HikCentral Professional Datasheet

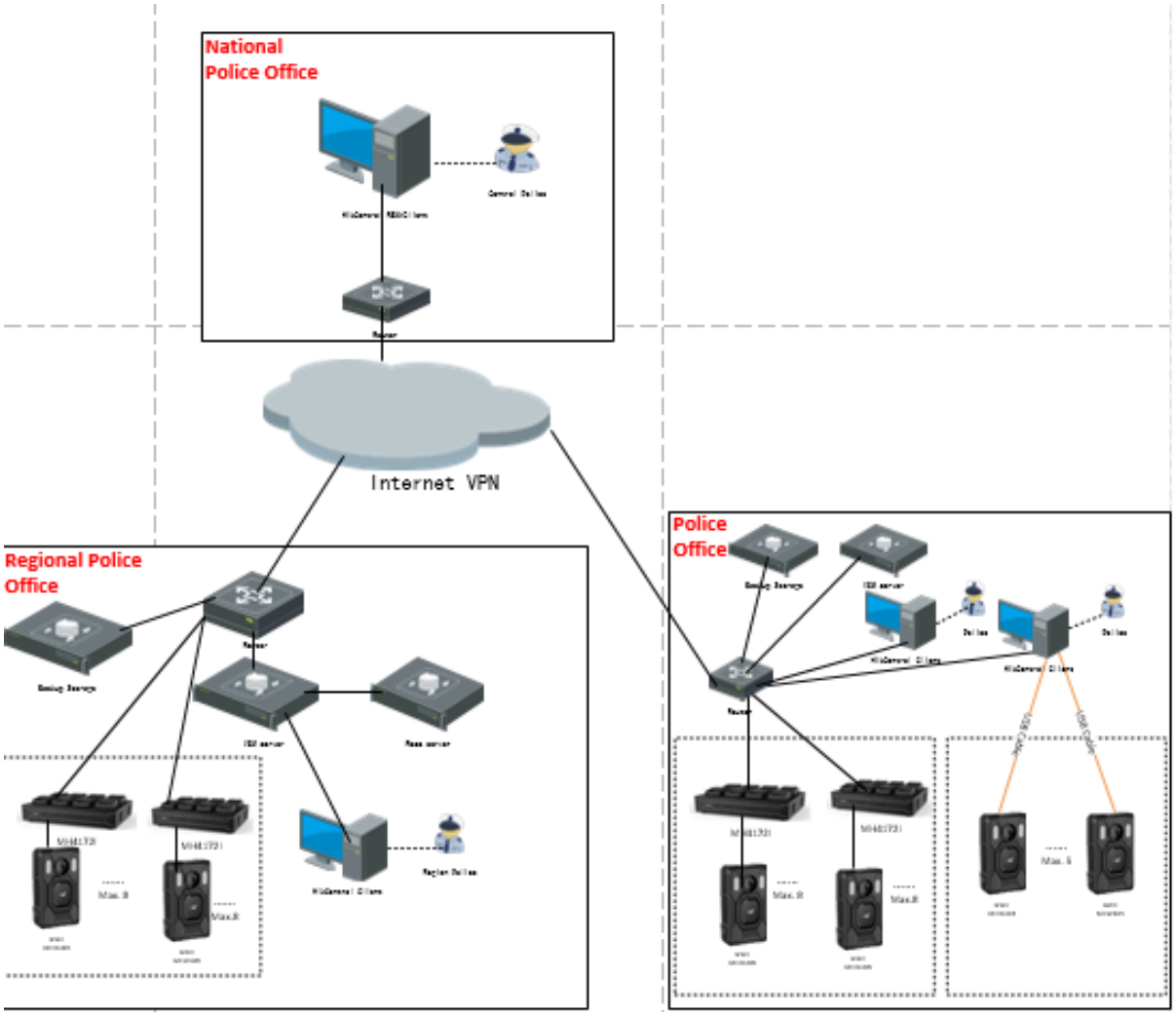
Introduction

HikCentral Professional is a flexible, scalable, reliable and powerful central surveillance system. It can be delivered after pre-installed on Dell server. HikCentral Professional provides central management, information sharing, convenient connection and multi-service cooperation. It is capable of adding devices for management, live view, storage and playback of video files, alarm linkage, access control, time and attendance, facial identification, and so on.

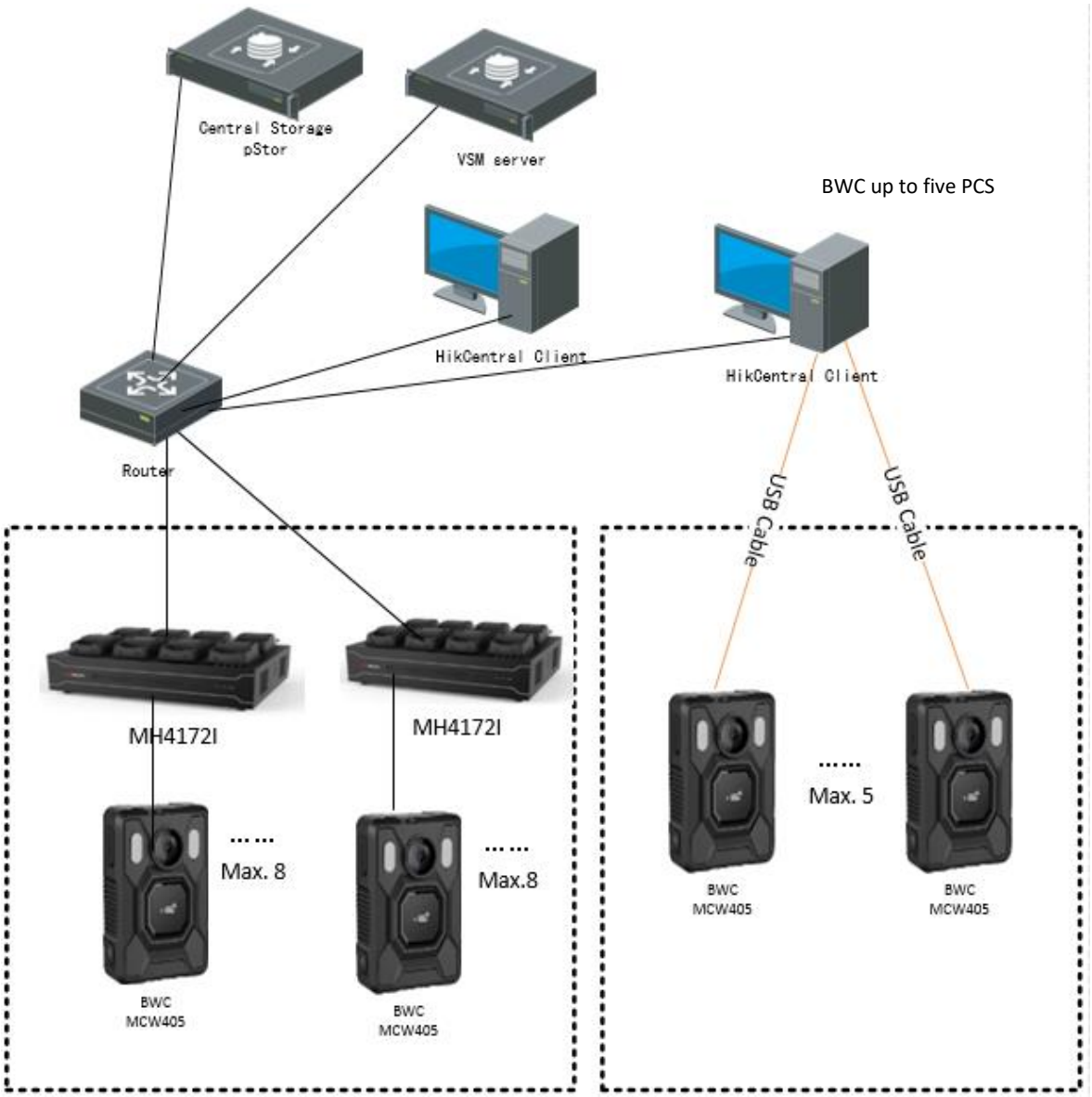
Key Components

System Management Service (SYS)
Application Data Service (ADS)
Streaming Service (Optional)
Web Client/Control Client/Mobile Client

Central server with remote clients connected via WAN

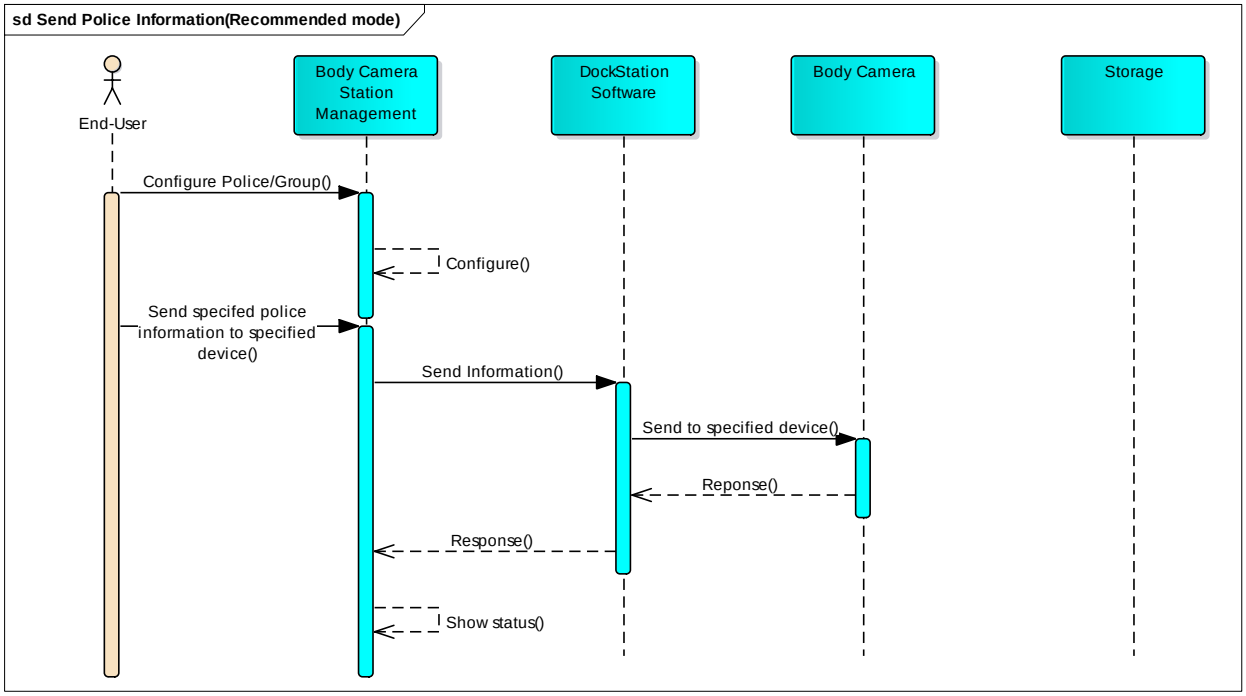


Police Office Recommend deployment
Managed locally as standalone.

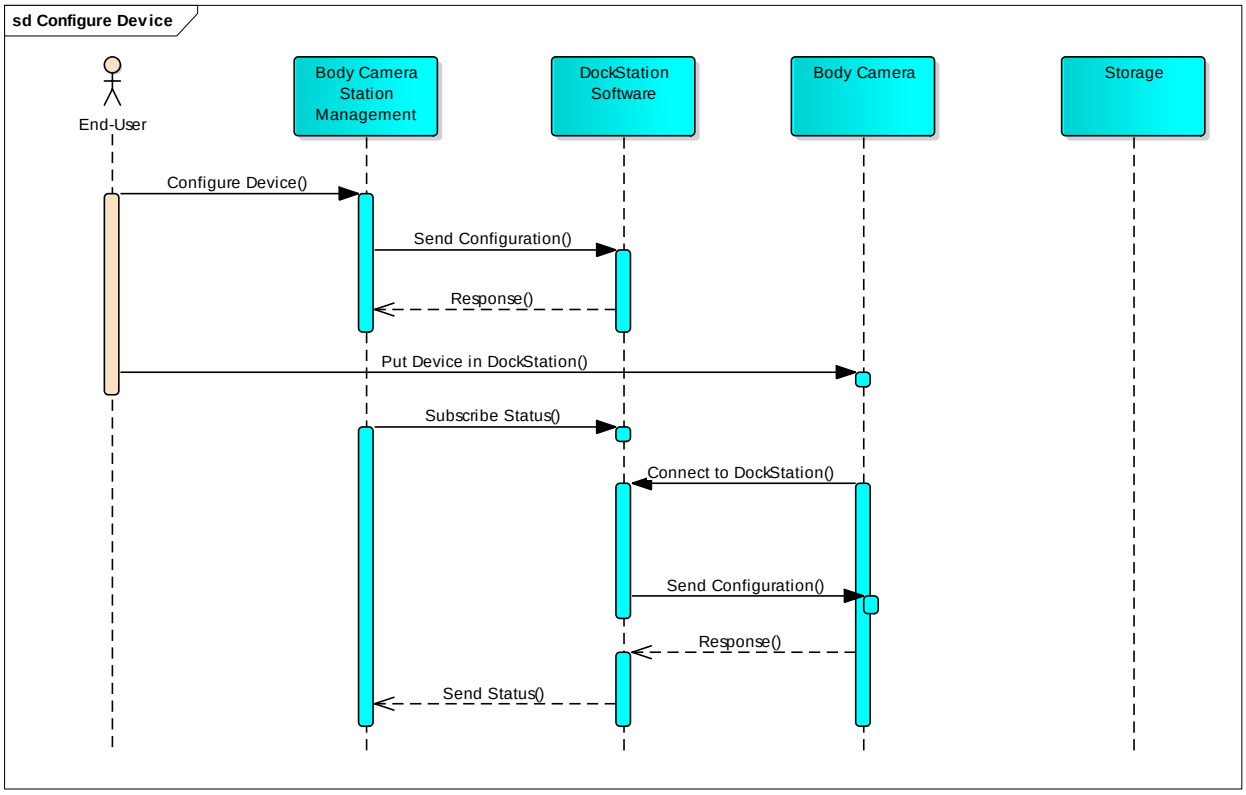


Workflow description

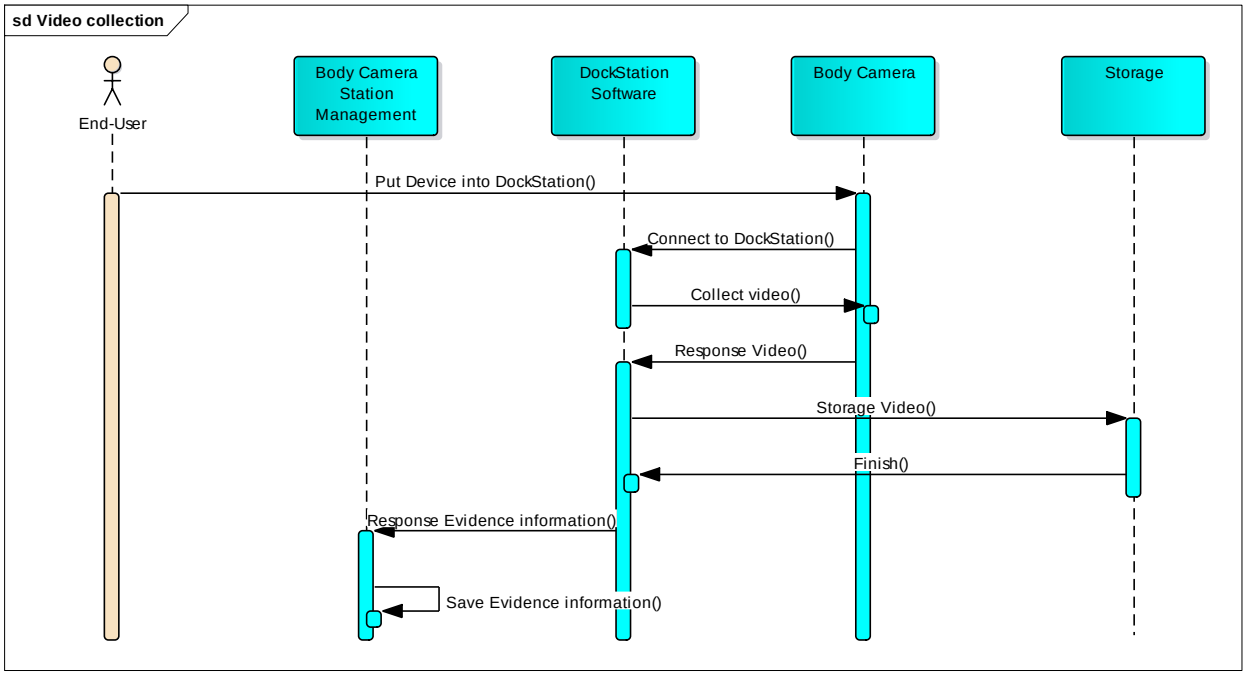
Police officer information Configuration



Configuration and assignment, by an operators



Record Collection



System Requirements

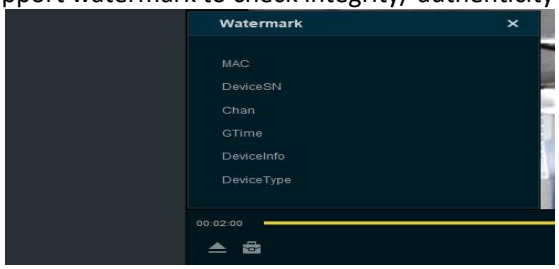
Feature	Description
OS for HikCentral Professional Server	Microsoft® Windows 7 SP1 (64-bit) Microsoft® Windows 8.1 (64-bit) Microsoft® Windows 10 (64-bit) Microsoft® Windows Server 2008 R2 SP1 (64-bit) Microsoft® Windows Server 2012 (64-bit) Microsoft® Windows Server 2012 R2 (64-bit) Microsoft® Windows Server 2016 (64-bit) Microsoft® Windows Server 2019 (64-bit) **For Windows 8.1 and Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) undated in April, 2014.*
OS for Control Client	Microsoft® Windows 7 SP1 (32/64-bit) Microsoft® Windows 8.1 (32/64-bit) Microsoft® Windows 10 (64-bit) Microsoft® Windows Server 2008 R2 SP1 (64-bit) Microsoft® Windows Server 2012 (64-bit) Microsoft® Windows Server 2012 R2 (64-bit) Microsoft® Windows Server 2016 (64-bit) Microsoft® Windows Server 2019 (64-bit) **For Windows 8.1 and Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) undated in April, 2014.*
Browser Version	Internet Explorer 10/11 and above

	Chrome 61 and above Firefox 57 and above Safari 11 and above (running on Mac OS X 10.3/10.4)
Database	PostgreSQL V9.6.13
OS for Smartphone	iOS 10.0 and later Android phone OS version 5.0 or later, and dual-core CPU with 1.5 GHz or above, and at least 2G RAM
OS for Tablet	iOS 10.0 and later Android tablet with Android OS version 5.0 or later
Virtual Machine	VMware® ESXi™ 6.x Microsoft® Hyper-V with Windows Server 2012/2012 R2/2016 (64-bit) **The Streaming Server and Control Client cannot run on the virtual machine.* **Virtual server migration is not supported.*

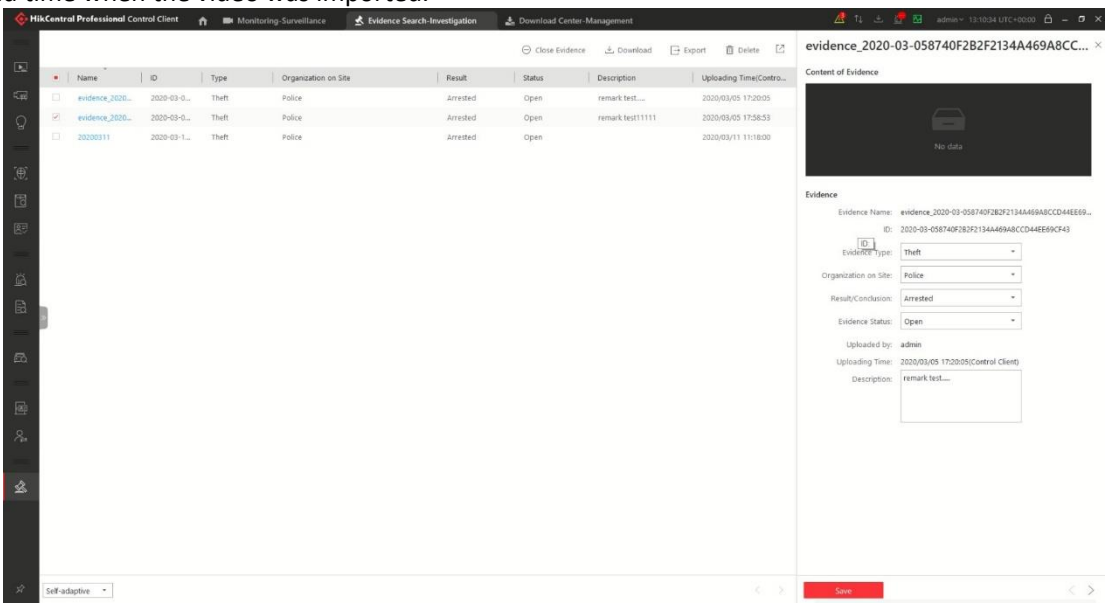
Function Features

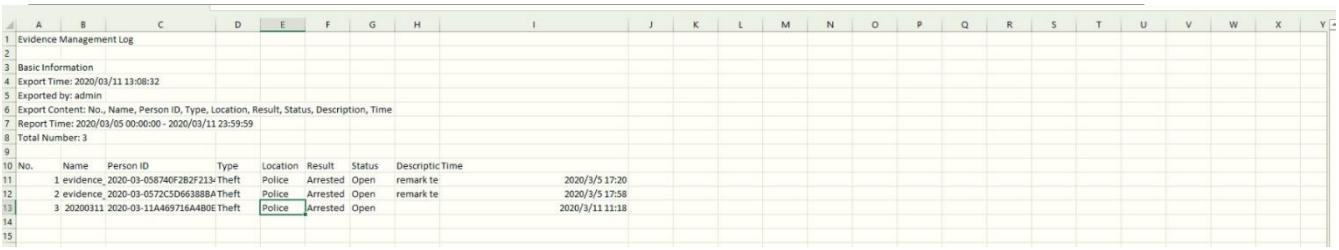
Streaming

- Forwards and distributes audio and video data
- Support watermark to check integrity/ authenticity of the recordings & export audit log.



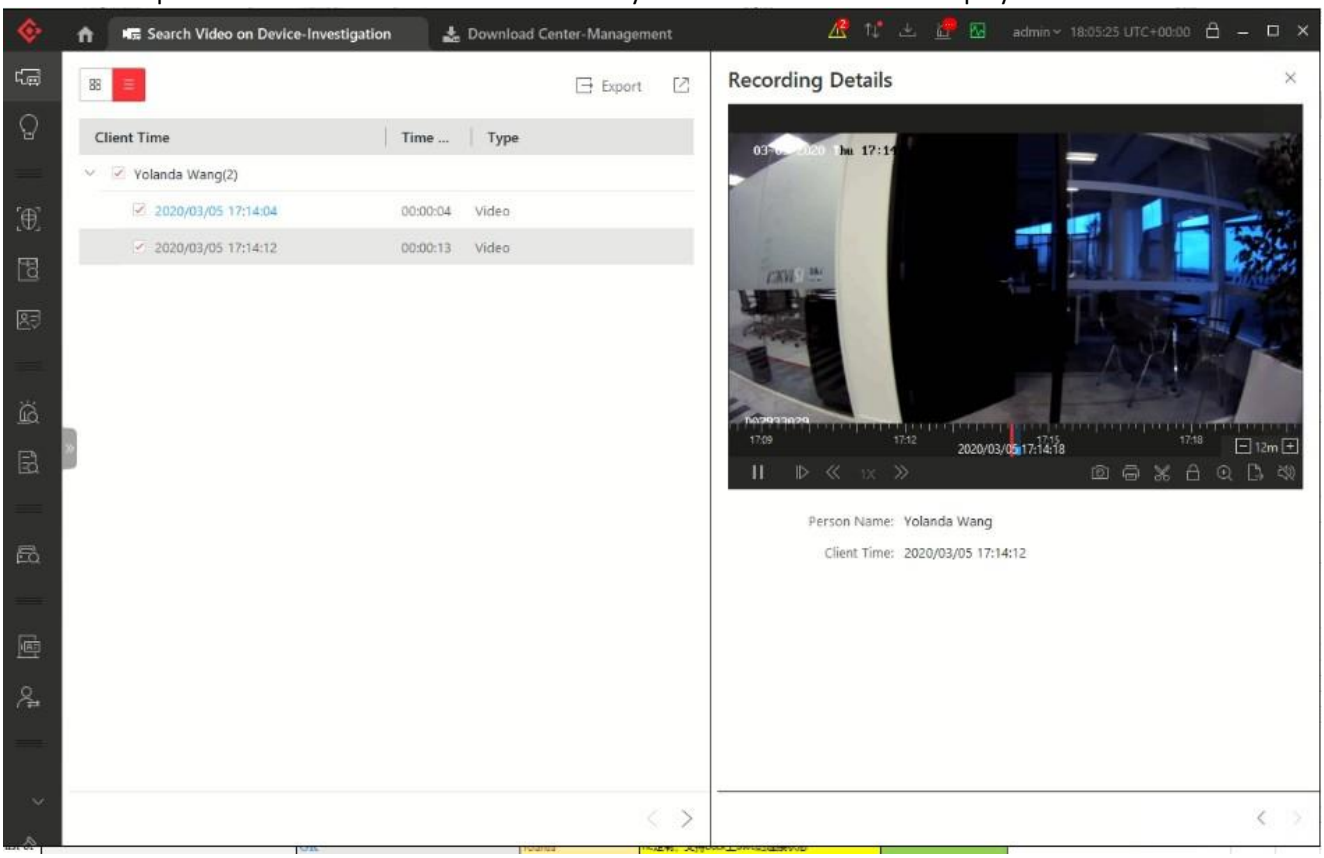
- Import records and associated metadata: BWC device's unique ID , date and time of the video reording, date and time when the video was imported.





	A	B	C	D	E	F	G	H	I
1	Evidence Management Log								
2									
3	Basic Information								
4	Export Time: 2020/03/11 13:08:32								
5	Exported by: admin								
6	Export Content: No., Name, Person ID, Type, Location, Result, Status, Description, Time								
7	Report Time: 2020/03/05 00:00:00 - 2020/03/11 23:59:59								
8	Total Number: 3								
9									
10	No.	Name	Person ID	Type	Location	Result	Status	Descriptic	Time
11	1	evidence_	2020-03-058740F2B2F213	Theft	Police	Arrested	Open	remark te	2020/3/5 17:20
12	2	evidence_	2020-03-0572C5D663888A	Theft	Police	Arrested	Open	remark te	2020/3/5 17:58
13	3	20200311	2020-03-11A469716A4B0E	Theft	Police	Arrested	Open		2020/3/11 11:18
14									
15									

- Editing the recordings (cutting recording) in the same time maintaining the authenticity of the file. It has to be able to export the video file in a format that allows you to view the file with free players



SYS Server

- Provides normal and hot spare installation mode
- Provides centralized management for users, roles, permissions, surveillance devices, and servers
- Provides log management and statistics function
- Scalable for medium and large-sized projects
- Manages Remote Sites for HikCentral Professional with RSM module
- Service manager for system health monitoring
  - Streaming gateway: a component that forwards and distributes audio and video data as well as forwards signaling

ADS Server

- Processes and stores the application data of the system

Web Client

- Access the system via IP address or domain name
- License management

- Online or offline activation
- Online or offline update
- Online or offline deactivation

- Dock station management
  - The password strength of the added dock station can be checked by the system for security purpose
  - Four adding modes for dock stations available:
    - ✓ By specifying the device IP address
    - ✓ By specifying an IP segment
    - ✓ By specifying a port segment
    - ✓ By importing in a batch
  - Set time zone for the device
- Restore or reset passwords for detected online devices
- Upgrade device firmware version
- Remote Site's central management:
  - Add Remote Site to the Central System (HikCentral Professional with an RSM module). Three adding modes for Remote Sites available:
    - ✓ By specifying the Remote Site's IP address or domain name
    - ✓ Adding Remote Site registered to the Central System.
    - ✓ By importing in a batch
  - Select the alarms configured on the Remote Site to receive in the Central System.
  - Back up the Remote Site's database in the Central System manually or regularly.
  - Synchronize the changed resources in the Central System (newly added cameras, deleted cameras, and name changed cameras) with the Remote Site.
- In distributed deployment, the SYS and ADS services can be installed on different servers:
  - Add ADS to the system and set standby server if necessary
  - Provides encrypted transmission between ADS and other services or clients
  - Notify admin user if ADS or standby ADS fails and show fault details
  - Standby ADS takes over automatically if ADS fails
  - Manually switch to standby ADS if necessary
- Recording Server management
  - Add pStor, Hybrid Storage Area Network (Hybrid SAN), NVR, Cloud Storage Server, or pStor Cluster Service as a Recording Server
  - Add pStor, Hybrid SAN, NVR, Cloud Storage Server, or pStor Cluster Service by IP address
  - Provides WAN access
  - Remotely configure the added pStor, Hybrid SAN, NVR, Cloud Storage Server, or pStor Cluster Service via a web browser
  - One-touch configuration for setting the Hybrid SAN storage
  - Set custom video copy-back for Hybrid SAN
  - Hybrid SAN N+1 hot spare
  - View storage information of the connected devices managed by the added pStor Cluster Service
  - Provides ANR function
- Streaming Server management
  - Add Streaming Server by IP address

- Provides WAN and LAN access

- Security Audit Server management
  - Add security audit server by IP address
  - Link encoding devices with security audit server for receiving security audit exception logs
- Smart wall management
  - Create password for inactive decoding device(s)
  - The password strength of the added decoding device can be checked by the system for security notification
  - Four adding modes for decoding devices available:
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device IP address
    - ✓ By specifying an IP segment
    - ✓ By specifying a port segment
  - Set cascade for decoders via a video wall controller to realize cross-decoder functions
  - Add smart wall and link decoding output with the window
- Manage resources by areas
- Recording
  - Two storage methods for storing video footage recorded by cameras in the current site:
    - ✓ Encoding Device: DVR/NVR/ network camera (SD card);
    - ✓ Recording Server: pStor, Hybrid SAN, NVR, Cloud Storage Server, or pStor Cluster Service
  - For Remote Site's cameras, store video files in the Central System's pStor, Hybrid SAN, Cloud Storage Server, or pStor Cluster Service
  - Continuous recording, event triggered recording, and command triggered recording.
  - Set video copyback schedule to upload the specific type of video files stored in one storage medium to the selected storage location
  - Set recording schedule: All-Day Time-Based Template, All-Day Event-Based Template, and Custom Template
  - Auxiliary storage
- Picture storage
  - Store the images uploaded from the devices, such as alarm triggered pictures, captured face pictures, and captured plate license pictures on the HDD of SYS server, Hybrid SAN, Cloud Storage Server, pStor, or NVR.
  - Store the pictures imported by the users, such as the original undercarriage pictures imported when adding vehicles, static map pictures, the face pictures in the person list, on the HDD of SYS server.

- Set resource groups
  - Alarm group
  - Entry & exit counting group
  - People counting group
  - Heat analysis group
  - Pathway analysis group

- Person feature analysis group
- Multi-door interlocking group
- Anti-passback group
- Emergency operation group
- Security control partition

- Events & Alarms
  - Set system-monitored events for the resources in the system
    - ✓ Remote Site exceptions: site offline
    - ✓ Resource group exceptions: person amount more/less than threshold
    - ✓ Device exceptions and operations: device offline, HDD full, HDD read/write error, etc. (including encoding devices, access control devices, elevator control devices, video intercom device, security control devices, decoding devices, and dock stations)
    - ✓ Resource group event: Person amount more/less than threshold alarm and pre-alarm
    - ✓ Server exceptions: high mainboard temperature, bad disk, disk loss, etc. (including Streaming Servers, Recording Servers, DeepinMind server, and HikCentral Professional Server)
    - ✓ Security audit server events: critical events, normal events, serious events
    - ✓ User events: user login or logout
    - ✓ User-defined events
    - ✓ Generic events
  - Send emails to notify users of triggered event information with email template configurable. For alarm input event, attach an entry & exit counting report in the email
  - Create a generic event rule to analyze the received TCP and/or UDP data packages, and trigger events
  - Customize a user-defined event to define the event which is not in the provided system-related event list. You can trigger it manually on the Control Client
  - Trigger the events as alarms and set alarm linkage actions including related cameras, related maps, pop-up window, displaying on smart wall (decoding or graphic), audible warning, and triggering user-defined event
  - Save event as alarm when editing event
  - In the Central System, detect camera alarms configured on Remote Site
  - Remote Site alarms, device exception alarms, server exception alarms, user alarms, user-defined alarms, and generic alarms
  - Set arming schedule for the events: all-day template, weekday template, weekend template, and custom template
  - Set arming schedule for the alarms: all-day template, weekday template, weekend template, custom template, or the alarms can be armed or disarmed when an event starts or ends
  - Set alarm priority: high, medium, low, and custom
  - Set alarm category: true, false, to be acknowledged, and to be verified

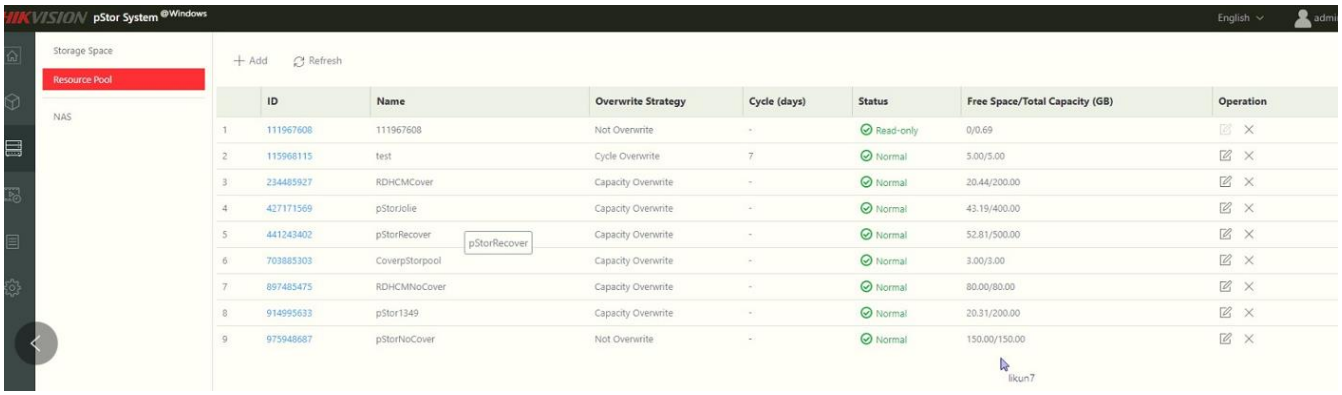
- Map management
  - Link e-map to area
  - Set map scale

- Search locations on GIS map
- Set the current site's and added Remote Site's location to the GIS map
- Add/edit/delete the hot region on the map
- Add/edit/delete hot spots (camera/alarm input/alarm output/door/elevator/radar /UVSS/third-party resource) on the map
- Add labels with description on the map
- Locate resource groups on the map

- Person management
  - Add person group
  - Enroll credentials (card numbers, fingerprints, faces) by Enrollment Station
  - Link person group with access group and attendance group
  - Add person information one by
- Dock station group
  - Group persons into dock station groups
  - Link dock station(s) to dock station group and the videos and pictures on the person's body cameras can be copied to the linked dock station(s)
- Role & User management
  - The default password of the admin user must be changed at first-time login.
  - Support changing the password of the admin user
  - The admin user can reset other users' password
  - The user account will be frozen for 30 minutes after 5 failed password attempts
  - Add/edit/delete roles and users
  - Role's permission applicable for rental scenario
  - Assign permission schedule template to role to define when the role's permissions are valid
  - Roles can be assigned with different permissions, including area display rule, resource access, and user permissions
  - Two default roles are supported: administrators and operators
  - The role name, expiry date, and text description can be set for the roles
  - The users can be assigned with the roles to obtain the corresponding permissions
  - The user name, expiry date, and text description can be set for the users
  - Customize the properties of person addition information, which are not pre-defined in the system
  - Import information of multiple persons in a batch by importing an Excel file
  - Import information of multiple persons in the domain in a batch
  - Import multiple persons' profiles in a batch
  - Import person information from devices, including access control devices, encoding devices, facial recognition servers, and Enrollment Stations
  - Profile format: JPG, JPEG, and PNG
  - Verify face quality by added access control device when collecting profiles by added device
  - Issue cards to multiple persons in a batch
  - Report card loss for person if the card is lost, and issue a temporary card
  - Cancel card loss if the lost card is found
  - Set credentials under duress and credentials for dismiss for persons
  - Link person with indoor station

- Two types of user status are supported: active and inactive
- Set an email address for the added user so that he/she can reset the password via email if he/she forgot the password
- Domain users can be imported in batches
- The user can be forced to logout by the admin user

- Security settings
  - Lock IP address for configurable duration when reaching the configured failed password attempts
  - Set the minimum password strength
  - Set the maximum password age
  - Lock the Control Client after a time period of inactivity
- System configuration & maintenance
  - Create a name for the current site
  - Set the first time of the week
  - Set the unit for the temperature
  - Enable GIS map function, configure the map API URL, and customize the icons of hot region and hot spot
  - Set the threshold for the SYS server's CPU usage and RAM usage
  - NTP settings
  - Active directory settings
  - Link person information in the domain with the person information in the system
  - Allow the system to receive the configured generic events.
  - For Central System, allow Remote Site registration
  - For Remote Site, register Remote Site to Central System
  - Allow devices of earlier ISUP protocols to access the system or not
  - A static IP address or a domain name can be set for the WAN access
  - Set network timeout (default waiting time) for the configurations on the Web Client
  - Set device access mode as automatically judge or proxy mode
  - SYS server NIC settings
  - Set the retention period for storing the data recorded in system
  - Enable evidence collection so that operators can save video footage as evidence on the Control Client



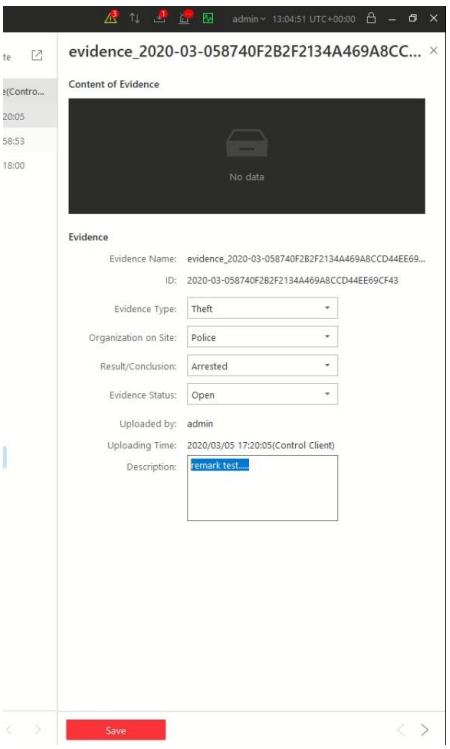
- Set unique IDs for the cameras in the system

  - Set transfer protocol as HTTP or HTTPS
  - Enable encrypted transmission between ADS and SYS
  - Add fuzzy matching rules for license plate search
  - System hot spare settings
  - Third-party system integration settings
  - Data interchange settings including database synchronization and access records dump
  - Reset network information of added devices
  - Export service component certificate from SYS server
  - Set open platform
  - Set database password
- Backup and restore database
- Live view
  - Manual recording
  - Capture
  - Instant playback
- Playback
  - Play the recorded video of the cameras
  - Playback by timeline
  - Playback for up to 16 cameras
  - Download the recordings for backup
  - Reverse playback
  - Playback frame-by-frame
  - Single-frame backward
  - Slow forward/fast forward
  - Turn on/off the audio in playback; adjust the volume
  - Video clipping and capture
  - Display video parameters
  - Customize playback speed
  - Select storage location and stream type for playback
- Local configuration
  - Set the network transmission settings
    - ✓ GPU hardware decoding
    - ✓ Set the window proportion threshold for switching between main stream or sub-stream
    - ✓ Network timeout: default waiting time for the operations in Applications on the Web Client
    - ✓ Video caching: small (1 frame)/medium (6 frames)/large (15 frame)
    - ✓ Captured picture format: JPEG/BMP
    - ✓ Device access mode: restore default/automatically judge/directly access/proxy
  - View local saving path of videos or pictures

Control Client

- Customize the module arrangement on the control panel

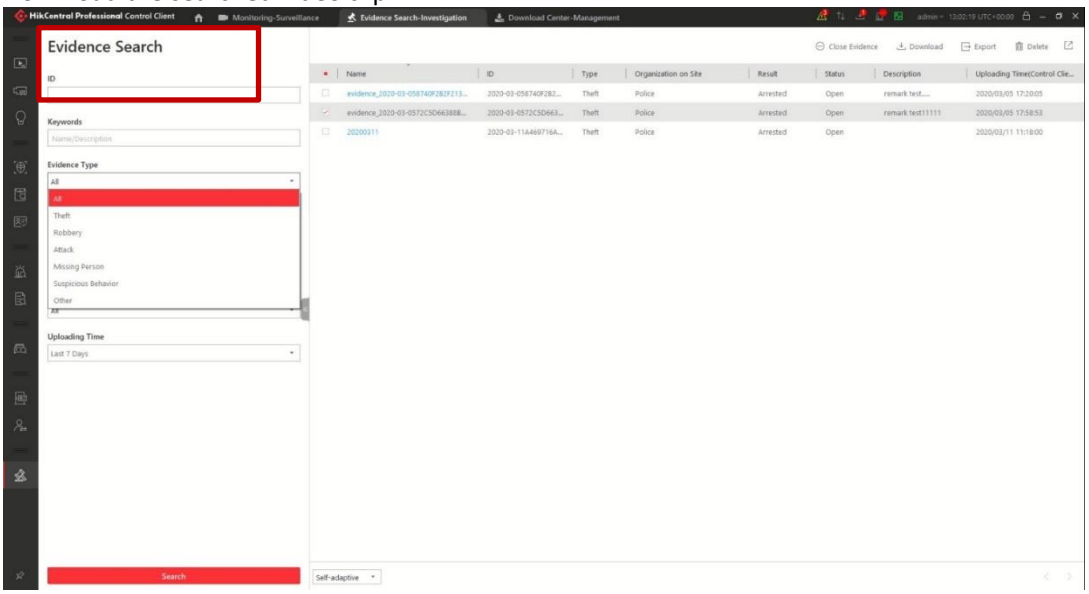
- GPU hardware decoding
- Access to SYS via IP address and domain name
- Log in with the domain user
- The user account will be frozen after 5 failed password attempts
- Playback
  - Normal playback for continuous recordings
  - Async/Sync playback for up to 16 cameras
  - Add default, customized tag to mark the important video footage
  - Play the tagged video footage



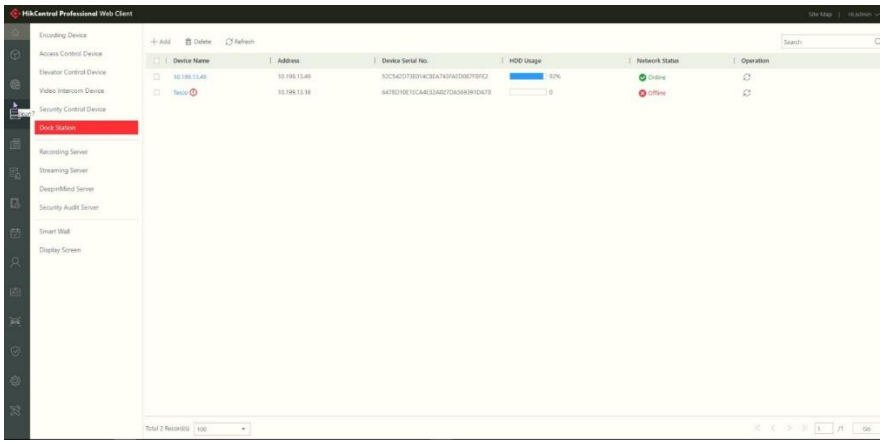
  - Play by files/timeline
  - Lock/unlock the video file for file protection
  - Download the video files
  - Reverse playback
  - Single-frame backward
  - Playback frame-by-frame
  - Slow forward/fast forward
  - Customize high speed playback settings
  - Turn on/off the audio in playback; adjust the volume
  - Provide video thumbnail on the timeline
  - Capture
  - Extract frames to play the images one by one
- Map control
  - View the geographic locations of resources on the map
  - View resource groups on map
  - Jump to the hot region map
  - Zoom in/out on the map
  - Select resource(s) on the map
  - Add labels with description on the map

- Print map
- Search and view access records

- Video search
  - Search video files stored on local devices or Recording Server
  - Search the video clip by time range
  - Search tagged/locked video
  - Search in storage location in Main Storage or Auxiliary Storage
  - Search the video/picture/audio stored on dock station
  - Play the searched video clip
  - Download the searched video clip



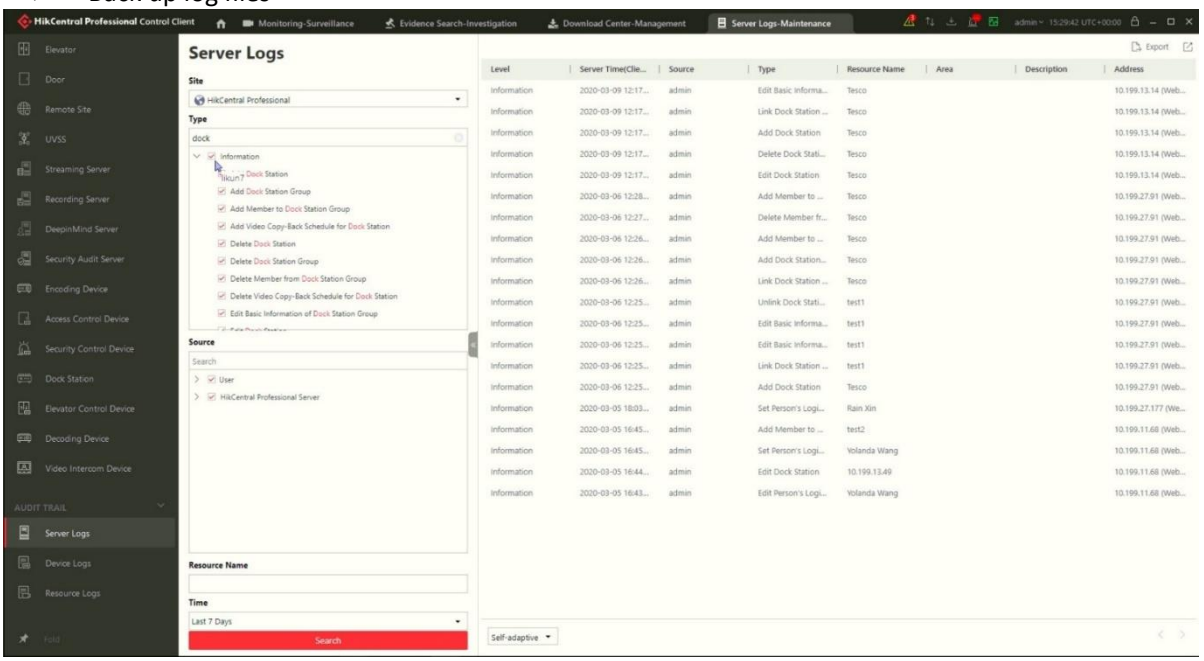
- Device status monitoring
  - History status overview of the managed resources including online rate, device online rate, and recording integrity rate
  - Detailed status page of cameras, encoding devices, doors, elevators, UVSSs, access control devices, elevator control devices, video intercom devices, security control devices, dock stations, Remote Sites, decoding devices, Recording Servers, Streaming Servers, DeepinMind servers, security audit servers
  - Set stream type for the resources to main stream, sub-stream, smooth stream, or restore to global stream



- Tools
  - VSPlayer
  - Broadcast

- Alarm Output
- Two-Way Audio
- Arming Control

- Download center
  - Check the downloading tasks and status
  - Continuous transmission on the breakpoint
  - Download the player for playing back the video footage
  - Arrange an off-peak time period to automatically download footage
- Audit Trail (The actions of the operators for the users can be logged)
  - Search log files of SYS, Remote Site, cameras, and smart walls that are connected to the system
  - Back up log files



- System settings
  - Configure general parameters
    - ✓ Global Stream: main stream, sub-stream, smooth stream for global usage
    - ✓ Set the window proportion threshold for switching between main stream or sub-stream
    - ✓ Network timeout: the default waiting time for the Control Client
    - ✓ Picture format: JPEG/BMP
    - ✓ Maximum mode: Maximize/Full Screen
    - ✓ Time zone: Device time or client time
    - ✓ Show time difference
    - ✓ Upper limit of bandwidth for downloading video from pStor
    - ✓ Auto-login
    - ✓ Resume last interface: Display control panel, specified view, or last interface
    - ✓ Display the number of each window
  - Configure image parameters
    - ✓ View scale: full screen or original resolution
    - ✓ Window scale: 4:3 or 16:9
    - ✓ Video caching: small (1 frame), medium (6 frames), or large (15 frames)

- ✓ Continuous decoding
- ✓ Enable/disable highlight for Motion
- ✓ Enable/disable VCA rule
- ✓ Enable/disable GPU hardware decoding
- ✓ Enable/disable display transaction information on live view and playback image
- ✓ Enable/disable display temperature information on live view and playback image

➢ Configure local saving path of videos/pictures/packages
➢ Configure keyboard and joystick parameters
➢ Configure live view and playback settings
- ✓ Configure icons on live view and playback toolbar
- ✓ Enable/disable toolbar display

➢ Set screen position according to real layout in order to switch screen by keyboard conveniently
➢ Set alarm sounds by local audio files or voice engine (require support of the OS)
➢ Set the refresh interval of resource status in Health Monitoring

● Software Specification

● The following table shows the maximum performance of the HikCentral Professional server. For other detailed data and performance, refer to *Software Requirements & Hardware Performance*.

Features		Maximum Performance
General	Cameras	Centralized Deployment: 3,000① Distributed Deployment: 10,000② Central System (RSM): 100,000③
	Managed Device IP Addresses **Including Encoding Devices, Access Control Devices, Elevator Control Devices, Security Control Devices, and Remote Sites*	Centralized Deployment: 1,024① Distributed Deployment: 2,048②
	Video Intercom Devices	1,024
	Alarm Inputs (Including Alarm Inputs of Security Control Devices)	3,000
	Alarm Outputs	3,000
	Dock Stations	1,500
	Security Radars	10
	Alarm Inputs of Security Control Devices	2,048
	DS-5600 Series Face Recognition Terminals When Applied with Hikvision Turnstiles	32
	Recording Servers	64
	Streaming Servers	64
	Security Audit Server	8
	Areas	3,000
	Cameras per Area	256
	Alarm Inputs per Area	256
	Alarm Outputs per Area	256

Recording	Recording Schedule	10,000
	Recording Schedule Template	200
Event & Alarm	Event and Alarm Rules	Centralized Deployment: 3,000 Distributed Deployment: 10,000 Central System (RSM): 10,000
	Storage of Events or Alarms without Pictures	Centralized Deployment: 100/s Distributed Deployment: 1000/s
	Events or Alarms Sent to Clients **The clients include Control Clients and Mobile Clients.*	120/s 100 Clients/s
Picture	Picture Storage **Including event/alarm pictures, face pictures, and vehicle pictures.*	20/s (Stored in SYS Server) 120/s (Stored in Recording Server)
Data Storage	Data Retention Period	Stored for 3 Years
	Operation Logs	5 million
	Service Information Logs	5 million
	Service Error Logs	5 million
	Recording Tags	60 million
Users and Roles	Concurrent Accesses via Web Clients, Control Clients, and OpenAPI Clients	100
	Users	3,000
	Roles	3,000
Streaming Server's Maximum Performance		
Video Input Bandwidth per Streaming Server		300 × 2 Mbps
Video Output Bandwidth per Streaming Server		300 × 2 Mbps

- ①: For one site, the maximum number of the added encoding devices, access control devices, and security control devices in total is 1,024. If the number of the manageable cameras (including the cameras directly added to the site and the cameras connected to these added devices) exceeds 3,000, the exceeded cameras cannot be imported to the areas.
- ②: For one site with Application Data Server deployed independently, the maximum number of the added encoding devices, access control devices, and security control devices in total is 2,048. If the number of the manageable cameras (including the cameras directly added to the system and the cameras connected to these added devices) exceeds 10,000, the exceeded cameras cannot be imported to the areas.
- ③: For one site, if the number of the manageable cameras (including the cameras managed on the current site and the cameras from the Remote Sites) in the Central System exceeds

100,000, the exceeded cameras cannot be managed in the Central System.

- ④: This recommended value refers to the number of thermal cameras connected to the system directly. It depends on the maximum performance (data processing and storage) in the situation.
- when the managed thermal cameras uploading temperature data to the system. For thermal cameras connected to the system via NVR, there is no such limitation.

Hardware Specification

Processor	Intel® Xeon® E-2124	
Memory	16G DDR4 DIMM slots, Supports UDIMM, up to 2666MT/s, 64GB Max. Supports registered ECC	
Storage Controllers	Internal Controllers: SAS_H330 Software RAID: PERC S140 External HBAs: 12Gbps SAS HBA (non-RAID) Boot Optimized Storage Subsystem: 2x M.2 240GB (RAID 1 or No RAID), 1x M.2 240GB (No RAID Only)	
Drive Bays	1T 7.2K SATA×2	
Power Supplies	Single 250W (Bronze) power supply	
Dimensions	Form Factor: Rack (1U) Chassis Width: 434.00mm (17.08 in) Chassis Depth: 595.63mm (23.45 in) (3.5″ HHD) Note: These dimensions do not include: bezel, redundant PSU	
Dimensions with Package (W × D × H)	750 mm × 614 mm × 259 mm (29.53" × 24.17" × 10.2")	
Net Weight	12.2kg	
Weight with Package	18.5kg	
Embedded NIC	2 x 1GbE LOM Network Interface Controller (NIC) ports	
Device Access	Front Ports: 1x USB 2.0, 1 x IDRAC micro USB 2.0 management port Rear Ports: 2 x USB 3.0, VGA, serial connector	
Embedded Management	iDRAC9 with Lifecycle Controller iDRAC Direct DRAC RESTful API with Redfish	
Integrations and Connections	Integrations: Microsoft® System Center VMware® vCenter™ BMC Truesight (available from BMC) Red Hat Ansible	Connections: Nagios Core & Nagios XI Micro Focus Operations Manager i (OMi) IBM Tivoli Netcool/OMNIbus

Operating Systems	Microsoft Windows Server® with Hyper-V


See Far, Go Further