



DSS V8.100.0000001.0

FAQ



Foreword

General

This manual provides the answers to DSS questions during daily use.






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	
	DANGER
	WARNING
	CAUTION
	TIPS
	NOTE

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

Foreword	I
1 Installation and Deployment	9
1.1 Failed to install DSS	9
1.2 Failed to switch DSS hot standby.....	9
1.3 DSS is not working properly	9
1.4 After installing DSS, failed to get the installation package of DSS client.....	9
1.5 Changes DSS made to operating system.....	10
1.6 View if a distributed service is working properly in the case of distributed deployment	10
1.7 In the client installation directory, double-click update.exe, and the platform cannot be updated directly	12
1.8 The newly installed sub server always shows that it is starting.....	12
1.9 The time of each sub server is different.....	12
1.10 Sub server cannot be online.....	13
1.11 DSS platform restarts automatically.....	13
1.12 The Rose service process is lost on the server where antivirus software is installed	13
2 License Authorization	14
2.1 Computer can open the external network address, but DSS cannot be activated online	14
2.2 Use the same activation code on new server.....	14
2.3 Fail to import offline activation file	14
2.4 Using the original offline license activation file, failed to activate when reinstalling or deactivating DSS on the same server	14
3 Product Update	15
3.1 Notes for upgrading from DSS V7 to latest V8	15
3.2 Use the license of DSS V7 after upgrading to DSS V8.....	15
3.3 Menus disappear after upgrading	15
3.4 Changes of DSS data after upgrading.....	15
4 Device Management	16
4.1 Add device manually when no device is found in the automatic discovery devices.....	16
4.2 Failed to add device	16
4.3 Device is offline when network is working.....	16
4.4 The functions displayed in the smart plug-in on the device configuration interface is inconsistent with the device.....	16
4.5 When adding ONVIF devices, the device information cannot be obtained automatically	16
4.6 When no channel of a multi-channel device added through ONVIF is online, the device displays as offline on the platform.....	17
5 User Management	18
5.1 Failed to add Super Admin	18
5.2 Failed to give permissions such as storage management and service management to newly created role	18
5.3 Corresponding relationship between roles and permissions when users have multiple roles.....	18
5.4 Failed to import domain users.....	18
6 Storage Settings	19
6.1 Some hard drives can be turned on and some can't when using the server's hard drive for storage.....	19

6.2 Disk of the server failed to be formatted as storage disk.....	19
6.3 After operating the server disk successfully, operation failure will be prompted if I operate it again. ...	19
6.4 For Windows system, close the server's task manager to delete the network disk	19
6.5 After formatting a partition disk (Like E disk) to a video disk, Windows system still prompts to format the disk	20
6.6 Some disks (Like C disk) are not displayed in the local disk list	20
6.7 A few more disks (Like E disk and F disk) appear after adding a network disk to the platform	20
7 Backup and Restore.....	22
7.1 Database did not work when the server is abnormally powered off during backup and restore.....	22
7.2 Backup and restore take so long	22
7.3 After restored successfully, the distributed service displays as "Starting"	22
8 Live Video.....	23
8.1 Situation for video to use video sub stream	23
8.2 Failed to get live video	23
8.3 Live video does not play smoothly.....	23
8.4 Notes for GPU decoding.....	23
9 PTZ Operation.....	24
9.1 Failed to operate PTZ when icon displays the PTZ camera	24
9.2 Failed to operated PTZ when PTZ camera is added.....	24
10 Recording Playback.....	25
10.1 Recording icon does not show on the calendar tab when there is a device recording.....	25
10.2 Failed to query video when there is a video on the video channel.....	25
10.3 Failed to playback video	25
10.4 Video record does not display on the time progress bar when playing video	26
10.5 Failed to play backwards	26
10.6 Error exists in video channel recording during sync playback.....	26
10.7 Failed to download video.....	26
10.8 The reason why the effect is not achieved when the video is played at high speed.....	26
11 Operation & Maintenance Center.....	28
11.1 Statistical information such as CPU and network of the operation and maintenance center is inconsistent with the display of the server resource manager.....	28
11.2 On Device Status interface in Maintenance Center, the total number of abnormal devices is different from the count of devices of abnormal running status.....	28
11.3 When searching for faults of devices in organization A, faults of devices in organization B are displayed	28
11.4 The device fails to update after the defined update start time of the update plan	28
11.5 A immediate task has been created, and the list time is inconsistent with the client.....	29
11.6 After restarting the server, the scheduled update plan is carried out five minutes later than the defined time	29
12 Video Wall	30
12.1 Channels prompt "Cross device decode-to-wall is not supported" when binding video sources	30
12.2 Live video on wall failed in direct decoder connection mode	30
12.3 Priority of live video on wall, playback on wall, and alarm linkage on wall.....	30
12.4 Window list is null when the display and control device channel is selected for playback on the wall.....	30
12.5 Sometimes video on wall fails	30
13 Map	31

13.1 GIS map opened on client is blank	31
13.2 Alarm is configured, but cannot flash on the electronic map when alarm is generated	31
14 Face Recognition	32
14.1 Face recognition camera is added, but cannot be displayed in face recognition business	32
14.2 Face recognition module at live view interface does not display real-time snapshots	32
14.3 There are multiple face recognition devices, but some devices do not support search face by image	32
14.4 The model and version of all IVSS devices should be the same in the environment.....	32
14.5 How to enable face recognition function on face recognition devices	33
14.6 Why some devices under the device tree are displayed as devices, and others are displayed as channels when arming faces	33
15 Video Metadata	34
15.1 Video metadata camera is added, but cannot be displayed in Video metadata business flow	34
15.2 Live video metadata module does not show real-time snapshots.....	34
16 POS	35
16.1 Overlay POS information is not clearly displayed in live video	35
16.2 What is the unit for the money in the receipt?	35
16.3 What should I do when the POS information of more than one channel is displayed on the live video because the NVR and the POS device are bound to the same channel?	35
17 Access Control	37
17.1 Method to distribute room numbers to the VTO device	37
17.2 Cannot use the configured password to directly open the door	37
17.3 Failed to distributing three fingerprints to devices	37
17.4 Batch distribution of cards to operating staff overrides their card information.....	37
17.5 Multi-door interlock set up for the integrated controller does not take effect.....	37
17.6 The access control device cannot open the door through face recognition, and the device cannot respond.....	38
17.7 A person has 5 access cards, but only 1 card can open the door	38
17.8 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	38
17.9 The holiday plan is sent successfully, and the corresponding configuration can be seen on the device, but the holiday permission is incorrect	38
17.10 The remote verification does not work after the permissions are sent and the remote verification is configured	39
17.11 Failed to unlock the door with the public password	39
17.12 The main control console does not report remote door opening events after clicking 	39
18 Visitor	40
18.1 The "Authorization" tab is not displayed when adding appointed visitors	40
18.2 Failed to unlock the door with the pass and the device prompts illegal card.....	40
18.3 Failed to unlock the door when using the pass and the device prompts wrong validity period.....	40
18.4 No email notification when a visitor arrives or leaves	40
18.5 Video intercom devices and entrance & exit points are not displayed during visitor appointment and registration	40
18.6 The language of the email template in "Visitor Config" page is different from that of the client.....	41

18.7 The "Sign out regularly" function does not work after the defined daily sign-out time has come	41
18.8 Failed to trigger automatic visit and leave when the plate number is authorized to the corresponding entrance & exit points and has been successfully identified	41
19 Video Call	42
19.1 Method to quickly add video intercom device	42
19.2 "Mismatch of building number or unit number" prompts when an added video intercom goes offline?	42
19.3 After adding VTO and VTH online, there is only VTO generated automatically in the device group, and VTO and VTH are disconnected	42
19.4 Failed to call management center when video intercom device is online, and VTO and VTH can call each other	42
19.5 Device status of a video intercom device is different from the SIP status.....	43
19.6 Private password was sent successfully but failed to unlock the door on VTO.....	43
19.7 The SIP ID of video call app users is identical with the called number of the VTH	43
19.8 The VTO only reports the access control event but not the door status when you click 	43
19.9 The short number of the VTH cannot be identical with that of the fence station	43
19.10 Why do I need to delete and add the two intercom devices after I swapped their call numbers?	44
20 Entrance and Exit.....	45
20.1 Parking site is bound with checkpoint devices, but system always prompt lifting failure when a car passes	45
20.2 Vehicles in blocklist can be automatically recognized and released	45
20.3 Video recordings are viewed via the card, but there is no recording at return	45
20.4 Card of passing vehicle records have no pictures in license plate recognition.....	45
20.5 Platform can distribute vehicles in allowlist to the checkpoint devices, but cannot appoint an NVR channel for the distribution	46
20.6 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.	46
20.7 The platform has added the video intercom device (entrance machine, unit entrance device), but parking site cannot be bound with the system.....	46
20.8 There is snapshot record, but no entrance or exit records.....	46
20.9 Vehicles with a forced exit record cannot restored to the status of in the parking lot.....	47
20.10 The entrance record shows that the vehicle has exited, but there is no corresponding exit record..	47
20.11 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	47
20.12 The available space detection is configured in the parking lot. After a vehicle exits, the available space is still 0	47
21 Attendance	48
21.1 Check-in or check-out time is one minute more than the swiping time.....	48
21.2 Failed to see the shift of staff groups	48
21.3 The additional staff are not assigned to any shift plan, but why is it displayed in a shift?.....	48
21.4 Failed to query the attendance card swiping record of the staff.....	48
21.5 Failed to query the attendance report of the staff.....	48
21.6 Failed to query the abnormal attendance record of the staff.....	49
21.7 One card swipe produces two records	49
21.8 Records of the attendance report such as the card swiping records cannot be fully exported	49

21.9 Attendance reports are not generated after synchronizing offline records	49
22 Case Bank.....	50
22.1 After saving a case, the case image cannot be viewed on the case interface	50
23 Event Center	51
23.1 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.....	51
23.2 Intelligent alarm of ONVIF device cannot be reported	51
23.3 There is an alarm report, but no data can be found in the event statistics.....	51
23.4 Cannot receive real-time alarms, but can find historical alarms.....	51
23.5 No linked snapshot	51
23.6 No linked video	52
23.7 When configuring the prerecord time of the linkage video, the platform prompts that the prerecord bandwidth is too large.....	52
24 Cascade	53
24.1 Cascade function	53
24.2 Devices that support cascading.....	53
25 Intelligent Analysis.....	54
25.1 The calibration time of the people counting group is changed, but the real-time count remains unchanged	54
25.2 Real-time count is different from historical count	54
25.3 The data searched by people counting group is different from data searched by channel	54
25.4 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	54
25.5 For historical people counting, the retention number in bar or line charts is different from that in report.	55
25.6 People counting group and the difference between by groups or resources when searching for historical people counting data	55
25.7 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 30 th of each month, but the 30 th does not exist in February	55
26 Synthesis.....	56
26.1 What is a bridge and what does it do.....	56
26.2 The types of database and business data that are supported when synchronizing data to third-party databases.....	56
26.3 Failed to synchronize the attendance report after being updated to V8.1.0.....	56
26.4 Data repetition occurs in the third-party database after system updating and data synchronization	56
27 Message push when the app is not running.....	57
27.1 Messages that support message push when the app is not running on the phone.....	57
27.2 Cannot receive messages when the app is not running.....	57
27.3 Only one phone receives offline messages when a user has logged in to the app in multiple phones	57
28 Center storage for hot standby	58
28.1 What is hot standby	58
28.2 Local hard disks cannot be formatted as video disk	58
28.3 The drive letter and number of drives of the two servers must be consistent for storage of images and incident files in hot standby.....	58

28.4 The main and sub server need to add different users of the EVS when it is used as image and files disks	58
28.5 In hot standby, main servers can add different EVS users, but the sub servers from distributed deployment can add only one user	59
28.6 Certain pictures and videos are lost after one server takes over the other one in hot standby	59
28.7 A prompt says mount point change/loss on the hot standby software	59
29 Independent Database Deployment	61
29.1 Failed to enable independent database deployment	61
29.2 Data that can be stored in the independent database. Will the data stored in the independent database also be stored in local disks	61
29.3 The independent database cannot be queried after it is restored to operation	61
29.4 After the independent database deployment is closed, can the data previously stored in the independent database be queried	61
29.5 Will the data be lost after disabling the independent database	61
30 MPT File Retrieval	62
30.1 After the MPT device is added and the file retrieval plan is configured, file retrieval is not performed in time	62
30.2 File retrieval failed when the MPT device is normal and the retrieval plan correctly configured	62
30.3 The time in the list of MPT record retrieval is inconsistent with the time in pictures and videos	62
30.4 After the MPT device is successfully added, the device suddenly goes offline, or offline and then online	62
31 Alarm Controller	63
31.1 When will force arming alarm controller fail	63
31.2 Cancel alarm for wired zones	63
31.3 Bypass the wired zone when the alarm controller is under arming	63
32 Virus Scan	64
32.1 Anti-virus software prompts "an exe program or dll library contains virus" when installing a program	64
33 NPT	65
33.1 NTP time synchronization does not work	65

1 Installation and Deployment

1.1 Failed to install DSS

- Check whether the server has installed a different version of DSS.
- Check whether the server's available memory meets the minimum requirements for installation, with at least 1.5G of the remaining available.
- Check whether the operating system is Windows 7 or Windows Server 2008 (R2). DSS services are no longer available on the two operating systems.

1.2 Failed to switch DSS hot standby

- The forced start of the hot standby might cause the switch failure.
- Occasional problems of hot standby occur because data copying is incomplete.
- When you need to use the hot standby, contact technical support to build environment. Contact technical support to recover when there are any problems.

1.3 DSS is not working properly

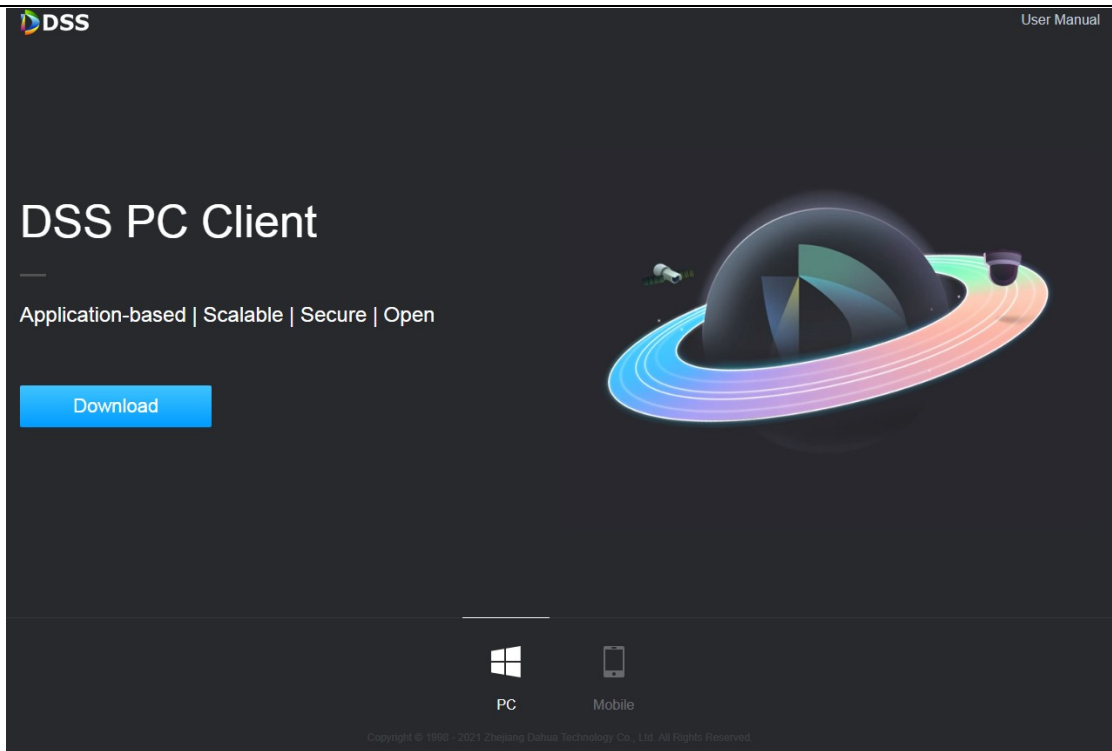
DSS failure to work properly might result from the service failure. Check the service configuration tool to see if the service is working properly.

1.4 After installing DSS, failed to get the installation package of DSS client

DSS Control Client provides desktop client program for DSS Express business operation. The installation steps are shown as follows:

Step 1 Open browser and enter IP address of the platform.

Step 2 Click Download.



Step 3 Save the file to PC.

1.5 Changes DSS made to operating system

- Install DSS file under the installation directory.
- Add program start menu and desktop shortcut.
- Configure the firewall needed by DSS.
- Configure local security policy.
- Add Windows service named as DSS Service.

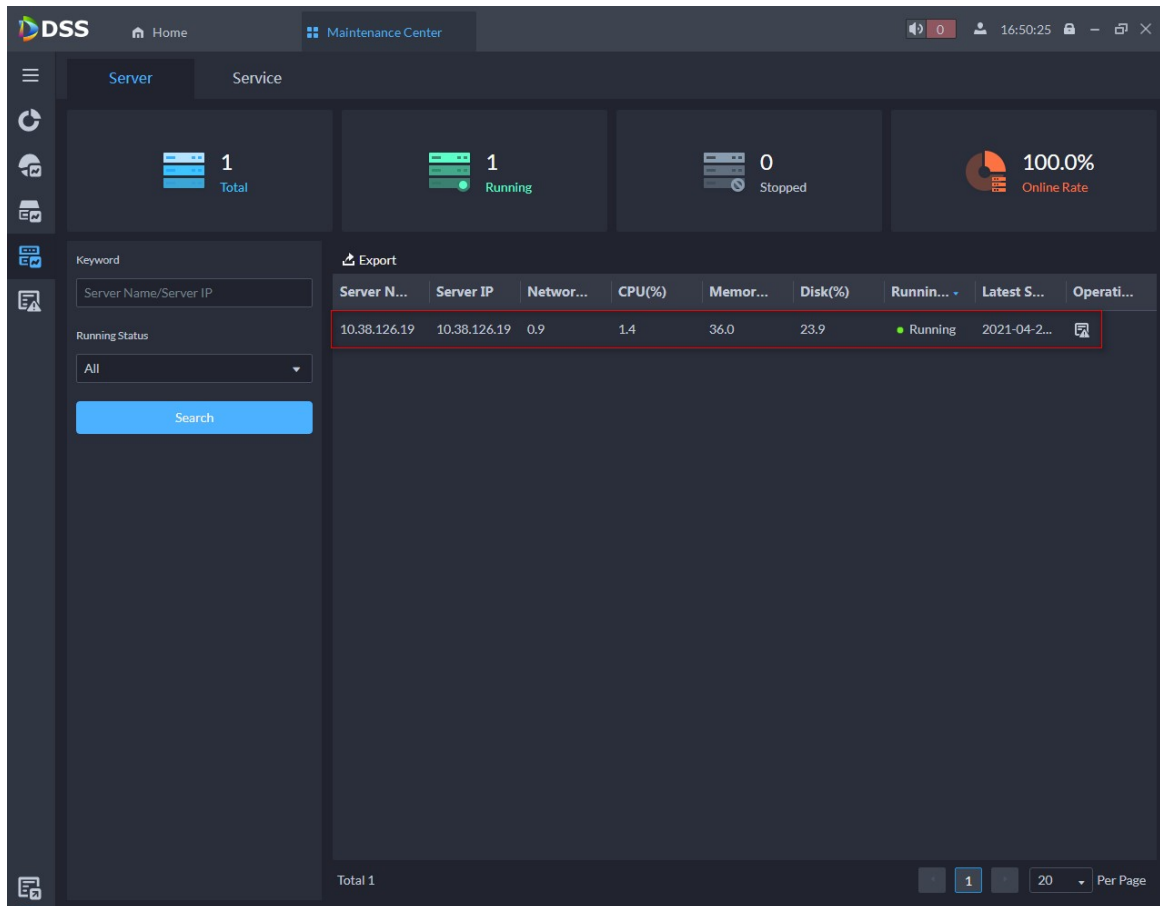
1.6 View if a distributed service is working properly in the case of distributed deployment

The server registration and running status need to be viewed on the administrator of the main server. The specific view path is: Main server client— operation and maintenance (O&M) Center. See the following steps:

Step 1 Login as main server client, and enter the O&M Center. You can see the number and status of all services in the Overview module, as shown in the following figure.



Step 2 Click service status module to view the service details, as shown in the figure below.



Step 3 Click service submodule to see the service details of this server, as shown in the figure below.

Service Name	Service Type	Running Se...	Running Se...	Running St...	Latest Statu...	Operation
DMS(400301)	DMS	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
PTS(1300301)	PTS	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
MCDRADAR(49...	MCDRADAR	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
PES(1100301)	PES	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
ACDG(11300301)	ACDG	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
MTS(200301)	MTS	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
ARS(800301)	ARS	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
ADS(1600301)	ADS	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
MCDLED(33003...	MCDLED	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
MCDALARM(31...	MCDALARM	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
SS(100301)	SS	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
PCPS(900301)	PCPS	10.38.126.18	10.38.126.18	Running	2021-04-27 11:...	
ADS(1600101)	ADS	10.38.126.19	10.38.126.19	Running	2021-04-27 11:...	
DMS(400101)	DMS	10.38.126.19	10.38.126.19	Running	2021-04-27 11:...	
SWITCHCENTE...	SWITCHCENTER	10.38.126.19	10.38.126.19	Running	2021-04-27 13:...	

1.7 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.

1.8 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 interface 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.

1.9 The time of each sub server is different

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

1.10 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.

1.11 DSS platform restarts automatically

- PC time is adjusted for more than 30 minutes.
- Tomcat runs out of memory. If this happens, a dump file will be generated on drive C by default, and then the platform restarts automatically.

1.12 The Rose service process is lost on the server where antivirus software is installed

The system driver will be installed when installing the Rose software. If the anti-virus software has been installed on the server, you need to add the bin directory under the Rose installation folder to the antivirus software allowlist.

2 License Authorization

2.1 Computer can open the external network address, but DSS cannot be activated online

Online activation requires the server to have access to the license activation address.

2.2 Use the same activation code on new server

To replace a server, you need to deactivate the original server first, and then activate it on the new server.

2.3 Fail to import offline activation file

- Make sure that the offline activation file is correct;
- View the failure reasons.

2.4 Using the original offline license activation file, failed to activate when reinstalling or deactivating DSS on the same server

To reinstall or deactivate DSS, reactivate the DSS by using the original activation code. The original activation file cannot be used directly.

3 Product Update

3.1 Notes for upgrading from DSS V7 to latest V8

When updating from DSS V7 to V8, you need to update it to V8.0.2 first, and then to the latest version according to the update strategies of V8. For details, see the corresponding update guide.

3.2 Use the license of DSS V7 after upgrading to DSS V8

You cannot use the V7 license on V8, but you can use it to apply for a new license.

3.3 Menus disappear after upgrading

The menu varies with versions. Please refer to the upgraded menu.

3.4 Changes of DSS data after upgrading

Most of data does not change after the upgrade, and some data does not support the upgrade. For details, see product upgrade instruction manual.

4 Device Management

4.1 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.

4.2 Failed to add device

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

4.3 Device is offline when network is working

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

4.4 The functions displayed in the smart plug-in on the device configuration interface 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.

4.5 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.

4.6 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.

5 User Management

5.1 Failed to add Super Admin

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

5.2 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.

5.3 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.

5.4 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.

6 Storage Settings

6.1 Some hard drives can be turned on and some can't when using the server's hard drive for storage

Different types of storage disks have different formats and different access rights to windows. The formats of video/bayonet picture disks are CQFS, which cannot be opened by ordinary users. The formats of face/alarm picture and evidence file disks are NTFS managed by OSS service, which can be accessed by ordinary windows users.

6.2 Disk of the server failed to be formatted as storage disk

If the system/DSS service configuration file is overwritten or the disk is full, the system /DSS service will not work normally, so neither the system disk of the server nor the DSS service installation disk can be formatted as a storage disk.

6.3 After operating the server disk successfully, operation failure will be prompted if I operate it again.

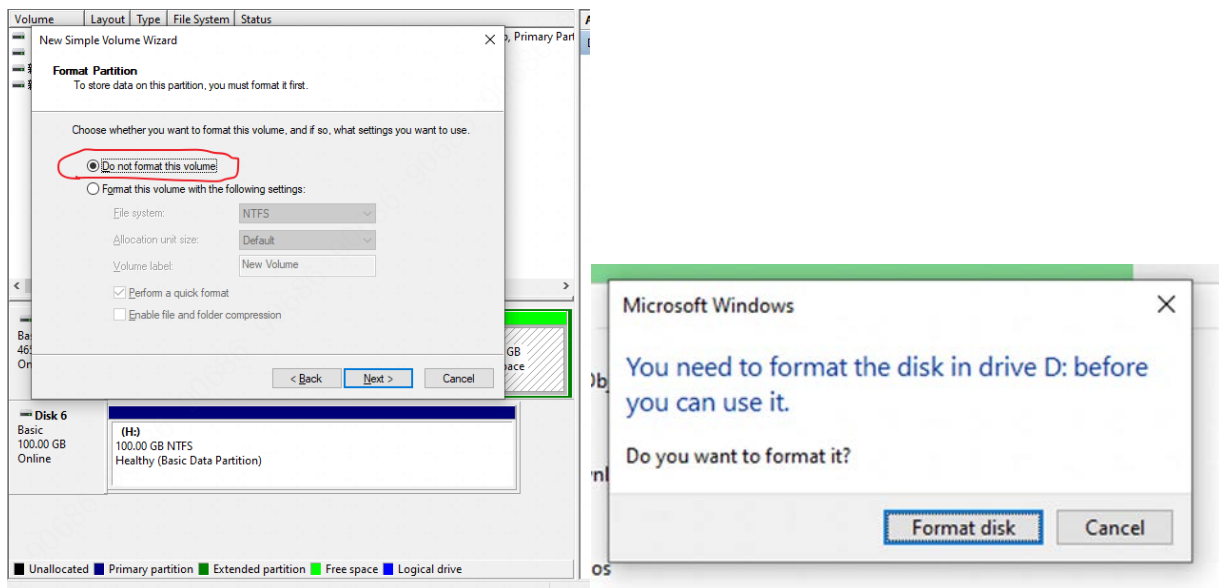
After operating the disk, the disk-related services (such as SS and PTS) will be restarted, and you need to wait for a few minutes for the service to restart before the next operation.

6.4 For Windows system, close the server's task manager to delete the network disk

After a network disk is added, if the server's task manager is not closed, the connection will be occupied. As a result, when deleting the disk, the process cannot be completely disconnected and the deletion might fail.

6.5 After formatting a partition disk (Like E disk) to a video disk, Windows system still prompts to format the disk

Video disks are in RAW (unformatted), but system partition disks are generally in NTFS. Therefore, the partition disks have to be changed to RAW format which are unformatted. When the system detects the unformatted disk, it prompts to notify users to format the disk. Click “No” or close the pop-up. Users can also set disks to RAW and select not to format the volume when creating a new volume.



6.6 Some disks (Like C disk) are not displayed in the local disk list

The virtual hard disk has been canceled. Considering the disk reading and writing pressure, as well as the wrong formatting operation, the system installation disk and the disk where the DSS program is installed are not displayed in the local disk list.

6.7 A few more disks (Like E disk and F disk) appear after adding a network disk to the platform

The network disk can be set as a picture disk or a file disk. After setting the network disk as a picture or file disk, the network disk will be formatted as a NTFS disk and displayed in Windows system. As a result, when a network disk for pictures and files storage is added, the Windows system will identify it as a newly added NTFS disk and assign it a drive letter so that it is displayed on Windows.

7 Backup and Restore

7.1 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.

7.2 Backup and restore take so 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.

7.3 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.

8 Live Video

8.1 Situation for video to use video sub stream

Enter local config interface 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.

8.2 Failed to get live video

- LAN/WAN mapping config 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;

8.3 Live video does not play smoothly

The main reasons are shown as follows:

- Poor network condition fails to make stream reach decoder normally, and it causes video unsmoothness;
- Beyond the server forwarding performance. For example, the rated forwarding performance of single server is 700M while the actual amount of forward is more than 700M.
- The server uses a 100Mbps cable, but the actual forwarding volume exceeds 100Mbps.
- PC performance trouble. The decoder CPU or memory fails to meet the supports of normal decoding display, and it causes video unsmoothness.
- Encoding trouble. It causes video unsmoothness if it fails to encode in time.

Contact technical support for help when video is unsmooth.

8.4 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.

9 PTZ Operation

9.1 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.

9.2 Failed to operated PTZ when PTZ camera is added

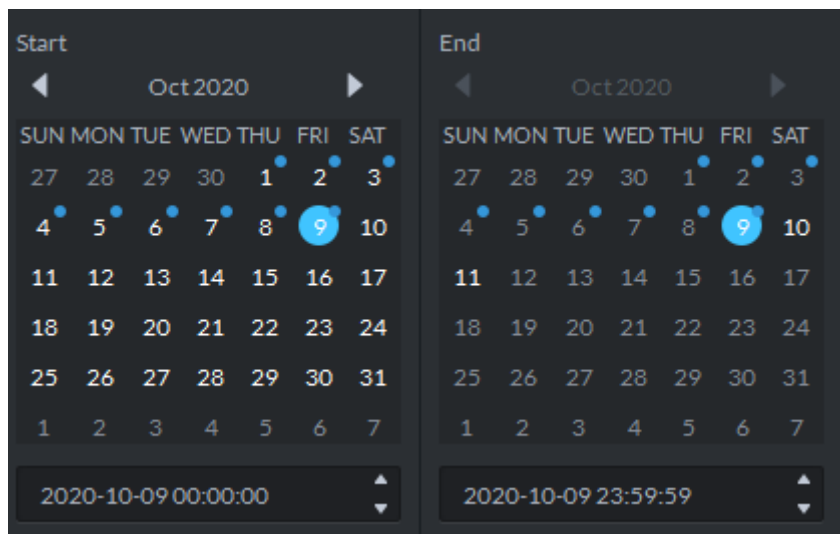
The operating video channel has PTZ function, but it is not enabled in device manager configuration; you need to select the **Speed Dome** as shown in the following figure.

Basic Info		Channel Number: 8 (0-1024)	Stream Type: Sub Stream 2	<input type="checkbox"/> Zero Channel Code
Video Channel	Name	Camera Type	Features	Unique ID
Alarm Input Channel	10.33.68.49_1	Speed Dome		
Alarm Output Channel	10.33.68.49_2	Fixed Camera		
	10.33.68.49_3	Speed Dome		
POS Channel	10.33.68.49_4	Dome Camera		
		Speed Dome		
HDCVI External	10.33.68.49_5	Speed Dome		
Alarm Box Channel	10.33.68.49_6	Speed Dome		
	10.33.68.49_7	Speed Dome		
	10.33.68.49_8	Speed Dome		

10 Recording Playback

10.1 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.



10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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 users general user to log in the operating system with high security level.

10.8 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.

11 Operation & Maintenance Center

11.1 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.

11.2 On Device Status interface in Maintenance Center, the total number of abnormal devices is different from the count of devices of abnormal running status

Abnormal devices and devices of abnormal running status are different in connotation:

- Abnormal devices include devices with hardware errors and alarm exceptions.
- Devices of abnormal running status include offline devices besides the former two.

Therefore, the two numbers are different.

11.3 When searching for faults of devices in organization A, faults of devices in organization B are displayed

This results from organization change of devices. When a device in organization A had failed in organization B, the fault will be detected.

11.4 The device fails to update after the defined update start time of the update plan

This results from the different time of the client and the server. The plan is carried out only when the server time meet the defined update start time of the schedule.

11.5 A immediate task has been created, and the list time is inconsistent with the client

This results from the different time of the client and the server. When the plan is carried out, the server time is displayed.

11.6 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.

12 Video Wall

12.1 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.

12.2 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.

12.3 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.

12.4 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 interface, 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 interface, delete the useless video wall in the video wall management interface, and finally save the video wall to be used on the platform.

13 Map

13.1 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.

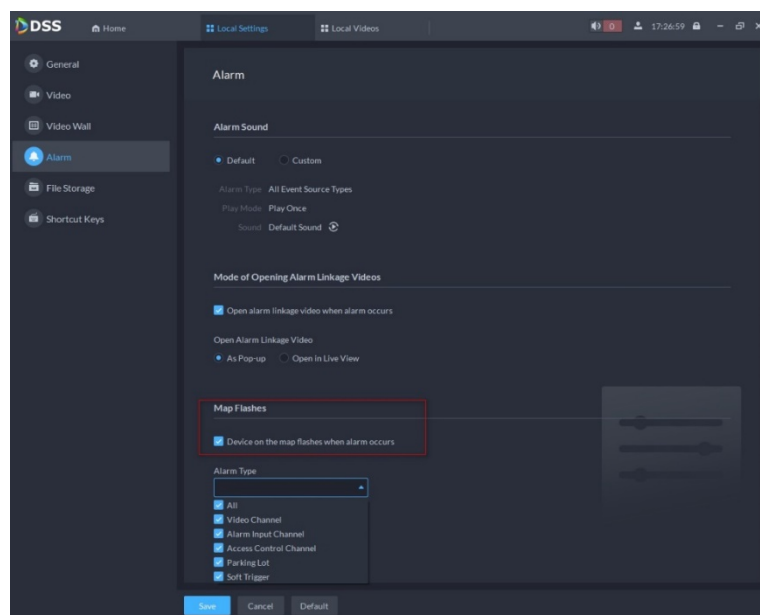
13.2 Alarm is configured, but cannot flash on the electronic map when alarm is generated

You need to turn on map flashing function on client local config 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 config, and find the following config options and select all the alarm types.



14 Face Recognition

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

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

14.2 Face recognition module at live view interface does not display real-time snapshots

In the Storage module of basic configuration on client interface, 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 interface to check whether the operation of device is normal.

14.3 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.

14.4 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.

14.5 How to 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.

14.6 Why some devices under the device tree are displayed as devices, and others are displayed 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.

15 Video Metadata

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

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

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

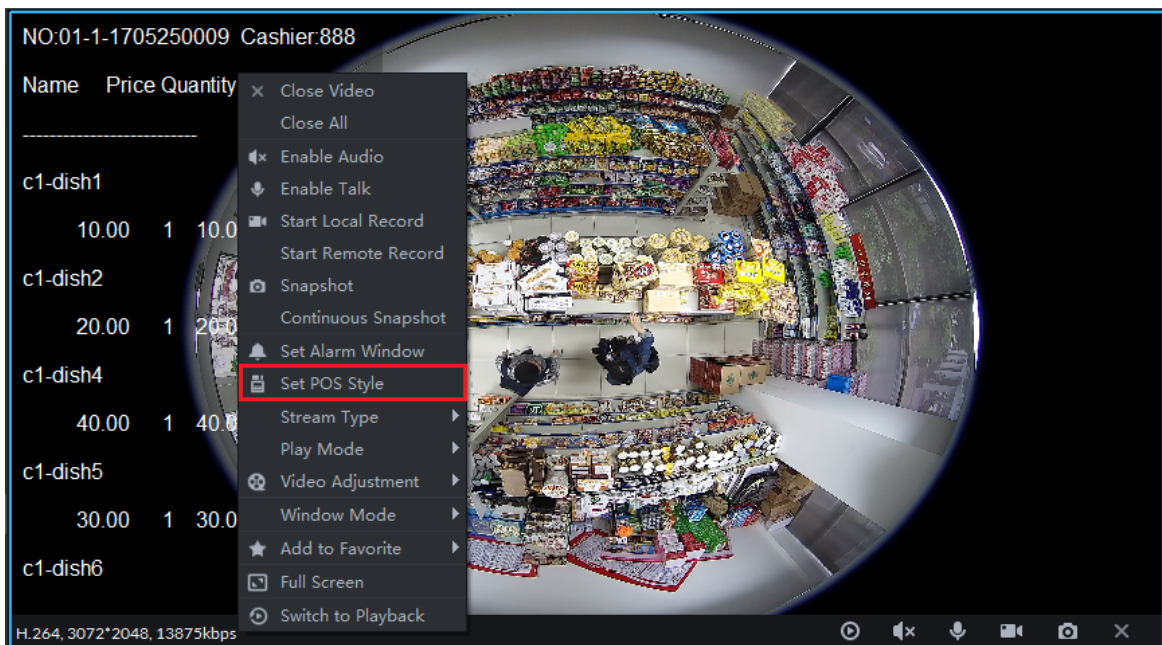
In Storage module of basic configuration on client interface, check whether the disk that stores images and files is configured on the distributed disk of the video metadata device.

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

16 POS

16.1 Overlay POS information is not clearly displayed in live video

As shown in the following figure, right-click the video window, and select **Set POS Style** to set POS style. Drag the black frame at the left side of the picture to set the display position of POS information. Other information that can be set includes overlay mode (page turning/rolling), font size (small/medium/large), background transparency, and font color.

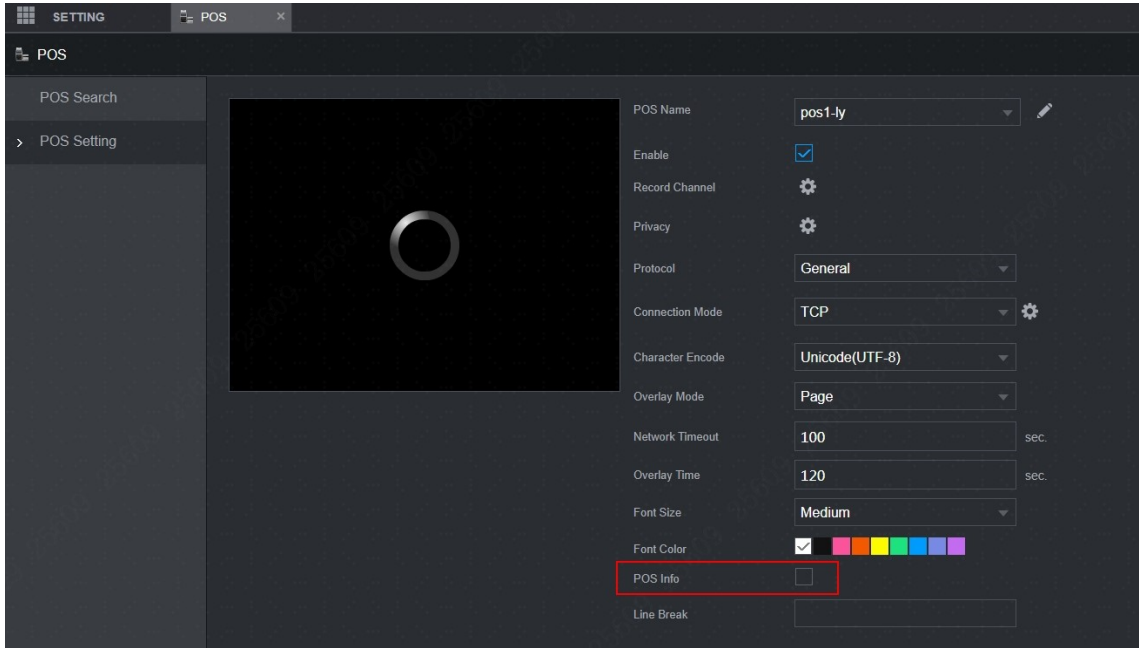


16.2 What is the unit for the money in the receipt?

In the POS information, the type of currency is not displayed, only the numbers. The type of currency should be the same as the local currency.

16.3 What should I do when the POS information of more than one channel is displayed on the live video because the NVR and the POS device are bound to the same channel?

Log in to the web manager of the NVR, select **Main Menu > POS > POS Setting**, and then cancel the selection of **POS Info**.



17 Access Control

17.1 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.

17.2 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.

17.3 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.

17.4 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.

17.5 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.

17.6 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.

17.7 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.

17.8 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.

17.9 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.

17.10 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.

17.11 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.

17.12 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.

18 Visitor

18.1 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.

18.2 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.

18.3 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.

18.4 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.

18.5 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.

18.6 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.

18.7 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.

18.8 Failed to trigger automatic visit and leave when the plate number is authorized to the corresponding entrance & exit points and has been successfully identified

Check whether entrance & exit points are selected in the automatic visit and leave configuration.

19 Video Call

19.1 Method to quickly add video intercom device

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

19.2 "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.

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

Check whether the 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.

19.4 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.

19.5 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.

19.6 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.

19.7 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.

19.8 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.

19.9 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.

19.10 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.

20 Entrance and Exit

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

Check whether the barrier connected to the web config interface of the checkpoint devices has its Enable switch turned on.

20.2 Vehicles in blocklist can be automatically recognized and released

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

20.3 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.

20.4 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.

20.5 Platform can distribute 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.

20.6 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.

20.7 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.

20.8 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.

20.9 Vehicles with a forced exit record cannot be 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 forced exit record cannot be restored.

20.10 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.

20.11 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.

20.12 The available space detection is configured in the parking lot. After a vehicle exits, the available space is still 0

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.

21 Attendance

21.1 Check-in or check-out time is one minute more than the swiping time

Review the statistics rule of the attendance config module and check if the setting is "In". If yes, any number of seconds above 0 is counted as one minute.

21.2 Failed to see the shift of staff groups

- The staff are included in a separate staff shift which prevails over the staff group shift and renders the latter void.
- The staff are included in a temporary shift which prevails over all other types of shift.

21.3 The additional staff are not assigned to any shift plan, but why is it displayed in a shift?

If additional staff are not assigned to any shift, they are by default subject to their department shift if there is one.

21.4 Failed to query the attendance card swiping record of the staff

- Check whether the access control module has the card swipe record. If there is but the attendance record shows no record, proceed to the next step
- To query the attendance card swiping record, first set up the device as the attendance checkpoint; at present, only the access control device can serve for this purpose
- The current card swiping time does not fall into the period of staff shift or holiday management

21.5 Failed to query the attendance report of the staff

- Check whether the attendance card swiping record of staff has the attendance report
- Check whether the card swiping record falls within the check in/out period of the shift
- Detect the query conditions and see if the period is normal, the keywords of fuzzy search, and the selected department

21.6 Failed to query the abnormal attendance record of the staff

Individual anomalies can be calculated the very day they take place. For example, if a check-in happens after the preset deadline, the report shows this check-in as abnormal. In another example, if the check-in of the is before the deadline but there is no corresponding check-out, the system calculates on the next day or even two days later if the person forgot to do the check-out or not.

- For a shift that does not span two calendar days, the system calculates all check in/out records at 00:30 the next day to see if they are abnormal.
- For a shift that spans two calendar days, the system calculates at 00:30 the two days later (counting from the day when the shift starts) to see if they are abnormal.

21.7 One card swipe produces two records

If Employee A is on a shift spanning two calendar days, two records are produced for a single card swiping action by A, because this action can either be the check-out on the first day, or the check-in on the second.

21.8 Records of the attendance report such as the card swiping records cannot be fully exported

Up to 100,000 records can be exported now.

21.9 Attendance reports are not generated after synchronizing offline records

Attendance reports are not generated in the following scenarios:

- Access control records failed to be extracted or personnel ID is null in the records.
- Access control records will be compared based on the duplication removal rules and duplicate data will be discarded.
- Access control records are extracted successfully, but there is no staff shift, nor it's during holidays.
- Access control records are extracted successfully and there is staff shift, but the rounding half to even rule is adopted for flexible attendance.

22 Case Bank

22.1 After saving a case, the case image cannot be viewed on the case interface

To use the case bank, you need to configure the incident disk with appropriate storage capacity on the storage interface. The data of the incident disk will not be overwritten when it is full, so configure an incident disk with larger capacity. It takes 2–3 minutes to save images and videos. Please be patient.

23 Event Center

23.1 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.

23.2 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.

23.3 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.

23.4 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.

23.5 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.

23.6 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.

23.7 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 (DSS Professional: 400 Mbps; DSS Express: 50 Mbps). Otherwise, videos might be lost.

24 Cascade

24.1 Cascade function

The superior can view the real-time video and recoding of the subordinate.

24.2 Devices that support cascading

Only encoding devices (POS channels, CVI alarm input channels and alarm channels of alarm boxes are excluded).

25 Intelligent Analysis

25.1 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.

25.2 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.

25.3 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.

25.4 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.

25.5 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.

25.6 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.

25.7 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.

26 Synthesis

26.1 What is a bridge and what does it do

A bridge connects a three-party system and the DSS platform. Compliant with the connection protocol between the third-party system and the platform, it is used to import events to the platform from a third-party system.

26.2 The types of database and business data that are supported when synchronizing data to third-party databases

Attendance and access control data on the platform can be synchronized to a third-party database; Mysql, Oracle, Sqlserver, and PostgreSQL databases are supported.

26.3 Failed to synchronize the attendance report after being updated to V8.1.0

UU_ID filed and UPDATE_TIME_UTC field are added to the attendance report in V8.1.0. You need to reconfigure the third-party system data table according to the synchronization rules before synchronization.

26.4 Data repetition occurs in the third-party database after system updating and data synchronization

UU_ID filed and UPDATE_TIME_UTC field are added to the attendance report in V8.1.0 and each record is assigned with these two fields. The UU_ID field must be synchronized to the third-party database as the unique ID to search for and update the third-party database. So the data will be synchronized again after updating. Data repetition will occur if the old data (without UU_ID field) is not cleaned up before the new data (with UU_ID filed) is synchronized to the third-party database. We recommend you clean up the data in the third-party database before synchronization.

27 Message push when the app is not running

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

Alarms and video/voice calls.

27.2 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.

27.3 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.

28 Center storage for hot standby

28.1 What is hot standby

Hot standby is a solution that uses two servers to improve system stability. The main server and sub server are connected through TCP/IP network and data replication is carried out through a software.

Under normal conditions, the main server works and the sub server monitors. Once the main server goes wrong, the sub server takes the place of the main server to ensure normal function.

28.2 Local hard disks cannot be formatted as video disk

At present, the video storage format cannot synchronize the data between the main and sub servers through folder synchronization. For the video center storage in hot standby, we recommend you add an EVS by IPSAN. It is required that the primary and standby computers add the same user of the EVS at the same time. When one server takes over the other one, the server attached to the EVS will be actively adjusted to ensure the normal reading and writing of video data.

28.3 The drive letter and number of drives of the two servers must be consistent for storage of images and incident files in hot standby

The pictures, files and evidence files under the hot standby are backed up synchronously through the hot standby software. The drive letters and capacities on both sides are required to be consistent.

If they are inconsistent, the data of the main and sub servers will be inconsistent or the data synchronization will be abnormal.

For example: If the main server is 500 G and the sub server is 100 G, some data of the main server cannot be synchronized to the sub. If the main server has an E disk but the sub server doesn't, the hot standby software will prompt that the mount point is lost and stop data synchronization.

28.4 The main and sub server need to add different users of the EVS when it is used as image and files disks

Under hot standby, when the network disk is added as a picture and file storage disk, the disk will be formatted as the NTFS disk, acting as a local disk of the server.

Under hot standby, the folder synchronization of pictures and files is performed through the hot standby software. If EVS is used for picture and file storage, it is necessary to ensure that the size and quantity of EVS storage disks added to the main and sub servers are the same, and the same disk

cannot be used by both servers. Therefore, it is generally recommended to add a single EVS through different users. It is necessary to ensure that the size and number of disks under the user are consistent, so that the user disks added to the main and sub servers through EVS can be synchronized normally. If the same user is added, two servers can read and write to the same disk at the same time, which will lead to abnormal data storage.

28.5 In hot standby, main servers can add different EVS users, but the sub servers from distributed deployment can add only one user

For sub server in distributed deployment in hot standby or not in hot standby, one EVS can be added in either user mode or normal mode. Any disk on the EVS can be set to store pictures, files or videos.

However in hot standby, the EVS added to the main server can only have one type of disk under one user. In order to satisfy that one EVS can store videos, pictures and files at the same time, the main server in hot standby can add multiple users under one EVS.

28.6 Certain pictures and videos are lost after one server takes over the other one in hot standby

It takes time for a server to completely takes over the other one. Pictures, incident files and videos generated during this time will be lost.

If a lot of files are lost, check if there is any of the following problems:

- Loss of video: Check whether all video disks of the main and sub servers are of the same user of the same EVS.
- Loss of pictures, files and incident files: Check whether the disks letters the number of disks that store pictures, files and incident files of the main and sub servers are the same; whether the disk type corresponding to each disk letter is the same; and whether the data source binding of all pictures, files and evidence files is configured on the hot standby software.
- If none is abnormal, contact the technical support.

28.7 A prompt says mount point change/loss on the hot standby software

Mount point change: during the data synchronization of the main and sub servers, the synchronized data is operated, and the synchronization of the hot standby software will stop based on the data protection mechanism. At this time, manual recovery needs to be carried out on the hot standby software manually: select data source for application and the hot standby synchronization will be restored automatically.

Mount point loss: please check whether you have deleted or switched the disk type of the disk configured with file synchronization. If yes, please update the file synchronization configuration on the hot standby software. If no, please confirm whether the file synchronization path configured on the hot standby software is consistent with the main and sub servers.

29 Independent Database Deployment

29.1 Failed to enable independent database deployment

Independent database deployment requires corresponding license. If it cannot be enabled, please check whether an official license has been purchased.

29.2 Data that can be stored in the independent database.

Will the data stored in the independent database also be stored in local disks

After the independent database deployment is enabled, events, faces and videos will be stored in the independent database, and the local database will no longer store those data.

29.3 The independent database cannot be queried after it is restored to operation

Wait for the client to indicate that the independent database has reconnected or manually add the database again.

29.4 After the independent database deployment is closed, can the data previously stored in the independent database be queried

No. After disabling the independent database, the data stored in the independent database will not be synchronized to the local database.

29.5 Will the data be lost after disabling the independent database

No. Previous data stored in the independent database will not be lost after you disable it.

30 MPT File Retrieval

30.1 After the MPT device is added and the file retrieval plan is configured, file retrieval is not performed in time

Check whether the retrieval plan is enabled only with WiFi connection. If yes, check whether the device is connected to Wifi.

30.2 File retrieval failed when the MPT device is normal and the retrieval plan correctly configured

Possible reasons:

- An image and file disk is not configured, for which files cannot be downloaded.
- If there are files in multiple time zone in the MPT device, the system will fail to query the device file list. You can delete the original time zone file, modify the device time zone and calibrate the device.
- The device versions do not match.
- When the platform is connected to the internet, file retrieval is only supported when the MPT device is also connected to the internet.

30.3 The time in the list of MPT record retrieval is inconsistent with the time in pictures and videos

The time recorded in the video and picture of the MPT device is the time in the time zone when the device is recording or taking pictures. The time zones of the client, device and server must be consistent to ensure that the time in the list is consistent with the time in the videos and pictures.

30.4 After the MPT device is successfully added, the device suddenly goes offline, or offline and then online

When the MPT device is uploading files, the device will be offline if its screen is locked automatically. It is recommended to set the screen to the always-on status during the file upload process. If the device is turned on for a long time, status abnormality might occur (the device goes offline from time to time). Restart the device to resolve the issue.

31 Alarm Controller

31.1 When will force arming alarm controller fail

There are several situations:

The defense zone is open but cannot be bypassed.

There are faults in the defense area, including shielding, short circuit and tampering.

The main AC power supply is lost and the device is under low battery.

31.2 Cancel alarm for wired zones

Disarm the sub system or the device twice to cancel the alarm when the wired zone is in alarm status.

31.3 Bypass the wired zone when the alarm controller is under arming

You can bypass the wired zone when the alarm controller is under arming or disarming.

32 Virus Scan

32.1 Anti-virus software prompts "an exe program or dll library contains virus" when installing a program

It is not possible to fully scan all antivirus software and libraries, some antivirus software may mistakenly identify the DSS platform as a virus, so you are assured to add trust and continue to use it.

33 NPT

33.1 NTP time synchronization does not work

The specific interval of NTP time calibration depends on the algorithm. We recommend you manually synchronize the time for first-time use if there is a big time error.

Step 1 Check whether the service network is connected to the NTP service network.

Step 2 In cmd terminal, execute the **w32tm /stripchart /computer:ntp_server_address** command to check whether the NTP server is available.

```
C:\Documents and Settings\xws>w32tm /stripchart /computer:XXX.XXX.XXX.XXX
TrackingXXX.XX.XX.XXX [XXX.XX.XX.XXX].
The current time is 2013-10-9 10:41:02 (local time).
10:41:02 error: 0x80072746
```

If the above-mentioned message appears, the NTP server is not available.

```
C:\Documents and Settings\xws>w32tm /stripchart /computer: XXX.XX.XX.XXX
Tracking XXX.XX.XX.XXX [XXX.XX.XX.XXX].
The current time is 2013-10-9 10:39:55 (local time).
10:39:55 d:-00.0000433s o:-2220.7617382s [ @ | ]
10:39:57 d:-00.0000399s o:-2220.7593686s [ @ | ]
```

If the above-mentioned message appears, the NTP server is available.

Step 3 Go to **Control Panel > Administrative Tools > Services** to check whether the **Windows Time** service is running.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883