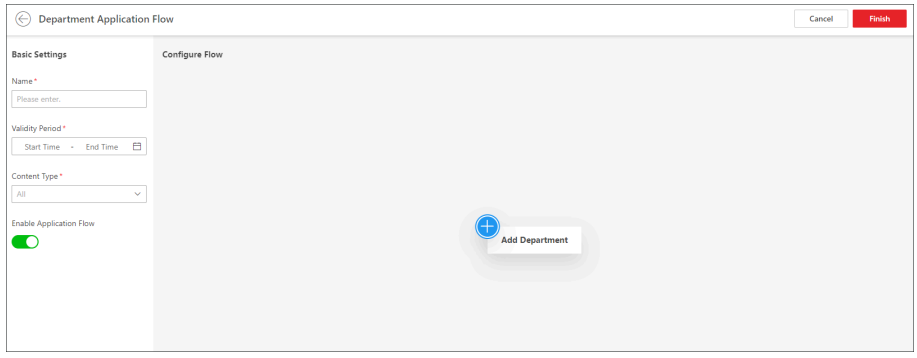


Figure 15-12 Add Department Application Flow

5. Click **Add Department** to select the application department(s).
6. Click + to add the reviewer(s) for the application flow.

1) Select the approval role of the reviewer(s).
2) Select the department(s) of the selected role(s) allowed to review applications.

Note

If the reviewers are from the different department, you need to select **All Departments**.

3) **Optional:** Select the approval role(s) to be notified of the review results in the current node.

4) **Optional:** Select the department(s) of the approval role(s) to be notified.

Note

If the person(s) to be notified are from the different department, you need to select **All Departments**.

5) Click **Add**.

Note

You can repeat this step to add more reviewers and persons to be notified for the application flow.

7. Click **Finish**.

8. Optional: Perform the following operations as needed.

Edit Application Flow	In the application flow list, click the name of the application flow to edit it. • Click **Reviewer** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete the node of the application flow.
Disable Application Flow	When adding an application flow, it is enabled by default. You can disable it in the application flow list.
Delete Application Flow	In the application flow list, you can click **Delete** to delete an application flow, or click **Delete All** to delete all application flows.

15.7.3 Add a Personal Application Flow

Personal application flow defines the approval process of reviewing applications of a person. Applications of the specified persons should be reviewed according to the personal application flow.

Before You Start

- Make sure the current admin user has the permissions for configuring the application flow. For details about user permissions, refer to ***Role and User Management*** .
- Make sure you have added roles of the application flow. For details about adding roles, refer to ***Add a Approval Role of Application Flow*** .

Steps

1. On the top, select **Attendance**.

2. Select **Application Flow → Application Flow** on the left.

3. Click **Personal Application Flow**.

4. On the left, set the basic information of the application flow.

The application is enabled by default. You can switch off **Enable Application Flow** to disable the application flow.

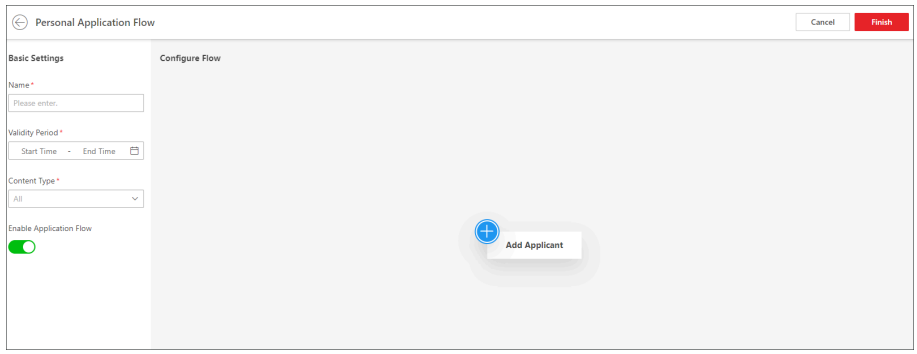


Figure 15-13 Add Personal Application Flow

5. Click **Add Applicant** and to select the applicant(s).

Note

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

6. Click + to add the reviewer(s) for the application flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department(s) of the selected role(s) allowed to review applications.

   Note

   If the reviewers are from the different department, you need to select **All Departments**.

   3) **Optional:** Select the approval role(s) to be notified of the review results in the current node.
   4) **Optional:** Select the department(s) of the approval role(s) to be notified.

   Note

   If the person(s) to be notified are from the different department, you need to select **All Departments**.

   5) Click **Add**.

   Note

   You can repeat this step to add more reviewers and persons to be notified for the application flow.

7. Click **Finish**.
8. **Optional:** Perform the following operations as needed.

Edit Application Flow	In the application flow list, click the name of the application flow to edit it. • Click **Reviewer** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete the node of the application flow.
Disable Application Flow	When adding an application flow, it is enabled by default. You can disable the flow in the application flow list.

Delete Application Flow	In the application flow list, you can click **Delete** to delete an application flow, or click **Delete All** to delete all application flows.

15.8 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.

15.8.1 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.

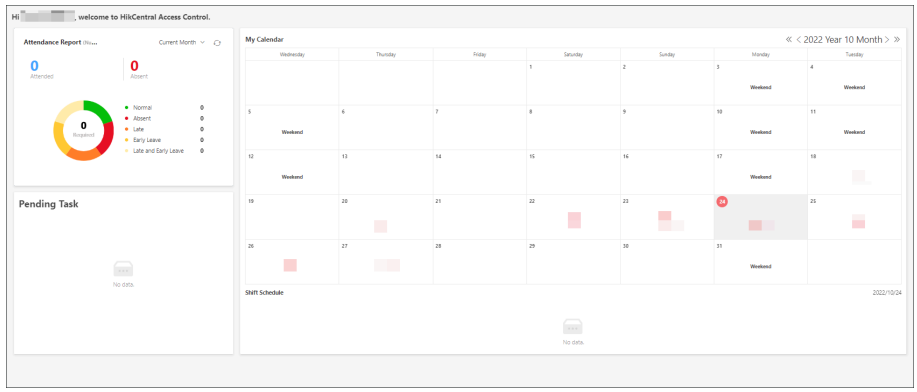


Figure 15-14 Overview of Personal Attendance Data

In **Attendance Report**, you can click ⌄ to select a time period to view the attendance records in the time period.

In **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*** .

In **Pending Task**, you can select an application and click **Handle** to handle the application.

15.8.2 Submit and View Applications

As an employee, you can submit attendance applications for leave, overtime, or attendance correction. Also, you can view the application details and the application flow to know the status of each handling.

Apply for a Leave

As an employee, you can apply for a leave by yourself. And the application will be reviewed by the administrator.

Before You Start
Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

Steps
1. Select **Apply → Leave** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Leave Type

   The leave type such as sick leave, maternity leave, annual leave, etc.

   Start Time

   The start time of leave.

   End Time

   The end time of leave.

   Application Reason (Optional)

   The application reason for the leave.

   Attachment (Optional)

   The attachment for the leave application, such as the medical records for sick leave.
5. Click **Add**.

What to do next
View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

Apply for a Check-In/Out Correction

As an employee, you can apply for correcting the check-in or check-out records according to actual need (e.g., you forgot to check in or check out). And the application will be reviewed by the administrator.

Before You Start
Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

Steps
1. Select **Apply → Attendance Correction** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Correction Item

   The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.

   Actual Time

   The right time of the attendance item.

   Application Reason (Optional)

   The application reason for the correction.

   Attachment (Optional)

   The attachment for the correction application, such as the certificate of the right attendance time.
5. Click **Add**.

What to do next
View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

Apply for Overtime

As an employee, you can apply for working overtime. And the application will be reviewed by the administrator.

Before You Start
Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

Steps
1. Select **Apply → Overtime** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Overtime Type

   The type of working overtime.

   Start Time

   The start time of working overtime.

   End Time

The end time of working overtime.

Application Reason (Optional)

The application reason for the leave.

Attachment (Optional)

The attachment for the overtime application.

5. Click **Add**.

What to do next

View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

View Submitted Applications

The employee can view the submitted application(s) for attendance.

Note

Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

1. Select **Apply → Leave/Overtime/Attendance Correction** on the left.
2. Select the **Pending** or **Closed** tab.
3. 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.
4. You can also select multiple employees to review or undo the employee's attendance applications.

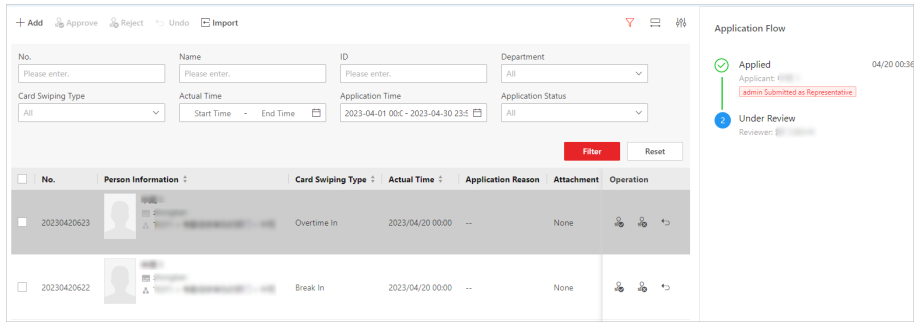


Figure 15-15 Review or Undo Employees' Applications

15.8.3 Review Employees' Applications

After employees submit the attendance applications for leave, overtime, or attendance correction, the administrator should review (including approving or rejecting) or undo the employee's application.

1. On the top, select **Attendance**. Select **Review → Leave/Attendance Correction/Overtime** .
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 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.
5. You can also select multiple employees to review or undo the employee's attendance applications.

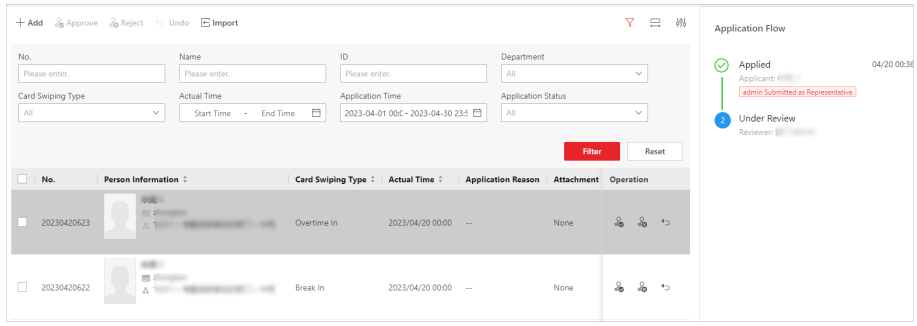


Figure 15-16 Review or Undo Employees' Applications

15.8.4 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.

Note

Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

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.

15.9 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.

15.9.1 Apply for a Leave

As the administrator, you can perform leave application for the employee one by one.

Steps

1. On the top, select **Attendance**.
2. Select **Review → Leave** .
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Leave Type

   The leave type such as sick leave, maternity leave, annual leave, etc.

   Start Time

   The start time of leave.

   End Time

   The end time of leave.

   Application Reason (Optional)

   The application reason for the leave.

   Attachment (Optional)

   The attachment for the leave application, such as the medical records for sick leave.

   Auto Approve (Optional)

   If the box is checked, the added application for the person will be approved automatically.
6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

15.9.2 Apply for a Check-In/Out Correction

As the administrator, you can apply for correcting the check-in or check-out records for the employee one by one.

Steps

1. On the top, select **Attendance**.
2. Select **Review → Attendance Correction** .
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Correction Item

   The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.

   Actual Time

   The right time of the attendance item.

   Application Reason (Optional)

   The application reason for the correction.

   Attachment (Optional)

   The attachment for the correction application, such as the certificate of the right attendance time.

   Auto Approve (Optional)

   If the box is checked, the added application for the person will be approved automatically.
6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

15.9.3 Apply for Overtime

As the administrator, you can apply for working overtime for the employee one by one.

Steps

1. On the top, select **Attendance**.
2. Select **Review → Attendance Correction** .
3. **Optional:** Click , enter a person's full name, card No., ID, etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Overtime Type

The type of working overtime.

Start Time

The start time of working overtime.

End Time

The end time of working overtime.

Application Reason (Optional)

The application reason for the leave.

Attachment (Optional)

The attachment for the overtime application.

Auto Approve (Optional)

If the box is checked, the added application for the person will be approved automatically.

6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

15.9.4 Import Applications

As the administrator, you can batch apply for leave, overtime, or attendance correction for multiple employees.

Steps

1. On the top, select **Attendance**.
2. Select **Review → Leave / Attendance Correction / Overtime** on the left.
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. Click **Import**.
5. In the pop-up window, click **Download Template** and edit the related information in the downloaded template.
6. Click and import the template with the corrected attendance records.
7. Click **Import**.

What to do next

You can review or undo the imported applications. For details, refer to ***Review or Undo Applications*** .

15.9.5 Review or Undo Applications

As an administrator, after applying for employees' leave, overtime, or attendance correction, you can review (including approve or reject) or undo the application.

1. On the top, select **Attendance**.
2. Select **Review → Leave/Attendance Correction/Overtime** .
3. (Optional) Click to filter the target employee by setting conditions (such as name, ID, department).
4. Select the target employee, the employee's application flow will be displayed on the right.
5. 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.
6. You can also select multiple employees to review or undo the employee's attendance applications.

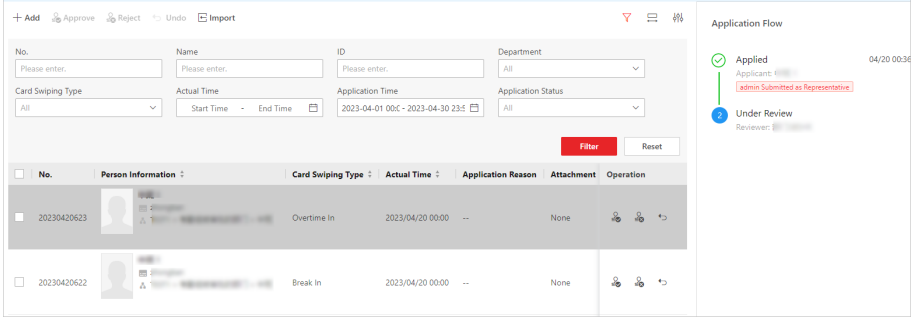


Figure 15-17 Review or Undo Employees' Applications

15.10 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.

15.10.1 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.

On the top, select **Attendance**. Then select **Attendance Record → Transaction** on the left.

Click **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.

15.11 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.

15.11.1 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.

15.11.2 View Daily/Weekly/Monthly/Summary Attendance Reports

You can view and export daily/weekly/monthly/summary attendance reports.

On the top, select **Attendance**.

Select **Daily Report**, **Weekly Report**, **Monthly Report**, or **Summary Report** on the left as needed.

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/ 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 ⚙ 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 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.

15.11.3 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 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. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email parameters such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

The report is an Excel file.

1. On the top, select **Attendance**.
2. Select **Basic Configuration → Report Settings → Scheduled Report** on the left.
3. Click **Add** (for first time) or click + .
4. Create a descriptive name for the report.
5. Select a type, format, and language for the scheduled report.

Note

You can select **TXT** as the format if the report type is **Time Card**.

6. In **Statistics Department**, check the department(s) of which the persons' attendance data will be delivered in this report.
7. In **Person**, click to include individual persons whose attendance data will be delivered in this report.
8. Set the statistical cycle to **By Day**, **By Week**, or **By Month** and set the report time range and sending time.

Daily Report

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.

Weekly/Monthly Report

The platform will send one report at the sending time every week or every month. The report contains the persons' attendance results of the recent one/two weeks or current/last month of the sending date.

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.

Note

- Daily or weekly report is not available when you set report type to monthly or weekly report.
- 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*** .

9. **Optional:** Click to set the effective period for the report.
10. **Optional:** Select and enable the way of sending the report from **Send Report via Email**, **Upload to SFTP**, and **Save to Local Storage**.

Note

To set up the SFTP or local storage, click > **SFTP Settings** or **Configure Local Storage**.

11. **Optional:** Select the email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

12. Click **Add** to save the report schedule.

    The report will be generated and sent to the recipient at the specified sending time.

15.11.4 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, select **Attendance**.
2. Select **Custom Report** on the left.
3. Click + .
4. Create a descriptive name for the report in the **Report Name** field.
5. Choose whether to merge the data of the same person/department/date.
6. Select a sorting rule for records from the **Table Display Rule** drop-down list.
7. Select the data items you want to include in the report from **Optional Fields**.

Note

- Selected data items will show in **Selected Fields**.
- You can drag the items in **Selected Fields** to set the order of the items.

8. **Optional:** Click **Preview** to view the report to make sure the format and content are correct.
9. Click **Add** to save the custom report, or click **Add and Continue** to add another one.
10. **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.
Send Report Regularly	You can set a schedule to send the report regularly. See details in ***Send Attendance Report Regularly*** .

Chapter 16 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.

16.1 Basic Settings of the Platform

You can add platform users as recipients of calls from devices. After adding recipients, when someone calls the platform, the recipient can receive the call. You can also add a call schedule template which defines when door stations can call indoor stations or call center. Besides, you can configure general parameters, including the storage location of configuration data and records, call parameters (such as the ring tone, auto hang up duration, and the maximum speaking duration with the device), and you can enable the function of receiving calls.

16.1.1 Add Call Recipients

After adding call recipients, when someone calls the system, the added recipient can receive and answer the call.

Note

Before recipients can receive calls form devices on the platform, you need to enable **Receive Calls** on the Call Parameter page. For details about enabling this function, refer to ***Configure General Parameters*** .

On the top, select **Video Intercom**. Then, select **Basic Settings → Call Recipient** on the left.

Click **Add** to add recipients.

Select users to receive calls and supported calling devices, and then click **Add**.

On the Call Recipients page, perform the following operations as needed.

- Check one or more call recipient and click **Delete** to delete the call recipient(s), or click ∨ → **Delete All** to delete all call recipients.
- In the upper-right corner, enter the keyword to search for specific users.

16.1.2 Add Call Schedule Template

Call schedule template defines when door stations can call indoor stations or the call center. For example, if a resident is absent from home during workdays, while he/she is at home during weekends and holidays, the resident can customize a schedule template which calls the management center during workdays and calls the indoor station during weekends and holidays.

Steps

1. On the top, select **Video Intercom → Basic Configuration → Call Schedule Template** .
2. Click + to add a schedule template.

   The two default templates, namely All-Day Call Schedule Template for Indoor Station and All-Day Call Schedule Template for Call Center, cannot be edited or deleted.
3. Create a name for the template.
4. **Optional:** Select an existing template from the **Copy from** drop-down list.
5. Select **Indoor Station** or **Management Center**.

   Note

   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.
6. **Optional:** Edit weekly schedule.

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 04 : 00 – 04 : 30 .
Erase Task Time	Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.

7. **Optional:** Click **Add Holiday** to select an existing holiday template, or click **Add** to add a new template. For detailed information, see ***Set Holiday*** .
8. Click **Add** to save the template.
9. **Optional:** Select a template from the template list, and then click 🗑 to delete it.

What to do next

Set call schedule for indoor stations and call center to define in which time period door stations can call indoor stations or call center. For details, refer to ***Add Call Schedule for Door Stations*** .

16.1.3 Configure General Parameters

You can configure general parameters, including the storage location of configuration data and records, and call parameters (such as the ring tone, auto hang up duration, and the maximum speaking duration with the device), and you can enable the function of receiving calls.

On the top, select **Video Intercom**. Then, select **Basic Configuration → General** on the left.

Configure the following parameters as needed, then click **Save** to save settings.

Storage of Configuration Data

You can store the configuration data of video intercom.

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.

Storage of Records

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 ***Configure Storage for Imported Pictures and Files*** .
- For **pStor**, make sure you have added pStor as the recording server. For details, refer to ***Add pStor*** .

Call Parameter

Ringtone

Click ··· to select a ring tone and click **Play** to play the ring tone.

Auto Hang Up After

The call will be hung up automatically after the duration.

Max. Speaking Duration with Indoor Stations / Door Stations / Access Control Devices

Enter the maximum duration during which you can speak with the device.

Receive Calls

Switch on **Receive Calls** to receive the calling notification from the device to the platform.

16.2 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 Mifare encryption, you can enable **Mifare Encryption** and select the sector. Only the card with the same encrypted sector can be granted by swiping the card on the card reader.

Related Cameras

For indoor station, you can relate the camera(s) with it to view the video of the related camera(s) on the indoor station. You can also delete the related camera(s). Up to 16 related cameras are supported.

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.

16.3 Manage Video Intercom Device

You can set location information for video intercom devices. After setting location information, you need to apply settings to all devices or the specified device(s).

16.3.1 Set Locations for Video Intercom Devices

You can add single device or batch add devices that have been added to the platform, and set location information for the added device(s).

Before You Start
Make sure you have added video intercom devices to the system.

Steps
1. On the top, select **Video Intercom**.
2. Select **Device Management** on the left.
3. Add the device(s).
   - Add single device.
     a. Click **Add** to add the device which has been added to the platform.
     b. Select a device type and a device.
     c. Set the location of the device, and click **Add**.
   - Add devices in a batch.
     a. Click ⌄ → **Batch Add** to add devices which have been added to the platform.
     b. Select the device type.
     c. Select the adding mode to add device.

Manually Select	i. Select devices manually in the drop-down list. ii. Set required information. **Note** - If the community is divided into different sections, enter the corresponding number. If not,enter 1. - If the building is composed of only one unit, enter 1.
Batch Import	i. Click **Download Template** to download the template file to your PC. ii. Open the downloaded template file and enter the required information. iii. Click 🗁 to select the file finished in the previous step.

     d. Click **Add**.
4. Click a device name.
5. In Location area, set parameters as needed.

Note
- If the community is divided into different sections, enter the corresponding number. If not,enter 1.
- If the building is composed of only one unit, enter 1.
- The parameters displayed vary with device types.

6. Set **Main and Sub Relation** to Main Module or Sub Module.

Note

This feature is only Available for door stations and indoor stations.

7. Click **Save** to save your edited information.

16.3.2 Apply Location to Video Intercom Devices

After setting location information for video intercom devices, you need to apply settings to devices.

On the top, select **Video Intercom**. Then, select **Device Management** on the left.

Click **Apply Settings**.

Select the device(s) to apply.

All Devices

By default, the changed settings will be applied to all devices. If you check **Apply (Initial)**, first clear all former information applied to the devices, and then apply all settings configured on the platform this time to the devices.

Specified Device(s)

Click to select devices. The settings will be applied to the selected device(s).

Apply (Initial)

First clear all former linkages applied to the devices, and then apply all linkages configured on the platform this time to the devices. This mode is mainly used for first-time deployment.

Click **Apply** to apply settings to the device(s).

The procedure of applying information will be displayed in the pop-up window, and the reasons for failures will be displayed in the Reason column. Move the cursor over , and click **Retry** to apply the settings to devices again. Also, move the cursor over , and click **View Details** to view the details. You can also click **Retry** to re-apply settings to devices.

16.4 Video Intercom Application

You can configure call schedule templates to define when indoor stations and call centers can receive the call from door stations. After you configure the templates, you can add the templates for door stations so that they will distribute calls to indoor stations or call centers as configured in the schedule template. Finally, you can apply call schedule to devices, so devices such as indoor/door stations and call centers can execute commands from the platform. You can also link single person to indoor stations for calling residents. In addition, you can 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.

16.4.1 Start Live View of Video Intercom Devices

For video intercom devices, you can start live view of these devices.

Before You Start
Make sure you have added the devices to the platform.

Steps
1. On the top, select **Access Control**. Then, select **Real-Time Monitoring** on the left.
2. Click a device and select **Live View**.

   The live view window of the device will be displayed on the right.
3. Hover the cursor on the live view window to show the tool bar at the bottom. You can click different buttons according to your need.

   Example

   You can click to start two-way audio with persons by the device.

16.4.2 Add Call Schedule for Door Stations

You can add call schedule for door stations to define when door stations can call indoor stations or call centers.

Before You Start
Make sure you have configured call schedule templates. For detailed information, see ***Add Call Schedule Template*** .

Steps
1. On the top, select **Video Intercom → Video Intercom Application → Door Station Call Schedule Settings** .
2. Click **Add** to add a door station call schedule.
3. Select a door station in the list.
4. Select a schedule template and room number for each button.

   Note

   As long as a template contains calling the call center, the Room cannot be selected. See ***Add Call Schedule Template*** for details about how to set a call schedule template.
5. **Optional:** Click to view the schedule details.
6. Click **Add** to save the schedule.

   The added schedule will be displayed in the list.
7. **Optional:** Perform the following operations.

Filter Door Stations	• Click on the top right to set conditions such as Door Station, Location Information, or Application Status to filter door stations. • Click **Reset** to reset search conditions.

Delete Door Stations	Select door stations and click **Delete** or click ⌄ → **Delete All** to delete the door stations.

What to do next

You can apply call schedules to devices. For detailed information, see ***Apply Call Schedule to Door Stations*** .

16.4.3 Apply Call Schedule to Door Stations

You can apply call schedules to door stations so that the communication between devices and the platform will be supported.

Before You Start

Make sure that you have added call schedules for door stations. For detailed information, see ***Add Call Schedule for Door Stations*** .

Steps

1. On the top, select **Video Intercom** → **Video Intercom Application** → **Door Station Call Schedule Settings** .
2. Click **Apply Settings** on the top of the device list page.
3. Select **All Door Stations** or **Specified Door Station**.
4. **Optional:** If you choose **Specified Door Station**, select door station(s) or click to batch select the door station(s) that you want to apply the call schedule to and click **Add**.

   Note

   Only the door stations with added call schedules will be displayed.
5. **Optional:** Check **Apply (Initial)** to clear all former call schedules applied to the devices, and then apply all call schedules configured on the platform.
6. Click **Apply**.

   The procedure of applying information will be displayed in the pop-up window, and the reasons will be displayed in the Reason column. Move the cursor over , and click **Retry** to apply the schedules to devices again. Also, you can move the cursor over , and click **View Details** to view the details. You can also click **Retry** to re-apply the schedule to devices.

16.4.4 Link Resources with Indoor Stations

After adding an indoor station to the system, you can link single person with an indoor station or multiple persons with the indoor station(s) at a time, so that linked persons can calling residents. Besides, you can relate a doorbell with an indoor station.

Link Persons to an Indoor Station

The person needs to be linked to an indoor station, which is used for calling residents. You can link single person to an indoor station or multiple persons to indoor station(s) at a time. Here we introduce you how to batch link persons to indoor station(s).

Steps

Note

For details about linking single person to an indoor station, refer to ***Add a Person Manually*** .

1. On the top, select **Video Intercom**.
2. Select **Video Intercom Application → Link Person to Indoor Station** on the left.
3. Click **Link**.

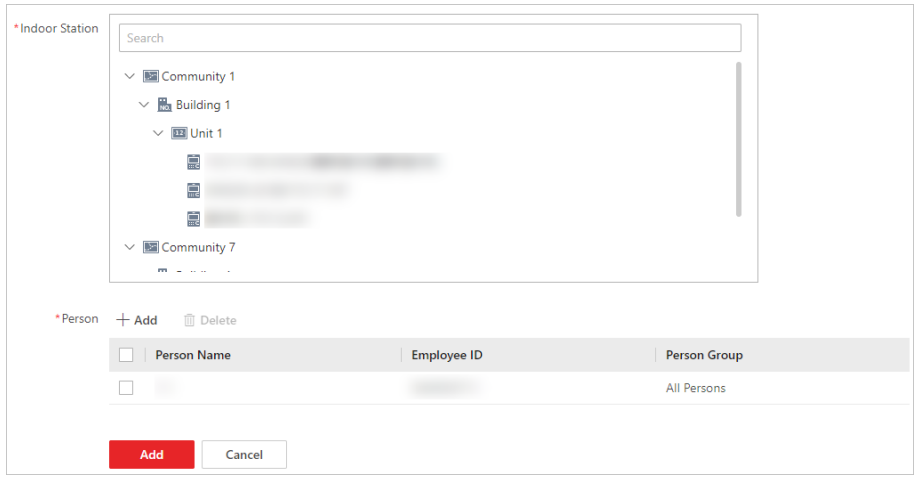


Figure 16-1 Add Linked Person

4. Select an indoor station.

   Note

   Up to 10 persons can be linked to one indoor station and the person cannot be linked to multiple indoor stations.

5. Click **Add** to select persons to be linked to the indoor station.
6. Click **Add**.

   The linked person information will be applied to the indoor station(s).

7. **Optional:** Perform the following operations.

Filter Indoor Stations	• Click ▽ on the top right to set conditions such as device name, location, or person name to filter indoor stations. • Click **Reset** to reset search conditions.
Unlink Person from Indoor Stations	Select indoor stations and click **Unlink**.

View Linked Person	On the page of the added indoor station list, click › to view linked persons.
Change Linked Persons	On the page of the added indoor station list, click the name of the indoor station to change linked persons.

Link Doorbell to an Indoor Station

You can link a doorbell with an indoor station. If the Call Management Center function of this doorbell is disabled, you can call the linked indoor station by the doorbell.

If you have added the doorbell to the system, you can link the doorbell with an indoor station as the following steps. If not, you can also link the doorbell with an indoor station when adding the doorbell (see ***Manage Video Intercom Device*** for more details).

Steps

1. On the top, select **Video Intercom → Video Intercom Application → Link Doorbell to Indoor Station** .
2. Click **Link** to enter the Link Doorbell with Indoor Station page.

   The added doorbells are displayed in the list.
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.
5. **Optional:** Check one or more doorbells and click **Unlink** to delete the doorbell(s).

Result

The doorbell will be linked to the selected indoor station(s).

16.4.5 View Event/Alarm Related Notices

You can filter and view event/alarm related notices by setting conditions. After filtering, you can export matched records, reapply failed notices, etc.

On the top, select **Video Intercom → Apply Data to Indoor Station → Manage Notice** on the left.

Select the **Event/Alarm-Related Notice Applying Records** tab.

In the top right corner, click ▽ to set conditions to search for matched records. Click **Filter** and the matched records will be displayed.

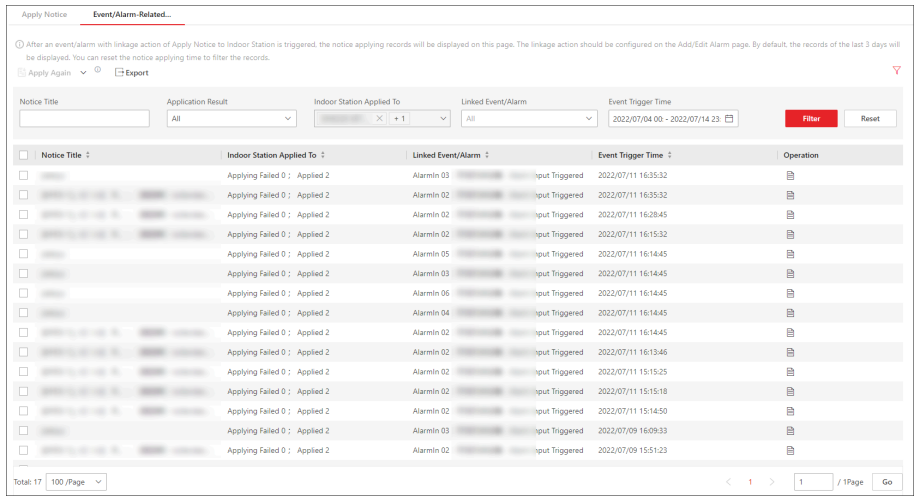


Figure 16-2 Filter Event/Alarm-Related Notice Applying Records

For the matched records, perform the following operations as needed.

Operation	Description
Reapply Failed Notice	• Check the failed notice(s) and click **Apply Again** in the top left corner to reapply the notice(s). • In the top left corner, click ⌄ → **Reapply All** to reapply all failed notices.
Export Records	In the top left corner, click **Export** to export all matched records.
View Notice Details	In the Operation column, click 🗎 to view the basic information and the application status of the notice. **Note** If the notice fails to be applied, you can also click **Apply Again** to reapply it in the Details panel.

16.4.6 Apply Data to Indoor Station

The platform supports applying notices and software packages to indoor stations. This is used for scenes where you want to notify people an emergency in a batch, or install a software on indoor stations in a batch. After applying a software package to the indoor stations, the software will be installed automatically.

Manage Notices

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. Before applying the copied notice, you can also edit the notice.

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.

Apply Software Package to Indoor Station

You can apply a software package to selected indoor stations and install the software automatically.

Before You Start

Make sure you have added indoor station(s) to the system. For details, refer to ***Add a Video Intercom Device by IP Address*** .

Steps

1. On the top, select **Video Intercom → Apply Data to Indoor Station → Apply Software Package** .

2. Click **Apply Software Package** on the top.

3. Select **All Indoor Stations** or **Specified Indoor Station(s)**.

Note

If you select **Specified Indoor Station**, check indoor stations and click .

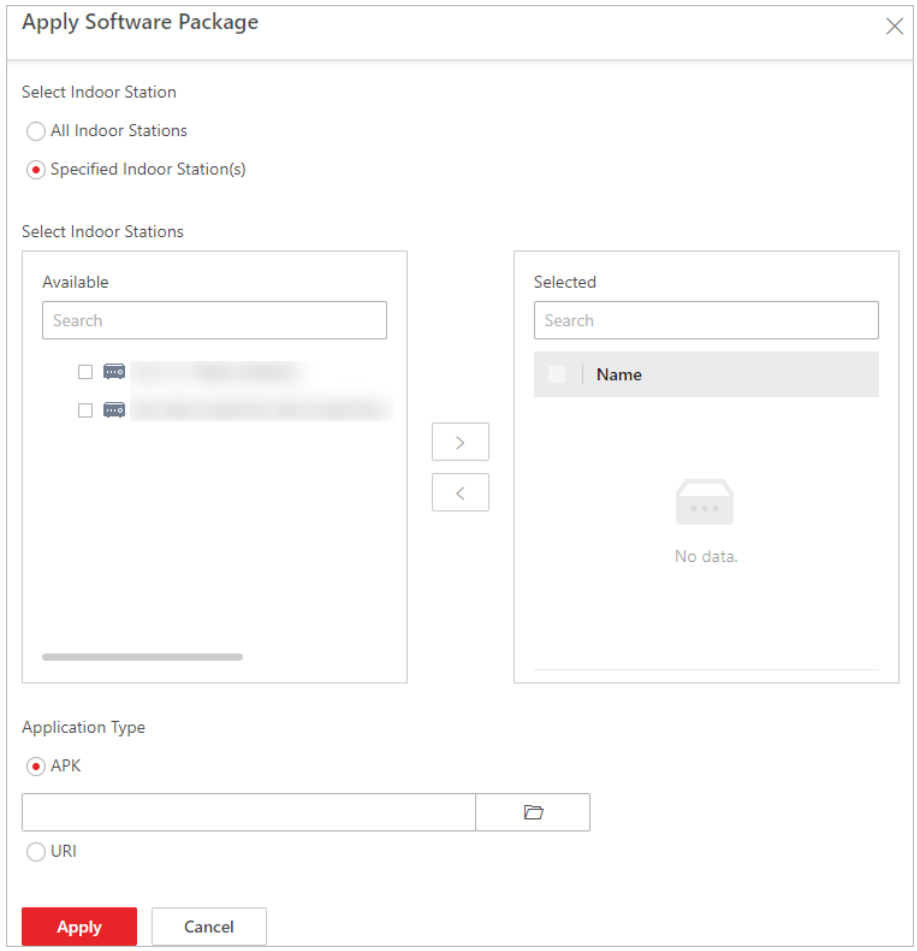


Figure 16-3 Apply Software Package

4. Select an application type.

APK

You need to upload an APK file so that the platform can send it to the device.

URI

Enter a URI so that the device will download the package via the URI and install it.

5. Click **Apply**.

The device will install the software package automatically.

16.4.7 Apply Advertisements to Door Stations

You can add picture(s) or a video in the advertisements, then apply the advertisements to door stations. After applying advertisements, you can filter or delete them.

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.

Note

You can click ‹ to remove it from the selected door station list on the left.

4. Add picture(s) or a video for an advertisement to be applied to door stations.

Note

For the picture advertisement, you can add more than one picture. For the video advertisement, you can add only one video.

- 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**.
7. Optional: Perform the following operations.

Filter Advertisement	Click ▽ and set filter conditions such as device name, and then click **Filter**.
Delete Advertisement	Select one or multiple advertisements in the list and click **Delete** to delete the advertisements. Also, you can click **Delete All** to delete all of the advertisements.

16.4.8 Search Data Recorded on Video Intercom Devices

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

Steps

1. On the top, select **Access Control**. Then, select **Search** on the left.
2. Select **Device Recorded Data Retrieval** on the left.
3. In the Time drop-down list, select a time range for searching.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

4. Switch on the resource types where you want to search for records.

Access Point(s)

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

Device

Devices include access control devices, elevator control devices, and video intercom devices. The data recorded in these devices covers all events triggered by devices (such as device faults).

Alarm Input

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

5. Select the record source(s) and record type(s).
6. Click **Search**.

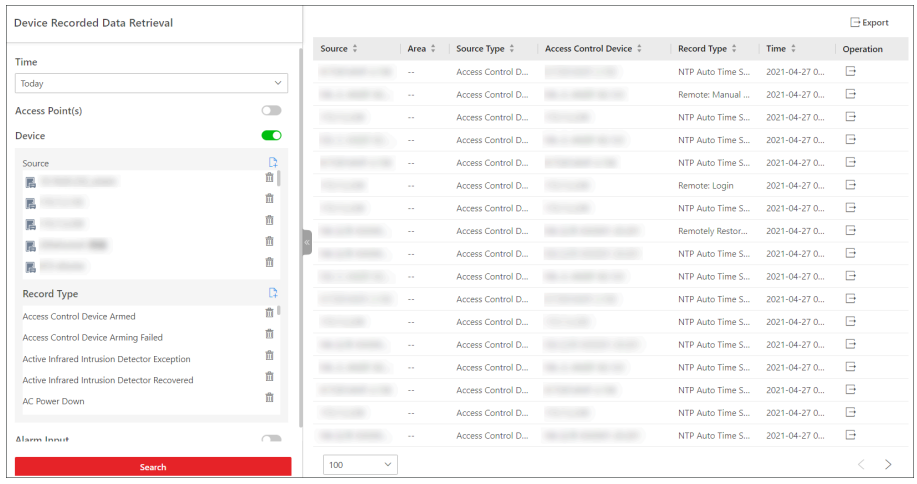


Figure 16-4 Device Recorded Data Retrieval

7. **Optional:** Perform further operations on the searched records.

View Record Details	Click the device name in the Source column to view the record details, such as 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 or a CSV file.

16.5 Call & Talk

In Call & Talk module, you can view contacts of indoor stations in a specific unit and call an indoor station conveniently. You can also view and export recents which include details such as the device name, call status, and device location. Besides, you can download recorded audios to the local PC.

16.5.1 Call an Indoor Stations

You can view names and locations of indoor stations, and person information. You can also call indoor stations directly on the platform in situations such as when the call the to the door station fails and when an emergency occurs.

On the top, select **Video Intercom**. Then, select **Video Intercom → Contacts** on the left.

On the left of the Contacts page, select an unit. The indoor stations in this unit will be listed on the right. In the upper-right corner, you can also set conditions and enter the keyword to search for indoor stations.

Click to call the indoor station.

16.5.2 View Recents

You can view and export call logs which include details such as the device name, call status, and device location. You can also download recorded audios to the local PC.

On the top, select **Video Intercom**. Then, select **Video Intercom → Recents** on the left.

Perform the following operations as needed.

Operation	Description
Export Logs	Check one or more devices and click **Export** to export call logs to Excel/CSV file format.
Filter Logs	Click to set conditions and click **Filter** to search for logs.
Download Recorded Audio	Click to download the recorded audio in MP4 format to the local PC.

Chapter 17 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. For details, refer to ***Set User Preference*** .

17.1 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.

17.1.1 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 **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.

17.1.2 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. For details, refer to ***Configure Other Parameters*** .

17.2 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.

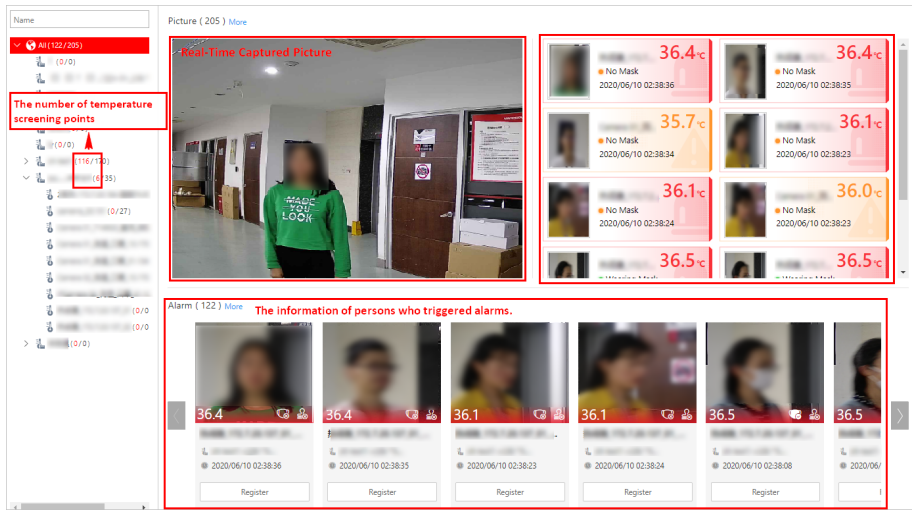


Figure 17-1 Real-Time Skin-Surface Temperature

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.

17.3 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.

17.4 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.

17.4.1 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.

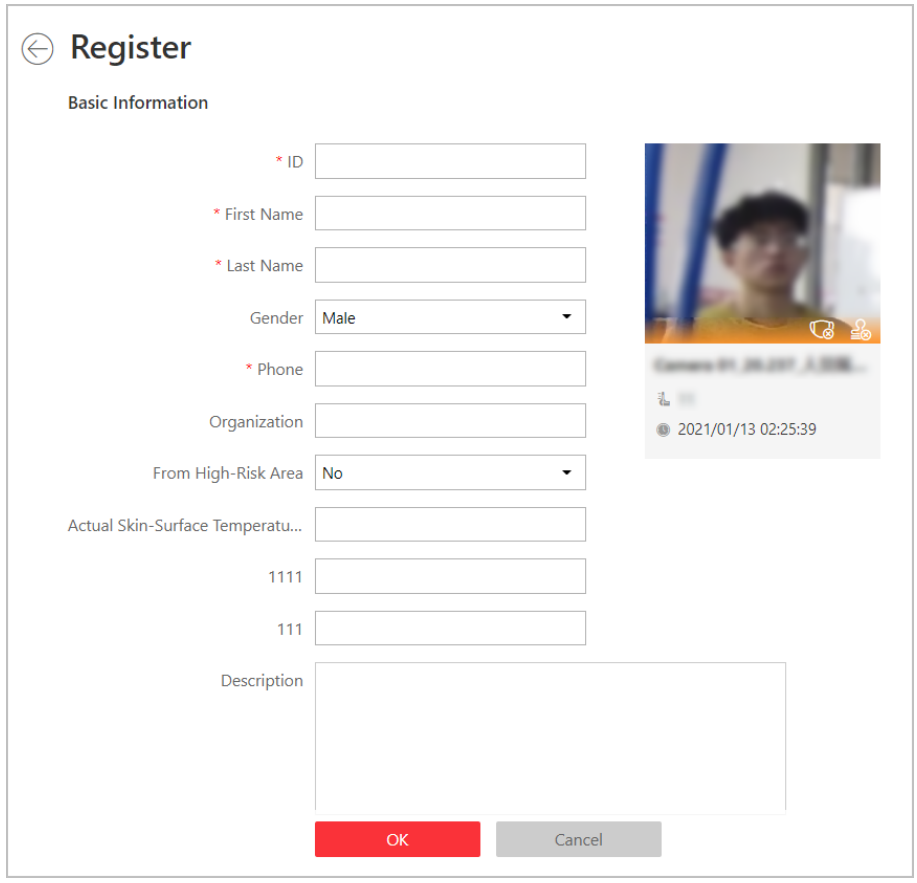


Figure 17-2 Register Page

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.

17.4.2 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.

17.4.3 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.

17.5 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**.

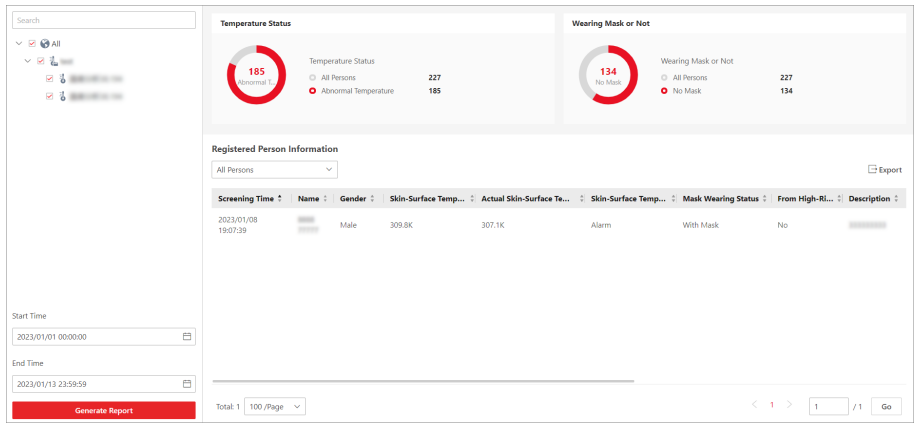


Figure 17-3 Skin-Surface Temperature Screening Records

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.

Chapter 18 Map Management

On the e-map, which is a static map, you can set and view the geographic locations of the installed cameras, alarm inputs, and alarm outputs, etc.

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 (e.g., camera, alarm input) placed on the map are called hot spots). You can see the physical locations of the cameras, alarm inputs, and alarm outputs, etc., and in what direction the cameras are pointing. 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.

After configuring the e-map via Web Client, you can view the live video and playback of the elements via Web Client.

For the hot regions, hot spots, combined alarms, you can set different icons for them to recognize them quickly on the map.

Steps

1. On the top, select **Map**.

2. Click **Map Settings** on the top right to enter the map settings page.

3. Click **Icon Settings** to set the customized icons.

1) Click **Hot Region** or the following device types 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 path.

Note

The icon picture format can only be PNG, JPG, or JPEG.

4) **Optional:** Click to constrain the aspect ratio.
5) Click **Save**.

Result

You can view the GIS map on Map Monitoring page and perform the following operations in the map area.

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	Hover over a resource, and you can view its latitude and longitude on the GIS map.

18.2 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. On the top, select **Map**.
2. Click **Map Settings** on the top right to enter the map settings page.
3. Select an area on the left.
4. Open the Add Map pane.
5. Select an adding mode.
6. 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.

7. Click **Add**.
8. 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. An accurate map scale is essential for defining a radar's detection area. Perform this step if you plan to add a radar to the map.

1) Click **Calibrate** 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.

9. 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.

10. Optional: Perform the following operations after adding map in the map area.

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	Drag the map or the red window in the lower part to adjust the map area for view.

18.3 Add Hot Spot on 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. Refer to ***Add E-Map for Area*** for details about adding e-map.

Steps
1. On the top, select **Map**.
2. Click **Map Settings** on the top right to enter the map settings page.
3. Select an area on the left.
4. **Optional:** Select a map.
5. Click **Resource Group** on the right.
6. Select a device type and an area from the drop-down lists.
7. Select a device and drag it to the map.

   The hot spot is displayed on the map.
8. **Optional:** Perform the following operations after adding the hot spot.

Adjust Hot Spot Location	Drag the added hot spot on the map to the desired 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.

18.4 Add Hot Region on Map

The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Steps
1. On the top, select **Map**.
2. Click **Map Settings** on the top right to enter the map settings page.
3. Select an area on the left.

4. **Optional:** Select a static map.
5. Click **+** on the **Hot Region** icon on the right.
6. Click a position on the map to select it as the location of the hot region.
7. Select an area from the area list.
8. Click **Save** on dialog to add the hot region.

   The added hot region icon will be displayed on the parent map.
9. **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.

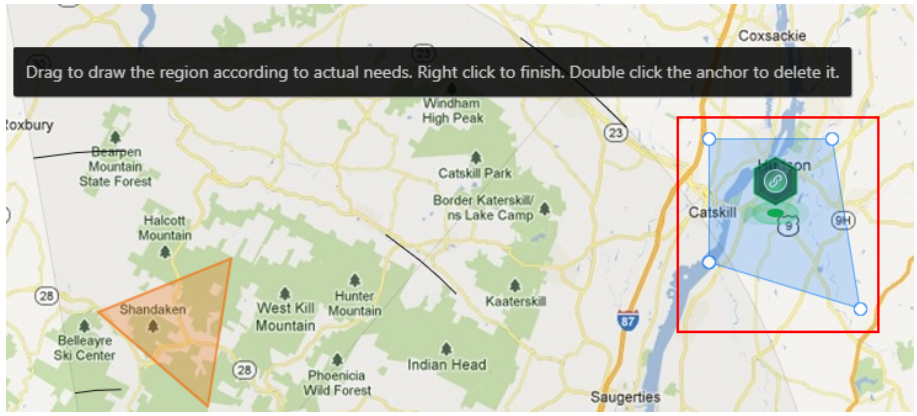


Figure 18-1 Edit Hot Region Area

18.5 Add Label on Map

You can add labels with description on the map.

Steps

1. On the top, select **Map**.
2. Click **Map Settings** on the top right to enter the map settings page.
3. Select an area on the left.
4. **Optional:** Select a static map.
5. Click **+** on the **Label** icon on the right.
6. Click on the map where you want to place the label.
7. Customize a name for the label, and you can input content for the label as desired.

8. Click **Save**.

The added label icon will be displayed on the map.

9. Optional: Perform the following operation(s) after adding the label.

Adjust Label Location	Drag the added label on the map to the desired locations.
Edit Label	Click the added label icon on the map to view and edit the detailed information, including name and content on the appearing dialog.
Delete Label	Click the label icon on the map and click **Delete** on the appearing dialog to delete the label.

18.6 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 border of the region for detection.

Currently, the following resource groups can be added on the map for further operations:

Pathway Analysis Group

After adding the pathway analysis group on the map, you can view the real-time number of people walking by in the Monitoring module on the Control Client.

For details about how to add a pathway analysis group, refer to .

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 ***Configure Area Anti-Passback Rules*** .

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***

Entry & Exit 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 Entry and Exit Counting Group*** .

Emergency Operation Group

After adding the emergency operation group on the map, you can operate access points (remaining locked/unlocked) in the group in a batch.

This function is mainly applicable for emergent situation. For example, after grouping the doors of the school's main entrances and exits into one emergency operation group, 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 an emergency operation group, refer to ***Add Emergency Operation Group*** .

18.7 Add Combined Alarm on Map

You can add the combined alarms on map to locate the alarm for a visualized monitoring.

Steps

1. On the top, select **Map**.
2. Click **Map Settings** on the top right to enter the map settings page.
3. Select an area on the left.
4. Optional: Select a map.
5. Click **Combined Alarm** on the right.
6. Drag a combined alarm to the map.

The combined alarm is displayed on the map.

7. Optional: Perform the following operations after adding the combined alarm.

Adjust Combined Alarm Location	Drag the added combined alarm on the map to the desired locations.
Edit Combined Alarm	Click the added combined alarm icon on the map and click **Edit** to edit the detailed information and selecting icon style).
Delete Combined Alarm	Click the combined alarm icon on the map and click **Delete** to remove the combined alarm from the map.

18.8 Operate Hot Spot

The resources added on the map are called the hot spots. The hot spots show the locations of the resources. You can operate the hot spot, such as starting live view of the door, arming or disarming the resources.

18.8.1 Preview Hot Spot

You can view locations of hot spots including cameras, alarm inputs, alarm outputs, access points, elevators, radars, sites, Under Vehicle Surveillance Systems (UVSS), 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.

Note

- 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.
- Click parking lot data, a panel of parking lot details will pop-up. You can view detailed parking lot information such as parking space occupancy rate and parking floor details.

5. Operate in the dialog.

- For camera and UVSS hot spot: Check the live view and playback of the camera, view its status, area, and remark, set the arming control, and view the history alarms.

  Note

  - To view the live view and playback of the camera, the user should be assigned with permissions of live view and playback of the camera. For details, refer to the *User Manual of HikCentral Access Control Web Client*.
  - For details about arming control, see ***Arm or Disarm Hot Spot*** .
  - For details about viewing history alarms, see ***View History Alarm*** .
- For alarm input hot spot: View its status, area, and remark, set the arming control, and view the history alarms.
- For alarm output hot spot: Turn on or off the linked alarm output.
- For access point hot spot: View the access point status, check the live view and playback of the access point's related camera(s), view the access point's basic information, control the door status, set the arming control, and view the history alarms and access records.

- For elevator hot spot: View the elevator status, area and remark, check the live view and playback of the elevator's related camera(s), control the floor status, set the arming control, and view the history alarms and access records.
- For radar hot spot: View the radar status, area and remark, check the live view and playback of the radar's related camera(s), set the arming control, view the history alarms.
- For radar PTZ camera hot spot: View camera's field of view and view the object's moving pattern.
- For site hot spot: View the site's resources and alarms which are not handled.
- For partition hot spot: Set the arming control including alarm clearing, disarming, away arming, stay arming, instant arming. For details, refer to ***Arm or Disarm Hot Spot*** .
- For parking lot hot spot: Click a certain floor and you will go to the parking lot management module so you can view the details of the parking floor in the parking lot.

  Hover your cursor on a parking lot, you can view the details of the parking lot. If nothing appears, you can click **Configure Now** to configure the parking lot.

18.8.2 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.

Before You Start

Configure the map settings via the Web Client. For details, see ***Map Management*** .

Steps

1.

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 to select a map.

4. Click the hot spot.

A window on which the related functions of the hot spot display is opened.

5. Click **Arm**/**Disarm** to arm/disarm the hot spot.

18.8.3 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.

Steps

1.

2. Click the hot spot.

A dialog pops up on which the related functions of the hot spot display.

3. Click to enter the event and alarm search page.

4. Search history alarms of the hot spot. See ***Search for Event and Alarm Logs*** for details.

18.9 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. On the top, select **Map**.
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.

18.10 Preview Resource Group

During displaying map, you can view locations and regions of the resource groups, including people counting group, multi-door interlocking group, and anti-passback group. You can also perform further operations on the resources in the group.

Note
Make sure you have configured the required resource group and map settings via the Web Client. For details, see ***Map Management*** .

On the top, select **Map**.

- People Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the region of the group will be highlighted on the map to notify the user on the Control Client.
- Pathway Analysis Group: You can view the real-time number of people walking by in the Monitoring module on the Control Client.
- Anti-Passback Group: When an anti-passback alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.
- Multi-Door Interlocking Group: When multi-door interlocking alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.
- Entry & Exit Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Control 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.

18.11 Operate Map

After opening map, you can perform one or more operations of the followings, such as zooming in or out map, selecting resource(s) on map, adding label, printing map, displaying map in full screen mode, and so on.After opening map, you can perform one or more operations of the followings, such as zooming in or out map, adding label, displaying map in full screen mode, and so on.

Zoom in/Zoom out Map

Use the mouse wheel or click + or − to zoom in or zoom out on the map.

Filter

Click and select the resource type you want to show on the map.

Add Label

Click to add a label with description to the map.

Search Location

By the search bar on the top of the map, you can search for hot spot/hot region on the e-map by entering keyword(s).

Chapter 19 Emergency Mustering

The emergency mustering helps users get prepared to account for all staff in a quick and efficient manner in an emergency situation, such as a fire.

You can configure an emergency solution beforehand and start a roll call by one click. In an emergency, the users can:

- Conduct a roll call with real-time data.
- Get immediate access to personal contact information.
- Filter persons based on status (In, Out & Not Check In, Checked In, and Unknown)

Based on the information provided by the platform, users can rescue persons who are still in the place.

On the top, select **Emergency Mustering** .

Select **Emergency Solution Settings** on the left.

Note

If you are configuring emergency solution for the first time, click **Configure**at the bottom of the page to enter the emergency solution configuration page.

Click **View Service Details** and configure the emergency solution following the guidance.

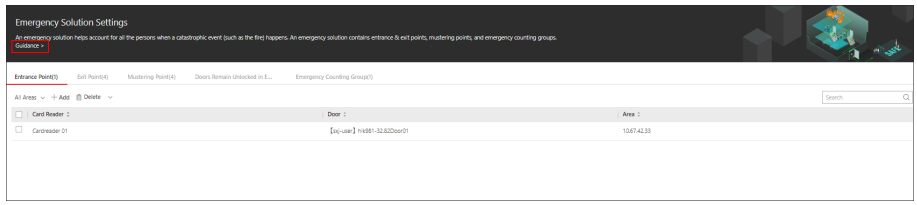


Figure 19-1 Entrance Point List

19.1 Emergency Solution Settings

An emergency solution refers to the preparation settings before a roll call. The emergency solution includes the settings of entrance points, exit points, mustering points, doors remaining unlocked in an emergency, and emergency counting groups. After setting the emergency solution, users can start a roll call by one click once an emergency happens.

On the top, select **Emergency Mustering**.

Select **Emergency Solution Settings** on the left.

1. Add Entrance Points

An entrance point is the card reader by which persons authenticate to check in before entering a place. If a person authenticates by an entrance point, the person's status is In.

Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as entrance points of the area.
You can check card readers and click **Delete** to cancel setting them as entrance points, or click ⌄ → **Delete All** to cancel setting all card readers as entrance points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the entrance points.
- To delete the entrance points, you should end the emergency first.

2. Add Exit Points

An exit point is the card reader by which persons authenticate for exiting from a place. If a person authenticates by an exit point, the person's status is Out.
Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as exit points in the area.
You can check card readers and click **Delete** to cancel setting them as exit points, or click ⌄ → **Delete All** to cancel setting all card readers as exit points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the exit points.
- To delete the exit points, you should end the emergency first.

3. Add Mustering Points

A mustering point is the card reader located in a refuge. When an emergency happens, persons exit from the place where they are, go to the refuge, and check in by the mustering point. The status of persons who have checked in at the mustering point is Out & Checked In.
Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as mustering points in the area.
You can check card readers and click **Delete** to cancel setting them as mustering points, or click ⌄ → **Delete All** to cancel setting all card readers as mustering points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the mustering points.
- To delete the mustering points, you should end the emergency first.

4. Add Doors Remaining Unlocked in Emergency

A door remaining unlocked in an emergency refers to the door that will be turned to the status of Remain Unlocked once an emergency happens. Thus the persons inside the place can exit from the place without authentication at the card reader.
Click ⌄ besides **All Areas** and select an area. Click **Add** and select doors to set them as doors remaining unlocked in an emergency in the area.
You can check doors and click **Delete** to delete them, or click ⌄ → **Delete All** to delete all doors.
You can also enter a door name on the top right to search for it.

Note

- Make sure you have added the door to the platform before selecting the doors.
- To delete the doors, you should end the emergency first.

5. Add Emergency Counting Groups

An emergency counting group refers to a person group based on which you can know how many persons are in, out, or out & checked in when the platform is in an emergency.
Click + to open the Add Emergency Counting Group pane. Enter a name for the group and click to add persons to the group. Click **Add** to add more persons to the group after adding the group.

Note

- Make sure you have added the persons to the platform beforehand.
- You can click **More** to enable custom information items and enter the keyword in the text filed to search for matched persons.

  Note

  Make sure you have customized additional information of persons. For details about customizing additional information, refer to ***Customize Additional Information*** .
- If you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

You can perform the following operations.

- Click ⌄ besides the **1 Day(s) Before** to update the persons in the group.
- Click a person name to view person details.
- Select a group and click 🗑 to delete it, or click ⌄ → **Delete All** to all groups.
- Check persons and click **Delete** to remove the selected persons from the group, or click ⌄ → **Delete All** to remove all the persons from the group.

19.2 Start a Roll Call

After configuring the emergency solution, you can start a roll call by one click once an emergency happens.

On the top, select **Emergency Mustering**.

Select **Roll Call** on the left.

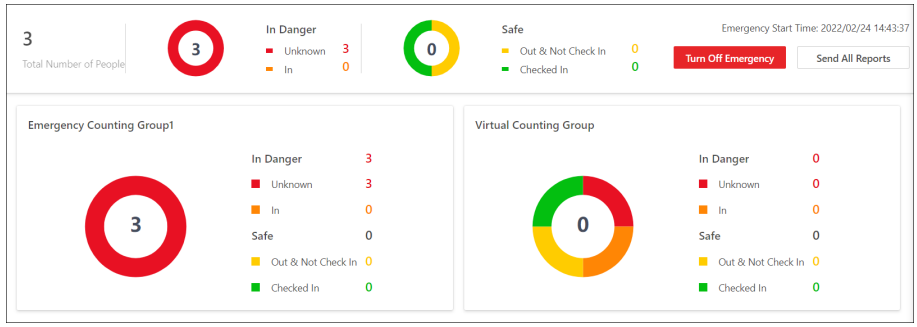


Figure 19-2 Data of Emergency Mustering

On the top left, the total number of persons in emergency counting groups is displayed. On the right of the total number of persons, the number of persons in danger and safe are both displayed. The persons in danger refer to persons who are still inside (checked in at the entrance point but did not check out at the exit point) the place where the emergency happens and the persons who did not check in at the entrance point. The persons who are safe refer to persons who have checked out at the exit point but not checked in at the mustering point and persons who have checked in at the mustering point.

The data of each emergency counting group is also displayed. You can click a group name to enter the page of the group for details. Click to check in a person who shows at the mustering point but the person status is not Checked In.

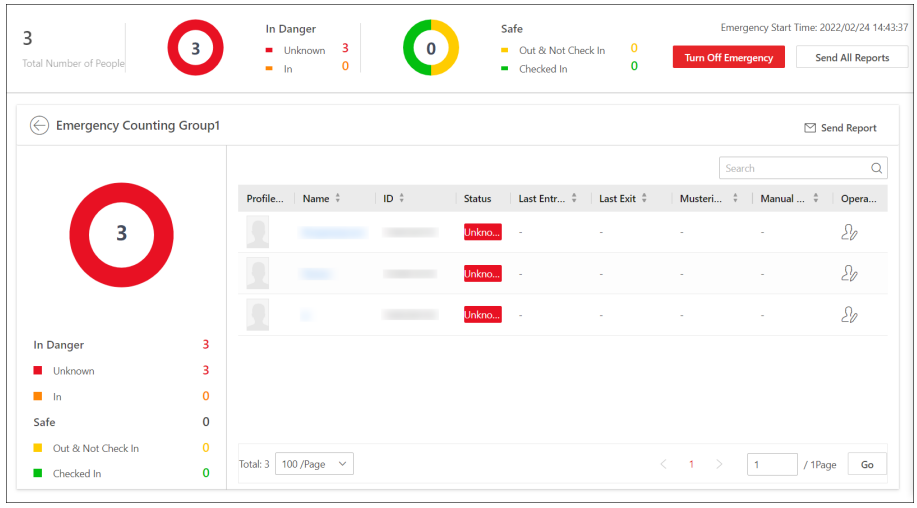


Figure 19-3 Data of an Emergency Counting Group

The virtual counting group refers to a group consisting of persons who are not added to any emergency counting group.

Perform the following operations if you need.

- Click **Turn Off Emergency** to end the emergency status of the platform.
- Click **Send All Reports** and select an email template to send the data of all the emergency counting groups to the recipients.

Note

- It is extremely important to remember that the data displayed and the reports contained in the email can only ever be accurate if all users follow the conventions of the system.
- During the emergency, editing the emergency solution is not allowed. You should end the emergency before editing it.

Chapter 20 System Configuration

The System page allows you to set basic parameters for the system, such as defining a customized name for your site, setting the WAN IP address for allowing to access your system via WAN (Wide Area Network), and configuring NTP (Network Time Protocol) settings to synchronizing the time between the system and the NTP server.

- For the system with Remote Site Management module, you can enable it to receive the registration from Remote Site.
- For the system without Remote Site Management module, you can set to register it to the Central System as a Remote Site.

20.1 Set User Preference

For different nations, regions, cultures and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, including the first day of a week and the temperature unit.

On the top, select **System**.

Select **Normal → User Preference** on the left.

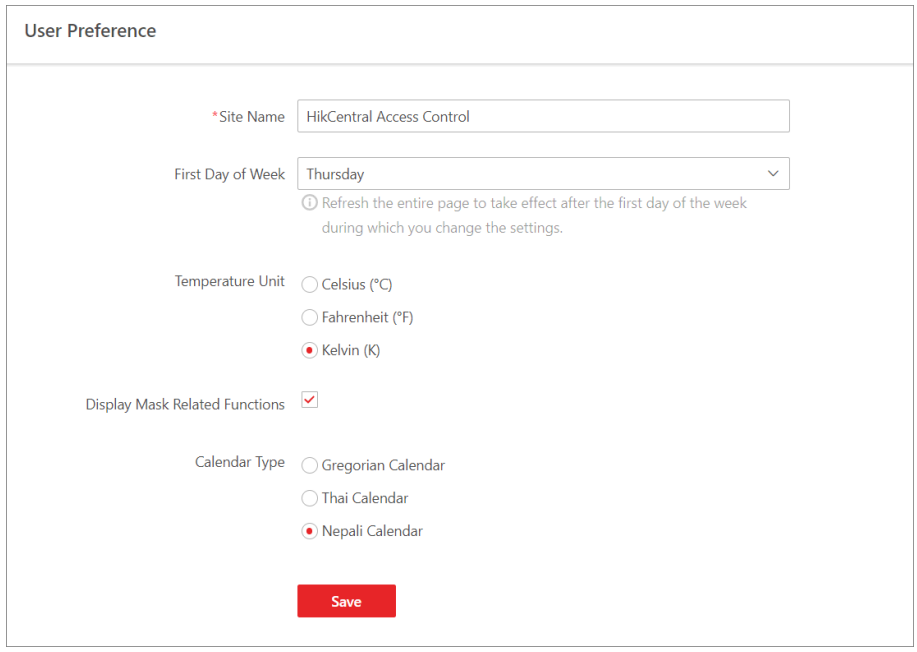


Figure 20-1 User Preference

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 intelligent analysis report generation, attendance settings, 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.

20.2 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.

On the top, select **System**.

Select **Normal → Holiday Settings** on the left.

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.

Click **Add** to open the adding holiday dialog.

Enter the holiday name and select **Regular Holiday** as the holiday type.

Set the parameters according to the following instructions:

Start Time

The start date of the holiday.

Holiday

The lasting days of the holiday.

Repeat Annually

If checked, the system will generate the date of the holiday according to the date of the VSM server.

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.
Click **Add** to open the adding holiday dialog.
Enter the holiday name and select **Irregular Holiday** as the holiday type.
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.

Holiday

The lasting days of the holiday.

Repeat Annually

If checked, the system will generate the date of the holiday according to the date of the SYS server.

Note

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

20.3 Set Printer

You can set printer(s) for the system, which can be used to print the stranded person list in some urgent evacuation scenario, such as fire hazard.

Note

Make sure the printer(s) are installed in the same network with the SYS server.

On the top, select **System**.

Select **Normal → Printer Settings** on the left.

Click **Add** and select the printer(s) detected by the HikCentral Access Control.

Note

After setting printer(s) for the system, you can link the printer when configuring alarm/event whose source type is alarm input. For details, refer to ***Add Normal Event and Alarm*** .

You can click in the Operation column to delete the printer.

You can also click **Delete All** to delete all printers.

20.4 Set Card Template

You can set the styles for card templates. After settings, the card will be applied in the format of the template.

Steps

1. In the top-left corner of the Home page, select → **All Modules** → **General** → **System Configuration** → **Normal** → **Card Template** .
2. On the top, select **System**.
3. Select **Normal** → **Card Template** on the left.
4. Click **Add**.
5. Create a name for the template.
6. **Optional:** Select the shape of the template.
7. 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. You can set the font and the font size for the text after clicking the text field.
Content	Check the attribute(s) for the content of the template. You can also click **Custom Information** to customize the attributes for the template.
Configure Text Settings	Set the text style as needed. You can set the text to bold, align content,etc.

Note

- You can drag any edge or corner to adjust the size of the picture and text box.
- You can select one or multiple text boxes on the template and click , , or to adjust the alignment of the text in the box.
- You can select multiple elements on the template and click , , or to adjust these elements.
- You can right-click on the element (except the background picture) and click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down** to adjust the layer of the element displayed on the template.

8. **Optional:** Set the back style of the template.

Note

You can set the back style according to step 5.

9. Click **Add** to add the template and go back to the card template list page.

   The email template will be displayed on the card template list.

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

View Template	Click ◎ to view the template.
Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click 🗑 in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

Note

On the card template list page, there are two default templates. You can view default templates but cannot edit or delete them.

20.5 Set NTP

You can set the NTP server for synchronizing the time between the resources (devices managed in the platform, recording servers, sites, SYS, etc.) and the NTP server.

Steps

1. On the top, select **System**.
2. Select **Network → NTP** on the left.
3. Switch on **Time Synchronization** to enable the NTP function.
4. Set the NTP server address and NTP port.

Note

If the local NTP service has been configured, you can click **Detect Local NTP** to fill in the NTP server address and NTP port automatically.

5. Enter the interval for the automatic time synchronization.
6. **Optional:** Click **Test** to test the communication between the resources and the NTP server.
7. **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.

8. Click **Save**.

20.6 Set Active Directory

If you have the 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 HikCentral Access Control conveniently.

Steps

1. On the top, select **System**.

2. Select **Network → Active Directory** on the left.

3. Configure the basic information parameters to connect to the AD domain controller.

Domain Name

The domain name of the AD domain controller.

Note

- HikCentral Access Control only supports the NetBIOS format, e.g., TEST\user, instead of the DNS Domain name format.
- To get the NetBIOS domain name, open the CMD window and enter ***nbtstat – n***.
  The NetBIOS domain name is the one in **GROUP** type.

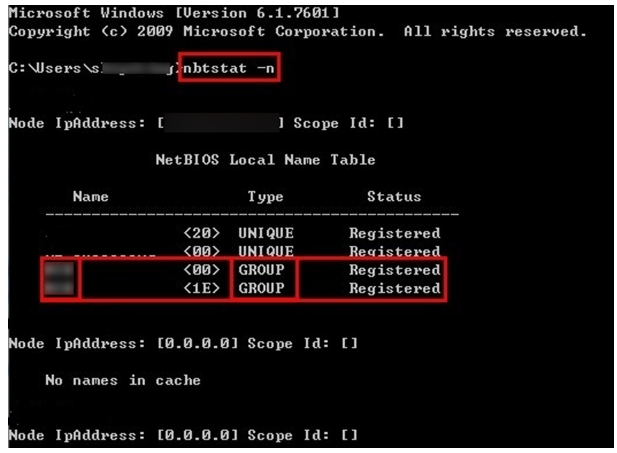


Figure 20-2 How to Get NetBIOS Domain Name

Host Name

The DNS server's IP address. You can get it in Network Connection Details.

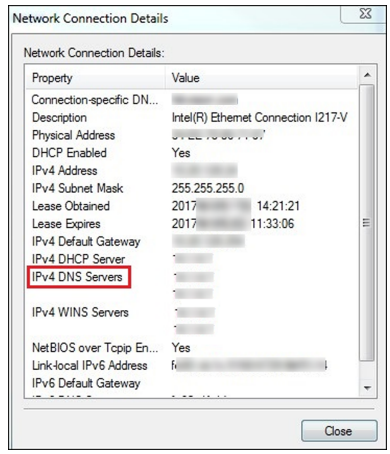


Figure 20-3 How to Get Host Name

Port No.

The port No. of the AD domain controller. By default, it is 389.

Enable SSL (Optional)

Enable SSL if it is required by the AD domain controller.

User Name

The user name of the AD domain controller. The user should be the domain administrator.

Password

The password of the AD domain controller.

Base DN (Distinguished Name)

Enter the filter condition in the text field if you are familiar with the format. Or you can click **Fetch DN** to get the filter condition entered automatically.

Note

- Only users found within an OU in the domain can be imported. Click **Fetch DN** to have the filter condition entered automatically.
- If you enter the Base DN manually, you need to define the root node as desired. If you click **Fetch DN**, then the entire structure stored in the AD domain controller will be obtained.

4. Set the time to automatically synchronize the users in the AD domain to the platform.

5. Optional: Link the person information you are concerned about in the domain to the person information in the system.

1) Switch on **Linked Person Information**.

The default and custom additional information items (see ***Customize Additional Information***) are displayed in the Person Information area 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 new person information item is also displayed on the Custom Additional Information page, where you can edit or delete the items. Refer to ***Customize Additional Information*** for details.
- The person information item is case-sensitive.

3) **Optional:** Click + to show the person information items stored in the domain.
4) Check the checkbox in the domain to link it to the added person information item when importing the domain's persons.
5) **Optional:** Hover over the linked person information in the domain and click × to remove the relationship. You can also change the relationship between each other by clicking and dragging one item to another.

6. Click **Save**.

After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on the User Management page.

If the Linked Person Information function is enabled, the corresponding person information in the system will match the linked person information in the domain and cannot be edited.

20.7 Device Access Protocol

Before adding devices supporting ISUP 2.6/4.0 to the system, you need to set the related configuration to allow these devices to access the system.

On the top, select **System**.

Select **Network → Device Access Protocol** on the left.

Switch on **Allow ISUP Registration**.

Check **Allow ISUP of Earlier Version**.

Note

The device may be attacked when accessing the system via ISUP of earlier versions.

Click **Save**.

20.8 Set WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for HikCentral Access Control to enable it to access the SYS via WAN (Wide Area Network). For example, if the SYS is in a local area network, and you need to visit the platform via

the Web Client running in WAN, you should enable WAN access and set a static IP address or a domain name and ports for HikCentral Access Control.

Steps

1. On the top, select **System**.
2. Select **Network → WAN Access** on the left.
3. Switch on **Access WAN** to enable the WAN access function.
4. Enter the IP address of the server for WAN access.
5. Set the client communication port.

   HTTP

   Used for the Web Client to access the platform via HTTP. By default, it is 80.

   HTTPS

   Used for the Web Client to access the platform via HTTPS. By default, it is 443.

   Cluster Port Segment

   Used for translating the network address and mapping the platform to access via WAN. By default, the internal network port is 18020, and you should specify the port of WAN.

   Note

   If the port is conflicted, you can view the exception on **System → Maintenance** .

6. If you adopt generic events to integrate HikCentral Access Control with external sources, you need to set the TCP port, UDP port, HTTP port, and HTTPS port for receiving the TCP, UDP, HTTP, and/or HTTPS data packages.

   Note

   For setting the generic event, refer to ***Add Generic Event*** .

7. Set the ISUP alarm receiving port.

   ISUP Alarm Receiving Port (TCP)

   Used for receiving alarms from ISUP devices via TCP. By default, it is 7332.

   ISUP Alarm Receiving Port (UDP)

   Used for receiving alarms from ISUP devices via UCP. By default, it is 7334.

   Note

   If the ISUP ports are disabled on the SYS, the ISUP related ports will not be displayed on the WAN Access page.

8. Set other ports.

   Real Time Streaming Port(TCP)

   Used for getting the stream for live view via the Control Client. By default, it is 554.

   ISUP Registration Port(TCP)

   Used for the ISUP devices registering to the platform. By default, it is 7660.

   Local Picture Storage Port on Server(TCP)

Used for storing local pictures on the server. By default, it is 6123.

Local File Picture Storage Port on Server(TCP)

Used for storing local files on the server. By default, it is 6203.

9. Click **Save**.

20.9 Set IP Address for Receiving Device Information

You can select the NIC of the current SYS so that the platform can receive the alarm information of the device connected via ISUP account.

Before You Start

Make sure the server's ports ranging from 8087 to 8097 are available.

Steps

1. On the top, select **System**.

2. Select **Network → Address for Receiving Device Info** on the left.

3. Select **Get from NIC** or **Enter Manually**.

Get from NIC

Usually, you can select **Get from NIC** to get IP address from the NIC of SYS.

Select the currently used NIC name of SYS in the drop-down list. The NIC information including description, MAC address, and IP address will display.

Enter Manually

If you have configured hot spare for the SYS. Manually enter the IP address for receiving device information.

4. Click **Save**.

20.10 Configure Storage for Imported Pictures and Files

The imported pictures (such as the static e-map pictures and the face pictures in the person list) can be stored on the HDD of SYS server. You can configure the storage locations and the corresponding quotas for them.

Steps

Note

You can configure the storage only when the current Web Client is running on SYS server.

1. On the top, select **System**.

2. Select **Storage → Storage on SYS Server** on the left.

The disks of the SYS server are displayed with current free space and total capacity.

3. Switch on **Enable Local Storage**.

4. 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.

5. 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.

6. Click **Save**.

20.11 Set Records Storage Information

The data retention period specifies how long you can keep the events, logs, and some records in the SYS server, such as recording tags and card swiping records.

Steps

1. On the top, select **System**.

2. Select **Storage → Records Storage** on the left.

3. Set the data retention period from the drop-down list for the required data types.

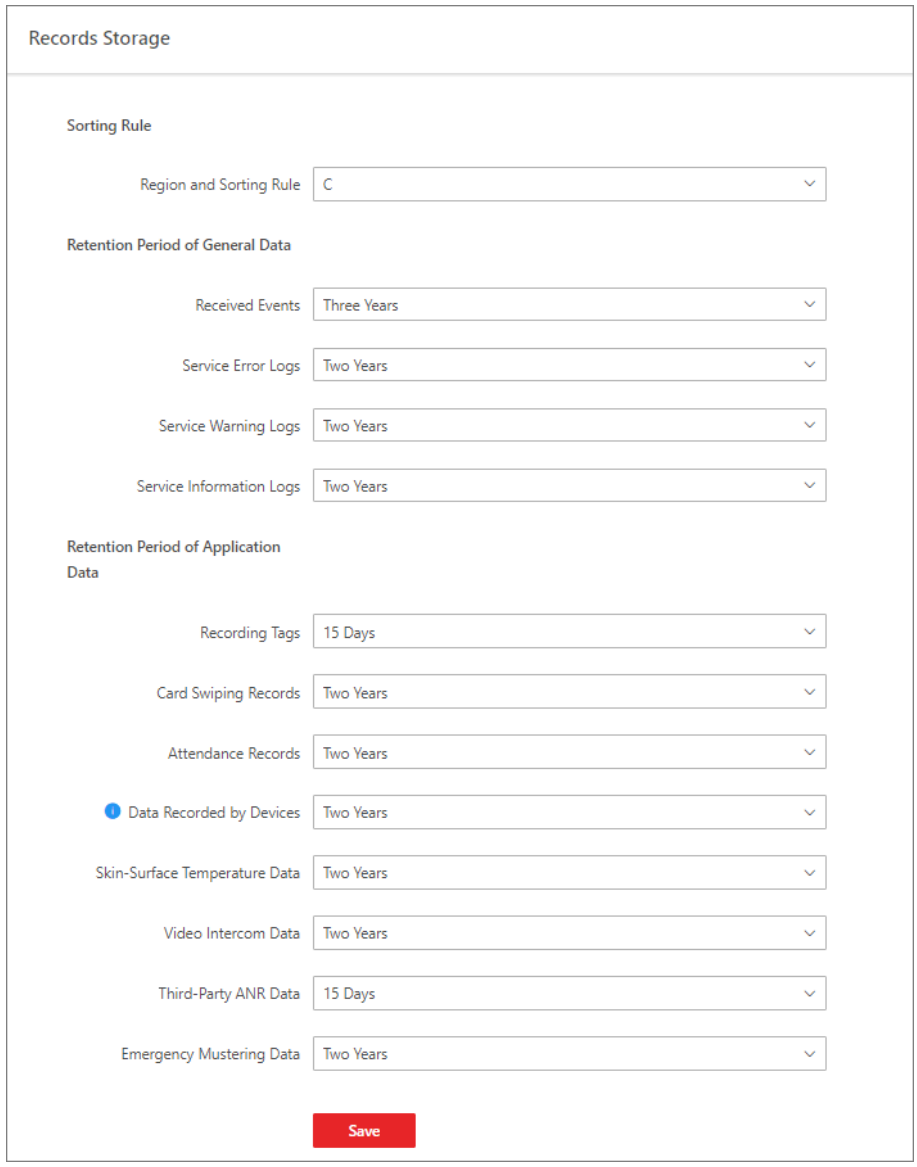


Figure 20-4 Set Data Retention Period

4. Click **Save**.

20.12 Set Email Template

Before sending report or sending event message to the designate email account(s) as email linkage, you should set the email template properly. The email templates include template for sending report and template for sending event message as linkage action when the event is triggered. The email template specifies the recipient, email subject, and content.

20.12.1 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. On the top, select **System**.

2. Select **Email → Email Settings** on the left.

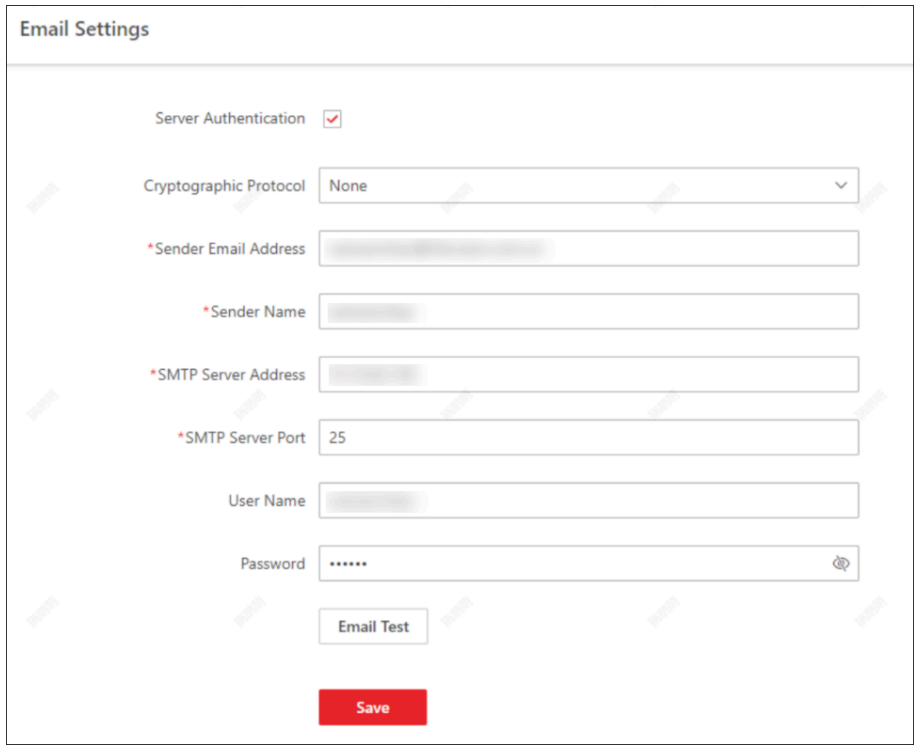


Figure 20-5 Email Settings

3. Configure the parameters according to actual needs.

Server Authentication (Optional)

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.

4. Click **Email Test** to test whether the email settings work or not.

The corresponding attention message box will pop up.

5. Click **Save**.

20.12.2 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

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. On the top, select **System**.

2. Select **Email → Scheduled Report Email Template** on the left.

3. Click **Add** to enter the Add Email Template page.

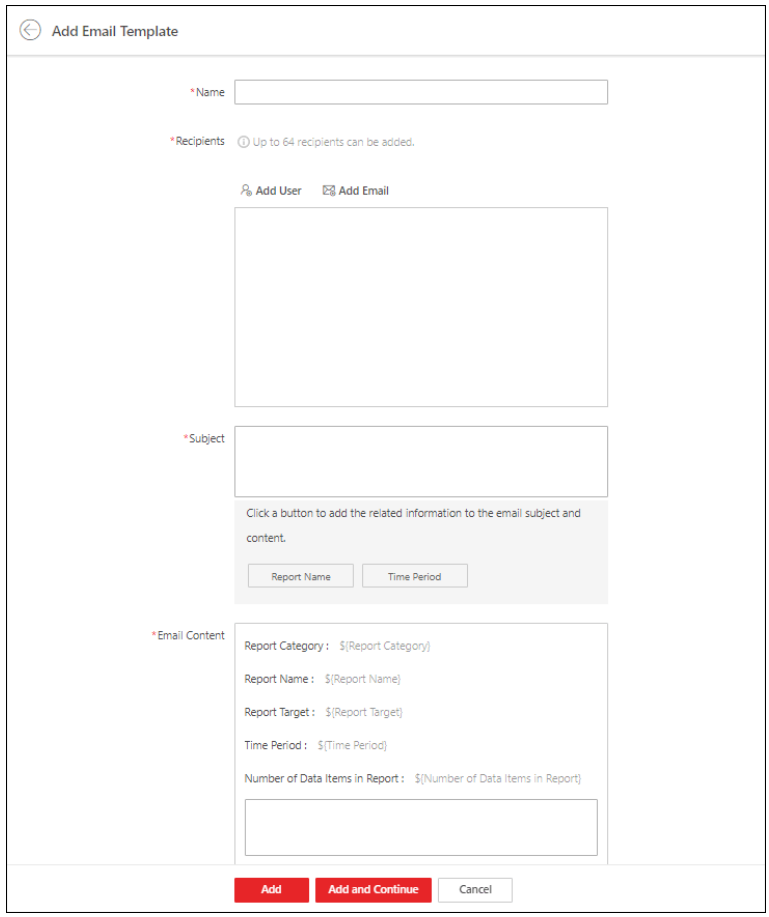


Figure 20-6 Add Scheduled Report Email Template

4. Enter the required parameters.

Name

Create a name for the template.

Recipients

- Click **Add User** and select the person's email as the recipient, which is configured when adding the person.
- Click **Add Email** and enter the recipient email address 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 the report content to be sent. You can also click buttons above the **Email Content** parameter to add the related information to the content.

Note

If you add the time period to the email subject or email content, and the email application (such as Outlook) and the platform are in different time zones, the displayed time period may have some deviations.

5. 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.

6. Optional: Perform the following operation(s) after adding the email template:

Edit Template	Click in the Operation column to edit template details.
Delete Template	Click in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

20.12.3 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

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. On the top, select **System**.

2. Select **Email → Event and Alarm Email Template** on the left.

3. Click **Add** to enter the Add Email Template page.

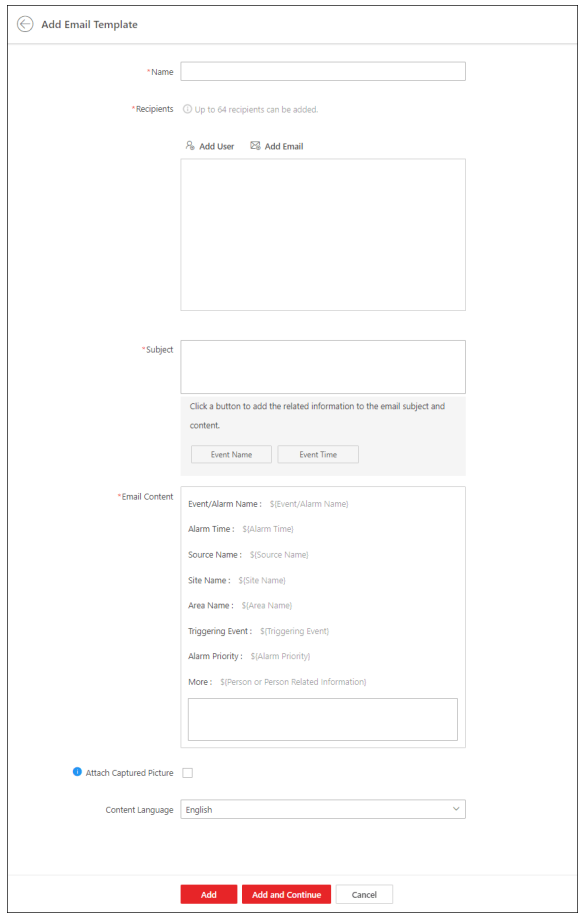


Figure 20-7 Add Event and Alarm Email Template

4. Enter the required parameters.

Name

Create a name for the template.

Recipients

Click **Add User** and select the person's email as the recipient, which is configured when adding the person.

Click **Add Email** and enter the recipient(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.

5. **Optional:** Check **Attach Captured Picture** to send email with image attachment.
6. Select a content language to define the language of the sent content.
7. 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 on the email template list.
8. Perform the following operation(s) after adding the email template:

Edit Template	Click in the Operation column to edit template details.
Delete Template	Click in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

20.13 Set Transfer Protocol

You can set the SYS server's transfer protocol to define the access mode for the SYS (via Web Client) as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Steps

1. On the top, select **System**.
2. Select **Security → Transfer Protocol** on the left.
3. In the **Clients and SYS Transfer** field, select **HTTP** or **HTTPS** as the transfer protocol between the clients (Web Client and Mobile Client) and the SYS servers.

   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.
4. If you select **HTTPS**, you are required to set the certificate. You can use the system provided certificate, or select **New Certificate** and click to select a new certificate file.

   Note

   - The new certificate should be in PEM format.
   - The public key and private key should be in the same certificate file.
5. **Optional:** You can add the upper-level certificate as needed.
   1) Click **Add** to open the Upload Certificate panel.

2) Click to select the file.
3) Click **Confirm**.
4) **Optional:** Select the added certificate(s) and click **Delete** to delete.
5) **Optional:** In the Operation column, click to download the certificate.

6. Click **Save**.

- The SYS server will reboot automatically after changing the clients and SYS server transmission settings.
- All the users logged in will be forced to log out during reboot. The reboot takes about one minute and after that, the users can log in again.

20.14 Set Database Password

You can set the database password of the system on the Web Client running on the SYS server.

Note

Setting database password is only available when you access the Web Client on the SYS server locally.

On the top, select **System**.

Select **Security → Database Password** on the left.

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

20.15 Set Third-Party Integration

HikCentral Access Control supports integrating third-party resources. Also, the system provides open platform to integrate the third-party system. By the Open APIs (application programming interface) provided on the open platform, the third-party system can obtain some functions of HikCentral Access Control, to develop more customized features.

On the top, select **System**.

Select **Third-Party Integration** on the left.

Note

- Setting open platform is only available when you access the Web Client on the SYS server locally.
- Only admin/administrator users have the permission to perform this function.

Open Platform

Note

Setting open platform is only available when you access the Web Client on the SYS server locally.

Select **Open API** on the left panel, switch on **Open API**, and set the IP address of the open platform, management port of the open platform, and the partner user.

Note

- The open platform should be deployed in the same network with the SYS server.
- The third-party system integrates the HikCentral Access Control by the partner user(s) you select, which defines the permission(s) of resources and operations in the HikCentral Access Control.

Click **Test** to test the service availability of the open platform.
Click **Save** to save the settings.

20.16 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.

20.16.1 Synchronize Card Swiping Records to Third-Party Database

You can enable synchronization function to apply the card swiping records of specified resources from HikCentral Access Control to the third-party database automatically.

Steps

1. On the top, select **System**.
2. Select **Third-Party Integration → Data Interchange** on the left.
3. Switch on **Data Interchange** to enable data interchange function.
4. Click **Add** and select the resource(s) for card swiping records synchronization. Set the direction to In, Out, or Null.

   Note

   - Setting the direction is only available for card readers. For other devices, Null will be displayed no matter what direction is selected.
   - You can click 🗑 in the Operation column to delete the resource or click **Delete All** to delete all added resources.

5. Select the encoding format of data interchange.
6. **Optional:** Check **Do Not Push Failed Records**.

   The failed records will not be pushed to the third-party system.
7. Select **Database Synchronization**.
8. **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.

9. **Optional:** Select **Database Type** from the drop-down list to set the database type.
10. Set the required parameters of the third-party database, including server IP address or domain name, server port, database name, user name, and password.
11. Click **Test Connection** to test whether database can be connected.
12. 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.
13. Click **Save**.

    The data will be written to the third-party database.

20.16.2 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. On the top, select **System**.
2. Select **Third-Party Integration → Data Interchange** on the left.
3. Switch on **Data Interchange** to enable the data interchange function.
4. Click **Add** and select the resource(s) for card swiping records synchronization. Set the direction to In, Out, or Null.

Note

- Setting the direction is only available for card readers. For other devices, Null will be displayed no matter what direction is selected.
- You can click in the Operation column to delete the resource or click **Delete All** to delete all added resources.

5. Select the encoding format of data interchange.
6. **Optional:** Check **Do Not Push Failed Records**.

   The failed records will not be pushed to the third-party system.
7. Select **Access Record Dump**.
8. In the Dump Rule area, click **Add** and set the required parameters.

Rule Name

The name of the dump rule.

Description

The description of the dump rule.

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 server. 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 server 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.

Person Group

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.

Content Written Format

For each HikCentral Access Control field, you can configure the written format of dumping card swiping records.

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 card swiping records.

Dump Time

The time when dumping card swiping records is started.

9. Click **Add**.

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.

10. Click **Save**.

20.17 Diagnose Remote Fault

When faults occur in HikCentral Access Control, you can get the system information using the authentication code generated by HikCentral Access Control to help diagnose the system faults.

On the top, select **System**.

Select **Advanced → Diagnosis & Maintenance** on the left.

Switch on **Remote Fault Diagnosis** to generate an authentication code for remote diagnosis. It will be canceled automatically after 60 minutes.

Note

The authentication code will be refreshed every time you switch on **Remote Fault Diagnosis**.

Launch Postman, create a new request, set the HTTP method to POST, and enter the request URL (format: ***http://<host>[:port]/ISAPI/Bumblebee/Platform/V1/TranckTaskInfo?&MT=GET***).

Then in the Body area, enter the request message in JSON format (set the **trackModuleNmae** to the module name and set the **AccessKey** to the authentication code generated on HikCentral Access Control), and click **Send**.

The response message is returned in the Body area of Response and it shows the system running information. You can perform fault diagnosis remotely according to the information.

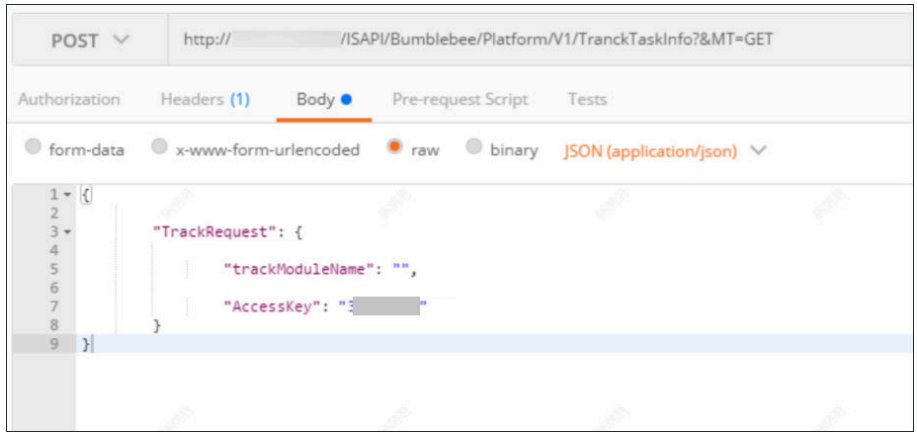


Figure 20-8 Get System Running Information Using Postman

20.18 View Event Tracking Information

You can view the event tracking information to get operation data in the platform.

Note

Viewing event tracking information is only available when you access the Web Client on the SYS server locally.

On the top, select **System**.

Select **Advanced → Event Tracking Information** on the left.

- You can view the exception information and general information.
- Click **Refresh** to refresh the page for getting the latest information.
- Click **Download Event Tracking Information** to download the information in a ZIP file.

20.19 Reset Device Network Information

When system network domain changes (such as server migration), you must reset the network information of the added device to adapt to the new network environment.

Perform this task when you need to reset the network information of the added device.

Steps

1. On the top, select **System**.

2. Select **Advanced → Reset Network Information** on the left.

3. Click **Reset** to one-touch reset the device network information.

20.20 Set Company Information

You can configure and show the company information on the Web Client for customization requirements.

On the top, select **System**.

Select **Company Information** on the left.

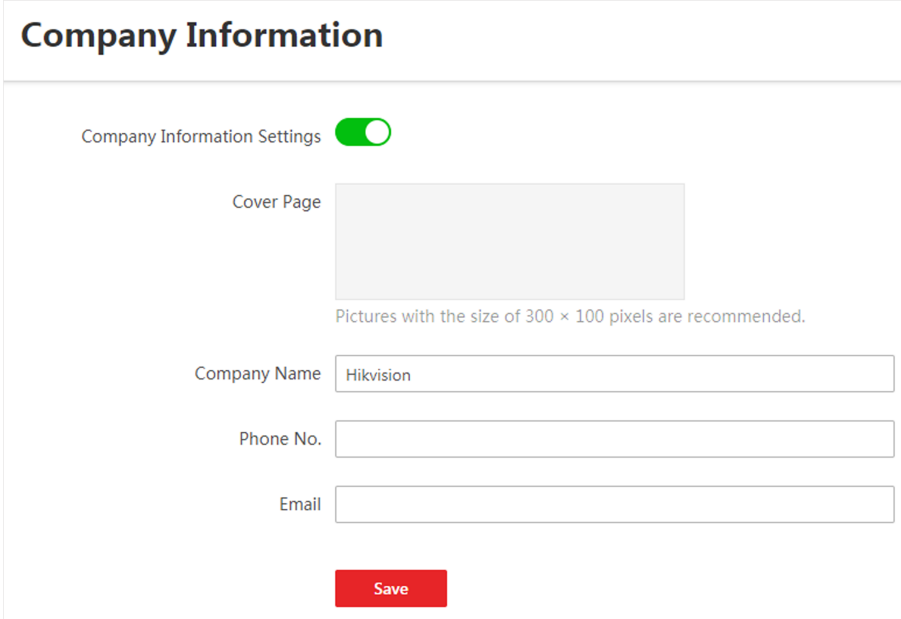


Figure 20-9 Company Information Settings

Switch on **Company Information Settings** to enable displaying company information on the Web Client. And 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.

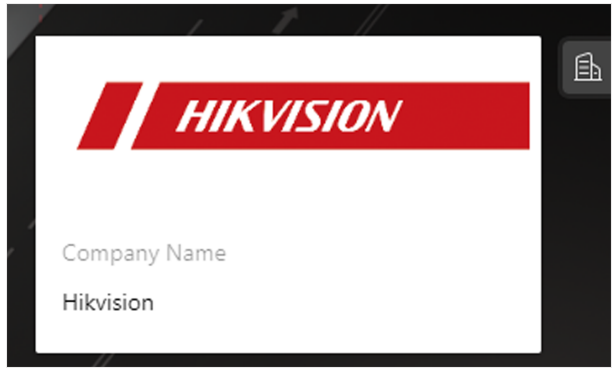


Figure 20-10 Company Information Displayed on Web Client

Chapter 21 System Security Settings

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.

Steps

1. On the top, select **Account and Security**.
2. Select **Security Settings** on the left.
3. On the top, select **System**.
4. Select **Account and Security → Security Settings** on the left.

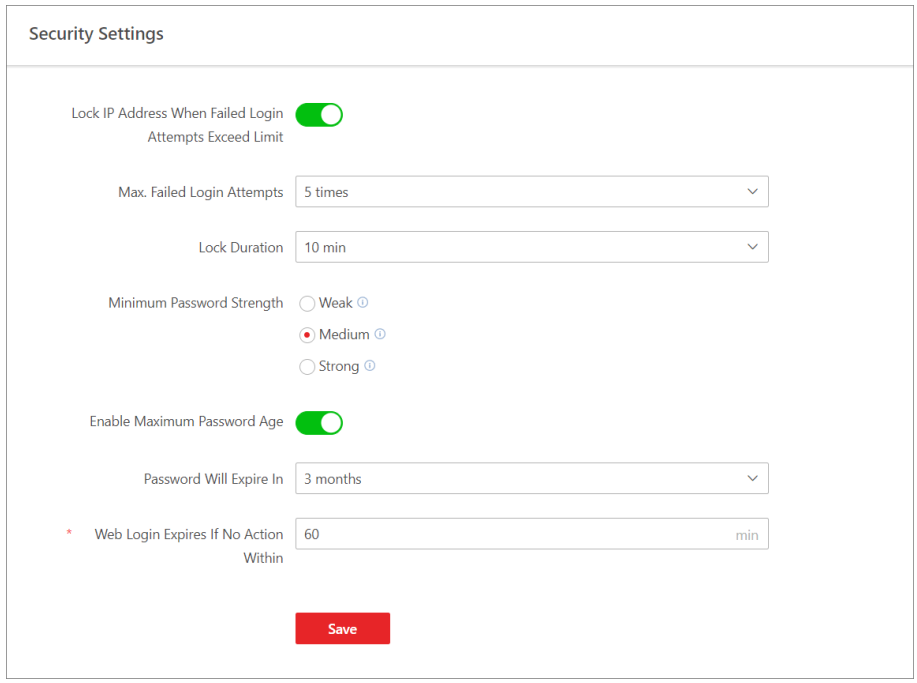


Figure 21-1 Security Settings Page

5. Switch on **Lock IP Address When Failed Login Attempts Exceeds Limits** to limit the number of failed login attempts.
   1) Select the maximum allowable login attempts for accessing HikCentral Access Control.

   Note

   Failed login attempts include failed password attempt and failed verification code attempt.

   2) Set the locking duration for this IP address. During the locking duration, the login attempt via this IP address is not allowed.

   The number of login attempts is limited.
6. Select the **Minimum Password Strength** to define the minimum complexity requirements that the password should meet.
7. Set the maximum password age.

1) Switch on **Enable Maximum Password Age** to force user to change the password when the password expires.
2) Set the maximum number of days that the password is valid.

Note

After the maximum number of days, you should change the password. You can select the predefined time length or customize the time length.

8. Set minutes after which the Web login will expire if there is no actions during the set minutes.
9. Click **Save** to save the above settings.

Chapter 22 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.

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.

Example

What is an Event

The event can be defined as intrusion ("triggering event") which happens in the bank vault and be detected by the camera mounted in the bank vault ("event source") on weekend ("when"), and triggers the camera to start recording ("what to do") once happened.

Example

What is an Alarm

The alarm can be defined as intrusion ("triggering event") which happens in the bank vault and be detected by the camera mounted in the bank vault ("alarm source") on weekend ("when"), and triggers the camera to start recording ("what to do") once happened. This alarm is marked as High priority ("priority"), and users including the admin and operators ("recipient") can receive this alarm notification and check the alarm details.

22.1 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.

22.1.1 Supported Events and Alarms

Currently, the platform supports events and alarms for the following 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.

Elevator

Events occurred in elevators, such as card swiping event and elevator 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.

Intelligent Analysis Group

Events occurred during the regional people counting process.

Maintenance

Operation exceptions occurred on the resources (e.g., doors, access control devices, elevator control devices, network device) added to the platform, such as the camera offline, server exception, and so on.

User

Events occurred during the user login and logout process.

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. See ***Add Generic Event*** for details.

22.1.2 Define Alarm Priority, Alarm Category, and Alarm Icon

The platform has predefined several alarm priorities, alarm categories, 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 acknowledgement.

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.

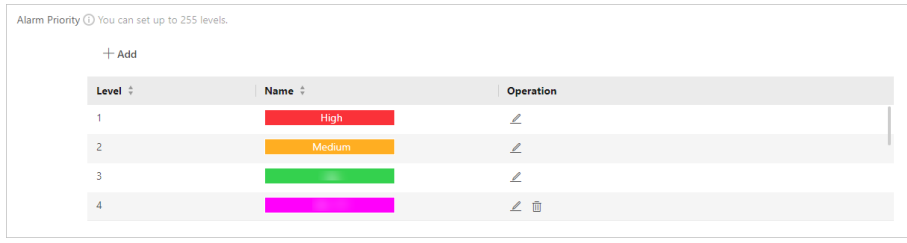


Figure 22-1 Alarm Priority

1) Click **Add** to open the adding alarm priority pane.

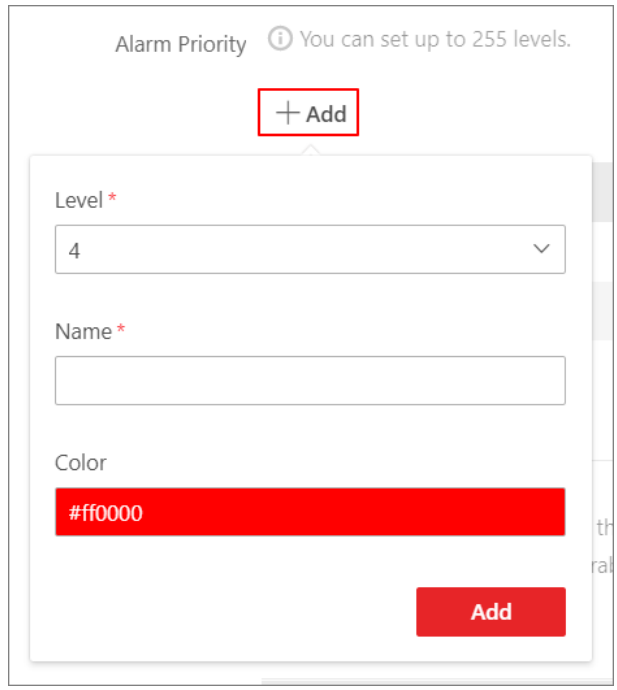


Figure 22-2 Add Alarm Priority

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.

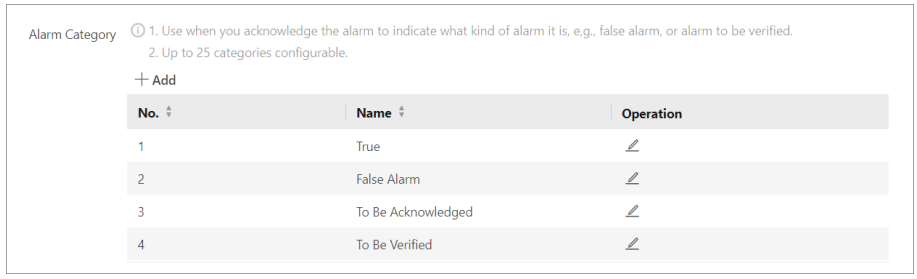


Figure 22-3 Alarm Category

1) Click **Add** to open the adding alarm category pane.

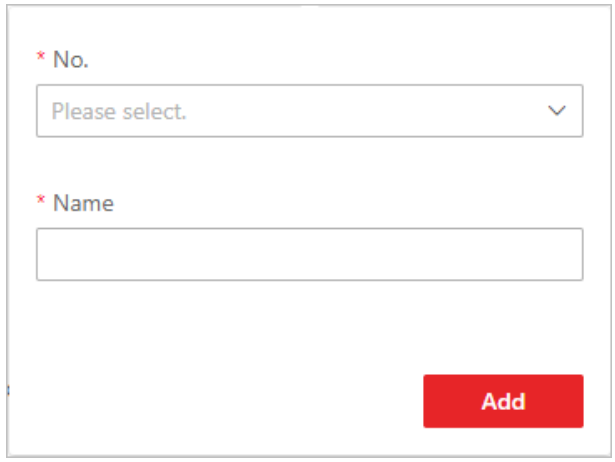


Figure 22-4 Add Alarm Category

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.

22.1.3 Add Normal Event and Alarm

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

On the top, select **System**.

Select **Event and Alarm → Normal Event and Alarm** on the left.

Click **Add** to enter the Add Event and Alarm page

Basic Information

Triggering Event

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

Source

This field refers to the specific entity (such as cameras, devices, servers, etc.) which can trigger this event and alarm.

Note

- When setting a thermal related event and alarm for thermal cameras, you can select areas, points, or lines as event and alarm sources.
- The Triggering Event and Source fields support fuzzy search.

Name

After selecting the source(s), you need to name the event or alarm. You can customize a name, or click the labels below to name the event or alarm by the selected label(s). If you name the event or alarm by the selected labels, the platform will display the event/alarm name by the combination of source name, area name, triggering event name, so that you can quickly know the location where the event/alarm occurs.

Face Comparison Group

If the triggering event you select is **Face**, you need to select the face comparison group so that the platform can compare the detected face pictures with face pictures in the group.

Threshold

If the triggering event you select is **Regional People Counting**, you need to set extra conditions to define the triggering event.

Currently, you can set **People Counting Above/Below Threshold** and **People Counting Above/Below Threshold (Pre-Alarm)** for people counting group. For these two alarms, you need to set the threshold which determines whether the selected people counting groups will trigger an alarm when the detected number of people stayed less than or more than the threshold.

For example, if you set the threshold as ***"≥ 100 or ≤ 10"***, when the number of people detected in the selected people counting group is more than 100 or less than 10, an alarm will be triggered to notify the security personnel.

Color

Select the color to indicate this event or alarm. You can set the color according to the emergency of this event or alarm. For example, you can set red color for the urgent alarm and set green color for the prompt event.

Ignore Repetitive Events/Alarms

This function is used to avoid the same event or alarm occurs frequently in a short time. You need to set the **Ignore For (Second)** which is the threshold of the recurring events or alarms.

For example, if you set **Ignore For (Second)** to 30 seconds, the events or alarms of the same type occurred on the same camera within 30 seconds will be regarded as one event or alarm.

Actions

The field links actions for the alarms, you can click **Add Linkage Action** to select actions.

Link Access Point

You can enable this function to trigger the access points (including doors and floors).

For doors, the doors can be locked, unlocked, remained locked, or remained unlocked when the event occurs.

For floors, the elevators can access the floors freely, with credentials, temporarily, or access forbidden.

For example, you can set to trigger all the doors remaining locked and all the floors access forbidden when intrusion of suspicious person is detected.

- **All Access Points**: When the alarm is triggered, the platform will trigger all the doors and floors to take certain action.
- **Specified Access Point:** Click **Add** to select specified access points or emergency operation groups as the linkage targets. When the event occurs, the platform will trigger these doors, floors, or doors/floors in the emergency operation groups to take certain action.

Link Alarm Input

Select alarm inputs and these alarm inputs will be armed or disarmed when the event occurs.

For example, when adding an intrusion alarm of camera A, which is mounted at the entrance of the building, you can link to arm the alarm input B, C, and D, which are PIR detectors mounted in different rooms in the building and are disarmed usually. When camera A detects intrusion alarm, these PIR detectors will be armed and trigger other events or alarms (if rules configured), so that the security personnel will get to known where the suspect goes.

Link Alarm Output

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

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the time period (unit: s) after which the alarm output(s) will be closed automatically.

Send Email

Select an email template to send the event information according to the defined email settings. If you have purchased the License of emergency mustering, you can select an emergency counting group in the drop-down list of **Send Data of Emergency Counting Groups**. When the event occurs, the platform will send the data of the selected emergency counting group to the email in a PDF file.

Note

For details about setting email template, refer to ***Set Email Template*** .

Attach with Entry & Exit Counting

If the source type you selected is **Alarm Input**, you can select an entry & exit counting group from the drop-down list to attach a report of entry & exit counting in the sent email.

For example, if the fire alarm input detects fire in the building, the security personnel will receive a file, which contains the information such as the number of people still in the building, their names and profile photos, phone numbers, and locations of last access.

Trigger User-Defined Event

Select the user-defined event(s) in the event list as the linkage action when the event occurs.

Note

- Up to 16 user-defined events can be selected as linkage actions.
- For setting the user-defined event, refer to ***Add User-Defined Event*** .

Link Printer

If the source type you selected is **Alarm Input**, you can link to print the entry & exit counting report of certain entry & exit counting group.

For example, if the fire alarm input detects fire in the building, the platform will automatically send the entry & exit counting report to all the printers configured on the platform so that they can get the information such as how many people are still in the building, their names and profile photos, phone numbers, and locations of last access.

For details about printer settings, refer to ***Set Printer*** .

Apply Notice to Indoor Station

If the source type you selected is **Alarm Input**, you can apply notice to specific indoor stations.

Receiving Schedule

The field defines a time period when the event or alarm can be triggered.

Receiving Schedule

The source is armed for detecting or triggering events or alarms during the receiving schedule. The platform provides two types of receiving schedule:

- **Schedule Template**: Select a receiving schedule template for the event or alarm to define when the event or alarm can be detected or triggered. For customizing a template, refer to ***Configure Receiving Schedule Template*** .
- **Event Based**: Specify a user-defined event or an alarm input as the start or end of the receiving schedule. You can set the **Stop Receiving** switch to on and set the specified time to automatically stop receiving this event or alarm even if the schedule does not end.

Note

For example, assume that you have set event A as the start event, event B as the end event, and set the value of **Automatically Stop Receiving After** to ***60 s***. Under these conditions, when event A occurs at T1, if event B occurs within 60 s , the receiving schedule ends at the occurrence of event B (see the following figure Receiving Schedule 1); if not, ends at 60 s after the occurrence of event A (see the following figure Receiving Schedule 2).

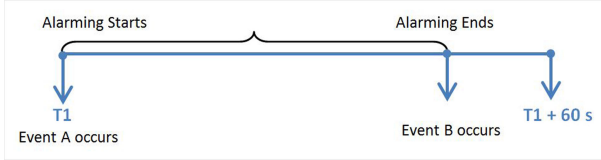


Figure 22-5 Receiving Schedule 1

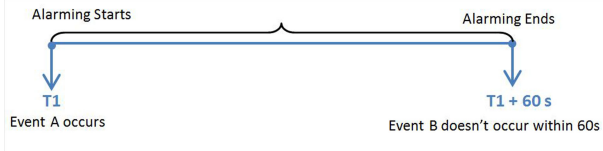


Figure 22-6 Receiving Schedule 2

When A occurs at time T1, the event or alarm will be armed from T1, if A occurs again at time T2 but B doesn't occur, the event or alarm will be armed from T2 again.

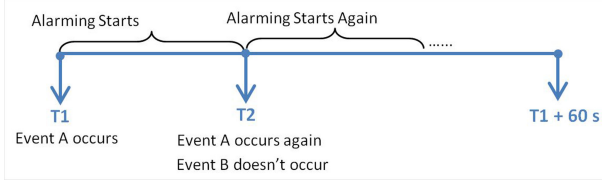


Figure 22-7 Receiving Schedule 3

Alarm Settings

Switch on **Trigger Alarm** to trigger the configured event as an alarm.

Alarm Priority

The field defines the importance or urgency of this alarm. Priority can be used for filtering alarms.

Recipients

The field defines users who can receive the alarm notification and check the alarm details when the alarm is triggered.

Select the recipient group(s) or user(s) to send the alarm information to and the recipient(s) can receive the alarm information when he/she logs in to HikCentral Access Control via the Mobile Client.

Note

By default, users configured as the default recipients on the Alarm Receiving Configuration page will be automatically selected and cannot be deselected. For how to configure default recipients and recipient groups, refer to ***Add Call Recipients*** .

Trigger Emergency

When the alarm is triggered by an emergency (such as fire), the platform automatically switches to the **Trigger Emergency** mode or **Turn Off Emergency** mode.

Link Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot (refer to).

Restrict Alarm Handling Time

Enable this function to trigger the user-defined event(s) / alarm output(s) or automatically acknowledge the alarm if the alarm is not handled within the configured alarm handling time.

Note

Up to 16 user-defined events and alarm outputs can be triggered when handling alarm timed out.

Other Operations

Click **Add** to add the event to the platform, or click **Add and Continue** to save the current settings and add another one. The added event will be listed on the Normal Event and Alarm page, and then you can perform the following operations if needed.

Table 22-1 Other Operations

Operation	Description
Edit Event	Click the event name to enter the details page and edit the settings.
Copy to Other Events	1. Click the event name to enter the details page. 2. Click **Copy To** in the top right corner of the page. 3. Specify the settings of the source and select the target(s). 4. Click **OK** to copy the current event's specified parameter(s) to other added events for batch configuration.
Delete Events	Select events and click **Delete** to delete the selected ones.
Delete All Invalid Events	Click **Delete All Invalid Items** to batch delete all the invalid events.
Enable Events	Select an event and click **Enable** → **Enable** to enable the selected event, or click **Enable** → **Enable All** to enable all the added events.

Operation	Description
Disable Events	1. Select an event and click **Disable → Disable** , or click **Disable → Disable All** . 2. Set the time when the event(s) start being disabled and the duration how long the event(s) will be disabled for. 3. (Optional) Enter the reason for disabling the event(s). 4. (Optional) Check **Disable Device Alarm** to change the alarm status of the device(s) displayed in the event list. 5. Click **OK** to disable the selected event(s) or all the events.
Test Events	Select the event(s) and click **Test** to manually trigger the event(s) for testing if the linkage actions work properly.

22.1.4 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 top, select **System**.

2. Select **Event and Alarm Configuration → Combined Alarm** on the left.

3. Click **Add Combined Alarm** to open the Add Combined Alarm pane.

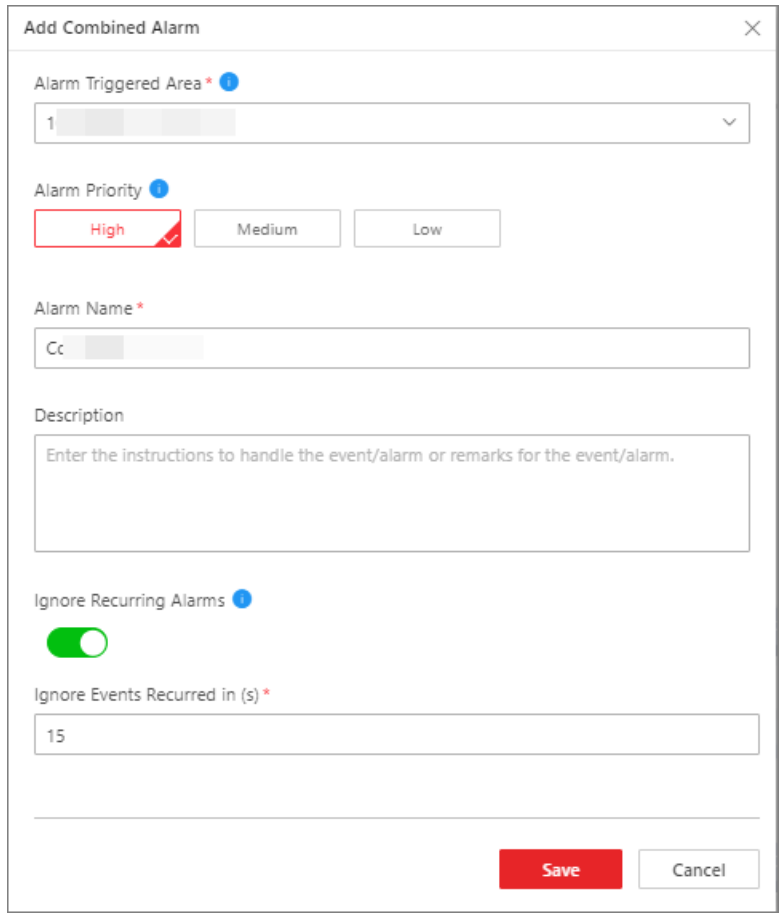


Figure 22-8 Add Combined Alarm

4. 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.

5. Click **Save** to enter the configuration page.

6. 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.

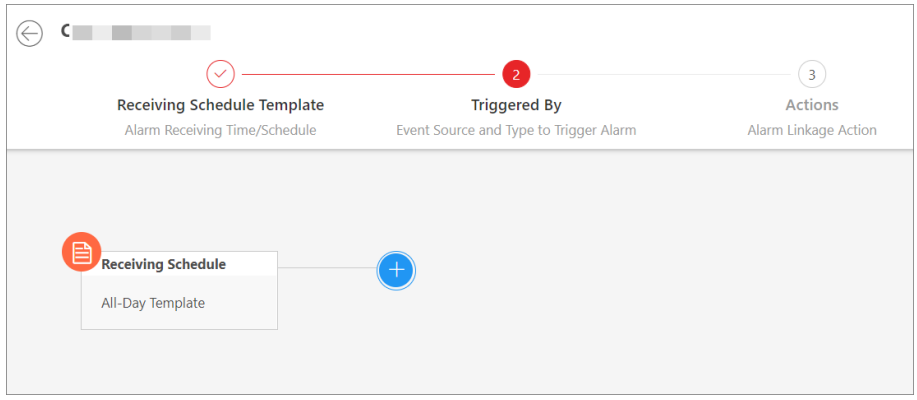


Figure 22-9 Receiving Schedule Card

7. 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.

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**.

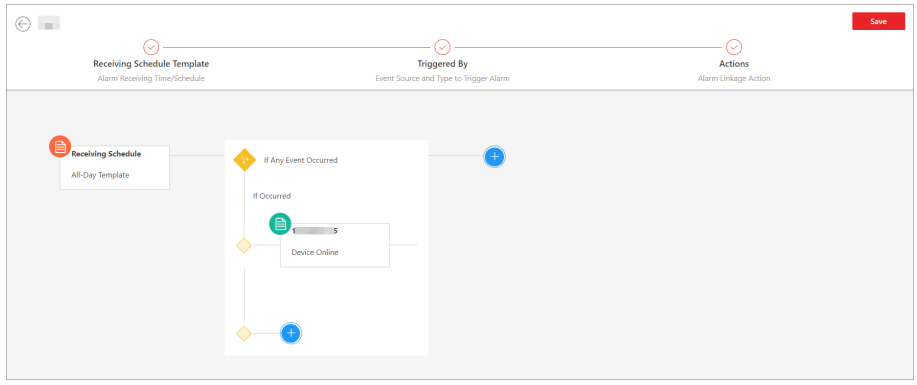


Figure 22-10 Condition Card

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.

8. 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 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 ***Add Normal Event and Alarm*** .

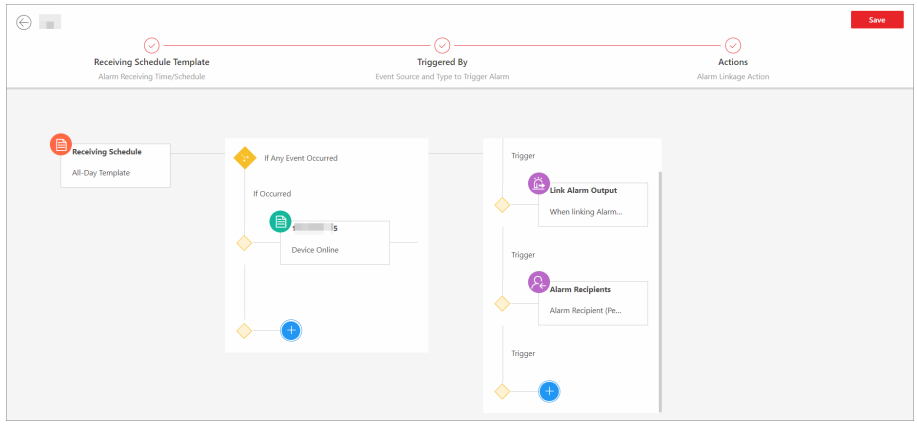


Figure 22-11 Action Card

5) **Optional:** Click ⊕ below the Alarm Recipients card to add more linkage actions.

9. Optional: Click the icon on the top left of each card to reselect the content.

10. 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.

11. 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.

12. Optional: Perform the following operations according to your requirements.

Add to Map	Click **Add to Map** to add this alarm to the map. After that, the alarm will be marked on the map when the alarm is triggered.
Copy Parameters to Existing Alarm	Click **Copy**, and then select the items (such as basic information, actions, receiving schedule, receiving mode), and select the target alarm to copy to.
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.

22.2 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.

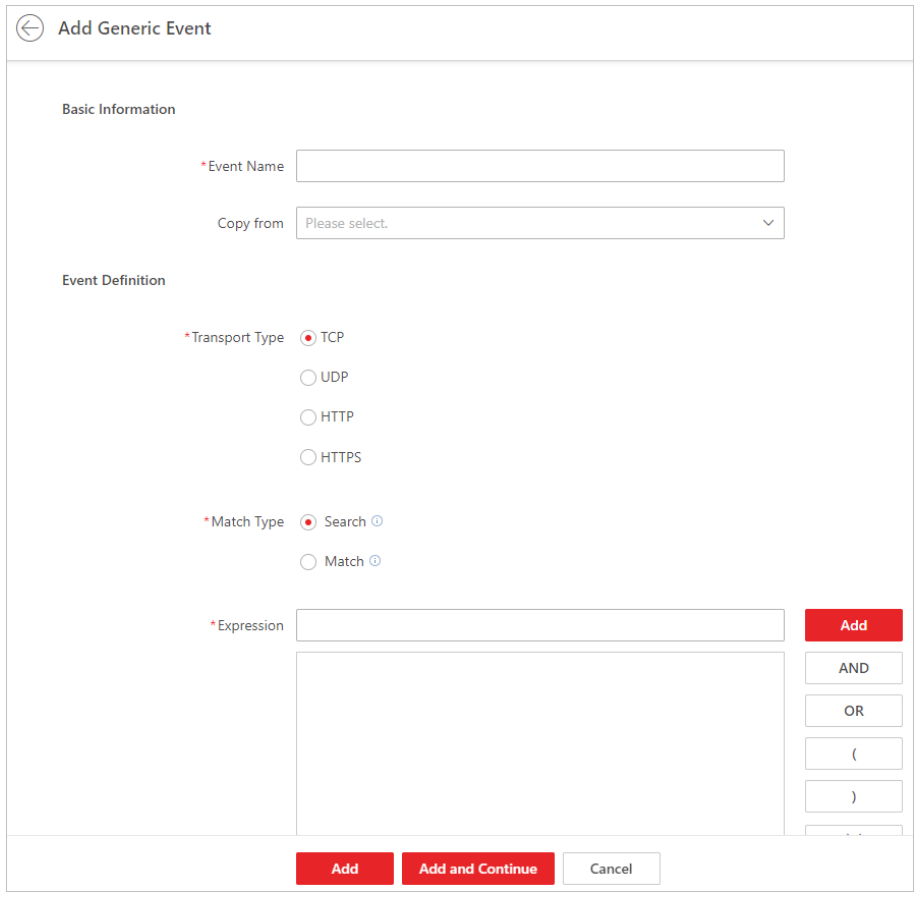


Figure 22-12 Add Generic Event Page

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 which indicates how particular your system should be when analyzing the received data packages:

Search

The received package must contain a part of text defined in the expression.

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

The text contained in the received package must be exactly the same as that defined in the expression.

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.

Delete Event Settings	Select the event(s) and click **Delete** to delete the selected event settings.
Delete All Event Settings	Check the checkbox in the heading row, and click **Delete** to delete all the event settings.
Receive Generic Event	Select the event(s), click **Receive Generic Event** to open the settings pane, and check the checkbox(es) to enable receiving the generic event(s) via different protocols.

22.3 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**.

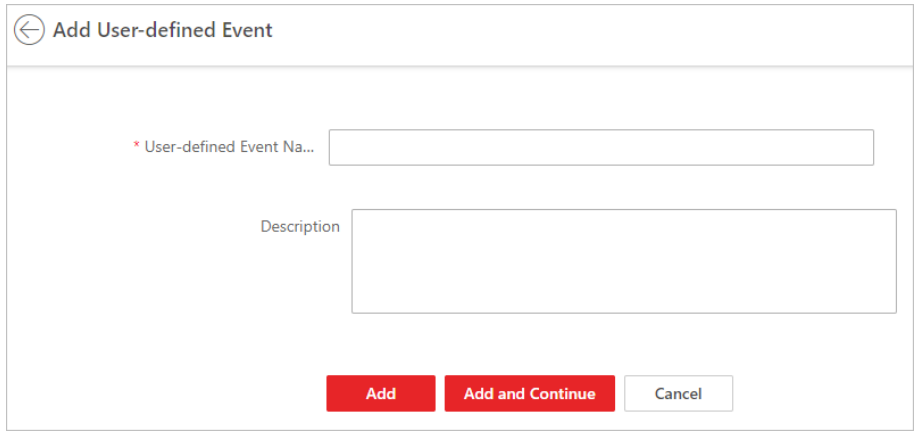


Figure 22-13 Add User-Defined Event

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.

22.4 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

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.

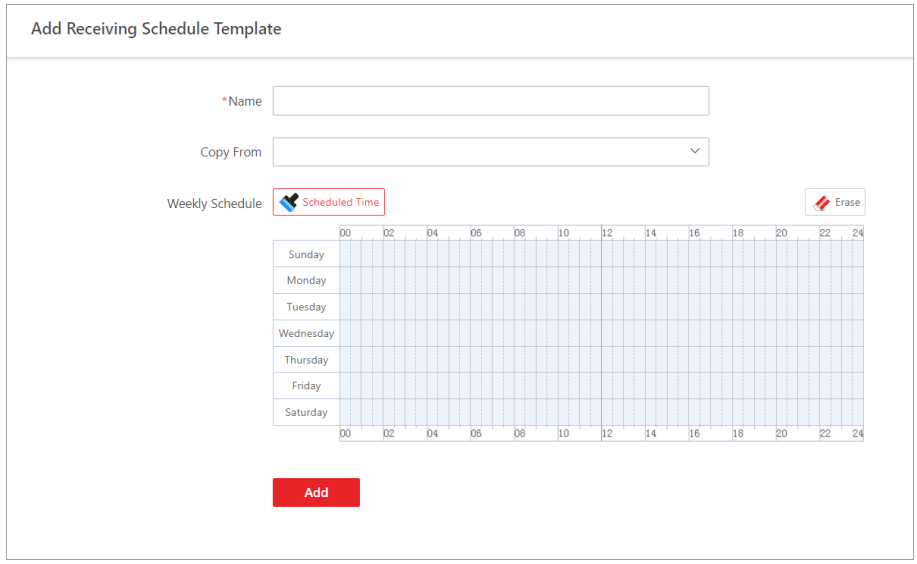


Figure 22-14 Add Receiving Schedule Template

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.

7. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
8. Click **Add** to add the template.

   The receiving schedule template will be displayed on the receiving schedule template list.
9. **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.

22.5 View Pop-Up Window Triggered by Alarm

On the Real-Time Monitoring page of the Access Control module, click a door which triggered an alarm, and then select **Alarm Details** to open the alarm information window. You can view the alarm time, the source device which triggered the alarm, the triggering event, and alarm status, etc.

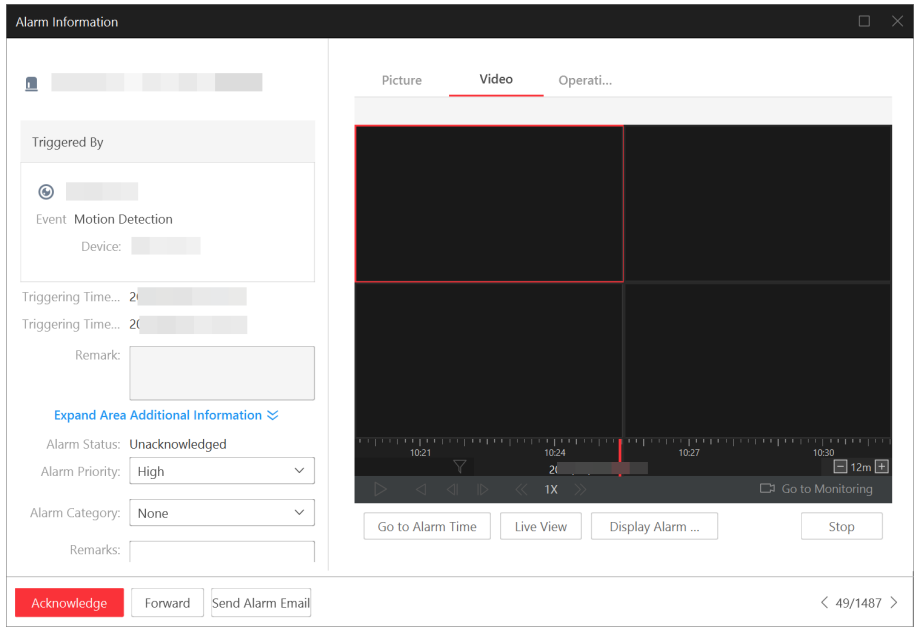


Figure 22-15 Alarm Triggered Pop-Up Window

Table 22-2 Functions and Operations Supported by Pop-Up Alarm Window

Function	Operation
View Area Additional Information	If you have set the additional information for the area where the alarm is triggered, click **Expand Area Additional Information** to display it.
Edit Alarm	Set the alarm priority, the alarm category, and remarks (e.g., enter "false alarm triggered by leaves" when you have checked

Function	Operation
	the alarm details and found that it is a false alarm) according to the detailed alarm information.
Start Two-Way Audio	Hover the cursor on the live view image, and click to start a two-way audio with people at the monitored place. You can adjust the volume of microphone and loudspeaker, and startd recording.
Acknowledge Alarm	Click **Acknowledge** to acknowledge the alarm.
Forward Alarm	For some specific alarms, you can click **Forward**to forward them to other users for acknowledgment. And you can set the priority to High to remind other users of acknowledging the alarms in the highest priority.
Unlock Door	Click **Unlock Door** to unlock the door triggered the alarm.
Send Alarm Email	Click **Send Alarm Email**, select an email template, and enter the recipient(s) of the alarm and remarks to send an email containing the information about this alarm to the selected recipients.
Control Alarm Output	Click **Alarm Output Control** to enable or disabled the linked alarm outputs if you have set linked alarm outputs in the alarm rule. For example, if a sounder is linked in the alarm rule, when the alarm is triggered, you can turn on or off the sounder.
View Previous or Next Alarm	Click < > to view the previous or next alarm information.
Enable Pop-Up Window	Uncheck **Enable Pop-up Window** to disable pop-up window when a new alarm is triggered. **Note** When the pop-up window remains open, the later alarm, if the alarm priority is higher, will be displayed in the pop-up window, and replace the earlier one.
Display Pop-Up Window in Full-Screen Mode	Check **Full Screen** to display the pop-up window in full-screen mode by default.

22.6 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.

22.6.1 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 22-16 Event and Alarm Analysis

Module	Description
1	The number of events or alarms in the last 7 days or last 30 days are displayed in vertical bar chart.
2	The data of top 5 event types or alarm categories triggered in today, last 7 days or last 30 days are displayed in 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 top 5 event or alarm areas in today, last 7 days or last 30 days are displayed in 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 on 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.

22.6.2 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 ***Add Normal Event and Alarm*** for details.

Steps

1. On the top, select **System**.
2. Select **Event and Alarm → Event and Alarm Search** on the left.
3. Set the time range for search.
   - Select a predefined time period for search.
   - Select **Custom Time Interval** and specify the start time and end time for search.
4. Select the event status (whether the event is triggered as the alarm).

   All

   Both events and alarms.

   Not Trigger Alarm

   The events happened but were not triggered as alarms.

   Trigger Alarm

   The events happened and were triggered as alarms. If you select **Trigger Alarm**, you can set conditions for filtering alarms by marking status, acknowledging status, alarm priority, or alarm category.
5. Switch **Area** on and then click to select the area of the event or alarm source.
6. Switch **Triggered By** 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.
7. Switch **Event/Alarm Name** on to select the event/alarm name in the drop-down list.
8. Click **Search**.

   The matched event or alarm logs will be listed on the right page.

9. **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.

22.7 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 ***Set Email Template*** .
- 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 Target field, click **Add** to select events or alarms 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 Report 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 ***Set Email Template*** .

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.

Chapter 23 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.

23.1 Health Monitoring

Health monitoring provides both near-real-time and history information about the status of the SYS and added resources. It is critical to multiple aspects of operating the servers or devices and is especially important for maintenance. When a resource exception occurs, you can enter this module to check the resource status and find out the abnormal device(s) and view the exception details.

23.1.1 Real-Time Health Status Overview

In the Health Monitoring module, you can view the real-time health status of the devices, servers, and resources managed on the platform. If there is no network transmission devices added, the Real-Time Overview page provides an at-a-glance view of the health status with charts and basic data of resource status.

On the top, select **System**.

Select **Maintenance → Real-Time Overview** on the left.

Click **Real-Time Overview** tab at the top to enter the Real-Time Overview page.

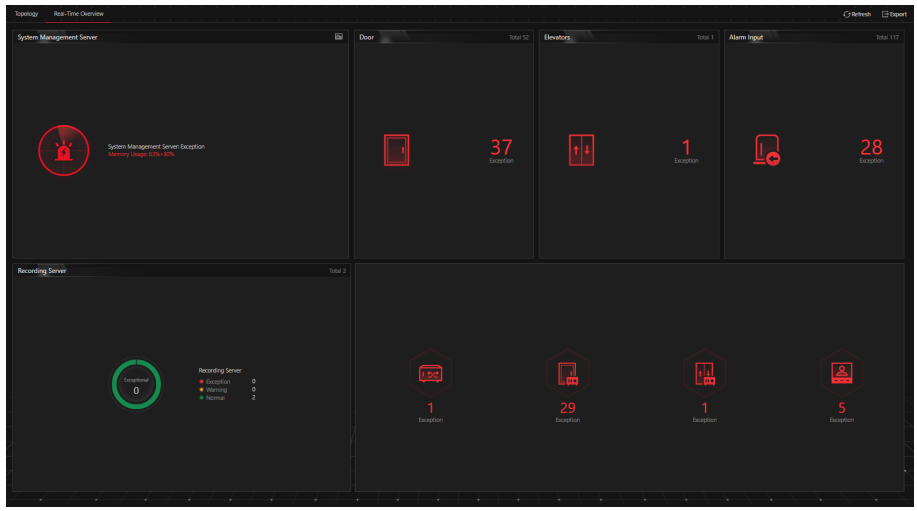
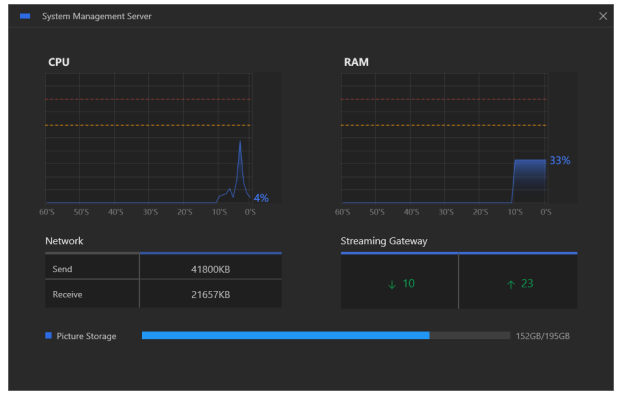
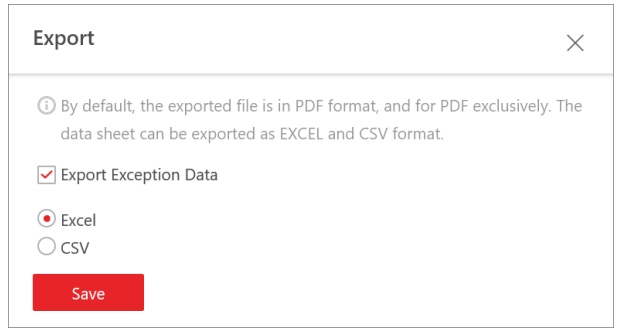


Figure 23-1 Real-Time Health Status Overview

Table 23-1 Real-Time Health Status Page

Section	Description
Resource Status	View the abnormal data of different resources (e.g., doors, elevators, or alarm inputs) added to the platform added to the areas of Central System in the graphical way.
System Management Server Status	View the network health status and server running status. Click in the upper right corner of System Management Server panel to view the running status details of the server, including CPU usage, RAM usage, etc.  **Figure 23-2 System Management Server Status Details**
Server Status	View the status (i.e., exception, warning, normal) of servers added on the platform. You can click the numbers and status types on the chart to view the real-time status details of servers.

Section	Description
Device Status	View the abnormal data of different devices added on the platform. You can click the numbers on the chart to view the real-time status details of devices. 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*** .
Refresh	• 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 → Health Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Health 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 23-3 Export Overview Page or Exception Data**

23.1.2 Real-Time Health Status Overview (Topology)

In the Health Monitoring module, you can view the real-time health status of the devices, servers, and resources managed on the platform. If there are network transmission devices managed on the platform, the Real-Time Overview page provides a topology of the managed devices. Topology is a figure that displays the connection relations among network transmission devices, security devices, etc. It is mainly used for network maintenance.

Note

- Make sure the network transmission devices have been added to the platform.
- If a network transmission device can not be recognized by the platform, it will be displayed as an unknown device.

On the top, select **System**.

Select **Maintenance → Real-Time Overview** on the left.

Click **Topology** tab at the top to enter the Topology page.

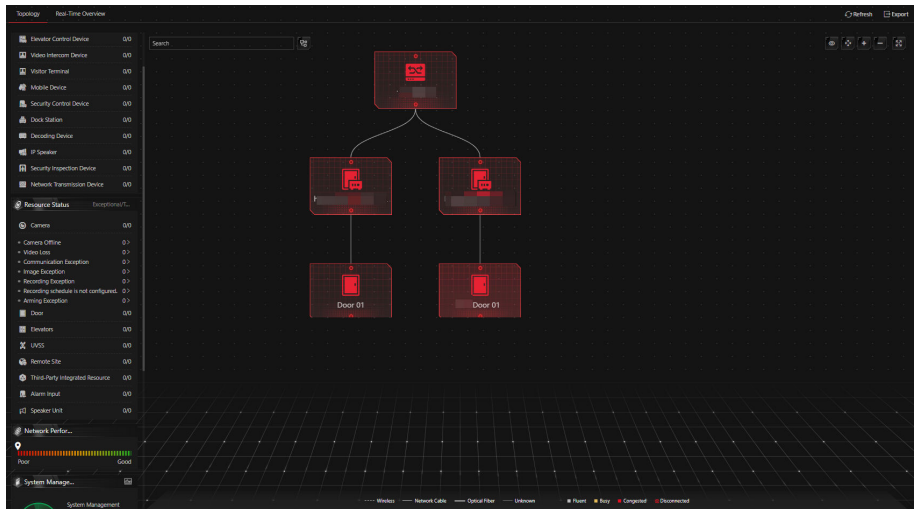
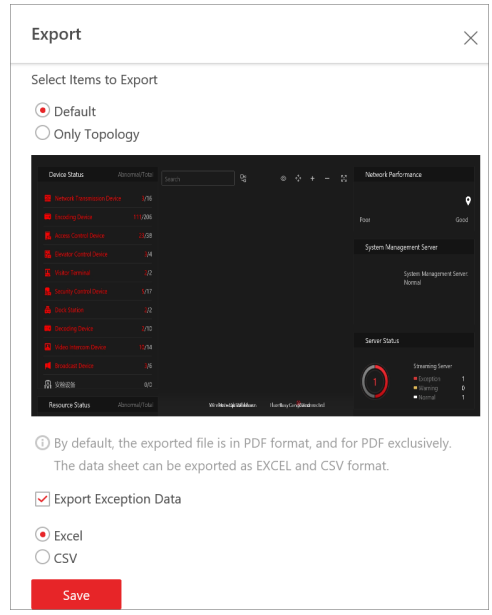


Figure 23-4 Topology Overview

Table 23-2 Topology Page

Section	Description
Device Status	View the abnormal data of different devices (e.g., access control devices) added on the Central System added on the platform. You can click the number to locate the abnormal device in the topology or view the devices' real-time status. If the icon appears beside the device type name, it indicates that the device firmware should be upgraded. For upgrading the firmware, refer to ***Upgrade Device Firmware*** .
Resource Status	View the abnormal data of different resources (e.g., doors, elevators, or alarm inputs) added to the platformadded to the areas of the Central System. You can click the number to view the real-time status details of resources or Remote Sites.
Topology Details	View the relationships among devices, device information, link status, alarm information, etc. See details in ***Topology Details*** .

Section	Description
Network Performance	View the current network performance (i.e., poor or good) of the System Management Server.
System Management Server Status	View the network health status and server running status. Click in the upper right corner of the System Management Server panel to view the running status details of the server, including its CPU usage, RAM usage, etc. **Figure 23-5 System Management Server Status Details**
Server Status	View the status (i.e., exception, warning, normal) of servers added on the Central System added on the platform.
Generate Topology Again	Click **Refresh → Generate Topology Again** to draw the network topology again.
Refresh	• Manual Refresh: Click **Refresh** in the upper right corner of the Real-Time Overview page to manually refresh the resource status on the page. • Auto Refresh: Go to **Maintenance → Basic Configuration → Health Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Health Check Frequency*** .
Export Topology or Exception Data	Click **Export** in the upper right corner of Topology page and select the export type as **Default** or **Only Topology** to export the topology in PDF format or the exception data in Excel/CSV format.

Section	Description
	Note • If the export type is selected as **Default**, the whole displayed information (topology and exception data) on the Health Monitoring page will be exported. • If the export type is selected as **Only Topology**, only the topology will be exported in PDF format.  **Figure 23-6 Export Topology**
Display on Smart Wall	Click to display the overview page on the smart wall if you have added and configured smart walls on the platform .

Topology Details

The topology of devices will display the hierarchical relationships among the devices, device information, link status, alarm information, etc.

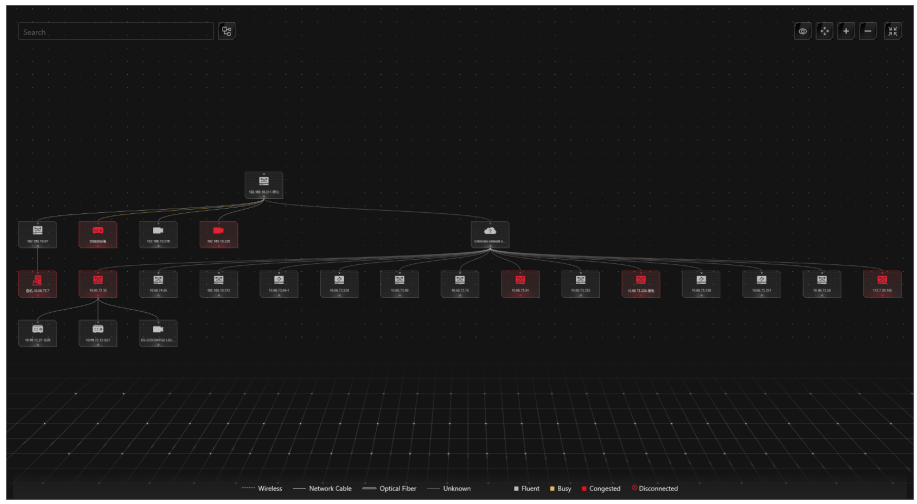


Figure 23-7 Topology Details

Device Node

The device nodes are displayed by icons, including the System Management Server, Recording Server, network transmission device, access control device, video intercom device, etc. Each device node displays the device name and IP address.

Note

- When the device information (device name, IP address, online/offline status) changes, you should manually refresh to generate the topology again or set auto-refresh.
- When the device hierarchy or physical connection changes, you should manually refresh to generate the topology again.
- If the node icon is displayed in red, it indicates that the device is abnormal or alarms are triggered. You can view the reason for device exception or alarm details.
- For the added online devices, the displayed device alias is the same as the device IP address.

View Device Details

Click the device node in the topology and click **Details** in the drop-down list. You can view the device details, including the basic information (i.e., device name, IP address and device model), device usage (e.g., RAM usage, CPU usage, PoE power), port status (port name, working mode, etc.), and device alarm.

Note

The device details vary with different device models.

Link

The color of link indicates the utilization rate of network bandwidth (red: congested, yellow: busy, gray: fluent). And the shape of link indicates the link type (wireless, network link, optical fiber).

View Link Details

Move the cursor to the link between nodes to display the link details. You can view the upstream rate and downstream rate to determine whether the network status is normal or not. You can also view the connected device type, IP address, port name, and port status.

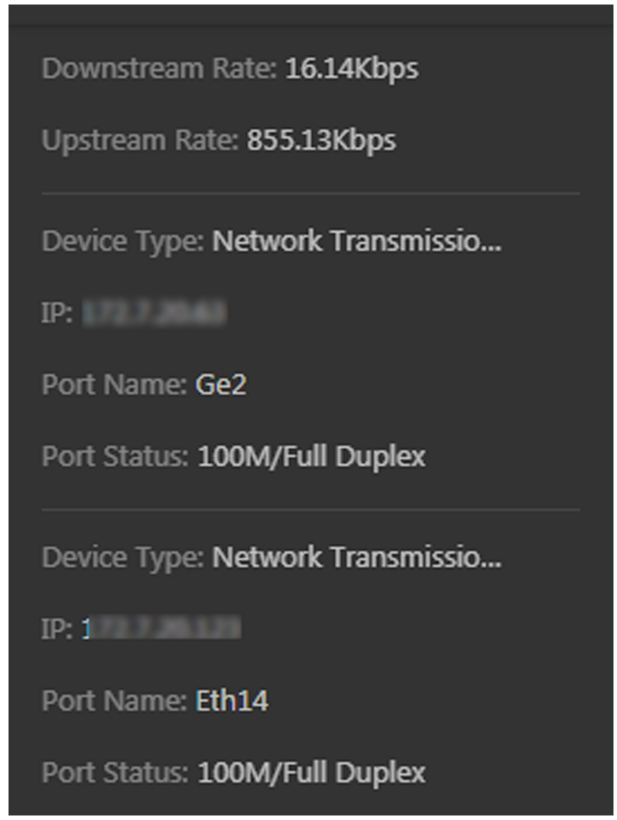


Figure 23-8 View Link Details

View Connection Path

If there is a data transmission failure between the devices, you can view the connection path to judge which link is disconnected, so as to restore the link as quickly as possible. Click the device node and in the topology and click **Show Connection Path** in the drop-down list. According to the information presented in the prompt window, click **Common Unknown Node** or **Select Node** to select the peer node, and then click **OK**. After that, the connection path between the two nodes will be displayed.

Remote Configuration

Click the device node in the topology and click **Remote Configuration** in the drop-down list to configure the device parameters, including system settings, network and port configuration. You can configure the network parameters and device port according to the network usage. For details, refer to the user manual of the device.

Note

This function should be supported by the device.

View Device Logs

When a device failure happens or trouble shooting is required, you can view the device's logs to know the alarms, notifications, operations and events of the device. Click the device node in the topology and click **View Device Logs** in the drop-down list to enter the Device Logs page, and you can set the conditions to search the device logs.

Note

This function should be supported by the device.

Set as Root Node

When you need to adjust the topology structure, you can click the device node in the topology and click **Set as Root Node** in the drop-down list to set the node as the root node.

Note

Only the switch, wireless network bridge, and fiber converter can be set as root node.

Zoom In/Zoom Out

Click + or − to zoom in or zoom out the device node(s) and the subsidiary device node(s). You can scroll the mouse wheel to zoom in or zoom out the topology.

Adjust Topology

Click the background of the topology to move the topology in up, down, right, or left direction.

Full Screen

Click on the upper-right corner of the topology to display the topology in full-screen mode.

Adaptive View

Click on the upper-right corner of the topology to adapt the topology to the current window, to help you know the whole topology hierarchy quickly.

Search

By entering the device name or IP address in the search box, you can quickly locate the device on the topology.

23.2 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, specify the health check frequency, and set the hierarchy and bandwidth threshold for the topology.

23.2.1 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.

On the top, select **System**.

Select **Maintenance → Server Usage Thresholds** on the left.

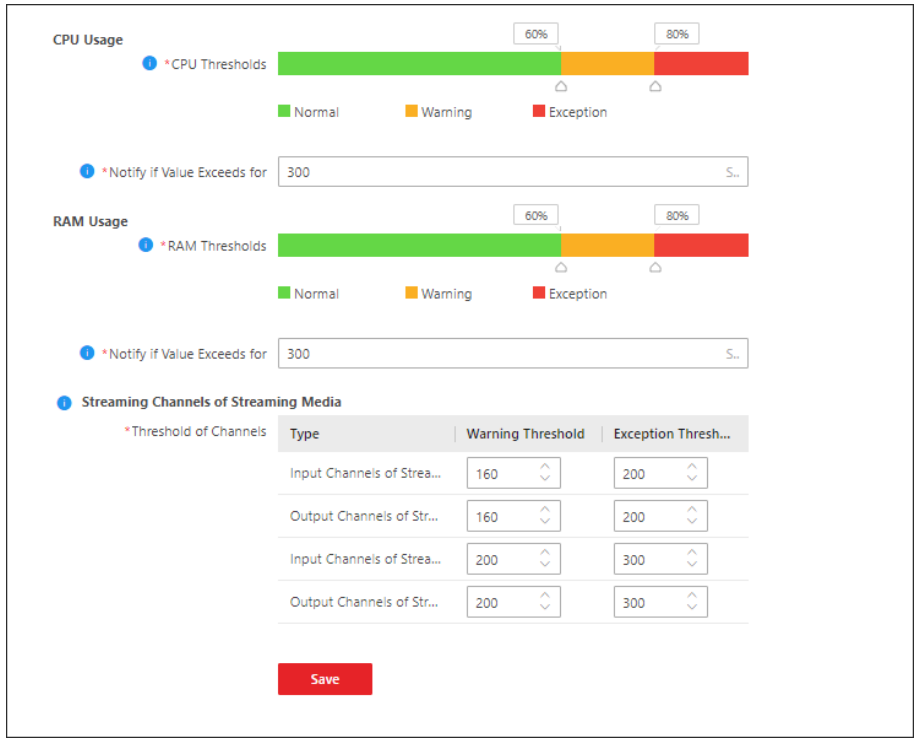


Figure 23-9 Set Server Usage Threshold

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 (see ***Add Normal Event and Alarm***), the alarm will be triggered when the CPU usage reaches 60% and lasts for 20 seconds.

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.

23.2.2 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.

On the top, select **System**.

Select **Maintenance → Network Timeout** on the left.

Select the network timeout and click **Save**.

Table 23-3 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.

23.2.3 Set Health 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 **System → Maintenance → Health Check Frequency** on the left.

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.

23.2.4 Set Topology Show Parameters

You can set parameters in the topology of Health Monitoring module, including topology hierarchy and bandwidth threshold.

Note

For details about health monitoring, see ***Health Monitoring*** .

On the top, select s**System**.

Select **Maintenance → Topology Show** on the left.

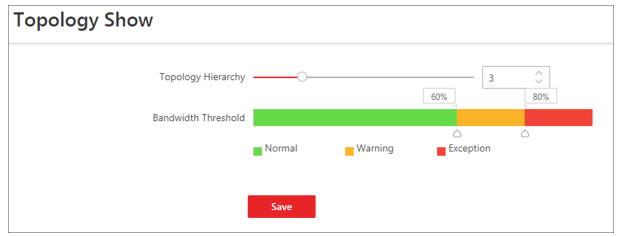


Figure 23-10 Topology Show Settings

Topology Hierarchy

If the devices connection hierarchy is complicated, you can set the topology hierarchy to display the primary devices.

Note

After setting the topology hierarchy, the topology will be generated again.

Bandwidth Threshold

When the bandwidth usage exceeds the threshold, the link on the topology will turns to the corresponding color.

23.3 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** , and select a resource type on the navigation panel on the left.

You can perform the following operations for different resource types.

- Check **Include Sub-area** to display the resources of child areas.
- 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.
- Click **Export** to export the status data as CSV or Excel to the local PC.
- 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 (see details in ***Set Health Check Frequency***).
- On the top-right corner, click to select the type of self-adaptive column width (complete or incomplete display of each column title).

23.3.1 Door Status

On the door status page, you can view the information such as the network status of related devices and door status.

Note

For the door linked to the video intercom device, the door status is not available to be displayed.

You can also perform the following operations.

- Click the door name to view the status details and basic information of the door, and view the live video of the related access control device (if the device is with a camera).
- Click the device name to view the status of the device to which the door is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified door. See details in ***Edit Door*** .
- Click in the Operation column and select a control type from the drop-down list to control the door status.
  - **Unlock**: When the door is locked, unlock the door and it will be open. After the open duration (configured via the Web Client), the door will be closed and locked again automatically.
  - **Lock**: When the door is unlocked, lock the door and it will be closed. The person who has the access permission can access the door with credentials.
  - **Remain Unlocked**: The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required (free access).

    Note

    For the door linked to video intercom device, setting its status to remain unlocked is not available.
  - **Remain Locked**: The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.
- Check the check box and select the exception type from the drop-down list on the top to filter the door status by exception type.

23.3.2 Floor Status

On the floor status page, you can view information, such as the network status of elevator control devices and the card reader status.

You can also perform the following operations.

- Click the name to view the status details and basic information.
- Click the device name to view the status of the device to which the floor is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified floor. See details in ***Edit Elevator*** .
- Check the check box and select the exception type from the drop-down list on the top to filter the floor status by exception type.

23.3.3 Alarm Input Status

You can view the alarm input status including resource usage status (online or offline), arming status, bypass status, fault status, alarm status, detector connection status, battery status, and so on.

You can also perform the following operations.

- Click the device name to view the status of the device to which the alarm input is related.
- Select the device type(s) from the first drop-down list on the top to filter the alarm input status by device type.
- Check the check box and select the exception type from the second drop-down list on the top to filter the alarm input status by exception type.
- Click in the Operation column to go to the Area page to configure the parameters of the alarm input. See details in ***Edit Alarm Input*** .

23.3.4 Recording Server Status

You can view the status and information of Recording Server, such as the recording status, CPU usage, RAM usage, HDD status, and so on.

You can also perform the following operations.

- Click the Recording Server name to view the status details and basic information.
- Click the status in Recording Status column to view the recording status of the channels configured to store the video files in this Recording Server.
- Click the status in Hardware Status or HDD Status column to view the hardware status and HDD exception details if the status is exceptional.
- Check the check box and select the exception type from the drop-down list on the top to filter the Recording Server status by exception type.

23.3.5 Access Control Device Status

You can view the status and information such as network status and battery status of the added access control devices. If the device is turnstile, you can view the status of master lane controller, slave lane controller, and component.

You can perform the following operations.

- Click the device name to view the status and basic information of the access control device, and the related doors and live videos (if the access control device is with a camera).
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified access control device.
- Check the check box and select the exception type from the drop-down list on the top to filter the Access Control Device status by exception type.

23.3.6 Elevator Control Device Status

You can view the information such as network status, arming status, and distributed elevator controller status.

- Click the device name to view the status and basic information of the elevator control device and the related floors.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified elevator control device.
- Check the check box and select the exception type from the drop-down list on the top to filter the elevator control device status by exception type.

23.3.7 Video Intercom Device Status

You can view the status information of the video intercom device such as network status, arming status, and the status of calling center from device (whether the device is able to call the security center of the platform).

You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Click the device name to view the status and basic information of the video intercom device and the related doors.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified video intercom device.
- Select the device type(s) from the first drop-down list on the top to filter the video intercom device status by device type.
- Check the check box and select the exception type from the second drop-down list on the top to filter the video intercom device status by exception type.

23.3.8 Network Transmission Device

You can view the network transmission devices' CPU usgae, RAM usage, PoE usage, occupied ports, and so on.

You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Check the check box and select the exception type from the drop-down list on the top to filter the network transmission device status by exception type.
- Click the device name to view the basic information, device usage, and port information of the network transmission device.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified network transmission device.

23.4 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;

23.4.1 Search for Server Logs

You can search for server logs, which contain error logs, warning logs and information logs. Server logs contain historical users and server activities. You can search for the logs and then check the details.

Steps

1. On the top, select **System**.
2. Select **Maintenance → Server Log** on the left.
3. In **Event**, select one or multiple log types and sub types.

   Note

   Error logs record failures or errors. Warning logs record license expiration events. Information logs refer to other general logs which record successful or unknown operation results.
4. In **Source**, select user and server to set the source of the logs that you want to search for.
5. **Optional:** In **Resource Name**, enter the name of a resource to search the logs of the resource.
6. In **Time**, select the time range of this search.

   Note

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

   All matched logs are listed with details on the right.
8. **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.

23.4.2 Search for Logs Stored on Device

You can search for the logs stored on access control devices, elevator control devices, and network transmission devices.

Steps

1. On the top, select **System**.
2. Select **Maintenance → Device Log** on the left.
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.

23.5 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.

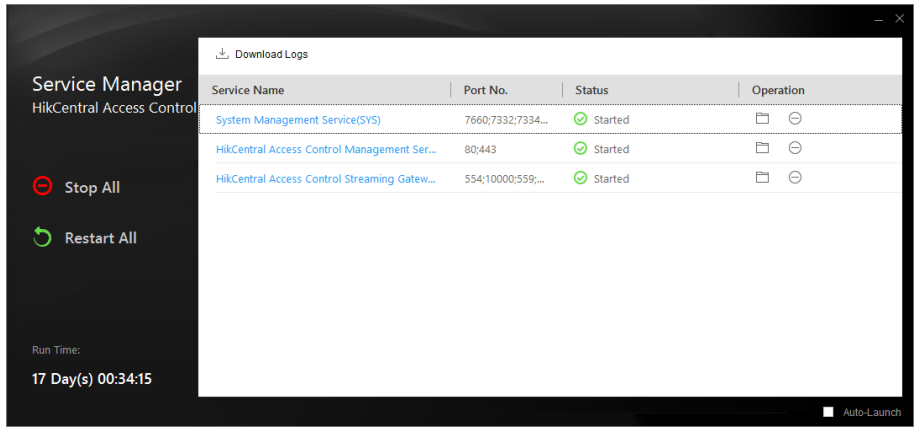


Figure 23-11 Service Manager Main Page

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:** Check **Auto-Launch** to enable launching the Service Manager automatically after the PC started up.
4. Click **Dual-Server Deployment** to deploy the database on another server.

23.6 Set System Data Backup

For purpose of restoring 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, face comparison data, card swiping data, maintenance data, etc.

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, select **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Back Up** tab.
3. In **Type**, select the system 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** if you need to back up the system data immediately.

23.7 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.

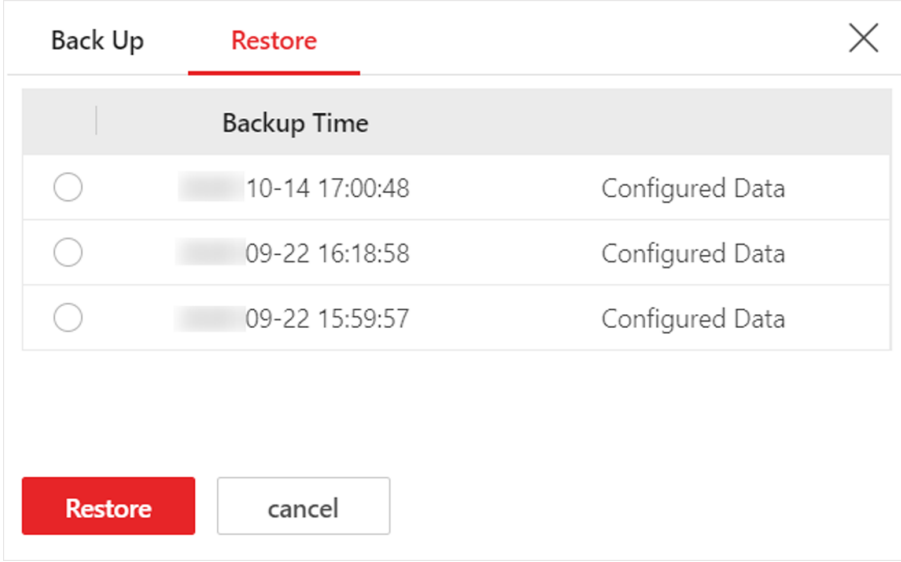


Figure 23-12 Restore System Data

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.

23.8 Export Configuration File

You can export and save configuration data to local disk, including recording settings and resource configurations.

Steps

1. In the top right of the Home Page, 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.

See Far, Go Further

UD31674B