HikCentral Professional V1.5

White Paper

White Paper

About this White Paper

This White Paper is applicable to HikCentral Professional.

The White Paper includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the White Paper is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this white paper under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT

WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Contents

Chapter 1 Product Overview

1.1 System Introduction

HikCentral Professional is an integrated surveillance system with AI functions. It provides a set of flexible, extensible, reliable and effective centralized management solutions for integrated surveillance projects. Besides, the system can realize information gathering, convenient deployment and multi-network management. It supports multiple functions such as surveillance device management and configuration, live view and playback, event and alarm linkage, access control, attendance management, vehicle management, license plate recognition, intrusion alarm, facial recognition, etc.
The core features of HikCentral Professional lie in the following three aspects:

1.1.1 Centralized

HikCentral Professional adopts centralized management. It integrates various applications such as video surveillance, event and alarm, access control, person management and vehicle management into one system. In this way, the system can break through the barriers between different applications, enable application linkage and cross-application process. As an extensible system, HikCentral Professional can serve both single-site projects with only a small number of video channels and multi-site projects with tens of thousands of video channels. Another advantage of HikCentral Professional is low-cost management since administrators can manage multiple application modules in one uniform system.

1.1.2 Collaborative

Developed by HIKVISION, HikCentral Professional stands for the best system to manage HIKVISION surveillance devices. When connected to the system, these devices can fully perform their advanced functions. Except for being applicable to HIKVISION devices, HikCentral Professional is also compatible with third-party devices. Moreover, with the help of OpenAPI tools, it can be integrated as a component with other third-party systems.

1.1.3 Intelligent

Adopting the latest AI technology of HIKVISION, HikCentral Professional supports multiple intelligent analysis functions including cross-network intelligent route, facial recognition, UVSS, license plate recognition, thermal imaging, heat maps, queue analysis, people counting, etc. The system can expand the range of surveillance applications and serves as a security escort for both companies and the public society.

1.2 System Background

1.2.1 Current Status of Surveillance Industry

With over fifty-year development and revolution, surveillance industry has gradually grown mature with a large-scale market. The revolution of surveillance industry can be analyzed from two dimensions.

Horizontally, faced with fierce market competition, surveillance companies continue to expand new application fields. Initially, surveillance market covers only political and military fields. As time goes by, surveillance companies also serve commercial areas like office buildings, hospitals, schools and transportation. Nowadays, surveillance products have entered common households.

Vertically, surveillance industry has experienced three stages. The first stage was characterized by hardware device production and sales. The second stage featured in providing solutions. And it is now in the third stage, aiming to realize online charging services based on system solutions.

For companies in this industry, great transformation has taken place in terms of income source and business model. On the one hand, the main income source of surveillance companies used to be device sales and installation; currently, surveillance service fee dominates in income. On the other hand, surveillance companies used to provide service for small-sized projects (such as single monitoring centers); currently, they provide service for large-sized projects that integrates multiple functions including access control, person management, vehicle management, etc.

To conclude, the global surveillance industry has already formed into a large-scale market with mature application fields and types.

1.2.2 Future Development of Surveillance Industry

With the development of information technology, surveillance industry has stepped into a new stage. At present, there are three main development directions:

Intelligent Front-End

Since chips become much more integrated and have greater processing capability, many manufacturers have launched intelligent front-end devices such as intelligent IPC, DVR and NVR. In the future, these devices will be further more intelligent with the help of more complex and specialized algorithms. The advantages of intelligent devices lie in low delay and low cost, and to some extent reducing the pressure of back-end analysis.

System-Oriented

In the process of promoting intelligent solutions, surveillance manufactories have also put more emphasis on integrating the system with its supporting hardware devices. Moreover, they make efforts to make uniform technical standards, APIs, etc. Gradually, the following industry pattern will be formed: large manufacturers make standards and launch effective systems; small manufacturers try to follow those standards. This is an inevitable trend for the development of surveillance companies.

Industry-Oriented

Surveillance products aim to solve customers' problems. Since requirements differ in various industries, a single product cannot meet all those requirements. Currently, proceeding from the specific industry, manufacturers try to do in-depth research of applications and processes in this industry. Then they analyze problems and search for solutions. Ultimately, they can provide high-quality intelligent solutions for customers.

1.3 Current Problems and Solutions

Currently, along with the continuous development of surveillance industry, problems in the mainstream surveillance solutions also appear. Based on the in-depth research and analysis of the surveillance industry, HIKVISION has developed and launched HikCentral Professional to provide customers with more flexible and effective solutions to address these problems.

1.3.1 Disconnection Between Device and System

With the development of intelligent chips, traditional monitoring devices tend to have increasingly intelligent processing capabilities. As one of the major manufacturers of intelligent surveillance devices, HIKVISION has launched many such devices including camera/NVR/DVR with facial recognition function, fingerprint attendance terminal, etc. These devices feature in high processing efficiency, low delay and low cost, greatly meeting the requirements of target customers. At present, however, many surveillance management systems do not support the advanced functions of these intelligent devices, which can only be connected to systems through universal protocols such as ONVIF protocol instead of a globally uniform API protocol.
To solve this problem, HIKVISION have researched and developed HikCentral Professional, and we have made efforts to integrate intelligent devices with the system by adopting the exclusive API protocols. When connected to the system, intelligent devices can fully perform their advanced functions, enhancing the overall efficiency of solutions.

1.3.2 Separated Surveillance Applications

With the development of surveillance industry, the core requirements of surveillance applications have gradually transformed from single video surveillance into three broad application categories, including video surveillance, person management and vehicle management. They can be further divided into multiple sub-applications such as access control, visitor management, attendance, entry and exit management, alarm, etc.
By contrast, the traditional surveillance systems tend to deal with only one or several of the above-mentioned sub-applications. For example, there is the system that only supports video surveillance or access control management. While one system corresponds to one function, such systems cannot meet users' overall requirements. Also, if users install one system for one application, then administrators have to learn to operate multiple systems, which leads to high learning cost and low-efficient interactions between different systems.
In the current surveillance market, there do exist some surveillance management systems that can provide uniform applications for the end users by integrating multiple third-party systems. However, such architecture involves the connection between different application systems of multiple manufacturers, requiring a relatively high cost of both the system providers and the end users. Therefore, it is not suitable for price-sensitive, small and medium-sized integrated surveillance projects.
Having worked in the field of integrated surveillance for many years, HIKVISION has formed a relatively mature and complete product system. Based on our surveillance products, HikCentral Professional integrates various applications (such as video surveillance, access control, entrance and exit, facial recognition, map, alarm, etc.) in different fields and break through barriers between different applications. Also, since HikCentral Professional adopts flexible and cascade design philosophy, it is applicable for both large and small sized integrated surveillance projects.

1.4 Core Requirements

Above all, HikCentral Professional meets the following major requirements.

1.4.1 Centralized Management

Users require to manage resources in various surveillance areas in a centralized system. Generally, users need to manage scattered surveillance areas that have different network environments. Correspondingly, HikCentral Professional supports the following functions: adapting to different network environments, managing and calling the resources of different surveillance areas, supporting live view, recording, event and alarm, etc.

1.4.2 Integrated Applications

Users require to manage various surveillance applications via one integrated system. Except for video surveillance, users have other application requirements such as access control, attendance management, person management, vehicle management, event and alarm, etc. Correspondingly, HikCentral Professional provides an integrated system that can manage all these applications.

1.4.3 High Definition Video Surveillance

The most crucial function of surveillance system is video surveillance. With the development of information network technology as well as video coding and decoding technology, users have higher requirements for high definition video surveillance. Correspondingly, HikCentral Professional is compatible with the mainstream video coding and decoding formats, and supports high definition live view and playback.

1.4.4 Integration with Device Intelligent Functions

Users require to use advanced and intelligent functions of various surveillance devices in the system.
HIKVISION surveillance products support many advanced intelligent functions, such as facial recognition, thermal imaging, heat map, queue analysis, license plate recognition and so on. Correspondingly, HikCentral Professional provides different modules to manage these applications, enabling users to perform advanced functions of devices in the system.

1.4.5 Integration with Third Parties

Except for integrating HIKVISION products, users also require to manage surveillance devices of multiple manufactures in one system or connect their application systems with the third-party systems. Correspondingly, HikCentral Professional can integrate surveillance devices of third-party manufactures, which can call the functions of HikCentral Professional through APIs.

Chapter 2 Product Design

2.1 Goal

We design HikCentral Professional as a multi-functional surveillance platform covering video, access control, vehicle, and person, etc. by advanced technologies to connect different modules in a reliable and effective way in order to meet users' multiple requirements.

HikCentral Professional supports multiple device models and functions with a stable host computer and storage, an effective database, and high compatibility of various network (wired or wireless) communication environment.

2.2 Components

HikCentral Professional consists of the following components:

- Database Management System: managing all the device data, configuration information, application data, etc.
- SYS Server: the core component of HikCentral Professional, provides:
  - Device access service.
  - Modules of different functions.
  - Management of the communication among modules and components.
- Streaming Media Server: a proxy server dealing with the input and transfer of composite streams.
- Remote Site Management Sever: a server managing both the central system and sub-systems registered to the central system.
- Web Application Server: provides application and APIs for web service.
- OpenAPI Server: provides APIs of open components and realize module logic.
- Control Client: HikCentral Professional operating on PC in Windows system.
- APP: HikCentral Professional running on mobile phones in Android and iOS systems.

2.3 Design Principle

2.3.1 Standardization

HikCentral Professional accords with the international mainstream application-design standards.

2.3.2 Strong Practicability

HikCentral Professional meets your requirements for scientific and effective security surveillance.

1. HikCentral Professional is applicable in various network environment.
2. HikCentral Professional adopts qualified hardware, operating system, and database.
3. HikCentral Professional is easy to install and start.
4. HikCentral Professional features user-friendly interface for you to learn and operate it easily.

2.3.3 Cutting-Edge Features

We adopt advanced tools, frame, database, and other supports to make HikCentral Professional reliable and safe enough.

2.3.4 Supporting Integration with Other Systems

Characterized in strong extensibility and compatibility, HikCentral Professional can provide open, standard APIs and can transfer data in different formats.

2.3.5 Supporting Extension

HikCentral Professional is strongly extensible in system structure, software & hardware system, and system scale. With flexible APIs and extensible and standard database design, it is easy to extend the system. Meanwhile, we have fully considered the future requirements to make the code extensible.

2.3.6 High Reliability

HikCentral Professional can provide accurate and reliable data with strong fault tolerance and emergency-dealing capability.

2.3.7 Comprehensive Security

HikCentral Professional provides all-around information safety protection that covers network configuration, operating system, database, running environment, transmission, and operations.

2.4 System Architecture

2.4.1 Logical Architecture

Logically, HikCentral Professional consists of 6 layers:

Network Layer

The basis for running HikCentral Professional. The Web Client and Control Client can communicate with various end devices, surveillance devices, storage devices and third-party systems by WAN/LAN/Wi-Fie/GPRS.

Data Layer

The data layer provides data for all modules. By adopting relational database, HikCentral Professional saves data respectively in databases of device, person, vehicle, configuration, event, etc.

Basic Supporting Layer

Basic supporting layer provides support for every module by different components. It is very effective because it gets reusable components together so that the modules can get supports easily.

Module Layer

Module layer focuses on logic design of every module based on users' requirements to make the operation reasonable and logical.

Presentation Layer

Presentation layer focuses on interaction design of the Web Client, Control Client, and

Mobile Client to improve user experience.

Access Layer

Access layer connects to devices and third-party systems by 3 modes:

1. Hikvision SDK: Through Hikvision SDK Protocol, HikCentral Professional communicates with devices manufactured by Hikvision.
2. ONVIF: Through ONVIF Protocol, HikCentral Professional communicates with devices for video surveillance from third-party manufactures.
3. OpenAPI: Through OpenAPI Protocol, HikCentral Professional accesses with systems from third-party manufactures.

2.4.2 System Deployment

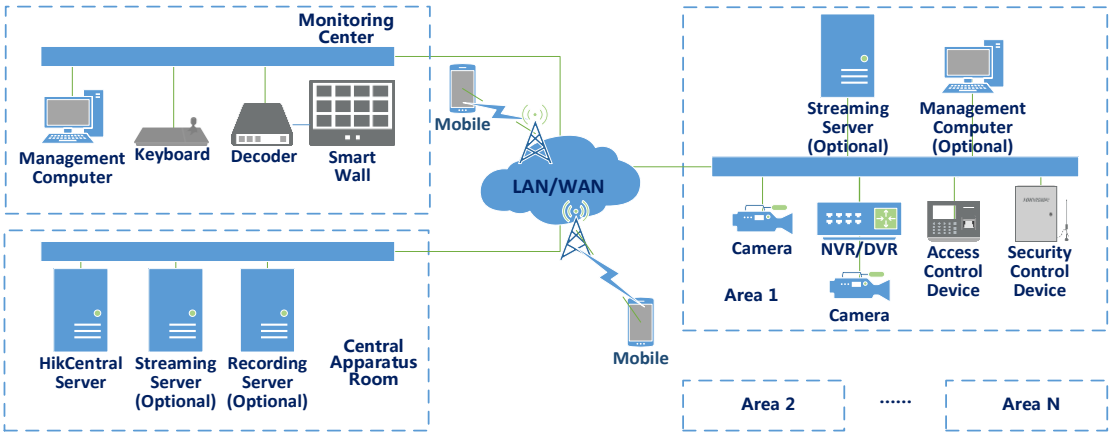
HikCentral Professional supports 3 deployment modes:

- SYS (System Management Service) Mode for single site management
- RSM (Remote Site Management)Mode
- Distributed deployment

SYS (System Management Service) Mode

With HikCentral Professional server as the core, SYS builds a comprehensive surveillance system by connecting devices, clients, and server together through the Internet. We design it for projects without remote sites.

The following is a typical architecture of SYS:



SYS contains 3 parts: central apparatus room, monitoring center, and surveillance area.

- **Central Apparatus Room**

  Central Apparatus Room is a place for server maintenance by system operators. Servers of HikCentral Professional are installed and deployed here. You can also put a recording server or streaming server here. Central Apparatus Room communicates with the monitoring center and areas by TCP/IP network including cable network,

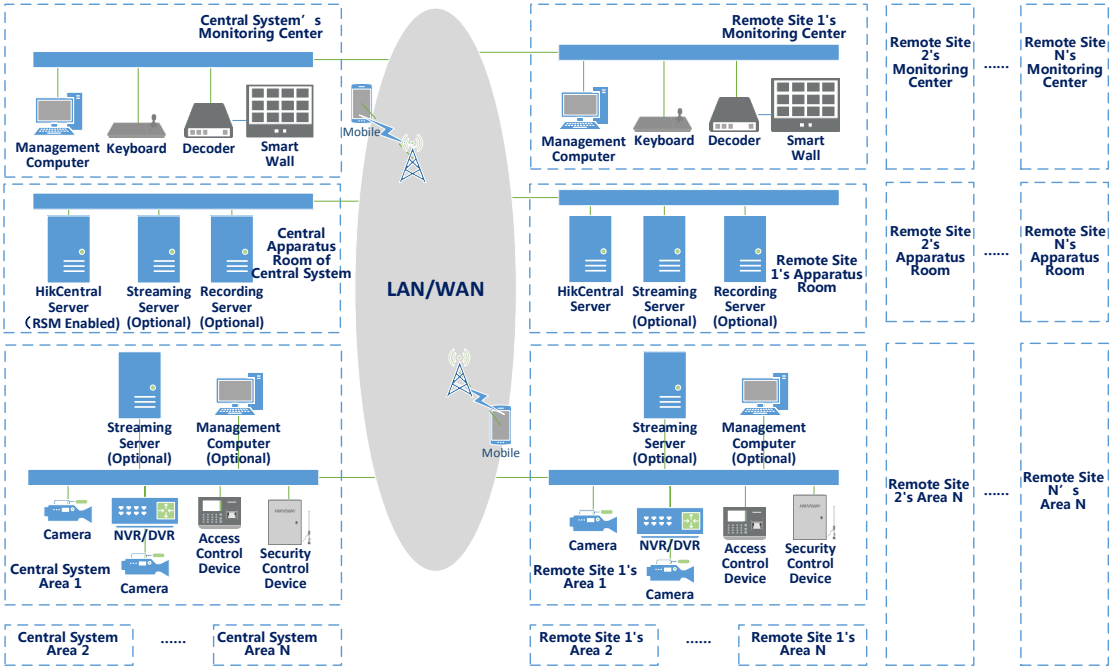
wireless network, WAN, and LAN.

- **Monitoring Center**
  Monitoring center is used for security guards to monitor and control the modules including video, alarm, access control, etc., in all surveillance areas. Generally, computers are deployed in monitoring centers to help performing monitoring function. For projects with large amount of cameras, you can install a smart wall in the monitoring center for overall surveillance.
- **Surveillance Area**
  The system aims to monitor and protect the surveillance areas. Therefore, we often put multiple types of devices including cameras, access control devices, security control devices, etc. in these areas for comprehensive management.
  You can also deploy a streaming server in an area to lower the load of the system.
  HikCentral Professional supports multiple surveillance areas. And you can give different users different permissions for managing area resources according to your need.
- **Mobile Terminal**
  The Mobile Client that communicates with the central apparatus room by GPRS supports monitoring area and managing resources if a user has the permission.

RSM (Remote Site Management) Mode

RSM mode is a large-scale-project-aimed management mode that means you can manage the SYS systems of remote sites by the Central System with RSM module. As the core of RSM mode, Central System connects the remote sites SYS systems through network and manages their resources.

The following is a typical architecture of RSM:



The difference between RSM mode and SYS mode is that RSM mode works based on both

Central System and remote sites.

- **Central System**
  Central System, in nature, is a HikCentral Professional system. Different from the remote sites, Central System has RSM module, so that you can add remote sites to the Central System and then manage the remote sites' resources. You can add up to 1,024 remote sites to a Central System.
  Besides, Central System enjoy the same function with basic HikCentral Professional. Therefore, you can add and manage areas by a Central System, and build a monitoring center for it.
- **Remote Site**
  You can understand a remote site as a HikCentral Professional without RSM module, which means it has the same functions with SYS mode.
- **Central System's Client**
  With a client (including Web Client, Control Client, and Mobile Client) connected to a Central System, you can not only manage resources of the Central System, but also the resources of the remote sites, and perform live view or playback of the remote sites' resources.

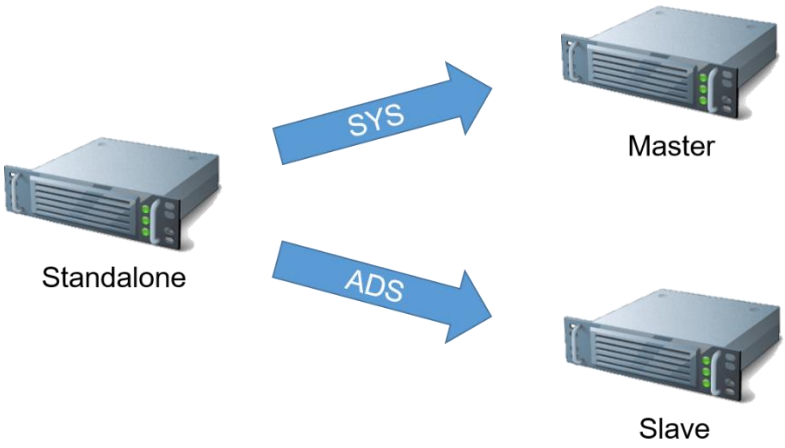
Distributed Deployment

Distribution mode means deploying one SYS server on 2 hardware devices in order to improve the system performance. It divides the services of HikCentral Professional into 2 types:

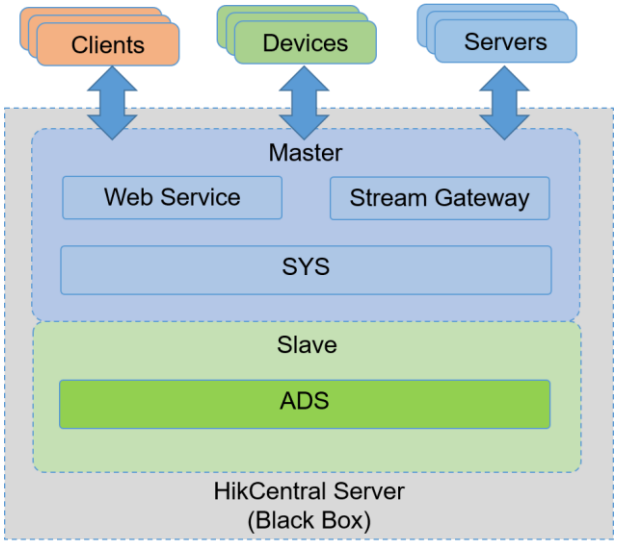
- SYS Service: mainly used for managing user permission, permission authentication, modules, devices, caches, running status caches, and device access, etc.
- ADS Service: mainly used for sorting out data collected by devices for data processing, pushing, searching and report-making, covering modules including event and alarm, facial recognition, ANPR, people counting, heat analysis, queue analysis, temperature analysis, and card authentication.

So we can install HikCentral Professional service on 2 different servers:

- Master: The server mainly used for SYS service, Web service, SG gateway, and database for SYS data. It is also the access of the clients and devices. And it manages the Slave.
- Slave: The server where ADS service and database for ADS are installed.

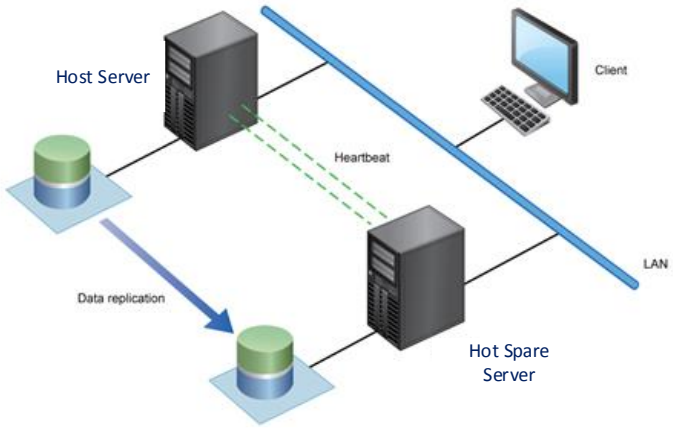


Distribution mode is a black box, which means the Master does the external interactions, while only the Mater can access and control the Slave.



Redundant Deployment

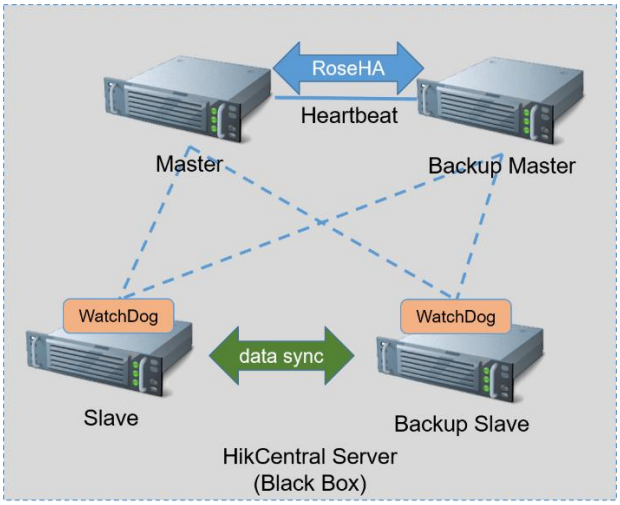
For the sake of the stability and performance of Master servers, you can set a hot spare connected with it, while the server connected with a hot spare is host server.



1. HikCentral Professional Hot Spare uses Data Mirroring .
2. You need to install RoseHA client in order to use both a host server and hot spare.
3. When the system is running, the host server and hot spare server works simultaneously. Generally, the host server works for the whole system and the hot spare works in standby mode.
4. RoseHA client monitors the status of two servers, and back up data of the host server to the hot spare in real time.
5. RoseHA will notice and move the servers IP resource to hot spare if the host server breaks down. The hot spare will take the host server's place and work for the system until the host server works properly.
6. When the host server recovers, RoseHA will back up data of hot spare to the host server.

Distributed Redundant Deployment

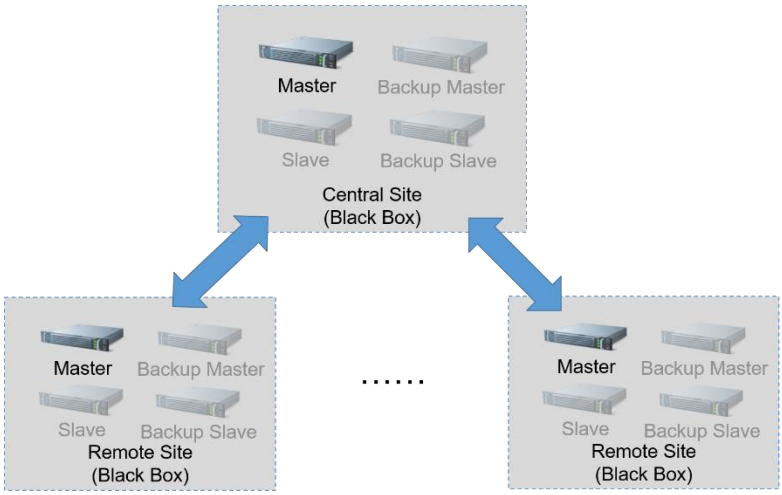
You can install a hot spare for both the Master server and Slave server as the picture below.



In this system, the Master server adopts RoseHA, while the Slave server does not. You can add the 2 Slave servers to the Master server which uses WatchDog to monitor the status of Slave servers. The Master server will switch its work to the Slave server if something wrong occurs to ensure the reliability.

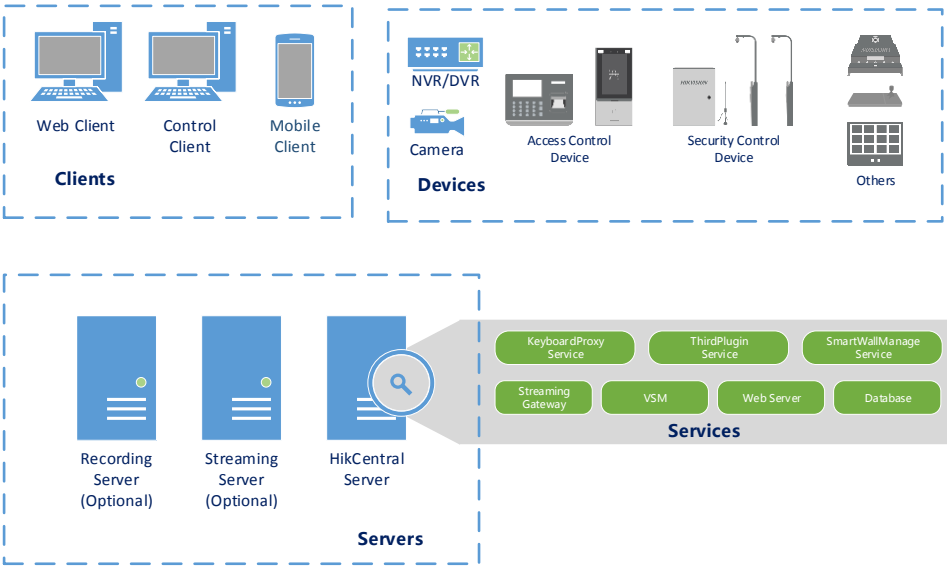
Distributed Deployment Combined with RSM

A distributed deployment system can work as a central system or remote site in RSM because it is a black box. The architecture is as the following picture:



2.5 System Component

The following is the system component architecture of HikCentral Professional:



HikCentral Professional consists of four components: central server, other servers, devices, and clients.

2.5.1 Central Server

HikCentral Professional Central Server consists of the following components:

Name	Description	Function
SYS	System Management Server	Responsible for module management, supporting RSM.
WebServer	Web Service and SG	Responsible for saving static pictures from front-end. As a SG meanwhile, it works for the signaling interaction between the clients and

		server, and works as reverse proxy for device configuration and signaling proxy for device.
StreamingGateway	An embedded Streaming Server	Used for passing through video stream and two-way audio stream, and streaming from third-party devices.
Third Party Plug-in Service	For third-party plug-in service	Used for accessing with third-party devices (e.g. log in to device, alarm configuration, arming, PTZ control, etc.)
SmartWallManagent Service	Smart Wall Management Service	Responsible for smart wall-related device (such as decoders and screens) management and smart wall operation management (including display live view, playback, and views on smart wall, etc.)
KeyboardProxy Service	Keyboard Proxy Service	Used for accessing network keyboard and perform operations by a network keyboard
DataBase	Database-related service	Used for storage of module data

2.5.2 Other Servers

You can select other servers depending on your need:

- Streaming Server: you can add a streaming server to HikCentral Professional to get video/audio data from it, thus to lower the load of the device.
- Recording Server: a server that can store data such as videos and pictures from device.

2.5.3 Security Device

Surveillance device refers to device installed and used in security areas for monitoring. Users can select device types according to their needs. HikCentral Professional supports the following security device types:

- Video Surveillance Device
- Access Control & Attendance Device
- LPR (License Plate Recognition) Device
- Facial Recognition Device
- UVSS Device
- Security Control Device
- Smart Wall

See *HikCentral Professional Compatibility Lists* for details about device types and models.

2.5.4 Client

HikCentral Professional adopts 3 clients: Web Client, Control Client, and Mobile Client.

Web Client

Web Client supports mainstream Web browsers including Internet Explorer, Chrome, and Firefox. It aims to system managers for resource management and configuration.

Control Client

Control Client runs in Windows operating system for monitoring surveillance areas. Users are often security staffs.

Mobile Client

Mobile Client runs in iOS and Android operating systems for users who need to monitor security areas.

2.6 System Module

HikCentral Professional provides basic modules and application modules.

2.6.1 Basic Modules

Basic modules provide a foundation for application modules. Basic modules include the following modules:

Module	Description
Resource Service Module	Used for management of encoding device configuration, areas, and cameras, etc.
Login and Authorization Service Module	Used for user login and authorization for accessing the system's resources.
System Configuration Service Module	Used for configuration of external network, NTP, and ports.
License Service Module	Used for license management, including license activation and deactivation, trial license management, etc.
Maintenance Service Module	Used for system maintenance, including database backup and restore, upgrade, and real-time status overview.
Permission Service Module	Used for the management of user permissions, including user

	configuration, role configuration, and permission authentication, etc.
Log Service Module	Used for log management, including retention and searching of operation logs and system logs.

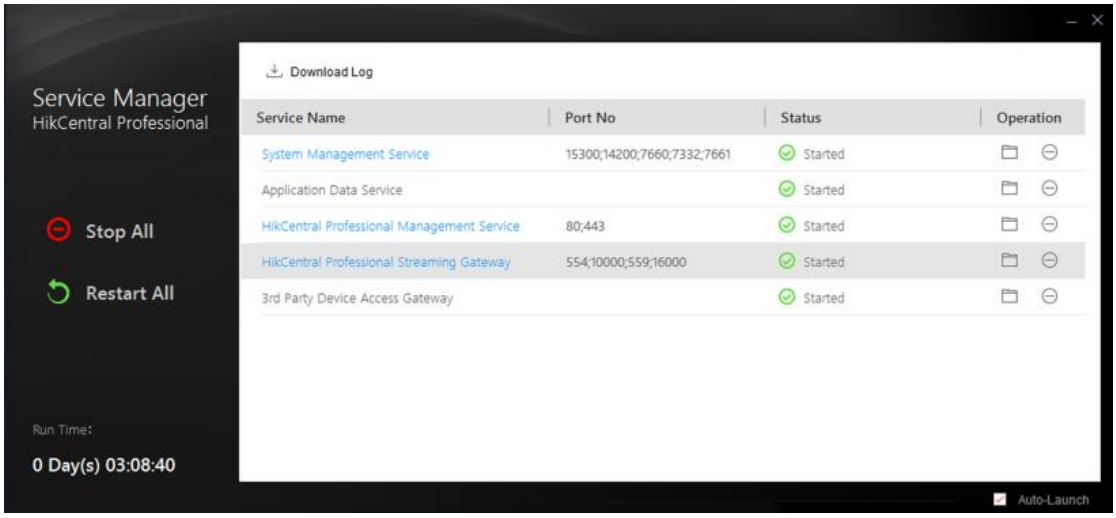
2.6.2 Application Modules

Application modules cover various surveillance functions including:

Module	Description
Monitoring	Used for live view, playback, two-way audio, and URL assembling, etc.
Access Control	Used for management of access point and access group, access level configuration, card issuing, certificates management, and access control event searching, etc.
Time and Attendance Management	For attendance-related operations including setting attendance check points, attendance groups, and time periods, and processing attendance data.
LPR (License Plate Recognition)	For license plate recognition, including vehicle management, and vehicle list management.
UVSS	For UVSS picture management, including vehicle-passing picture management, and undercarriage picture searching, etc.
Security Control	For management of security control devices and alarm linkage actions, etc.
Facial Recognition	For face comparison group management, real-time facial recognition, and face search, etc.
Maps	For management of e-map, GIS map, hot spot, and hot region.
Smart Wall	You can access a smart wall to HikCentral Professional to display related resource on the wall.
Event and Alarm	For event and alarm related functions, including event and alarm configuration, receiving alarm notifications, searching and saving history events, etc.
Storage	For storage related functions, including configuration and management of recording server and recording schedule.

Chapter 3 System Function

3.1 Service Manager



- Display and control the status of all the services.
- Supports run time calculation.
- Supports downloading system logs.

3.2 Web Client

3.2.1 Remote Site Management (RSM)

- 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.
- Configure GIS location of Remote Sites
- RSM function shall be supported by the Central System activated by the license that takes this function

3.2.2 License Management

- Supports online/offline activate/deactivate license, online/offline update the license, and view license detailed information for system capabilities
- After activating the license, show the capability that the system supports, including the supported function modules and detailed amount.
- Display the expiry date for the trial license.
- During the trial period, if the remaining trial period is less than 7 days, the system will prompt the user when the user logs in.
- Supports license list.
- For facial recognition camera/ANPR camera/thermal camera (report supported), user can select the added cameras as these three types of cameras. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

3.2.3 Physical View

- Supports adding and managing devices including network cameras, NVRs, DVRs, encoders, decoding devices, Streaming Servers, Hybrid SANs, pStors, Cloud Storage Servers, access control devices, security control devices, elevator control devices, dock stations, security radars, security audit server, DeepinMind servers, Application Data Servers, etc.
- View the device address, serial No., version, available resources, network status, etc.
- Enter the device remote configuration page to set more parameters.
- Add devices by Hikvision SDK protocol. Add devices by IP address, domain name, batch importing, IP segment, and port segment. The device can be offline when adding by batch importing. Add encoding devices and security control devices by Hik-Connect, and the devices will be added to Hik-Connect service after adding to the system.
- Add third-party network cameras by ONVIF protocol.
- Add encoding devices and access control devices by EHome protocol by device ID, ID segment, and batch importing.
- Supports device deployment in different time zones and checking DST time. When the device's time zone mismatches with the system, apply time zone settings to the device.
- Import all or part of the channels when adding a device. When importing all channels, system will import these logical resources into a area named by the device name. You can also select an existing area or create a new area.
- Set the recording setting of the logical resources when adding an encoding device. By device, the storage location is encoding device. Supports getting recording schedule from device. By default, you can complete the storage settings without editing any parameters. Supports central storage location such Hybrid SAN, Cloud Storage Server, and pStor.

- For encoding devices, Edit bandwidth for video downloading.
- Add pStor, Network Video Recorder (only for picture storage), Cloud Storage Server and Hybrid SAN as Recording Server.
- Add decoding devices by IP address, IP segment, and port segments. The device can be offline when adding by IP segment and port segment.
- Support the linkage between decoding device’s or video wall controller’s decoding outputs and smart wall windows.
- Set the decoding output of the decoder as the signal input of video wall controller.
- Add Streaming Server via IP address, and import service component certificate to Streaming Server
- Supports cascade when adopting both decoders and video wall controllers in smart wall by linking decoder's output with the video wall controller's input.
- Add facial recognition server by IP address and add cameras to facial recognition server.
- Add behavior analysis server by IP address and set analysis tasks.
- Change devices' passwords in a batch.
- Online device detection function is available on the Web Client accessed via Internet Explorer, Google Chrome and Firefox, and the active online devices in the same local subnet with the Web Client/ SYS Server will be displayed on a list.
- Add application data server for distributed deployment to improve the system's performance.

3.2.4 Logical View

- Manage resources (cameras, alarm inputs, alarm outputs, doors, elevators, and UVSSs) by areas.
- Synchronize camera name, moving the camera to other area, and displaying elements of sub-areas, remote configuration on device, copying the current camera’s specified configuration parameters to other cameras for batch configuration.
- Synchronize access point name, moving the access point to other area, and displaying elements of sub-areas, copying the current access point’s specified parameters to other access points.
- Synchronize/apply access point name.
- Get recording schedule from the device.
- Enter the remote configuration page of the device to set move detailed parameters.
- Add alarm inputs/outputs, the functions of moving the inputs/outputs to other area, and display elements of sub-areas.
- Move the UVSS to other area, and display elements of sub-areas.
- Copy configuration information of stream type, protocol type, main storage, and auxiliary storage to other channels.
- Set maps for the areas and locate the logical resources on the map.
- Set resource groups in areas including: alarm groups, people analysis groups, heat analysis groups, pathway analysis groups, person feature analysis groups, multi-door interlocking groups, anti-passback groups, and security control partitions.

- Locate resource groups on maps.

3.2.5 Recording Settings

- Configure recording settings for cameras in current and Remote Site.
- Set main storage and auxiliary storage for cameras.
- Synchronize recording settings to device.
- Get recording settings from device.
- Select storage location as Encoding Device, Hybrid Storage Area Network, pStor, Cloud Storage Server for cameras of current site.
- Select storage location as pStor, Hybrid Storage Area Network or Cloud Storage Server of central system for cameras of Remote Site.
- Set recording schedule template.
- Select stream type as main stream or sub-stream.
- Set pre-record and post-record for recording the video.
- Select the storage mode for the recorded videos of cameras of current site: overwrite the oldest videos when disk or allocated quota is full, and automatically delete the oldest videos after the specified retention period.
- Select a Streaming Server to get the video stream of the camera.
- Enable the ANR function to turn Automatic Network Replenishment on to temporarily store the video in the camera when the network fails and transport the video to storage devices when the network recovers if the video files are stored in an Encoding Device or Hybrid SAN.
- Set picture storage settings for cameras, including pictures captured by facial recognition cameras, ANPR cameras, and alarm pictures.
  - Set storage location as system management server.
  - Set storage location as Hybrid SAN.
  - Set storage location as Cloud storage server.
  - Set storage location as a pStor.
- Supports hot spare settings of Hybrid SANs and NVRs.
- Supports one-touch configuration of Hybrid SANs.
- Enter the web page of pStors, Hybrid SANs, and Cloud Storage Servers for detailed parameters settings.
- Show the used space of the Recording Servers, as well as remaining space and storage channel information.

3.2.6 Event and Alarm Settings

- Set system-monitored events and alarms for the resources, including cameras, doors, elevators, radars, alarm inputs, ANPR cameras, persons, UVSSs, Remote Sites, encoding devices, access control devices, elevator control devices, security control devices, dock stations, decoding devices, resource groups, Recording Servers, Streaming Servers, DeepinMind servers, security audit servers, SYS servers, users,

user-defined events, and 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, 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
- 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

3.2.7 Map Management

- Supports Google Map and locate cameras, alarm inputs, alarm outputs, doors, UVSSs on the Google Map. Link hot regions (other maps) to the Google Map. Add label on the map. Locate sites on the map.
- Relate maps with areas. Locate cameras, alarm inputs, alarm outputs, doors, elevators, UVSSs, radars, elevators on the Google Map. Link hot regions (other maps) to the Google Map. Add label on the map.
- Customize the icon and size of the cameras, alarm inputs, alarm outputs, and other elements.
- Set API URL of Google Map to meet the needs of different regions. Users should purchase API URL from Google.
- Set related map when setting alarms. When checking the alarm information, you can view the alarm source's location on the map.
- Supports OpenStreet offline map.
- Supports setting map's map scale, which will affect the camera's field of view.

3.2.8 Vehicle Management

- Add vehicle information manually
- Import vehicle information according to the pre-defined template
- Add basic vehicle information in one list, i.e. license plate number, effective period, brand, model, owner and phone number.
- Upload undercarriage picture to view both the current vehicle's captured undercarriage picture and the uploaded picture for comparison
- Edit vehicle's effective period one by one or in a batch.

3.2.9 Person Management

- Add person group.
- Link person group with access group and attendance group.
- Add person information one by one.
- Set person profile.
  - Collect profile by added access control device
  - Take a picture by webcam
  - Upload a picture from local PC
- Custom 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.
- Profile format: JPG, JPEG, and PNG.
- Import person information from added devices.
- Verify face quality by added access control device when collecting profile by added device.
- 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.
- Report card loss for person if the card is lost, and issue a temporary card.
- Cancel card loss if the lost card is found.
- Export all persons information and set password for decompressing.

3.2.10 Face Comparison

- Create face comparison groups and select persons from person list to add them into face comparison groups. Import persons into a face comparison group. Specify a face comparison group when importing persons from AD domain.
- Set similarity threshold for each face comparison group.
- Apply the face comparison group to facial recognition cameras.

- View all the facial recognition cameras that the face comparison group applied to.

3.2.11 Access Control

- Add access control devices to the system; Set time zone for the added devices. Set time synchronization mode: NTP server or manual. Set DST of the devices. Set custom Wiegand. Reboot device. Reset device parameters. Enter remote configuration page for more parameters.
- Add access point(s) to the access level and select the access schedule to define in which time period the person is authorized to access the access points.
- Group persons with same access permission into access groups
- Assign the access level to some access group(s) so that the person(s) in the access group(s) will have the access permission to access the access point(s)
- When adding person, enable 'Super User' function to exempt this person from remaining locked (credentials failed) restrictions, all anti-passback rules, and first card authorization.
- When adding person, enable 'Extended Access' function to open the access point for longer time for person with special requirements.
- When adding person, set credential information for the person:
  - PIN code
  - Card
    - ✓ Set issuing mode as card enrollment station or card reader
    - ✓ Set card format as normal or Wiegand
    - ✓ Audio on/off
    - ✓ Set effective period for the card
    - ✓ Up to 5 cards for one person
  - Fingerprint
    - ✓ Set issuing mode as USB Fingerprint Recorder or Fingerprint and Card Reader
    - ✓ Add a new fingerprint
    - ✓ Record up to 10 fingerprints for one person
    - ✓ One fingerprint can only be related to one card
  - Credentials under duress and credentials for dismiss
- Set anti-passback rule
- Set multi-door interlocking rule
- Set multi-factor authentication rule
- Set entry & exiting counting rule

3.2.12 Time and Attendance

- Group persons into attendance groups. Add persons into attendance group from person list. Import persons into attendance group by a template file.
- Set effective period of the attendance group.
- Link attendance group with person group.

- When adding person, add person to attendance group.
- When adding person, enable 'Super User' function to exempt this person from remaining locked (credentials failed) restrictions, all anti-passback rules, and first card authorization.
- When adding person, enable 'Extended Access' function to open the access point for longer time for person with special requirements.
- When adding person, set credential information for the person:
  - PIN code
  - Card
    - ✓ Set issuing mode as card enrollment station or card reader
    - ✓ Set card format as normal or Wiegand
    - ✓ Audio on/off
    - ✓ Set effective period for the card
    - ✓ Up to 5 cards for one person
  - Fingerprint
    - ✓ Set issuing mode as USB Fingerprint Recorder or Fingerprint and Card Reader
    - ✓ Add a new fingerprint
    - ✓ Record up to 10 fingerprints for one person
    - ✓ One fingerprint can only be related to one card
  - Credentials under duress and credentials for dismiss
- 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.
- Synchronize access records to third-party database.
- Adopt access control devices or facial recognition cameras for time and attendance.

3.2.13 Dock Station Group

- Group persons into dock station groups for evidence collection.
- 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)

3.2.14 Visitor Management

- Add visitor group
- Add visitor one by one.
- Import information of multiple visitors in a batch by importing an Excel file.
- When adding a visitor, enter visitor name, ID type, ID number, gender, profile, visitor group, email, phone number, visitee, visit reason, visit time, access level, etc.
- When adding a visitor, enable 'Extended Access' function to open the access point for longer time for person with special requirements.
- When adding a visitor, set credential information for the person:
  - PIN code
  - Card
    - ✓ Set issuing mode as card enrollment station or card reader
    - ✓ Set card format as normal or Wiegand
    - ✓ Audio on/off
    - ✓ Set effective period for the card
    - ✓ Up to 5 cards for one person
  - Fingerprint
    - ✓ Set issuing mode as USB Fingerprint Recorder or Fingerprint and Card Reader
    - ✓ Add a new fingerprint
    - ✓ Record up to 10 fingerprints for one person
    - ✓ One fingerprint can only be related to one card
- Edit information of the visitor who is checked-in.
- View QR code of the visitee.
- Visitor check-out: manually check-out and automatically check-out.

3.2.15 Security Control

- Alarm Output: Triggers, alarm lamps, sirens, locks on the security control devices are alarm inputs in the system.
- Alarm Input: Zones on the security control devices are alarm inputs in the system.
- Security Control Partition: Partitions on the security control devices are security control partitions in the system.
- Add security control devices to the system; Enter remote configuration page to set detailed parameters; Show all the alarm inputs (zones) and related partitions.
- In Logical View, import alarm inputs into areas; Set alarm input name and detector

type, such as panic switch, humidity detector, etc. Set zone type, such as instant alarm zone, delayed zone, internal zone, etc.

- Show names of the imported security control partitions and other information.
- When adding a security control device, its alarm inputs can be imported to the system. Supports importing the 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.
- In defense schedule, there are three arming modes: stay arming, instant arming, or away arming.
  - Stay Arming: It is used when people stay inside the detection area. During stay arming, all the perimeter burglary detections (such as perimeter detector, magnetic contacts, curtain detector in the balcony) will be turned on. Meanwhile, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and not trigger an event or alarm.
  - Instant Arming: It is used when people leave the detection area. The zone will be immediately triggered when it detects event or alarm with no delay and notify the security personnel.
  - Away Arming: It is used when people leave the detection area. Event or alarms will be activated when the zone is triggered or tampered. For delayed zone, the alarm will not be activated when the zone detects triggering event during entry/exit delay.
- For panic alarm stations, besides the alarm inputs, the cameras should be imported into areas.
- Locate alarm inputs on the GIS map or e-map.

3.2.16 Security (User & Role)

- One role can be used by multiple users; One user can be assigned with multiple roles.
- 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
  - Area Display Rule: Restrict user profile access for administration functions defined as logical areas.
  - Resource Access: Set resource access for logical resources, encoding devices, decoding devices, access control devices, dock stations, etc.
  - User Permission: Including resource permission (operations for cameras, access

points, UVSSs, security control partitions, encoding devices, etc.), configuration permission (functions on the Web Client), and control permissions (functions on the Control Client).

- Manage Security: With this permission, the role can manage the security permissions for the Web Client. It means when setting roles, the user with this role can assign these permissions to other roles according to actual needs .

- 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
- Display all the added users, show the user's login status, user status, expiry date, connection number (view all the types of logins of each users, including login via Web Client, Control Client, Mobile Client, OpenAPI Client, KPS Client, etc.).
- 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

3.2.17 Maintenance

- Shall backup and restore system data:
  - Shall set database backup of HikCentral Professional system, including configured data, configured pictures, received events, received alarms, face comparison data, card swiping records, attendance records, vehicle passing records, video analysis data, and server logs
  - Shall set the frequency of backup as daily, weekly or monthly
  - Shall set the backup date
  - Shall set the backup time
  - Shall check the saving path
  - Shall set the max. number of backups
  - Shall restore the configured data
- Shall export configuration data of Remote Site, encoding device, and recording settings
- Shall download HikCentral Professional Control Client on the Web Client
- Upgrade device firmware via Web Client or EZVIZ Cloud Service
  - Simultaneous upgrade

- Set upgrade schedule

3.2.18 System Configuration

- Create a name for the current site.
- Set the first time of the week.
- Set temperature unit as Celsius, Fahrenheit, or kelvin
-
- Server usage thresholds: Set event/alarm for notification if the CPU usage or RAM usage approaches the pre-determined threshold and lasts for certain duration.
- Enable GIS map function, configure the map API URL, and customize the icons of hot region and hot spot.
- NTP settings.
- Active directory settings: If you have the AD (Active Directory) domain controller which contains the information (e.g., user data, computer information), you shall be able to configure the settings to get the related information. In this way, you can add the users that belong to an organization unit (e.g., a department of your company) to HikCentral Professional conveniently.
- Link person information 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.
- 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
- Select the NIC of the current SYS so that the system can receive the alarm information of the third-party device connected via ONVIF protocol.
- 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 camera ID as identifier number on the keyboard to display live view on smart wall
- 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.

- Reset network information of added devices.
- Export service component certificate from SYS server.
- Set frequency for health check.
- Set open platform.
- Set database password by admin user.

3.2.19 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

3.2.20 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.

3.2.21 Intelligent Analysis

- View intelligent reports on the Web Client.
- Create dashboard and add reports to the dashboard.
  - Report dashboard
  - People counting report
  - Queue analysis report
  - Heat analysis report
  - Pathway analysis report
  - Person feature analysis report
  - Temperature analysis report
  - Vehicle analysis report
- Set report type and time of the reports in one dashboard for as the range of data for display

3.2.22 Local Configuration

- Set the network transmission settings
  - GPU hardware decoding: Enable the GPU decoding for live view and playback to save CPU resources.
  - 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: Video caching should be determined based on network performance, computer performance, and bit rate. 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

3.2.23 Application Data Server

- Provides distributed deployment for the two core services: System Management Service and Application Data Service. Distributed deployment can improve the system performance and the number of connectable cameras can be increased to 10,000.
- Download installation package of Application Data Server.
- In Physical View, add Application Data Server on the SYS server.
- Add a standby server.

- Set threshold of failure status: If the system disconnects with the Application Data Server or Application Data Standby Server and the disconnection lasts for specified time, the system will regard the server as failure and notify the administrator to maintain it.

3.2.24 Download Installation Package

- Download installation package of Application Data Server.
- Download installation package of Control Client.

3.3 Control Client

3.3.1 Login

- Supports setting IP address and port number for login, login by HTTP protocol (default port number 80) or HTTPS protocol (default port number 443).
- Supports remembering password after login, so there is no need to enter the password again when you log into the system next time.
- Supports auto-login.
- A QR-code is displayed on the login page for scanning to download the Mobile Client.
- The user account will be frozen after 5 failed password attempts.
- Supports multiple languages.
- Log in with the domain user account.
- Automatic launch the client and login with the domain user.
- Startup wizard guides you through new functions.

3.3.2 Main View

- Customize the module arrangement on the control panel

3.3.3 Live View

- View real-time video from up to 256 cameras on current site or cameras imported from Remote Site.
- Switch to playback during live view of multiple cameras.
- Get the live view of the cameras and other related cameras of the resources on the map.
- View resource groups on map, such as multi-door interlocking group, entry & exit counting group, etc., which are configured on the Web Client.
- Switch the live view stream to main stream, sub-stream, or smooth stream.
- Customize window division.

- Live view on 4 screens and 64 cameras for each screen. Switch to playback for one of the 4 screens.
- 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.
- Quick-jump to Vehicle Search page.
- Tool bar on the live view window, including manual recording, capture, instant playback, digital zoom, two-way audio, turning on/off the audio in live view, 3D positioning, PTZ control, camera status detection, arming control, switching stream, start on smart wall, VCA playback, alarm output control, view fisheye camera's live view in fisheye dewarping modes, adding tag.
- Customize tool bar of live view window.
- Public view and private view
- Save a map as a view.
- Auto-switch one area's cameras
- Auto-switch one view's cameras
- PTZ control
- View live videos of door and elevator's related camera(s).
- Control doors to lock, unlock, remain locked, or remain unlocked.
- Control floors status as temporary access, access with credential, free access, or access forbidden.
- View live video of the radar's calibrated cameras, arm/disarm radar during live view of its related cameras, and show moving pattern of detected people.
- Enable/disable wipers in a batch.
- Control status of all doors.
- Trigger user-defined events.
- View detected events in live view, including resource events, face comparison events, and access events.
- Subscribe access events including normal card swiping events, device events, abnormal card swiping events, alarm input events, and other events.
- Show/hide event list.
- View capture camera's live view and view detected and matched persons, including captured time, comparison result, device name, face comparison group name, gender, person ID, email, phone number, etc.
- Quick-jump to video search page for face comparison events.
- Quick-jump to search page for access events.
- Add mismatched persons to person list during live view.

3.3.4 Playback

- Async/Sync playback for up to 16 cameras of the current sites and remote sites, and the time will show when hovering the cursor on the time line
- Export the installation package of VSPlayer as well as recorded videos in MP4\AVI\EXE format, and supports encryption when exporting videos in MP4 and EXE format.

- Playback in fisheye dewarping mode, add default, customized tag to mark the important video footage, visual tracking, lock/unlock the video file for file protection, download the video files, VCA search, Turn on/off the audio in playback; adjust the volume, switch the video stream to main stream, sub-stream, or smooth stream, transcoding playback.
- Pause/continue playback, playback frame-by-frame, slow/fast forward.
- Playback on smart wall.
- Play the tagged video footage.
- Enable/disable thumbnail display.
- Zoom in/out timeline.
- Playback of door-related cameras. Playback of 2 cameras related to a door is displayed in one window and support switching camera.
- Search video footage by video type, tags, and storage location.

3.3.5 Alarm Center

- Receive alarms and perform related operations, including view alarm's remarks, name, priority, occurring time, source, area, triggering time, status, types. Support quick operation on single alarm, including quick-jump to event search page, two-way audio, export alarm information, and delete alarm.
- Display system alarm information including time and description, edit alarms' priority and type, add remark for handling alarms.
- Acknowledge multiple alarms in a batch.
- Sort alarms by the selected property, such as mark status, priority, and alarm status.
- View the live video from the related camera, and check the alarm location on the map.
- Customize the arrangement of alarm center: video and map/video/map.
- Enable/disable the alarm audio.
- Enable/disable alarm triggered pop-up window.
- Arming control: arming and disarm.
- Pop up Alarm Center on the auxiliary window for convenient management.
- Display captured pictures in Alarm Center.

3.3.6 Event & Alarm Search

- Search event by event source, type, and time.
- Search alarm by source, type, marked/unmarked, priority, alarm status, category, and alarm time.
- Export all searched alarms as a file in CSV/PDF/Excel format
- Configure amount of displayed events/alarms on each page.

3.3.7 Video Search

Video Clip Search

- Search videos of certain time period by time range, tag, and locking status.
- Select video segment or interval when searching video by time range.
- Search video clip by stream type.
- Search video clips on Remote Sites.
- Export video clip in a batch.
- Switch display mode of searched result between list and thumbnail mode.
- Edit amount of displayed video footages on each page.

Search Video Stored on Device

- Search video stored on dock station by time, dock station group, and file type.
- Search transaction video footage stored on some NVR by time, camera category, case sensitive, key words, etc.
- Search ATM transaction event triggered video footage by time, transaction No., and camera.

VCA Search

- Search video footage on Remote Sites.
- Search VCA event related video including motion detection, intrusion, and line crossing by source, time, VCA rule, sensitivity on condition that the camera supports VCA event and you have enabled VCA event on the camera and NVR.
- Export video footages in a batch.
- Switch between list mode and thumbnail mode.

3.3.8 Person Search

Search by Face Picture

- Search face picture to view face-related face pictures and videos. It includes 3 types:
  - Search matched pictures: search videos of a person who is added to the face comparison group.
  - Search captured pictures: search related videos of an uploaded face picture by camera, time, person information, and similarity.
  - Search frequently appeared persons: search persons who appear frequently.

Search by Archive

- The system will save the features and information (including captured picture and video) of the captured person as archive.
- Upload a picture and search the related archives of a face picture to check the captured pictures or videos of similar persons.
- Adjust the similarity.
- Check whether a person is a stranger.
- Export the search results.

Search by Identity Verification

- Upload a picture and search the persons who are similar with the person in the picture. Check the matched person information.
- Upload two pictures and compare them to see the similarity of the persons in those two pictures.
- Adjust the similarity.

3.3.9 Search Vehicle Passing Record

- Search vehicle passing records by time, source (ANPR or UVSS cameras), marked/unmarked, country/region, license plate No., vehicle owner, vehicle brand, vehicle color, etc.
- Mark a vehicle.
- View detailed vehicle passing records, including marked/unmarked, license plate No., passing time, channel name, vehicle owner, country/region, etc.
- Add detected vehicles to vehicle list.
- Export vehicle passing records and related videos.
- View captured passing vehicles and undercarriage pictures, view related video of vehicles.
- Edit license plate No. in the detected passing vehicle records.

3.3.10 Search Access Records

Identity Access Search

- Search identity access event by time, door, person (normal person and visitor), access event, and entry & exit records.
- View access related video footage.
- View details of access event, including person name, person ID, event type, and

access result, etc. Filter normal persons or visitors.
- Forgive anti-passback violation.
- Export one or multiple access events.

Entry & Exit Counting

- Search people stayed, people exited, or all the people who entered and exited.
- Filter persons and visitors in the entry & exit records.

3.3.11 Evidence Management

- Save recorded video during live view and clipped video during playback as evidence.
- Save downloaded video footage as evidence.
- Upload video stored on Dock Station to the platform and save it as evidence.
- Search evidence by ID, key words, type, organization, result, status, and time period.
- Download, close, delete, and export evidences.

3.3.12 Dashboard

- Add reports to customized Dashboard, including people counting report, queue analysis report, heat analysis report, pathway analysis report, person feature analysis report, temperature analysis report, vehicle analysis report
- Add/delete dashboard, edit dashboard name.
- Save different reports as a Dashboard, export Dashboard data, display Dashboard on auxiliary screen.

3.3.13 Person Analysis

People Counting

- Generate people counting report by camera or predefined people counting group, report type, and time.
- Switch between line chart and histogram, view entered people amount, exited people amount, and the sum of entered and exited people amount.
- Hide or show certain camera's data.
- Export people counting report as a file in CSV/Excel format
- Display report on dashboard.
- Display report on auxiliary screen.

Queue Analysis

- Generate queue report by queue length and waiting duration, and calculate person amount in queue during different time periods. Waiting duration report displays people amount of a queue during different time periods. Queue length report displays report of queues with defined people amount.
- Hide or show certain camera's data.
- Export queue analysis report as a file in CSV/Excel format.
- Display report on dashboard.
- Display report on auxiliary screen.

Heat Analysis

- Generate heat analysis report by camera or predefined heat analysis group, report type, time, analysis type, dwell time, average dwell time, people amount, etc.
- Hide or show certain camera's data.
- Export heat analysis report as a file in PDF/Excel format.
- Display report on dashboard.
- Display report on auxiliary screen.

Pathway Analysis

- Generate pathway analysis report on the map. The pathway should be configured on the Web Client.
- Export pathway analysis report as a file in PDF/Excel format.
- Display report on dashboard.
- Display report on auxiliary screen.

Person Feature Analysis

- Generate person feature analysis report by camera or predefined person feature analysis group, and specify the time range.
- Export person feature analysis report as a file in PDF/Excel format.
- Display report on dashboard.
- Display report on auxiliary screen.

3.3.14 Temperature Analysis

- Generate temperature report to show the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry

points on different presets.
- Export temperature report as a file in CSV/Excel format.
- Display report on dashboard.
- Display report on auxiliary screen.

3.3.15 Vehicle Analysis

- Generate vehicle analysis report by time and report type
- Export vehicle analysis report as a file in CSV/Excel format
- Display report on dashboard
- Display report on auxiliary screen

3.3.16 System Maintenance

Real-Time Status

- Real-time status overview of the resources, including cameras, access points, UVSSs, encoding devices, access control devices, security control devices, dock stations, Remote Sites, decoding devices, SYS servers, Recording Servers, Streaming Servers, and facial recognition servers.
- Self-adaptive display.
- Display network speed and usage of CPU, RAM, and Streaming Server status.
- Configure automatic refreshing interval.
- Export data as a file in PDF/CSV/Excel format
- Display report on dashboard
- Display report on smart wall and auxiliary screen

History Status Overview

- History status overview of the managed resources including resource online rate, device online rate, and recording integrity rate
- Total offline duration and offline times of resources and devices.
- Click resource or device name to go to the log search page.
- Search by time.
- Export history overview report as a file in PDF/Excel/CSV format.
- Display history overview on smart wall and auxiliary screen.

Health Monitoring

- Detailed status page of cameras, encoding devices, doors, elevators, UVSSs, access

control devices, elevator control devices, security control devices, dock stations, Remote Sites, decoding devices, Recording Servers, Streaming Servers, DeepinMind servers, security audit servers, etc.

- Filter exceptions of resources and devices.
- Refresh manually.
- Export health monitoring report as a file in Excel/CSV format.
- Display health monitoring page on smart wall and auxiliary screen.

3.3.17 Log Management

- Search log files of servers, Remote Sites, cameras, and smart walls that are connected to the system by time period.
- Export logs as a file in Excel/CSV format
- Display logs on auxiliary screen

3.3.18 Smart Wall

- Smart Wall (Decoding Device)
  - Display live view, playback, and alarm related video on smart wall
  - Window division (up to 36 windows), show/hide window No. and camera ID
  - Add/delete/edit views and view groups
  - Lock/unlock selected window
  - Auto-switch of views
  - Join windows
  - Create a roaming window
  - View camera status
  - Switch the live view stream to main stream or sub-stream
  - PTZ control
  - Quick-jump to Alarm Center
  - Export and print window No. and camera ID
  - Search smart wall related logs
- 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
- Support 1005K USB network keyboard
  - Used 1005K USB network keyboard to perform live view in fisheye expansion mode

- 1005K USB network keyboard to perform PTZ control

3.3.19 Tools

- VSPlayer
- Broadcast
- Alarm output
- Two-way audio

3.3.20 System Settings

- View and manage downloading tasks in the Download Center.
- View/delete/print manually captured pictures.
- View and delete manually recorded videos.
- 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.

3.4 Mobile Client

3.4.1 Login

- The user will be asked to change password for the first time login, when password expired, when the password strength is too low, or when the password is reset.
- Show password strength when changing password.
- Login via domain account.
- Enter domain name in the IP Address field.
- Auto-login.
- Login via HTTP or HTTPS protocol. When login via HTTP, the default port is 80. When login via HTTPS, the default port is 443.

3.4.2 Logical Resource

- View logical resources on the current site and on the managed Remote Sites.
- Display thumbnails of the logical resources.
- Display online resources only. Display area name. Icons available: Go to Live View, Go to Playback, Add to Favorites.
- Live view and playback of a group of resources in the view.
- Search resources by keywords or filter resources by site, area, or resource type.

3.4.3 Live View

- View the live video of a single channel or simultaneously view multiple channels.
- Add more channels during live view to view the live videos of the newly-added channels and the existing channels simultaneously.
- Switch cameras if the door, radar or elevator controller links two cameras.
- Switch from live view to playback.
- Up to 4 (for HD: 9) live view windows can be displayed on one page. Swipe to the right/left to switch pages if more than 4 (for HD: 9) resources are under live view.
- Drag to adjust the window sequence in multi-window mode.
- Perform PTZ control for cameras with pan/tilt/zoom functionality, and set preset, patrol, pattern, as well as 3D positioning for cameras in PTZ control mode.
- Record (clip) video files and capture pictures manually during live view.
- Preview the captured picture and recorded video footage.
- Save the captured picture or recorded video footage to the photo album of the phone.
- Send the captured picture or recorded video footage to others by email.
- Play the live video of the fisheye camera in fisheye dewarping mode.
- View ANPR camera's live video. The license plates of the passing vehicles (including motorcycles) in the field of views of the ANPR cameras will be recognized.

- Control the status of doors (including turnstiles) and view the card swiping record in real time when viewing the live video of the door's related cameras. If the door is a turnstile, select entrance control or exit control.
- View the live video of the radar's related camera.
- Arm/disarm the radar during the live view of the radar's related camera.
- View the live video of the elevator's related camera.
- During live view of elevator's related camera, set the access level (temporary access, access with credential, free access, or access forbidden) for each floor linked to the elevator control device.
- View the live video of the UVSS's related camera (for HD only).
- Display the real-time information of the passing vehicles, including undercarriage pictures, captured pictures (undercarriage and vehicle), license plate number, passing time, etc. (for HD only).
- Mark on the captured undercarriage pictures to mark the important information and save on the server (for HD only).
- Add vehicle to the vehicle list.
- Display the real-time facial recognition information, including captured faces, original faces, similarity, matched person information, captured time, etc. (for HD only).
- Add mismatched person to person list (for HD only).
- Trigger user-defined events manually.
- Add logical resources to favorites during live view.
- Turn on or turn off audio of the selected channel.
- Perform two-way audio via NVR or channel during live view.
- Zoom in or zoom out the live view image.
- Set the stream type of a channel to main stream, sub-stream, or smooth stream during live view.

3.4.4 Playback

- View the video footage of a single channel or multiple channels.
- Switch to live view during playback.
- Adjust playback speed to 1/4X, 1/2X, 1X, 2X, and 4X.
- Up to 4 playback windows can be displayed on one page. Swipe to the right/left to switch pages if more than 4 resources are under playback (for HD only).
- Trigger user-defined events manually.
- Select video footage in main storage, auxiliary storage, or central storage for playback.
- Set the stream type of a channel to main stream or sub-stream
- Clip video footage and capture pictures during playback.
- Preview the captured picture and clipped video footage.
- Save the captured picture or clipped video footage to the photo album of the phone.
- Send the captured picture or clipped video footage to others by email.
- Adjust the frame rate, bitrate and image resolution during playback according to the bandwidth conditions.
- Zoom in or zoom out the playback image.

- Play the recorded video of the fisheye camera in fisheye dewarping mode.
- Turn on or turn off audio of the selected channel.
- Play video files of multiple channels simultaneously in terms of the recorded time.
- Add resource to Favorites during playback.
- Supports PIP (Picture in Picture) mode, to display the live view window as an inset floating over the playback window so as to view the video footage and live view of the logical resource simultaneously.
- Supports VCA search (for HD only).
- Add mismatched person to person list (for HD only).
- Search access events, including person details and device information (for HD only).
- Subscribe events of access control and face comparison (for HD only).
- Add tags to a specific video footage which contains important information and search video footage by tags (for HD only).

3.4.5 Alarm Center

- Push near-real-time alarm notifications if you allow notifications from the Mobile Client in the OS of your phone or tablet.
- Swipe upwards to load more alarms, and swipe downwards to get the latest alarms.
- Set filter conditions to filter alarms.
- View the alarm related picture displayed on the Alarm Details page.
- Play the alarm related video displayed on the Alarm Details page.
- Mark specific items of alarm information.
- Acknowledge alarm(s) if the related event is handled. Set alarm priority and category when acknowledging alarm.
- Trigger user-defined events manually

3.4.6 View

- View the live video of channels managed in a view, which is a window division with channels configured to each window.
- Private view is only accessible to its creator.
- Public view is accessible to all the users of your system.
- View the camera's live video in full screen mode.
- View the resources in Favorites by resource type.

3.4.7 Map (HD)

- Show the locations of the logical resources on GIS map or e-map.
- Zoom in or zoom out the map.
- Add and edit labels with descriptions to specific locations on map, or delete the labels.
- Switch between different e-maps.

- Switch between e-map and GIS map.
- View the live video of a resource on map.
- View history alarms of resources on map and view the alarm related video footage (if exists).
- Show the resources of a HikCentral Site on the map of the Site.
- Control status of the doors on map.
- Search and view the access records of an access control devices or elevator controller on map.
- View the moving pattern of the object detected by the radar.
- Tap a radar on the map, and then arm/disarm the radar.
- Set access level (temporary access, access with credential, free access, or access forbidden) for the floor linked to the elevator controller.

3.4.8 Search (HD)

- Search the tagged video footage by the configured conditions (including tag name, camera, tag type, storage mode, and time).
- Search the face pictures matched with the pictures in the selected face comparison group(s) during the selected time periods.
- Search the face pictures of the persons in the selected person list captured by the selected camera(s) during the selected time period.
- Search the frequently appeared persons.
- Search the records (captured pictures) in stranger libraries of the face recognition 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.
- Upload a target picture and then search the persons whose face similarities with the target picture are higher than the configured similarity threshold.
- Search the information of the passing vehicles (including motorcycles), including owner name, recognized time, etc.
- Search the person information of the access records of the selected doors (doors or elevators) to view the event details, including the person picture, person name, ID, and time, etc.

3.4.9 Report (HD)

- Heat map report.
- Vehicle analysis report.
- Temperature report.
- People counting report.
- Queue analysis report.
- Pathway analysis report.

3.4.10 Person Management

- Registration for persons and visitors.
- Set the required information such as ID, profile picture, last name, face comparison group, and effective period, and then upload the person information to the system.
- Set the required information such as ID type, profile picture, last name, person group, visit purpose, and effective period, and then upload the visitor information to the system.

3.4.11 Others

- View the current user, server information, server address, as well as the account list, which displays the accounts of which the passwords are remembered when you logging in.
- Log in and enable the Mobile Client to remember account password so as to add account to the account list
- Switch account.
- View and manage the local video files and pictures that you manually record (clip) video files and capture pictures in the Live View Playback page. And export the pictures to the local album, or share the pictures and video files to other applications.
- Add person information such as a face picture to person list, and then add the person information to face comparison group(s) and set its effective period.
- Set the device access mode of the Mobile Client to Automatically Judge, Direct Connection, Proxy Mode or the same with the corresponding setting of the Web Client to define how the system accesses all the added encoding devices
- Set main stream or sub-stream as the default stream type for accessing the resources of all the encoding devices.
- Display detection frames (including motion detection frames, fire source information, temperature, etc.) on video.
- Automatically refresh the thumbnails of the resources displayed on the Logical Resource page and Favorites page.
- Supports hardware decoding which can provide better decoding performance and lower CPU usage when playing the HD videos during live view or playback.
- Set the time for the Mobile Client.
- Display the time zone information on the time.
- Allow the HikCentral system to push alarm information of the added resources to your Mobile Client.
- View the mobile data usage on the Mobile Client.
- View the Mobile Client information as well as details about Terms of Privacy, Open Source Software License, and End User License Agreement.
- View the Mobile Client information as well as details about Terms of Privacy, Open Source Software License, and End User License Agreement.

Chapter 4 System Performance

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

Features		Maximum Performance
General	Cameras	Centralized Deployment: 3,000① Distributed Deployment: 10,000② Central System (RSM): 100,000③
	Managed Device IP Addresses **Including Encoding Devices, Access Control Devices, Elevator Control Devices, Security Control Devices, and Remote Sites*	Centralized Deployment: 1,024① Distributed Deployment: 2,048②
	Alarm Inputs (Including Alarm Inputs of Security Control Devices)	3,000
	Alarm Outputs	3,000
	Dock Stations	1,500
	Security Control Devices	16
	Security Radars	10
	Alarm Inputs of Security Control Devices	2,048
	DS-5600 Series Face Recognition Terminals When Applied with Hikvision Turnstiles	32
	Facial Recognition Servers	64
	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: 20④
	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 for One Report	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
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	256
	Persons in One Access Group	10,000
	Access Levels	128
	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
Smart Wall	Decoding Devices	32
	Smart Walls	32
	Views	1,000
	View Groups	100
	Views in One View Group	10
	Cameras in One View	256
	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.

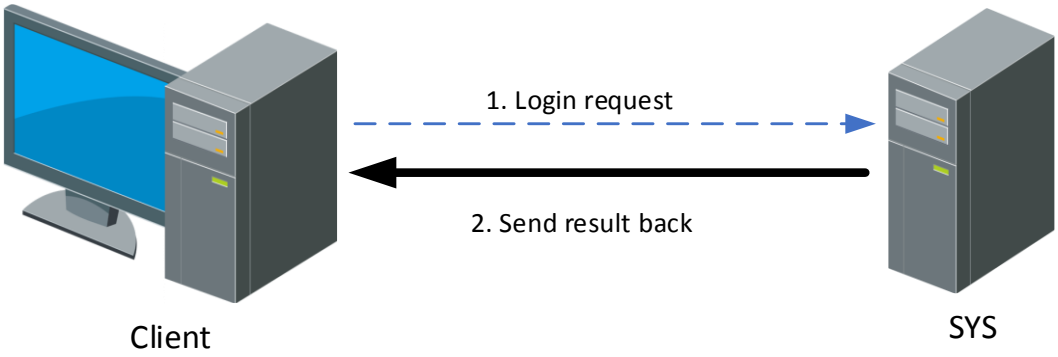
②: For one site with Application Data Server deployed independently, the maximum number of the added encoding devices, access control devices, and security control devices in total is 2,048. If the number of the manageable cameras (including the cameras directly added to the system and the cameras connected 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.

Chapter 5 Signal Flow

5.1 Login



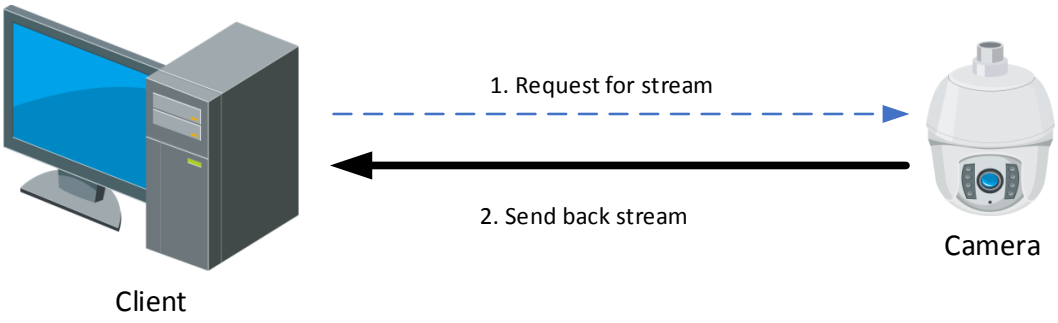
During the login, the signaling is exchanged between the client (Web Client/Control Client/Mobile Client) and the SYS server.

The signaling interaction process is as follows:

1. Enter the user name and password (domain name) on the client, which will be sent to the SYS server.
2. The SYS server receives the information, checks whether the user name and password (domain name) are correct, and sends the result to the client.

5.2 Live View

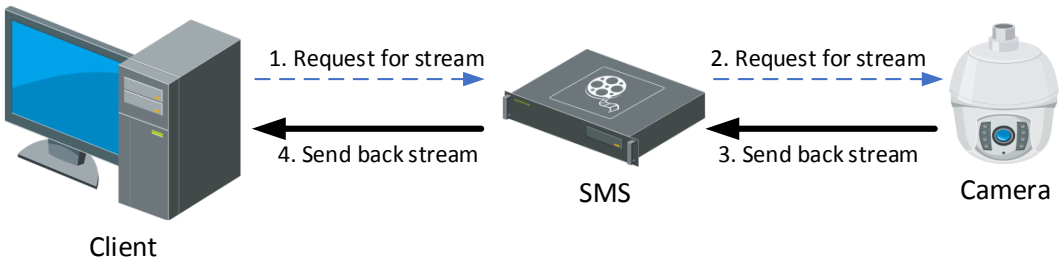
5.2.1 Live View for Directly Connected Device



If the SYS server, devices and the client are deployed in the same LAN network, the client can directly obtain the stream. The signaling process is as follows:

1. The client sends a request to the device for obtaining the stream.
2. The device sends back the corresponding stream to the client.

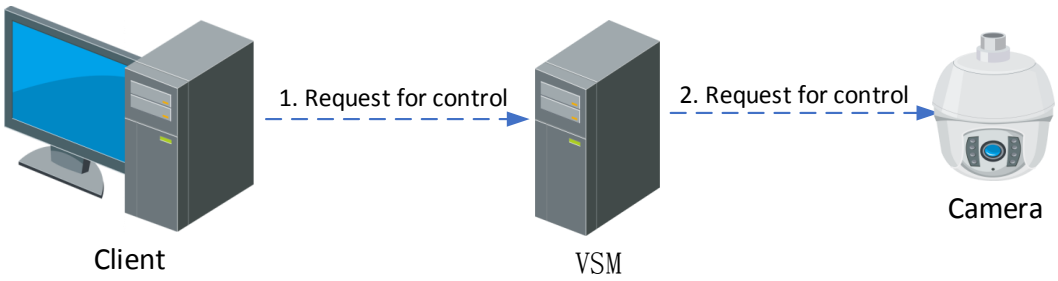
5.2.2 Live View via Streaming Server



In the following situations, the SMS (Streaming Server) needs to be deployed:
The client obtains streams from third-party devices.
Multiple clients request the same stream from the same device. To reduce the bandwidth for obtaining the stream, the stream is forwarded via SMS to solve this problem.
The signaling process is as follows:

1. The client sends a request to the SMS for obtaining the stream.
2. The SMS forwards the request to the device for obtaining the stream.
3. The device sends back the corresponding stream to the SMS.
4. The SMS forwards the obtained stream to the client.

5.2.3 PTZ Control



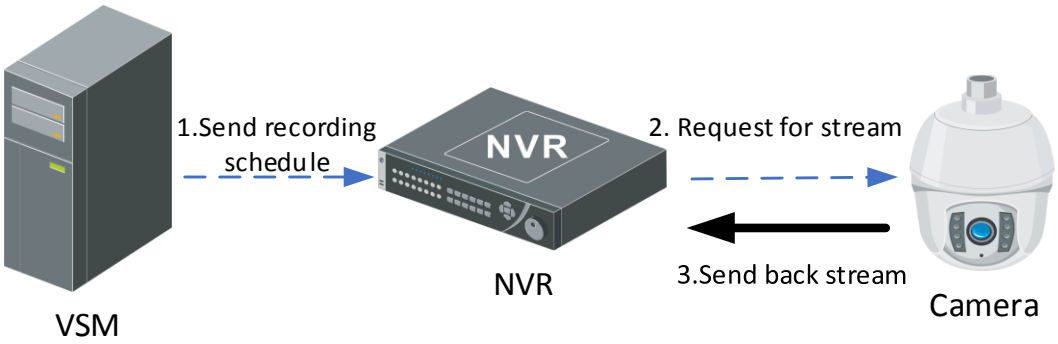
HikCentral Professional controls the PTZ camera via the SYS server.
The signaling process is as follows:

1. The client sends a request to the SYS server to control the PTZ camera.
2. The SYS server forwards the request to the corresponding device for PTZ control.

5.3 Video Storage and Playback

Device storage and playback includes: video stream storage, video file retrieval and playback.

5.3.1 Video Storage in NVR/DVR



As shown in the figure above, the signaling process is as follows:

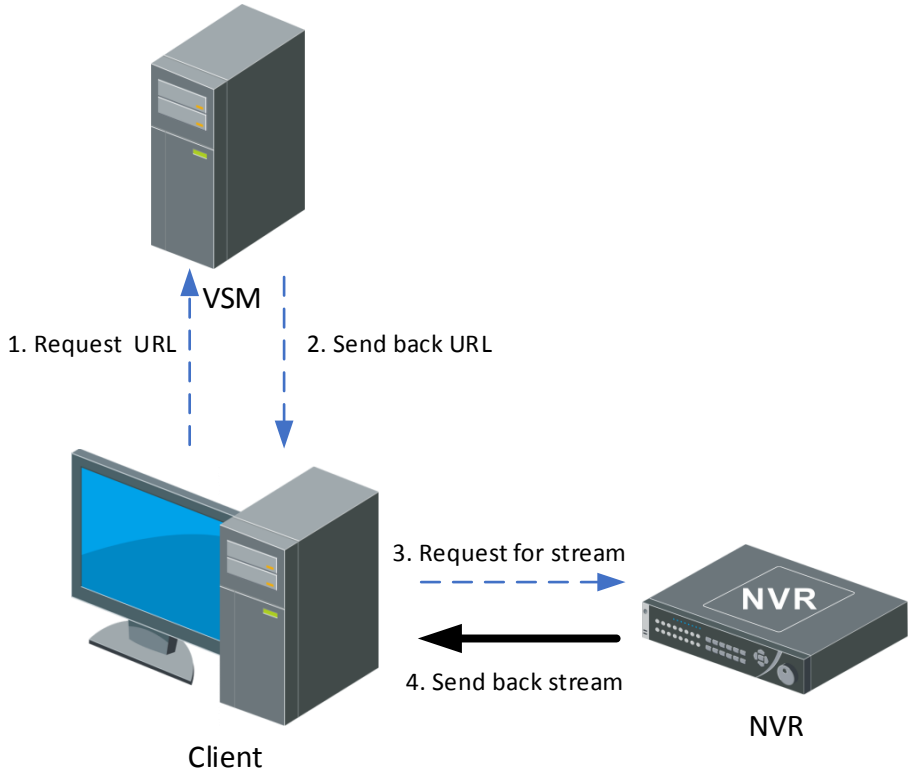
1. The SYS server sends the recording schedule (event-based recording schedule and time-based recording schedule) to the NVR.
2. When the recording schedule condition is met (within the time segment or an event is triggered), the NVR sends a request to the camera for obtaining the stream.
3. he camera sends back the corresponding stream to the NVR.

Note: When manual recording is performed on the Control Client, the preceding steps are triggered manually, but not triggered by recording schedule.

5.3.2 Playback of Video in NVR/DVR

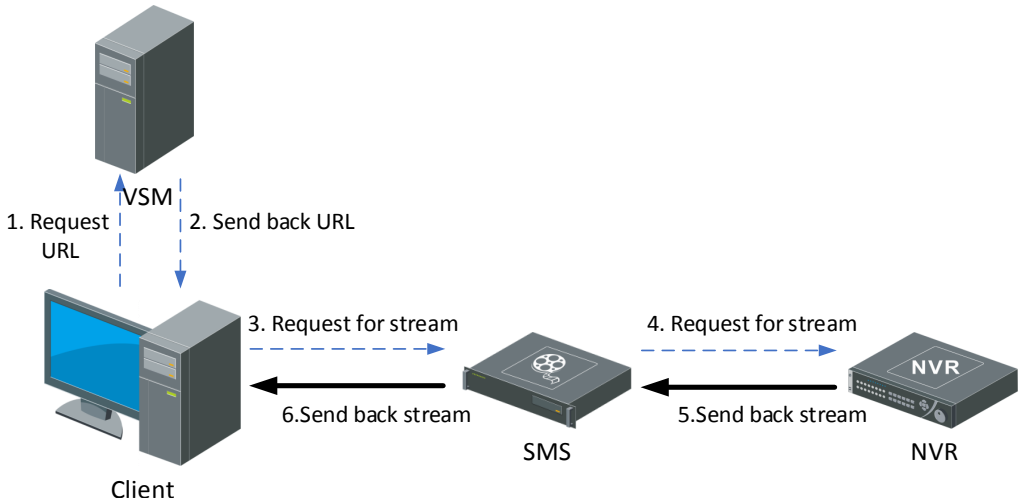
There are two modes for playing back video in NVR/DVR: The client obtains the stream directly from the NVR/DVR, and the client obtains the stream from the NVR/DVR via SMS. The signaling processes are as follows:

Playback of Video in Directly Connected Device



1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to the NVR for obtaining the stream.
4. The NVR sends back the corresponding stream to the client according to the request.

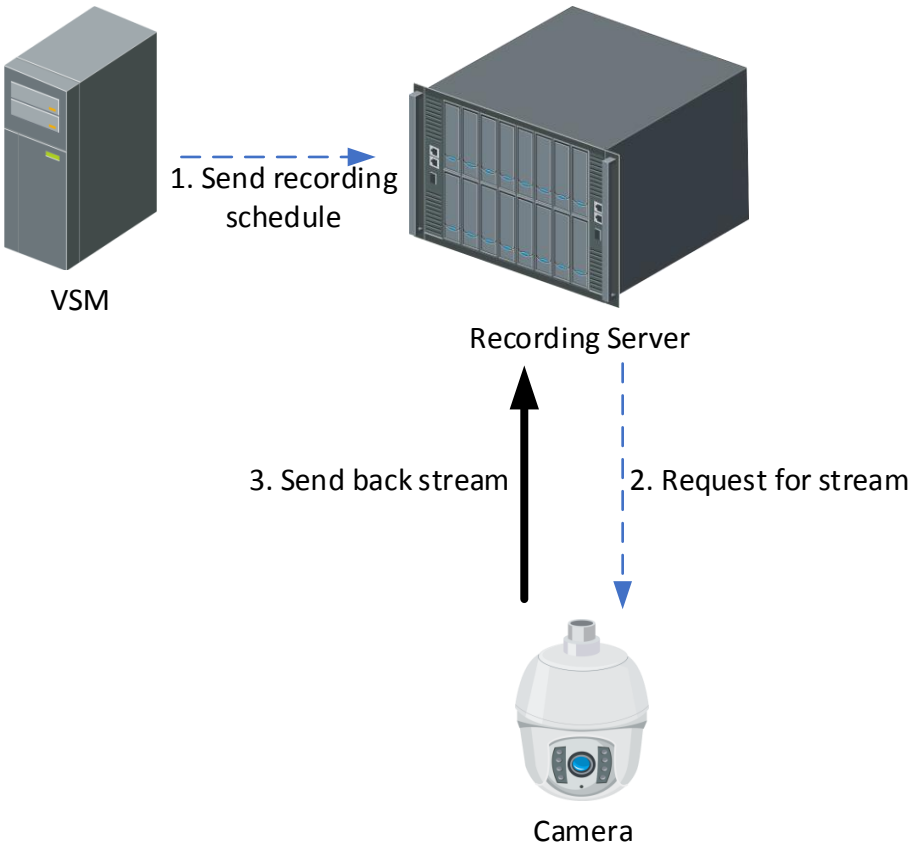
Playback via Streaming Server



1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to the SMS (Streaming Server) for obtaining the stream.

4. The SMS forwards the request to the NVR for obtaining the stream.
5. The NVR sends back the corresponding stream to the SMS according to the request.
6. The SMS forwards the corresponding stream to the client.

5.3.3 Video Storage in Recording Server



Recording Servers include: Hybrid SAN, cloud storage, and pStor. If the video is stored on the recording server, the signaling process is as follows:

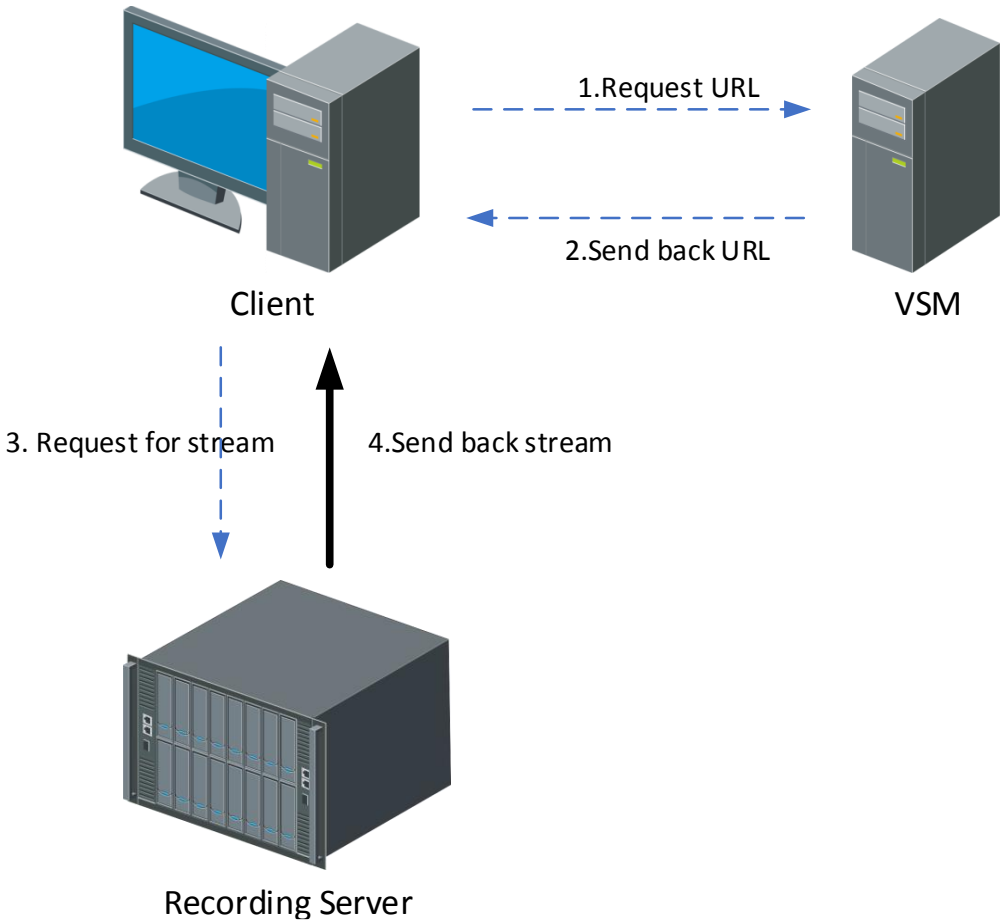
1. The SYS server sends the recording schedule (time-based recording schedule and event-based recording schedule) to the recording server.
2. The recording server sends a request to the camera for obtaining the stream according to the recording schedule.
3. The camera sends back the corresponding stream to the recording server according to the request.

Note: When manual recording is performed on the Control Client, the preceding steps are triggered manually, but not triggered by recording schedule.

5.3.4 Playback of Video in Recording Sever

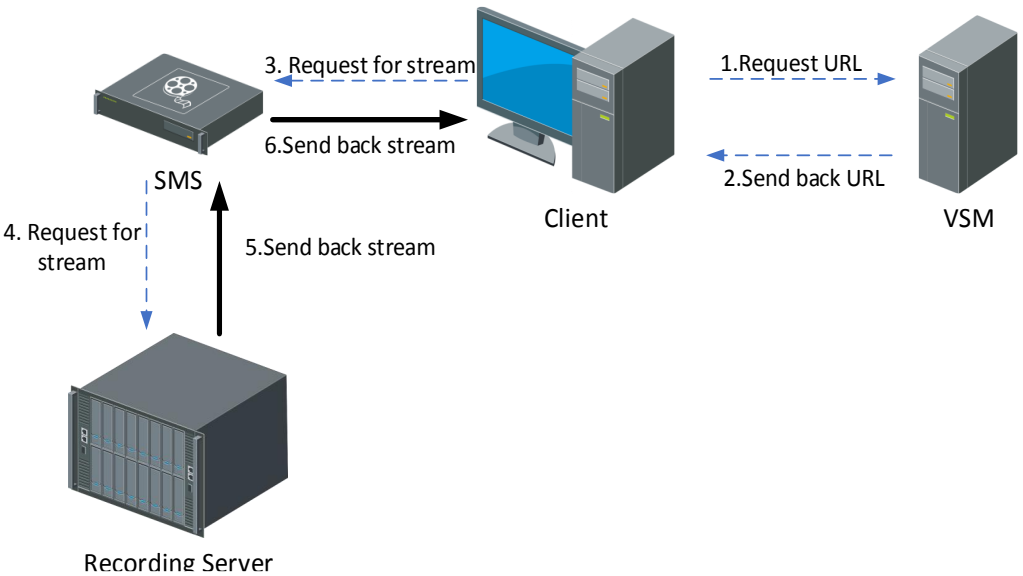
There are two modes for playing back video from recording server: The client obtains the stream directly from the recording server, and the client obtains the stream from the recording server via SMS. The signaling processes are as follows:

Playback of Video in Directly Connected Recording Server



1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to the recording server for obtaining the stream.
4. The recording server sends back the corresponding stream to the client according to the request.

Playback via Streaming Server

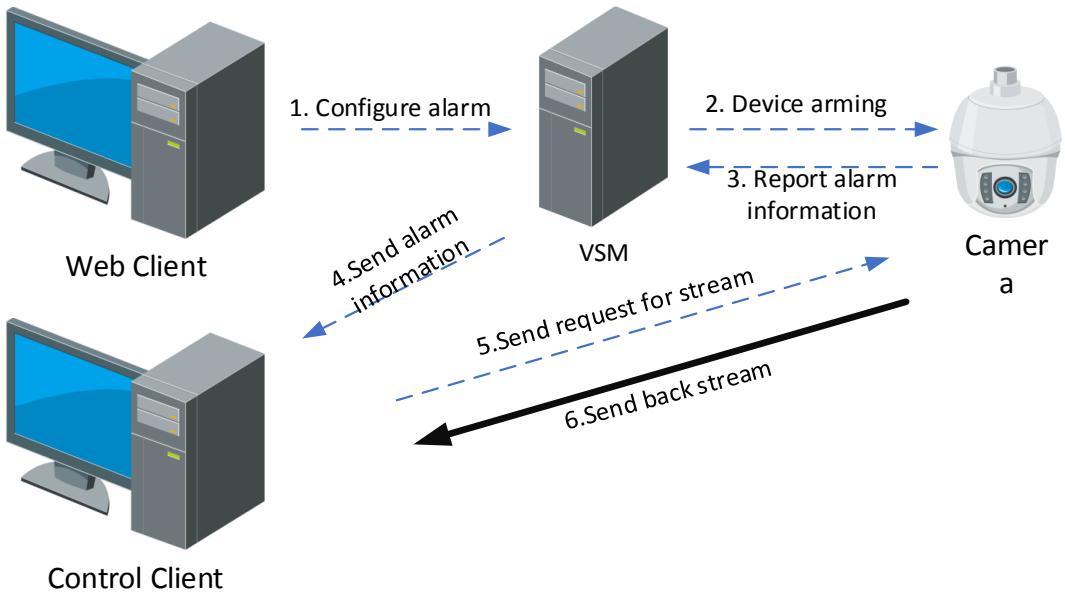


1. The client sends a request to the SYS server for obtaining the stream URL.
2. The SYS server sends back the stream URL to the client.
3. The client sends a request to SMS for obtaining the stream.
4. The SMS forwards the request to the recording server for obtaining the stream.
5. The recording server sends back the corresponding stream to the SMS according to request.
6. The SMS forwards the corresponding stream to the client.

5.4 Alarm

When an alarm is triggered, there are two modes for the Control Client to obtain the alarm related stream from the device: Obtain the stream via directly connected device and obtain the stream via SMS. The signaling processes are as follows:

5.4.1 Obtain Alarm Related Stream Directly



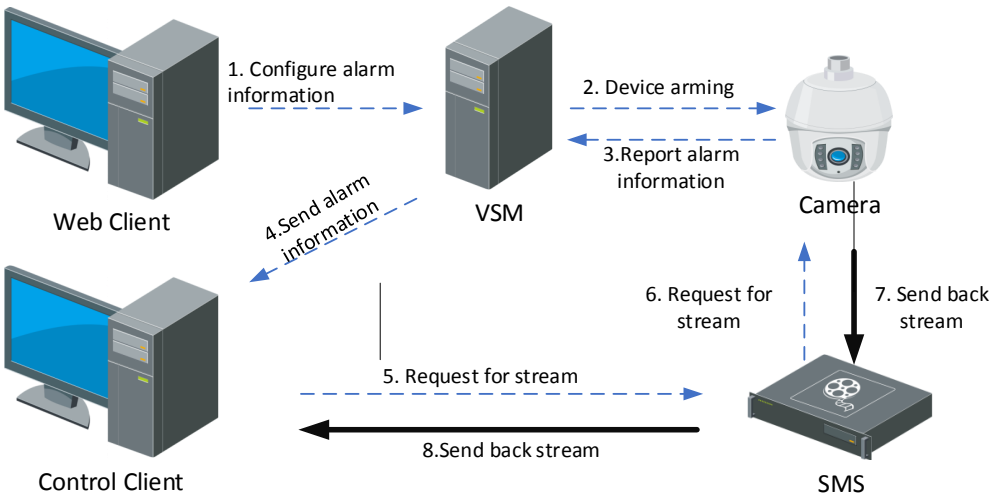
The process of alarm configuration is as follows:

1. Configure alarm via the Web Client, and the alarm configuration is sent to the SYS server.
2. The device is armed by the SYS server according the arming schedule.

The process of reporting an alarm is as follows:

1. The device analyzes the obtained stream. If an alarm is triggered, the device reports the alarm to the SYS server.
2. The SYS server sends the alarm information to the Control Client.
3. If the linkage of live view for the alarm is configured, the Control Client sends a request to the device for obtaining the stream.
4. The device sends back the corresponding stream to the Control Client according to the request.

5.4.2 Obtain Alarm Related Stream via Streaming Server



The process of alarm configuration is as follows:

1. Configure the alarm via the Web Client, and the alarm configuration is sent to the SYS server.
2. The device is armed by the SYS server according the arming schedule.

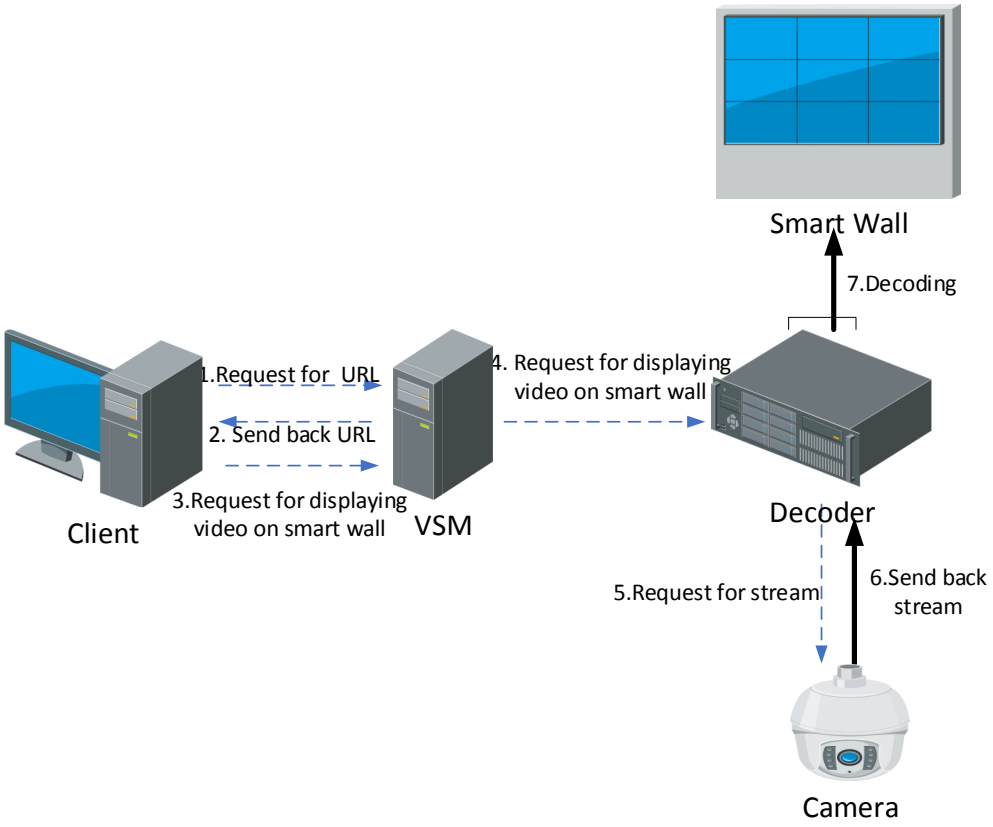
The process of reporting an alarm is as follows:

1. The device analyzes the obtained stream. If an alarm is triggered, the device reports an alarm to the SYS server.
2. The SYS server sends the alarm information to the Control Client.
3. If the linkage of live view or playback for the alarm is configured, the Control Client sends a request to the SMS for obtaining the stream.
4. The SMS forwards the request to the camera for obtaining the stream.
5. The camera sends back the corresponding stream to the SMS according to the request.
6. The SMS forwards the stream to the Control Client.

5.5 Smart Wall

5.5.1 Display Video on Smart Wall

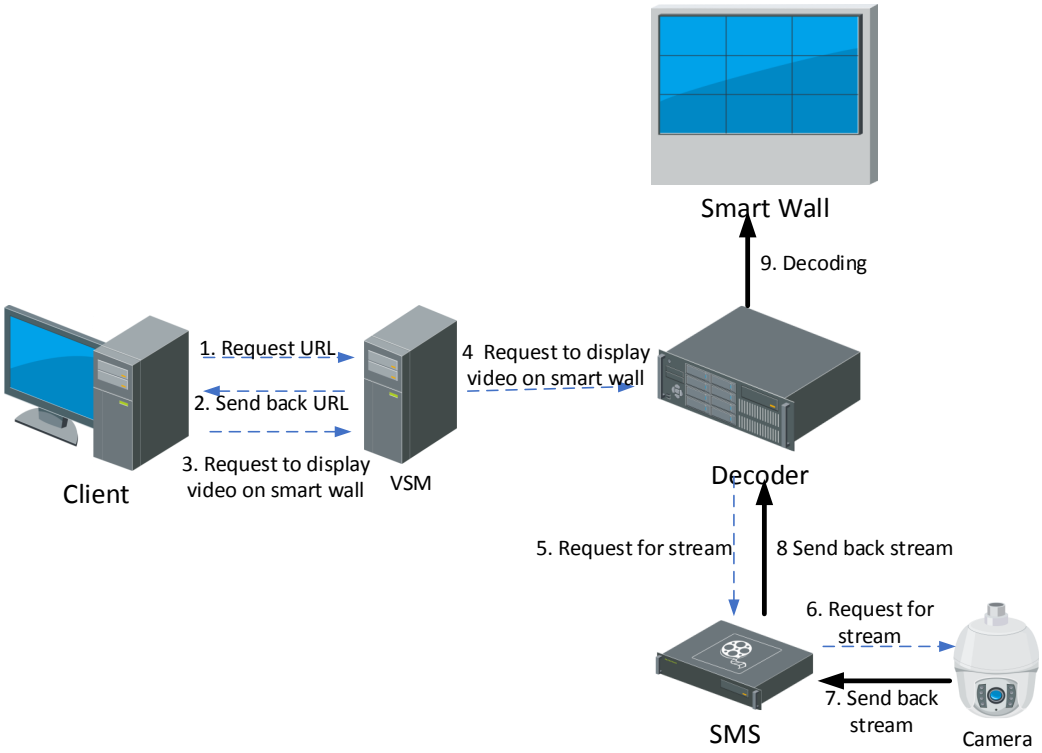
Display Video of Directly Connected Device on Smart Wall



When the decoder obtains the stream directly from the device, the signaling process is as follows:

1. The Smart Wall Client sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the Smart Wall Client.
3. The Smart Wall Client sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.
5. The decoder sends a request to the device for obtaining the stream.
6. The device sends back the corresponding stream to the decoder.
7. The decoder decodes the obtained stream and displays the video on the smart wall.

Display Video on Smart Wall via Streaming Server

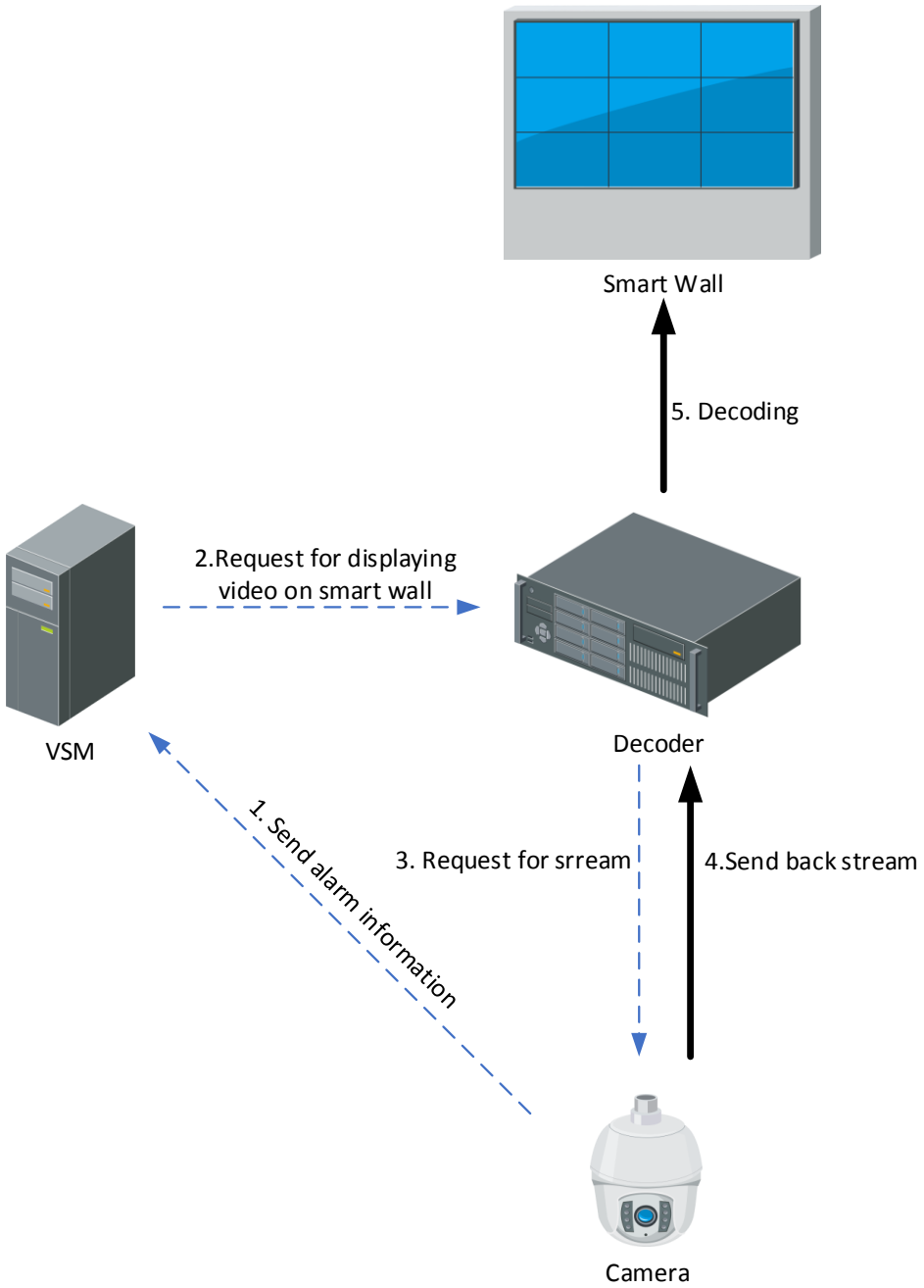


If the decoder obtains the stream via SMS, the signaling process is as follows:

1. The Smart Wall Client sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the Smart Wall Client.
3. The Smart Wall Client sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.
5. The decoder sends a request to the SMS (Streaming Server) for obtaining the stream.
6. The SMS forwards the request to the device for obtaining the stream.
7. The device sends back the corresponding stream to the SMS.
8. The SMS forwards the stream to the decoder.
9. The decoder decodes the obtained stream and displays the video on the smart wall.

5.5.2 Display Alarm Video on Smart Wall

Display Alarm Video of Directly Connected Device on Smart Wall



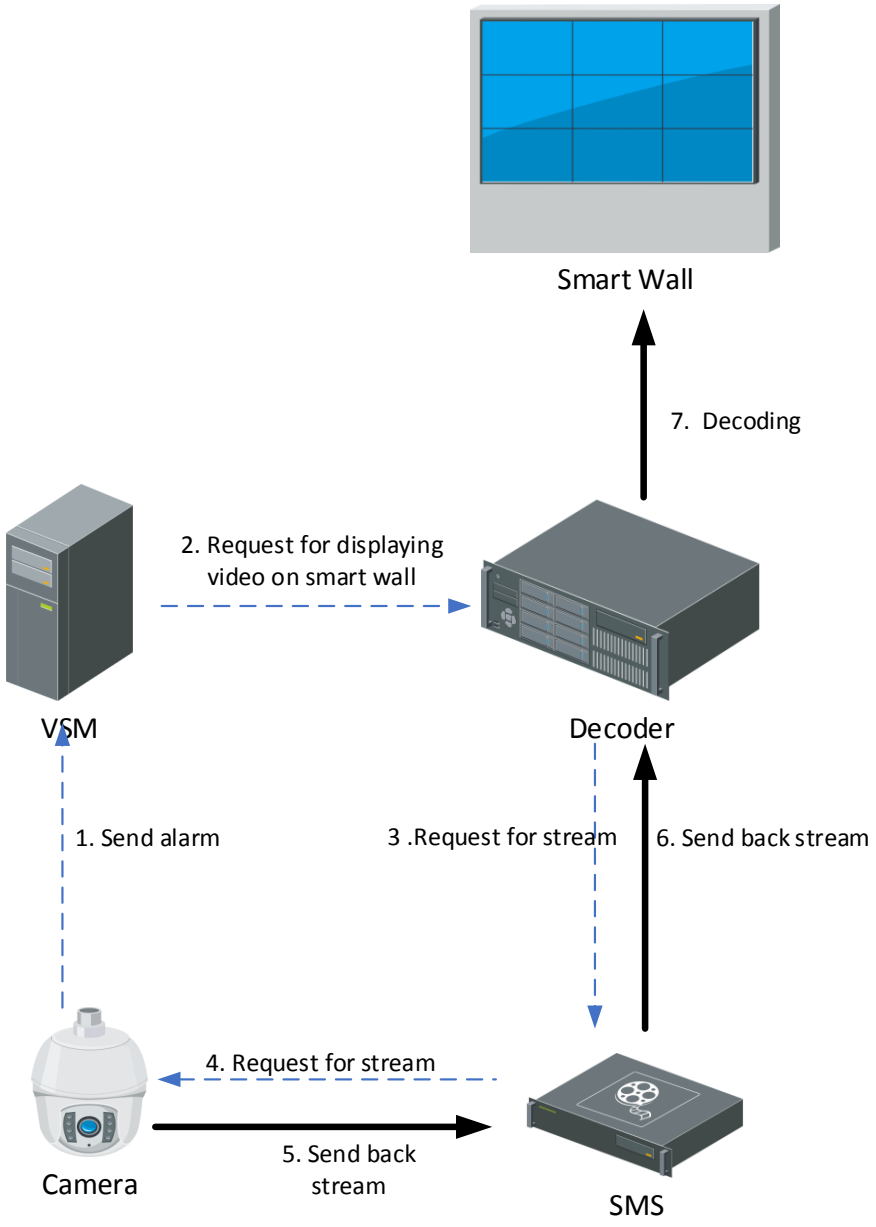
The process of displaying alarm video of directly connected device on smart wall is as follows:

1. The camera analyzes the obtained streams. If an alarm is triggered, the camera sends the alarm to the SYS server.
2. According to the alarm, the SYS server estimates whether the video of the camera need to be displayed on the smart wall. If yes, the SYS server sends a request to the

decoder to display video on smart wall.

3. The decoder sends a request to the corresponding camera for obtaining the alarm video stream.
4. The camera sends back the stream according to the corresponding request.
5. The decoder decodes the obtained stream and displays the video on the smart wall.

Display Alarm Video on Smart Wall via Streaming Server



The process of displaying alarm video of device on smart wall via SMS is as follows:

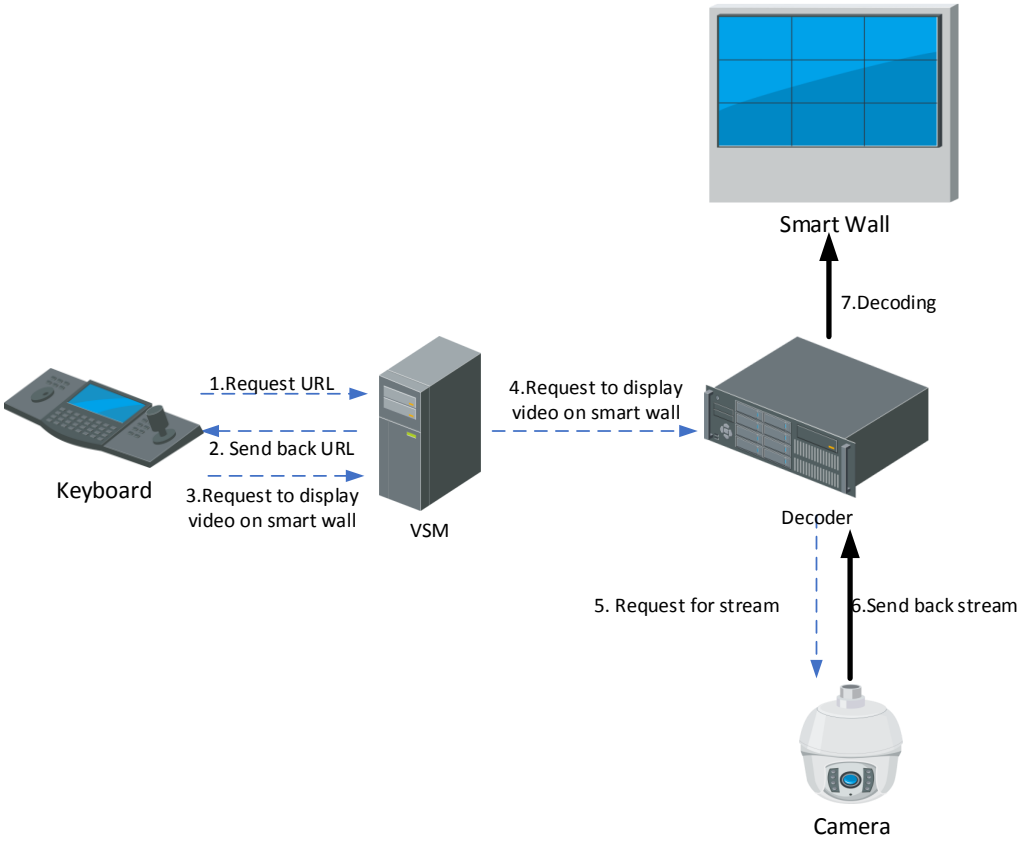
1. The camera analyzes the obtained streams. If an alarm is triggered, the camera sends the alarm to the SYS server.
2. According to the alarm, the SYS server estimates whether the video of the camera need to be displayed on the smart wall. If yes, the SYS server sends a request to the

decoder to display video on smart wall.

3. The decoder sends a request to the SMS (Streaming Server) for obtaining the stream.
4. The SMS forwards the request to the corresponding camera for obtaining the stream.
5. The camera sends back the stream to the SMS according to the corresponding request.
6. The SMS forwards the obtained streams to the decoder.
7. The decoder decodes the obtained stream and display the video on the smart wall.

5.5.3 Display Video Controlled by Keyboard on Smart Wall

Display Video of Directly Connected Device Controlled by Keyboard on Smart Wall

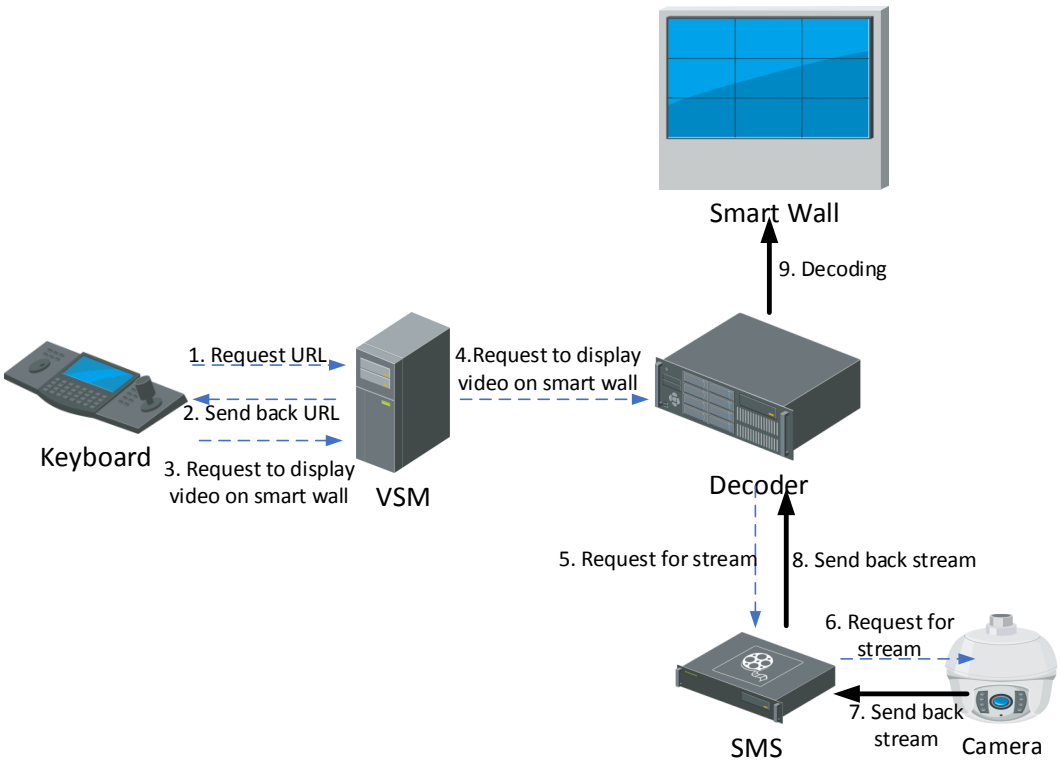


If the decoder obtains the stream directly from the device, the signaling process is as follows:

1. The keyboard sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the keyboard.
3. The keyboard sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.

5. The decoder sends a request to the device for obtaining the stream.
6. The device sends back the corresponding stream to the decoder.
7. The decoder decodes the obtained stream and displays the video on the smart wall.

Display Video Controlled by Keyboard on Smart Wall via Streaming Server

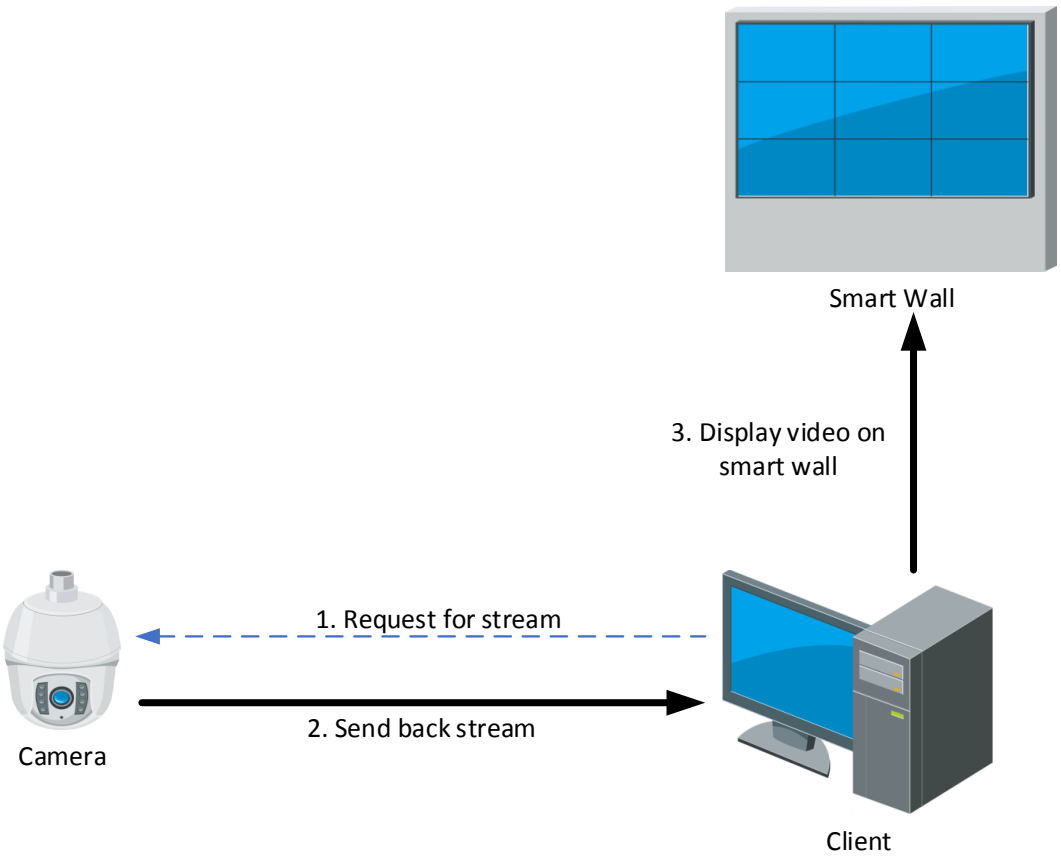


If the decoder obtains the stream via SMS, the signaling process is as follows:

1. The keyboard sends a request to the SYS server for obtaining the URL information (including the smart wall information and device information).
2. The SYS server sends back the URL information to the Smart Wall Client.
3. The keyboard sends a request to the SYS server to display the video on the smart wall.
4. The SYS server forwards the request to the decoder to display the video on the smart wall.
5. The decoder sends a request to the SMS (Streaming Server) for obtaining the stream.
6. The SMS forwards the request to the device for obtaining the stream.
7. The device sends back the corresponding stream to the SMS.
8. The SMS forwards the stream to the decoder.
9. The decoder decodes the obtained stream and displays the video on the smart wall.

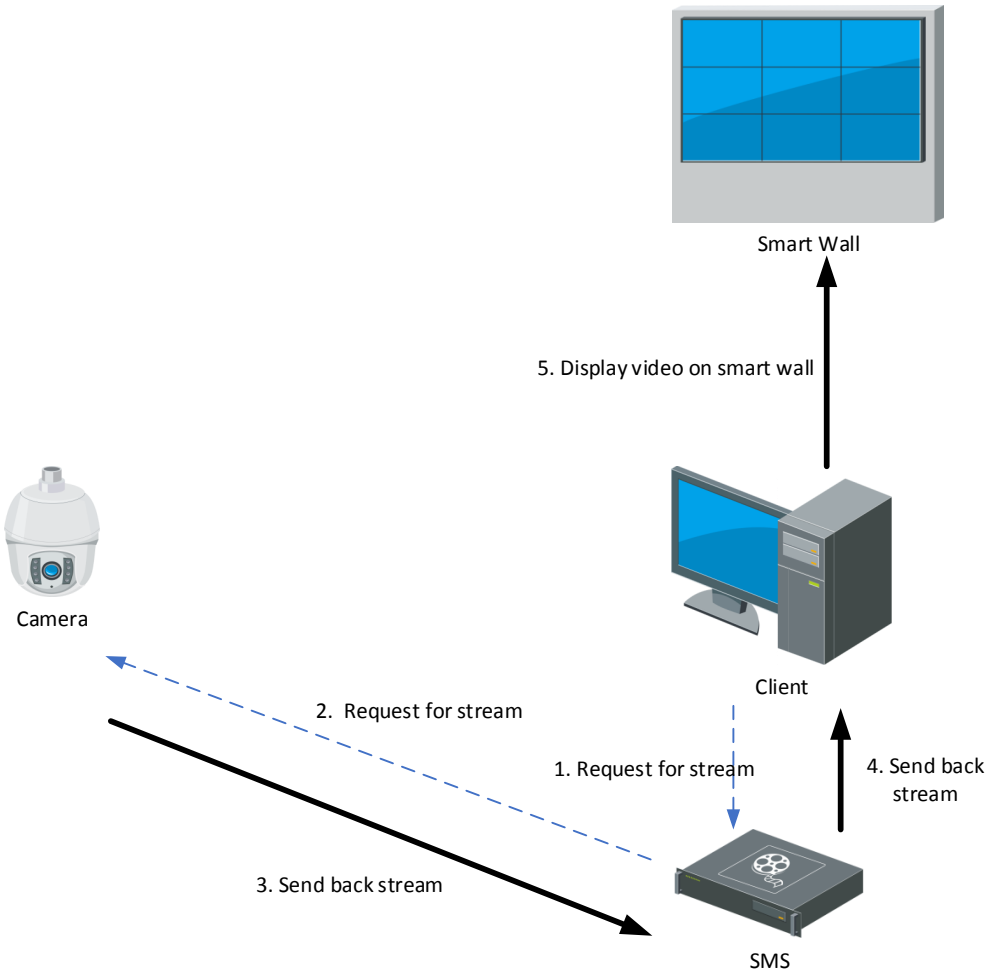
5.5.4 Display Video on Smart Wall (Graphic Card)

Display Video of Directly Connected Device on Smart Wall (Graphic Card)



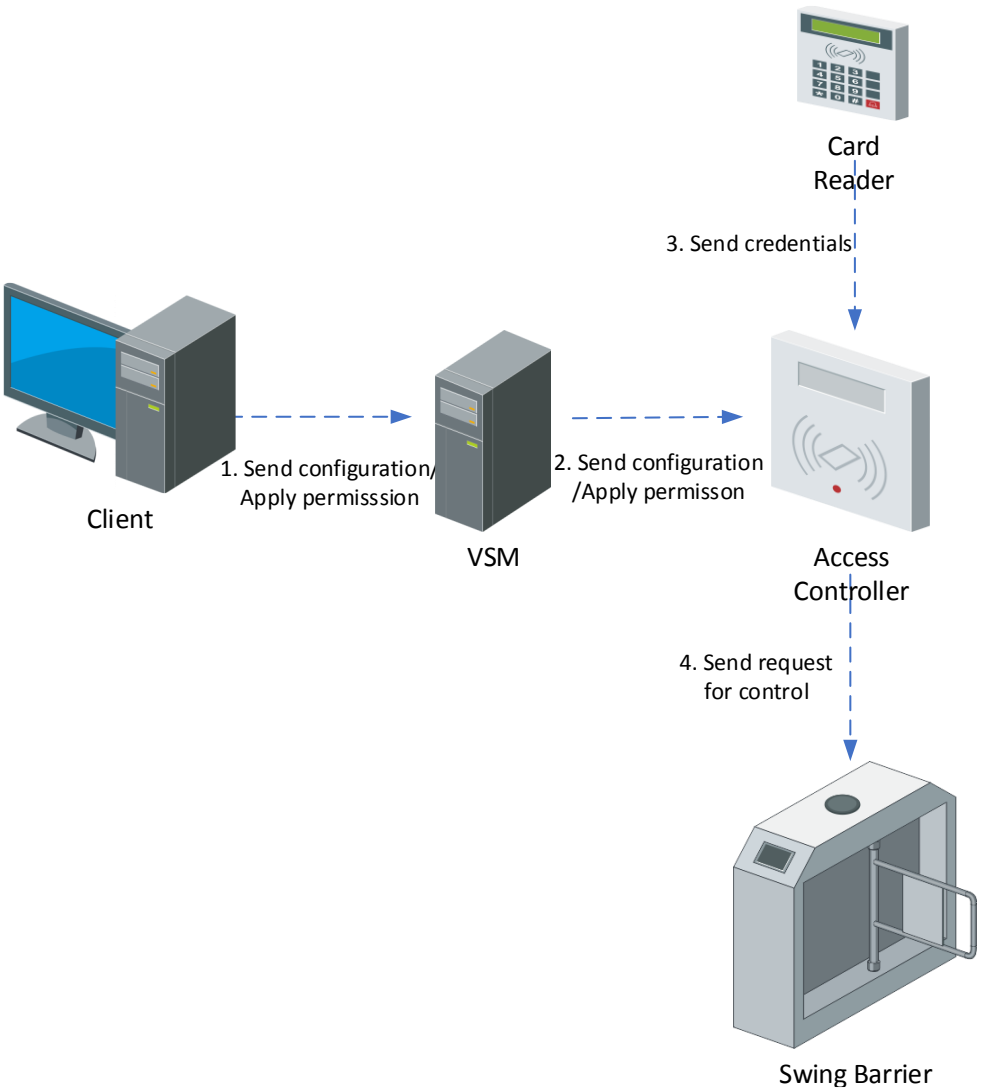
1. The client sends a request to the camera for obtaining the stream.
2. The camera sends back the corresponding stream to the client.
3. The client sends the stream to display on the Smart Wall (Graphic Card).

Display Video on Smart Wall (Graphic Card) via Smart Wall



1. The client sends a request to the SMS (Streaming Server) for obtaining the stream.
2. The SMS forwards the request to the camera for obtaining the stream.
3. The camera sends back the corresponding stream to the SMS.
4. The SMS forwards the obtained stream to the client.
5. The Client sends the stream to display on the Smart Wall (Graphic Card).

5.6 Access Control

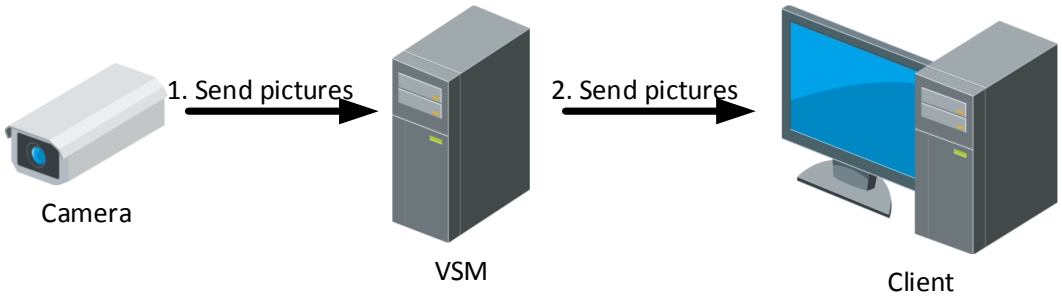


The signaling process of access control and management is as follows:

1. The Web Client sends an access control configuration command (including personnel permission, device configuration and event configuration) to the SYS server.
2. The SYS server sends the configuration command to the device.
3. The card reader obtains the corresponding instruction, and sends the credential information to the access controller.
4. The access controller sends the control request to the swing barrier according to the obtained instruction to control the switch status of the swing barrier.

5.7 ANPR

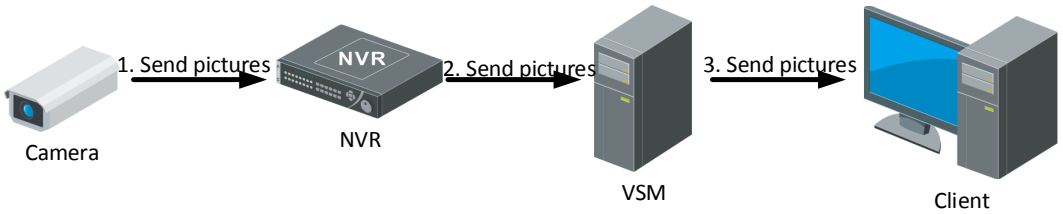
5.7.1 View Pictures Captured by ANPR Camera



According to the settings of the platform, the pictures can be stored in the SYS server locally or in the picture storage server.

If the picture is stored in the SYS server, the signaling process is as follows:

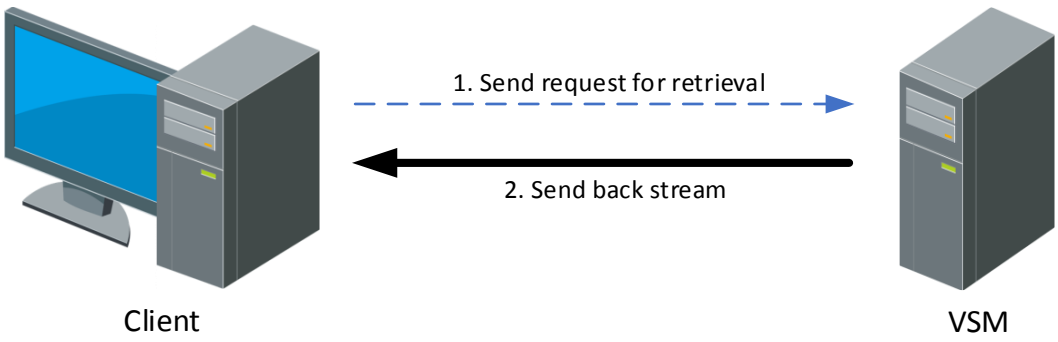
1. The ANPR camera captures the picture, and uploads the picture to the SYS server.
2. The SYS server sends the obtained picture to the Control Client for display.



If the picture is stored in the picture storage server (e.g. NVR), the signaling process is as follows:

1. The ANPR camera captures the picture, and uploads the picture to the NVR.
2. The NVR sends the obtained picture to the SYS server.
3. The SYS server sends the obtained picture to the Control Client for display.

5.7.2 Retrieval Pictures Stored in SYS Server

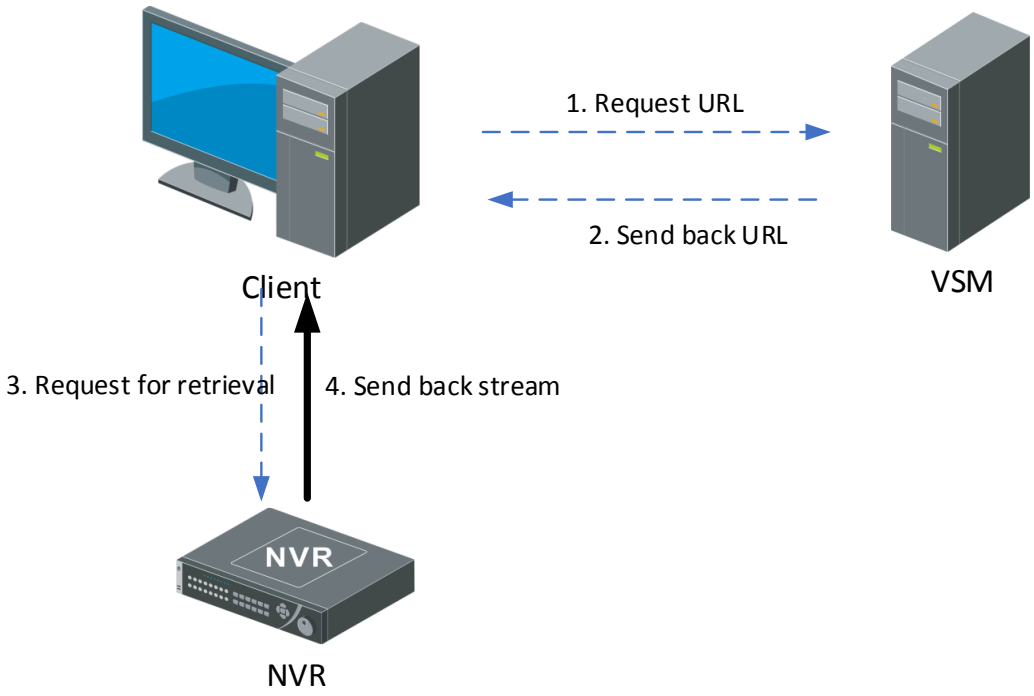


If the ANPR pictures is stored in the SYS server, the signaling process of ANPR picture retrieval and display is as follows:

1. The Control Client sends a picture retrieval instruction to the SYS server.
2. The SYS server search the required picture(s) and sends back the result to the Control Client.

5.7.3 Retrieval Pictures Stored in NVR

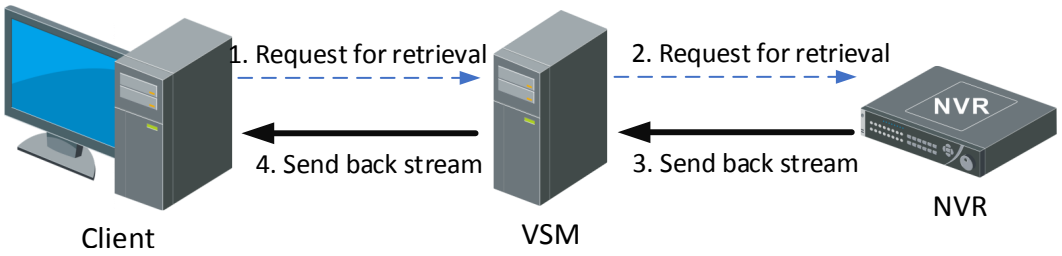
Client and NVR are in the Same LAN



If the video is stored in the NVR that is in the same network with the Control Client, the process of obtaining the pictures captured by ANPR cameras is as follows:

1. The Control Client sends a request to the SYS server for obtaining the NVR URL information.
2. The SYS sends the corresponding URL information to the Control Client.
3. According to the obtained URL information, the Control Client sends an instruction to the NVR for obtaining the pictures captured by ANPR camera.
4. The NVR sends back the corresponding pictures to the Control Client according to the obtained instruction.

Client and NVR are in Different LANs



If the video is stored in the NVR that is not in the same network with the Control Client, the process of obtaining the pictures captured by ANPR cameras is as follows:

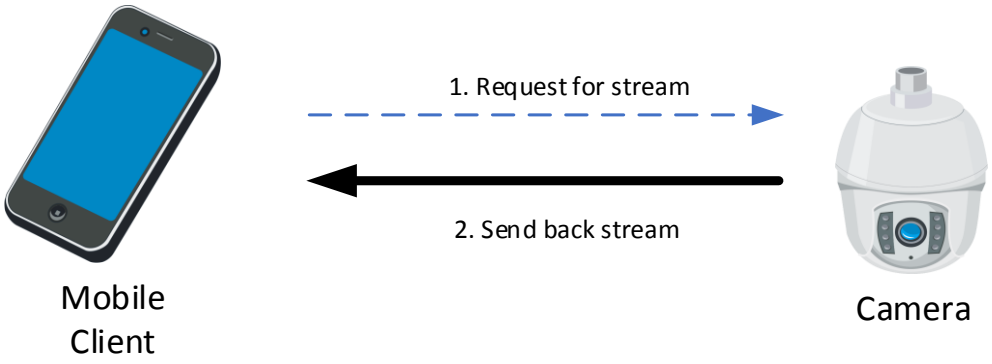
1. The Control Client sends a request to the SYS server for picture retrieval.
2. The SYS server sends the retrieval request to the NVR.
3. The NVR sends back the picture captured by ANPR camera to SYS server according to the request.
4. The SYS server forwards the obtained picture to the Control Client according to the actual instruction.

5.8 Mobile Client

5.8.1 Live view

The Mobile Client, like other clients, belongs to the HikCentral client. Therefore, the process of obtaining streams is the same as that of other clients.

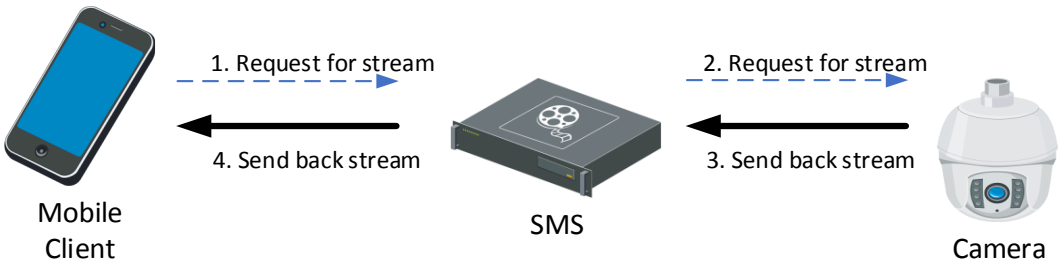
Live View for Directly Connected Device



If the Mobile Client and device are directly connected, the process of live view on the Mobile Client is as follows:

1. The Mobile Client sends a request to the device for obtaining the stream.
2. The device sends back the corresponding stream to the Mobile Client.

Live View via Streaming Server

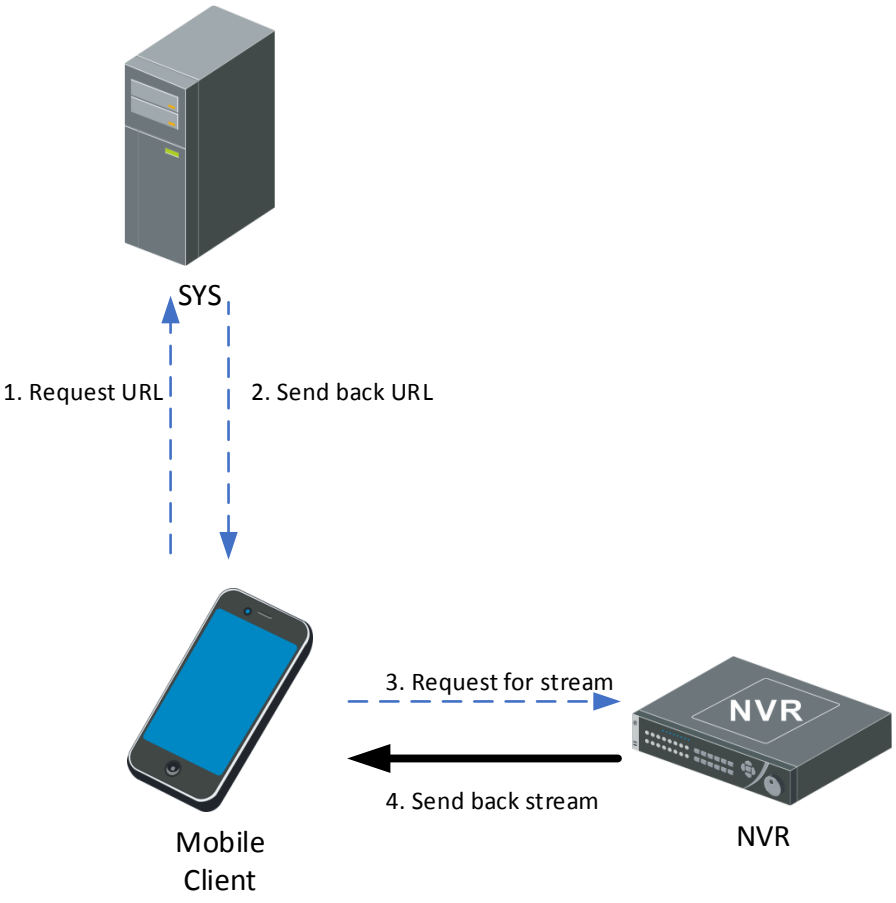


If the Mobile Client obtains the stream from the device via SMS (Streaming Server), the process is as follows:

1. The Mobile Client sends a request to the SMS for obtaining the stream.
2. The SMS forwards the request to the device for obtaining the stream.
3. The device sends back the corresponding stream to the SMS according to the request.
4. The SMS sends back the stream to the Mobile Client.

5.8.2 Playback

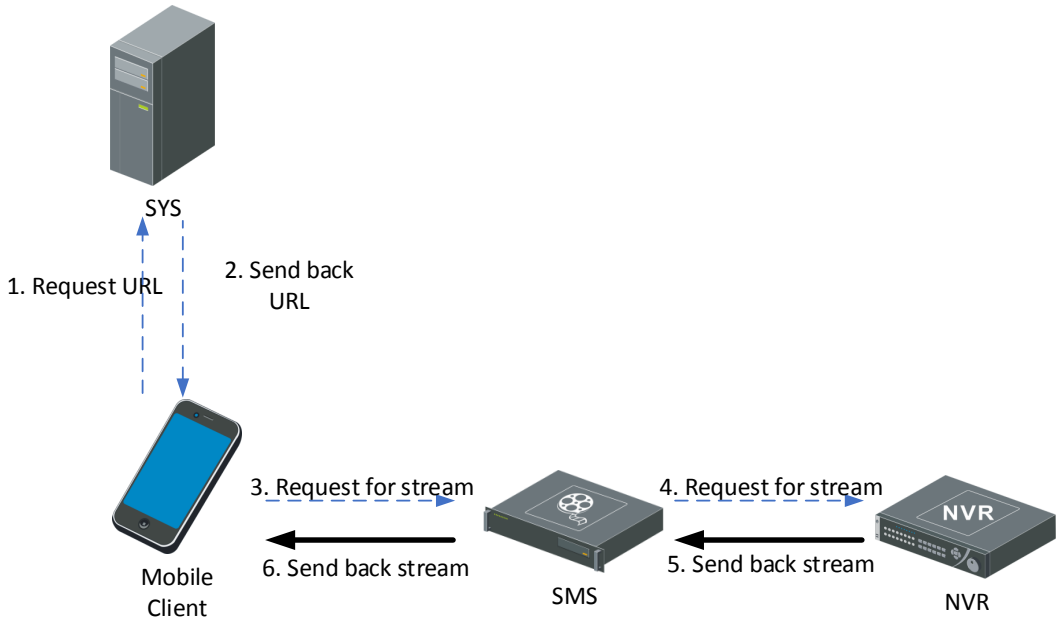
Playback of Video in Directly Connected Device



If the video file is stored in the directly device, the process is as follows:

1. The Mobile Client sends a request to the SYS server for obtaining the stream URL.
2. The SYS sends the stream URL information to the Mobile Client.
3. The Mobile Client sends a request to the directly connected storage device for obtaining the stream.
4. The storage device sends back the corresponding stream of playback to the Mobile Client.

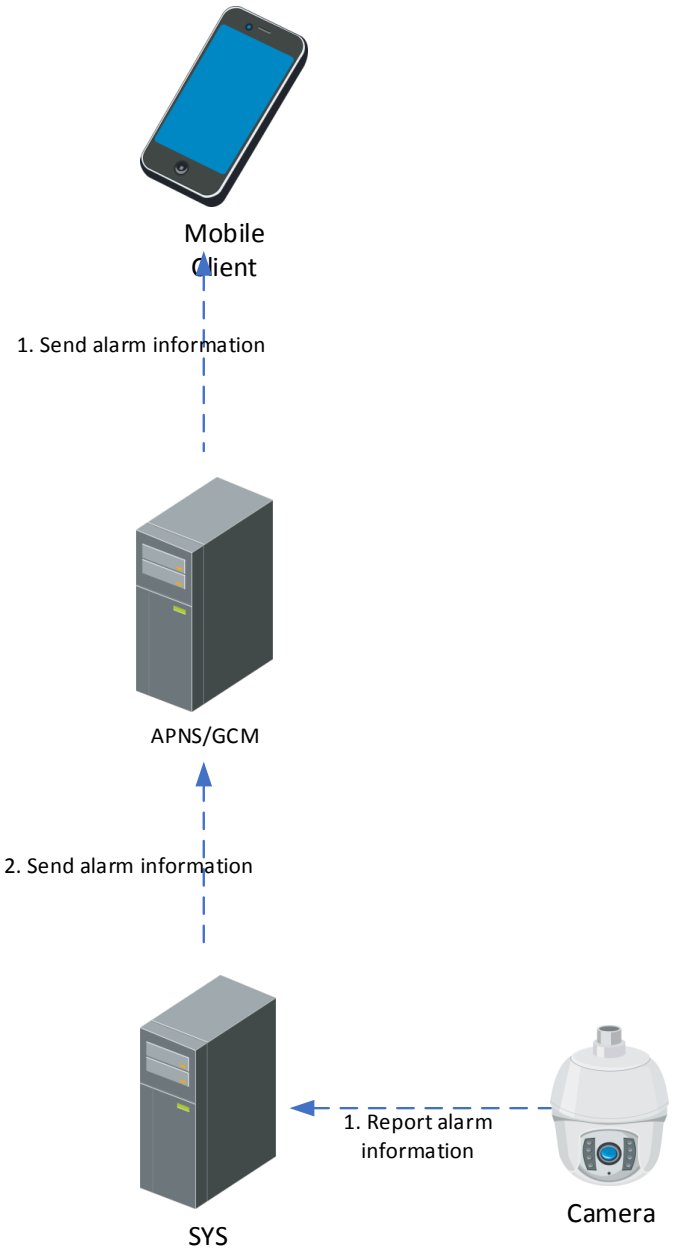
Playback via Streaming Server



If the Mobile Client obtains stream via SMS, the process is as follows:

1. The Mobile Client sends a request to the SYS server for obtaining the stream URL.
2. The SYS sends the stream URL information to the Mobile Client.
3. The Mobile Client sends a request to the SMS for obtaining the stream.
4. The SMS forwards the request to the NVR for obtaining the stream.
5. The NVR sends back the stream of playback to the SMS.
6. The SMS forwards the obtained stream to the Mobile Client.

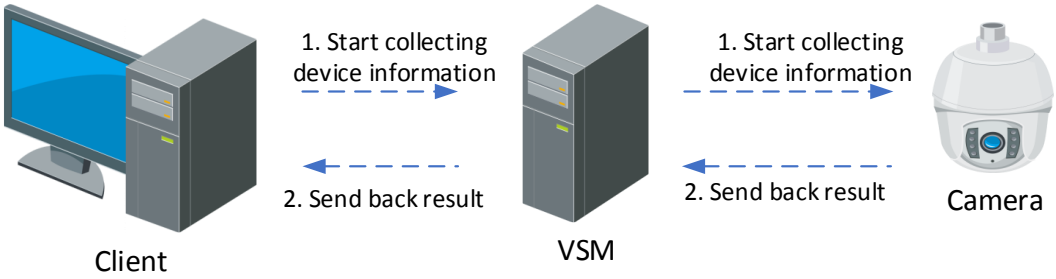
5.8.3 Alarm



Similar to the other clients, the process of receiving alarm video on Mobile Client is as follows:

1. The device reports an alarm to the SYS server.
2. The SYS server sends the obtained alarm information to the APNS/GCM server.
3. The APNS/GCM server sends the corresponding alarm information to the Mobile Client.

5.9 Status Monitoring



The device status inspection consists of the following two situations: interaction between the client and the SYS server, and between the device and the SYS server.

The platform initiates inspection information every 3 minutes.

5.9.1 Interaction Between SYS Server and Device

1. The SYS server sends an inspection command to the device.
2. The device sends back the status of the device to the SYS server.

5.9.2 Interaction Between Client and SYS Server

1. The Control Client sends an inspection command to the SYS server.
2. The SYS server sends the current status of the device to the Control Client.

Chapter 6 System Security

6.1 Security Design Overview

The HikCentral Professional system consists of the server, client, service component, and platform SDK. The interaction between server and client, server and service component, server and platform SDK support HTTP and HTTPS.
To ensure the security of data storage, the sensitive data stored in the server is all encrypted. Sensitive information that does not need to be decrypted is all encrypted by irreversible encryption scheme. Sensitive information that needs to be decrypted is all encrypted by encryption scheme that can be decrypted.
The HikCentral Professional adopts the following encryption algorithms: RSA, AES, SHA, and MD5. All the encryption algorithms come from the standard open-source library OpenSSL-1.0.2K. The OpenSSL version will be updated according to the policies of Hikvision security lab.

6.2 System Security Solution

6.2.1 Access Protocol

By default, the HTTP protocol is used for web access. By optional, you can enable the HTTPS protocol.
HTTPS: Users can import the HTTPS certificate to improve the security of data transmission.
HTTP: In HTTP mode, provide an independent security solution to prevent replay attacks.

6.2.2 Streaming Server Authentication

To ensure the overall security of the system, when the clients obtain live view or playback streams from devices via SMS (Streaming Server), the device must be authenticated by the SMS first.

6.2.3 Login Authentication

The system authenticates users based on user name and password. The password strength and expiration time can be configured separately on the system. If the administrator forgets the login password, the system allows you to reset the password by license. To ensure the system security, the input information is hidden during password input.
During the transmission, the password is encrypted by RSA algorithm in HTTP mode, and

the HTTPS internal encryption mechanism is used in HTTPS mode. In system login authentication, the verification code + user lock + IP address lock are used to prevent brute force cracking from malicious user, to improve the system security level.
Man-Machine Authentication: If an incorrect password is entered during the login, you need to manually enter the verification code.
User Lock: This parameter is mandatory enabled. If the password is entered incorrectly for five consecutive times, the user cannot log in to the system within 30 minutes.
IP Address Lock: This parameter is enabled by default. You can manually configure the number of error times and lock period. If the number of incorrect login attempts for the same IP address exceeds the specified value, the IP address cannot be used to log in to the system within the specified lock period.

6.2.4 Platform Access

After the client successfully logs in to the system, the server randomly generates a session for each client. The session can effectively reduce the cracking risks caused by the frequent user name and password interaction verification during the business. Each session has a fixed lifetime. When a session carried by a client expires, the user needs to log in to the system again.
In HTTP mode, to ensure that the system is not attacked by replay attacks, each session must carry an anti-replay token, which is unique in each session. The token is invalid immediately after each request to prevent repeated token attacks. The token is encrypted using AES.

6.2.5 Sensitive Information Processing

For sensitive information such as user name and password that are daily used, HikCentral Professional provides security solutions based on the actual service scenarios.
All sensitive information is encrypted during the interaction between the client and server. In HTTP mode, the AES encryption is used to generate a random AES key for each login, to ensure that data is not easily stolen. In HTTPS mode, SSL certificate encryption is used.
For the sensitive information storage, HikCentral Professional provides different storage scheme according to the different business requirements. To prevent the leakage of the encryption key of a platform from affecting other platforms, HikCentral Professional adopts the dynamic AES encryption scheme for sensitive information (such as the database access password and device access password) that needs to be locally stored. To prevent system user password leakage caused by system data file leakage, the system user password is encrypted by SHA algorithm and stored in cipher text.

6.3 Security Audit Server

Supports access of Hikvision Security Audit Server, which is used to monitor the logs of the

managed devices in the system. You can set event and alarm rules for the security audit server via the Web Client. When the logs of the managed devices are regarded as abnormal, an event or alarm will be triggered and you can receive the alarm via the Control Client. In this way, the system can monitor the running status of the managed devices by the security audit server, reaching the system security requirements.

Chapter 7 System Requirement

7.1 Software Running Environment

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 (32-bit) Chrome 61 and above (32-bit) Firefox 57 and above (32-bit) 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.*

7.2 Hardware Recommended Configurations

7.2.1 SYS Server

CPU	Intel® Xeon® E3-1220 V5 @ 3.00 GHz 3.00 GHz
Memory	16 GB
Network Controller	GbE Network Interface Card
HDD for Operating System	SATA-II 7200 RPM Enterprise Class HDD
HDD for Picture Storage	Surveillance-class HDD or high performance network HDD. It should support 20 MB/s writing and 20 MB/s reading.
HDD for Installation	At least 650 GB

7.2.2 RSM Server

CPU	Intel® Xeon® E5-2620 V4 @ 2.40 GHz 2.40 GHz
Memory	16 GB
Network Controller	GbE Network Interface Card
HDD for Operating System	SATA-II 7200 RPM Enterprise Class HDD
HDD for Picture Storage	Surveillance-class HDD or high performance network HDD. It should support 20 MB/s writing and 20 MB/s reading.
HDD for Installation	At least 650 GB

7.2.3 Streaming Server

CPU	Intel® Xeon® E3-1220 V5 @ 3.00 GHz
Memory	16 GB
Network Controller	GbE Network Interface Card
HDD for Operating System	SATA-II 7200 RPM Enterprise Class Hard Drives
HDD for Installation	At least10 GB

7.2.4 PC Running Control Client

CPU	Intel® Core™ i7 Processor
Memory	16 GB
Network Controller	GbE Network Interface Card
Graphics Card	NVIDIA GeForce GTX 1070
HDD Type	SATA II Hard Drive or Better
HDD for Installation	At least 240 GB

Chapter 8 Open Platform

8.1 Access Solution of Third-Party Devices

8.1.1 Introduction

HikCentral Professional provides access capabilities based on standard ONVIF protocol for the third-party devices. The third-party devices can connect to the HikCentral Professional via ONVIF protocol to implement the functionalities of live view, playback, PTZ control, video search, alarm, and so on.

To connect the third-party devices with HikCentral Professional, there are mainly two methods. One method is that, the third-party devices firstly connect to the Hikvision NVR, and then connect to HikCentral Professional via the NVR. The other method is that, the third-party devices directly connect to HikCentral Professional by configuring pStor, Hybrid SVN, or cloud storage. In the above two method, the NVR, pStor, Hybrid SVN, or cloud storage are used to save the video files, and the HikCentral Professional is used to manage and play the videos.

8.1.2 Overall Design

The server of HikCentral Professional contains multiple components for the access of the third-party devices. You can log in to, manage, and operate the third-party devices on HikCentral Professional via these components.

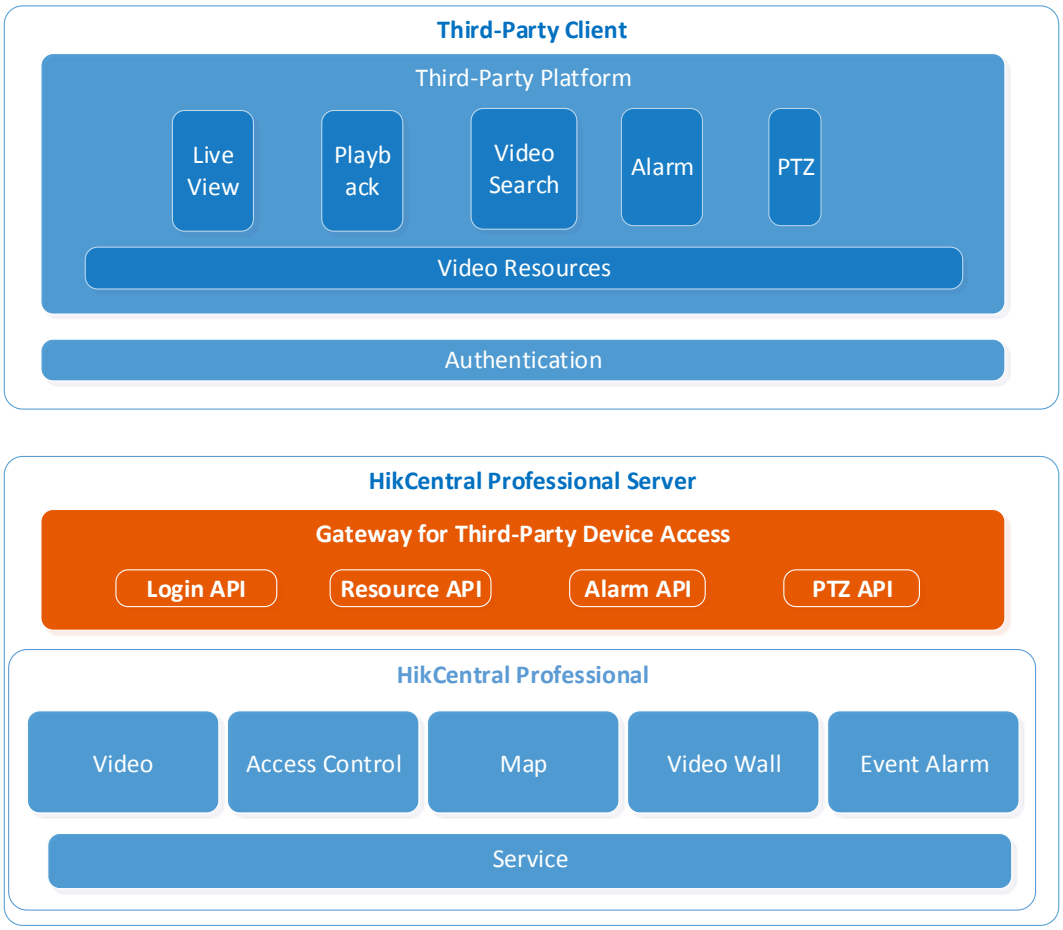


Figure 8-1 Overall Design Diagram

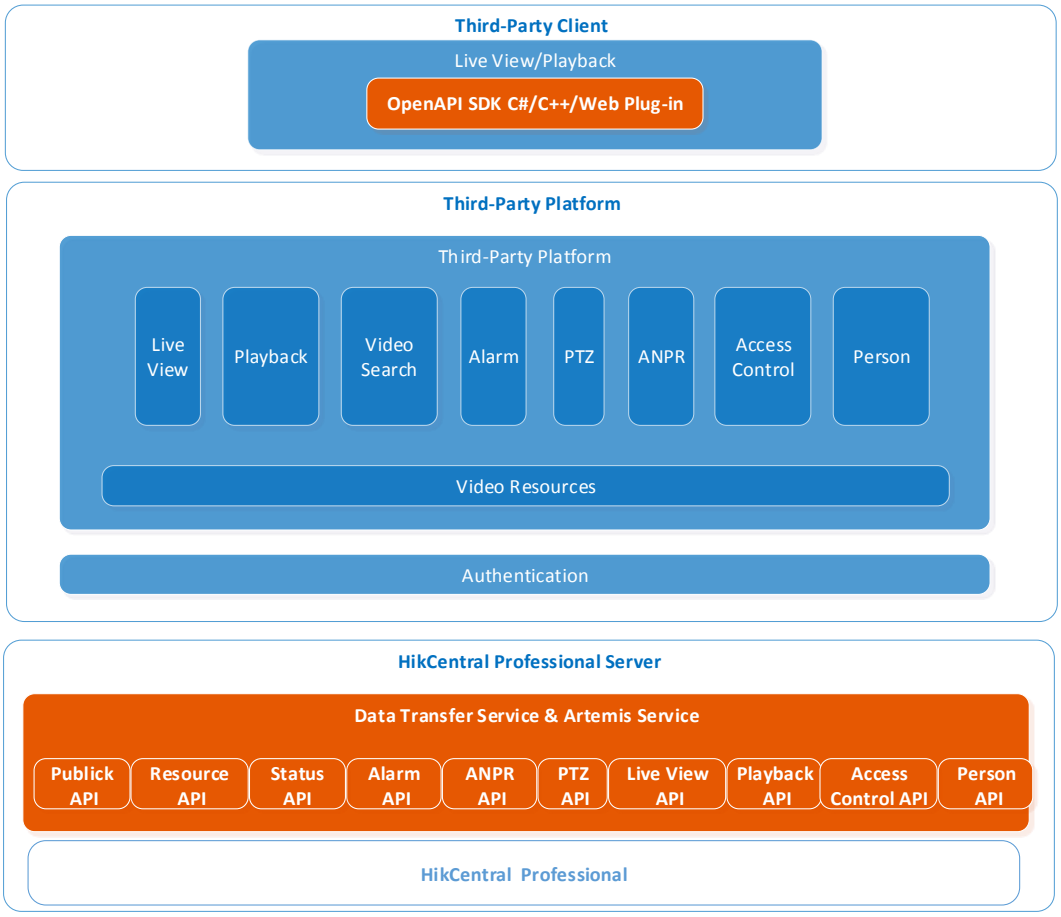
8.2 Integration Solution of Third-Party Platform

8.2.1 Introduction

HikCentral Professional provides OpenAPI for the connection between third-party platform and HikCentral Professional. The third-party platform can implement the core functionalities of HikCentral Professional via OpenAPI, such as video, alarm, resources, access control, and so on.

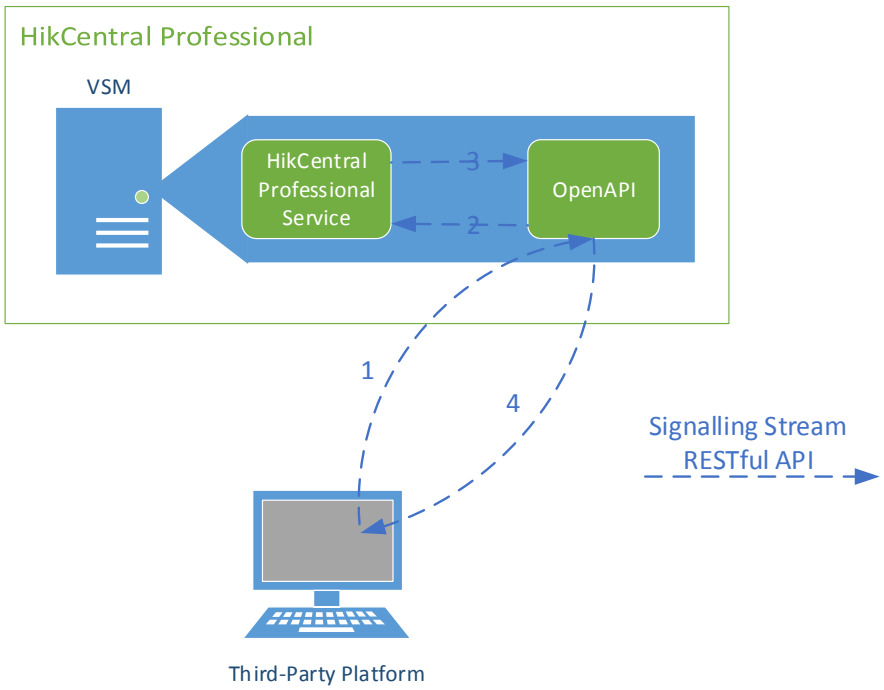
8.2.2 Overall Design

OpenAPI consists of Data Transfer Service, Artemis Gateway, and Video SDK. The Data Transfer Service converts the protocols between servers of HikCentral Professional and third-party platform. The Artemis Gateway provides the API protocol management, third-party integration management, and authentication. The Video SDK provides the capabilities of live view, playback, two-way audio, and so on, which helps the third-party client to integrate the video related functions quickly.

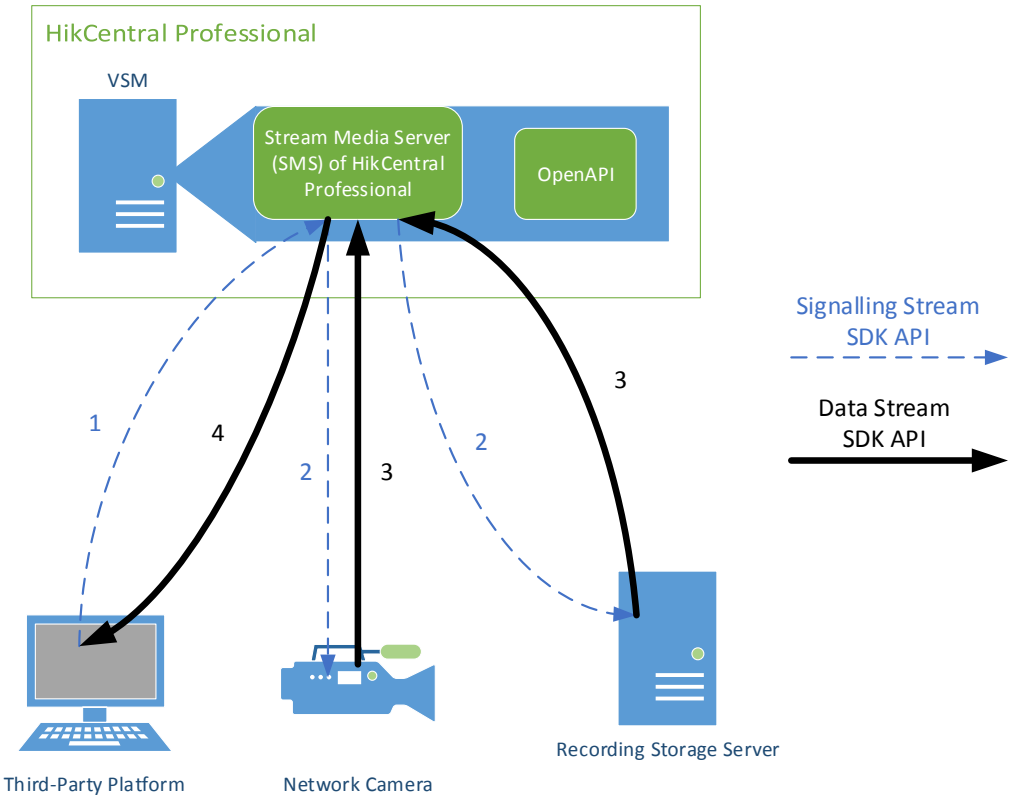


8.2.3 Network Topology

As there are multiple domain scenes deployed for HikCentral Professional services and OpenAPI, to ensure the stability of OpenAPI and the security of whole system, the OpenAPI and HikCentral Professional must be in same LAN (Local Area Network), but they can be installed in different computers or same computer.



The communication between the third-party platform and OpenAPI is based on RESTful protocol, and it is used for getting resources, operating the resources, and so on. Firstly, the third-party platform sends request command to OpenAPI service, and then the OpenAPI converts the command to support the internal protocol of HikCentral Professional and sends the converted command to HikCentral Professional server. The HikCentral Professional will send a response to OpenAPI after receiving and processing the request command. Finally, the OpenAPI converts the response to support OpenAPI protocol and sends the converted response to the third-party platform.



The above figure shows the interaction process between third-party platform and Video SDK, which realizes the live view and playback. Firstly, the third-party platform sends live view or playback request to HikCentral Professional, and then the Streaming Server (SMS) of HikCentral Professional finds the devices to start live view or playback. Finally, the video stream will also be returned to the third-party platform from the device via the SMS.

8.2.4 Overall APIs

The interaction and transmission of OpenAPI adopts RESTful protocol and it only supports HTTPS. The following table shows the API classes and the corresponding functional descriptions, for details, refer to *HikCentral Professional OpenAPI_Developer Guide_V1.5.0.pdf*.

API Class	Description
Public API	Provide public functions, such as getting version information of platform and so on.
Resource (Encoding Device) API	Provide functions related with encoding devices, such as management, refreshing, activation, and so on.
Resource (Server)	Provide functions related with servers, such as Streaming Server management, Storage Server management, and so on.
Logical Resource API	Provide functions related with logical resources, such as area management, camera management, door management, alarm input and output management, and so on.
Alarm API	Provide alarm functions, such as alarm configuration and receiving,

	and so on.
ANPR API	Provide ANPR functions, such as list configuration, vehicle passing record search, vehicle information settings and management, and so on.
Log Search API	Provide functions related with platform logs, such as alarm log search, and so on.
Status Detection API	Provide functions of camera status detection, device status detection, server, status detection, and so on.
PTZ API	Provide function related with PTZ control, such as preset, patrol, pattern, and so on.
Live View and Playback API	Provide functions of getting live view URL, playback URL, tag management, and so on.
Access Control API	Provide functions of opening door, closing door, person information management, searching for card swiping records, and so on.
Person API	Provide functions of getting person list, getting person information, and so on.

The API classes and functional descriptions of OpenAPI Video SDK are shown in the table below.

API Class	Description
Live View API	Provide functions of starting or stopping live view, stream type switch, capturing, audio control, recording, and so on.
Playback API	Provide functions of starting or stopping playing, pausing or resuming playback, reverse playback, fast or slow forward, capturing, audio control, searching or downloading video files, and so on.
Two-Way Audio API	Provide function of starting two-way audio between device and platform.

8.2.5 Installation Environment and Development Language

The OpenAPI must be installed on the computer with Window operating system.
For protocol integration, there is no development language limit; but for Video SDK integration, the development language should be C# or C++, or by developing a plug-in on web browser via some certain language.

Chapter 9 Key Advantages

9.1 Easy Deployment

Flexible Expansion: The number of channels can be extended to several hundreds, several thousands, and tens of thousands. Support horizontal and vertical expansion. Flexibly adapt to the actual application scenario by license.
Lightweight: Support 500 channels camera management by computer with Intel i5 series CPU. Provide 200 MB installation package for easy transmission and deployment. Support downloading the matched clients from the server, which is suitable for the distributed network scenario.
One-Station Solution: Meet multi-service requirements by one server: for small and medium-sized building monitoring, provide one-station solution to integrate video, access control, ANPR, security control panel access and business intelligence together.
Quick Deployment: Support deploying the server by one-click within 1 minute, suitable for different network modes. Allow users without computer administrator privilege to use the client. Allow administrators to statically install, uninstall, and upgrade the Client in a batch. Adapt to small, medium and large business scenarios.
Pre-installed Server: Provide the Dell server with pre-installed HikCentral Professional, which can work immediately after starting the server.

9.2 Easy to Use

Easy to Configure: Support detecting the encoding devices within the same network with the server or with the client, and adding the detected devices in a batch and configuring the recording schedule, to implement live view and playback immediately via the Control Client， which reduces the labor and maintenance cost.
Unified Entrance: The Monitoring module integrates live view, playback, map, event monitoring, face recognition, license plate recognition, and under vehicle scan module together, to integrate all the real-time events and operations in one page.
Excellent Video Operation Experience: Provide continuous basic video optimization, smooth drag, VCA retrieval, thumbnail playback, low-bandwidth network adaptation, multi-channel simultaneous downloading, to provide a smooth video operation experience

9.3 Easy Operation

One Page to Display All: Display the status of all the servers, physical and logical resources on the same page and provide the detailed error reason diagnosis, to help you estimate the health status of the system and manage the system better.
Efficient Operation: Support sending event reports regularly. Periodically record and view the system running status, to predict the health status in advance. Integrate the AD domain

users as system login credentials, or as credentials for access control and attendance.

9.4 Intelligent Application

Scenario-Based: Integrate the advantages of Hikvision intelligent camera and NVR, to provide scenario-based solution and flexible combination of multiple intelligent applications.

Multiple Usage of Face Recognition: Support searching pictures by face picture, real-time facial comparison, blacklist alarm, real-time monitoring for multiple face comparison groups, access control by facial recognition, and facial recognition for attendance, to provide personalized solutions for casino, airport, high-end retail outlet, etc.

Intelligent Analysis: Support people counting, queuing duration statistics, queuing number statistics, heat map, path analysis, and multiple personnel analysis data, to assist business operation.

ANPR: Support statistics on the number of passing vehicles. Support passing vehicle report, license plate recognition, license plate retrieval and license plate alarm, etc.

Chapter 10 Terms and Abbreviations

AI	Artificial Intelligence
IPC	IP Camera
DVR	Digital Video Recorder
NVR	Network Video Recorder
VSM	Video System Management
SYS	System Management Service
ADS	Application Data Service
RSM	Remote Site Management
LAN	Local Area Network
VLAN	Virtual Local Area Network
WAN	Wide Area Network
B/S	Browser/Server
C/S	Client/Server
GIS	Geographic Information System
P2P	Peer To Peer
C10S	C10S Series Video Wall Controller
ANR	ANR
N+1	N+1
ANPR	Automatic Number Plate Recognition
UVSS	Under Vehicle Surveillance System
PTZ	Pan/Tilt/Zoom
AD	Active Dictionary
NTP	Network Time Protocol
VCA	Video Content Analysis
ATM	Automatic Teller Machine
Hybrid SAN	Central Video Recorder
ONVIF	Open Network Video Interface Forum
APNs	Apple Push Notification service
GCM	Google Cloud Messaging
API	Application Programming Interface
Token	Token
pStor	pStor
SMS	Streaming Server


See Far, Go Further