# Table of Contents

DSS Installation Configuration and Business Use Guide ........................................... 1

1 DSS Deployment ........................................................................................................... 6

1.1 DSS Overall Frame Intro ......................................................................................... 6

1.1.1 System Frame ........................................................................................................ 6

1.1.2 DSS Structure ....................................................................................................... 7

1.1.3 Live Video Flow ................................................................................................... 8

1.1.4 Device Record Search and Playback Signal Stream .......................................... 10

1.2 Upgrade .................................................................................................................. 11

1.3 Network Deployment ............................................................................................. 13

1.3.1 IP Config ............................................................................................................. 13

1.3.2 Standalone Mode ................................................................................................. 18

1.3.3 WAN Mapping .................................................................................................... 20

1.3.4 Dual Hot Spare ................................................................................................... 25

1.3.5 Distribution Server Config .................................................................................. 28

1.3.6 N+M Backup ...................................................................................................... 32

2 Business Function Operation .................................................................................. 33

2.1 TV Wall ................................................................................................................... 33

2.1.1 Add Video Wall Device ...................................................................................... 33
2.1.2 TV Wall Config.................................................................................................. 34
2.1.3 Video on Wall Operation....................................................................................... 35
2.1.4 Real-time Output to Wall ...................................................................................... 42
2.1.5 Alarm Output to Wall ............................................................................................ 44
2.1.6 Playback on Wall ................................................................................................. 44
2.1.7 E-map on Wall ...................................................................................................... 45
2.2 Record Operation...................................................................................................... 45
  2.2.1 Search Record by Record Type ............................................................................ 45
  2.2.2 Download Record ................................................................................................ 46
  2.2.3 Lock Record ......................................................................................................... 46
  2.2.4 Download Record by Time .................................................................................. 47
2.3 Central Alarm Management ..................................................................................... 48
  2.3.1 Setup Flow .......................................................................................................... 48
  2.3.2 Contacts .............................................................................................................. 49
  2.3.3 Set Link Level ...................................................................................................... 50
  2.3.4 Set Alarm Time Template .................................................................................... 50
  2.3.5 Set Alarm Storm .................................................................................................. 51
  2.3.6 Output Alarm Video to the Wall ......................................................................... 52
  2.3.7 Set Alarm Scheme ............................................................................................... 53
2.3.8  Alarm Record Search.................................................................54

2.4  Client Alarm Management ................................................................55
  2.4.1  Alarm scheme ...........................................................................55
  2.4.2  Alarm Manager .........................................................................58

2.5  E-Map ..........................................................................................60
  2.5.1  Google Map ...............................................................................60
  2.5.2  Google Offline Map ....................................................................61
  2.5.3  Raster Map ...............................................................................62
  2.5.4  Super Map ...............................................................................65

2.6  Video Quality Diagnosis ..................................................................66
  2.6.1  Video Diagnosis Setting ............................................................66
  2.6.2  Manager Channel Diagnosis Statistics .........................................68
  2.6.3  Client Video Diagnosis ...............................................................68

2.7  Access Control Business .................................................................69
  2.7.1  Add Access Control Device .......................................................69
  2.7.2  Access Control Link Video Setup ..............................................70
  2.7.3  Unlock Overtime Alarm ..............................................................70
  2.7.4  Access Control Alarm Display ..................................................71
  2.7.5  Alarm Link Video ......................................................................71
2.7.6 Access Controller Remote Control

2.8 Fisheye Device Support

2.8.1 Add Fisheye Device

2.8.2 Fisheye Installation Mode Setup

2.8.3 Fisheye View Mode Setup

2.8.4 Fisheye Video Correction

2.9 Intelligent Application

2.9.1 General Intelligent

2.9.2 Face Recognition

2.10 Logic Organization Structure

2.11 DSS Device Sync Time

2.12 User and Related Rights

2.12.1 Role Management

2.12.2 User Management

2.13 Storage Plan
1. DSS Deployment

1.1 DSS Overall Frame Intro

1.1.1 System Frame

- DSS

According to project demand, deploy host, hot spare, slave device, you can select DSS7016 or DSS4004. DSS7016 has better overall performance than DSS4004, and it supports local storage, may plug in 16 disk slots, one as system disk, other 15 may be storage disks, and it can expand into multiple DSS7016 to support larger demand on storage.

- Storage

You can select EVS as front storage, not as central storage, and this scheme is more suitable for DSS4004.

Central storage scheme need to deploy more DSS to support forwarding storage, DSS quantity and storage bandwidth are related, mainly depending on storage and bandwidth size, and in order to reduce platform investment, we recommend EVS front storage.

If you select DSS7016 as central storage, no using EVS.
• TV Wall

Select M70 to control video wall.

1.1.2 DSS Structure

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Function</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS</td>
<td>Manage other server registration and signal deployment</td>
<td>9000</td>
</tr>
<tr>
<td>DMS</td>
<td>Responsible to login front encoder, receive alarm, forward alarm, send alarm and send calibration command</td>
<td>9200</td>
</tr>
<tr>
<td>MTS</td>
<td>Responsible to get A/V stream from front device and forward to SS, client and decoding device.</td>
<td>9100</td>
</tr>
<tr>
<td>SS</td>
<td>Responsible for record storage and record search and playback</td>
<td>9320</td>
</tr>
<tr>
<td>VMS</td>
<td>Responsible to login decoding device and send video wall task to decoding device</td>
<td></td>
</tr>
<tr>
<td>MGW</td>
<td>Responsible to send MTS address to decoding device</td>
<td></td>
</tr>
<tr>
<td>ARS</td>
<td>Responsible to auto register device listening, login and get and</td>
<td>9500</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>PCPS</td>
<td>Responsible for Hikvision, onvif device login and to get and forward stream to MTS</td>
<td></td>
</tr>
<tr>
<td>ASC</td>
<td>Responsible to resolve alarm scheme into ADS and some APP</td>
<td></td>
</tr>
<tr>
<td>ADS</td>
<td>Response to send alarm info to different objects according to different schemes</td>
<td></td>
</tr>
<tr>
<td>ADP</td>
<td>Responsible for cascading of alarm business</td>
<td></td>
</tr>
<tr>
<td>VQDS</td>
<td>Perform video quality diagnosis, currently diagnosis options on 7016 are: video loss, high brightness, low brightness, contrast, definition, color shift</td>
<td></td>
</tr>
<tr>
<td>PES</td>
<td>Responsible to manage MCD</td>
<td></td>
</tr>
<tr>
<td>MCD</td>
<td>Responsible for alarm host, access control and environment device input and alarm receiving and forwarding</td>
<td></td>
</tr>
</tbody>
</table>

### 1.1.3 Live Video Flow

![Live Video Flow Diagram](image-url)
1.1.3.1 Live Preview Signal Flow

1. Client send request to CMS;
2. CMS send command to MTS;
3. MTS receive command, and send its address back to CMS;
4. CMS receive MTS return and send MTS address to client;
5. Client get video from MTS according to address;
6. If MTS does not request this channel of video, it will send signal data to device;
   If device is Hikvision, then MTS get video from PCPS;
   If it is auto registration of device, MTS get video from ARS;

1.1.3.2 Live Preview Data Flow

- Auto Registration
  DVR——ARS——MTS——client;
- Hikvision device
  HKDVR——PCPS——MTS——client;
- Directly login device
  DHDVR——MTS——client;
1.1.4 Device Record Search and Playback Signal Stream

1.1.4.1 Search

1. Client send request to search record to CMS ;
2. CMS send signal of search device record to SS ;
3. SS call SDK to search front device record ;
4. Front device return record info to SS ;
5. SS return record info to CMS ;
6. CMS return record info to client ;
1.1.4.2 Playback

1. Client double click a time point to playback——client send playback request signal to CMS ;
2. CMS send playback signal to SS ;
3. SS send record date request to font device ;
4. Front device return record data to SS ;
5. SS send its own RTSP address to CMS ;
6. CMS send SS address to client ;
7. Client requires corresponding SS request record data ;

1.1.4.3 Data

Front device——SS server——client

1.2 Upgrade

If during upgrading, you need to clear config, the correct flow is :

Config Backup->Upgrade program->Config clear->Restore system default
Step 1: Login manager web.

Step 2: Select System -> Upload, and click button to download the Config tool.

Step 3: Choose at downloaded folder and unzip. Click to open DSSConfig folder and unzip the file, then select file to open.
Step 4: Click Login and pop up Login interface, input IP address, Username, Password and Port of DSS7016 or DSS4004, then Login.

Note: User name and Password are “admin” in Default, the port is 3800.

Step 4: Download and copy the upgrading file to PC. Click “open” button to select the upgrading file, and click “Upgrade” button.

About 5 minute later, system will prompt Upgrade Finished and Reboot, click OK to finish the upgrade.

Note: Make sure the upgrading file which is copied to PC is complete, if not or select the file from uDISK directly, system will prompt file error.

1.3 Network Deployment

1.3.1 IP Config

1.3.1.1 DSS4004

Step 1: Connect monitor to DSS4004, and login, username: root, initial password is dahua2006
Step 2: Select Network Configuration and Ethernet card to config.
Step 3: Modify IP info, and save.
Note: After login, you can re-enter network config interface via “setup” command.

### 1.3.1.2 DSS7016

**Step 1**: After system boot up, system pop up “startup guide” box.

**Step 2**: Click “next”, pop up “general setup” box to set.
Step 3: Config IP address

After basic setup is complete, click next, pop up “network config” box to set.

- **Load balance**:

  4 network ports bound to form one virtual network port, only need to configure one IP, in actual work, 4 network ports will switch data (according to front device and client MAC address and DSS7016 4 network ports MAC address calculate to ensure that a certain front-end or client uses a certain network port to switch.)

![Network configuration screen]

- **Multi-address mode**

  multi-address mode is 4 network ports which can independently work, no matter whether other network connect to Ethernet cable or not, 4 Ethernet port IP must config as different segments; If one network port is LAN, and one network port is WAN, you need to set default network to connect to WAN card;
After local LCD configured multi-address, login config tool, [http://ip/config](http://ip/config), click Segment Setup, and select "Extension Address", click "+", input LCD panel configured IP, click Apply.

### 1.3.2 Standalone Mode

For small surveillance system, you can use directly DSS7016 or DSS4004 matrix monitoring platform to achieve.

Note: to guarantee system stability, we recommend you to deploy one more DSS, for dual hot spare.
● DSS

According to project need, deploy host, hot spare, extension, you can select either DSS7016 or DSS4004.

● Storage

Select EVS as front storage, or you can directly use DSS7016 as central storage.

● TV Wall

Use M70 to control video wall.

DSS7016 and DSS4004 performance as follow:

<table>
<thead>
<tr>
<th></th>
<th>DSS7016</th>
<th>DSS4004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Storage</td>
<td>1-System HDD</td>
<td>Not support</td>
</tr>
<tr>
<td></td>
<td>2-16- Storage HDD</td>
<td></td>
</tr>
<tr>
<td>Transfer capability</td>
<td>700Mbps</td>
<td>300Mbps</td>
</tr>
<tr>
<td>Devices</td>
<td>500</td>
<td>200</td>
</tr>
<tr>
<td>Channels</td>
<td>2000</td>
<td>500</td>
</tr>
<tr>
<td>Accounts</td>
<td>Support 10000 accounts management and 1000 online users</td>
<td>Support 2000 accounts management and 100 online users</td>
</tr>
</tbody>
</table>

Note: If adopts DSS7016 as storage, you need to format HDD.

1. Login system config interface, format is: http://IP/config;

2. Storage config->select disk to format->click format button;
1.3.3 WAN Mapping

1. Map DSS’s IP for DMZ, map out all ports of this DSS’s IP, and this is the easiest method;

2. In LAN is there are multiple device or PC need WAN mapping, to make WAN mapping, you may make port mapping to open WAN for port to be used by DSS, in general LAN DSS each server port maps to WAN as the same port, if 7016 server needed port is already occupied by other server in WAN, such as admin used login port is 80, but WAN port 80 is occupied, than you can map LAN port 80 to WAN port 82 or 90. However, when WAN admin login, need to input: http://X.X.X.X:82; If CMS 9000 port is also occupied in WAN IP port, then you can map LAN 9000 to other port, such as: 9001, so when WAN user logins CMS, need to input port no.: 9001;

3. WAN mapping need to open port: Tomcat—80; CMS—9000; DMS—9200; MTS—9100; SS—9320; ARS—9500; ADS—9600; ASC—9700; ADP—9800; MGW—9090; config tool—9092; CRT tool—22;

WAN mapping has two methods, now we use NETGEAR wireless router as example, and please note different model may have different configuration interface.
1.3.3.1 DMZ Host Method

- First login router management interface.
- Client WAN Setup in menu on the left.
- In WAN Setup interface “Default DMZ Server” check this option, and fill in IP address of DMZ computer you want to set as host. The IP address shall be static which you can manually set.

Note: the advantage of DMZ method is the easy setup, you can use when you are not sure to open which port. Set computer as DMZ host, its all ports will open to internet, and this will lead to risk. After set DMZ host, all ports mapping indicate toward DMZ host. Invalid when indicate toward other computer’s port mapping.

1.3.3.2 Port Mapping Method

- First login router management interface.
- Click “Port Forwarding&Port Triggering” in menu on the left.
- Click button “Add Custom Service” to map port, make ADS server as example, port to map is 9500, server IP address is the LAN IP address to be mapped to WAN (this IP address need to be manually
set static, perform the same operation to other server mapping.

Note: the advantage of port mapping is relatively safe since it shall be added one by one manually, only some ports are open to public.

Note:

1. external port no: it is to map LAN port to which port of WAN, such as to map LAN port 80 to
WAN port 81, or LAN cms port 9000 to WAN port 9002. (In general, WAN and LAN shall match each other, but sometimes WAN port 9000 is occupied by other server, then need different mapping)

2. internal port no: fill in port of LAN that you want to map to WAN;

3. IP address: fill in LAN address you want to map to WAN;

### 1.3.3.3 DSS Config After WAN Mapping

After router has configured WAN mapping, you need to go to WEB and config:

- **First login WEB config interface**

  [http://172.6.5.25/config/user_toLoginPage.action](http://172.6.5.25/config/user_toLoginPage.action)

1. Click Segment Setup option on the left, click “+” button, in Extension Address fill in mapping WAN IP address.

2. Click Server Config on the left, select DMS option, Extension Address by default fill in IP address from previous step, default port is 9200, if port is not modified, maintain default is fine, other server MT S, MGW, SS, ADS, PES, ASC, ARS, PCPS, PTS with the same operation.
Login WEB manager

http://172.6.5.25/admin/login_login.action

Select System option -> Parameters, fill in CMS option WAN Port 9000 (by default), PCS option WAN Port 9001 (default), WEB Server option WAN Port 80 (by default), Alarm Picture FTP Server option WAN Path ftp://60.12.11.50/alarm/
1.3.4 Dual Hot Spare

1.3.4.1 Framework

Hot standby mode can improve the stability of system, when the active server fail or disconnect, the hot standby server change to active mode automatically and the system keep on work normally.

Note:

Instruction before you deploy the hot standby system.

- The two DSS7016 of hot standby system as the center management server generally, but not as the storage.
- The hot standby system need to be configured a VIP(Virtual IP), which is not be used in business network. You need only login by VIP after configuration.
- The NTP timing must be done between the two DSS7016 before deploying the hot standby system, to ensure clock synchronization.
- If you want to link the SMS and Email when the alarm happen, you must to finish relevant option in both DSS7016 before deploying the hot standby system.
1.3.4.2 Network Connection

- Connect the lan 2 between two DSS7016 by cable, and must be configured with the same network segment, to keep alive and data sync.
- Connect the lan 1 of both DSS7016 to switch, to manage the other devices.
- VIP(Virtual IP) must be not used in business network. this can be ensured by PING utility.

1.3.4.3 Config

Step 1:
For example, 172.7.1.166 and 172.7.1.169 are the IP address of active server and hot standby server, login in the web manage of active server and hot standby server respectively, then configure VIP as the web server IP and submit.

Step 2:
Choose the 172.7.1.166 as the standard server
Enter and login the Configure System bia http:// 172.7.1.166/config
Enter Quick Guide, select Master and check “Hot spare or not” option.
Step 3:
Set the VIP as the extension address, and adjust it to first line.

Step 4:
Choose the mode for the standard server, then fill in parameters. Check up the parameters by clicking “One-key Check” button, then “Execute Dual Hot Spare”, system will synchronize the data between active server and hot standby server. Then finish configuration of this hot standby system after rebooting.
Note:

- Make sure that Mask is consistent with business network.
- Virtual router ID is the identification number which distinguish the hot standby system.
- Another DSS7016 can not login during configuration, or the calibration can not be passed through.

1.3.4.4 Tear Down

If you want to teardown the hot standby system, you must login configure system and uncheck the “Hot Spare or not” option in both active server and hot standby server.

1.3.5 Distribution Server Config

Via pile, may fulfill requirement of larger surveillance system. Mainly control DSS to complete main role, and manage extension mode DSS, support distribution; extend mode DSS then complete forwarding, storage (DSS7016) and device management function, max support 20 unit of pile.

1.3.5.1 Framework
Distribution system, there are two types of the type of server, master server and slave server, but only one main service, the other is slave server; the role of the primary server is the master, make data management, equipment management and disposal of other work slave server, Therefore, the system only the master server starts the database (mysql service), tomcat and CMS and other services, and role of slave server is a device access + forwarding + storage, just start the appropriate service functions, such as DMS, MTS, SS, ARS, PCPS, etc. the only interface of the entire system to the user is IP address of the master server;

Using the System Config tool to config the salve server with master server IP, the services in salve server will register to CMS services of primary server automatically, when the master server CMS service receives information, it will assigned server ID to register server, which distinguish the different type of service and the same type of service which from different registration server, and the registration information and service type are written in the database, meanwhile notify Tomcat service to read the data from the database. At this time, master server will show up the distribution server info;

1.3.5.2 Config

Two units of DSS address are 172.6.5.25 and 172.6.5.28, hope to set 172.6.5.28 as master server, and set 172.6.5.25 as slave server.

Step 1: Via visiting the IP address to be set to sub server, enter Config interface, such as http://ip/config
Step 2: Enter quick guide, select “slave”. Fill in main control IP address. Click Next, to enter next, configure related info and save. Reboot server.

Step 3: Login main server 172.6.5.28
Step 4: Enter General->Server->Distributor Server, click icon, enter "Edit Distributed Server" interface.

Step 5: Select Video Unit and Picture Unit, check Enable, select Home Server, and save, enable distribution server;
1.3.6 N+M Backup

1.3.6.1 Principle

N + M backup is a backup mechanism for distribution server, where N is the number of units home servers, M refers to several alternate server, the home server means the server has ownership relations with equipment (selecting server when add device), alternate server refers to the backup machine of home server;

After the designated home server add alternate server, if the home server is down and can not be started within 60 seconds, CMS will the equipment and business on home server assigned to the backup server machine, while the video is stored on disk of backup services;

During the alternate server work, the existence records of the home server can be queried but can not be played, but if the original home service has been restored from the exception, although the device does not move back , the original home records can also be played back;

When the home server is restored to normal, the device can be moved back to the original home server, then the home video services and alternate server can query and playback;

1) N+M backup in general is for distribution device ;

2) About config N+M backup device number , in general $1 \leq N \leq 20,1 \leq M \leq 5$. N+1 is used in more applications ;

3) N+M backup can be manually switched.
1.3.6.2 **Config Method**

Match 1.3.6 distribution server config, only when at Step 5 select Alternate Server, and check available alternative server.

---

### Business Function Operation

#### 2.1 TV Wall

##### 2.1.1 Add Video Wall Device

**Step 1:** Login manager, select General->Device->Matrix

![Image of device selection](image1)

**Step 2:** Fill in M70 IP address account and password, click "Getting Info" to auto get device info.

![Image of device information](image2)

**Note:** M70 device channel info can only be get by clicking "Getting info" button, cannot manually input, so when adding M70 device, please ensure the device and 7016 are well connected and device are
2.1.2 TV Wall Config

Step 1: Business -> TV Wall -> Add

Step 2: Input TV Wall Scheme Name, select screen layout, if to configure cubeless video wall, select screen to combine and click combine button at the upper-right.

Step 3: Bind decode channel with screen

2.1.3 Video on Wall Operation

Login client, open Output to Wall.
2.1.3.1 Output to Wall

Step 1: Select TV Wall dropdown list, select corresponding TV wall.

Step 2: Drag device in right list to window of TV wall.

Intro of functional buttons

1. 📺 Apply Now: When select, drag video channel to window, video will be output to wall, you do not need to click output video wall button.

2. 🛡️ TV Wall: Output video wall button, display current bound video source on wall.

4. Custom window: user can custom split mode by self.

5. Screen on/off: Remote control to enable and disable display screen of TV wall.

6. One-key setup: Batch set stream type and stay time.

7. Multiple Selection Operation: Simultaneously select multiple windows.

On client, click the arrow at the lower-right corner to pop up eagle eye thumbnail, zoom in to quickly find location of eagle eye.

2.1.3.2 Vide in Small Window

Step 1: Device tree select a channel, right click, open video, select bit stream type.
Step 2: Display in small window.

2.1.3.3 Video Wall Task

Step 1: After binding video channel and screen in client, click Add Task, click +, input task name, click OK to save.
Follow the same steps, you can add more video wall tasks. And you can switch among multiple tasks to achieve manual output of different tasks.
2.1.3.4 Video Wall Plan

Step 1: Enter TV Wall Plan, select +.
Step 2: Select plan type: Schedule Plan or Tour Plan

Step 3: Fill in Plan Name, Select task, Set the stay time, and Add.

According to need you can add multiple tasks to tour and save.
Step 4: In TV Wall Plan interface, display configured task, open enable, as to enable video wall task.

2.1.4 Real-time Output to Wall

Step 1: In live preview window, select ;
Step 2: In pop-up window, drag resource to corresponding window to output.
2.1.5 Alarm Output to Wall

When alarm occurs, link alarm to wall, see Ch 2.3.6.

2.1.6 Playback on Wall

Client pushes record data to decoder, and only can push to physical screen, cannot push to cubeless video wall.
2.1.7 E-map on Wall

Step 1: Click pane button, select area to output to wall, display device list within the area.

Step 2: Select TV Wall, drag channel corresponding screen to output to video wall.

2.2 Record Operation

2.2.1 Search Record by Record Type

Support alarm record, motion detection and all record classification search.
2.2.2 Download Record

After record search is complete, click record download button, pop up File Download box, you can select file and download by time.

2.2.3 Lock Record

Step 1: Record bar right click will pop up menu and you can select lock start and end time, select end time will pop up box as shown below, you can input reason of lock and click Lock.
Step 2: In record lock unit, search and unlock.

2.2.4 Download Record by Time

On time axis, select one start point, right click, select start, and select one end point, right click, select End, the following interface pops up.
2.3 Central Alarm Management

For admin, who managed all of the system, may link to email, SMS, center video wall, and center storage.

2.3.1 Setup Flow

DSS Manager supports alarm, including Alarm Scheme, Output Alarm Video to the Wall, Alarm Type, Alarm Time Template, Link Level and Contacts.

- Alarm Scheme: set alarm scheme template.
- Output Alarm Video to the Wall: Make alarm video display on wall.
- Alarm Storm: Set system alarm interval as batch.
- Alarm Time Template: Set alarm time template.
- Link Level: Set alarm link level.
- Contacts: Set user who to receive alarm notice.

Configuration progress as follow:

2.3.2 Contacts

When you add user into contacts and if the setup of Link Level includes email or sms, then system will send email or sms to the new contact.
2.3.3 Set Link Level

Set Link Level Name and select Link Mode. including Email, Record, SMS, TV Wall.

2.3.4 Set Alarm Time Template

Input Template Name, select cycle period or Single Period. Set Period and link level.
Note:

If you check the Copy box next to Template Name, then you need to select template in the dropdown box.

Click + to set Link Level of other periods.

2.3.5 Set Alarm Storm

You can set alarm interval as batch.
Note: Set alarm interval to 10s by default, if alarm interval is too frequent, alarm info will not be able to be solved efficiently, which is equivalent to device’s anti-dither function.

### 2.3.6 Output Alarm Video to the Wall

Step 1. Add TV Wall task.

Step 2. Input Task Name and select TV Wall, set duration.

Step 3. Drag channel on the left to TV wall window, and save.

Note: You shall configure TV wall before outputting alarm video to the TV wall.
2.3.7 Set Alarm Scheme

Step 1: Add Alarm Scheme.

Step 2: Add alarm Source and corresponding link operation.
In Alarm Source area, select alarm source (Device, Video channel, Alarm input Channel, Intelligent Channel, A&C Channel, System).

In Corresponding Link Operation area, select link operation(Record, Email, SMS, TV Wall).

Note: If you need pre-record, then there needs to be record on the device.

Step 3: alarm preview

![Alarm Preview](image)

2.3.8 Alarm Record Search

Login DSS client, enter playback interface, select center storage record.
Note: Center alarm link to center alarm record, for rights owned by all client users, including search, playback and download.

2.4 Client Alarm Management

For operator, config alarm plan for resources within right range.

2.4.1 Alarm scheme

Step 1: Enter Alarm Scheme interface.

Step 2: Input Scheme Name, Description, Time, Audio and Others.
Step 3: Set Alarm Source.

Select Alarm Type to be armed and channel on the left. Click on ➤. System will add alarm source to list on the right.

Step 4: Set Link Video

Select alarm source on the left. Select video channel under Link Video tab. Click on ➤ to add selected link video to area on the right.
If you want link alarm out, Select alarm output device under Event Alarm Type tab.

Step 5: Enable alarm scheme

After you add alarm scheme, click on operation bar, and close status turn to open. Click on open can enable alarm scheme and click on Enable Time to select time template to enable.
Note: time template is set by manager in manage web.

2.4.2 Alarm Manager

If alarm scheme is configured, when alarm occurs, Alarm Manager displays corresponding alarm.

- Real-time Alarm

System displays all alarms by level.

Double click the alarm info, show alarm details and mark the alarm with pending, fixed, in progress, false alarm, ignore and results.
- **Alarm History**

Select corresponding channel in list on the right, and select Alarm Type, Period, Alarm Status, Progress Period, Progress Status. Click on “Search” to search alarm records meeting above criteria. It will list alarm info by list mode or chart mode.
2.5 E-Map

2.5.1 Google Map

Step 1: Login system config interface, such as http://IP/config

Step 2: Map Config, select Google, set default longitude and latitude (position to default area) -> Apply.
Step 3: Display on client

Note: client google map language pack selection depends on IE browser language option.

2.5.2 Google Offline Map

Step 1: Login system config interface, such as http://IP/config

Step 2: Map Config, select Google offline Map, set map engine path and map WAN IP -> Apply.
Note:

Map engine path: map located path;

Map engine WAN IP: Map server and program are not on the same device, you need to configure map server IP address.

2.5.3 Raster Map

Step 1: E-map type select: select raster maps click Apply, and effect after reboot;

Step 2: Log in manager, enter Business->Map
Step 3: Add map picture.

Step 4: Add video channel.

Step 5: Add access control channel
Step 6: Add alarm channel

Step 6: Client display

Show device online and offline statuses and channel info.
View channel video, and support PTZ operation. Channel with record storage, may playback record.

2.5.4 Super Map

Step 1: Select Super Map—configure map engine path—config map shortest path analysis—configure map engine WAN IP—application.
Note:

Map engine path: map located path;

Map shortest path analysis: server path used to analyze the shortest distance between two points on map.

Map engine WAN IP: map server and program are not on the same device, need to config map server and IP address.

2.6 Video Quality Diagnosis

2.6.1 Video Diagnosis Setting

Step 1: Diagnosis item config

Video quality diagnosis mainly include video loss, high brightness, low brightness, contrast, definition, color shift. These values’ normal, warning and abnormal ranges may be set in diagnosis option.
Step 2: Task config

Step 3: Scheme config
2.6.2 Manager Channel Diagnosis Statistics

In maintenance statistics→device statistics→channel diagnosis statistics module, you can see result of diagnosis. It has list and graph formats.

2.6.3 Client Video Diagnosis

On client you can view video diagnosis abnormal info.
On client view video diagnosis abnormal info result

### 2.7 Access Control Business

#### 2.7.1 Add Access Control Device

Platform manager → basic config → device management → device → access control → add

Access control support DH-BSC1221A/DH-BSC1202B/DH-BSC1202C device input, while DH-BSC1202B is new device.
2.7.2 Access Control Link Video Setup

Platform manager ➔ business config ➔ video link ➔ access control ➔ config

Click non-bold source channel on the left, and check video channel on the right, click OK to config.

2.7.3 Unlock Overtime Alarm

In platform manager ➔ business config ➔ in unlock overtime config unlock overtime, for example config info in the following figure, if unlock time is 6 min, then the client will generate level 5, level 4 and level 3 overtime alarms.

If trigger access control overtime alarm, at bottom of in client access control module, all or overtime alarm bar will show overtime message.
2.7.4 Access Control Alarm Display

In client access control module, there are display of access control alarm info. Click option tab next to all, you can display alarm info by type.

2.7.5 Alarm Link Video

In alarm scheme, add alarm scheme, set scheme name.
In alarm scheme, add alarm scheme, alarm type and alarm source.

In alarm scheme module, set alarm link video.
Enable access control, client auto pop up linked alarm video.

2.7.6 Access Controller Remote Control

Mo remotely unlock and lock door, and open bound video.
2.8 Fisheye Device Support

2.8.1 Add Fisheye Device

When add, Function need to select fisheye.

2.8.2 Fisheye Installation Mode Setup

In platform client, select live preview module, select device supporting fisheye function, in video interface right click to set fisheye installation mode.
2.8.3 Fisheye View Mode Setup

And select view mode.

2.8.4 Fisheye Video Correction

In fisheye view PTZ mode, you can click correction function at the lower-right.
2.9 Intelligent Application

2.9.1 General Intelligent

For general intelligent (tripwire, cross warning zone, people count, intelligent tracking), the recommended scheme is the DSS platform direct management over front-end camera with intelligent function.

2.9.1.1 Add Intelligent Device

Step 1: Input the IP address of DSS in Internet Explorer and press Enter.
Step 2: Input username and password, select user type, then press Login.

![Image of login interface]

Step 3: Open the manager interface, select General>Device>Device>Encoder.

![Image of manager interface]

Step 4: Click , system displays Add Encoder box.

![Image of Add Encoder box]

Step 5: Set the Input Info, input Device Name, and select smart IPC in Device Type. Click Getting Info,
System will automatically get info of video channel, alarm input channel and alarm output channel.

Click OK as finishing adding encoder.

Step 5: Smart IPC Configuration

- You can right click smart IPC on the client device tree, choose SmartIPC Config to enter the smart IPC config WEB page, where you can set intelligent rules on IPC.
Or you can go to device WEB page via config button in Manager device list.

2.9.1.2 Intelligent Alarm Config

Refer to Ch 2.3.

2.9.1.3 Intelligent Application

- Behavior analysis, including tripwire, Instrusion, Object Abandoned and etc.
People Count

Note: display people count in the upper-left.

2.9.2 Face Recognition

For face recognition, we recommend to use IVS-F7200. IVS-F7200 can achieve face detection, face comparison and database.
2.9.2.1 System Framework

IVS-F7200 related face recognition records are stored on EVS. Client query the alarm record from EVS.

2.9.2.2 IVS-F7200 Config

Refer to IVS-F7200 manual.

2.9.2.3 Storage Config

In system framework, EVS deploys as front storage, so need to manually configure.

Step 1: Add EVS
Step 2: Configure EVS remote channel.

Login EVS web, Configure remote device. Make the IVS alarm records storage in EVS.

Step 3: Binding EVS channel and IVS channel

EVS is as front-end storage in framework, so platform does not know where IVS record is, need to manually bind ( future support auto method )
2.9.2.4 Client Business

1. Enter IVS-F interface and select IVSF Monitor Tab, it will show real time video and show the face picture on the bottom of interface.

2. Double click the picture, it will pop-up register add interface, which can add the picture to register library. When this person appear next time, system will produce an alarm info in alarmsearch tab.
3. In Register Search Tab, you can search all the face picture which store in register library, also you can import one designated face picture to search if this face is stored in library or not.

4. In historysearch tab, you can search all picture which appeared in video. Through import image, you can search designated person if appear in designated location and period.
5. In alarmsearch tab, it show all the alarm info list, which is produced when matching degree between the capture face and register picture exceed the appointed percentage. you also can play the relative record.

2.10 Logic Organization Structure

Logic organizational structure is different from general device structure, according to his need, user can manage channels of different devices under the same directory for easy management. This function can apply to lower control right, but not limited to device conditions.

Step 1 : Enter General->Org->Logic Org.
Step 2: Click Create Logic Org on the left, in pop-up interface enter Org Name, and save. Complete logic organization directory creation.

Step 3: Select organization directory organization, click +Add button, and input related info, select channel to add into current logic organization structure, add content.

Step 4: In General->Account->Role, add role, in Edit Role interface Device Rights tab, select Device Tree Display Right column, on the right, Select Organization Directory to display the logic organizational
directory just created, check corresponding directory and save.

Step 5: Create user, role is belong to the just created role.

Step 6: After login client using the corresponding account, in resource list only display logic organizational directory with allocated rights.

2.11 DSS Device Sync Time

Working Principle:

DSS server’s DMS server send sync time command to front-end device via network SDK, after front device sync time, will return DMS server to info channel and sync device time to certain time.

Check object to sync time(server, device), set sync start time and period, click sync time button.
Note: Sync time principle is 7016 via Netsdk to sync device time, so the device does not need to enable NTP server.

2.12 User and Related Rights

2.12.1 Role Management

Step 1: Add role

Click add button

Step 2: Check channel to grand corresponding control right.
Note: device tree display can only be in one organizational structure at the same time.

2.12.2 User Management

Step 1: Add user

Click add button.

Note: select corresponding right role for user.
2.13 Storage Plan

Login Manager—business config—record management;

Step 1: Configure time template.

Step 2: Configure storage plan.

Enter storage plan config interface.

Add storage plan: check channel to store, input plan name, and select time template and bit stream type,
check enable.