DSS7016D/DR-S2 and DSS4004-S2

FAQ

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Foreword

General

This manual provides answers to problems that may occur when using the product.

Attention

This manual is for reference only. Not all the DSS problems are included.

- You can contact us for any unknown problems, and we will add them into the manual to perfect it.
- You can contact your local retailer or after-sale engineer directly for more help.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1 Installation and Deployment

1.1 What browsers can I use to log in to the configuration system?

- Firefox: Version 91 and later.
- Google Chrome: Version 70 and later.
- Microsoft Edge: Version 100 and later.

1.2 Why did switchover fail in hot standby?

- Switchover might fail if you force hot standby to start.
- Switchover fails occasionally because data copying is incomplete between the two servers.
- When you need to use the hot standby, contact technical support to build environment. In case of any problem during use, also contact technical support immediately.

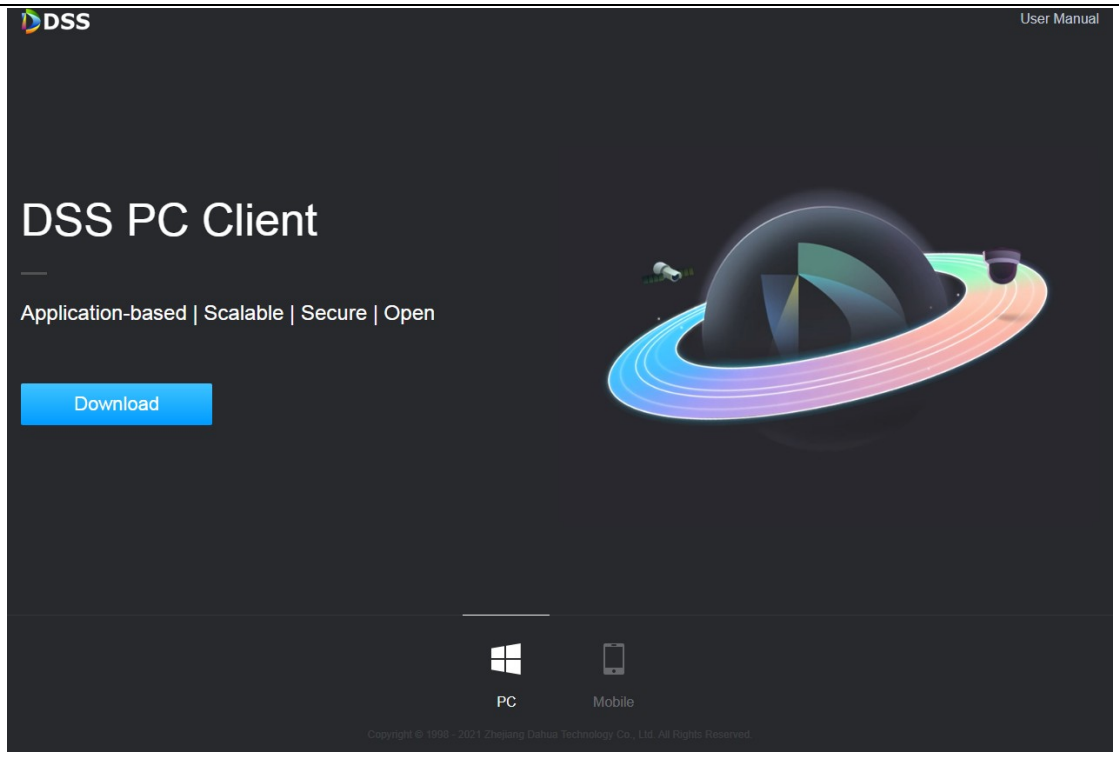
1.3 Why does the platform not work properly?

Log in to the configuration system, select **System Status** > **Service Status**, and then check whether all the services are running normally.

1.4 How do I get the installation package of DSS client?

Step 1 Go to the IP address of the platform in the browser.

Step 2 Click **PC Client** at the bottom of the page, and then click **Download**.

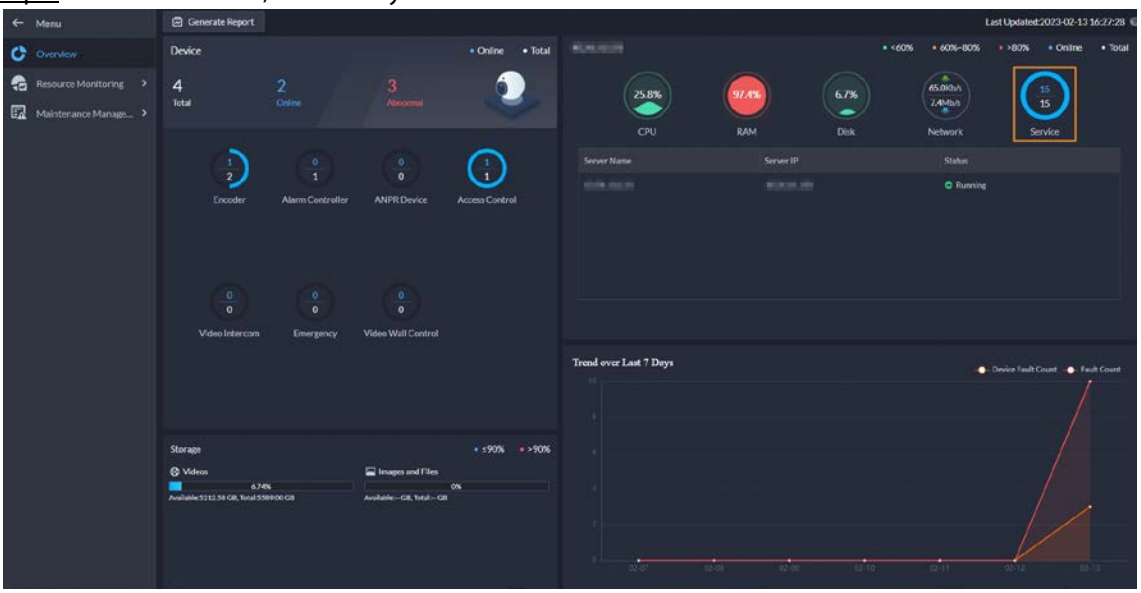


Step 3 Save the installation package to your computer.

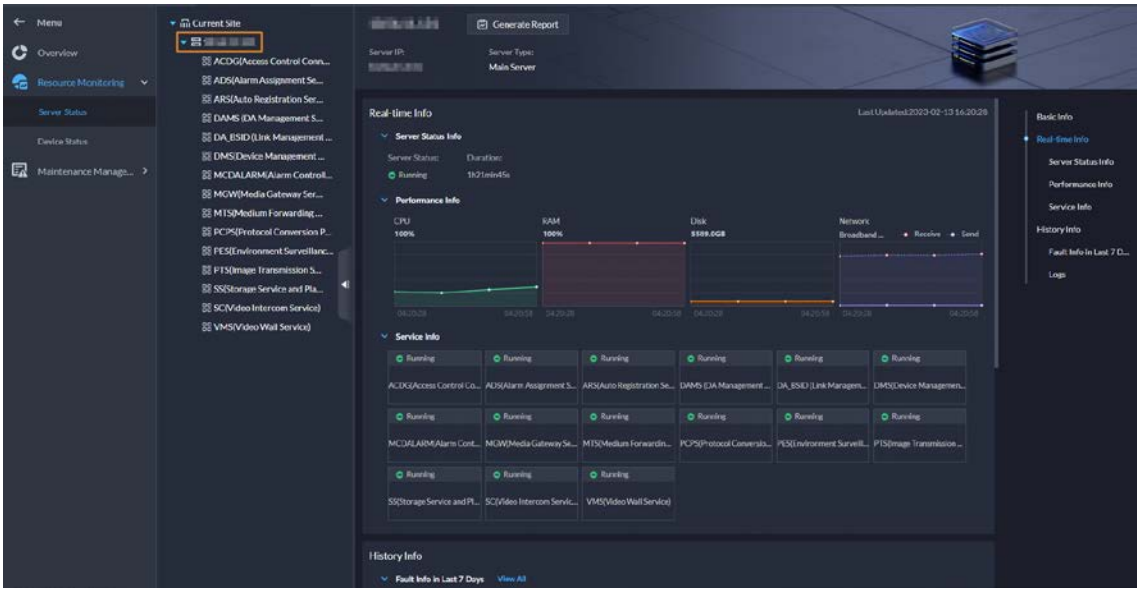
1.5 How do I know if a service of a sub server is working normally?

Step 1 Log in to the DSS client of the main server, and then go to **Maintenance Center**.

Step 2 Click **Overview**, and then you can see the number and status of all services.



Step 3 Select **Resource Monitoring > Server Status**, and then you can view all the servers and their services.



1.6 In the client installation directory, double-click update.exe, and the platform cannot be updated directly

The update.exe in the directory is for program use and cannot be used alone. The update .exe will check the version information when users log in to the client. If there is a new version available, it will prompt you to update.

1.7 The newly installed sub server always shows that it is starting.

For information security, the newly installed sub server needs to be enabled on Distributed Config in System Deployment the service management page of the client in order to have access to the database or other information from the central database. Otherwise, the sub server cannot connect to the central database and will always show that it is starting.

1.8 The time of each sub server is different

Check whether the server time, time zone and corresponding DST are consistent.

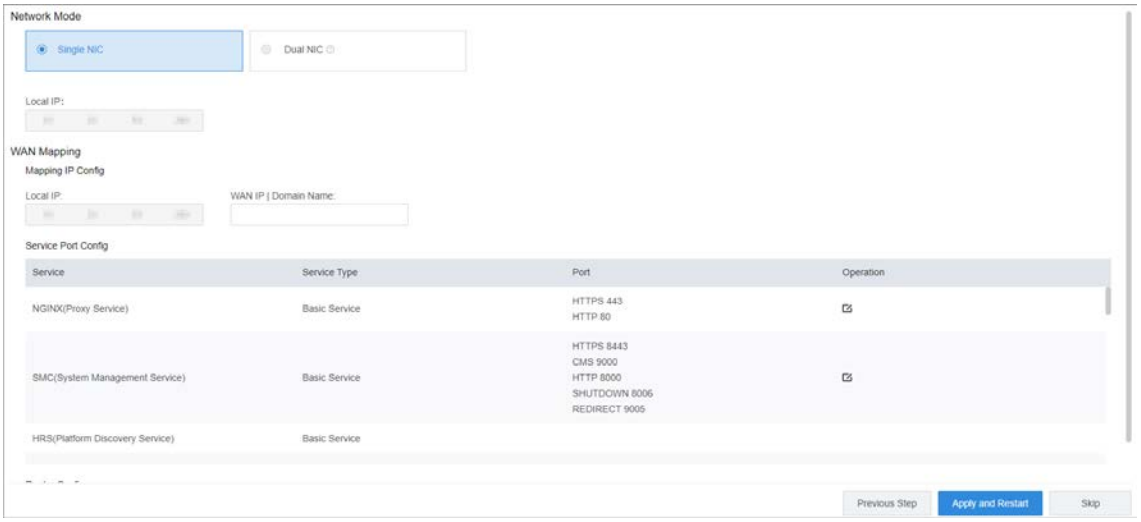
1.9 Sub server cannot be online

V8 will check the version when you register sub servers to avoid potential problems. If their versions are not the same, you cannot register them.

1.10 How do I configure LAN and WAN mapping?

Step 1 Log in to the configuration system.

Step 2 Select **Quick Guide** > **Network Mode**, and then enter the IP address or domain name to which you want to map the IP address of the platform.



Step 3 In the **Service Port Config** section, change the port numbers that might be in conflict.

If there is no conflict, skip this step.

Step 4 On the router, map the port numbers on the configuration system to the ones of the IP addresses you are mapping the platform to. The port numbers must be consistent.

If there is one or more sub servers, the port numbers on these sub servers must not be the same as those on the main server.

2 Product Update

2.1 What should I know when upgrading from V1.X to latest version?

You need to update the platform to V8.0.2 first, and then update from V8.0.2 to the latest version. For details, see the update guide.

2.2 Why do certain menus disappear after upgrade?

The menus will change with the new functions we added to each upgrade.

3 Device Management

3.1 Add device manually when no device is found in the automatic discovery devices

The automatic search function is realized by UDP multicast, and the IP segment search function is realized by UDP unicast. If UDP group/unicast messages between platforms and devices are unreachable, devices cannot be discovered.

3.2 Failed to add device

- Device connection failed.
- The device account number, password, port information was entered incorrectly.

3.3 Device is offline when network is working

Check that your device's login account, password, and port are correct.

3.4 The functions displayed in the smart plug-in on the device configuration page is inconsistent with the device

The smart plug-in is independently developed for device configuration. Considering the compatibility and upgrade of the device, the functions displayed might be different from the device.

3.5 When adding ONVIF devices, the device information cannot be obtained automatically

Only information of devices added through Dahua protocol can be automatically obtained. For devices added through other protocols, you need to manually edit and add device information.

3.6 When no channel of a multi-channel device added through ONVIF is online, the device displays as offline on the platform

For a multi-channel device added to the platform through ONVIF, when none of its channels is online, the device cannot be logged into and displays offline. For example, when a NVR added through ONVIF has no channel online, the NVR displays as offline on the platform.

4 User Management

4.1 Failed to add Super Admin

Only the system account can create users for Super Admin account.

4.2 Failed to give permissions such as storage management and service management to newly created role

Role permissions are arranged in a more refined way. Super administrator, administrator and custom role have different menu rights; Among them, the custom role does not have storage management and service management rights.

4.3 Corresponding relationship between roles and permissions when users have multiple roles

When having more than one role, users have permissions of all the roles. For example, role 1 has playback permission and video viewing permission for device 1, and role 2 has video intercom and video locking permission for device 2. When users have the permission of both Role 1 and Role 2, they will have the permission for playback, visual intercom, video viewing of Device 1, and video locking of Device 2.

4.4 Failed to import domain users

To import domain users, you need to configure the active directory first. The configuration path is: **Home > Configuration > System Parameters> Active Directory**.

5 Backup and Restore

5.1 Database did not work when the server is abnormally powered off during backup and restore

To ensure the stable power supply of the server, do not restart the server during backup and restore, If the database is abnormal, contact technical support to solve the problem.

5.2 Backup and restore take too long

Backup and restore are operations to save and restore data, which depends on the performance of database and disk I/O. The larger the amount of data, the longer it takes.

5.3 After restored successfully, the distributed service displays as "Starting"

The distributed service is disabled after restoration and needs to be configured manually. Start distributed service in **System Config** > **System Deployment** > **Distributed Config**.

6 Live Video

6.1 Situation for video to use video sub stream

Enter local configuration page of client, select **Video** and then you can configure Stream Type stream according to window split. Default 9 splits, the main stream is enabled by default when it is 9 splits or less, and sub stream is enabled by default when it is more than 9 splits.

6.2 Failed to get live video

- LAN/WAN mapping configuration is incorrect. Generally, the device is online but it fails to request stream.
- Forwarding server trouble. Generally, it happens when forwarding is under great pressure or forwarding server offline.
- Device trouble. The device login info is possibly tampered or login user has reached upper limit.

You can contact technical support for help when it fails to request stream.

6.3 Live video does not play smoothly

The main reasons are shown as follows:

- Video stream does not meet the requirements of the decoder in poor network connection.
- The actual video stream being forwarded exceed the forwarding performance of the server. For example, the forwarding performance of one server is 700 Mbps, but the actual video stream to be forwarded is larger than 700 Mbps.
- The server uses a 100 Mbps network cable, but the actual video stream to be forwarded is larger 100 Mbps.
- The CPU or memory of the decoder is not enough to decode the video stream to be forwarded.
- The encoder cannot encode in time the video stream to be forwarded.

If live video does not play smoothly, contact technical support for help.

6.4 Notes for GPU decoding

- Intel 3 generation with NVIDIA GTX750 or higher is recommended to avoid blurry screen.
- AMD graphics cards are not recommended, because the measured performance is weak.
- The graphics driver needs to be matched, otherwise it is easy to cause the crash of the client.

7 PTZ Operation

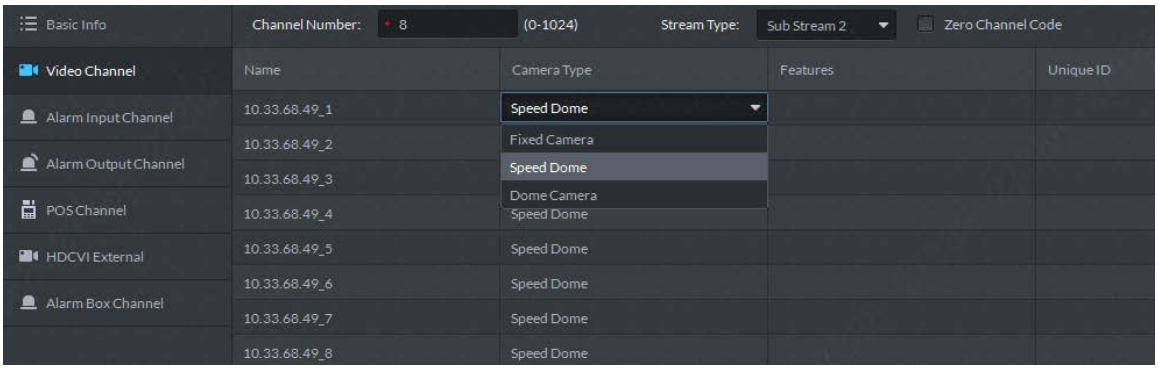
7.1 Failed to operate PTZ when icon displays the PTZ camera

The video channel might be locked by user with higher PTZ permission.

Contact technical support for help when the PTZ is out of control.

7.2 Failed to operated PTZ when PTZ camera is added

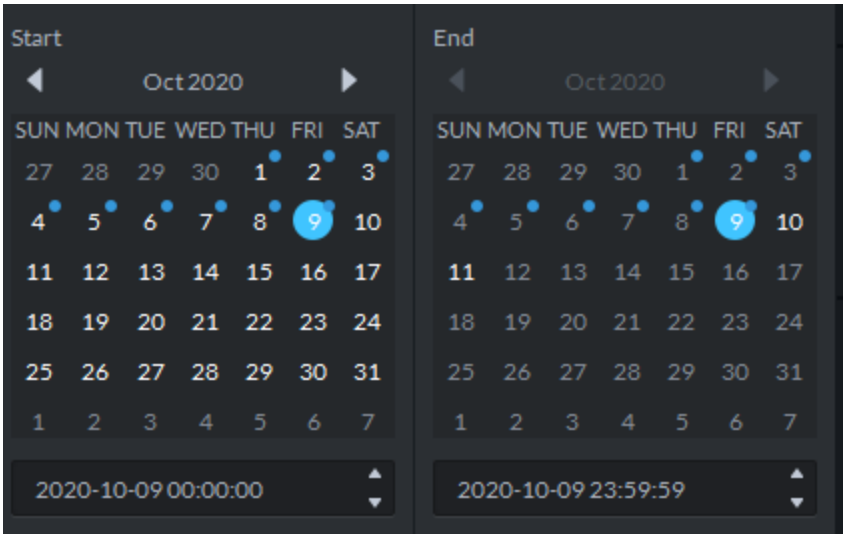
The operating video channel has PTZ function, but it is not enabled in device manager configuration; you need to select the **Speed Dome** as shown in the following figure.



8 Recording Playback

8.1 Recording icon does not show on the calendar tab when there is a device recording

To make it convenient to search video, we marked the date with video on the calendar; But sometimes it fails to mark because the device fails to support the protocol. In addition, Hik and ONVIF devices do not have such function at present.



8.2 Failed to query video when there is a video on the video channel

- If it selects the video on the recorder, then it needs to make sure the recorder is online and there is video within the period.
- If it selects the video on the server, then it needs to make sure there is video on the server within the period.
- Storage service fails. Storage service is the background process which supports video query. It needs to make storage service normal to realize video query;

Contact technical support for help when it fails to query video in other situations.

8.3 Failed to playback video

- Storage plan is not implemented upon the corresponding storage target, and it causes no video;
- Storage service fails. Storage service is the background process which supports video query. It needs to make storage service normal to realize video query;

- Device login parameter is tampered. If device login info is tampered while it is not updated in DSS, it will cause playback failure;
- Network trouble. It also causes playback failure when network malfunction happens;
- Contact technical support for help when it fails to query video in other situations.

8.4 Video record does not display on the time progress bar when playing video

Generally, it is because the video stream time is not in accordance with actual time. The actual stream time shall be in accordance with storage target (maybe recorder or storage server) to guarantee the time is correct. Use device timing function to make front-end device time in accordance with DSS server time.

8.5 Failed to play backwards

Generally, it fails to play backwards because the device backwards protocol is not in accordance with the platform; Currently the platform mainly realizes playing backwards upon new devices.

Besides, neither ONVIF nor Hik device can realize the function of playing backwards.

8.6 Error exists in video channel recording during sync playback

The error of sync playback is mainly because the time sequence of each channel is different, the error becomes more obvious as time accumulates to some degree. Currently it is modified during playback and makes it synchronous visually.

8.7 Failed to download video

The possible causes other than the ones indicated by the platform are shown as follows:

- The partition where the target folder is located is already full.
- Write access of target folder is unavailable. For example, it uses general user to log in the operating system with high security level.

8.8 The reason why the effect is not achieved when the video is played at high speed

- Poor read/write performance.

- The network bandwidth is limited. For example, if the 8 Mbps code stream is played at 64x speed, 512 Mbps bandwidth is required.

8.9 Why there was no video for a particular period even if I had configured a network disk?

The platform might be reduced to only "Read" permission for the network disk if the network disk reconnects to the platform after experiencing a power outage or network disconnection. In this case, you need to delete the network disk and add it to the platform again.

9 Operation & Maintenance Center

9.1 Statistical information such as CPU and network of the operation and maintenance center is inconsistent with the display of the server resource manager

The shortest statistical sampling period of the dashboard in operation and maintenance center is 1 min, which is not the real-time data. There are also some differences between the specific statistical algorithm of operation and maintenance center and resource manager.

9.2 Why did the numbers of device faults on Overview and Fault not match?

The numbers of device faults on the lower-right corner of Overview only include devices, but the numbers on Fault include both devices and channels.

9.3 After restarting the server, the scheduled update plan is carried out five minutes later than the defined time

After the server restarts, all devices need to log in to the platform again. To prevent update failure caused by devices being offline, the plan will be executed 5 minutes later.

10 Video Wall

10.1 Channels prompt "Cross device decode-to-wall is not supported" when binding video sources

Local signal of the display and control device support the display on wall after the video source binding operation in the device.

10.2 Live video on wall failed in direct decoder connection mode

In direct decoder connection mode, the display and control device will log directly into the video source-owned device to pull the stream decoding on the wall. You need to check whether the video source-owned device allowlist configuration contains the display and control device.

Display and control devices added through domain name do not support direction connection mode.

10.3 Priority of live video on wall, playback on wall, and alarm linkage on wall

Priority from high to low: live video on wall, alarm linkage on wall, and playback on wall.

10.4 Window list is null when the display and control device channel is selected for playback on the wall

Open window or split corresponding TV wall channel after selecting the corresponding TV wall channel on the client TV wall module or the video control device web manager, and then playback on the wall.

12.5 Sometimes video on wall fails

This might occur with matrix devices. The platform adds video walls through the matrix, and the number of video walls stored in the matrix device might have reached the maximum value. You need to log in to the device web manager, delete the useless video wall in the video wall management page, and finally save the video wall to be used on the platform.

11 Map

11.1 GIS map opened on client is blank

The common failure to open a map is found in vector maps. The main reason is that the computer network where the control client is located cannot access the Google Maps link. If it is offline maps, it is possible that the offline data is not imported.

For other reasons, contact technical support.

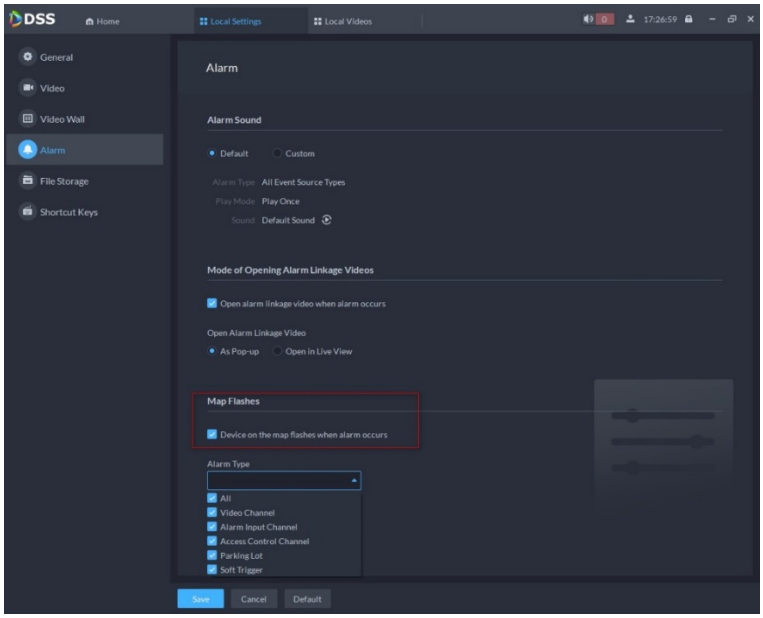
11.2 Alarm is configured, but cannot flash on the electronic map when alarm is generated

You need to turn on map flashing function on client local configuration and select alarm types. The steps are as follows:

Step 1 Configure the early alarm scheme at the administrator.

Step 2 Open the **Map**, and place the device or channel in the correct location on the map. You can refer to **How to configure a raster map**.

Step 3 Enter client local configuration, and find the following configuration options and select all the alarm types.



12 Face Recognition

12.1 Face recognition camera is added, but cannot be displayed in face recognition business

In Resources module of basic configuration on the client, you need to check whether the corresponding Face Recognition Feature is selected in Features.

12.2 Face recognition module at live view page does not display real-time snapshots

In the Storage module of basic configuration on the client, check whether the disk that stores images and files is configured on the distributed disk of the face recognition device.

If the picture storage disk has been configured, but still does not display real-time snapshots, you can log in to the web manager to check whether the operation of device is normal.

12.3 There are multiple face recognition devices, but some devices do not support search face by image

The platform distinguishes the method of searching face by image according to the capabilities provided by the device program version. If multiple devices have different capabilities, the one with an older program version will not be able results of searching face by image. We recommend updating the device program version.

12.4 The model and version of all IVSS devices should be the same in the environment

For IVSS devices, there are two versions of search by image:

- The image is sent to the device for search, and the device returns matching data;
- The image is sent to the device to extract the features, and the platform searches the records according to the features.

The two are mutually exclusive. You can only use either one at the same time.

12.5 How do I enable face recognition function on face recognition devices?

- AI by recorders: Log in to the web of the device, and then enable face recognition of a channels on **Event**.
- AI by cameras: You can login in to the web client, and enable the face recognition function.

12.6 Why were certain devices under the device tree displayed as devices, but some as channels when arming faces?

The platform automatically identifies devices according to AI by recorders and devices of AI by cameras. Devices of AI by recorders are displayed as channels, and devices of AI by cameras are displayed as devices.

12.7 Why were an IVSS not displayed in the device tree when I used the search by image function, but the device could upload face capture records to the platform?

If the IVSS supports face recognition, you can perform search by image on it. But an IVSS can also upload face capture records from IPCs when it does not support the function. For the second case, you cannot perform the search by image function on the IVSS, and therefore it will not be displayed in the device tree.

13 Video Metadata

13.1 Video metadata camera is added, but cannot be displayed in Video metadata business flow

In Resources module of basic configuration on the client, check whether Video Metadata is selected in Video Metadata Features.

13.2 Live video metadata module does not show real-time snapshots

In Storage module of basic configuration on the client, check whether the disk that stores images and files is configured on the distributed disk of the video metadata device.

If the picture storage disk has been configured, but still does not display real-time snapshots, you can log in to the web manager to check whether the operation of device is normal.

14 Access Control

14.1 Method to distribute room numbers to the VTO device

Basic information of staff includes the room numbers which shall be filled following the Enable status of buildings and units in the residential block settings; make sure the VTO devices and the platform are consistent in enabling buildings and units; when choosing authorization via the VTO devices, the room numbers are distributed to VTO devices.

14.2 Cannot use the configured password to directly open the door

The platform supports 2 types of passwords: unlock password and card, and personnel password. For the first generation of access control devices, after setting unlock password, you can open the door directly with the password. The first generation of access control devices use card password and need to set up the card+password method for opening the door, with the involvement of the card; people can use the configured password to directly open the door in the case of the second generation of access control.

14.3 Failed to distributing three fingerprints to devices

Different access control devices have different fingerprint capacities. Some only allow 2 fingerprints, and thus prompt failure when trying to distribute 3.

14.4 Batch distribution of cards to operating staff overrides their card information

The batch card distribution logic of the platform is about updating and replacing all card numbers.

14.5 Multi-door interlock set up for the integrated controller does not take effect

In addition to setting up the multi-door interlock rule, the integrated controller also needs to select the multi-door interlock mechanism in door settings to make this happen.

14.6 The access control device cannot open the door through face recognition, and the device cannot respond

There are several situations:

- The face algorithm license of the device expires.
- Check whether unlock by face recognition is enabled.
- If the methods above failed, try to restore the device to factory settings.

14.7 A person has 5 access cards, but only 1 card can open the door

The first-generation access control devices only support 1 card (main card); the second-generation access control and VTO devices support 5 cards.

14.8 Person's information is sent to the second-generation access control device and is added to the multi-card unlock group, but the platform prompts that some person do not have the access control channel permission when adding multi-card unlock configuration

There is no authority of the person to unlock the door (card, password, fingerprint, face) is sent to the second-generation access control device. However, to configure multi-cards unlock, the person must have one of the permissions of card, password, fingerprint, and face.

14.9 The holiday plan is sent successfully, and the corresponding configuration can be seen on the device, but the holiday permission is incorrect

Check whether it is a sub server. The time zone and time of the central server and the sub server must be consistent; otherwise the sent holiday time might be incorrect and thus the platform prompts incorrect permissions.

14.10 The remote verification does not work after the permissions are sent and the remote verification is configured

Check whether the access type of the person is VIP. VIP can unlock the door without verification.

14.11 Failed to unlock the door with the public password

Check whether the public password function is enabled in the **Door Config** page. If it is not enabled, the public password cannot be sent.

14.12 The main control console does not report remote door opening events after clicking 

Check whether the device supports reporting remote door opening events. For example, ASI-1212D does not support reporting remote door opening events.

15 Visitor

15.1 The "Authorization" tab is not displayed when adding appointed visitors

The **Authorization** tab is displayed only when the automatic visit function is enabled in **Visitor Config** page.

15.2 Failed to unlock the door with the pass and the device prompts illegal card

Only one decryption message is kept in the device. If the device is added to multiple platforms, the decryption message of the QR code will be overwritten, and thus the access control device will be not able to identify the card information of the pass.

15.3 Failed to unlock the door when using the pass and the device prompts wrong validity period

- Without time synchronization, there is a big time difference between the VTO and the server.
- The device is added to multiple platforms with different time zones.

15.4 No email notification when a visitor arrives or leaves

- The mailbox server is not configured, or the mailbox server is unavailable.
- The email template function is not enabled.
- The email information is not added.

15.5 Video intercom devices and entrance & exit points are not displayed during visitor appointment and registration

The video intercom device is displayed only when the room number is added. The entrance & exit points are displayed only when the plate number is added.

15.6 The language of the email template in "Visitor Config" page is different from that of the client

For first-time use, the language of the email template is the same as that of the client, and it will not be changed when you switch the language of the client.

15.7 The "Sign out regularly" function does not work after the defined daily sign-out time has come

This results from the different time of the client and the server. The regular sign-out is carried out only when the server time meets the defined time.

15.8 Failed to trigger automatic visit and leave when a plate number was sent to devices at entrance and exit, and was successfully recognized

Check whether the devices at the entrance and exit are selected in the automatic visit and leave configuration.

15.9 Why did the visitor fail to receive an appointment email after I enabled the email template for visitor appointment and entered an email address when I added an appointment?

Make sure that a visitor pass has been generated for the visitor. Otherwise, the platform will not send an email to the visitor.

16 Video Call

16.1 Method to quickly add video intercom device

Use the template of the video intercom export excel in the platform to import devices in batches

16.2 "Mismatch of building number or unit number" prompts when an added video intercom goes offline?

To keep a DSS added device online, the device must be consistent with the residential block settings of the platform. If the device has enabled buildings and units, the platform must do the same. So when this problem comes up, check if the Enable status of the buildings and units are the same as the platform.

Go to homepage-> Config->Video Intercom ->Residential Block Settings to do the setup.

16.3 After adding VTO and VTH online, there is only VTO generated automatically in the device group, and VTO and VTH are disconnected

Check whetherthe room number configured for VTH contains an extension number or whether the extension number is correct. In order to automatically generate the device group link, the extension number configured for VTH should be 0~99 according to the SIP white paper rules.

16.4 Failed to call management center when video intercom device is online, and VTO and VTH can call each other

- The correlation between the device group and management group is incorrectly bound.
- Check whether your account is reused. System account can be reused, which can put the call management center in an abnormal status. In light of this, login with a non-system account is recommended at this stage.
- The center number at the device terminal should be 888888. Check if this is followed.

16.5 Device status of a video intercom device is different from the SIP status

The two status are different in connotation and inconsistency may exist.

Device offline and SIP online:

- If the device is offline due to power failure or network disconnection, the status is inconsistent only temporarily and the SIP will be offline in some time. If the device is offline because the building and unit function is not consistent among VTO devices, it displays as device offline and SIP online.
- Device online and SIP offline: Check whether the IP address and port of SIP is correct.
- For normal use, please make sure that the both the video intercom device and SIP is online.

16.6 Private password was sent successfully but failed to unlock the door on VTO

Private password is bound to Contacts. Send Contacts before sending private password.

16.7 The SIP ID of video call app users is identical with the called number of the VTH

This is because the VTH is not configured with an extension number #0.

Change the called number of the VTH and register app users again.

16.8 The VTO only reports the access control event but not the door status when you click 

The VTO is unable to report the door status if there is no door sensor on the door.

16.9 The short number of the VTH cannot be identical with that of the fence station

The platform cannot tell whether to call the VTH or the fence station if the short number of the two are the same.

16.10 Why do I need to delete and add the two intercom devices after I swapped their call numbers?

After you swap their call numbers with each other, the platform will consider call numbers have been repeated in the same call group, so you cannot call them. Deleting and adding them to the platform again will solve this problem.

17 Parking Lot

17.1 Parking site is bound with checkpoint devices, but system always prompt lifting failure when a car passes

Log in to the web manager of the checkpoint devices and check whether the barrier connected is enabled.

17.2 Vehicles in blocklist can be recognized and allowed to pass

- Check whether the vehicle blacklist has expired.
- Check the parking lot permission settings of the vehicle.

17.3 Video recordings are viewed via the card, but there is no recording at return

The established procedure of querying videos is to query those of the platform. If no results are returned, try the device recordings. If the system prompts that no recordings are found, check if the platform has set up a recording plan for the target device; if no, check if the checkpoint devices have storage cards and have been set up with a recording plan, and whether the storage device (NVR) connected to the checkpoint has set up a recording plan for the checkpoint channel;

Besides, the system clock must be in perfect sync across the device-platform-client; otherwise it risks returning nothing to recording searches.

17.4 Card of passing vehicle records have no pictures in license plate recognition

Check whether the platform has set up the disk that stores images and files.

17.5 Platform can send vehicles in allowlist to the checkpoint devices, but cannot appoint an NVR channel for the distribution

NVR can be bound with different types of device, such as ITC and IPC. The platform does not know the exact type, and thus cannot distribute through an appointed channel. Instead, the distribution is based on device and completed through all channels. In other words, NVR can automatically distribute blocklist and allowlist to all connected ITC platforms.

17.6 The platform distributes the allowlist to the NVR device, but occasionally the platform prompts a successful distribution, when the ITC allowlist does not include corresponding data.

When the platform distributes allowlist to NVR and NVR confirms a successful receipt, it only means allowlist is distributed to NVR. The NVR then auto syncs the allowlist to all connected ITCs. However, the NVR cannot guarantee successful sync across all ITCs. Possible causes include network connection problems or an ITC not supporting the sync.

17.7 The platform has added the video intercom device (entrance machine, unit entrance device), but parking site cannot be bound with the system

The video intercom device must be built with the access control channel before being bound to the parking site.

17.8 There is snapshot record, but no entrance or exit records

Check the entrance and exit rules of the parking lot. If the entrance and exit rules of the group to which the vehicle belongs are not configured correctly, the vehicle cannot enter and exit the parking lot. Therefore, only the snapshot record can be found.

17.9 Vehicles with a forced exit record cannot restored to the status of in the parking lot

If there is an updated entrance and exit record or forced exit record for the same plate number in the same parking lot, the older force exit record cannot be restored.

17.10 The entrance record shows that the vehicle has exited, but there is no corresponding exit record

If the entrance record is forced to exit, no exit record will be generated, and only the entrance record and forced exit record can be found.

17.11 When there is a record of passing vehicle at the entrance and exit, sometimes there is an entry or exit notification, but sometimes there is no notification

Only when the video playback of the channel is enabled on the video preview window, the entrance and exit notification of the channel can be displayed.

17.12 Why does the number of available parking space remain 0 after a vehicle exits the parking lot when parking space counting has been enabled?

Although available space is 0, vehicles can still enter the parking lot. The available space on the interface is 0, and the actual system records the negative parking space. When a vehicle exits, the negative parking space in the system starts to add 1. When the negative parking space becomes positive, the real parking space can be displayed on the interface, otherwise it will be 0.

18 Event Center

18.1 When the platform is connected to intranet and the ONVIF device is connected to the extranet, the alarm of the ONVIF device cannot be reported

The alarm principle of the ONVIF device is that the ONVIF device detects an alarm and pushes it to a certain IP and port of the platform through the push mode. However, the current ONVIF client sends the intranet IP to the ONVIF device, and the device cannot push it to the intranet address.

18.2 Intelligent alarm of ONVIF device cannot be reported

ONVIF database currently does not support pushing intelligent alarm. All intelligent alarm will be converted to other alarms (such as motion detection) and then reported to the platform. Therefore, the platform cannot receive intelligent alarm.

18.3 There is an alarm report, but no data can be found in the event statistics

Event statistics is based on the time zone of the server, and the alarm time displayed on the client is converted according to the time zone of the client.

18.4 Cannot receive real-time alarms, but can find historical alarms

Real-time alarms are only pushed to the linked users configured according to event, and only online linked users can receive real-time alarm.

18.5 No linked snapshot

Linked snapshot should be configured; the server of the device should have a disk to store images and files on storage interface; the device is online; the channel can normally pull the stream.

18.6 No linked video

Linked video should be configured; the server of the device should have a video disk or network disk on storage interface; the device is online; the channel can normally pull the stream.

18.7 When configuring the prerecord time of the linkage video, the platform prompts that the prerecord bandwidth is too large

In earlier versions, the prerecorded video is acquired from the device video, and then combined with the center recordings to synthesize a complete alarm linkage video.

In this version, platform acquires the stream in advance and stores the prerecorded video, which will occupy the bandwidth.

Do not exceed the bandwidth limit for prerecording. Otherwise, videos might be lost.

19 Intelligent Analysis

19.1 The calibration time of the people counting group is changed, but the real-time count remains unchanged

It will take effect when the new calibration time is reached. After the calibration time is changed, the previous calibration time will still be effective and the real-time data not affected before the new calibration time is reached.

19.2 Real-time count is different from historical count

The real-time number of people in the group equals to the number of people entered minus the number of people left, the latter two number are uploaded by devices. The number of people in the group can be changed manually, and when you do that, the changed data will not be synchronized to the devices. Also, the historical count data is not affected by time, while the real-time count is calculated within each calibration cycle.

19.3 The data searched by people counting group is different from data searched by channel

When you search for data from a channel, all historical data from this channel will be displayed, including the one generated by the people counting rules that have been deleted. When you search for data from a people counting group, only data from existing people counting rules will be displayed.

19.4 People counting has been enabled for the features of a channel, but the channel cannot be displayed under the resource tree of historical count or in-area number analysis

You also need to add people counting rules for the channel.

19.5 For historical people counting, the retention number in bar or line charts is different from that in report.

The retention number in bar or line chart for a period is the sum of the retention numbers of all the periods before it (for example, the retention number for 02:00 is the sum of 0:00-01:00 and 01:00-02:00), and that in the list is the number of retention for each period.

19.6 People counting group and the difference between by groups or resources when searching for historical people counting data

"People counting group" is a combination of the people counting rules from different devices. For example, you can add the people counting rules of all entrances and exits of a store to one people counting group to view the overall people flow of the store.

When searching for historical data by resources, you can view the data from all people counting rules of one or more channel.

19.7 When configuring send time, the date you configured does not exist in certain months. For example, if you configure the report to be sent on the 30th of each month, but the 30th does not exist in February

In this situation, the report is sent on the last day in February. For example, in February, the report is sent on February 28th (February 29th in the leap year), and in March, the report is sent on March 30th.

20 Message push when the App is not running

20.1 Messages that support message push when the app is not running on the phone

Alarms and video/voice calls.

20.2 Cannot receive messages when the app is not running

Possible reasons for message push failure when the server can connect to the third-party message push:

- No account ever logs in to the app.
- The event does not link the user.
- The alarm type is not subscribed on the app.
- The user log out of the app or the account is frozen. Users will need to log in to the app again after unfreezing the account before they can normally receive offline messages.

20.3 Only one phone receives offline messages when a user has logged in to the app in multiple phones

Check whether the user enabled SPOP (Single Point of Presence). If yes, only the last phone on which the user logged in to the app can receive offline message.

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