HikCentral Enterprise-Commercial

White Paper

White Paper

About this White Paper

This White Paper is applicable to HikCentral Enterprise-Commercial.

The White Paper includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the White Paper is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this white paper under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT

WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Contents

Chapter 1 Preface

1.1 About this Document

This document introduces the design, key technologies, architecture, functions, system requirements, and performance of HikCentral Enterprise-Commercial.
The target audience of this document are technical supports, pre-sales, and solution designers.

1.2 Terms and Abbreviations

Term/Abbreviation	Description
LDAP	The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
RESTful	Representational state transfer (REST) is a software architectural style that defines a set of constraints to be used for creating Web services.
SDK	Software Development Kit
ONVIF	ONVIF (Open Network Video Interface Forum) is a global and open industry forum with the goal of facilitating the development and use of a global open standard for the interface of physical IP-based security products. ONVIF creates a standard for how IP products within video surveillance and other physical security areas can communicate with each other.
ISUP 5.0	SDK based on Intelligent Security Uplink Protocol. It provides APIs, library files, and commands for the third-party platform to access Hikvision devices. The Hikvision devices, such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc., support this protocol. With this protocol, the third-party platform can realize functions such as live view, playback, two-way audio, PTZ control, etc., of the Hikvision devices.
RFID Card	Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects.
Mifare Card	MIFARE (derived from the term MIkron FARE Collection System) is NXP's well-known brand of passive RFID chip used in RFID cards and tags with a typical read/write distance of 10 cm (4 inches).
CPU Card	A CPU card is a printed circuit board (PCB) that contains the

	central processing unit (CPU) of a computer.
View	A view is a window division with resource channels (e.g., cameras and access points) linked to each window.
Multiple Authentication	In access control, multi-factor authentication is an authentication method in which the door will unlock only after multiple persons present authenticating multiple credentials in turn.
Anti-Passback	The anti-passback feature is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback function establishes a specific sequence in which cards must be used in order to grant access.
Multi-Door Interlocking	Multi-door interlocking is used to control the entry of persons to a secure area in which only one door can be opened simultaneously.

Chapter 2 Product Overview

2.1 Introduction

HikCentral Enterprise-Commercial is a centralized and intelligent platform that realizes integration and linkage of security information by accessing video surveillance devices, one-card system devices, parking lot devices, and alarm system devices, etc. to give you diversified intelligent applications with e-map. Based on an “Integrated Software Framework”, HikCentral Enterprise-Commercial will keep satisfying users’ quickly updating needs by advanced componential technology. It is applicable for every industry for its integration and centralized management of different resources.

2.2 Requirements

- **Integrated Components**
  Users have been bothered by Information Island for a long time. A platform getting different components together for an integrated and centralized management and better coordination is what users really need.
- **Friendly Operation**
  Users tend to prefer a friendly system with easy operations and management, because they want to lower the cost of operation and maintenance and improve the running efficiency.
- **Component Scalability**
  Users are eager to get rid of a platform that realizes a function by newly added components or newly integrated system. This kind of system is hard and costly to reuse and maintain. And users are hard to be satisfied by quality of this kind of system.
- **Intelligent Applications**
  Intelligent security products has been brought up for years, but old image recognition and processing algorithm limit the spread of intelligent applications for their insufficient recognition and environmental capability.
- **Open Accessing Mode**
  Third-party system access is facing with difficulties in many aspects including data interaction and resource sharing. Users need a platform with better interaction performance after accessing with a third-party system.

2.3 Our Goal

- **Integrated Components**
  HikCentral Enterprise-Commercial manages different components by the same platform and interfaces, so that the same persons, organizations, and resources can be operated in each different component.

- **Centralized Monitoring**
  HikCentral Enterprise-Commercial Operation and Management Center provides one-stop installation, operation, and maintenance for technical supporters and maintainers. Users will learn real-time status of the platform, so as to locate and solve problems quickly.
- **Scalability**
  Based on a componential design, HikCentral Enterprise-Commercial can be expanded easily by adding new components to meet new user needs. With this way, you don't have to make a complicated system by accessing multiple platforms.
- **Intelligent Applications**
  HikCentral Enterprise-Commercial takes advantages of advanced technologies including deep learning algorithm to improve functions like license plate recognition and facial recognition instead of using old surveillance technologies.
- **Open API**
  Based on a centralized framework and unified developing rule, HikCentral Enterprise-Commercial provides open APIs for third-party integration according to RESTful protocol. And the platform can access third-party devices quickly.

Chapter 3 Product Design

3.1 Design Principle

3.1.1 Modularization

HikCentral Enterprise-Commercial is composed of several modules (components), which improves the reuse of the product's functions. Other product can adopt the functions of HikCentral Enterprise-Commercial by reusing the related components. Each component is developed and maintained by professional teams and we can provide better solutions for each industry. The efficiency of issue fixing is also much higher.
What's more, developing by different components brings benefits on product extension. It costs less to extend the supported functions of the platform by integrating more components.
The main components of the HikCentral Enterprise-Commercial include: video surveillance, access control, parking lot, intrusion, time and attendance, elevator control, video intercom, patrol management, facial surveillance, map, video wall, maintenance, area management, user management, person management, vehicle management, panic alarm, visitor management, campus checkpoint, etc.

3.1.2 Scalability

When designing the platform, we take the scalability of each service into consideration, especially key services such as device access service, event, database, etc. To provide better performance for different scales of projects and different application scenarios, we adopt distributed design for HikCentral Enterprise-Commercial. You can deploy the components of the system on different servers if needed. This improves the stability and capability of the system. For example, for media gateway service, it supports large-scale and high-bandwidth stream forwarding after cascading deployment.
For smaller-sized projects, you can deploy the services on less servers or even on the same server.
Besides distributed deployment, we also adopt technologies, such as reverse proxy, distributed cache, WebSocket protocol, event-dispatching, to increase the responding speed and decrease the performance loss, thus improve the running fluency of the system.

3.1.3 Maintainable

HikCentral Enterprise-Commercial provides Web Client for management and configuration, Control Client for operation, and Web Client for operation. These three clients make system configuration and maintenance much more convenient. You can configure

parameters for search modules via System Configuration, configure parameters of services in Resource Maintenance, and perform live view and playback of cameras on the Web Client. Meanwhile, the platform also supports system log search and health status monitoring so that when an exception occurs on the servers or devices, it will notify the maintainers in time.

Besides, we also provide you Operation & Maintenance Center for quick and convenient deployment and maintenance. This eases the burden of the maintainers. The maintainers can monitor the running status of services, check logs and alarms, set service parameters, etc. If the service is offline, the Operation & Maintenance Center will start it automatically, or you can also restart or stop the service manually in the Operation & Maintenance Center manually.

3.1.4 Secure and Reliable

The following contents show what we do for the security of the system.

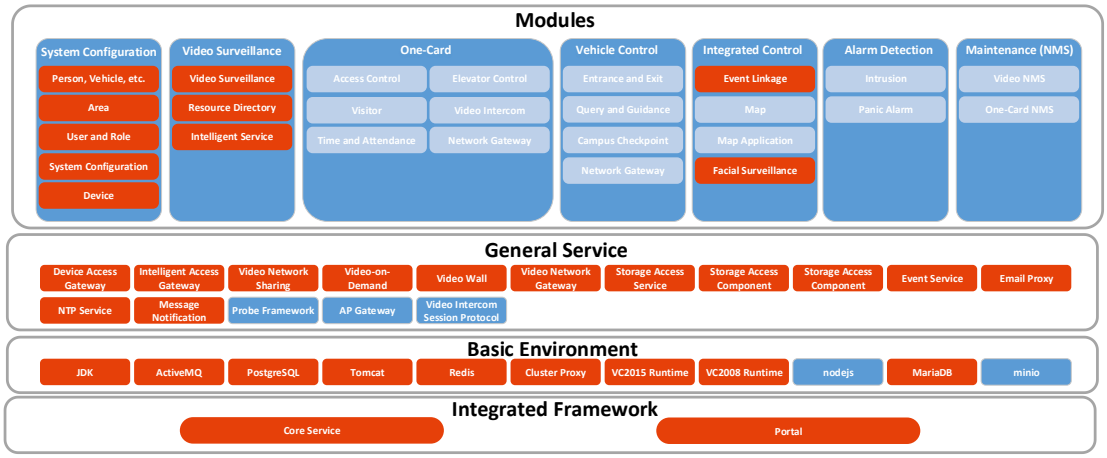
- Device: You need to enter the device's user name and password to verify the identity before accessing the device, such as encoding device, storage device, etc.
- Network: Supports accessing the Web Client in HTTPS protocol. All the sensitive information in the platform is transmitted after encryption.
- Data: For security, the login information is encrypted to ensure the security of the accounts. All the sensitive information in the platform is transmitted after encryption.
- Application: You cannot access the system by terminals which are not trusted. It provides uniform user identity verification and API authentication, so that users need to enter user name and password before login and verify the APIs before calling the service APIs. The user's password is encrypted by tamper-proof and irreversible encryption arithmetic, which can prevent the password from leakage and tampering.

3.1.5 High Compatibility

HikCentral Enterprise-Commercial supports access of Hikvision devices, Dahua devices, and third-party devices (by ONVIF protocol), and security control panels of Bosch, Honeywell, etc. It also supports access of devices of SONY, Samsung, Axis, etc., by the SDK protocol (or other mainstream protocol) provided by the device manufacturer.

3.2 System Architecture

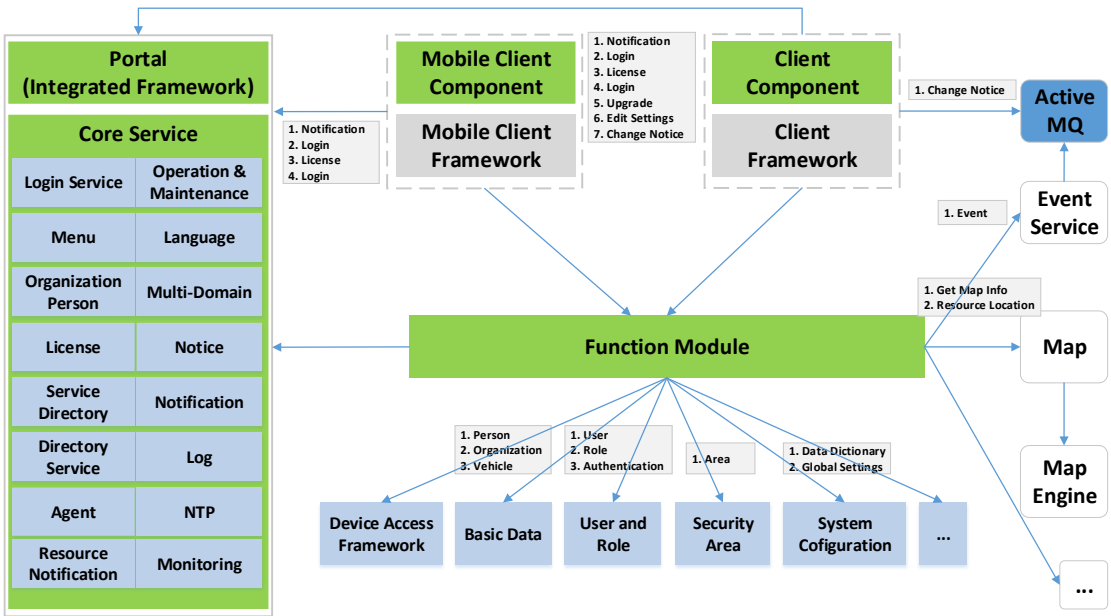
3.2.1 Function Architecture



The HikCentral Enterprise-Commercial is composed of multiple components. Each component provides different functions.

In general, the whole system includes following modules: video surveillance, one-card, vehicle control, alarm detection, integrated control, system configuration, and maintenance. Each module is composed of components.

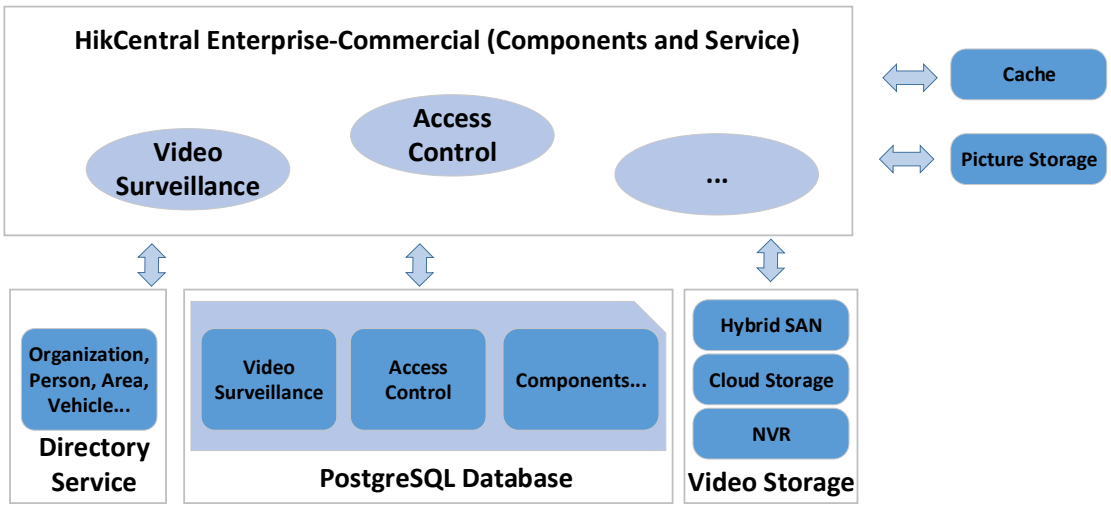
3.2.1 Logical Architecture



You can access HikCentral Enterprise-Commercial via Portal (Web Client), Control Client, and Mobile Client. As you can see on the above image, Portal is an integrated framework

accessed via web browser, which provides menus and interfaces of all the components. Control Client is designed based on control client framework and integrates multiple client components by client framework. Mobile Client is designed based on mobile client framework and integrates multiple mobile client components by client framework. The function modules is designed based on core service, system configuration, and general services. Each component provides APIs for function calling.

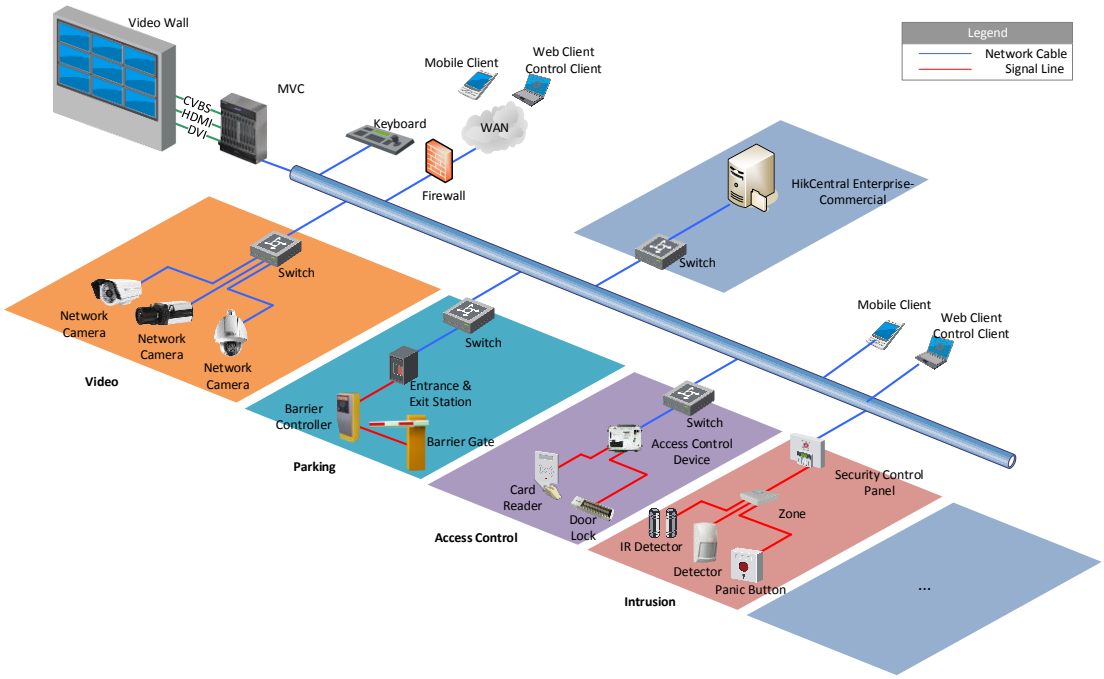
3.2.2 Data Architecture



As you can see from the above image, the system data includes structural function data, resource data, video data, picture data, and cache. The function data is saved in PostgreSQL database. Resource data is saved in directory service (LDAP). Video data is saved on NVR, Hybrid SAN, and cloud storage. Picture data is saved in ASW component (storage access service) and central storage device (Hybrid SAN or cloud storage).
Each component uses independent database which brings benefits for upgrade, migration, expansion, and maintenance.

3.2.3 Deployment Architecture

The following picture shows the deployment architecture when deploying all the services on the same server.



Deployment Architecture: Single Server Deployment

3.3 Key Technology

3.3.1 Modularization

HikCentral Enterprise-Commercial is composed of several modules (components), which improves the reuse of the product's functions. Other product can adopt the functions of HikCentral Master by reusing the related components. Each component is developed and maintained by professional teams and we can provide better solutions for each industry. The efficiency of issue fixing is also much higher.

What's more, developing by different components brings benefits on product extension. It costs less to extend the supported functions of the platform by integrating more components.

Developing by different components also brings some difficult issues: Integration of different components; The databases of each component are independent. The data consistency and API calling are much more complex. Due to this reason, the logic of the whole program is also much more complex to handle the exceptional situations.

3.3.2 Distribution

The product supports distributed deployment by installing services and components on different servers. This can improve the system capacity and performance, especially in large-scale project. Meanwhile, distributed deployment significantly improves the usability: if an error or fault occurs in one component, the whole system can still running properly,

rather than breakdown.
The services and components can also be installed on the same server, which meets the needs of small-scale project.
As a result, you can deploy the service which requires high performance and may cause large load balance independently on an independent server, thus to improve the efficiency. This also reduces the influence and pressure to other services.

3.3.3 Single Sign On

The system is composed of multiple components. As a result, identity verification is required when accessing the functions of these components. The system supports SSO (Single Sign On), which brings convenience for the users that after login, he/she can access all the components without login again with certain time duration.

3.3.4 Security

- By default, you need to access the system in HTTPS protocol. With authenticated certificate, it can reduce the risk of Man-In-The-Middle (MiTM) attacks. Encrypted transmission by HTTPS protocol also prevents from information leakage during plaintext transmission.
- Accessing the system by proxy after setting encryption algorithm can reduce the risk of internal service port exposure and improve service security.
- Only trusted IP address can access the system services. The access from untrusted terminals and cross-site scripting attacks are not allowed.
- The storage of each component is independent and the secret keys are also saved independently. Even though one or part of the secret keys are attacked, it will not affect the data storage of other components.
- The user's password is encrypted by tamper-proof and irreversible encryption arithmetic, which can prevent the password from leakage and tampering.
- The sensitive information of requests from front-end to back-end is transmitted in HTTPS protocol and is encrypted by asymmetric cryptographic algorithm.
- The system accesses storages and devices by security certificate respectively.

3.3.5 Operation and Maintenance Center

HikCentral Enterprise-Commercial provides Operation and Maintenance Center for service maintenance. It supports monitoring the status of servers, running status of services, triggering an alarm when service or server is exceptional, restarting offline service, etc.
It provides remote configuration to set the parameters for the services and restart services.
Supports auto-collection logs and clearing logs.
Supports installation and uninstallation of components, installation of patches, updating of resource packages, etc.

Supports multi-domain configuration, NTP configuration, manually adding service, activating and deactivating Licenses, etc.
Supports backup and restore of system data.
Provides FAQ to solve the frequently asked questions.
Provides system menu management.

3.3.6 Data Storage Technology

The system provides multiple video storage modes: storage on cameras, storage on embedded storage servers, storage on Hybrid SANs, and cloud storage.
The pictures on the system can be stored on ASW (storage access service) or central storage servers (Hybrid SANS or cloud storage service).
The structural data of the functions and applications is saved in the relational database, and you can add, edit, and delete the relation data if needed.
The resource data is saved in the LDAP and provides visualized trees to display, search, and share the resources in the system.

3.4 System Security

3.4.1 Encrypted Storage

- For sensitive data (such as device password), adopts AES-256 encryption.
- For user password, adopts HMAC- SHA-256 encryption.

3.4.2 Encrypted Transmission

- The process of calling service API is encrypted by DH shared secret exchange.
- When accessing the Web Client via WAN or public network, adopts HTTPS protocol.
- The sensitive data transmitted between Web Client and server are encrypted by RSA-2048 encryption.

3.4.3 Identity Verification

- **Man-Machine Identity Verification**
  - **Accessing System:** Identify the identity of the user login. Verification code is required after three failed password attempts.
  - **Accessing Device:** Verify the device's user name and password.
- **Machine-Machine Identity Verification**
  - Service API Calling Verification: Token verification. Generating token by HMAC algorithm.
  - Media Gateway Streaming Verification

- Picture Storage Access Verification
- Hybrid SAN Access Verification
- Cloud Storage Access Verification

Chapter 4 Applications

4.1 Basic Configuration

4.1.1 Person Management

The platform supports person organization management, including moving up/down organization;
Person management supports configuring person information including basic information, face picture/fingerprint connection. You can edit basic information of a person or recover a deleted person; the platform supports setting ID number, phone number, employ ID as the unique identifier of a person.
Furthermore, you can customize up to 5 fields of basic person information for a person.
The platform supports collecting face picture by a USB camera (such as DS-K5603(F)).

4.1.2 Vehicle Management

Supports adding/editing/deleting vehicles, and importing/exporting vehicle information in a batch.
You can also configure the owner information for the vehicle.

4.1.3 Security Area Management

Supports adding/editing/deleting an area, importing/exporting area information in a batch, and moving up/down an area.
Supports switching to cascade scene from non-cascade scene.

4.1.4 User & Role

1. Supports adding/editing/deleting a user group, importing/exporting user groups information in a batch, and moving up/down a user group.
2. Supports adding/editing/deleting/enabling/disabling a user, importing/exporting user information in a batch, linking a user with a real person in the system, and resetting a user’s password.
3. Supports synchronizing users from Windows domain.
4. Supports adding/editing/deleting a role, and assign a role to a user.
5. Supports assigning users permissions for accessing and managing the system.

4.2 Video Surveillance

Video surveillance centers on security surveillance by video-related functions. You can

perform real-time monitoring and view videos or pictures to know what happened at the monitored place by managing encoding devices, making recording schedule and capture schedule, etc.

4.2.1 Video Surveillance Configuration

Encoding Device Management

- **Access Protocol**
  1. Supports adding encoding devices to the system by Hikvision Device Network SDK protocol, EHome protocol, and ONVIF protocol.
  2. Hikvision SDK protocol: a protocol based on Hikvision device network SDK, used for Hikvision encoding devices in LAN.
  3. EHome protocol: Hikvision private protocol, used for Hikvision encoding devices in WAN.
  4. ONVIF protocol: ONVIF (Open Network Video Interface Forum) is a global and open industry forum with the goal of facilitating the development and use of a global open standard for the interface of physical IP-based security products. ONVIF creates a standard for how IP products within video surveillance and other physical security areas can communicate with each other.
  5. Dahua SDK protocol: a protocol based on Dahua device network SDK, used for Dahua encoding devices in LAN.
- **Device Management**
  1. Supports importing/exporting devices in a batch, configuring device connection parameters, and adding/deleting/editing/searching a device.
  2. Supports synchronizing device information (including device name, serial number, etc.) from the platform to devices, and vice versa. Supports synchronizing camera name from the platform to device, and vice versa.
  3. Supports configuring IP channel for an NVR, including adding and deleting encoding devices.
  4. Supports adding/deleting/editing/searching a camera.
  5. Supports configuring basic information of cameras, including device type, access protocol, location, longitude and latitude, height, keyboard control ID, etc.
  6. Supports configuring camera parameters, including:
     - ✧ OSD Configuration: display channel name, current date and time, and current day on the image.
     - ✧ Text Overlay: you can overlay up to 4 strings on the image.
     - ✧ Video Parameter: stream type, solution, bit rate, image quality, and frame rate.
     - ✧ Configuration of privacy protection, video masking alarm, motion detection alarm, and video loss alarm.
     - ✧ Adding/deleting/editing/searching alarm devices and configuring alarm input/output.

Central Storage Management and Configuration

Supports centralized management of central storage resources including Hybrid SAN and cloud storage. You can categorize domain by geographical area and type, create a storage domain, and devices within a domain should be able to communicate with each other. And you can add different types of real storage devices in to the created storage domains. The administrator can create a storage resource pool and assign users with reading or editing permissions for the pool. Users assigned with permissions can use the storage resource pool such as searching information in the pool.

- **Physical Resource Management**
  1. Supports adding/deleting/editing/searching a Hybrid SAN and cloud storage, and importing devices in a batch.
  2. Supports displaying storage device status, including online status, storage capability, rest capability, amount of connected channels, CPU usage, and memory usage, etc.
  3. Supports checking disk information and status of storage devices.
- **Storage Domain Management**
  1. A storage domain is used for virtual operations of physical storage devices, and allocation of resources for resource pool for video storage.
  2. Supports adding/deleting/editing/searching a storage domain.
  3. Hybrid SAN domain is used for managing Hybrid SAN storage resources, supporting linking multiple Hybrid SAN devices to the storage domain and virtual disposition of physical storage resources.
  4. Cloud storage is used for managing cloud storage resources. A cloud storage domain can be linked to a cloud storage device.
  5. Supports displaying storage status including domain type, device amount, total capability, and rest capability.
- **Resource Pool Management**
  1. Resource pool is used for recorded video management. You can apply recording schedule to a specified resource pool when configuring central storage for cameras.
  2. Supports adding/deleting/editing/searching a resource pool.
  3. Supports displaying resource pool status, such as storage status, resource pool type, resource pool usage, and channel amount, etc.

Recording Schedule Configuration

1. You can select device storage or central storage.
2. Supports displaying recording schedule, including recording status, storage location, and recording schedule template, etc.
3. Supports copy recording schedule to other devices in a batch, during which you can view the copy progress, schedule amount, and copied schedule amount.
4. You can select main stream or sub-stream as the stream type for device storage. Supports configuring video retention time when you use Hikvision Device Network

SDK protocol for communication.

5. Stream type selection mentioned above is also applicable for central storage. The streaming mode can be direct streaming or stream media streaming.
6. Supports setting recording schedule template as all-day template, workday template, weekend template, and customized template, and saving recording schedules of all cameras in the current computer.

Capture Schedule Settings

Capture schedule template is time arrangement for picture capturing. You can customize capture schedule to define when and how the device captures pictures with the predefined parameters. HikCentral Enterprise-Commercial provides two capture schedule template modes: time segment template and time point template.
The platform supports adding/deleting/editing a capture schedule for a camera, configuring capture schedule, and customizing capture interval and quality.

Event Arming Control

This function is oriented for scenes with large amount of channels of which multiple events need to be armed/disarmed for saving time.
You can arm/disarm the added devices for the following events: motion detection, video tampering detection, video loss detection, alarm input, and alarm output.
Supports configuring arming schedule for cameras in a batch, configuring arming schedule, and displaying arming status.

4.2.2 Live View

The platform supports viewing the real-time video of the camera under live view. Supports viewing live video and viewing in view mode. Supports real-time two-way audio between the platform and the camera. Supports batch broadcast and PTZ control.

View Live Video

The platform supports live view on the Web client and Control client.

1. Supports displaying the status (online/offline) of camera on the resource tree.
2. Supports displaying the VCA information during live view, including motion detection, line crossing, etc.
3. Supports regular window division modes for live view, including 1*1, 2*2, 3*3, 4*4 and 5*5. Supports customized window division modes, including 1+2, 1+5, 1+7, 1+8, 1+9, 1+12, 1+16, 4+9, 3+4, 1+1+12, etc. Supports corridor window division modes, including 1*2 and 1*4.
4. Supports opening an auxiliary screen for live view.
5. Supports viewing all the camera resources in the area. Supports closing the current

display window in a batch. Supports the view scale of the playback window as self-adaptive mode and full-screen mode

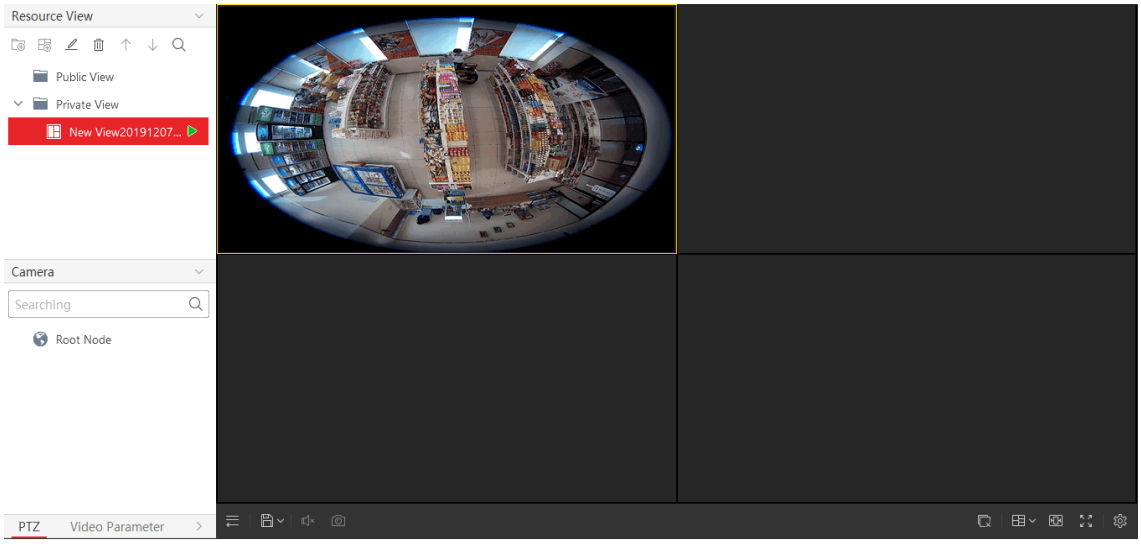
6. Supports capturing pictures during live view. Supports audio on/off, digital zoom, switching streams, and viewing stream information. Supports customizing (adding/removing) icons on the live view toolbar.
7. Supports picture surveillance if capture schedule has been configured for the camera. You can switch between video live view and picture surveillance in the live view window.
8. Supports stream self-adaptive and switches streams automatically according to the number of windows. The main stream is automatically switched to sub-stream when the number of windows is bigger than the set value.
9. Supports emergency recording during live view, serving as a recording and prove for abnormal problems.
10. Supports switching to instant playback to view the recorded video files during live view.
11. Supports auto-switch of cameras in a group according to the predefined auto-switch interval, the window division mode, etc. Supports managing auto-switch group. You can add/delete/edit/search auto-switch group. Supports configuring parameters of an auto-switch group, including auto-switch interval, sorting auto-switch, etc.
12. Supports resuming last live view. You can configure this function in the platform.
13. Supports displaying temperature detected by thermal cameras on the live view image. Supports accessing Hik-Connect account; Supports live view and playback of Hik-Connect devices.

View in View Mode

A view is a window division with resource channels (e.g., cameras and access control points) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows as favorite so that you can quickly access these channels.

Two types of view modes are available: public view and private view. Public views can be viewed by other users with the permissions, while private views can only be viewed by the logged-in user.

The platform supports managing view and view group. You can add, delete and move view in the view group. Also, you can edit camera and window division mode in the view.



Two-Way Audio & Broadcast

The platform supports real-time two-way audio for the camera under live view. Supports configuring auto recording during two-way audio. Supports batch broadcast function. You can add and delete the broadcast groups. The number of broadcast channels should be less than 100.

PTZ and Video Parameters Control

1. The platform supports PTZ control for cameras with pan/tilt/zoom functionality during live view. Supports direction control, zoom in/out, focus, Iris +/-, wiper control, light control, and PTZ locking and preemption.
2. Supports setting the preset, patrol and pattern for the camera. Supports recording and playing patterns.
3. Supports PTZ lock and setting lock time according to user levels. Users in higher permission level have the priority to use or lock PTZ when lower-level users are controlling PTZ. During the lock time, users in lower level cannot use PTZ.
4. Supports displaying the information of PTZ operator on the live view image.
5. Supports adjusting video parameters, including luminance, chromaticity, contrast, and saturation.

4.2.1 Playback

The platform supports searching, locating, playing the video playback. Supports video flow control, downloading video footage, etc.

Video Playback

The platform supports video playback on the Web client and Control Client.

1. Supports searching video playback by video type, including continuous recording, motion recording, and recording triggered by alarm. You can also view other types of recordings during video playback. Supports searching video playback by video storage mode, including device storage and central storage;
2. Supports multiple window division modes for playback, such as 1 × 1, 2 × 2, 3 × 3, 4 × 4, etc.
3. Supports capturing the pictures during playback, viewing stream information, audio on/off, digital zoom, etc.
4. Supports searching video by time period. Supports locating video by specific time.
5. Supports video flow control, including normal playback, reverse playback, fast/slow forward playback, fast/slow reverse playback, single frame playback, reverse single frame playback. In slow forward/reverse playback, 1/2x, 1/4x, 1/8x, and 1/16x playback speed can be supported. In fast forward/backward playback, 2x, 4x, 8x, and 16x playback speed can be supported.
6. Supports adding tag (red, blue, green and yellow) and description to the video. You can search the video footage according to the tag type, description and the tag time.
7. Supports locking and unlocking the video. You can set the video footage to be locked and customize locking duration by day/week/month/year. The locked video footage cannot be overwritten or deleted.
8. Supports scrolling the mouse to scale the timeline of video.
9. Supports displaying the VCA information during playback, including motion detection, line crossing, etc.

Download and Clip Video

The platform supports downloading video. You can select the video footage to be downloaded and the download address. Supports searching, deleting, pausing, and continuing the downloading task. Supports starting and pausing all the downloading tasks in a batch. Supports filtering the downloading task according to task status.
Supports clipping video. You can set the video footage to be clipped and the saving path of clipped video.
Supports downloading and clipping single video footage.

4.2.3 Picture Search

The Web Client supports searching pictures captured by cameras as capture schedule, and filtering the search results by camera name and capture time.
You can start a slideshow of the search results and download them. Configuration of slideshow speed is also supported.

4.2.4 Video Wall

Video wall displays videos collected by encoding devices on the video wall screens by decoding devices. It provides functions including decoding device management, video wall resource management, video wall/window control, and displaying contents on the wall.

Decoding Device Management

1. You can add/delete/edit/search a video wall which includes LED video wall and LCD video wall, add/delete/edit/search a decoding device, and the decoding resource's access protocol is Hikvision Device Network SDK Protocol.
2. Supports linking decoding channels to the video wall, and one decoding channel can be linked to only one screen after which the decoding channel cannot be shifted to other screens.
3. Supports adjusting window position, size, and solution on the wall.

Window Control

1. The video wall supports opening a window so you can display videos on the window when there are no vacant windows. You can drag the added window to move it, enlarge or compress it.
2. Supports window division, which means you can split a window into multiple small windows to display videos of more cameras, after which you can joint them together. You can name or number a window, and put a window on the top/bottom.
3. The video wall provides LED text configuration function, such as text length, contents, transparency, character scrolling, etc.
4. The windows can be displayed on the wall, which means you can display desktop/live view/playback on the wall. For analog signal sources, you can only display their live view on the wall. The streaming mode during displaying on the wall can be configured, and you can display intelligent information on the wall.
5. You can set a window as an alarm window with different alarm priority, so that the alarm-related video will be displayed on the wall automatically when alarms with corresponding priority are triggered.
6. The video wall also supports viewing Hikvision decoding devices' decoding status.

Scene Management

1. The video wall scene is a collection of video wall status, including window division/jointing, camera auto-switch, alarm window, etc. You can add scenes for the video wall for configuration and management, such as camera auto-switch schedule, scene change plan, etc. A video wall scene can be deleted/edited/configured.

2. You can configure scene auto-switch and scene change plan. You can also configure camera auto-switch for a scene, and you can pause/resume the auto switch or go to the previous/next page when the scene auto-switch is displayed on the wall.

Other Functions

1. Supports switching stream when displaying windows on the wall; and you can set the stream as sub-stream mandatorily, which means the video will switch to sub-stream automatically when divided window amount exceeds a certain number.
2. During displaying on the video wall, you can open the audio of a certain channel.
3. You can display live view and playback of local cameras with online status shown.
4. Supports connecting a network keyboard to the video wall, and using the network keyboard for displaying video on the wall.
5. Supports displaying video on the wall by the Control Client running on a PAD.
6. The Control Client has two skins: black and blue between which you can switch according to your actual need.
7. Supports configuring a scene as a device scene or platform scene. For example, you can use a device scene when you divide a window to a large amount of small windows.

4.2.5 Panoramic Surveillance

1. The Control Client supports a panoramic surveillance by 180° /360° panoramic camera.
2. During a panoramic surveillance, you can switch the monitoring mode of a 360° panoramic camera between auto-location and manual location.
3. In a panoramic image, you can capture a picture, start recording instantly, and perform digital zoom.
4. In the image of a speed dome, you can capture a picture, start recording instantly, and perform digital zoom and PTZ control.

4.3 One-Card System

4.3.1 Card Issuing

For businesses (such as access control, parking lot, and elevator control) that use cards in the system, you need issue cards to persons in the Card Issuing module.
This function is often used in places like enterprises, banks, and prisons to ensure the security.

Supported Devices

The HikCentral Enterprise-Commercial supports issuing a Mifare card/CPU card/Bluetooth card/RFID card/ID card to a person.
Configure card enrollment device parameters, customizing number for a CPU card and long-range card, encrypting a card number.
Supports encryption of Mifare card to avoid card copying.

Features

In the person list page, you can view person information and persons' card information.
Supported card operations include reporting card loss, returning card, replacing card, importing card, etc.
Supports importing card information in a batch, setting card password and expiration date, searching a card, operating a single card, and virtual card management.

4.3.2 Access Control

The platform can provide access control service for areas including companies, apartments, etc. The following devices can be accessed to the platform:
single-door/two-door/four-door access controller, swing barrier, access control terminal, etc. Supports configuring three credentials: card, fingerprint, and face picture. Supports multiple advanced functions including configuring special cards, multiple authentication, remaining open with first card, anti-passback, multi-door interlocking, remaining open/closed, etc.

Access Control Configuration

1. The platform supports configuring parameters for the following access control devices, including access controller, lane controller, and access control terminal.
2. Supports importing/exporting access control devices and exporting access control points, which can improve management efficiency
3. Supports configuring timeout period of authentication interval parameters. If the interval between the two authentication exceeds the maximum interval of authentication, you should restart multiple authentication.
4. Supports configuring capture settings for access control terminal. You can set capture times. If the capture times is set as 0, the device will not capture picture.
5. Supports configuring storage location for storing pictures captured by the access control devices.
6. Support configuring auto-apply permission parameters.
7. The platform supports copying permission settings from parent organization. Access control permission can be automatically copied to newly added organizations.
8. Supports setting event record retention period, which starts from the time when the event occurs. And the event information will be deleted when the retention period expires.

9. Supports allowing platform to verify permission. If this function is enabled, the platform can control the door status according to the configured user permission even if the permission has not been applied to the device.
10. Supports configuring event type parameters, including device event, normal access event, and access exception event.

Access Control Management

- **Permission Configuration**
  1. The platform supports configuring three access credentials: card, fingerprint, and face picture.
  2. Supports configuring permission by organization, by person group, and by person. Supports configuring different schedule templates for different access control groups and access control points.
  3. Supports adding, deleting and viewing permissions. Supports viewing the details of access control schedule template.
  4. Supports applying access control permissions to the device, including card, fingerprint and face picture. Supports initializing all the previous permissions and applying the new permission configuration to the device.
  5. Supports tracking and viewing permission applying task.
- **Biometric Recognition Configuration**
  1. The platform supports configuring two biometric access credentials: fingerprint and face picture.
  2. Supports searching the access control points by the name of area or access control point.
  3. Supports viewing the number of face credentials and fingerprints on the access control device. Supports manually adjusting the number of face credentials and fingerprints on the access control device.
- **Group Management**
  1. The platform supports managing access control group. Supports adding, editing, deleting, and viewing details of the access control group. Supports searching access control group. The searched results include access control group, access control point, and description.
  2. The platform supports managing person group. Supports adding person group by organization and by rule (gender, ID type, etc.). Supports adding, editing, deleting and viewing details of person group. Supports searching person group. The searched results include person group, person/rule details, and description.
- **Schedule Template**
  1. The platform supports managing schedule template. You can add, edit, delete, and view schedule template. The default weekly schedule cannot be edited or deleted.
  2. Supports managing holiday group. You can add, edit, delete, and view holiday group.

3. The schedule template contains weekly schedule and holiday schedule. You can configure holiday schedule according to holiday group.

- **Permission Search**
  1. The platform supports searching permissions. You can set one or more of the following search conditions, including name, ID No., organization, access control point, controller, area, permission applying state of card, fingerprint and face picture, and configuration time.
- **Permission Applying Record**
  1. The platform supports searching permission applying record. You can set one or more of the following search conditions, including task code, controller, access control point, current area, applying type and result, start and end time of applying. Supports exporting the details of permission applying record.

Advanced Applications

- **Card Holder of Special Card**
  1. Special cards include card for disabled person, card in blacklist, duress card and super card.
  2. The card for disabled person is usually used for people with mobility difficulty. The door will remain open for the configured time period for the card holder.
  3. Card in blacklist is for people in blacklist. When they swipe cards, the door will remain closed and it will trigger alarm.
  4. Duress card is used when person is under duress. The door will be unlocked when he/she swipes the card and the Control Client will receive a duress alarm to notify the security personnel.
  5. Super card is set for super users. If the person is set as a super user, he/she will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization.
  6. The platform supports managing card for disabled person. You can search, add, edit, and delete the card.
  7. Supports managing card in blacklist. You can search, add, edit, and delete the card.
  8. Supports managing duress card. You can search, add, edit, and delete the card.
  9. Supports managing super card. You can search, add, edit, and delete the card.
  10. Supports applying the configuration parameters to the device. Batch applying is supported.
  11. Supports copying the configuration parameters to other access control controller devices.
- **Multiple Authentication**
  1. The platform supports multiple authentication. For security purpose, the door in certain important site requires to be opened by multiple authentications from different persons.
  2. Supports setting different authentication methods for different time periods.

3. Supports adding authentication role groups. Supports adding multiple persons to one role group. The authentication of one person in the role group can stand for the authentication of the role group.
4. Supports designating the authentication sequence.
5. Supports the following authentication methods:
   - Local Authentication: Authenticate via the access control device. When the persons swipe the cards in the card group, the door will be opened.
   - Local Authentication + Remotely Opening Door: Authenticate via the access control device and opening door via the system. After the persons swipe the cards in the card group, opening door operation on the Control Client is required to open the door.
   - Local Authentication + Super Permission: Authenticate via the access control device and entering the super password. When the persons swipe the cards in the card group, and then enter the super password, or swipe the super card, the door will be opened.
6. The platform supports managing authentication person group. You can group persons with the same authentication method. Supports adding, deleting and viewing the details of group.
7. Supports searching authentication person group.
8. The platform supports managing access control points. You can add, edit, delete, and view details of the access control points.
9. Supports searching access control point(s). You can set one or more of the following search conditions, including the name of access control point, controller and status.
10. Supports applying multiple authentication parameters to the device. Supports batch applying parameters.
11. Supports deleting multiple authentication parameters. And the platform will automatically apply the new settings to the device.
12. Supports copying multiple authentication parameters to other access control points.
13. Supports Control Client secondary permission authentication.

- **Remain Open with First Card**

1. The platform supports remaining open with first card. After the person swipes the first card, the door will remain unlocked or be authorized for some time.
2. Supports searching the devices configured with remaining open with first card. You can set one or more of the following search conditions, including the name of controller, device type and status.
3. Supports managing the devices configured with remain open with first card. You can add, edit, and delete the devices.
4. Supports copying remaining open with first card parameters to other access control points.
5. Supports applying remaining open with first card parameters to the device. Batch applying parameters is supported.

- **Anti-Passback**

1. The platform supports anti-passback. The person should exit via the door in the anti-passback if he/she enters via the door in the anti-passback. It minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access.
2. Supports searching devices configured with anti-passback. You can set one or more of the following search conditions, including the name of controller, device type and status.
3. Supports managing devices configured with anti-passback. You can add, edit, and delete the devices.
4. Supports copying anti-passback parameters to other access control points.
5. Supports applying anti-passback parameters to the device. Batch applying parameters is supported.
6. Supports deleting the configuration. And the platform will automatically apply the new settings to the device.

- **Multi-Door Interlocking**
  1. The platform supports setting the multi-door interlocking function between multiple doors of the same access control device. To unlock one of the doors, other doors must remain locked.
  2. Supports searching devices configured with multi-door interlocking. You can set one or more of the following search conditions, including the name of controller, device type and status.
  3. Supports managing devices configured with multi-door interlocking. You can add, edit, and delete the devices.
  4. Supports applying multi-door interlocking parameters to the device. Batch applying parameters is supported.
  5. Supports deleting the configuration. And the platform will automatically apply the new settings to the device.
- **Reader Authentication Mode**
  1. The platform supports reader authentication mode. You can set different authentication rules including card, face picture, fingerprint, etc. for different time periods.
  2. Supports searching access control points/card readers. You can set one or more of the following search conditions, including the name of access control point, controller, device type, status, and description.
  3. Supports managing access control points/card readers. You can add, edit, and delete the access control points/card readers.
  4. Supports applying reader authentication parameters to the device. Batch applying parameters is supported.
  5. Supports copying reader authentication parameters to card readers in other access control points.
- **Remain Open/Closed**
  1. The platform supports configuring weekly time periods for an access control point (door) to remain open or closed. During the remaining open time, the door is open without any authentication method; and during the remaining closed time,

only super users can access the door.

2. Supports searching the access control points configured with remaining open/closed. You can set one or more of the following search conditions, including the name of access control point, controller, device type, status, and description.
3. Supports managing the access control points configured remaining open/closed. You can add, edit, and delete the access control points.
4. Supports applying remaining open/closed parameters to the device. Batch applying parameters is supported.

- **Access Control Terminal Linkage**
  1. The platform supports configuring access control terminal linkage. The access control terminal is linked with camera and can capture pictures for specific access control events (e.g., duress alarm).
  2. Supports searching devices. You can set one or more of the following search conditions, including access control point, controller, device type, status, and description.
  3. Supports managing devices. You can add, edit, and delete the devices.
  4. Supports applying access control terminal linkage parameters to the device. Batch applying parameters is supported.
  5. Supports deleting the configuration. And the platform will automatically apply the new settings to the device.

Search Access Control Event

- **Person Entry/Exit Event**
  1. The platform supports searching person entry/exit event. You can set one or more of the following search conditions, including the name, employee No., parent organization, access control point, controller, access control point area, event time and type, captured picture.
  2. Supports exporting person access control event, including name, employee No., card No., parent organization, access control point, controller, area, exit/entry, event type, captured picture, event time, etc.
  3. Supports manually syncing person entry/exit event data from the access control device.
- **Device Event**
  1. The platform supports searching access control device event. You can set one or more of the following search conditions, including controller, access control point, card reader, controller area, event type and time.

Operations on Control Client

- **View Access Control Details**
  1. The platform supports displaying the access control points that the current user

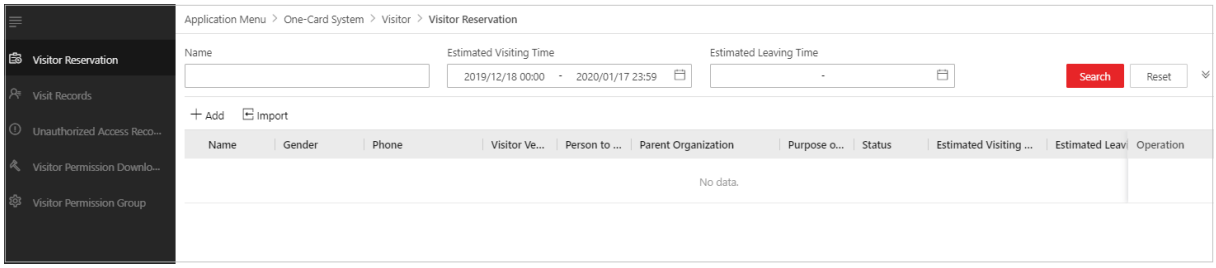
has the permission to.

2. Supports displaying access control events, including name, card No., face picture, etc. Supports displaying access control events in the form of list.
3. Supports displaying access control points and their status in different areas. Supports controlling the status of access control points.
4. Supports counting the number of access control points being open/closed/offline in the current area.

- **Control Door Status**
  1. The platform supports controlling door status, including opening/closing door, and remaining open/closed. Supports displaying the current status of door on the Control Client.
  2. Supports secondary permission authentication on the Control Client for access control points configured with multiple authentication.
  3. Supports adding specific door(s) to Favorites, and viewing the added door(s) in Favorites.
  4. Supports access control terminal (DS-K1T500/501/604) calling the surveillance center; Supports two-way audio between the access control terminal and the Control Client.
- **View Access Event**
  1. The platform supports searching events by event type. Supports viewing the detailed information about access control events in full screen mode, such as swiping time, access control point, card No., card holder, etc.

4.3.3 Visitor

HikCentral Enterprise-Commercial provides visitor management system which provides visitor management and registration solution. Core features include visitor registration, message notification, visitor registration, visitor pass, etc.



Make a Reservation

A reservation is performed on the Web Client. On the Web Client, you can make reservation for one visit one by one by entering the visitor and visitee information in the system. After that, you can view the reservation records or cancel a reservation.

Visitor Management

- **Visit Records**
  On the Web Client, you can search or export the visit records, and add a visitee to the visitor list.
- **Unauthorized Web Client**
  You can add a visitor to the visitor list after viewing the access details such as visitor name, credential type, recorded time, etc.
- **View Permissions Applied to Visitors**
  Supports viewing the visitor permission applying details such as visitor credential details, applying status, device applied to, etc. and apply permissions again.
- **Visitor Permission Group**
  Supports adding/editing/deleting permission group with access control/elevator control/face picture authentication/parking lot permissions. In the permission group list, you can search a permission group to view visitors in this group and set a default permission group.

Check-in

1. With the manual visitor client, a visitor can check-in on his/her own by scanning QR code, entering verification code on the manual visitor terminal. A visitor can check-in without a reservation. The manual visitor terminal will give the visitor a visitor card for access control and print a visitor pass for the visitor. You can customize the template for the visitor pass.
2. During the check-in, the visitor can collect his/her face picture by the manual visitor terminal, and he/she can perform access control authentication by the face picture after applying the face picture to the manual visitor terminal.
3. You can select a visitor pass template on the manual visitor terminal.
4. The visitor will receive a prompt when checking in if he/she is a person in the person list.
5. On the manual visitor terminal, you can apply permissions to the visitor again when the permission group is edited, and check out for the visitor.

4.3.4 Video Intercom

The video intercom component is applicable for the community. It supports server management, video intercom device management (including master station, outer door station, door station, and indoor station), permission configuration (including access control permission and video permission of indoor station), biometric recognition configuration (e.g., face, fingerprint), event search, call log search, etc. Based on the audio, video, and access control function, the video intercom provides real-time communication and access control for property management personnel, residents, and visitors, and make sure the multi-level security by real-time video and alarm.
The residents can use face and fingerprint to enter or exit the door, instead of swiping card, by 9613 series and 9502 series face door station/outer door station, which provides good face recognition solutions about person access.

Video Intercom Configuration

- **Video Intercom Device Management**
  1. It is supported to add, edit, delete master station, outer door station, door station and indoor station in the same subnet. Batch adding, importing and exporting indoor stations are supported. You can search the devices by device name, device type, IP address, and password strength.
  2. The new device models of door stations (DS-KD9603 and DS-KD9203 with 4.3-inch and 10-inch landscape) and indoor stations (DS-KH8520/8350/8330/6220/6320) are accessed.
  3. Batch importing door stations is supported.
  4. The access control terminals (DS-K1T671MF、DS-K1T607MF、DS-K1T641M、DS-K5671-ZV、DS-5607-ZV) can be used as door station/villa door station/outer door station.
- **Video Intercom Device Parameter Configuration**
  1. You can configure calling priority for master station. The smaller the master station No. is, the higher the calling priority will be. The default priority is based on the sequence of adding devices. The first added device has the highest priority. The order can be adjusted.
  2. You can select picture storage pool (Hybrid SAN and cloud storage) for storing the captured pictures by video intercom devices.
  3. Auto applying access control permission is supported.
  4. You can enable or disable auto applying permission function. If enabled, permission application at the fixed time (applying time interval configurable) or for fixed times (up to 5 fixed time points) can be performed.
  5. It is supported to configure event parameters, including event type (device event and person entering/entering event) and event record retention period. The events are divided to two types: door station/outer door station, and door station.
  6. The events of door station/outer door station include Device Tampering Alarm, Duress Alarm, Incorrect Password, Door Not Open, and Door Not Closed.
  7. The events of indoor station include SOS Alarm, Water Detector Alarm, Active Infrared Alarm, Smoke Detector Alarm, Gas Detector Alarm, Passive Infrared Alarm, etc.
  8. The person entering/exiting events include Open Lock by Password, Open Lock by Duress Code, Open Lock by Swiping Card, Open Lock by Indoor Station, Open Lock by Center Platform, Open Lock by Bluetooth, Open Lock by QR Code, Open Lock by Face Picture, and Open Lock by Fingerprint.
  9. The system can receive the selected events, and ignore the unselected events. The configured linkage rules of the events will help to reminder administrator to take actions.
  10. When the specified device events, person entering, exiting events, or call logs occur, the system can receive the events and save the event records for a period, which can be set as 1 month, 2 mouths, 6months, etc.

11. It is supported to access door stations by EZVIZ, and apply person card number, face picture, and fingerprint permissions. The supported device mode is DS-KD9203.

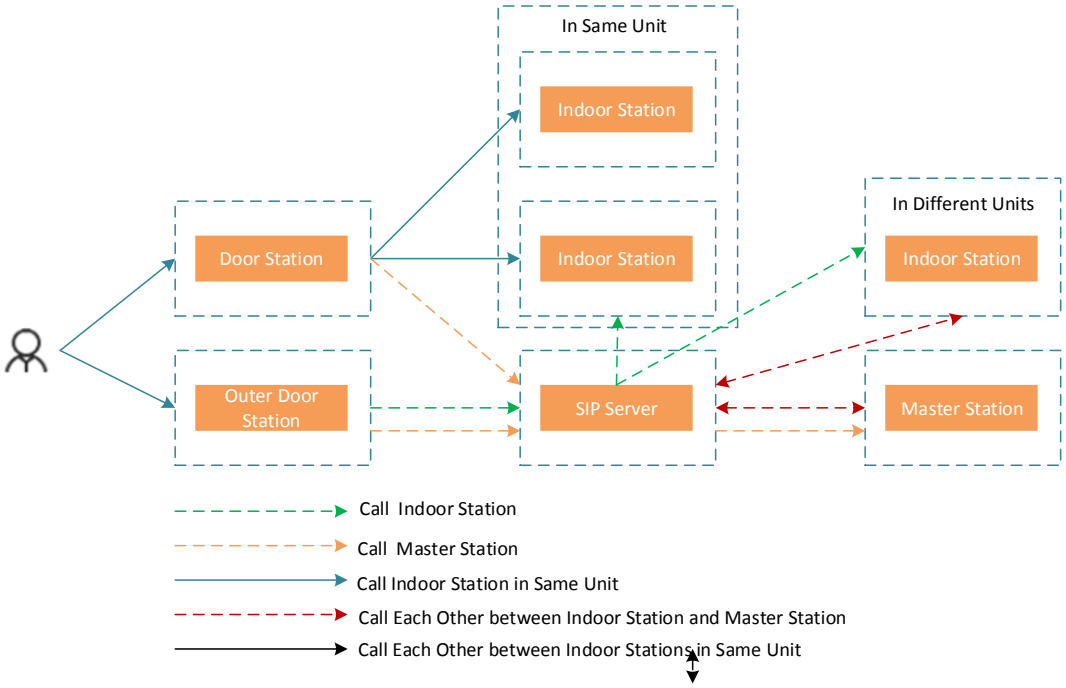
Video Intercom Service Management

- **Session Information Applying**
  The device contacts and device information can be applied to the SIP server and video intercom devices, respectively. The IP address of main master station, door station, SIP server, and video intercom drive service can be applied to the video intercom devices by DAS address.
- **Access Control Permission Configuration**
  It is supported to configure access control permissions, including adding and deleting permission by organization and person, verifying permission, fingerprint, and face picture, applying permissions, and checking and exporting applying records.
- **Biometric Recognition Configuration**
  It is supported to view, enable and disable biometric recognition (including fingerprint or face).
- **Assigned Permission Search**
  It is supported to search and export assigned permission by name, organization, door station, outer door station, area, card, fingerprint, face picture, and configuration time.
- **Permission Applying Record**
  It is supported to search and export permission applying records by task code, door station, outer station, area, applying type, applying result. start time, and end time.

Event Search

- **Person Entering/Exiting Event**
  It is supported to search and export person entering/exiting event by name, card No., organization, event source, device type, event source, area, event type, and event time.
- **Device Event**
  It is supported to search and export device event by device name, area, event type, and event time.
- **Call Log**
  It is supported to search and export call logs by caller, callee, calling time and connected/disconnected.

Video Intercom Service Flow



Video Intercom Service Flow

1. Call indoor station from outer door station through SIP server.
2. Call indoor station in same unit from door station and directly start talking without SIP server.
3. Call center master station from outer door station, door station, and indoor station through SIP server.
4. Call each other between indoor stations in the same unit and directly start talking without SIP server and master station.

4.3.5 Elevator Control

The Elevator Control module is applicable to elevator control management of the elevator controllers. It provides multiple functionalities, including floor group management, elevator control permissions configuration, searching elevator control event, etc.

Elevator Control Configuration

1. The platform supports managing elevator control devices, including adding, editing, deleting and online test of the elevator control device. Also, you can search and view devices according to device name, IP address and password strength.
2. The platform supports setting permission parameters. You can enable auto apply permission. After that, the platform can automatically apply all configured permissions.
3. Currently, two methods of auto applying are supported: applying at fixed time of each day and applying for fixed times each day.
4. The platform supports setting event parameters, including selecting event type and

configuring event retention period. You can select device event and person access event. Device events mainly include 31 elevator controller events (such as relay disconnected, device offline, etc.) and 4 card reader events (such as card reader offline). As for person access event, there are 9 common events, including card permission expired, permission mismatched, etc. If you have configured linkage actions for the event, the platform will notify the corresponding personnel to handle the event timely when the event happens. Also, the platform supports setting event retention period, which starts from the time when the event occurs. The event information will be deleted when the retention period expires. You can select the event retention period as 1 month, 3 months, 6 months, 9 months, etc.

Elevator Control Management

- **Permission Configuration**
  The platform supports permission configuration. Supports adding and deleting permission by organization and by person.
- **Floor Group**
  The platform supports managing floor groups. Supports viewing the details of floor groups. You can add, delete and edit floor groups.
- **Permission Applying Record**
  The platform supports permission applying record. You can set the relevant search conditions including task code, elevator name, current area, start and end time of applying to search the applying record and view the details of permission applying record.

Advanced Applications

The platform supports setting remaining open/closed status of floor according to weekly schedule.

Search Elevator Control Event

- **Person Access Event**
  The platform supports searching person access events. You can set one or more of the following search conditions, including the name, ID No., card No., organization, elevator name, current area, event time and type. Supports viewing and exporting person access events, including person name, ID No., card No., organization, elevator name, etc.
- **Device Event**
  The platform supports searching elevator control device events. You can set one or more of the following search conditions, including elevator name, card reader name, current area, event type and time. Supports viewing and exporting access control

device events.

4.3.6 Patrol

This function is mainly oriented for scenes like edifices, factories, and storehouses needing guards' patrol to ensure security of the buildings and people in the buildings. The Web Client supports setting different patrol points and patrol routes, and appointing certain guards to patrol, so that you can manage the patrol efficiently. Meanwhile, you can link cameras and alarm devices to patrol points to view live view and receive alarm notifications when an alarm is triggered.

Patrol Configuration

You can set a card reader or alarm I/O as a patrol point.
The Web Client supports searching card reader/alarm device patrol points by patrol points name, linked device name, IP address, and device No., adding/deleting/editing patrol points.

Patrol Parameters

- **Patrol Route**

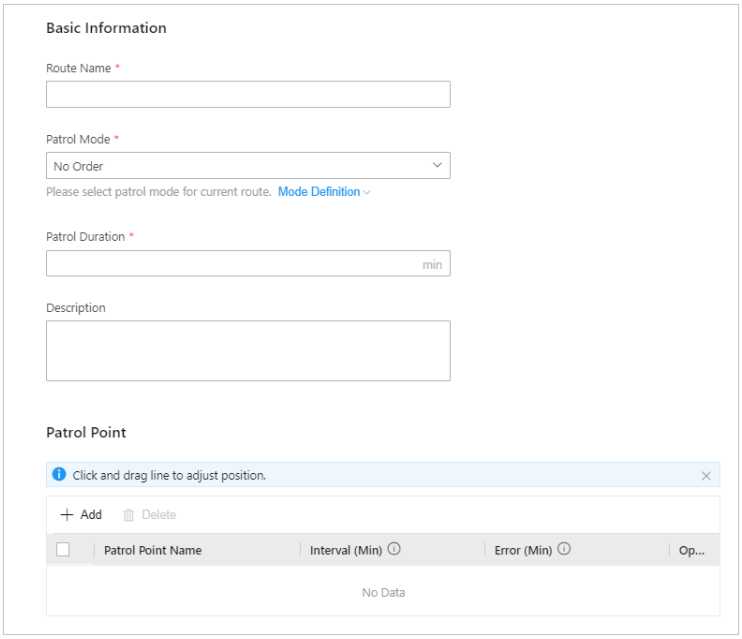
Supports adding/deleting/editing patrol routes, and setting route name, patrol duration, patrol mode, patrol points, and description, etc.

- **Holiday**

Supports adding/deleting/editing holidays during the patrol, and setting holiday name, holiday duration, date, and description.

- **Patrol Schedule**

Supports adding/deleting/editing patrol schedules, setting schedule name, selecting patrol route, patrol person, and holiday for the schedule, and setting date for the schedule, etc.



Patrol Information Search and Reports

- **Patrol Information Search**

Supports searching shift information/patrol history by patrol route name, patrol person, patrol time, and patrol results, and then saving the searching results in the local computer.

- **Generate Patrol Reports**

Patrol points will send real-time patrol-related information to the platform so that you can generate a patrol report to know the details of patrols during a certain time period. You can also save the report in your computer.

4.3.7 Time and Attendance

Based on access control point, Time and Attendance function provides attendance calculation according to card swiping data and attendance rule, and integrated management about attendance check points, attendance rules, attendance records, attendance results, etc. The attendance reports are supported.

Time and Attendance Configuration

1. Configuring retention period of attendance details is supported. The longest period is 36 months.
2. Configuring retention period of card swiping records is supported. The longest period is 36 months.

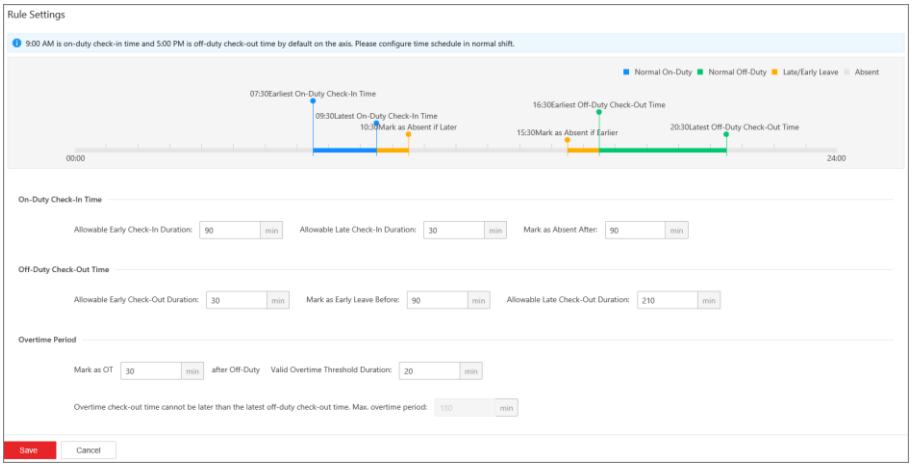
Attendance Service Management

- **Shift Group Management**

  It is supported to add, delete, and edit shift group, including shift group name, person, description, etc. Up to 1000 shift groups can be added and up to 500 persons can be added to a shift group.

- **Shift Rule Management**

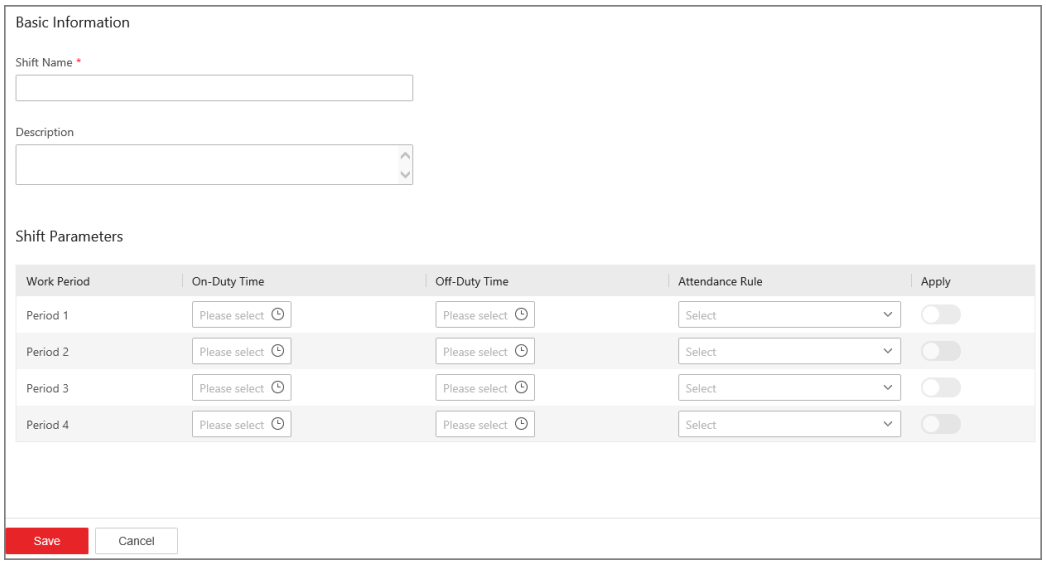
  It is supported to add, delete, and edit shift rule, including allowable early check-in duration (min), allowable late check-in duration (min), mark as absent after start-work time (min), allowable early check-out duration (min), allowable late check-out duration (min), mark as early leave before end-work time (min), etc. Attendance rule search is supported.



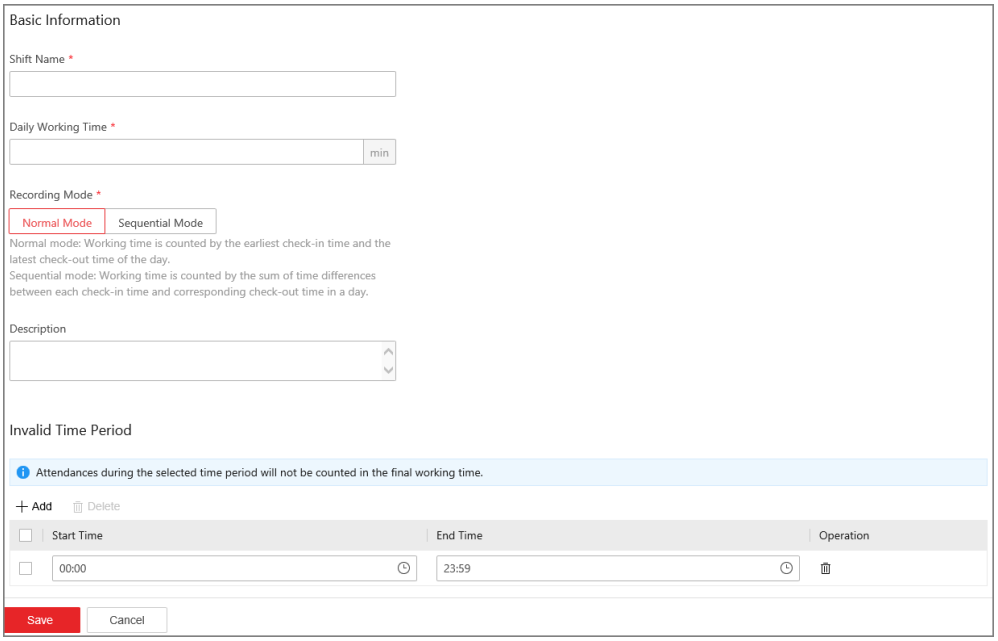
Rule Management

- **Shift Management**

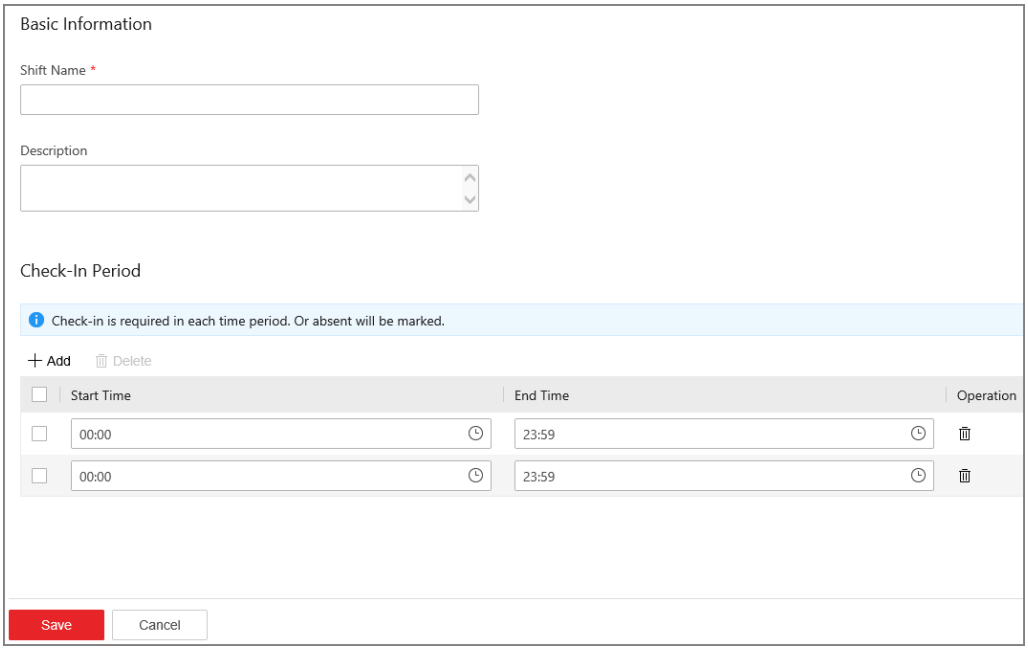
  It is supported to add, edit, and delete normal shift, including shift name, description, and period information. The normal shift search is supported and can be cross-day. You can add attendance rule and select the attendance rule for a normal shift. Four start-work periods and end-work periods can be set by default. It can be applied according to actual requirements.



It is supported to add, edit, and delete Man-Hour shift, including shift name, description, recording mode, daily working time, and invalid time period. The Man-Hour shift search is supported. The Man-Hour shift only supports natural day and cannot be cross-day. The recording mode divides into normal mode and sequential mode. The working time in normal mode is counted by the earliest check-in time and the latest check-out time of the day, and the working time in sequential mode is counted by the sum of time differences between each check-in time and corresponding check-out time in a day.



It is supported to add, edit, and delete Check-In shift, including shift name, description, and check-in period. The Check-In shift search is supported. The Check-In shift only supports natural day and cannot be cross-day. You can set check-in period(s), during each of which the employee need to check-in. Up to 10 check-in periods can be added.



- **Holiday Management**

  It is supported to add, edit and delete holiday, including holiday name, holiday days (one or more days), and description. The holiday search is supported.

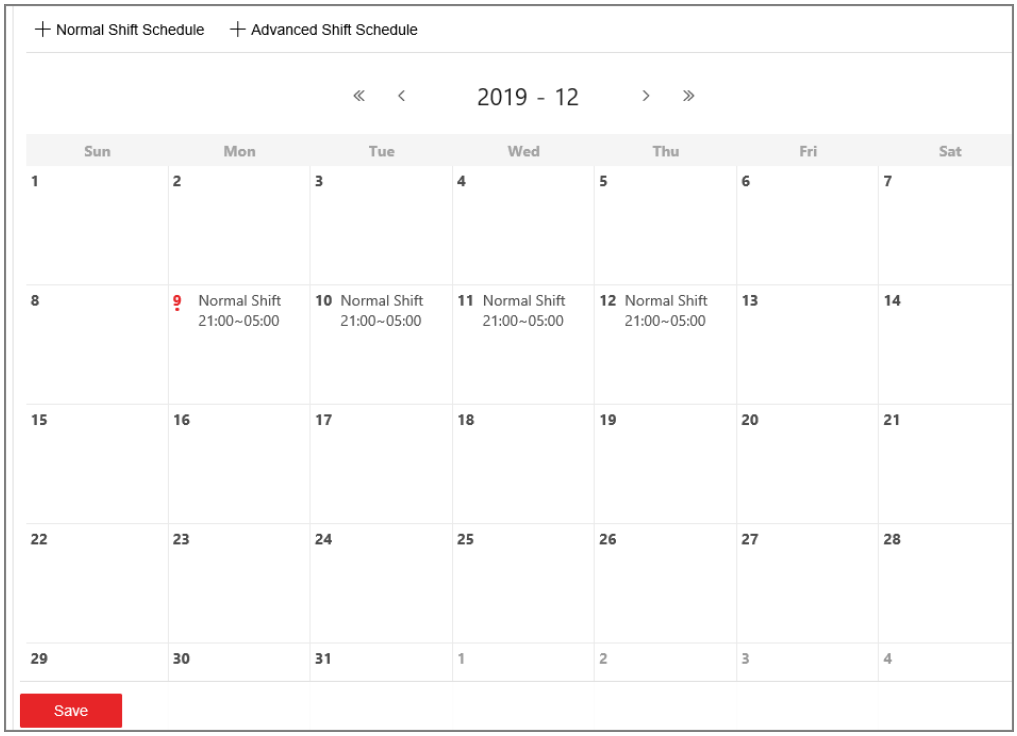
- **Shift Schedule Management**

  It is supported to set normal shift schedule, including assigning one shift for the shift group during the specified time range, and setting one or more holiday(s) during which the check-in or check-out is invalid.

It is supported to set advanced shift schedule, including assigning multiple shifts for one shift group during the specified time range, setting the interval between two shifts in the group, and setting one or more holidays during which the cheek-in or check-out is invalid.

It is supported to clear schedule record of the shift group on current day or later.

It is supported to check all shift schedules and search shift schedules according to the conditions.



- **Attendance Adjustment Management**

  The adjustment reason can be configured. It is supported to apply for, edit, delete, cancel, search and export the attendance adjustment form.

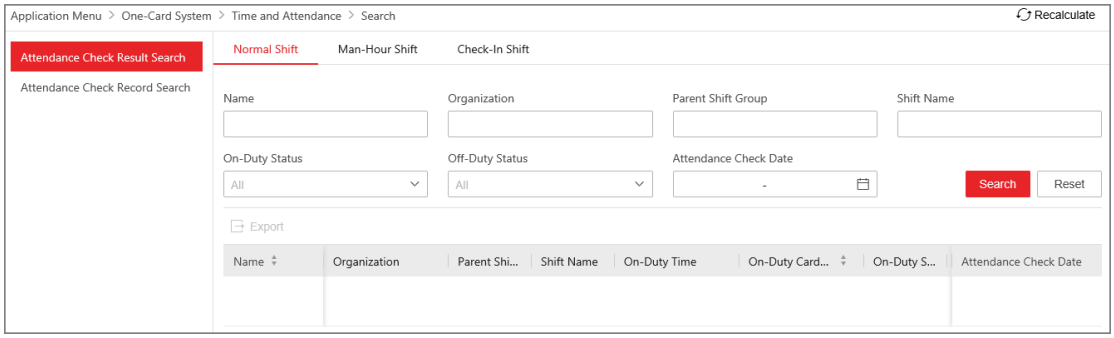
- **Attendance Check Point Management**

  It is supported to set the access control points as attendance points, and set the validity period and type of the attendance points, so that different attendance points can be used for different attendance scenes.

Statistics Analysis

- **Information Search**

  It is supported to search and export the attendance check results, manually calculate the attendance data, search and export the check records.



➢ **Statistics and Reports**

It is supported to search and export the person attendance report, and search and export the organization attendance report.

4.4 Integrated Control

The Integrated Control module, which provides rich linkages of functions and integrated applications, can be used for the monitoring, search, and check of events, monitoring on e-map, as well as smart applications based on facial recognition.

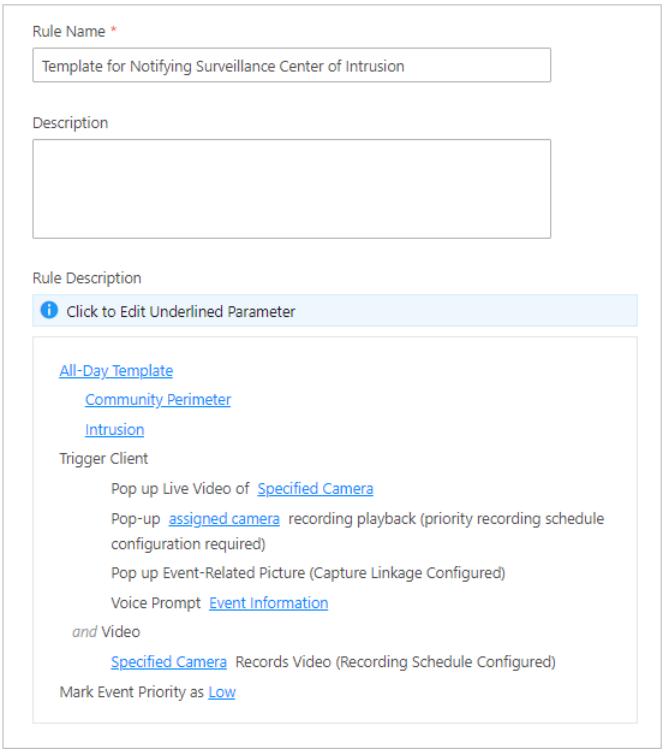
4.4.1 Event Linkage

Event is the signal sent by resources (e.g., cameras) when something occurs. You can configure an event rule to define an event that calls the alertness of the security personnel. The rule includes linkage actions (such as popping up event-related video on the Control Client and Mobile Client) for the detected events. After the rule being configured when an event is detected, the system will trigger linkage actions and send the information of the event as alarm to the Control Client and the Mobile Client. The security personnel can check the alarm details via one of the two Clients and handle the particular situation of the event. This function is used in scenes like campus, enterprises, and communities to ensure security.

Configure Event Parameters

Supports configuring schedule template for events, including all-day template, workday template, and weekend template, and you can set one of them as default. Meanwhile, you can add a customized template. The platform also supports existing event rules. When you are adding an event rule, you can add by template or customize one.
Supporting configuring event parameters including event type, priority, time, area, source, location, etc.
Various event types are supported, for example, intrusion alarm, access control alarm,

parking alarm, and so on. Meanwhile, the platform supports configuring multiple linkage actions for the events, such as pop-up live view/playback/captured picture. And you can download the recorded videos triggered by events.
After configuring event rule, you can search them by rule name, description, and status, and enable/disable the rules.
Supports setting event retention time after which the event will be cleared automatically.
You can test the event to pre-view the linkage actions.



Event Linkage

Event linkage can send notifications to security persons when an event happens, so that they can respond to the event quickly. Evet linkages include recording, capturing, two-way audio, messages, and emails.
You can search events by area, location, source, time, priority, etc., and display search results by event type and event rule name.
When an event is triggered, you can view event details, e.g. live view, playback, captured pictures, and add note for the event.
You can save the searched events to the local computer.
The Control Client also supports searching events in the above-mentioned way, and supports acknowledging one or more alarms, marking events, enabling/disabling functions like sound notification and pop-up window.

4.4.2 Map

After configuring the map via Web Client, you can view the live view and playback of the

resources added to the map, and get a notification message from the map when the alarm is triggered.

Map Configuration

Two types of map are available: GIS map and static map. On the GIS map, you can set and view the hot spot and element's geographic location. On the static map, you can set the view the locations of the installed cameras, alarm inputs, alarm outputs, etc.
Supports dragging resources added to the map to move them, deleting resources on the map, alignment of resources on the map.
Supports adding/editing/deleting a hot region on the map, clearing/editing configurations of the map, copy a static map of an area to another area, and switching static map.
Cameras configured longitude and latitude will be shown on the map automatically.
Supports setting data source and API URL for a GIS map, and configuring offline map.

Resource Monitoring

Supports selecting multiple cameras on the map to start live view/playback of the selected cameras, adding label for a location on the map, measuring distance or area on the map, selecting resources you want to display on the map. Or you can just double-click a camera to start live view.
You can add/delete/edit a label for a location on the map, and add a remark.
Supports marking camera icons by different colors to indicate their status.
For GIS map, you can search a camera or location on the map to view its details.
You can also select which resource type to display on the map.
For key resources on the map, you can add them to the Favorites so that you can view them quickly next time.
You can locate alarm to show its source and location on the map, display hot spot name on the map, open a hot region by clicking its icon on the map, and switch map type.
When a camera triggers an alarm, it will be displayed at the center of the map for attention.

View Real-Time Alarm

You can view the triggered alarm information of the hot spot on the map in real time or search history alarm information including alarm time, alarm location, captured alarm picture, etc. You can also add your suggestion on how to process the alarm event.

Play Driving Pattern

You can search and view the history driving pattern of the vehicle installed with mobile devices (such as mobile DVR, PVR, etc.) in the specified time period. During the driving pattern playback, you can set the playing speed, measure the distance between two points, and enable playback in the middle of the screen.

Supports marking interval after selecting time in the drop-down list to mark the distance by time on the driving pattern, and enabling centered playback to fix the driving pattern being played back in the middle of the screen.

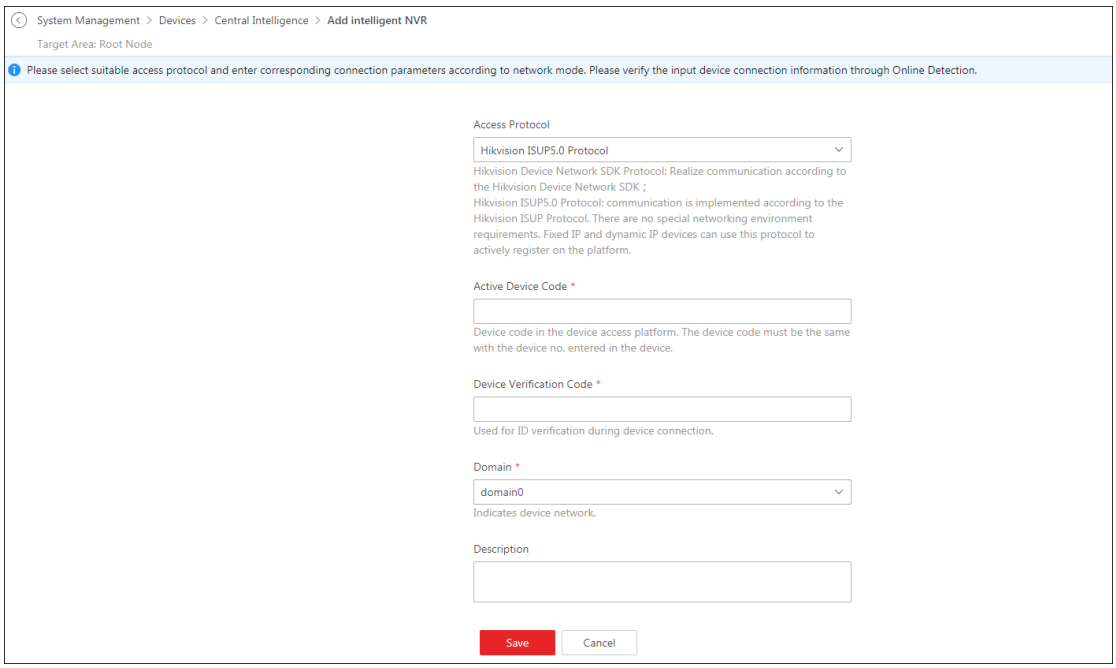
4.4.3 Facial Surveillance

Facial surveillance provides face capture, analysis, and retrieval via the facial recognition devices (such as capture cameras) and facial analysis servers (such as intelligent NVRs), based on the facial recognition technology. It supports auto-recognizing the faces appeared in the video image, capture, as well as management, retrieval, and arming by different face groups.
Supported devices: capture cameras, face comparison cameras, facial recognition server, DeepinMind NVR, etc.

- **Face Capture Camera:** Supports detecting moving faces as well as tracking, capture, grading, filtering, and then giving the best captured faces to users.
- **Facial Comparison Camera:** Supports face capture (detecting moving faces as well as tracking, capture, grading, filtering, and then giving the best captured faces to users) and facial recognition (comparing the captured faces with the faces in the face group in real-time, and then trigger an alarm if the captured face matches the one in the face group).
- **Facial Recognition Server:** Including pure analysis and stand-alone facial recognition server. Supports face capture, facial comparison, and face retrieval.
- **DeepinMind NVR:** Intelligent NVR. Supports face capture, facial comparison, and face retrieval.

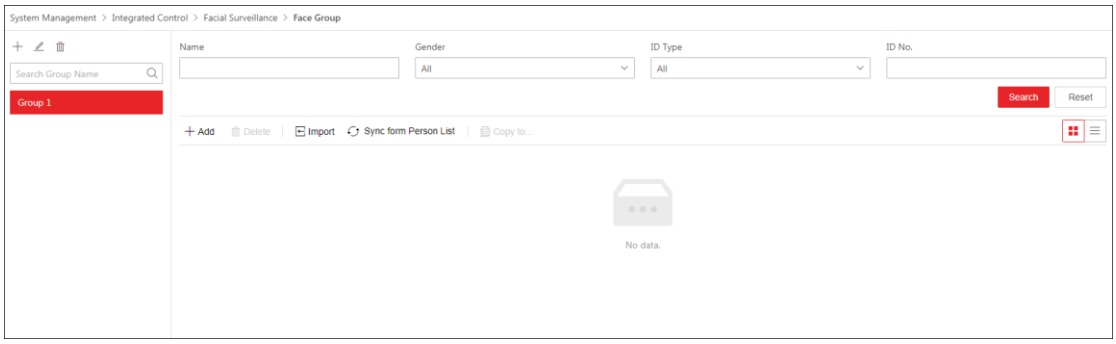
Facial Surveillance Configuration

- **Device Management**
  1. Supports adding, editing, and deleting devices of different models for facial recognition servers and DeepinMind NVRs.
  2. Supports testing the online status of the devices.
  3. Supports adding DeepinMind (DS-8632N-I8) via ISUP 5.0 protocol.



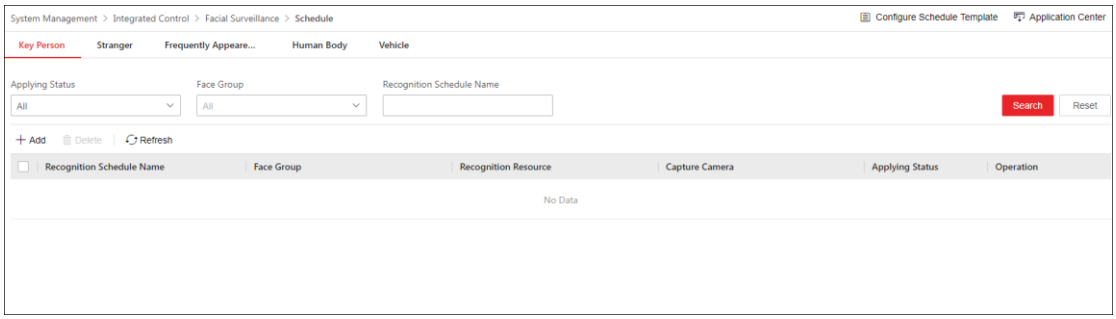
➢ **Face Group Management**

1. Supports adding, editing, and deleting face groups.
2. Supports adding face pictures to face groups and setting basic information (name, gender, and ID number). Supports adding face pictures one by one, importing by a package, synchronization from person list, and copying from other groups.
3. Supports editing and deleting the added face information.
4. Displaying faces in the face group by list or thumbnail.
5. Supports searching faces by name, gender, and ID type.



➢ **Recognition Schedule Settings**

1. Supports setting recognition schedule for the key persons, strangers, and frequently appeared persons



2. Supports applying key person recognition schedules to devices (DeepinView cameras, DeepinMind NVRs, stand-alone facial recognition servers, and pure analysis facial recognition servers). After setting the recognition schedule, the schedule can be applied to the devices automatically and you can view the applying details.
3. Supports applying stranger recognition schedules to devices (DeepinView cameras and pure analysis facial recognition servers). After setting the recognition schedule, the schedule can be applied to the devices automatically and you can view the applying details.
4. Supports applying frequently appeared person recognition schedules to devices (DeepinMind NVRs). After setting the recognition schedule, the schedule can be applied to the devices automatically and you can view the applying details.
5. Supports exporting the applying records of all the recognition schedules.
6. Supports applying the recognition schedules to the device again.
7. Supports setting face similarity threshold of the related face group.
8. Supports enabling and disabling configured recognition schedule.
9. Filtering recognition schedules by status, face group, and schedule name.

- **Parameter Configuration**
  1. Setting storage location of face pictures in the face groups and the captured faces.
  2. Set the retention period of the capture and recognition records, including key person recognition records, stranger recognition records, capture records, and frequently appeared person recognition records. You can set the retention period as 1 month, 3 months, 6 months, 9 months, 12 months, 18 months, 24 months, 30 months, and 36 months.
  3. Set receiving face capture events or not.

Real-Time Recognition

1. Supports displaying recognized faces on the Control Client in real-time.
2. When receiving a face capture event, the captured picture and recognized information will be displayed in real-time.
3. Supports viewing the person information, original picture, person's moving pattern, recorded video footage, etc.
4. Supports filtering real-time recognition records by event type (all events, key person recognition events, stranger recognition events, and frequently appeared person events).
5. Support filtering real-time recognition records by face groups.
6. Supports locking the current recognition details and the latest event will not show until unlocked.

Key Person Recognition

1. Supports checking the recognition results of key persons of different groups or all groups.
2. Supports viewing in list mode or thumbnail mode.
3. Supports filtering recognition results by start time, end time, capture camera, similarity, age group, gender, ID number, wearing glasses or not, etc.
4. Sorting the recognition results by similarity.
5. Sorting the recognition results by time.
6. Supports viewing the person information, original picture, person's moving pattern, recorded video footage, etc.
7. When viewing person's moving pattern, supports searching specified pattern by start time, end time, and similarity.
8. Supports downloading captured pictures, original captured pictures, and face pictures to your local PC.

Stranger Recognition

1. Supports viewing in list mode or thumbnail mode.
2. Supports filtering recognition results by start time, end time, capture camera, age group, gender, ID number, wearing glasses or not, etc.
3. Supports view the stranger information, original picture, person's moving pattern, recorded video footage, etc.
4. When viewing stranger's information, supports checking her/his appeared times within the latest three days.
5. When viewing stranger's moving pattern, supports searching specified pattern by start time, end time, and similarity.
6. Supports downloading captured pictures to your local PC.
7. Supports adding the captured face picture to the specified face group.

Frequently Appeared Person Recognition

1. Supports checking the recognition results of frequently appeared persons.
2. Supports viewing in list mode or thumbnail mode.
3. Supports filtering recognition results by start time, end time, capture camera, and appeared times.
4. Sorting the recognition results by time.
5. Sorting the recognition results by similarity.
6. Supports view the person information, captured picture, appeared times, etc.
7. When viewing person's moving pattern.
8. Supports exporting recognition records and captured pictures.
9. Supports downloading captured pictures to your local PC.

10. Supports adding the captured face picture to the specified face group.

Search History Capture Records

1. Supports filtering capture records by start time, end time, capture camera, similarity, age group, gender, ID number, wearing glasses or not, etc.
2. Supports display records in list mode or thumbnail mode.
9. Supports viewing person information, original picture, person's moving pattern, recorded video footage, etc.
10. Supports checking her/his appeared times within the latest three days.
11. When viewing person's moving pattern, supports searching specified pattern by start time, end time, and similarity.

Search Face by Face Picture

1. Supports searching faces by uploading a face picture of the target person.
2. Supports uploading a picture of one face or multiple faces for search. If you upload one picture with multiple faces, the system will generate multiple pictures with these faces separately. You can select the target face in the analysis result for search.
3. Supports filtering results by start time, end time, capture camera, and similarity.
4. Supports searching person's moving pattern in the search result.
5. Supports checking search results in list or thumbnail mode.
6. Supports viewing the recorded video of the search result.
7. Set the search result as condition for secondary search.

4.5 Vehicle Control

HikCentral Enterprise-Commercial provides parking control for small lots as well as large, complex parking systems. It allows users to register vehicles to the system, set entry and exit rules, control entry & exit, etc., for parking facilities, shopping centers, airports, hotels, arenas, etc.

4.5.1 Parking

The parking system provides barrier control of the configured entrance and exit. The real-time vehicle passing records will display and you can view the vehicle details like license plate number, card number. With the guidance component, you can find your car in the parking lot quickly.

Vehicle Group

The platform supports the following functions:

1. Adding/editing/deleting/importing/exporting permanent vehicles;
2. Adding/editing/deleting/importing/exporting vehicle groups;
3. Adding/editing/deleting/importing/exporting vehicle blacklist;
4. Adding/editing/deleting/importing/exporting temporary vehicles.

Reservation

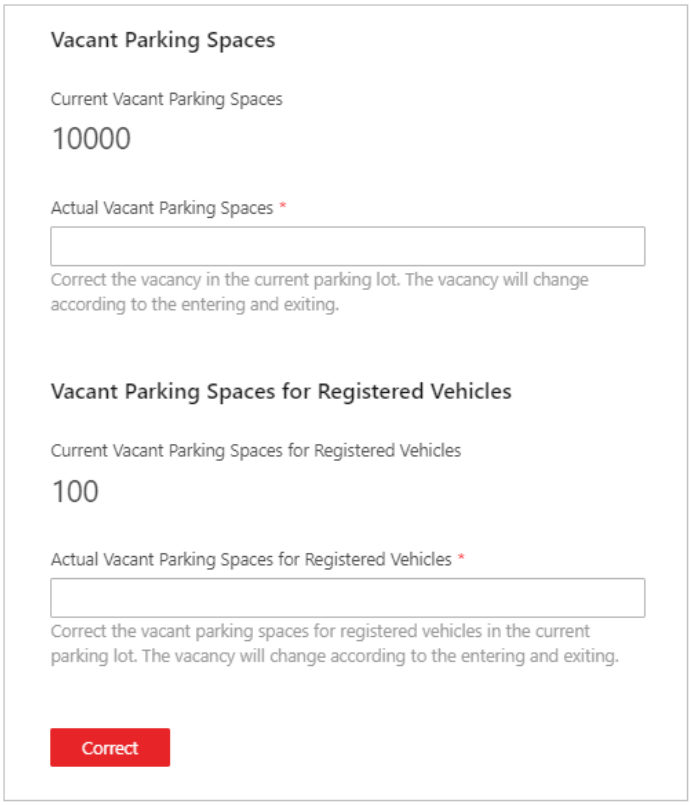
The platform supports the following functions:

1. Reserving a parking space and cancelling reservation;
2. Selecting the entry times;

Parking Space Management

The parking lot supports the following functions:

1. Correction of total vacant parking spaces and vacant parking spaces for registered vehicles.
2. Linkage between a vehicle license plate number and parking space type.
3. Displaying parking space occupation.
4. Alarm of illegal parking space occupation.



Information Query

1. The parking system supports searching vehicle's passing records, vehicles that are in

the parking lot currently, parking records, and reservation records.
2. Vehicle's passing records can be searched by parking lot name, entrance/exit name, passing direction, allowed or not, vehicle type, vehicles in blacklist, etc.
3. You can display the search results in list or picture, and export the passing vehicles' picture.
4. You can search vehicles in the parking lot currently by entering time and parking duration. After searching, you can correct license plate number and delete the parking records.
5. You can search parking records by license plate number, parking space number, floor, parking lot name, and entry/exit time, and display the search result in list or picture.
6. You can search reservation records by license plate number, mobile phone number, parking lot, and reservation type.
7. Support generating traffic flow report by parking lot name, parking time, vehicle type, vehicle category, and vehicle group, and exporting the generated report.

Manage Advertisements

Supports uploading a poster to the system and release it for advertisement and setting the display interval of the released advertisement.

Control Client

In the Parking Lot Module of the Control Client, you can perform the following functions:
1. View the real-time passing vehicle records.
2. Control barriers at the entrance or exit.
3. Perform two-way audio.
4. Deal with exit exceptions (including license plate number correction, manually matching, abnormal allowing, and manually opening barriers).
5. View vacant parking spaces and occupied parking spaces.
6. For dedicated parking spaces, you can configure occupation alarms and clear the alarms when they are triggered.

4.5.2 Campus Checkpoint

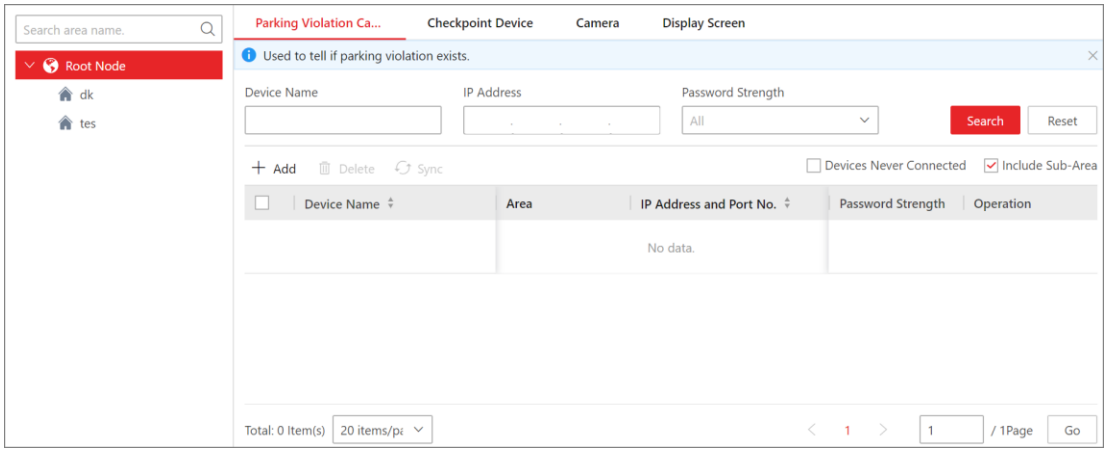
The Checkpoint module provides functionality including vehicle speed measurement, blacklist vehicle arming, whitelist management, driving pattern, etc., based on checkpoint device management and related configurations. It also supports searching passing vehicle records, violation events, and the statistics of traffic flow and violation events of specific checkpoints.

Checkpoint Configuration

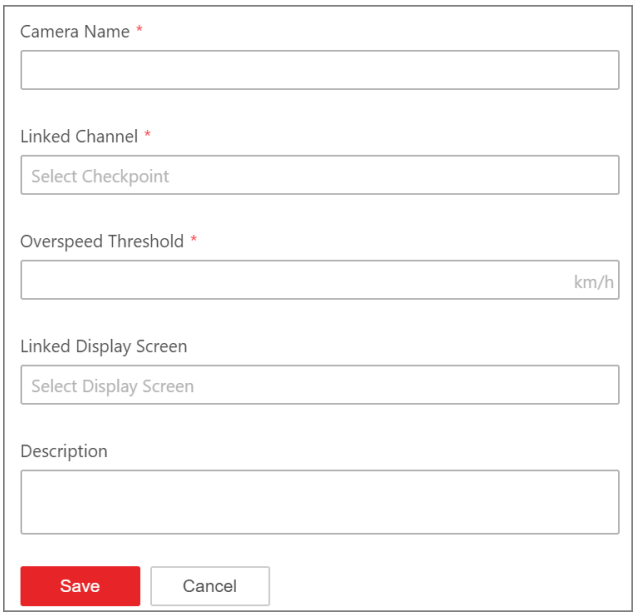
1. It is supported to manage checkpoint devices and display screens.
2. It is supported to add parking violation camera and checkpoint by Hikvision Device

Network SDK Protocol and test if the device information is correct.

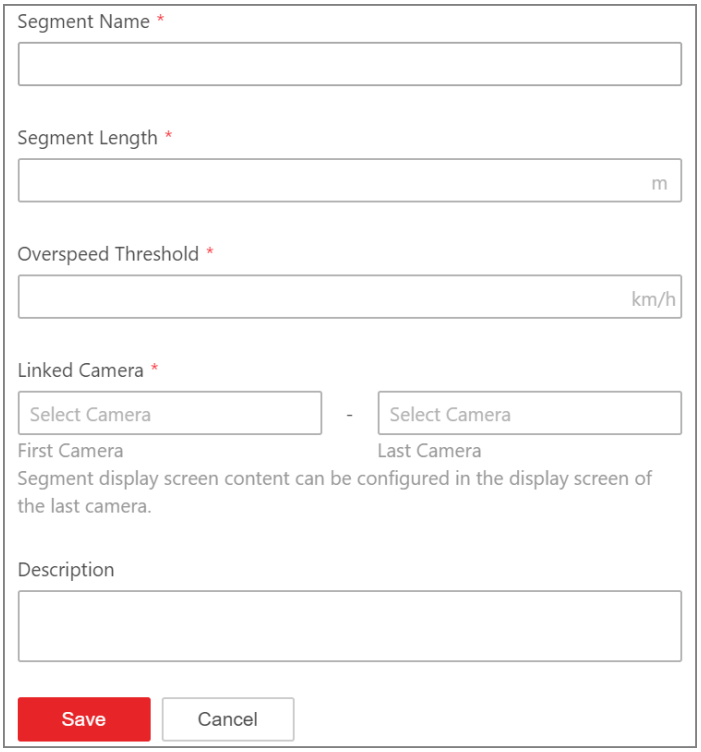
3. It is supported to add, edit and delete traffic camera.



4. It is supported to add display screen, configure display contents and text color, and test if the device information is correct.
5. The speed measurement of single checkpoint is supported and the overspeed threshold needs to be configured.
6. The overspeed information can be displayed on display screen.



7. The speed measurement of segment is supported, and segment length and overspeed threshold needs to be configured.
8. The overspeed information of segment can be displayed on display screen.



- **Vehicle Violation Configuration**
  1. You can enable violated vehicle management rule and set allowed violation times (1 to 50) and period interval (1 month to 12 months).
  2. If the violation times of a vehicle exceeds the upper limit, it will be added to the blacklist. The entrance and exit can limit the vehicle passing, and the information reminder can be displayed on display screen.
- **Parameter Configuration**
  1. It is supported to configure picture storage location.
  2. It is supported to configure capture record retention duration.
  3. The central storage (Hybrid Storage Area Network and cloud storage) is supported for storing captured vehicle pictures.

Vehicle Arming Control

1. It is supported to add vehicles to blacklist for arming them. The arming reasons include stolen vehicle, robbed vehicle, suspect vehicle, illegal vehicle, emergently controlled vehicle, and rule-violated vehicle.
2. It is supported for managing whitelist, which cannot be armed by any checkpoint.

Event Search

1. The capture events can be searched by license plate No., vehicle type, event source (checkpoint), license plate type, vehicle speed, start time and end time. The records and captured pictures can be exported in a batch. You can view the search results by list mode or thumbnail mode.
2. The violation events can be searched by license plate No., violation type, event source

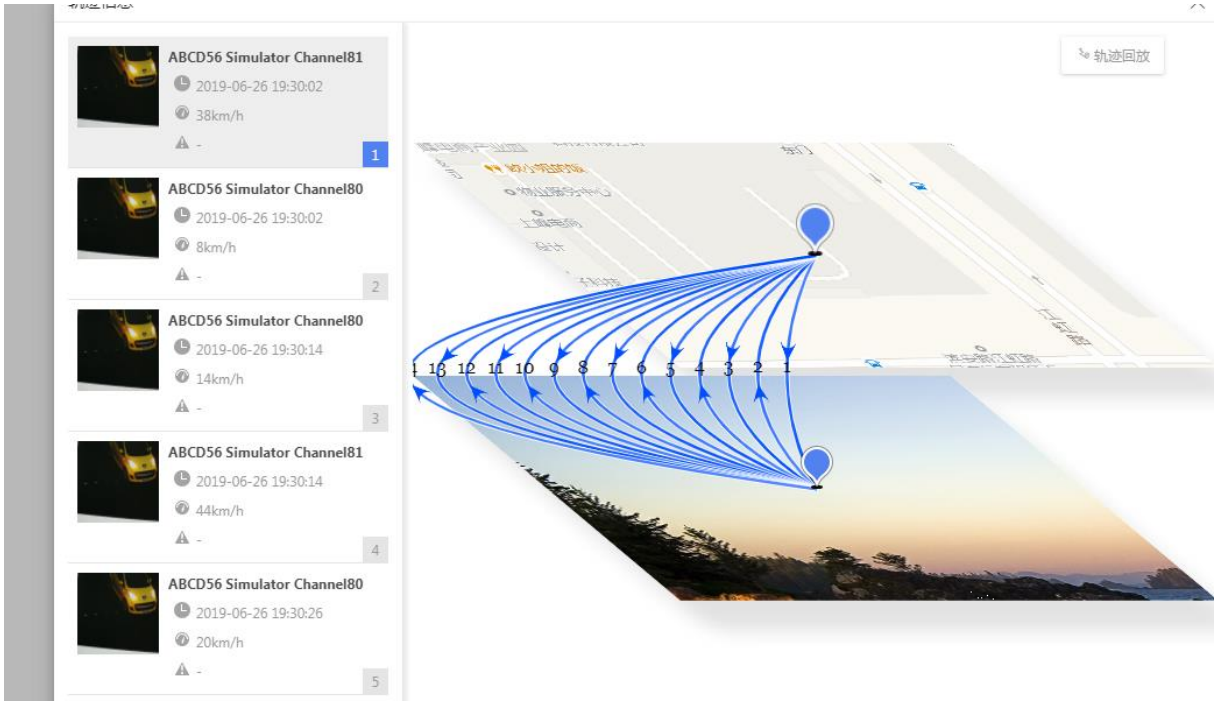
(checkpoint), speed detection type (camera speed detection or segment speed detection), arming reason, start time and end time. The records and captured pictures can be exported in a batch. You can view the search results by list mode or thumbnail mode. The event-related video can be displayed to verify the situation at that time.

Statistics and Reports

1. The traffic follow report can help the user to check traffic flow information.
2. The total traffic flow can be calculated according to time (default or custom) and checkpoint. You can export the traffic flow report.
3. The violation report can help the user to check vehicle violation information.
4. The different types of violation events can be calculated according to time (default or custom) and checkpoint. You can export the violation report.

Pattern Information

1. The driving pattern information can be searched by license plate No., area (single area or cross-area), and time.
2. The search results show the checkpoint name, vehicle speed, time and captured pictures.



4.6 Alarm Detection

4.6.1 Intrusion Alarm

Intrusion Alarm Configuration

1. The platform supports managing and configuring intrusion alarm devices. You can add security control panel to the selected area.
2. The platform supports the following security control panels: Hikvision network security control panel, Hikvision video security control panel, Hikvision bus network security control panel, Honeywell CK23 series, Honeywell security control panel and Bosch DS7400 security control panel. Hikvision devices can be accessed to the platform through Hikvision SDK network protocol and MTA protocol. The third-party devices can be accessed to the platform through MTA protocol.
3. Supports getting the online device information, moving, deleting device, editing device information, and viewing device details.
4. Supports managing alarm outputs of the security control panel.
5. Supports linking zones for alarm partition and moving zones to other areas.

Intrusion Alarm Applications

1. The Control Client and the platform supports filtering partitions according to their names and status. The Control Client supports arming/disarming/clearing alarm of the partition. You can also arm/disarm all the partitions.
2. The Control Client supports filtering zones according to their names and status. Supports receiving the real-time intrusion alarm events. Supports arming/disarming the zone. Supports bypass, bypass recovery, etc.
3. The platform supports searching and exporting history alarm events by event source, start and end time, event type, event priority, etc.

4.6.2 Panic Alarm

Panic Alarm Configuration

1. The platform supports managing and configuring panic alarm devices. You can add panic alarm devices to the selected area.
2. The following panic alarm devices can be accessed to the platform through SDK protocol, including panic alarm station, box panic alarm station, and pole panic alarm station.

3. Supports adding devices in a batch. You can view the progress during batch adding devices. After adding devices, you can select to save settings directly or save settings after testing if the device information is correct.

Panic Alarm Applications

1. The platform supports searching and exporting the history panic alarm events according to time, event source and event type.
2. Supports configuring linkage actions for panic alarm events. Supports linking devices to view live view, two-way audio, turn on/off alarm lights for box panic alarm station, etc.

4.7 Resource Maintenance

The Maintenance module provides functionality for checking the health status of the video resources and one-card resources. For video resources, the resource running status, recording status, and image quality can be checked; For one-card resources, the running status of the one-card resources can be checked. This allows the maintenance personnel to monitor the health status of the video resources and one-card resources in a visualized, controllable, and manageable way, thus helping the maintenance personnel locate and handle faults. In this way, the stability and reliability of video surveillance system and one-card system can be achieved.

4.7.1 Maintenance Configuration

Health Monitoring Schedule

The user can set health monitoring schedules based on his or her needs to define the time and frequency for checking the health status of the resources added to the platform. Customizing health monitoring schedule is supported. The customization of health monitoring schedule includes the customization of the target for health monitoring (encoding device status, camera status, CVR status, NVR status, cloud storage status, decoding device status, access control device status, smart lock gateway status, video intercom device status, video loss, video retention days, video quality, video decoding, and cascaded camera status), editing of schedule name, configuration of checking type, time template for checking, as well as configuration of the interval for checking (5 minutes, 10 minutes, 15 minutes, 30 minutes, 1 hour, or 24 hours); The configuration of time template is also supported: the user can select the platform-provided templates, or customize an template.
The user can enable, disable, delete the health monitoring schedule(s). The user can also filter health monitoring schedules by checking type or whether the schedule(s) are enabled

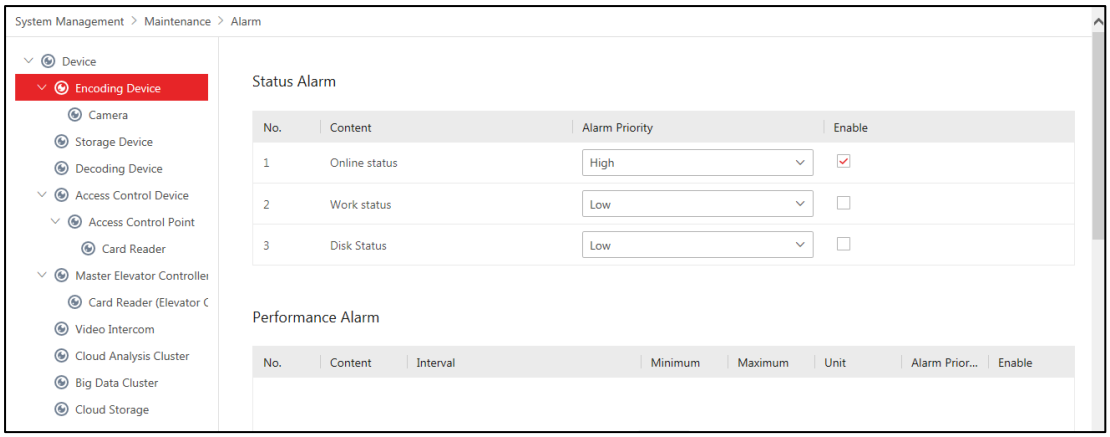
or not. Only the disabled schedule(s) can be deleted.

Status Alarm Configuration

The user can configure the threshold of triggering a status alarm and the alarm level (prompt, warning, low, medium, high) for encoding device, camera, access control device, access control point, card reader, elevator control device, card reader linked to elevator control device, video intercom device, storage device, decoding device, and cloud storage device.

The supported alarm types for each type of devices are as follows:

1. Encoding device: online status, work status, and HDD status.
2. Camera: online status, video loss, video quality diagnostics, hardware status, video retention days, main stream frame rate, sub-stream frame rate.
3. Access control device: online status, interconnecting cable status, IR adapter status, IR sending board status, master lane controller status, slave lane controller status, fire input status, motor sensor status, dismantling status, etc.
4. Access control point: door lock work status.
5. Card reader: online status, tampering status
6. Elevator control device: online status
7. Card reader linked to elevator control device: online status.
8. Video intercom device: online status
9. Storage device: online status, work status, disk status.
10. Decoding device: online status, work status.
11. Cloud storage: online status, disk status, storage volume status.



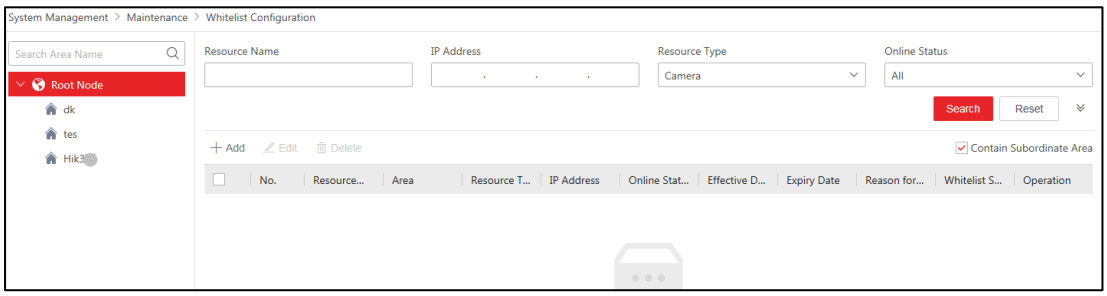
Subordinate Platform Management

The user can add subordinate platforms so as to get the data of camera status, video loss and VQD of the subordinate platform on the current level platform. The cascading cameras support self-cascading or obtaining status information from NCG.

Self-cascading is used when the current level platform and the subordinate platform are both HikCentral Enterprise-Commercial platforms. If one of them is not HikCentral Enterprise-Commercial platform, status information can only be obtained from NCG.
The supported subordinate platforms include video status maintenance platform and 9300 operating and maintenance platform.

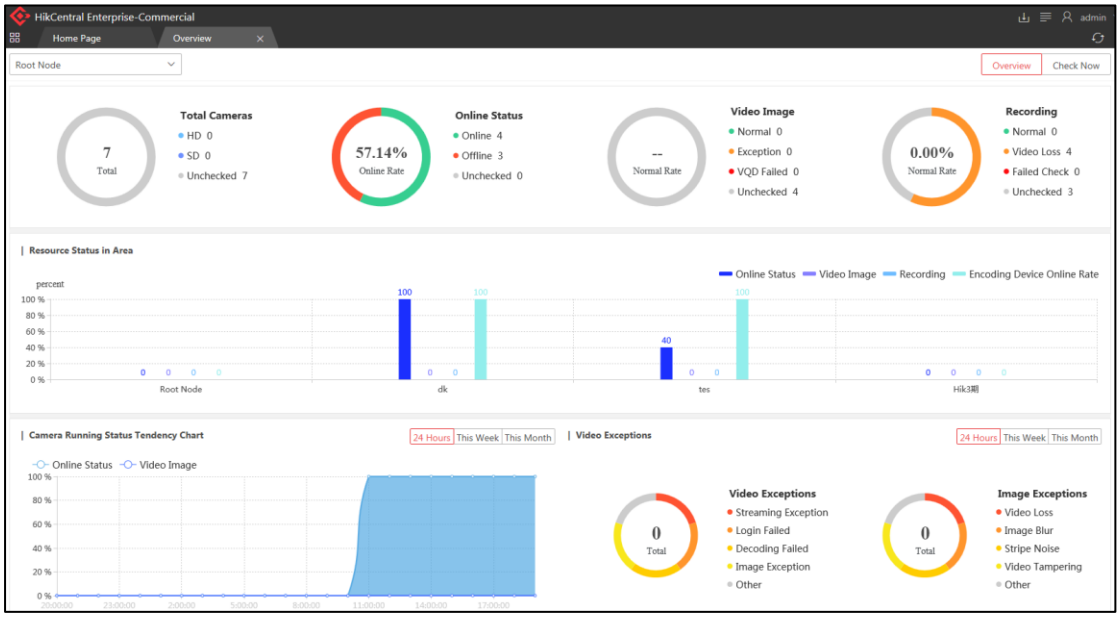
Whitelist Configuration

The resources can be added to the whitelist for special reasons including municipal construction, special device (PVR, MVR), power outage, network outage, device exception, or other custom reasons. This ensures that alarms will not be triggered during special cases such as the case when device exception occurs. The device types include encoding device, camera, storage device, decoding device, access control device, access control point, card reader, elevator control device, video intercom, cloud storage, cloud storage node, cloud storage disk, and storage volume of cloud storage.



4.7.2 Maintenance Overview

The user can get at-a-glance view of the overview of the camera running status (including total camera amount, camera online status, video image normal rate, and recording status) from charts.

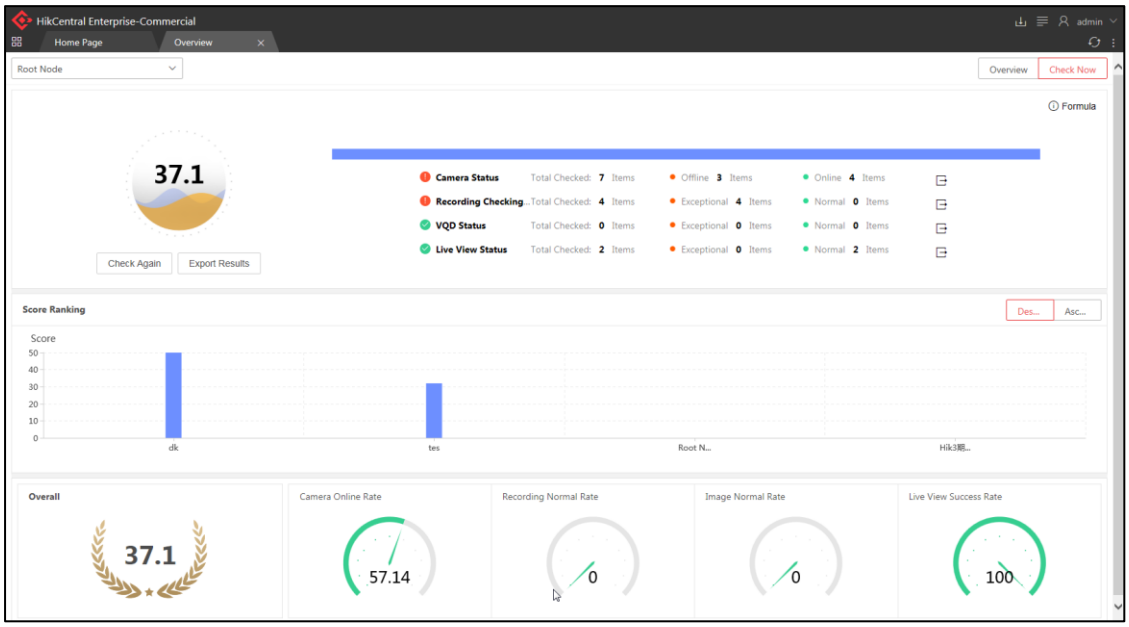


1. The Total Amount chart at the top displays the total camera amount, HD camera amount, SD camera amount, and unchecked camera amount using different colors; Viewing data details is also supported.
2. The Online Rate chart at the top displays the online camera amount, offline camera amount, unchecked camera amount, as well as the camera online rate using different colors; Viewing the data details is also supported.
   Note: ***Camera Online Rate = Online Camera Amount / (Online Camera Amount + Offline Camera Amount)***
3. The Video Image chart displays the amount of cameras whose images are normal, the amount of cameras whose images are abnormal, the amount of cameras whose VQD failed, and unchecked camera amount by different colors, and calculates the video image normal rate using the above-mentioned data.
   Note: ***Video Image Normal Rate = Amount of Cameras whose Images Are Normal / (Amount of Cameras whose Images are normal + Amount of Cameras whose Images are Abnormal + Amount of Cameras whose VQD failed).***
4. The Recording chart displays the amount of cameras whose video recording status are normal, the amount of cameras whose video recording status are abnormal (video losses occur), the amount of cameras whose health monitoring failed, and the amount of unchecked cameras using different colors. Viewing the data details is also supported.
   Note: ***Recording Normal Rate = Amount of Cameras whose recording are Normal / (Amount of Cameras whose recording are Abnormal + Amount of Cameras whose recording are Abnormal + Amount of Cameras whose health monitoring failed).***
5. The platform also supports statistics of the resource running status in a specific area. Viewing the data details is also supported.
6. Filtering statistics results by area is supported.
7. Statistics of camera resolution, camera online rate, image normal rate, and recording normal rate is supported. Viewing data details is supported.
8. The user can rank areas by camera resolution, camera online rate, image normal rate, recording normal rate, and encoding device online rate; Viewing data details and data search are also supported.
9. The user can also view the fluctuation trends of the camera online rate and image normal rate in recent 24 hours, recent week, and recent month.
10. Statistics of video/image exceptions in recent 24 hours, recent week, recent month is supported. Viewing data details and data search are also supported.

4.7.3 One-Touch Maintenance

One-touch maintenance obtains resource status information from the database and displays the resource status information instantly.
Camera amount, decoding device amount, encoding device amount, storage device amount, recording-status-checked camera amount, video-quality-diagnosed camera amount are supported to be displayed. And the user can view the details of these data and export them out.

Filtering data by area is supported;
Scoring overall resource health status of a specific area by camera status, recording status, VQD results, and VOD status is supported;
Ranking areas by theirs scores of overall resource health status is supported;
Viewing the score information of a specific area is supported.



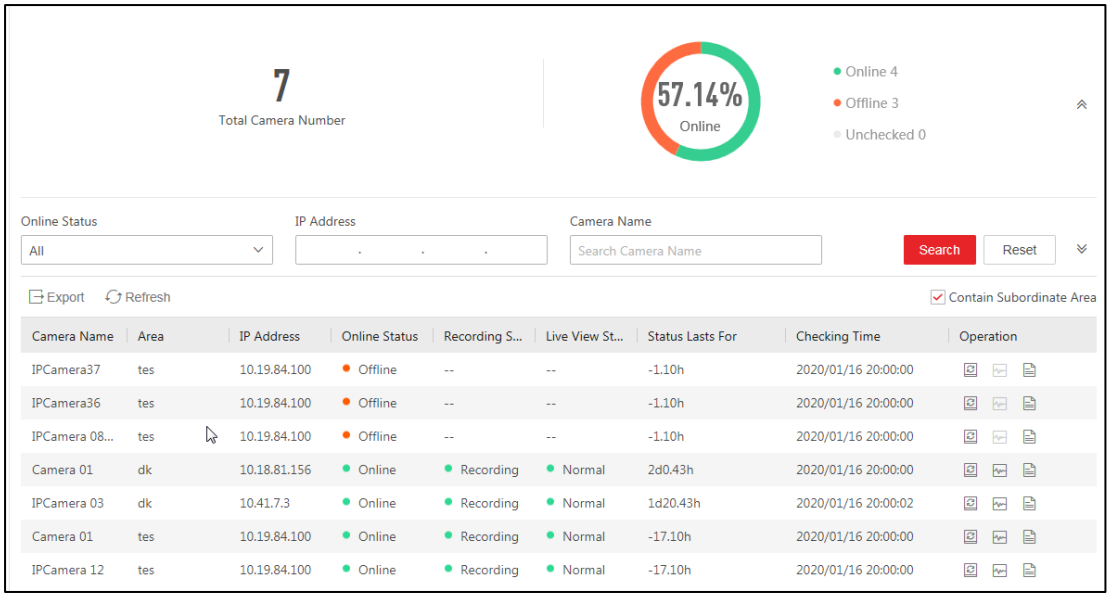
One-Touch Maintenance

4.7.4 Video Resource Status Monitoring

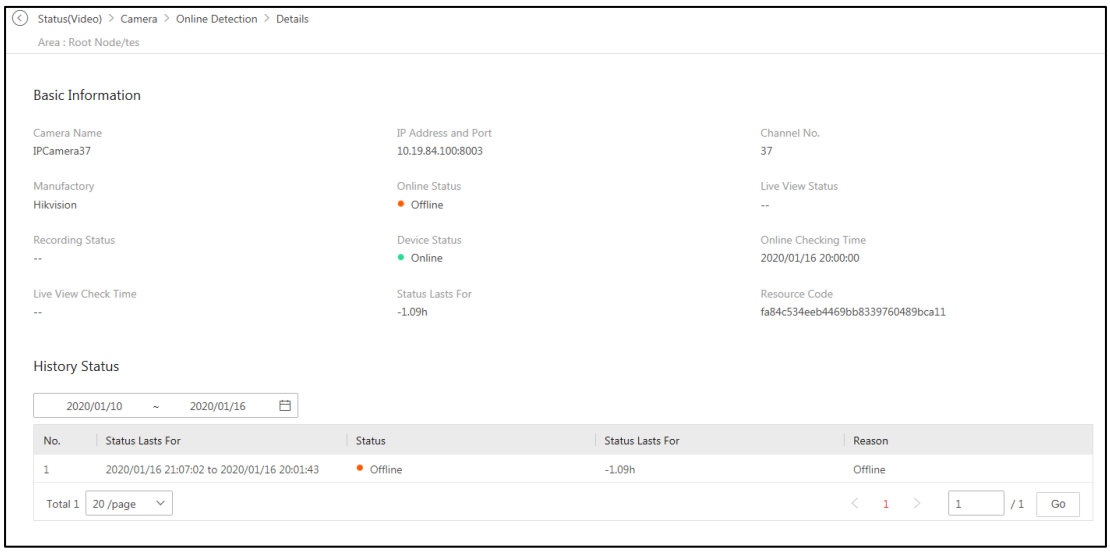
Video resource status monitoring refers to the checking of the online status of the cameras, encoding devices, and storage devices through the execution of health monitoring schedule and topology.

Camera Monitoring

- **Online Detection**
  1. Camera online status and other camera information can be displayed in chart and list.
  2. The Online chart displays offline camera amount, online camera amount, unchecked camera amount by different colors, and calculates the camera online rate using these data.
     ***Note:** Camera Online Rate = Online Camera Amount / (Online Camera Amount + Offline Camera Amount)*
  3. The list displays camera name, area, IP address, online status, recording status, live view status, and status lasting time, and the checked time.



4. The chart displays the total camera amount, online camera amount, offline camera amount, and unchecked camera amount. And the chart can be hidden.
5. The user can filter cameras by online status, IP address, recording status, live view status, camera name, resource source, and status lasting time;
6. The results of the online detection can be exported to the local PC as a CSV file.
7. The list data can be refreshed;
8. The user can view the camera details including basic information of the camera and its history status. The basic information includes camera name, area, IP address, port No., online status, VOD status, recording status, status of the device to which the camera is linked, manufacturer, resource code, channel No., and the checked time; The history status can be searched by time.
9. Camera streaming link diagnostics is supported.

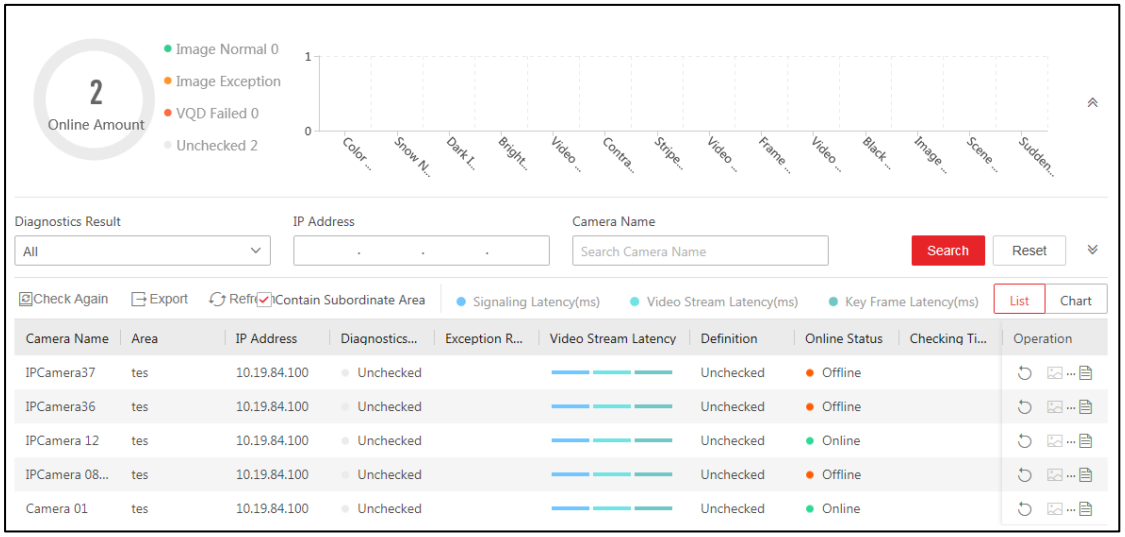


➢ **Video Quality Diagnosis**

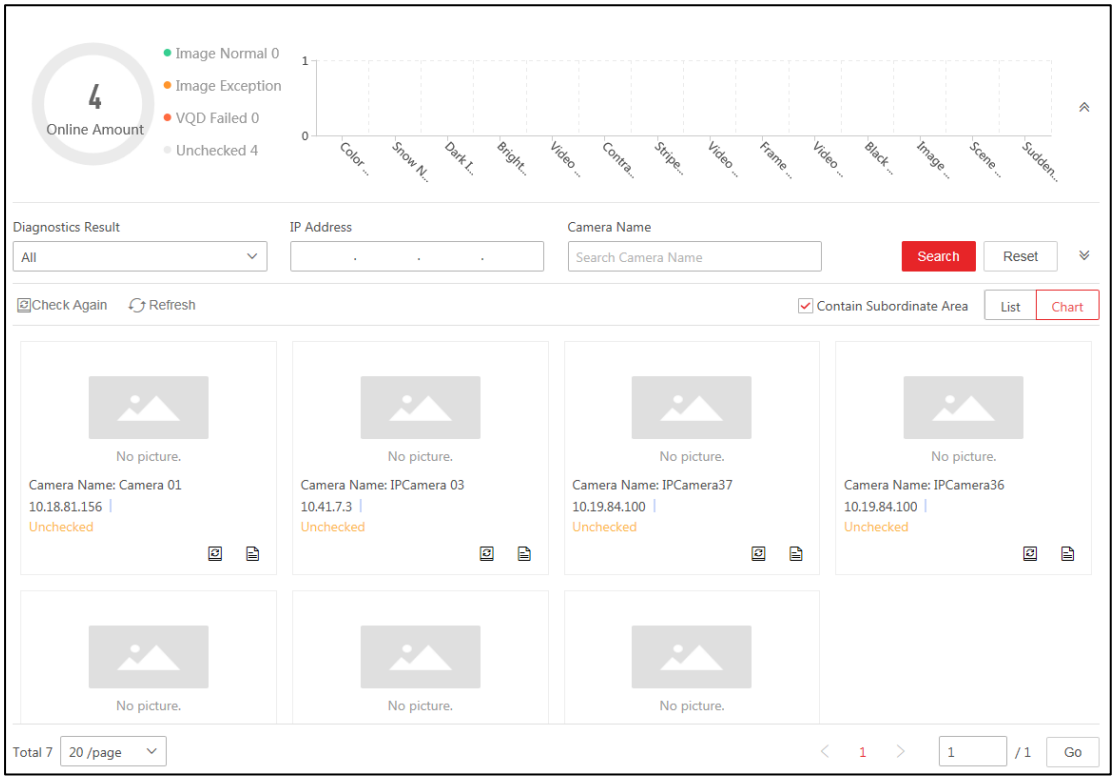
1. The platform can diagnose the image of the video resources added to it to determine the amounts of the video resources whose image quality is normal and

abnormal. Abnormal image status includes color cast, image noise, dark image, over bright image, image jittering, abnormal contrast, image stripes, image tampered, frame loss, signal loss, black and white image, blurred image, scene switching, sudden change of images.

2. The diagnosis results can be displayed in chart and list;
3. The histogram chart displays the total camera amount, the amount of the cameras whose images are normal, the amount of the cameras whose images are abnormal, the amount of cameras whose diagnosis failed, and the amount of the cameras which are not diagnosed.
4. The list displays camera name, area, device to which the camera is linked, camera IP address, camera online status, VQD results, exception item, video stream latency, definition, and the checked time;



5. The chart can be hidden. Once hidden, the page displays total camera amount, amount of the cameras whose images are normal, the amount of the cameras whose images are abnormal, the amount of the cameras whose VQD failed, and the unchecked camera amount.
6. The user can filter the diagnosis data by diagnosis result, IP address, camera name, exception item, online status, video stream definition, and video stream latency.
7. The VQD result of each camera can be displayed as thumbnails.



8. The user can select cameras and diagnose the selected cameras again instantly.
9. Checking the image quality of a single camera is also supported.
10. The VQD results can be exported to the local PC as a CSV file.
11. The user can also view the VQD related picture when checking the image details.
12. The user can view the camera basic information, the VQD related picture, and history diagnosis (displayed in calendar picture). The basic information includes area, camera name, IP address and Port No., manufacturer, diagnosis results, online status, status of the device to which the camera is linked, definition (with image width and height displayed), video checking time, online checking time, exception reason, and resource code.

➢ **Recording Check**

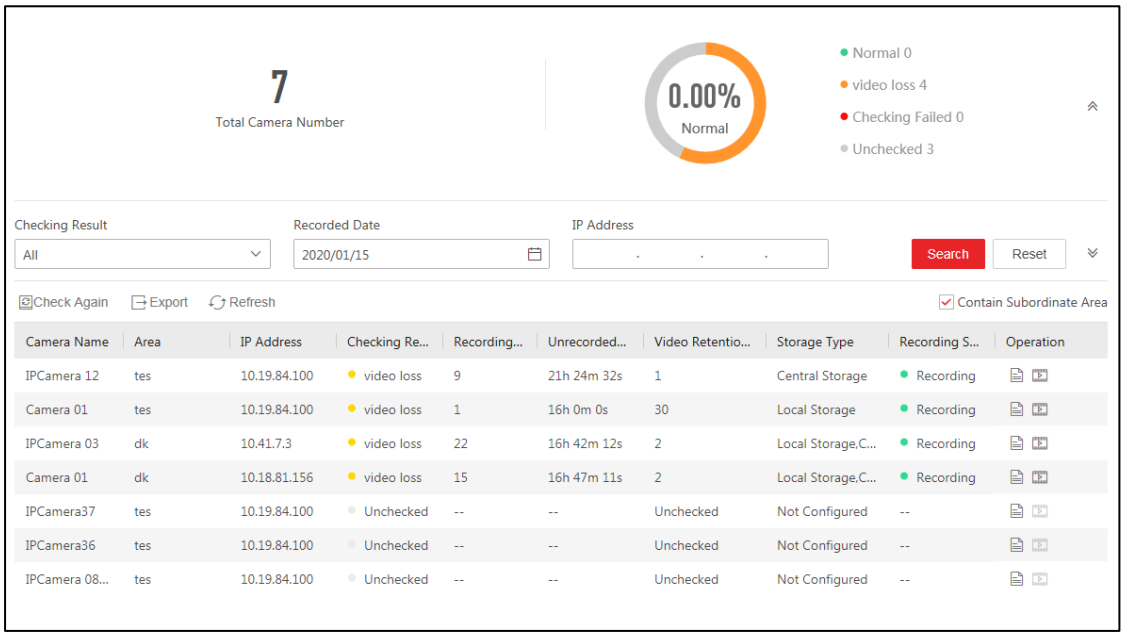
1. The user can check if video loss occurred in the previous day on the camera which has been configured with recording schedule.
2. The results can be displayed in chart and list.
3. The chart displays the total camera amount, the amount of cameras on which no video loss occurred, the amount of the cameras on which video loss occurred, the amount of cameras on which recording check failed, and the unchecked camera amount. The chart also displays the calculated recording normal rate.

   Notes:

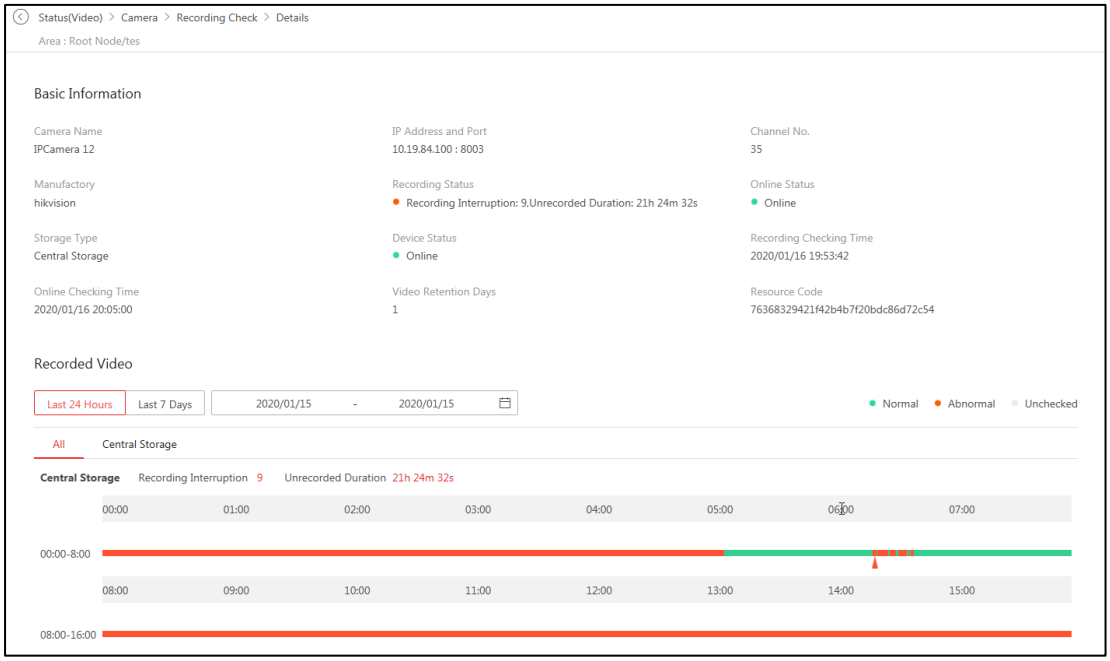
   - Recording Normal Rate = Amount of the Cameras on which No Video Loss Occurred / (Amount of the Cameras on which No Video Loss Occurred + Amount of the Cameras on which Video Loss Occurred)
   - If a camera has been configured with multiple storage types, the following rules shall prevail in determining if the recording status of the camera is normal.

- If no video loss occurred in any one type of the storages, the camera recording status is regarded as normal.
- If recording status is abnormal in all storage types, and video loss occurred, the camera recording status is regarded as abnormal (video loss exists).
- If neither normal nor abnormal recording status exists in all the storage types, but there're unchecked storage type(s), the camera recording status is regarded as unchecked.
- If the recording status check for all storage types failed, the camera recording status is regarded as check failed.

4. The list displays camera name, area, IP address, check results, recording interruption times, unrecorded duration, video retention days, storage type, and recording status.



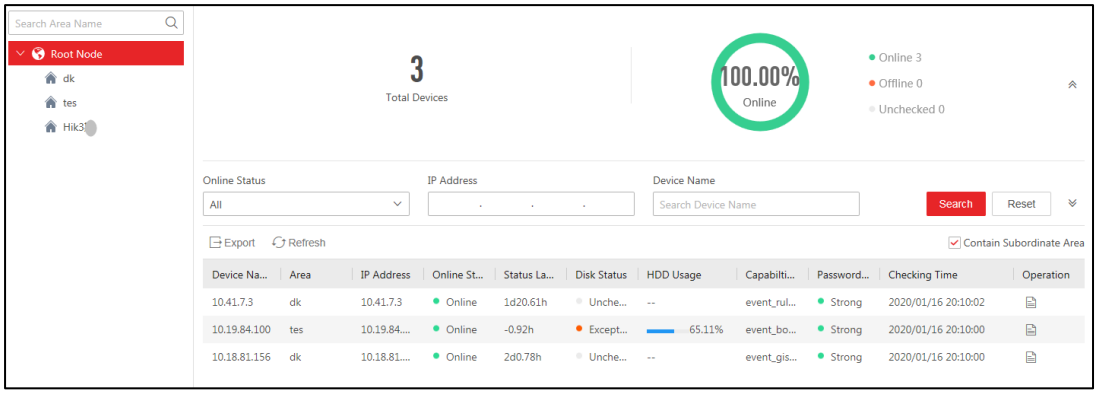
5. The chart can be hidden. Once hidden, the page displays the total camera amount, the amount of cameras on which no video loss occurred, the amount of the cameras on which video loss occurred, the amount of cameras on which recording check failed, and the unchecked camera amount.
6. The user can filter results by checking results, recorded date, camera name, IP address, recording status, and video retention days;
7. The results can be exported to the local PC as a CSV file.
8. The data displayed in the list can be refreshed;
9. The user can view the camera basic information and the recording status. The basic information includes area, camera name, IP address and port No., channel No., manufacturer, recording status, online status, storage type, the status of the device to which the camera is linked, video checking time, online checking time, video retention days, and resource code; The user can also select time period (latest 24 hours, latest 7 days or customized time period) or storage type for displaying the details of the history recording status
10. The recording status of the cascaded cameras can also be checked.



Device Monitoring

➢ **Encoding Device Status Monitoring**

1. The check results can be displayed in chart and list;
2. The chart displays the total device amount, online device amount, offline device amount, unchecked device amount, and the calculated device online rate.
   Note: Device Online Rate = Online Device Amount / (Online Device Amount + Offline Device Amount)
3. The list displays the device name, area, IP address, online status, status lasting time, disk status, disk usage, capability, password strength, and the checked time.



4. The chart can be hidden. Once hidden, the page displays the total device amount, online device amount, offline device amount, and unchecked camera amount.
5. The user can filter devices by device online status, IP address, disk status, capability, password strength, status lasting time.
6. The results can be exported to the local PC as a CSV file.
7. The data displayed in the list can be refreshed.

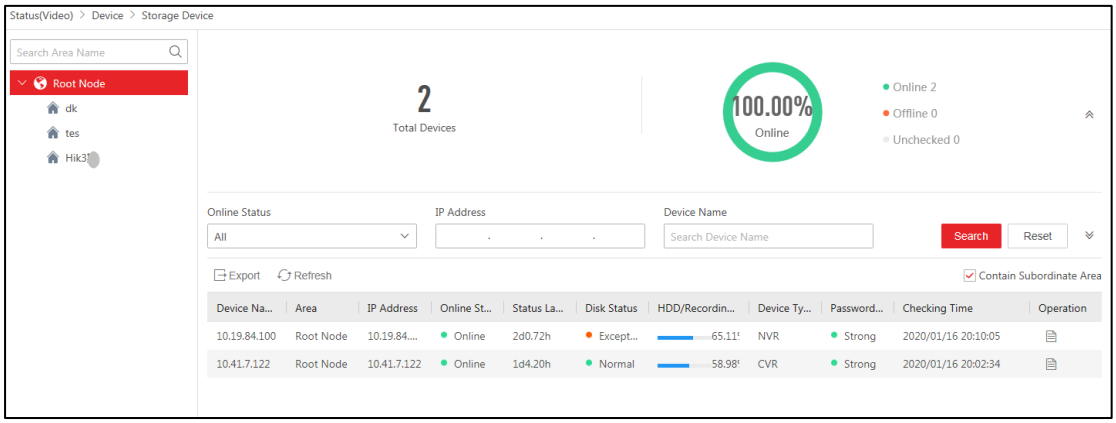
8. The user can view the device details including device basic information, disk information, and history status. The basic information includes device name, area, IP address and port No., manufacturer, online status, password strength, resource code, device model, device firmware version, access protocol, channel amount(total/online/offline), disk usage, offline duration, and online checking time; The disk information includes disk No., disk status; The history status can be searched by time.

- **Decoding Device Status Monitoring**

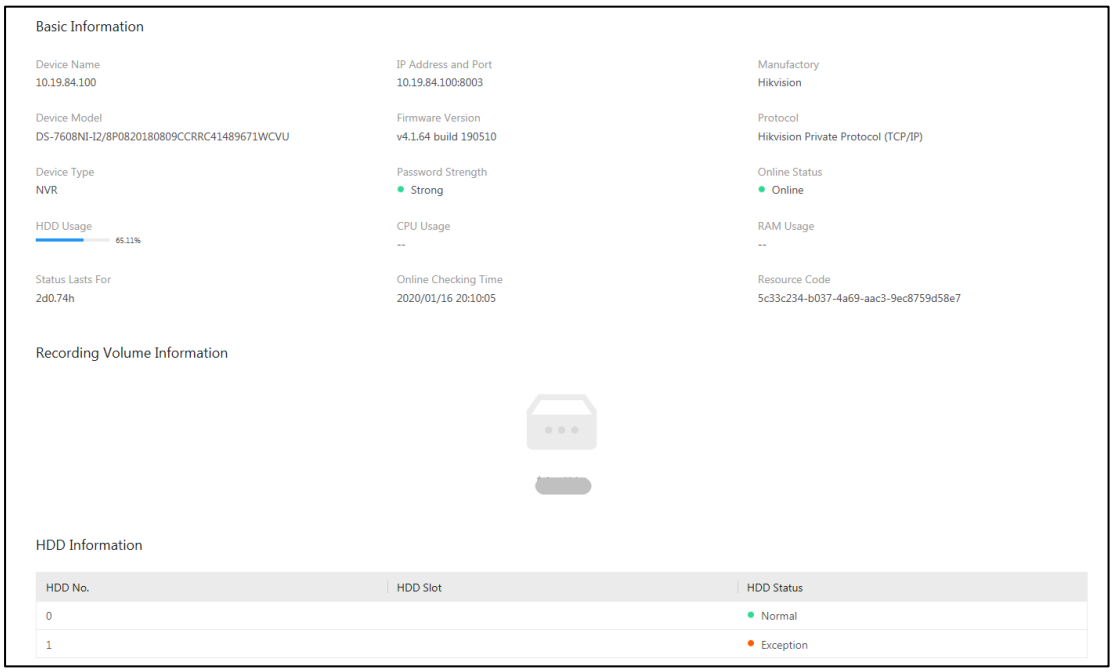
1. The results of the decoding device status check can be displayed in chart and list.
2. The chart displays total device amount, online device amount, unchecked device amount, and the calculated device online rate.
   Note: Device Online Rate = Online Device Amount / (Online Device Amount + Offline Device Amount).
3. The list displays decoder name, area, IP address, online status, status lasting time, password strength, and the checked time.
4. The chart can be hidden. Once hidden, the page displays total device amount, online device amount, offline device amount, and unchecked device amount.
5. The user can filter devices by device online status, password strength, device name, IP address, and status lasting time;
6. The results can be exported to the local PC as a CSV file;
7. The data displayed in the list can be refreshed;
8. The user can view the device details including device basic information and history status. The basic information includes device name, area, IP address and port No., online status, password strength, manufacturer, firmware version, access protocol, offline duration, resource code, and checked time; The history status can be searched by time.

- **Storage Device Status Monitoring**

1. The check results can be displayed in chart and list.
2. The chart displays total device amount, online device amount, offline device amount, unchecked device amount, and the calculated device online rate.
   Note: Device Online Rate = Online Device Amount / (Online Device Amount + Offline Device Amount).
3. The list displays device name, area, IP address, online status, status lasting time, password strength, HDD status, HDD/video volume usage, checked time, and device type.



4. The chart can be hidden. Once hidden, the page displays total device amount, online device amount, offline device amount, and unchecked device amount.
5. The user can filter devices by device online rate, password strength, HDD status, device name, IP address, device type (NVR or CVR), and status lasting time.
6. The results can be exported to the local PC as a CSV file.
7. The data displayed in the list can be refreshed.
8. The user can view the device details include device basic information, video volume information, HDD information and history status. The basic information include area, device name, IP address and port No., manufacturer, device model, firmware version, access protocol, device type, online status, password strength, video volume usage, CPU usage, resource code, status lasting time, and checked time; The HDD information includes HDD No., HDD location, and HDD status; The history status can be searched by time.

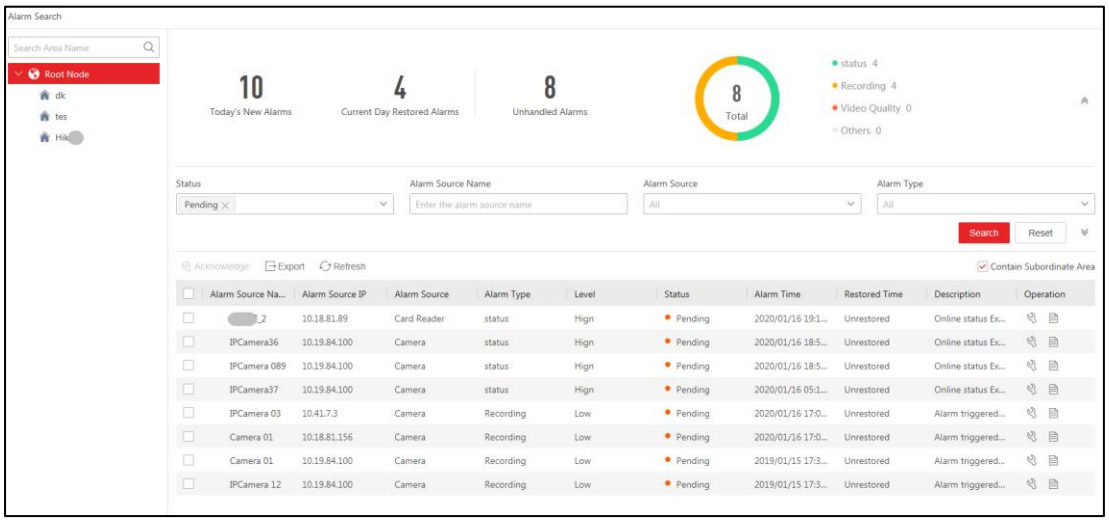


Monitoring vis Topology

1. The platform supports customizing topology. Users are allowed to add, edit, and delete topology. The supported elements include surveillance device (camera, encoding device, decoding device, and storage device), network device (server, switch), and service (network sharing device, device access service, and media gateway). Linking elements to resources, viewing resource details by double-clicking the elements linked to resources, and adding subordinate topology to existing topology are also supported.
2. Supports automatically generating topology structure. User can use the structure to generate topology.

4.7.5 Alarm Search

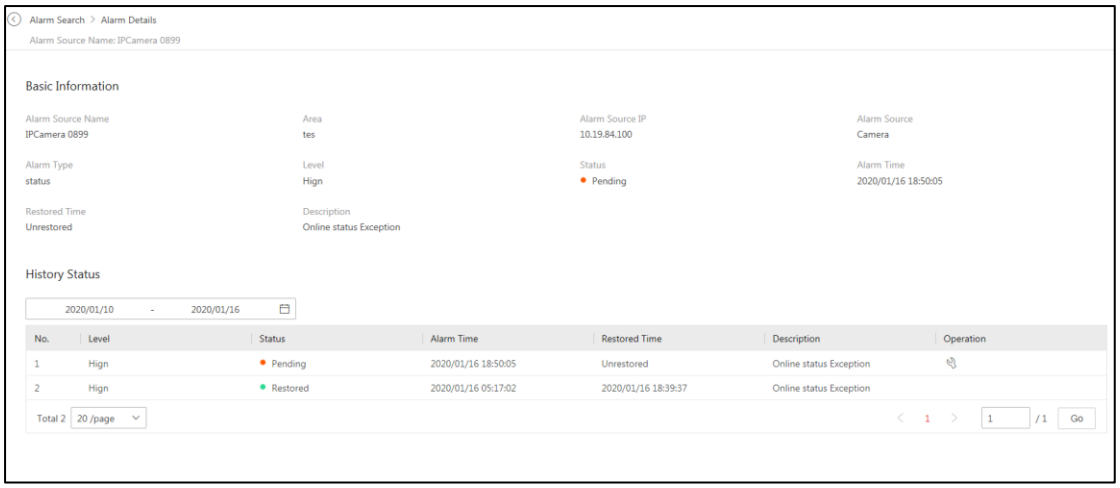
1. The platform provides the alarm search functionality for searching the alarms generated by the resources in the platform, including encoding device, camera, storage device, decoding device, access control device, access control point, card reader, elevator control device, video intercom device, and cloud storage device.
2. The alarm data can be displayed in chart and list;
3. The user can view the amount of new alarms of the current day, the total alarm amount, and the amount of each type of alarms (status, recording, video quality, and others).
4. The list displays alarm source name, alarm source IP, alarm source type, alarm type, alarm level, status, alarm time, alarm restored time, and alarm description;



5. The chart can be hidden. Once hidden, the page displays the new alarms of the current day, the restored alarm of the current day, the ongoing alarms, the status alarm amount, the recording alarm amount, the video quality alarm amount, and the amount of other alarms.
6. The user can filter the alarms by area, whether contain subordinate area(s) or not, status, alarm level, alarm type, alarm source type, alarm source name, alarm time,

and restored time.

7. The user can also acknowledge the alarms. Once acknowledged, the alarm status will change from pending to restored.
8. The alarms can be deleted (if deleted, the related data in the database will also be deleted).
9. The alarms can be exported to the local PC as CSV file.
10. The data displayed on the list can be refreshed.
11. The user can view the alarm details including basic information and history status. The basic information includes alarm source name, area, alarm source IP, alarm source type, alarm type, alarm level, status, alarm time, restored time, alarm description, and alarm acknowledgement information. The alarm history status can be filtered by alarm time.



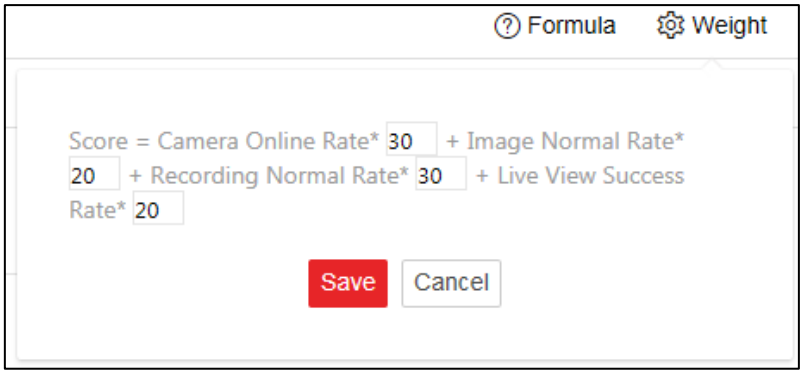
4.7.6 Reports

The platform supports generating reports about camera online status, video quality, recording status. The report types include area overview report, video quality report, recording status report, streaming status report, camera status report, video retention status report, and camera offline duration report.

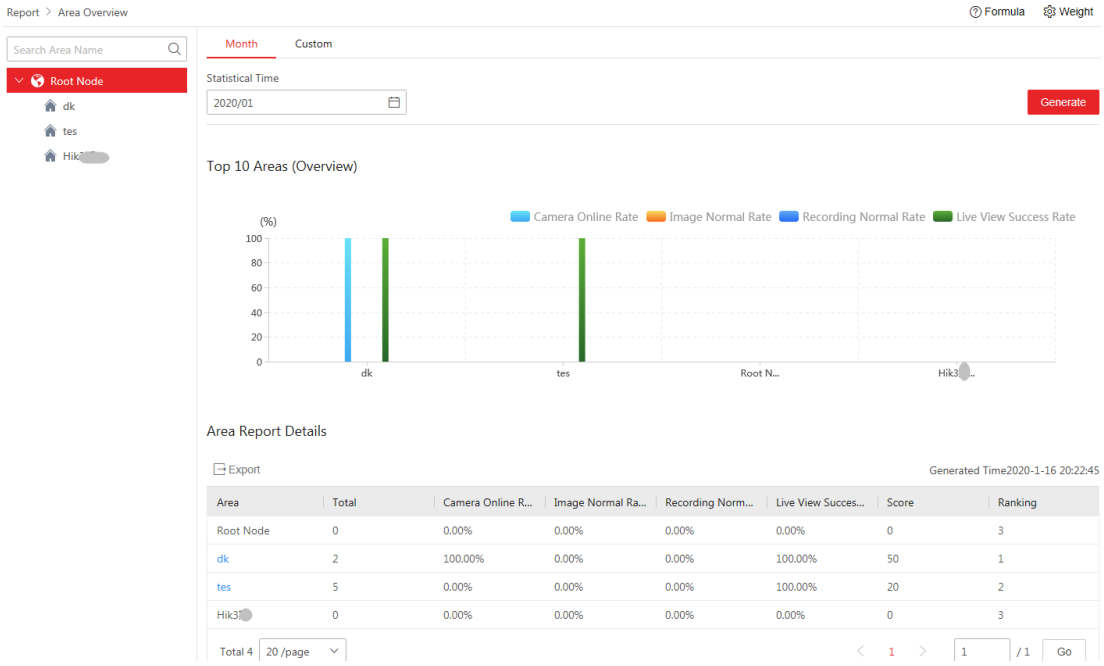
Area Overview Report

1. The user can generate the statistical results of the selected area, including area, total amount, camera online rate, video image normal rate, recording normal rate, VOD success rate, score, and rank.
2. The report can be generated by month or by custom time period.
3. The top 10 sub-areas in terms of the score of resource health status will be displayed in chart, in which the X axis represent the sub-areas, and the Y axis represents the camera online rate, image normal rate, recording normal rate, and VOD success rate. The user can select to display or hide the camera online rate, image normal rate, recording normal rate, and VOD success rate.

4. Supports viewing the formula for calculating camera online rate, image normal rate, recording normal rate the VOD success rate, and configuring the weights for calculating scores.



5. Supports displaying the details of the resource health status in each area, including area, total resource amount, camera online rate, image normal rate, recording normal rate, VOD success rate, score, and rank.

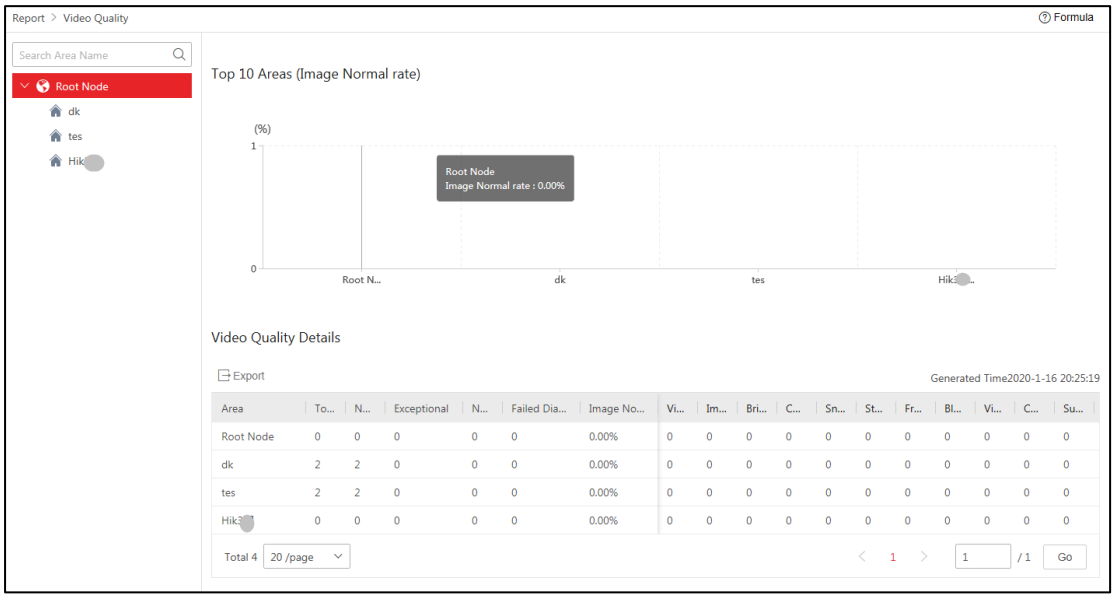


6. The report details can be exported the local PC as a CSV file.

Video Quality Report

1. The platform supports generating reports about video quality of the cameras in the selected areas. The user can view the formula for calculating the image normal rate.
2. The report can be generated by month or custom time period.
3. The top 10 sub-areas in terms of image normal rate are displayed in chart, in which the X axis represents the areas, and the Y axis represents the image normal rate of each sub-area.
4. The user can view the video quality details in the report, including area, total resource amount, the amount of cameras not configured with video quality diagnosis,

exception amount, normal amount, amount of cameras to which diagnosis failed, image normal rate, and 14 types of image exceptions (color cast, image noise, dark image, over bright image, video jittering, contrast, image stripe, video tampering, frame loss, signal loss, black and white image, blurred image, scene change, and sudden change of video image).



5. The video quality report can be exported to the local PC as a CSV file.

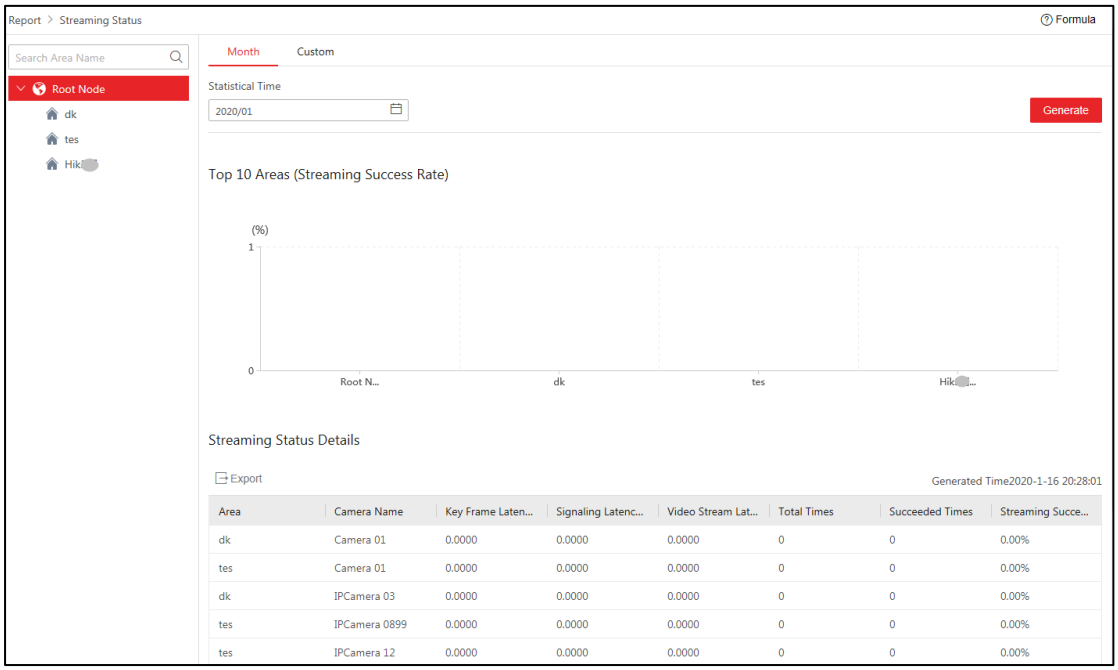
Recording Status Report

1. The platform supports generating the report about recording status of the selected area. The user can view the formula for calculating the recording normal rate.
2. The report can be generated by month or custom time period.
3. The top 10 sub-areas in terms of recording normal rate will be displayed in a histogram chart, in which the X axis represents the sub-areas, and the Y axis represent s the recording normal rate of each sub-area.
4. The user can view the recording status details including area, recording normal rate, and date.

5. The recording status report can be exported to the local PC as a CSV file.

Streaming Status Report

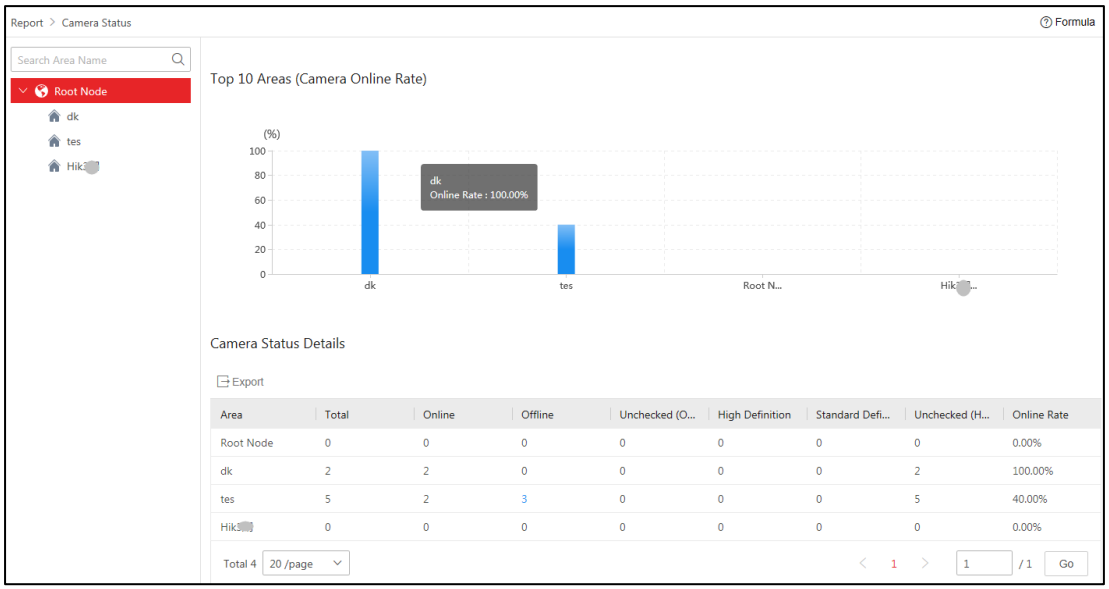
1. The platform supports generating the report about camera streaming status in the selected area. The user can view the formula for calculating the streaming success rate.
2. The report can be generated by month or custom time period.
3. The top 10 sub-areas in terms of streaming success rate will be displayed in a histogram chart, in which the X axis represents the sub-areas, the Y axis represents the streaming success rate of each sub-area.
4. The user can view the streaming status details, including area, camera name, key frame latency, signaling latency, video streaming latency, total streaming times, streaming succeeded times, and streaming success rate.



5. The report can be exported to the local PC as a CSV file.

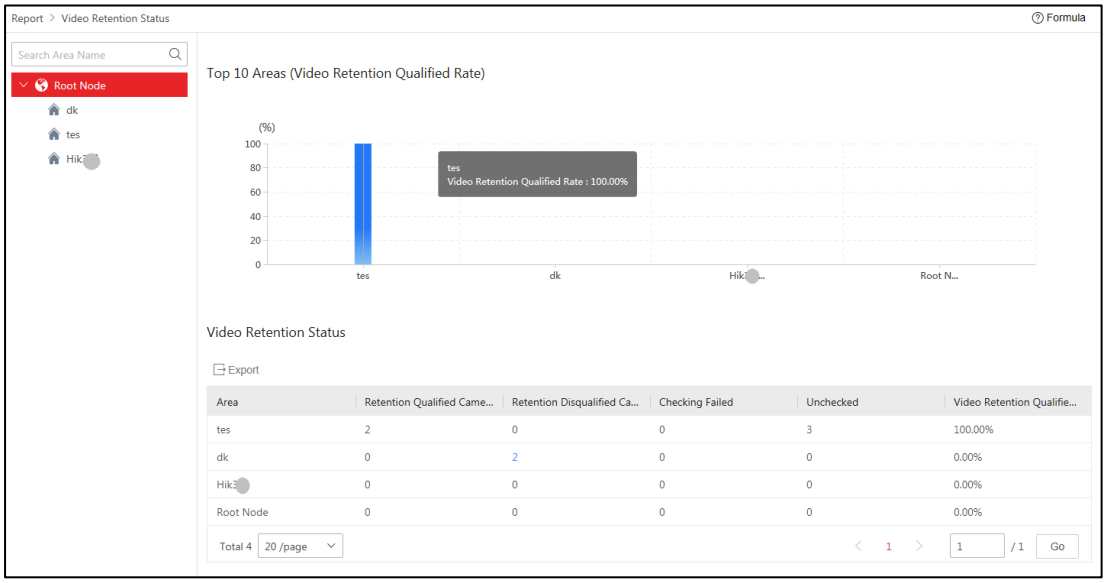
Camera Status Report

1. The top 10 sub-areas in terms of camera online rate can be displayed in a histogram chart.
2. Supports displaying the statistical results of each area in list, including area, total camera amount, online camera amount, offline camera amount, amount of cameras whose online status are not checked, HD camera amount, SD camera amount, amount of cameras whose definitions are not checked, and camera online rate.
3. The report can be exported to the local PC as a CSV file.



Video Retention Status Report

1. The top 10 sub-areas in terms of video retention qualified rate will be displayed in a histogram chart.
2. The user can view the details in the list, including area, the amount of cameras with qualified video retention, amount of cameras with disqualified video retention, checking failed times, amount of unchecked cameras, and video retention qualified rate.
3. The report can be exported to the local PC as a CSV file.



Camera Offline Duration Report

The platform supports generating the report about camera offline duration by time and offline duration. The results are displayed in list, including camera name, area, camera IP address, online status, offline duration, video loss duration, and status changed times. The report can be exported to the local PC as a CSV file.

4.7.7 One-Card Resource Maintenance

You can monitor the running status of the one-card resources, including access control devices (and related card readers and access control points), video intercom devices, and elevator control devices (and related card readers). The running status information includes device online status, exception device number, offline device number, etc.

Access Control Resource Maintenance

➢ **Access Control Device Status**

1. You can view the running status of the access control devices, including total number of access control devices, online devices, offline devices, unchecked devices, online rate, normal devices, abnormal devices, unknown status devices, and normal rate.
2. Supports shows the following information of the access control devices: device name, area, device type, IP address, port, checking time, online status, component status, and operation.
3. Supports filtering access control devices by online status (all/online/offline/unchecked), component status (all/normal/abnormal/unknown), device name, device type, and IP address.
4. Supports displaying device basic information, including device name, area, device type, IP address, port, device model, serial No., access protocol, and firmware version.
5. Supports displaying the running status of the access control devices, including current online status and latest checking time.
6. Supports displaying status devices' components.
7. Supports displaying the device status changes (online to offline, offline to online) and status changed time). Supports filtering data according to checking time (start time to end time).

- **Card Reader Status**
  1. Supports displaying card reader's running status, including number of card readers, online card readers, offline card readers, unchecked card readers, online rate, normal card readers, abnormal card readers, unknown card readers, and normal rate.
  2. Supports displaying card reader name, access control device, access control point, card reader model, access protocol, checking time, online status, component status, and operation.
  3. Supports filtering access control devices by card reader online status (all/online/offline/unchecked), component status all/normal/abnormal/ unknown), card reader name, access control device, and card reader model.
  4. Supports display basic information of card readers, including card reader name, type, access control device, access control point, access protocol, device type, and firmware version.
  5. Supports displaying the card reader's running status, including current online status and latest checking type.
  6. Supports displaying the status of card reader components.
  7. Supports displaying the card reader status changes (online to offline, offline to online) and status changed time). Supports filtering data according to checking time (start time to end time).
- **Access Control Point Status**
  1. Supports displaying access control point's running status, including number of access control points, normal access control points, remaining open access control points, remaining closed access control points, and normal status rate.
  2. Supports displaying access control point name, area, access control device,

channel No., work status (normal, remaining open, and remaining closed), checking time, and operation.

3. Supports filtering access control points by work status (normal, remaining open, and remaining closed), access control point name, and access control device.
4. Supports display basic information of access control points, including access control point name, access control device, area, channel No., location information, and description.
5. Supports displaying the access control points' running status, including work status.

Video Intercom Resource Maintenance

- **Door Station Status**
  1. You can view the running status of the door stations, including total number of door stations, online door stations, offline door stations, unchecked door stations, and online rate.
  2. Supports shows the following information of the door stations: device name, area, device type, IP address, port, checking time, online status, and operation.
  3. Supports filtering door stations by online status (all/online/offline/unchecked), device name, device type, and IP address.
  4. Supports displaying door station basic information, including device name, area, device type, IP address, port, device model, serial No., access protocol, and firmware version.
- **Indoor Station Status**
  1. You can view the running status of the indoor stations, including total number of indoor stations, online indoor stations, offline indoor stations, unchecked indoor stations, and online rate.
  2. Supports shows the following information of the indoor stations: device name, area, device type, IP address, port, room number, checking time, online status, and operation.
  3. Supports filtering indoor stations by online status (all/online/offline/unchecked), device name, device type, and IP address.
  4. Supports displaying indoor station basic information, including device name, area, device type, IP address, port, device model, serial No., access protocol, and firmware version.
- **Master Station Status**
  1. You can view the running status of the master stations, including total number of master stations, online master stations, offline master stations, unchecked master stations, and online rate.
  2. Supports shows the following information of the master stations: device name, area, device type, IP address, port, number, checking time, online status, and operation.
  3. Supports filtering master stations by online status (all/online/offline/unchecked),

device name, device type, and IP address.

4. Supports displaying master station basic information, including device name, area, device type, IP address, port, device model, serial No., access protocol, and firmware version.

- **Outer Door Station Status**
  1. You can view the running status of the outer door stations, including total number of outer door stations, online outer door stations, offline outer door stations, unchecked outer door stations, and online rate.
  2. Supports shows the following information of the outer door stations: device name, area, device type, IP address, port, number, checking time, online status, and operation.
  3. Supports filtering outer door stations by online status (all/online/offline/ unchecked), device name, and IP address.
  4. Supports displaying outer door station basic information, including device name, area, device type, IP address, port, device model, serial No., access protocol, and firmware version.

Elevator Control Resource Maintenance

- **Elevator Control Device Status**
  1. You can view the running status of the elevator control devices, including total number of elevator control devices, online devices, offline devices, unchecked devices, and online rate.
  2. Supports shows the following information of the elevator control devices: device name, area, device type, IP address, port, checking time, online status, and operation.
  3. Supports filtering elevator control devices by online status (all/online/offline/ unchecked), device name, device type, and IP address.
  4. Supports displaying device basic information, including device name, area, device type, IP address, port, device model, serial No., access protocol, and firmware version.
- **Card Reader Status**
  1. Supports displaying card reader's running status, including number of card readers, online card readers, offline card readers, unchecked card readers, online rate, normal card readers, abnormal card readers, unknown card readers, and normal rate.
  2. Supports displaying card reader name, elevator control device, card reader model, access protocol, checking time, online status, component status, and operation.
  3. Supports filtering elevator control devices by card reader online status (all/online/offline/unchecked), component status all/normal/abnormal/ unknown), card reader name, elevator control device, and card reader model.

Chapter 5 Operation and Management Center

Operation and Management Center provides the basic maintenance, which can monitor the stability and performance of itself. More importantly, it can help the users to locate the problem or fault quickly, through status monitor, alarm and log function. As the integrator of background services, Operation and Management Center also provides the components' own status monitoring and configuration page by using its integration capability for configuration, log and status monitoring. Single sign-on is also supported.

5.1 Installation

5.1.1 Install via Disk

1. It is supported to Install and deploy product via disk.
2. The application(s) can be selected for installation.
3. It is supported to select installation directory and scan disk size.
4. It is supported to scan running environment, including operating system and server hardware.
5. It is supported to install client framework.
6. After installation, one-button uninstallation icon is displayed in Control Panel.

5.1.2 Install in Local Server

1. It is supported to install and deployment components in local server.
2. It is supported to monitor installation environment and port conflicts.

5.1.3 Install in Operation and Management Center

1. Distributed deployment is supported.
2. The components can be installed on Web page.
3. Before installing components, the server needs to be selected.
4. The items which the components depend on are monitored when installing components.
5. The server can be added to Operation and Management Center. For Linux operating system, you can install the server directly without local agent.
6. Upgrading component is supported. For failed upgrading, the component version can be restored to the previous version.
7. The patch can be installed on the specified server. It is supported to install multiple

patches on a server in attach and restore this patch installation.

5.2 Software Package Management

1. It is supported to upload software packages, including component, framework, device drive, language package, skin package, document package, and other resource package.
2. The details of software package can be checked.
3. The software package can be deleted.
4. The software package can be installed.

5.3 Parameter Configuration

5.3.1 Center Service Parameter Configuration

1. It is supported to configure component and service parameters on Web page of Operation and Management Center and verify the parameter values.
2. It is supported to detect port conflicts.

5.3.2 Local Service Parameter Configuration

1. It is supported to configure component and service parameters via local service parameter configuration tool, and keep inconsistent or synchronize with Operation and Management Center.
2. It is supported to detect port conflicts.
3. The parameter value can be verified.

5.3.3 Center Alarm Parameter Configuration

1. It is supported to configure alarm strategy on Web page of Operation and Management Center.
2. The alarm strategy can be restored to default settings.

5.3.4 Local Alarm Parameter Configuration

1. It is supported to configure alarm strategy in local alarm configuration, and keep inconsistent with Operation and Management Center.
2. It is supported to configure alarm strategy in local alarm configuration, and keep inconsistent with Operation and Management Center.

5.3.5 Time Synchronization Configuration

1. NTP service in central management server or external servers can be set.
2. Auto time synchronization is supported.
3. Manual time synchronization is supported.

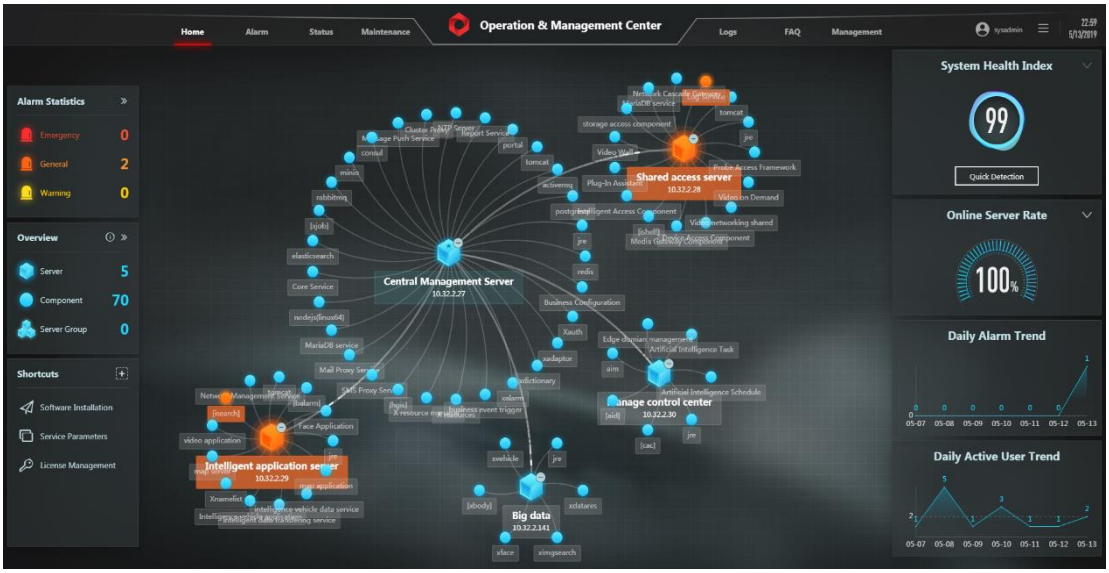
5.3.6 Multi-Domain Configuration

1. Service name, server name, port, and keywords can be used for search.
2. The domain can be added.
3. It is supported to edit the domain settings for the specified service.

5.4 Status Monitoring

5.4.1 Graphic Status Monitoring on Home Page

1. The running topology and running status of servers and components is displayed in graph. The statistic of alarms and status is also displayed on Home Page.
2. The running status of servers and components can be displayed on Video Wall.
3. The scores are used for current system running status.
4. The statistics of servers' online rate and online details is supported.
5. The number of daily alarms (including solved, ignored, unhandled) for last 7 days is counted.
6. The number of daily active users for last 7 days is counted.



5.4.2 Server Status Monitoring

1. It is supported to show server running status, including CPU usage, memory usage, and disk capacity.
2. The statistics of server alarms is supported. The user can handle the alarms.
3. The maintenance record in server about software is displayed.
4. The basic information of server is displayed.

5.4.3 Component Status Monitoring

1. It is supported to show component running status, including CPU usage, and memory usage.
2. It is supported to start or stop the services in component.
3. The component status including its own monitoring items is displayed.
4. The statistics of component alarms is supported. The user can handle the alarms.
5. The service parameters of the component can be configured.
6. The maintenance record about component is displayed.
7. The basic information of component displayed.

5.4.4 Service Start/Stop

1. It is supported to start or stop all services or selected service(s) at the same time.
2. It is supported to start or stop a service.

5.5 Alarm Handling

1. All alarms of the whole system can be searched.
2. Batch handling unhandled alarms, including batch handing and ignoring alarms, is supported.
3. It is supported to provide handling suggestion about different alarms which helps the users to solve the system problems. After solving problems, the solutions can be recorded in FAQ.
4. The search results of alarm can be exported.

5.6 Log Analysis

5.6.1 System Log

1. The system logs can be searched according to service, log time, log level, and keywords. The search results are displayed by the selected service in tab page.

2. The error code and trace chains can be displayed in log details, which can show the related contents when clicking it.
3. The search results of system logs can be exported.

5.6.2 Operation Log

1. The operation logs can be searched according to log time, operation result, and keywords.
2. The search results of operation logs can be exported.

5.7 FAQ

1. Sharing experience is supported. The user can record solutions about solving problems in FAQ.
2. It is supported to export solutions in FAQ.
3. It is supported to import solutions in FAQ.
4. The solutions in FAQ can be searched by entering keywords.

5.8 Cluster Management

1. Three load balance strategies (polling, IP hash, and URL hash) are supported.
2. Managing the HTTP certificates of clusters is supported.

5.9 License Management

1. It is supported to import license file and authorize the product.
2. Activating new product license in online/offline mode, and deactivating license is supported.
3. The authorized status including authorization item and authorized value can be checked.

5.10 Service Management

1. The services can be searched according to component, service type, server, and keywords.
2. The service can be added manually. Editing, viewing and deleting is also supported.

5.11 Organization and Person Management

1. The organization nodes can be added manually and imported in a batch.

2. The organization can be exported.
3. The organization nodes can be edited.
4. The person information can be added manually. The available card types include ID card, passport, household register, driving license, student ID card, etc.
5. The person information can be imported in a batch.
6. The person information can be exported.

5.12 Data Backup

1. The specified or all components data can be backed up. The backup file is also deleted manually.
2. Auto backup is supported, and the auto backup strategy can be set.

Chapter 6 Provided Clients

The platform provides three kinds of terminal for accessing the functions of the platform, including Web Client, Control Client, and Mobile Client (App).

6.1 Web Client

Web Client supports mainstream Web browsers including Internet Explorer, Chrome, and Firefox. It aims to system managers for resource management and configuration.

6.2 Control Client

Control Client aims to system operators for operations and control, including central Control Client (supports integrated control, video surveillance, access control, campus checkpoint, intrusion detection), Booth Client, Manual Visitor Client, and Self-Service Client.

On the central Control Client, the operators can perform live view, playback, PTZ control, video wall control, door status control, receiving real-time access event, viewing resources on map, checking received events, view passing vehicle's information, barrier gate control in parking lot, etc.

6.3 Mobile Client

Mobile Client runs in iOS and Android operating systems for users who need to monitor security areas, such as live view, playback, viewing events and alarms.

Chapter 7 System Requirements

7.1 Hardware Requirements

7.1.1 Recommended Requirements for Servers

Item	Recommended Requirements
CPU	HG3189×1/32GB DDR4/600G 10K SAS×1/SAS_HBA/1GbE×2+10GbE×2/350W Golden/1U
RAM	32GB DDR4 and above
HDD	600G and above. SAS or SSD disk recommended.
NIC	Intel or RealTek 1000 Mbps (latest NIC drive installed)

7.1.2 Recommended Requirements for PC Running Control Client

Item	Recommended Requirements
CPU	i3-7100 and above
RAM	8GB DDR4 and above
HDD	400G and above. SAS or SSD disk recommended.
NIC	Intel or RealTek 1000 Mbps (latest NIC drive installed)
Graphics	Intel HD Graphics 630 and above

7.2 Software Requirements

Item	Recommended Requirements
OS for Server	CentOS 7.2 (64-bit) CentOS 7.4 (64-bit) CentOS 7.6 (64-bit) CentOS-7.6-hik-r5 (64-bit)
OS for Web Client and Control Client	Windows 7 SP1 Home/Pro (32/64-bit) Windows 10 Professional (32/64-bit) Internet Explorer 11 and above Chrome 63.0.3239.108 and above
OS for Mobile Client	Android 5.0 and above iOS 10 and above

Chapter 8 System Performance

Component	Feature	Max. Performance
Base Functions	Areas	20,000
	Organizations	50,000
	Users	200,000
	Simultaneous Online Users	5,000
	Roles	10,000
	Persons	300,000
	Cards	300,000
Events	Simultaneous Events	300 Events/s
	Event Storage	72,000,000 Events in Total (3,000,000 events for one month. Once exceeded, the earliest events will be overwritten.)
	Event Retention Period	3 Years
Maps	Resources in Map	20,000
	Maps per Area	4
Video Surveillance	Channels for Video Surveillance	100,000
	Video Walls	10
	Decoding Devices	128
	Screens per Video Wall	25 × 25
Access Control	Access Control Devices	20,000
	Access Control Points	20,000
	Access Records Storage	50,000,000 Records
	Access Records Retention Period	3 Years
Time & Attendance	Persons for Time and Attendance	20,000
	Access Records Storage	40,000,000 Records
	Attendance Records Storage	10,000,000 Records
	Access Records Retention Period	3 Years
	Attendance Details Retention Period	3 Years
Elevator Control	Elevator Control Devices	500
	Access Records Storage	20,000,000 Records
	Access Records Retention Period	3 Years
Patrol Management	Simultaneous Patrol Routes	50 Routes
	Card Swiping Records Storage for Patrol	8,000,000 Records
	Patrol Data Retention Period	3 Years
Video Intercom	Residences	10,000
	Video Intercom Devices	10,000

	Access Records Storage	50,000,000 Records
	Access Records Retention Period	3 Years
Parking	Vehicles per Day	100,000 Vehicles per Day
	Parking Lots	20
	Lanes	60
	Parking Spaces in Total	10,000
	Parking Spaces per Floor	2,000
	Registered Vehicles	30,000
Campus Checkpoint	Traffic Cameras	30
	Display Screens	30
	Passing Vehicle Records Storage	10,000,000 Records
	Passing Vehicle Records Retention Period	3 Years
Facial Surveillance	Facial Recognition Servers	5
	Face Capture Cameras	500
	DeepinMind NVRs	100
	Faces	300,000
	Face Groups	16
	Face Pictures per Face Group	30,000
	Simultaneous Facial Recognition Events	200 Events/s
Intrusion	Security Control Panels	100
	Zones	1,000
	Zones per Area	1,000
	Alarm Records Storage	1,000,000 Records
	Alarm Records Retention Period	3 Years
Panic Alarm	Panic Alarm Devices	500
	Alarm Records Storage	1,000,000 Records
	Alarm Records Retention Period	3 Years
Central Storage	Channels	100,000


See Far, Go Further