



HIKVISION[®]

A&E System Specification

HikCentral Professional

ALL TRADEMARKS ARE THE PROPERTIES OF THEIR RESPECTIVE OWNERS

This A&E specification is written according to Construction Specifications Institute (CSI) 3-Part Format, based on MasterFormat™ (2016 Edition) and The Project Resource Manual – CSI Manual of Practice.

www.csiresources.org Manufacturer is responsible for the accuracy of the technical data included in this specification.

Division 28 – Electronic Safety and Security

Section 28 20 00 – Video Security

Section 28 23 00 – Video Management System

Section 28 23 11 – Video Management System Analytics

Section 28 23 13 – Video Management System Interfaces

Part 1 General

1.1 Summary of Requirements

A. HikCentral Professional System

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

B. Related Requirements

- | | |
|-------------------------|--|
| 1. Section 27 20 00 | Data Communications |
| 2. Section 28 05 00 | Common Work Results for Electronic Safety and Security |
| 3. Section 28 05 19 | Storage Appliances for Electronic Safety and Security |
| 4. Section 28 05 19.11 | Digital Video Recorders |
| 5. Section 28 05 19.13 | Hybrid Digital Video Recorders |
| 6. Section 28 05 19.15 | Network Video Recorders |
| 7. Section 28 06 20 | Schedules for Video Security |
| 8. Section 28 21 00 | Security Cameras |
| 9. Section 28 21 13 | IP Cameras |
| 10. Section 28 27 00 | Video Security Sensors |
| 11. Section 28 33 00 | Video Security – Security Monitoring and Control |
| 12. Section 28 51 19.15 | Smart Walls |

1.2 References

A. Abbreviations

- | | |
|----------|-------------------------------------|
| 1. AD | Active Directory |
| 2. AGC | Automatic Gain Control |
| 3. AWB | Automatic White Balance |
| 4. BLC | Back Light Compensation |
| 5. CIF | Common Intermediate Format |
| 6. CD | Client Device |
| 7. DDNS | Dynamic Domain Name Server |
| 8. DHCP | Dynamic Host Configuration Protocol |
| 9. DNR | Digital Noise Reduction |
| 10. DNS | Domain Name Server |
| 11. DSCP | Differentiated Services Code Point |
-

12. DVR	Digital Video Recorder
13. FPS	frames per second
14. FTP	File Transfer Protocol
15. GIS	Geographic Information System
16. GUI	Graphical User Interface
17. HLC	High Light Compression
18. HTTP	Hypertext Transfer Protocol
19. HTTPS	Secure HTTP
20. Hybrid SAN	Hybrid Storage Area Network
21. ICMP	Internet Control Message Protocol
22. IGMP	Internet Group Management Protocol
23. IP	Internet Protocol
24. JPEG	Joint Photographic Experts Group
25. LPR	License Plate Recognition
26. MicroSD	Removable Miniaturized Secure
27. MicroSD	Removable Miniaturized Secure Digital Flash Memory Card
28. MPEG	Moving Pictures Experts Group
29. MWB	Manual White Balance
30. NAS	Network Attached Storage
31. NIC	Network Interface Controller
32. NTP	Network Time Protocol over Ethernet
33. NVR	Network Video Recorder
34. PIR	Passive Infrared Sensor
35. PoE	Power over Ethernet
36. POS	Point of Sale
37. PPPoE	Point-to-Point Protocol over Ethernet
38. PTZ	Pan Tilt Zoom
39. QoS	Quality of Service
40. ROI	Region of Interest
41. RSM	Remote Site Management
42. RTP	Real-Time Transport Protocol
43. RTSP	Real-Time Streaming Protocol
44. SD Card	Secure Digital Flash Memory Card
45. SMTP	Simple Mail Transfer Protocol
46. TCP	Transmission Control Protocol
47. UDP	User Datagram Protocol
48. UPnP	Universal Plug and Play
49. UVSS	Under Vehicle Surveillance System
50. VCA	Video Content Analysis
51. VMS	Video Management System
52. WB	White Balance
53. WDR	Wide Dynamic Range
54. SYS	System Management Service

1.3 Certifications, Standards and Ratings

Reference Standards

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

1.4 Submittals

A. Product Data

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

1.5 Qualifications

A. Requirements

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

1.6 Delivery, Storage and Handling

A. General

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

1.7 Licensing and Support Agreements

1. Requires no Software Support Agreements with the manufacturer.

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

A. Support

1. Technical support shall be based in North America.
2. Technical support shall be available weekdays from 5 a.m. to 5 p.m. PST.

END OF SECTION

Part 2 Product

2.1 Manufacturer

A. Manufacturer:

Hikvision USA Inc.
18639 Railroad Street
City of Industry, CA 91748
Phone: +1-909-895-0400 | Fax: +1-909-595-2788
Web: www.HikvisionUSA.com

- B. Product: HikCentral Professional– shall be designed to manage distributed sites or large groupings of cameras recording on NVRs, DVRs, pStor, Hybrid SANs, and Cloud Storage Servers.**

2.2 Service Description

A. HikCentral Professional System Management Service:

1. SYS maximum capacity for devices management and event handling:
 - a. Manages up to 2,048 resources, including Encoding Devices, Access Control Devices, Elevator Control Devices, Security Control Device, Digital Signage Terminal, and Remote Sites
 - b. Imports up to 100,000 video channels (Network Camera or analogue/TVI)
 - c. Manages up to 64 Recording Servers per SYS
 - d. Imports up to 3,000 alarm inputs/outputs respectively per SYS.

B. Service Manager: An application that manages the following Services

1. HikCentral Professional System Management Service is the core component of HikCentral, providing authentication, permission granting, and management services. It authenticates the Control Client access, manages the users, roles, permissions and monitors devices, and provides the interface for third-party system integration. It includes the following service:
 - a. 3rd Party Device Access Gateway
 - i. Communication between SYS and third-party device
 - b. System Management Service
 - i. Provide the unified authentication service for connecting with the clients and servers
 - ii. Provides the centralized management for the users, roles, permissions, devices, and services.
 - iii. Provides the configuration interface for security and management module.
 - c. HikCentral Professional Management Service
 - i. The content server and signaling gateway of HikCentral
 - ii. Mainly responsible for storage of static pages and reverse proxy of device configuration
 - d. HikCentral Professional Streaming Gateway
 - i. A component of SYS which forwards and distributes the video and audio data

- ii. Shall support up to 200 video channels @ 2 Mbps input and 200 video channels @ 2 Mbps output. It is used for concurrent live view or playback
- iii. Shall not be added to the web client as Streaming Server
- 2. Keyboard Proxy Service
 - a. Used with network keyboard to access the Keyboard Proxy Service
 - b. Network keyboard can be used for the live view operations on the smart wall
- 3. Smart Wall Management Service
 - a. Manage smart wall for displaying decoded video on smart wall
 - b. Responds to Control Client's request and sends real-time messages to Control Client

2.3 Accessibility and Management Capabilities

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

2.4 Network

- A. Security Access**
 - 1. Shall have a built-in password protection not dependent on server
 - 2. The System shall have User Authentication
 - 3. Secure Activation
 - a. A system algorithm shall check the user defined password for strength, based on the manufacturer's criteria.
 - b. System shall determine and display password security level as "weak", "medium", or "strong".

- c. Password shall contain a minimum of two kinds of characters (lowercase letters, uppercase letters, numbers and special characters).
- d. Only ASCII characters shall be allowed.
- e. Password length shall be eight characters minimum.

2.5 PC Requirements (for HikCentral Professional Control Client)

- A. Minimum PC Intel® Core™ i3-8100k @ 3.60 GHz
- B. RAM 8 GB
- C. Network GbE network interface card
- D. Graphics Card Intel® UHD Graphics 630+GT1030
- E. Hard Disk Type SATA-II Hard Drive or better
- F. Hard Drive Capacity 60 GB for OS and HikCentral Professional Control Client
- G. Other Microsoft® Windows 10 (64-bit)

2.6 PC Requirements (for HikCentral Professional SYS Server without RSM)

- A. Minimum PC Intel® Core™ i5-4590 @3.3 GHz
- B. RAM 8 GB
- C. Network GbE network interface card
- D. Graphics Card NVIDIA® GeForce® GTX
- E. Hard Disk Type SATA-II 7200 RPM Enterprise Class HDD
- F. Hard Drive Capacity 650 GB for the HDD where SYS service is installed
- G. Other Microsoft® Windows 8.1 64-bit

2.7 PC Requirements (for HikCentral Professional SYS Server with RSM)

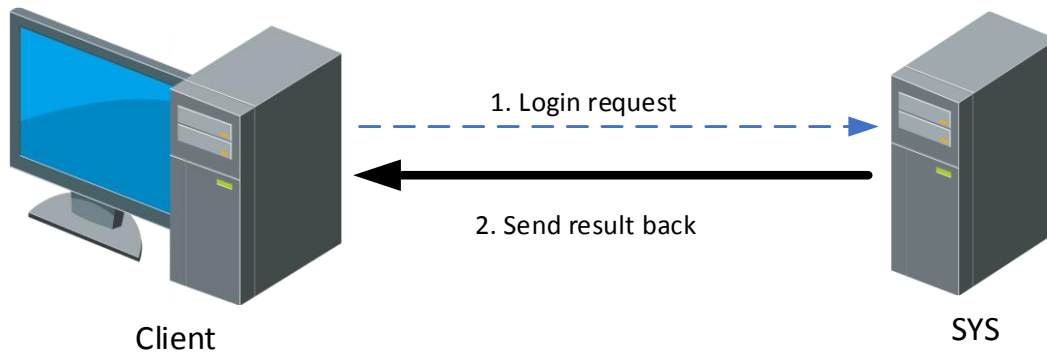
- A. Minimum PC Intel® Xeon® E-2124 V5 @3.00 GHz
- B. RAM 16 GB
- C. Network GbE network interface card
- D. Hard Disk Type SATA-II 7200 RPM Enterprise Class HDD
- E. Hard Drive Capacity 650 GB for the HDD where SYS service is installed
- F. Other Microsoft® Windows Server 2012 (R2) 64-bit

2.8 PC Requirements (for Streaming Server)

- A. Minimum PC Intel® Core™ i5-4590 @3.3 GHz
- B. RAM 8 GB
- C. Network GbE network interface card
- D. Hard Disk Type SATA-II 7200 RPM Enterprise Class HDD
- E. Hard Drive Capacity 10 GB for Streaming server log files

2.9 Signal Flow

2.9.1 Login



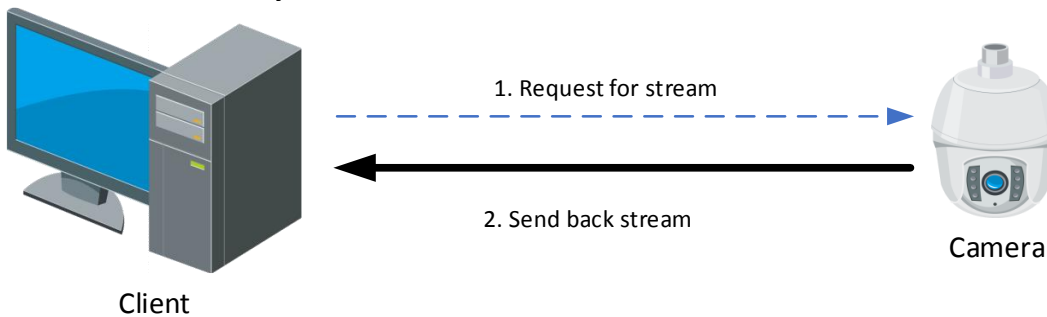
During the login, the signaling is exchanged between the client (Web Client/Control Client/Mobile Client) and the SYS server.

The signaling interaction process is as follows:

1. Enter the user name and password (domain name) on the client, which will be sent to the SYS server.
2. The SYS server receives the information, checks whether the user name and password (domain name) are correct, and sends the result to the client.

2.9.2 Live View

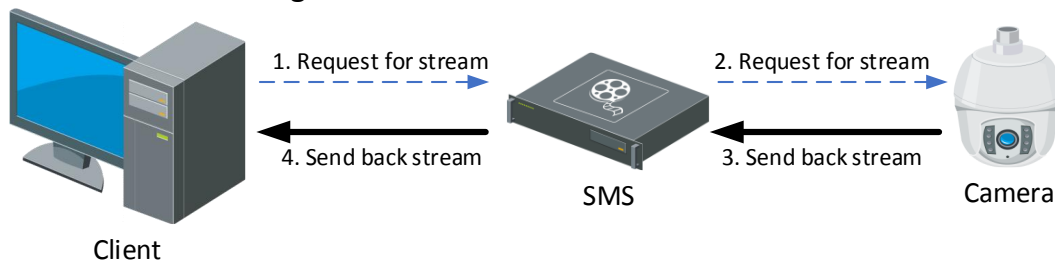
A. Live View for Directly Connected Device



If the SYS server, devices and the client are deployed in the same LAN network, the client can directly obtain the stream. The signaling process is as follows:

1. The client sends a request to the device for obtaining the stream.
2. The device sends back the corresponding stream to the client.

B. Live View via Streaming Server



In the following situations, the SMS (Streaming Server) needs to be deployed:

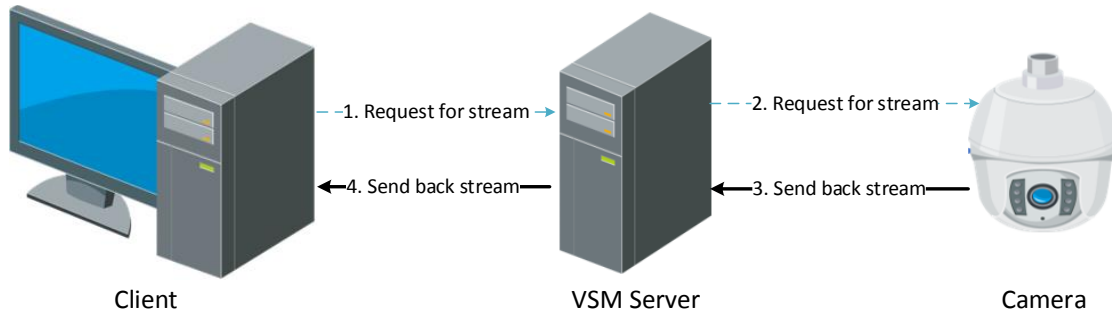
The client obtains streams from third-party devices.

Multiple clients request the same stream from the same device. To reduce the bandwidth for obtaining the stream, the stream is forwarded via SMS to solve this problem.

The signaling process is as follows:

1. The client sends a request to the SMS for obtaining the stream.
2. The SMS forwards the request to the device for obtaining the stream.
3. The device sends back the corresponding stream to the SMS.
4. The SMS forwards the obtained stream to the client.

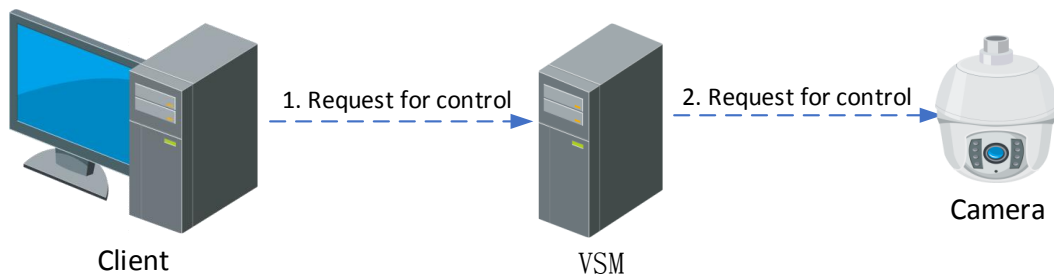
C. Live View via VSM Server



The signaling process is as follows:

1. The client sends a request to the VSM Server for obtaining the stream.
2. The VSM Server forwards the request to the device for obtaining the stream.
3. The device sends back the corresponding stream to the VSM Server.
4. The VSM Server forwards the obtained stream to the client.

D. PTZ Control



HikCentral Professional controls the PTZ camera via the SYS server.

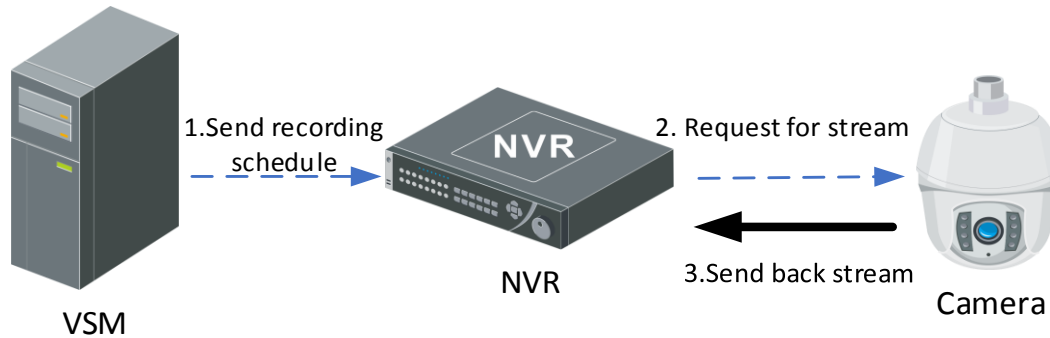
The signaling process is as follows:

1. The client sends a request to the SYS server to control the PTZ camera.
2. The SYS server forwards the request to the corresponding device for PTZ control.

2.9.3 Video Storage and Playback

Device storage and playback includes: video stream storage, video file retrieval and playback.

A. Video Storage in NVR/DVR



As shown in the figure above, the signaling process is as follows:

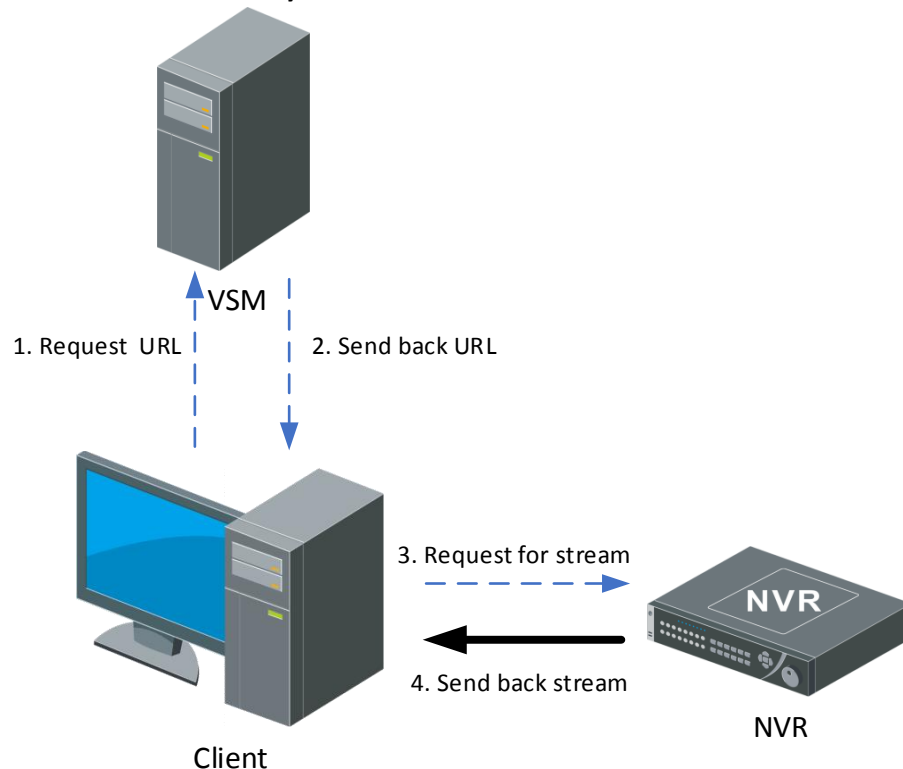
1. The SYS server sends the recording schedule (event-based recording schedule and time-based recording schedule) to the NVR.
2. When the recording schedule condition is met (within the time segment or an event is triggered), the NVR sends a request to the camera for obtaining the stream.
3. The camera sends back the corresponding stream to the NVR.

Note: When manual recording is performed on the Control Client, the preceding steps are triggered manually, but not triggered by recording schedule.

B. Playback of Video in NVR/DVR

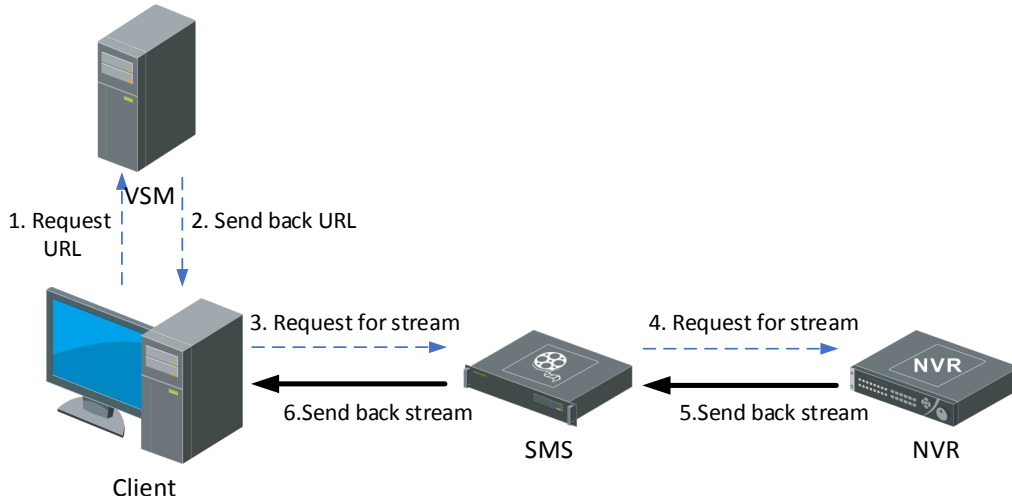
There are two modes for playing back video in NVR/DVR: The client obtains the stream directly from the NVR/DVR, and the client obtains the stream from the NVR/DVR via SMS. The signaling processes are as follows:

1. Playback of Video in Directly Connected Device



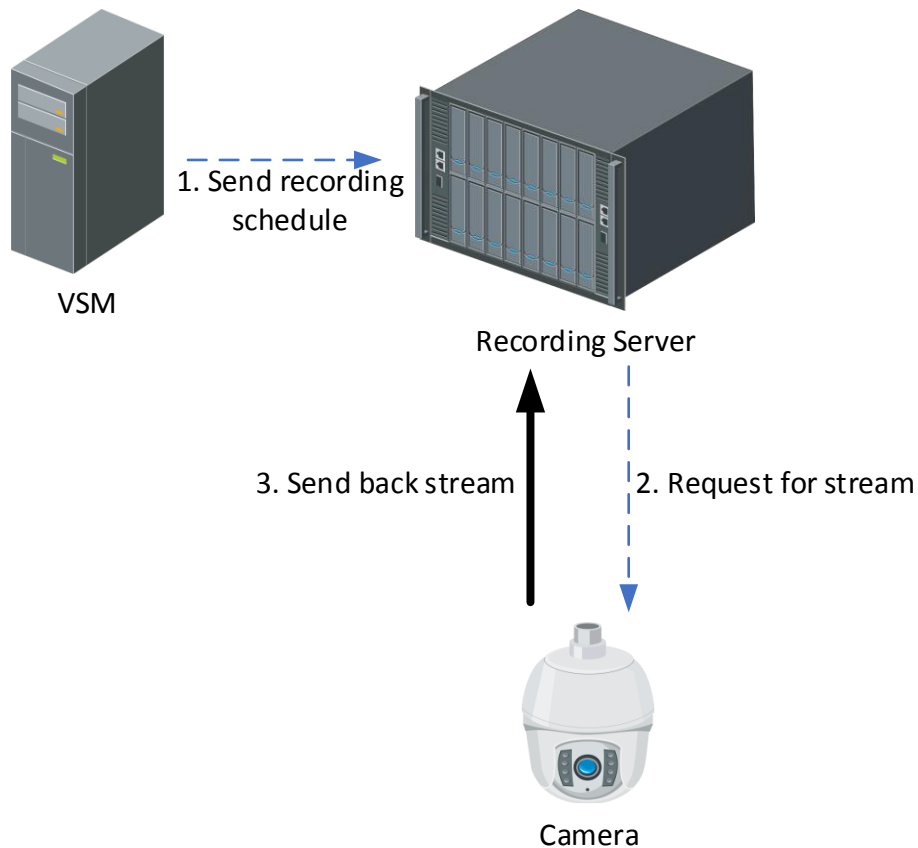
1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to the NVR for obtaining the stream.
4. The NVR sends back the corresponding stream to the client according to the request.

2. Playback via Streaming Server



1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to the SMS (Streaming Server) for obtaining the stream.
4. The SMS forwards the request to the NVR for obtaining the stream.
5. The NVR sends back the corresponding stream to the SMS according to the request.
6. The SMS forwards the corresponding stream to the client.

C. Video Storage in Recording Server



Recording Servers include: Hybrid SAN, cloud storage, and pStor. If the video is stored on the recording server, the signaling process is as follows:

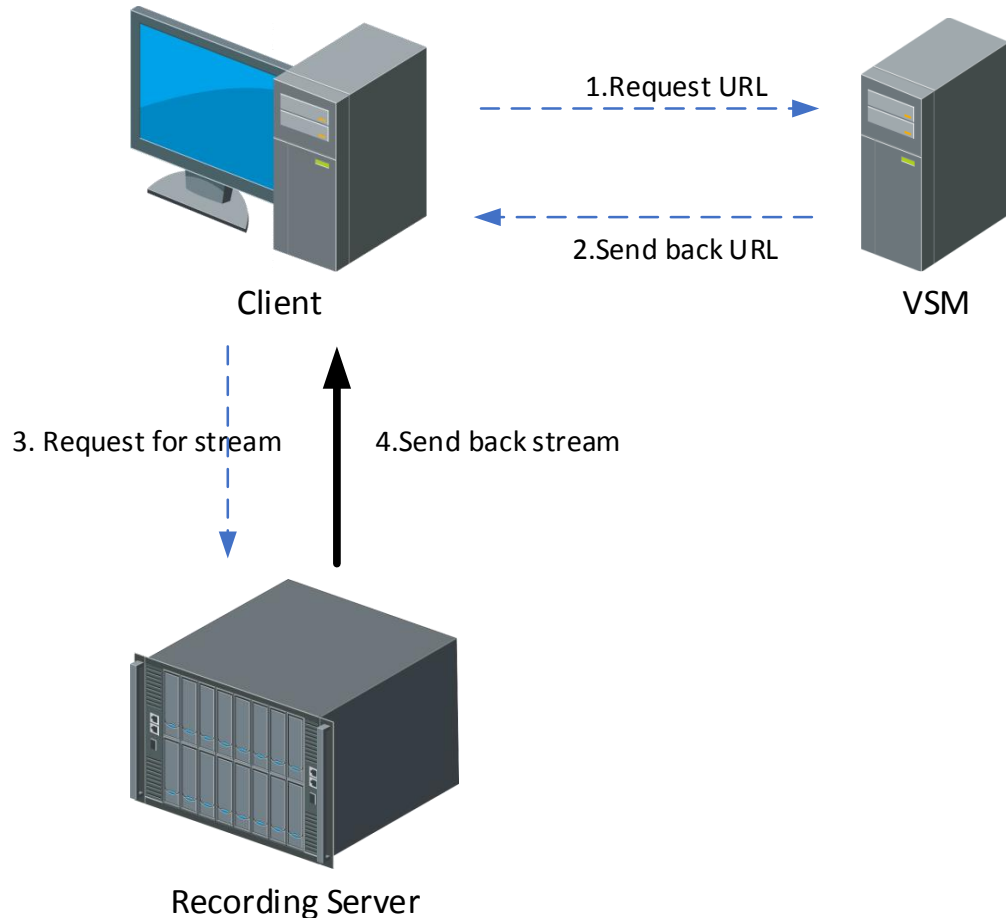
1. The SYS server sends the recording schedule (time-based recording schedule and event-based recording schedule) to the recording server.
2. The recording server sends a request to the camera for obtaining the stream according to the recording schedule.
3. The camera sends back the corresponding stream to the recording server according to the request.

Note: When manual recording is performed on the Control Client, the preceding steps are triggered manually, but not triggered by recording schedule.

D. Playback of Video in Recording Sever

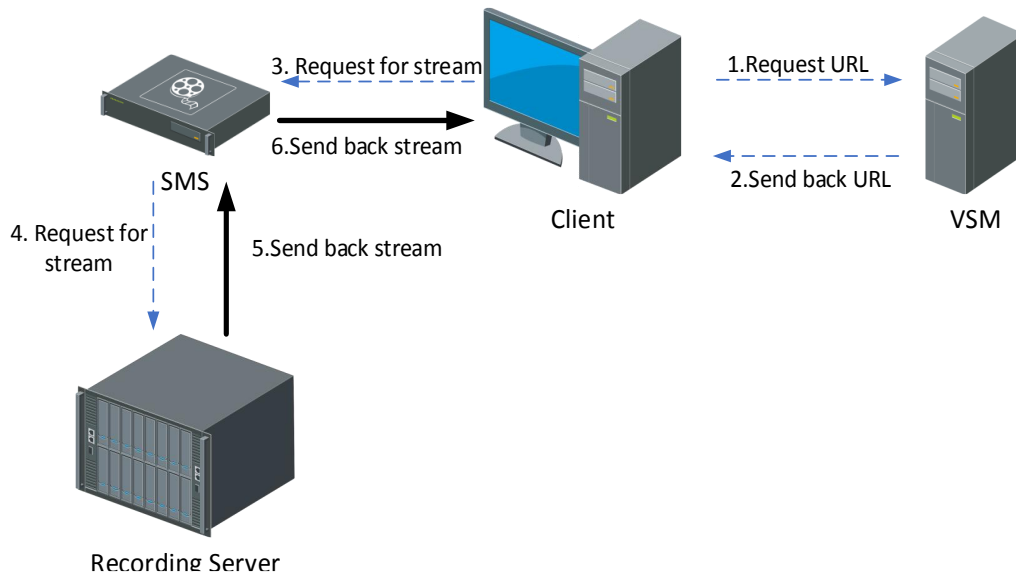
There are two modes for playing back video from recording server: The client obtains the stream directly from the recording server, and the client obtains the stream from the recording server via SMS. The signaling processes are as follows:

1. Playback of Video in Directly Connected Recording Server



1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to the recording server for obtaining the stream.
4. The recording server sends back the corresponding stream to the client according to the request.

2. Playback via Streaming Server

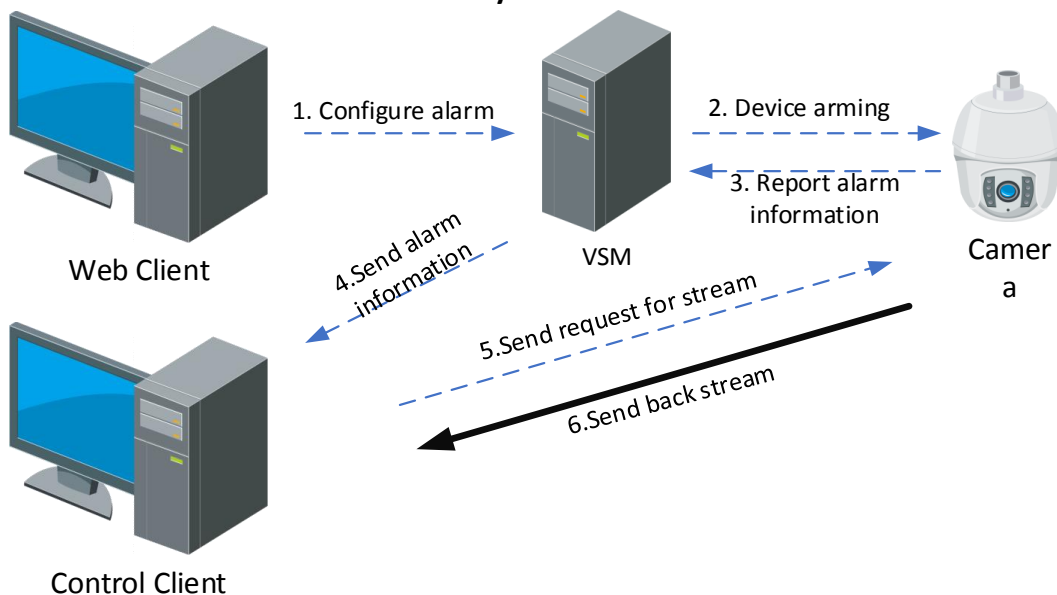


1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to SMS for obtaining the stream.
4. The SMS forwards the request to the recording server for obtaining the stream.
5. The recording server sends back the corresponding stream to the SMS according to request.
6. The SMS forwards the corresponding stream to the client.

2.9.4 Alarm

When an alarm is triggered, there are two modes for the Control Client to obtain the alarm related stream from the device: Obtain the stream via directly connected device and obtain the stream via SMS. The signaling processes are as follows:

A. Obtain Alarm Related Stream Directly



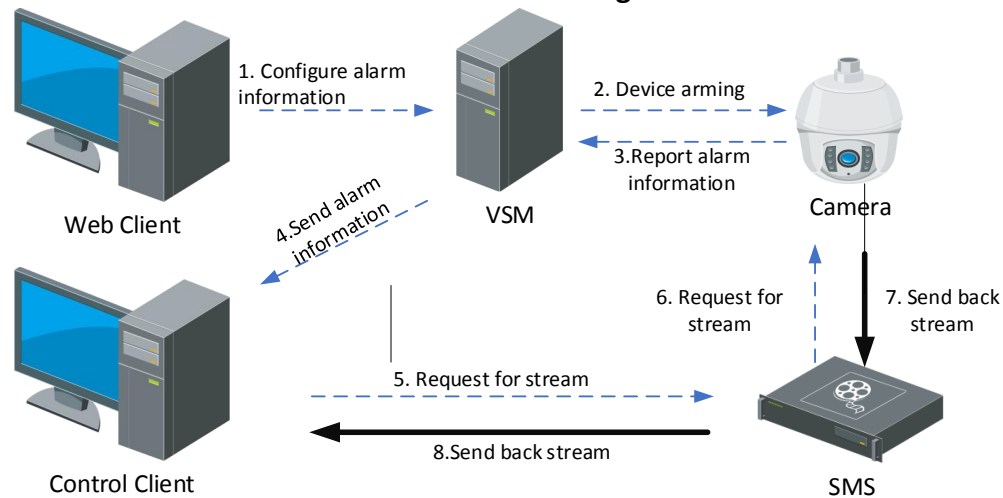
The process of alarm configuration is as follows:

1. Configure alarm via the Web Client, and the alarm configuration is sent to the SYS server.
2. The device is armed by the SYS server according the arming schedule.

The process of reporting an alarm is as follows:

1. The device analyzes the obtained stream. If an alarm is triggered, the device reports the alarm to the SYS server.
2. The SYS server sends the alarm information to the Control Client.
3. If the linkage of live view for the alarm is configured, the Control Client sends a request to the device for obtaining the stream.
4. The device sends back the corresponding stream to the Control Client according to the request.

B. Obtain Alarm Related Stream via Streaming Server



The process of alarm configuration is as follows:

1. Configure the alarm via the Web Client, and the alarm configuration is sent to the SYS server.
2. The device is armed by the SYS server according the arming schedule.

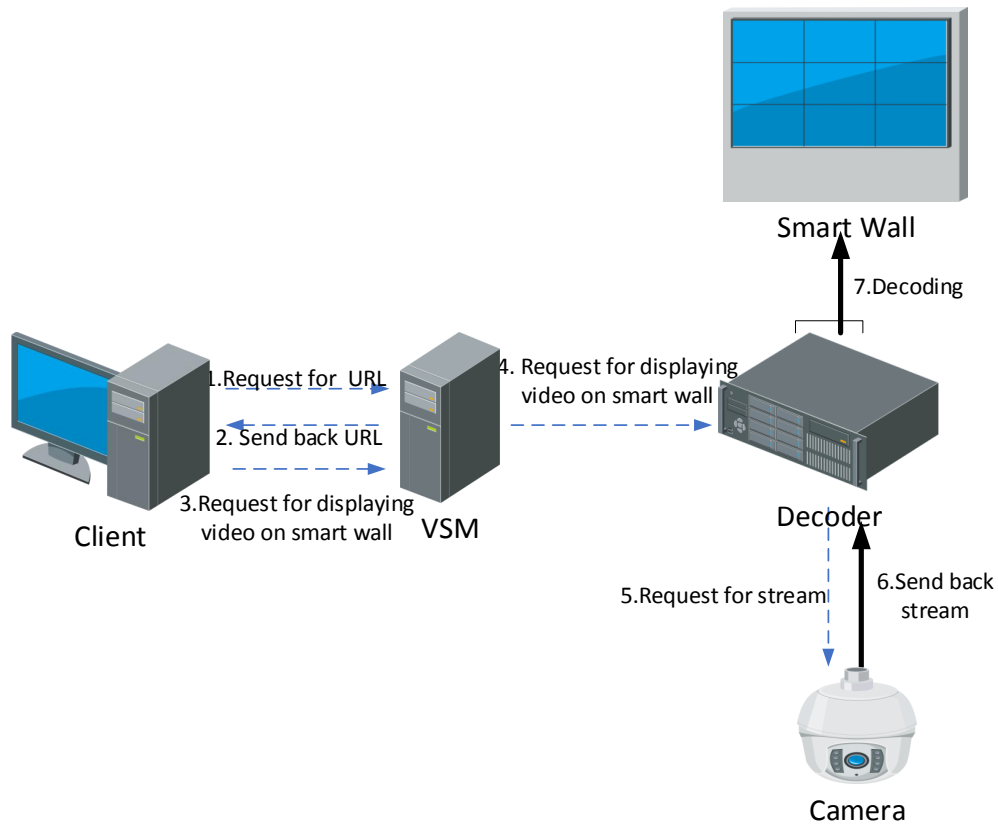
The process of reporting an alarm is as follows:

1. The device analyzes the obtained stream. If an alarm is triggered, the device reports an alarm to the SYS server.
2. The SYS server sends the alarm information to the Control Client.
3. If the linkage of live view or playback for the alarm is configured, the Control Client sends a request to the SMS for obtaining the stream.
4. The SMS forwards the request to the camera for obtaining the stream.
5. The camera sends back the corresponding stream to the SMS according to the request.
6. The SMS forwards the stream to the Control Client.

2.9.5 Smart Wall

A. Display Video on Smart Wall

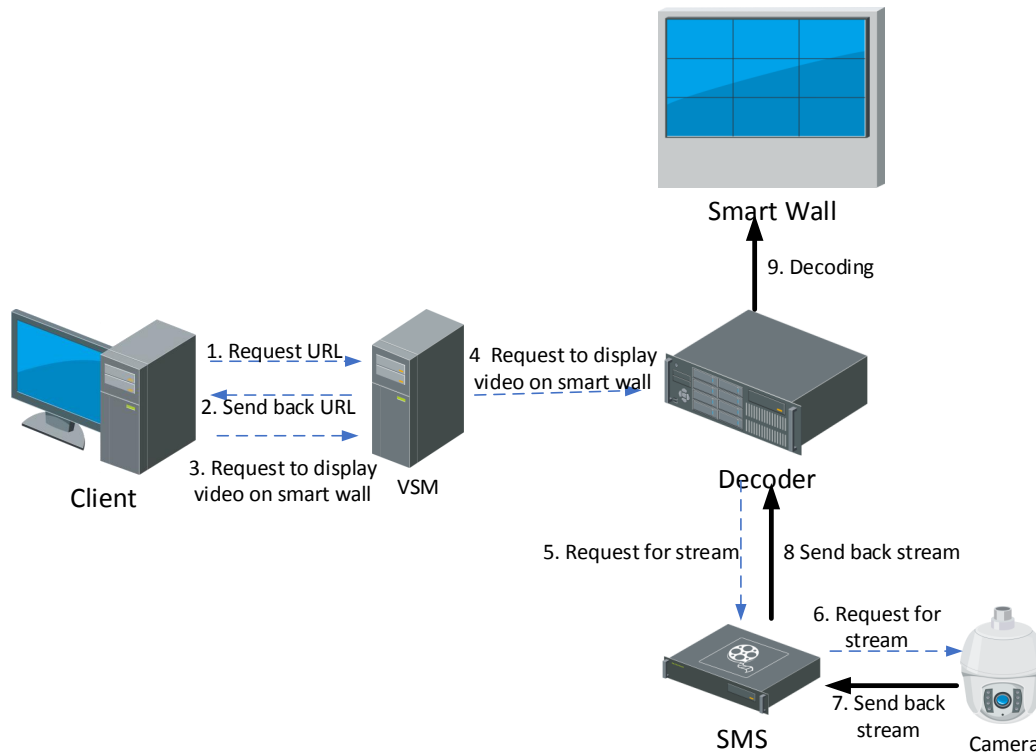
1. Display Video of Directly Connected Device on Smart Wall



When the decoder obtains the stream directly from the device, the signaling process is as follows:

1. The Smart Wall Client sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the Smart Wall Client.
3. The Smart Wall Client sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.
5. The decoder sends a request to the device for obtaining the stream.
6. The device sends back the corresponding stream to the decoder.
7. The decoder decodes the obtained stream and displays the video on the smart wall.

2. Display Video on Smart Wall via Streaming Server

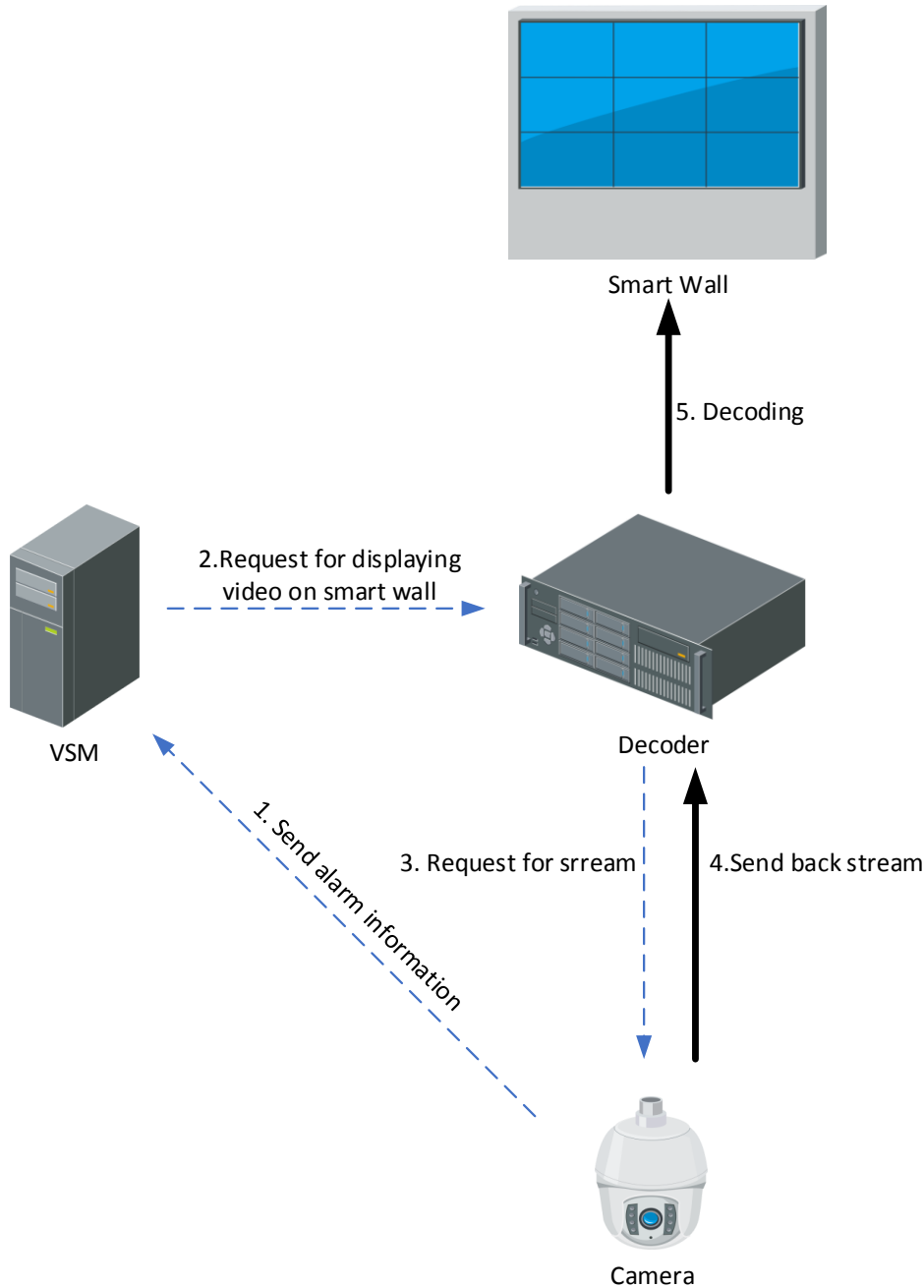


If the decoder obtains the stream via SMS, the signaling process is as follows:

1. The Smart Wall Client sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the Smart Wall Client.
3. The Smart Wall Client sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.
5. The decoder sends a request to the SMS (Streaming Server) for obtaining the stream.
6. The SMS forwards the request to the device for obtaining the stream.
7. The device sends back the corresponding stream to the SMS.
8. The SMS forwards the stream to the decoder.
9. The decoder decodes the obtained stream and displays the video on the smart wall.

B. Display Alarm Video on Smart Wall

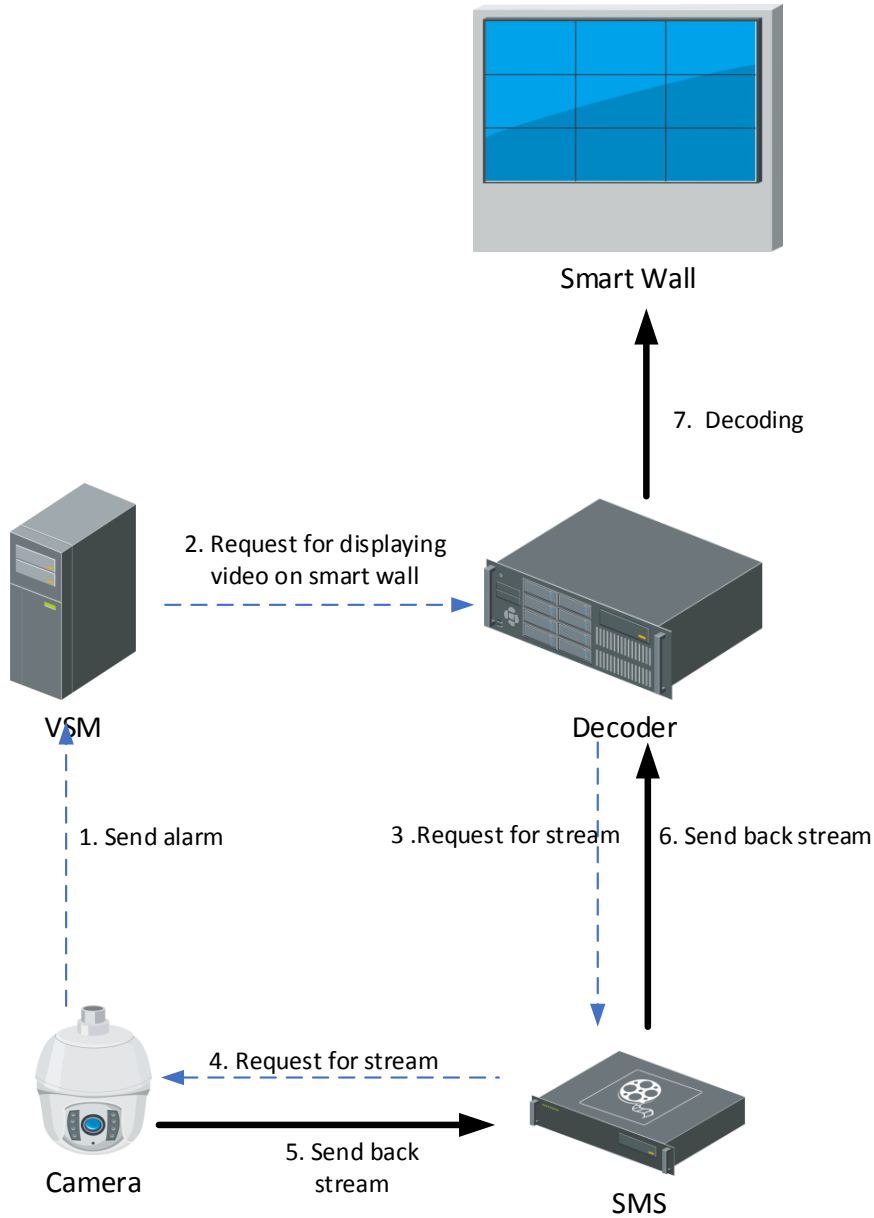
1. Display Alarm Video of Directly Connected Device on Smart Wall



The process of displaying alarm video of directly connected device on smart wall is as follows:

1. The camera analyzes the obtained streams. If an alarm is triggered, the camera sends the alarm to the SYS server.
2. According to the alarm, the SYS server estimates whether the video of the camera need to be displayed on the smart wall. If yes, the SYS server sends a request to the decoder to display video on smart wall.
3. The decoder sends a request to the corresponding camera for obtaining the alarm video stream.
4. The camera sends back the stream according to the corresponding request.
5. The decoder decodes the obtained stream and displays the video on the smart wall.

2. Display Alarm Video on Smart Wall via Streaming Server

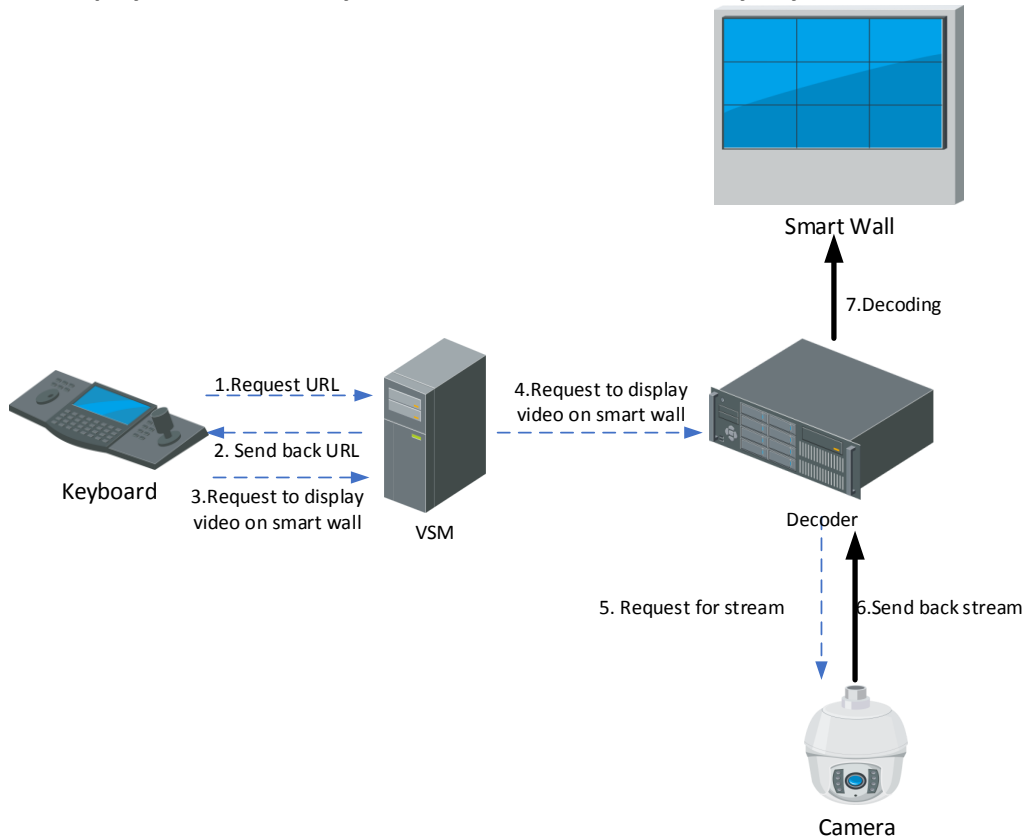


The process of displaying alarm video of device on smart wall via SMS is as follows:

1. The camera analyzes the obtained streams. If an alarm is triggered, the camera sends the alarm to the SYS server.
2. According to the alarm, the SYS server estimates whether the video of the camera need to be displayed on the smart wall. If yes, the SYS server sends a request to the decoder to display video on smart wall.
3. The decoder sends a request to the SMS (Streaming Server) for obtaining the stream.
4. The SMS forwards the request to the corresponding camera for obtaining the stream.
5. The camera sends back the stream to the SMS according to the corresponding request.
6. The SMS forwards the obtained streams to the decoder.
7. The decoder decodes the obtained stream and display the video on the smart wall.

C. Display Video Controlled by Keyboard on Smart Wall

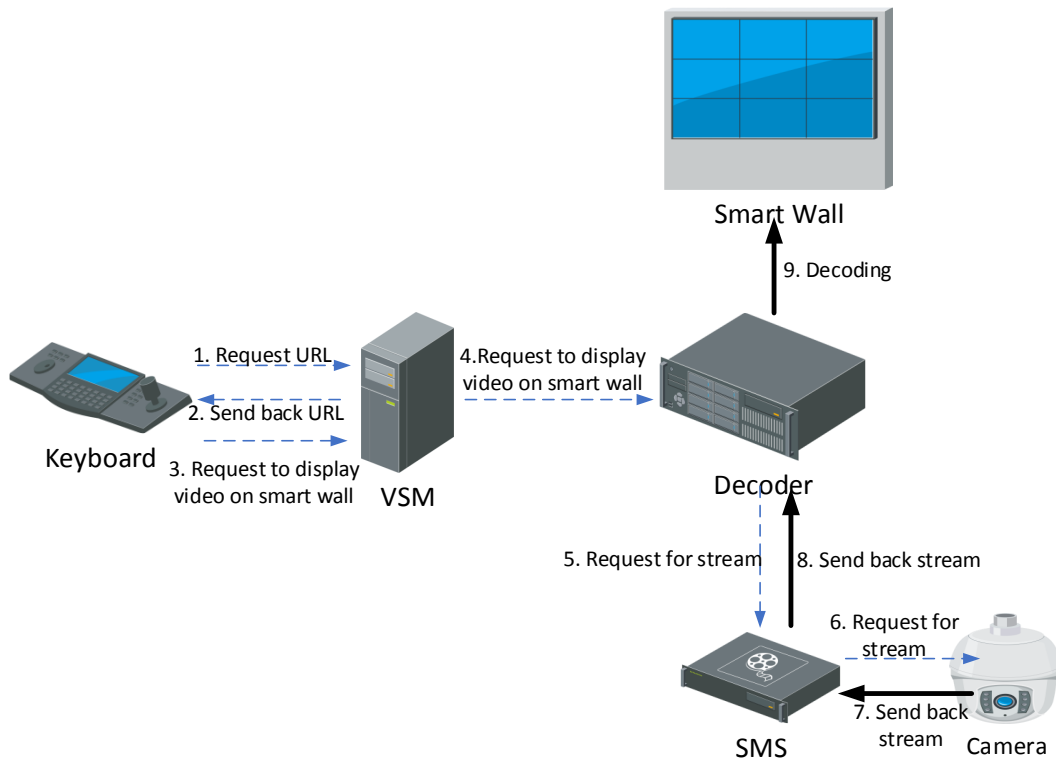
1. Display Video of Directly Connected Device Controlled by Keyboard on Smart Wall



If the decoder obtains the stream directly from the device, the signaling process is as follows:

1. The keyboard sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the keyboard.
3. The keyboard sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.
5. The decoder sends a request to the device for obtaining the stream.
6. The device sends back the corresponding stream to the decoder.
7. The decoder decodes the obtained stream and displays the video on the smart wall.

2. Display Video Controlled by Keyboard on Smart Wall via Streaming Server

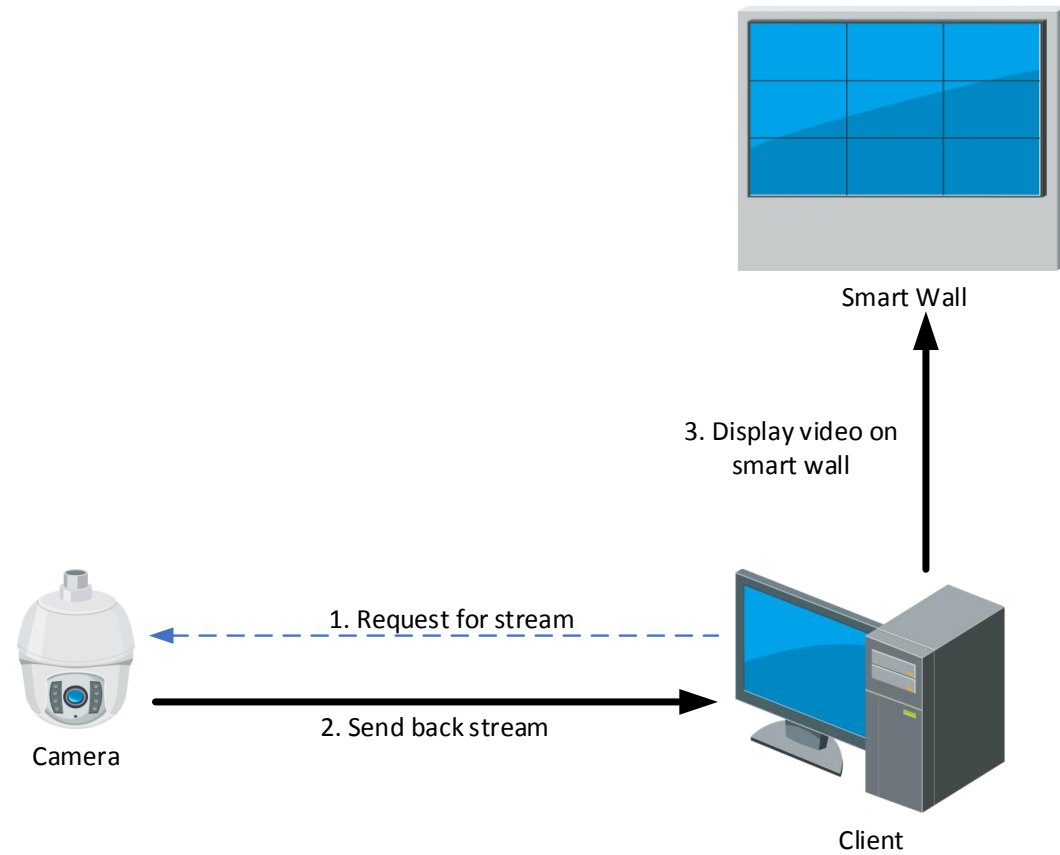


If the decoder obtains the stream via SMS, the signaling process is as follows:

1. The keyboard sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the Smart Wall Client.
3. The keyboard sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.
5. The decoder sends a request to the SMS (Streaming Server) for obtaining the stream.
6. The SMS forwards the request to the device for obtaining the stream.
7. The device sends back the corresponding stream to the SMS.
8. The SMS forwards the stream to the decoder.
9. The decoder decodes the obtained stream and displays the video on the smart wall.

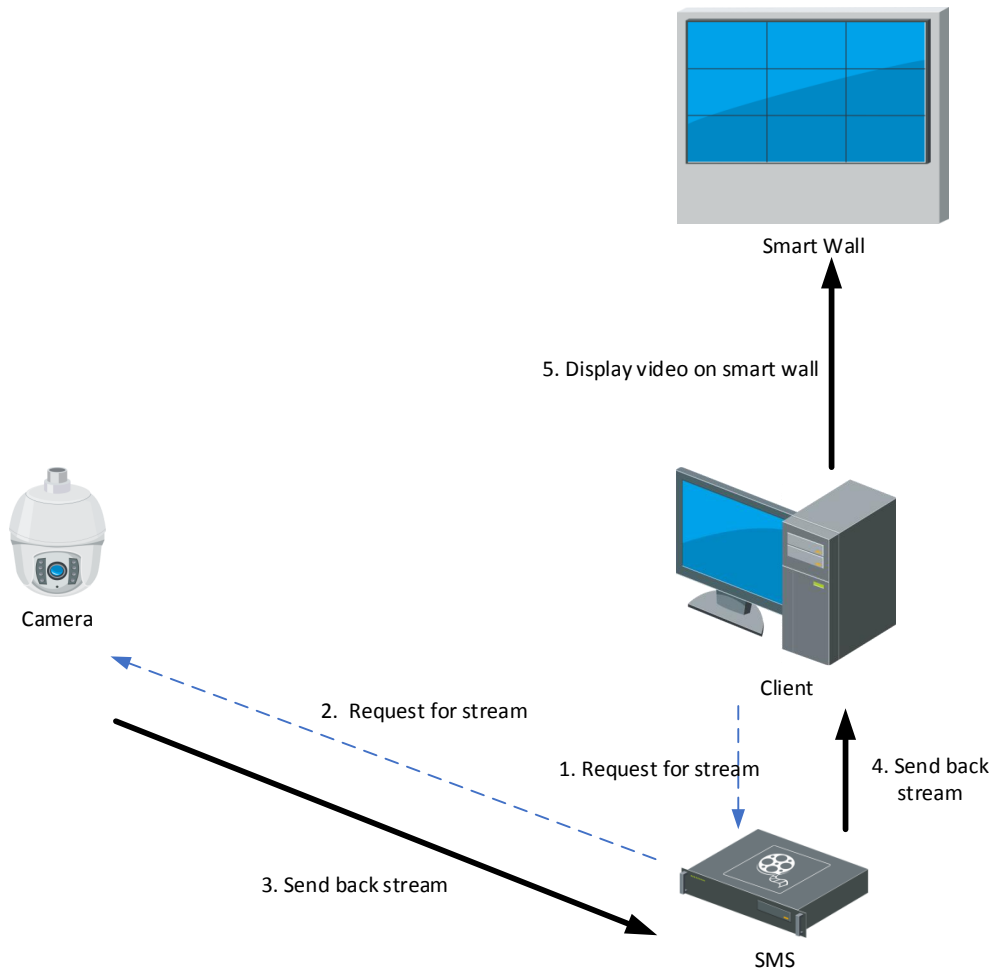
D. Display Video on Smart Wall (Graphic Card)

1. Display Video of Directly Connected Device on Smart Wall (Graphic Card)



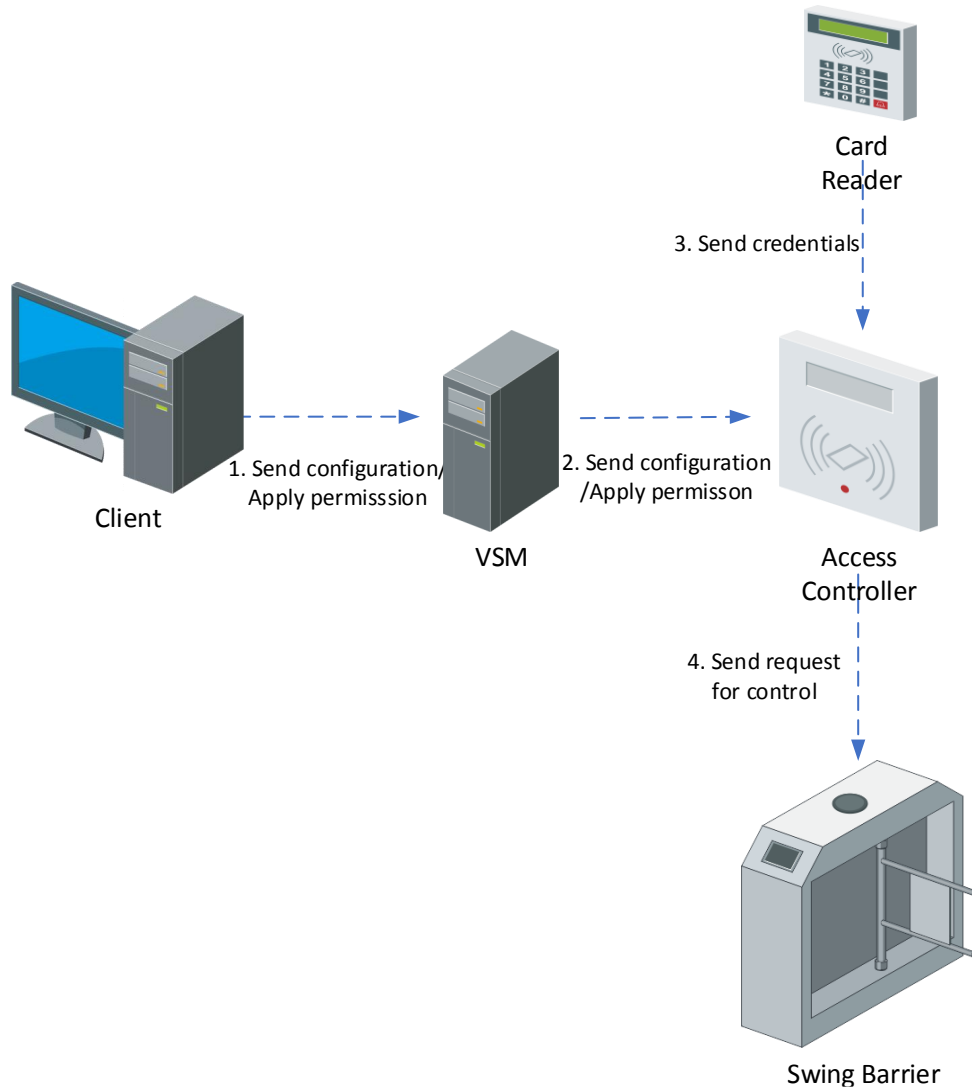
1. The client sends a request to the camera for obtaining the stream.
2. The camera sends back the corresponding stream to the client.
3. The client sends the stream to display on the Smart Wall (Graphic Card).

2. Display Video on Smart Wall (Graphic Card) via Smart Wall



1. The client sends a request to the SMS (Streaming Server) for obtaining the stream.
2. The SMS forwards the request to the camera for obtaining the stream.
3. The camera sends back the corresponding stream to the SMS.
4. The SMS forwards the obtained stream to the client.
5. The Client sends the stream to display on the Smart Wall (Graphic Card).

2.9.6 Access Control

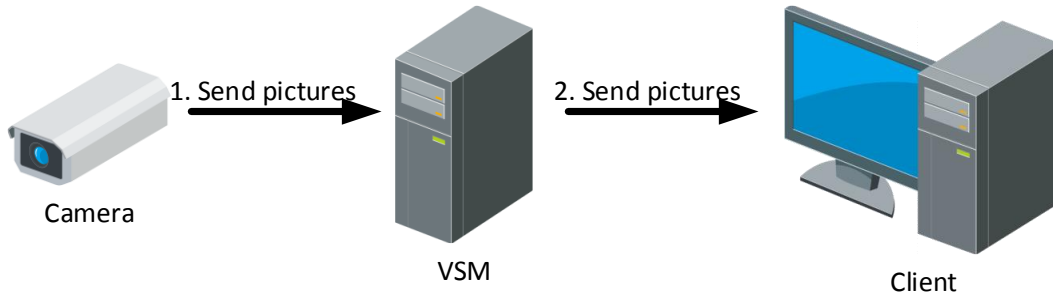


The signaling process of access control and management is as follows:

1. The Web Client sends an access control configuration command (including personnel permission, device configuration and event configuration) to the SYS server.
2. The SYS server sends the configuration command to the device.
3. The card reader obtains the corresponding instruction, and sends the credential information to the access controller.
4. The access controller sends the control request to the swing barrier according to the obtained instruction to control the switch status of the swing barrier.

2.9.7 ANPR

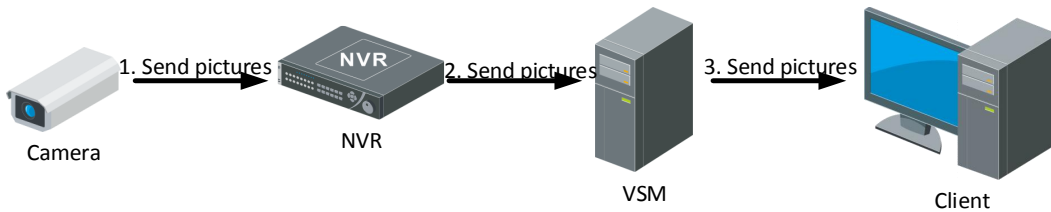
A. View Pictures Captured by ANPR Camera



According to the settings of the platform, the pictures can be stored in the SYS server locally or in the picture storage server.

If the picture is stored in the SYS server, the signaling process is as follows:

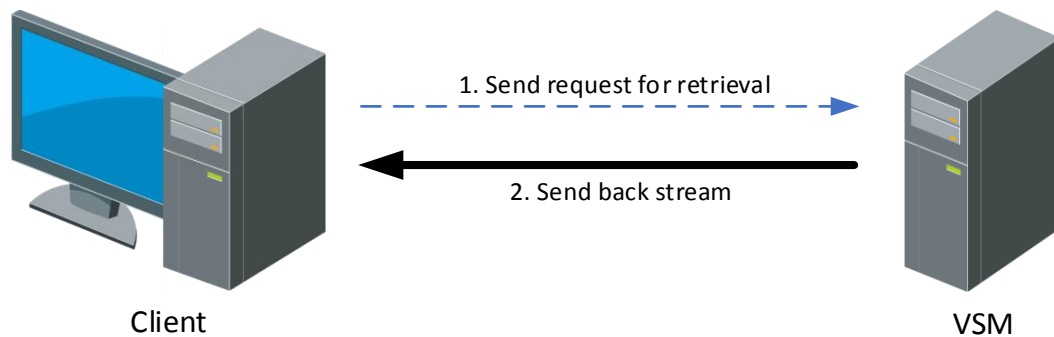
1. The ANPR camera captures the picture, and uploads the picture to the SYS server.
2. The SYS server sends the obtained picture to the Control Client for display.



If the picture is stored in the picture storage server (e.g. NVR), the signaling process is as follows:

1. The ANPR camera captures the picture, and uploads the picture to the NVR.
2. The NVR sends the obtained picture to the SYS server.
3. The SYS server sends the obtained picture to the Control Client for display.

B. Retrieval Pictures Stored in SYS Server

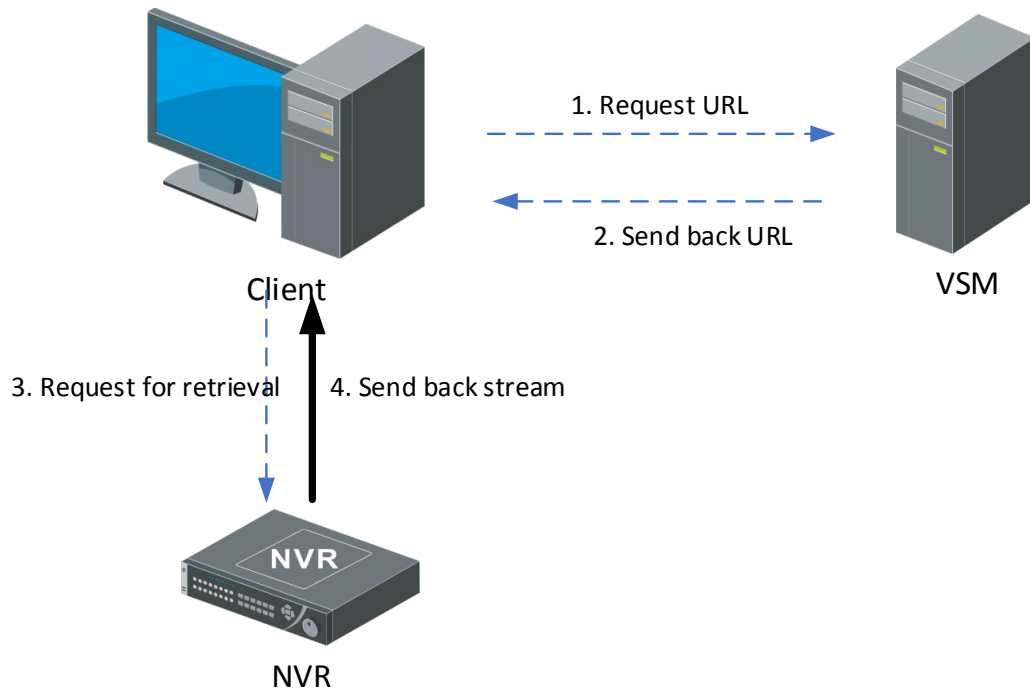


If the ANPR pictures is stored in the SYS server, the signaling process of ANPR picture retrieval and display is as follows:

1. The Control Client sends a picture retrieval instruction to the SYS server.
2. The SYS server search the required picture(s) and sends back the result to the Control Client.

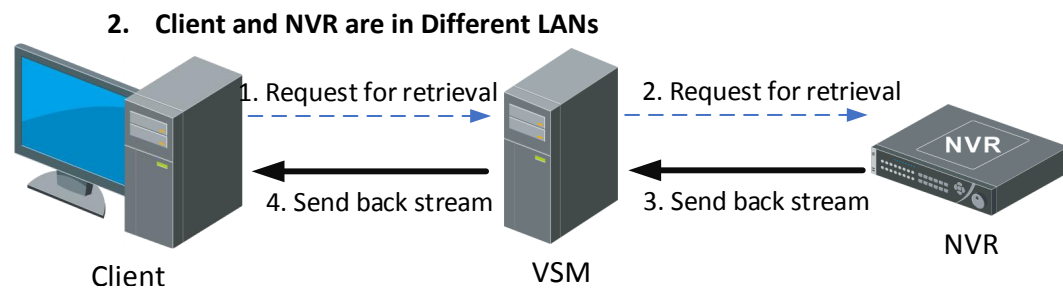
C. Retrieval Pictures Stored in NVR

1. Client and NVR are in the Same LAN



If the video is stored in the NVR that is in the same network with the Control Client, the process of obtaining the pictures captured by ANPR cameras is as follows:

1. The Control Client sends a request to the SYS server for obtaining the NVR URL information.
2. The SYS sends the corresponding URL information to the Control Client.
3. According to the obtained URL information, the Control Client sends an instruction to the NVR for obtaining the pictures captured by ANPR camera.
4. The NVR sends back the corresponding pictures to the Control Client according to the obtained instruction.



If the video is stored in the NVR that is not in the same network with the Control Client, the process of obtaining the pictures captured by ANPR cameras is as follows:

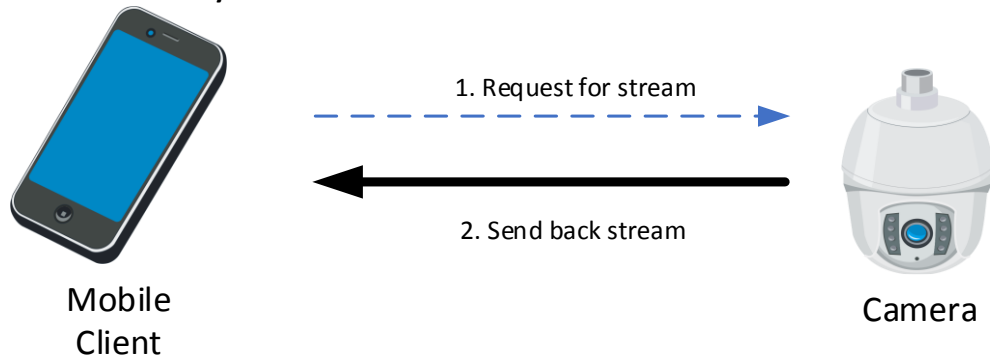
1. The Control Client sends a request to the SYS server for picture retrieval.
2. The SYS server sends the retrieval request to the NVR.
3. The NVR sends back the picture captured by ANPR camera to SYS server according to the request.
4. The SYS server forwards the obtained picture to the Control Client according to the actual instruction.

2.9.8 Mobile Client

A. Live view

The Mobile Client, like other clients, belongs to the HikCentral client. Therefore, the process of obtaining streams is the same as that of other clients.

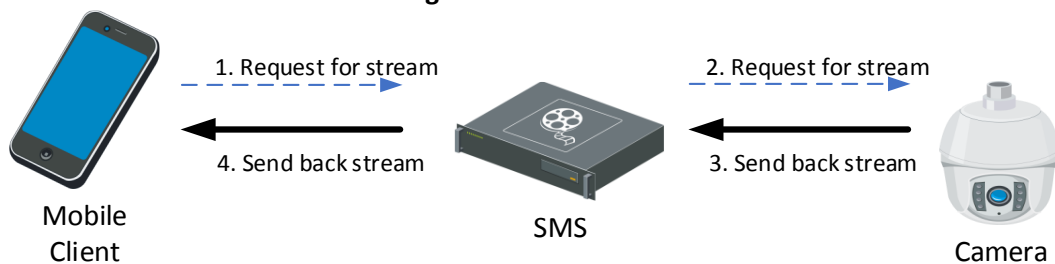
1. Live View for Directly Connected Device



If the Mobile Client and device are directly connected, the process of live view on the Mobile Client is as follows:

1. The Mobile Client sends a request to the device for obtaining the stream.
2. The device sends back the corresponding stream to the Mobile Client.

2. Live View via Streaming Server

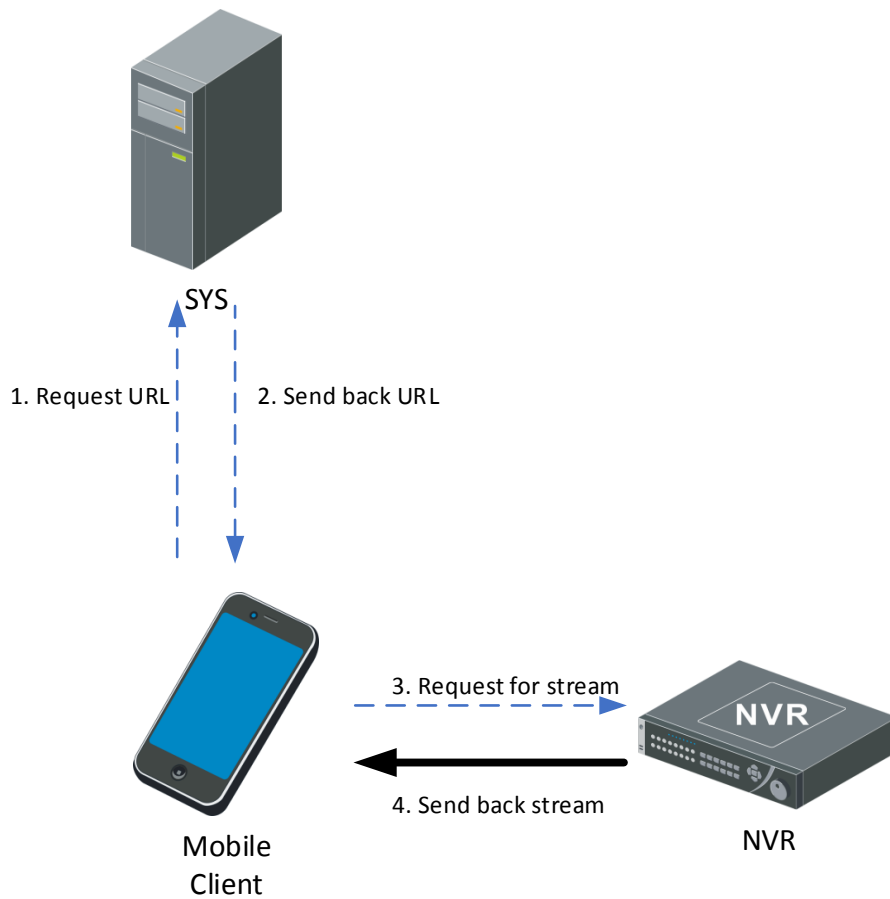


If the Mobile Client obtains the stream from the device via SMS (Streaming Server), the process is as follows:

1. The Mobile Client sends a request to the SMS for obtaining the stream.
2. The SMS forwards the request to the device for obtaining the stream.
3. The device sends back the corresponding stream to the SMS according to the request.
4. The SMS sends back the stream to the Mobile Client.

B. Playback

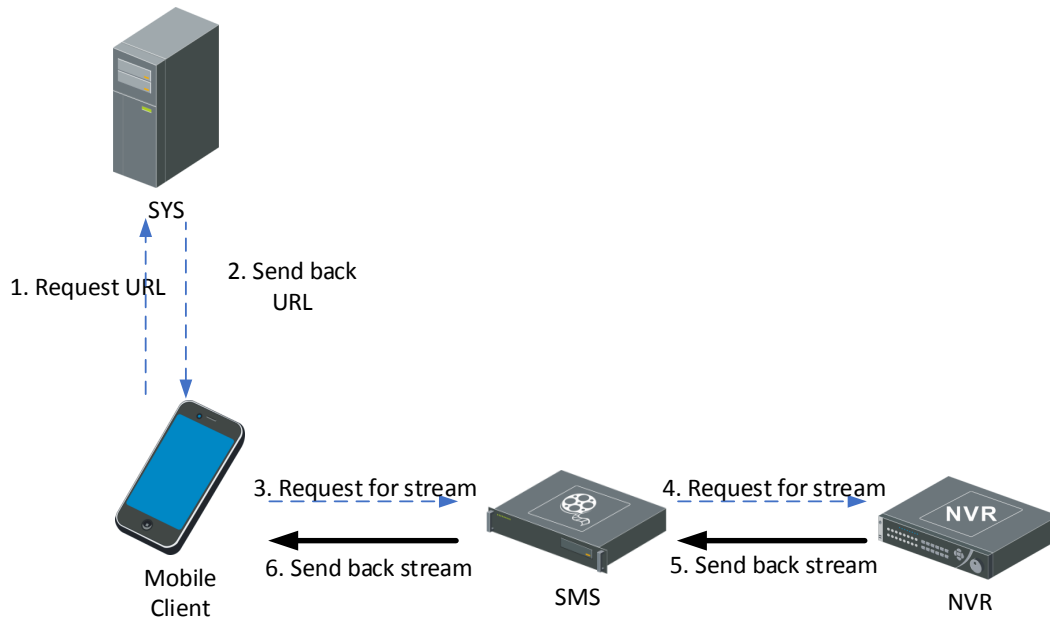
1. Playback of Video in Directly Connected Device



If the video file is stored in the directly device, the process is as follows:

1. The Mobile Client sends a request to the SYS server for obtaining the stream URL.
2. The SYS sends the stream URL information to the Mobile Client.
3. The Mobile Client sends a request to the directly connected storage device for obtaining the stream.
4. The storage device sends back the corresponding stream of playback to the Mobile Client.

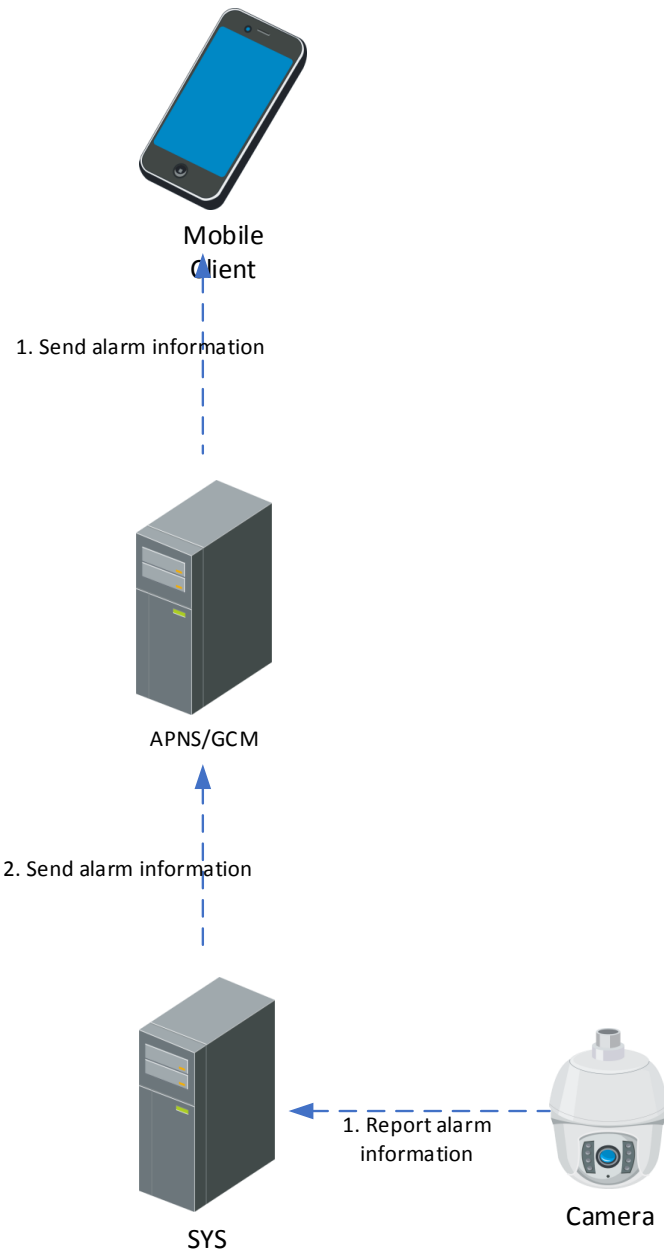
2. Playback via Streaming Server



If the Mobile Client obtains stream via SMS, the process is as follows:

1. The Mobile Client sends a request to the SYS server for obtaining the stream URL.
2. The SYS sends the stream URL information to the Mobile Client.
3. The Mobile Client sends a request to the SMS for obtaining the stream.
4. The SMS forwards the request to the NVR for obtaining the stream.
5. The NVR sends back the stream of playback to the SMS.
6. The SMS forwards the obtained stream to the Mobile Client.

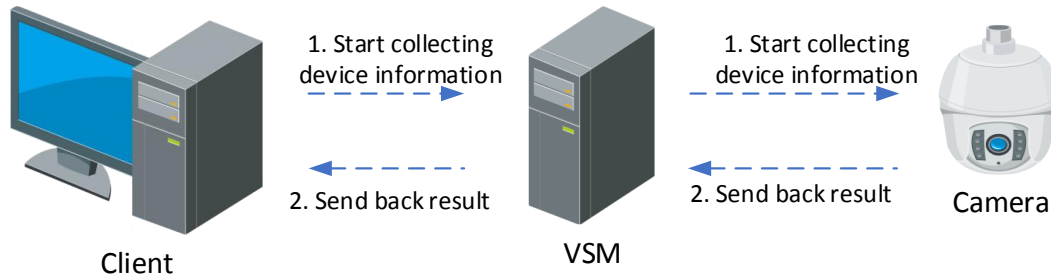
C. Alarm



Similar to the other clients, the process of receiving alarm video on Mobile Client is as follows:

1. The device reports an alarm to the SYS server.
2. The SYS server sends the obtained alarm information to the APNS/GCM server.
3. The APNS/GCM server sends the corresponding alarm information to the Mobile Client.

2.9.9 Status Monitoring



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

The platform initiates inspection information every 3 minutes.

A. Interaction Between SYS Server and Device

1. The SYS server sends an inspection command to the device.
2. The device sends back the status of the device to the SYS server.

B. Interaction Between Client and SYS Server

1. The Control Client sends an inspection command to the SYS server.
2. The SYS server sends the current status of the device to the Control Client.

2.10 System Security

2.10.1 Security Design Overview

The HikCentral Professional system consists of the server, client, service component, and platform SDK. The interaction between server and client, server and service component, server and platform SDK support HTTP and HTTPS.

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

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

2.10.2 System Security Solution

A. Access Protocol

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

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

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

B. Streaming Server Authentication

To ensure the overall security of the system, when the clients obtain live view or playback streams from devices via SMS (Streaming Server), the device must be authenticated by the SMS first.

C. Login Authentication

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

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

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

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

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

D. Platform Access

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

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

E. Sensitive Information Processing

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

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

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

2.10.3 Security Audit Server

Supports access of Hikvision Security Audit Server, which is used to monitor the logs of the managed devices in the system. You can set event and alarm rules for the security audit server via the Web Client. When the logs of the managed devices are regarded as abnormal, an event or alarm will be triggered and you can receive the alarm via the Control Client. In this way, the system can monitor the running status of the managed devices by the security audit server, reaching the system security requirements.

2.11 Open Platform

2.11.1 Access Solution of Third-Party Devices

A. Introduction

HikCentral Professional provides access capabilities based on standard ONVIF protocol for the third-party devices. The third-party devices can connect to the HikCentral Professional via ONVIF protocol to implement the functionalities of live view, playback, PTZ control, video search, alarm, and so on. To connect the third-party devices with HikCentral Professional, there are mainly two methods. One method is that, the third-party devices firstly connect to the Hikvision NVR, and then connect to HikCentral Professional via the NVR. The other method is that, the third-party devices directly connect to HikCentral Professional by configuring pStor, Hybrid SVN, or cloud storage. In the above two method, the NVR, pStor, Hybrid SVN, or cloud storage are used to save the video files, and the HikCentral Professional is used to manage and play the videos.

B. Overall Design

The server of HikCentral Professional contains multiple components for the access of the third-party devices. You can log in to, manage, and operate the third-party devices on HikCentral Professional via these components.

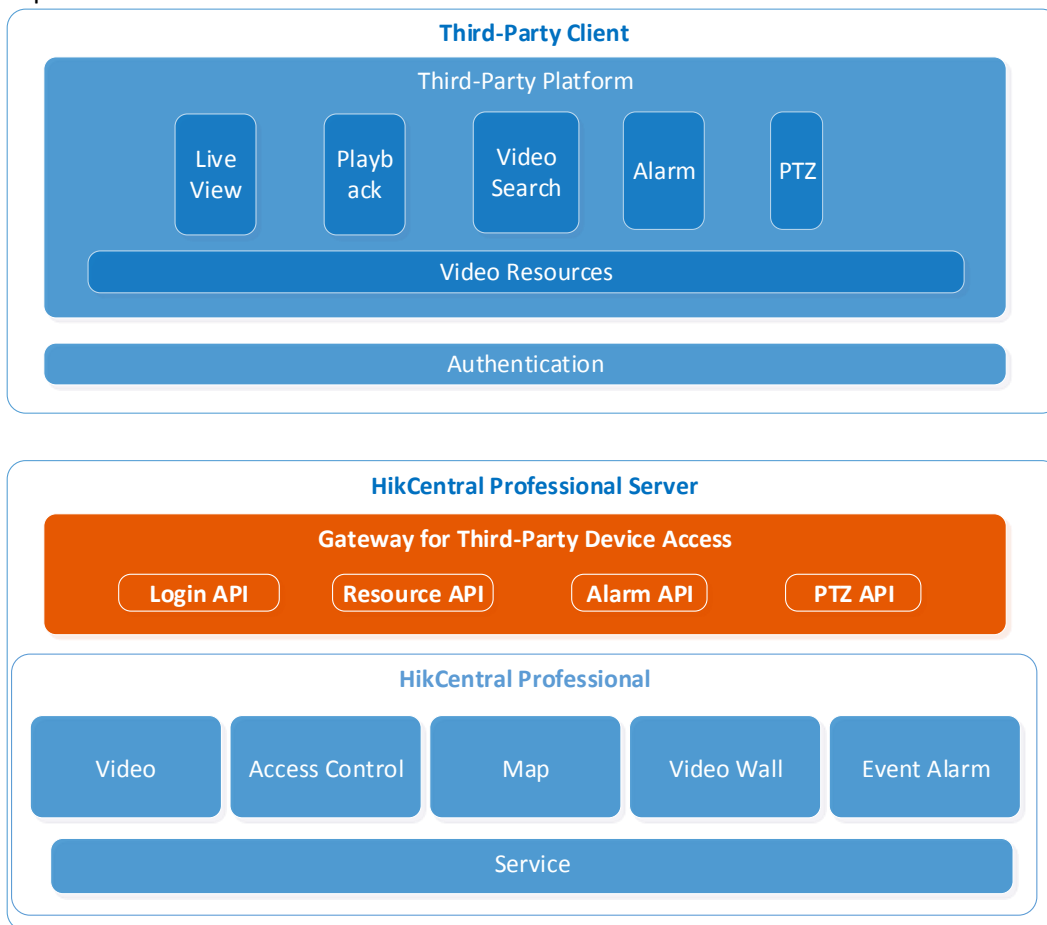


Figure 8-1 Overall Design Diagram

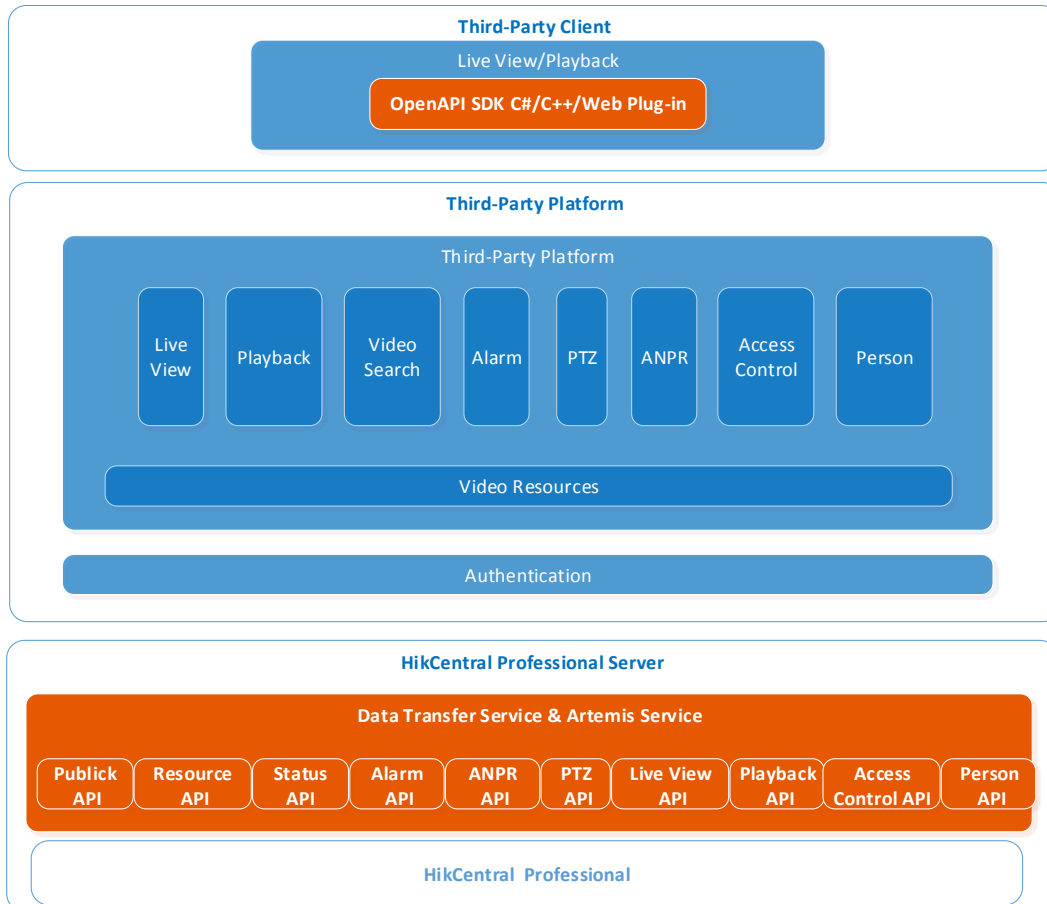
2.11.2 Integration Solution of Third-Party Platform

A. Introduction

HikCentral Professional provides OpenAPI for the connection between third-party platform and HikCentral Professional. The third-party platform can implement the core functionalities of HikCentral Professional via OpenAPI, such as video, alarm, resources, access control, and so on.

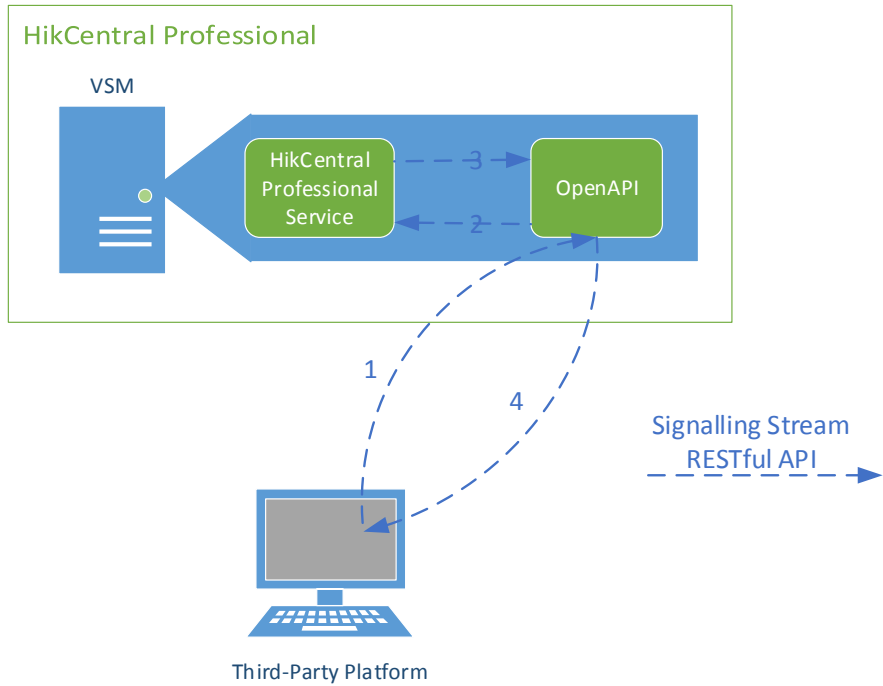
B. Overall Design

OpenAPI consists of Data Transfer Service, Artemis Gateway, and Video SDK. The Data Transfer Service converts the protocols between servers of HikCentral Professional and third-party platform. The Artemis Gateway provides the API protocol management, third-party integration management, and authentication. The Video SDK provides the capabilities of live view, playback, two-way audio, and so on, which helps the third-party client to integrate the video related functions quickly.

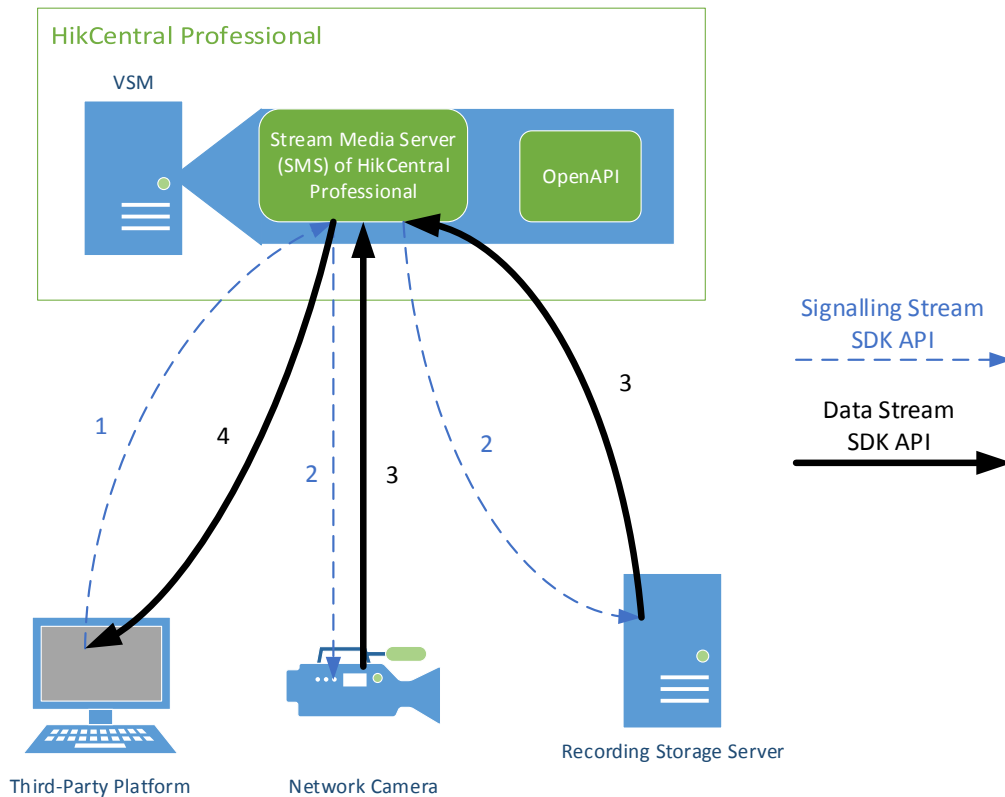


C. Network Topology

As there are multiple domain scenes deployed for HikCentral Professional services and OpenAPI, to ensure the stability of OpenAPI and the security of whole system, the OpenAPI and HikCentral Professional must be in same LAN (Local Area Network), but they can be installed in different computers or same computer.



The communication between the third-party platform and OpenAPI is based on RESTful protocol, and it is used for getting resources, operating the resources, and so on. Firstly, the third-party platform sends request command to OpenAPI service, and then the OpenAPI converts the command to support the internal protocol of HikCentral Professional and sends the converted command to HikCentral Professional server. The HikCentral Professional will send a response to OpenAPI after receiving and processing the request command. Finally, the OpenAPI converts the response to support OpenAPI protocol and sends the converted response to the third-party platform.



The above figure shows the interaction process between third-party platform and Video SDK, which realizes the live view and playback. Firstly, the third-party platform sends live view or playback request to HikCentral Professional, and then the Streaming Server (SMS) of HikCentral Professional finds the devices to start live view or playback. Finally, the video stream will also be returned to the third-party platform from the device via the SMS.

D. Overall APIs

The interaction and transmission of OpenAPI adopts RESTful protocol and it only supports HTTPS. The following table shows the API classes and the corresponding functional descriptions, for details, refer to HikCentral Professional OpenAPI_Developer Guide_V1.6.0.pdf.

API Class	Description
Public API	Provide public functions, such as getting version information of platform and so on.
Resource (Encoding Device) API	Provide functions related with encoding devices, such as management, refreshing, activation, and so on.
Resource (Server)	Provide functions related with servers, such as Streaming Server management, Storage Server management, and so on.
Resource API	Provide functions related with resources in area, such as area management, camera management, door management, alarm input and output management, and so on.
Alarm API	Provide alarm functions, such as alarm configuration and receiving, and so on.
ANPR API	Provide ANPR functions, such as list configuration, vehicle passing record search, vehicle information settings and management, and so on.
Log Search API	Provide functions related with platform logs, such as alarm log search, and so on.

Status Detection API	Provide functions of camera status detection, device status detection, server, status detection, and so on.
PTZ API	Provide function related with PTZ control, such as preset, patrol, pattern, and so on.
Live View and Playback API	Provide functions of getting live view URL, playback URL, tag management, and so on.
Access Control API	Provide functions of opening door, closing door, person information management, searching for card swiping records, and so on.
Person API	Provide functions of getting person list, getting person information, and so on.

The API classes and functional descriptions of OpenAPI Video SDK are shown in the table below.

API Class	Description
Live View API	Provide functions of starting or stopping live view, stream type switch, capturing, audio control, recording, and so on.
Playback API	Provide functions of starting or stopping playing, pausing or resuming playback, reverse playback, fast or slow forward, capturing, audio control, searching or downloading video files, and so on.
Two-Way Audio API	Provide function of starting two-way audio between device and platform.

E. Installation Environment and Development Language

The OpenAPI must be installed on the computer with Window operating system.

For protocol integration, there is no development language limit; but for Video SDK integration, the development language should be C# or C++, or by developing a plug-in on web browser via some certain language.

END OF SECTION

Part 3 Functions

The content in this section describes the functions of HikCentral Professional. All the information hereinafter are for description and explanation only. The information contained here is subject to change, without notice, due to firmware updates or other reasons. For detailed instructions about these functions, please refer to the *User Manual of HikCentral Professional*.

3.1 General Functions

A. On initial set up and during first login on Web Client, Control Client, and Mobile Client, the Administrator is forced to create a complex password for future logins sessions. The new password shall reach Medium password strength

B. Manage Devices and Servers on Web Client

1. Add encoding devices, decoding devices, access control devices, elevator control devices, video intercom devices, security control devices, dock stations, UVSSs (Under Vehicle Surveillance System), network transmission devices, guidance screens, digital signage terminals, IP speakers, guidance terminals, security inspection devices, Recording Servers, Streaming Servers, DeepinMind Servers, and Security Audit Servers.
2. Upgrade device firmware via Web Client, Hik-Connect, or FTP
 - a. Simultaneous upgrade
 - b. Set upgrade schedule
3. Restore/reset device password
4. Create password for inactive devices and edit online device's network information

C. Area Management on Web Client

1. Create up to 3,000 areas with 5 levels, and up to 100,000 areas for Remote Site Management
2. Add up to 256 resources (including cameras, doors, elevators, alarm inputs, alarm outputs, UVSS, radars, digital signage terminals, speaker units, and third-party integrated resources) respectively to one area per SYS
3. Add resources to other area, and display resources in sub-areas
4. Synchronize resource names from devices and apply resource names to devices

D. Map Management on Web Client

1. Shall have the ability to configure related map settings for current site:
 - a. Shall upload picture or import existing map of other area to link related map to the area
 - b. Shall edit picture or map name
 - c. Shall unlink the map to cancel the linkage between the map and area
 - d. Shall view the map in full-screen mode
 - e. Shall zoom in or zoom out the map
 - f. Shall adjust the map area for view and switch between GIS map and related map
 - g. Shall add resources, including cameras, alarm inputs, alarm outputs, access points, radars, UVSS, and third-party integrated resources, as hot spots on the related map
 - h. Shall adjust the hot spot location, edit, and delete hot spot
 - i. Shall add a map to another map as a hot region
 - j. Shall adjust hot region location, edit hot region, and delete hot region
 - k. Shall add/edit/delete labels on map, and adjust label location
 - l. Shall add/edit/delete resource groups, including people counting group, heat analysis group, pathway analysis group, people feature analysis group, multi-door interlocking

- group, anti-passback group, emergency operation group, entry & exit counting group, and security control partition (area) on map, and adjust resource group location
- m. Shall add/edit/delete the parking lot or entrance & exit on map, and adjust its location
- n. Shall add/edit/delete the combined alarm on map, and adjust combined alarm location
- o. Shall display the following elements on the map: hot spots, hot region, label, resource group, parking lot/entrance & exit, and combined alarm
- 2. Shall have the ability to configure GIS map settings of current site:
 - a. Shall add cameras/access points/radars/alarm inputs/alarm outputs/UVSSs on GIS map to show the geographic location
 - b. Shall locate cameras on map automatically according to the GIS location information settings on the device
 - c. Shall add up to 4 UVSS(s) to each SYS
 - d. Shall set GPS location for hot spot and hot region
 - e. Shall set icon style and name color, and add remark to GIS map
 - f. Shall add/delete/edit labels
 - g. Shall add/edit/delete resource groups, including people counting group, heat analysis group, pathway analysis group, people feature analysis group, multi-door interlocking group, anti-passback group, emergency operation group, entry & exit counting group, and security control partition (area)
 - h. Shall add/edit/delete parking lot/entrance & exit
 - i. Shall add/edit/delete combined alarm
 - j. Shall add/edit/delete the Remote Site and adjust its location
 - k. Shall choose to display the following elements on the map: hot spots, hot region, label, resource group, parking lot/entrance & exit, combined alarm, and Remote Site.
 - l. Shall search geographic location in GIS map
 - m. Shall enable GIS map function and support online map (configure the map API URL) and offline map, and set the icons of the hot region, camera, access point, alarm input, alarm output, UVSS, etc., on the map

E. Security Settings on Web Client

1. Shall create user profile groups defined as Roles
2. Role shall restrict user profile access for administration functions defined as logical areas
3. Shall set the role's effective period
4. Shall set the permission schedule
5. Shall set the role status as active or inactive
6. Shall set resource access for the following types:
 - a. Resource in area:
 - Access all resources in shown area
 - Access specified resources in shown area
 - b. Intelligent analysis group
 - People Counting Group
 - Heat Analysis Group
 - Person Feature Analysis Group
 - Pathway Analysis Group
 - c. Security control partition (area)
 - d. Encoding device (NVR, Network Camera)
 - e. Decoding device
 - f. Access control device

- g. Video intercom device
 - h. Elevator control device
 - i. Security control device
 - j. Dock stationNetwork transmission device
 - k. Smart wall
 - l. Guidance screen
 - m. Digital Signage Terminal
 - n. IP speaker
 - o. Security inspection device
 - p. Servers
 - q. Person group
 - r. Face Comparison Group
 - s. Dock Station Group
 - t. Visitor List
 - u. Vehicle List
 - v. Custom additional information
 - w. User-defined event
 - x. User
7. Shall set the following user permission:
 - a. Resource permission
 - b. Configuration permission
 - a. Operation permission
 8. Shall support general application scenario
 9. Shall set management permissions for every module. Users without module permissions cannot edit permission settings through security module
 10. Shall manage the permission of checking, adding, deleting, editing of each module on the Control Client
 11. Shall support the 'copy from' function to copy features of the existing roles
 12. Users
 - a. Create user name
 - b. Default password or set a password for initial login and then user must create a unique password
 - c. Set expiry date of user profile
 - d. Email address setting: if the user forgets his/her password, he/she can reset password via email
 - e. Select user status as active or inactive
 - f. For each user, restrict concurrent logins
 - g. PTZ control permission level: notify the user with lower PTZ permission that PTZ control has been appropriated by another user with higher permissions
 - h. Assign permission of automatically receiving alarms to user
 - i. Assign roles to the user
 - j. View role list and detailed information
 - k. Import domain users (group)
 - Select importing mode as user, group, or security group
 - Select domain users (user group)
 - Configure domain users
 - Select domain user status as active or inactive
 - Restrict concurrent logins

- Set PTZ control permission
 - Assign permission of automatically receiving alarms
 - Assign role to the domain user
 - View role list and detailed information
- l. Force logout
 - m. Select users and activate/inactivate them in a batch
13. Synchronize domain users
 14. Active Directory Integration
 - a. Import Windows domain users and assign them to roles
 - b. Domain user login supported in the Control Client and Mobile Apps (iOS and Android)
 15. Security Settings for Users
 - a. Lock IP address after failed password attempts
 - Configurable: 1 to 5 attempts
 - Lock for: 10, 20, 30, 40, 50, or 60 minutes
 - b. Minimum password strength: Shall have the ability to select from the following:
 - Weak: a combination of at least 8 characters including two types of characters among lowercase letters, uppercase letters, numbers, and special characters.
 - Medium: a combination of at least 8 characters including two types of characters among lowercase letter, uppercase letters, numbers, and special characters. The combination cannot be (number + lowercase letters) or (number + uppercase letters)
 - Strong: a combination of at least 8 characters including a minimum of three types of characters among lowercase letters, uppercase letters, numbers, and special characters
 - c. Shall enable Maximum Password Age
 - Configurable: 1 months, 3 months, 6 months or “custom” number of days ranging from 1 to 365
 - d. Shall have the ability to auto lock Control Client after a time period of inactivity on Control Client
 - Configurable: Lock in 10 minutes, 20 minutes, 30 minutes or “custom” number of minutes ranging from 10 to 30
 - e. Shall enable Double Authentications
 - Select authenticator and users who need authentication
 - Authenticatable permissions: Playback, Manual Recording, and Export Video
 16. Shall set permission schedule template

F. System Configuration on Web Client

1. Shall set the following normal parameters
 - a. Set user preference
 - Site name
 - First day of week
 - Temperature unit: Celsius, Fahrenheit, or kelvin
 - Display or hide mask related functions: After disabled, all the functions about masks will be hidden on Web Client, Control Client, and Mobile Client
 - Calendar type: Gregorian Calendar, Thai Calendar, and Nepali Calendar
 - b. Set holiday parameters
 - Holiday name
 - Holiday type: Regular Holiday or Irregular Holiday

- Start date
 - Number of days
 - Repeat Annually
- c. Set printers
 - d. Set template for printing cards
 - Template name
 - Shape: Vertical or Horizontal
 - Front style
 - Back style
2. Shall set the following network parameters
 - a. NTP settings: shall be able to be set for syncing the time between the SYS and the NTP server
 - b. Active directory: If you have the AD (Active Directory) domain controller which contains the information (e.g., user data, computer information), you shall be able to configure the settings to get the related information. In this way, you can add the users that belong to an organization unit (e.g., a department of your company) to HikCentral Professional conveniently
 - Link person information (email and custom additional information items by default)
 - c. Allow ISUP registration or not and allow devices of ISUP version 2.6 or 4.0 to access the system or not
 - d. Set a static IP address or domain name for the WAN access, and set the ports
 - e. Select the IP address for receiving information from devices by ONVIF protocol and ISUP protocol. Set the NIC of the current SYS server or enter an IP address manually
 3. Shall set the following storage parameters:
 - a. Storage on SYS server:
 - Select storage location for pictures and files
 - Restrict quota for pictures and files
 - Set storage quota
 - b. Set the data recorded duration for the follow types of records:
 - Received events
 - Service error logs
 - Service warning logs
 - Service information logs
 - Recording tags
 - Face comparison data
 - Video analysis data
 - Card swiping records
 - Attendance records
 - Visitor check-in record
 - Vehicle passing records
 - Vehicle entering/exiting records
 - Radar pattern data
 - Data recorded by devices: Including data recorded by the access control devices, elevator control devices, video intercom devices, and alarm inputs of these devices, and other records except access records on the doors.
 - Skin-surface temperature data
 - Visitor Reservation data

- Payment data
 - Parking records
 - Set the duration as three months/six months/one year/two year/three years
4. Shall add email template:
 - a. Add email template for receiving reports
 - Template name
 - Recipients: domain user or email address
 - Email subject
 - Email content
 - b. Add email template for event and alarm linkage
 - Template name
 - Recipients: Up to 64 recipients can be added; add domain user/ email address as recipient
 - Email subject
 - Email content
 - Image attachment
 - Content language
 - c. Configure the following email parameters
 - Server authentication
 - Cryptographic protocol
 - Sender email address
 - Sender name
 - SMTP server address
 - SMTP server port
 - User name
 - Password
 - Email test
 5. Shall set security parameters
 - a. Set Clients and SYS server transfer protocol as HTTP or HTTPS Advanced settings:
 - b. Generate certificate between services in system and export certificate between system and Recording Server
 - c. Before adding the Streaming Server or Cloud Storage Server to the system, you should export the service component certificate on this page and import it to the Streaming Server or Cloud Storage Server you want to add
 6. Shall set third-party integration parameters
 - a. Enable integration via Optimus
 - b. Enable Integration via OpenAPI
 - c. Enable data interchange including database synchronization and access records dump
 7. Shall set advanced parameters
 - a. Enable hot spare configuration
 - b. Reset network information
 - c. Set database password by admin user
 8. Shall enable company information display and set company information for customization requirement
 9. For facial recognition camera/ANPR camera/thermal camera (report supported), you shall select the added cameras as these three types of cameras on License details page.

Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally on the platform.

G. Log into the Control Client

1. Shall have the ability to enable auto-login, and login via domain name and password
2. Shall have the ability to automatically launch the client and login with the domain user
3. Shall have the ability to log in to the Control Client through HTTP or HTTPS
4. Shall have the ability to customize module arrangement on Control Panel

H. Control Panel Management on Control Client

1. Group modules and customize the module arrangement on the control panel
2. Add modules to the navigation bar, clicking a module on navigation bar to quickly access the module, and searching for modules
3. Display the resource updating indicator, time, and CPU usage/network speed on the title bar of Control Client
4. Guidance about how to start using the Control Client for the first-login user
5. Display the default control panel for the first-login user
6. Edit the name and the layout (including adding windows, deleting windows, editing windows, moving windows, and adjusting the window size) of control panel
7. Restoring to the default control panel when editing
8. Self-adaptive layout of the control panel based on different screen resolutions
9. Manage multiple control panels, including adding, deleting, and switching control panels
10. Open and close auxiliary screen for the control panel
11. Display the control panel in the full screen mode and exiting the mode, maximize or minimize the window, and display the window in auxiliary screen
12. Restore the control panel after restarting the Control Client or switching users

I. Map Management on Control Client and Mobile Client

1. Ability to show the related map of the alarm
2. Ability to show resource and view the details on the map
3. Ability to switch between the configured maps
4. Ability to filter resources on the map according to resource type
5. Ability to view live view of a single/multiple resource(s) on the map
6. Ability to search, then jump to the pointed place
7. Ability to add label to map
8. Ability to view history alarm
9. Ability to control status of the doors on the map
10. Cross-site map display and operation
11. Ability to operate the third-party integrated device on map
12. Ability to view the number of people in specified region in real-time on the map according to the resource group settings

J. Maintenance on Web Client

1. Create maintenance reports to be regularly sent
 - a. Set the following report type:
 - People counting
 - People counting for one camera
 - People counting in one region
 - People density analysis

- Queue analysis
 - Heat analysis
 - Heat analysis for one camera
 - Heat analysis in one region
 - Pathway analysis
 - Person feature analysis
 - Feature analysis for one camera
 - Feature analysis in one region
 - Skin-surface temperature analysis
 - Temperature screening point
 - Person group
 - Temperature analysis
 - Vehicle analysis
- b. Set the report name
 - c. Set the event report target
 - d. Set report type
 - e. Set report sending time
 - f. Select email template
 - g. Set the report language
2. Server usage thresholds: Set event/alarm for notification if the CPU usage or RAM usage approaches the pre-determined threshold and lasts for certain duration
 3. Set network timeout
 - a. Default
 - b. Default x 1.5
 - c. Default x 2
 4. Set health check frequency
 - a. Device health status
 - b. Server health status
 - c. Others
 5. Backup and restore system data:
 - a. Shall set database backup of HikCentral Professional system, including configured data, configured pictures, received events, received alarms, face comparison data, card swiping records, attendance records, vehicle passing records, video analysis data, and server logs
 - b. Shall set the frequency of backup as daily, weekly or monthly
 - c. Shall set the backup date
 - d. Shall set the backup time
 - e. Shall check the saving path
 - f. Shall set the max. number of backups
 - g. Shall restore the configured data
 6. Export configuration data of Remote Site, encoding device, and recording settings
 7. Download HikCentral Professional Control Client on the Web Client
 8. Activate/deactivate license in online/offline mode, update the license in online/offline mode, and view license detailed information for system capabilities (available for admin user only)
 9. Set when to send a SUP upgrade prompt and who can receive the prompt
- K. Audit Trial on Web Client and Control Client: Search and View Logs**
1. Server Logs

- a. Error Log
- b. Warning Log
- c. Information Log
- 2. Device Logs
 - a. Online/offline logs
 - b. Logs on device
- 3. Resource Logs
 - a. Online/offline logs
 - b. Recording status
- 4. Log searches are based on operation, user, and time interval searches of:
 - a. Today
 - b. Yesterday
 - c. Current week
 - d. Last 7 days
 - e. Last 30 days
 - f. Custom time interval

L. Health Monitoring on Web Client, Control Client and Mobile Client (iOS)

1. Ability to provide near real-time information about the status of the SYS server and added resources (e.g. Recording Servers, Streaming Servers, connected cameras, encoding devices). It is critical to multiple aspects of operating the servers or devices and is especially important for maintenance. When a resource exception occurs, you can enter this module to check the resource status and find out the abnormal device(s) and view the exception details.
Part of the following functions may not be supported by Mobile Client.
2. Overview: Provide status of the following devices and the ability to click on items for a detailed report if there is no network transmission device added in the platform:
 - a. Set auto refresh or refresh manually
 - b. Display health monitoring on smart wall (graphic card)
 - c. Display health monitoring on auxiliary screen
 - d. Offline/total number of cameras
 - e. Number of camera with video loss
 - f. Number of camera with communication exception
 - g. Number of camera with recording exception
 - h. Number of camera with no recording schedule
 - i. Number of camera with arming exception
 - j. Abnormal/total number of access points
 - k. Offline/total number of UVSS(s)
 - l. Offline/total number of Remote Sites
 - m. HikCentral Professional Service status
 - Management server status
 - Memory status
 - CPU status
 - RAM status
 - Network status
 - Streaming gateway usage
 - Picture storage usage
 - n. Recording Server status

- o. DeepinMind Server status
 - p. Security audit server status
 - q. Number of streaming server with exception
 - r. Number of streaming server with notice
 - s. Number of normal streaming server
 - t. Total number of streaming server
 - u. Number of recording server with exception
 - v. Number of recording server with notice
 - w. Number of normal recording server
 - x. Total number of DeepinMind server
 - y. Number of DeepinMind server with exception
 - z. Number of DeepinMind server with notice
 - aa. Number of normal DeepinMind server
 - bb. Abnormal/total number of encoding devices
 - cc. Abnormal/total number of access control devices
 - dd. Abnormal/total number of video intercom devices
 - ee. Abnormal/total number of elevator control devices
 - ff. Offline/total number of decoding devices
 - gg. Abnormal /total number of security control devices
 - hh. Abnormal /total number of dock stations
 - ii. Abnormal/total number of IP speakers
 - jj. Abnormal/total number of security inspection devices
3. Overview (Topology): If there are network transmission devices managed in the system, the topology of devices will be displayed for network maintenance, which is a figure that displays the connection relation of network transmission devices, security devices, etc.
 - a. Display the hierarchical relationship of the devices, device information, link status and alarm information, etc.
 - b. View device details, including basic information, device usage, device panel status and port information
 - c. View link details, including stream rate, connected device type and port information, etc.
 - d. If there is data transmission failure between the devices, you can view the connection path to judge which link is disconnected, to maintain the link efficiently
 - e. Export the real-time status overview page in PDF format, or export the exception data in Excel/CSV format
 4. Camera of Central System: Provide the status of the followings:
 - a. Name
 - b. Address
 - c. Area
 - d. Connection number
 - e. Network status
 - f. Video signal
 - g. Recording status
 - h. Arming status
 - i. Operation: Refresh to get the real-time status immediately of the camera; go to area of the camera; view the online/offline records; view recording status; view the videos of cameras with abnormal images and export the image diagnosis results
 5. Camera of Remote Site: Provide the status of the followings:
 - a. Name

- b. Address
 - c. Area
 - d. Network status
 - e. Recording Status (in Central System)
 - f. Arming status
 - g. Operation: Refresh to get the real-time status immediately of the camera; go to area of the camera; view the videos of cameras with abnormal images and export the image diagnosis results
6. Door: Provide the status of the followings:
- a. Name
 - b. Access Control Device
 - c. Area
 - d. Access Control Device network status
 - e. Face Recognition Terminal network status
 - f. Door status
 - g. Configured Door status
 - h. Operation: Refresh to immediately get the real-time status of the door; go to area of the door; Control door status as: Unlock/Lock/Remain Unlocked/Remain Locked
7. Elevator: Provide the status of the followings:
- a. Name
 - b. Elevator Control Device
 - c. Area
 - d. Elevator Control Device network status
 - e. Card reader status
 - f. Floor status
 - g. Configured floor status
 - h. Operation: Refresh to immediately get the real-time status of the floor; go to area of the elevator; Control floor status as: Temporary Access/Access with Credential/Free Access/Access Forbidden
8. Alarm Input: Provide the status of the followings:
- a. Name
 - b. Linked device
 - c. Area
 - d. Security partition (area)
 - e. Network status
 - f. Arming status
 - g. Bypass status
 - h. Fault status
 - i. Alarm status
 - j. Detector status
 - k. Power status
 - l. Checking time
 - m. Operation: Refresh to immediately get the real-time status of the alarm input; filter status by device type
9. UVSS: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Area

- d. Network status
 - e. Line Scan Camera status
 - f. Capture Camera status
 - g. Storage status
 - h. Operation: Refresh to immediately get the real-time status of the UVSS; go to area of the unit
10. Speaker Unit: Provides the status of the followings:
- a. Name
 - b. IP speaker
 - c. Area
 - d. Network performance
 - e. Checking time
 - f. Operation: Refresh to immediately get the real-time status of the speaker unit; go to area of the unit
11. Third-Party Integrated Resource: Provides the status of the followings:
- a. Name
 - b. Resource type
 - c. Manufacturer
 - d. Area
 - e. Network status
 - f. Resource status
 - g. Operations: Refresh to immediately get the real-time status of the speaker unit; go to area of the unit
12. Remote Site: Provide the status of the followings:
- a. Name
 - b. Version
 - c. Address
 - d. Network Status
 - e. Default Stream
 - f. Operation: Refresh to immediately get the real-time status of the site; switch the device accessing mode between automatically judge or proxy; restore All Network Connections; switch stream type between main stream, sub-stream, smoothing or default stream type
13. Recording Server: Provide the status of the followings
- a. Name
 - b. Address
 - c. Type
 - d. Network status
 - e. CPU usage
 - f. RAM usage
 - g. Hot Spare Property
 - h. Recording status
 - i. Hardware status
 - j. HDD status
 - k. HDD usage
 - l. First added time (client time)
 - m. Checking time (client time)
 - n. Operation: Refresh to immediately get the real-time status of the Recording Server

14. DeepinMind Server: Provide the status of the followings
 - a. Name
 - b. Address
 - c. Type
 - d. Network status
 - e. CPU usage
 - f. RAM usage
 - g. First added time (client time)
 - h. Checking time (client time)
 - i. Operation: Refresh to immediately get the real-time status of the DeepinMind Server
15. Streaming Server: Provide the status of the followings
 - a. Name
 - b. Address
 - c. Total streams
 - d. Incoming streams
 - e. Outgoing streams
 - f. Network status
 - g. CPU Usage
 - h. RAM Usage
 - i. First added time (client time)
 - j. Checking time (client time)
 - k. Operation: Refresh to immediately get the real-time status of the Streaming Server
16. Security Audit Server: Provide the status of the followings
 - a. Name
 - b. Address
 - c. HDD status
 - d. Network status
 - e. CPU Usage
 - f. RAM Usage
 - g. First added time (client time)
 - h. Checking time (client time)
17. Encoding Device: Provide the status of the followings
 - a. Name
 - b. Address
 - c. Device Serial No.
 - d. Version
 - e. Network status
 - f. HDD status
 - g. HDD usage
 - h. Recording status(Local Device)
 - i. Default Stream
 - j. Access Protocol
 - k. Hot spare property
 - l. Arming status
 - m. RAID
 - n. First added time (client time)
 - o. Checking time (client time)

- p. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
 - q. Switch Device Access Mode in batch:
 - Restore Default: Restore the way the configuration end is set up to access the device
 - Automatically Judge: Determine the way to access the device according to the current network
 - Directly Access: The client directly accesses the device
 - Proxy: The client accesses the device through Steaming gateway and the Management service
 - r. Switch stream type of Encoding Devices in batch:
 - Main stream
 - Sub-stream
 - Smoothing
 - Default stream type
18. Access Control Device: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Device Serial No.
 - d. Version
 - e. Network status
 - f. Main/Sub lane controller network status
 - g. Component status
 - h. Battery status
 - i. Arming status
 - j. First added time (client time)
 - k. Checking time (client time)
 - l. Operation: Refresh to immediately get the real-time status of the Device; go to Web Client to configure the parameters of the device
19. Video Intercom Device: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Device Serial No.
 - d. Version
 - e. Network status
 - f. Calling center status
 - g. Arming status
 - h. First added time (client time)
 - i. Checking time (client time)
 - j. Operation: Refresh to immediately get the real-time status of the Device; go to Web Client to configure the parameters of the device
20. Elevator Control Device: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Device Serial No.
 - d. Version
 - e. Network status

- f. Battery status
 - g. Arming status
 - h. Distributed elevator controller status
 - i. First added time (client time)
 - j. Checking time (client time)
 - k. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
21. Security Control Device: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Device Serial No.
 - d. Version
 - e. Network status
 - f. Battery status
 - g. Arming status
 - h. First added time (client time)
 - i. Checking time (client time)
 - j. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
22. Dock Station: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Device Serial No.
 - d. Version
 - e. Network status
 - f. HDD status
 - g. HDD usage
 - h. First added time (client time)
 - i. Checking time (client time)
 - j. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
23. Decoding Devices: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Device Serial No.
 - d. Version
 - e. Network status
 - f. Manufacturer
 - g. First added time (client time)
 - h. Checking time (client time)
 - i. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
24. IP speaker: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Serial No.
 - d. Version
 - e. Network performance

- f. Checking time
 - g. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
25. Network Transmission Device: Provide the status of the followings:
- a. Name
 - b. Address
 - c. Type
 - d. Serial No.
 - e. Version
 - f. Network performance
 - g. CPU usage
 - h. RAM usage
 - i. Occupied ports
 - j. Abnormal ports
 - k. PoE usage
 - l. Device exception
 - m. First added time
 - n. Checking time
 - o. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
26. Security Inspection Device: Provide the status of the followings:
- p. Name
 - q. Address
 - r. Serial No.
 - s. Version
 - t. Network performance
 - u. Manufacturer
 - v. First added time
 - w. Checking time
 - x. Operation: Refresh to immediately get the real-time status of the device; go to Web Client to configure the parameters of the device
27. Display host server and spare server when hot spare function is enabled

M. Tools on Control Client

1. Quick icon to download or open standalone VSPlayer
2. Broadcast:
 - Ability to do a general audio announcement to all audio-enabled network cameras and end devices
 - Ability to speak or play audio to all speaker units
 - Ability to search for live broadcast records
3. Alarm Output Control: Ability to turn on/off the alarm outputs of the connected camera
4. Two-Way Audio: Ability to select camera with audio in/out and receive and send audio communications between the Control Client and the camera
5. Arming Control: Ability to arm or disarm the configured alarms of the resources; ability to arm or disarm partitions, bypass zones, clear alarms, arm or disarm radars

N. Download Center on Control Client: Ability to view status of all video files being exported

1. Start (all)

2. Stop (all)
3. Delete all
4. Download (VS) Player
5. Set download time as 00:00-06:00, 06:00-12:00, 12:00-18:00, 18:00-24:00, or custom time settings
6. Arrange an off-peak time period to automatically download

O. Local Picture Management on Control Client

1. Ability to easily browse snapshots that have been stored in accessible Windows file folders
2. Ability to save, print, or delete the captured pictures

P. Local Recording Management on Control Client

3. Ability to easily browse video clips that have been stored in accessible Windows file folders
4. Ability to save or delete the video clips

Q. System Configuration on Control Client

1. General settings
 - a. Shall set the default waiting time for the Control Client as default value, default valuex1.5, or default valuex2
 - b. Shall set the maximum mode as Full Screen or Maximize
 - c. Set time zone as client time or device time
 - d. Enable time difference
 - e. Shall enable Auto-login
 - f. Shall open Home page, last interface, or specific view after starting the Control Client
 - g. Enable large-scale display mode
 - h. Shall edit saving path of manual recorded video footage, captured pictures, and installation packages, and users will receive a reminder to download the latest version if the Control Client differs with the accessed SYS in version
2. Video settings
 - a. Shall set network parameters
 - Global stream: main stream, sub-stream or smooth stream
 - Window division amount with main stream: 2, 4, 9, 16, 25, 36, 49, 64
 - Set bandwidth to affect downloading from pStor
 - b. Shall set file parameters
 - Picture format: JPEG or BMP
 - c. Shall set display parameters
 - View scale: Full Screen or Original Resolution
 - Window scale: 4:3 or 16:9
 - Display window No.
 - Display VCA rule
 - Video caching: Small (1 Frame), Medium (6 Frames) or Large (15 Frames); larger frame caching will result in better video performance
 - Continuous decoding: when switching between one window and multiple windows after enabling continuous decoding
 - Enable highlight
 - Overlay transaction information
 - Overlay temperature information
 - GPU hardware decoding
 - Display real-time people counting data
 - d. Shall customize the icons on the live view and playback toolbar

- e. Shall set shortcut for network keyboard and joystick operation on live view and playback
- 3. Set alarm sound to enable voice engine or local audio files
- 4. Set interval of auto-refreshing resource status as 30s, 1 min, 3 min, 5 min, 10 min, 15 min, and restore the interval as 3 min
- 5. Configure screen position according to the actual position
- 6. Enable printing parking receipts when the final charge is 0 for parking
- 7. Switch Home page mode to Visualization Mode or Menu Mode
- 8. Set ringtone for callings from access control devices, video intercom devices, and barrier gates in the parking lot

R. Log into Mobile Client

- 1. Ability to change the password on the first time login
- 2. Ability to remember password
- 3. Ability to show the security level of the password
- 4. Ability to log in to the system via Active Directory
- 5. Ability to log in to the system via domain name
- 6. Ability to log in to the system automatically
- 7. Ability to support HTTPS/HTTP

S. Settings on Mobile Client

- 1. Ability to check the current account information
 - a. User name
 - b. Server information
 - c. Server address
 - d. Server versionAccount list
- 2. Ability to add account to account list
- 3. Ability to switch account
- 4. Ability to manage multimedia: view and manage the local video files and pictures; export pictures to local album; share pictures and video files to other applications
- 5. Ability to switch between the following accessing device modes when performing live view or playback:
 - a. Restore default
 - b. Automatically judge
 - c. Directly connection
 - d. Proxy
- 6. Ability to set default stream type as main stream or sub-stream
- 7. Ability to display detection frames (including motion detection frames, fire source information, temperature, etc.) on video
- 8. Ability to automatically refresh the thumbnails of the resources displayed on the Monitoring page and Favorites page
- 9. Ability to enable hardware decoding
- 10. Ability to set time zone: Client Time and Device Time
- 11. Ability to enable displaying time difference
- 12. Ability to enable notification to allow the SYS to push alarm information of the added resources to the Mobile ClientAbility to show network traffic data used in the following environments:
 - a. Mobile Network
 - b. Wi-Fi

T. Favorites Management on Mobile Client

1. Ability to manage frequently checked resources in favorites
2. Ability to display resources by resource types (camera, door, elevator controller, speaker unit, and radar) or displaying all the resources in the Favorites
3. Display the mixed list of camera, door, elevator controller, speaker unit, and rada or list of some specific resources

3.2 Video Security

A. Wizard and Overview on Web Client

1. View Wizard
 - a. Add an encoding device
 - b. Add a camera to area
 - c. Add resource to map
 - d. Add recording schedule template
 - e. Set video and picture storage
 - f. Add events and alarms
 - g. View live view and playback
2. Display overview of health status, face picture applying status, and face capture records

B. Manage Encoding Devices on Web Client

1. Add encoding devices to the system by Hikvision Private Protocol via the following discovery options:
 - a. IP/Domain
 - b. Hik-Connect
 - c. IP Segment
 - d. Port Segment
 - e. Batch Import
2. Add encoding devices to the system by Hikvision ISUP Protocol via the following discovery options:
 - a. Device ID
 - b. Device ID Segment
 - c. Batch Import
3. Add encoding devices to the system by ONVIF Protocol via the following discovery options:
 - a. IP/Domain
 - b. IP Segment
 - c. Port Segment
 - d. Batch Import
4. Add online devices in the same local subnet with the Local Network/Server Network using Search Active Device Protocol (SADP), by Hikvision Private Protocol, Hikvision ISUP Protocol, or ONVIF Protocol
5. Verify stream encryption key
6. Set mapped port if any
7. Add camera to area
8. Set the time zone for the device, including manually setting time zone and getting device's time zone
9. Apply time zone settings to the device
10. Select Streaming Server for the area
11. Select video storage location for the camera
12. Get device's local recording settings

13. Refresh the status of the added devices
14. Set remote configuration of the added devices
15. Change password of the added devices (in batch)
16. Replace the device with a new device if the original device malfunctions
17. Edit bandwidth for video downloading
18. Activate the online devices (in batch)
19. Set N+1 hot spare for device
20. When adding devices, shall have the option to automatically create logical areas by device name or add to an existing area
21. Synchronize NVR channel names with the names displayed on the Web Client

C. Manage Recording Server on Web Client

1. Add pStor, Network Video Recorder (only for picture storage), Cloud Storage Server, Hybrid SAN, and pStor Cluster Service as Recording Server
2. Import service component certificate to pStor and Cloud Storage Server
3. View storage information for the Recording Server, including used space and free space
4. Enable picture storage function of pStor, Hybrid Storage Area Network and Cloud Storage Server
5. Custom video copy-back to copy back recorded videos from Hybrid SAN's managed device automatically and set start time and end time
6. Set video expiration duration for Hybrid SAN
7. View channel information configured to store video in Recording Server
8. View connected device information of pStor Cluster Service:
9. When adding Hybrid SANs, shall be able to set as host recording server for network camera or as an N+1 hot spare for Hybrid SANs recording redundancy
10. Enable WAN access for the Recording Server

D. Manage Streaming Server on Web Client

1. Add Streaming Server via IP address (in LAN or WAN),
2. Import service component certificate to Streaming Server

E. Area Management on Web Client

1. Group cameras into different areas
2. Synchronize camera name
3. Move the camera to other area
4. Display cameras in sub-areas
5. Set camera ID as identifier number on the keyboard to display live view on smart wall
6. Shall have the ability to edit the following basic information of cameras for current and Remote Site:
 - a. Camera name
 - b. Protocol type
 - c. Check the live view and instant playback of the camera in the same screen
 - d. Configure recording for the camera
 - e. Configure the camera remotely
7. Shall have the ability to configure camera recording settings for current and Remote Site:
 - a. Set main storage and auxiliary storage for cameras
 - b. Synchronize recording settings to device
 - c. Get recording settings from device
 - d. Select storage location as Encoding Device, Hybrid Storage Area Network, pStor, Cloud Storage Server, and pStor Cluster Service for cameras of current site

- e. Select storage location as pStor, Hybrid Storage Area Network or Cloud Storage Server of central system for cameras of Remote Site
 - f. Set recording schedule template
 - g. Select stream type as main stream or sub-stream
 - h. Set pre-record and post-record for recording the video
 - i. Select the storage mode for the recorded videos of cameras of current site: overwrite the oldest videos when disk or allocated quota is full, and automatically delete the oldest videos after the specified retention period
 - j. The Recording Server can get videos from the camera directly, avoiding the risk that if the NVR camera connected is offline, the recording server can not get video from the offline NVR
 - k. Select a Streaming Server to get the video stream of the camera
 - l. Enable the ANR function to turn Automatic Network Replenishment on to temporarily store the video in the camera when the network fails and transport the video to storage devices when the network recovers if the video files are stored in an Encoding Device or Hybrid Storage Area Network
 - m. Add new Recording Server
8. Shall have the ability to set picture storage settings for cameras
 - a. Set storage location as system management server
 - b. Set storage location as Hybrid SAN
 - c. Set storage location as Cloud Storage Server
 - d. Set storage location as a pStor
 - e. Set storage location as a NVR
 9. Remote configuration on device
 10. Copy configuration information of stream type, protocol type, main storage, and auxiliary storage to other cameras for batch configuration

F. View Management on Web Client and Control Client

1. Add the view group, including Public View and Private View
2. Add views to the group
3. Set window division mode for the view and link resources (i.e., cameras and map) to the view

G. Local Configuration, Live View, and Playback on Web Client:

1. Network parameters:
 - a. Global stream:
 - Main stream
 - Sub stream
 - Smooth stream
 - b. Window divisions for main stream: 2, 4, 9, 16, 25, 36, 49, and 64
 - c. Network timeout:
 - Default
 - Default x 1.5
 - Default x 2
2. File parameters:
 - a. Picture format:
 - BMP
 - JPEG
 - b. File saving path

3. Display parameters:
 - a. View scale:
 - Full screen
 - Original resolution
 - b. Window scale:
 - 4:3
 - 16:9
 - c. Enable/disable displaying window No.
 - d. Enable/disable displaying VCA rule
 - e. Video caching:
 - Small (1 frame)
 - Medium (6 frames)
 - Large (15 frames)
 - f. Enable/disable continuous decoding
 - g. Enable/disable highlight
 - h. Enable/disable transaction information overlay
 - i. Enable/disable temperature information overlay
 - j. Enable/disable GPU hardware decoding
4. Customize icons on live view and playback window:
 - a. Icons on live view window:
 - Audio control
 - Capture
 - Record
 - Instant playback
 - Two-way audio
 - Digital zoom
 - PTZ control
 - Fisheye expansion
 - Switch stream type
 - Alarm output
 - Video enhancement
 - b. Icons on playback window:
 - Audio control
 - Capture
 - Clip
 - Add tag
 - Lock video
 - Digital zoom
 - Fisheye expansion
 - Stream switch
 - Video enhancement
5. Start live view in area and view mode
6. Auto-switch cameras in an area
7. Shall live view up to 64 cameras simultaneously Shall view image thumbnail
8. Shall playback up to 16 cameras simultaneously

9. Shall support capturing, manual recording, digital zoom, two-way audio, PTZ control, select stream type, displaying camera status of resolution and frame rate, audio on/off, switching to instant playback during live view
10. Shall support capturing, clipping, digital zoom, displaying camera status, switching between main stream, sub stream and smooth stream, audio on and off, selecting from main storage and auxiliary storage
11. Shall support selecting playback date from the calendar

H. Live View on Control Client

1. Ability to view up to 256 cameras
2. Ability to display GIS map/related map after the camera is added on the map
3. Ability to display the configured resource groups on the map and view the details, such as number of person in the group, triggered alarm details, etc.
4. Ability to display thumbnail of camera
5. Ability to auto switch to sub stream of network camera according to the configuration of stream threshold
 - a. Enable auto-switching between main stream and sub stream
 - b. Enable to set the main stream threshold as 1/2, 1/4, 1/9, 1/16, 1/25, 1/36, 1/64
 - c. Enable to switch the live view stream to main stream, sub stream or smooth stream, the smooth stream will show if the device supports smoothing function, you can switch to smooth stream if in low bandwidth situation to make live view more fluent
6. Shall support up to 4 auxiliary screens during live view and 1 screen for playback
7. The following functions are available on the tile toolbar for easy access to operator:
 - a. Audio control
 - b. Capture: ability to save snapshots
 - c. Print camera image
 - d. Enable manual recording of displayed Network Camera
 - e. Enable and utilize two-way audio
 - f. Enable view instant playback
 - g. Digital zoom
 - h. 3D positioning for PTZ camera
 - i. Activate on-screen PTZ controls
 - j. Show camera status
 - Frame rate
 - Resolution
 - Stream format
 - Bit rate
 - Connection number
 - Network status
 - Signal status
 - Recording status
 - Access mode
 - Channel type
 - Device name
 - IP address
 - Access protocol
 - Area name
 - Main storage/auxiliary storage

- Storage location
 - Storage type
 - Recording schedule template
 - Video stream
 - Streaming server
 - Pre-record: enabled/disabled
 - Post-record: duration
 - ANR: enabled/disabled
 - Picture storage location
- k. Arming control
 - l. Switch stream type of camera
 - m. Edit transcoded stream
 - n. Live view on smart wall by graphic card
 - o. VCA playback
 - p. Alarm output
 - q. Create zooming areas and dewarped zooming areas on the video image to view detailed live view
 - r. Save area as view
 - s. Area auto-switch
 - t. Add tag
 - Set time range
 - Add description
 - Select storage type
 - u. Visual tracking
 - v. People density monitoring to view people density data and real- time statistics of people amount.
 - w. Search for the target person by the captured pictures
 - x. Support the following fisheye expansion functions:
 - Zoom to expand the video by the wheel
 - Flexible PTZ operation
 - Multiple cameras of fisheye expansion
 - Save fisheye expansion as view
8. Ability to customize camera tile toolbar
 - a. Re-order icons to user preference
 - b. Remove icons of functions not required for user
 9. Ability to create tile patterns with selected cameras and save as a view
 - a. Save as private view, only accessible to the user profile creating the view
 - b. Save as public view, accessible to all users
 - c. Play in batch: play all cameras belonging to one area on different screens
 - d. View group auto-switch
 - e. Auto-switch: loop all cameras belonging to one area on one screen or play in batch:
 - (a) Automatically change cameras every 5s, 10s, 15s, 20s, 30s, 40s, 1min, 3min, and 5min
 - Pause/Start guard tour
 - Manually switch to next/previous camera live view
 - (b) Display cameras added to one map in one screen or play in batch. Automatically change cameras every 5s, 10s, 15s, 20s, 30s, 40s, 1min, 3min, and 5min

- (c) Display on smart wall of graphic card
- 10. PTZ Control: Shall have following options to control PTZ cameras
 - a. On-screen PTZ icon
 - Able to control all PTZ functions available directly on camera
 - b. On tile “point and go” directional control
 - Able to use mouse wheel for zoom in after PTZ control is enabled
 - c. 3D Positioning: ability to draw box for region of interest to zoom in on tile
- 11. Live view of Remote Site’s cameras
- 12. After reopening the client, display the view before closing the client
- 13. Set preset and patrol for common cameras
- 14. Set preset and patrol settings of fisheye camera
- 15. View detected events in live view
 - a. View/filter/clear the detected events, including face comparison event and access event
 - b. View access event details
 - c. Quick-jump to Access Record module
 - d. Add the person to person list
 - e. Add recognized vehicle to vehicle list
 - f. Subscribe events
 - For face comparison events, shall subscribe events of all the resources
 - For access events, shall subscribe according to event types: all events, normal card swiping events, abnormal card swiping events, device exceptions, alarm input events, and other events
- 16. Diagnose when live view failed
 - a. Display the details of the camera
 - b. Display the exception description
 - c. Display the diagnosis details, including requesting URL status, logging into encoding device status, getting stream from encoding device status
 - d. Quick link to event log, server log, device log, health monitoring
 - e. Mark the diagnosis
- I. Playback on Control Client**
 - 1. Ability to play back 1 to 16 cameras simultaneously
 - 2. Ability to display GIS map/related map
 - 3. When playing multiple cameras simultaneously, have ability to view in non-synchronized and synchronized mode
 - 4. Ability to hover on the timeline to show the time
 - 5. Ability to fast-forward by 1x, 2x, 4x, 8x, 16x, and slow-forward by 1/16x, 1/8x, 1/4x, 1/2x
 - 6. Ability to export one or multiple cameras displayed simultaneously:
 - a. Set export location
 - b. Set whether to download VSPlayer for viewing
 - c. Export video files in MP4/AVI/EXE format
 - d. Set saving path
 - e. Search and export video files of over 48 hours duration
 - f. Synchronize downloading time
 - 7. The following functions are available on the camera playback tile toolbar for easy access to operator:
 - a. Capture: ability to save JPEG snapshots and search video by the captured picture
 - b. Print camera image

- c. Clipping: ability to quickly export video clips
- d. Add tag to video
- e. Digital zoom
- f. Lock video: to prevent video segments from being over written by schedule
- g. Camera status
 - Frame rate
 - Resolution
 - Stream format
 - Bitrate
 - Connection number
 - Network status
 - Signal status
 - Recording status
 - Access Mode
 - Channel type
 - Encoding device/site name
 - IP address
 - Access protocol
 - Area name
 - Main storage/auxiliary storage
 - Storage location
 - Storage type
 - Recording schedule template
 - Video stream type
 - Streaming server
 - Pre-record: enable/disable
 - Post-record duration
 - ANR status
 - Picture storage settings
- h. Stream type switch
- i. Extract frames from the video and play the extracted images (frames) one by one
- j. Playback on smart wall
- k. Transcoding playback
- l. Audio on/off
- m. Video download
- n. VCA search
- o. Fisheye dewarping
- p. Visual tracking
- q. Create zooming areas and dewarped zooming areas on the video image to view detailed playback
- r. Search for the target person by the captured pictures
- 8. Customize camera tile tool bar
 - a. Re-order icons to user preference
 - b. Remove icons of functions not required for user
- 9. Support display video on the smart wall
- 10. Playback channels of Remote Sites
- 11. Search video files by time

12. Display the date with video files marked with a triangle
13. Support ATM-DVR, its playback type shall be set as command playback
14. Select storage location of recorded video files (central storage or remote storage)
15. Enable/disable thumbnails
16. Zoom in or zoom out on the timeline
17. Support dual-stream playback
18. Support video downloading
 - a. Support AVI format for video file download
 - b. Encrypt to download in MP4/EXE format, and click and play directly after downloading with player in MP4 format
 - c. Support save the downloading file as evidence
 - d. Support privacy mask after downloaded and played with VSPlayer
 - e. Adjust downloading time
 - f. Check the merged video files in one folder
19. Diagnose when playback failed
 - a. Display device information
 - b. Display exception description
 - c. Quick link of server log
 - d. Mark the diagnosis

J. Live View on Mobile Client

1. Ability to add/delete cameras for multiple view, and view up to 8 cameras simultaneously
2. Ability to set 1/4/9 window division for tablet
3. Ability to switch to saved view pattern
4. Ability to view real-time video from stream encryption device
5. Ability to view real-time video from the UVSS's related camera (only for tablet)
6. Ability to play the live videos or video footage of multiple resources simultaneously
7. Ability to view the live video of the door's related camera.
8. Ability to control the status of doors (including turnstiles) and view the card swiping record in real time when viewing the live video of the door's related cameras. If the door is a turnstile, select entrance control or exit control
9. Ability to view the live video of the elevator 's related camera
10. Ability to control the status for each floor (temporary access, access with credential, free access, or access forbidden) linked to the elevator control device
11. Ability to view real-time video from the door station's related camera(s)
12. Ability to receive card-swiping events when viewing real-time video from the door station's related camera(s)
13. Ability to view the live video of the radar's related camera.
14. Ability to arm/disarm the radar during the live view of the radar's related camera.
15. Ability to display persons' real-time access records, including person profile, person name, and access results
16. Ability to view the recognized passing vehicle information, including license plate number and passing time
17. Ability to view the detected passing vehicle information, including real-time undercarriage picture, configured original undercarriage picture, vehicle picture, license plate number, and passing time (only for tablet)
18. Ability to mark on the captured real-time undercarriage picture (only for tablet)
19. Ability to add new vehicle to the vehicle list

20. Ability to view the person's face comparison information (real-time and history), including captured face picture, person details, captured time, and similarity
21. Ability to add mismatched person into person list
22. Ability to trigger user-defined event manually
23. Ability to subscribe all access and face comparison events(only for tablet)
24. Ability to switch cameras if the access control point links two cameras
25. Has the following functions available on tile toolbar for easy access:
 - a. Upload the generic event during live view
 - b. Toggle the settings between 1, 4, 9 tiles (only for tablet)
 - c. Stop/recover all the live views
 - d. Capture: ability to save snapshots, and share the captured pictures via email
 - e. Preview the captured picture and recorded video footage
 - f. Enable manual recording of displayed cameras, and share the manual recording files via email
 - g. Switch on/off audio
 - h. Enable and utilize two-way audio
 - i. Digital zoom
 - j. Switch between sub-stream and main stream
 - k. Add the camera/view to Favorites/View
 - l. PTZ control
 - Start/stop the auto-scan
 - Zoom +/-
 - Focus +/-
 - Iris +/-
 - Manage presets
 - 3D positioning
 - m. Fisheye dewarping
 - n. Ability to live view in full-screen mode

K. Playback on Mobile Client

1. Ability to playback 1 to 4 cameras simultaneously for tablet
2. Ability to playback up to 1 camera simultaneously for phone
3. Ability to playback video from stream encryption device
4. Ability to stop playback of all cameras in one step or one by one
5. Ability to choose date and storage location for playback
6. Ability to search cameras for playback by name or choose cameras added to Favorites
7. Ability to restore the playback interface when the user logs out
8. Ability to switch the window for playback
9. Ability to search Logical Area/Access point/Camera via key words
10. Ability to support synchronous playback
11. Ability to playback the cameras of Remote Sites
12. Ability to support VCA search (only for tablet)
13. Ability to add person into Person List (only for tablet)
14. Ability to search access records: search the persons' access records and view the access details including person details and access point information (only for tablet)
15. Ability to add/delete/edit tags and search video via tags (only for tablet)
16. Ability to playback single camera in full-screen mode
17. Has the following functions available on camera playback tile toolbar for easy access:

- a. Capture: ability to save snapshots
 - b. Clipping: ability to quickly create and export video clip
 - c. Pause the playback
 - d. Digital Zoom
 - e. Add tag during Playback
 - f. Switch the playback speed to 1/4X, 1/2X, 1X, 2X and 4X
 - g. Stop/resume the playback
 - h. Switch on/off audio
 - i. Fisheye dewarping
 - j. Locate the timeline of playback manually
18. Fisheye dewarping
19. Activate on-screen PTZ controls

L. Video Settings on Web Client

- 1. Ability to set recording schedule template
- 2. Ability to set visual tracking parameters by associating the camera with other cameras nearby and create on-video overlays.
- 3. Ability to set smart linkage parameters to manually locate or track the target appeared in the view of bullet or box camera with a linked speed dome
- 4. Ability to enable evidence collection:
 - a. SFTP address
 - b. Port
 - c. User name
 - d. Password
 - e. Path
 - f. Evidence type: add/delete/delete all
 - g. Organization on site: add/delete/ delete all
 - h. Result/conclusion: Add/delete/delete all
- 5. Ability to set network parameters.
 - a. For the system without a Remote Site Management module (as we called Remote Site), it shall be able to register to the Central System after enabling this function and setting the Central System's parameters
 - a. For the system with a Remote Site Management module (as we called Remote Site), it shall be able to receive the site registration after enabling this function and set the Remote Site's parameters.
 - b. Set device access mode as automatically mode or proxy

M. Video Search on Control Client and Mobile Client

- 1. Ability to search for specific types of indexed video:
 - a. Tag: Video that has been auto tagged or manually tagged at a certain timestamp
 - b. Lock: Search only video that has been "locked" to not be overwritten by schedule
 - c. Segment: Ability to search for up to 7 days of video averagely divided into segments from 1 to 100
 - d. Interval: Ability to search for up to 7 days of video divided by intervals from 1 to 60 minutes or seconds
 - e. Transaction Event
 - Ability to search for up to 7 days of transaction items by keywords when NVR/DVR is integrated with a Point of Sales (POS) system
 - Enable/disable case sensitive for key word searching

- f. Search ATM event triggered video footage by the card number that is contained in the ATM information
 - g. Search Video/Picture/Audio Stored on Dock Station
 - Select dock station
 - Filter time settings
 - Check the video, person name, capture picture
 - Export file (in batch) to local PC in the format of MP4 and AVI
 - Encrypt the video files in MP4 format
 - Save the video files and create as new evidence
 - Create new evidence ID
 - Create new evidence name
 - Select evidence type
 - Select organization on site
 - Set the result/conclusion
 - Set evidence status
 - Save the video files and add to existing evidence
 - Lock file
 - h. Supports thumbnails
 - i. Ability to search main stream in all main storage
 - j. Ability to search sub-stream in all main storage
 - k. Ability to search main stream in all auxiliary storage
 - l. Ability to search sub-stream in all auxiliary storage
 - m. Ability to search the video files from Central System or Remote site
2. VCA Search
- a. Support Motion Detection
 - b. Support Line Crossing Detection
 - c. Support Intrusion Detection
 - d. Support reverse playback
 - e. Support downloading the searched video clips
 - f. Support displaying the video clips in the list or thumbnail mode
 - g. Support playing searched video clips in order
 - h. Support viewing large picture and the related video
 - i. Support downloading the current picture and video in the format of MP4, AVI and EXE

N. Evidence Search on Control Client

1. Set the following search conditions:
 - a. ID
 - b. Keywords
 - c. Evidence type
 - d. Organization on site
 - e. Result/conclusion
 - f. Evidence status
 - g. Uploading time
2. Check the search result:
 - a. Name
 - b. ID
 - c. Type
 - d. Organization on site

- e. Result
 - f. Status
 - g. Description
 - h. Uploading time
3. Check and download the content of evidence

3.3 Event and Alarm

A. Event and Alarm Configuration on Web Client

1. Shall batch add the following events from cameras:
 - a. Other Video Event
 - Audio Exception Detection
 - Captured Picture Uploading Event
 - Installing Scanner
 - Sudden Change of Sound Intensity Detection
 - Sudden Increase of Sound Intensity Detection
 - Sudden Decrease of Sound Intensity Detection
 - Vibration Detected Alarm
 - b. VCA Event
 - Defocus Detection
 - Fast Moving (Detection)
 - Intrusion (Detection)
 - Intrusion (Radar PTZ Camera)
 - Line Crossing
 - Line Crossing (Radar PTZ Camera)
 - Motion Detection
 - Object Removal
 - Region Entrance
 - Region Exiting
 - Reserve Entering Alarm
 - Scene Change Detection
 - Unattended Baggage
 - Video Tampering Detection
 - c. People Related Event
 - Abnormal Face
 - Absence Detection
 - Climbing Detection
 - Distance Measurement
 - Face Capture
 - Face Detection
 - Falling Down
 - Getting Up Detection
 - Hard Hat Detection
 - In-Toilet Overtime Detection
 - Key Person Getting Up Detection
 - Loitering

- Multi-Target-Type Detection
 - Multiple Faces
 - No Mask
 - Number of People Exception
 - Overstay Detection
 - People Density
 - People Density Analysis
 - People Gathering
 - People Queuing-Up Alarm
 - Physical Conflict
 - Physical Conflict (Indoor)
 - Playground Overstay Detection
 - Playing Mobile Phone
 - Police Absence
 - Probable Physical Conflict (Indoor)
 - Sitting Detection
 - Sleep on Duty Detection
 - Standing Up Detection
 - Sticking Scrip
 - Tailing
 - Using Mobile Phone
 - Waiting Time Detection Alarm
 - Wearing Sunglasses
- d. Vehicle Related Event
- Driving on the Lane Line
 - Illegal Lane Change
 - Illegal Parking
 - Illegal U-Turn
 - Motor Vehicle on Non-Motor Vehicle Lane
 - Parking
 - Vehicle Blocklist Alarm
 - Vehicle Overspeed
 - Vehicle Allowlist Alarm
 - Wrong-Way Driving
- e. Thermal Related Event
- Abnormal Temperature
 - Fire Source Detection
 - PIR
 - Temperature Difference Alarm
 - Temperature Pre-Alarm
- f. Maintenance Event
- Camera Communication Exception
 - Camera Communication Recovered
 - Camera Offline
 - Camera Online
 - Camera Recording Exception

- Camera Recording Recovered
 - Channel Armed
 - Channel Arming Failed
 - Image Exception Event
 - Operation Timeout
 - Video Loss
2. Shall batch add the following Alarm Input events
 - Alarm Input Triggered
 - Alarm Input Restored
 - Alarm Input Armed
 - Alarm Input Disarmed
 - Bypass
 - Bypass Restored
 - Tampered
 - Tampering Restored
 3. Shall batch add the following Face events
 - Abnormal Temperature
 - Face Matched Event
 - Face Mismatched Event
 - Frequently Appeared Person
 - Rarely Appeared Person Event
 - No Mask
 4. Shall batch add the following Door events
 - a. Normal Card Swiping
 - Access Granted by Card
 - Access Granted by Card and Fingerprint
 - Access Granted by Card and PIN
 - Access Granted by Card, Fingerprint, and PIN
 - Access Granted by Employee ID and Face
 - Access Granted by Employee ID and Fingerprint
 - Access Granted by Employee ID and PIN
 - Access Granted by Employee ID, Fingerprint, and PIN
 - Access Granted by Face
 - Access Granted by Face and Card
 - Access Granted by Face and Fingerprint
 - Access Granted by Face and PIN
 - Access Granted by Face, Card, and Fingerprint
 - Access Granted by Face, PIN, and Fingerprint
 - Access Granted by Fingerprint
 - Access Granted by Fingerprint and PIN
 - Combined Authentication Passed
 - Duress Alarm
 - Password Authenticated
 - Skin-Surface Temperature Measured
 - b. Abnormal Card Swiping
 - Access Denied (Door Remained Locked or Inactive)

- Access Denied (First Card Not Authorized)
- Access Denied (NFC Card Reading Disabled)
- Access Denied by Card and Fingerprint
- Access Denied by Card and PIN
- Access Denied by Card, Fingerprint, and PIN
- Access Denied by Employee ID and Fingerprint
- Access Denied by Employee ID and PIN
- Access Denied by Employee ID, Fingerprint, and PIN
- Access Denied by Employee ID and Face
- Access Denied by Encrypted CPU Card
- Access Denied by Face
- Access Denied by Face and Card
- Access Denied by Face and Fingerprint
- Access Denied by Face and PIN
- Access Denied by Face, Card, and Fingerprint
- Access Denied by Face, PIN, and Fingerprint
- Access Denied by Fingerprint
- Access Denied by Fingerprint and PIN
- Access Denied by Invalid M1 Card
- Access Timed Out by Card and Fingerprint
- Access Timed Out by Card and PIN
- Access Timed Out by Card, Fingerprint, and PIN
- Access Timed Out by Employee ID and Fingerprint
- Access Timed Out by Employee ID and PIN
- Access Timed Out by Employee ID, Fingerprint, and PIN
- Access Timed Out by Face and Card
- Access Timed Out by Face and Fingerprint
- Access Timed Out by Face and PIN
- Access Timed Out by Face, Card, and Fingerprint
- Access Timed Out by Face, PIN, and Fingerprint
- Access Timed Out by Fingerprint and PIN
- Anti-Passback Server Respond Failed
- Anti-Passback Violation
- Access Denied by Abnormal Feature
- Authentication Mode Mismatched
- Card Not in Multi-Factor Authentication Duration
- Card Not in Multi-Factor Authentication Group
- Card Number Expired
- Combined Authentication Timed Out
- CPU Card Reading Disabled
- EM Card Reading Disabled
- Employee ID Not Exist
- EM Card Reading Disabled
- Face Recognition Failed
- Failed Password Attempts AlarmFingerprint Not Found
- Invalid Time Period

- Live Face Detection Failed
 - Lost Card Authenticated
 - M1 Card Reading Disabled
 - Max. Card and Password Authentication Times
 - Max. Card Access Failed Attempts
 - Multi-Door Interlocking
 - No Access Level Assigned
 - No Card Number Found
 - PIN Mismatched
 - Verifying Card Encryption Information Failed
 - Verifying Desfire Card Encryption Failed
- c. Other Door Event
- Abnormal Temperature Access Failed When Free Passing
 - Access Granted with First Person In Started
 - Access Granted with First Person In Stopped
 - Barrier Obstructed
 - Barrier Obstruction Recovered
 - Blocklist Event
 - Card Reader Tamper Alarm
 - Card Reader Tamper Restored
 - Climbing Over Barrier
 - Door Abnormally Open (Door Contact)
 - Door Bell Rang
 - Door Button Pressed Down
 - Door Button Released
 - Door Closed (Door Contact)
 - Door Locked (Door Lock)
 - Door Locked by Keyfob
 - Door Not Closed
 - Door Not Open
 - Door Open (Door Contact)
 - Door Open Timed Out (Door Contact)
 - Door Remained Unlocked by Keyfob
 - Door Unlocked (Door Lock)
 - Door Unlocked by Keyfob
 - Enter Dismiss Code
 - Fire Alarm Relay Triggers Door Recovered
 - Fire Alarm Relay Triggers Door Remain Open
 - First Card Authorization Ended
 - First Card Authorization Started
 - Force Accessing
 - Identity Card Reading Disabled
 - Intrusion
 - Multi-Factor Authentication Timed Out
 - Multi-Factor Authentication: Access Denied by Remote Client
 - Multi-Factor Authentication: Access Denied by Super Password

- Multi-Factor Authentication: Access Granted
 - Multi-Factor Authentication: Remotely Open Door
 - Multi-Factor Authentication: Repeated Authentication
 - Multi-Factor Authentication: Super Password Access Granted
 - No Mask
 - Opening Door by Linkage Failed When Door Remaining Closed or in Sleep Mode
 - Opening Door by Exit Button Failed When Door Remaining Closed or in Sleep Mode
 - Overstay
 - Passing Timeout
 - Remaining Locked Status Ended
 - Remaining Locked Status Started
 - Remaining Unlocked Status Ended
 - Remaining Unlocked Status Started
 - Remote: Locked Door
 - Remote: Remained Locked (Credential Failed)
 - Remote: Remained Unlocked (Free Access)
 - Remote: Unlocked Door
 - Reverse Passing
 - Secure Door Control Unit Tamper Alarm
 - Secure Door Control Unit Tamper Restored
 - Tailgating
 - Unlock by Center
 - Unlock by Duress
 - Unlock by Householder
 - Unlock by Password
- d. Maintenance Events
- Face Recognition Terminal Offline
 - Face Recognition Terminal Online
5. Shall batch add Elevator events
- a. Normal Card Swiping
- Access Granted by Card
 - Access Granted by Card and Fingerprint
 - Access Granted by Card and PIN
 - Access Granted by Card, Fingerprint, and PIN
 - Access Granted by Fingerprint
 - Access Granted by Fingerprint and PIN
 - Duress Alarm
- b. Abnormal Card Swiping
- Access Denied (NFC Card Reading Disabled)
 - Access Denied by Card and PIN
 - Access Denied by Card, Fingerprint, and PIN
 - Access Denied by Encrypted CPU Card
 - Access Denied by Fingerprint
 - Access Denied by Fingerprint and PIN
 - Access Denied by Invalid M1 Card
 - Access Denied in Sleep Mode

- Access Timed Out by Card and PIN
 - Access Timed Out by Card, Fingerprint, and PIN
 - Access Timed Out by Fingerprint and PIN
 - Anti-Passback Server Respond Failed
 - Authentication Mode Mismatched
 - Card Number Expired
 - CPU Card Reading Disabled
 - EM Card Reading Disabled
 - Invalid Time Period
 - Lost Card Authenticated
 - M1 Card Reading Disabled
 - Max. Card and Password Authentication Times
 - Max. Card Access Failed Attempts
 - No Access Level Assigned
 - No Card Number Found
 - PIN Mismatched
 - Verifying Card Encryption Information Failed
- c. Other Door Event
- Access Granted with First Person In Started
 - Access Granted with First Person In Stopped
 - Auto Button Relay Connected
 - Auto Button Relay Disconnected
 - Button Relay Connected
 - Button Relay Disconnected
 - Card Reader Tamper Alarm
 - Card Reader Tamper RestoredEnter Dismiss Code
 - Fire Alarm Button Resumed
 - Fire Alarm Button Triggered
 - Fire Input Open Circuit Alarm
 - Fire Input Restored
 - Fire Input Short Circuit Alarm
 - Maintenance Button Restored
 - Maintenance Button Triggered
 - Panic Button Restored
 - Panic Button Triggered
 - Remaining Locked Status Ended
 - Remaining Locked Status Started
 - Remaining Unlocked Status Ended
 - Remaining Unlocked Status Started
 - Remote: Locked Door
 - Remote: Remained Locked (Credential Failed)
 - Remote: Remained Unlocked (Free Access)
 - Remote: Unlocked Door
6. Shall batch add the following Person events
- Person Matched Event
 - Card Number Matched Event

7. Shall batch add the following Vehicle Features events
 - License Plate Matched Event
 - License Plate Mismatched Event
 - Vehicle Type Matched Event
8. Shall batch add the following Parking Lot events
 - Blocklist Alarm
 - Calling Center
 - Frequently Appeared Vehicle
 - No Vacant Parking Space
 - Overstayed Event
 - Park in Forbidden Period
 - Parking Lot Occupied Alarm
 - Vehicle Matched Event
 - Vehicle Mismatched Event
9. Shall batch add Security Radar events
 - Auto-Arming
 - Auto-Arming Failed
 - Auto-Disarming
 - Auto-Disarming Failed
 - Disarming
 - Instant Arming
 - Line Crossing
 - Region Entrance
10. Shall batch add the following Regional People Counting events
 - Person Amount More/Less than Threshold
 - Person Amount More/Less than Threshold (Pre-Alarm)
11. Shall batch add the following Digital Signage events
 - Abnormal Temperature
 - Person Amount More than Threshold
12. Shall batch add Maintenance events from UVSS
 - Offline
 - Online
13. Shall batch add Maintenance events from Encoding Device
 - Array Exception
 - Camera/Recording Resolution Mismatch
 - Device Armed
 - Device Arming Failed
 - Device Offline
 - Device Reconnected
 - Encoding Device Recording Exception
 - Encoding Device Recording Recovered
 - HDD Bad Sector
 - HDD Full
 - HDD High Temperature
 - HDD Impact Detection
 - HDD Severe Failure

- Illegal Login
 - R/W HDD Failure
 - Video Standard Mismatch
14. Shall batch add Maintenance events from Decoding Device
- Decoding Device Offline
 - Decoding Device Online
15. Shall batch add Maintenance events from Access Control Device:
- Active Infrared Intrusion Detector Exception
 - AC Power Off
 - AC Power On
 - Battery Voltage Recovered
 - Calling Security Center
 - CAN BUS Exception
 - Communicated with IR Adapter Exception
 - Communicated with Light Board Failed
 - Connection Recovered with Anti-Passback Server
 - Device Armed
 - Device Arming Failed
 - Device Offline
 - Device Online
 - Device Power Off
 - Device Power On
 - Device Tampered
 - Device Tamper Restored
 - Disconnected with Anti-Passback Server
 - Edit Central Group Configuration
 - Edit GPRS Parameters
 - Edit Network Center Configuration
 - Export Card Permission Parameters
 - Export Normal Configuration File
 - Flash Writing/Reading Exception
 - ID Card Reader Connected
 - ID Card Reader Disconnected
 - Import Card Permission Parameters
 - Import Normal Configuration File
 - Indicator Turned Off
 - Indicator Turned On
 - Lane Controller Connected
 - Lane Controller Disconnected
 - Lane Controller Fire Input Alarm
 - Lane Controller Tamper Alarm
 - Local: Login
 - Local: Login Locked
 - Local: Login Unlocked
 - Local: Logout
 - Local: Restored Default Parameters

- Local: Upgrade
- Local: Upgrade Device Firmware via USB Flash Drive
- Local: Upgrading Failed
- Low Battery Voltage
- Low Battery Voltage Recovered
- Low Storage Battery Voltage
- Motor or Sensor Exception
- No Memory for Offline Event Storage
- NTP Auto Time Synchronization
- Operation Failed: Code Not Matched with Keyfob
- Pedestal Temperature Too High
- Remote: Arming
- Remote: Capture
- Remote: Clear Card No.
- Remote: Disable Alarm Output Manually
- Remote: Disarming
- Remote: Enable Alarm Output Manually
- Remote: Export Configuration File
- Remote: Extension Module Upgraded
- Remote: Extension Module Upgrading Failed
- Remote: Fingerprint Module Upgraded
- Remote: Fingerprint Module Upgrading Failed
- Remote: Import Configuration File
- Remote: Login
- Remote: Logout
- Remote: Manual Time Synchronization
- Remote: Reboot
- Remote: Restored Default Parameters
- Remote: Upgrade
- Remote: Upgrading Failed
- SD Card Full Alarm
- Secure Door Control Unit Connected
- Secure Door Control Unit Disconnected

16. Shall batch add Maintenance events from Elevator Control Device:

- Device Armed
- Device Arming Failed
- Device Power Off
- Device Power On
- Device Tampered
- Device Tamper Restored
- Distributed Controller Tampered
- Distributed Controller Tamper Restored
- Distributed Elevator Controller Offline
- Distributed Elevator Controller Online
- Edit Central Group Configuration
- Edit GPRS Parameters

- Edit Network Center Configuration
- Elevator Controller Offline
- Elevator Controller Online
- Flash Writing/Reading Exception
- Local: Restored Default Parameters
- Local: Upgrading Failed
- Low Battery Voltage Recovered
- No Memory for Offline Event Storage
- NTP Auto Time Synchronization
- Remote: Arming
- Remote: Clear Card No.
- Remote: Disable Alarm Output Manually
- Remote: Disarming
- Remote: Enable Alarm Output Manually
- Remote: Login
- Remote: Logout
- Remote: Manual Time Synchronization
- Remote: Reboot
- Remote: Restored Default Parameters
- Remote: Upgrade
- Remote: Upgrade Failed

17. Shall batch add Maintenance events from Alarm Device:

- AC Power Down
- Alarm Cleared
- Auto Arming Failed
- Away Arming
- Battery Fault
- BUS Open-Circuit Alarm
- BUS Short-Circuit Alarm
- Cellular Network Data Exceeded
- Control Panel Reset
- Device Armed
- Device Arming Failed
- Device Moved
- Device Offline
- Device Online
- Device Tampered
- Disarming
- Duress Report
- Expander Added
- Expander Deleted
- Extension Module Disconnected
- Extension Module Exception
- Extension Module Tampered
- Forced Arming
- HDD Exception

- HDD Full
- Instant Arming
- IP Address Conflicted
- Key Zone Arming
- Key Zone Disarming
- Keypad Locked
- Keypad Unlocked
- Late to Disarm
- Low Battery of Wireless Siren
- Low Battery Voltage
- Low Wireless Device Battery
- Overcurrent Protection Restored
- Overcurrent Protection Triggered
- Overvoltage Protection Restored
- Overvoltage Protection Triggered
- Panic Alarm
- Partition (Area) Arming Failed
- Partition (Area) Auto-Armed
- Partition (Area) Auto-Disarmed
- Power Restored
- Radar Transmitter Fault
- Repeater AC Power Down
- Repeater AC Power Restored
- Repeater Battery Disconnected
- Repeater Battery Low
- Repeater Battery Restored
- RF Signal Exception
- Stay Arming
- Tampering Alarm Started
- Telephone Communication Failed
- Video Standard Mismatch
- Virtual Zone Fire Alarm
- Virtual Zone Panic Alarm
- Wi-Fi Signal Exception
- Wired Network Disconnected
- Wireless Network Disconnected
- WirelessDevice Added
- Wireless Device Deleted
- Wireless Device Disconnected
- Wireless Device Tampered
- Wireless Repeater Added
- Wireless Repeater Deleted
- Wireless Repeater Disconnected
- Wireless Repeater Tampered
- Wireless Siren Added
- Wireless Siren Deleted
- Wireless Siren Disconnected

- Wireless Siren Tampered
 - XBUS Module Disconnected
18. Shall batch add Maintenance events from Dock Station
- Dock Station Offline
 - Dock Station Online
19. Shall batch add Maintenance events from Remote Site: Site Offline
20. Shall batch add Maintenance events from Network Transmission Device
- Fiber Optical Port Lost
 - Network Interface Lost
 - PoE-Max
 - PoE Interface Powered Off
 - Switch Armed
 - Switch Arming Failed
 - Switch Offline
 - Switch Online
 - Wireless Connection Disconnected
 - Wireless Upstream Rate Exception
21. Shall batch add Maintenance events from Digital Signage Terminal
- Digital Signage Terminal Offline)
22. Shall batch add Maintenance events from Recording Server
- Array Degradation
 - Array Detection
 - Array Expansion
 - Array Initialization
 - Array Rebuilding
 - Array Repair
 - Array Unavailable
 - Bad Disk
 - Chip Temperature Too High
 - CPU Temperature Too High
 - Disk Disconnected
 - Disk Loss
 - Disk Warning
 - Environment Temperature Too High
 - Hybrid SAN: Fan Exception
 - Hybrid SAN: Network Status Exception
 - Hybrid SAN: Power Supply Exception
 - Hybrid SAN: Storage Enclosure Exception
 - Mainboard Temperature Too High
 - Memory Exception
 - Memory Temperature Too High
 - pStor Resource Pool Exception
 - Physical Volume Alarm
 - Recording Exception Alarm
 - Recording Server Recording Exception
 - Recording Server Recording Recovered

- Server Exception
 - System Temperature Too High
 - Video Loss Alarm
23. Shall batch add Maintenance events from the Streaming Server: Server Exception
 24. Shall batch add Maintenance events from the DeepinMind Server
 - DeepinMind Server Offline
 - DeepinMind Server Online
 25. Shall add maintenance events for Security Audit Server
 - Critical Event
 - Normal Event
 - Serious Event
 26. Shall batch add Maintenance events from System Management Server
 - CPU Exception
 - CPU Recovered
 - CPU Warning
 - Hot Spare Switch
 - RAM Exception
 - RAM Recovered
 - RAM Warning
 - System Service Abnormally Stopped
 - System Service Recovered to Run
 27. Shall batch add Maintenance events from Video Intercom Device:
 - Calling Security Center
 - Device Armed
 - Device Arming Failed
 - Device Offline
 - Device Online
 - Device Tampered
 - Secure Door Control Unit Tampered
 - SOS
 28. Shall batch add Maintenance events from Third-Party Database:
 - Data Pushing Failed
 - Database Connected
 - Database Connection Failed
 29. Shall batch add Maintenance events from IP Speaker:
 - IP Speaker Offline
 - IP Speaker Online
 30. Shall batch add Maintenance events from Security Inspection Device:
 - Security Inspection Device Offline
 - Security Inspection Device Online
 31. Shall batch add user events: User Login/Logout
 32. Shall batch add User-Defined Event
 33. Shall batch add Generic Event
 34. Shall batch add visitor events: Not Check Out in Effective Period
 35. Shall batch add Broadcast events: Alarm Input Triggered
 36. Shall batch add Security Inspection events:

- Absence Detection Alarm
 - Metal Detection Alarm
 - Package Detection Alarm
37. If an event is added or batch added and is not configured, the Web Client will offer to activate and remotely configure, if the event type is supported on the NVR or network cameras but not configured on the device
 38. Shall batch delete all invalid events
 39. Shall trigger any of the above stated events as user-defined events
 40. Shall convert any of the above stated events into an alarm
 41. Shall enable Ignore Recurring Events for events and set threshold for ignoring events recurred in
 42. For Person Amount More/Less than Threshold event of resource groups, shall set the threshold
 43. Shall set the following linkage actions of Event & Alarm
 - a. Set and view Receiving Schedule Template
 - b. Trigger recording of source related camera or up to 16 specified cameras and set pre-record and post-record duration, and video files of events can be searched and played
 - c. Lock video files
 - d. Create tag for related videos
 - e. Capture picture from the source camera or specified camera, and set the capture time
 - f. Link doors or floors. Set door status as unlock, lock, remain unlocked, or remain locked; Set floor status as free access, access with credential, temporary access, access forbidden.
 - g. Link alarm input
 - h. Link alarm output
 - i. Link speaker unit
 - j. Close alarm output manually or automatically
 - k. Trigger PTZ
 - l. Link third-party integrated resource
 - m. Send email and set the added email template. For alarm input events, attach with entry & exit counting report and link printer
 - n. Trigger user-defined event
 44. Shall have the ability to configure the same events list as alarm in Event & Alarm part
 45. Same list of events listed above in section "1,2,3" shall be available to be programmed as alarms on the SYS
 - a. When selecting a triggering event to program as alarms, only events supported by a device will appear in the Web Client
 - b. Alarm priority shall be configured to one of three levels by default:
 - High
 - Medium
 - Low
 - c. Alarm Priority of up to 255 levels can be added as required
 - d. Shall have the ability to set alarm type to different variation and states of response for alarm management and reporting
 - True
 - False
 - To be acknowledged

- To be verified
 - Custom (up to additional 25 user defined status names shall be possible)
- e. Shall have the ability to view the alarm icons for alarms in Monitoring and for alarms on Map
 - f. Shall set notification schedule template as schedule template or event-based
 - g. Shall enable Ignore Recurring Alarms for alarms and set threshold for ignoring alarms recurred in
 - h. Shall specify a user defined event or alarm input as the start or end event of the arming schedule
 - i. Shall set alarm recipients from users accounts set up in the SYS
 - j. Shall associate the source camera or up to 16 other cameras recording with alarm events
 - k. Shall lock associated alarm event video footage, so it is not auto-erased based on the camera schedule
 - l. Shall set pre-record and post-record duration
 - m. Shall display the recorded video when alarm occurred or live view by default
 - n. Shall associate a map with an alarm
 - o. Capture picture from the source camera or specified camera, and set the capture time
 - p. Shall trigger a pop-up window with an alarm event
 - q. Shall display on smart wall
 - Shall display video of the camera
 - Shall display public view
 - Set smart wall as wall related to graphic card and select smart wall No.
 - Set smart wall as wall related to decoding device and select up to 16 display windows
 - Select stream type on smart wall as main stream or sub stream
 - Stop displaying alarm after specified duration
 - Replace it with other alarm with higher priority
 - r. Shall enable restrict alarm handling time and select up to 16 user-defined events and alarm outputs to trigger events if timeout occurs
 - s. Shall trigger audible warning
46. Shall delete invalid items (in batch)
 47. Shall enable/disable alarms (in batch)
 48. Shall import newly-added alarms of Remote Sites, edit the alarm name or synchronize alarm name from site, set active control, and support alarm linkage of pop-up windows, restrict alarm handling time, set trigger event if timeout, audible warning, alarm output, alarm input, display on smart wall, email linkage, and user-defined event linkage
 49. Alarm source, trigger events, and alarm priority can also be displayed
 50. Shall support displaying alarms in alphabetical order
 51. Shall support copying alarm priority, arming schedules, receiver, pop-up window settings, trigger action controls, audio alarms, and e-mail alarms to other alarm settings
 52. Shall support template replacement function when deleting arming schedule, e-mail template, alarm priority, and users shall confirm the deleting message when deleting a template
 53. Shall support setting regular reports of events and alarms
 - a. Up to 32 events or alarms can be configured in one report, and up to 10,000 events or alarms can be calculated in total

- b. Select report type as daily or weekly
 - c. Select the sending time
 - d. Set the email template
 - e. Select the format as Excel or PDF
54. Shall support testing alarm configuration: click the button and the system will trigger an alarm automatically

22. Combined Alarm Configuration on Web Client

1. Shall select alarm triggered area
2. Shall set alarm priority
3. Shall edit alarm name
4. Shall edit description
5. Shall enable ignoring recurring alarms
6. Shall add arming schedule template
7. Shall add event source and type as the conditions to trigger alarm
8. Shall add linkage action for the combined alarm and set recipient to receive alarm

23. Generic Event Configuration on Web Client: The signal that a resource (e.g., other software, device) sends when something occurs, and is received by the system in TCP or UDP data packages

1. Shall have the ability to edit the event name
2. Shall have the ability to support 'copy from' functions
3. Shall have the ability to select transport type as TCP/UDP
4. Shall have the ability to set the match type as Search/Match
5. Shall have the ability to set the expression

24. User-Defined Event Configuration on Web Client

25. Alarm Configuration on Web Client

26. Alarm and Event Search on Web Client and Control Client: Ability to search for alarms and events, based on the following:

1. Event and Alarm Overview
 - Alarm Analysis report
 - Alarms Top 5
 - Warning Zones Top 5
2. Event Source
 - Camera
 - Door
 - Elevator
 - Alarm Input
 - ANPR
 - Person
 - UVSS
 - Remote Site
 - Encoding Device
 - Decoding Device
 - Access Control Device
 - Video Intercom Device
 - Elevator Control Device
 - Security Control Device

- Network Transmission Device
 - Dock Station
 - Digital Signage Terminal
 - Resource Group
 - Recording Server
 - Streaming Server
 - DeepinMind Server
 - Security Audit Server
 - HikCentral Professional Server
 - User
 - User-Defined Event
 - Generic Event
 - Third-Party
3. Event Type: The same event types configured on the Web Client
 4. Time
 - Last Hour
 - Today
 - Yesterday
 - Current Week
 - Last 7 Days
 - Custom Time Interval
 5. Ability to check and export alarms and events

27. Alarm Center on Control Client

1. After launching the Control Client, the user will receive the latest 500 unacknowledged alarms
2. All received alarms' information will be displayed
3. Supports selecting different layout of the Alarm Center of the Control Client, namely Related Video & Picture, Map, and both of them
4. Supports manually triggering a user-defined event
5. Supports displaying alarm details, including related map, video, picture, description, operation logs. For different event types, the details vary
6. Supports selecting video or picture as the default displayed content in the alarm information
7. Supports displaying alarm-related map, video and picture on an auxiliary screen
8. Supports selecting the items displayed in the alarm list, such as marking status, priority, number, source, area, triggering event
9. Supports counting the numbers of all alarms in the platform, including shielded alarms, disabled alarms, alarm inputs, zones, and security radars
10. Supports displaying shielded alarms only
11. Supports displaying alarms that are displayed on the smart wall only
12. Supports filtering real-time alarm list by priority, marking status, and alarming status
13. Supports enabling audible warning for an alarm.
14. Supports customizing the played text, or playing the audio defined by the platform. The audio will be displayed until the alarm ends.
15. Supports triggering the pop-up window of alarm Supports jumping to the history event list on which the alarms share the same triggering event and source
16. Supports viewing live view and playback related to the alarm
17. Supports displaying alarm-related videos on the smart wall

18. Supports downloading information of an alarm, including alarm details, picture, video, and map
19. Supports ignoring an alarm. After ignoring, the platform will not receive the alarm when it is triggered.
20. Supports acknowledging an alarm or batch acknowledging
21. Supports editing acknowledged alarm as unacknowledged
22. Supports marking alarms for highlighting
23. Supports disabling an alarm. After disabling, the user will not receive the alarm when it is triggered.
24. Supports enabling alarms after disabling.
25. Supports bypassing or restoring bypassed alarm inputs.
26. Supports bypassing or restoring bypass alarm outputs.
27. Supports forwarding an alarm to specified users.

28. Alarm Center on Mobile Client

1. Alarm Notification: Ability to receive pop-up alarm notifications
 - a. Alarm notification includes the following information:
 - Alarm type
 - Alarm time
 - Live view of the camera
 - Playback of the camera
 - b. Alarm Information: Ability to check and manage alarm history information
 - c. Alarm messages shall include the following information:
 - Alarm priority
 - Alarm category
 - Alarm source
 - Alarm time
 - Alarm name
 - Whether acknowledged
 - Server time
 - Triggering event
 - Acknowledge information
2. Alarm center has the following functions:
 - Refresh to check latest alarm information
 - Filter alarm by time, marking status, alarm priority, alarm category and alarm status
 - Switch to show marked/unmarked alarm only
 - Mark alarm message
 - Live view and playback the related video
3. For iOS mobile client, the client will play audio prompt when receiving an alarm no matter the App is running background or front, when the mobile device's audio is on
4. Ability to view logs of the calls from door stations
5. Ability to view notifications about calls from door stations

3.4 Person

A. Person Management on Web Client

1. Add person group
 - a. Relate the person group to a parent group
 - b. Set person group name

- c. Set authentication via PIN code
- 2. Add Person
 - a. Add a person manually or by reading from the ID card
 - b. Basic Information
 - ID
 - First name and last name
 - Gender
 - Person group
 - Profile picture: From Access Control Device, Video Intercom Device, or Enrollment Station; Take a Picture; Upload Picture; supports batch adding profile pictures
 - Skin-surface temperature and status
 - Effective period
 - Super user
 - Extended Access
 - Administrator Permission
 - PIN Code
 - c. Manage Credentials
 - i. PIN code
 - ii. Card
 - Set issuing mode as card enrollment station, card reader, or Enrollment Station
 - Set card format as normal or Wiegand
 - Set reading frequency as single or dual
 - Set card encryption
 - Audio on/off
 - Set effective period for the card
 - Up to 5 cards for one person
 - iii. Fingerprint
 - Set issuing mode as USB Fingerprint Recorder, Enrollment Station, or Fingerprint and Card Reader
 - Add a new fingerprint
 - Record up to 10 fingerprints for one person
 - One fingerprint can only be related to one card
 - iv. Credentials under Duress: set credentials to swipe the card or scan the fingerprint under duress, and the door will be unlocked and the Control Client will receive a duress alarm to notify the security personnel
 - v. Credentials for Dismiss: Set credentials (card number and fingerprint) so that when an alarm is triggered, you can swipe the card or scan the fingerprint configured here. The alarm will be dismissed.
 - d. Assign access levels to person
 - e. View shift schedule
 - f. Add person to face comparison group
 - g. Add person to dock station group
 - h. Set resident information to link person with indoor station and room number
 - i. Set custom public information
 - vi.
- 3. Manage person
 - a. Batch issue cards to persons

- b. Batch import persons/profile pictures
 - i. Import by excel file
 - ii. Import by importing profiles
 - Add to person group
 - Verify face quality by device
 - Add imported person to face comparison group
 - iii. Import domain persons
 - Set import mode as person or group
 - Select domain person
 - Add the domain person in existing group or add new
 - iv. Import persons from device
 - Import from access control device
 - Import from encoding device
 - Import from facial recognition server
 - Import from Enrollment Station
 - Add to person group
- c. Synchronize domain persons
- d. Cancel card loss in a batch
- e. Link persons with indoor stations in a batch
- f. Export all persons information and set password for decompressing
- g. Customize public and private information as the options for configuring a person's basic information
- h. Self-registration
 - Download the QR code for self-registration
 - Enable face quality verification by device
 - Enable self-verification reviewing
 - Set default person groups for self-registered persons
 - Approve or reject the self-registered persons
- i. Delete the selected persons
- j. Delete all the persons
- k. Move to other person group
- l. Clear assigned access levels
- m. Check person authorization
- n. Check Include Sub-Group to display persons in both parent groups and sub-groups
- o. Print persons' information onto blank physical cards

B. Person Management on Mobile Client

1. Registration for persons and visitors
2. Ability to set the required information such as ID, profile picture, last name, face comparison group, and effective period, and then upload the person information to the system
3. Ability to set the required information such as ID type, profile picture, last name, person group, visit purpose, and effective period, and then upload the visitor information to the system

3.5 Visitor

A. Visitor Registration on Web Client

1. Add a visitor
 - a. First name and last name

- b. Visitee
- c. Visit reason
- d. Visit time
- e. License plate number
- f. ID type
- g. ID number
- h. Profile picture
- i. Gender
- j. Skin-surface temperature and temperature status
- k. Visitor type
- l. Email
- m. Phone number
- n. Company
- o. Remarks
- p. Valid times for visit
- q. Access level
- r. Extended access: open the access point for longer time for person with special requirements
- s. Credential information:
 - i. Pin code
 - ii. Card
 - Set issuing mode as card enrollment station or card reader
 - Set card format as normal or Wiegand
 - Audio on/off
 - Set effective period for the card
 - Up to 5 cards for one person
 - iii. Fingerprint
 - Set issuing mode as USB Fingerprint Recorder or Fingerprint and Card Reader
 - Add a new fingerprint
 - Record up to 10 fingerprints for one person
 - One fingerprint can only be related to one card
- 2. Import visitor information file to add visitors in a batch
- 3. Add visitor type
- 4. Edit information of the visitor who is checked-in
- 5. View QR code of the visitee
- 6. Visitor check-out: manually check-out and automatically check-out
- 7. Export visitor information
- 8. Filter visitors by ID number, name, phone number, company, visitee, visit reason, visit time, status, and skin-surface temperature
- 9. Move visitor(s) to other visitor type

B. Visitor Reservation on Web Client

- 1. Administrator can make reservations for visitors on the Web Client and Mobile Client
- 2. Supports batch importing visitor reservation information and replacing repeated visitors
- 3. Employees can make reservations for visitors on a web browser by scanning a QR code using a mobile phone
- 4. Supports enabling face quality verification on a device that have the capability

5. Supports enabling self-service reservation approval. When it is enabled, all self-service reservations will be effective after the review and approval of the administrator
6. Supports setting the default visitor group of self-service reservation
7. Administrator can review the self-service reservation records and then approve, reject, or delete the reservations
8. Supports sending a 4-digit or 6-digit reservation code to the visitor via email automatically when making reservations

C. Set Self-Service Check-Out Point on Web Client

D. Visitor Access on Web Client

1. Supports setting the access levels of visitors and setting a default access level for new visitors
2. Supports applying the access levels to access control devices automatically after checking in
3. Supports withdrawing the access levels of visitors after checking out
4. Supports moving visitors to blocklist
5. Supports removing visitors from blocklist
6. Supports batch importing visitor information to blocklist and replacing repeated visitors
7. Users cannot make reservation or check in for the visitors in the blocklist. Supports notifying the user when reserving or checking in for visitors in the blocklist
8. When making a reservation or checking in for a visitor, users can upload a picture or take a picture of the certificate via PC webcam (Web Client) or mobile phone camera (Mobile Client)
9. Supports displaying the certificate picture when checking out
10. When making a reservation or checking in for a visitor, users can upload a picture or take a picture of the visitor's belongings via PC webcam (Web Client) or mobile phone camera (Mobile Client)
11. Supports displaying the certificate picture when checking out. User can choose to take the picture again

E. Check Visitor Access Records on Web Client

1. View the visatee, visit reason, location of last access, checked-in time, checked-in location, checked-out time, checked-out location, and status of visitor
2. Filter visitor access records by ID number, name, phone number, company, visatee, visit reason, visit time, status, and skin-surface temperature
3. Export visit access records

F. Manage Entry & Exit Rule for Visitor's Vehicle on Web Client

G. Visitor terminal

1. Self-Service Visitor Terminal
 - a. One screen which displays the operation interface for the visitors to operate by themselves
 - b. Visitor registration
 - c. Visitor check-out
2. Staff-Service Visitor Terminal
 - a. Two screens. The auxiliary screen for the visitors only displays the greeting image or the facial-image-capturing interface; While the touchscreen for the reception personnel displays the operation interface.
 - b. Visitor registration
 - c. Visitor check-out
 - d. View visitor details

- e. Export visitor information
- 3. System Settings
 - a. Language
 - b. Time
 - Time zone
 - Current time
 - c. Person and ID comparison
 - Person and ID comparison threshold
 - Allow skipping person and ID comparison
 - Allow skipping person and ID comparison/temperature screening
 - d. Face rating threshold
 - e. Temperature screening
 - Temperature alarm threshold (max.)
 - Temperature alarm threshold (min.)
 - Max. measurement distance
 - f. Visitor credential
 - Card
 - Visitor pass
 - g. Required visitor information
 - h. Use ID photo as profile
 - i. Network settings
 - Wired network
 - Wi-Fi
 - Platform access
 - j. Visitor privacy settings
 - Save and display captured face picture
 - Visitor records retention period

3.6 Access Control and Elevator Control

A. Wizard and Overview on Web Client

1. View wizard
 - a. Add an access control device
 - b. Add an access schedule template
 - c. Add a person
 - d. Add an access level
 - e. Assign an access level to person
 - f. Control door and elevator status
 - g. Perform access control retrieval
2. Display overview of health status, person credential status, access event statistics, and person access events

B. Manage Access Control Devices on Web Client

1. Add access control device to the platform by Hikvision Private Protocol via the following discovery options:
 - a. IP Address
 - b. IP Segment
 - c. Batch Import

2. Add access control device to the platform by Hikvision ISUP Protocol via the following discovery options:
 - a. Device ID
 - b. Device ID Segment
 - c. Batch Import
3. Add online devices in the same local subnet with the Local Network/Server Network using Search Active Device Protocol (SADP) by Hikvision Private Protocol or Hikvision ISUP Protocol
4. Add doors to area
5. Apply time zone settings to the device
6. Synchronize name
7. Set configuration of the added devices
 - a. Time settings for the device
 - b. Turnstile parameters
 - c. Reboot the device
 - d. Restore default
 - e. Custom Wiegand
 - f. Linkage
 - g. Card swiping parameters
 - h. More remote configuration parameters
8. Refresh the status of the added devices
9. Reset device password (in batch)
10. Activate the online devices

C. Manage Elevator Control Devices on Web Client

1. Add elevator control device to the system by Hikvision Private Protocol via the following discovery options:
 - a. IP Address
 - b. IP Segment
 - c. Batch Import
2. Add online devices in the same local subnet with the Local Network/Server Network using Search Active Device Protocol (SADP)
3. Add floors to area
4. Apply time zone settings to the device
5. Synchronize name
6. Set configuration of the added devices
 - a. Time settings for the device
 - b. Reboot the device
 - c. Restore default
 - d. More remote configuration parameters
7. Refresh the status of the added devices
8. Reset device password (in batch)
9. Activate the online devices

D. Area Management on Web Client

1. Shall edit the following settings of doors for current site:
 - a. Basic information
 - door name
 - Set door contact as normally open or normally closed

- Set exit button type connection mode as normally open or normally closed
- Open duration(s)
- Extended open duration(s)
- Enable door open timeout alarm
- Set maximum open duration(s), and the system can receive the alarm after configuring alarm in Event & Alarm module
- Set duress code
- Set super password
- b. Related cameras
 - Link up to two camera(s) to the door to view its live view
 - Enter super password after granted
- c. Picture storage settings
 - Set storage location as system management server
 - Set storage location as Hybrid SAN
 - Set storage location as Cloud Storage Server
 - Set storage location as a pStor
 - Set storage location as an NVR
- d. Card reader settings
 - Edit card reader parameters
 - Card reader name
 - Set polarity
 - Set minimum card swiping interval
 - Set the duration of entry reset on keypad
 - Enable failed card attempts alarm and set maximum failed attempts
 - Enable tampering detection
- e. Add face recognition terminal for the turnstile
 - Add face recognition terminal by online devices
 - Add face recognition terminal by IP address
 - Add face recognition terminal by device ID
- f. Synchronize and apply door name
- g. Map settings
 - Add the door to map
 - Set map icons
- 2. Shall edit the following settings of elevators for current site:
 - a. Basic information
 - Elevator name
 - Open duration(s)
 - Extended open duration(s)
 - Enable elevator door open timeout alarm
 - Set maximum open duration(s), and the system can receive the alarm after configuring alarm in Event & Alarm module
 - Set duress code
 - Set super password
 - Set dismiss code
 - b. Manage the floors of the elevator
 - Edit floor name

- Reset imported floor No.
 - c. Related cameras
 - Link up to two camera(s) to the elevator to view its live view
 - d. Card reader settings
 - Edit card reader parameters
 - Card reader name
 - Set polarity
 - Set minimum card swiping interval
 - Set the duration of entry reset on keypad
 - Enable failed card attempts alarm and set maximum failed attempts
 - Enable tampering detection
 - e. Synchronize and apply floor name
 - f. Map settings
 - Add the elevator to map
 - Set map icons
- E. Set Access Schedule Template on Web Client**
1. Affect the applied access levels and access control application parameters after edited
 2. Apply the changes to the device after edited
- F. Enable Event Subscription on Web Client**
1. Device events
 2. Normal access events
 3. Abnormal access events
- G. Set User to Receive Access Control Calls**
- H. Access Level Configuration on Web Client**
1. Add access level
 - a. Add the access point(s) to the access level
 - b. Select the access schedule to define in which time period the person is authorized to access the access points:
 - Customize a new schedule
 - All-day Template
 - Weekday Template
 - Weekend Template
 - Copy from other defined templates
 - Add new holiday schedule
 2. Delete (all) access level(s)
 3. Filter the access levels from the following conditions:
 - a. Access level
 - b. Access schedule
 - c. Access point
 4. Modify the access level name, description, access point(s), access schedule
 5. Assign the access levels to person(s) so that the person(s) will have the access permission to access the access point(s)
 - a. Assign an access level to persons
 - b. Assign access levels to persons
 - c. Assign access levels to person groups
 - d. Assign access levels to access groups
 - Create a name for a access group

- Select person(s) from person groups for the access group
 - Edit access group name
 - Manage the persons in the group: adding person(s) and removing person(s) from the group
 - Delete an access group or delete all
6. Apply person's access level settings to device
 - a. Manually apply
 - Apply changes: Apply the person's changed (newly added, edited, deleted) access levels to the device
 - Apply all: First, clear all the access levels configured on the device. Then, apply all the person's access levels configured in the system to the device. This mode is mainly used for first time deployment
 - b. Regularly apply (scheduled)
 - Apply at fixed time
 - Apply every certain hours

I. Access Control Application on Web Client

1. Free Access & Access Forbidden: set doors and floors accessible or inaccessible during certain periods
2. First Person In: only after the first person is authorized to enter with his or her card, fingerprint, or face, can other people's permission be activated
 - a. Enable to set remaining unlocked duration
 - b. Enable to set authorization: the door is locked and access is denied with credentials until you swipe the first card. After swiping the first card, the door is authorized and the persons with corresponding access level are granted to access. The authorization will be invalid at 00:00 am every day
3. Multi-Factor Authentication: The door will unlock only after multiple persons present authenticating multiple credentials in turn. Three access modes are available:
 - c. Unlock after access granted
 - d. Remotely unlock after granted
4. Multi-Door Interlocking: enable the multi-door interlocking function between multiple doors of the same access control device
5. Anti-Passback: The person should exist via the door in the anti-passback if he/she enters via the door in the anti-passback. It minimizes the misuse of fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access.
 - a. Forgive anti-passback violation regularly
6. Emergency Operation Group: add a group for access points which need to be operated (remaining locked/unlocked) in a batch
7. Entry & Exit Counting: enable this function to count the persons entering and exiting the doors in the group
8. Card Reader Access Mode
 - a. Select mode of applying card reader access mode settings as Batch or Single
 - b. Select card reader access mode
 - c. Enable custom card reader access mode
 - d. Copy access mode settings to other card reader
9. Apply application settings to device

J. Access Control Test (Troubleshooting) on Web Client

1. Shall be able to view the status of the credentials

- a. Persons with no credential configured
 - b. Persons with no card configured
 - c. Persons with no fingerprint configured
 - d. Persons with temporary card
 - e. Persons with card reported as lost
2. Shall be able to view the status of the access control devices and elevator control devices
 - a. Device name
 - b. Network status
 - c. Arming status
 - d. Device time
 - e. Persons on device and credentials on device
 - f. Persons in system and credentials in system
 - g. Persons applying to device failed and credentials applying to device failed
 - h. Persons to be applied to device
 3. Shall be able to test whether the persons can access the target access points according to the current settings
 - a. Authorization settings of persons/visitors applying to device failed
 - b. Authorization settings of persons/visitors applying to device succeeded
 - c. Authorization settings of persons/visitors to be applied to device
 4. Shall be able to test whether the access points can run according to the current settings.

K. Live View of Door-Related Camera on Control Client

1. Shall view the live video of up to two related cameras in one display window. When the door links two cameras, the video will display in Picture-in-Picture mode, and you can view the live video of the two cameras in one display window.
2. Shall support fisheye expansion, displaying camera status, setting arming control, switching stream type, viewing the live video on smart wall, displaying VCA search window, turning on/off the alarm outputs, and audio control
3. Shall control the door status as unlock, lock, remain unlocked, remain locked, and view the card swiping record in real-time
4. Shall forgive anti-passback violation
5. Shall check the turnstile status and control it as unlock, lock, remain unlocked, remain locked
6. Shall control all doors status as forbid/allow all doors access
7. Shall trigger user-defined event
8. Shall handle opening door request from video access control terminal, including voice talk and unlocking door
9. Shall show access point's real-time status
10. Shall support two-way audio between video access control terminal and control client

L. Live View of Elevator-Related Camera on Control Client

1. Shall view the live video of up to two related cameras in one display window. When the elevator links two cameras, the video will display in Picture-in-Picture mode, and you can view the live video of the two cameras in one display window
2. Shall support fisheye expansion, displaying camera status, setting arming control, switching stream type, viewing the live video on smart wall, displaying VCA search window, turning on/off the alarm outputs, and audio control
3. Shall control the floor status as temporary access, access with credential, free access, or access forbidden in real-time
4. Shall control all floors status as forbid/allow all floors access

5. Shall trigger user-defined event
6. Shall show floor's real-time status

M. Playback of Door-Related Camera on Control Client

1. Shall view the playback of up to two cameras in one display window
2. Shall trigger user-defined event

N. Playback of Elevator-Related Camera on Control Client

1. Shall view the playback of up to two cameras in one display window
2. Shall trigger user-defined event

O. Control Door Status in Real-Time on Web Client and Control Client

1. Lock door
2. Unlock door
3. Remain door unlocked
4. Remain door locked
5. Recover door status
6. Control status of all the doors or part of the doors in specified emergency operation group

P. Control Elevator Status in Real-Time on Web Client and Control Client

1. Temporary access
2. Access with credential
3. Access forbidden
4. Free Access
5. Recover floor status
6. Control status of all the floors or part of the floors in specified emergency operation group

Q. Access Control Retrieval on Web Client, Control Client and Mobile Client

1. Search access records
 - a. Support searching access events
 - b. Support viewing access event related video
 - c. Support viewing the person profile, card number, person name, ID, time, access point, access result, and access mode
 - d. Supports forgiving anti-passback violations
 - e. Support forgiving all the anti-passback violation events in the search result
 - f. Support downloading the searched person information
 - g. Support filtering results by normal person and visitor
 - h. Support exporting card swiping records
2. Perform entry & exit counting
 - a. Select one entry & exit counting group
 - b. Select persons
 - c. Search records within 24 hours
 - d. Set entry & exit counting type as people stayed/ people exited/all
 - e. View event details: profile, name, entry & exit counting type, phone number, location of last access
 - f. Display the access direction (entering/exiting) of turnstile
 - g. Download single record
 - h. Export all searched records in excel format

3.7 Video Intercom

A. Manage Video Intercom Devices on Web Client

1. Add indoor station and door station to the system by Hikvision Private Protocol via the following discovery options:
 - a. IP Address
 - b. Batch Import
2. Add outer door station and master station to the system by Hikvision Private Protocol via the following discovery options:
 - a. IP Address
3. Add online devices in the same local subnet with the Local Network/Server Network using Search Active Device Protocol (SADP)
4. Set device location information including community, building, unit, and room for indoor station
5. Set device location information including community, building, unit for door station
6. Set device location information including community for outer door station and master station
7. Add floors to area
8. link indoor station with resident
9. Apply time zone settings to the device
10. Set configuration of the added devices
 - a. Time settings for the device
 - b. Calling management center settings for door station
 - c. Card encryptions for door station and outer door station
 - d. Set related cameras for indoor station
 - e. Reboot the device
 - f. Restore default
 - g. More remote configuration parameters
11. Refresh the status of the added devices
12. Reset device password (in batch)
13. Activate the online devices
14. Apply Device Settings: Clear the original data on the device and apply the current settings in system to the device(s) after restoring the database or device's default configurations

B. Video Intercom on Control Client and Mobile Client

1. Shall view live videos of door's related camera(s)
2. Shall control doors to lock, unlock, remain locked, or remain unlocked during live view
3. Shall call the added indoor station for starting voice talk with the resident, viewing the video of the indoor station's camera, etc.
4. Shall answer the call from the added door station and open door if needed

3.8 Time and Attendance

A. Wizard and Overview of Time and Attendance on Web Client

- 1.

B. Set Timetable on Web Client

1. Add a break timetable
2. Set a name for the timetable
3. Set the timetable type as timetable for normal shift: the required start-work time and end-work time is fixed
 - a. Set scheduled work time
 - b. Set valid check-in/out period

- c. Set minimum work hours
 - d. Set flexible mode as Allow Late/Early Leave and set allowable duration respectively
 - e. Set flexible mode as Flexible Period and set the flexible duration
 - f. Select break timetable to set the break time
4. Set the timetable type as timetable for man-hour shift: no required start-work time and end-work time, but the minimum work hours should be met
 - a. Set calculation mode:
 - Calculated By: First In & Last Out, Each Check-In/Out
 - Enable T&A Status on Device
 - b. Set valid check-in/out period
 - c. Set minimum work hours
 - d. Select break timetable to set the break time

C. Set Shift on Web Client

1. Set a name for the shift
2. Copy the settings from other existing shift
3. Set repeat by week: the shift will repeat every 7 days or two weeks based on the week
4. Set repeat by day(s)
 - a. Set the frequency of repeat days
 - b. Set the start date for reference
5. Set the shift type as normal shift or man-hour shift
6. Set the timetable for the shift
7. Set access record calculation mode as First In & Last Out or Each Check-In/Out
8. Enable Time and Attendance status on device so that the attendance status set on the attendance terminal is valid
9. Add holidays to define the special days when the shift is disabled

D. Manage Shift Schedule on Web Client

1. Shift schedule overview
2. Assign shift schedule to person group
3. Assign shift schedule to person
4. Add temporary schedule

E. View Attendance Record on Web Client

5. Filter the attendance records according to the following conditions:
 - a. Time Period
 - b. Time
 - c. Person name
 - d. Status
6. View the attendance details and the person's attendance report for one day
 - a. Person name
 - b. ID
 - c. Date
 - d. Status
 - e. Scheduled work time
 - f. Required work hours
 - g. Actual work time
 - h. Late duration
 - i. Early leave duration
 - j. Break duration

- k. Leave duration
- l. Overtime 1 duration
- m. Overtime 2 duration
- n. Overtime 3 duration
- 7. View the attendance details and the person's attendance report for more than one day
 - a. Person name
 - b. ID
 - c. Times of late and specific date
 - d. Times of early leave and specific date
 - e. Times of absent and specific date
 - f. Times of late and early leave and specific date
 - g. Times of normal and specific date
 - h. Actual work hours
 - i. Break duration
 - j. Times of leave and specific date
 - k. Total overtime duration
- 8. Get attendance records from managed devices
- 9. Calculate attendance again manually
- 10. Handle exceptional records
 - a. Correct check-in/out time
 - b. Apply for leave
 - c. Handle for one record or for multiple records in a batch
- 11. Export the filtered attendance records
 - a. Set the format of the exported file
 - b. Select the items for export
 - c. Export attendance details
- 12. View handling records
- 13. Search the history attendance result even if this person has been deleted from the system
- 14. When the device is online, upload the records to system of the device offline duration
- 15. Support different time zone of the device and HikCentral Professional platform

F. Attendance Configuration on Web Client

- 1. Set Attendance Check Point on Web Client
 - a. Add the access point as attendance check point
 - b. Add the facial recognition camera as attendance check point
 - c. Attendance check point type includes: check-in & out, check-in only, check-out only
- 2. Set General Attendance Rules Configuration on Web Client
 - a. Set weekends
 - b. Define absence
 - If check in late for longer than the threshold, mark as absent
 - If check out earlier for longer than the threshold, mark as absent
 - If no check-in, mark as absent or late
 - If no check-out, mark as absent or early leave
 - c. Set authentication mode:
 - Card
 - Fingerprint
 - Face
 - d. Set time point for attendance result auto-calculation

- e. Set display time by minute or by hour
- 3. Define Overtime Configuration on Web Client
 - a. Set work hour rate
 - b. Define overtime in workdays
 - Enable/disable overtime on workdays
 - Set calculation mode as By Total Work Hours
 - Define valid overtime if overtime exceeds required work hours for certain minutes
 - Set daily overtime level
 - Set calculation mode as By Total Work Hours or By Time Periods
 - Count early check-in as overtime
 - Count late check-out as overtime
 - Set daily overtime level
 - c. Define overtime on weekends
 - Enable/disable overtime on weekends
 - Define valid overtime if works longer than certain minutes
 - Set maximum length of overtime
 - Set overtime level for overtime on weekends
 - d. Define overtime on holidays
 - Define valid overtime if overtime is longer than certain minutes
 - Set maximum length of overtime
 - Set overtime level for overtime on holidays
- 4. Define Leave on Web Client
 - a. Define major types of leaves
 - b. Define minor types of leaves
- 5. Set auto-calculation time of attendance results
- 6. Configure attendance results accuracy
 - c. Min. Unit
 - d. Rounding
 - e. Display Format

G. Set Display Rules for Attendance Report on Web Client

- 1. Set company information
- 2. Set format of date and time
- 3. Set marks of different status

H. Attendance Reports on Web Client

- 1. Create an attendance report
 - a. Set report name
 - b. Set event report target
 - c. Set report content
 - d. Set report type
 - e. Set report sending time
 - f. Select email template
 - g. Set the report language
- 2. Customize an attendance report
 - a. Set report name
 - b. Select predefined report type
 - c. Select data items to be include in the report
 - d. Select a sorting rule for records

I. View and Export Attendance Reports on Web Client

1. Export normal attendance report
 - e. Department report
 - f. Daily report
 - g. Monthly overview
 - h. Access records
 - i. Start/End work time
 - j. First/Last Access
2. Export Abnormal attendance report
 - a. Abnormal overview
 - b. Absence
 - c. Early leave
 - d. Late
 - e. Check-in/out correction
 - f. Leave
3. Export overtime report
 - a. Monthly Overtime Details
 - b. Monthly Overtime Overview
4. Select the person or department for the report
5. Set time range of the report
6. Set format of the report
7. Set display rules of attendance reports
 - a. Company information: company name and logo
 - b. Format of date and time
 - c. Marks of different status

3.9 Security Control

A. Wizard and Overview of Alarm Detection on Web Client

1. View wizard
 - a. Add security control device
 - b. Add alarm input
 - c. Add security control partition (area)
 - d. Add alarm input and partition (area) to map
 - e. Add defense schedule template
 - f. Configure event and alarm parameters
2. Display overview of resource status and alarm detection events

B. Manage Security Control Devices on Web Client

3. Add security control device to the system by Hikvision Private Protocol via the following discovery options:
 - a. IP Address
 - b. Hik-Connect
 - c. IP Segment
 - d. Port Segment
 - e. Batch Import
4. Add security control device to the system by Hikvision ISUP Protocol via the following discovery options:
 - a. Device ID

- b. Device ID Segment
- c. Batch Import
- 5. Add online devices in the same local subnet with the Local Network/Server Network using Search Active Device Protocol (SADP)
- 6. Add alarm inputs and other channels to area
- 7. Apply time zone settings to the device
- 8. Set remote configuration of the added security control devices
- 9. Refresh the status of the added devices
- 10. Reset device password (in batch)
- 11. Activate the online devices
- C. Area Management on Web Client**
 - 1. Select security control device's zones as alarm inputs to add into the area
 - 2. Set defense schedule for the arming mode in different time periods for the partitions of the added security control devices
 - 3. Arm/disarm radar
- D. View Radar-Related Live View on Control Client**
 - 1. Shall view the live video of the radar's calibrated cameras.
 - 2. Shall arm or disarm the radar's zones
 - 3. Shall show the people's moving pattern tracked by the radar on the map
- E. View Radar-Related Playback on Web Client**
 - 1. Shall view the playback in one display window
 - 2. Shall trigger user-defined event

3.10 Vehicle and Parking

- A. Wizard and Overview on Web Client**
 - 1. View wizard
 - a. Vehicle and card management:
 - Manage vehicles
 - b. Parking lot management:
 - Add entrance & exit devices
 - Add entrances & exits for parking lots
 - Add entry & exit rules
 - Search vehicle passing records
 - c. Parking fee:
 - Enable parking fee
 - Add parking fee rules
 - Manage the parking pass and top-up for registered vehicles
 - Search parking fee records
 - d. Parking lot guidance:
 - Add guidance terminals, guidance screens, and parking cameras
 - Add parking spaces
 - Monitor real-time status of parking spaces
 - Search parking records
 - 2. Display overview of resource status, parking space statistics, vehicle passing statistics, and vehicle passing events
- B. Basic Settings on Web Client**
 - 1. Customize vehicle information

- a. Add vehicle types
- b. Add custom information for vehicles
- 2. Set parking fee mode
 - a. Charge mode
 - b. Free mode
- 3. Add rules for plate fuzzy search
- 4. Add users to receive calls from parking lot
- 5. Create overtime parking report to be regularly sent
 - a. Set the report name
 - b. Set report type
 - c. Set report sending time
 - d. Select email template
 - e. Set the report language

C. Parking Lot Management on Web Client

- 1. Add one parking lot
 - a. Parking lot name
 - b. Number of entrances and exits
 - c. Capacity
 - d. Number of vacant parking spaces
 - e. Total parking spaces for registered vehicles
 - f. Vacant parking spaces for registered vehicles
 - g. Maximum parking duration
 - h. Expiration prompt
 - i. One account with multiple vehicles
- 2. Add multiple parking lots
- 3. Add entrance and exit to the parking lot
- 4. Add lane to the entrance and exit
 - a. Lane type: Entrance or Exit
 - b. Lane name
 - c. Link a capture unit with the lane
 - d. Link an access control device or video intercom device with the lane for opening barrier by card or video intercom
 - e. Link a display screen with the lane
 - f. Set device for barrier control
- 5. Set content displayed on the display screen
 - a. Display mode: Still, scroll up, scroll down, scroll left, scroll right
 - b. Font Color
 - c. Alignment: Align left, align right, align center
 - d. Text on Screen: Plate number, entering time, parking duration, and expiration prompt

D. Set Entry & Exit Rule on Web Client

- 1. Set entry & exit mode and account deduction
 - a. Entry mode:
 - No Repeated Entry
 - License Plate and Card Match
 - b. Exit mode: License Plate and Card Match
 - c. Enable/disable Auto account deduction
 - d. When parking fee is 0:
 - Allow

- Not Allow
2. Set entry & exit rule for temporary/registered vehicles
 - a. Entry method:
 - Manual
 - Automatic
 - b. Exit method:
 - Manual
 - Automatic
 - c. When no vacancy for temporary/registered vehicle:
 - Allow
 - Not Allow
 3. Set entry & exit rule for visitor vehicles
 - a. Entry method:
 - Manual
 - Automatic
 - b. Exit method:
 - Manual
 - Automatic
 - c. Entry & exit time range:
 - All-Day
 - Custom
 4. Add entry & exit rule for vehicles in list
 - a. Rule name
 - b. Vehicle list
 - c. Entry method:
 - Manual
 - Automatic
 - d. Exit method:
 - Manual
 - Automatic
 - e. Parking space control:
 - Capacity
 - Vacant
 - When no vacant parking spaces for vehicles in list: Allow, Not Allow
 5. Add free entry & exit rule on holidays
 - a. Type of holiday:
 - Holiday Template
 - Day of Week: Holiday name, holiday range, and day of the week
 - b. Description

E. Set Parking Fee Rule on Web Client

1. Set parking fee rule for temporary vehicles
 - a. Rule name
 - b. Vehicle type
 - c. Charge by:
 - Free
 - Unit Parking Duration
 - Session

- Time range
 - Clock time
 - Time and Sessions in Daytime and Nighttime
 - Unit Time Range
2. Set parking fee rule for registered vehicle
 - a. Rule name
 - b. Parking pass type:
 - Annual
 - Monthly
 - Custom Day(s)
 - Monthly (Idle Time)
 - c. Parking fee
 3. Set parking fee rule for vehicles in list
 - a. Rule name
 - b. Vehicle list
 - c. Charge by:
 - Free
 - Unit Parking Duration
 - Session
 - Time range
 - Clock time
 - Time and Sessions in Daytime and Nighttime
 - Unit Time Range
 4. Set discount rule
 - a. Rule name
 - b. Discount method
 - Discount
 - Free discount
 - Free
 - Parking duration reduction
 - c. Discount rate
 - d. Effective period
 - e. Description
 5. Set parking fee rule for exceptional pass
 - a. Rule name
 - b. Parking fee
 - c. Effective period
 - d. Description
 - e. Set as default
 6. Additional configurations about parking fee
 - a. Set free parking duration after payment
 - b. Set pricing mode for multiple vehicles under one account:
 - Charge Extra Entering Vehicle
 - First Exiting Vehicles Pay

F. Vehicle and Card Management on Web Client

7. Add a registered vehicle
 - a. License plate name

- b. Vehicle list
- c. Vehicle type
- d. Color
- e. Brand
- f. Undercarriage picture
- g. Vehicle owner information
- 8. Add registered vehicles in a batch
- 9. Delete expired registered vehicles
- 10. Export all registered vehicles' information
- 11. Add a vehicle list
 - a. List name
 - b. List color
 - c. Entry & exit rule
 - d. Parking space control
 - e. Effective period
 - f. Description
- 12. Add vehicles to the vehicle list
- 13. Filter and export visitor vehicles
- 14. Add a vehicle to blacklist, import vehicles to blacklist, and export information of vehicles in blacklist
- 15. Issue temporary cards to temporary vehicles

G. Add Parking Passes and Top-Up for Registered Vehicles on Web Client

- 1. Select a vehicle to be topped up
- 2. Select the parking lot
- 3. Select the parking pass rule
- 4. Set number of parking passes
- 5. Set effective period
- 6. Select top-up method
- 7. Top up for all registered vehicles

H. Parking Guidance Configuration on Web Client

- 1. Add floors to the parking lot
- 2. Relate guidance terminals and guidance screens to the floor
- 3. Configure a map for the floor
- 4. Mark guidance screen on the map
- 5. Configure types for parking spaces on the map

I. Parking Space Overview on Web Client

- 1. View occupancy rate of the parking spaces in a parking lot,
- 2. View number of vacant parking spaces,
- 3. View occupied parking spaces
- 4. View parking spaces with unknown status
- 5. View number of overtime parking and parking violations
- 6. Click one parking space on the map to view its detailed information, such as its status and type. In addition, you can enter the parking space No., license plate No., or parking time to search for specific information

J. Toll Center on Web Client

- 1. Swipe the temporary card or enter the license plate number of a vehicle
- 2. Set discount rule

3. Pay the parking fee
4. Print receipt

K. Vehicle Search on Web Client

1. Ability to search for visitor vehicles, vehicle passing records, parking records, parked vehicles, payment records, vehicle top-up and refund records, transaction records of vehicle owner account, work records of operators, and coupon records by setting different conditions
2. Ability to export the searched records in EXCEL or CVS format

L. Statistics and Reports on Web Client

1. View and export the statistics related to the operations of parking lots, such as the parking lot occupation rate, parking duration distribution, traffic flow statistics
2. View and export the statistics related to the revenue and expenditure of parking lots, such as the trend and type of revenue and expenditure, the revenue and expenditure generated in a specific period

M. ANPR Camera Live View on Control Client

1. Ability to display license plate number when viewing LPR camera after the LPR function is activated in license
2. Ability to mark a vehicle license plate number
3. Ability to add the vehicle to vehicle list
4. Ability to go to Vehicle Search by quick link:
 - a. Label
 - b. License Plate number
 - c. Vehicle passing time
 - d. Camera name
 - e. Owner
 - f. Phone
 - g. Country/region
 - h. Operation
 - Add to vehicle list
 - Download
5. View the live video of the UVSS's linked camera, the undercarriage picture, and recognized license plate number of the passing vehicles
6. Drag on the undercarriage picture to mark important information
7. Mark the vehicle license plate number

N. UVSS Live View on Control Client

1. View the live video of the UVSS's linked camera, the undercarriage picture, and recognized license plate number of the passing vehicles
2. Perform the following operations in live view:
 - a. Mark on undercarriage picture
 - b. Mark vehicle
 - c. Add vehicle to vehicle list
 - d. Search vehicle

O. Entrance & Exit Control on Control Client

1. Vehicle real-time number of free parking spaces and total capacity of the parking lot
2. View information of vehicles entered or exited from the parking lot
 - a. Vehicle picture
 - b. License plate number
 - c. Vehicle list

- d. Direction
 - e. Entering/Exiting time
 - f. How to open barrier
 - g. Allowed or not
3. Add the new detected vehicle to the vehicle list
 4. Search logs of recognized vehicle license plate and the related vehicle passing information
 5. Mark vehicle if needed
 6. Open barrier automatically according to the configured entry & exit rule
 7. Open barrier automatically after the vehicle owner swiping her/his card
 8. Open barrier manually and enter remark information (optional)
 9. Open barrier manually during video intercom
 10. Correct the license plate numbers recognized by capture units
 11. Barrier control to open, close, or remain the barrier open
 12. Lock/unlock single barrier gate or all barriers

P. Vehicle Search on Control Client

1. Ability to search for vehicle passing records, parking records, parked vehicles, payment records, and multiple vehicles under one account status by setting different conditions
2. Ability to export the searched records in EXCEL or CVS format

3.11 Intelligent Recognition

A. DeepinMind Server Management on Web Client

1. Enable WAN access
2. Add cameras to DeepinMind server for analysis tasks

B. Face Comparison Group Management on Web Client

1. Add face comparison group
 - a. Group name
 - b. Set similarity threshold
 - c. Add description
 - d. Add person(s) to the group
 - Add existing persons from person list or other face comparison groups
 - Add new persons
 - e. Remove the person(s) from the face comparison group
2. Edit the face comparison group and view the cameras that it is applied to
 - a. Delete the face comparison group
 - b. Delete all the face comparison groups
3. Apply the face comparison group(s) to camera(s)

C. Intelligent Recognition Task Management on Web Client

1. Ability to add task schedule template
2. Ability to add different tasks with types:
 - a. Facial recognition task
 - b. Human body recognition task
 - c. Frequently appeared person analysis task
 - d. Rarely appeared person analysis task
 - e. Archive analysis task
 - f. Behavior analysis task

D. Applying Center on Web Client

1. Apply face information to devices

- a. Ability to apply specific face information to devices
- b. Ability to apply face comparison groups to devices
- c. Ability to automatically apply changed face information to devices
- 2. View applying status of cameras and faces
- 3. Apply abnormal applying record again:
 - a. Cameras failing to receive faces
 - b. Cameras to be applied to
 - c. Faces failed to be applied
 - d. Faces to be applied

A. View Detected and Matched Face in Live View on Control Client and Mobile Client

- 1. View the face comparison information between the detected faces and the face pictures in the selected face comparison group
- 2. Display person's profile (configured in the Web Client):
 - a. Captured time
 - b. Compared result
 - c. Device name
 - d. Face comparison group
 - e. Gender
 - f. ID number
 - g. Email address
 - h. Phone number
- 3. Search video of the person by the captured face picture
- 4. Add mismatched person to person list
- 5. Display the similarity between the captured face picture and the original face picture in person list

B. Person Search on Control Client and Mobile Client

- 1. Search by Face Picture: Ability to search face picture to view face-related face pictures and videos. It includes 3 types:
 - a. Search matched pictures: Ability to search videos of a person who is added to the face comparison group
 - b. Search captured pictures: Ability to search related videos of an uploaded face picture by camera, time, person information, and similarity
 - c. Search frequently appeared persons: Ability to search persons who appear frequently
- 2. Search by Archive
 - a. The system will save the features and information (including captured picture and video) of the captured person as archive.
 - b. Ability to upload a picture and search the related archives of a face picture to check the captured pictures or videos of similar persons
 - c. Ability to adjust the similarity
 - d. Ability to check whether a person is a stranger
 - e. Ability to export the search results
- 3. Search by Identity Verification
 - a. Ability to upload a picture and search the persons who are similar with the person in the picture. Check the matched person information
 - b. Ability to upload two pictures and compare them to see the similarity of the persons in those two pictures
 - c. Ability to adjust the similarity

3.12 Temperature Screening and Mask Detection

A. Set Skin-Surface Temperature When Adding Persons and Visitors on Web Client

B. Temperature Screening Configuration on Web Client

1. Group temperature screening points
2. Configure temperature screening parameters
 - a. Temperature screening threshold
 - b. Alarm threshold

C. Real-Time Skin Surface Temperature Monitoring on Web Client and Control Client

1. View detected people information in real-time
2. View skin-surface temperature of the detected people
3. View whether the people wears a mask
4. View triggered alarms

D. Real-Time People Counting on Control Client

1. View number of people in specified region in real-time
2. Triggers an alarm when the number of people exceeds the configured threshold and highlights the region on the map

E. Search History Temperature Screening Data on Web Client

F. People Registration on Web Client

1. Register the person information for the persons detected
2. Custom registration template
3. View registered person information

G. Generate Report on Web Client

3.13 Dock Station

A. Manage Dock Station Devices on Web Client

1. Add devices to the system via the following discovery options:
 - c. IP Address/domain
 - d. IP Segment
 - e. Port Segment
 - f. Batch Import
2. Apply time zone settings to the device
3. Add to dock station group

B. Dock Station Group Management on Web Client

1. Add dock station group
 - a. Edit the dock station group name
 - b. Add person to the group
 - Add existing person from person list
 - Add new person
 - c. Set dock stations for the persons in the group. The videos stored in the persons' body cameras can be uploaded to these dock stations
 - d. Group name
 - e. Shift schedule
 - f. Attendance shift schedule on every day
2. Manage the persons in the group, such as adding existing person from the person list, adding new person, editing, deleting, importing and exporting persons, etc.
3. Delete (all) dock station group(s)

3.14 Smart Wall

A. Smart Wall Configuration on Web Client

1. Supports detecting online devices: detecting online devices in the same network segment with the server or the client via SADP
2. Supports adding devices via IP address, IP segment, and port segment
3. Supports jumping to the remote configuration page of the device via web browser
4. Supports cascading configuration of decoders(DS-69 series) and video wall controllers(DS-C10S series)
5. Supports adding, deleting, and editing the LCD smart wall
6. Supports adding, deleting, and editing the LED smart wall
7. Supports batch editing resolutions of the outputs of decoders
8. Supports linking the decoding output with the window and releasing this linkage
9. Configuring the audio port of the smart wall
10. Supports setting the background color/picture of the output
11. Supports displaying the decoding output port No. on the large screen
12. Supports configuring stream types (sub/main stream) and auto-switching the stream type
13. Supports displaying and downloading the camera ID
14. Supports signal sources streaming the live view in a batch

B. Smart Wall (Graphic Card) on Control Client

1. Display all contents in live view on smart wall
2. Display live view of one camera on smart wall
3. Display live view of all cameras in one area on smart wall
4. Display e-map and GIS map on smart wall
5. Display view and view group on smart wall
6. Display alarm's related video on smart wall
7. Display Health Monitoring page on smart wall
8. Display videos of triggered alarm in windows that are marked with red frame

C. Smart Wall (Decoding Device) on Control Client

1. Supports window division mode (2/4/6/8/9/12/16/35/36-window), locking window, enlarging/restoring the size of the sub-window by double-click, and sticking the window on top or at bottom
2. Supports creating, deleting, moving, stick on top/at bottom, and changing the size of roaming windows
3. Supports enabling/disabling the VCA rule
4. Supports displaying the window No.
5. Supports displaying the local signal source (single or in a batch) on the smart wall via ONVIF, Hikvision Protocol, or the domain name of the camera
6. Supports controlling the loop video wall display of a camera in a single window, including pausing, continuing, viewing the last/next, and adjusting the loop schedule
7. Supports switching the main/sub stream of the signal source manually
8. Supports PTZ control
9. Supports customizing the camera ID displayed on the smart wall
10. Supports the echo, video wall playback, and control of the video image in the window
11. Supports displaying the decoding status of the output port
12. Supports the client displaying the images the same as those on the full smart wall
13. Supports adding a logo on the window
14. Supports configuring the background picture

15. Supports rolling/static captions on LED smart wall
16. Supports displaying the clock on the window of LED smart wall
17. Supports layout preview of the LED smart wall
18. Supports joining windows on the LED smart wall

3.15 Intelligent Analysis

A. Set Resource Groups for Intelligent Analysis on Web Client

B. Create Intelligent Analysis Reports to Be Regularly Sent

3. Set the following report type:
 - g. People counting
 - People counting for one camera
 - People counting in one region
 - h. People density analysis
 - i. Queue analysis
 - j. Heat analysis
 - Heat analysis for one camera
 - Heat analysis in one region
 - k. Pathway analysis
 - l. Person feature analysis
 - Feature analysis for one camera
 - Feature analysis in one region
 - m. Skin-surface temperature analysis
 - Temperature screening point
 - Person group
 - n. Temperature analysis
 - o. Vehicle analysis
4. Set the report name
5. Set the event report target
6. Set report type
7. Set report sending time
8. Select email template
9. Set the report language

C. Intelligent Analysis on Web Client, Control Client, and Mobile Client (HD)

10. Dashboard
 - a. Ability to add reports to customized Dashboard, including people counting report, queue analysis report, heat analysis report, pathway analysis report, person feature analysis report, temperature analysis report, vehicle analysis report
 - b. Ability to add/delete dashboard, edit dashboard name
 - c. Ability to save different reports as a Dashboard, export Dashboard data, display Dashboard on auxiliary screen
 - d. Ability to select resource or resource group for report
 - e. Ability to select Enter or Exit to display person entered or exited report on the Dashboard
11. People Counting
 - a. Ability to select network cameras enabled with people counting analytics or configured people counting groups to calculate people counting for each camera or in one region

- b. Ability to view the people counting statistics in a line chart or histogram, and switch between line chart and histogram
 - c. Ability to set report type (Daily, Weekly, Monthly, Annual, or customize the time interval for a report)
 - d. Ability to set time to regularly clear the people counting statistics of the group.
 - e. Ability to limit the people amount in the group.
 - f. Ability to select shorter time period to view more detailed data of each camera
 - g. Ability to export the detailed data of counting report in CSV/Excel format
 - h. Ability to search the video linkage by month, date, week, hour, and play corresponding video to check people counting
 - i. Ability to display up to 20 people counting cameras with different colors in people counting report of entry/exit
 - j. Ability to view entered/exited/both entered and exited statistics
 - k. Ability to show/hide data of certain cameras
 - l. Ability to view both entered and exited statistics of single cameras
 - m. Ability to play linked video of camera(s)
 - n. Ability to add report to dashboard
12. People Density Analysis
- a. Ability to select network cameras enabled with people density analytics to calculate people counting for each camera or in one region
 - b. Ability to view the people counting statistics in a line chart or histogram, and switch between line chart and histogram
 - c. Ability to set report type (Daily, Weekly, Monthly, Annual, or customize the time interval for a report)
 - d. Ability to select shorter time period to view more detailed data of each camera
 - e. Ability to export the detailed data of counting report in CSV/Excel format
 - f. Ability to search the video linkage by month, date, week, hour, and play corresponding video to check people counting
 - g. Ability to show/hide data of certain cameras
 - h. Ability to view both entered and exited statistics of single cameras
 - i. Ability to play linked video of camera(s)
 - j. Ability to add report to dashboard
13. Queue Analysis
- a. Ability to generate a report to show the number of queue exceptions and number of persons in each queue
 - b. Ability to display the queue status including waiting duration and queue length
 - c. Ability to generate the report as daily, weekly, monthly, or annual report
 - d. Ability to set the time period in the time field for statistics
 - e. Ability to set the waiting duration to display the number of persons in each queue who have waited for specified duration at different time points
 - f. Ability to set the queue length to display how many seconds each queue status lasts
 - g. Ability to show/hide certain data of certain element
 - h. Ability to view the report of the single queue, including the number of exceptions, number of people in queue, and waiting duration
 - i. Ability to switch between number of exceptions, number of people, and queue length
 - j. Ability to set the report type and report time
 - k. Ability to select shorter time period to view more detailed data of each queue

- l. Ability to select the queue exception, people amount exceeding, waiting timeout, person amount in queue, queue status to export
 - m. Ability to select the saving path
 - n. Ability to set the format as Excel or CSV
 - o. Ability to add report to dashboard
14. Heat Analysis
- a. Ability to select network cameras enabled with heat map analytics or configured heat analysis groups to calculate heat for each camera or in one region
 - b. Ability to set report type (Daily, Weekly, Monthly, Annual, or customize the time interval for a report)
 - c. Ability to calculate people dwell time, people amount, and average dwell time
 - d. Ability to export heat map report in PDF/Excel format
 - e. Ability to add report to dashboard
15. Pathway Analysis
- a. Ability to calculate the number of people walking by
 - b. Ability to set the time as daily, weekly, monthly, annually, or custom time interval
 - c. Ability to generate the report to view the line chart or heat map of the people amount
 - d. Ability to export heat map report in PDF/Excel format
 - e. Ability to add report to dashboard
16. Person Feature Analysis
- a. Ability to select network cameras enabled with feature analytics or configured person feature analysis groups to calculate the features of detected people for each camera or in one region
 - b. Ability to set report type (Daily, Weekly, Monthly, Annual, or customize the time interval for a report)
 - c. Ability to calculate the age and gender of the detected people
 - Gender: Male and female
 - Age: Infant, child, teenage, adolescent, youth, prime, middle-aged, middle and old age, elderly
 - d. Ability to export report in CSV/Excel format
 - e. Ability to add report to dashboard
17. Temperature Analysis
- a. Ability to display the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry points on different presets
 - b. Ability to select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report
 - c. Ability to show/hide certain data of preset or thermometry point
 - d. Ability to display temperature report of single preset
 - e. Ability to display temperature report of single thermometry point
 - f. Ability to display the number of exceptions that the temperature at this thermometry point is higher or lower than the pre-defined temperature
 - g. Ability to display the maximum/minimum temperature at this thermometry point during the set time period
 - h. Ability to select the camera and preset, and set the report type and report time
 - i. Ability to select shorter time period to view more detailed data
 - j. Ability to export the number of exceptions on temperature of each thermometry point
 - k. Ability to export the maximum temperature and minimum temperature of each thermometry point

- l. Ability to set the saving path of the report
- m. Ability to export the report in the format of Excel or CSV
- n. Ability to add report to dashboard
- 18. Vehicle Analysis
 - a. Ability to display the number of passing vehicles detected by the specified cameras during specified time period
 - b. Ability to select up to 20 ANPR camera for statistics at the same time
 - c. Ability to select the report type as daily, weekly, monthly, annual report or customize the time interval
 - d. Ability to select shorter time period to view more detailed data
 - e. Ability to customize the saving path of the report
 - f. Ability to export the report in the format of Excel or CSV
 - g. Ability to add report to dashboard
- 19. Skin-Surface Temperature Analysis
 - a. Ability to select temperature screening point or person group as the analysis type
 - b. Ability to select the report type as daily, weekly, monthly, annual report or customize the time interval
 - c. Ability to select shorter time period to view more detailed data
 - d. Ability to customize the saving path of the report
 - e. Ability to export the report in the format of Excel or CSV

3.16 Remote Site Management (RSM)

A. Manage Remote Sites on Web Client

1. You can add other HikCentral Professional without RSM module to the HikCentral Professional with RSM module as the Remote Site for central management
2. HikCentral Professional shall support 100,000 cameras via Remotes Sites
3. Add Remote Sites via IP/domain
4. Add Remote Sites registered to Central System (in batch)
5. Add Remote Sites in batch
6. After adding Remote Sites, channels shall display according to permission, and the Central System list will be the same as Remote Sites list
7. Support database backup of Remote Sites, up to 5 copies of database backup for each Remote Sites are supported, and saving paths cannot be edited
8. Import Remote Site alarms (support filtering by source, triggering event, and alarm priority)
9. Shall have the ability to display the online/offline status of Remote Sites in Central System
10. Support logging in to Remote Sites and configuring Remote Sites
11. Synchronize Remote Site names in the Central System manually
12. Refresh Remote Site channels manually, after channels of Remote Sites are added or deleted, users can update the changes from the Remote Site
13. Synchronize channel names manually
14. Edit Remote Site names, IPs, ports, user names, passwords, and description information
15. Import cameras in logical view after channel updates of Remote Sites
16. Remind users of deletion and display offline devices after deleting channels on Remote Sites
17. Import areas of added cameras on Remote Sites into the Central System

B. Backup Remote Site's Configured Data in Central System on Web Client

1. Set scheduled database backup
2. Set maximum number of backup

3. View the database saving path in Central System

C. View Resource Changes on Remote Site

1. Newly added cameras
2. Deleted cameras
3. Name changed cameras
4. Synchronize the resources in the Central System with the Remote Site
5. Remove the deleted cameras from the Central System in batch

3.17 Digital Signage

A. Resource Overview on Web Client

1. Material Statistics
2. Program Statistics
3. Schedule Statistics
4. Release Statistics
5. Recent Program

B. Material Management on Web Client

1. Ability to upload local materials with different types and different formats
 - a. Picture: BMP, JPG, PNG, GIF; the largest resolution for a picture material is 3840 × 2160
 - b. Video: ASF, AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4 , RM, RMVB
 - c. Audio: MP3, WAV, WMA
 - d. Document: TXT, PDF, EXCEL, WORD, PPT
 - e. Webpage: HTML, HTM
 - f. Android APP: APK
2. Ability to create and upload dynamic materials
 - a. Select material type
 - Webpage
 - URL picture
 - Stream Media Server
 - Network camera
 - b. Enter material name
 - c. Select area which the material belongs to
 - d. Set property
 - Public
 - Private
3. Ability to replace the uploaded materials
4. Ability to edit /delete/refresh materials
5. Ability to Switch display mode of materials
6. Ability to search for materials
7. Ability to set location for storing materials

C. Program Management on Web Client

1. Ability to create normal program
 - a. Enter program name
 - b. Select screen size
 - c. Set property
 - Public
 - Private
 - d. Select area which the program belongs to

- e. Enter description
 - f. Select template
 - g. Edit page properties
 - Page name
 - Background
 - Play time
 - h. Add materials for the program
 - i. Set window properties
 - Window position
 - Window type: Normal or Pop-up Window
 - Switching method: Jump to Next Window or Jump to Next Page
 - Move window layer
 - Play time
2. Ability to create attendance program
- a. Enter program name
 - b. Select screen size
 - c. Set property
 - Public
 - Private
 - d. Select area which the program belongs to
 - e. Enter description
 - f. Select template
 - g. Set basic parameters
 - Content and font size of title and sub title
 - Welcome words
 - Alarm temperature threshold
 - h. Set displaying parameters of check-in information
 - Added person information
 - Unknown person information
 - i. Set background picture
3. Ability to create people counting & temperature screening program
- a. Enter program name
 - b. Select screen size
 - c. Set property
 - Public
 - Private
 - d. Select area which the program belongs to
 - e. Enter description
 - f. Select template
 - g. Set general parameters for display
 - Title
 - Prompt for people counting
 - People counting icon
 - Title of people stayed
 - Number of people stayed
 - Title of Remaining Entries
 - Remaining number of people entries

- h. Set displaying parameters of alarm status
 - Prompt for abnormal temperature
 - Maximum people stayed
 - Enable voice alarm for no mask, abnormal temperature, and people full
 - Upload audio file for voice alarm
- i. Add advertisements when the Temperature Screening Template is selected
- j. Set background picture
- 4. Ability to edit/preview program
- 5. Ability to cut in the program
- 6. Ability to create schedule for program

B. Schedule Management on Web Client

1. Ability to create a Schedule
 - a. Set schedule parameters
 - Name
 - Property: Public or Private
 - Area which the schedule belongs to
 - Description
 - b. Select play mode
 - Play by Date
 - Play by Week
 - Custom Play
 - c. Select a program
 - d. Specify playing time on timeline
 - e. Adjust schedule
2. Ability to create a loop schedule
 - a. Set schedule parameters
 - Name
 - Property: Public or Private
 - Area which the schedule belongs to
 - Description
 - b. Select play mode as Loop
 - c. Select a program
 - d. Set play mode
 - Normal Mode
 - Period Mode
 - e. Add more playlists
3. Ability to create a default schedule
 - a. Set schedule parameters
 - Name
 - Property: Public or Private
 - Area which the schedule belongs to
 - Description
 - b. Select play mode as By Default
 - c. Select a program
4. Ability to edit/delete/refresh schedule
5. Ability to release schedule
6. Ability to search for schedules

B. Release Approval on Web Client

1. Ability to approve contents one by one
2. Ability to approve contents in a batch
3. Ability to support three types of check status: Passed, Denied, To be Checked

C. Release Management on Web Client

1. Ability to view release records
 - a. View details of release tasks: terminal name, release progress, and current release status
 - b. Release unreleased schedules
 - c. Delete release tasks
 - d. Release tasks that failed to be released again
2. Ability to release program schedules
 - a. Enter release task name
 - b. Select release mode as Release Later or Release Now
 - c. Select effective mode as Take Effect Later or Take Effect Now
 - d. Select device(s) to be released to
3. Ability to cut in text message
 - a. Select online device(s)
 - b. Enter task name
 - c. Enter text content and playing time
 - d. Set text message property
 - Configuration mode
 - Font size
 - Font color
 - Background picture
4. Ability to cut in program
 - a. Enter task name
 - b. Select cut-in mode as Play Duration or End Time
 - c. Select terminal(s)

B. Terminal Control on Web Client

1. Ability to display added devices by thumbnail or list
2. Ability to refresh device status
3. Ability to view device details
4. Ability to search for devices
5. Ability to start up, shut down, or reboot terminals
6. Ability to start or stop playing program
7. Ability to cut in message
8. Ability to stop playing cut-in message or program message
9. Ability to clear content on terminal
10. Ability to enable or disable timed startup or shutdown of terminal
11. Ability to enable timed volume on/off
12. Ability to manually control the validity of default schedule
13. Ability to generate screenshots
14. Ability to restore the parameters of terminals to default settings
15. Ability to adjust volume
16. Ability to enable remote debugging
17. Ability to export terminal logs in ZIP file

C. Data Migration on Web Client

1. Migrate data about terminals, materials, programs, and schedules from the platform with old version to the one with new version
2. View data migration records

3.18 IP Speaker

A. Media Library Management on Web Client

1. Supports managing the media library by group
2. Supports uploading the audio file in MP3 format
3. Supports displaying the format and the size of the audio file. Supports downloading the audio file

B. Storage Configuration for Broadcast on Web Client

1. Supports setting storage location (local PC or pStor) for the broadcasted audio and the uploaded media files
2. Supports enabling/disabling recording audios during the live broadcast
3. Supports searching for live broadcast records

C. Live Broadcast on Web Client, Control Client, and Mobile Client

1. Supports live speaking via group
2. Supports live speaking by area
3. Supports live speaking when viewing the live view of IP speaker's related cameras
4. Supports broadcasting the audio file by group
5. Supports broadcasting the audio file by area
6. Supports broadcasting the audio file when viewing the live view of IP speaker's related cameras

D. Scheduled Broadcast on Web Client

1. Supports adding multiple scheduled broadcast tasks
2. Supports broadcasting by group
3. Supports broadcasting by area.
4. Supports setting the period type for broadcast, including Every Day, One Time, and Every Week
5. Supports setting the priority for scheduled broadcast tasks
6. Supports selecting audio file(s) for the scheduled broadcast task, and setting the playing duration for each audio file
7. Supports setting the play mode: Once or Specific Duration

3.19 Security Inspection

A. Security Inspection Channel Management on Web Client

1. Supports adding/editing/deleting security inspection channels to the area
2. Supports linking devices to the security inspection channel. Up to 1 analyzers and 3 walk-through metal detectors can be linked.

B. Security Inspection Visualization on Web Client

1. Supports viewing real-time package information, including the package picture, total number of packages, total number of packages with prohibited articles, and total number of prohibited articles
2. Supports marking detected articles in package pictures
3. Supports configuring prohibited articles for real-time alarm
4. Supports viewing real-time picture of the package's owner

5. Supports live view and playback of the analyzer's inspection videos
6. Supports marking detected articles in video stream. Supports video magnification, capturing, recording, and switch between main stream and sub stream.
7. Supports viewing the package's pictures and the package owner's picture
8. Supports viewing real-time detected information
9. Supports viewing real-time temperature information of the detected person (if the walk-through metal detector supports temperature measurement function)

C. Statistics and Reports of Security Inspection on Web Client

1. Supports generating package detection reports by day, week, month, and year
2. Supports viewing the total number of detected packages and total number of packages with prohibited articles of specific security inspection channels within a specific period
3. Supports viewing percentage of packages with prohibited articles of specific security inspection channels within a specific period
4. Supports viewing prohibited article types within a specific period
5. Supports generating people inspection reports by day, week, month, and year
6. Supports viewing the total number of detected persons and total number of persons with metals of specific security inspection channels within a specific period
7. Supports viewing percentage of metal detection alarms of specific security inspection channels within a specific period

D. Search Historical Data of Security Inspection on Web Client

1. Supports searching for package detection records by time, prohibited article type, and channel. The result includes package detection time, location, article type, and number of prohibited articles.
2. Supports viewing package details, including package's pictures, capture picture of the package owner, and videos recorded before/after the package is detected
3. Supports searching for metal detection records by time and channel. The result includes detection time, location, and signal strength of the metal.
4. Supports viewing metal details, including metal location, signal strength, and videos recorded before/after the metal is detected
5. Supports searching for absence records by time and channel. The result includes absence time, location, and absence duration.
6. Supports viewing absence details, including the videos recorded before the personnel leaves and after the personnel comes back

END OF SECTION

Part 4 Execution

4.1 Examination

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

4.2 Preparation

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

4.3 Installation

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

4.4 Field Quality Control

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

4.5 Adjusting

- A.** Execute the necessary modifications to the Video Management System for proper operation in accordance with the instructions provided by the manufacturer.
- B.** Ensure the customers unique requirements are reflected in the camera settings.

4.6 Demonstration

- A.** Upon final inspection, validate the video solutions system and its device functions correctly.

END OF SECTION

Part 5 Appendix

5.1 Server Logs

The server logs file refer to the logs files stored in the SYS server on the Current Site and the Remote Site

5.1.1 Error Logs

The Error Log shall be searchable by the following subcategories:

Adding Access Control Device Failed
Acknowledging Alarm Failed
Activating License Failed
Adding Application Data Server Error
Adding Entry & Exit Counting Rule Failed
Adding Leave Application in a Batch
Adding Major Leave Type
Adding Minor Leave Type
Adding Visitor
Adding Visitors in a Batch
Adding Access Point Failed
Adding Anti-Passback Rule Failed
Adding Dashboard Failed
Adding Decoding Device Failed
Adding DeepinMind Server Failed
Adding Element to Access Level Failed
Adding Elevator Control Device Failed
Adding Encoding Device Failed
Adding Facial Recognition Server Error
Adding Location for GIS Resource Group Failed
Adding Location for Resource Group Failed
Adding Multi-door Interlocking Rule Error
Adding Person Group Failed
Adding Radar Element Failed
Adding Recording Server Failed
Adding Resource Group for Alarm Failed
Adding Resource Group for Heat Analysis Failed
Adding Resource Group for Pathway Analysis Failed
Adding Resource Group for People Counting Failed
Adding Resource Group for Person Features Failed
Adding Security Audit Server Failed
Adding Smart Wall Failed
Adding Streaming Server Failed
Adding Tag Failed
Adding txt Template for Attendance Report Failed
Adding UVSS Failed
Adding View for Smart Wall Failed

Adding View Group for Smart Wall Failed
Adding View Schedule Failed
Adjusting Order of Smart Wall Views
Adjusting Screen Brightness Failed
Adjusting Screen Contrast Failed
Adjusting Screen Resolution Failed
Adjusting Screen Saturation Failed
Alarm Output Operation Failed
Answering Call Failed
Applying Leave for One Person Failed
Arming /disarming in Live View Failed
Arming Failed
Assigning Floor to Access Level Failed
Backing Up Access Events Failed
Batch Displaying Live View on Smart Wall Failed
Calculating Attendance Manually Failed
Capture in Live View Failed
Capture in Playback Failed
Changing Auto-Switching Interval on Smart Wall Failed
Checking Details in Live View Failed
Checking Details in Playback Failed
Closing Screen Failed
Correct Attendance Records in a Batch
Creating Roaming Window Failed
Data Backup Plan Failed
Database Backup Right Now Failed
Database Restore Failed
Deactivating License Failed
Delete Attendance Handling Records in a Batch
Delete Major Leave Type
Delete Minor Leave Type
Delete Visitor
Delete Visitors in a Batch
Deleting Dashboard Failed
Deleting Decoding Device Failed
Deleting DeepinMind Server Failed
Deleting Elevator Control Device Failed
Deleting Linkage Configuration for Access Control Device Failed
Deleting Location for GIS Resource Group Failed
Deleting Location for Resource Group Failed
Deleting Person Group in a Batch Failed
Deleting Radar Element Failed
Deleting Resource Group for Alarm Failed
Deleting Resource Group for Heat Analysis Failed
Deleting Resource Group for Pathway Analysis Failed
Deleting Resource Group for People Counting Failed

Deleting Resource Group for People Features Failed
Deleting Roaming Window Failed
Deleting Security Audit Server Failed
Deleting Smart Wall Failed
Deleting txt Template for Attendance Report Failed
Deleting View for Smart Wall Failed
Deleting View Group for Smart Wall Failed
Deleting View Schedule Failed
Digital Zoom in Live View Failed
Digital Zoom in Playback Failed
Disabling VCA Display Failed
Disarming Failed
Disarming Radar Failed
Displaying Alarm on Smart Wall Failed
Displaying Auto-Switch in One Window Failed
Displaying Auto-Switch in Tile Mode Failed
Displaying Real-Time Person Number Failed
Displaying Window on Top Layer Failed
Download QR Code
Edit Configuration of Third-Party Database
Edit General Rule
Edit Major Leave Type
Edit Minor Leave Type
Edit Overtime
Edit Relation between Person Group and Other Groups.
Edit Security Settings Failed
Edit Visitor
Editing Attendance Point Failed
Editing Attendance Report Display Failed
Editing Camera's Virtual Tracking Failed
Editing Configuration of DeepinMind Server Failed
Editing Dashboard Failed
Editing Decoding Device Failed
Editing DeepinMind Server Failed
Editing Element in Access Level Failed
Editing Elevator Control Device Failed
Editing Location for GIS Resource Group Failed
Editing Location for Resource Group Failed
Editing Logo of Attendance Report Failed
Editing OpenAPI configuration Failed
Editing Person Group Failed
Editing Persons in Access Group by Group Failed
Editing Radar Element Failed
Editing Resource Group for Alarm Failed
Editing Resource Group for Heat Analysis Failed
Editing Resource Group for Pathway Analysis Failed

Editing Resource Group for People Counting Failed
Editing Resource Group for People Features Failed
Editing Secret Key for File Transmission Failed
Editing Security Audit Server Failed
Editing Security Audit Server's Linked Device Failed
Editing Smart Wall Failed
Editing txt Template for Attendance Report Failed
Editing View for Smart Wall Failed
Editing View Group for Smart Wall Failed
Editing View Schedule Failed
Enabling VCA Display Failed
Enlarging Roaming Window Failed
Enlarging Sub-Window Failed
Exit: Locking Door Failed
Exit: Remaining Door Locked Failed
Exit: Remaining Door Unlocked Failed
Exit: Unlocking Door Failed
Exporting Heat Analysis Report of Resource Group Failed
Exporting Matrix Data of Heat Analysis Failed
Exporting People Counting Report of Resource Group Failed
Exporting Person Feature Report Failed
Exporting Person Feature Report of Resource Group Failed
Exporting Queue Report of Camera Failed
Fast Forward Playback on smart wall Failed
Fisheye Expansion in Live View Failed
Fisheye Expansion in Playback Failed
Floor Control: Access Forbidden Failed
Floor Control: Access With Credential Failed
Floor Control: Free Access Failed
Floor Control: Temporary Access Failed
Getting Devices' Card Swiping Records Failed
Getting Heat Analysis Report of Resource Group Failed
Getting People Counting Report of Resource Group Failed
Getting Person Feature Report Failed
Getting Person Feature Report of Resource Group Failed
Getting Recording Schedule on Camera Error
Going to VCA Search in Live View Failed
Going to VCA Search in Playback Failed
Importing Face Comparison Groups from Device Failed
Instant Playback Failed
Linkage Configuration for Access Control Device Failed
Linking Decoding Output with Smart Wall Failed
Live View on Smart Wall via Network Keyboard Failed
Locking All Doors Failed
Locking Door Failed
Locking Failed

Locking Video File Failed
Login via Network Keyboard Failed
Logout via Network Keyboard Failed
Managing Persons in Face Comparison Group by Group Failed
Marking Alarm Failed
Moving Roaming Window Failed
Obtaining Live View Parameters via Network Keyboard Failed
Opening Screen Failed
Pausing Camera Auto-Switch on Smart Wall Failed
Pausing Playback on Smart Wall Failed
Performing Window Division via Network Keyboard Failed
Processing Call Failed
PTZ Control Failed
PTZ Control in Live View Failed
Recovering All Doors Failed
Recovering All Failed
Refreshing Decoding Device Failed
Refreshing Security Audit Server Failed
Remaining All Locked Failed
Remaining All Unlocked Failed
Remaining Door Locked Failed
Remaining Door Unlocked Failed
Removing Element from Access Level Failed
Removing Floor from Access Level Failed
Restoring Roaming Window Failed
Restoring Sub-Window Failed
Resuming Camera Auto-Switch on Smart Wall Failed
Resuming Camera Auto-Switch on Smart Wall Failed
Resuming Play on Smart Wall Failed
Searching History Access Events Failed
Searching Video Failed
Setting Attendance Parameters for Access Control Device Failed
Setting Decoding Output Resolution Failed
Setting Floor's Access Forbidden Schedule Failed
Setting Floor's Free Access Schedule Failed
Setting Time for Calculating Attendance Data Automatically Failed
Slow Forward Playback on Smart Wall Failed
Sorting Views for Smart Wall Failed
Start Clipping in Playback Failed
Start Preview Record Failed
Starting Auto-Switch of Smart Wall Views Failed
Starting Camera Auto-Switch on Smart Wall Failed
Starting Elevator Live View Failed
Starting Elevator Playback Failed
Starting Live View Failed
Starting Live View of Door Failed

Starting Live View of Signal Source on Smart Wall Failed
Starting Live View on Smart Wall Failed
Starting Wipers Failed
Stopping All Live Videos on Smart Wall Failed
Stopping Auto-Switch of Smart Wall Views Failed
Stopping Elevator Live View Failed
Stopping Elevator Playback Failed
Stopping Live View of Door Failed
Stopping Live View of Single Source on Smart Wall Failed
Stopping Live View on Smart Wall Failed
Stopping Playback of Door Failed
Stopping Playback on Smart Wall Failed
Stopping Wipers Failed
Switching Live View on Smart Wall via Network Keyboard Failed
Switching Stream for Smart Wall Failed
Switching Stream in Live View Failed
Switching Stream in Live View Failed
Switching View for Smart Wall Failed
Switching View via Network Keyboard Failed
Synchronizing Floor Name from Device to System Failed
Synchronizing Floor Name from System to Device Failed
Transcoding Playback Failed
Two-way Audio in Live View Failed
Unlinking Decoding Output with Smart Wall Failed
Unlocking Door Failed
Unlocking Failed
User Login Failed
Viewing Live View of Next Camera on Smart Wall Failed
Viewing Live View of Previous Camera on Smart Wall Failed
Visitor Check out Manually
Window Division Failed
Deleting Encoding Device Failed
Editing Encoding Device Failed
Activating Device Failed
Changing Device Password Failed
Deleting UVSS Failed
Editing UVSS Failed
Editing Access Control Device Failed
Deleting Access Control Device Failed
Rebooting Access Control Device Failed
Activating Access Control Device Failed
Rebooting Elevator Control Device Failed
Activating Elevator Control Device Failed
Adding Security Control Panel Failed
Editing Security Control Panel Failed
Deleting Security Control Panel Failed

Adding Dock Station Failed
Editing Dock Station Failed
Deleting Dock Station Failed
Adding Elevator Control Device Failed
Editing Elevator Control Device Failed
Deleting Elevator Control Device Failed
Adding Video Intercom Device Failed
Editing Video Intercom Device Failed
Deleting Video Intercom Device Failed
Deleting LED Screen Failed
Rebooting Video Intercom Device Failed
Activating Video Intercom Device Failed
Editing Network Transmission Device Failed
Deleting Network Transmission Device Failed
Rebooting Network Transmission Device Failed
Editing Card Reader Access Mode Failed
Adding Remaining Open after First Person Rule Failed
Editing Remaining Open after First Person Rule Failed
Deleting Remaining Open after First Person Rule Failed
Adding Free Access and Access Forbidden Rule Failed
Editing Free Access and Access Forbidden Rule Failed
Deleting Free Access and Access Forbidden Rule Failed
Adding Multi-factor Authentication Group Failed
Editing Multi-factor Authentication Group Failed
Deleting Multi-factor Authentication Group Failed
Adding Multi-factor Authentication Group Failed
Editing Multi-factor Authentication Group Failed
Deleting Multi-factor Authentication Group Failed
Exporting Evidence Management Failed

5.1.2 Warning Logs

The Warning Log shall be searchable by the following subcategories

License Expired

5.1.3 Information Logs

The Information Log shall be searchable by the following subcategories

Access Forbidden
Access Forbidden Schedule
Access With Credential
Acknowledge Alarm
Activate Access Control Device
Activate Device

Activate Elevator Control Device
Activate License
Activate Online Device
Activate Recording Server
Activating Elevator Control Device Failed
Add Attendance Check Point
Add Camera Element
Add Access control Device
Add Access Group(Basic Information)
Add Access Level (Basic Information)
Add Access Level in Access Group
Add Access Schedule Template
Add Alarm Category
Add Alarm Input Element
Add Alarm Output Element
Add Alarm Priority
Add Alarm Settings
Add Anti-Passback Rule
Add Application Data Server
Add Area
Add Arming Schedule Template
Add Card to Person
Add Dashboard
Add Decoding Device
Add DeepinMind Server
Add Defense Schedule Template
Add Device Upgrade Schedule
Add Dock Station
Add Dock Station Group
Add Door
Add Door to Access Level
Add Door to Anti-Passback Rule
Add Element to Access Level
Add Elevator Control Device
Add Elevator Resource
Add Elevator's Related Camera
Add Email Template
Add Encoding Device
Add Entry & Exit Counting Rule
Add Event Settings
Add Evidence
Add Face Comparison Group
Add Facial Recognition Server
Add Fingerprint to Person
Add Fuzzy Matching Rule
Add Generic Event

Add Holiday
Add Hot Region
Add Hot Region on GIS Map
Add Hot Spare for NVR
Add Hot Spot
Add Hot Spot on GIS Map
Add Icon
Add Label on GIS Map
Add Leave Application in a Batch
Add Linked Holiday for Shift Schedule
Add Location for GIS Resource Group
Add Location for Resource Group
Add Major Leave Type
Add Map
Add Map Label
Add Member to Dock Station
Add Minor Leave Type
Add Multi-Door Interlocking Rule
Add N+1 Hot Spare
Add Partition
Add Pathway
Add Permission Schedule
Add Person
Add Person Additional Information
Add Person Group
Add Person Profile
Add Person to Access Group
Add Person to Face Comparison Group
Add Radar Element
Add Recording Schedule
Add Recording Server
Add Recording Template
Add Related Camera to Access point
Add Remote Site
Add Report
Add Resource Group for Alarm
Add Resource Group for Heat Analysis
Add Resource Group for Pathway Analysis
Add Resource Group for People Counting
Add Resource Group for Person Features
Add Role
Add Security Audit Server
Add Security Control Device
Add Shift Schedule
Add Site to GIS Map
Add Smart Wall

Add Streaming Server
Add txt Template for Attendance Report
Add User
Add User-Defined Event
Add UVSS
Add Vehicle
Add Vehicle List
Add Video Copy-back Schedule for Dock Station
Add Video Tag
Add View
Add View Group
Add View Schedule
Add Visitor
Add Visitors in a Batch
Adding Elevator Resource Failed
Adding Elevator's Related Camera Failed
Adjust Screen Brightness
Adjust Screen Contrast
Adjust Screen Definition
Adjust Screen Saturation
Adjust View Sequence
Alarm Arming
Alarm Disarming
Alarm Input Bypass Recovered
Alarm Input Bypassed
Apply Access Control Applications
Apply Face Comparison Group to Device and Link Camera
Apply Hot Spare Settings to NVR
Apply Leave for One Person
Arming/Disarming in Live View
Assign Access Level to Access Group
Assign Door to Access Level
Assign Floor to Access Level
Auto-Switch of Live View on Smart Wall: Next Camera
Auto-Switch of Live View on Smart Wall: Previous Camera
Back Up Captured Pictures
Back Up Database in Schedule
Back Up Database Now
Back Up Recorded Video Files
Back Up Vehicle Records
Batch Correct Attendance Record
Batch Delete Persons
Batch Display Live View on Smart Wall
Batch Edit Time Zone for Access Control Devices
Batch Edit Time Zone for Elevator Control Devices
Batch Edit Time Zone for Encoding Devices

Batch Edit Time Zone for Security Control Panels
Batch Editing Time Zone for Access Control Devices Failed
Batch Editing Time Zone for Elevator Control Devices Failed
Batch Editing Time Zone for Encoding Devices Failed
Batch Editing Time Zone for Security Control Panels Failed
Batch Enable Face Credential
Batch Import Domain Group Persons
Batch Import Domain Persons
Batch Import Person Information
Batch Issue Cards to Persons
Broadcast
Call Answered
Call Processed
Cancel Face Comparison Group Linkage with Camera
Cancel Linkage between Access Level and Access Group
Cancel Linkage between Domain Group and Access Group
Cancel Linkage between Domain Group and Face Comparison Group
Capture Picture in Live View
Capture Picture in Playback
Card Issuing Settings
Change Device Password
Change User Password
Checking Frequency
Clear Alarm Info
Collect Face by Device
Configure Multiple Authentication
Correct Attendance Records in a Batch
Correct Check-in/out
Create Roaming Window
Customize Additional Information
Database Recovery
Deactivate User
Delete Access Control Device
Delete Access Group
Delete Access Level
Delete Access Schedule Template
Delete Alarm Category
Delete Alarm Input Element
Delete Alarm Output Element
Delete Alarm Priority
Delete Alarm Settings
Delete All Shift Schedules
Delete Anti-Passback Rule
Delete Application Data Server
Delete Area
Delete Arming Schedule Template

Delete Attendance Check Point
Delete Attendance Handling Records in a Batch
Delete Camera Element
Delete Customized Additional Information
Delete Dashboard
Delete Decoding Device
Delete DeepinMind Server
Delete Defense Schedule Template
Delete Device Upgrade Schedule
Delete Dock Station
Delete Dock Station Group
Delete Door
Delete Elevator Control Device
Delete Elevator Resource
Delete Email Template
Delete Encoding Device
Delete Entry & Exit Counting Rule
Delete Event Settings
Delete Evidence
Delete Face Comparison Group
Delete Facial Recognition Server
Delete Files from FTP
Delete Fuzzy Matching Rule
Delete Generic Event
Delete Holiday
Delete Hot Region
Delete Hot Spare for NVR
Delete Hot Spot
Delete Icon
Delete Linkage Configuration for Access Control Device
Delete Linked Holiday for Shift Schedule
Delete Location for GIS Resource Group
Delete Location for Resource Group
Delete Major Leave Type
Delete Map
Delete Map Label
Delete Member from Dock Station Group
Delete Minor Leave Type
Delete Multi-Door Interlocking Rule
Delete N+1 Hot Spare
Delete Partition
Delete Pathway
Delete Permission Schedule Template
Delete Person
Delete Person Additional Information
Delete Person Group in a Batch

Delete Person's Card
Delete Person's Fingerprint
Delete Radar Element
Delete Recording Schedule
Delete Recording Server
Delete Recording Template
Delete Remote Site
Delete Report
Delete Resource Group for Alarm
Delete Resource Group for Heat Analysis
Delete Resource Group for Pathway Analysis
Delete Resource Group for People Counting
Delete Resource Group for People Features
Delete Roaming Window
Delete Role
Delete Security Audit Server
Delete Security Control Device
Delete Shift Schedule
Delete Smart Wall
Delete Streaming Server
Delete txt Template for Attendance Report
Delete User
Delete User-Defined Event
Delete UVSS
Delete Vehicle
Delete Vehicle List
Delete Video Copy-Back Schedule for Dock Station
Delete Video Tag
Delete View
Delete View Group
Delete View Schedule
Delete Visitor
Delete Visitors in a Batch
Deleting Elevator Resource Failed
Digital View in Live View
Digital View in Playback
Disable Face Credentials
Disable VCA Display
Disarm All Partition of Security Control Panel
Disarm Partition
Disarm Radar
Display Alarm on Smart Wall
Display Auto-Switch in One Window
Display Auto-Switch in Tile Mode
Display on Top Layer
Display Real-Time Person Number

Door Control: Close Door
Door Control: Open Door
Door Control: Remain Locked
Door Control: Remain Unlocked
Download Alarm Details
Download Alarm Details
Download Events
Download Files from FTP
Download QR Code
Edit Access Control Device
Edit Access Control Device working mode
Edit Access Group (Basic Information)
Edit Access Level (Basic Information)
Edit Access Level in Access Group
Edit Access Schedule Template
Edit Alarm Category
Edit Alarm Input Element
Edit Alarm Output Element
Edit Alarm Priority
Edit Alarm Settings
Edit Anti-Passback Rule
Edit Application Data Server
Edit Area
Edit Arming Schedule Template
Edit Attendance Point
Edit Attendance Report Display
Edit Auto-Switch of Live View on Smart Wall
Edit Backup Information
Edit Basic Information of Dock Station Group
Edit Camera Capabilities
Edit Camera Element
Edit Camera's Virtual Tracking
Edit Configuration of DeepinMind Server
Edit Configuration of Third-Party Database
Edit Contact Information
Edit Customized Additional Information
Edit Customized Additional Information
Edit Dashboard
Edit Decoding Device
Edit DeepinMind Server
Edit Defense Schedule Template
Edit Device Access Mode
Edit Dock Station
Edit Door
Edit Door in Access Level
Edit Door Related Camera

Edit Element in Access Level
Edit Elevator Control Device
Edit Elevator Resource
Edit Elevator's Related Camera
Edit Email Settings
Edit Email Template
Edit Entry & Exit Counting Rule
Edit Event Settings
Edit Evidence
Edit Face Comparison Group (Basic Information)
Edit Facial Recognition Server
Edit Files on FTP
Edit First Day of Week
Edit Fuzzy Matching Rule
Edit General Rule
Edit Generic Event
Edit Holiday
Edit Hot Region
Edit Hot Region on GIS Map
Edit Hot Spare for NVR
Edit Hot Spare Settings
Edit Hot Spot
Edit Hot Spot on GIS Map
Edit Label on GIS Map
Edit Linked Holiday for Shift Schedule
Edit Location for GIS Resource Group
Edit Location for Resource Group
Edit Logo of Attendance Report
Edit Major Leave Type
Edit Map
Edit Map Label
Edit Minor Leave Type
Edit Multi-Door Interlocking Rule
Edit N+1 Hot Spare
Edit Network Performance
Edit NTP Settings
Edit Online Devices Network Parameters
Edit OpenAPI Settings
Edit Operation Recommendation
Edit Overtime
Edit Partition
Edit Pathway
Edit Permission Schedule
Edit Person
Edit Person Additional Information
Edit Person Card

Edit Person Fingerprint
Edit Person Group
Edit Person in Access Group
Edit Person Profile
Edit Person's Login Password of Dock Station
Edit Person's Login Password of Dock Station failed.
Edit Persons in Access Group by Group
Edit Picture Storage
Edit Radar Element
Edit Recognized Plate Number
Edit Recording Schedule
Edit Recording Server
Edit Recording Template
Edit Registering to Central System Settings
Edit Relation between Person Group and Other Groups.
Edit Remote Site
Edit Report
Edit Resource Group for Alarm
Edit Resource Group for Heat Analysis
Edit Resource Group for Pathway Analysis
Edit Resource Group for People Counting
Edit Resource Group for People Features
Edit Retention Time of Data Recorded in System
Edit Role
Edit Secret Key for File Transmission
Edit Security Audit Server
Edit Security Audit Server's Linked Device
Edit Security Control Device
Edit Security Settings
Edit Server NIC Settings
Edit Service Status
Edit SFTP Settings
Edit Shift Schedule
Edit Site on GIS Map
Edit Smart Wall
Edit Streaming Server
Edit System Properties
Edit Temperature Unit
Edit Transfer Protocol to HTTPS
Edit txt Template for Attendance Report
Edit URL of GIS Map API
Edit User
Edit UVSS
Edit Vehicle List
Edit Vehicle's Marking Status
Edit Video Copy-Back Schedule for Dock Station

Edit Video Tag
Edit View
Edit View Group
Edit View Schedule
Edit Visitor
Edit WAN Access Settings
Editing Elevator Resource Failed
Editing Elevator's Related Camera Failed
Email Test
Enable VCA Display
Enable Video Function Management Service
Enable/Disable Alarm
Enable/Disable Receiving Generic Event
Enlarge Roaming Window
Enlarge Sub Window
Enter VCA Search from Live View
Enter VCA Search from Playback
Exit: Close Barrier
Exit: Open Barrier
Exit: Remain Barrier Closed
Exit: Remain Barrier Open
Export Access Records
Export Attendance Records
Export Event/Alarm Logs
Export Heat Analysis Report of Resource Group
Export Heat Map
Export Heat Values of Heat Map
Export Logs
Export Matrix Data of Heat Analysis
Export Pathway Analysis Report
Export People Counting Report
Export People Counting Report of Resource Group
Export Person Feature Report
Export Person Feature Report of Resource Group
Export Person Information
Export Queue Report of Camera
Export Temperature Report
Export Vehicle Information
Export Vehicle Reports
Fast Forward Playback on Smart Wall
Fisheye Expansion in Live View
Fisheye Expansion in Playback
Force Logout
Forgive Anti-Passback
Free Access
Get Camera Name

Get Camera's Recording Schedule
Get Card Swiping Records from Device
Get Heat Analysis Report of Resource Group
Get Heat Values of Heat Map
Get Hot Spare Settings from NVR
Get License Exception
Get Matrix Data of Heat Map
Get Pathway Analysis Report
Get People Counting Report
Get People Counting Report of Resource Group
Get Person Feature Report
Get Person Feature Report of Resource Group
Get Persons from Device
Get Queue Report from Camera
Get Temperature Report
Get Vehicle Report
Import Face Comparison Groups from Device
Import Vehicle Information
Input Person Additional Information
Instant Playback
Link Decoding Output
Link Dock Station Group with Dock Station
Link Domain Group with Access Group
Link Domain Group with Face Comparison Group
Link Person's Additional Information with Person Information in Domain
Linkage Configuration for Access Control Device
Lock
Lock All Doors
Lock Video in Playback
Log Search
Manage Persons in Face Comparison Group by Group
Manual Update Resource
Manually Apply Access Levels
Manually Calculate Attendance
Manually Close Alarm Window
Manually Display Alarm's Related Camera's Video on Smart Wall
Manually Display Alarm's Related View on Smart Wall
Manually Stop Maintenance
Manually Synchronize Person in Domain or Domain Group
Mark Alarm
Mifare Encryption
Modify AD Configure
Modify Vehicle
Move Roaming Window
Move View
Network Keyboard Login

Network Keyboard Logout
Network Keyboard: Display Live View on Smart Wall
Network Keyboard: Get Live View Parameters
Network Keyboard: Switch Live View on Smart Wall
Network Keyboard: Switch View
Network Keyboard: Window Division
One-Touch Configuration
Partition: Away Arming
Partition: Delayed Arming
Partition: Instant Arming
Pause Playback on Smart Wall
Pause Area Auto-Switch
Pause Auto-Switch in Custom View
Pause Auto-Switch of Live View on Smart Wall
Pause Single-Screen Auto-Switch
Play in the Specific Window on Control Client
Play in the Specific Window on Smart Wall
PTZ Control
PTZ in Live View
PTZ: Batch Disable Wipers
PTZ: Batch Enable Wipers
Push Subscription
Reboot Access Control Device
Reboot Elevator Control Device
Rebooting Elevator Control Device Failed
Record Fingerprint from Device
Recover All
Recover All Doors
Recover Arming
Refresh Decoding Device
Refresh Security Audit Server
Remain All Locked
Remain All Unlocked
Remove Door from Access Level
Remove Door from Anti-Passback
Remove Element from Access Level
Remove Floor from Access Level
Remove Hot Region from GIS Map
Remove Hot Spot from GIS Map
Remove Label from GIS Map
Remove Multi-Doors from One Multi-Door Interlocking Rule
Remove One Door from Multiple Multi-Door Interlocking Rules
Remove Person from Access Group
Remove Person from Face Comparison Group
Remove Related Camera for Door
Remove Site from GIS Map

Reset Area Auto-Switch
Reset Network Information
Reset Online Device Password
Reset User Password
Restore All Settings
Restore All Settings of Elevator Control Device
Restore Default of Elevator Control Device
Restore Default Settings
Restore Roaming Window
Restore Sub Window
Restore User
Restore User Password
Restoring All Settings of Elevator Control Device Failed
Restoring Default of Elevator Control Device Failed
Resume Area Auto-switch
Resume Auto-switch in Custom View
Resume Auto-switch of Live View on Smart Wall
Resume Playback on Smart Wall
Resume Single-Screen Auto-Switch
Search Access Records
Search Alarm Log
Search Event Log
Search Evidence
Search Files on FTP
Search Heat Map
Search Vehicle Passing Records
Search Vehicle Records
Search Video Tag
Send Report Rule
Send to Spare Server
Set Access Control Device Parameters
Set Access Forbidden Schedule
Set Attendance Parameters for Access Control Device
Set Card Reader Access Mode
Set Card Reader Parameters
Set Custom Wiegand
Set Decoding Output Resolution
Set Door Parameters
Set Elevator Parameters
Set Floor's Free Access Schedule
Set Free Access Schedule
Set Mifare Card Encryption for Elevator Control Device
Set Network Parameters
Set Opening Door with First Card Parameters
Set Parameters for Elevator Control Device
Set Person's Access Group

Set Person's Login Password of Dock Station
Set Person's Login Password of Dock Station failed.
Set Time for Auto-Apply Access Levels
Set Time for Auto-Calculating Attendance
Set Time Parameters
Set Time Parameters for Elevator Control Device
Setting Elevator Parameters Failed
Setting Mifare Card Encryption for Elevator Control Device Failed
Setting Parameters for Elevator Control Device Failed
Setting Time Parameters for Elevator Control Device Failed
Slow Forward Playback on Smart Wall
Start Area Auto-switch
Start Auto-switch in Custom View
Start Auto-switch of Live View on Smart Wall
Start Downloading Video Files
Start Elevator Live View
Start Elevator Playback
Start Live View
Start Live View of Door Related Camera
Start Live View of Local Signal Source on Smart Wall
Start Live View of Radar
Start Live View on Smart Wall
Start Playback
Start Playback of Radar
Start Playback on Smart Wall
Start Recording in Live View
Start Remote Playback Recording
Start Single-Screen Auto-Switch
Start Two-Way Audio
Start View Auto-switch
Stop All Live View on Smart Wall
Stop Area Auto-switch
Stop Auto-switch in Custom View
Stop Auto-switch of Live View on Smart Wall
Stop Downloading Video File
Stop Elevator Live View
Stop Elevator Playback
Stop Live View
Stop Live View of Door Related Camera
Stop Live View of Local Signal Source on Smart Wall
Stop Live View of Radar
Stop Playback
Stop Playback of Door Related Camera
Stop Playback of Radar
Stop Playback on Smart Wall
Stop Recording in Live View

Stop Recording in Playback
Stop Single-Screen Auto-Switch
Stop Two-Way Audio
Stop View Auto-Switch
Subscribe Access Control Event
Switch Application Data Server
Switch Stream in Live View
Switch View
Sync Device's Recording Settings to Device
Sync Floor Name from Device to System
Sync Floor Name from System to Device
Synchronize Camera Name
Synchronize Domain Users
Synchronize Door Name
Synchronize Partition
SYS Stopped
System Settings on Control Client
Temporary Access
Test Alarm Configuration
Test Event Rule
Transcoding Playback
Trigger User-Defined Event
Turn off Alarm Output
Turn off Screen
Turn on Alarm Output
Turn on Screen
Two-Way Audio in Live View
Deactivate License
Unlink Decoding Output
Unlink Dock Station Group with Dock Station
Unlink Person's Additional Information with Person Information in Domain
Unlock
Unlock Video during Playback
Upgrade Device
Upload File to FTP
User Login
User Logout
Video Search
View Captured Picture
View Details in Live View
View Details in Playback
Visitor Check out Manually
Window Division
Call Answered
Call Processed
Unlock Video During Playback

Unmark Alarm
Upload Local Material
Upload Dynamic Material
Delete Material
Download Local Material
Cover Local Material
Approve Material
Upload Program
Download Program
Delete Program
Edit Program
Approve Program
Upload Schedule
Download Schedule
Delete Schedule
Edit Schedule
Release Schedule
Set Terminal Timed Startup/Shutdown Schedule
Set Terminal Timed Volume Schedule
Terminal Screen Shot
Upgrade Terminal
Set Terminal Timed Input Switch Schedule
Set Terminal Debugging Parameters
Set Terminal Volume
Set Terminal LOGO
Enable Default Schedule
Set Camera Parameters
Set Terminal SADP Switch (Security)
Set Weather Web Manufacturer
Edit Material
Set Terminal Backlight Parameters
Cut-In Message
Upload Program Thumbnail
Batch Delete Release Schedule
Release Again
Clear Terminal Playing Information
Set Terminal HDMI Output
Batch Remote Debugging of Terminal
Get Template
Get Release Details
Upload Template Thumbnail
Add Template
Delete Template
Edit Template
Add Release Schedule
Edit Release Schedule

Cancel Releasing Schedule
Get Schedule
Create Cut-In
Cancel Cut-In
Approve Schedule
Apply Data from Third-Party Component to Information Release Terminal
Get Statistics Information
Add Terminal
Delete Terminal
Edit Terminal Parameters
Set Terminal IP Address
Set Terminal
Terminal Control
Add Email Template for Regularly Sending Report
Edit Email Template for Regularly Sending Report
Delete Email Template for Regularly Sending Report
Search Log
Backup Log
Backing Up Log Failed
Add Email Template for Event and Alarm Linkage
Edit Email Template for Event and Alarm Linkage
Delete Email Template for Event and Alarm Linkage
Add UVSS
Edit UVSS
Delete UVSS
Add Information Release Terminal
Edit Information Release Terminal
Delete Information Release Terminal
Assign Shift Schedule to Person Group
Assign Shift Schedule to Person
Cancel Assigning Shift Schedule to Person
Add Temporary Shift Schedule
Edit Temporary Shift Schedule
Delete Temporary Shift Schedule
Add Intelligent Recognition Task
Edit Intelligent Recognition Task
Delete Intelligent Recognition Task
Add Intelligent Recognition Task Schedule
Edit Intelligent Recognition Task Schedule
Delete Intelligent Recognition Task Schedule
Edit Profile in Person Group
Download Profile Template
Batch Import Profile to Person Group
Batch Export Profile from Person Group
Apply Profile to Device Again
Apply Face Comparison Group to Device Again

Edit Card Reader Access Mode
Add Remaining Open after First Person Rule
Edit Remaining Open after First Person Rule
Delete Remaining Open after First Person Rule
Add Free Access and Access Forbidden Rule
Edit Free Access and Access Forbidden Rule
Delete Free Access and Access Forbidden Rule
Add Multi-Factor Authentication Group
Edit Multi-Factor Authentication Group
Delete Multi-Factor Authentication Group
Add Multi-Factor Authentication Group
Edit Multi-Factor Authentication Group
Delete Multi-Factor Authentication Group
Add Person to Receive Remote Door Open Request (Multi-Factor Authentication)
Delete Person to Receive Remote Door Open Request (Multi-Factor Authentication)
Add Person to Receive Remote Door Open Request (Multi-Factor Authentication)
Delete Person to Receive Remote Door Open Request (Multi-Factor Authentication)
Edit Subscription Record
Add Person with Access Level
Edit Person with Access Level
Delete Person with Access Level
Relate Access Level to Person Group
Cancel Relation Between Access Level and Person Group
Add Visitor Access Level
Edit Visitor Access Level
Delete Access Level
Add Visitor Types
Edit Visitor Types
Delete Visitor Types
Batch Delete Visitor Types
Edit Visitor Card
Export Real-Time Resource Status
Export Real-Time Overview of Resource Health Status
Export Device Logs
Export History Resource Status
Export History Status Overview
Delete Invalid Elements
Edit Event and Alarm Types for Statistics
Export Entry & Exit Records
Export Other Device Records
Set Free Access and Access Forbidden Rule
Setting Free Access and Access Forbidden Rule Failed
Edit Visitor Fingerprint
Edit Visitor Photo
Export Evidence Management

5.2 Device Logs

Log information on Encoding Device and Security Control Device are searchable by major type and corresponding minor types:

5.2.1 Encoding Device Logs -Alarm

The Alarm Log shall be searchable by the following subcategories

Alarm Input	Alarm Output	Answering Question Detection Started	Answering Question Detection Stopped
Audio Exception Detection	Audio Loss Detection	Audio Loss Detection Started	Audio Loss Detection Stopped
Defocus Detection Started	Defocus Detection Stopped	Digital Channel Alarm Input Started	Digital Channel Alarm Input Stopped
Emergency Alarm Started	Emergency Alarm Stopped	Face Detection Alarm Started	Face Detection Alarm Stopped
Face Detection Started	Face Detection Stopped	Fast Moving Detection Started	Fast Moving Detection Stopped
Fire and Smoke Detection Ended	Fire and Smoke Detection Started	Intrusion Detection Started	Intrusion Detection Stopped
ITS Alarm Started	ITS Alarm Stopped	Lecture Detection Alarm Started	Lecture Detection Alarm Stopped
License Plate Recognition Started	License Plate Recognition Stopped	Line Crossing Detection Started	Line Crossing Detection Stopped
Loitering Detection Alarm Started	Loitering Detection Alarm Stopped	Motion Detection Alarm Started	Motion Detection Alarm Stopped
Network Camera External Alarm	Object Removal Detection Alarm Started	Object Removal Detection Alarm Stopped	Parking Detection Alarm Started
Parking Detection Alarm Stopped	People Gathering Alarm Started	People Gathering Alarm Stopped	PIR Alarm started
PIR Alarm stopped	POS Started	POS Stopped	Region Entrance Detection Started
Region Entrance Detection Stopped	Region Exiting Detection Alarm Started	Region Exiting Detection Alarm Stopped	Scene Change Detection Alarm Started
Scene Change Detection Alarm Stopped	Scene Detection Alarm	Ship Detection	Sudden Change of Sound Intensity Started
Sudden Change of Sound Intensity Stopped	Sudden Decrease of Sound Intensity Detection	Temperature Difference Alarm Started	Temperature Difference Alarm Stopped
Temperature Measurement Alarm Started	Temperature Measurement Alarm Ended	Temperature Measurement Pre-Alarm Started	Temperature Measurement Pre-Alarm Ended
Unattended Baggage Detection Alarm Started	Unattended Baggage Detection Alarm Stopped	Vandal-proof Detection Started	Vandal-proof Detection Ended

VCA Alarm Started	VCA Alarm Stopped	Video Tampering Alarm Started	Video Tampering Alarm Stopped
VQD Alarm Started	VQD Alarm Stopped	Wireless Alarm Started	Wireless Alarm Ended
Other			

5.2.2 Encoding Device Logs - Exception

The Exception Log shall be searchable by the following subcategories

Accessory Board Exception	ANR Recording Failed	Backup Device Exception	Buffer Overflow
Camera/Recording Resolution Mismatch	Capture Error	Cloud Storage Data Uploading Exception	Dial Exception
DSP Exception	Ezviz Offline Exception	Face Detection Stopped	Fan Exception
HDD Error	HDD Exception	HDD Full	Illegal Login
IP Address Conflicted	IPC Module Reboot Abnormally	Memory Card Damaged	Memory Card Defective
MODEM Offline	Network Camera Disconnected	Network Disconnected	Overheating Protection
POE Power Exception	Rear Panel Temperature Exception	Recording Error	Scene Exception
Starting MAS of Network Camera Failed	Sub-system IP Address Conflict	Sub-system Network Disconnected	Synchronizing Network Camera Password Exception
Temperature Exception	Video Input Error	Video Signal Loss	Video Standard Mismatch
Other			

5.2.3 Encoding Device Logs -Operation

The Operation Log shall be searchable by the following subcategories

Add Plan	Add Scene	Add Signal Source	Adjust Volume
Bring Smart Wall Window to Back	Bring Smart Wall Window to Front	Cancel Master Screen of Smart Wall	Cancel Sub Screen of Smart Wall
Control Decoding Channel Ratio	Control Digital Zoom	Control Online by Dialing	Control Online/Offline by Short Message
Control Passive Decoding	Control Plan	Control Remote Playback	Cut Background Picture
Cut Video Source	Delete Plan	Delete Scene	Delete Signal Source
Display Logo	Display Operation	Download Background Picture	Edit Input
Edit Output	Edit Signal Source	Edit Virtual LED	Get All Valid Windows
Get Auto-Switch Plan	Get Current Used Scene	Get Decoder Auto-Switch Settings	Get Decoding Board Parameters
Get Decoding Channel Information	Get Decoding Channel Status	Get Decoding Channel Switch	Get Device Information
Get Display Channel Settings	Get Input Signal List	Get Plan List	Get Scene

Get Scene List	Get Signal Window Information	Get Status of Remote Playback	Get User Configuration
Get Smart Wall Connection	Get Smart Wall Scene	Get Virtual LED	Hide Logo
Illegal Shutdown	Local: Activate Device	Local: Add Network Camera	Local: Add Network HDD
Local: Add Working Device	Local: Auto-Restore	Local: Backup End Time	Local: Backup Record File(s)
Local: Configuration	Local: Configure PIN	Local: Configure SIP Server	Local: Create Array
Local: Create Logical Disk	Local: Delete Array	Local: Delete HDD	Local: Delete Logical Disk
Local: Delete Network Camera	Local: Delete Network HDD	Local: Delete Working Device	Local: Device Type Configuration
Local: Disable Wireless Dial-up	Local: Expand Logical Disk	Local: Expand Blocklist & Allowlist	Local: Export Configuration File
Local: Export Heat Map File	Local: Export Heat Map Flow	Local: Export IPC Configuration File	Local: Export Picture Files
Local: Format HDD	Local: HDD Detect	Local: Hot Spare Device Configuration	Local: Hot Standby
Local: Import Blocklist & Allowlist	Local: Import Configuration File	Local: Import IPC Configuration File	Local: Live View
Local: Lock Video Files	Local: Logout	Local: Manual Clear or Trigger Alarm	Local: Manual Rebuild Array
Local: Move Array	Local: N+1 Configuration	Local: One-touch Configuration	Local: Operate Tag
Local: Output Switch	Local: Playback By File	Local: Playback By Time	Local: PTZ Control
Local: Reboot	Local: Reset Admin's Password	Local: Restore Logical Disk	Local: Restore to Factory Settings
Local: Resume Default Admin Password	Local: Search Message	Local: Send Message	Local: Set Dial-up Parameters
Local: Set Dial-up Plan	Local: Set Network HDD	Local: Set RAID Speed	Local: Set Allowlist
Local: Setting Network Camera	Local: Start Backup	Local: Start Burning	Local: Start Capture
Local: Start Recording	Local: Stop Backup	Local: Stop Capture	Local: Stop Recording
Local: Switch Output	Local: Time Settings	Local: Unlock Video Files	Local: Upgrade
Local: Upgrade IPC	Local: Upgrade RAID	Local: View Message	MVC: Login Code Splitter
MVC: Logout Code Splitter	Platform Operation	Power On	Reboot Intelligent Library
Receive Message	Reconnect Passive Decoder	Remote: Activate Device	Remote: Add NAS Disk
Remote: Add Storage Pool	Remote: Add Working Device	Remote: Alarm Output Triggering	Remote: Arm
Remote: Auto Restore	Remote: Close Transparent Channel	Remote: Configure Parameters	Remote: Configure PIN

Remote: Configure SIP Server	Remote: Create Array	Remote: Create Logical Disk	Remote: Delete Array
Remote: Delete Logical Disk	Remote: Delete NAS Disk	Remote: Delete Pictures	Remote: Delete Storage Pool
Remote: Delete Video File	Remote: Delete Working Device	Remote: Device Type Configuration	Remote: Disable Cloud System
Remote: Disarm	Remote: Edit Storage Pool Capacity	Remote: Edit Storage Pool Parameters	Remote: Enable Cloud System
Remote: Enable Manual Dial-up	Remote: Establish Transparent Channel	Remote: Expand Logical Disk	Remote: Export Blocklist & Allowlist
Remote: Export Configuration File	Remote: Export IPC configuration	Remote: Export Picture Files	Remote: Export Video Files
Remote: Format HDD	Remote: Get Parameters	Remote: Get Status	Remote: Hot Spare Device Configuration
Remote: Hot Standby	Remote: Import Blocklist & Allowlist	Remote: Import Configuration File	Remote: Import IPC Configuration File
Remote: IPC Addition	Remote: IPC Deletion	Remote: IPC Setting	Remote: Lock File
Remote: Login	Remote: Logout	Remote: Manual Rebuild Array	Remote: Move Array
Remote: N+1 Configuration	Remote: One-Touch Configuration	Remote: Operate Tag	Remote: Playback by File
Remote: Playback by Time	Remote: PTZ Control	Remote: Reboot	Remote: Reset admin's Password
Remote: Restore Default Parameters	Remote: Restore Logical Disk	Remote: Restore to Factory Settings	Remote: Search Message
Remote: Send Message	Remote: Set Dial-up Parameters	Remote: Set Dial-up Plan	Remote: Set NAS Speed
Remote: Set RAID Speed	Remote: Set Allowlist	Remote: Shutdown	Remote: Start Capture
Remote: Start Recording	Remote: Start Two-way Audio	Remote: Stop Capture	Remote: Stop Recording
Remote: Stop Two-way Audio	Remote: Unlock File	Remote: Upgrade	Remote: Upgrade IPC
Remote: Upgrade RAID	Remote: View Message	Restore Initial Status	Scene Control
Screen Control	Send Alarm Message	Send Auto-Switch Plan	Set Background Picture
Set Decoder Auto-Switch Settings	Set Decoding Board Parameters	Set Decoding Channel Switch	Set Decoding Delay Level
Set Display Channel	Set External Matrix	Set Master Screen of Smart Wall	Set OSD
Set Output Resolution	Set Remote Playback	Set Single Scene	Set Sub Screen of Smart Wall
Set Transparency	Set Two-way Audio Record	Set User Configuration	Set User Password
Set Smart Wall Connection	Set Smart Wall Scene	Shutdown	Start Auto-Switch Decoding
Start Dynamic	Start Passive Decoding	Start PPPoE Connection	Stop Auto-Switch

Decoding			Decoding
Stop Dynamic Decoding	Stop Passive Decoding	Stop PPPoE Connection	Stream Compression Configuration
Switch Scene	Upload Background Picture	Upload Logo	VCA Configuration
Smart Wall Display Area Setup	Window Control	Other	

5.2.4 Encoding Device Logs - Information

The Information Log shall be searchable by the following subcategories

Accessory Board Information	Add ANR Duration	ANR Record Started	ANR Record Stopped
Backing Up Work Device Started	Backing Up Work Device Ended	Backing Up Device Information	Buffer Status Log
Call Log	Connect to Network Camera	Delete ANR Duration	Delete Expired Picture
Delete Expired Video Files	Dial-up Status	Ezviz Running Status	Global Error Information
HDD Error Detailed Information	HDD Information	Login Server	Login Server Again
Logout Server	Network Camera Disconnected	Network HDD Information	Platform Information
POE power Exception	RAID Information	Recording Synchronization Completed	Recording Synchronization Exception
Recording Synchronization Started	Recording Synchronization Stopped	S.M.A.R.T Information	Server Status Information
Start Capture	Start Recording	Stop Capture	Stop Recording
Unlocking Log	Zone Alarm	Other	

5.2.5 Access Control Device Logs - Alarm

Capture Linkage Alarm
Card Reader Tamper Restored
Card Reader Tampered
Device Tamper Restored
Device Tampered
Duress Alarm
Event Input Alarm
Event Input Restored
Fire Input Open Circuit Alarm
Fire Input Restored
Fire Input Short Circuit Alarm
Lane Controller Fire Input Alarm

Lane Controller Fire Input Restored
Lane Controller Tamper Restored
Lane Controller Tampered
Low Face Quality
Low Fingerprint Quality
Max. Card Authentication Times
No Memory Alarm
No Memory for Offline Event Storage
POS Disabled
POS Enabled
SD Card Full Alarm
Secure Door Control Unit Tamper Restored
Secure Door Control Unit Tampered
Smart Door Lock Duress Alarm
Zone Alarm Restored
Zone Exception Alarm
Zone Open Circuit Alarm
Zone Short Circuit Alarm
Other

5.2.6 Access Control Device Logs-Exception

Active Infrared Intrusion Detector Exception
Active Infrared Intrusion Detector Recovered
AC Power Disconnected
Alternating Current Restored
Battery Voltage Recovered (for Facial Recognition Device)
Battery Voltage Recovered
Camera Connected
Camera Disconnected
Card Reader Offline
Card Reader Online
CAN Bus Exception
CAN Bus Restored
Communication with Anti-Passback Server Disconnected
Communication with Anti-Passback Server Restored
Communication with IR Adaptor Exception
Communication with IR Adaptor Restored
Communication with Light Board Exception
Communication with Light Board Restored
COM Port Connected
COM Port Disconnected
Device Does Not Authorized
Device Offline
Device Online
Distributed Access Controller Network Disconnected
Distributed Access Controller Network Restored

Distributed Access Controller Offline
Distributed Access Controller Online
Fingerprint Module Connected
Fingerprint Module Disconnected
Flash Writing/Reading Exception
High Pedestal Temperature
ID Card Reader Connected
ID Card Reader Disconnected
Indicator Restored
Indicator Off
Lane Controller Offline
Lane Controller Online
Local Login: Lock
Local Login: Unlock
Low Battery Voltage (for Facial Recognition Device)
Low Battery Voltage
Master Controller RS-485 Loop Circuit Node Connection Recovered
Master Controller RS-485 Loop Circuit Node Disconnected
Motor Sensor Exception
Network Disconnected
Network Recovered
Power Off
Power On
Recording Error
Reset Watchdog
RS-485 Connection Exception
RS-485 Connection Restored
Secure Door Control Unit Offline
Secure Door Control Unit Online
Other

5.2.7 Decoding Device Logs - Exception

Enabling DSP Failed
Smart Rule Not Supported
Other

5.2.8 Decoding Device Logs - Operation

Add Division
Add Plan
Add Signal Source
Backplane Temperature Exception
Control Division
Control Plan
Delete Division
Delete Plan

Delete Signal Source
Digital Zoom
Download Background Picture
Edit Division
Edit Input Source
Edit Logo
Edit Output Channel
Edit Plan
Edit Signal Source
Edit Virtual LED
Fan Exception
Get All Valid Windows
Get Currently Used Scene
Get Decoding Board Parameters
Get Device Information
Get Display Unit Connection Settings
Get Division List
Get List of Input Signal Sources
Get List of Plans
Get Matrix Settings
Get One Window Information
Get User Settings
Get Smart Wall Scene
Get Virtual LED
Get Window Division
Hide Logo
IP Address Conflicted
Live View Operation
Network Disconnected
Recover to Initial Status
Screen Control
Set Background Picture
Set Decoding Board Parameters
Set Decoding Output Latency Level
Set Display Area on Display Unit
Set Display Unit Connection
Set Division of Background Picture
Set Layer Transparency
Set Matrix
Set OSD
Set Resolution of Display Output
Set User
Set User Password
Set Smart Wall Scene
Set Window Division
Set Window Division of Video Source

Show Logo
Sub-board Disconnected with Network
Sub-board Exception Started
Sub-board IP Address Conflicted
Sub-board Plugged In
Sub-board Unplugged
Switch Scene
Temperature Exception
Upload Background Picture
Window Control
Other

5.2.9 Security Control Device Logs - Alarm

The Alarm Log shall be searchable by the following subcategories

Alarm Reset	Alarm Restored	Business Consulting	Business Consulting Over
Detector Restored	Detector Tampered	Device Restored	Device Tampered
Dust Detector Alarm	Dust Detector Alarm Restored	Electricity Meter Alarm	Electricity Meter Alarm Restored
Environment Acquisition Device Alarm	Environment Acquisition Device Alarm Restored	Gas Detection Alarm	Gas Detection Alarm Restored
Incorrect Password Attempts	Invalid Card ID	Keypad Restored	Keypad Tampered
Motion Detection Alarm Started	Motion Detection Alarm Stopped	Open-Circuit Alarm	Panic Alarm
Panic Alarm Restored	Panic Button Pressed Down	Panic Button Restored	Power Supply On/Off Alarm
Power Supply On/Off Alarm Restored	Sensor Higher than Threshold 1	Sensor Higher than Threshold 2	Sensor Higher than Threshold 3
Sensor Higher than Threshold 4	Sensor Lower than Threshold 1	Sensor Lower than Threshold 2	Sensor Lower than Threshold 3
Sensor Lower than Threshold 4	Short-Circuit Alarm	Temperature-Humidity Sensor Alarm	Temperature-Humidity Sensor Alarm Restored
Transformer Temperature Alarm	Transformer Temperature Alarm Restored	UPS Alarm	UPS Alarm Restored
Video Tampering Alarm Started	Video Tampering Alarm Stopped	Virtual Zone Burglary Alarm	Virtual Zone Fire Alarm
Virtual Zone Panic Alarm	Water Level Sensor Alarm	Water Level Sensor Alarm Restored	Zone Module Restored
Zone Module Tampered	Other		

5.2.10 Security Control Device Logs - Exception

The Exception Log shall be searchable by the following subcategories

3G Communication Exception	3G Communication Restored	AC Power Down	AC Power On
Analog Sensor Fault	Analog Sensor Recovery	Battery Voltage Recovery	Detector Battery Low
Detector Battery OK	Detector Online	GPRS Communication Exception	GPRS Communication Restored
GPRS Module Error	HDD Error	HDD Full	Illegal Access
IP Address Conflicted	KBUS Module Connected	KBUS Module Disconnected	Low Battery Voltage
MCU Rebooted	MODEM Offline	Network Camera Disconnected	Network Camera IP Address Conflicted
Network Connected	Network Disconnected	Network Flow Exceeded	Normal RF Signal
Normal Wired Network	Power Down	Power On	Printer Error
Printer Recovered	Recording Error	Remote: Formatting HDD Failed	RF Signal Exception
RS-485 Channel Connected	RS-485 Channel Disconnected	RTC Real-time Clock Exception	SIM Card Exception
SIM Card Restored	Sub-board Communication Error	Telephone Connected	Telephone Disconnected
Telephone Module Error	Trigger Module Connected	Trigger Module Disconnected	USB Communication Error
USB Communication Recovered	Video Input Exception	Video Signal Loss	Video Standard Mismatch
WDT Reset	Well Connected Wi-Fi	Wi-Fi Communication Fault	Wired Network Exception
XBUS Module Connected	XBUS Module Disconnected	Zone Module Connected	Zone Module Disconnected
Other			

5.2.11 Security Control Device Logs – Operation

The Operation Log shall be searchable by the following subcategories

Add Administrator	Add Back-End Operator	Add Detector to Zone	Add Front-End Operator
Add Keyfob User	Add Keyfob/Card Reader User	Audio Off	Audio On
Auto Arming	Auto Disarming	Bypass	Bypass Recovered
Capture Settings	Card Arming/Disarming	Card Settings	Change Administrator's Password
Change Back-End Operator's Password	Change Front-End Operator's Password	Check Detector Battery	Check Detector Signal
Clear Alarms	Close Door	Control Trigger	DDNS Settings
Delete Administrator	Delete Back-End Operator	Delete Detector from Zone	Delete Front-End Operator
Delete Keyfob User	Delete Keyfob/Card Reader User	Detector Arming	Detector Disarming

Disable Function Key	Disable Siren	Duress	Edit 3G Parameters
Edit Access Control Parameters	Edit Dialing Settings	Edit Event Trigger Action Settings	Edit GPRS Parameters
Edit Network Uploading Parameters	Edit Partition System Parameters	Edit Print Parameters	Edit RS-485 Settings
Edit Security Control Panel Settings	Edit Sensor Settings	Edit System Fault Settings	Edit Trigger Settings
Edit Uploading Mode Settings	Edit Zone Settings	Enable Function Key	Enable Siren
Expanded Network Center Settings	Format SD Card	Group Bypass	Group Bypass Recovered
HiDDNS Settings	Instant Arming	Key Arming/Disarming Zone Arming	Key Arming/Disarming Zone Disarming
Local: Activate Device	Local: Lock	Local: Reboot	Local: Restore to Factory Settings
Local: Unlock	Local: Upgrade	Mobile Phone Alarm Clearing	Mobile Phone Arming
Mobile Phone Disarming	Mobile Phone Instant Arming	Mobile Phone Stay Arming	Network Card Settings
Network Module Settings	Normal Arming	Normal Disarming	One-Touch Away Arming
One-Touch Stay Arming	Open Door	Re-register External Module	Remote Arming
Remote Disarming	Remote Keypad Upgrade	Remote: Activate Device	Remote: Export Configuration File
Remote: Export Video Files	Remote: Format HDD	Remote: Import Configuration File	Remote: Lock
Remote: Lock File	Remote: Playback by File	Remote: Playback by Time	Remote: PTZ Control
Remote: Reboot	Remote: Restore to Factory Settings	Remote: Start Recording	Remote: Stop Recording
Remote: Turn Off Alarm Lamp	Remote: Turn On Alarm Lamp	Remote: Unlock	Remote: Unlock File
Remote: Upgrade	Remote: Upgrade Keypad	Remote: Upgrade Network Module	Remote: Upgrade Zone Module
Remote: User Login	Remote: User Logout	Restore Default Settings	RS-485 Bus Re-registration
RS-485 Bus Settings	Scheduled Arming/Disarming Parameters	Scheduled Enable/Disable Trigger Settings	Search External Module
Single Zone Arming	Single Zone Arming/Disarming	Single Zone Disarming	Start Broadcast
Start Passthrough	Start Two-Way Audio	Start Arming	Stop Broadcast
Stop Passthrough	Stop Two-Way Audio	Swipe Patrol Card	Temporary Password Operation
Trigger Off	Trigger On	Turn Off Keypad Alarm	Upgrade Sub-board

		Sound	
Allowlist Settings	Wi-Fi Settings	Zone Tamper-proof Settings	Other

5.2.12 Security Control Device Logs – Event

The Event Log shall be searchable by the following subcategories

Activating Trigger Failed	Auto Arming	Auto Arming Failed	Auto Disarming
Auto Disarming Failed	B Code Time Synchronization	Deactivating Trigger Failed	Disable Trigger by Schedule
Enable Trigger by Schedule	Forced Arming	Insert USB	Keypad Locked
Pull Out USB	Scheduled Synchronization	SDK Time Synchronization	Sub-board Plug In
Sub-board Pull Out	Other		