A&E System Specification

HikCentral

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 Video Surveillance Management Service

1. A Video Surveillance Management Service (VSM) that centrally manages Network Video Recorders (NVRs), Digital Video Recorders (DVRs), Hybrid Storage Area Networks (Hybrid SANs), Cloud Storage Servers, Access Control Devices, UVSSs, Doors and network cameras via an IP-based network.

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.	VSM	Video Surveillance Management
53.	WB	White Balance
54.	WDR	Wide Dynamic Range

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 VMS (Video 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 – shall be designed to manage distributed sites or large groupings of cameras recording on NVRs, DVRs, Hybrid SANs, and Cloud Storage Servers.

2.2. Description

A. HikCentral Video Surveillance Management Service:

1. VSM 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 VSM
   d. Imports up to 3,000 alarm inputs/outputs respectively per VSM.

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

1. HikCentral Video Surveillance 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 VSM and third-party device
   b. HikCentral 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
   c. HikCentral Streaming Gateway
      i. A component of VSM 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. Communicates with VSM
   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 VSM 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 VSM via LAN, WAN, or Internet
3. Mobile Client: Basic security operator features shall be accessed through the Mobile Client connected to VSM 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

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 VSM 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
        - IP Segment
        - Port Segment
        - Batch Import
        - Add online devices in the same local subnet with the Web Client using Search Active Device Protocol (SADP)
    b. Add camera to area
    c. Select Streaming Server for the area
    d. Select video storage location for the camera
    e. Get device’s local recording settings
    f. View the following detailed information of the added devices:
        - Alias

        - Address
        - Serial number
        - Available cameras
        - Alarm I/O
        - Network status
        - Password
    g. Refresh the status of the added devices
    h. Set remote configuration of the added devices
    i. Activate the online devices
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
        - IP Address
        - IP Segment
        - Port Segment
        - Batch Import
    b. Add doors to area
    c. Synchronize door name
    d. Set remote configuration of the added devices
    e. Refresh the status of the added devices
    f. Reset device password (in batch)
    g. Activate the online devices
3. Add up to 64 Recording Servers and 64 Streaming Servers respectively to the VSM
4. Import service component certificate to Cloud Storage Server
5. Shall add Cloud Storage Server and Hybrid SAN as Recording Server
6. View storage information for the Recording Server, including used space and free space
7. View information of cameras configured to store video files in Recording Server:
    a. Camera name
    b. Area
    c. Site
    d. IP address
    e. Recording schedule
    f. Network status
8. 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. 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
11. 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
12. Once added, show the online/offline status of devices in both physical view and logical view
13. Shall remotely configure NVRs and network cameras and set all functions that are available

14. 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 will be displayed on a list
15. Shall enable WAN access for the Recording Server
16. Shall display channels in the same area in alphabetical order
17. Shall synchronize NVR channel names with the names displayed on the Web Client
18. Shall support the following functions of smart wall:
    a. Shall add up to 32 smart walls and display multiple smart walls
    b. Shall delete, edit, and view the added walls
    c. Shall access and control up to 32 decoding devices
    d. Shall add online decoding devices via SADP in the same local subnet with the Web Client or add decoding devices 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 automatically judge, LAN IP address, or WAN IP address
    g. Shall support the linkage between decoding device’s decoding outputs and smart wall windows
    h. Shall set role permission of smart walls, decoding devices, and windows
    i. Shall support alarm linkage of smart walls, select walls and windows for alarm linkage, and divide windows according to the number of alarms
    j. Shall support smart wall database backup and restoration via hot spare

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

1. A Remote Site is defined as a VSM or Blazer Express, and Blazer Pro managed through IP or domain name
2. HikCentral shall support 1,024 resources, including encoding devices, access control devices, and Remote Sites
3. HikCentral 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. After adding Remote Sites, channels shall display according to permission, and the Central System list will be the same as Remote Sites list
7. Support database backup of Remote Sites, up to 5 copies of database backup for each Remote Sites are supported, and saving paths cannot be edited
8. Import Remote Site alarms (support filtering by source, triggering event, and alarm priority)
9. Display Remote Sites in alphabetical order
10. Support logging in to Remote Sites and configuring Remote Sites
11. Synchronize Remote Site names in the Central System manually
12. Refresh Remote Site channels manually, after channels of Remote Sites are added or deleted, users can update the changes from the Remote Site
13. Synchronize channel names manually
14. Edit Remote Site names, IPs, ports, user names, passwords, and description information
15. Display site address, site port, alias, user name, system IDs, and version information
16. Configure GIS location of Remote Sites
17. View the Remote Site’s GIS location, hot spot, and hot region settings in Map module
18. Scheduled database backup and manual database backup
19. 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

20. 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 VSM, and up to 100,000 areas for remote site management
2. Add up to 64 cameras, doors, alarm inputs, alarm outputs, and UVSS respectively to one area and 3,000 in total per VSM
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 doors, including
    a. Name
    b. Address
    c. Access Control Device
    d. Access Control Device Status
    e. Door 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. Area
    e. 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. Shall support the functions of synchronizing 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. Shall support the functions of synchronizing door name, moving the door to other area, and displaying elements of sub-areas, copying the current door's specified parameters to other doors
10. Shall support adding alarm inputs/outputs, the functions of moving the inputs/outputs to other area, and displaying elements of sub-areas
11. Shall support the functions of moving the UVSS to other area, and displaying elements of sub-areas
12. Shall support switching and selecting the added sites, displaying channels of Remote Sites in logical view, and switching to logical view of the selected site when the RSM module is enabled,
13. Shall support importing cameras in logical view after channel updates of Remote Sites
14. Shall support reminding users of deletion and displaying offline devices after deleting channels on Remote Sites
15. Support importing areas of added cameras on Remote Sites into the Central System
16. Support copying configuration information of stream type, protocol type, main storage, and auxiliary storage to other channels
17. Shall 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
        - Stream type
        - 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 of current site
        - Select storage location as Hybrid Storage Area Network, Encoding Device, or Cloud Storage Server for cameras of current site
        - Select storage location as Hybrid Storage Area Network or Cloud Storage Server 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 configure event settings for cameras of current site
        - Select the triggering event
        - Trigger user-defined event

d. 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, door, site, UVSS, hot region, and label

e. Shall have the ability to configure GIS map settings of current site:
    - Shall add sites/cameras/doors/alarm inputs/alarm outputs/UVSSs on GIS map to show the geographic location
    - Shall add up to 4 UVSS(s) to each VSM
    - 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, door, site, UVSS, hot region, and label
    - Shall search geographic location in GIS map

18. Shall edit the following settings of doors for current site:

a. Basic information
    - Door name
    - Door magnetic sensor connection mode
    - Exit button type connection mode
    - Open duration(s)
    - Extended open duration(s)
    - Enable door open timeout alarm
    - Set maximum open duration(s)
    - Set duress code
    - Set super password
    - Set dismiss code
    - Set free access schedule to keep the door open

b. Related cameras
    - Link up to two camera(s) to the door

c. Application
    - Anti-Passback: The person should exist via the door in the anti-passback if he/she enters via the door in the anti-passback. It minimizes the misuse of fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access

    - Open door with first card: After swiping the first card, the door will remain unlocked or be authorized. The status depends on the card swiping times (odd or even). For odd, the door 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 door is locked and access is denied with credentials until you swipe the first card. After swiping the first card, the door is authorized and the persons with corresponding access level are granted to access. The authorization will be invalid at 00:00 am every day
    - 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
        - Enable custom card reader access mode
            - Set custom time period
    - 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. Access level
    - Add the door to access level

f. Attendance settings
    - Set the door as attendance check point

g. Event settings
    - Set triggering event(s) for the door
    - Trigger user-defined event

h. Map settings
    - Add the door to map
    - Set map icons

19. 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
    - Edit name color
20. 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
21. 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-Related Events:

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

- Audio Exception Detection
- Blacklist Alarm
- Camera Communication Exception
- Camera Communication Recovered
- Defocus Detection
- Face Capture
- Face Detection
- Fast Moving (Detection)
- Fire Source Detection
- Intrusion (Detection)
- Line Crossing (Detection)
- Loitering (Detection)
- Motion Detection
- Object Removal (Detection)
- Parking (Detection)
- People Gathering (Detection)
- PIR
- Region Entrance (Detection)
- Region Exiting (Detection)
- Scene Change Detection
- Sudden Decrease of Sound Intensity Detection
- Sudden Increase of Sound Intensity Detection
- Temperature Alarm
- Temperature Difference Alarm
- Unattended Baggage (Detection)
- Video Loss
- Video Tampering Detection
- Whitelist Alarm

b. Shall batch add the following Door Events

- Anti-Passback Server Respond Failed
- Card Number Expired
- Card Reader Tamper Alarm
- Door Bell Rang

- Door Button Pressed Down
- Door Button Released
- Door Locked
- Door Normally Locked
- Door Normally Unlocked
- Door Open with First Card Ended
- Door Opened with First Card Started
- Door Unlocked
- Door Unlock Timed Out
- Duress Alarm
- Fingerprint Not Found
- First Card Authorization Ended
- First Card Authorization Started
- Invalid Time Period
- Max. Card Access Failed Attempts
- No Access Level Assigned
- No Card Number Found
- Remaining Locked Status Ended
- Remaining Locked Status Started
- Remaining Unlocked Status Ended
- Remaining Unlocked Status Started
- Remote: Locked Door
- Remote: Remained Locked (Credential Failed)
- Remote: Remained Unlocked (Free Access)
- Remote: Unlocked Door
- Secure Door Control Unit Tamper Alarm

c. Shall batch add alarm input events

d. Shall Add Under Vehicle Surveillance System Event:
   - Offline
   - Online

e. Shall Add Remote Site Event: Site Offline

f. Shall batch add Health Monitoring events from Encoding Device:
   - Array Exception
   - Camera/Recording Resolution Mismatch
   - Device Offline
   - Device Reconnected
   - HDD Full
   - Illegal Login
   - R/W HDD Failure
   - Video Standard Mismatch

g. Shall batch add health monitoring events from Access Control Device:
   - AC Power Off
   - AC Power On
   - Connection Recovered with Anti-Passback Server
   - Device Offline
   - Disconnected with Anti-Passback Server

- Low Battery Voltage
- No Memory for Offline Event Storage
- Tampering Alarm

h. 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
   - 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
   - Physical Volume Alarm
   - Recording Exception Alarm
   - Server Exception
   - System Temperature Too High
   - Video Loss Alarm

i. Shall batch add health monitoring events from the Streaming Server: Server Exception

j. Shall batch add Health Monitoring events from the HikCentral Server:
   - CPU Exception
   - CPU Recovered
   - CPU Warning
   - RAM Exception
   - RAM Recovered
   - RAM Warning
   - System Service Abnormally Stopped
   - System Service Recovered to Run

k. Shall batch add user events: User Login/Logout

l. Shall be able to add generic event as system-related event

m. 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

n. Shall batch delete all invalid events that are not supported on NVR or Network Camera

o. Shall have the ability to trigger any of the above stated events as user-defined events
p. Shall have the ability to convert any of the above stated events into an alarm
q. Shall support generic events, temperature events, and temperature difference events
r. After configuring a recording schedule, video files of events can be searched and played

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 alarms triggered by camera:
      - Audio Exception Detection
      - Face Detection
      - Intrusion Detection
      - Line Crossing Detection
      - Motion Detection
      - Object Removal Detection
      - Region Entrance Detection
      - Region Exiting Detection
      - Sudden Decrease of Sound Intensity Detection
      - Sudden Increase of Sound Intensity Detection
      - Unattended Baggage Detection
      - Video Tampering Detection
      - Whitelist Alarm
      - Blacklist Alarm
   b. Shall have the ability to configure alarms triggered by LPR events
      - License Plate Matched Event
      - License Plate Mismatched Event
   c. Add alarms triggered by person
      - Face Matched Event
      - Face Mismatched Event
   d. Add alarms triggered by Remote Sites events: Site Offline
   e. Same list of events listed above in section "1,2,3" shall be available to be programed as alarms on the VSM
      i. When selecting a triggering event to program as alarms, only events supported by a device will appear in the Web Client
      ii. Individual alarm triggers are based on a schedule, and shall support up to 200 schedule templates
      iii. Alarm priority shall be configured to one of three levels by default:
         - High
         - Medium
         - Low
      iv. Alarm Priority of up to 255 levels can be added up to 255 levels as required

v. 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)

vi. Shall have the ability to set arming schedule template

vii. Shall have the ability to specify a user defined event to an alarm input as the start or end event of the arming schedule

viii. Shall have the ability to set alarm recipients from users accounts set up in the VSM

ix. Shall have the ability to associate up to 16 cameras recording with alarm events

x. Shall have the ability to associate a map with an alarm

xi. Shall have the ability to trigger a pop-up window with an alarm event

xii. Shall have the ability to enable restrict alarm handling time and select up to 16 user-defined events and alarm outputs to trigger events if timeout occurs

xiii. Shall have the ability to lock associated alarm event video footage, so it is not auto-erased based on the camera schedule

xiv. Shall have the ability to trigger alarm actions
   - Trigger Audible Warning
   - Link Door
   - Link Alarm Output
   - Trigger PTZ
   - Display on Smart Wall
   - Create Tag
   - Send Email
     - Ability to create unlimited custom email templates
   - Trigger User-Defined Event

f. Shall support importing newly-added alarms of Remote Sites, editing the alarm name or synchronizing alarm name from site, 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

g. Alarm source, trigger events, and alarm priority can also be displayed

h. Shall support alarm linkage of smart walls; smart walls and screens can be selected

i. Shall support displaying alarms in alphabetical order

j. 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

k. 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

l. 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

m. 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 door(s) to the access level
   b. Select the access schedule to define in which time period the person is authorized to access the doors:
      - Customize a new schedule
      - All-day Template
      - Weekday Template
      - Weekend Template
      - Copy from other defined templates
2. Delete (all) access level(s)
3. 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 door(s)
4. Modify the access level name, description, door(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 door 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

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

c. View the attendance details and the person's attendance report for more than one days
    - 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
    - Work hours

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

H. Person

1. Person List

a. Edit ID

b. Edit first name

c. Edit last name

d. Select gender as male/female/unknown

e. Edit email address

f. Edit phone number

g. Edit remark

h. Edit address

i. Add the person into the face comparison group

j. Configure effective period of access control and time & attendance for the access group

k. Enable the 'Bypass Access Control Apps' function to exempt this person from remaining locked (credentials failed) restrictions, all anti-passback rules, and first card authorization

l. Enable the 'Extended Access' function to open the door for a longer time for person with special requirements

m. Add the person to the existing attendance group if the person participants in time and attendance, and one person can be added only one attendance group

n. Set credential information for the person:

i. PIN number

ii. Card
    - Set card format
    - Set card encryption
    - Configure audio settings
    - Issue up to 5 cards for one person

iii. Fingerprint
  - 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 door will be unlocked and the Control Client will receive a duress alarm to notify the security personnel
  - Card
  - Fingerprint

o. View the details of the persons:

i. Name

ii. ID

iii. Phone

iv. Face comparison group name

v. Access group name

vi. Attendance group name

vii. Effective period

viii. Credential information
  - Number of fingerprints
  - Number of cards

ix. Remark

p. Batch issue cards to persons

i. Card enrollment station settings
  - Set card format
  - Set card encryption
  - Audio on/off

q. Batch import persons/profiles

r. Export all persons information and set password for decompressing

s. Customizable additional information other than the basic information, such as address, income, etc.

t. HikCentral supports up to 10,000 persons

2. Face Comparison Group

a. Add face comparison group

i. Group name

ii. Add person(s) to the group

iii. 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)

i. Set similarity threshold for cameras

iii. One face comparison group can be applied to up to 3,000 cameras

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)
      iii. Set access level
        - Select the existing access level and view the door(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. Manually apply all access groups to device to apply the access groups to the linked access control device
    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. Add person(s) to the attendance 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
    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 by:

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. Add basic vehicle information in one list, i.e. license plate number, owner and phone number, support up to 5,000 vehicles managed in one list
8. Upload undercarriage picture to view both the current vehicle's captured undercarriage picture and the uploaded picture for comparison

J. Security

1. Shall have the ability to create user profile groups defined as Roles
2. Role shall be able to restrict user profile access for administration functions defined as:
    a. Configuration and Control: create definable access to
        i. Web Client for sub-admin roles
            - Resource Management

- Event and Alarm settings
- Access Level
- Time & Attendance
- Person
- Vehicle
- Role and User settings (Security)
- System settings
- Data Backup and restore settings

ii. Control Client: for different levels of operator access

- Monitoring
    - Live view
    - Playback
    - Map
- Alarm center
    - View
    - Arm and disarm
    - Delete alarm
    - Acknowledge alarm
    - Trigger pop-up window
- Event & Alarm search
- Video search
- Access control
- Vehicle search
- Add new vehicle to vehicle list
- Add person to face comparison group
- People counting
- Heat map
- Health monitoring
- Client parameter settings
- Logout
- Manage security

b. Resource: Each "Role" can sub-divide the system and shall allow or deny access to the following features:

i. Shall support the following features on a per-camera basis:

- Live view
- Playback
- Capture and Print Pictures
- Video Search
- Download video
- Manual Recording
- Two-Way Audio
- Tag Video
    - Add tag
    - Edit tag
    - Delete tag
    - View tag

- Lock video so it can’t be overwritten by a schedule
    - Add lock
    - Edit lock
    - Delete lock
    - View lock
- PTZ Control
- Audio Control
- Show Health Status
- Manage Security

ii. Shall support the following features of encoding device (NVR, Network Camera):

- Device parameters settings
- Broadcast
- Search log
- Show health status
- Manage security

iii. Shall support the following features of access control device:

- Configuration on device
- Show health status
- Manage security

iv. Shall support the following features of decoding device:

- Device parameters settings
- Show health status
- Manage security

v. Shall support the following features of alarm output：

- Alarm output control
- Manage security

vi. Shall support the following features of site:

- Device parameter settings
- Search log
- Show health status
- Manage security

vii. Shall support the following features of server:

- Show health status
- Manage security

viii. Shall support the following features of user-defined event:

- Trigger alarm manually
- Manage security

ix. Shall support the following features of user:

- Search log
- Manage security

c. Shall add up to 64 roles for user management per VSM

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
    i. Alarm Center
        i. View
        ii. Arm and Disarm
        iii. Delete Alarm
        iv. Acknowledge
        v. Trigger Pop-up Window
        vi. Search Alarm
    j. Shall manage resources of Remote Sites
    k. Shall support the 'copy from' function to copy features of the existing roles

3. Users: Up to 3,000 users shall be able to 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. Select user status
    e. For each user, restrict concurrent logins
    f. PTZ control permission level: notify the user with lower PTZ permission that PTZ control has been appropriated by another user with higher permissions
    g. Assign roles to the user
    h. View role list and detailed information
    i. Import domain users (group)
        i. Select importing mode
        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
4. Active Directory Integration: Shall have the ability to import Windows domain users and assign them to roles
    a. Domain user login supported in the Control Client and Mobile Apps (iOS and Android)
5. 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

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 create a name for the current site
2. Shall set a static IP address for the WAN access
3. The NTP settings shall be able to be set for syncing the time between the VSM and the NTP server
4. 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 conveniently
5. Configure picture storage to store pictures of the passing vehicles, events and alarms on the HDD of VSM server
6. Set the threshold for the VSM’s CPU usage and VSM’s RAM usage and the related value can be monitored via the Control Client
7. Set event/alarm for notification if the CPU usage or RAM usage approaches the pre-determined threshold and lasts for certain duration
8. Configure schedule template for recording schedule, arming schedule, and access schedule
9. Add holidays to define the special days that can affect shift schedules or access control schedules
10. Configure the parameters of the sender’s email account to send the message to the designate email account(s) as email linkage
11. Enable GIS map function and configure the map API URL, and set the icons of the hot region, camera, door, alarm input, alarm output, and UVSS on the map
12. The system shall be able to receive the configured generic events
13. 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
14. For the system with a Remote Site Management module (as we called Central System), it shall be able to receive the registration from other Remote Sites after enabling this function

15. You shall be able to select the NIC of the current VSM so that the system can receive the alarm information of the third-party device or HIKVISION device connected via ONVIF protocol
16. Shall set transfer protocol as HTTP or HTTPS
17. Shall have system hot spare settings
18. Shall switch device access mode for all the added encoding devices between automatically judge or proxy
19. Shall reset network information of added devices
20. 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
21. Shall set database backup and restore of HikCentral system, including smart wall database
22. Shall export configuration data of Remote Site, encoding device, and recording
23. Shall reset the network information of the added device to adapt to the new network environment when system network domain changes
24. Shall download HikCentral Control Client on the Web Client
25. Shall support the applications module (including Live View, Playback, and Local Configuration) when accessing the Web Client via Internet Explorer via HTTPS protocol
26. 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
27. Admin user shall online/offline activate/deactivate license, online/offline update the license, and view license detailed information for system capabilities

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

a. Network performance:
   - Normal
   - Better
   - Best

b. Video caching:
   - Small (1 frame)
   - Medium (6 frames)
   - Large (15 frames)

c. Picture format:
   - BMP
   - JPEG

d. Device access mode:
   - Restore default
   - Automatically judge
   - Directly access
   - Proxy

e. Shall view the saving path of video files and captured pictures on the current PC

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 VSM. 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 V1.2_Software Requirements & Hardware Performance):

- CPU: Intel® CoreTM 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: 120 GB for OS and Control Client
- Other: 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 login 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 following modules and functions:

1. Monitoring: Live view
   - a. Ability to view up to 256 cameras
     - i. Up to 20 pre-defined tile patterns
     - ii. Ability to create up to 5 user-defined tile patterns
   - b. Ability to display GIS map/related map after the camera is added on the map
   - c. Ability to auto switch to sub stream of Network Camera, if the live view window is smaller than one ninth of the whole screen
     - i. Option to enable auto-switching
   - d. Ability to display license plate number when viewing LPR camera after the LPR function is activated in license
   - e. Ability to mark a vehicle license plate number
   - f. Ability to add the vehicle to vehicle list
   - g. 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
   - h. The following functions are available on the tile toolbar for easy access to operator:
     - i. Capture: ability to save snapshots
     - ii. Print camera image
     - iii. Enable manual recording of displayed Network Camera

iv. Enable and utilize two-way audio
v. Enable view instant playback
vi. Digital zoom
vii. 3D positioning for PTZ camera
viii. Activate on-screen PTZ controls
ix. Show camera statistics

- Connection number
- Net status
- Signal status
- Recording status
- Channel type
- Device name
- IP
- Manufacturer
- Area name
- Storage location
- Recording schedule template
- Video stream
- Streaming server
- Pre-record
- Post-record
- ANR

x. Arming control
xi. Edit transcoded stream
xii. Switch to sub or main stream of camera
xiii. Live view on smart wall
xiv. VCA playback
xv. Alarm output
xvi. Audio control
xvii. 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

i. Ability to customize camera tile toolbar
i. Re-order icons to user preference
ii. Remove icons of functions not required for user

j. 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 a batch: play all cameras belonging to one area on different screens
iv. Single screen auto-switch: loop all cameras belonging to one area on one screen:
(a) Automatically change cameras every 20s, 40s, 1min, 3min, and 5min

- Pause/Start guard tour
- Manually switch to next/previous camera live view

k. 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

l. Supports decoding and displaying Remote Site’s cameras and current site’s cameras on smart wall

m. Displays resolution ratio, encoding format, and frame rate of cameras

n. Live view of Remote Site’s cameras

o. After reopening the client, displays the view before closing the client

p. Sets preset and patrol for common cameras

q. Supports preset and patrol settings of fisheye camera

r. Sets offline alarm schedule for Remote Sites

s. Ability to view the live video of the UVSS’s linked camera, the undercarriage picture, and recognized license plate number of the passing vehicles

t. Ability to drag on the undercarriage picture to mark important information

u. Ability to mark the vehicle license plate number

v. Ability to view door-related live view

i. Shall view the live video of the two cameras in one display window

ii. Shall support fisheye expansion, displaying camera status, setting arming control, switching between main stream and sub-stream, viewing the live video on smart wall, displaying VCA search window, turning on/off the alarm outputs, and audio control

iii. Shall control the door status as unlock, lock, remain unlocked, remain locked, and view the card swiping record in real time. When the door links two cameras, the video will display in Picture-in-Picture mode, and you can view the live video of the two cameras in one display

iv. Shall control all doors status as Lock all doors or Recover all doors

v. Shall trigger user-defined event

w. Shall support up to 4 auxiliary screens during live view and 2 screens switching from live View to Playback

x. Shall support up to 4 auxiliary screens during playback and 1 screen switching from Playback to Live View

2. Monitoring: Playback

a. Ability to play back 1 to 16 cameras simultaneously

b. Ability to display GIS map/related map after the camera is added on the map

c. When playing multiple cameras simultaneously, have ability to view in non-synchronized and synchronized mode

d. Ability to export one or multiple cameras displayed simultaneously:

i. Set export location

ii. Set whether to download VSPlayer for viewing

iii. Export only in MP4/AVI format

e. The following functions are available on the camera playback tile toolbar for easy access to operator:

i. Capture: ability to save JPEG snapshots

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

viii. Stream type switch

ix. Playback on smart wall

x. Transcoding playback

xi. Audio on/off

xii. Video download

xiii. VCA search

xiv. Fisheye expansion

f. Ability to customize camera tile tool bar

i. Re-order icons to user preference

ii. Remove icons of functions not required for user

g. Ability to support channel decoding on the smart wall

h. Ability to display resolution ratio, encoding format, and frame rate of cameras

i. Ability to play back channels of Remote Sites

j. Ability to search video files by time

k. Ability to display the date with video files marked with a triangle

l. Ability to support ATM-DVR, its playback type shall be set as command playback

m. Ability to set storage location of recorded video files (central storage or remote storage)

n. Ability to support thumbnails

o. Ability to zoom in or zoom out on the timeline

p. Ability to support dual-stream playback

q. Ability to support AVI format for video file download

r. Ability to support encryption for downloading in MP4 format, and click and play directly after downloading with player in MP4 format

s. Ability to support privacy mask after downloaded and played with VSPlayer

t. Ability to adjust download time

u. Ability to check the merged video files in one folder

v. Ability to show/hide thumbnail

y. Ability to view door related playback

i. Shall view the playback of the 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, audio on/off

iii. Shall control the door status as unlocking, locking, remaining unlocked, remaining locked, and view the card swiping record in real time. When the door 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 doors status as locking all doors or recovering all doors

v. Shall trigger user-defined event

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
- Area
- Triggering event
- Alarm status
- Alarm category
- Quick link:
    - Alarm&event search
    - Two-way audio
    - Download
    - Display on smart wall
    - Delete the alarm

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. 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

viii. Supports alarm linkage to smart wall

ix. Alarm linkage of smart wall supports window division and jointing

x. Central system can receive alarms from Remote Sites

xi. Alarm center can display map or video, or map and video

xii. Supports multiple time zones of clients

xiii. Supports displaying alarm video on smart wall

4. Alarm and Event Search: Ability to search for alarms and events, based on the following:

i. Event Source

- Camera
- Door
- Alarm Input
- ANPR
- Person
- Remote Site
- Encoding Device
- Access Control Device
- Recording Server
- Streaming Server
- HikCentral Server
- User
- User-Defined Event
- Generic Event

ii. Event Type

- Audio Exception Detection
- Blacklist Alarm
- Video Loss

- Video Tampering Detection
- Motion Detection
- PIR
- Scene Change Detection
- Defocus Detection
- Sudden Increase of Sound Intensity Detection
- Sudden Decrease of Sound Intensity Detection
- Face Detection
- Face Capture
- Fire Source Detection
- Scene Change Detection
- Temperature Alarm
- Temperature Difference Alarm
- Video Loss
- Video Tampering Detection
- Line Crossing (Detection)
- Region Entrance (Detection)
- Region Exiting (Detection)
- Intrusion (Detection)
- Loitering (Detection)
- People Gathering (Detection)
- Fast Moving (Detection)
- Parking (Detection)
- Unattended Baggage (Detection)
- Object Removal (Detection)
- Fire Source Detection
- Blacklist Alarm
- Whitelist Alarm
- Access Denied (Card 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 Fingerprint
- Access Denied by Fingerprint and Password
- Access Granted by Card
- Access Granted by Card and Fingerprint
- Access Granted by Card and Password
- Access Granted: Card, Fingerprint, and Password
- 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 Fingerprint and Password
- Anti-Passback Failed

- Anti-Passback Server Respond Failed
- Card and Password Access Granted
- Card Number Expired
- Card Reader Tamper Alarm
- Door Bell Rang
- Door Button Pressed Down
- Door Button Released
- Door Locked
- Door Normally Locked
- Door Normally Unlocked
- Door Unlocked Timed Out
- Door Open with First Card Ended
- Door Open with First Card Started
- Door Unlocked
- Duress Alarm
- Fingerprint Not Found
- First Card Authorization Ended
- First Card Authorization Started
- Invalid Time Period
- Max. Card Access Failed Attempts
- No Access Level Assigned
- No Card Number Found
- Remaining Locked Status Ended
- Remaining Locked Status Started
- Remaining Unlocked Status Ended
- Remaining Unlocked Status Started
- Remote: Locked Door
- Remote: Unlocked Door
- Remote: Remain Closed
- Remote: Remaining Locked (Credential Failed)
- Remote: Remaining Unlocked (Free Access)
- Secure Door Control Unit Tamper Alarm
- Alarm Input
- Under Vehicle Surveillance System Offline
- Under Vehicle Surveillance System Online
- Array Exception
- Camera/Recording Resolution Mismatch
- Device Offline
- Device Reconnected
- HDD Full
- Illegal Login
- R/W HDD Failure
- Video Standard Mismatch
- AC Power Off
- AC Power On
- Connection Recovered with Anti-Passback Server

- Device Offline
- Disconnected with Anti-Passback Server
- Low Battery Voltage
- No Memory for Offline Event Storage
- Tampering Alarm
- Array Degradation
- Array Detection
- Array Expansion
- Array Initialization
- Array Rebuilding
- Array Repair
- Array Unavailable
- Bad Disk
- Chip Temperature Too High
- CPU Temperature Too High
- Disk Disconnected
- Disk Loss
- Disk Warning
- Environment Temperature Too High
- Hybrid SAN: Fan Exception
- Hybrid SAN: Network Status Exception
- Hybrid SAN: Power Supply Exception
- Hybrid SAN: Storage Enclosure Exception
- Mainboard Temperature Too High
- Memory Exception
- Memory Temperature Too High
- Physical Volum Alarm
- Recording Exception Alarm
- Server Exception
- System Temperature Too High
- Video Loss Alarm
- Streaming Server Exception
- CPU Exception
- CPU Warning
- CPU Recovered
- RAM Exception
- RAM Warning
- RAM Recovered
- System Service Abnormally Stopped
- System Service Recovered to Run
- User Login
- User Logout
- User-Defined Event

iii. Time

- Last Hour
- Today

- Yesterday
- 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 is integrated with a Point of Sales (POS) system

      vi. Supports ATM event search
      vii. Supports thumbnails
      viii. Ability to search main stream in all main storage
      ix. Ability to search sub-stream in all main storage
      x. Ability to search main stream in all auxiliary storage
      xi. Ability to search sub-stream in all auxiliary storage
      xii. 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 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
      - Support adding the person to the person list

6. 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 adding tag
   iv. Support viewing the label status, plate number, vehicle passing item, camera, owner, phone number, country/region of the vehicle
   v. Support add the vehicle to vehicle list
   vi. Support downloading the vehicle information and video
   vii. Support viewing the captured vehicle picture, undercarriage picture, or related video

viii. Support exporting the searched vehicle records and downloading the related video

7. Access Control
    i. Support searching access control event
    ii. Support viewing access control event related video
    iii. Support viewing the person profile, person name, ID, time, door, access result, and access mode
    iv. Support downloading the searched person information
    v. Support exporting card swiping records
8. Video Analysis
    a. People Counting
        i. Ability to search network cameras enabled with people counting analytics to create reports based on Daily, Weekly, Monthly, or Annual time intervals
            (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 export the detailed data of counting report in CSV (Excel) format
            (c) Support video linkage searching by month, date, week, hour, and play corresponding video to check people counting
            (d) Ability to display up to 8 people counting cameras with different colors in people counting report of entry/exit
            (e) Ability to view entered/exited/both entered and exited statistics
            (f) Ability to play linked video of camera(s)
    b. 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
            (a) Ability to export heat map report in PDF format
9. Health Monitoring
    a. Ability to monitor the status of the VSM server, Recording Server, Streaming Server, connected cameras, doors, Under Vehicle Surveillance System (UVSSs), encoding devices, decoding devices, and access control devices, such as VSM's working status, camera's online status and recording status
    b. Overview: Provide status of the following devices and the ability to click on items for a detailed report:
        i. Offline/total number of cameras
        ii. Number of camera with video loss
        iii. Number of camera with communication exception
        iv. Number of camera with record exceptions
        v. Number of camera with no recording schedule
        vi. Offline/total number of Doors
        vii. Offline/total number of UVSS(s)
        viii. Offline/total number of Remote Sites
        ix. Video Surveillance Management Server status
        x. The number of incoming/outcoming steams of Streaming Gateway
        xi. Recording Server Status
        xii. Encoding Device status
        xiii. Access Control Device status
        xiv. Decoding Device status
    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. 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. Operation: Refresh to get the real-time status immediately of the camera; go to logical view of the camera

e. Door: Provide the status of the followings:

i. Name

ii. Access Control Device

iii. Area

iv. Access Control Device net status

v. Door status

vi. Configured Door status

ix. Operation:

- Refresh to immediately get the real-time status of the door
- 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. Operation:

- Refresh to immediately get the real-time status of the site
- Switch the device accessing mode to Proxy mode

vi. Restore All Network Connections

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. Streaming Server: Provide the status of the followings

   i. Total number
   ii. Number of Streaming Server with exception
   iii. Number of Streaming Server with warning
   iv. Number of Streaming Server in normal status

j. Encoding Device: Provide the status of the followings

   i. Name
   ii. Address
   iii. Device Serial No.
   iv. Version
   v. Net status
   vi. HDD usage
   vii. Recording status(Local Device)
   viii. Manufacturer
   ix. Operation
   - Refresh to immediately get the real-time status of the device
   - Go to Logical View of the camera
   x. 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
   - Direct Connection: The client directly accesses the device
   - Proxy: The client accesses the device through Steaming gateway and the Management service

k. Access Control: Provide the status of the followings:

   i. Name
   ii. Address
   iii. Device Serial No.
   iv. Version
   v. Net status
   vi. Battery status

vii. Operation: Refresh to immediately get the real-time status of the Access Control Device

l. 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

m. Display host server and spare server when hot spare function is enabled

10. 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 add view and view group, edit view name and view group name, and delete view and view group

iv. Shall support auto-switch of views belonging to the same view group, and set time interval between views

v. Shall save views, and sort views via created time or manually

vi. Shall create a roaming window

vii. Shall view the camera status

viii. Shall stop decoding and displaying

ix. Shall support window division of up to 16 windows, window jointing via dragging, and display/hide the window ID for Keyboard usage

x. Shall lock/unlock the selected window

xi. 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

xii. Shall support PTZ control, auto-switch stream type, switching to sub-stream manually, and stopping decoding manually

xiii. Shall display alarm-related video on smart wall, and mark on the alarm window

xiv. Shall query smart wall logs

xv. Shall display one smart wall in the center, or up to three walls side-by-side

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

11. 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

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
    iii. Ability to upload the captured pictures to FTP
  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
    iii. Ability to upload the video clips to FTP
  d. Basic Settings:
    i. General settings: support the following settings:
      - Shall set the network performance as Best, Better, or Normal
      - Shall set picture format as JPEG or bmp
      - Shall set the maximum mode as Full Screen or Maximize
      - Shall enable Auto-login
      - Shall resume last interface
    ii. Image Settings
      - Support setting the view scale in live view or playback as Full Screen, 4:3, 16:9, or Original Resolution
      - Support switching stream type manually during live view even after enabling auto-change stream type
      - Support decoding continuously when switching between one window and multiple windows after enabling continuous decoding
      - Support highlight motion detecting area
      - Support setting video caching parameters based on network performance, computer performance, and bit rate. Larger frame caching will result in better video performance
      - Support GPU decoding
      - Support overlay transaction information to view ATM transaction information in live view and playback
      - Support displaying overlay temperature information on the live view and playback
      - Support displaying the VCA rule in the live view and playback
    iii. Edit saving path of manual recording files, captured pictures, and installation packages, and users will receive a reminder to download the newest version if the Control Client differs with the accessed VSM platform in version
  e. Support the operation of Network keyboard to live view and playback
  f. Support configuring alarm sound to enable voice engine or local audio files

12. Log: search and view logs for the following
  a. Server Log
    i. Operation Log, see 4.1 Table 1: Server Logs -Operation Log
    ii. System Log, see 4.1 Table 2: Server Logs - System Log
  b. Device log: Log
    i. All
    ii. Alarm logs: see 4.2 Table 3: Device Logs -Alarm Log
    iii. Exception: see 4.2 Table 4: Device Logs - Exception
    iv. Operation: see 4.2 Table 5: Device Logs -Operation
    v. Information: including, see 4.2 Table 6: Device Logs - Information

c. Smart Wall Log: see 4.3 Table 7: Smart Wall Logs

d. Remote Site Log: log files of the Remote Site, shall be searchable by major type and corresponding minor types:

  i. Operation: including, see 4.4 Table 8: Remote Site Logs – Operation Log

  ii. System Log: see 4.4 Table 9: Remote Site Logs - System Log

e. Log searches are based on operation, user, and time interval searches of:

  i. Today

  ii. Last 6 hours

  iii. Yesterday

  iv. Last 7 days

  v. 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 8 or higher versions

C. On initial log in, users must input the VSM 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 log in to the system via Active Directory
3. Ability to log in to the system via domain name
4. Ability to log in to the system automatically
5. Ability to support HTTPS/HTTP
6. Ability to view logical area of the current site or Remote Sites
7. Ability to display logical areas, and the thumbnail of cameras in each area
8. Ability to filter to display the resources of cameras or doors
9. Ability to search passing vehicles log for HD version via category (camera by default), time, country, mark status, vehicle plates, and owner
10. Ability to support multiple time zones for searching recording files, alarm logs, and heat map reports
11. Logical Resources: Ability to switch between Live View and Playback

  a. Live View:

    i. Ability to view up to 9 camera tiles

    ii. Ability to switch to saved view pattern

    iii. Ability to view real-time video from the Under Vehicle Surveillance System’s related camera (only for tablet)

    iv. Ability to view real-time video from the door’s related camera(s)

    v. Ability to lock/unlock door manually

vi. Ability to display persons' real-time access records, including person profile, person name, and access results

vii. Ability to view the recognized passing vehicle information, including license plate number and passing time

viii. 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)

ix. Ability to mark on the captured real-time undercarriage picture (only for tablet)

x. Ability to add new vehicle to the vehicle list

xi. Ability to view the person's face comparison information (real-time and history), including captured face picture, person details, captured time, and similarity

xii. Ability to add mismatched person into person list

xiii. Ability to trigger user-defined event manually

xiv. 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 and 16 tiles
- Stop/recover all the live views
- Capture: ability to save snapshots, and share the captured pictures via email
- 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

(a) Ability to set style of 4 different Fisheye dewarping modes:

- Dual-180° panorama for ceiling mounting and table mounting
- 360° panorama view for ceiling mounting and table mounting
- Panorama for wall mounting
- Virtual Pan-Tilt-Zoom viewing capability

(b) Activate on-screen Pan-Tilt-Zoom viewing controls

- Ability to live view in full-screen mode

b. Playback

i. Ability to playback 1 to 4 cameras simultaneously

ii. Ability to stop playback of all cameras in one step or one by one

iii. Ability to choose date and storage location for playback

iv. Ability to search cameras for playback by name or choose cameras added to Favorites

v. Ability to restore the playback interface when the user logs out

vi. Ability to switch the window for playback

vii. Ability to support Heat Map reports for HD version

viii. Ability to search Logical Area/Door/Camera via key words

ix. Ability to support synchronous playback

x. Ability to playback the cameras of Remote Sites

xi. Ability to support VCA search for HD version

xii. Ability to add person into Person List for HD version

xiii. Ability to add tags and search video via tags for HD version

xiv. Ability to playback single camera in full-screen mode

xv. 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
- 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

xvi. Ability to set style of 4 different Fisheye dewarping modes:

- Dual-180° panorama for ceiling mounting and table mounting
- 360° panorama view for ceiling mounting and table mounting
- Panorama for wall mounting
- Fisheye overview for ceiling mounting, table mounting and wall mounting

xvii. Activate on-screen PTZ controls

c. 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 door information

iv. Ability to add person to person list

d. 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

e. Favorites

- Ability to manage frequently checked cameras

f. 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

12. View
i. View the favorites list of cameras and doors
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

13. 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 category
(b) Alarm source
(c) Alarm time
(d) Alarm name
(e) Server time
(f) Server IP
(g) Triggering event
ii. Alarm center has the following functions:
(a) Refresh to check latest alarm information
(b) Filter alarm by time
(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

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 switch between the following accessing device modes when performing live view or playback:
i. Restore default
ii. Automatically judge
iii. Directly access
iv. Proxy
f. Ability to enable GPU decoding
g. Ability to show network traffic data used in the following environments:
i. Mobile Network
ii. Wi-Fi
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 by inputting the IP address, KPS port, HikCentral user name and password
B. Shall view the logical areas of Remote Sites and current sites
C. Shall select the window to decode cameras of Remote Sites and the current site for live view
D. Shall support the PTZ function of Light, Wiper, Focus, Iris, Zoom, and control PTZ permissions and release PTZ permissions via the logged user
E. Shall split windows
F. Shall support using the saved preset, patrol, and pattern
G. Shall support 3D PTZ function
H. Shall display wall list on the keyboard
I. Shall switch views saved in Smart Wall

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

A.	Minimum PC	Intel® CoreTM i5-4590 @3.30GHz
B.	RAM	8G
C.	Network	GbE network interface card
D.	Graphics Card	NVIDIA® GeForce® GTX 970
E.	Hard Disk Type	SATA-II 7200 RPM Enterprise Class Hard Drives
F.	Hard Drive Capacity	120 GB for OS and Control Client
G.	Other	**Windows 8.1_**64-bit_en

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

1. Operation Log

The Operation Log shall be searchable by the following subcategories

Table 1: Server Logs -Operation Log

Acknowledge Alarm	Activate Device	Activate License
Activate Access Control Device	Activate Recording Server	Activate User
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 Anti-Passback Rule
Add Attendance Check Point	Add Attendance Group	Add Card to Person
Add Door	Add Door to Access Level	Add Door to Anti-Passback
Add Face Comparison Group	Add Fingerprint to Person	Add Holiday
Add Hot Region on GIS map	Add Label on GIS Map	Add Linked Holiday for Shift Schedule
Add Person	Add Person in Attendance Group	Add Person Profile
Add Person to Access Group	Add Person to Face Comparison	Add Related Camera to Door
Add Report	Add Shift Schedule	Add Under Vehicle Surveillance System
Add User-Defined Event	Add Alarm Category	Add Alarm Input Element
Add Alarm Output Element	Add Alarm Priority	Add Alarm Settings
Add Area	Add Arming Schedule Template	Add Camera Element
Add Email Template	Add Encoding Device	Add Event Settings
Add Generic Event	Add Hot Region	Add Hot Spot
Add Icon	Add Map	Add Map Label
Add N+1 Hot Spare	Add Recording Server	Add Recording Schedule
Add Recording Template	Add Remote Site	Add Role
Add Site to GIS Map	Add Streaming Server	Add User
Add Vehicle	Add Vehicle List	Add Video Tag
Add View	Add View Group	Alarm Arming
Apply Face Comparison Group to device and link camera	Assign Access Level to Access Group	Assign Door to Access Level
Assign Shift Schedule to Attendance Group	Alarm Disarming	Back Up Captured Pictures
Back Up Database Now	Back Up Recorded Video Files	Batch Correct Attendance Record
Batch Import Person Information	Batch Issue Cards to Persons	Broadcast
Cancel Face Comparison Group Linkage with Camera	Cancel Linkage between Access Level and Access Group	Capture Picture in Live View
Clear Anti-Passback	Correct Check-in/out	Customize Additional Information
Delete Access Control Device	Capture Picture in Playback	Change Device Password

Change User Password	Database Recovery	Deactivate License
Deactivate User	Delete Alarm Category	Delete Alarm Input Element
Delete Alarm Output Element	Delete Alarm Priority	Delete Alarm Settings
Delete Area	Delete Attendance Check Point	Delete Attendance
Delete Access Group	Delete Access Level	Delete Access Schedule Template
Delete All Shift Schedules	Delete Anti-Passback Rule	Delete Camera Element
Delete Customized Additional Information	Delete Arming Schedule Template	Delete Camera Element
Delete Email Template	Delete Door	Delete Email Template
Delete Face Comparison Group	Delete Holiday	Delete Person
Delete Person Additional Information	Delete Person Fingerprint	Delete Person in Attendance Group
Delete Recording Schedule	Delete Encoding Device	Delete Event Settings
Delete Generic Event	Delete Hot Spot	Delete Hot Region
Delete Icon	Delete Map	Delete Map Label
Delete N+1 Hot Spare	Delete Recording Schedule	Delete Recording Server
Delete Recording Template	Delete Remote Site	Delete Role
Delete Streaming Server	Delete Under Vehicle Surveillance System	Delete User
Delete Vehicle	Delete Vehicle List	Delete Video Tag
Delete View	Delete View Group	Door Control: Close Door
Door Control: Open Door	Door Control: Remain Locked	Door Control: Remain Unlocked
Edit Access Control Device	Edit Access Group (Basic Information)	Edit Access Level(Basic Information)
Edit Access Level in Access Group	Edit Access Schedule Template	Edit Anti-Passback Rule
Edit Attendance Group	Edit Attendance Group’s Assigned Shift Schedule	Edit Customized Additional Information
Edit Device Access Mode	Edit Door	Edit Door in Access Level
Edit Door Related Camera	Edit Face Comparison Group Basic Information	Edit Holiday
Edit Hot Region on GIS Map	Edit Hot Spot on GIS Map	Edit Active Directory Settings
Edit Alarm Category	Edit Alarm Settings	Edit Alarm Input Element
Edit Alarm Output Element	Edit Alarm Priority	Edit Alarm Settings
Edit Area	Edit Arming Schedule Template	Edit Backup Information
Edit Camera Element	Edit Email Settings	Edit Email Template
Edit Encoding Device	Edit Event Settings	Edit Generic Event
Edit Hot Spot	Edit Hot Region	Edit Hot Spare Settings
Edit Icon	Edit Map	Edit Map Label
Edit NTP Settings	Edit N+1 Hot Spare	Edit Label on GIS Map
Edit Linked Holiday for Shift Schedule	Edit Map	Edit Map Label
Edit N+1 Hot Spare	Edit NTP Settings	Edit Person Profile
Edit Person	Edit Person Additional Information	Edit Person Card

Edit Person Fingerprint	Edit Person in Access Group	Edit Person in Attendance Group
Edit Report	Edit Service Status	Edit Shift Schedule
Edit Shift Schedule's Assigned Attendance Group	Edit Under Vehicle Surveillance System	Edit URL of GIS Map API
Edit User	Edit Picture Storage	Edit Recognized Plate Number
Edit Recording Template	Edit Recording Schedule	Edit Recording Server
Edit Registering to Central System Settings	Edit Remote Site	Edit Role
Edit Server NIC Settings	Edit Site on GIS Map	Edit Streaming Server
Edit System Properties	Edit Transfer Protocol to HTTPS	Edit URL of GIS Map API
Edit User	Edit Vehicle	Edit Vehicle List
Edit Video Tag	Edit View	Edit View Group
Edit WAN Access Settings	Email Test	Enable/Disable Alarm
Enable/Disable Receiving Generic Event	Export Access Records	Export Attendance Records
Export Person Information	Export Alarm/Event logs	Export Heat Map
Export logs	Export People Counting Data	Export Vehicle Information
Export Vehicle Records	Force Logout	Get Device's Recording Schedule
Get Device's Recording Settings	Get License Exception	Import Vehicle Information
Input Person Additional Information	Lock All Doors	Log Search
Manual Update Resource	Manually Apply	Mifare Encryption
Modify User Defined Event	One-Touch Configuration	Pause Area Auto-switch
Pause Auto-switch in Custom View	PTZ Control	Push Subscription
Reboot Access Control Device	Recover All Doors	Remove Card from Person
Remove Door from Access Level	Remove Door from Anti-Passback	Remove Hot Spot from GIS Map
Remove Label from GIS Map	Remove Linked Holiday from Shift Schedule	Remove Person from Access 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 User Password
Resume Area Auto-switch	Resume Auto-switch in Custom View	Restore All settings
Restore Default Settings	Search Access Records	Search Alarm Log
Search People Counting	Search Vehicle Passing Record	Search Video Tag
Send to Spare Server	Set Card Reader Access Mode	Set Door Free Access Schedule
Set Access Control Device Parameters	Set Network Parameters	Set Opening Door with First Card Parameters
Set Door Parameters	Set Time Parameters	Set Scheduled Applying Time
Start Area Auto-switch	Start Auto-switch in Custom View	Start Live View of Door Related Camera
Start Downloading Video File	Start Live View	Start Recording in Live View
Start Playback	Start Remote Playback Recording	Start Two-way Audio
Stop Area Auto-switch	Stop Auto-switch in Custom View	Stop Downloading Video File

Stop Live View	Stop Recording in Live View	Stop Playback
Stop Live View of Door Related Camera	Stop Playback of Door Related Camera	Stop Recording in Playback
Stop Two-way Audio	Subscribe Access Control Event	Sync Recording Settings to Device
Synchronize Door Name	Synchronize Camera Name	System Settings on Control Client
Turn Off Alarm Output	Test Alarm Configuration	Trigger User-Defined Event
Turn On Alarm Output	Video Search	View Captured Picture
Upgrade Device		

2. System Log

System Log, shall be searchable by the following subcategories

Table 2: Server Logs - System Log

All
Database Backup Completed
Database Backup Failed
Database Restored
Disable Video Function Management Service
Enable Video Function Management Service
Lock
Restoring Database Failed
Unlock
User Login
User Logout

4.2. Device Log

Log information on DVRs, NVRs, and network cameras with SD cards, are searchable by major type and corresponding minor types:

1. All
2. Alarm Logs: including, but not limited to, the following basic minor types:

Table 3: Device Logs -Alarm Log

All	Alarm Input	Alarm Output
Answering Question Started	Answering Question Stopped	Audio Loss Detection
Audio Loss Detection Started	Audio Loss Detection Stopped	Class Began
Class Over	Defocus Detection Alarm Started	Defocus Detection Alarm Stopped
Emergency Alarm Started	Emergency Alarm Stopped	Face Detection Alarm Started
Face Detection Alarm Stopped	Fast Moving Detection Alarm Started	Fast Moving Detection Alarm Stopped
Fire and Smoke Detection	Fire and Smoke Detection	IP Camera External Alarm

Started	Ended	
IP Channels Alarm Input Ends	IP Channels Alarm Input Starts	ITS Alarm Started
ITS Alarm Stopped	Intrusion Detection Alarm Started	Intrusion Detection Alarm Stopped
License Plate Recognition Started	License Plate Recognition Stopped	Line Crossing Detection Alarm Started
Line Crossing Detection Alarm Stopped	Loitering Detection Alarm Started	Loitering Detection Alarm Stopped
Motion Detection Alarm Started	Motion Detection Alarm Stopped	Object Removal Detection Alarm Started
Object Removal Detection Alarm Stopped	PIR Alarm Started	PIR Alarm Stopped
POS Started	POS Stopped	Parking Detection Alarm Started
Parking Detection Alarm Stopped	People Gathering Alarm Started	People Gathering Alarm Sopped
Region Entrance Detection Alarm Started	Region Entrance Detection Alarm Stopped	Region Exiting Detection Alarm Started
Region Exiting Detection Alarm Stopped	Scene Change Detection Alarm	Scene Change Detection Alarm Started
Scene Change Detection Alarm Stopped	Ship Detection	Sudden Change of Sound Intensity
Sudden Change of Sound Intensity Started	Sudden Change of Sound Intensity Stopped	Sudden Decrease of Sound Intensity
Temperature Difference Alarm Ended	Temperature Difference Alarm Started	Temperature Measurement Alarm Ended
Temperature Measurement Alarm Started	Temperature Measurement Pre-Alarm Started	Temperature Measurement Pre-Alarm Ended
Unattended Baggage Detection Alarm Started	Unattended Baggage Detection Alarm Stopped	VCA Alarm Started
VCA Alarm Stopped	VQD Alarm Started	VQD Alarm Stopped
Vandal-proof Detection Ended	Vandal-proof Detection Started	Video Tampering Detection Started
Video Tampering Detection Stopped	Wireless Alarm Started	Wireless Alarm Ended

3. Exception: including, but not limited to, the following basic minor types:

Table 4: Device Logs - Exception

All	ANR Recording Failed	Accessory Board Exception
Backup Device Exception	Camera/Recording Resolution Mismatch	Buffer Overflow
Capture Failed	Cloud Storage Data Uploading Exception	DCD Lost

DSP Exception	Device Exception for Decoding System	Ezviz Offline Exception
Fan Exception	HDD Error Details	HDD Exception
HDD Full	IP Address Conflicted	Network Camera Disconnected
Network Camera Module Reboot Abnormally	Illegal Login	Input Signal Lost
Memory Card Damaged	Memory Card Defective	Network Disconnected
Overheating Protection	Power Supply Exception	Rear Panel Temperature Exception
Record Error	Smart Analysis Region Exception	Starting MAS of Network Camera Failed
Sub-system IP Address Conflict	Sub-system Network Disconnected	Synchronize Network Camera Password Exception
Temperature Exception	Video Input Error	Video Standard Mismatch
Wireless Dial Exception		

4. Operation: including, but not limited to, the following basic minor types:

Table 5: Device Logs -Operation

All	Add Plan	Add Scene
Add Signal	Adjust Volume	Auto Dial-up via Calling
Auto Dial-up via Message	Bring the Smart Wall Window to Back	Bring the Smart Wall Window to Front
Cancel Master Screen of Smart Wall	Cancel Slave Screen of Smart Wall	Close Transparent Channel
Configure Smart Wall Connection	Control Decoding Channel Ratio	Control Digital Zoom
Control Passive Decoder	Control Plan	Control Remote Playback
Cut Background Picture	Cut Video Source	Dedicated for Trial
Delete Plan	Delete Scene	Delete Signal
Display Logo	Display Operation	Download Background Picture
Edit CYC Configuration	Edit Input Configuration	Edit output Configuration
Edit Plan	Edit Signal	Edit Virtual LED Configuration
End Time of Local Backup	Get All Valid Windows	Get CYC Configuration
Get Current Scene	Get Decoding Board Parameters	Get Decoding Channel Information
Get Decoding Channel Status	Get Device Information	Get Input Signal List
Get Plan List	Get Plan of Cycle Decoding	Get Remote Playback
Get Scene	Get Scene List	Get Signal Window Information
Get Status of Remote Playback	Get Switch of Decoding Channel	Get User Settings
Get Smart wall Connection	Get Smart Wall Scene	Get Virtual LED
Hide Logo	Illegal Shutdown	Layout Control
Local: Restore Logical Disk	Local Network HDD Addition	Local Operation: Activation
Local Operation: Add Working Device	Local Operation: Delete HDD	Local Operation: Delete Working Device
Local Operation: Device Type Configuration	Local Operation: Export Heat Map File	Local Operation: Export Network Camera Configuration File
Local Operation: Factory Defaults	Local Operation: HDD Detect	Local Operation: Hot Spare Device Configuration
Local Operation: Import Network Camera Configuration File	Local Operation: N+1 Configuration	Local Operation: Output Switch
Local Operation: Set RAID Speed	Local Operation: Switch Output	Local Operation: Upgrade Network Camera

Local: Add Network Camera	Local: Auto Restore	Local: Backup Record File(s)
Local: Backup the Start Time	Local: Configuration	Local: Configure PIN
Local: Configure SIP Server	Local: Configure Whitelist	Local: Configure Wireless Dial-up Parameters
Local: Configure Wireless Dial-up Schedule	Local: Create Array	Local: Create Logical Disk
Local: Delete Array	Local: Delete Network Camera	Local: Delete Logical Disk
Local: Delete Network HDD	Local: Disable Wireless Dial-up	Local: Expand Logical Disk
Local: Export Blacklist & Whitelist	Local: Export Heat Map Flow	Local: Export Picture Files
Local: Format HDD	Local: Hot Standby	Local: Import Black-white List
Local: Live View	Local: Locking Record Files	Local: Login
Local: Logout	Local: Manual Clearing or Triggering of Alarm	Local: Manual Rebuild Array
Local: Move Array	Local: One-key Configuration	Local: Operate Tag
Local: PTZ Control	Local: Parameter Export	Local: Parameter Import
Local: Playback By File	Local: Playback By Time	Local: Reboot
Local: Resume the Default Admin Password	Local: Search Message	Local: Send Message
Local: Setting Network Camera	Local: Setting Network HDD	Local: Start Backup
Local: Start Capture	Local: Start Recording	Local: Stop Backup
Local: Stop Capture	Local: Stop Recording	Local: Time Setting
Local: Unlocking Record Files	Local: Upgrade	Local: Upgrade RAID
Local: Restore Logical Disk	Local: View Message	Locally Restore Default Parameters
Login Codesplitter Remotely	Logout Codesplitter Remotely	Platform Operations
Power On	Reboot Intelligent Library	Receive Message
Reconnect Passive Decoder	Remote: Start Capture	Remote Disarming
Remote Operation: Activation	Remote Operation: Add Storage Pool	Remote Operation: Add Working Device
Remote Operation: Delete HDD	Remote Operation: Delete Pictures	Remote Operation: Delete Storage Pool
Remote Operation: Delete Video File	Remote Operation: Delete Working Device	Remote Operation: Device Type Configuration
Remote Operation: Enable Cloud System	Remote Operation: Disable Cloud System	Remote Operation: Edit Storage Pool Capacity
Remote Operation: Export Network Camera Configuration File	Remote Operation: Factory Defaults	Remote Operation: Hot Spare Device Configuration
Remote Operation: Import Network Camera Configuration	Remote Operation: N+1 Configuration	Remote Operation: Set RAID Speed

File		
Remote Operation: Upgrade Network Camera	Remote: Alarm Output Network Camera	Remote: Arming
Remote: Auto Restore	Remote: Configure PIN	Remote: Configure SIP Server
Remote: Configure Whitelist	Remote: Configure Wireless Dial-up Parameters	Remote: Configure Wireless Dial-up Schedule
Remote: Create Logical Disk	Remote: Create Array	Remote: Delete Array
Remote: Delete Logical Disk	Remote: Disable Wireless Dial-up	Remote: Enable Wireless Dial-up
Remote: Establish Transparent Channel	Remote: Expand Logical Disk	Remote: Export Blacklist & Whitelist
Remote: Export Picture Files	Remote: Export the Configuration File	Remote: File Export
Remote: File Locking	Remote: File Unlocking	Remote: Format HDD
Remote: Hot Standby	Remote: Network Camera Addition	Remote: Network Camera Deletion
Remote: Network Camera Setting	Remote: Import Black-white List	Remote: Login
Remote: Logout	Remote: Manual Rebuild Array	Remote: Move Array
Remote: Network HDD Addition	Remote: Network HDD Deletion	Remote: Network HDD Setting
Remote: One-key Configuration	Remote: Operate Tag	Remote: PTZ control
Remote: Parameter Getting	Remote: Parameter Import	Remote: Parameters Configuration
Remote: Playback by Time	Remote: Reboot	Remote: Restore Logical Disk
Remote: Playback by File	Remote: Search Message	Remote: Send Message
Remote: Shutdown	Remote: Search Message	Remote: Send Message
Remote: Shutdown	Remote: Start Recording	Remote: Start Two-way Audio
Remote: Status Getting	Remote: Stop Capture	Remote: Stop Recording
Remote: Upgrade	Remote: Upgrade RAID	Remote: View Message
Remote: Playback by File	Remotely Restore Default Parameters	Reset Admin's Password Locally
Reset Admin's Password Remotely	Restore Decoding Status	Scene Control
Screen Control	Send Alarm Message	Set Background Picture Area
Set Decoding Delay Level	Set Decoding Parameters	Set External Matrix Configuration
Set Layout	Set Master Screen of Smart Wall	Set OSD
Set Output Resolution	Set Plan of Cycle Decoding	Set Remote Playback
Set Slave Screen of Smart Wall	Set Switch of Decoding Channel	Set Transparency
Set Two-way Audio Record	Set User Configuration	Set User Password
Set Smart Wall Scene	Shutdown	Start CYC Decoding

Start Dynamic Decoding	Start PPPoe Connection	Start Passive Decoder
Stop CYC decoding	Stop Dynamic Decoding	Stop PPPoe Connection
Stop Passive Decoder	Stream Compression Configuration	Switch Scene
Upload Logo	Upload Picture	VCA Configuration
Smart Wall Display Area Setup	Window Control	

5. Information: including, but not limited to, the following basic minor types:

Table 6: Device Logs - Information

All	ANR Record Started	ANR Record Stopped
Accessory Board Information	Add ANR Duration	Alarm Log
Backing Up Work Device Ended	Backing Up Work Device Started	Backing Up Device Information
Buffer Status Log	Call Log	Connect to IP Camera, etc.
Delete ANR Duration	Delete Expired Record Files	Delete the Expired Picture Files
Ezviz Operation	Global Error Information	HDD Error Details
IP Camera Disconnected	Local: Start Capture	Local: Stop Capture
Login Server	Logout Server	Network HDD Information
POE power Exception Information	Platform Information	RAID Information
Recording Synchronization Completed	Recording Synchronization Exception	Recording Synchronization Started
Recording Synchronization Stopped	Relogin Server	S.M.A.R.T. Information
Server Status Information	Start Recording	Stop Recording
Unlocking Log	Wireless Dial-up Status	

4.3. Smart Wall Logs

Including, but not limited to, the following basic minor types:

Table 7: Smart Wall Logs

All	Add Decoding Device	Add Smart Wall
Add View	Add View Group	Add View Order
Adjust Window Size	Auto-Switch of View Groups	Create Roaming Window
Delete Decoding Device	Delete Smart Wall	Delete View
Delete View Group	Edit Decoding Device	Edit Smart Wall
Edit View	Edit View Group	Link Decoding Output
Live View On Wall (Camera)	Live View On Wall (Signal Source)	Lock Window
Log Search	Playback Control	Split Window
Start Playback	Stop All Live View on Wall	Stop Live View on Wall

Stop Playback	Switch View	Unlink Decoding Output
Unlock Window		

4.4. Remote Site Logs

Log files of the Remote Site, shall be searchable by major type and corresponding minor types

1. Operation Log : including, but not limited to, the following basic minor types:

Table 8: Remote Site Logs – Operation Log

All	Acknowledge alarm	Activate Device
Activate License	Activate User	Add Alarm Category
Add Alarm Input Element	Add Alarm Output Element	Add Alarm Priority
Add Alarm Settings	Add Area	Add Arming Schedule Template
Add Camera Element	Add Email Template	Add Encoding Device
Add Event Settings	Add Generic Event	Add Hot Region
Add Hot Spot	Add Icon	Add Map
Add Map Label	Add N+1 Hot Spare	Add Recording Schedule
Add Recording Server	Add Recording Template	Add Role
Add Streaming Server	Add User	Add Vehicle
Add Vehicle List	Add Video Tag	Add View
Add View Group	Alarm Arming	Alarm Disarming
Back Up Captured Pictures	Back Up Database Now	Back Up Recorded Video Files
Broadcast	Capture Picture in Live View	Capture Picture in Playback
Change Device Password	Change User Password	Database Recovery
Deactivate License	Deactivate User	Delete Alarm Category
Delete Alarm Input Element	Delete Alarm Output Element	Delete Alarm Priority
Delete Alarm Settings	Delete Area	Delete Arming Schedule Template
Delete Camera Element	Delete Email Template	Delete Encoding Device
Delete Event Settings	Delete Generic Event	Delete Hot Region
Delete Hot Spot	Delete Icon	Delete Map
Delete Map Label	Delete N+1 Hot Spare	Delete Recording Schedule
Delete Recording Server	Delete Recording Template	Delete Role
Delete Streaming Server	Delete User	Delete Vehicle
Delete Vehicle List	Delete Video Tag	Delete View
Delete View Group	Edit Active Directory Settings	Edit Alarm Category
Edit Alarm Input Element	Edit Alarm Output Element	Edit Alarm Priority
Edit Alarm Settings	Edit Area	Edit Arming Schedule Template
Edit Backup Information	Edit Camera Element	Edit Email Settings
Edit Email Template	Edit Encoding Device	Edit Event Settings

Edit Generic Event	Edit Hot Region	Edit Hot Spare Settings
Edit Hot Spot	Edit Icon	Edit Map
Edit Map Label	Edit N+1 Hot Spare	Edit NTP Settings
Edit Picture Storage	Edit Recognized Plate Number	Edit Recording Schedule
Edit Recording Server	Edit Recording Template	Edit Registering to Central System Settings
Edit Role	Edit Server NIC Settings	Edit Streaming Server
Edit System Properties	Edit Transfer Protocol to HTTPS	Edit User
Edit Vehicle	Edit Vehicle List	Edit Video Tag
Edit View	Edit View Group	Edit WAN Access Settings
Email Test	Enable/Disable Alarm	Enable/Disable Receiving Generic Event
Export Alarm/Event Logs	Export Heat Map	Export Logs
Export People Counting Data	Export Vehicle Information	Export Vehicle Records
Force Logout	Get Device’s Recording Schedule	Get License Exception
Get Device’s Recording Settings		
Import Vehicle Information	Log Search	Manual Update Resource
One-Touch Configuration	PTZ Control	Pause Area Auto-switch
Pause Auto-switch in Custom View	Reset Network Information	Reset User Password
Resume Area Auto-switch	Resume Auto-switch in Custom View	Search Alarm Log
Search Event Log	Search Heat Map	Search People Counting
Search Vehicle Passing Record	Search Video Tag	Send to Spare Server
Start Area Auto-switch	Start Auto-switch in Custom View	Start Downloading Video File
Start Live View	Start Playback	Start Recording Live View
Start Remote Playback Recording	Start Two-way Audio	Stop Area Auto-switch
Stop Auto-switch in Custom View	Stop Downloading Video File	Stop Live View
Stop Playback	Stop Recording in Live View	Stop Recording in Playback
Stop Two-way Audio	Sync Recording Settings to Device	Synchronize Camera Name
System Settings on Control Client	Turn Off Alarm Output	Turn On Alarm Output
Video Search	View Captured Picture	

2. System Log: including, but not limited to, the following basic minor types

Table 9: Remote Site Logs - System Log

All	Database Backup Completed	Database Backup Failed
Database Restored	Disable Video Function Management Service	Enable Video Function Management Service
Lock	Restoring Database Failed	Unlock
User Login	User Logout	