iVMS-5200 Enterprise-level Platform

Architecture and Engineering Specifications

V2.2.0

Table of Contents

Chapter 1 Overview

1.1 Product Introduction

A. Designed for large-scale enterprise projects, the centralized surveillance management system provides the 24/7 uninterrupted service.

B. The centralized surveillance management system is developed based on the standard component and mature technology, and adopts various communication protocols.

C. As the key component of the centralized surveillance management system, iVMS-5200 management software passes the rigorous testing process and quality verification.

Notes:

- During the installation and maintenance of the centralized surveillance management system, all the installation, configuration, debugging and other related operation must be accomplished by the professional technicians from HIKVISION or trained by HIKVISION.
- The centralized surveillance management system shall be released under the authorization of HIKVISION and it is forbidden to give other video surveillance brands without authorization.

1.2 System Description

A. The centralized surveillance management system adopts a distributed structure and provides no limitation on the amount of sites and servers. The system also provides unified management of devices, servers and users, and flexible mechanism for enabling the system according to the task schedule or triggering by events.

B. The centralized surveillance management system supports the following operating systems (for server: 64-bit OS, for control client: 32-bit OS) with the latest service packs: Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2008 and Microsoft Windows 7 (Business / Enterprise / Ultimate).

C. The centralized surveillance management system contains the following main modules:

1. CMS (Central Management Server)

a) Provide the unified authentication service for connecting with the clients and servers.

b) Provide the centralized management for the users, roles, permissions, surveillance devices, alarm device and servers.

c) Provide the configuration interface for surveillance and management module, and sub-systems.

d) Provide the log management and statistics function.

2. Database Server

a) Supports various mainstream databases, including SQL Server, PostgreSQL, MySQL, Oracle, etc.

3. VRM (Video Recording Manager)

a) Configure the recording schedule of the cameras and provide the functions of video query and video on demand.

b) Provide the unified management of the storage of the front-end device, support PB-scale data storage and provide query result with sub-second response time.

4. VOD (Video-On-Demand) Server

a) Forward and distribute the recorded audio & video data.

5. AMS (Alarm Management Server)

a) Manage and handle the various alarm events, distribute the alarm information and upload it to the management center.

b) The available linkage actions include control client linkage (triggering pop-up image of camera, two-way audio, audible warning, text overlay), PTZ linkage, recording linkage, email linkage, message linkage, alarm output linkage (audible and visual alarm), etc.

c) The alarm logs can be recorded automatically for query by time or event type afterwards.

6. VWS (Video Wall Server)

a) Realize the unified management of decoding devices and configuration of decoding resource

b) Provide linkage actions to handle the alarm events.

7. SMS (Stream Media Server)

a) Forward and distribute the audio and video data of live view.

b) Provide the function of live view via mobile control client.

8. PTZ Server

a) Provide the control of PTZ unit.

b) Receive the control command from the control client and realize the control of pan/tilt/zoom movements, patrol, etc.

c) Support PTZ control preemption according to different user's priority level authorized.

9. NMS (Network Management Server)

a) Monitor the running status of the devices and servers of the security system in real-time and display the status in various forms of figures.

b) Provide other functions, such as resource management, log management, query and statistics of the service data, and generating the reports.

10. PAG (Peripherals Access Gateway)

a) Synchronize the time of all the SDK devices and servers.

D. Three types of control client are provided for accessing and managing the system, including B/S control client, C/S control client and mobile control client.

E. The centralized surveillance management system adopts network framework which allows multiple authorized users of Control Center to simultaneously access the video resource of the site and the inferior site.

F. The centralized surveillance management system supports the function of switching to a redundant or standby server upon the failure or abnormal termination of the core server and ensuring the non-loss of the key data and the normal working of the functions.

G. The centralized surveillance management system provides the function of two-way audio between the control client and devices, and the broadcast from the control client to the devices.

Chapter 2 Functions Introduction

2.1 Resource Management

A. Site Management

1. Add, edit and delete the sites and monitoring areas.
2. Support management of 5-level sites and areas.

B. Device Management

1. Add devices by IP address and remotely obtain device information.
2. Add devices by IP segment.
3. Support the remote configuration for HIKVISION devices, including camera information, device information, network parameters, PPPoE settings, I/O alarm and device version, etc.
4. Edit and delete the device information. When deleting the device, the cameras and I/O linked to it are deleted, and the linked alarms, linkage actions and recording schedule (both on the CMS and device) of the cameras and I/O are also deleted.
5. Manually and automatically synchronize the device information.
6. Import and export device information in batch.
7. Search devices by IP address, device name, device type, etc.

C. Server Management

1. Add, edit and delete the servers, including SMS, VRM, AMS, NMS, PTZ Server, CVR (Center Video Record) and VWS.
2. Support remote configuration of the server port and parameters, remotely restarting the server.
3. Support managing by site, multi-domain configuration to meet the requirements of cross-domain access.

D. Decoding Device Management

1. Add, edit and delete the decoding devices, and remotely obtain the device information.
2. Search decoding devices by IP address, device name and device type.

E. Camera Management

1. Add, edit and delete cameras, and the recording schedule can be kept after the camera is deleted.
2. Support the configuration for getting-stream, PTZ information, stream type, camera information, and copying the configuration information of the camera in batch.
3. Search the camera by IP address, device name, device type, etc.
4. Set keyboard code for quick calling of the keyboard.

F. I/O Alarm Management

1. Add, edit and delete the I/O alarm host.
2. Edit the name of the alarm host.
3. Search the I/O alarm host by IP address, device name, device type, etc.

2.2 VCA (Video Content Analysis) Management

A. Support connecting with VCA devices (VCA network camera, VCA encoder and VCA DVR) and behavior analysis server, configuring VCA rules and analyzing the VCA events, such as traversing virtual plane, region entrance, region exiting, intrusion, people counting, auto-tracking, etc., providing the corresponding alarm linkage.

2.3 User Management

A. Role Management

1. Add, edit and delete the roles.
2. Freely choose the permission for operating and configuring the control client according to role type.
3. Support the hierarchical user management mechanism to grant or revoke the permission according to the user level.
4. Subdivide the permission to camera, monitoring region or control center.
5. Clone and inherit the role and quick settings of the role.
6. Set the temporary role and the expiration time of the role.

B. User Management

1. Check, add, edit and delete the user by the users who have the permission.
2. Edit the user information, including user name, password, level, status, expiration time, real name, mobile phone No., email address, department, etc.
3. Edit the user information, but excluding the name, status and expiration time of the default administrator.
4. Delete the user, but excluding the default administrator.
5. Divide the users by department.

6. Set the expiration time for user.
7. Divide the user in 100 levels to realize the permission assignment for PTZ control by level.

2.4 Alarm Management

A. Server Alarm

1. Configure arming schedule of the exception for the server and the arming schedule including all-day template, workday template, weekend template and 8 customized templates.
2. Support audible warning, message linkage and email linkage for handling the alarm via control client.
3. Grade the alarm level to high, medium and low.
4. Preferentially use the AMS of the inferior site when the site and the inferior site both add the AMS.
5. Enable the same alarm settings for the inferior site when the site adds the AMS and the inferior site does not add the AMS.

B. Device Alarm

1. Configure the alarm for device offline and device HDD full by site.
2. Support audible warning, message linkage and email linkage for handling the device alarm via control client.
3. Grade the alarm level to high, medium and low.

C. Support statistics for alarm by site and record the number of camera alarm, I/O alarm, server alarm and device alarm.

D. Camera Alarm

1. Configure arming schedule of the camera alarm and the arming schedule including all-day template, workday template, weekend template and 8 customized templates.
2. Add, edit and delete the camera alarm.
3. Support control client linkage (pop-up image of camera, audible warning, two-way audio, text overlay), recording linkage, PTZ linkage, alarm output linkage, message linkage and email linkage for handling the alarm.

4. Grade the alarm level to high, medium and low.
5. Copy the information of alarm configuration in batch.
6. Available alarm types including video tampering, video loss, motion detection and VCA alarm (traversing virtual plane, region entrance, region exiting, intrusion, people counting and auto-tracking).
7. Configure the triggered rules of the alarm (enter the VCA Management for VCA alarm settings).
8. Search the camera alarm by IP address, alarm name, alarm type, etc.

E. I/O Alarm

1. Configure arming schedule of the I/O alarm and the arming schedule including all-day template, workday template, weekend template and 8 customized templates.
2. Add, edit and delete the I/O alarm, and add the I/O alarm in Alarm Management by default after adding the site.
3. Support control client linkage (pop-up image of camera, audible warning, two-way audio, text overlay), recording linkage, PTZ linkage, alarm output linkage, message linkage and email linkage for handling the alarm.
4. Grade the alarm level to high, medium and low.
5. Copy the information of alarm configuration in batch.
6. Search the I/O alarm by device type, IP address, alarm name, etc.

2.5 Recording Management

A. Record Schedule Management

1. Configure recording schedule template, including all-day template, workday template, weekend template and customized template.
2. Configure the schedule template by 7 days. The minimum unit of recording time is 30 min., and 4 time periods can be set for each day.
3. Configure the continuous recording and motion detection recording.

B. Camera Recording Configuration

1. Support multiple storage mediums, such as local HDD, SD card and IP SAN.
2. Support multiple storage types, such as device storage.
3. Select main stream and sub-stream, and disk groups.

4. Delete and copy the information of the recording configuration in batch.
5. Search by IP address, name, recording status, VRM, storage mode, etc.
6. Support statistics for the configuration information of the camera recording by site.

2.6 Network Management

A. Exception Information Report

1. Support query, statistics and displaying of the exception information.
2. Export the exception information.
3. Search by network unit type, name, site, IP address, etc.

B. Server Information Report

1. Support statistics of the running status of the server.
2. Check and display the running status of the server.
3. Remotely control the server.
4. Export the server information.
5. Support statistics by server type.

C. Device Information Report

1. Support query, statistics and displaying of the device information.
2. Export the device information.
3. Check the running status of the device.
4. Check the camera status and HDD status of the device.
5. Display the device information by filtering the device status.

D. User Information Report

1. Display the statistics of the user information and export the information.
2. Display the statistics of online users and export the information.

2.7 E-map Management

A. Add, edit and delete the static map (in JPG or BMP format and the photo size no more than 10MB).

B. Link with monitoring regions, manage by level and hierarchy, and the e-map

can be linkable to multiple sub-maps.

C. Add, edit and delete the map elements, including camera, alarm output, alarm input, link and mark.

2.8 Live View

A. Support window division and the window aspect ratio of 4:3 provides 1, 4, 6, 8, 9, 10, 13, 14, 16, 17, 22, 25-window division, and the window aspect ratio of 16:9 provides 1, 4, 6, 9, 16, 24-window division.

B. Search by camera name on the device tree.

C. Manually switch the main stream and sub-stream during live view.

D. Display the resource of the user interface by verifying the user permission.

E. Support PTZ control, including the movement in 8 directions on the live view, and direction control, step control, auto-scan, focus adjustment, iris adjustment, zoom adjustment, wiper control and light control on the PTZ control panel.

F. Support full-screen display in single-window or multiple windows.

G. Support self-adaptive window ratio, including 4:3, 16:9, 1:1 and fill display.

H. Provide instant playback for playing back the record in last several seconds to a few minutes by memory or time.

I. Support digital zoom.

J. Adjust the image parameters, including brightness, contrast, saturation, and hue.

K. Configure 128 presets and quick calling of the presets.

L. Support capture and burst mode, and provides quick printing of the pictures.

M. Provide emergency manual recording and set the file size for saving locally.

N. Enable and disable the audio while the stream type set as video and audio.

2.9 Playback and Download

A. Record Playback

1. Search video files by camera, time, recording type, storage location, alarm event, etc.
2. Support playback of local and remote video files, and fast forward, slow forward, single-frame playback, locating by dragging the mouse.
3. Enable the audio of the video and audio video files.
4. Support self-adaptive window ratio.
5. Support 1, 4, 9, 16-window division during playback, and precisely locating the record data by time.
6. Support digital zoom.
7. Support capture and video clip.
8. Support synchronous and asynchronous playback of multiple windows.
9. Search alarm triggered recording by alarm time.
10. Manage the video data via graphical interface.
11. Simultaneous playback of daily video files by 16 average segments for each camera.
12. Support playback by event.
13. Extract the snapshot of the video files. The searched record will be equal divided, and the snapshot of the equal division point will be saved for quick retrieval during playback.
14. Display the thumbnail view of the video on the progress bar.

B. Export and Download

1. Support downloads in batch.
2. Provide multiple export modes, such as local export, BD (Blu-ray disc) export and uploading to the ftp.
3. The exported or downloaded files are in MP4 format.
4. Configure the parallel number.

2.10 Log Management

A. System Log

1. Search the system logs by log type, operation type, user, start/end time, etc.
2. Show the statistics of the log information in chart form.
3. Export the logs.

B. Device Log

1. Search the device log by type and time.
2. Provide search condition of main type and minor type under type.
3. Export the logs.

2.11 System Configuration

A. Multi-domain configuration allows access by different domains.

B. Automatically and manually synchronize the time.

C. Configure the expired time for the logs.

D. Support email settings and email test.

E. Export the environment information of the platform.

2.12 Two-way Audio

A. Support two-way audio between users.

B. Support two-way audio between the user and device.

C. Support broadcasting to devices.

D. Support two-way audio among the users of the same site.

2.13 Video Wall Control

A. Video Wall Switch and Window Adjustment

1. Switch video wall.
2. Drag to adjust the window size ranging from 50% to 200%.

B. Support 1, 4, 9, 16-window division.

C. Live View on Video Wall

1. Support live view on the video wall by dragging the camera.
2. Display and refresh the decoding status of live view on video wall.
3. Manually stop the decoding of single-window or multi-window.

D. Live View and PTZ Control

1. Select the decoding window for live view via soft decoding of the cameras.
2. Support PTZ control of the cameras displaying on video wall via control client.

E. Joint the adjacent windows.

F. Support various operations on the jointed window, such as windowing, roaming, sticking at top, sticking at bottom, lock, maximizing, closing and restoring.

G. Quickly save the configured scene, switch scenes and configure the default scene.

H. Cycling Decoding on Video Wall

1. Manage the cycling schedule and the available cycling type including single-scene and multi-scene.
2. Set the switching interval.
3. Select the cameras of different areas when configuring the cycling schedule.
4. Move up, move down and delete the cycling cameras.
5. Start, pause, and resume the cycling decoding.

I. Playback on Video Wall

1. Search video files by recording time, recording type and camera.
2. Drag the search result for playback on video wall.
3. Support playback on the jointed window and opened window.

J. Alarm Triggered Video Wall Display

1. Manage and configure the alarm scene.
2. Configure the alarm linkage.
3. Display the alarm linked video on the video wall and the latest video will cover

the previous one.

2.14 Mobile Control Client

A. Support various operating systems, such as iOS and Android.

B. Support live view and playback via mobile phone.

C. Support PTZ control.

D. Support capture, saving video files and other functions.

2.15 Service Port

A. In the actual project, because of the complex network, such as internal network, external network, cross network and private network, the ports the platform and servers need to be mapped to ensure the regular transmission of the signaling and data.

CMS Port	
80	Used for web browser access.
61616	The port of MQ (message queue). Used for receiving the alarm information by the C/S client.
8005	The port for remotely stopping the Tomcat.
8009	Tomcat: The port of AJP.
Database Server Port	
5432	The data port of the default database PostgreSQL.
1433	The data port of SQL Server.
1521	The data port of Oracle.
3306	The data port of MySQL.
Video Recording Manager Port	

6300	The communication port between the CMS and the VRM.
6301	The port of the network management agent. Used for inspecting the status of the Network Management Server.
VOD Server Port	
6304	Used for accepting the request of RTSP.
6307	The port of the network management agent. Used for inspecting the status of the Network Management Server.
6309	The communication port between the CMS and the VOD Server.
20000-21999	The value range for the stream transmission of RTP/UDP transport (supported by V3.0 and V4.0 VTDU clients).
20000-21999	The value range for the stream transmission of RTP/TCP transport (supported by V3.0 VTDU client).
Alarm Management Server Port	
6500	The communication port between the CMS and the Alarm Management Server.
6501	The port of the network management agent.
6502	The monitoring port of manual alarm.
7200	Used for receiving the alarm of HIKVISION devices in listening mode.
Video Wall Server Port	
6600	The communication port between the CMS and the Video Wall Server.
6601	The port of the network management agent.
6666	Used for the communication between the video wall control client and the Video Wall Server.

6667	Used for controlling the keyboard.
SMS Port	
6678	The communication port between the CMS and the SMS.
6001	The port of the network management agent.
6010	Getting-stream port of TCP transport.
554	Used for accepting the request of RTSP.
10000-12000	The value range for the getting-stream port pair (RTP/UDP) via UDP transport and the value range for the getting-stream port pair (RTP/RTSP) via TCP transport.
PTZ Server Port	
7000	Used for receiving the command of the control client.
7001	The port of the network management agent.
7002	The communication port between the CMS and the PTZ Server in TCP mode, while receiving the command of the mobile client in UDP mode.
Network Management Server Port	
6100	The communication port between the CMS and the Network Management Server.
162	The port for the function server to upload the inspection information.
Peripherals Access Gateway Port	
7300	The communication port between the CMS and the Peripherals Access Gateway.
7301	The port of the network management agent. Used for inspecting the status of the Network Management Server.

7302	The port for communicating with the control client.
Mobile Access Gateway Port	
7071	The port of the network management agent. Used for inspecting the status of the Network Management Server.
7072	The communication port between the CMS and the Mobile Access Gateway.
556	Used for accepting the request of RTSP.
12000-14000	The value range for the getting-stream port pair (RTP/UDP) via UDP transport.
FTP Port	
21	The access port of FTP.

Chapter 3 System Requirements

3.1 Operating System

A. The Server should adopt the OS of Windows Server 2008 (64-bit) or Windows Server 2003 (64-bit).

B. The control client should adopt the OS of Windows XP (32-bit) or Windows 7 (32-bit).

C. It is recommended to use IE8 (for IE9 or above version, please set the browser mode as IE8).

3.2 Hardware Requirements of Central Management Server

The following table shows the recommended specifications of the server.

Components	Specification

Components	Specification
Processor	Intel® Xeon® E5-2620 series processor with 6 cores (up to 2.0 Ghz), QPI (6.4 / 5.86 / 4.8 GTps), large capacity cache (4 / 8 / 12 MB).
Memory	8GB DDR3 ECC
Network controller	Two RJ45 Intel® 82574L Gigabit self-adaptive Ethernet interfaces

3.3 Hardware Requirements of Stream Media Server

The following table shows the recommended specifications of the server.

Components	Specification
Processor	One Intel® Xeon® E3-1230 V2 processor (up to 3.3 GHz).
Memory	8GB 1600 DDR3 ECC UDIMM.
Network controller	Two RJ45 Intel® 82574L Gigabit self-adaptive Ethernet interfaces.

3.4 Hardware Requirements of Video Recording Manager

The following table shows the recommended specifications of the server.

Components	Specification
Processor	One Intel® Xeon® E3-1230 V2 processor (up to 3.3 GHz).
Memory	8GB 1600 DDR3 ECC UDIMM.
Network	Two RJ45 Intel® 82574L Gigabit self-adaptive Ethernet interfaces.

Components	Specification
controller	

3.5 Hardware Requirements of Alarm Management Server

The following table shows the recommended specifications of the server.

Components	Specification
Processor	Intel® Xeon® E5-2620 series processor with 6 cores (up to 2.0 Ghz), QPI (6.4 / 5.86 / 4.8 GTps), large capacity cache (4 / 8 / 12 MB).
Memory	8GB DDR3 ECC
Network controller	Two RJ45 Intel® 82574L Gigabit self-adaptive Ethernet interfaces.

3.6 Hardware Requirements of Video Wall Server

The following table shows the recommended specifications of the server.

Components	Specification
Processor	One Intel® Xeon® E3-1230 V2 processor (up to 3.3 GHz).
Memory	8GB 1600 DDR3 ECC UDIMM.
Network controller	Two RJ45 Intel® 82574L Gigabit self-adaptive Ethernet interfaces.

3.7 Hardware Requirements of PTZ Server

The following table shows the recommended specifications of the server.

Components	Specification
Processor	One Intel® Xeon® E3-1230 V2 processor (up to 3.3 GHz).
Memory	8GB 1600 DDR3 ECC UDIMM.
Network controller	Two RJ45 Intel® 82574L Gigabit self-adaptive Ethernet interfaces.

3.8 Hardware Requirements of Network Management Server

The following table shows the recommended specifications of the server.

Components	Specification
Processor	One Intel® Xeon® E3-1230 V2 processor (up to 3.3 GHz).
Memory	8GB 1600 DDR3 ECC UDIMM.
Network controller	Two RJ45 Intel® 82574L Gigabit self-adaptive Ethernet interfaces.