



HikCentral V1.3.2 Specification

Introduction

HikCentral is a flexible, scalable, reliable and powerful central video system. It can be delivered after pre-installed on Dell server. HikCentral 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

Video Surveillance Management (VSM) Service

Streaming Service (Optional)

Web Client/Control Client/Mobile Client

System Requirements

| Feature | Description |
|------------------------------|--|
| OS for VSM Server | Microsoft® Windows 7 (64-bit) Microsoft® Windows 8 (64-bit) Microsoft® Windows 8.1 (64-bit) Microsoft® Windows 10 (64-bit) Microsoft® Windows Server 2008 R2 (64-bit) Microsoft® Windows Server 2012 (64-bit) Microsoft® Windows Server 2016 (64-bit) |
| OS for Control Client | Microsoft® Windows 7 (32/64-bit) Microsoft® Windows 8 (32/64-bit) Microsoft® Windows 8.1 (32/64-bit) Microsoft® Windows Server 2008 R2 (64-bit) Microsoft® Windows Server 2012 (64-bit) Microsoft® Windows 10 (64-bit) Microsoft® Windows Server 2016 (64-bit) |
| Browser Version | Internet Explorer 10/11 and above (32-bit) Chrome 35 and above (32-bit) Firefox 32 and above (32-bit) |
| Database | PostgreSQL V9.6.2 |
| OS for Smartphone | iOS 8.0 and later Android phone OS version 4.0 or later, and dual-core CPU with 1.5 GHz or above, and at least 2G RAM |
| OS for Tablet | iOS 8.0 and later Android tablet with Android OS version 4.1 or later |
| Virtual Machine (VSM) | VMware® ESXi™ 6.x Microsoft® Hyper-V with Windows Server 2012 R2 <i>*The Streaming Server and Control Client cannot run on the virtual machine.</i> |

Function Features

VSM 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
- Manage Remote Sites for HikCentral with RSM module
- Service manager for system health monitoring
- Streaming gateway: a VSM component that forwards and distributes audio and video data as well as forwards signaling

Streaming Service

- Forwards and distributes audio and video data

Web Client

- Access to the VSM service via IP address or domain name
- License management
 - Online or offline activation
 - Online or offline update
 - Online or offline deactivation
- Startup wizard guides you through basic operations including
 - Adding encoding devices
 - Adding access control devices
 - Configuring event parameters
 - Managing system users
- Supports standard ONVIF™ protocol
- Remote Site's central management:
 - Add Remote Site to the Central System (HikCentral 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.
- 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 available:
 - ✓ By detecting online devices in the same subnet with the VSM 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
- 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
 - Five adding modes for access control devices available:
 - ✓ By detecting online devices in the same subnet with the VSM server or current PC
 - ✓ By specifying the device IP address
 - ✓ By specifying an IP segment
 - ✓ By specifying a port segment
 - ✓ By importing in a batch
- 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
 - Five adding modes for security control devices available:
 - ✓ By detecting online devices in the same subnet with the VSM 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
- Restore or reset passwords for detected online devices
- Recording Server manageable
 - Add pStor, Hybrid Storage Area Network (Hybrid SAN) or Cloud Storage Server as a Recording Server
 - Add pStor, Hybrid SAN or Cloud Storage Server by IP address
 - Provides WAN access
 - Provides searching the video files stored in Cloud Storage Server via the HikCentral Mobile Client.
 - Remotely configure the added pStor, Hybrid SAN or Cloud Storage Server via a web browser
 - One-touch configuration for setting the Hybrid SAN storage
 - Hybrid SAN N+1 hot spare
 - Provides ANR function
- Streaming Server manageable

- Add Streaming Server by IP address
- Provides WAN and LAN access
- Smart wall manageable
 - 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 VSM 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, access points, and UVSSs) by areas
- Recording
 - Two storage methods for storing the video files:
 - ✓ Encoding Device: DVR/NVR/ network camera (SD card);
 - ✓ Recording Server: pStor, Hybrid SAN or Cloud Storage Server
 - For Remote Site's cameras, store video files in the Central System's pStor, Hybrid SAN or Cloud Storage Server
 - Continuous recording, event triggered recording, and command triggered recording.
 - Set uploading 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 VSM server, Hybrid SAN, Cloud Storage Server, or pStor.
 - 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 VSM server.
- Edit access point'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
- Set related camera(s) to view the video on Control Client
- Edit application settings
 - ✓ Anti-passback
 - ✓ Open door with first card
- 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
- Group zones into different security control partitions
 - 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
- Events & Alarms
 - Set system-monitored events for the resources in the system
 - ✓ Camera events: motion, video loss, line crossing, etc.
 - ✓ Access point events: access events, door status events, etc.
 - ✓ 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
 - ✓ Remote Site exceptions: site offline
 - ✓ Device exceptions: device offline, HDD full, HDD read/write error, etc. (including encoding devices, access control devices, and security control devices)
 - ✓ Server exceptions: high mainboard temperature, bad disk, disk loss, etc. (including Streaming Servers, Recording Servers, and HikCentral Server)
 - ✓ User events: user login or logout
 - ✓ User-defined events
 - ✓ Generic events
 - Set event linkage actions such as recording, creating tag, capturing pictures, linking access points, linking alarm outputs, PTZ actions, sending emails, and triggering user-defined events
 - Send emails to notify users of triggered event information with email template configurable
 - 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, 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, alarm input alarms, ANPR alarms, person alarms, Remote Site alarms, encoding 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
 - 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 region on the map
 - Add/edit/delete hot spots (camera/alarm input/alarm output/door/UVSS) on the map
 - Add labels with description on the map
- Vehicle management
 - Add vehicle information manually
 - Import vehicle information according to the pre-defined template
 - Set effective period for the added vehicles
- Person list management
 - Add person information one by one
 - Import information of multiple persons in a batch
 - Import information of multiple persons in the domain in a batch
 - Import multiple persons' profiles in a batch
 - Profile format: JPG, JPEG, and PNG
 - Enable the person profile as the person's face credential which is used when access via face recognition terminal
 - Issue cards to multiple persons in a batch
- Access control
 - Group persons with same access permission into access groups
 - 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
- Time and attendance
 - Group persons into attendance groups
 - Add/delete the shift schedule

- Assign the shift schedule to attendance group
- Add/delete the access control checkpoint
- Search the attendance records
- Correct single person's attendance record
- Correct multiple persons' attendance records
- Face comparison group
 - Group persons into face comparison group
 - Set similarity threshold when adding face comparison
 - Apply the face comparison group to device
- 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
 - 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
 - Enable GIS map function, configure the map API URL, and customize the icons of hot region and hot spot
 - Set the threshold for the VSM server's CPU usage and RAM usage
 - NTP settings
 - Active directory settings
 - 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
 - A static IP address 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
- VSM 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, and defense schedule, and set holidays to adopt different shift schedule or access control 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, and temperature
- Set unique IDs for the cameras in the system
- 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
- System hot spare settings
- Reset network information of added devices
- Export service component certificate from VSM server
- 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

Control Client

- GPU hardware decoding
- Receive alarm
- Access to VSM 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
 - Camera auto-switch/View auto-switch
 - Manual recording
 - Capture
 - Instant playback
 - 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, and access 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
 - 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 files 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, UVSSs, and doors on the map
 - Arming control: arm and disarm cameras, alarm inputs, UVSSs, and doors on the map
 - Search and view history alarms of cameras, alarm inputs, UVSSs, and doors on the map
 - Get a notification message on the map when alarm is triggered
 - 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
- Capture
- Print map
- Locate resource on the map
- View the live video or playback of the resources on the map
- 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
 - View the live video from the related camera
 - Play the alarm related video on smart wall
 - Add a tag to the alarm information
 - Acknowledge the alarm with a text description
 - 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
- 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
- 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
- Access control
 - View live videos of access point's related camera(s)
 - Play back the recorded video files of door's related camera(s)

- Control access points to lock, unlock, remain locked, or remain unlocked
- View the card swiping record in real time
- Search the access control events triggered on the added access points
- Subscribe to receive access events from all the access points
- Video search
 - Search video files stored on local devices or Recording Server
 - Search the video clip by tag, lock, segment, or interval
 - 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
 - Set VCA rules to search the video where a VCA event occurs
 - Search capture face pictures and related video by uploading a picture
 - Search matched face pictures and related video by selecting face comparison groups
 - Play the searched video clip
 - Download the searched video clip
- Report
 - 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 map report: Generate a report to analyze the visit times and dwell time of customers
 - 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
 - Status overview of the resources, including cameras, access points, UVSSs, encoding devices, access control devices, security control devices, Remote Sites, decoding devices, VSM, Recording Servers, and Streaming Servers
 - Detailed status page of cameras, encoding devices, access points, UVSSs, access control devices, Remote Sites, decoding devices, Recording Servers, and Streaming Servers
 - Set stream type for the resources to main stream, sub-stream, smooth stream, or restore to global stream
- Tools
 - Smart Wall
 - ✓ 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

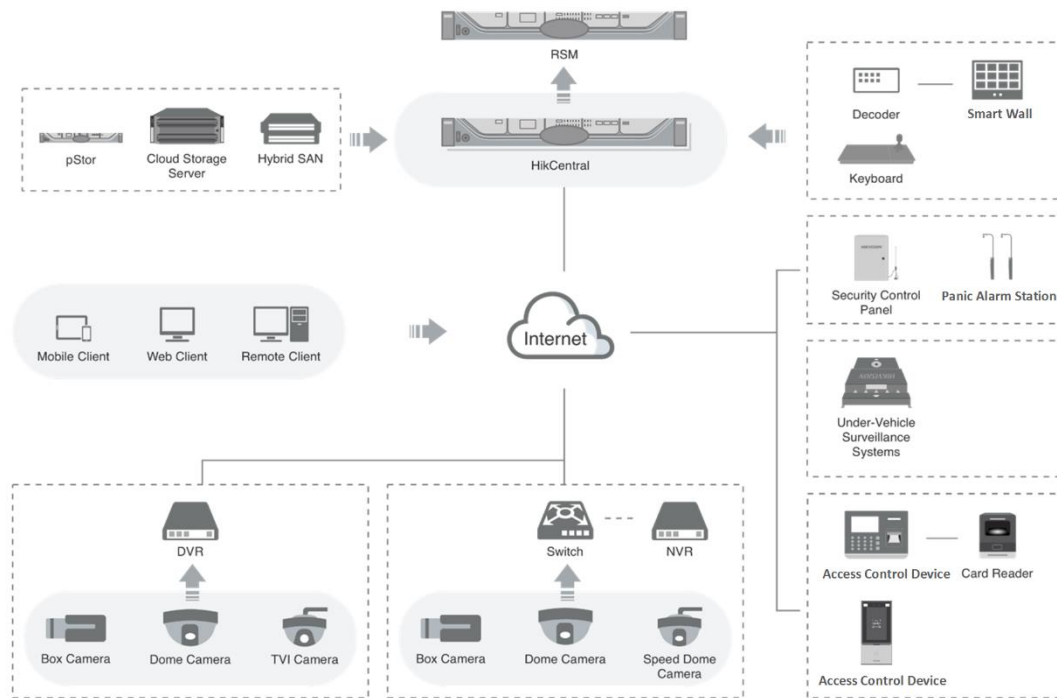
- ✓ Switch to playback
- ✓ View auto-switch
- ✓ Create a roaming window
- ✓ Enlarge and restore window
- ✓ View and export window No. and camera ID
- VS Player
- Broadcast
- Alarm Output
- Two-Way Audio
- Download center
 - Check the downloading tasks and status
 - Continuous transmission on the breakpoint
 - Download the player for playing back the video files
- Audit Trail
 - Search log files of VSM, 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
 - ✓ Auto-login
 - ✓ Resume 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
 - Configuring local saving path of videos/pictures/packages
 - Configuring keyboard and joystick parameters
 - Configuring live view and playback settings
 - ✓ Configure icons on live view and playback toolbar
 - ✓ Enable/disable toolbar display
 - Set alarm sounds by local audio files or voice engine (require support of the OS)

Mobile Client

- Access to the VSM 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)
 - Set 1/4/9 window division
 - 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
 - Display persons' real-time access records, including person profile, person name, and access results
 - View the recognized passing vehicle 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
 - Trigger user-defined event manually
- Playback
 - 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 (only for tablet)
- Scale up or scale down the playback timeline bar
- 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 alarms
- 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
- Map control (only for tablet)
 - View the geographic locations of resources on the map
 - Get the live view and playback of the cameras, UVSSs, and doors on the map
 - Get a notification message on the map when alarm is triggered
 - 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
- Subscribe events of all the access points and all face comparison groups (only for tablet)
- Search (only for tablet)
 - 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
 - Add person to person list
- BI report (only for tablet)
 - Heat map report
 - Temperature report
 - Queue analysis report
 - People counting report
 - Vehicle ANPR report
- 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

Typical Application



Software Specification

The following table shows the maximum performance of the VSM service. For other detailed data and performance, refer to *HikCentral V1.3.2_Software Requirements & Hardware Performance*.

| Features | | Without RSM (E3-1220) | With RSM (E5-2620) |
|-----------|--|---|--|
| General | Cameras | 3,000 ^① | 3,000 ^② (Current Site) |
| | | | 100,000 ^③ (Central System) |
| | Encoding Device | 1,024 | 1,024 (Current Site) |
| | Access Control Device | 128 | 128 (Current Site) |
| | Encoding Devices, Access Control Devices, and Security Control Devices | 1,024 ^① | |
| | Encoding Devices, Access Control Devices, Security Control Devices, and Remote Sites | | 1,024 ^{②③} (Current Site) |
| | Alarm Inputs (Including Alarm Inputs of Security Control Devices) | 3,000 | |
| | Alarm Outputs | 3,000 | |
| | DS-5600 Series Face Recognition Terminals When Applied with Hikvision Turnstiles | 32 <i>*If DS-5600 series devices are applied with third-party turnstiles, they are regarded as access control devices and the maximum amount is 128.</i> | |
| | ANPR Cameras | 3,000 | |
| | People Counting Cameras | Recommended: 300 | |
| | Heat Map Cameras | Recommended: 70 | |
| | Thermal Cameras | Recommended: 20 | |
| | Queue Management Cameras | Recommended: 300 | |
| | Recording Servers | 64 | |
| | Streaming Servers | 64 | |
| | Areas | 3,000 | |
| | Area Hierarchies | 5 | |
| | Cameras per Area | 64 | |
| | Alarm Inputs per Area | 64 | |
| | Alarm Outputs per Area | 64 | |
| | Email Templates | Unlimited | |
| Recording | Recording Schedules | 3,000 | 30,000 (for Cameras on |

| | | | |
|--------------------------|---|--|---|
| | | | Current Site and from Remote Sites) |
| | Recording Schedule Templates | 200 | |
| Event & Alarm | Event and Alarm Rules | 3,000 | 10,000 (Current Site and Remote Sites) |
| | Storage of Events or Alarms without Pictures | 100/s | |
| | Storage of Events or Alarms with Pictures | 20/s (Each Picture 500 KB, Stored in VSM Server) 80/s (Each Picture 500 KB, Stored in Recording Server) | |
| | Events or Alarms Sent to Clients | 120/s 100 Clients/s <i>*The clients include Control Clients and Mobile Clients.</i> | |
| | Arming Schedule Templates | 200 | |
| | Alarm Categories | 25 | |
| | Alarm Priorities | 255 | |
| | | | |
| 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 for One Report <i>*With this limitation, you can generate a neat and clear report via the Control Client and it costs less time.</i> | <ul style="list-style-type: none"> ● 20 People Counting Cameras for One People Counting Report ● 20 ANPR Cameras for One Vehicle Analysis Report ● 20 Queues for One Queue Analysis Report ● 20 Presets for One Temperature Report | |
| Data Storage | Data Recorded in System <i>*Including event logs, recording tags, face comparison data, card swiping records, attendance records, ANPR records, video analysis data, service error logs, service warning logs, and service information logs.</i> | Stored for 3 Years | |
| | Alarm Logs | 60 Million | |
| | BI Data <i>*Including heat map records, passing vehicle records, people counting records, temperature records, and queue analysis records.</i> | Stored for 3 Years | |
| Users and | Concurrent Accesses via Web Clients, | 100 | |

| | | |
|------------------------|--|---|
| Roles | Control Clients, and OpenSDK Clients | |
| | Concurrent Accesses via Mobile Clients and OpenSDK Clients | 100 |
| | Users | 3,000 |
| | Roles | 3,000 |
| Map | E-maps | 1,024 |
| | Map Resolution | 8192×8192 |
| | Hot Regions per Map | 64 |
| | Camera Hot Spots per Map | 128 |
| | Alarm Input Hot Spots per Map | 128 |
| | Alarm Output Hot Spots per Map | 128 |
| | Labels per Map | 128 |
| | Hot Regions in Total | 1,024 |
| | Camera Hot Spots in Total | 3,000 |
| | Alarm Input Hot Spots in Total | 3,000 |
| | Alarm Output Hot Spots in Total | 3,000 |
| | Labels in Total | 3,000 |
| | Elements on GIS Map in Total | 3,000 |
| Vehicle (ANPR) | Vehicle Lists | 100 |
| | Vehicles per Vehicle List | 5,000 |
| | Under Vehicle Surveillance Systems | 4 |
| | Vehicle Undercarriage Pictures | 3,000 |
| | Storage of License Plate Matched/Mismatched Events | 20/s with Pictures (Each Picture 500 KB, Stored in VSM Server) 120/s with Pictures (Each Picture 500 KB, Stored in Recording Server) |
| Face Comparison | Face Pictures | 10,000 |
| | Face Comparison Groups | 64 |
| | Persons in One Face Comparison Group | 10,000 |
| | Storage of Face Matched/Mismatched Events | 120/s without Pictures 20/s with Pictures (Each Picture 500 KB, Stored in VSM Server) 120/s with Pictures (Each Picture 500 KB, Stored in Recording Server) |
| Person | Persons | 10,000 |
| | Cards | 50,000 |
| | Fingerprints | 40,000 |
| | Credentials (Card + Fingerprint) | 50,000 |
| | Size of Each Profile | 300 KB |
| | Total Size of Profiles | 3 GB |
| Access Control | Access Points | 128 |
| | Access Points on Each E-map | 128 |

| | | | |
|---|--|------------------|---|
| | Access Points on E-maps in Total | | 128 |
| | Anti-Passback Rules | | 128 |
| | Access Points in One Anti-Passback Rule | | 16 |
| | Access Groups | | 64 |
| | Persons in One Access Group | | 1,000 |
| | Access Levels | | 128 |
| | Access Points in One Access Level | | 128 |
| | Access Levels Assigned to One Access Group | | 8 |
| | Access Schedules | | 32 |
| | Attendance Groups | | 64 |
| | Persons in One Attendance Group | | 1,000 |
| | Shift Schedules | | 128 |
| | Holidays | | 16 |
| | Smart Wall | Decoding Devices | |
| Smart Walls | | 32 | |
| Views | | 1,000 | |
| View Groups | | 100 | |
| Views Auto-Switched Simultaneously | | 32 | |
| Opened Windows for Each Decoding Output | | DS-C10S | In Normal Mode: <ul style="list-style-type: none">● Total Amount: 16 windows● Total Area: 4 times of the area of the base window^④ In Tile Mode: <ul style="list-style-type: none">● Total Amount: 8 Windows |
| | | DS-6900UDI | <ul style="list-style-type: none">● Total Amount: 36 windows● Total Area: 3 times of the area of the base window |
| | | DS-6400HDI-T | <ul style="list-style-type: none">● Total Amount: 16 windows● Total Area: 3 times of the area of the base window |
| Operation Logs Storage | | 500,000 | |
| 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 VSM server, the maximum number of the added encoding devices, access control devices, and security control in total is 1,024. If the number of the manageable cameras (including the cameras directly added to the VSM and the cameras connected to these added devices) exceeds 3000, the exceeded cameras cannot be imported to the areas.

②: For one VSM server, the maximum number of the added encoding devices, access control devices, security control devices, and Remote Sites in total is 1,024. If the number of the

manageable cameras (including the cameras directly added to the VSM and the cameras connected to these added devices) exceeds 3000, the exceeded cameras cannot be imported to the areas.

③: For one VSM server, the maximum number of the added encoding devices, access control devices, security control devices, and Remote Sites in total is 1,024. 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: Base window refers to the window linked with one decoding output, and the windows are opened and overlapped on it.

Hardware Specification

Hikvision bought 3-year platinum service from Dell. You can get assistance from your regional Dell support center if you encounter any problems on the Dell server.

For details, refer to *Maintenance Guide of Dell All-In-One Server*.

| Feature | E3-1220 V5 |
|--|---|
| Processor | E3-1220 V5 (4-Core, 3.0 GHz) |
| Operating System | Microsoft® Windows Server 2012 R2 |
| Memory | 16G DDR4, 2400MT/s UDIMMS |
| Storage | 1T SATA × 2, 3.5" Enterprise SATA 7.2k HDDs |
| RAID | H330 RAID Controller with RAID 1 |
| NIC | 1GbE × 2 |
| Chassis | 1U, Rack Mount |
| Battery | CR-2032 Coin Cell/Lithium/0.0032kg |
| Power Supply | 250W Cabled PSU |
| Dimensions (W × D × H) | 482.38 mm × 567.92 mm × 42.8 mm (18.99" × 22.36" × 1.69") |
| Weight | 9.5 kg |
| Dimensions with Package (W × D × H) | 750 mm × 614 mm × 259 mm (29.53" × 24.17" × 10.2") |
| Weight with Package | 15.8 kg (34.8 lb) |
| License | License with 64 Cameras Manageable; License with 300 Cameras Manageable. |



See Far, Go Further