HIKVISION

HikCentral Access Control

AE Specification

Contents

Chapter 1 Disclaimer

ALL TRADEMARKS ARE THE PROPERTIES OF THEIR RESPECTIVE OWNERS

Division 28 - Electronic Safety and Security

Section 28 01 00 - Operation and Maintenance of Electronic Safety and Security

Section 28 01 10 - Operation and Maintenance of Access Control

Chapter 2 General

2.1 Summary of Requirements

HikCentral Access Control Platform

The System Management Service (SYS) provides unified authentication service for connecting with the clients and servers.

Related Requirements

1. Section 27 20 00 - Data Communications
2. Section 28 05 00 - Common Work Results for Electronic Safety and Security
3. Section 28 05 19 - Storage Appliances for Electronic Safety and Security

2.2 References

Abbreviations

1. AD - Active Directory
2. CIF - Common Intermediate Format
3. CD - Client Device
4. DDNS - Dynamic Domain Name Server
5. DHCP - Dynamic Host Configuration Protocol
6. DNS - Domain Name Server
7. DSCP - Differentiated Services Code Point
8. FTP - File Transfer Protocol
9. GUI - Graphical User Interface
10. HTTP - Hypertext Transfer Protocol
11. HTTPS - Secure HTTP
12. ICMP - Internet Control Message Protocol
13. IGMP - Internet Group Management Protocol
14. IP - Internet Protocol
15. JPEG - Joint Photographic Experts Group
16. MicroSD - Removable Miniaturized Secure Digital Flash Memory Card
17. MPEG - Moving Pictures Experts Group
18. NAS - Network Attached Storage
19. NIC - Network Interface Controller
20. NTP - Network Time Protocol over Ethernet
21. PoE - Power over Ethernet
22. PPPoE - Point-to-Point Protocol over Ethernet
23. QoS - Quality of Service
24. RTP - Real-Time Transport Protocol

25. RTSP - Real-Time Streaming Protocol
26. SD Card - Secure Digital Flash Memory Card
27. SMTP - Simple Mail Transfer Protocol
28. TCP - Transmission Control Protocol
29. UDP - User Datagram Protocol
30. UPnP - Universal Plug and Play
31. SYS - System Management Service

2.3 Certifications, Standards and Ratings

Reference Standards

1. Network Standard:
   IEEE – 802.3 Ethernet Standards
2. Video Compression:
   ITU-T H.264 standard and ISO/IEC MPEG-4 AVC standard (formally, ISO/IEC 14496-10 – MPEG-4 Part 10, Advanced Video Coding), H.264+, H.265, and H.265+ encoding formats

2.4 Submittals

Product Data

1. Manufacturer's hard (physical) or soft (electronic) datasheets
2. Installation and operating manuals for any and all equipment required for a SYS (System Management System)
3. Manufacturer's warranty documentation

2.5 Qualifications

Requirements

1. This product shall be manufactured by an enterprise whose quality systems are in direct compliance with ISO-9001 protocols.
2. All installations, integration, testing, programming, system commission, and related work shall be done by installers who are trained, authorized, and certified by the manufacturer.

2.6 Delivery, Storage, and Handling

General

The product shall be delivered in accordance with the manufacturer's recommendations.

2.7 Licensing and Support Agreements

Requires no Software Support Agreements with the manufacturer.

2.8 Tech Support (STAYS THE SAME UNLESS WARRANTY TERMS HAVE CHANGED)

Support

Technical support shall be based in each area.

Chapter 3 Product

3.1 Manufacturer

1. Manufacturer:
   No.555 Qianmo Road, Binjiang District, Hangzhou 310051, China
   Phone: +86-0571-8807-5998
   Web: www.hikvision.com
2. Product:
   HikCentral Access Control - shall be designed to manage distributed sites or large groupings of cameras recording on pStor.

3.2 Service Description

HikCentral Access Control System Management Service

SYS maximum capacity for devices management and event handling:

1. Manages up to 2,048 resources, including Access Control Devices and Elevator Control Devices
2. Imports up to 5,000 alarm inputs and 3,000 alarm outputs per SYS.

Service Manager: An application that manages the following Services

System Management Service is the core component of HikCentral Access Control, providing authentication, permission granting, and management services. It authenticates the Mobile Client access, manages the users, roles, permissions and monitors devices, and provides the interface for third-party system integration. It includes the following service:

1. System Management Service
   a. Provide the unified authentication service for connecting with the clients and servers
   b. Provides the centralized management for the users, roles, permissions, devices, and services.
   c. Provides the configuration interface for security and management module.
2. Management Service
   a. The content server and signaling gateway of HikCentral Access Control
   b. Mainly responsible for storage of static pages and reverse proxy of device configuration
3. Streaming Gateway
   a. A component of SYS which forwards the video and audio data
   b. Shall support up to 200 devices @ 2 Mbps input and 200 devices @ 2 Mbps output.
   c. Responds to Mobile Client's request and sends real-time messages to Mobile Client

3.3 Accessibility and Management Capabilities

1. Up to 100 simultaneous devices shall be able to connect via an App on a smart phone (iOS or Android). There is no connection licenses required
2. Shall support Active Directory integration for user management of Mobile Client (iOS and Android mobile operating systems)
3. Administration functions and operation functions are performed separately in the following clients:
    a. Web Client: All administration of SYS shall be performed using a web browser client via LAN, WAN or Internet. No client software is required for administration of the system
    b. Mobile Client: Basic security operator features shall be accessed through the Mobile Client connected to SYS via LAN, WAN, or Internet
4. Shall support H.264, H.264+, H.265, and H.265+ encoding formats
5. Shall support SUP management of license to ensure smooth upgrade of HikCentral Access Control
6. Shall support Downloading logs from the Service Manager
7. Shall support multi-time zone and DST

3.4 Network

Security Access

1. Shall have a built-in password protection not dependent on server
2. The System shall have User Authentication
3. Secure Activation
    a. A system algorithm shall check the user defined password for strength, based on the manufacturer’s criteria.
    b. System shall determine and display password security level as “weak”, “medium”, or “strong”.
    c. Password shall contain a minimum of two kinds of characters (lowercase letters, uppercase letters, numbers and special characters).
    d. Only ASCII characters shall be allowed.
    e. Password length shall be eight characters minimum.

3.5 PC Requirements

HikCentral Access Control SYS:

- Intel® Core™ i3-8100 @ 3.60 GHz
- RAM: 4 GB
- Network: GbE network interface card
- Hard Disk Type: Micron 1300 SATA SSD
- Hard Drive Capacity: 256 GB for the HDD where SYS is installed
- Other: Microsoft® Windows 10 (64-bit)

3.6 Signal Flow

3.6.1 Login

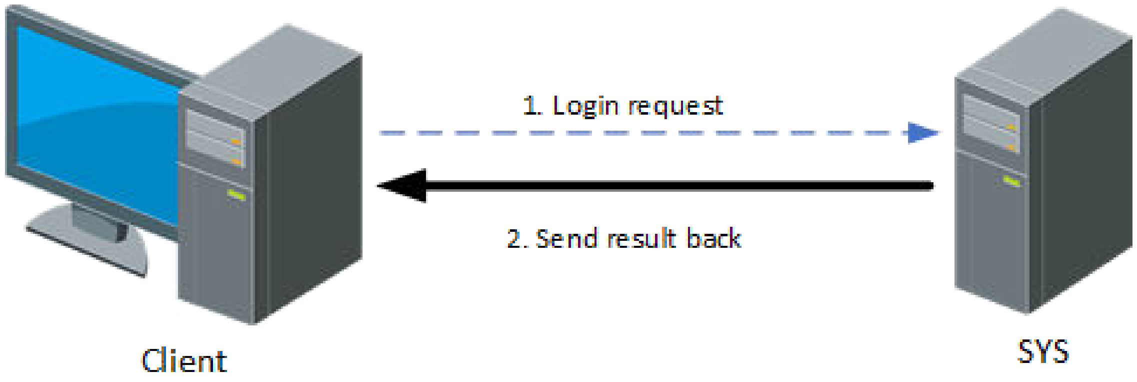

Figure 3-1 Login Flow

During the login, the signaling shall be exchanged between the client (Web Client/Mobile Client) and the SYS.

The signaling interaction process is as follows:

1. Enter the user name and password (domain name) on the client, which shall be sent to the SYS.
2. The SYS shall receive the information, check whether the user name and password (domain name) are correct, and send the result to the client.

3.6.2 Alarm

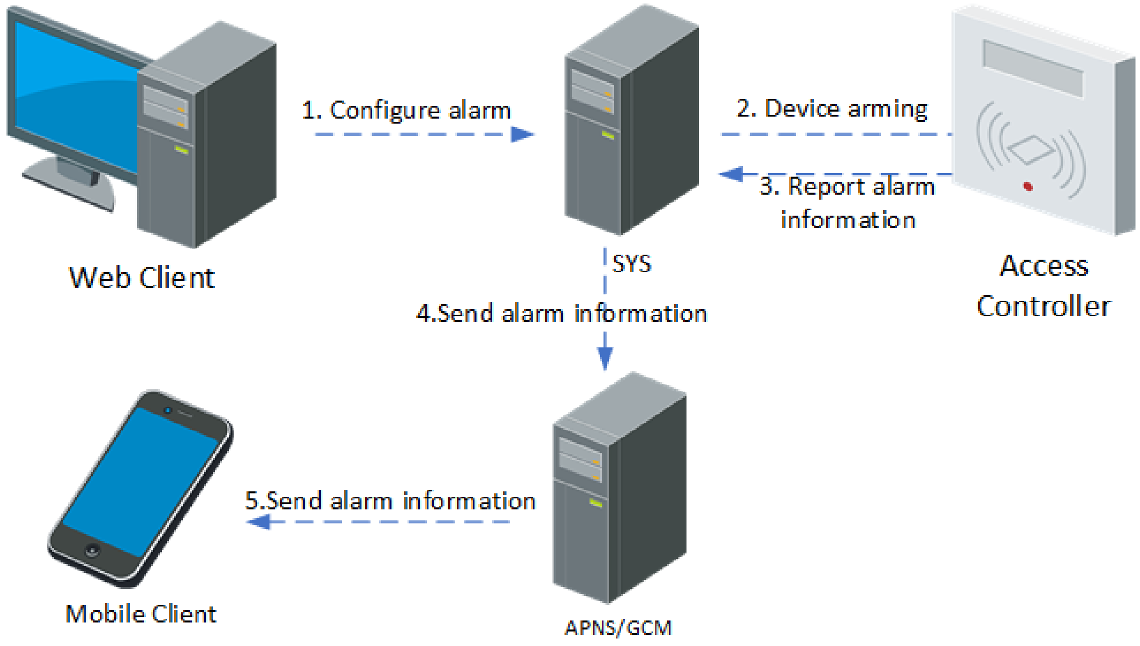

Figure 3-2 Alarm Flow

The process of alarm configuration is as follows:

1. Configure alarm on the Web Client, and the alarm configuration shall be sent to the SYS.
2. The device shall be armed by the SYS according the arming schedule.

The process of reporting an alarm is as follows:

1. If an alarm is triggered, the device shall report the alarm to the SYS.
2. The SYS shall send the obtained alarm information to the APNS/GCM server.
3. The APNS/GCM server shall send the corresponding alarm information to the Mobile Client.

3.6.3 Access Control

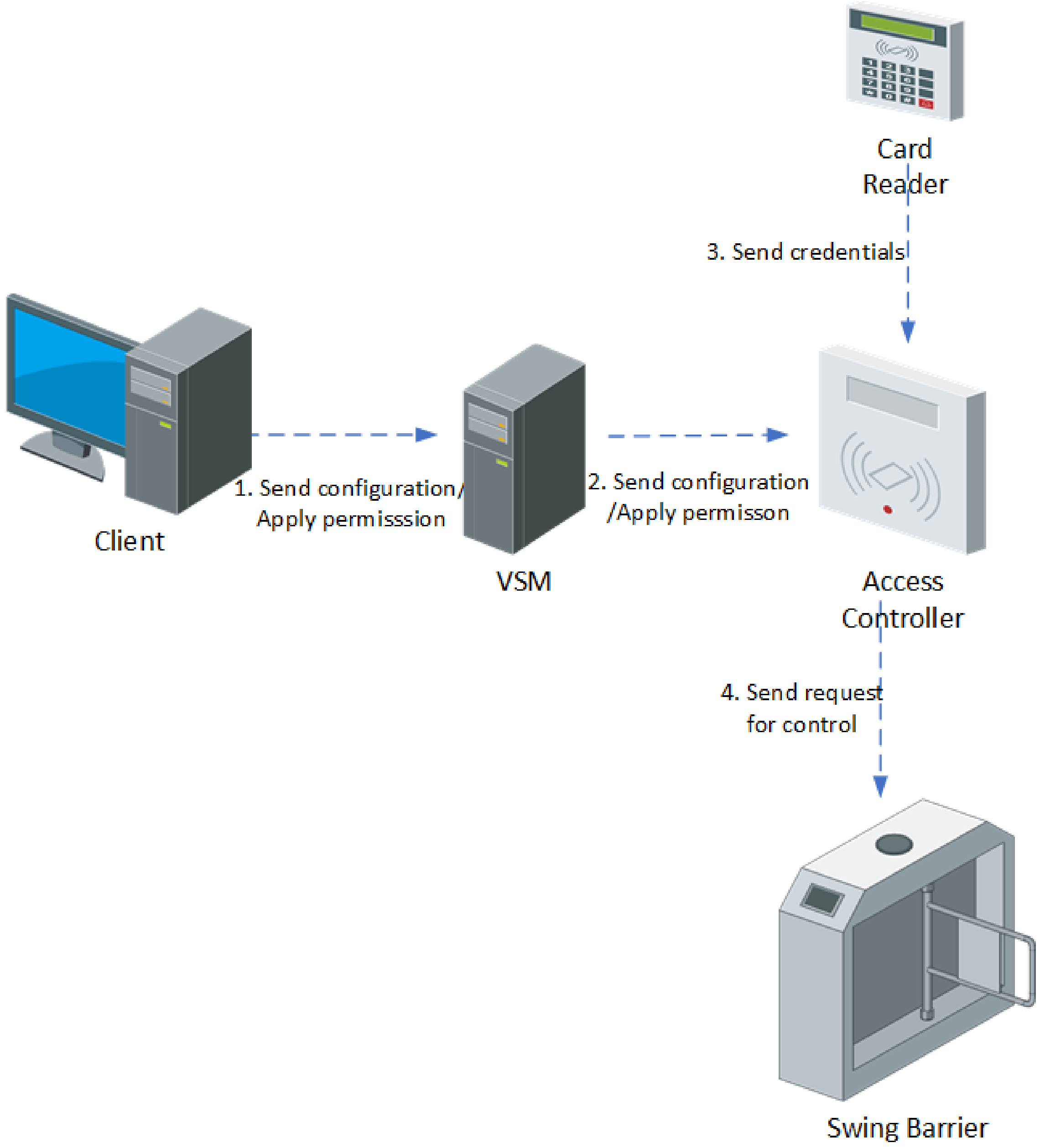

Figure 3-3 Access Control Flow

The signaling process of access control and management is as follows:

1. The Web Client shall send an access control configuration command (including personnel permission, device configuration and event configuration) to the SYS.
2. The SY shall send the configuration command to the device.

3. The card reader shall obtain the corresponding instruction, and send the credential information to the access controller.
4. The access controller shall send the control request to the swing barrier according to the obtained instruction to control the switch status of the swing barrier.

3.6.4 Status Monitoring

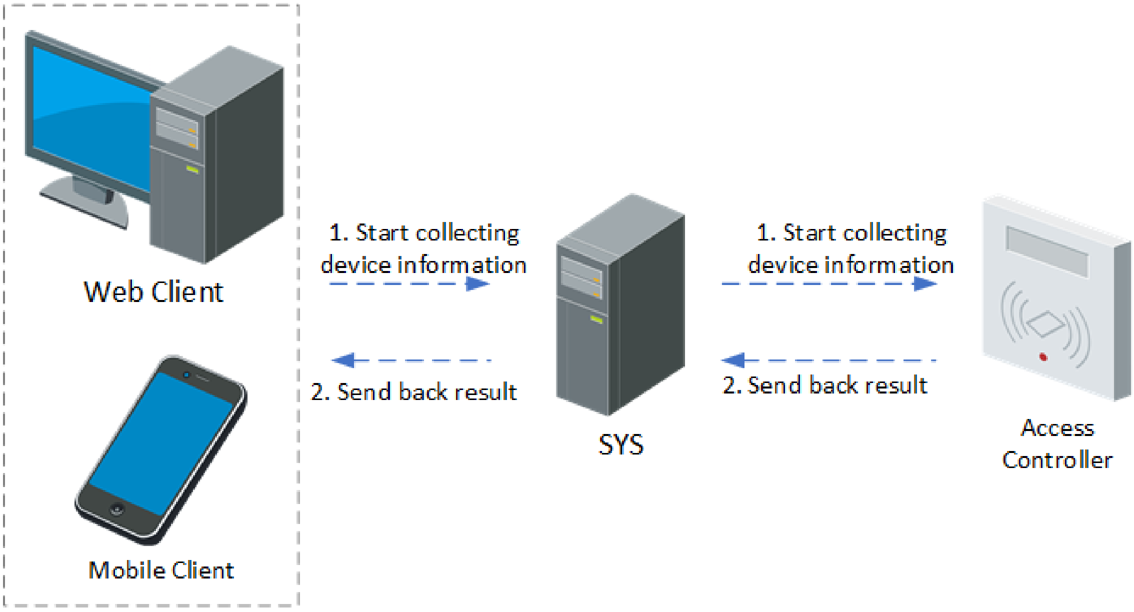

Figure 3-4 Flow of Status Monitoring

The device status inspection shall consist of the following two situations: interaction between the client and the SYS, and between the device and the SYS.

The platform shall initiate inspection information every 3 minutes.

Interaction Between SYS and Device

1. The SYS shall send an inspection command to the device.
2. The device shall send back the status of the device to the SYS.

Interaction Between Client and SYS

1. The Web Client and Mobile Client shall send an inspection command to the SYS.
2. The SYS shall send the current status of the device to the Web Client and Mobile Client.

3.7 System Security

3.7.1 Security Design Overview

The HikCentral Access Control platform shall consist of the server, client, service component, and platform SDK. The interaction between server and client, server and service component, server and platform SDK shall support HTTP and HTTPS.

To ensure the security of data storage, all the sensitive data stored in the server shall be encrypted. All the sensitive information that does not need to be decrypted shall be encrypted by irreversible encryption scheme. All sensitive information that needs to be decrypted shall be encrypted by encryption scheme that can be decrypted.

The HikCentral Access Control shall adopt the following encryption algorithms: RSA, AES, SHA, and MD5. All the encryption algorithms shall come from the standard open-source library OpenSSL-1.0.2K. The OpenSSL version shall be updated according to the policies of Hikvision security lab.

3.7.2 System Security Solution

Access Protocol

By default, the HTTP protocol is used for web access. By optional, users can enable the HTTPS protocol.

HTTPS: Users can import the HTTPS certificate to improve the security of data transmission.

HTTP: In HTTP mode, the platform shall provide an independent security solution to prevent replay attacks.

Login Authentication

The platform authenticates users based on user name and password. The password strength and expiration time can be configured separately on the platform. If the administrator forgets the login password, the platform shall allow users to reset the password by license. To ensure the system security, the input information shall be hidden during password input.

During the transmission, the password shall be encrypted by RSA algorithm in HTTP mode, and the HTTPS internal encryption mechanism shall be used in HTTPS mode. In platform login authentication, the verification code + user lock + IP address lock shall be used to prevent brute force cracking from malicious user, to improve the platform security level.

Man-Machine Authentication: If an incorrect password is entered during the login, users shall manually enter the verification code.

User Lock: This parameter is mandatory enabled. If the password is entered incorrectly for five consecutive times, the user cannot log in to the system within 30 minutes.

IP Address Lock: This parameter is enabled by default. Users can manually configure the number of error times and lock period. If the number of incorrect login attempts for the same IP address exceeds the specified value, the IP address cannot be used to log in to the system within the specified lock period.

Platform Access

After the client successfully logs in to the system, the server shall randomly generate a session for each client. The session can effectively reduce the cracking risks caused by the frequent user name and password interaction verification during the business. Each session shall have a fixed lifetime. When a session carried by a client expires, the user shall log in to the platform again.

In HTTP mode, to ensure that the platform is not attacked by replay attacks, each session shall carry an anti-replay token, which is unique in each session. The token is invalid immediately after each request to prevent repeated token attacks. The token shall be encrypted using AES.

Sensitive Information Processing

For sensitive information such as user name and password that are daily used, HikCentral Access Control shall provide security solutions based on the actual service scenarios.

All sensitive information is encrypted during the interaction between the client and server. In HTTP mode, the AES encryption shall be used to generate a random AES key for each login, to ensure that data is not easily stolen. In HTTPS mode, SSL certificate encryption shall be used.

For the sensitive information storage, HikCentral Access Control shall provide different storage scheme according to the different business requirements. To prevent the leakage of the encryption key of a platform from affecting other platforms, HikCentral Access Control shall adopt the dynamic AES encryption scheme for sensitive information (such as the database access password and device access password) that needs to be locally stored. To prevent system user password leakage caused by system data file leakage, the platform user password shall be encrypted by SHA algorithm and stored in cipher text.

Chapter 4 Function

The platform shall support the functions below.

4.1 Person Management

- ***Person Management***
- ***Credential Management***
- ***Resignation Management***
- ***Position Management***

4.1.1 Person Management

Person Information

- The platform shall support entering person information, including basic information, access level, shift schedule, face comparison group, dock station group, resident information, and custom public information. Basic Information: ID (16 digits and letters); Person group; first name (up to 128 characters); last name (128 characters); skin-surface temperature and status; effective period (10 years from the current time); e-mail; phone No.; super user; extended access; device administrator; PIN code; remark; custom private information.
- The platform shall support changing a person's organization.
- The platform shall support exporting all the added person information as a ZIP file and setting a password for decompressing the ZIP file.
- The platform shall support segmenting person information by tabs on the Add Person page.
- The platform shall support exporting person information with additional items.
- The platform shall support importing person information via template with additional items.
- The platform shall support adding a person to the emergency counting group.
- The platform shall support editing credentials (including card, print, face, and iris) in the person list.

Batch Person Management

- The platform shall support batch adjusting the effective period for persons.
- The platform shall support filtering and batch exporting the expired person information.
- The platform shall support batch reporting cards loss.
- The platform shall support disabling and restoring access levels of persons temporarily.

Customize Person Information

- The platform shall support customizing up to 20 private information items and 4 types per information item including text, value, date, and single selection (limited by the permission of the platform).
- The platform shall support customizing up to 20 public information items and one type (only text) per information item (limited by the permission of the platform).

Login

- The platform shall support administrator enabling employees' self-service login (enabled by default) and setting employees' password (employee ID by default).
- The platform shall support employees' self-service login to the platform.
- The platform shall support locking IP address for a specified period of time after specific number of failed password attempts.
- The platform shall support setting maximum password age.
- The platform shall support requiring employees to change the password upon the first login, sending notes when the password expires, and resetting new password if employees forgot the password.
- The platform shall support login expiring after a period during which no action happens.

Self-Service Uploading Person Information

- The platform shall support entering the Self-Registration page by scanning the self-registration QR code, entering, and submitting person information to the platform.
- The platform shall support enabling the face picture quality verification of the device. After it is enabled, you can choose any device with the face picture quality verification function as a device for verification. It is disabled by default.
- The platform shall support enabling Review Self-Registered Persons function. After it is enabled, all person information submitted in a self-service manner must be reviewed and approved by the Administrator before being imported to the platform.
- The platform shall support importing person information added in a self-service manner into a specific organization (root organization is the default).
- The platform shall support administrators verifying person information uploaded by self-service: approve, reject, and delete.

Import Persons

- The platform shall support importing person information via Excel file and setting parameters about whether to replace duplicate persons and card numbers.
- The platform shall support importing profile pictures in ZIP format and enabling/disabling face picture quality evaluation.
- The platform shall support importing persons from devices.

AD Domain Synchronization

- The platform shall support configuring the mapping relation between the AD domain and the person.
- The platform shall support synchronizing the AD domain with the person or the person group.
- The platform shall support synchronizing the AD domain with the security group.

Handling Persons' Permissions Quickly

- The platform shall support clearing permissions.
- The platform shall support detecting permission status.
- The platform shall support disabling access levels and restoring access levels in a batch.

Person Resignation

- The platform shall support resignation management.
- The platform shall support deleting the resigned persons' access levels at the resignation date.
- The platform shall support enabling/disabling attendance calculation during the period between applying for resignation and resignation date.
- The platform shall support searching for access and attendance records of resigned persons.

4.1.2 Credential Management

Card Management

1. Support up to 20 digits for one card number.
2. Support adding up to five cards to a person.
3. Support entering the card number manually.
4. Support card enrollment stations reading card numbers.
5. Support encrypting card sectors (one sector for a time) only when the encryption is via the card enrollment station(communicating with the platform via USB).
6. Support enrollment station (communicating with the platform via network) reading card numbers (supported card types including EM, M1, ID, DESfire, FeliCa, and CPU).
7. Support enrollment station (communicating with the platform via USB) reading card numbers (supported card types including EM, M1, ID, DESfire, FeliCa, and CPU).
8. Support any card reader of remote access control devices reading card numbers .
9. Card types: common, duress, and dismiss.
10. Support issuing cards in a batch.
11. Support reporting card loss and canceling the card loss report.

Fingerprint Management

1. Support up to 10 fingerprints per person.
2. Support fingerprint enrollment devices enrolling fingerprints.

3. Support enrolling fingerprints via enrollment station(communicating with the platform via network).
4. Support enrolling fingerprints via enrollment station(communicating with the platform via USB).
5. Support any card reader of remote access control devices enrolling fingerprints.
6. Fingerprint types: common, duress, and dismiss.
7. Support fingerprint duplicate checking and fingerprint quality grading.

Face Picture Management

1. Support only one face picture per person.
2. Support uploading local face pictures.
3. Support using a USB camera or a laptop with a camera enrolling face pictures.
4. Support enrolling face pictures via enrollment station (communicating with the platform via network).
5. Support enrolling face pictures via enrollment station (communicating with the platform via USB).
6. Support collecting face pictures via remote access control devices.
7. Support exporting all face pictures of all added persons as a ZIP file and setting a password for decompressing the ZIP file.
8. Support deleting a facial credential or batch deleting facial credentials.

Password Management

Support setting the password (unique, containing 4 to 8 digits, and only one password per person)

Iris Management

1. Support collecting 2 irises for each person.
2. Support collecting irises by device remotely as person credentials and applying irises to devices.

4.1.3 Resignation Management

1. The platform shall support resignation management.
2. The platform shall support deleting the resigned persons' access levels at the resignation date.
3. The platform shall support enabling/disabling attendance calculation during the period between applying for resignation and resignation date.
4. The platform shall support searching for access and attendance records of resigned persons.

4.1.4 Position Management

1. The platform shall support adding, deleting, and editing positions.
2. The platform shall support importing positions in a batch.
3. The platform shall support linking a position to different persons.

4. The platform shall support linking a person to a position on the person information page.
5. The platform shall support viewing person numbers of a position and the number of resigned persons.

4.2 System Management

- ***General Settings***
- ***System Security***
- ***License Management***
- ***Others***
- ***Data Compatibility***

4.2.1 General Settings

Quick Start

- The Home page displays instructions of new features and release notes.
- Totally new navigation bar (The first-level menu is displayed on the top; the second-level and third-level menu is displayed on the left; the tab pages are displayed on the right).
- Support quick configuration guide for Access Control and Time & Attendance.
- Support up to 20 quick starts for different functions.
- Support downloading center.

Dashboard

- Support displaying the statistics of persons, devices, and attendance results.
- Support displaying pending tasks of attendance application flow.
- Support displaying real-time events and alarm notifications.
- The Person Credential Status, Device Status, and Attendance Report on the Home page supports click the pie chart for details.

User Preference

1. Support setting the site name
2. Support setting the first day of the week
3. Support setting the displayed temperature unit for the platform, including Celsius, Fahrenheit, and Kelvin
4. Support setting whether to display the mask related functions
5. Support setting the displayed calendar type for the platform, including Gregorian Calendar, Thai Calendar, and Nepal Calendar

Printer Settings

Support adding printers to the platform

Card Template

Support setting templates for printing cards

Network Settings

1. Support setting the NTP server for time synchronization
2. Support setting AD (Active Directory) domain for synchronizing person information
3. Support protocols for devices accessing the platform. The supported protocol types include the Open Video Network Interface protocol and ISUP v5.0 or below.
4. Support setting ports for WAN access
5. Support resetting device network information

Storage Settings

1. Support setting the local storage location, the picture or file quota, and the overwriting strategy for pictures and files
2. Support setting the retention period (unit: year) for the general data (such as events, logs) and the function data (such as card swiping records)

Other Settings

1. Support setting holidays and the repeating strategy. The holiday type includes regular holiday (e.g., May Day) and irregular holiday (e.g., Mother's Day)
2. Support setting email templates (including recipients, subject, and content) for regularly sending reports or events/alarms to the related persons

Time Zone Settings

1. Support reading time zone list from the operating system
2. Support setting the time zone for devices and getting the device's time zone

Multi-Level Organization Management

1. Support up to 10 lower-levels of an organization displayed as a tree structure
2. Basic information: parent group, organization name, and description

4.2.2 System Security

System Security

1. Support setting transfer protocol to HTTPS, and setting the IP address for receiving device information
2. Support setting the password for the local database

3. Support viewing the service component certificate, including Streaming Service and Cloud Storage Service.
4. Support setting security strategy for login, including locking IP address if the failed login attempts exceeded the limit, enabling maximum password age, automatically locking the Control Client after the defined time period of inactivity, and setting double authentications

User Security

1. Support setting permissions for roles, including resource access permissions, resource permissions, configuration and operation permissions, user status (inactivate or activate), and role effective period
2. Support manually adding users and user groups, importing AD (Activate Directory) domain users, activating or inactivating users, forcing logout, and so on

4.2.3 License Management

Basic Management

1. Support activating Licenses in online or offline mode
2. Support updating Licenses in online or offline mode
3. Support deactivating Licenses in online or offline mode
4. Support viewing the License details

SSP Expiration Prompt Settings

Support setting the expiration prompt (upgrading or adding values) for SSP (Software Service Program)

License Exception Detection

1. Support detecting whether the License file is damaged
2. Support detecting whether the number of resources exceeded limit
3. Support detecting whether the basic activation code is available
4. Support detecting whether there are multiple abnormal basic activation codes
5. Support detecting whether the update is limited
6. Support detecting whether the exception occurred when updating the License
7. Support restoring the server after the exception occurred

4.2.4 Others

SSP Expiration Prompt

Support setting SSP expiration prompt for sending a reminding email to the user when the SSP or SUP is going to expire

Company Information

Support setting the company information

4.2.5 Data Compatibility

The platform shall support importing configuration files (including information about devices, persons, and events) of iVMS-4200 and iVMS-4200 AC.

4.3 Maintenance

- ***Scheduled Report***
- ***Server Network Management***
- ***Health Monitoring***
- ***Resource Status***
- ***System Log***

4.3.1 Scheduled Report

Support regularly calculating resource logs and device logs, and support sending reports to email.

4.3.2 Server Network Management

Server Usage Threshold

1. Support configuring usage thresholds of CPU and RAM of the whole server.
2. Support monitoring the usage of CPU and RAM in real time.

Network Timeout

Support configuring interaction request timeout according to the network status. The default timeout is 60s, which can be configured as 90s or 120s.

Health Check Frequency

1. Support checking device and service status.
   a. Device: access control device, elevator control device, video intercom device, and network transmission device.
   b. Server: recording server.
   c. Checking frequency: minute, hour, day (minimum: 1 minute ； maximum ： 30 days; default: 3 minutes).
2. Support checking device capabilities.

Checking frequency: minute, hour, day (minimum: 1 minute; maximum; 30 days; default: 3 minutes).

3. Support checking recording status.
   Checking frequency: minute, hour, day (minimum: 1 minute; maximum; 30 days; default: 3 minutes).
4. Support enabling alarm/event.
   Checking frequency: minute, hour, day (minimum: 1 minute; maximum: 30 days; default: 3 minutes).

4.3.3 Health Monitoring

Real-time Overview

1. Support displaying device status (normal and exception), displaying server and resource status (normal, exception and warning).
2. Support refreshing manually and refreshing regularly the status of device, resource and server.
3. Support configuring refreshing regularly on the Mobile Client (by default, refreshing regularly on the web client every 3 minutes).
4. Support exporting data of all device status and resource status as EXCEL or CSV format.
5. Support exporting the selected data (all or exception data).
6. Support exporting only topology or topology with data when there is topology.
7. Support showing and refreshing topology hierarchy of network.
8. Support zooming in and out the topology, enlarging view, full screen, and self-adaptive.
9. Support searching for resource location and connection path.
10. Support viewing details, remote configuration and device logs.
11. Support displaying normal and exception data of System Management Server.
12. Support displaying real-time CPU, RAM, picture storage space, network(sending and receiving), and streaming gateway.
13. Support displaying network status (poor to good) for Smart Managed Switch.

History Overview

1. Support viewing the resource online rate.
2. Support sorting resource by total offline and offline times.
3. Support viewing device online rate.
4. Support sorting devices by total offline and offline times.
5. Support redirecting to the Device Logs page.
6. Support viewing recording integrity rate.
7. Support refreshing manually.
8. Support exporting data (all or exception data) as EXCEL or CSV format.
9. Support exporting the selected data (all or exception data).

4.3.4 Resource Status

Door

1. Support door status (network status, face recognition terminal network status, door status, configured door status, and card reader status) and checking time.
2. Support refreshing manually and refreshing regularly
3. Support exporting door status data.
4. Support viewing door details.
5. Supports viewing status of face recognition terminals.
6. Supports viewing card reader status.
7. Supports controlling door status remotely.

Elevator

1. Support viewing door status (network status and card reader status) and checking time.
2. Support refreshing manually and refreshing regularly
3. Support exporting elevator status data.
4. Supports viewing elevator resource status.
5. Supports viewing card reader status.

Access Control Device

1. Support viewing access control device status (network status, main/sub lane controller network, component, arming, tampering status and calling center from device) and checking time.
2. Support refreshing manually and refreshing regularly.
3. Support exporting access control device status data.
4. Support viewing device details and the detailed information of linked resources (door and camera).

Elevator Control Device

1. Support viewing elevator control device status (network status, battery status, arming status and distributed elevator control device status) and checking time.
2. Support manual refresh and scheduled refresh
3. Support exporting data of elevator control device status.
4. Support viewing details of elevator control device.
5. Support controlling the elevator remotely.

Video Intercom Device

1. Support viewing video intercom device status (network status, arming status and calling center from device) and checking time.
2. Support refreshing manually and refreshing regularly.
3. Support exporting data of video intercom device status.

4. Support viewing details of video intercom device.
5. Support dialing on the Mobile Client for indoor station.

Alarm Input

1. Support viewing alarm input status (name, area, serial No., version, disk status, network status, arming status and first added time) and checking time.
2. Support refreshing manually and refreshing regularly.
3. Support exporting data of alarm input status.
4. Support viewing details of alarm input resource.
5. Support viewing alarm input status according to device type.

Third-Party Integrated Resource

1. Support viewing third-party integrated resource status (network status and resource status) and manufacturer.
2. Support refreshing manually and refreshing regularly.
3. Support exporting third-party integrated resource status data.
4. Support viewing third-party integrated resource details.

Network Transmission Device

1. Support network transmission device status (network status, POE usage) and checking time.
2. Support refreshing manually and refreshing regularly.
3. Support exporting network device status data.
4. Support viewing network transmission device status (network status, CPU usage, RAM usage, occupied ports, PoE usage, device exception as first added time) and checking time.

4.3.5 System Log

Server Logs

1. Support searching for the log according to log type, log trigger, filtered resource and selected time.
2. Support exporting logs as EXCEL or CSV format.

Device Logs

1. Support searching for the local logs of access control device, elevator control device, and network device.
2. Support exporting local logs of the device.
3. Support exporting online/offline logs of multiple devices.
4. Support exporting online/offline logs for the device.
5. Support displaying by graph and list about device online duration records and the latest offline time.

4.4 Map Management

4.4.1 Map Settings

Resource Configuration: Support dragging hot spots, labels, general resources, alarm devices to maps.

4.4.2 Map Monitoring

1. Health Monitoring: Support viewing real-time device/platform status.
2. Access Control: Support checking access control records, recognition exceptions, etc. of the current day.
3. Alarm: Support viewing the number of alarms and alarm handling information of the current day.

4.4.3 Map Applications

1. Customize Labels: Support customizing label icons.
2. Google Map: Support the Google Map.
3. Filter Resources: Support filtering resources on maps.

4.5 Event and Alarm

4.5.1 Triggering Event

Classification

1. The triggering events are classified by modules, including access control, alarm, maintenance, user, user-defined event, and generic event.
2. The Edit Alarm page shall provide the icon for remote configuration of the triggering source. Users can click the icon to open the remote configuration page of the device or server.

Generic Event

1. Support selecting TCP or UDP as the transport type.
2. Support transport types of HTTP and HTTPS.
3. Support selecting Search or Match as the match type.
4. Support selecting AND or OR as the expression.

User-Defined Event

Support setting self-defined event if the system-monitored events or the generic event cannot meet the users' need.

4.5.2 Event Receiving

Event Receiving Schedule

1. Support setting self-defined event if the system-monitored events or the generic event cannot meet the users' need.
2. Support setting receiving schedule template of events, including All-Day, Weekday, and Holiday template. Users can select the templates defined by the platform or customize a template.
3. The Add Event and Alarm page supports enabling the function of ignoring recurred events or alarms, and users can configure the duration for ignoring.
4. Support configuring alarm recipient groups: After adding users to the alarm recipient group, the users in the group will receive notifications once alarms are triggered without setting recipients for each alarm.
5. Support batch adding users as alarm recipients.
6. Support selecting alarm recipients or alarm recipient group for each alarm.
7. Support configuring both triggering event and alarm for a source.
8. Support configuring one or multiple holidays for an alarm receiving schedule template.

4.5.3 Alarm Linkage

Linkage Actions

1. Support configuring the colors for events.
2. Support adding color templates for further reuse.

3. Support setting Link Alarm Input as the linkage action. Select alarm inputs and these alarm inputs will be armed or disarmed when the alarm occurs.
4. Support setting Link Alarm Output as the linkage action: select different ways for closing the alarm output when the alarm output works, select closing the alarm output automatically or manually.
5. Support setting Link Third-Party Integrated Resource as the linkage action. Select the control about details operations that will happen when the alarm occurs.
6. Support setting Send Email as the linkage action. Select an email template to send the alarm information according to the defined email settings.
7. Support setting Link Printer as the linkage action. If the source type is alarm input, users can link to print entry & exit counting report of certain entry & exit counting group.
8. Support triggering a user-defined event.

Real-Time Alarm Management

1. The pop-up window of alarms supports editing the priority of the alarm. By default, three priorities are provided: high, medium, and low.
2. The pop-up window of alarms supports editing the type of the alarm. By default, four types are provided: true, false, to be acknowledged, and to be verified.
3. The Web Client supports setting whether an event can be triggered as an alarm. When setting this, users can select the recipients of the alarm and set alarm priority.
4. The Web Client supports setting the Restrict Alarm Handling Time for the alarm. The linked alarm output or user-defined events will be triggered after the configured duration.
5. The Web Client supports enabling the following functions for an alarm: pop-up window, displaying alarm-related video on smart wall, relating an alarm to a map, and triggering audible warning.
6. When setting trigger recording as the linkage action. Support selecting displaying recorded video or live view when alarm occurred.
7. Support acknowledging alarms by the platform automatically. When the delayed duration ends, the alarm will be acknowledged automatically.
8. Support displaying multiple unhandled alarms and the number of total unhandled alarms in one pop-up alarm window on the Control Client.

4.5.4 Combined Alarm

Rule Configuration

1. Support linking a combined alarm with an alarm triggered area, which is used for counting the alarms triggered in the area.
2. Support enabling the function of ignoring recurring alarms, and users can configure the duration for ignoring.
3. Support setting any triggering source types.
4. Support four alarm triggering logic, and support configuring the triggering interval between two alarms.

5. Support enabling or disabling alarms. When disabling an alarm, users can set the start time and duration of disabling. Once an alarm is disabled, users will not receive the alarm notifications.
6. Combined alarm supports all linkage actions except Link Printer.

Combined Alarm Display

1. Support adding a combined alarm to the map.
2. Support copying the settings of a combined alarm to other combined alarms.
3. Support testing a combined alarm.

4.5.5 Configuration and Management

1. When adding an event, support selecting multiple triggering events and sources.
2. Support deleting all invalid events quickly by clicking the Delete All Invalid Items button.
3. Support setting multiple events as alarms in a batch.
4. Support enabling and disabling multiple alarms in a batch.
5. Support testing alarms.
6. Support filtering events that are set as alarms.
7. Support filtering events and alarms by source type, event & alarm name, area, source, and triggering event.
8. Support highlighting abnormal events and alarms with a red exclamation mark.
9. Support highlighting events and alarms that are not supported by the sources.
10. Support event and alarm statistics.
11. Support classifying events and alarms by modules.

4.5.6 Real-Time Alarm Display

Alarm Report

1. Support counting the numbers of all alarms in the platform, including shielded alarms, disabled alarms, alarm inputs, zones.
2. Support displaying shielded alarms only.
3. Support displaying alarm sources, alarm types, and the triggering times of each alarm. Support expanding an alarm type to display all the alarm list.

Map

Support displaying an alarm on the map, viewing alarm details on the map, and acknowledging an alarm on the map.

4.5.7 Alarm Operation

1. Support displaying alarm details, including related map, description, operation logs. For different event types, the details vary.
2. The Overview page supports selecting an event or alarm and switch to the Event & Alarm Search page to search for its history events/alarms.
3. The alarm-related video window supports two-way audio between the people on-site and the user of the platform.
4. Support downloading information of an alarm, including alarm details and map.
5. Support shielding an alarm.
6. Support acknowledging an alarm or batch acknowledging. Once acknowledged, the alarms will be removed from the Overview page.
7. Support editing acknowledged alarm as unacknowledged.
8. Support marking alarms for highlighting.
9. Support disabling alarms. After disabling, the user will not receive the alarm when it is triggered.
10. Support enabling alarms after disabling.
11. Support bypassing or restoring bypassed alarm inputs.
12. Support arming and disarming partitions (areas), alarm inputs.
13. Support manually triggering user-defined event
14. The alarm pop-up window supports sending emails containing alarm information after selecting the recipients & email template and entering the description.
15. Support forwarding an alarm to specified users.

4.5.8 Search and Exporting

Event & Alarm Search

1. Support searching for events by time, area, event type, and event name.
2. Support searching for alarms by triggering time, marking status, priority, alarm type, acknowledging status, area, event type, and alarm name.
3. Support searching for both events and alarms by the same conditions.
4. After searching for the events and alarms, support viewing event & alarm details and operation logs.

Alarm Record

The operation logs of an alarm contain all the operations on the alarm, including records of forwarding, shielding, receiving, marking, disabling, and the user information related to the operations.

Export Events & Alarms

1. After searching for the events and alarms, Support exporting the searching results to the PC as a CSV/PDF file. PDF Support up to 5,000 pieces of information. Support exporting related pictures of no more than 500.
2. Support exporting the matched or mismatched alarms with detailed information, such as person information, card number, license plate number, and so on.

4.5.9 Statistics and Analysis

Alarm Overview

Support counting alarms of the current day, including alarms that are acknowledged and unacknowledged.

Alarm Trend

1. Support counting alarms triggered in the last 7 and 30 days.
2. Support generating trend map of specified event types.
3. Support generating and exporting trend map of alarms of 7 days in PDF, PNG, and JPG format.

Top 5 Alarm Analysis

1. Support displaying the top 5 events and alarms triggered today or during the last 7 and 30 days.
2. Support displaying the top 5 areas of all the triggered events and alarms of today, the last 7 and 30 days.
3. Support counting specified event types and generating the top 5 event types.
4. Support exporting the events in PDF, PNG, or JPG format.

Scheduled Report of Events & Alarms

1. Support sending event and alarm reports via emails regularly.
2. Support sending daily reports containing information about alarms and events triggered on the day before the current day.
3. Support sending weekly reports containing information about alarms and events triggered during the last 7 or 14 days.
4. Support setting the date and time of sending event/alarm reports.
5. Support generating alarm reports in Excel or PDF format.
6. Support generating alarm reports in multiple languages.
7. Support backing up event and alarm reports to the SFTP server regularly.
8. Support backing up event and alarm reports to the SYS regularly.

4.5.10 Permission Management

Event and Alarm Receiving Permission

Support selecting recipients of an alarm. The users with the permission for receiving alarms can receive the alarm information.

Event and Alarm Operation Permission

1. Support assigning user permission of arming or disarming alarm input.
2. Support assigning user permission of bypassing or recovering bypassed alarm input of security control device.
3. Support assigning user permission of acknowledging alarm.
4. Support assigning user permission of batch acknowledging alarms.
5. Support assigning user permission of acknowledging alarm without entering remarks.
6. Support assigning user permission of forwarding alarms.
7. Support assigning user permission of marking acknowledge alarm as unacknowledged.

Event and Alarm Search Permission

Support assigning user permission of event & alarm search.

4.6 Access Control

- ***Application Wizard***
- ***Access Control Device Management***
- ***Resource Management in Multiple Areas***
- ***Card Printing***
- ***Access Level Management***
- ***Advanced Function Management***
- ***Real-Time Monitoring on Map***
- ***Effective Emergency Response***
- ***Access Records***
- ***Visualized Report***
- ***Privacy Protection Settings***

4.6.1 Application Wizard

Configuration wizard of access control which is on the right and will be displayed when you hover the cursor on it.

4.6.2 Access Control Device Management

Device Access via Multiple Protocols

1. Support accessing devices via Device Network SDK by IP address, IP segment, or batch importing.
2. Support accessing devices via ISUP by device ID, ID segment, or batch importing.
3. Device information list: device name, address, serial No., version No., number of doors, number of readers, network status, and password strength.
4. The platform shall support accessing devices via ISAPI by IP address, IP segment, or batch importing.

Device Configuration

1. Platform configuration (Device Network SDK): IP address, port, alias, user name, password, time zone, and channel resource.
2. Platform configuration (ISUP): device ID, key, alias, storage configuration, time zone, and channel resource.
3. Support going to the web page of device configuration.
4. Support adding access control devices via domain name.
5. For devices that do not support configuration via web browser, it supports going to the remote configuration page.

Remote Device Control

1. Support editing passwords one by one or in a batch.
2. Time zone settings: Support configuring time zone one by one or in a batch; Support getting time zone settings from devices and applying time zone settings to devices.
3. Support restoring to default settings for devices one by one or in a batch.

Real-Time Device Status Monitoring

1. Support viewing online status.
2. Support viewing network status.
3. Support viewing main and sub lane controller status (only for turnstiles).
4. Support viewing turnstile component status (only for turnstiles).
5. Support viewing arming status.
6. Support viewing device tampering status.
7. Support viewing power supply status.
8. Support viewing first added time and inspection time.

Opening Door by Mobile Client

1. The platform shall support opening door via bluetooth.
2. The platform shall support opening door via NFC.

4.6.3 Resource Management in Multiple Areas

Door Management

1. Basic information: door name, device, door magnetic sensor, exit button type, door open duration, extended open duration, door open timeout alarm, maximum door open duration, duress code, super password, and duress code. The actual parameters depend on the device capability.
2. The platform shall support linking to cameras: no more than two cameras can be linked to each door.
3. The platform shall support linking face recognition terminals to a barrier gate to control the access of persons.
4. The platform shall support linking face recognition terminals to an access controller to control the access of persons.
5. Picture storage: local storage, CVR, cloud storage, pStor, and Network Video Recorder (NVR). It is valid when camera(s) are linked and the picture storage is enabled.
6. Reader: enable or not, reader name, reader type, minimum card swiping interval, resetting entry settings, failed card attempts alarm, tampering detection, OK LED polarity, ERR LED polarity, buzzer polarity, and fingerprint security level. The actual parameters depend on the device capability.
7. Resource information list: door name, device IP address, device, network status, reader information, status of remaining open/closed, and area.
8. Support getting door names from the devices.
9. Support applying door names to devices.
10. Support setting the capture priority for linked cameras.

Floor Management

1. Basic information: elevator name, device, door open duration, extended open duration, door open timeout alarm, maximum door open duration, duress code, super password, and duress code. The actual parameters depend on the device capability.
2. Floor: No. and name. Support resetting floors in a batch.
3. Support linking to cameras: no more than two cameras can be linked to each door.
4. Picture storage: local storage, CVR, cloud storage, pStor, and Network Video Recorder (NVR). It is valid when camera(s) are linked and the picture storage is enabled.
5. Reader: enable or not, reader name, reader type, minimum card swiping interval, resetting entry settings, failed card attempts alarm, tampering detection, OK LED polarity, ERR LED polarity, buzzer polarity, and fingerprint security level. The actual parameters depend on the device capability.
6. Resource information list: elevator name, device IP address, device, network status, and area.
7. Support getting floor names from devices.
8. Support applying floor names to devices.

Alarm Input Management

1. Basic information: alarm input name and device.
2. Resource information list: alarm input name, device IP address, device, partition No., area, and network status.

Alarm Output Management

1. Basic information: alarm output name.
2. Resource information list: alarm output name, device IP address, device, and area.

Resource Management by Area

1. Support adding multiple areas and each area contains multiple different resources.
2. Support multiple levels of areas.

4.6.4 Card Printing

Card Template Customization

1. Support customizing card templates: set the shape to vertical or horizontal, set the front and/or back style, insert pictures, insert text, and insert person information fields.
2. Support previewing the card template.
3. Support text alignment and content alignment.
4. Support adjusting the layer of content and text on the card.
5. Support customizing the size of the text on the card and horizontal alignment.
6. Support customizing the size of pictures added to the card.
7. Support configuring font color and bold font.
8. Support auto line break of inserted text, name, first name, last name, email, remark, and custom information.

Compatible with Mainstream Card Printers

1. The platform shall support mainstream card printers, such as HID Fargo and Magicard; the supported card specification is CR80; Support single-sided or dual-sided printing.
2. The platform shall support Zebra ZC350 for printing cards.
3. The platform shall support accessing card printers via USB.

Quick Card Printing

Support printing cards one by one or in a batch.

4.6.5 Access Level Management

Dashboard

1. Support wizard, device health status, person credential status, access trend, abnormal records top 5, entry & exit counting, and real-time entry & exit events.
2. Support quickly configuring access control on the Access Control Overview page.

Holiday Management

Support configuring up to 32 regular or irregular holidays.

Access Schedule Template Management

1. Support three default access schedule templates: all-day template, weekday template, and weekend template. The default templates cannot be edited or deleted.
2. Support creating new access schedule templates or copying from an existing template. The templates include week schedules and holiday schedules.
3. Support manually entering the time accurate to hour and minute for drawing time periods of schedule templates.

Access Level Management

Support configuring access levels for all or specific doors and/or floors.

Multi-Dimensional Access Level Assignment

1. Support assigning access levels by access level.
2. Support assigning access levels by person.
3. Support assigning access levels by organization.
4. Support assigning specific access levels by access group.
5. Support searching for persons by name and employee ID.
6. Support automatically applying access level settings to devices after assigning access levels to persons, departments, and access groups.

Manual Access Level Applying

1. Support specifying persons and devices to apply access levels immediately or later.
2. Support applying access levels initially (first clear and then apply).
3. Support displaying the applying progress and applying failure details.
4. Support status statistics of applying access levels.

Automatic Access Level Applying

1. Support automatically applying access levels at fixed time every day. The time can be configured and is 1:00 a.m. by default.
2. Support automatically applying access levels every certain hours every day. The interval can be configured and is 1 hour by default.

Access Level Overview and Quick Exception Processing

1. Support credential status statistics: number of persons, faces, cards, fingerprints, and persons with no credentials; Support viewing and exporting person statistics of different status.
2. Support device status statistics: device exception, to be applied, and exceptional when applying, and Support viewing and exporting device statistics of different status.
3. Support detecting access level applying status by specified person, including applying failed, applying succeeded, and to be applied; Support applying access levels again.
4. Support detecting access level applying by specified access point, including applying failed and applying succeeded; Support applying access levels again.

4.6.6 Advanced Function Management

First Person In

1. Support remaining open with first card and first card authorization.
2. Support remaining open with first person and first person authorization.

Multi-Factor Authentication

1. Support adding multi-factor authentication groups.
2. Support configuring multi-factor authentication rule based on multi-factor authentication group, including access schedule template, authentication mode, card-swiping order of the authentication group, and card-swiping interval.
3. Support specifying users to open the door remotely.

Multi-Door Interlocking

Support multi-door interlocking of one device.

Anti-Passback

1. Support area anti-passback of one device or across multiple devices.
2. Support route anti-passback of one device or across multiple devices.
3. Support enabling or disabling regular forgiving anti-passback.
4. Support configuring anti-passback for barrier gates.

Remaining Open or Closed

Support configuring free access and access forbidden schedules in a batch.

Authentication Mode

1. Support configuring reader authentication modes.
2. Support configuring person private authentication modes.

Open Door by Mobile Client

1. Support opening door via Bluetooth.
2. Support opening door via NFC.

Applying Advertisement

Support applying advertisements to access control devices.

Audio Broadcast

1. Support batch configuring audio broadcasts, including daily audio broadcasts and particular audio broadcasts.
2. Support viewing record details of devices and captured pictures (if any) in Device Recorded Data Retrieval module.

4.6.7 Real-Time Monitoring on Map

Real-Time Door Status Monitoring

1. Support displaying the status of the door magnetic/door lock.
2. Support starting live view of linked cameras.

Real-Time Event Monitoring

1. Support uploading events in real time.
2. Support filtering by event type.
3. Support filtering by access point.
4. Support customizing columns to be displayed.
5. Support subscribing to specific event types.
6. Support a lasting display of the information about the current recognized person, including profile photo, face picture, and person introduction. Support transforming the window to a thumbnail window.

Real-Time Monitoring on Map

1. Support displaying resource status in real time (door, floor, alarm input, and alarm output).
2. Support real-time remote control (door, floor, alarm input, and alarm output).
3. Support displaying alarms of resources (door, floor, alarm input, and alarm output) in real time.
4. Support real-time live view of the camera linked with the door.
5. Support displaying regional entry & exit counting in real-time.
6. Support displaying multi-door interlocking in real time.
7. Support displaying anti-passback in real time.

4.6.8 Effective Emergency Response

Batch Emergent Door Control

Support remotely controlling doors one by one or in a batch in real time.

Roll Call

1. Support alarm input linkage to automatically remain all doors or doors of a specific area open.
2. Support automatically triggering the printer to print the list of stayed people of all areas or a specified area.

4.6.9 Access Records

Identity Access Records Retrieval

1. Support searching for identity access records and export to Excel or CSV files.
2. Support automatically getting lost identity access records from the device by schedule.
3. Support manually getting all identity access records during the specified time period from the device.
4. Support manually importing identity access records exported from the device to the platform.
5. The Identity Access Search page supports customizing column items to be displayed.

Device Recorded Data Retrieval

Support searching for device recorded data which can be exported to Excel or CSV files.

Entry & Exit Counting Retrieval

Support searching for entry & exit counting results which can be exported to Excel or CSV files.

4.6.10 Visualized Report

1. Support today's access records which can be exported to PDF, JPG, or PNG files.
2. Support today's access trend which can be exported to PDF, JPG, or PNG files.
3. Support today's abnormal records top 5 which can be exported to PDF, JPG, or PNG files.
4. Support regional stayed people counting.

4.6.11 Privacy Protection Settings

1. Event storage configuration: overwrite, delete old events regularly, and delete old events by specified time.
2. Authentication configuration: whether to display the photo, name, employee No., and temperature in the authentication result.
3. Picture uploading and storage configuration: upload recognized or captured pictures, save recognized or captured pictures, save profile photos, upload event and alarm pictures, save event and alarm pictures, upload thermal pictures, and save thermal pictures.

4. Clear pictures stored on the device quickly: clear face pictures and clear recognized or captured pictures.
5. Delete face pictures of one person or all persons.

4.7 Temperature Screening

- ***Service Configuration***
- ***Person Registration***
- ***Temperature Monitoring***
- ***Statistics and Reports***

4.7.1 Service Configuration

Device Management

Support adding cameras with temperature screening functions.

Temperature Screening Configuration

1. Support creating temperature screening point groups and adding temperature screening points to the groups.
2. Support configuring the threshold for temperature screening.
3. Support configuring the threshold for temperature alarms.

4.7.2 Person Registration

Support registering person information if the screened person is not registered, including the person's name, ID, phone number, whether from high-risk areas, description, etc.

4.7.3 Temperature Monitoring

Temperature Monitoring

1. Support registering person information if the screened person is not registered, including the person's name, ID, phone number, whether from high-risk areas, description, etc.
2. Support viewing the real-time captured pictures of the specified temperature screening point group.
3. Support viewing previously captured pictures in thumbnail mode with the person's face picture, temperature, temperature mark color, mask wearing status, etc.
4. Support viewing alarm information of the specified temperature screening point group, including the person's captured picture, temperature, temperature mark color, mask wearing status, etc.
5. Support viewing the real-time captured pictures of the specified temperature screening point.

6. Support viewing previously captured pictures in thumbnail mode with the person's face picture, temperature, temperature mark color, mask wearing status, person group, etc.
7. Support viewing real-time temperature screening events, including the person's name, temperature, temperature mark color, mask wearing status, etc.

History Data

1. Support searching for historical temperature screening data of the specified temperature screening point group. The result includes the person's captured picture, temperature, temperature mark color, mask wearing status, person group, etc.
2. Support searching for registered person information. The result includes person name, ID, phone number, whether from high-risk areas, person in charge of registering, register time, screening time, etc.
3. Support searching for temperature screening events of the specified temperature screening point. The result includes event time, channel, mask wearing status, whether the temperature is abnormal, etc.

4.7.4 Statistics and Reports

1. Support the following report types: daily report, weekly report, monthly report, annual report, and report with a custom time interval.
2. Support analyzing results by temperature screening point. Support displaying the overall screening statistics and the statistics of people with abnormal temperature or those not wearing any face masks.
3. Support analyzing results by department. Support displaying the overall screening statistics and the statistics of people with abnormal temperature or those not wearing any face masks.
4. Support exporting the report to the local PC.

4.8 Video Intercom

- ***Independent Module***
- ***Video Intercom Device Management***
- ***Live Two-Way Audio***
- ***Notice Applying***
- ***Call Log***
- ***Centralized Management of Video Intercom Module***

4.8.1 Independent Module

1. Supports independent video intercom module and independent entry to the module.
2. Supports the dashboard which includes device maintenance, daily statistics of applied notices, and statistics of calls of the current day.
3. Supports batch configuring parameters for video intercom devices.

4.8.2 Video Intercom Device Management

Accessing Devices via Multiple Protocols

1. Support accessing devices via Device Network SDK or IP address.
2. Support displaying device information, including device name, location, serial number, version, the number of doors, the number of cameras, the number of alarm inputs, location No., network status, and password strength.

Device Configuration

1. Platform Parameters Configuration (Device Network SDK): IP address, port, alias, username, password, time zone, and channel resource.
2. Device Location Number Configuration
   - Indoor Station: community No., building No., unit No., and room No.
   - Door Station: community No., building No., and unit No.
   - Outer Door Station/Main Station: community No.
3. Support linking resident information (only for indoor station).
4. Support jumping to the configuration page of the device.
5. Support accessing configuration library (only for the devices not supporting the configuration via web browser).
6. Support linking indoor stations with cameras (up to 16 cameras per indoor station).
7. Support linking the doorbell with the indoor station.
8. Support applying software packages to indoor stations in a batch.

Device Settings Applying

Support applying the location No. and the corresponding network parameters of all video intercom devices to all devices.

Remote Control of Device

1. Support changing the password (single or in a batch).
2. Time zone settings: getting the time zone settings of a device and applying these settings to other devices (single or in a batch).
3. Support restoring the default parameter (single or in a batch).

Real-Time Detection of Device Status

1. Support displaying online status of device.
2. Support viewing the network status of the device.
3. Persistent connection status of the two-way audio called by device.
4. Support viewing arming status.
5. Support viewing battery status of the device.
6. Supporting viewing the time when the device is added for the first time and the time of its first inspection.

4.8.3 Live Two-Way Audio

Call Schedule of Door Station

Support configuring schedules for calling the indoor station or the management center (platform or main station).

Two-Way Audio Between Platform and Door Station

1. Support two-way audio.
2. Support live view during two-way audio.
3. Support recording and saving video and audio to the local PC.
4. Support remote door control during two-way audio.
5. Support remotely unlocking the door before answering the call.

Two-Way Audio Between Platform and Indoor Station

1. Support two-way audio.
2. Support live view during two-way audio.
3. Support starting two-way audio in the event pop-up window.

Specify Persons to Answer Calls

1. Support specific persons answering the call from the device.
2. Support specific persons answering calls at specified time periods.

Two-Way Audio Between Device and Web Client

Supports calling indoor stations and answering calls from devices via the Web Client.

Sequence of Answering Calls

When video intercom devices call the Center, the earliest and unanswered call will be listed as the first one to be answered.

Automatically Saving Volume of Two-Way Audio

In the Video Intercom module, the two-way audio volume of microphone and loudspeaker will be saved and used in the following two-way audio.

4.8.4 Notice Applying

Batch Applying Notices to Indoor Stations

1. Supports batch applying notices to indoor stations. Notices can include pictures and texts which can be displayed in multiple languages, for example, Russian.
2. Supports searching history notices by setting conditions including the theme, content, resident, type, and time.
3. Supports exporting history notices.

4.8.5 Call Log

Calls Between Platform and Indoor Stations / Door Stations

1. Supports saving logs of calls between the platform and indoor stations / door stations.
2. Supports viewing call statistics (the number and logs of calls answered or not answered) quickly.
3. Supports searching logs of calls by setting conditions including device, call duration (start time and end time), and call status.
4. Supports viewing details of any call log and calling the indoor station again.

4.8.6 Centralized Management of Video Intercom Module

1. The platform shall support independent video intercom module and independent entry to the module.
2. The platform shall support the dashboard which includes device maintenance, daily statistics of applied notices, and statistics of calls of the current day.
3. The platform shall support batch configuring parameters for video intercom devices.
4. The platform shall support upgrading firmware of door stations in a batch.

4.9 Time and Attendance

- ***Attendance Wizard***
- ***Attendance Rules***
- ***Leave Management***
- ***Attendance Reports***
- ***Attendance System Operation***
- ***Employee Self-Service***
- ***Check-In&Check-Out via Mobile Client***
- ***Third-Party Integration***

4.9.1 Attendance Wizard

Provide guidance to help the user set up an attendance system.

4.9.2 Attendance Rules

Attendance Group

1. The platform shall support adding, deleting, and editing attendance groups.
2. The platform shall support adding persons to attendance groups.

Attendance Rule

1. The platform shall support configuring global and department attendance rules.
2. The platform shall support configuring group attendance rules.
3. The platform shall support setting the day change time.
4. The platform shall support adding pay codes.
5. The platform shall support editing fixed codes.

Break Timetable

1. Support adding break timetables.
2. Support setting a fixed break duration or calculating the break duration by actual check-in/out interval.
3. Support marking early return as overtime (level 1/2/3).
4. Support marking late return as normal, late, early leave, or absence duration.
5. Support calculating the break duration by the interval of the first and last check-in/out or the interval of each check-in/out.
6. Support enabling the attendance status on attendance check devices.
7. Support counting early or late return time by time point.
8. Support counting early or late return time by duration.

Timetable

1. Support adding work timetables.
2. Support adding normal timetables and set the flexible mode to Allow Late Arrival/Early Leave or Flexible Period.
3. Support adding flexible timetables.
4. The timetable supports setting a valid check-in period and valid check-out period exceeding 24 hours.
5. Support adding multiple break timetables to one timetable.
6. Support timetable overview.
7. Support setting a dedicated absence rule for a timetable, whose priority is higher than the global absence rule. Support marking late check-in and early check-out as absent. Support marking no check-in or check-out as absent or late.
8. Support calculating the work hours by the interval of the first and last check-in/out or the interval of each check-in/out.
9. Support enabling the attendance status on attendance check devices.
10. Support configuring the latest check-in time.
11. The platform shall support viewing the changes of the timeline when configuring the timetable.
12. The platform shall support configuring timetables following the tabs, including Basic Settings, Break Period, Overtime, and Attendance Calculation.

Shift

1. Support adding shifts.
2. Support setting the shift's repeating pattern: By Week (1 to 52 weeks), By Day (1 to 31 days), and By Month (1 to 12 months).
3. Support set the repeat cycle to week or day.
4. The platform shall simplify the shift management by deleting calculation mode and overtime rule.
5. Support calculating the work hours by the interval of the first and last check-in/out or the interval of each check-in/out.
6. Support enabling the attendance status on attendance check devices.
7. Support setting a dedicated overtime rule for a shift, whose priority is higher than the global overtime rule. Support setting the work hour rate of each overtime level, overtime calculation rule on workdays, overtime rule on holidays, and whether to calculate the overtime that is not in valid attendance check period.
8. Support setting holidays for a shift. Attendance check will be disabled on holidays.
9. Support displaying multiple shifts of a person in the Schedule Overview module.
10. Support configuring different effective periods for different schedules when assigning schedules by person or department.

Schedule

1. Support schedule overview.
2. The platform shall support viewing schedule overview by month and week.
3. Support assigning a schedule to departments.
4. Support assigning a schedule to persons.
5. Support assigning a temporary schedule to persons in different departments.
6. The platform shall support assigning a schedule to attendance groups.
7. Support setting the effective period, whether to require check-in/out, and whether overtime is effective when assigning a schedule.
8. Support adding multiple shifts to a schedule.
9. Support linking a schedule to attendance check points.
10. The platform shall support quickly configuring temporary schedules on the calendar.
11. The platform shall support selecting timetables for the temporary schedules.
12. The platform shall support quickly configuring schedules and using different colors to mark different schedules on the calendar.

Global Overtime Rule

1. Support setting the work hour rate for 3 overtime levels.
2. Support setting the overtime rule on workdays. Support setting the overtime calculation mode to ""By Total Work Hour"" or ""By Time Points""

- By Total Work Hour - Count the extra work hours as overtime. Support setting the overtime duration calculation mode to ""Fixed"" or ""Actual"".
- By Time Points - Count early check-in or late check-out as overtime. Support setting the duration calculation mode."

3. Support setting the overtime rule on weekends by defining a daily threshold for valid overtime calculation.
4. Support setting the overtime rule on holidays. Support setting a daily threshold for valid overtime calculation, the maximum limit for overtime, and the overtime level for each holiday.
5. Support setting whether to calculate the overtime that is not in valid attendance check period.
6. Support two digits after the decimal point when setting the work hour rate.

Global Absence Rule

1. Support marking the late check-in as absent and setting the threshold.
2. Support marking the early check-out as absent and setting the threshold.
3. Support marking no check-in as absent or late.
4. Support marking no check-out as absent or late.

Attendance Result Accuracy

1. Support setting the minimum unit, rounding, and display format of the duration of each attendance status.
2. Support calculating attendance by second.

Attendance Check Point

1. The platform shall support checking attendance via all devices on the platform by default.
2. Support setting any access point as the attendance check point. Support setting the attendance check point type to Check-In & Out, Check-In Only, or Check-Out Only.
3. Support setting any card reader of a door as the attendance check point. Support setting the attendance check point type to Check-In & Out, Check-In Only, or Check-Out Only.

Customization

1. Support setting any days of the week as the weekends.
2. Support setting the attendance authentication mode to card, fingerprint, and/or face.
3. Support customizing the leave types.
4. Support setting the attendance mode on attendance check devices to Manual, Automatic, and Manual And Auto.
5. Support customizing the attendance status name displayed on attendance check devices, including check-in/out name, break start/end name, and overtime start/end name.
6. Support setting the time periods of each attendance status on the attendance check devices when the attendance mode is Automatic and Manual & Auto.

4.9.3 Leave Management

1. The platform shall support configuring different leave types.
2. The platform shall support configuring leave rules.
3. The platform shall support assigning different leave rules to persons.
4. The platform shall support automatically deduct remaining days of leave according to employees' leave applications.

4.9.4 Attendance Reports

Predefined Attendance Reports

1. Attendance record
   - Transaction
   - Time Card
   - Check-In&Out Record
   - First&Last Access Report
   - Leave Record
   - Overtime Record
   - Check In&Out Correction Report
2. Daily report
   - Total Time Card
   - Worked Hrs
   - Overtime Report
   - Leave Report
   - Late Report
   - Early Leave Report
   - Absent Report
   - Exception Report
   - Multiple Break Time
3. Weekly report
   - Weekly Details
   - Weekly Worked Hrs
   - Weekly Overtime
4. Monthly report
   - Monthly Details
   - Monthly Status
   - Monthly Worked Hrs
   - Monthly Overtime
   - Monthly Break Time
   - Monthly Check In&Out
   - Monthly Absent

  - Monthly Late
  - Monthly Early Leave
5. Summary report
   - Person Attendance Summary
   - Person Overtime Summary
   - Person Leave Summary
   - Department Attendance Summary
   - Group Attendance Summary
   - Department Overtime Summary
   - Group Overtime Summary
   - Person Attendance Overview
   - Person Attendance Details
   - Person Attendance Statistics
6. Support viewing weekly report in three modes: weekly statistics, weekly details, and weekly overview.
7. Support viewing monthly report in three modes: weekly statistics, weekly details, and weekly overview.
8. Department overview
9. Department overtime overview
10. Support previewing all types of reports.

Report Template Customization

1. Support customizing new report templates from the predefined reports.
2. Support customizing the fields, order, and sorting order of the customized reports.
3. Support selecting all the available fields when customizing reports.
4. Support merging the data of the same person/department/date. Support setting the sorting rule for records such as sorting in ascending order of person ID.
5. Support previewing the customized reports.

Report Exporting

1. Support generating attendance reports of specific persons (including resigned and employed) or departments.
2. The platform shall support sending attendance report of specified attendance groups according to a schedule.
3. Support exporting in PDF, Excel, and CSV format.
4. If you select PDF as the format of the report, support printing the report according to the selected paper size and the printing direction. If you select Self-Adapt to Paper Based on Content, support automatically specifying a paper size according to the selected report type, and the specified paper size will show in the brackets behind Self-Adapt to Paper Based on Content.

Report Display Customization

1. Support adding company logo to reports.
2. Support setting the format of date and time.
3. Support setting the abbreviation and color of each attendance status.

4.9.5 Attendance System Operation

Dashboard

1. Support checking the abnormal attendance statistics (absent, late, early leave, late and early leave) of the current day, previous day, current week, last week, current month, and last month, last 3 months, last 6 months, current year, and customized time period. Support exporting the statistic chart as a PDF, PNG, or JPG file.
2. Support checking the attendance status statistics (normal and absent) of the current day, previous day, current week, last week, current month, and last month, last 3 months, last 6 months, current year, and customized time period. Support exporting the statistic chart as a PDF, PNG, or JPG file.
3. Support checking the overall work hours/overtime statistics of the current day, previous day, current week, last week, current month, and last month, last 3 months, last 6 months, current year, and customized time period. Support exporting the statistic chart as a PDF, PNG, or JPG file.

Automatic Attendance Calculation

1. Support calculating the attendance results of the previous day at 4:00 AM. Support changing the auto calculation time.
2. Support setting the time of recalculating historical attendance data.

Manual Attendance Calculation

Support calculating the attendance results of any specific persons during a specific time period manually.

Transaction Management

1. Supports searching and listing all transactions.
2. Support exporting transactions in PDF, Excel, or CSV format.
3. Support customizing the data items, item order, and record sorting order when exporting records.

Attendance Calculation Results

1. Support listing all attendance calculation results.
2. Support sorting the attendance calculation results according to person ID or date.
3. Support hiding or showing specific data items of attendance records.

4. Support exporting attendance records in PDF, Excel, or CSV format.
5. Support customizing the data items, item order, and record sorting order when exporting records.
6. Support searching attendance records by time, including today, current week, current month, this year, yesterday, last 7 days, last week, previous month, last 3 months, last 6 months, last year, or custom.

Attendance Record Integrity

1. Support getting the lost entry & exit records from devices automatically.
2. Support importing all entry & exit records in a specific time range from devices manually.
3. Support importing the device-exported entry & exit records (files) from the local PC manually.

Exception Attendance Handling

- Support submitting applications for employees to handle exception attendance (leave, overtime, and check-in/check-out correction.
- Support reviewing exception attendance applications according to configured application flows.

Auto Sending Attendance Reports via Email

1. Support setting report schedules to send predefined reports or customized reports via email.
2. Support customizing email templates.
3. Support selecting the report language.
4. Support setting the statistics cycle: By Day (select one or multiple days from Monday to Sunday), By Week (select one day from Monday to Sunday), or By Month (select any day from the first day of the month to the last day of the month).
5. Support sending the attendance report to the recipients automatically.

4.9.6 Employee Self-Service

Employee Self-Service

- The platform shall support the administrator in setting the employee self-service password, which is the employee ID by default.
- The platform shall support employees in logging in to the platform via Web Client and the Mobile Client.
- The platform shall support self-service dashboard for employees.
- The platform shall support searching for the personal attendance results, status, and reports.
- The platform shall support submitting applications for the exception attendance (leave, overtime, check-in/check-out correction).
- The platform shall support searching for an application and viewing the approval flow status.
- The platform shall support self-undoing the submitted application.
- The platform shall support reviewing (approving or rejecting) or undoing the exception attendance application (this function is only valid for reviewers).

- The platform shall support employees in changing login password.
- The platform shall support employees submitting applications for leave.
- The platform shall support employees searching for remaining days of leave.

Approval Flow Management

- The platform shall support customizing approval roles.
- The platform shall support customizing approval flow.

4.9.7 Check-In&Check-Out via Mobile Client

1. The platform shall support HR configuring valid check-in/out scope on the GIS map. Support selecting a location and setting the Max. radius.
2. The platform shall support HR enabling and disabling Taking Photo Required.
3. The platform shall support HR enabling or disabling check-in&check-out via Mobile Client for a single person or multiple persons.
4. The platform shall support HR adding an approval flow for attendance groups.
5. The platform shall support HR viewing all to-be-reviewed applications for check-in&check-out via Mobile Client.
6. The platform shall support employees checking in&out via Mobile Client.
7. The platform shall support employees viewing all records of current day's check-in&check-out via Mobile Client.
8. The platform shall support admins approving or rejecting employees' applications for check-in&check-out via Mobile Client.
9. When an approval flow of check-in&check-out via Mobile Client ends, the platform shall support calculating attendance results automatically.

4.9.8 Third-Party Integration

Integration via Intermediate Files

1. Support exporting entry & exit records to the local PC as CSV or TXT files.
2. Support exporting entry & exit records to the SFTP service as CSV or TXT files.
3. Support customizing the fields and data format to be included in the exported file.
4. Support customizing the file name.
5. Support adding date and time information in the file name.
6. Support setting the frequency and time of file export.
7. Support setting the length and complementing method of person ID.
8. Support setting the length and complementing method of card number.
9. Support setting whether to overwrite the exported files.

Integration via Database

1. Support writing the entry & exit records into third-party database such as PostgreSQL, MS SQL Server, MySQL, and Oracle in real time.
2. Support setting the mapping between the data fields of the platform and those of the third-party database.
3. The platform shall support setting the direction as Enter or Exit.
4. Support setting the data writing format.
5. Support showing the third-party database synchronization status in real time.
6. Support entering the server IP address or domain name in third-party database synchronization.
7. Support pushing multi-character data to the third-party database.
8. Support sending person additional information if you have configured the additional information.
9. Support configuring the time interval of sending records failed to be pushed.

4.10 Emergency Mustering

Emergency Solution Configuration

1. Provide a guidance for configuring the emergency solution.
2. Support configuring multiple doors in different areas as the doors remaining unlocked when an emergency is triggered.
3. Support configuring entrance points, exit points, and mustering points.
4. Support adding emergency counting groups for roll call.

Quick Response

1. Support starting and ending an emergency automatically and manually. When the platform is in emergency, the platform will send a report containing person roll call information.
2. Support starting and ending an emergency via the Web Client, Control Client, and Mobile Client.

Real-Time Roll Call

1. Support starting a roll call by which users can account for all the persons in the emergency counting groups. Support getting data including total people number, people in danger, people out but not checked in, people out and checked in.
2. Support viewing the last entrance/exit information in the real-time statistics list of emergency counting groups.
3. Support checking in persons in emergency counting groups on the platform.
4. The real-time statistics shall support displaying the location of last check-in.
5. Support viewing details of each person when an emergency is triggered.
6. Support sending reports manually.

Permission

Support configuring the permission of configuring emergency solutions and starting a roll call.

4.11 OpenAPI

- ***Physical Resource APIs***
- ***Logical Resource APIs***
- ***Alarm Service APIs***
- ***Access Control APIs***
- ***Event Service APIs***
- ***Common API***

4.11.1 Physical Resource APIs

Access Control Device

Support getting the information of a specific access control device and information list of all access control devices. Support searching for specific access control devices by device name.

Recording Server

1. Support getting the information of a recording server and information list of all Recording Servers, including recording status, HDD information, etc.
2. Support getting the storage status of all cameras linked to a Recording Server.

System Management Server

Support getting the information of the System Management Server, including CPU usage, network status, etc.

4.11.2 Logical Resource APIs

Organization

Support getting the information of root organization and getting information list of lower-level organizations by parent organization. Support getting the information of a specific organization and information list of all organizations. Support adding, deleting, and editing the information of an organization. Support searching for specific organizations by conditions.

Area

Support getting the information of a specific area and information list of all areas. Support getting lower-level areas by parent area.

Alarm Input

Support getting the information of a specific alarm input and information list of all alarm inputs. Support searching for alarm inputs by conditions (input alarm name, device ID, area ID, etc.).

Alarm Output

1. Support getting the information of a specific alarm output and information list of all alarm outputs. Support searching for alarm outputs by conditions (input alarm name, device ID, area ID, etc.).
2. Support controlling alarm output.

Access Point

1. Support getting the information of a specific access point and information list of all access points. Support getting the information list of access points in a specific area. Support searching for access points by conditions.
2. Support getting card reader information of a specific access point.

Person

1. Support getting the information of a specific person and information list of all persons. Support searching for specific persons by conditions.
2. Support getting person's profile picture uploaded when adding the person.
3. Support adding, deleting, and editing person information, including the person's face and fingerprint information.
4. Support applying person's access level settings or information (person ID, person name, face picture, fingerprint, card No., validity, etc.) to access control devices.
5. Support getting status details of applying person information or person's access level settings to the devices. Support returning applying failures and person information waiting to be applied.
6. Support getting and editing a person's custom information.
7. Support verifying the validity of face pictures before they are applied to MinMoe devices.

Access Level

1. Support assigning and unassigning access levels to persons.
2. Support getting access level list. Support getting person list related to an access level.

Face Information

1. Support adding information of a single face to the specified face comparison group and deleting information of a single face from the specified face comparison group.
2. Support searching for information of all faces in the specified face comparison group.
3. Support downloading the specified face picture according to the URL.
4. Support searching for the information about faces by camera.

4.11.3 Video Service APIs

Live View

1. Support getting the streaming URL for live view.
2. Support specifying stream type and streaming protocol.
3. Support streaming via RTSP from CCTV cameras that are added via ISUP.
4. The streaming protocol is available for:
   a. Getting stream in Hikvision's custom type by cooperating with VideoSDK.
   b. Getting stream via WebSocket by cooperating with JsDecoder SDK.
   c. Getting stream via standard RTSP.

Playback

1. Support getting the streaming URL for playback.
2. Support specifying camera ID, start and end time, and streaming protocol.
3. The streaming protocol is available for:
   a. Getting stream in Hikvision's custom type by cooperating with VideoSDK.
   b. Getting stream via WebSocket by cooperating with JsDecoder SDK.

Two-Way Audio

Support getting the streaming URL for two-way audio. Currently, the two-way audio function can only be realized with the cooperation of VideoSDK and WebSDK.

PTZ Control

1. Support adding and deleting a preset of a camera.
2. Support searching for the preset information of a camera.
3. Support adding and deleting a patrol of a camera.
4. Support searching for the patrol information of a camera.
5. Support controlling the PTZ by camera ID.

Video SDK

1. Video SDK, without video interface, provides applications in PC client, including live view, recording, video search, playback, single-frame playback, video downloading, capture, audio control, two-way audio, etc.
2. Provides both the C++ and C# demos for Video SDK

Video WebSDK

1. Video WebSDK, with basic video interface and tool bar, provides a plug-in running on web browser to implement several video functions, such as live view, playback, creating plug-in window, window size adjustment, window division, etc.
2. Provide demos for WebSDK.

jsDecoder SDK

1. jsDecoder SDK, with basic video interface, provides a no plug-in solution to start live view (including manual recording, manual capturing, audio control, full-screen display, digital zoom, 3D positioning) and playback (pause, stop, fast/slow forward, single-frame playback, manual recording, digital zoom, 3D positioning) of the device via the web browser. jsDecoder SDK Support WSS streaming type.
2. Provide demos for jsDecoder SDK.
3. Support two-way audio.

Standard Streaming

Support standard playback via RTSP, live view and playback via HLS, and live view and playback via RTMP.

4.11.4 Intelligent Analysis APIs

People Counting Statistics

1. Support getting people counting statistics of the specified camera by minute, hour, day, and month. Support uploading alarm information by priority.
2. Support getting the real-time statistics of resource groups.
3. Support getting the list of resource groups.

Heat Map

Support getting people's dwell time and people counting statistics.

4.11.5 Alarm Service APIs

Alarm Record Search

Support searching for alarm records.

Alarm Picture

Support downloading alarm pictures.

Alarm Acknowledgement

Support acknowledging alarms.

Alarm/Event Types

Support 38 alarm/event types about card swiping, such as duress alarm, access granted by employee ID and fingerprint, and access denied by employee ID and face.

4.11.6 ANPR Service APIs

Vehicle Passing Record Search

Support searching for the vehicle passing records.

Passing Vehicle Picture

Support searching for and downloading pictures of the passing vehicles.

4.11.7 Access Control APIs

Door Control

Support controlling doors by door ID, including opening doors, closing doors, remaining doors open, and remaining doors closed.

Access Record Search

Support searching for access records by time, person name, access point ID, and event type.

Access Event

Support getting pictures of access events.

4.11.8 Event Service APIs

Event Subscription

Support subscribing to events by event type, such as intrusion event, temperature alarm event, license plate matched alarm, abnormal temperature alarm, and access event (authenticated via face and password).

Subscribed Event Search

Support searching for subscribed events by user ID.

Generic Event

Support adding, deleting, and editing a generic event. Support getting the information list of generic events. Support configuring parameters to receive alarms of the generic events.

4.11.9 Parking Lot APIs

Parking Lot Management

Support getting the parking lot information list. Support searching the vehicle passing records of a specific parking lot and the vehicle's parking records and parking duration. Support getting the occupancy of parking spaces on specific floors and parking spaces of each type.

Parking Fee

1. Support getting the parking fee and the parking duration according to the license plate number.
2. Support returning the confirmation information after the parking fee is paid. The vehicle can exit the parking lot after that.

4.11.10 Mobile Monitoring APIs

Vehicle List

Support getting the vehicle list in the Mobile Monitoring module.

Vehicle Information

Support getting the detailed vehicle information according to the vehicle No.

Two-Way Audio

Support direct two-way audio with the mobile devices.

GPS Information

Support getting the real-time GPS information, and searching for historical GPS information.

Report Alarm

Support reporting mobile device alarms to the platform, including ADAS event alarm, driving behavior event alarm, emergency alarm, etc.

4.11.11 Common API

Support getting version information of the platform.

Chapter 5 Execution

5.1 Examination

1. Inspect chosen area of installation prior to receiving devices and report any conditions that affect the installation process or any subsequent operation.
2. Please do not begin installation until all unacceptable conditions are rectified.

5.2 Preparation

Devices packaged in such way to help prevent any damage during construction.

5.3 Installation

1. Devices shall be installed in accordance with the manufacturers' instructions provided, as well as instructions based off any indicated floor design specifications.
2. Location of installation shall provide reasonable conditions for optimum device functionality. Temperature and humidity level conditions shall be taken into consideration.
3. All installations shall be performed with qualified service professionals only.
4. All devices shall be installed in accordance with the National Electric Code or applicable local codes.
5. Ensure location of installation provides a minimum possibility of accidental damage.

5.4 Field Quality Control

1. Assess the compatibility of mounting screws for all equipment to be installed.
2. Properly test all non-video systems against standard operational requirements.
3. Define, conclude, and report all issues with equipment to the manufacturers' customer service representatives.

5.5 Adjusting

1. Execute the necessary modifications to the Non-Video Management System for proper operation in accordance with the instructions provided by the manufacturer.
2. Ensure the customers unique requirements are reflected in the access control settings.

5.6 Demonstration

Upon final inspection, validate the non-video system and its device functions correctly.

See Far, Go Further