



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 Surveillance

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. It is consisted of System Management Service (SYS) providing unified authentication service for connecting with the clients and servers, and Application Data Service (ADS) providing data storage processing.

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 Surveillance |
| 8. Section 28 21 00 | Surveillance Cameras |
| 9. Section 28 21 13 | IP Cameras |
| 10. Section 28 27 00 | Video Surveillance Sensors |
| 11. Section 28 33 00 | Video Surveillance – Security Monitoring and Control |
| 12. Section 28 51 19.15 | Video 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
55. ADS	Application Data 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. Description

A. HikCentral Professional System Management Service:

1. SYS maximum capacity for devices management and event handling:
 - a. Manages up to 1,024 resources, including encoding devices, access control devices, and Remote Sites
 - b. Imports up to 3,000 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 surveillance and management module.
 - c. Application Data Service
 - i. Provide data storage and processing.
 - d. 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
 - e. 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

Web Client

A. On initial set up and during first login, the Administrator is forced to create a complex password for future logins sessions.

- 1. The new password shall reach Medium password strength

B. Shall remotely connect to the SYS server via TCP/IP and perform the following functions:

- 1. Manage encoding devices
 - a. Add encoding devices to the system via the following discovery options:

- IP/Domain
- Hik-Connect
 - Add devices added to Hik-Connect service to the system
 - Hik-Connect Device List
- IP Segment
- Port Segment
- Batch Import
- Verify stream encryption key
- Add online devices in the same local subnet with the Local Network/Server Network using Search Active Device Protocol (SADP)
 - Hikvision Private Protocol
 - Hikvision EHome Protocol
- b. Add camera to area
- c. Apply time zone settings to the device
- d. Select Streaming Server for the area
- e. Select video storage location for the camera
- f. Get device's local recording settings
- g. View the following detailed information of the added devices:
 - Alias
 - Address
 - Serial number
 - Available cameras
 - Alarm I/O
 - Network status
 - Password strength
- h. Refresh the status of the added devices
- i. Set remote configuration of the added devices
- j. Change password of the added devices (in batch)
- k. Edit bandwidth for video downloading
- l. Activate the online devices (in batch)
- m. Set N+1 hot spare for device
- 2. Manage access control devices
 - a. Add access control device to the system via the following discovery options:
 - Add online device(s) (in batch) via SADP function
 - Hikvision Private Protocol
 - Hikvision EHome Protocol
 - IP Address
 - IP Segment
 - Port Segment
 - Batch Import
 - b. Add access points to area
 - c. Apply time zone settings to the device
 - d. Synchronize access points name
 - e. Set configuration of the added devices
 - Time settings for the device
 - Turnstile parameters
 - Reboot the device

- Restore default
 - Switch to the local page of the device for more remote configuration parameters
- f. Refresh the status of the added devices
 - g. Reset device password (in batch)
 - h. Activate the online devices
 - i. Apply Application 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
3. Manage security control devices
 - a. Add devices to the system via the following discovery options:
 - Add online device(s) (in batch) via SADP function
 - IP Address
 - Hik-Connect
 - Add devices added to Hik-Connect service to the system and the devices will automatically register to the EZVIZ account
 - Hik-Connect Device List
 - IP Segment
 - Port Segment
 - Batch Import
 - b. Add alarm inputs to area
 - c. Apply time zone settings to the device
 - d. Set remote configuration of the added security control devices
 - e. Refresh the status of the added devices
 - f. Reset device password (in batch)
 - g. Activate the online devices
 4. Manage dock station devices
 - a. Add devices to the system via the following discovery options:
 - IP Address/domain
 - IP Segment
 - Port Segment
 - Batch Import
 - b. Apply time zone settings to the device
 - c. Add to dock station group
 5. Upgrade device firmware via Web Client or EZVIZ Cloud Service
 - a. Simultaneous upgrade
 - b. Set upgrade schedule
 6. Restore/reset device password
 7. Manage application data service
 - a. Add Application Data Server by IP address
 - b. Add an Application Data Standby Server
 - c. Encrypt the data transmitted between the Application Data Server and other services or clients
 - d. Set Threshold of Failure Status
 - e. Automatically/manually Switch to Application Data Standby Server if the Application Data Server fails
 - f. Perform maintenance of server fault
 8. Manage Recording Server

- a. Add up to 64 Recording Servers, 64 Streaming Servers, pStor respectively to the SYS
- b. Add pStor, Network Video Recorder(only for picture storage), Cloud Storage Server and Hybrid SAN as Recording Server
- c. Import service component certificate to pStor, and Cloud Storage Server
- d. View storage information for the Recording Server, including used space and free space
- e. Enable picture storage function of pStor, Hybrid Storage Area Network and Cloud Storage Server
- f. Custom video copy-back to copy back recorded videos from Hybrid SAN's managed device automatically and set start time and end time
- g. Set video expiration duration for Hybrid SAN
- h. View channel information configured to store video files in Recording Server:
 - Camera name
 - Area
 - IP address
 - Storage type
 - Recording schedule
 - Recording status
 - Network status
- i. 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
9. Add Streaming Server via IP address, and import service component certificate to Streaming Server
10. Manage Facial Recognition Server
 - a. Enable WAN access
 - b. Add cameras to facial recognition server
11. When adding NVRs and network cameras, devices shall have the option to automatically create logical areas by device name or add to an existing area
12. When adding NVRs and network cameras, shall have the option to automatically
 - a. Synchronize logical camera name assigned at device level
 - b. Automatically add device's recording schedule
 - i. Shall be able to set and modify NVR recording schedules
 - c. When adding an NVR, user can check the online and offline status of NVR channels
13. Once added, show the online/offline status of devices in both physical view and logical view
14. Remotely configure NVRs and network cameras and set all functions that are available
15. Online device detection function is available on the Web Client accessed via Internet Explorer, Google Chrome and Firefox, and the active online access control devices in the same local subnet with the Web Client/ SYS Server will be displayed on a list
16. Enable WAN access for the Recording Server
17. Display channels in the same area in alphabetical order
18. Synchronize NVR channel names with the names displayed on the Web Client
19. Support the following functions of smart wall:
 - a. Shall add up to 32 smart walls and display multiple smart walls
 - b. Shall add up to 32 decoding devices and video wall controllers
 - c. Shall delete, edit, and view the added walls
 - d. Shall add online decoding devices via SADP in the same local subnet with the Web Client /SYS Server or add decoding devices or video wall controllers via IP address, and batch add decoding devices via IP segment, and port segment modes

- e. Shall activate and refresh decoding devices
- f. Shall edit the device's network location as LAN IP address, or WAN IP address
- g. Shall support the linkage between decoding device's or video wall controller's decoding outputs and smart wall windows
- h. Shall set the decoding output of the decoder as the signal input of video wall controller
- i. Shall set role permission of smart walls, decoding devices, and windows
- j. Shall support alarm linkage of smart walls, select walls and windows for alarm linkage, divide windows according to the number of alarms, and select wall related to graphic card or decoding card
- k. Shall support smart wall database backup and restoration via hot spare

C. Remote Site Management (RSM): Manages multiple SYSs, shall have the ability to:

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 up to 2,048 resources by distributed deployment, including encoding devices, access control devices, and Remote Sites
3. HikCentral Professional shall support 100,000 cameras via Remotes Sites
4. Add Remote Sites via IP/domain
5. Add Remote Sites registered to Central System (in batch)
6. Add Remote Sites in batch
7. After adding Remote Sites, channels shall display according to permission, and the Central System list will be the same as Remote Sites list
8. 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
9. Import Remote Site alarms (support filtering by source, triggering event, and alarm priority)
10. Display Remote Sites in alphabetical order
11. Support logging in to Remote Sites and configuring Remote Sites
12. Synchronize Remote Site names in the Central System manually
13. Refresh Remote Site channels manually, after channels of Remote Sites are added or deleted, users can update the changes from the Remote Site
14. Synchronize channel names manually
15. Edit Remote Site names, IPs, ports, user names, passwords, and description information
16. Display site address, site port, alias, user name, system IDs, GPS location, and version information
17. Configure GIS location of Remote Sites
18. View the Remote Site's GIS location, hot spot, and hot region settings in Map module
19. Backup Remote Site's configured data in Central System
 - a. Set scheduled database backup
 - b. Set maximum number of backup
 - c. View the database saving path in Central System
20. View the resource changes on the Remote Site
 - a. Newly added cameras
 - b. Deleted cameras
 - c. Name changed cameras
 - d. Synchronize the resources in the Central System with the Remote Site
 - e. Remove the deleted cameras from the Central System in batch
21. RSM function shall be supported by the Central System activated by the license that takes this function

D. Logical View: Area management, shall have the ability to:

1. Create up to 3,000 areas with 5 levels per SYS, and up to 100,000 areas for remote site management
2. Add up to 256 cameras, access points, alarm inputs, alarm outputs, and UVSS respectively to one area and 10,000 by distributed deployment in total per SYS
3. Configure the camera remotely
4. Check detailed information of cameras, including
 - a. Name
 - b. Address
 - c. Encoding device alias
 - d. Network status (for video channels only)
 - e. Recording schedule status (for video channels only)
 - f. Area Name
 - g. Manufacturer
 - h. Added to map or not
5. Check detailed information of access points, including
 - a. Name
 - b. Address
 - c. Access control device address
 - d. Network Status
 - e. Access point status
 - f. Access level
 - g. Area
 - h. Added to map or not
6. Check detailed information of alarm inputs/outputs, including
 - a. Name
 - b. Address
 - c. Device/Site
 - d. Partition (only for alarm input)
 - e. Area
 - f. Added to map or not
7. Check detailed information of UVSS, including
 - a. Name
 - b. Address
 - c. Network Status
 - d. Area
 - e. Added to map or not
8. Synchronize camera name, moving the camera to other area, and displaying elements of sub-areas, remote configuration on device, copying the current camera's specified configuration parameters to other cameras for batch configuration
9. Synchronize access point name, moving the access point to other area, and displaying elements of sub-areas, copying the current access point's specified parameters to other access points
10. Synchronize/apply access point name
11. Add alarm inputs/outputs, the functions of moving the inputs/outputs to other area, and display elements of sub-areas
12. Move the UVSS to other area, and display elements of sub-areas

13. Add Entry &Exit Counting rules, Multi-Door Interlocking rules, Anti-passback rules, and Security Control Partitions
14. Display the number of Entry &Exit Counting rules, Multi-Door Interlocking rules, Anti-Passback rules, and Security Control Partitions
15. Switch and select the added sites, display channels of Remote Sites in logical view, and switch to logical view of the selected site when the RSM module is enabled
16. Import cameras in logical view after channel updates of Remote Sites
17. Remind users of deletion and displaying offline devices after deleting channels on Remote Sites
18. Import areas of added cameras on Remote Sites into the Central System
19. Copy configuration information of stream type, protocol type, main storage, and auxiliary storage to other channels
20. Select security control device's zones as alarm inputs to add into the area
21. Set defense schedule for the arming mode in different time periods for the partitions of the added security control devices
22. Edit the following basic information, recording settings, event settings, and map settings of the cameras:
 - a. Shall have the ability to edit the following basic information of cameras for current and Remote Site:
 - Camera name
 - Protocol type
 - Check the live view and instant playback of the camera in the same screen
 - Configure recording for the camera
 - Configure the camera remotely
 - b. Shall have the ability to configure camera recording settings for current and Remote Site:
 - Set main storage and auxiliary storage for cameras
 - Synchronize recording settings to device
 - Get recording settings from device
 - Select storage location as Encoding Device, Hybrid Storage Area Network, pStor, Cloud Storage Server for cameras of current site
 - Select storage location as pStor, Hybrid Storage Area Network or Cloud Storage Server of central system for cameras of Remote Site
 - Set recording schedule template
 - Select stream type as main stream or sub-stream
 - Set pre-record and post-record for recording the video
 - 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
 - Select a Streaming Server to get the video stream of the camera
 - 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
 - Add new Recording Server
 - c. Shall have the ability to set picture storage settings for cameras
 - 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
 - d. Shall have the ability to configure event settings for cameras of current site
 - Select the triggering event
 - Trigger user-defined event
 - e. Shall have the ability to configure related map settings for current site:
 - Shall upload picture or import existing map of other area to link related map to the area
 - Shall edit picture or map name
 - Shall unlink the map to cancel the linkage between the map and area
 - Shall view the map in full-screen mode
 - Shall zoom in or zoom out the map
 - Shall adjust the map area for view and switch between GIS map and related map
 - Shall add cameras as hot spots on the related map
 - Shall adjust the hot spot location, edit, and delete hot spot
 - Shall add a map to another map as a hot region
 - Shall adjust hot region location, edit hot region, and delete hot region
 - Shall add/edit/delete labels on map, and adjust label location
 - Shall display the following resources on the map: camera, alarm input, alarm output, access point, site, UVSS, hot region, and label
 - Shall set exit & entry for fisheye camera before generate pathway analysis report
 - f. Shall have the ability to configure GIS map settings of current site:
 - Shall add sites/cameras/access points/alarm inputs/alarm outputs/UVSSs on GIS map to show the geographic location
 - Shall add up to 4 UVSS(s) to each SYS
 - Shall set GPS location for hot spot and hot region
 - Shall set icon style and name color, and add remark to GIS map
 - Shall add/delete/edit hot regions
 - Shall add/delete/edit labels
 - Shall choose to display the following resources on the map: camera, alarm input, alarm output, access point, site, UVSS, hot region, and label
 - Shall search geographic location in GIS map
23. Shall edit the following settings of access points for current site:
- a. Basic information
 - Access point name
 - Set access point 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 access point 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
 - Set free access schedule to keep the access point open

- Set access forbidden schedule to remain the access point closed
- b. Related cameras
 - Link up to two camera(s) to the access point to view its live view
- c. Application
 - Entry & Exit Counting: enable this function to count the persons entering and exiting the access points in the group
 - Multi-Door Interlocking: enable the multi-door interlocking function between multiple doors of the same access control device
 - Anti-Passback: The person should exist via the access point in the anti-passback if he/she enters via the access point 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
 - Open access point with first card: After swiping the first card, the access point will remain unlocked or be authorized. The status depends on the card swiping times (odd or even). For odd, the access point will remain unlocked or be authorized. For even, it will exit the unlocked or authorized mode.
 - Enable to set remaining unlocked duration
 - Enable to set authorization: the access point is locked and access is denied with credentials until you swipe the first card. After swiping the first card, the access point is authorized and the persons with corresponding access level are granted to access. The authorization will be invalid at 00:00 am every day
 - Set remaining unlocked duration(s)
 - Assign the first card permission to person(s)
- d. Hardware settings
 - Edit card reader parameters
 - Card reader name
 - Set polarity
 - Set card reader access mode
 - Card
 - Fingerprint
 - Card and Fingerprint
 - Card or Fingerprint
 - Card and PIN
 - PIN and Fingerprint
 - Card, PIN, and Fingerprint
 - Face or Fingerprint or Card
 - Face and Fingerprint
 - Face and PIN
 - Face and Card
 - Face
 - Face, Fingerprint, and Card
 - Face, PIN, and Fingerprint
 - Enable custom card reader access mode
 - Set custom time period and access mode
 - 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 access point of the turnstile
 - Add face recognition terminal by online devices
 - Add face recognition terminal by IP address
 - f. Access level
 - Add the access point to access level
 - g. Attendance settings
 - Set the access point as attendance check point
 - h. Event settings
 - Set triggering event(s) for the access point
 - Set linkage action for the event:
 - Arming schedule template
 - Trigger recording
 - Create tag
 - Capture picture
 - Link access point
 - Link alarm output
 - Trigger PTZ
 - Send email
 - Trigger user-defined event
 - i. Map settings
 - Add the access point to map
 - Set map icons
24. Shall edit the following settings of alarm inputs for current site:
- Edit alarm input name
 - Edit the event settings of the camera
 - Trigger user-defined event
 - Add the alarm input to map
 - Edit map icons
25. Shall edit the following settings of alarm outputs for current site:
- Edit the alarm output name
 - Add the alarm output to map
 - Edit map icons
26. Shall edit the following settings of UVSS for current site:
- a. Edit basic information of the UVSS
 - IP address
 - Port number
 - Alias
 - User name
 - Password
 - b. Edit additional settings of the UVSS
 - Link camera(s) to the UVSS
 - c. Edit map settings of the UVSS
 - Add the UVSS to map
 - Edit the map icons

E. Event & Alarm: Shall have the ability to configure the following:

1. To avoid flooding operators with alarms, shall have the option of adding just an event from a device, that will be searchable via the Control Client, but not broadcast as an alarm, including System-Monitored Events:

a. Shall batch add the following Video Content Analysis (VCA) events from cameras:

- Abnormal Face
- Audio Exception Detection
- Blacklist Alarm
- Camera Communication Exception
- Camera Communication Recovered
- Camera Offline
- Camera Online
- Camera Recording Exception
- Camera Recording Recovered
- Channel Armed
- Channel Arming Failed
- Defocus Detection
- Driving on the Lane Line
- Face Capture
- Face Detection
- Falling Down
- Fast Moving (Detection)
- Fire Source Detection
- Frequently Appeared Person
- Illegal Lane Change
- Illegal Parking
- Illegal U-Turn
- Installing Scanner
- Intrusion (Detection)
- Line Crossing (Detection)
- Loitering (Detection)
- Motion Detection
- Motor Vehicle on Non-Motor Vehicle Lane
- Multiple Faces
- Object Removal (Detection)
- Operation Timeout
- Parking (Detection)
- People Density
- People Gathering (Detection)
- People Queuing-Up Alarm
- PIR
- Region Entrance (Detection)
- Region Exiting (Detection)
- Scene Change Detection
- Sticking Scrip
- Sudden Decrease of Sound Intensity Detection

- Sudden Increase of Sound Intensity Detection
 - Tailing
 - Temperature Alarm
 - Temperature Difference Alarm
 - Temperature Pre-Alarm
 - Unattended Baggage (Detection)
 - Using Mobile Phone
 - Video Loss
 - Video Tampering Detection
 - Violent Motion
 - Waiting Time Detection Alarm
 - Wearing Sunglasses
 - Whitelist Alarm
 - Wrong-Way Driving
- b. Shall batch add the following Access Point Events
- Access Denied (Access point Remained Locked or Inactive)
 - Access Denied (First Card Not Authorized)
 - Access Denied by Card and Fingerprint
 - Access Denied by Card and Password
 - Access Denied by Card, Fingerprint, and Password
 - Access Denied by Face
 - Access Denied by Face and Card
 - Access Denied by Face and Fingerprint
 - Access Denied by Face and Password
 - Access Denied by Face, Card, and Fingerprint
 - Access Denied by Face, Password, and Fingerprint
 - Access Denied by Fingerprint
 - Access Denied by Fingerprint and Password
 - Access Failed When Free Passing
 - Access Granted by Card
 - Access Granted by Card and Fingerprint
 - Access Granted by Card and Password
 - Access Granted by Card, Fingerprint, and Password
 - Access Granted by Face
 - Access Granted by Face and Card
 - Access Granted by Face and Fingerprint
 - Access Granted by Face and Password
 - Access Granted by Face, Card, and Fingerprint
 - Access Granted by Fingerprint
 - Access Granted by Fingerprint and Password
 - Access Timed Out by Card and Fingerprint
 - Access Timed Out by Card and Password
 - Access Timed Out by Card, Fingerprint, and Password
 - Access Timed Out by Face and Card
 - Access Timed Out by Face and Fingerprint
 - Access Timed Out by Face and Password

- Access Timed Out by Face, Card, and Fingerprint
- Access Timed Out by Face, Password, and Fingerprint
- Access Timed Out by Fingerprint and Password
- Anti-Passback Server Respond Failed
- Anti-Passback Violation
- Barrier Obstructed
- Barrier Obstruction Recovered
- Calling Surveillance Center
- Card Number Expired
- Card Reader Tamper Alarm
- Climbing Over Barrier
- Door Abnormally Open (Access point Contact)
- Door Bell Rang
- Door Button Pressed Down
- Door Button Released
- Door Closed (Door Contact)
- Door Locked (Door lock)
- Door Locked by Keyfob
- Door Open (Door Contact)
- Door Open Timed Out (Door Contact)
- Door Open with First Card Ended
- Door Open with First Card Started
- Door Remained Unlocked by Keyfob
- Door Unlocked (Door Lock)
- Door Unlocked by Keyfob
- Duress Alarm
- Face Recognition Failed
- Face Recognition Terminal Offline
- Face Recognition Terminal Online
- Fingerprint Not Found
- First Card Authorization Ended
- First Card Authorization Started
- Force Accessing
- Intrusion
- Invalid Time Period
- Live Face Detection Failed
- Max. Card Access Failed Attempts
- Multi-Door Interlocking
- No Access Level Assigned
- No Card Number Found
- Passing Timeout
- Remaining Locked Status Ended
- Remaining Locked Status Started
- Remaining Unlocked Status Ended
- Remaining Unlocked Status Started
- Remote: Locked Access point

- Remote: Remained Locked (Credential Failed)
 - Remote: Remained Unlocked (Free Access)
 - Remote: Unlocked Access Point
 - Reverse Passing
 - Secure Door Control Unit Tamper Alarm
 - Tailgating
 - Verifying Card Encryption Information Failed
- c. Shall batch add Alarm Input events
- d. Shall batch add the following ANPR Event:
- License Plate Matched Event
 - License Plate Mismatched Event
- e. Shall batch add the following Person Event:
- Face Matched Event
 - Face Mismatched Event
- f. Shall batch add the following Under Vehicle Surveillance System Event:
- Offline
 - Online
- g. Shall batch add Remote Site Event: Site Offline
- h. Shall batch add health monitoring 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 Full
 - Illegal Login
 - R/W HDD Failure
 - Video Standard Mismatch
- i. Shall batch add health monitoring events from Access Control Device:
- Active Infrared Intrusion Detector Exception
 - AC Power Off
 - AC Power On
 - Battery Voltage Recovered
 - CAN BUS Exception
 - Communicated with IR Adapter Exception
 - Communicated with Light Board Failed
 - Connection Recovered with Anti-Passback Server
 - Device Arming Failed
 - Device Offline
 - Device Online
 - Device Tampered
 - Disconnected with Anti-Passback Server
 - Lane Controller Fire Input Alarm

- Lane Controller Tamper Alarm
 - Low Battery Voltage
 - Low Storage Battery Voltage
 - Motor or Sensor Exception
 - No Memory for Offline Event Storage
 - Pedestal Temperature Too High
- j. Shall batch add health monitoring events from Security Control Device:
- Ac Power Down
 - Alarm Cleared
 - Auto Arming Failed
 - Away Arming
 - BUS Open-Circuit Alarm
 - BUS Short-Circuit Alarm
 - Control Panel Reset
 - Device Armed
 - Device Arming Failed
 - 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
 - Keypad Locked
 - Keypad Unlocked
 - Low Battery Voltage
 - Stay Arming
 - Telephone Communication Failed
 - Virtual Standard Mismatch
 - Virtual Zone Fire Alarm
 - Virtual Zone Panic Alarm
 - Wired Network Disconnected
 - Wireless Network Disconnected
 - Wireless Network Exception
 - 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
- k. Shall batch add health monitoring events from Dock Station
- Dock Station Offline
 - Dock Station Online
- l. Shall batch add health monitoring 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
 - HDD Full
 - 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
- m. Shall batch add health monitoring events from the Streaming Server: Server Exception
- n. Shall batch add health monitoring events from the Facial Recognition Server:
- Facial Recognition Server Offline
 - Facial Recognition Server Online
- o. Shall batch add Health Monitoring events from the HikCentral Professional Server:
- CPU Exception
 - CPU Recovered

- CPU Warning
 - RAM Exception
 - RAM Recovered
 - RAM Warning
 - System Service Abnormally Stopped
 - System Service Recovered to Run
- p. Shall batch add user events: User Login/Logout
 - q. Shall batch add User-Defined Event as System-Monitoring Event
 - r. Shall batch add Generic Event as System-Monitoring Event
 - s. 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
 - t. Shall batch delete all invalid events
 - u. Shall trigger any of the above stated events as user-defined events
 - v. Shall convert any of the above stated events into an alarm
 - w. Shall enable active control for events and set threshold for reactivation
 - x. Shall set the following linkage actions of System-Monitored Event:
 - Set and view Arming Schedule Template
 - 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
 - Create tag for related videos
 - Capture picture from the source camera or specified camera, and set the capture time
 - Lock video files
 - Link up to 16 access point and set access point status as unlock, lock, remain unlocked, or remain locked
 - Link alarm output
 - Close alarm output manually or automatically
 - Trigger PTZ
 - Send email and set the added email template
 - Trigger user-defined event
2. Generic Event: 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
 - a. Shall have the ability to edit the event name
 - b. Shall have the ability to support 'copy from' functions
 - c. Shall have the ability to select transport type as TCP/UDP
 - d. Shall have the ability to set the match type as Search/Match
 - e. Shall have the ability to set the expression
 3. User-Defined Event: Shall have the ability to set user-defined events
 4. Alarms: shall support the following functions:
 - a. Shall have the ability to configure the same events list as alarm in System-Monitored Events Part
 - b. Same list of events listed above in section "1,2,3" shall be available to be programed as alarms on the SYS
 - i. When selecting a triggering event to program as alarms, only events supported by a device will appear in the Web Client

- ii. Alarm priority shall be configured to one of three levels by default:
 - High
 - Medium
 - Low
- iii. Alarm Priority of up to 255 levels can be added as required
- iv. 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)
- v. Shall set arming schedule template as schedule template or event based
- vi. Shall enable active control and set threshold for reactivation
- vii. Shall specify a user defined event or alarm input as the start or end event of the arming schedule
- viii. Shall set alarm recipients from users accounts set up in the SYS
- ix. Shall associate the source camera or up to 16 other cameras recording with alarm events
- x. Shall lock associated alarm event video footage, so it is not auto-erased based on the camera schedule
- xi. Shall set pre-record and post-record duration
- xii. Shall display the recorded video when alarm occurred or live view by default
- xiii. Shall associate a map with an alarm
- xiv. Shall trigger a pop-up window with an alarm event
- xv. 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
- xvi. Shall enable restrict alarm handling time and select up to 16 user-defined events and alarm outputs to trigger events if timeout occurs
- xvii. Shall trigger audible warning
- xviii. Shall trigger User-Defined Event
- c. Shall delete invalid items (in batch)
- d. Shall enable/disable alarms (in batch)
- e. 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, display on smart wall, email linkage, and user-defined event linkage
- f. Alarm source, trigger events, and alarm priority can also be displayed
- g. Shall support displaying alarms in alphabetical order

- h. 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
- i. 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
- j. Shall support setting reports of events and alarms:
 - 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
 - Select report type as daily or weekly
 - Select the sending time
 - Set the email template
 - Select the format as Excel or PDF
- k. Shall support testing alarm configuration: click the button and the system will trigger an alarm automatically

F. Access Level:

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 group
 - c. Access schedule
 - d. Access point
4. Assign the access level to some access group(s) so that the person(s) in the access group(s) will have the access permission to access the access point(s)
5. Modify the access level name, description, access point(s), access schedule, and assigned access group(s) of access level

G. Time & Attendance

1. Shall have the ability to add a new shift schedule
 - a. Set a name for the schedule
 - b. Set repeat by week: the schedule will repeat every 7 days based on the week
 - c. Set repeat by day(s)
 - i. Set the frequency of repeat days
 - ii. Set the start date for reference
 - d. Set shift type as fixed: the required start-work time and end-work time is fixed
 - i. Set scheduled work time
 - ii. Set break duration

- iii. Calculate the work hours
 - iv. Set the valid check-in/out period
 - e. Set shift type as flexible: the start-work time and end-work time is flexible
 - i. Set flexible duration
 - ii. Set break duration
 - iii. Set minimum work hours
 - iv. Set valid check-in/out period
 - v. Support 'Save and Copy to' function to copy the schedule to other days
 - vi. Calculate the work hours
 - vii. Set valid check-in/out period
 - f. Add holidays to define the special days that can affect shift schedules or access control schedules
 - g. Assign shift schedule to attendance group
 2. Shall have the ability to set attendance check point
 - a. Add the access point as attendance check point
 3. Shall have the ability to check attendance record
 - a. Filter the attendance records according to the following conditions:
 - Time
 - Attendance group
 - Person name
 - Status
 - Additional information
 - b. View the attendance details and the person's attendance report for one day
 - Person name
 - ID
 - Attendance group
 - Status
 - Scheduled work time
 - Actual work time
 - Break duration
 - c. View the attendance details and the person's attendance report for more than one day
 - Person name
 - ID
 - Attendance group
 - Times of late and specific date
 - Times of early leave and specific date
 - Times of absent and specific date
 - Times of normal and specific date
 - Schedules work time
 - Actual work time
 - Break duration
 - d. (Batch) correct check-in/out time for the exceptional records
 - Configure correction time
 - Edit correction reason
 - e. Export the filtered attendance records in CSV format
 - Person name
 - ID

- Attendance group
 - Scheduled work time
 - Actual start time
 - Actual end time
 - Actual work time
 - Break duration
 - Status
- f. Search the history attendance result even if this person has been deleted from the system
 - g. When the device is online, upload the records to system of the device offline duration
 - h. Support different time zone of the device and HikCentral Professional platform

H. Person

1. Person List
 - a. Edit ID
 - b. Edit first name
 - c. Edit last name
 - d. Select gender as male/female/unknown
 - e. Set person profile
 - Collect profile by added access control device
 - Take a picture by webcam
 - Upload a picture from local PC
 - f. Edit email address
 - g. Edit phone number
 - h. Edit remark
 - i. Customize additional information
 - Set optional information
 - Add additional information
 - j. Check the face comparison group, time and attendance group, access group and dock station group of the person
 - k. Configure effective period of access control and time & attendance for the access group
 - l. Enable the 'Super User' function to exempt this person from remaining locked (credentials failed) restrictions, all anti-passback rules, and first card authorization
 - m. Enable the 'Extended Access' function to open the access point for longer time for person with special requirements
 - n. Add the person to the existing attendance group if the person participates in time and attendance, and one person can be added only one attendance group
 - o. Set credential information for the person:
 - i. PIN number
 - 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
- iv. Duress credentials: set credentials to swipe the card or scan the fingerprint under duress, and the access point will be unlocked and the Control Client will receive a duress alarm to notify the security personnel
 - Card
 - Fingerprint
- p. Add to Dock Station Group
 - i. Set Login Password
 - ii. Select the existing dock station group
 - iii. Add new dock station group
- q. View the details of the persons:
 - iv. Name
 - v. ID
 - vi. Phone
 - vii. Type
 - viii. Face comparison group name
 - ix. Access group name
 - x. Attendance group name
 - xi. Effective period
 - xii. Credential information
 - Number of fingerprints
 - Number of cards
 - Enable/disable profile as Face Credentials
- r. Batch issue cards to persons
 - i. Set card issuing mode:
 - Card Enrollment Station
 - Card format
 - Reading frequency
 - Card encryption
 - Audio on/off
 - Card reader
 - Select card reader
 - Enter manually: enable/disable auto increment card number
- s. Enable/disable face credentials
- t. Batch import persons/profiles
 - i. Import by excel file
 - ii. Import by importing profiles
 - 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
- u. Synchronize domain persons
- v. Export all persons information and set password for decompressing

- w. Customizable additional information other than the basic information, such as address, income, etc.
 - x. HikCentral Professional supports up to 1,000,000 persons
 - y. Delete the selected persons
 - z. Delete all the persons
2. Face Comparison Group
- a. Add face comparison group
 - i. Group name
 - ii. Set similarity threshold
 - iii. Add description
 - iv. Add person(s) to the group
 - Import from person list
 - Import from existing face comparison group
 - Imported domain group
 - Add all persons
 - v. Remove the person(s) from the face comparison group
 - b. Edit the face comparison group and view the cameras that it is applied to
 - i. Delete the face comparison group
 - ii. Delete all the face comparison groups
 - c. Apply the face comparison group(s) to camera(s)
3. Access Group
- a. Add access group
 - i. Create a name for the access group
 - ii. Set person(s) in the access group
 - Copy from the existing group
 - Add person(s) from person list/domain group
 - iii. Set access level
 - Select the existing access level and view the access point(s) and access schedule
 - Add new access level
 - b. View the details of the access group:
 - Group name
 - Person(s)
 - Access level
 - c. Delete (all) the access group(s)
 - d. Edit the access group
 - e. Apply access groups to device
 - i. Apply changes: Apply the person's changed (newly added, edited, deleted) access levels to the device
 - ii. 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
 - f. Regularly apply all access groups to device: set the time and the system can apply all the access groups to the access control device on a scheduled basis
4. Attendance Group
- a. Add attendance group
 - i. Edit the attendance group name
 - ii. Configure effective period for the group

- iii. Select one of the following modes to add person:
 - Person List
 - Imported Domain Group
- iv. Set the shift schedule for the persons in the group
 - Set shift type as fixed
 - Set shift type as flexible
 - Set holiday schedule
- v. Set the time zone
- b. View the details of the added attendance group
 - i. Group name
 - ii. Shift schedule
 - iii. Attendance shift schedule on every day
- c. Edit the added attendance group
- d. Delete (all) attendance group(s)

I. Vehicle: Shall have the ability to manage up to 100 vehicle lists:

1. Import vehicle list
2. Import vehicle list in batch
3. Export vehicle list
4. Delete vehicle list
5. Delete vehicle information in one list
6. Rename vehicle list name
7. Replace repeated license plate number when import vehicle list
8. Add basic vehicle information in one list, i.e. license plate number, effective period, brand, model, owner and phone number, support up to 5,000 vehicles managed in one list
9. Upload undercarriage picture to view both the current vehicle's captured undercarriage picture and the uploaded picture for comparison

J. Security

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 resource access for the following types:
 - a. Logical resource:
 - Access all resources in shown area
 - Access specified resources in shown area
 - b. Entry & Exit Counting
 - c. Encoding device (NVR, Network Camera)
 - d. Decoding device
 - e. Access control device
 - f. Dock Station
 - g. Security control device
 - h. Smart wall and screen
 - i. Server
 - j. Face Comparison Group
 - k. Dock Station Group
 - l. Custom additional info.
 - m. User-defined event

- n. User log
- 4. Shall set the following user permission:
 - a. Resource permission:
 - Camera
 - Live view
 - Playback
 - Capture and print pictures
 - Video search
 - Download video
 - Manual recording
 - Two way audio
 - View tag
 - Add tag
 - Edit tag
 - Delete tag
 - View lock
 - Add lock
 - Edit lock
 - Delete lock
 - PTZ control
 - Audio control
 - Show health status
 - Show face recognition information
 - Manage security
 - Access point
 - Live view
 - Playback
 - Control door status
 - Forgive anti-passback
 - Show health status
 - Manage security
 - UVSS
 - Live view
 - Search
 - Show health status
 - Manage security
 - Security Control Partition
 - Arm and disarm
 - Manage security
 - Encoding device
 - Configuration on device
 - Broadcast
 - Search log
 - Show health status
 - Manage security
 - Decoding device
 - Configuration on device

- Show health status
 - Manage security
 - Access control device
 - Configuration on device
 - Show health status
 - Manage security
 - Security control device
 - Configuration on device
 - Broadcast
 - Search log
 - Show health status
 - Manage security
 - Dock Station
 - Search file
 - Lock file
 - Download File
 - Show health status
 - Manage security
 - Alarm output
 - Alarm output control
 - Manage security
 - Server
 - Show health status
 - Manage security
 - User-defined event
 - Trigger alarm manually
 - Manage security
5. Configuration permission: create definable access to
- a. Web Client for sub-admin roles
- Resource Management
 - Physical view: view/add/edit/delete encoding device/access control device/security control device/dock station/recording server/streaming server/facial recognition server/smart wall
 - Logical view: view/add/edit/delete
 - Event and Alarm settings: view/add/edit/delete
 - Access Level: view/add/edit/delete
 - Time & Attendance: view/add/edit/delete
 - Person
 - Person list: view/add/edit/delete/custom addition info.
 - Face comparison group: view/add/edit/delete
 - Access group: view/add/edit/delete/apply to device/apply to device(scheduled)
 - Attendance group: view/add/edit/delete
 - Dock station group: view/add/edit/delete
 - Vehicle: view/add/edit/delete
 - Security: view/add/edit/delete
 - System: view/edit

- Backup and restore system data
 - Batch upgrade firmware
 - Camera settings in license
 - Manage security
- b. Operation permission: for different levels of operator access
- Monitoring
 - Live view
 - Playback
 - Map
 - Public view: add/edit/delete
 - Alarm center
 - View
 - Arm and disarm
 - Acknowledge alarm
 - Trigger pop-up window
 - Event & Alarm search
 - Video search
 - Person access
 - Vehicle search
 - Evidence collection
 - Search
 - Edit
 - Download
 - Delete
 - Upload
 - Add new vehicle to vehicle list
 - Add person to face comparison group
 - People analysis
 - Heat map
 - Temperature Analysis
 - Vehicle Analysis
 - Health monitoring
 - Audit Trail
 - System
 - Close auxiliary screen
 - Logout
 - Manage security
- c. Shall add up to 3,000 roles for user management per SYS
- d. Shall display by areas, or channels
- e. Shall separate resources and permission settings
- f. Shall set management permissions for every module. Users without module permissions cannot edit permission settings through security module
- g. Shall manage the permission of checking, adding, deleting, editing of each module on the Control Client
- h. Shall hide modules on the Control Client
- o. Shall manage resources of Remote Sites
- p. Shall support the 'copy from' function to copy features of the existing roles

6. Users: Up to 3,000 users shall be added manually
 - 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
 - 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 roles to the user
 - i. View role list and detailed information
 - j. Import domain users (group)
 - i. Select importing mode as user or group
 - ii. Select domain users
 - iii. Configure domain users
 - iv. Restrict concurrent logins
 - v. Set PTZ control permission
 - vi. Assign role to the domain user
 - vii. View role list and detailed information
 7. Synchronize domain users
 8. 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)
 9. Security Settings for Users
 - a. Lock IP Address
 - i. 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:
 - i. Weak: a combination of at least 8 characters including two types of characters among lowercase letters, uppercase letters, numbers, and special characters.
 - ii. 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)
 - iii. 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
 - i. 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
 - i. Configurable: Lock in 10 minutes, 20 minutes, 30 minutes or "custom" number of minutes ranging from 10 to 30
 - e. Shall have the ability to view the details of the existing users:
-

- i. Name
- ii. Type
- iii. Role
- iv. Connection number
 - Connection number of Web Client
 - Connection number of Control Client
- v. Login status
- vi. User status
- vii. Expiry date

K. System and Maintenance

1. Shall set the following normal parameters:
 - a. Site name
 - b. Enable GIS map function and configure the map API URL, and set the icons of the hot region, camera, access point, alarm input, alarm output, and UVSS on the map
 - c. Set first day of week
 - d. Set temperature unit as Celsius, Fahrenheit, or kelvin
 - e. 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
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. Receiving generic event
 - d. 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
 - e. For the a 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
 - f. Set a static IP address or domain name for the WAN access
 - g. Set default waiting time for the configuration on the Web Client. The configuration will be regarded as failure if no response within the configured timeout time
 - h. Set device access mode as automatically mode or proxy
 - i. Select the NIC of the current SYS so that the system can receive the alarm information of the third-party device connected via ONVIF protocol
3. Shall set the following storage parameters:
 - a. Storage on SYS server:
 - Select storage location
 - Restrict quota for pictures
 - Set storage quota

- b. Set the data recorded duration for the follow types of records:
 - Received events
 - Recording tags
 - Face comparison data
 - Card swiping records
 - Attendance records
 - Vehicle passing records
 - Video analysis data
 - Service error logs
 - Service warning logs
 - Service information logs
 - Set the duration as three months/six months/one year/two year/three years
 4. Shall set the following schedule:
 - a. Recording schedule template
 - b. Arming schedule template
 - c. Access schedule template
 - Affect the applied access levels and access control application parameters after edited
 - Apply the changes to the device after edited
 - d. Permission schedule template
 - e. Defense schedule template
 - f. Holiday settings
 5. Add email template:
 - a. Add up to 64 recipients
 - b. Add domain user/email address as recipient
 - c. Set email subject
 - d. Set email content
 - e. Attach image
 - f. Configure the following email settings:
 - Server authentication
 - Cryptographic protocol
 - Sender email address
 - Sender name
 - SMTP server address
 - SMTP server port
 - User name
 - Password
 6. Configure report settings
 - a. Set the following report type:
 - Event
 - Alarm
 - Vehicle
 - People counting
 - Queue
 - Heat map
 - Pathway
-

- Temperature
 - Attendance
- b. Set the report name
 - c. Set the event report target
 - d. Set report type
 - e. Select email template
 - f. Set format as excel or PDF
7. 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
 8. Advanced settings:
 - a. Set Clients and SYS transfer as HTTP or HTTPS
 - b. Set camera ID as identifier number on the keyboard to display live view on smart wall
 - c. Working mode: set the working mode for the DS-K5600 face recognition series as face recognition terminal if it is applied with HIKVISION turnstile or access control terminal if it is applied with other third-party turnstile
 - d. Export service component certificate
 - e. Set health check frequency
 - Device health status:
 - Encoding device
 - Access control device
 - Security control device
 - Dock station
 - Server health status:
 - Recording server
 - Facial recognition server
 - Others:
 - Device capabilities
 - Recording
 - Alarm/event enabled or not
 - Remote alarm enabled or not
 - f. Add rules for plate fuzzy search
 - g. Hot spare
 - h. Reset network information
 - i. Set database password by admin user
 9. Select the NIC of the current SYS so that the system can receive the alarm information of the third-party device connected via ONVIF protocol
 10. Export Configuration Data, 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
 11. Shall 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
12. Shall export configuration data of Remote Site, encoding device, and recording
 13. Shall download HikCentral Professional Control Client on the Web Client
 14. Shall support the applications module (including Live View, Playback, and Local Configuration) when accessing the Web Client via Internet Explorer via HTTPS protocol
 15. Shall support Live View and Playback modules when accessing the Web Client via Internet Explorer, Google Chrome, and Firefox via HTTP protocol, and support local configuration module only for Internet Explorer
 16. Admin user shall online/offline activate/deactivate license, online/offline update the license, and view license detailed information for system capabilities
 17. For facial recognition camera/ANPR camera/thermal camera (report supported), you shall select the added cameras as these three types of cameras. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

L. Local Configuration for Live View and Playback in Web Client:

1. Network transmission:
 - i. GPU hardware decoding:
 - Enable
 - Disable
 - ii. Global stream:
 - Main stream
 - Sub stream
 - Smooth stream
 - iii. Threshold for main/sub-stream:
 - 1/4
 - 1/9
 - 1/16
 - 1/64
 - iv. Network timeout:
 - Default
 - Default x 1.5
 - Default x 2
 - v. Video caching:
 - Small (1 frame)
 - Medium (6 frames)
 - Large (15 frames)
 - vi. Time zone:

- Client time
 - Device time
 - vii. Picture format:
 - BMP
 - JPEG
 - viii. Device access mode:
 - Restore default
 - Automatically judge
 - Directly access
 - Proxy
2. Shall view the saving path of video files and captured pictures on the current PC
 3. Shall live view up to 64 cameras simultaneously
 4. Shall view image thumbnail
 5. Shall playback up to 16 cameras simultaneously
 6. Shall support capturing, manual recording, digital zoom, two-way audio, select stream type, displaying camera status of resolution and frame rate, audio on/off, switching to instant playback during live view
 7. 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
 8. Shall support selecting playback date from the calendar

Control Client

- A.** The Control Client is a Windows-based software for security operators to access NVRs, Hybrid SANs, and network cameras using authorized client login credentials and view through the SYS. It shall provide multiple operating functionalities, including real-time live view, PTZ control, video playback and download/exporting, alarm management, VCA search, log query, and health monitoring module
- B.** Recommended Control Client specification shall be the following (for more details about Control Client Specifications, please refer to the document, HikCentral Professional V1.4_Software Requirements & Hardware Performance):
 - CPU: Intel® Core™ i5-4590 @3.30GHz
 - RAM: 8G
 - Network: GbE network interface card
 - Graphics Card: NVIDIA® GeForce® GTX 970
 - Hard Disk Type: SATA II hard drive or better
 - Hard Drive Capacity: 60 GB for OS and Control Client
 - Other: Microsoft® Windows 7 (64-bit Operating System)
- C.** On initial login, the user must use “one time” default password and shall be forced to create a new password that is not the default for future log-ins
 1. Password must at minimum contain 8 characters with at least three of the following categories: numbers, lowercase letters, uppercase letters, and special characters
- D.** Shall have the ability to enable auto-login, and login via domain name and password
- E.** Shall have the ability to log in to the Control Client through HTTP or HTTPS
- F.** Shall have the ability to display the online/offline status of Remote Sites in Central System
- G.** Shall have the ability to customize module arrangement on Control Panel
- H.** Shall have the following modules and functions:

1. Monitoring: Live view
 - a. Ability to view up to 256 cameras
 - b. Ability to display GIS map/related map after the camera is added on the map
 - c. Ability to display thumbnail of camera
 - d. Ability to auto switch to sub stream of Network Camera according to the configuration of stream threshold
 - i. Enable auto-switching between main stream and sub stream
 - ii. Enable to set the main stream threshold as 1/2, 1/4, 1/9, 1/16, 1/25,1/36, 1/64
 - iii. 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
 - e. Shall support up to 4 auxiliary screens during live view and 1 screen for playback
 - f. Ability to display license plate number when viewing LPR camera after the LPR function is activated in license
 - g. Ability to mark a vehicle license plate number
 - h. Ability to add the vehicle to vehicle list
 - i. Ability to go to Vehicle Search by quick link:
 - i. Label
 - ii. License Plate number
 - iii. Vehicle passing time
 - iv. Camera name
 - v. Owner
 - vi. Phone
 - vii. Country/region
 - viii. Operation
 - Add to vehicle list
 - Download
 - j. The following functions are available on the tile toolbar for easy access to operator:
 - i. Audio control
 - ii. Capture: ability to save snapshots
 - iii. Print camera image
 - iv. Enable manual recording of displayed Network Camera
 - v. Enable and utilize two-way audio
 - vi. Enable view instant playback
 - vii. Digital zoom
 - viii. 3D positioning for PTZ camera
 - ix. Activate on-screen PTZ controls
 - x. Show camera status
 - Frame rate
 - Resolution
 - Stream format
 - Bit rate
 - Connection number
 - Net 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
- xi. Arming control
 - xii. Switch stream type of camera
 - xiii. Edit transcoded stream
 - xiv. Live view on smart wall by graphic card
 - xv. VCA playback
 - xvi. Alarm output
 - xvii. Save area as view
 - xviii. Area auto-switch
 - xix. Add tag
 - Set time range
 - Add description
 - Select storage type
 - xx. 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
- k. Ability to customize camera tile toolbar
 - i. Re-order icons to user preference
 - ii. Remove icons of functions not required for user
 - l. Ability to create tile patterns with selected cameras and save as a view
 - i. Save as private view, only accessible to the user profile creating the view
 - ii. Save as public view, accessible to all users
 - iii. Play in batch: play all cameras belonging to one area on different screens
 - iv. View group auto-switch
 - v. 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
- m. Support smart wall (graphic card)
 - i. Display all contents in live view on smart wall
 - ii. Display live view of one camera on smart wall
 - iii. Display live view of all cameras in one area on smart wall
 - iv. Display e-map and GIS map on smart wall
 - v. Display view and view group on smart wall
 - vi. Display alarm's related video on smart wall
 - vii. Display Health Monitoring page on smart wall
- n. PTZ Control: Shall have following options to control PTZ cameras
 - i. On-screen PTZ icon
 - (a) Able to control all PTZ functions available directly on camera
 - ii. On tile "point and go" directional control
 - (a) Able to use mouse wheel for zoom in after PTZ control is enabled
 - iii. 3D Positioning: ability to draw box for region of interest to zoom in on tile
- o. Support decoding and displaying Remote Site's cameras and current site's cameras on smart wall
- p. Live view of Remote Site's cameras
- q. After reopening the client, display the view before closing the client
- r. Set preset and patrol for common cameras
- s. Set preset and patrol settings of fisheye camera
- t. Set offline alarm schedule for Remote Sites
- u. View the live video of the UVSS's linked camera, the undercarriage picture, and recognized license plate number of the passing vehicles
- v. Drag on the undercarriage picture to mark important information
- w. Mark the vehicle license plate number
- x. View access point-related live view
 - i. Shall view the live video of up to two related cameras in one display window
 - ii. 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
 - iii. Shall control the access point status as unlock, lock, remain unlocked, remain locked, and view the card swiping record in real time. When the access point 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
 - iv. Shall forgive anti-passback violation
 - v. Shall check the turnstile status and control it as unlock, lock, remain unlocked, remain locked
 - vi. Shall control all access points status as Lock/Unlock or Recover all access points
 - vii. Shall trigger user-defined event
 - viii. Shall handle opening door request from video access control terminal, including voice talk and unlocking door
 - ix. Shall show access point's real-time status
 - x. Shall support two-way audio between video access control terminal and control client
- y. View detected events in live view
 - i. View/filter/clear the detected events, including ANPR events, face comparison event and access event

- ii. View access event details
 - (a) Profile
 - (b) Card number
 - (c) Person name
 - (d) Event
 - (e) Source
 - (f) Description
 - (g) Client time
- iii. Add the person to person list
- iv. Add recognized vehicle to vehicle list
- v. Subscribe events of all resources
- z. View detected and matched face in live view:
 - i. View the face comparison information between the detected faces and the face pictures in the selected face comparison group
 - ii. Display person's profile (configured in the Web Client):
 - (h) Captured time
 - (i) Compared result
 - (j) Device name
 - (k) Face comparison group
 - (l) Gender
 - (m) ID number
 - (n) Email address
 - (o) Phone number
 - iii. Search video of the person by the captured face picture
 - iv. Add mismatched person to person list
 - v. Display the similarity between the captured face picture and the original face picture in person list
- aa. View/hide detected events in live view
 - i. View the detailed information of the events
 - Event result
 - Source
 - Description
 - Time
 - ii. Operation
 - Check the face comparison information
 - Add the mismatched person to person list
 - Search video about the person by the captured pictures and matched pictures
- bb. View UVSS's live view
 - i. View the live video of the UVSS's linked camera, the undercarriage picture, and recognized license plate number of the passing vehicles
 - ii. Perform the following operations in live view:
 - Mark on undercarriage picture
 - Mark vehicle
 - Add vehicle to vehicle list
 - Search vehicle
- cc. Diagnose when live view failed

- i. Display the details of the camera
 - ii. Display the exception description
 - iii. Display the diagnosis details, including requesting URL status, logging into encoding device status, getting stream from encoding device status
 - iv. Quick link to event log, server log, device log, health monitoring
 - v. Mark the diagnosis
2. Monitoring: Playback
- a. Ability to play back 1 to 16 cameras simultaneously
 - b. Ability to display GIS map/related map
 - c. When playing multiple cameras simultaneously, have ability to view in non-synchronized and synchronized mode
 - d. Ability to fast-forward by 1x, 2x, 4x, 8x, 16x, and slow-forward by 1/16x, 1/8x, 1/4x, 1/2x
 - e. Ability to export one or multiple cameras displayed simultaneously:
 - i. Set export location
 - ii. Set whether to download VSPlayer for viewing
 - iii. Export video files in MP4/AVI/EXE format
 - iv. Set saving path
 - v. Search and export video files of over 48 hours duration
 - vi. Synchronize downloading time
 - f. The following functions are available on the camera playback tile toolbar for easy access to operator:
 - i. Capture: ability to save JPEG snapshots and search video by the captured picture
 - ii. Print camera image
 - iii. Clipping: ability to quickly export video clips
 - iv. Add tag to video
 - v. Digital zoom
 - vi. Lock video: to prevent video segments from being over written by schedule
 - vii. Camera status
 - Frame rate
 - Resolution
 - Stream format
 - Bitrate
 - Connection number
 - Net 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
- viii. Stream type switch
 - ix. Playback on smart wall
 - x. Transcoding playback
 - xi. Audio on/off
 - xii. Video download
 - xiii. VCA search
- g. Customize camera tile tool bar
 - i. Re-order icons to user preference
 - ii. Remove icons of functions not required for user
 - h. Support channel decoding on the smart wall
 - i. Playback channels of Remote Sites
 - j. Search video files by time
 - k. Display the date with video files marked with a triangle
 - l. Support ATM-DVR, its playback type shall be set as command playback
 - m. Select storage location of recorded video files (central storage or remote storage)
 - n. Enable/disable thumbnails
 - o. Zoom in or zoom out on the timeline
 - p. Support dual-stream playback
 - q. Support AVI format for video file download
 - r. Encrypt to download in MP4/EXE format, and click and play directly after downloading with player in MP4 format
 - s. Support save the downloading file as evidence:
 - i. Create evidence
 - ii. Add to existing evidence
 - t. Support privacy mask after downloaded and played with VSPlayer
 - u. Adjust downloading time
 - v. Check the merged video files in one folder
 - w. Show/hide thumbnail
 - x. View access point related playback
 - i. Shall view the playback of up to two cameras in one display window
 - ii. Shall support capturing, printing captured picture, clipping, adding tags, lock the video, zoom in/out, downloading the video, fisheye expansion, VCA playback, displaying camera status, viewing the playback on smart wall, transcoded playback, switching between main stream and sub stream, audio on/off
 - iii. Shall control the access point status as unlocking, locking, remaining unlocked, remaining locked, and view the card swiping record in real time. When the access point is related to two cameras, the video will display in Picture-in-Picture mode, and you can view the live video of the two cameras in one window
 - iv. Shall control all access points status as locking/unlocking all access points or recovering all access points
 - v. Shall trigger user-defined event:
 - End arming

- Not handled
 - Start arming
 - y. Diagnose when playback failed
 - i. Display device information
 - ii. Display exception description
 - iii. Display the following requesting playback parameters:
 - Name
 - Online status
 - Streams number
 - CPU usage
 - RAM usage
 - HDD usage
 - iv. Quick link of server log
 - v. Mark the diagnosis
- 3. Alarm Center
 - a. Alarm Management: Ability to receive and view alarm video pre-configured in the Web Client as alarms
 - i. Ability to view the following alarm information:
 - Mark status
 - Alarm name
 - Alarm priority
 - Alarm time(Control client)
 - Alarm source
 - Logical Area
 - Triggering event/alarm
 - Alarm status
 - Alarm category
 - Quick link:
 - Alarm & event search
 - Two-way audio
 - Download
 - ii. View 1 to 16 cameras associated with alarms
 - iii. Optionally, auto view e-map and position of camera(s) on map in alarm state
 - iv. Turn audio off/on
 - v. Enable/disable alarm pop-up window
 - vi. Arm/disarm alarms
 - vii. Display the alarm related video on smart wall
 - viii. Click on the alarm name to access the following functions:
 - Check detailed alarm information and capture
 - Select alarm priority and category
 - Add remark to the alarm
 - Acknowledge the alarm
 - ix. Switch between related picture and videos
 - x. Select to display related video or related picture preferred
 - xi. Supports alarm linkage to smart wall, including smart wall of graphic card and decoding device
 - xii. Alarm linkage of smart wall supports window division and jointing

- xiii. Central system can receive alarms from Remote Sites
 - xiv. Alarm center can display map or video, or map and video
 - xv. Supports multiple time zones of clients
 - xvi. Supports displaying alarm video on smart wall including smart wall of graphic card and decoding device
4. Alarm and Event Search: Ability to search for alarms and events, based on the following:
- i. Event Source
 - Camera
 - Access Point
 - Alarm Input
 - ANPR
 - Person
 - UVSS
 - Remote Site
 - Encoding Device
 - Access Control Device
 - Security Control Device
 - Dock Station
 - Recording Server
 - Streaming Server
 - Facial Recognition Server
 - HikCentral Professional Server
 - User
 - User-Defined Event
 - Generic Event
 - ii. Event Type
 - Abnormal Face
 - Audio Exception Detection
 - Blacklist Alarm
 - Camera Communication Exception
 - Camera Communication Recovered
 - Camera Offline
 - Camera Online
 - Channel Armed
 - Channel Arming Failed
 - Camera Recording Exception
 - Camera Recording Recovered
 - Defocus Detection
 - Face Capture
 - Face Detection
 - Falling Down
 - Fast Moving (Detection)
 - Fire Source Detection
 - Frequently Appeared Person
 - Installing Scanner
 - Intrusion (Detection)

- Line Crossing (Detection)
- Loitering (Detection)
- Motion Detection
- Multiple Faces
- Object Removal (Detection)
- Operation Timeout
- Parking (Detection)
- People Density
- People Gathering (Detection)
- People Queuing-Up Alarm
- PIR
- Region Entrance (Detection)
- Region Exiting (Detection)
- Scene Change Detection
- Sticking Scrip
- Sudden Decrease of Sound Intensity Detection
- Sudden Increase of Sound Intensity Detection
- Tailing
- Temperature Alarm
- Temperature Difference Alarm
- Unattended Baggage (Detection)
- Using Mobile Phone
- Video Loss
- Video Tampering Detection
- Violent Motion
- Waiting Time Detection Alarm
- Wearing Sunglasses
- Whitelist Alarm
- Access Denied (Access point Remained Locked or Inactive)
- Access Denied (First Card Not Authorized)
- Access Denied by Card and Fingerprint
- Access Denied by Card and Password
- Access Denied by Card, Fingerprint, and Password
- Access Denied by Face
- Access Denied by Face and Card
- Access Denied by Face and Fingerprint
- Access Denied by Face and Password
- Access Denied by Face, Card, and Fingerprint
- Access Denied by Face, Password, and Fingerprint
- Access Denied by Fingerprint
- Access Denied by Fingerprint and Password
- Access Failed When Free Passing
- Access Granted by Card
- Access Granted by Card and Fingerprint
- Access Granted by Card and Password
- Access Granted by Card, Fingerprint, and Password

- Access Granted by Face
- Access Granted by Face and Card
- Access Granted by Face and Fingerprint
- Access Granted by Face and Password
- Access Granted by Face, Card, and Fingerprint
- Access Granted by Fingerprint
- Access Granted by Fingerprint and Password
- Access Timed Out by Card and Fingerprint
- Access Timed Out by Card and Password
- Access Timed Out by Card, Fingerprint, and Password
- Access Timed Out by Face and Card
- Access Timed Out by Face and Fingerprint
- Access Timed Out by Face and Password
- Access Timed Out by Face, Card, and Fingerprint
- Access Timed Out by Face, Password, and Fingerprint
- Access Timed Out by Fingerprint and Password
- Anti-Passback Server Respond Failed
- Anti-Passback Violation
- Barrier Obstructed
- Barrier Obstruction Recovered
- Calling Surveillance Center
- Card Number Expired
- Card Reader Tamper Alarm
- 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 Open (Door Contact)
- Door Open Timed Out (Door Contact)
- Door Open with First Card Ended
- Door Open with First Card Started
- Door Remained Unlocked by Keyfob
- Door Unlocked (Door Lock)
- Door Unlocked by Keyfob
- Duress Alarm
- Face Recognition Failed
- Face Recognition Terminal Offline
- Face Recognition Terminal Online
- Fingerprint Not Found
- First Card Authorization Ended
- First Card Authorization Started
- Force Accessing

- Intrusion
- Invalid Time Period
- Live Face Detection Failed
- Max. Card Access Failed Attempts
- Multi-Door Interlocking
- No Access Level Assigned
- No Card Number Found
- Passing Timeout
- Remaining Locked Status Ended
- Remaining Locked Status Started
- Remaining Unlocked Status Ended
- Remaining Unlocked Status Started
- Remote: Locked Access point
- Remote: Remained Locked (Credential Failed)
- Remote: Remained Unlocked (Free Access)
- Remote: Unlocked Access point
- Reverse Passing
- Secure Door Control Unit Tamper Alarm
- Tailgating
- Verifying Card Encryption Information Failed
- License Plate Matched Event
- License Plate Mismatched Event
- Face Matched Event
- Face Mismatched Event
- UVSS offline
- UVSS online
- Array Exception
- Camera/Recording Resolution Mismatch
- Device Armed
- Device Arming Failed
- Device Offline
- Device Reconnected
- Encoding Device Recording Exception
- Encoding Device Recording Recovered
- HDD Full
- Illegal Login
- R/W HDD Failure
- Video Standard Mismatch
- Active Infrared Intrusion Detector Exception
- AC Power Off
- AC Power On
- Battery Voltage Recovered
- CAN BUS Exception
- Communicated with IR Adapter Exception
- Communicated with Light Board Failed
- Connection Recovered with Anti-Passback Server

- Device Offline
- Device Online
- Device Tampered
- Disconnected with Anti-Passback Server
- Lane Controller Fire Input Alarm
- Lane Controller Tamper Alarm
- Low Battery Voltage
- Low Storage Battery Voltage
- Motor or Sensor Exception
- No Memory for Offline Event Storage
- Pedestal Temperature Too High
- Ac Power Down
- Alarm Cleared
- Arming/Disarming Failed
- Away Arming
- BUS Open-Circuit Alarm
- BUS Short-Circuit Alarm
- Control Panel Reset
- Device Armed
- Device Arming Failed
- 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
- Keypad Locked
- Keypad Unlocked
- Low Battery Voltage
- Stay Arming
- Telephone Communication Failed
- Virtual Zone Burglary Alarm
- Virtual Zone Fire Alarm
- Virtual Zone Panic Alarm
- Wired Network Disconnected
- Wireless Network Disconnected
- Wireless Network Exception

- 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
- Dock Station Offline
- Dock Station Online
- 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
- HDD Full
- 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
- Facial Recognition Server Offline
- Facial Recognition Server Online
- CPU Exception
- CPU Recovered
- CPU Warning

- RAM Exception
 - RAM Recovered
 - RAM Warning
 - System Service Abnormally Stopped
 - System Service Recovered to Run
 - User Login
 - User Logout
 - User-defined Event
 - Generic Event
 - Wrong-Way Driving
 - Illegal U-Turn
 - Driving on the Lane Line
 - Illegal Lane Change
 - Illegal Parking
 - Motor Vehicle on Non-Motor Vehicle Lane
 - Temperature Pre-Alarm
- iii. Time
- Last Hour
 - Today
 - Yesterday
 - Current Week
 - Last 7 Days
 - Custom Time Interval
- iv. Ability to check and export alarms and events
5. Video Search
- a. Ability to search for specific types of indexed video:
- i. Tag: Video that has been auto tagged or manually tagged at a certain timestamp
 - ii. Lock: Search only video that has been “locked” to not be overwritten by schedule
 - iii. Segment: Ability to search for up to 7 days of video averagely divided into segments from 1 to 100
 - iv. Interval: Ability to search for up to 7 days of video divided by intervals from 1 to 60 minutes or seconds
 - v. 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
 - vi. Search ATM event triggered video footage by the card number that is contained in the ATM information
 - vii. 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
- viii. Supports thumbnails
- ix. Ability to search main stream in all main storage
- x. Ability to search sub-stream in all main storage
- xi. Ability to search main stream in all auxiliary storage
- xii. Ability to search sub-stream in all auxiliary storage
- xiii. Ability to search the video files from Central System or Remote site
- b. VCA Search
 - Support Motion Detection
 - Support Line Crossing Detection
 - Support Intrusion Detection
 - Support reverse playback
 - Support downloading the searched video clips
 - Support displaying the video clips in the list or thumbnail mode
 - Support playing searched video clips in order
 - Support searching face picture and related video by picture
 - Support searching matched face picture and relate video
 - Support searching frequently appeared person's pictures
 - Support using the added person's face picture or upload one as desired
 - Support displaying the searched results in list mode or thumbnail mode
 - Support viewing large picture and the related video
 - Support downloading the current picture and video in the format of MP4, AVI and EXE
 - Support adding the person to the person list
- 6. Evidence Search
 - i. Set the following search conditions:
 - ID
 - Keywords
 - Evidence type
 - Organization on site
 - Result/conclusion
 - Evidence status
 - Uploading time
 - ii. Check the search result:
 - Name
 - ID
 - Type
 - Organization on site
 - Result
 - Status

- Description
 - Uploading time
 - iii. Check and download the content of evidence
7. Vehicle Search
- i. Support searching vehicles via ANPR camera or UVSS
 - ii. Support filtering vehicles via the marked/unmarked status, country/region, plate number, owner, or time
 - iii. Support searching vehicles with no license plate
 - iv. Support adding tag
 - v. Support viewing the label status, plate number, vehicle passing item, camera, owner, phone number, country/region of the vehicle
 - vi. Support adding the vehicle to vehicle list
 - vii. Support downloading the vehicle information and video
 - viii. Support viewing the captured vehicle picture, undercarriage picture, or related video
 - ix. Support exporting the searched vehicle records and downloading the related video
 - x. Support modifying the recognized license plate number
8. Identity Access Search
- i. Search access records
 - Support searching access control events
 - Support viewing access control event related video
 - Support viewing the person profile, card number, person name, ID, time, access point, access result, and access mode
 - Supports forgiving anti-passback violations
 - Support forgiving all the anti-passback violation events in the search result
 - Support downloading the searched person information
 - Support exporting card swiping records
 - ii. Perform entry & exit counting
 - Select one entry & exit counting rule
 - Select persons
 - Set time range
 - Set entry & exit counting type as people stayed/ people exited/all
 - View event details: profile, name, entry & exit counting type, phone number, location of last access
 - Display the access direction (entering/existing) of turnstile
 - Download single record
 - Export all searched records in excel format
9. Video Analysis
- a. People Counting
 - i. Ability to search network cameras enabled with people counting analytics to create reports based on Daily, Weekly, Monthly, Annual time intervals, or customize the time interval for a report
 - (a) View the people counting statistics of the people counting cameras in a line chart or histogram, and switch between line chart and histogram
 - (b) Ability to select the camera and set the report type and report time when exporting the detailed data of counting report
 - (c) Ability to select shorter time period to view more detailed data of each camera

- (d) Ability to export the detailed data of counting report in CSV /Excel format
 - (e) Ability to search the video linkage by month, date, week, hour, and play corresponding video to check people counting
 - (f) Ability to display up to 20 people counting cameras with different colors in people counting report of entry/exit
 - (g) Ability to view entered/exited/both entered and exited statistics
 - (h) Ability to show/hide data of certain cameras
 - (i) Ability to view both entered and exited statistics of single cameras
 - (j) Ability to play linked video of camera(s)
- b. Queue Analysis
- i. Ability to generate a report to show the number of queue exceptions and number of persons in each queue
 - ii. Ability to display the queue status including waiting duration and queue length
 - iii. Ability to generate the report as daily report, weekly report, monthly report, or annual report
 - iv. Ability to set the time period in the time field for statistics
 - v. 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
 - vi. Ability to set the queue length to display how many seconds each queue status lasts
 - vii. Ability to show/hide certain data of certain element
 - viii. Ability to view the report of the single queue, including the number of exceptions, number of people in queue, and waiting duration
 - ix. Ability to switch between number of exceptions, number of people, and queue length
 - x. Ability to set the report type and report time
 - xi. Ability to select shorter time period to view more detailed data of each queue
 - xii. Ability to select the queue exception, people amount exceeding, waiting timeout, person amount in queue, queue status to export
 - xiii. Ability to select the saving path
 - xiv. Ability to set the format as Excel or CSV
- c. Heat Map
- i. Ability to search network cameras enabled with heat map analytics to create reports with thermal graphics of heat generated in images, based on Daily, Weekly, Monthly, and Annual time intervals
 - ii. Ability to calculate people dwell time and people amount
 - (a) Ability to export heat map report in PDF/EXCEL format
- d. Pathway analysis
- i. Ability to calculate the number of people walking by
 - ii. Set the time as daily, weekly, monthly, annually, or custom time interval
 - iii. Generate the report to view the line chart or heat map of the people amount
- e. Temperature
- i. Ability to display the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry points on different presets
 - ii. Ability to select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report
 - iii. Ability to show/hide certain data of preset or thermometry point
 - iv. Ability to display temperature report of single preset

- v. Ability to display temperature report of single thermometry point
- vi. Ability to display the number of exceptions that the temperature at this thermometry point is higher or lower than the pre-defined temperature
- vii. Ability to display the maximum/minimum temperature at this thermometry point during the set time period
- viii. Ability to select the camera and preset, and set the report type and report time
- ix. Ability to select shorter time period to view more detailed data
- x. Ability to export the number of exceptions on temperature of each thermometry point
- xi. Ability to export the maximum temperature and minimum temperature of each thermometry point
- xii. Ability to set the saving path of the report
- xiii. Ability to export the report in the format of EXCEL or CSV
- f. Vehicle Analysis
 - i. Ability to display the number of passing vehicles detected by the specified cameras during specified time period
 - ii. Ability to select up to 20 ANPR camera for statistics at the same time
 - iii. Ability to select the report type as daily, weekly, monthly, annual report or customize the time interval
 - xiv. Ability to select shorter time period to view more detailed data
 - iv. Ability to customize the saving path of the report
 - v. Ability to export the report in the format of EXCEL or CSV

10. Health Monitoring

- a. 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.
- b. Overview: Provide status of the following devices and the ability to click on items for a detailed report:
 - i. Set auto refresh or refresh manually
 - ii. Display health monitoring on smart wall (graphic card)
 - iii. Display health monitoring on auxiliary screen
 - iv. Offline/total number of cameras
 - v. Number of camera with video loss
 - vi. Number of camera with communication exception
 - vii. Number of camera with recording exception
 - viii. Number of camera with no recording schedule
 - ix. Number of camera with arming exception
 - x. Abnormal/total number of access points
 - xi. Offline/total number of UVSS(s)
 - xii. Offline/total number of Remote Sites
 - xiii. HikCentral Professional Service status
 - Management server status
 - Memory status
 - CPU status
 - RAM status

- Network status
 - Streaming gateway usage
 - Picture storage usage
- xiv. Recording Server status
 - xv. Facial Recognition Server status
 - xvi. Application Data Server status
 - xvii. Application Data Standby Server status
 - xviii. Number of streaming server with exception
 - xix. Number of streaming server with notice
 - xx. Number of normal streaming server
 - xxi. Total number of streaming server
 - xxii. Number of recording server with exception
 - xxiii. Number of recording server with notice
 - xxiv. Number of normal recording server
 - xxv. Total number of facial recognition server
 - xxvi. Number of facial recognition server with exception
 - xxvii. Number of facial recognition server with notice
 - xxviii. Number of normal facial recognition server
 - xxix. Abnormal/total number of Encoding Devices
 - xxx. Abnormal/total number of Access Control Devices
 - xxxi. Offline/total number of Decoding Devices
 - xxxii. Abnormal /total number of Security Control Devices
 - xxxiii. Abnormal /total number of dock station
- c. Camera of Central System: Provide the status of the followings:
 - i. Name
 - ii. Address
 - iii. Area
 - iv. Connection number
 - v. Net status
 - vi. Video signal
 - vii. Recording status
 - viii. Arming status
 - ix. Operation: Refresh to get the real-time status immediately of the camera; go to logical view of the camera
 - d. Camera of Remote Site: Provide the status of the followings:
 - i. Name
 - ii. Address
 - iii. Area
 - iv. Net status
 - v. Recording Status (in Central System)
 - vi. Arming status
 - vii. Operation: Refresh to get the real-time status immediately of the camera; go to logical view of the camera
 - e. Access point: Provide the status of the followings:
 - i. Name
 - ii. Access Control Device
 - iii. Area
 - iv. Access Control Device net status

- v. Face Recognition Terminal Network status
- vi. Door status
- vii. Configured Door status
- x. Operation:
 - Refresh to immediately get the real-time status of the Door
 - Control door status as: Unlock/Lock/Remain Unlocked/Remain Locked
- f. UVSS: Provide the status of the followings:
 - i. Name
 - ii. Address
 - iii. Area
 - iv. Net status
 - v. Line Scan Camera status
 - vi. Capture Camera status
 - vii. Storage status
 - viii. Operation:
 - Refresh to immediately get the real-time status of the UVSS
 - Go to logical view of the unit
- g. Remote Site: Provide the status of the followings:
 - i. Name
 - ii. Version
 - iii. Address
 - iv. Net Status
 - v. Default Stream
 - vi. Operation:
 - Refresh to immediately get the real-time status of the site
 - Switch the device accessing mode between automatically judge or proxy
 - vii. Restore All Network Connections
 - viii. Switch stream type between main stream, sub-stream, smoothing or default stream type
- h. Recording Server: Provide the status of the followings
 - i. Name
 - ii. Address
 - iii. Type
 - iv. Net status
 - v. CPU usage
 - vi. RAM usage
 - vii. Hot Spare Property
 - viii. Recording status
 - ix. Hardware status
 - x. HDD status
 - xi. HDD usage
 - xii. Operation
 - Refresh to immediately get the real-time status of the Recording Server
- i. Facial Recognition Server
 - i. Name
 - ii. Address
 - iii. Type

- iv. Net status
- v. CPU usage
- vi. RAM usage
- vii. Operation:
 - Refresh to immediately get the real-time status of the server
- j. Streaming Server: Provide the status of the followings
 - i. Name
 - ii. Address
 - iii. Total streams
 - iv. Incoming streams
 - v. Outgoing streams
 - vi. Net status
 - vii. CPU Usage
 - viii. RAM Usage
 - ix. Operation:
 - Refresh to immediately get the real-time status of the Streaming Server
- k. Encoding Device: Provide the status of the followings
 - i. Name
 - ii. Address
 - iii. Device Serial No.
 - iv. Version
 - v. Net status
 - vi. HDD status
 - vii. HDD usage
 - viii. Recording status(Local Device)
 - ix. Default Stream
 - x. Access Protocol
 - xi. Hot spare property
 - xii. Arming status
 - xiii. RAID
 - xiv. Operation
 - Refresh to immediately get the real-time status of the device
 - Go to Logical View of the camera
 - xv. 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
 - xvi. Switch stream type of Encoding Devices in batch:
 - Main stream
 - Sub-stream
 - Smoothing
 - Default stream type
- l. Access Control: Provide the status of the followings:

- i. Name
 - ii. Address
 - iii. Device Serial No.
 - iv. Version
 - v. Net status
 - vi. Master/Slave lane controller network status
 - vii. Component status
 - viii. Battery status
 - ix. Arming status
 - x. Operation: Refresh to immediately get the real-time status of the Device; go to physical view of the device
- m. Security Control device: Provide the status of the followings:
- i. Name
 - ii. Address
 - iii. Device Serial No.
 - iv. Version
 - v. Net status
 - vi. Battery status
 - vii. Arming status
 - viii. Operation: Refresh to immediately get the real-time status of the Access Control Device
- n. Dock Station: Provide the status of the followings:
- i. Name
 - ii. Address
 - iii. Device Serial No.
 - iv. Version
 - v. Net status
 - vi. HDD status
 - vii. HDD usage
 - viii. Operation: Refresh to immediately get the real-time status of the decoding device
- o. Decoding Devices: Provide the status of the followings:
- i. Name
 - ii. Address
 - iii. Device Serial No.
 - iv. Version
 - v. Net status
 - vi. Manufacturer
 - vii. Operation: Refresh to immediately get the real-time status of the decoding device
- p. Display host server and spare server when hot spare function is enabled
11. Tools
- a. Smart Wall
- i. Shall synchronize the logging mode with the video surveillance client
 - ii. Shall refresh and synchronize the smart wall information
 - iii. Shall select camera or signal source as the encoding device type
 - iv. Shall add view and view group, edit view name and view group name, and delete view and view group
 - v. Shall support auto-switch of views belonging to the same view group, and set time interval between views

- vi. Shall save views, and sort views via created time or manually
- vii. Shall create a roaming window, adjust window size, enlarge window, and display window on top layer
- viii. Shall view the camera status, switch stream type, enable PTZ control, switch to playback, or stop decoding and displaying during live view on smart wall
- ix. Shall support window division of up to 36 windows, window jointing, and display/hide the window ID for Keyboard usage
- x. Shall view, download and print the window No. and camera ID
- xi. Shall enable auto-switch stream type and view window No. and camera ID
- xii. Shall lock/unlock the selected window
- xiii. Shall decode and display a Remote Site's cameras and current site's cameras on the smart wall for the functions of live view, playback, and displaying related video of alarm
- xiv. Shall display live view of cameras of added video security control panels and video access control terminals
- xv. Shall support PTZ control, auto-switch stream type, switching to sub-stream manually, and stopping decoding manually
- xvi. Shall display alarm-related video on smart wall, and mark on the alarm window
- xvii. Shall query smart wall logs
- xviii. Shall display one smart wall in the center, or up to three walls side-by-side
- xix. Shall switch to alarm center to check alarm list
- b. Quick icon to download or open standalone VSPlayer
- c. Broadcast: Ability to do a general audio announcement to all audio-enabled network cameras and end devices
- d. Alarm Output Control: Ability to turn on/off the alarm outputs of the connected camera
- e. Two-Way Audio: Ability to select camera with audio in/out and receive and send audio communications between the Control Client and the camera

12. Management

- a. Download Center: Ability to view status of all video files being exported
 - i. Start (all)
 - ii. Stop (all)
 - iii. Delete all
 - iv. Download (VS) Player
 - v. Set download time as 00:00-06:00, 06:00-12:00, 12:00-18:00, 18:00-24:00, or custom time settings
 - vi. View the status of video files uploading :
 - Start all
 - Stop all
 - Delete all
 - Download player
 - vii. View the status of video files downloaded:
 - Save as
 - Delete
 - Download player
- b. Local Picture Management:
 - i. Ability to easily browse snapshots that have been stored in accessible Windows file folders

- ii. Ability to save, print, or delete the captured pictures
 - c. Local Recording management:
 - i. Ability to easily browse video clips that have been stored in accessible Windows file folders
 - ii. Ability to save or delete the video clips
 - d. Basic Settings:
 - i. General settings: support the following settings:
 - Shall set global stream as main stream, sub-stream or smooth stream
 - Shall set threshold for main/sub-stream as 1/2, 1/4, 1/9, 1/16, 1/25, 1/36, 1/64
 - Shall set the default waiting time for the Control Client as default value, default value \times 1.5, or default value \times 2
 - Shall set picture format as JPEG or BMP
 - Shall set the maximum mode as Full Screen or Maximize
 - Set time zone as client time or device time
 - Enable time difference
 - Set bandwidth to affect downloading from pStor
 - Shall enable Auto-login
 - Shall resume last interface
 - Shall enable display window No.
 - ii. Image Settings
 - Shall set the view scale in live view or playback as Full Screen or Original Resolution
 - Shall set the window scale as 4:3 or 16:9
 - Shall set video caching as small(1 frame), medium(6 frames) or large(15 frames)
 - Shall decode continuously when switching between one window and multiple windows after enabling continuous decoding
 - Shall set video caching parameters based on network performance, computer performance, and bit rate. Larger frame caching will result in better video performance
 - Shall support GPU decoding
 - Shall display overlay transaction information to view ATM transaction information in live view and playback
 - Shall display overlay transaction information on the live view and playback
 - Shall display overlay temperature information on the live view and playback
 - Shall display the VCA rule in the live view and playback
 - iii. 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
 - e. Support the operation of Network keyboard and joystick to live view and playback
 - f. Support configuring alarm sound to enable voice engine or local audio files
 - g. Support setting 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
13. Audit Trial: search and view logs for the following
- a. Server Logs
 - i. Error Log, see 0 Table 1: Error
 - ii. Warning Log, see 0 Table 1: Error
 - iii. Information Log, see 0 Table 1: Error
 - b. Device Logs

- i. Alarm Log: see 0 Table 4: Encoding Device Logs -Alarm
- ii. Exception Log: see 0 Table 5: Encoding Device Logs – Exception Log
- iii. Operation Log: see 0 Table 6: Encoding Device Logs -Operation Log
- iv. Information Log: see 0 Table 7: Encoding Device Logs - Information Log
- v. Alarm Log: see 0 Table 4: Encoding Device Logs -Alarm
- vi. Exception Log: see 0 Table 5: Encoding Device Logs – Exception Log
- vii. Operation Log: see 0 Table 6: Encoding Device Logs -Operation Log
- viii. Information Log: see 0 Table 7: Encoding Device Logs - Information Log
- c. Search logs by the following sources:
 - i. User
 - ii. HikCentral Professional Server
- d. Log searches are based on operation, user, and time interval searches of:
 - i. Today
 - ii. Yesterday
 - iii. Current week
 - iv. Last 7 days
 - v. Last 30 days
 - vi. Custom time interval

Mobile Client

- A.** Mobile Client is an App on a smart phone or tablet (Apple iOS or Android) for security operators to access the platform remotely via LAN, WAN or Internet. It shall provide multiple operating functionalities, including real-time live view, PTZ control, video playback and alarm notification
- B.** System Requirements:
 - 1. Hardware: Dual-core CPU with 1.5 GHz or above, and at least 2G RAM
 - 2. Software: Android 4.1 or higher versions/iOS 9.0 or higher versions
- C.** On initial log in, users must enter the SYS's IP and port number in the server address box
- D.** Users shall be able to log in with HTTP or HTTPS transfer protocol
- E.** Shall support 18 languages, including Chinese, English, Russian, Bulgarian, Hungarian, German, Italian, Czech, French, Dutch, Portuguese, Spanish, Danish, Finnish, Turkish, Traditional Chinese, Thai, Japanese
- F.** Mobile Client shall have the following modules and functions:
 - 1. Ability to modify 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
 - 8. Ability to view logical area of the current site or Remote Sites
 - 9. Ability to display logical areas, and the thumbnail of cameras in each area
 - 10. Ability to add tag during playback
 - 11. Ability to add person to face comparison group
 - 12. Ability to mark the days with recorded videos on the calendar when setting the time to start playback

13. Ability to display resources by resource types (camera, door or UVSS) or displaying all the resources in the Favorites
14. Ability to filter to display the resources of cameras or access points
15. Ability to search passing vehicles log for HD version via category (camera by default), time, country, mark status, vehicle plates, and owner
16. Ability to support multiple time zones for searching recording files, alarm logs, and heat map reports
17. Logical Resources: Ability to switch between Live View and Playback
 - a. Live View:
 - i. Ability to add/delete cameras for multiple view, and view up to 8 cameras simultaneously
 - ii. Ability to set 1/4/9 window division for tablet
 - iii. Ability to switch to saved view pattern
 - iv. Ability to view real-time video from stream encryption device
 - v. Ability to view real-time video from the Under Vehicle Surveillance System's related camera (only for tablet)
 - vi. Ability to play the live videos or video footage of multiple resources simultaneously
 - vii. Ability to view real-time video from the access point's related camera(s)
 - viii. Ability to lock/unlock/remain locked/remain unlocked access point manually(include turnstile and face recognition terminal)
 - ix. Ability to display persons' real-time access records, including person profile, person name, and access results
 - x. Ability to view the recognized passing vehicle information, including license plate number and passing time
 - xi. 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)
 - xii. Ability to mark on the captured real-time undercarriage picture (only for tablet)
 - xiii. Ability to add new vehicle to the vehicle list
 - xiv. Ability to view the person's face comparison information (real-time and history), including captured face picture, person details, captured time, and similarity
 - xv. Ability to add mismatched person into person list
 - xvi. Ability to trigger user-defined event manually
 - xvii. Ability to subscribe all access and face comparison events(only for tablet)
 - xviii. Ability to switch cameras if the access control point links two cameras
 - xix. Has the following functions available on tile toolbar for easy access:
 - Upload the generic event during live view
 - Toggle the settings between 1, 4, 9 tiles (only for tablet)
 - Stop/recover all the live views
 - Capture: ability to save snapshots, and share the captured pictures via email
 - Preview the captured picture and recorded video footage
 - Enable manual recording of displayed cameras, and share the manual recording files via email
 - Switch on/off audio
 - Enable and utilize two-way audio
 - Digital zoom
 - Switch between sub-stream and main stream

- Add the camera/view to Favorites/View
 - PTZ control
 - Start/stop the auto-scan
 - Zoom +/-
 - Focus +/-
 - Iris +/-
 - Manage presets
 - 3D positioning
 - Fisheye dewarping
 - Ability to live view in full-screen mode
- b. Playback
- i. Ability to playback 1 to 4 cameras simultaneously for tablet
 - ii. Ability to playback up to 1 camera simultaneously for phone
 - iii. Ability to playback video from stream encryption device
 - iv. Ability to stop playback of all cameras in one step or one by one
 - v. Ability to choose date and storage location for playback
 - vi. Ability to search cameras for playback by name or choose cameras added to Favorites
 - vii. Ability to restore the playback interface when the user logs out
 - viii. Ability to switch the window for playback
 - ix. Ability to search Logical Area/Access point/Camera via key words
 - x. Ability to support synchronous playback
 - xi. Ability to playback the cameras of Remote Sites
 - xii. Ability to support VCA search (only for tablet)
 - xiii. Ability to add person into Person List (only for tablet)
 - xiv. 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)
 - xv. Ability to add/delete/edit tags and search video via tags (only for tablet)
 - xvi. Ability to playback single camera in full-screen mode
 - xvii. Has the following functions available on camera playback tile toolbar for easy access:
 - Capture: ability to save snapshots
 - Clipping: ability to quickly create and export video clip
 - Pause the playback
 - Digital Zoom
 - Add tag during Playback
 - Switch the playback speed to 1/4X, 1/2X, 1X, 2X and 4X
 - Stop/resume the playback
 - Switch on/off audio
 - Fisheye dewarping
 - Locate the timeline of playback manually
 - xviii. Fisheye dewarping
 - xix. Activate on-screen PTZ controls
- c. Make the HD version's user interfaces of Live View and Playback page consistent with the phone version
- d. Search (only for tablet)
- i. Ability to search video: search tagged video and VCA event related video

- ii. Ability to search passing vehicle logs: search record of the passing vehicle, and view the vehicle details
 - iii. Ability to search access records: search the persons' access records and view the access details including person details and access point information
 - iv. Ability to add person to person list
 - e. Camera: Ability to show the following camera information and functions:
 - i. Net status
 - v. PTZ control permission
 - vi. Area name
 - vii. Live view
 - viii. Playback
 - ix. Add/remove to/from Favorites
 - f. Favorites
 - Ability to manage frequently checked cameras
 - Display the mixed list of camera, door and UVSS or list of some specific resources
 - g. Picture and Video
 - i. Ability to manage pictures and video clips manually captured or clipped in Live View and Playback
 - View or play
 - (a) Capture a picture of the playback video
 - (b) Pause the playback
 - (c) Switch on/off audio
 - (d) Play back in full screen
 - ii. Send via email
 - iii. Share to social Apps
 - iv. Export the captured pictures to the local system of iOS client
 - v. Delete
 - h. Supports sub-areas in the resource tree
18. View
- i. View the favorites list of cameras and access points
 - ii. View the saved views list, and Live View or Playback the resources of the views
 - iii. View the Live View and Playback of the views
 - iv. View public view/private view
19. Alarm
- a. Alarm Notification: Ability to receive pop-up alarm notifications
 - i. Alarm notification includes the following information:
 - (a) Alarm type
 - (b) Alarm time
 - (c) Live view of the camera
 - (d) Playback of the camera
 - b. Alarm Information: Ability to check and manage alarm history information
 - i. Alarm messages shall include the following information:
 - (a) Alarm priority
 - (b) Alarm category
 - (c) Alarm source
 - (d) Alarm time
 - (e) Alarm name
 - (f) Whether acknowledged

- (g) Server time
- (h) Triggering event
- (i) Acknowledge information
- ii. Alarm center has the following functions:
 - (a) Refresh to check latest alarm information
 - (b) Filter alarm by time, marking status, alarm priority, alarm category and alarm status
 - (c) Switch to show marked/unmarked alarm only
 - (d) Mark alarm message
 - (e) Live view and playback the related video
- iii. Filter from and display the following alarm types:
 - (a) Normal alarm
 - (b) ANPR alarm
 - (c) UVSS alarm
 - (d) Face comparison alarm
 - (e) Access control alarm
 - (f) Log in/out alarm
 - (g) Generic alarm
 - (h) Server alarm
 - (i) Alarm information from security control devices
- iv. 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.

20. Video Analysis(only for tablet)

- i. Ability to generate people counting report and filter the specific information
- ii. Ability to generate queue analysis report and filter the specific information
- iii. Ability to generate temperature report and filter the specific information
- iv. Ability to generate vehicle analysis report and filter the specific information
- v. Ability to support Heat Map reports

21. Map(only for tablet)

- i. Ability to show the related map of the alarm
- ii. Ability to show resource and view the details when click the icon
- iii. Ability to switch e-map
- iv. Ability to filter according to resource type
- v. Ability to view live view of a single/multiple resource(s)
- vi. Ability to search, then jump to the pointed place
- vii. Ability to add label to map
- viii. Ability to view history alarm
- ix. Ability to perform access control
- x. Cross-site map display and operation

G. Other Functions

1. Basic Information

- a. Ability to check the current account information
 - i. User name
 - ii. Login mode
 - iii. Server information
 - iv. Server address
 - v. Server version

- b. Ability to rename server alias
 - c. Ability to view the account list
 - d. Ability to logout
 - e. Ability to upload person information
 - f. Ability to switch between the following accessing device modes when performing live view or playback:
 - i. Restore default
 - ii. Automatically judge
 - iii. Directly access
 - iv. Proxy
 - g. Ability to enable GPU decoding
 - h. Ability to show network traffic data used in the following environments:
 - i. Mobile Network
 - ii. Wi-Fi
 - i. Ability to mark logical areas with sub-areas
2. About
- a. Ability to show the current App version
 - b. Ability to show new features of the current version
 - c. Ability to update to the latest version

Keyboard

- A.** Shall login to HikCentral Professional by inputting the IP address, KPS port, HikCentral Professional user name and password
- B.** Shall login to HikCentral Professional by HTTP/HTTPS
- C.** Shall view the logical areas of Remote Sites and current sites
- D.** Shall select the window to decode cameras of Remote Sites and the current site for live view
- E.** Shall support the PTZ function of Light, Wiper, Focus, Iris, Zoom, and control PTZ permissions and release PTZ permissions via the logged user
- F.** Shall split windows (only for DS-1100KI, DS-1600KI and DS-1200KI)
- G.** Shall support using the saved preset, patrol, and pattern (only for DS-1600KI, DS-1100KI and DS-1200KI)
- H.** Shall support 3D PTZ function
- I.** Shall set preset (only for DS-1600KI) and pattern(only for DS-1600KI), and auto-scan
- J.** Shall display wall list on the keyboard (only for DS-1600KI)
- K.** Shall switch views saved in Smart Wall, and refresh logical area (only for DS-1600KI)
- L.** Shall enlarge and restore windows (only for DS-1600KI)
- M.** Shall roam windows (only for DS-1100KI and DS-1600KI)
- N.** Shall display graphic card screen, live view on screen, PTZ control and fisheye dewarping (only for DS-1005KI)

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™ i5-4590 @3.3 GHz
- B. RAM 8 GB
- C. Network GbE network interface card
- D. Graphics Card NVIDIA® GeForce® GTX 970
- 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 Windows 7 64 bit

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

- A. Minimum PC Intel® Core™ i5-4590 @3.30 GHz 3.30 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 Windows 8.1 64-bit

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

- A. Minimum PC Intel® Xeon® E3-1220 V5 @3.00 GHz 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 Windows Server 2012 (R2) 64-bit

2.8. PC Requirements (for Streaming Server)

- A. Minimum PC Intel® Core™ i5-4590 @3.30 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

END OF SECTION

Part 3 Execution

3.1 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.

3.2 Preparation

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

3.3 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.

3.4 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.

3.5 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.

3.6 Demonstration

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

END OF SECTION

Appendix

4.1 Server Logs

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

Table 1: Error

The Error Log shall be searchable by the following subcategories:

Acknowledging Alarm Failed	Activating License Failed	Adding Access Control Device	Add Application Data Server Error	Adding Access Point Failed
Adding Anti-Passback Rule Failed	Adding Decoding Device Failed	Add Entry & Exit Counting Rule Failed	Adding Encoding Device Failed	Adding Facial Recognition Server Error
Adding Multi-door Interlocking Rule Error	Adding Recording Server Failed	Adding Smart Wall Failed	Adding Streaming Server Failed	Adding UVSS Failed
Adding Tag Failed	Adding View for Smart Wall Failed	Adding View Group for Smart Wall Failed	Adjusting Screen Brightness Failed	Adjusting Order of Smart Wall Views
Adjusting Screen Contrast Failed	Adjusting Screen Resolution Failed	Adjusting Screen Saturation Failed	Alarm Output Operation Failed	Answering Call Failed
Arming /disarming in Live View Failed	Arming Failed	Backing Up Access Events 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	Creating Roaming Window Failed
Data Backup Plan Failed	Database Backup Right Now Failed	Database Restore Failed	Deactivating License Failed	Deleting Decoding Device Failed
Deleting Roaming Window Failed	Deleting Smart Wall Failed	Deleting View for Smart Wall Failed	Deleting View Group for Smart Wall Failed	Digital Zoom in Live View Failed
Digital Zoom in Playback Failed	Disarming Failed	Displaying Alarm on Smart Wall Failed	Displaying Window on Top Layer Failed	Editing Decoding Device Failed
Editing Smart Wall Failed	Editing View for Smart Wall Failed	Editing View Group for Smart Wall 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	Fast Forward Playback on smart wall Failed

Fisheye Expansion in Live View Failed	Fisheye Expansion in Playback Failed	Getting Recording Schedule on Camera Error	Going to VCA Search in Live View Failed	Going to VCA Search in Playback Failed
Instant Playback 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	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
Remaining Door Locked Failed	Remaining Door Unlocked 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 Decoding Output Resolution Failed
Slow Forward Playback on Smart Wall Failed	Start Preview Record Failed	Starting Auto-Switch of Smart Wall Views Failed	Starting Camera Auto-Switch on Smart Wall Failed	Start Clipping in 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	Stopping All Live Videos on Smart Wall Failed
Stopping Auto-Switch of Smart Wall Views 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	Switching Stream in Live View Failed	Switching Live View on Smart Wall via Network Keyboard Failed	Switching Stream in Live View Failed	Switching Stream for Smart Wall Failed
Switching View	Switching View	Transcoding	Two-way Audio in	Unlinking

for Smart Wall Failed	via Network Keyboard Failed	Playback Failed	Live View Failed	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
Window Division Failed				

Table 2: Warning

The Warning Log shall be searchable by the following subcategories

License Expired			
-----------------	--	--	--

Table 3: Information

The Information Log shall be searchable by the following subcategories

Acknowledge Alarm	Activate Access Control Device	Activate Device	Activate License
Activate Online Device	Activate Recording Server	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 Attendance Check Point	Add Attendance Group	Add Camera Element	Add Card to Person
Add Decoding Device	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 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 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 Linked Holiday for Shift Schedule	Add Map	Add Map Label
Add Member to Dock Station	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 in Attendance Group	Add Person Profile	Add Person to Access Group	Add Person to Face Comparison Group
Add Recording Schedule	Add Recording Server	Add Recording Template	Add Related Camera to Access point
Add Remote Site	Add Report	Add Role	Add Security Control Device
Add Shift Schedule	Add Site to GIS Map	Add Smart Wall	Add Streaming Server
Add UVSS	Add User	Add User-Defined Event	Add Vehicle
Add Vehicle List	Add Video Copy-back Schedule for Dock Station	Add Video Tag	Add View
Add View Group	Adjust Screen Brightness	Adjust Screen Contrast	Adjust Screen Definition
Adjust Screen	Alarm Arming	Alarm Disarming	Alarm Input Bypass

Saturation			Recovered
Alarm Input Bypassed	Apply Access Control Applications	Apply Face Comparison Group to Device and Link Camera	Apply Hot Spare Settings to NVR
Arming/Disarming in Live View	Assign Access Level to Access Group	Assign Door to Access Level	Assign Shift Schedule to Attendance Group
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 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 Attendance 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	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 Group	Delete Camera Element	Delete Customized Additional Information
Delete Decoding Device	Delete Defense Schedule Template	Delete Device Upgrade Schedule	Delete Dock Station
Delete Dock Station Group	Delete Door	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 Generic Event	Delete Holiday
Delete Hot Region	Delete Hot Spare for NVR	Delete Hot Spot	Delete Icon
Delete Linked Holiday for Shift Schedule	Delete Map	Delete Map Label	Delete Member from Dock Station Group
Delete Multi-Door Interlocking Rule	Delete N+1 Hot Spare	Delete Partition	Delete Pathway
Delete Permission Schedule Template	Delete Person	Delete Person's Card	Delete Person's Fingerprint
Delete Person Additional Information	Delete Recording Schedule	Delete Recording Server	Delete Recording Template
Delete Remote Site	Delete Report	Delete Roaming Window	Delete Role
Delete Security Control Device	Delete Shift Schedule	Delete Smart Wall	Delete Streaming Server
Delete UVSS	Delete User	Delete User-Defined	Delete Vehicle

		Event	
Delete Vehicle List	Delete Video Copy-Back Schedule for Dock Station	Delete Video Tag	Delete View
Delete View Group	Digital View in Live View	Digital View in Playback	Disable Face Credentials
Disarm All Partition of Security Control Panel	Disarm Partition	Display Alarm on Smart Wall	Display on Top Layer
Door Control: Close Door	Door Control: Open Door	Door Control: Remain Locked	Door Control: Remain Unlocked
Download Alarm Details	Download Events	Download Files from FTP	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 Group	Edit Attendance Group's Assigned Shift Schedule
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 Contact Information	Edit Customized Additional Information	Edit Decoding Device
Edit Defense Schedule Template	Edit Device Access Mode	Edit Dock Station	Edit Door
Edit Door in Access Level	Edit Door Related Camera	Edit Email Settings	Edit Email Template

Edit Customized Additional Information	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 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 Map	Edit Map Label
Edit Multi-Door Interlocking Rule	Edit N+1 Hot Spare	Edit Network Performance	Edit NTP Settings
Edit Online Devices Network Parameters	Edit Operation Recommendation	Edit Partition	Edit Pathway
Edit Permission Schedule	Edit Person	Edit Person Additional Information	Edit Person Card
Edit Person Fingerprint	Edit Person in Access Group	Edit Person in Attendance Group	Edit Person Profile
Edit Picture Storage	Edit Recognized Plate Number	Edit Recording Schedule	Edit Recording Server
Edit Recording Template	Edit Registering to Central System Settings	Edit Remote Site	Edit Report
Edit Retention Time of Data Recorded in System	Edit Role	Edit Security Control Device	Edit Server NIC Settings
Edit Service Status	Edit SFTP Settings	Edit Shift Schedule	Edit Shift Schedule's Assigned Attendance Group
Edit Site on GIS Map	Edit Smart Wall	Edit Streaming Server	Edit System Properties

Edit Temperature Unit	Edit Transfer Protocol to HTTPS	Edit UVSS	Edit URL of GIS Map API
Edit User	Edit Vehicle's Marking Status	Edit Vehicle List	Edit Video Copy-Back Schedule for Dock Station
Edit Video Tag	Edit View	Edit View Group	Edit WAN Access Settings
Email Test	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 Event/Alarm Logs	Export Attendance Records	Export Heat Map
Export Heat Values of Heat Map	Export Logs	Export Pathway Analysis Report	Export People Counting Report
Export Person Information	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	Get Camera's Recording Schedule	Get Camera Name	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 Persons from Device	Get Queue Report from Camera	Get Temperature Report
Get Vehicle Report	Import Vehicle Information	Input Person Additional Information	Instant Playback
Link Decoding	Link Dock Station	Link Domain Group	Link Domain Group

Output	Group with Dock Station	with Access Group	with Attendance Group
Link Domain Group with Face Comparison Group	Link Person's Additional Information with Person Information in Domain	Lock	Lock All Doors
Lock Video in Playback	Log Search	Manual Update Resource	Manually Apply Access Levels
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: 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 Area Auto-Switch	Pause Auto-Switch in Custom View	Pause Auto-Switch of Live View on Smart Wall
Pause Playback on Smart Wall	Play in the Specific Window on Control Client	Play in the Specific Window on Smart Wall	PTZ Control
PTZ in Live View	Push Subscription	Reboot Access Control Device	Record Fingerprint from Device
Recover All Doors	Recover Arming	Remove Door from	Remove Door from

		Access Level	Anti-Passback
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 Attendance Group	Remove Person from Face Comparison Group
Remove Related Camera for Door	Remove Shift Schedule from Attendance Group	Remove Site from GIS Map	Reset Network Information
Reset Online Device Password	Restore All Settings	Reset User Password	Restore Default Settings
Restore Roaming Window	Restore Sub Window	Restore User	Restore User Password
Reset Area Auto-Switch	Resume Area Auto-switch	Resume Auto-switch in Custom View	Resume Auto-switch of Live View on Smart Wall
Resume Playback on Smart Wall	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 Card Reader Access Mode	Set Card Reader Parameters
Set Custom Wiegand	Set Decoding Output Resolution	Set Door Parameters	Set Free Access Schedule
Set Network Parameters	Set Opening Door with First Card Parameters	Set Person's Access Group	Set Time for Auto-Apply Access Levels
Set Time Parameters	Slow Forward Playback on Smart	Start Area Auto-switch	Start Auto-switch in

	Wall		Custom View
Start Auto-switch of Live View on Smart Wall	Start Downloading Video Files	Start Live View	Start Live View of Door Related Camera
Start Live View of Local Signal Source on Smart Wall	Start Live View on Smart Wall	Start Playback	Start Playback on Smart Wall
Start Recording in Live View	Start Remote Playback Recording	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 Live View	Stop Live View of Door Related Camera	Stop Live View of Local Signal Source on Smart Wall
Stop Playback	Stop Playback of Door Related Camera	Stop Playback on Smart Wall	Stop Recording in Live View
Stop Recording in Playback	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
Synchronize Camera Name	Synchronize Domain Users	Synchronize Door Name	Synchronize Partition
System Settings on Control Client	SYS Stopped	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	Unactive License
Unlink Decoding	Unlink Dock Station Group with Dock	Unlink Person's Additional Information	Unlock

Output	Station	with Person Information in Domain	
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	Window Division	Add Fuzzy Matching Rule	Edit Fuzzy Matching Rule
Delete Fuzzy Matching Rule	Collect Face by Device		

4.2 Device Logs

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

Table 4: 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	License Plate	Line Crossing	Line Crossing

Recognition Started	Recognition Stopped	Detection Started	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 Sopped	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			

Table 5: 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			

Table 6: Encoding Device Logs -Operation

The Operation Log shall be searchable by the following subcategories

Add Plan	Add Scene	Add Signal Source	Adjust Volume
Bring Video Wall Window to Back	Bring Video Wall Window to Front	Cancel Master Screen of Video Wall	Cancel Slave Screen of Video 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 Video Wall Connection	Get Video 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 Blacklist & Whitelist	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 Blacklist & Whitelist	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 Whitelist
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	Remote: Add Working	Remote: Alarm Output	Remote: Arm

Storage Pool	Device	Triggering	
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 Blacklist & Whitelist
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 Blacklist & Whitelist	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 Whitelist	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 Video Wall	Set OSD
Set Output Resolution	Set Remote Playback	Set Single Scene	Set Slave Screen of Video Wall
Set Transparency	Set Two-way Audio Record	Set User Configuration	Set User Password
Set Video Wall Connection	Set Video Wall Scene	Shutdown	Start Auto-Switch Decoding
Start Dynamic Decoding	Start Passive Decoding	Start PPPoe Connection	Stop Auto-Switch Decoding
Stop Dynamic Decoding	Stop Passive Decoding	Stop PPPoe Connection	Stream Compression Configuration
Switch Scene	Upload Background Picture	Upload Logo	VCA Configuration
Video Wall Display Area Setup	Window Control	Other	

Table 7: 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	

4.2 Security Control Device Log

Table 8: 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	Environment Acquisition Device	Gas Detection Alarm	Gas Detection Alarm

Alarm	Alarm Restored		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		

Table 9: 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			

Table 10: 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 Sound	Upgrade Sub-board
Whitelist Settings	Wi-Fi Settings	Zone Tamper-proof Settings	Other

Table 11: 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		