DHI-DSS7116D/DR

A&E Specification

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

This A&E specification is written according to Construction Specifications Institute (CSI) 3-Part Format, based on MasterFormat™ (2016 Edition) and The Project Resource Manual – CSI Manual of Practice www.csiresources.org

Manufacturer is responsible for the accuracy of the technical data included in this specification.

Division 28 – Electronic Safety and Security

Section 28 20 00 – Video Surveillance
Section 28 23 00 – Video Management System
Section 28 23 11 – Video Management System Analytics
Section 28 23 13 – Video Management System Interfaces

Part 1 General

1.1 Summary

A. DSS7116D/DR System

1. DSS7116D/DR connects clients and servers through its SMC (System Management Center) which provides a unified authorization service. MTS and SS services are responsible for streaming media forwarding and storage.

B. Related Requirements

1. Section 27 20 00 Communications
2. Section 28 05 00 Common Work Results for Electronic Safety and Security
3. Section 28 05 19 Storage Appliances for Electronic Safety and Security
4. Section 28 05 19.11 Digital Video Recorders
5. Section 28 05 19.13 Hybrid Digital Video Recorders
6. Section 28 05 19.15 Network Video Recorders
7. Section 28 06 20 Schedules for Video Surveillance
8. Section 28 21 00 Surveillance Cameras
9. Section 28 21 13 IP Cameras
10. Section 28 27 00 Video Surveillance Sensors
11. Section 28 33 00 Security Monitoring and Control
12. Section 28 51 19.13 Video Walls

1.2 References

A. Abbreviations

1. 3G The 3rd Generation Mobile Telecommunications
2. 4G Fourth Generation Wireless Communications
3. AAC Advanced Audio Coding
4. ADS Alarm Dispatch Service
5. ANPR Automatic Number Plate Recognition
6. ARS Auto Register Service
7. ASP Active Simple Profile
8. AVI Audio Video Interactive
9. CPU Central Processing Unit
10. DHCP Dynamic Host Configuration Protocol
11. DVR Digital Video Recorder
12. EULA End User License Agreement

13. EVS Enterprise Video Storage
14. GIS Geographic Information System
15. HDD Hard Disk Drive
16. HDMI High-Definition Multimedia Interface
17. HTTP Hypertext Transfer Protocol
18. HTTPS Secure HTTP
19. ID Identification
20. IP Internet Protocol
21. IPC IP Camera
22. iSCSI Internet Small Computer System Interface
23. IVSS Intelligent Video Surveillance Server
24. JPEG Joint Photographic Experts Group
25. LAN Local Area Network
26. MAC Media Access Control
27. MCD Multi-Control Device
28. MD5 Message-Digest Algorithm 5
29. MKV Matroska Multimedia Container
30. MPEG Moving Pictures Experts Group
31. MTS Media Transmission Service
32. MQ Message Queue Service
33. NVR Network Video Recorder
34. OSS Object Storage Service
35. P2P peer-to-peer
36. PCPS ProxyList control Proxy Service
37. POS Point of Sale
38. PTS Picture Transfer Server
39. PTZ Pan Tilt Zoom
40. RAID Redundant Arrays of Independent Disks
41. RAM Random Access Memory
42. RPM Revolutions per Minute
43. SDK Software Development Kit
44. SS Storage Service
45. SMC System Management Center
46. TLS Transport Layer Security
47. UTC Universal Time Code
48. VDP Video Door Phone
49. VGA Video Graphics Array
50. VMS Video Matrix Service
51. WAN Wide Area Network

B. Reference Standards

1. Network Standard
   a. IEEE – 802.3 Ethernet Standards
2. Video Compression
   a. ITU-T H.264 standard and ISO/IEC MPEG-4 AVC standard (formally, ISO/IEC 14496-10 – MPEG-4 Part 10, Advanced Video Coding), H.264+, H.265, and H.265+ encoding formats

C. Definitions

1. Contractor: Firm selected by Owner and any of Contractor's subcontractors, vendors, suppliers or fabricators, to perform work specified in these contract documents and supporting documentation. Contractor shall supply all equipment, labor, material and services necessary to complete the project construction in accordance with Contract Documents.
2. Central Processing Unit (CPU): General purpose electronic circuitry within a computer that carries out the instructions of a computer program, typically contained in a single integrated circuit chip.
3. Open Network Video Interface Forum (ONVIF): Global and open industry forum for the creation of standards for how IP-networked products within video surveillance and other physical security areas can communicate with each other.
4. Pre-recording: Automatically recording video and audio starting a specified number of seconds just before the event or time condition that initiated the recording.
5. PTZ Tour: Automatically moving a camera through a specified series of preset PTZ positions, dwelling on those positions for a specified amount of time, and transitioning between the preset positions at a specified speed.

1.3 Submittals

A. Submission

1. Submit under provisions of Section 01 30 00 - Administrative Requirements.

B. Product Data

1. Provide manufacturer's datasheets.
2. Installation and operating manuals on each product to be used.

C. Shop Drawings

1. System network topology.

1.4 Closeout Submittals

1. Warranty: Manufacturer's warranty documentation.

1.5 Quality Assurance

A. Qualifications

1. This product shall be manufactured by an enterprise whose quality systems are in direct compliance with ISO-9001 protocols.
2. All installations, integration, testing, programming, system commission, and related work shall be done by installers who are trained, authorized, and certified by the manufacturer.
3. Contractors /Installers:
   a. License: Contractors or sub-contractors shall be licensed to perform security installations in the state/region where the work is to be performed if so required.
   b. Experience: Contractors or sub-contractors shall have a minimum of three years of experience installing and servicing systems of similar scope and complexity.
   c. References: Contractors shall provide four current VMS project references from clients with systems of similar scope and complexity which became operational in the past three years.

1) At least three references shall be utilizing the same system components, in a similar configuration as the proposed system.
2) References shall include a current point of contact, company or agency name, business address, telephone number, and if the contact agrees, include a basic system description and date of project completion. The owner reserves the option to visit the reference sites, with the site owner's permission and representative, to verify the quality of installation and the reference's level of satisfaction with the system.

4. Technician Certification: Utilize professionally-trained technicians to install, program, and service Video Management System.
   a. Ensure technicians have a minimum of five continuous years of technical experience in electronic security systems including IP networking and VMS solutions.

1.6 Delivery, Storage and Handling

A. Deliver

1. The product shall be delivered in accordance with the manufacturer's recommendations.

1.7 Licensing and Support Agreements

1. Requires no Software Support Agreements with the manufacturer.

1.8 Warranty and Support

A. Manufacturer Warranty

1. Software Warranty
   a. Manufacturer's software warranty must be described in the manufacturer's EULA for the product.
2. Software Support
   a. Provide free access to any software service updates or hot fixes released due to a material error or defect in the product.
   b. Provide new device driver packs, multiple times per year, to extend support for additional devices without the need for a new version of the product.
3. Software Updates and Upgrades
   a. Make software upgrades available for a period of one year from activation of the software license. Coverage options shall include:
      1) Free access to any new product versions for the purchased Dahua VMS software product.
      2) 100% credit on owners current Dahua VMS software products when upgrading to a more advanced Dahua VMS product.
      3) Case Management online tool for submitting and tracking technical cases.
      4) Direct Access to technical support via e-mail and phone.
      5) Prioritized handling of support phone call response times based upon criticality of issue, for questions submitted by email or that cannot be answered in initial phone call.
      6) Additional years of software upgrades available for purchase separately.

B. Manufacturer Support

1. ITR Technical Support Center in Hangzhou, China.

2. Technical support is available from 8:30 a.m. to 17:30 a.m. on weekdays.
3. Regional technical support teams are responsible for the respective regional technical issues.

C. Contractor Warranty

1. Fully warrant parts, materials and labor for a minimum of one year from date of the final acceptance of the VMS, including wiring, software, hardware and third-party products, including:
   a. Provision of all new software service releases during the warranty period.
   b. Provision of all new device driver packs.

D. Maintenance and Service

1. General Requirements:
   a. Provide all services required and equipment necessary to maintain VMS in an operational state as specified for one year from formal written acceptance of system.
   b. Provide all necessary material required for performing scheduled adjustments or other non-scheduled work.
   c. Minimize impacts on facility operations when performing scheduled adjustments or other non-scheduled work.
2. Description of Work: Deployment of VMS includes installation and setup of new server hardware and software.
3. Personnel: Service personnel shall be certified in the maintenance and repair of the selected type of equipment and integrations, and qualified to accomplish all work promptly and satisfactorily.
4. Schedule of Work: Work shall be performed during regular workweek working hours, as determined by the deployment facility's locale, excluding federal/public holidays.
5. Emergency Service Response
   a. Owner has sole authority for determining catastrophic and non-catastrophic system failures.
   b. Catastrophic system failure is defined as any system failure that Owner determines will place a facility at increased risk.
   c. For catastrophic system failures, provide same-day four-hour service response with continued status updates at least every four hours.
   d. For non-catastrophic failures, provide service response within eight hours with continued status updates at least twice a week.
6. Verification of Operation: As part of scheduled adjustments and repairs, verify operation of system as demonstrated by performance verification testing.

END OF SECTION

Part 2 Products

2.1 Manufacturer

A. Manufacturer

Zhejiang Dahua Vision Technology Co., Ltd
No.1399, Binxing Road, Binjiang District, Hangzhou, China
P.C: 310053
Tel: +86 571 8768 8883
Fax: +86 571 8768 8815
E-mail: software_support@dahuatech.com
Website: www. dahuasecurity.com

B. Products

1. DSS7116D/DR manages devices such as IPCs, NVRs, DVRs, EVSs, and Access Control devices deployed across various sites. Camera recording can be stored directly in the video monitoring devices for local storage, but also can be stored in the center through IP SAN. In addition to the basic video features, DSS7116D/DR supports AI functions such as face recognition and ANPR and access control features.

2.2 Description

A. Center Management Service

1. System maximum capacity for devices management and sub server management:
   a. Manages maximum 2000 resources including encoder, access control device and alarm controller for single service.
   b. Manages maximum 1000 video channels.
   c. Manages up to 200 TB central storage per server.
   d. Manages maximum 200 access control devices and 500 access control channels for single service.
   e. Manages maximum 600 access control devices and 1500 access control channels for distributed services.
   f. Supports up to 2000 VDP devices.

B. Service Manager: An application that manages the following services:

1. NGINX Proxy Service (NGINX): Provides access to the platform.
2. System Management Service (SMC): Manages services and provides access to various functions.
3. Redis Data Cache Service (REDIS): Stores data that is frequently accessed.
4. MySQL Database Service (MySQL): Stores data for a long time.
5. System Config Service (CFGS): Monitors system resources and synchronizes configurations across the distributed environment.
6. MQ Push Notifications Service (MQ): Pushes messages among clients and platforms.
7. Media Gateway Service (MGW): Acquires video streams for video walls.
8. Protocol Conversion Proxy Service (PCPS): Accesses third-party video devices.
9. Device Management Service (DMS): Accesses video devices.
10. Alarm Distribution Service (ADS): Filters and distributes alarms from devices.
11. Device Auto Registration Service (ARS): Accesses devices added through automatic registration.
12. Image Transmission Service (PTS): Accesses ANPR devices and transfers images between the devices and the platform.
13. Alarm Controller Access Service (MCD): Accesses alarm controllers and LED devices.
14. Device Search Service (SOSO): Searches for and obtains configurations from devices in local networks.
15. Video Intercom Service (SC): Manages audio talks among PC clients and app, and video intercom devices.
16. DA Management Service (DAMS): Manages DA_BSID.

17. Link Management Service (DA_BSID): Downloads files from devices, manages the sleep and wake status of low-power consumption cameras that uses 4G network, and redirects to the webpage of devices added through automatic registration.
18. Access Control Management Service (ACDG): Manages MCDDOOR.
19. Access Control Connection Service (MCDDOOR): Accesses access control devices.
20. Video Storage Service (SS): Stores and forwards recorded videos on the platform.
21. Video Decoding to Wall Service (VMS): Accesses decoders outputs videos to video walls.
22. Object Storage Service (OSS): Stores files of the platform.
23. Media Forwarding Service (MTS): Forwards real-time video streams.

2.3 Accessibility and Management Capabilities

1. Support up to 200 users to log in to DSS7116D/DR at the same time using a PC client or a mobile client.
2. There is no license limit on the number of client connections.
3. Support active directory to facilitate the use of domain users to log in to PC Client.
4. Administration functions and operation functions are performed separately in the following clients:
   a) PC Client: All security operator features shall be accessed through the Control Client connected to DSS7116D/DR via LAN, WAN, or Internet.
   b) Mobile Client: Basic security operator features shall be accessed through the Mobile Client connected to DSS7116D/DR via LAN, WAN, or Internet.
5. Supports H.264, H.264+, H.265, and H.265+ encoding formats.
6. Supports Downloading logs from DSS7116D/DR.

2.4 System Requirements

A. System Requirements for PC Client

1. Minimum

Item	Requirement
CPU	Intel® Core i5-9500 @3.00 GHz
RAM	16 GB
Network	1000 Mbps
Graphics Card	Intel® UHD Graphics 630
Hard Disk	100 GB free space for PC Client

2. Recommended

Item	Requirement
CPU	Intel® Core i7-11700 @2.50 GHz
RAM	16 GB
Network	1000 Mbps
Graphics Card	NVIDIA® GeForce® RTX 3060
Hard Disk	200 GB free space for PC Client

2.5 Operating System

A. Operating System for PC Client

1. Windows 10 20H2 Pro (32-bit)
2. Windows 10 20H2 Pro (64-bit)
3. Windows 10 20H2 Pro (64-bit) (virtual machine)
4. Windows server 2019 standard (64-bit)
5. Windows 11 21H2 Pro (64-bit)

B. Operating System for Mobile Client

1. iOS: iOS12.0 or later
2. Android: Android 8.0 or later

2.6 System Design Criteria

A. **High Scalability**: Provide component-based system architecture to support scaling of VMS from small systems (up to 100 devices) to very large systems (several thousand devices) for single-site or multi-site deployment, whereby:
   1. For Small Systems: All software components can be installed on the same server if the server is able to handle the combined load.
   2. For Large Systems: Software components can be installed on separate dedicated servers to scale and distribute the load.

B. **High Availability and Impressive Performance**: Provide the following capabilities to ensure high VMS availability and performance.
   1. Storage solution shall be configured with RAID10 for Live database and RAID5 or RAID6 for archive database.

C. **Operating Systems**: Provide server and client software Microsoft Windows applications.

D. **Network Addressing**: Support both IPv4 and IPv6 addressing.

E. **Video Standards**: Provide simultaneous live streaming and recording of video from IP cameras and IP video encoders without any software limitations on the number of cameras per Recording Server, with support for the following codecs and options:
   1. Codecs:
      a. H.264 and H.265
      b. MPEG-4 and MPEG-4 ASP
      c. MJPEG

F. **Audio Standards**: Provide simultaneous digital two-way audio streaming and recording of audio without any software limitations on the number of devices per Recording Server, with support for the following codecs and options:
   1. Codecs:
      a. AAC
      b. G711
      c. G726

G. **PTZ Control Priorities**
   1. Provide different PTZ priority levels for control of rights between different users and automatic scanning and touring schemes.
   2. PTZ Scans and Tours shall pause for higher-priority manual or event-based camera control, and resume after manual session timeout and completion of event camera control period.

H. **Multiple Languages**: Provide support for multiple languages: Arabic, Bulgarian, Czech, Danish, English (United States), Finnish, French, German, Hungarian, Italian, Japanese, Korean, Macedonian, Polish, Brazilian Portuguese, Russian, Simplified Chinese, Spanish, Spanish (Latin America), Thai, Traditional Chinese, Turkish, Ukrainian, Vietnamese, Hebrew.

2.7 System Security

A. **User Authentication**
   1. The system requires password strength to be greater than medium.
   2. When you set a password, you are prompted of the strength of the password. Password strength includes three levels: Weak, Medium, Strength.
   3. An IP will be locked out from logging in to the platform after 5 failed attempts.

B. **User Rights Management**: Provide common and central detailed management of user rights, using roles and users:
   1. User Rights: Define roles, add and delete users, manage permissions for roles and users, generate user rights management reports.
   2. Roles: Define role permissions that determine which system features may be accessed by users.

C. **Confidentiality**
   1. Encrypted transmission of sensitive information.
   2. Web client is accessed via HTTPS by default.
   3. User password saved with MD5.
   4. TLS1.2 is used by default. You will be notified of the security risks if you enable TLS1.0 or TLS1.1.

2.8 Logging

A. Logs user activity, alarms, system information, errors, warnings, and logs about other related information.

1. User Logs: Logs user activities in client applications including, but not limited to, user system login and access, configuration changes, and other actions.
2. Alarm-Triggered Logs: Logs alarms that have been detected and triggered by video monitoring devices.
3. System Logs: Logs all system-related information, warnings and errors for troubleshooting.
4. Log Search: Logs can be searched and filtered based on user, time, operation time, video source, and more.
5. Log Exporting: Logs can be exported as .csv (comma-separated-values) files.

2.9 PC Client

A. The client can automatically discover platforms on the current network and display them for you to connect to.

B. Languages: Arabic, Bulgarian, Czech, Danish, English (United States), Finnish, French, German, Hungarian, Italian, Japanese, Korean, Macedonian, Polish, Brazilian Portuguese, Russian, Simplified Chinese, Spanish, Spanish (Latin America), Thai, Traditional Chinese, Turkish, Ukrainian, Vietnamese, Hebrew.

C. You can use a domain user account and normal user account to log in to the PC client to achieve the following functions.

1. Client Login
   a. The client displays IP addresses and port numbers of platforms in a drop-down list.
   b. The client remembers the information of the platforms that you have logged in to.
   c. The client discovers IP addresses and port numbers of platforms on the same network.
2. Homepage
   a. Toolbar
      - Displays account name, platform model, platform version, client version, software license agreement and company copyright, time and UTC time zone of the PC client.
      - Lock and unlock client.
      - Support changing passwords.
      - Notification Center: Displays system messages, such as an export task is complete, or the information of a device was edited or deleted.
   b. System Overview
      - Display permitted device information of the user: Total devices, online devices, and offline devices.
      - Display event information under login user permissions: Total events, processed events and pending events.
      - Client PC status: Network, CPU, and RAM.
   c. Main Panel
      - Applications: Monitoring center, event center, DeepXplore, access management, parking lot, intelligent analysis, and maintenance center.
      - Configuration: Configurations related to basic settings, application and the system.
      - Management: Download center, local images and videos, logs, help and quick commands.
   d. Notification Center
      - Users can view system messages, such as the information of a device was edited or deleted. The permissions of a user will determine what messages can be seen. For example, if user A does not have the permission of device A, then user A will not get the message when device A is deleted.
3. Basic Configuration
   a. Device: Device Management
      - Device group management via organization.
      - Device initialization: Initialize Dahua's device.

- Multiple ways for adding devices: Auto search, IP, Domain, IP segment, P2P, automatic registration (for 3G, 4G, DHCP devices, and alarm controllers). Supports importing devices in batches using a template.
- Access of various kinds of devices: Network camera, network speed dome, NVR, DVR, access control device, video intercom, alarm controller, decoder, and third-party devices through ONVIF protocol, and more.
- Device information editing: Support changing Dahua devices' IP addresses, modifying time zones one by one or in batches, and obtaining device information.
- Obtain device information in batches. After operation, the current information will be replaced.
- Bind the associated camera: Link cameras when configuring events.
- Support managing channel features one by one or in batches. Channel features can be configured with the following functions: Intelligent Alarm, Electric Focus, IR Temperature Analysis, Face Detection, Face Recognition, Metadata Attribute Report Capability, Fisheye, Main Sub Track, People Counting, Privacy Mask, General Heat Map, Advanced Heat Map, Entrance ANPR, Road ANPR, and Face & Body Detection.
- Device search: Support filtering devices according to the add mode (IP address, auto registration, IP segment, domain name, and P2P) and access protocol (Dahua and ONVIF).
- Increased port for ONVIF devices to ensure successful streaming even when ONVIF device is connected to WAN and the platform is connected to LAN.
- Supports voice intercom when using devices added through ONVIF Profile T protocol.
- Shortened the period between ONVIF devices go offline, and the platform detects that they are offline.
- Add devices to the platform.
  - ◇ When adding a device, you can filter the supported device types based on the add mode and access protocol. The system displays only supported information of selected device.
  - ◇ When you select a device type in the second step, you can only select from the supported device types.
  - ◇ The platform displays only the resources supported by the device type.
  - ◇ When you edit a device, the system sorts corresponding resource information based on business priority.
- Displays an icon that is used to go to the webpages of devices.
- When adding a single device by searching for an IP address, the window is automatically closed after the device is added.
- Obtains the channel names of EVS.
- Acquires video streams from ONVIF devices in a LAN and WAN networks.
- Dahua devices for China cannot be accessed to overseas DSS platforms through ONVIF protocol.
- Imou devices cannot be accessed to DSS platform.
- Access of third-party devices through RTSP, and these devices support functions such as live view, video on wall, map, storage and playback of central recordings, event source of soft trigger when configuring events.
- When adding a device, click Get Info, the alarm output channels of the decoders can be obtained.
- Add an option to include sub-organizations. When selecting the option, devices from sub-organizations are displayed; if not selected, only devices from the current organization will be displayed.
- When editing a device, the features cannot be obtained if the number of video channel features is insufficient.
- Supports ONVIF profile T authentication.

b. Device: Device Configuration

- Device parameter configuration: Door parameters, such as reader direction, door status, NO/NC period, unlock length, method, and more.

- Recording plan: Configure center recording plans for video channels one by one or in batches, or a recoding plan for each video channel.
- A video channel can be bound to itself.
- Remote device management: Remotely restart access controllers; remotely open device web browser page.
- Multicast can be configured for video channels. After multicast is configured, video streams can be forwarded by the router.

c. Role and User Management
- Three types of roles: platform administrator, administrator, and normal user.
- Platform administrators can reset their security questions.
- Manage the user's permission by role (device, control, and menu permissions)
- User can be assigned with the roles to obtain the corresponding permissions
- Supports importing domain users and assigning roles to them.
- Update domain users.
- Log in to multiple clients at the same time with the same user.
- Set user parameters: PTZ permissions for user, password expiry date, password validity, forced password change at first login, user email.
- Users can be restricted by MAC addresses and expiry information.
- Users can be locked to prevent them from logging in to the platform.
- When users forget their passwords, users with higher permissions can help reset their passwords. When the system user forgets the password, resetting through security questions is supported.
- Supports resetting password through email: If the platform has been configured an email server and an email address has been configured in a user, this user can reset its password through the email address.
- Supports PTZ operation and configuration permission, and PTZ operation permission.
- Supports video sound permission. Users without the permission cannot turn on video sound.
- Add user group. Supports configuring user group to receive events.

d. Storage
- Supports edge storage and central storage, which extends storage via iSCSI.
- The images of faces, license plates, metadata events, and alarms can be stored on EVS.
  - ◇ Rule 1: If an image is captured by the platform in an alarm, the image can only be stored on the platform no matter the image is captured by the alarm source or a linked channel.
  - ◇ Rule 2: If a device (such as an IPC) is connected to the platform through EVS and an event image (alarm, face, license plate, and target detection event) is generated by the event source, you can select a location to store the image.
  - ◇ Rule 3: If a device (such as an IPC) is directly connected to the platform and an event image (alarm event, face, license plate, target detection event) is generated by the event source, the image can only be stored on the platform.
- Alarm recordings can be stored on devices such as EVS, IVSS, NVR, and DVR.
  - ◇ Rule 1: If a device (such as an IPC) is connected to the platform through IVSS, EVS, NVR, or DVR, you can normally view alarm videos on the platform, but they are linked to the ones stored on the devices.
  - ◇ Rule 2: If a device (such as an IPC) is directly connected to the platform, alarm videos can only be stored on the platform.
  - ◇ If you store alarm recordings on devices, we recommend you configure a 24-hour device recording plan.
  - ◇ When you configure events, you can view the storage location of recordings of channels.
  - ◇ You can configure and obtain the retention time of videos and images stored on EVS.
- Notification of storage exceptions.
  - ◇ The platform will notify you when read/write exceptions or faults occur in an IPSAN or local disk.
  - ◇ You can search for records of read/write exceptions or faults in the Maintenance Center.
- Support IP SAN in normal mode and user mode.

- Network disks store videos, images and files.
- Server local disks store videos, images and files as well as evidence files.
- Disk quota: Group the disk, and cameras can be allocated to different disk groups.
- Flexible storage: Images of faces, license plates, metadata events and alarms are stored to EVS. Alarm videos can be stored to storage devices such as EVS, IVSS, NVR and DVR.
- The storage capacity of the platform can be up to 200 TB.

e. Authorization
- Displays the number of resources that you can add to the platform, such as 100 video channels can be added to the platform besides the 50 video channels that have been added.
- Video channels of access control devices will also be considered as general video channels.

f. Resource Monitoring
- Supports saving webpage information in views.
- Displays the buttons for access control functions in the upper-right tool bar only when you are viewing the real-time video of an access control channel.
- Real-time videos can be viewed directly on maps.
  - ◇ Double-click a video on a map to open the real-time video of a device in an available window.
  - ◇ When the monitoring center is fully occupied, the system selects an available window from another monitoring center tab to open the real-time video of a device.
- Zoom level will be kept when you pause a playback.

4. System Configuration

a. Deployment
- Delete a sub server.
- Enable and disable a sub server.
- Support N+M redundancy.
- Manually or automatically assign devices to different servers to balance the server load.
- Two network cards and LAN and WAN mapping can be deployed at the same time.

b. License
- Displays the number of resources that you can add to the platform, such as 100 video channels can be added to the platform besides the 50 video channels that have been added.

c. System Settings
- Configuring the data storage duration of logs, alarms, face recognition, vehicle records, access control record, video intercom record, and more.
- Time synchronization: Synchronizes time for the client and device based on the time of the server.
- Email setting: After an email server has been configured, emails can be sent to users when setting alarm linkage or processing alarms.
- After an CA certificate is configured, when accessing the platform through a browser, the browser will validate the certificate. If the certificate is installed in the browser, the browser will consider the platform as secure, and will grant it access.
- Device login modes: Security mode and compatible mode.
- Connects and sends operator logs to the log server for backup at 3 am every day.
- Configure independently installed data to record business data.
- Supports turning on or off the push notification function and adding devices through P2P.
- Supports configuring display duration for alarm pop-up windows. This configuration only applies to the current client.
- File security: You can configure whether authentication is needed when downloading data, and whether export files need encryption.

d. Backup and Restore
- Automatically back up system database (by day, week or month).
- Manually back up system database.
- Restore system database from server or local file.

5. Application Configuration

a. Recording Plan

- Configure center recording plans for video channels one by one or in batches.
- Configure a recording backup plan for a video channel.
- Configure a retrieval plan to upload videos that devices record when they cannot connect to the platform. The video from the day executing a retrieval plan will also be retrieved.
- Motion detection recording plan.
  - ◇ The platform records videos on motion detection events reported by devices.
  - ◇ The platform can record motion detection videos based on the motion detection recording plans.
- Device recording management.
  - ◇ The platform can obtain the recording plans of EVS, or configure and send recording plans to EVS. In either way, the recording plans on the device and the platform are the same.
  - ◇ For devices not installed with the latest version, the original configuration logic for device recording plans remains unchanged. The platform only sends recording plans, but not obtain the changes of device recording plans.
- Increased the maximum number of from 100 to 1,000 when configuring general recording plans and motion detection recording plans for multiple channels at the same time.

b. Event Management

- You can monitor and process over 200 types of alarms right in the event center. In addition to predefined alarm types that are triggered by devices, manual alarms are available for situations such as taking a snapshot or sending an email to the administrator when you see something important, or custom alarms for events that are supported by devices but not yet by the platform.
- Supports DHOP events.
- For pre-recording, the pre-recorded video can be cached by the platform, or stored on the device. When the event occurs, the pre-recorded video is written to the central storage.
- Combined events can be used to trigger an alarm according to the relationship of the time of trigger for two alarms.
- Supports configuring a holiday template so that an alarm will not be triggered during the defined period.
- Supports configuring trigger intervals for alarms so that only one alarm will be triggered during the defined interval.
- Alarm controller.
  - ◇ Alarm controllers ARC3000H and ARC3008C can be added to the platform through automatic registration.
  - ◇ The real-time and fault status of the zones of alarm control panels are displayed. This allows you to know whether zones are enabled.
  - ◇ Supports controlling alarm output control and siren.
- Supports configuring the stream type of the real-time video when an alarm is triggered.
- For events whose recorded videos are stored on the platform, the platform will obtain the pre-recorded portion in the cache and add it to the event video.
- Supports up to 100 icons for soft trigger events.
- After you select a category of events, all events under that category are selected by default.
- Supports confirmation when clearing real-time events.
- Parking lot events.
  - ◇ The default email template contains plate number and vehicle group.
  - ◇ Event details contain information such as plate number and vehicle group.
- Supports configuring plate number and vehicle group in the email template.
- Vehicle arming events can display plate numbers.
- When searching for historical events:
  - ◇ Multiple event categories can be selected at the same time.
  - ◇ After you select an event category, all events under that category are selected by default.
  - ◇ No limit is set on the number of selected events. However, a search timeout occurs if the search range is too large.

- Supports configuring multiple temperature monitoring rules for a thermal channel. The rules can also be displayed when viewing real-time video.
- Sequence numbers are displayed in the list of alarms that are searched to help you know the number of alarms on each page.
- Alarm linkage videos.
  - ◇ When the same alarm source reports the same event, the real-time video will be replaced. When different alarm sources report the same event, the platform will find an available alarm window. If there is no available alarm window, the earliest real-time alarm video will be replaced.
- Supports configuring generic events received from third-party devices or systems through HTTP/HTTPS/TCP/UDP protocols. You can configure the IP address allowlist. Only addresses in the allowlist can receive generic events.
- Added alarm controller subsystem event.
- Supports configuring and receiving arming and disarming status change events of alarm controllers in event center.
- Enable client sound linkage when configuring events, and the system plays the defined sound when alarms are triggered.
- Add map and linkage control information in alarm pop-ups. Supports manual control of linkage alarm outputs, and more.
- Add event notification to user groups. Supports configuring user groups to receive events, and the notification recipients will automatically update with the change of group users.
- When searching for history events, you can search for events by entering remarks that are defined when processing or forwarding the event.
- For alarm controller zone alarms, you can upload PIRCAM images and videos.
- HTTP URL command can be customized or copied from existing command when configuring HTTP URL command linkage.
- Optimized sudden sound intensity change events. Supports receiving sudden sound intensity change events detected by IPCs and reported through NVR, including audio types.
- Optimized alarm video opening method. When an alarm is triggered, you can configure not automatically switching to the monitoring center (if you have opened the alarm window in the monitoring center menu). Supports setting the duration for which the alarm linkage video opens in the monitoring center, after which it will automatically close.
- The duration that the device flashes on the map can be set when an alarm is triggered. You can select from 20 s, 40 s, 1 min, 5 min, 10 min, Always, or click Custom to customize the duration.
- Supports processing alarms in batches.
- Optimized email content and menus in event configuration.
- Alarm storm can be configured by alarm source and alarm type.
- Displays vehicle information such as plate number, speed, and more in alarm pop-ups, and details of real-time events and history events.
- You can disarm an event for a period, or disarm until the defined time.

c. Map Configuration

- Google online map, Google offline map, raster map, and satellite map.
- Submaps can be added on a map. A submap can be up to 8 levels deep.
- The information of the main map will be saved after entering a sub map. When going back to the main map, the information from the previous operation will not be reset, such as the zoom level, latitude and altitude.
- Displays all alarms in a list. Click an alarm to locate the alarm source.
- Google Maps will be in the same language as the client.
- Supports canceling operations such as selection and visible range by pressing Esc.
- Supports double-clicking a channel to open its real-time video.
- Tips are provided for visual area, initial angle, moving resources, selecting a single or multiple channels, adding submaps, measuring length and area, adding marks, and more.
- For selecting channels, adding submaps, measuring length and area, and adding marks, you can perform multiple operations until you press Esc to cancel the function.

- View the visual area of a device.
  - ◇ When using the visual area function, all cameras that support it are selected by default.
  - ◇ Double-click a camera to adjust its visual area.
- When you click a channel and the pop-up card is not fully visible, the system automatically adjusts its location to show a full card.
- The platform only loads the part of the map that is visible in the current page to display icons of channels faster.
- You can hide the names of resources.
- Supports displaying only the selected types of devices.

d. Person and Vehicle information: Personnel List
- Add, edit and delete person and vehicle groups.
- A group can only be accessed by the selected roles and their users.
- Upload face images by selecting files or taking pictures.
- Import face images in batches.
- Import personnel information (ID, Card, fingerprint, IR face, or vehicles) from devices or files in batches.
- More information can be customized for people.
- Grant people or person groups access to doors by access rules. If you grant access to a person group, the access will also be granted to all people in the group.
- Issue the card, fingerprint via USB reader or devices.
- Issue cards in batches.
- Card, password, fingerprint and face authentications.
- Person classification: Classify person into normal, VIP, visitor, patrol, blocklist to facilitate person management.
- Add the person's face to the face comparison group.
- Add the vehicle information of the person to the entrance and exit vehicle group, and configure the number of parking spaces for the person.
- When importing personnel from access control devices, if the person already exists, you can choose whether to keep the existing data. If not, the existing data will be overwritten by the new one.
- Supports searching for records by company name on the Person and Vehicle Info page.
- Supports canceling the access permissions of personnel.
- Supports DESFire cards for access.
- Displays the user information after swiping the card on the card reader.
- Removed visitor from access type when configuring access permissions for a person.

e. Person and Vehicle information: Vehicle List
- Add, edit and delete person and vehicle groups.
- Add, edit, and delete vehicles.
- Import vehicles in batches according to templates.
- Bind people information to vehicles.
- Add vehicles to the entrance and exit vehicle group or the vehicle arming group.
- Export vehicle information.

f. Watch List: Face Watch List
- Face watch list management.
- Add, edit and delete face comparison groups.
- A group can only be accessed by the selected roles and their users.
- Add face one by one, or import faces from the personnel list.
- Send face comparison group to face recognition devices, and configure the similarity.
- For devices connected to the platform have face recognition capability (such as IVSS), the face comparison database will be sent to the device. For devices do not have such capability (such as EVS), the face comparison database will be sent to the face recognition camera connected to the device.
- Supports sending face comparison groups to face recognition IPC cameras connected to EVS.
  - ◇ The platform separates sending and arming face comparison groups.

- ◇ If a device, such as IVSS, supports face recognition, the platform sends face comparison groups to the device.
- ◇ If a device, such as EVS, does not support recognition, the platform sends face comparison groups to the channels connected to the EVS.

g. Watch List: Vehicle Watch List
- Vehicle watch list management.
- Add, edit and delete vehicle watch list.
- Import vehicles from the vehicle list.
- Set start time and end time for vehicle restricted list.

h. Access Control
- Access points include door channels.
- Manage zones. Access points are managed in different zones. Each zone can be configured with different permissions that only specified roles and their users can access a zone.
- Use access rules to grant people access. Access rules include general verification, normally open, normally closed, first-person unlock, multi-person unlock, anti-passback, multi-door unlock, and remote verification.
- View exceptions that happen when access rules are being applied to access points. You can handle the exceptions accordingly and then quickly apply them again in one click.
- Use the consistency verification to quickly check the people on a device against those on the platform, and quickly address issues if any occurs.
- Count people that have entered, exited, or entered but did not exit a zone. Also, you can invalidate or validate a record, and then the statistics and status of the person will change accordingly.
- If devices go offline and then online again, the platform can automatically synchronize records from them during that period at the defined time.
- You can extract person images when acquiring access records.
- You can search the records of people entering and exiting by selecting Person, ID, Access Point, Company, or Department, and then entering the keywords.

i. Video Intercom
- Residence configuration: Set whether to enable Building No. and Unit No.
- Issue VTH contact list to VTO.
- Set VTH private password for unlocking VTO.
- View, delete and freeze users of DSS Mobile for VDP.
- Supports extracting person information on VTO.

j. Visitor
- Configure visitor default settings, such as automatic visit, automatic leave and default permissions.
- Automatic visit: An appointed visitor can automatically register the visit through pass or ANPR.
- Automatic leave: Support ANPR.
- Configure visitor default permissions of access control, video intercom, and entrance.
- Configures the email template for emails being sent when visitors make appointments (visitors and hosts), arrive and leave.
- Configures pass remark.
- The platform can automatically fill in the information of host and visitor when making visitor appointment or registering visitors.
- You can import the visitor appointment information in batches, and view the records.
- The visitor can configure the appointment information or invited by the host. After approval, the visitor will receive an access credential for visit.
- Check out visitors that are overstayed in batches and send notifications to them.

k. Parking Lot Management
- Supports multiple fuzzy match rules for license plate recognition.
- Supports excluding certain vehicles from parking space counting.
- Supports verification before opening the barrier: Manual verification by security and verification by card swiping.

- Supports configuring the parameters of parking lot events, including No Entry and Exit Record.
- Changed the dual-camera collaboration time from 1 s–10 s to 1 s–5 s.
- Information displays of the latest version can connect to entrance/exit cameras through RS-485 without being connected to the platform. You can click it and quickly go to the web page of the display to make configurations.
- With custom passing rules, you can configure whether to enable card swiping for opening barriers. If card swiping is disabled, you cannot open a barrier by swiping a card.
- You can send the allowlist and blocklist to specified entrance/exit points.
- Real-time monitoring at the entrance/exit of parking lots.
  - ◇ The device tree on the left is canceled and changed to the pop-up mode, so that there is more space to display videos.
  - ◇ For dual-camera entrance or exit, the real-time videos of both cameras will be displayed in the same window, so that you can view more real-time videos from more entrance/exit points.
  - ◇ When you open a real-time video, the latest record of barrier not opened that is linked to the entrance or exit of this real-time video is displayed.
  - ◇ A record of barrier not opened will only be displayed for 10 minutes.
  - ◇ If a record of barrier not opened is at an exit point, the corresponding entrance record will be displayed to show the parking duration of the vehicle.
  - ◇ Passing permissions are displayed.
  - ◇ Vehicle passing records can be displayed in a list or card. In list mode, you can view more information.
  - ◇ You can manually open barrier on the real-time video.
  - ◇ When you select opening the barrier directly, you can specify whether to count a parking space.
  - ◇ When you select opening the barrier and record the plate number, you can manually enter the plate number of the vehicle, and then the platform will capture an image of the vehicle and open the barrier.
- Parking lot configuration.
  - ◇ You can set fuzzy matching rules for matching passed vehicles with vehicles in the vehicle group.
  - ◇ You can select a general passing rule, which applies to most situations.
  - ◇ You can set custom passing rules. For example, you can specify that only registered vehicles can pass, all vehicles can pass, or whether vehicles can pass if there is no parking space. You can also set whether verification or card swiping is required to open the barrier, and specify that certain vehicles do not occupy parking spaces after passing.
  - ◇ You can send the allowlist and blocklist to specified entrance/exit points.
- Event parameters.
  - ◇ You can configure parking timeout parameters, including overtime parking threshold, detection interval, and vehicles to trigger alarms.
  - ◇ You can configure parameters related to no entry/exit records, including no entry/exit record duration and statistical time point.
  - ◇ After you configure event parameters, the parameters are used to trigger events.
- Voice talk function.
  - ◇ The real-time video of the VTO will be displayed in the same window as entrance/exit videos. You can switch the videos for on the top of the window.
  - ◇ When a call come through, records of barrier not opened are automatically displayed if there is any. If there is no such record, you can manually open the barrier.
- Information search.
  - ◇ You can search for records based on card swiping information.
  - ◇ Vehicle brand and color are used as separate search conditions.

l. Entrance and Exit: Vehicle Group

- Entrance and exit vehicle group management.
- Add, edit and delete vehicle group.
- Import vehicles from the vehicle list.

- Get vehicle information from the personnel list.
- There are 3 vehicle groups by default, normal, VIP and blocklist.

m. Intelligent Analysis

- To improve services and profitability, understanding how many people are in an area at any time, where people go to the most, and when peak numbers occur with people number analytics and heat maps can provide valuable and actionable insights.
- Supports displaying the number of people that passed by.
- Supports turning off calibrating the number of people staying every day.
- Supports AI heat maps.
- Supports sending historical people flow data on a regular basis to one or more email addresses.
  - ◇ Daily report: Data from yesterday will be sent to your email at a defined time. If set to 03:00:00, the data from the day before (00:00:00–23:59:59) will be sent to your email at 03:00:00 every day.
  - ◇ Weekly report: Data from last week will be sent to your email at a defined time. If set to 03:00:00 on Wednesday, the data from Wednesday to Tuesday of each week will be sent to your email at 03:00:00 every Wednesday.
  - ◇ Monthly report: Data from last month will be sent to your email at a defined time. If set to 03:00:00 on 3rd, the data from 3rd of last month to 2nd of the current month will be sent to your email at 03:00:00 on 3rd of each month.
- Regular heat maps are combined to ensure that heat map search and display on the platform are the same as these on devices.
- Allow you to search for real-time data of regular heat map devices on an hourly basis. However, you can only search offline data on a daily basis.

6. Applications

a. Monitoring Center: Live View

- With the highly customizable live view function, you can view real-time videos in any way you want. With up to 4 live view pages, you can watch real-time videos from up to 256 channels at the same time, enabling you to keep close attention to more areas. Additionally, the layout can be arranged to display different videos in different sizes, so that areas that are more important can be displayed in a more visible way. On special occasions, you can directly operate on devices, such as talking to nearby people through a camera, or unlocking the barrier of a turnstile to let people in. When something important happens, such as a robbery, the manual recording is only one click away to save that particular part of the video as evidence.
- Supports displaying the recording status of a device connected to IVSS when you are viewing its real-time video.
- E-PTZ target tracking in multi-window modes.
  - ◇ 2 window modes.
  - ◇ The tracking function can be disabled.
  - ◇ The camera will be tracking the target until it disappears.
- Multiple-monitor Support: You can see multiple monitors where each monitor shall show multiple floating or full-screen windows for display of views or individual view items.
- View window aspect ratios: Support multiple views in 4:3 and 16:9 display settings in both landscape and portrait orientations.
- Public view groups: Only specified roles and their users can access the resources in them. Only administrators have permission to configure public views.
- Private view groups: Private views are configured and owned by each user, and can be shared to other users.
- View layout persistence: Same view layout in both live and playback modes.
- View arrange and restoration: Support simple drag-and-drop re-arrangement of cameras in views for optimized monitoring of incidents, including replacement of individual cameras with different cameras, with single-click restore of original view layout.

1) View creation: Views that display up to 100 view items including cameras, web pages, images, text and interactive items. View capabilities include, but are not limited to:

2) Camera View Item: Live and recorded camera video displayed in resizable view windows, utilized in several workspaces within the application. Each camera view item contains the following:
Video Status Indicator: A round dot indicating one of four states:
Green: A connection to the camera is established.
Red: Video from the camera is being recorded.
Yellow: Playing back recorded video.
Gray: The video has not changed for more than two seconds.
3) Motion indicator: An icon of a moving person that appears only when motion is detected since it was last cleared.
4) Bounding box display: Display of metadata bounding boxes as provided by supported cameras and integrated analytics in live and playback views.
5) Intelligent area overlay: When viewing real-time videos or playing back videos, detection area and exclusion area can be overlaid on the window.
6) Update on motion only: Optimizes CPU use by allowing motion detection to control whether the image should be decoded and displayed.
7) PTZ Camera View Item: PTZ camera view item can be configured to provide virtual joystick camera control and PTZ navigation overlay buttons on the video image.
8) Overlay Buttons: Used to add manually controlled speakers, events, outputs, PTZ cameras and to start/stop recording.
9) Camera Navigator: User-defined views of specific sets of cameras in relation to each other, for example, according to floor plan, to enable visually tracking people and objects as they move from one camera's field of view to another. Camera Navigator function provides an add-on to the Map with no special configuration needed.
10) Carousel: Allow a specific view item to automatically sequence rotate through pre-defined set of cameras that are not necessarily present in the view at the same time. Operators may select default or custom display times for each camera, and they are able to manually switch to the next or previous camera in the carousel list.
11) Hotspot: Global hotspot function shall allow users to work in detail with any camera selected from any view. Local hotspot function shall allow users to work in detail with a camera selected from the same view.
12) Matrix: Shows live video from multiple cameras in any view layout with customizable rotation paths, remotely controlled by the computers sending matrix remote commands.
13) Navigable Map Pages: Static or active map pages may be used to provide a good overview of premises, and for switching between different views, such as map page displaying a floor plan.
14) 3rd party plug-ins: Add 3rd party plug-ins to extend the behavior of DSS Client.

- Live Video: Views provide camera live viewing capabilities including, but not limited to:

1) Live Viewing: View live video of camera view items on the Live tab.
2) Manual PTZ Control: Manual PTZ control options:
Video overlaid PTZ control.
Joystick.
Virtual joystick function.
PTZ point-and-click control.
PTZ preset positions.
Overlay buttons to activate PTZ preset positions.
PTZ zoom to a defined rectangle.
Start, stop, and pause patrolling.
View who have PTZ control and time to automatic release, including anonymous users.
3) Send Video to Destination: Option to send current camera to the following destinations:
4) View item in an existing window.
5) New floating window.
Digital Zoom: Magnification of video to facilitate detail viewing.
Bookmarks: Create quick or detailed bookmarks, to facilitate incident review and documentation.
6) System generated headline for quick bookmark.

7) Optional headline and description information for detailed bookmark.
Independent Video Playback:
8) Playback of video in multiple camera view items, each on its own independent timeline.
9) Option to initiate playback mode and synchronizing playback timeline with current time in independent playback.
Instant Change of Camera: Drag-and-drop placement of a different camera in a camera view item, instantly changes the content to video from the new camera, according to the camera view item's current timeline position.
Centralized Search: Initiate Centralized Search for the camera in a new window.
Manual Recording: Start and stop manual recording with automatic stop of recording after a configurable number of minutes.

- Timeline: An overview of recorded sequences and bookmarks via integrated video timeline with time navigation and playback controls, including the following functionality:

1) Timeline Video Playback: Video from multiple camera view items integrated to a common video timeline, with common timeline control from any of the integrated camera view item.
2) Single and Consolidated Timeline: Two timelines with the first showing overview of selected camera view item and second showing a consolidated overview of all camera view items in the view.
3) Timeline Period: Select which period timeline covers.
5, 10, 20 minutes.
1, 2, 4, 8, 12, 16, 20 hours.
1, 2, 4 days.
1, 2, 4 weeks.
4) Recorded Sequences Overview: Recorded sequences of video and audio are shown in the timeline. The timeline displaying light-red to indicate recording, red for motion, light-green for incoming audio, and green for outgoing audio. If there are additional sources of data available, these are displayed as other colors.
5) Bookmarks Overview: Bookmarks are shown in the timeline with instant preview of the recorded video.
6) Integrated Time Interval Selection: Integrated function to select a time interval for export or video and audio retrieval from edge storage devices.
Visual selection on timeline.
Select start and end date/time.
Loop selected period on playback.
7) Multi-Window Timeline: Ability to use one timeline to control playback of cameras in multiple view windows.
8) Recording Search: Search listing of camera sequences or bookmarks.
Preview: Search results may be previewed.
Print: Print of still image from the selected video clip may be initiated.
Export: Export of selected video clips may be initiated, reducing time needed to prepare forensic video material.

- Two-Way Audio: Audio from cameras with built-in or attached microphones can be configured for listening, or used to talk to individuals near speakers. Additional capabilities include:

1) Broadcast: Broad announcements can be made by selecting the All Speakers option when talking.
2) Lock to Selected Audio Devices: Enables continued use of microphones and speakers from selected cameras, while viewing video from a different set of cameras. This enables, for example, informing an individual at risk about the safety status of nearby areas.
3) Level Meter: Level meter indicates the volume of the speaking operator's voice, to indicate whether the operator is at a correct distance from the microphone.

- Centralized Search: Shall enable users to apply search categories and filters to find recording sequences, recordings with motion and bookmarks. From the search results, users shall be able to preview video and perform various actions, e.g. by exporting the

search results or sending the search results to PDF. The search results shall be presented instantly as thumbnail images:

1) Sequence Search: Search in recording sequences on one or more cameras.
2) Motion Search: Search for sequences with motion, or Smart Search for motion in selected areas on one or more cameras.
3) Bookmark Search: Search for bookmark headlines or descriptions.
4) Navigation: Ability to jump to search results through a clickable timeline, or the ability to scroll through the search results.
5) Preview: Selected sequence previews with auto play and direct export support.

- Video Export and Documentation: Smart options for video export and documentation include, but are not limited to:

1) Snapshot: Produce instant visual documentation of a camera by saving the camera image to a file.
2) Print: Produce instant visual documentation of a camera by sending it directly to a printer.
3) Storyboarding: The storyboarding function makes it possible to include video sequences from different or overlapping time intervals from different cameras in the one and the same export.
4) Export Preview: Review video just prior to export, with looped playback option.
5) Export Other Formats: Create evidence material in media player format (AVI files), MKV format, or still image format (JPEG images).
6) Bulk Export: In a single step, export in multiple formats to multiple destinations, including direct export to optical media, to ensure consistency across exported video sequences in various formats, and reduce human error possibilities.
7) Export of Comments: Two video formats support inclusion of comments in exported video.
8) Video Incident Report Printing: Utilize still images rather than clips to print incident reports including images, surveillance details and free-text user comments.

b. Monitoring Center: Playback

- The playback function allows you to play back videos stored on the server or devices in the layout that you have tailored to your needs. To help you efficiently wade through tons of videos, you can play them 64X faster to skip the part you are not interested in, and focus on the important content by slowing down to 1/64X minimum. Besides, you can also add tags to mark any important content for later review, and lock it to prevent it from being overwritten when the disk space is full. The filter function can also be very helpful when you only need to deal with a specific type of videos, or a type of target that appear in one or more areas.
- Supports playing back videos from multiple channels synchronously.
- When pausing a video playback, the play icon and black mask will not be displayed so that you can see the image clearly. Also, at this time, zooming in is also supported.
- Supports acquiring playback streams directly from devices.
- Supports acquiring real-time video streams and playback streams directly from devices added through P2P.
- Supports tagging on a video to be quickly played next time.
- Supports locking a period of up to 30 days of a video so that it will not be deleted or overwritten.

c. Monitoring Center: Video Wall

- Video wall is used to display videos on a large screen that consists of many smaller screens. The layout of the video wall is also highly customizable so that you can display real-time videos or recorded ones on it and be able to magnify every little detail. With the task function, you can display videos from different channels on the video wall at the specified time or in a loop.
- Display modes.
  - ◇ Image and video modes are supported.
  - ◇ In video mode, you can open the real-time videos of all the channels bound to the video wall at the same time.

d. Monitoring Center: Map

- The map is a very useful function that allows you to keep track of anything with its location information. For example, you can mark a device on the map and be able to immediately know its location when it triggers an alarm and flashes red on the map, or add a submap of an area to the map, such as a plan view of a public square, to know where exactly a person is in the public square.
- Support satellite map.

e. Event Center
- Real-time and history event information.
- Event display: Displays alarm schemes; event statistics by day, week and month; event information statistics, which include total events, processing and processed.
- Alarm details: Live video, record and pictures from related camera, event source location on the map.
- Process events one by one or in batches: Acknowledge the event, forward the event to relevant user, fill out the handling comments, and manually send event email to relevant person. Events that have been processed can also be sent by email.
- Mandatory remarks for processing events. When a user is processing an event, the user must enter remarks.
- Pre-processing remarks for events. When users are processing an event, the defined remarks will be filled in by default.
- Arming control for event source.
- Search event by event source, event time, status, handle user, priority.
- Export the event list.
- Refresh alarms as scheduled.
- Count events according to priorities: High, Medium and Low.
- Event trend report.
- Analyze event resources and types of the top occurrence frequency.
- Alarm controller.
  - ◇ Arming for the device, sub systems and partitions; force arming if arming failed; disarming for the device and system.
  - ◇ Enable or disable temporary or eternal bypass functions.
- Unified the time format of exported cases.
- Supports adding one person to different face arming groups.

f. DeepXplore
- Powered by AI technologies, you can easily search for targets and recordings, and generate tracks to locate their whereabouts with simple search conditions.
- Add the image of license plate and business group information in the motor vehicle snapshot details when searching for the vehicle.
- The snapshots of searching results can be viewed in slideshow-style in the details.
- UI interface refactoring for the DeepXplore. You can search for person, vehicle and records in integrated retrieval.
- Optimizes the function of person searching. The person searching includes searching by feature, searching by image and searching by archives. For the searching by feature and by image, you can set the search target, face or human body.
- Optimizes the function of vehicle searching. The vehicle searching includes searching by feature, searching by image and searching by archives. For the searching by feature, you can set the search target, motor vehicle or non-motor vehicle.
- Optimizes the function of records searching. You can select the search mode from multiple or single. For multiple searching mode, you can configure the record type including metadata records, file records and other records.
- Supports the new and old devices for result comparison when searching by image.

g. Maintenance Center
- By just visiting one page, you can stay up to date with information on alerts, devices, servers and more to instantly recognize issues such as offline devices and abnormal servers. Scheduled reports are also sent based on the information collected to give you a full picture of how your system is running.

h. Access Management: Access Control
   - In the access control panel, door channels in different zones can be viewed and controlled.
   - For access records, you can view historical access events, analysis on people entering and exiting, and the movement path of people.
   - Event linkage recording on the access control panel: Only displays the recorded video of the channel linked to the access control channel.
   - Event linkage image on the access control panel: Displays the snapshots reported by access control devices and captured through events.
   - On the Access Control Panel page, the face information can be automatically refreshed.
   - The reset time of anti-passback can be between 1 minute and 24 hours.
   - When exporting access records, you can select the fields to be exported.
   - Optimized admin configuration of local device when configuring access control device.

i. Access Management: Video Intercom
   - All video intercom devices can be managed based on different in one single interface. With two-way communication and remote access control, you have the ability to secure access to your premises. Also, residents will be able to call and report emergencies quickly, allowing you to take immediate actions. To make building management easier, messages that a lot of people should know, such as the electricity will be out for a few hours for maintenance purposes, can be sent to their indoor monitors with only a few steps.

j. Access Management: Visitor
   - DSS7116D/DR offers a complete process to manage visitors, including registration, access permission authorization, and ending visit with all permissions canceled. A complete, detailed record of all visits is available for your review at any time.
   - When searching for visit records, the appointment arrival time or visit time can be set to 60 days before at most.
   - Number of visits when making visitor appointment or registering the visitor.

k. Parking Lot Management
   - View real-time license plate recognition in split mode or full screen.
   - Open the barriers via VTO with cards or remotely.
   - Support check detail vehicle information.
   - Supports searching for entrance records, exit records, forced exit records, on-site vehicles, snapshot records and ANPR details.
   - When parking space counting by entering and exiting vehicles is enabled for a parking lot, and a vehicle will be counted for available parking space, forcing the vehicle will add an available parking space to the parking lot.
   - Force existing vehicles to leave.
   - Search and export the vehicle records.
   - After enabling SIRA certification, more information of a vehicle capture record can be displayed, such as the place of issue of a license plate.
   - Support resetting available parking space.
   - Support allocating parking spaces according to vehicle groups, which is generally used for allocating company parking spaces.
   - Add the event of parking lot full and alarm for vehicles of unknown plates.
   - Optimized reports of entered and exited vehicles including search conditions and list display.
   - Optimized the linked video of parking lot record including the display of the entrance, exit and parking records, the detailed information display including snapshot and video.
   - Adds the plate snapshots to the entrance and exit records.

l. Intelligent Analysis
   - View the real-time number of people in the group and the number of people allowed to enter.
   - Search for history people flow statistics of cameras and people counting groups by day, month, week and year and export reports.
   - Generates and exports thermal maps.
   - Analyzes the number of people staying in the region and exports the report.

- The chart displays the total of the statistics.

7. Management
   a. Download Center
      - Download record from central storage or device, supports avi, dav, mp4, asf.
      - Download record by timeline, files or tags.
      - Supports multi-task download.
      - Restore face images from face privacy mask.
   b. Local Picture
      - Open local picture folder.
   c. Local Recording
      - Open local video folder.
      - Play local or downloaded videos.
   d. Local Settings
      - General: Configure the window size of the client, synchronize the time of the client with the server, auto startup and login in after restart, set CPU threshold, client auto lock and encrypted transmission of audios and videos, and more.
      - Video: Customizable split screens, select display mode of video window, stream switching rules, the way to obtain real-time stream, play mode and decoding mode. Select video stream type of instant playback and the interval and number of snapshots.
      - Select default stream type, stream switching type, video play duration and the way of video on wall.
      - Configure default or custom alarm tone, and the way to open alarm-related videos and alarm flashing on the map.
      - Video and image storage configurations for file storage.
      - Select PC keyboard or joystick USB keyboard with shortcut keys.
   e. Log
      - Operator, device, system, and service logs.
      - Search and export logs.
      - Download logs are generated by file, with each including detailed device name, IP address, channel name, channel number, start and time of the video, and file name.
      - Live view logs include detailed device name, IP address, channel name, channel number, and start and end time of live view.
   f. Help
      - Open the user manual.
8. Others
      - The client supports Windows 11.
      - The SOSO service supports distributed deployment. Device information on sub servers can be obtained.
      - SIRA.
      - All services now support 64-bit operating systems to utilize more hardware resources such as CPU and RAM.
      - The maximum size of the logs of a single service is now 200 MB. This prevents logs from occupying too much storage.

2.10 DSS Agile Mobile Client

A. DSS Agile is an App on a smart phone (Apple iOS or Android) for security operators to access the platform remotely via LAN, WAN or Internet. It shall provide multiple operating functionalities, including real-time live view, PTZ control, video playback and alarm notification.

B. On initial log in, users must input the DSS server IP and Port number in the server address box.

C. Users shall be able to log in with HTTPS transfer protocol.

D. DSS Agile shall have the following modules and functions:

1. History Record
   - Show recently viewed channels; you can open live video or playback via history records.
   - Display up to 20 latest history records.

2. Live View
    - Even when you are away from your computer, you can also ensure the safety of your area right on DSS Agile. You can watch the real-time videos remotely from up to 16 channels at the same time with 3 stream types for you to choose according to the status of your mobile network. PTZ control is also supported so that you can cover most of the area. When anything of interest happens, you can take snapshots or recordings as evidence that stores on your phone, or send a voice message to deter unwanted activities.
3. Playback
    - Videos stored on devices or the server can both be played up to 8X faster or 1/8X slower on DSS Agile. You can also use the manual recording function to record important content and save it to your phone.
    - Views provide additional camera playback capabilities including, but not limited to:

    1) Playback: Time synchronized play back video of camera view items on the Playback tab.
    2) Navigation: Advanced video navigation includes:
    Forward and backwards playback at different speeds:
    Playback Speeds: ¼x, ½x, 1x, 2x, 4x, 8x, 16x.
    Instant Real-time Speed: Toggle 1x playback speed or selected playback speed.
    3) Forward and backwards frame-by-frame.
    4) Skip to next or previous recorded sequence.
    5) Skip to beginning or end of recordings.
    6) Jump to date/time.
4. Face Recognition
    - Support searching the face database or snapshot records for target faces by uploading a face picture.
    - Support face database management.
    - Face library search.
    - Snapshot library search.
    - Face library management.
    - Face statistics.
5. Video Metadata
    - Search for targets classified by people, vehicle and non-motor vehicle.

    a. Alarm Center
    - Alarm subscription.
    - Offline notification push.
    - Search for alarm messages by category.
    - Claim and handle alarm messages.
    - History alarm message search.
6. Map
    - Support GIS map and raster map.
    - Display the video channel on the map.
    - View live and recorded videos by clicking device icon on the map.
7. Access Control
    - With DSS Agile, you can remotely monitor and operate all access control devices. For example, you can open a door for someone who has a proven identity, or set a door to be always closed so that no one can access.
8. Video Intercom
    - You can receive and process various types of alarms. You can also receive alarms when DSS Agile is not running with a subscription button.
9. Favorite
    - Quickly view video of channel added to the favorite.
10. File Management
    - Snapshots and videos stored on devices or the server can be managed as you need, such as deleting them or exporting them to your album.
11. Target Tracking

- For suspicious activities, you can locate targets directly in DSS Agile by searching for face recognition records from a period, uploading a face image of a specific target, or searching for capture records of people, non-motor vehicles, and motor vehicles by features.

12. Others
    - Supports controlling alarm output channels.
    - Supports adding faces and licenses to person groups and vehicle groups.
    - Support soft trigger.
    - Supports Russian.
    - Supports clipping recorded videos.
    - Updated the UI and interaction of the preview and playback screen.
    - Supports searching for recorded videos by category

2.11 DSS Agile VDP Mobile Client

A. DSS Agile VDP Mobile Client shall have the following modules and functions:

1. Resource Monitoring
    - Supports viewing real-time videos of linked IPC channels.
2. Visitor Management
    - You can easily manage visitors by registering their information and generating visitor passes with necessary access permissions. When they arrive, they can use the passes to gain access to where you are. DSS Agile VDP will log when visitors begin and end their visits.
3. Intercom Monitoring
    - When guests arrive, they can call you on the door station or you can verify their identities through the live video. After confirming they are who you are expecting, you can remotely open the door for them directly on DSS Agile VDP. If you spot any unwanted activities, tap and call the management center to report an emergency.
    - DSS Agile VDP supports arming VTH remotely.
4. Message Center
    - The unlock records and alarm messages on the indoor monitor are fully accessible on DSS Agile VDP, allowing you to identify potential threats and ensure the safety of your residence.

2.12 Keyboard

A. Supports connecting NKB 1000 to client PC via USB. Functions are as follows:

1. Window Control
    - Open/exit full-screen display via the FN key.
    - Set the number of screen and window splits.
    - Select a window on the screen to output video.
    - Support switching video input sources.
    - Support switching stream types.
2. PTZ Control
    - Control the eight directions of PTZ camera via joy stick.
    - Set PTZ step length via the number keys.
    - Perform adjustment of aperture, focus, and zoom with buttons.
    - Call PTZ presets via numbers plus buttons.
    - Use buttons for horizontal rotation, scanning, tour, tracking, and menu operation.
3. Video Wall Control
    - Select TV walls and plans.
    - Set the number of screen splits and clear the screen.
    - Set the number of window splits and clear windows.
    - Select a window on the screen to output video.
    - Support switching windows.
    - Support switching video input sources.
    - Support switching stream types.
    - Support stopping playing video on the wall.

- Support shortcut operation; shortcut information can be viewed on the client.

B. NKB5000 can log in to DSS7116D/DR after entering IP address and port number of DSS7116D/DR in itself. The following functions can be achieved

1. Live View
   - Support outputting live videos via VGA and HDMI interfaces.
   - Support screen switching by double-clicking or dragging.
   - Support screen splits, including 1, 4, 9, 16 splits.
   - Support maximizing, multi-selecting, and clearing windows.
2. PTZ Control
   - The live view supports performing rotating and zooming at the same time.
   - The live view supports PTZ zoom, focusing, aperture, light, and wiper.
   - The live view supports presets, PTZ tour (settings not supported), scanning, and pattern.
3. Video Wall
   - Support acquiring and switching video wall tasks.
   - Support acquiring and switching video wall layouts.
   - Create, modify, and save tasks.
   - Support for platform TV wall segmentation, including 1, 4, 9, 16, M-N segmentation.
   - Support window maximization, stream type switching, and clearing window.
   - Support using the small keyboard for video switching (number+ Mon, Mult, Win, Cam, Previous, Next), and PTZ operation (Preset, Scan, Tour, Pattern, Pan, PTZ).
   - Support using virtual keyboard for video switching (d number+ Mon, Mult, Win, Cam, previous, next).

2.13 Licensing

A. License Activation

1. VMS shall offer easy-to-use automatic or manual online activation via the Internet and alternatively, offline activation via email and web for closed surveillance networks.

B. License Administration: Provide license information presenting the license use.

2.14 Configuration

A. System status

1. View service status, CPU status, network status, and local disk status.
2. The local disk status supports displaying the slot number, and when there is a bad sector alarm, a warning prompt will be received at the upper right of the Config system or the client.

B. Network configuration

3. NIC configuration

When the server has multiple NICs, NIC mode can be selected.

a. Multi-address: Access multiple segments.
b. Load balancing: Provides network capacity larger than bandwidth of a single network port, and reassigns the load to another available network port in case of abnormal interruption of the network port, to ensure network reliability.
c. Fault-tolerance: 4 network ports are all connected to cables. Normally, only one port is used. If the port is broken, another port is selected to continue running.
d. Link aggregation: Combines multiple physical ports to form a logical port to share load of incoming and outgoing data and on each port.

4. Network mode

a. Mapping mode: Access the platform by mapping IP address. When there is Intranet and Extranet, you can access the platform with Extranet IP by mapping Intranet IP to Extranet IP.
b. Multi-IP mode: To use multiple network ports of the platform to connect devices of different networks, enter the IP address of other network ports here.
c. Supports selecting the working network of the decoding device on the platform. When decoding to the video wall, the system will provide the corresponding IP address to the decoding device for video on wall.

5. Connection detection

Check whether the IP address and URL are connected normally.

6. Routing settings

Configure static routing.

C. Service mode

1. Main server and sub server modes are available. Main server mode supports hot standby.
2. With dual hot standby configured, when the main server crashes, the other server will work to ensure the stable operation of the system.

D. Security configuration

1. Enable or disable SSH connection and TLS 1.0. After enabling SSH connection, you can set the enabled period and port of SSH connection.
2. After enabling trusted verification, only executable files that are correctly signed will be allowed to run normally on the platform.

E. System maintenance

1. Supports basic maintenance operations, including reboot the device, shut down the device, restore the device to default settings, and reset password.
2. Download service log.
3. System update (overwrite installation). Update through web or by ConfigTool.
   Back up data before update.
4. Supports printing and downloading system log.
5. Supports updating the system through fix pack.

F. Basic configuration

1. User management: Change the password of admin account.
2. Time configuration: Configure system time zone, date and time.

END OF SECTION

Part 3 Execution

3.1 Examination

A. Verification of Conditions

1. Inspect the site and confirm that the conditions on the site are in accordance with the project design. Sort out all the conditions and subsequent operations that will affect the installation. Do not take any corrective action without the written permission from the owner.
2. General
   a. Verify whether existing site conditions are suitable for product installation according to the manufacturer's instructions.
   b. Verify wire lines and make sure that related conditions are ready.
3. Cable and Wiring
   a. Check whether the channels used for the cable meets the requirements.
   b. Check whether wiring channel, cable tray and other components meet the space allocation requirements; check the installation tolerances, cable installation dangers, and other conditions that may affect the installation.
4. LAN/WAN
   a. Verify the LAN connection between DSS Server and DSS PC Client.
   b. Provide a fixed public IP address for accessing the DSS service from the public network via port mapping.
5. Power Connections
   a. According to the manufacturer's instructions, verify whether the installation circuit meets the requirements.

3.2 Preparation

A. Discuss with the owner about the required functions and configuration items.

1. Determine the network deployment and whether public network access is required.
2. Username and password for servers and workstations for easy installation and commissioning.
3. The default password set for the software at the beginning of debugging.

3.3 Installation

A. Devices shall be installed in accordance with the manufacturers' instructions provided, as well as instructions based off any indicated floor design specifications.

B. Location of installation shall provide reasonable conditions for optimum device functionality. Temperature and humidity level conditions shall be taken into consideration.

C. All installations shall be performed with qualified service professionals only.

D. All devices shall be installed in accordance with the National Electric Code or applicable local codes.

E. Ensure location of installation provides a minimum possibility of accidental damage.

3.4 Site Quality Control

A. Proper testing of all video systems according to the standard operating requirements.

B. Define, conclude, and report all issues with equipment to the manufacturers' customer service representatives.

3.5 Adjusting

A. Execute the necessary modifications to the Video Management System for proper operation in accordance with the instructions provided by the manufacturer.

B. Ensure the customers unique requirements are reflected in the camera settings.

3.6 Demonstration

A. Upon final inspection, validate the video solutions system and its device functions correctly.

END OF SECTION

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188