HikCentral Professional V1.6.0
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

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

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

Streaming Service

- Forwards and distributes audio and video data

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
  - ➢ Set added cameras as facial recognition cameras, ANPR cameras, and thermal cameras (report supported)
- ● Encoding device management
  - ➢ Multiple devices can be added: network cameras, network speed domes, video encoders, NVRs, etc.
  - ➢ Create password for inactive encoding device(s)
  - ➢ The password strength of the added encoding device can be checked by the system for security purpose
  - ➢ Six adding modes for encoding devices in Hikvision private protocol available:
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device IP address or domain name
    - ✓ By adding the devices added to a Hik-Connect account
    - ✓ By specifying an IP segment
    - ✓ By specifying a port segment
    - ✓ By importing in a batch
  - ➢ Four adding modes for encoding devices in Hikvision ISUP protocol available:
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device ID and key
    - ✓ By specifying an ID segment
    - ✓ By importing in a batch
  - ➢ Five adding modes for encoding devices in standard ONVIF™ protocol available:
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device IP address or domain name
    - ✓ By specifying an IP segment
    - ✓ By specifying a port segment
    - ✓ By importing in a batch
  - ➢ Set time zone for the device
  - ➢ For device added in Hikvision private protocol, set mapped port if necessary
  - ➢ Limitation of bandwidth for video downloading for specific NVRs
  - ➢ N+1 hot spare for the added NVRs
- ● Access control device management
  - ➢ Create password for inactive access control device(s)
  - ➢ The password strength of the added access control device can be checked by the system for security purpose
  - ➢ Four adding modes for access control devices in Hikvision private protocol 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 importing in a batch
  - ➢ Four adding modes for access control devices in Hikvision ISUP protocol available (a recording server is required):
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device ID and key

    - ✓ By specifying an ID segment
    - ✓ By importing in a batch
  - ➢ Set time zone for the device
- Elevator control device management
  - ➢ Create password for inactive elevator control device(s)
  - ➢ The password strength of the added elevator control device can be checked by the system for security purpose
  - ➢ Four adding modes for elevator control devices in Hikvision private protocol 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 importing in a batch
  - ➢ Set time zone for the device
- Video intercom device management, including indoor station, door station, outer door station, and master station
  - ➢ Create password for inactive video intercom device(s)
  - ➢ The password strength of the added video intercom device can be checked by the system for security purpose
  - ➢ Three adding modes for elevator control devices in Hikvision private protocol available:
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device IP address
    - ✓ By importing in a batch
  - ➢ Set device location information
  - ➢ For indoor stations, set related resident (person) information
  - ➢ Set time zone for the device
  - ➢ Relate camera with indoor station
- Security control device management
  - ➢ Create password for inactive security control device(s) (such as security control panel, panic alarm station, etc.)
  - ➢ The password strength of the added security control device can be checked by the system for security purpose
  - ➢ Six adding modes for security control devices in Hikvision private protocol available:
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device IP address
    - ✓ By adding the devices added to a Hik-Connect account
    - ✓ By specifying an IP segment
    - ✓ By specifying a port segment
    - ✓ By importing in a batch
  - ➢ Three adding modes for security control devices in Hikvision ISUP protocol available:
    - ✓ By detecting online devices in the same subnet with the SYS server or current PC
    - ✓ By specifying the device ID and key
    - ✓ By specifying an ID segment
    - ✓ By importing in a batch
  - ➢ Set time zone for the device

- 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
- Display screen management: Add display screen by IP address
- 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
- DeepinMind Server management
  - Add facial recognition server by IP address
  - Add behavior analysis server by IP address
  - Provides WAN access
  - Link cameras and face comparison group(s) with facial recognition server
  - Link cameras with behavior analysis server and set analysis task
- 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 (cameras, alarm inputs, alarm outputs, doors, elevators, UVSSs, and third-party integrated 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.

- Configure visual tracking by associating one camera with other cameras nearby, so that you can track an individual (such as a suspect) across different areas without losing sight of the individual.
- Edit door's parameters
  - Edit basic information
    - ✓ Door contact: Normally Open / Normally Closed
    - ✓ Exit button type: Normally Open / Normally Closed
    - ✓ Open duration(s)
    - ✓ Extended open duration(s)
    - ✓ Door open timeout alarm
    - ✓ Duress code
    - ✓ Super password
    - ✓ Dismiss code
    - ✓ Free access schedule
    - ✓ Access forbidden schedule
  - Set related camera(s) to view the video on Control Client
  - Set picture storage for video access control terminal
  - Edit application settings
    - ✓ Entry & exit counting
    - ✓ Multi-door interlocking
    - ✓ Anti-passback
    - ✓ Open door with first card
    - ✓ Multi-factor authentication
  - Edit hardware settings
    - ✓ Edit card reader related parameters: OK LED Polarity, Error LED Polarity, Buzzer Polarity
    - ✓ Set card reader's access mode
    - ✓ Set minimum card swiping interval
    - ✓ Specify the seconds after which the entry on keypad will be reset
    - ✓ Enable failed card attempt alarm
    - ✓ Enable tampering detection
  - Link facial recognition terminals with turnstile
  - Set door as attendance checkpoint and set attendance type: Check-In Out, Check-Out Only, Check-In/Out
  - Set event for the door
  - Locate the door on the map
- Edit elevator's parameters
  - Edit basic information
    - ✓ Open duration(s)
    - ✓ Extended open duration(s)
    - ✓ Elevator door open timeout alarm
    - ✓ Duress code
    - ✓ Super password

    - Dismiss code
  - Set floors of the elevator
    - Free access schedule
    - Access forbidden schedule
    - Access level
    - Edit floor name
    - Reset imported floor No.
  - Set related camera(s) to view the video on Control Client
  - Edit hardware settings
    - Edit card reader related parameters: OK LED Polarity, Error LED Polarity, Buzzer Polarity
    - Set card reader's access mode
    - Set minimum card swiping interval
    - Specify the seconds after which the entry on keypad will be reset
    - Enable failed card attempt alarm
    - Enable tampering detection
  - Set event for the elevator
  - Locate the elevator on the map
- Edit radar's parameters
  - Edit basic information including name
  - Add radar on map
  - Set GPS location of the radar on the map
  - Configure radar zone on the map
  - Set related calibrated cameras
- 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
    - Camera events: motion, video loss, line crossing, etc.
    - Door events: normal card swiping, abnormal card swiping, etc.
    - Elevator events: normal card swiping, abnormal card swiping, etc.
    - Radar events
    - Device alarm input (including zones) events
    - Person event for face comparison (face matched or mismatched)
    - ANPR event (license plate matched or mismatched)

  - ✓ UVSS exceptions: UVSS online or offline
  - ✓ Parking lot event: Calling center, overstayed, parking in forbidden period, Vehicle matched or mismatched
  - ✓ 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
- ➢ Active control for events and alarms to avoid same event/alarm triggered in short time
- ➢ Set event linkage actions such as recording, creating tag, capturing pictures, linking access points, linking alarm outputs, PTZ actions, linking integrated third-party resources, sending emails, and triggering user-defined 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
- ➢ Detect camera alarms, door alarms, elevator alarms, radar alarms, alarm input alarms, ANPR alarms, UVSS alarms, person alarms, parking lot alarms, 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
- Vehicle management
  - Add vehicle list and set its name, color, entry & exit rule, parking space control, effective period, etc.
  - Add vehicle information to the vehicle list one by one
  - Enter vehicle owner information for each vehicle
  - Import vehicle information according to the pre-defined template
  - Set effective period for the added vehicles
  - Set undercarriage picture for each vehicle
  - Export vehicle information
- Parking lot management
  - Add one parking lot and set capacity, number of free parking spaces, maximum parking duration, and expiration prompt
  - Add entrance and exit for the parking lot
  - Add lanes for entrance and exit
    - ✓ Set lane type as entrance or exit
    - ✓ Link capture unit with lane
    - ✓ link a video intercom device or access control device with the lane for video intercom or opening barrier by swiping card
    - ✓ Link display screen with lane
    - ✓ Set device which controls to open the barrier: capture unit or device for video intercom or opening barrier by swiping card
  - If you have linked one display screen with the lane, set contents displayed on the screen
  - Set entry & exit rule
    - ✓ set rule for vehicles in the vehicle list: automatically or manually open the barrier gate when detecting vehicles in the vehicle list
    - ✓ Set rule for vehicles not in the vehicle list: automatically or manually open the barrier gate
    - ✓ Set schedule for the rules
- 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 one

  - 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
- Access control
  - Group persons with same access permission into access groups
  - Link access group with person group
  - Group access points into access levels and set schedule to define the authorized time periods
  - Assign the access level to access group
  - Apply all the access groups to device manually or regularly
  - Set access control schedule including weekly schedule and holiday schedule
  - Set anti-passback rule
  - Set multi-door interlocking rule
  - Set multi-factor authentication rule
  - Set entry & exiting counting rule
  - Set emergency operation group for operating the access points in the group in emergency
  - Quick start of access control
  - Access control test which tests whether the configurations about access control are set correctly and completely and whether the devices are running properly.
- Visitor management
  - Add visitor group
  - Add visitor one by one
  - Import information of multiple visitors in a batch by importing an Excel file
  - View and delete visitors in visitor list
  - Apply visitor's access levels to device
  - Visitor check-out: manually check-out and automatically check-out
- Time and attendance
  - Group persons into attendance groups
  - Link attendance group with person group
  - Add normal shift schedule
  - Add man-hour shift schedule

  - Assign shift schedule to attendance group
  - Set attendance parameters
    - ✓ Define weekends
    - ✓ Define absence
    - ✓ Set overtime parameters
    - ✓ Add attendance check point
    - ✓ Manage leave type
  - Search attendance records
  - Handle attendance records
    - ✓ Correct single person’s attendance record
    - ✓ Correct multiple persons’ attendance records
    - ✓ Apply for leave for single person
    - ✓ Apply for leave for multiple persons
  - Manually calculate attendance results
  - Get attendance records from device
  - Set display rule for attendance reports
  - Export attendance reports
- Face comparison
  - Group persons into face comparison groups
  - Set similarity threshold when adding face comparison
  - Apply the face comparison group to device
- Security control
  - Import added security control panel's alarm inputs into different security control partitions according to the relation between zones and partitions configured on device
  - Set defense schedule to define when and how to arm the alarm inputs
- 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

  - 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
  - PTZ control permission level (1~100) can be set
  - 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
  - Pre-define schedule templates including recording schedule, arming schedule, access schedule, permission schedule, and defense schedule
  - Pre-define email templates
  - Pre-define rules for regular report so that the system can send a report to the receivers regularly, with content including events, alarms, passing vehicles, people counting, queue status, heat map, pathway analysis, temperature, attendance records, device logs, resource logs, etc.
  - 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 frequency for health check
  - Set working mode as face recognition terminals or access control terminals for the managed DS-5600 face recognition series

- 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

Supported Database Type	Version
Microsoft® SQL Server	2008 R2 and above
PostgreSQL	9.6.2 and above
MySQL	8.0.11 and above

- Reset network information of added devices
- Export service component certificate from SYS server
- Set open platform
- Set database password
- Set SUP upgrade prompt

- Backup and restore database
- Live view
  - View real-time video from the cameras on the current site or cameras imported from a Remote Site
  - PTZ control
  - Manual recording
  - Capture
  - Instant playback
  - Digital zoom
  - Two-way audio
  - Switch between main stream or sub-stream
  - Display live view parameters.
  - Turn on/off the audio in live view; adjust the volume
  - Set the window division
  - POS Live View
    - ✓ Display transaction data alongside corresponding video
    - ✓ Transaction information video overlay/separate display
- Playback
  - Play the recorded video of the cameras on the current site and cameras imported from a Remote Site
  - 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

    - Set the window division
    - Digital zoom
    - Display video parameters
    - Customize playback speed
    - Select storage location and stream type for playback
- Local configuration
    - Set the network transmission settings
        - ✓ GPU hardware decoding
        - ✓ Stream type for global usage: main stream, sub-stream, and smooth stream
        - ✓ 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
- Intelligent analysis
    - Report dashboard
    - People counting report
    - Queue analysis report
    - Heat analysis report
    - Pathway analysis report
    - Person feature analysis report
    - Temperature analysis report
    - Vehicle analysis report

Control Client

- Customize the module arrangement on the control panel
- GPU hardware decoding
- Receive alarm
- 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
- The window division is self-adaptive according to the number of cameras under live view or playback
- Live view
    - View real-time video from the cameras on current site or cameras imported from Remote Site
    - PTZ control
    - PTZ control lock/unlock
    - Public view and private view

- Auto-switch one area's cameras
- Auto-switch one view's cameras
- Auto-switch one view group's views
- Manual recording
- Capture
- Instant playback
- Visual tracking
- Auxiliary screen preview
- Digital zoom
- Two-way audio
- Turn on/off the audio in live view; adjust the volume
- Camera status detection
- Arming control
- Switch the live view stream to main stream, sub-stream, or smooth stream
- Start live view on smart wall
- View fisheye camera's live view in fisheye dewarping modes
- View detected events in live view, including resource events, face comparison events, access events, and recognized vehicle events

- Playback
  - Normal playback for continuous recordings
  - VCA playback based on motion analysis/intrusion/line crossing events
  - Async/Sync playback for up to 16 cameras
  - Playback in fisheye dewarping mode
  - Add default, customized tag to mark the important video footage
  - Play the tagged video footage
  - Play by files/timeline
  - Visual tracking
  - 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
  - Accurate positioning for playback
  - Digital zoom
  - Video clipping
  - Capture
  - Camera status detection
  - Arming control
  - Switch the video stream to main stream, sub-stream, or smooth stream
  - Playback on smart wall

    - Transcoding playback
    - Extract frames to play the images one by one
- Manage captured pictures and recorded/clipped video footage during live view and playback which are stored in local PC
- Map control
    - View the geographic locations of resources on the map
    - Get the live view and playback of the cameras and other related cameras of the resources on the map
    - Arming control: arm and disarm cameras, alarm inputs, UVSSs, doors, and other resources on the map
    - Search and view history alarms of cameras, alarm inputs, UVSSs, doors, and other resources on the map
    - Get a notification message on the map when alarm is triggered
    - 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
    - Locate resource on the map
    - View the live video or playback of the resources on the map
    - Control access points on map
    - Search and view access records
- Alarm center
    - Display alarm info including alarm time, alarm name, alarm status, etc.
    - Display system alarm info including time and description
    - Play the video from the alarm time
    - Visual tracking
    - View the live video from the related camera
    - Play the alarm related video on smart wall
    - Add a tag to the alarm information
    - Acknowledge an alarm with a text description
    - Acknowledge multiple alarms in a batch
    - Arming control for alarms
    - Sort alarms by the selected property
    - Clear alarms manually
    - Enable/disable the alarm audio
    - Enable/disable alarm triggered pop-up window
    - Search event log files and alarm log files
    - Manually trigger user-defined event
- ANPR control
    - View ANPR camera’s live view and view recognized license plate number
    - Mark the detected vehicle
    - Add the new detected vehicle to the vehicle list

  - Search logs of vehicle license plate recognized by the camera and the related vehicle passing information
  - Search logs of passing vehicles with no license plate
- UVSS control
  - View UVSS’ live view and view captured undercarriage pictures of the passing vehicles and license plate number
  - Mark on undercarriage picture
  - Mark the detected vehicle
  - Add the new detected vehicle to the vehicle list
  - Search logs of vehicle license plate recognized by the camera and the related vehicle passing information
- Entrance & exit control
  - View information of vehicles entered or exited from the parking lot
  - Add the new detected vehicle to the vehicle list
  - Search logs of recognized vehicle license plate and the related vehicle passing information
  - Open barrier automatically according to the configured entry & exit rule
  - Open barrier automatically after the vehicle owner swiping her/his card
  - Open barrier manually and enter remark information (optional)
  - Open barrier manually during video intercom
  - Correct the license plate numbers recognized by capture units
  - Barrier control to open, close, or remain the barrier open
- Face comparison
  - View capture camera's live view and view detected and matched persons
  - View the face comparison information
  - Add mismatched persons to person list
  - Upload a face picture to search the video when the face picture captured
  - Subscribe to receive face matched/mismatched events from all the face comparison groups
  - Search capture face pictures and related video by uploading a picture
  - Search matched face pictures and related video by selecting face comparison groups
  - Search frequently appeared persons
  - Search archives
  - Identity verification
- Access control and elevator control
  - View live videos of door or elevator's related camera(s)
  - Play back the recorded video footage of door/elevator’s related camera(s)
  - Visual tracking
  - Control doors to lock, unlock, remain locked, or remain unlocked during live view
  - Control floors status as temporary access, access with credential, free access, or access forbidden during live view
  - Control all doors/elevators or part of them by emergency operation group
  - View the card swiping record in real time
  - Search the access records triggered on the added access points

  - Subscribe to receive access events from all the access points
  - Door and Elevator module to control door and elevator status
  - Forgive anti-passback violations
  - Entry & exit counting
  - Open door for multi-factor authentication
  - Handle opening door request from video access control terminal
- Video intercom
  - View live videos of door's related camera(s)
  - Control doors to lock, unlock, remain locked, or remain unlocked during live view
  - Call the added indoor station for starting voice talk with the resident, viewing the video of the indoor station's camera, etc.
  - Answer the call from the added door station and open door if needed
- Security control
  - View live video of the radar's calibrated cameras
  - Arm or disarm partitions
  - Bypass zones
  - Bypass recovery
  - Clear alarms
- 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 transaction event by entering the keywords in POS information
  - Search ATM event by entering card number that is contained in the ATM information
  - Search the video/picture/audio stored on dock station
  - Set VCA rules to search the video where a VCA event occurs
  - Play the searched video clip
  - Visual tracking
  - Download the searched video clip
- Intelligent analysis report
  - Report dashboard
  - People counting report: Generate a report for the added people counting camera(s) to view the number of people entered, exited, or both entered and exited
  - Queue analysis report: Generate a report to show the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length
  - Heat analysis report: Generate a report to analyze the visit times and dwell time of customers
  - Pathway analysis report: Generate a report to analyze the people counting on the pathways in shopping mall
  - Person feature analysis report: Generate a report to analyze features (including age and gender) of recognized human faces
  - Temperature report: Generate a report to show the number of exceptions

    (temperature too high or too low) and maximum/minimum temperature of different thermometry points
  - Vehicle analysis report: Generate a report to show the number of passing vehicles detected by the ANPR cameras during specified time period
  - Export report and save in local PC
- Health monitoring
  - Real-time status overview of the resources, including cameras, access points, UVSSs, encoding devices, access control devices, elevator control devices, video intercom devices, security control devices, dock stations, Remote Sites, decoding devices, SYS servers, Recording Servers, Streaming Servers, and facial recognition servers
  - 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
- Smart Wall
  - Smart Wall (Decoding Device)
    - ✓ Decode and display the video streams from the camera on the smart wall
    - ✓ View camera status
    - ✓ Switch the live view stream to main stream or sub-stream
    - ✓ PTZ control
    - ✓ Window division
    - ✓ Switch to playback
    - ✓ View auto-switch
    - ✓ Area's cameras auto-switch
    - ✓ Create a roaming window
    - ✓ Enlarge and restore window
    - ✓ View alarm's related video on smart wall
    - ✓ View and export window No. and camera ID
  - Smart Wall (Graphic Card)
    - ✓ Display all contents (cameras, access points, maps, face comparison groups) in live view on smart wall
    - ✓ Display camera on smart wall
    - ✓ Display area on smart wall
    - ✓ Display map on smart wall
    - ✓ Display view and view group on smart wall
    - ✓ Display alarm's related video on smart wall
    - ✓ Display health monitoring page on smart wall
    - ✓ Display GPU usage of graphics card
- 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
  - 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

Mobile Client

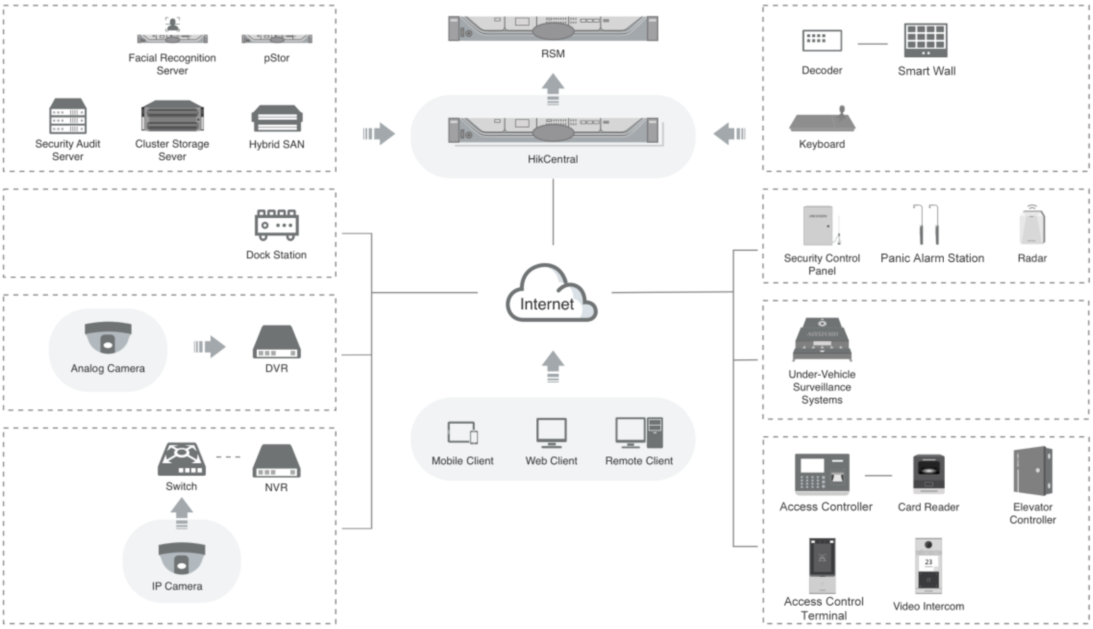
- Access to the SYS via IP address
- Log in with normal user or domain user
- Log in with HTTP or HTTPS transfer protocol
- The user account will be frozen after 5 failed password attempts
- Add/remove cameras to/from My Favorites
- Search cameras in different sites
- Live view
  - View real-time video from the cameras
  - View real-time video from the access point's related camera(s)
  - View real-time video from the UVSS's camera (only for tablet)
  - View real-time video from the elevator control device's related camera(s)
  - View real-time video from the radar's related camera(s)
  - View real-time video from the door station's related camera(s)
  - Receive card-swiping events when viewing real-time video from the door station's related camera(s)
  - PTZ control
  - Turn on/off the audio in live view
  - Set the video quality
  - Manual recording
  - Capture
  - Two-way audio
  - Digital zoom
  - Slide on the image to realize fisheye dewarping
  - Lock/unlock door manually
  - Set the access level (temporary access, access with credential, free access, or access forbidden) for each floor linked to the elevator control device
  - Arm/Disarm radar
  - Display persons' real-time access events, including person profile, person name, and access results
  - Display information of face comparison events, including captured face picture, time, captured camera, etc.
  - View the recognized passing vehicle (including motorcycle) information, including license plate number and passing time
  - View the detected passing vehicle information, including real-time undercarriage picture, configured undercarriage picture, vehicle picture, license plate number and passing time (only for tablet)
  - Mark on the captured real-time undercarriage picture (only for tablet)
  - Add new vehicle to the vehicle list
  - View the person's face comparison information (real-time and history), including

  captured face picture, person details, captured time, and similarity
  - Add mismatched person into person list
  - Add mismatched vehicle into person list
  - Trigger user-defined event manually
  - Switch stream type (main stream, sub stream, or smooth stream) for a channel
  - Set main stream or sub-stream as the default stream type for accessing the resources of all the encoding devices
- Playback
  - Play back one channel or simultaneously play back multiple channels
  - Search by date/storage mode
  - Provide three storage modes: encoding devices, Hybrid SAN, and Cloud Storage Server
  - Playback the recordings
  - Turn on/off the audio in playback
  - Video clipping
  - Capture
  - Synchronous playback
  - Digital zoom
  - Switch the video stream to main stream or sub-stream
  - Slide on the image to realize fisheye dewarping
  - Transcoding playback
  - PIP mode
  - Scale up or scale down the playback timeline bar
  - Add tags to a specific video footage which contains important information
- View mode
  - View public view and private view
  - Live view and playback in view mode
- Video Intercom
  - Receive call(s) from door station(s)
  - Switch calls to answer if there're multiple incoming calls simultaneously
  - Open door when answering a call
- Third-party Integrated Resource
  - Operate the third-party integrated device based on the device capability set obtained by the system
  - Locate the device on map
- Receive alarms
  - Receive and display alarm notification and view alarm related live video or recording
  - View the alarm time of current site and Remote Site
  - Filter alarms by alarm priority, alarm status, alarm category
  - View alarm sources on related maps
  - Acknowledge alarm(s)
  - View logs of the calls from door stations
  - View notifications about calls from door stations
  - View alarm-related instant video (7s) on the alarm details page to determine if the alarm is a false alarm (only supported by Axiom Hub security control panel)

- Display alarms of security control devices in real-time
- Display the camera details including online status, PTZ control, etc.
- Turnstile and face recognition devices accessible, and you can control them such as opening/closing door
- Add person information
- Add person information to face comparison group
- Map control
    - View the geographic locations of resources on the map
    - Get the live view and playback of the cameras, UVSSs, and doors on the map
    - Search and view history alarms of cameras, alarm inputs, UVSSs, and doors on the 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
    - Locate resource on the map
    - View the live video or playback of the resources on the map
    - Control status of the doors linked to access controllers
    - Open and close doors linked to door stations
    - Display the moving pattern of the object detected by the radar
    - Search and view access records
    - Operate the third-party integrated device on map
- Subscribe events of all the access points and all face comparison groups (only for tablet)
- Search
    - Search video: search tagged video and VCA event related video
    - Search passing vehicle logs: search records of passing vehicles and view vehicle details
    - Search access records: search the persons' access records and view the access details including person details and door information
    - Search Persons:
        - Search the face pictures matched with the pictures in the selected face comparison group(s) during the selected time periods, and view the result details including match time, related video footage, and related picture.
        - Search the captured pictures persons in the selected person list captured by the selected camera(s) during the selected time periods.
        - Search the frequently appeared persons captured by the selected cameras during the selected time period, and view the result details including captured time, related video footage, and related picture.
        - Search the records captured pictures) in stranger libraries of the selected face comparison devices and the history face comparison records of the selected face comparison groups.
        - Search for a specific person's identity by uploading his/her face picture and setting a similarity threshold.
    - Add person to person list
- BI report (only for tablet)
    - Heat map report

  - Temperature report
  - Queue analysis report
  - People counting report
  - Vehicle ANPR report
  - Pathway analysis report
- Registration
  - Upload person information (name, gender, face comparison group, person group, effective period, etc.) to the system
  - Upload visitor information (ID type, name, person group, visitee, purpose, etc.) to the system
- View/delete/share the captured images and video clips
- Provide traffic flow statistics of Current Day/Current Month/History
- Set device access mode as Restore Default/Automatically Judge/Directly Access/Proxy Mode to define the accessing device mode when performing live view or playback
- Provide hardware decoding
- Display detection frames (including motion detection frames, fire source information, temperature, etc.) on live video
- Automatically refresh the thumbnails of the resources displayed on the Logical Resource page and Favorites
- Use the time of the time zone where the phone running the Mobile Client locates in, or the time of the time zone where the device locates in
- Display the zone information on the time (e.g., 2018-12-12 12:12:12 +8:00)
- Update the Mobile Client to its latest version if new version is available
- Switch account

Typical Application



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: 3,000[1] Distributed Deployment: 10,000[2] Central System (RSM): 100,000[3]
	Managed Device IP Addresses _*Including Encoding Devices, Access Control Devices, Elevator Control Devices, Security Control Devices, and Remote Sites_	Centralized Deployment: 1,024[1] Distributed Deployment: 2,048[2]
	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
	DeepinMind Server	64
	ANPR Cameras	3,000
	People Counting Cameras	Recommended: 300
	Heat Map Cameras	Recommended: 70
	Thermal Cameras	Recommended: 20[4]
	Queue Management Cameras	Recommended: 300
	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
	Arming Schedule Templates	200
Picture	Picture Storage **Including event/alarm pictures, face pictures, and vehicle pictures.*	20/s (Stored in SYS Server) 120/s (Stored in Recording Server)
Reports	Regular Report Rules	100
	Event or Alarm Rules in One Event/Alarm Report Rule	32
	Records in One Sent Report	10,000 or 10 MB
	Resources Selected in One Report **With this limitation, you can generate a neat and clear report via the Control Client and it costs less time.*	20
Data Storage	Data Retention Period	Stored for 3 Years
	People Counting	5 million
	Heat Map	0.25 million
	ANPR	60 million
	Events	60 million
	Alarms	60 million
	Access Records	1.4 billion
	Attendance Records	55 million
	Visitor Records	10 million
	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
	Concurrent Accesses via Mobile Clients and OpenAPI Clients	100
	Users	3,000
	Roles	3,000
Vehicle (ANPR)	Vehicle Lists	100
	Vehicles per Vehicle List	5,000
	Under Vehicle Surveillance Systems	4
	Vehicle Undercarriage Pictures	3,000
Entrance & Exit	Lanes	8
	Cards Linked with Vehicles	250,000
	Vehicle Passing Frequency in Each Lane	1 Vehicle/s
Face Comparison	Persons with Profiles for Face Comparison	1,000,000
	Face Comparison Groups	64

	Persons in One Face Comparison Group	1,000,000
Access Control	Persons with Credentials for Access Control	50,000
	Visitors	10,000
	Total Credentials (Card + Fingerprint)	250,000
	Cards	250,000
	Fingerprints	200,000
	Profiles	50,000
	Access Points (Doors + Floors)	512
	Access Groups	512
	Persons in One Access Group	50,000
	Access Levels	512
	Access Schedules	32
Time and Attendance	Persons for Time and Attendance	10,000
	Attendance Groups	256
	Persons in One Attendance Group	10,000
	Shift Schedules	128
	Major Leave Types	64
	Minor Leave Types of One Major Type	128
Smart Wall	Decoding Devices	32
	Smart Walls	32
	Views	1,000
	View Groups	100
	Views in One View Group	10
	Cameras in One View	150
	Views Auto-Switched Simultaneously	32
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