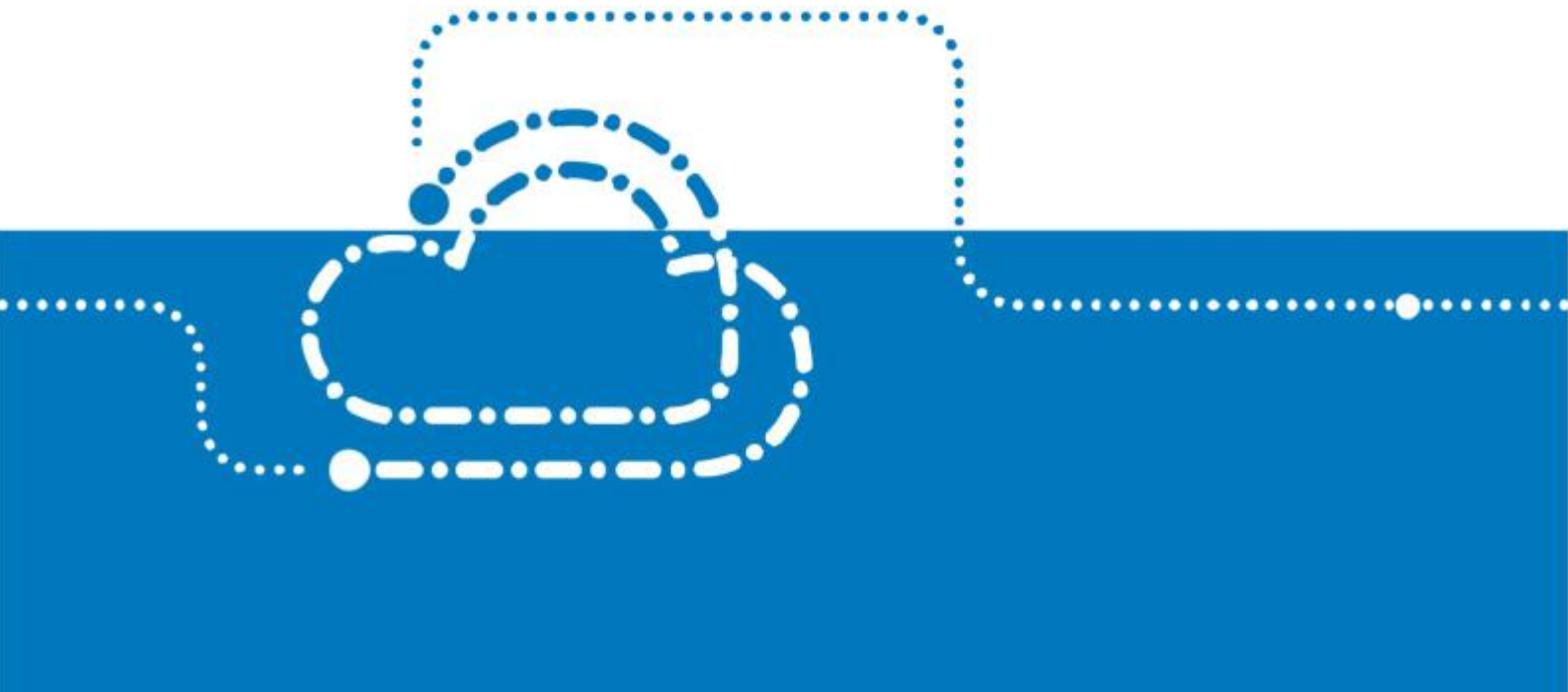
ZXIMCU PT01 P200 Portable Emergency Command System Operation Manual



Version update instruction

Version	Date	Author	Auditor	Remark
1.0	2021-01-19			

Caltta Technologies Co.,Ltd.

Address 12F, Building G2, International E-City, Nanshan, Shenzhen,
Zip code 518052
Website http://www.caltta.com
Email caltta.sales@zte.com.cn
Telephone +86-755-26774767

INDEX

Figure Index

1 Overview

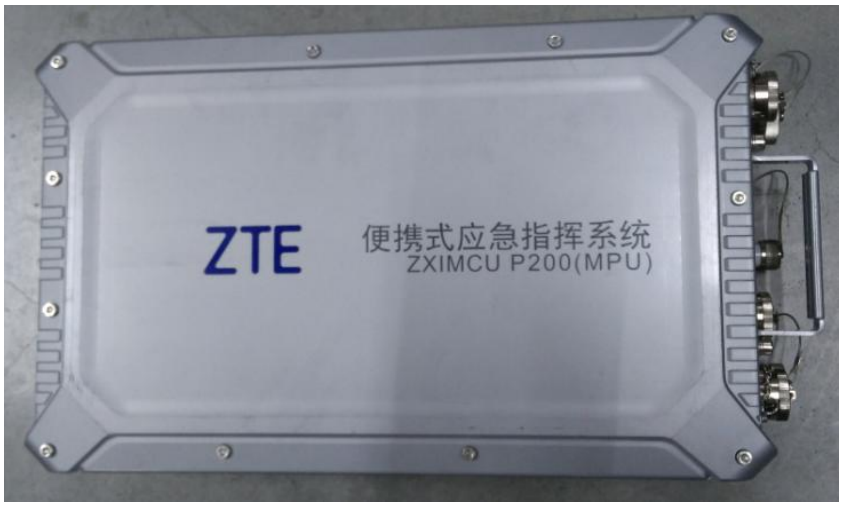
This manual covers introduction and operating instruction of Caltta LTE Emergency Command System, which includes configuration and operation methods for MDS, core network, base station, terminals and peripheral supporting products. Please select the corresponding operation steps according to the actual system and device.

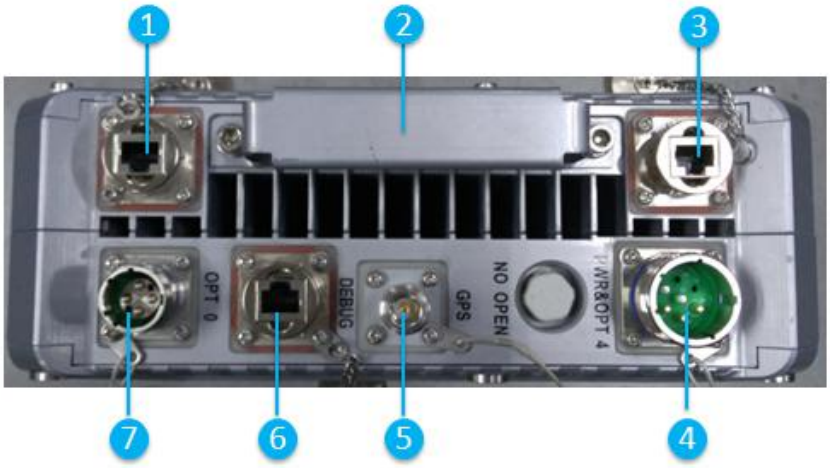
2 ZXIMCU PT01 P200 Version 3.0

2.1 Introduction of ZXIMCU PT01 P200 Version 3.0

The distributed structure of control unit and RF unit helps P200 reduce its weight, which is more convenient for carrying. The System consists of MPU, RRU, power connection line, etc.

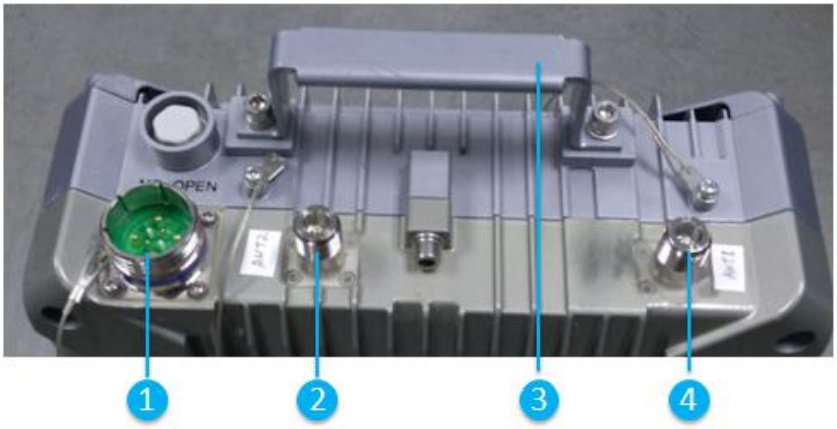
Figure 2-1 ZXIMCU PT01 P200 MPU





1) Network Interface 1: used for connecting with dispatch console or backhaul device
2) Handle: convenient to carry
3) Network Interface 2: used for connecting with dispatch console or backhaul device
4) Optoelectronic Input Interface: connect with RRU via power line.
5) CPS Antenna Interface: connect with GPS Antenna
6) System Debugging Interface
7) Extended Optical Fiber Interface

Figure 2-2 ZXIMCU PT01 P200 RRU



1) Power Input Interface: power input and connect with MPU
2) RF Antenna Interface
3) Handle
4) RF Antenna Interface

Figure 2-3 ZXIMCU PT01 P200 Power Line

1) A Connector : Waterproof connector with large size diameter, connect to RRU
2) B Connector , Waterproof connector with small size diameter, connect to MPU
3) C Connector : Triangle plug, connect to external power supply

2.2 ZXIMCU PT01 P200 Connection Operation

Step 1: Take out the device as shown below

Figure 2-4 ZXIMCU P200 device

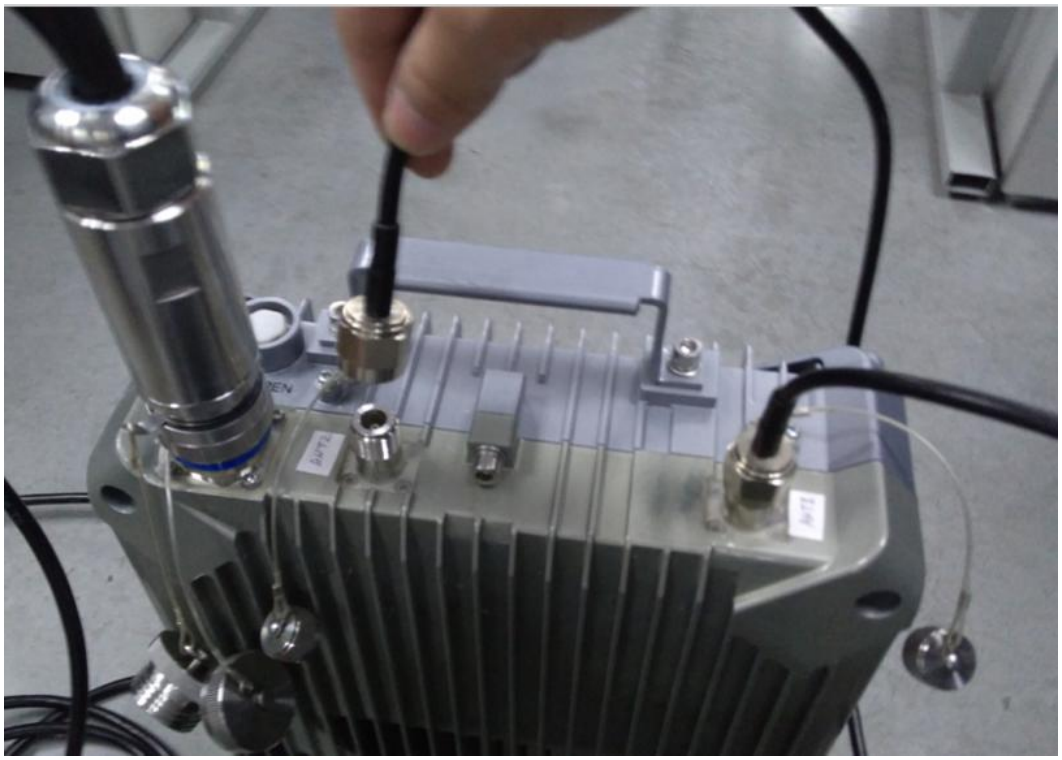
MPU Power Cable RRU

Step 2: Connect the A connector of the power line to RRU, connect B connector to MPU, and tighten them up

Figure 2-5 Connection between MPU and RRU with the the power line

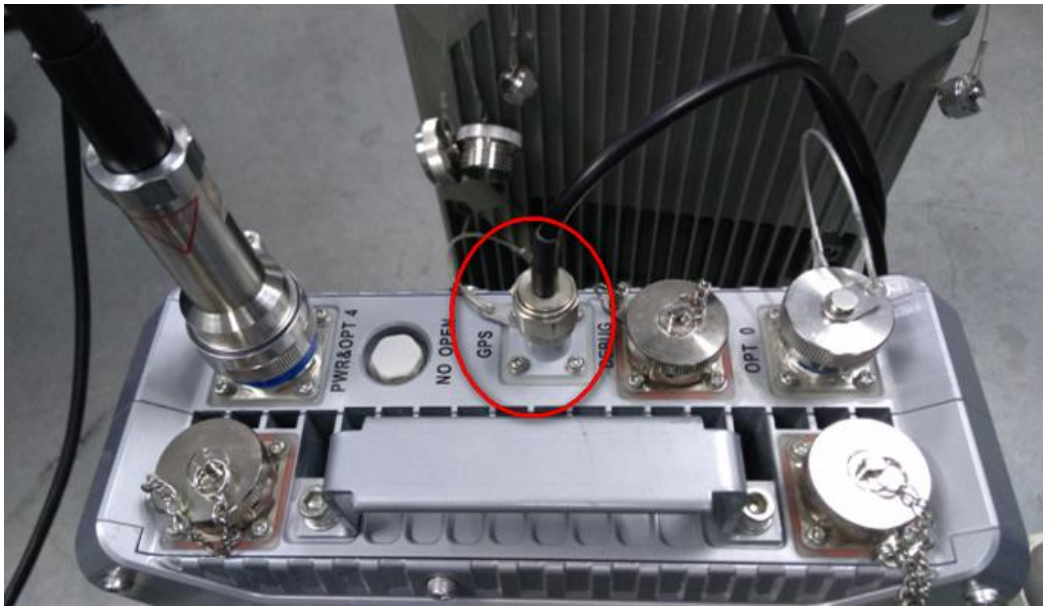
Step 3: Connect feeder and antenna: Connect one end of the antenna feeders (2 pieces) to the RF interface of RRU, connect the other end to the RF antenna. Make sure to tighten them up when connecting, otherwise it may cause the weak signal and lead to failure of registration when the terminal is slightly far away from the system.

Figure 2-6 Connection of the feeder and antenna



Step 4: Connect GPS Antenna (no need to connect if the device is used as a stand-alone station): Connect one end of the GPS feeder to the GPS antenna interface of MPU, the other end to the GPS antenna

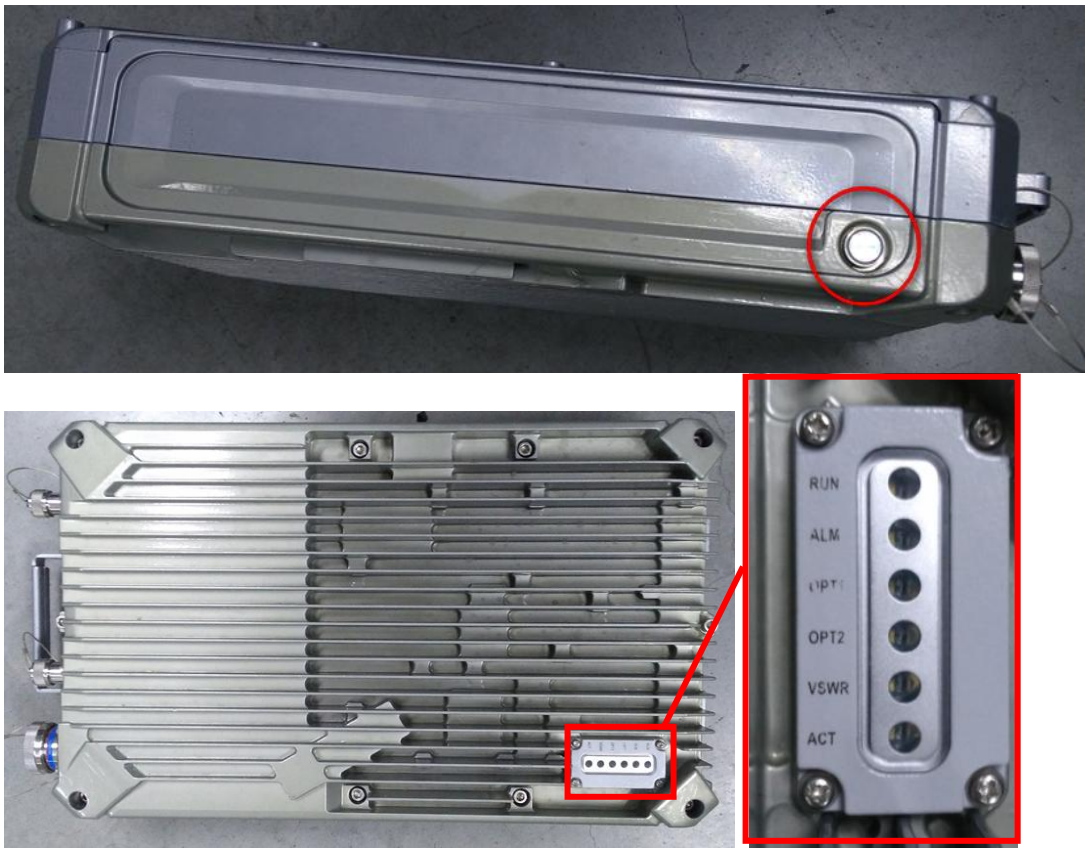
Figure 2-7 Connection of GPS antenna



Step 5: Connect the C connector of the power line to the Power Input Interface (100-240V AC, 50/60Hz), then turn on the main power switch of the device. The main power switch is on the side of the RRU.

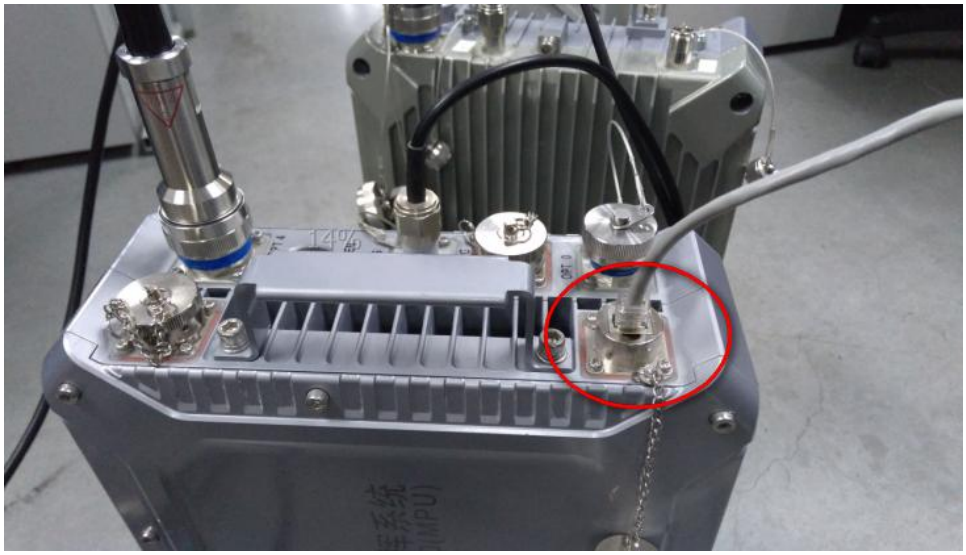
Observe the RRU indicators. The RUN indicator flashes after power-on, the RUN and OPT1 indicator flash after the system starts normally, and the ACT indicator is always on.

Figure 2-8 Power switch and indicator light



Step 6: Use network cable to connect the dispatching laptop to any of the MPU network interface. The network interface could also be used as output interface of the system transmission.

Figure 2-9 Connection of the dispatch console

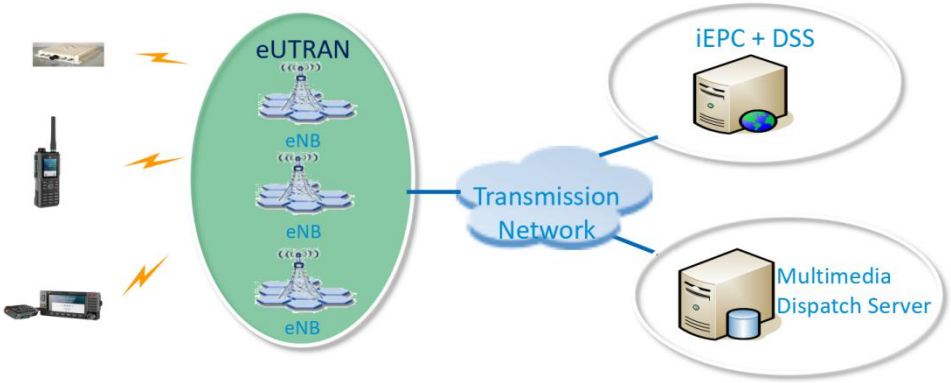


3 Network Architecture Introduction

Caltta LTE portable emergency command system is based on All-IP flat network architecture. The system follows B-TrunC Broadband Trunking standard, integrates LTE core network iEPC, professional voice and video trunking network DSS, multimedia dispatching server MDS, base station system and terminals, and provides end-to-end multimedia command and dispatch solution. While providing kinds of multimedia service such as voice, video and data, the system can also support data bearer and transmission for the third-party, keeping the system in openness.

LTE Portable Emergency Command System network topology is shown as follows:

Figure 3-1 System Network Architecture



Remark: The network architecture diagram of the system is a schematic diagram of each network unit. The physical form of the device is determined by different products.

LTE core network iEPC is a common LTE core network device complying to 3GPP standard specification, consists of MME, S/P-GW, and HSS, which is used for providing common LTE services.

Trunking core network system DSS is composed of PDS and DAS. PDS provides trunking services for trunking users. DAS provides dispatching services and industry customized services.

Multimedia dispatching server MDS has various functions such as mobile video surveillance, Video pull, video distribution, video dubbing, etc.

4 Dispatching PC Configuration

Both common PC or laptop can be used as dispatching PC. The PC operating system requires Win 7 or above.

4.1 IP Address Setting

The IP address of PC needs to interconnect with the IP address of MDS server (defaults to 192.168.13.20) and the IP address of trunking dispatch console (defaults to 192.168.13.21). Interconnecting to OMM IP address is also required while login the OMM system.

The following two IP addresses can be configured individually in the LAN to communicate with MDS dispatch console, trunking dispatch console and OMM system , to login the dispatch console (in the LAN, the IP address of the dispatch console needs to be set in the same network segment with the trunking dispatch console and MDS dispatch console, and there is no IP address conflict):

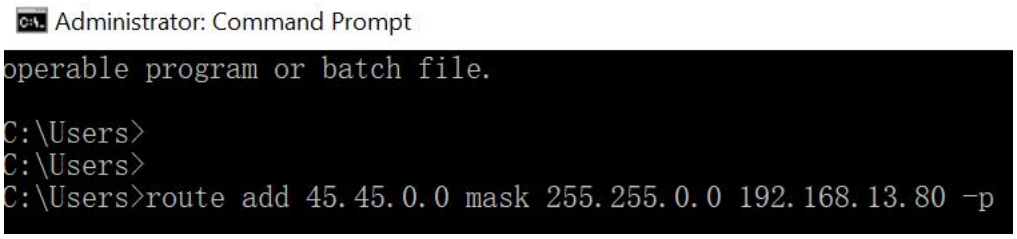
192.168.13.160/24

192.168.90.160/24

Open the PC command terminal and add a static route for the direct access to the individual device, CPE and camera:

route add 45.45.0.0 mask 255.255.0.0 192.168.13.80 –p

Figure 4-1 Adding Route

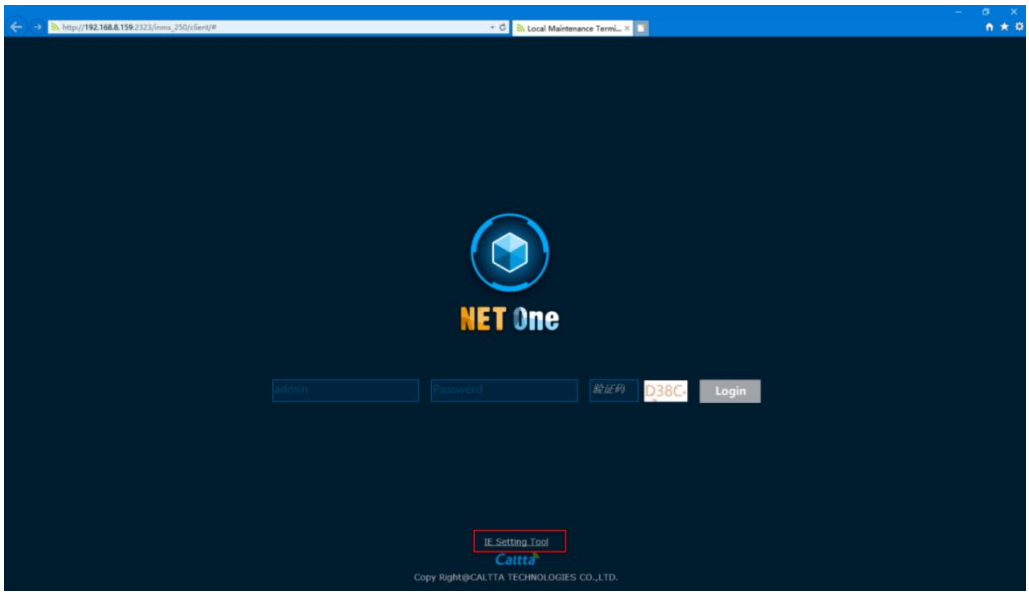


4.2 IE 11 Browser Setting

Login to the OMM system via browser. Support both IE and Chrome browser. If using IE browser, version 11 is required.

Before logging in, make sure the PC has been installed with Adobe flash player and the IE settings are correct, otherwise the OMM interface may not open. The Adobe flash player plug-in and IE setting script can be downloaded and installed on the OMM interface.

Figure 4-2 Download plug-in and script on the OMM interface



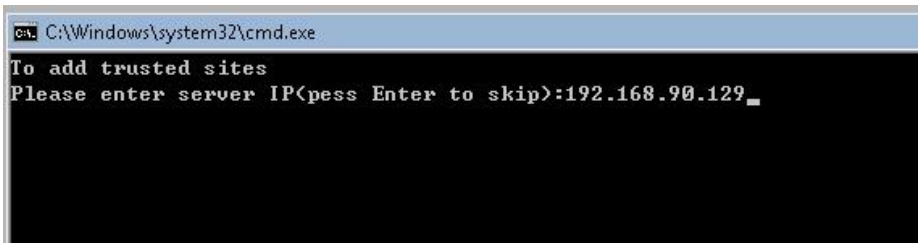
Script setting of IE trusted site:

Extract the following compressed package (or the batch file downloaded from the OMM), open Internet Explore11 to set up the script:

IE11SettingsZh.7z

Input the OMM server address in the CMD window, which defaults to 192.168.90.129.

Figure 4-3 Trusted site script setting of IE browser



Press Enter button after inputting the IP address, the script will set up automatically. Click any key to exit when finishing set up.

5 Trunking Services Operations

5.1 Operations of DAS Unified Dispatch Console

5.1.1 Dispatch Console Installation

Install the dispatch console software on the PC in advance and login the DAS dispatch console via the CS client.

Input the defaulted IP address 192.168.13.21 in the IE browser, then it will enter into the interface of plug-in and client downloading.

After downloading the client and plug-in., install the plug-in first, then install the client later according to the defaulted settings. Restart the PC after the installation.

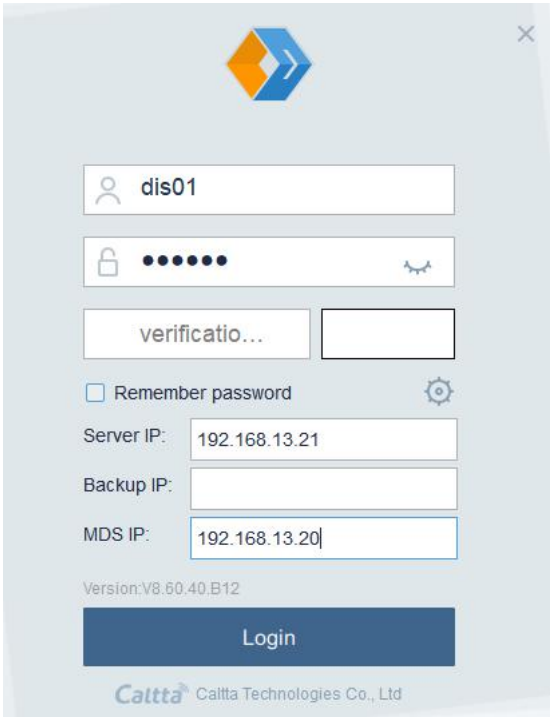
Figure 5-1 Downloading client and plug-ins of the dispatch console

5.1.2 Dispatch Console Login

Double click the DAS dispatch console icon and open the software. The DAS software will pop up the IP selection interface if the fixed IP address changes or for first time login. Select 192.168.13.160 as the dispatch console local IP address. Click **OK** to enter the login interface.

Figure 5-2 Selecting dispatch console local IP address

Figure 5-3 Login interface of the dispatch console



Input the account number and password on the login interface of dispatch console , select Remember Password and click the setting icon on the right side, Input the server IP address (IP address of the trunking dispatch console) and MDS IP address, then click Login to login in the dispatch console. The defaulted parameters of the dispatch console are as follows:

Account number: dis01, Password: 666666

Server IP address (IP address of the trunking dispatch console) : 192.168.13.21

MDS IP address: 192.168.13.20

Tip 1: Modifying the Local IP Address of the Dispatch Console

Enter to the login interface of the dispatch console after the local IP address is configured. Will fail to access to the server if selecting the wrong IP address.

There are two methods to modify the local IP address:

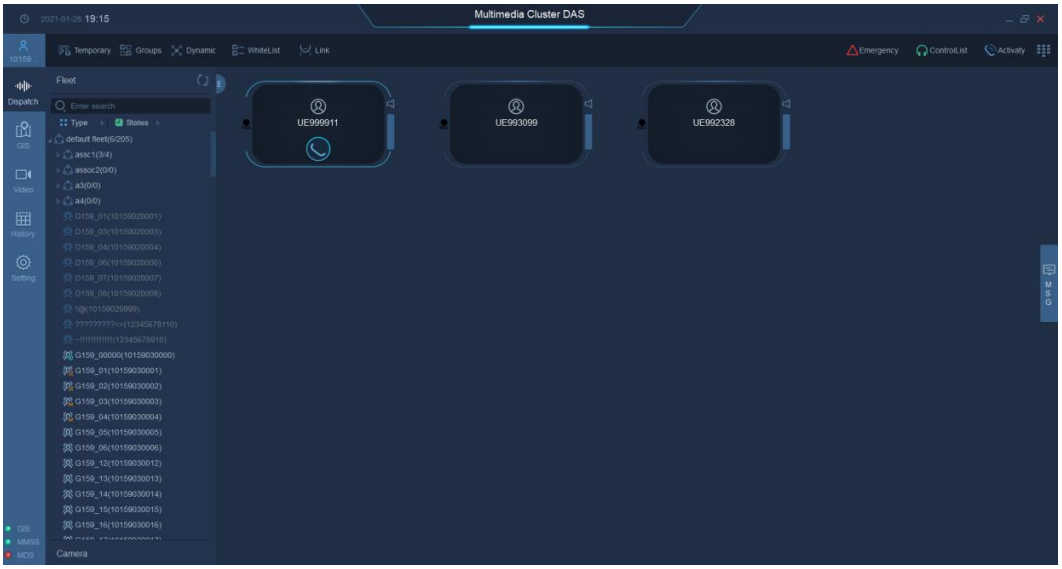
1. Method 1: Delete the local fixed IP address and add another IP address, then re-select the IP address.

2. Method 2: Modify the configuration file in the DAS software installation directory. Change the local IP address by modifying the localIP=192.168.13.160 in the "config.ini" file.

5.1.3 Dispatch Console Interface Introduction

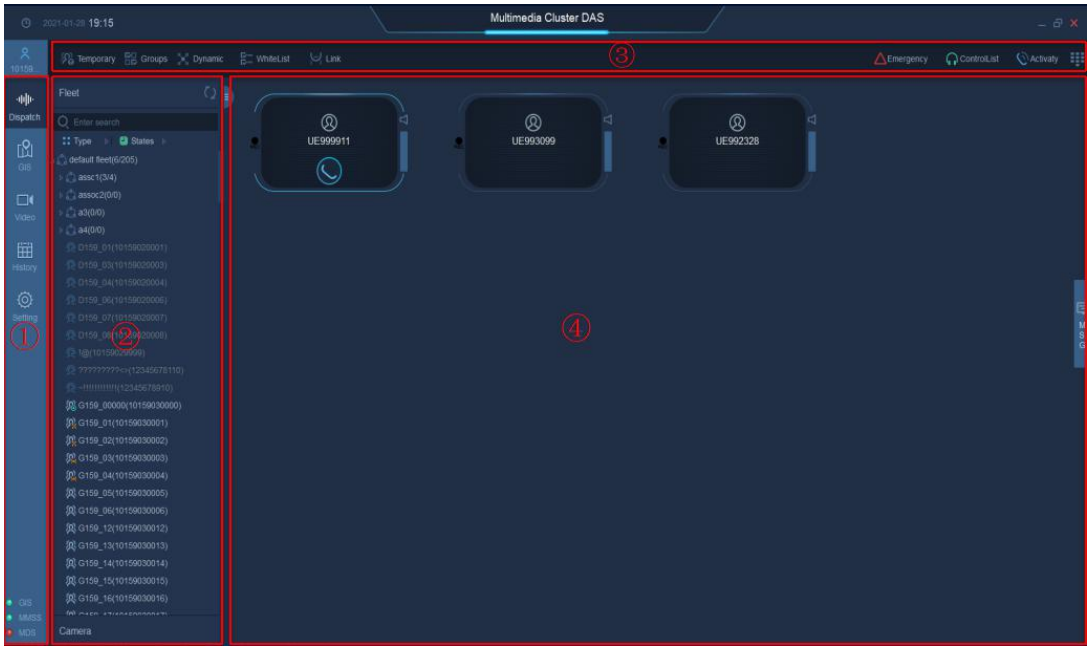
The dispatch console interface is shown as follows after login:

Figure 5-4 Dispatch console interface



5.1.3.1 Dispatch Console Interface Layout

Figure 5-5 Dispatch console interface layout



The dispatch console interface is divided into four areas as shown above, introduction of each (marked with number) is as follows:

- Area 1: Menu area, with five icons of Dispatch, GIS, Video, History and Setting, corresponds to different interfaces.
- Area 2: User list area, which shows the authorized users of the system and user online status. The hand-held terminal means default fleet user, individual device means camera user. Click the icon on the upper right corner of user list to display or hide the user list.
- Area 3: Toolbar and shortcut tools of trunking functions, such as temporary group, dynamic regroup, emergency alarm, etc..
- Area 4: Function display area which displays different functions of dispatch, map, video and so on according to menu selections.

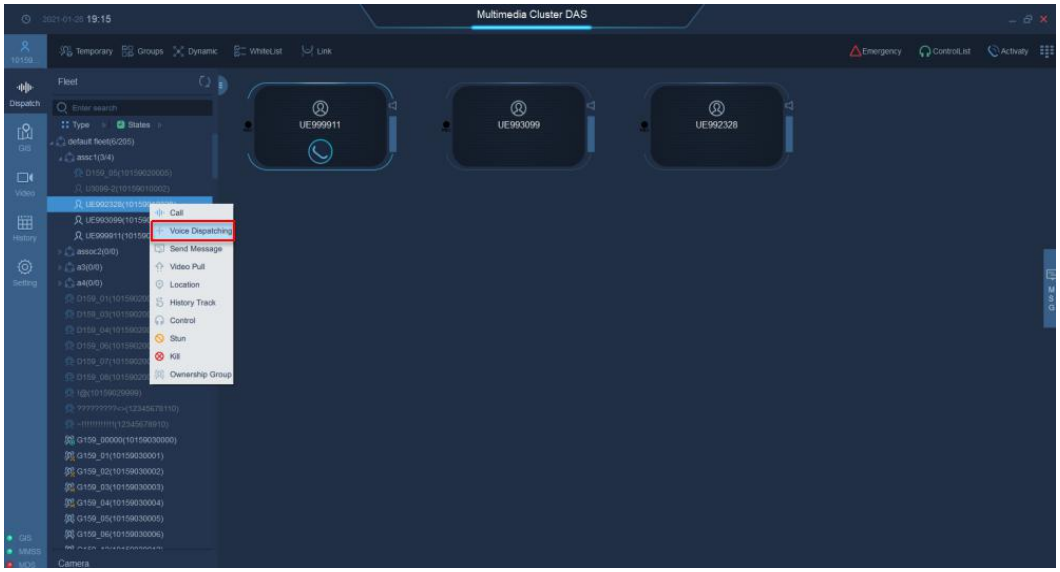
5.1.3.2 General Operations of Trunking Dispatch

Select **Dispatch** on the menu and enter the dispatching interface.

Adding users to the dispatching operation area:

Select the user / group / dispatch console that needs to be dispatched on the user information list, double click to add the user / group / dispatch console to the dispatching operation area. Or right click and select Voice Dispatch to add the user / group / dispatch console to the dispatching operation area.

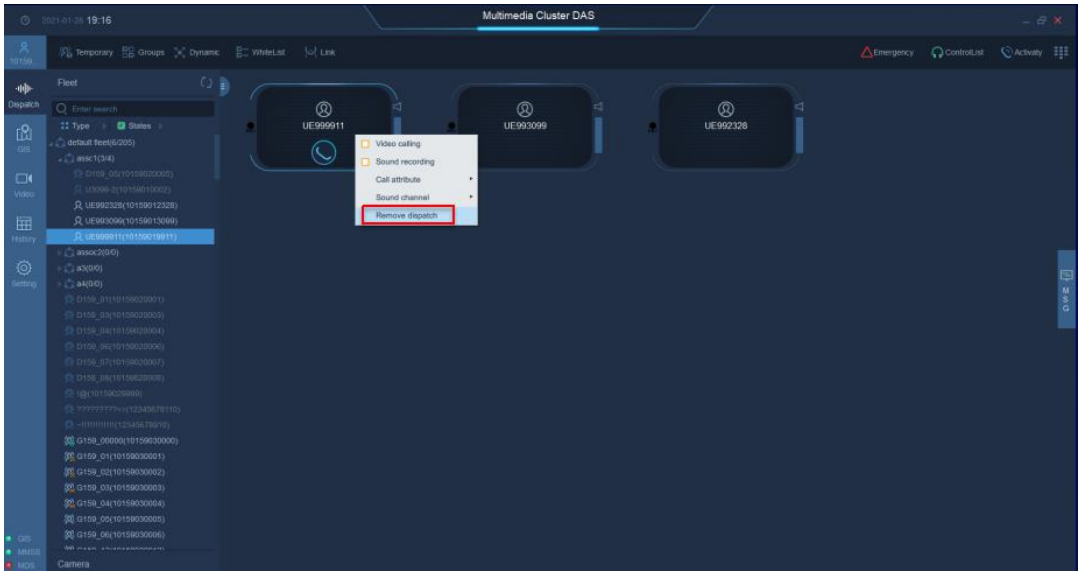
Figure 5-6 Add user to dispatching operation area



Remove users from dispatching operation area:

Move cursor to the user to be removed, right click and select **Remove dispatch**.

Figure 5-7 Remove user from dispatching operation area

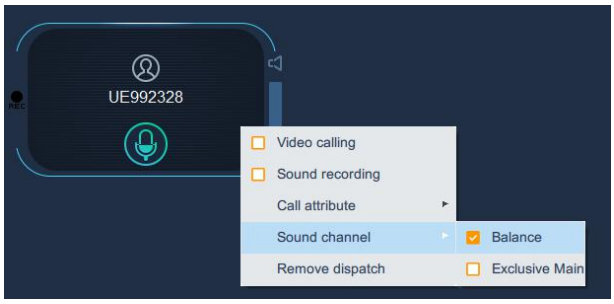


Sound channel selection:

When the dispatch console dispatches users, groups or dispatchers, it supports switching between balance channel model and exclusive main channel model.

Right click the user/group/dispatcher and select **Sound channel** from the shortcut menu. The corresponding channel can be selected as required. By default, balance channel is selected.

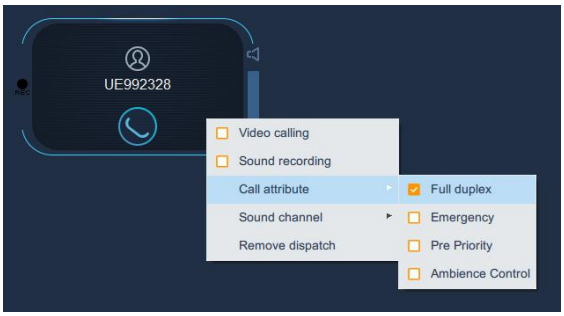
Figure 5-8 Sound channel selection



User call attribute setting:

Move cursor to a user, right click and select **Call attribute** from the shortcut menu. Select the corresponding call attribute as required. If select **Full duplex**, the dispatch console will make a full duplex call with the user. Otherwise, it is a half-duplex call.

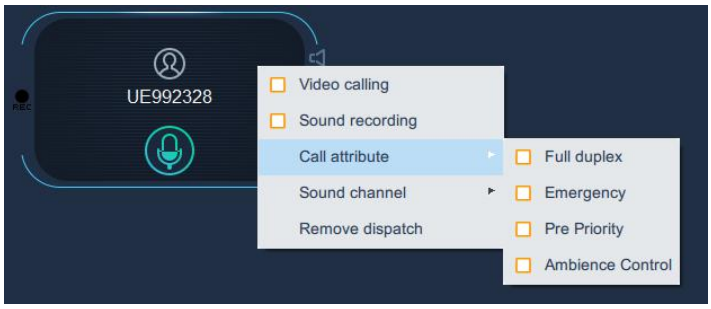
Figure 5-9 User call attribute setting



Group call attribute setting:

Move cursor to a group, right click and select **Call attribute** from the shortcut menu to select a call attribute as required.

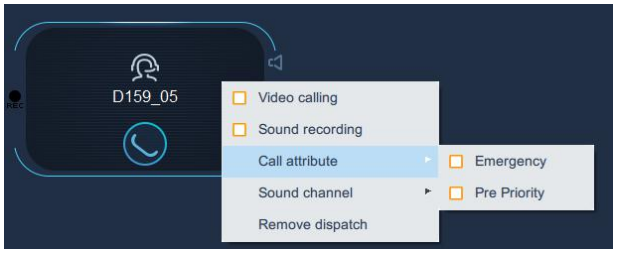
Figure 5- 10 Group call attribute setting



Dispatcher call attribute setting:

Move cursor to the dispatch console, right click and select **Call attribute** from the shortcut menu to select the call attribute as required.

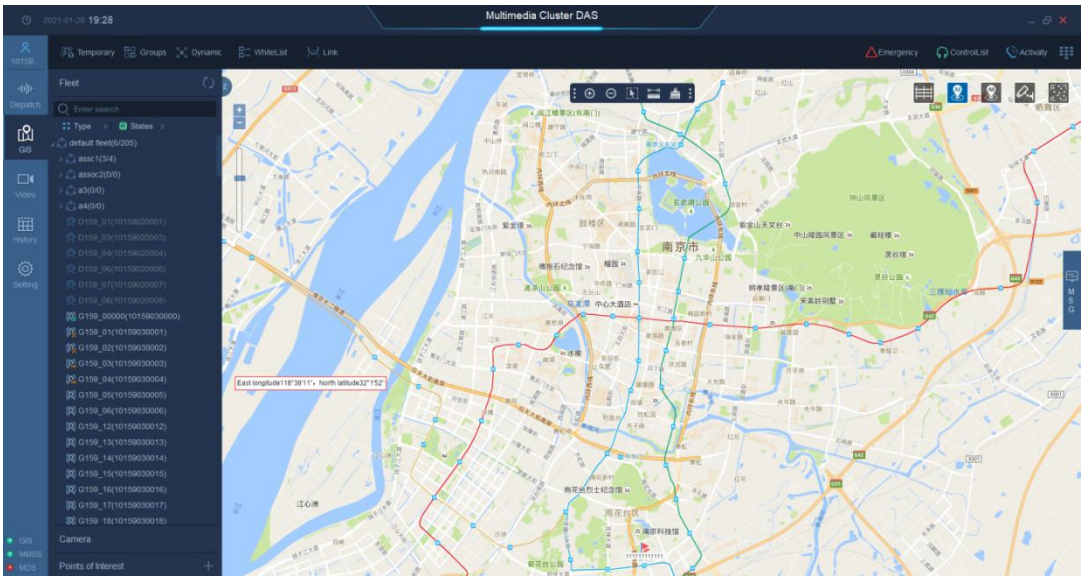
Figure 5- 11 Dispatcher call attribute setting



5.1.3.3 General Operations of GIS Dispatch

Select **GIS** from the menu, display the map interface.

Figure 5- 12 GIS interface of the dispatch console



The dispatch console supports both online and offline maps. Make sure the dispatching PC has been connected to the map server before logging to the dispatch console. If using online map, the PC is required to access to Internet before logging to the DAS dispatch console, otherwise map data cannot be loaded.

Similar to general map operations, zoom in or zoom out the map by scrolling the mouse wheel, drag the left mouse button to move the map, and search for locations.

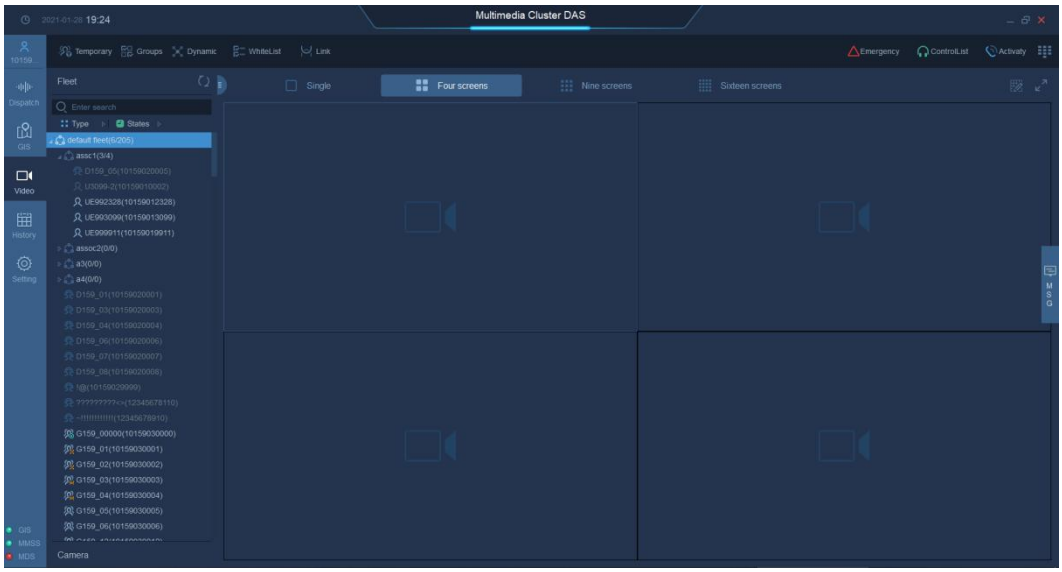
The toolbar  is on middle top of the map , which provides functions of Zoom in, Zoom out, Frame select, Ranging, Clean, and so on.

5.1.3.4 General Operations of Video Dispatch

Select **Video** on the menu to display the video dispatching interface

The upper part of the video dispatch area is the split-screen control button, which controls the single screen, 4-split screen, 9-split screen, and 16-split screen of video display. It also controls self-defined split screen, self-defined allocation and editing, and split screen / full screen display. The system displays different video split screen layout in accordance with different split screens, and switches the number of displayed screens.

Figure 5- 13 Video dispatch interface



5.1.4 Dispatch Console Initiates a Half-duplex Voice Private Call

Move cursor to the user on the trunking dispatch interface, right click and select **Call attribute** from the shortcut menu and and uncheck the "Full duplex" option;.

Click the call origination icon  in the middle, the terminal automatically joins the call, the dispatch console has the floor, and the terminal can hear the voice of the dispatch console.

During the call, you can change the sound channel and choose whether to locally record the call.

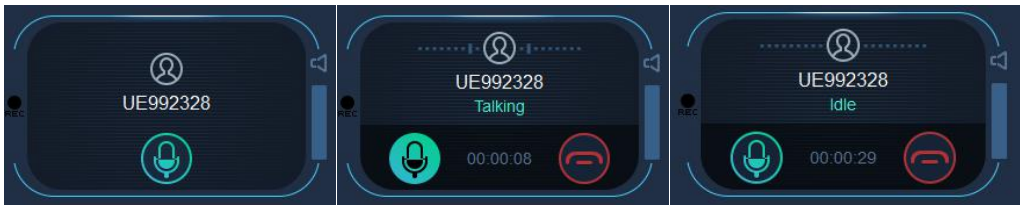
Move cursor to the upper part of the terminal that is calling, and click  to release the floor or apply for the floor.

After dispatch console releases the floor, the terminal can apply for the floor by pressing PTT button.

Move cursor to the top of terminal that is calling, click  to end the call.

The following figure shows the status of call origination, dispatch console speaking in progress, and call idle.

Figure 5- 14 Dispatch console initiates a half-duplex voice private call



5.1.5 Dispatch Console Initiates a Full-duplex Voice Private Call

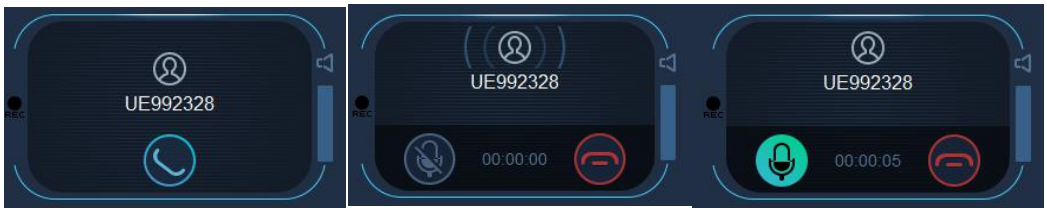
Move cursor to the user (**Call attribute** defaults to **Full duplex**) and click the Call origination icon in the middle, then the dispatch console and corresponding terminal will ring. After the terminal answers the call, the full duplex voice call is established.

During the call, you can change the sound channel and choose whether to locally record the call.

Move cursor to the user that is calling, click  to end the call.

The following figure shows the status of call origination, callee is ringing, and call is established.

Figure 5- 15 Dispatch console initiates a full-duplex voice private call



5.1.6 Dispatch Console Initiates a Full-duplex Video Private Call.

Move cursor to the user (**Call attribute** defaults to **Full duplex**) and right click, select **Video calling**, the dispatch console and terminal will ring. After the terminal answers the call, the full-duplex video call is established. The video of the terminal and the dispatch console itself are displayed in the lower right corner of the interface, double click the video to display in full screen.

During the call, you can change the sound channel and choose whether to locally record the call.

Move cursor to the user that is calling, click  to end the call.

The following figure shows the status of call origination, callee is ringing, and call is established.

Figure 5- 16 Dispatch console initiates a full-duplex video private call

5.1.7 Dispatch Console Initiates a Voice Group Call

Move cursor to a group and click Initiate Call in the middle, the terminals in the group will automatically answer the call and establish a voice group call. By default, the dispatch console has the floor.

During the call, you can change the sound channel and choose whether to locally record the call.

Move cursor to the upper part of the group call in progress to display floor switch icon, then click  to release floor or apply for floor.

After dispatch console releases the floor, terminal can apply for floor by pressing PTT button.

Move cursor to the bottom of the group call in progress, the call termination icon will be displayed. Click  to end the call.

The following figure shows the status of call origination, call in progress, before apply for / after release the floor .

Figure 5- 17 Dispatch console initiates a voice group call

5.1.8 Dispatch console initiates a video group call

Move cursor to a group, right click and select **Video group call**, the terminal will automatically answer the call and establish a group video call. Video will be displayed in the lower right corner. By default, the dispatch console has the floor.

During the call, you can change the sound channel and choose whether to locally record the call.

Move cursor to the upper of the group that is calling, the floor switch icon will be displayed, then click  to release the floor or apply for the floor.

After dispatch console releases the floors, the terminal can apply for the floor by pressing PTT button.

Move cursor to the bottom of group call in progress, the call termination icon will be displayed. Click  to end the call.

The following figure shows the status of call origination, call in progress, before apply for / after release the floor .

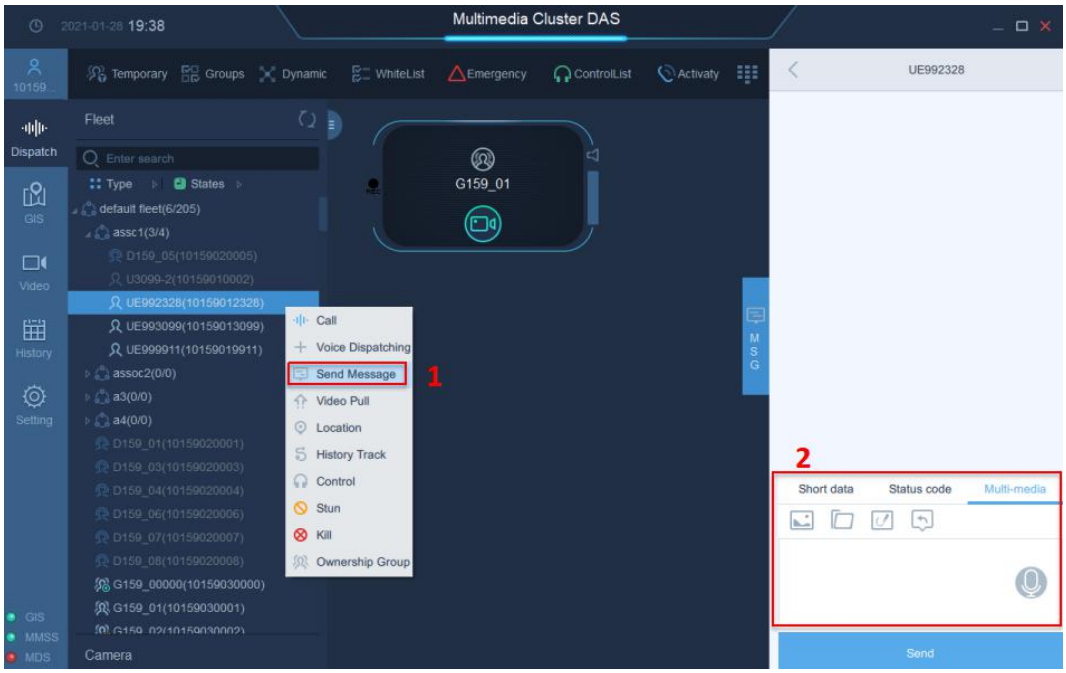
Figure 5- 18 Dispatch console initiates a video group call

5.1.9 Sending SMS and MMS

Move cursor to an online user in the user list, right click and select **Send Message** from the shortcut menu to send SMS and MMS to the terminal. Multiple file formats are supported (up to 20 MB).

Group operation is also supported. Right click a group to send SMS and MMS to the online group members.

Figure 5- 19 Sending SMS and MMS



5.1.10 Forced Release and Forced Insertion by the Dispatcher

Forced Release

The dispatcher can forcibly release a private call or a group call in progress. When a terminal initiates a call, the call activation list on the dispatch console will display the ongoing call.

Select the ongoing call, and click  to forcibly release the call.

Figure 5-20 Forced release by the dispatcher

Forced Insertion

Forced insertion is only applicable to group call. When a terminal initiates a group call and the group is not added to the dispatch area (if the group is already added to the dispatch area, the dispatcher participates in the group call by default and can directly apply for the floor), the dispatcher can directly obtain the floor by forced insertion.

When a terminal originates a group call, the call activation list on the dispatch console will display the ongoing group call.

Select an ongoing group call and click  to insert the call. The group will be automatically added to the dispatch area and the dispatch console obtains the floor.

Figure 5-21 Forced insertion by dispatcher

5.1.11 Dynamic Regroup

The dispatch console can dynamically regroup users based on the target group, and add users that do not belong to the group to this group through the dynamic regroup function to implement unified dispatch.

Click  on the toolbar of the dispatch console, open the dynamic regroup interface.

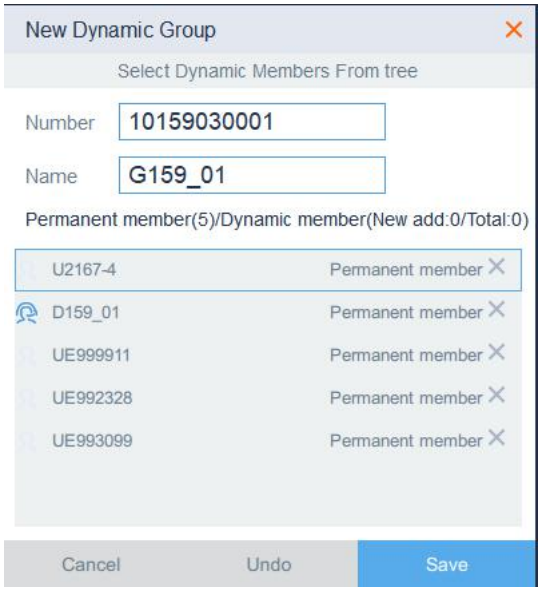
Double click the target group in the user list to add it.

Select the users to be added from the user list, the users will be shown in the dynamic member list.

Click  , the user will be added. The system will automatically send the group information to the new member.

To remove a dynamic member, click  under the corresponding member.

Figure 5-22 Dynamic regroup



5.1.12 Temporary Group Call

Different from dynamic regroup, temporary group call is to temporarily create a group. The group will disappear when it is removed from the dispatch area. To the contrary, the group information of the dynamic group will be saved and can be dispatched later.

Click 

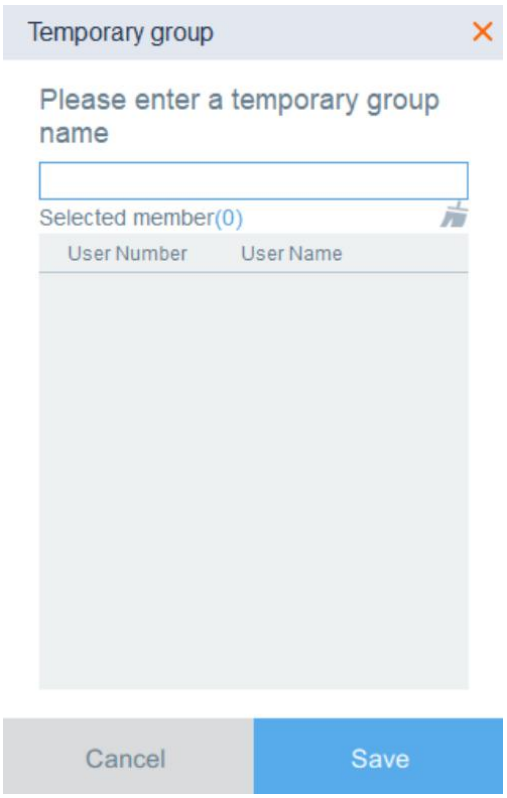
on the toolbar of the dispatch console to open the temporary group interface.Input a temporary group name, and double click the user to be added from the user list.

To remove a dynamic member, click  on the right side of the member.

Click 

to add the user, the group will be added to the dispatch area by default, so that group dispatch can be performed for the temporary users.

Figure 5-23 Temporary group call



5.1.13 Emergency call

In case of emergency, you can press the SOS emergency call button on the terminal to send an emergency call to the dispatch console and other terminals in the group.

The dispatch console can display the information of the user who initiates an emergency call and the time when the user initiates the call.

The dispatcher can click  to intervene the emergency call and switch to voice group call, and contact the user or other group members for proper handling.

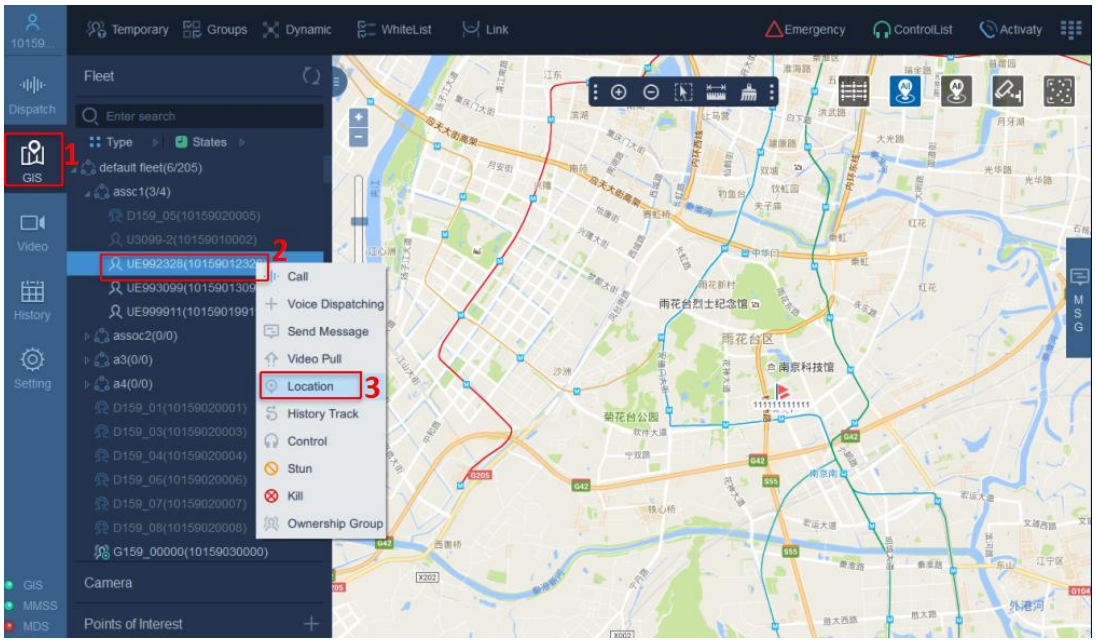
Figure 5-24 Emergency call

5.1.14 Dispatch Console Location

Select **GIS** from the system menu, and switch to the GIS interface. Move cursor to a user, and the user will be highlighted. Right click the user and display the operation menu.

Click **Location** to locate the terminal user. When the terminal has displayed the positioning status, click **Cancel Location** to end the positioning.

Figure 5-25 Dispatch console location operation

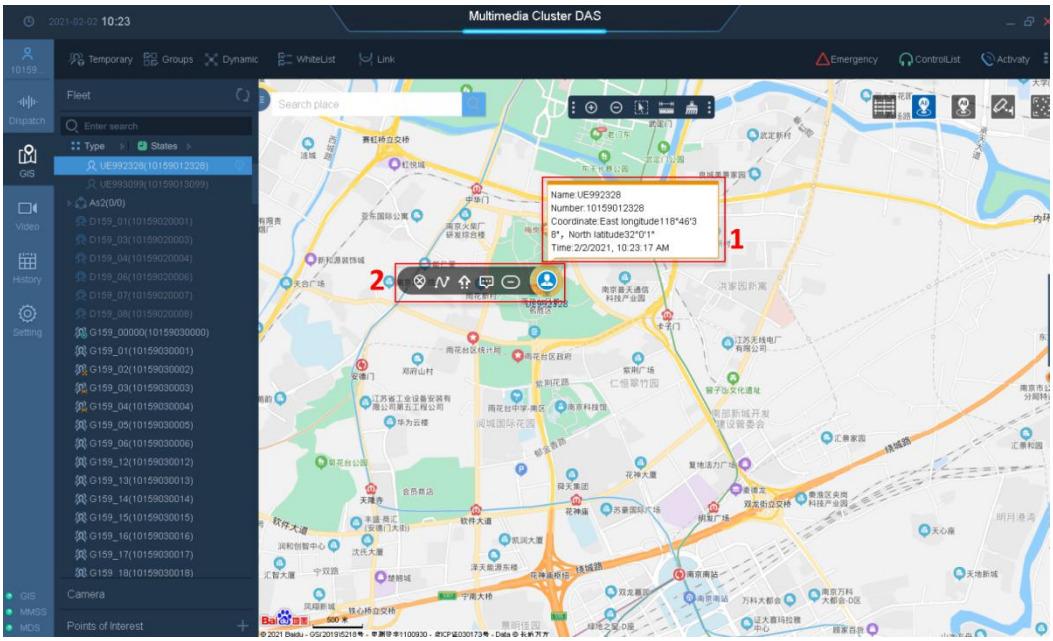


The location is successful if the terminal information is shown on the map. Move cursor to a terminal on the map, the detailed location information will be displayed in the following red box 1 .

Click a terminal to dispatch it on the map, as the following red box 2.

Click  to end the location. Click  to display the moving path of the terminal. Click  to pull the terminal video. Click  to send a message. Click  to initiate a voice call.

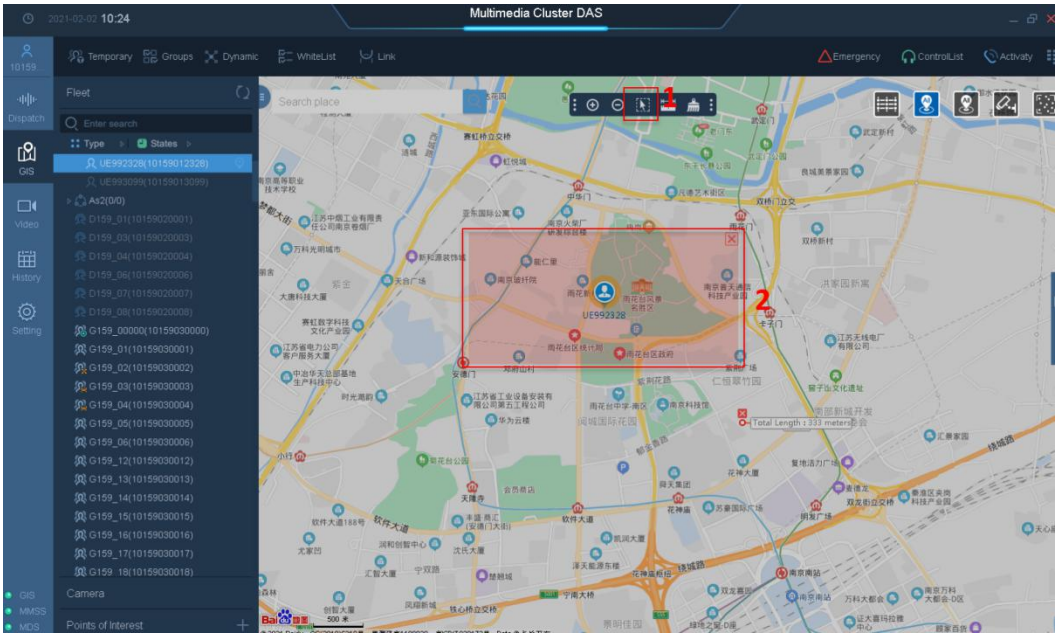
Figure 5-26 Map interface display and operation



5.1.15 Frame Select and Dispatch on the Map

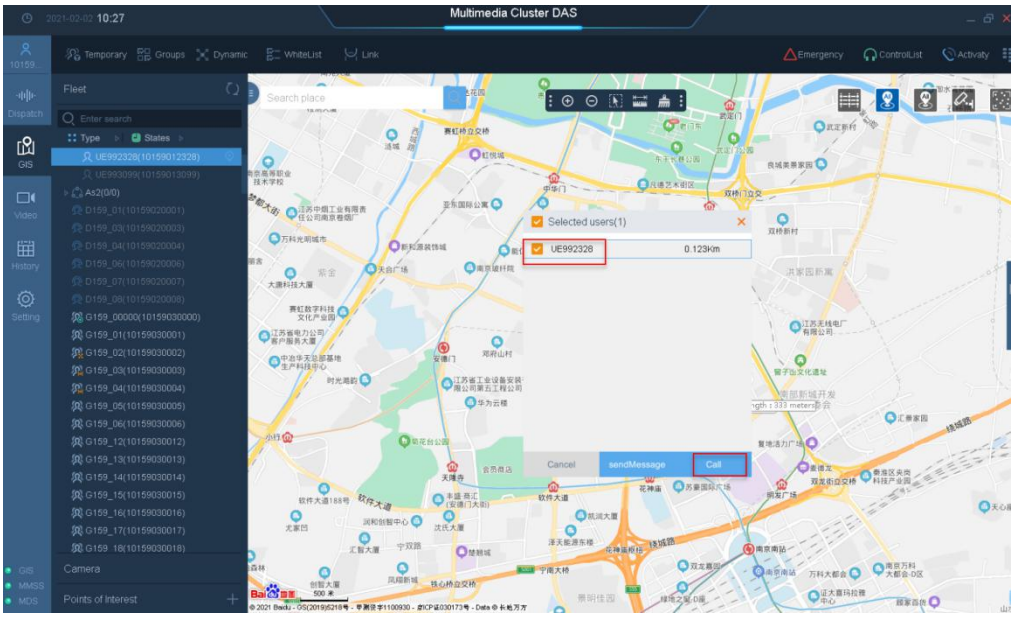
Frame select terminals on the map to make a temporary group call.

Figure 5-27 Frame select on the map



Tick the terminals in the pop-up box that need to be called, and click **Call** to start the group call.

Figure 5-28 Frame select and dispatch on the map



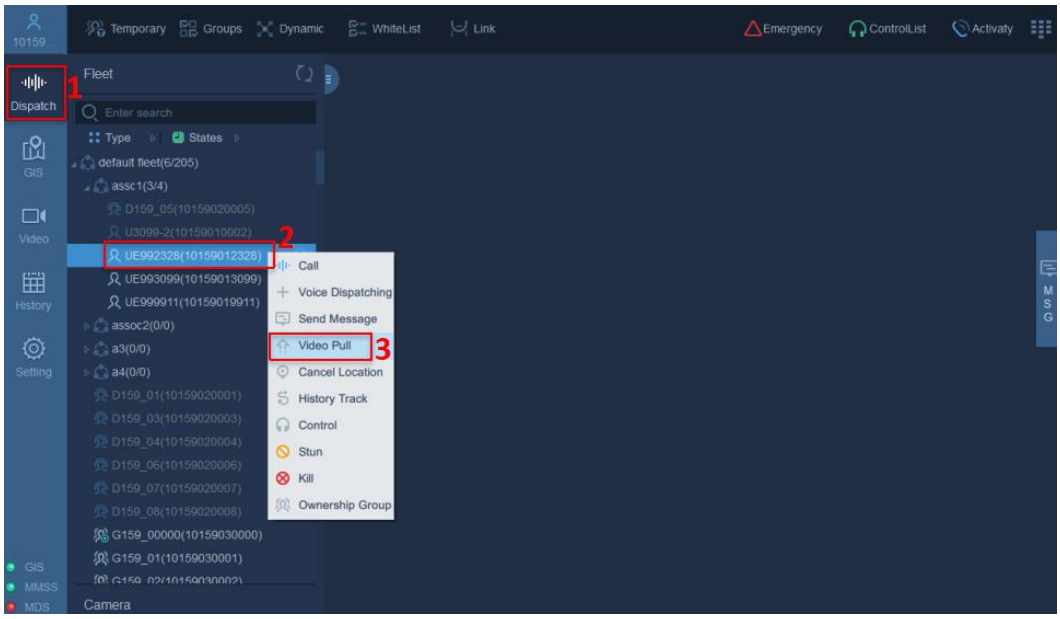
5.1.16 Dispatch Console Initiates Video Pull.

Select **Dispatch** on the system menu, and then switch to the Video Dispatch interface. Move cursor to a user, the user will be highlighted. Right click the user to display the operation menu.

Select **Video Pull**, the terminal video can be pulled to the dispatch console (the setting of the terminal video dispatch is configured correctly and registered successfully).

If **auto Rcv & Push** is not ticked in terminal video dispatch setting, the video will be pulled to the dispatch console only after the terminal answers manually.

Figure 5-29 Dispatch console initiates a video pull

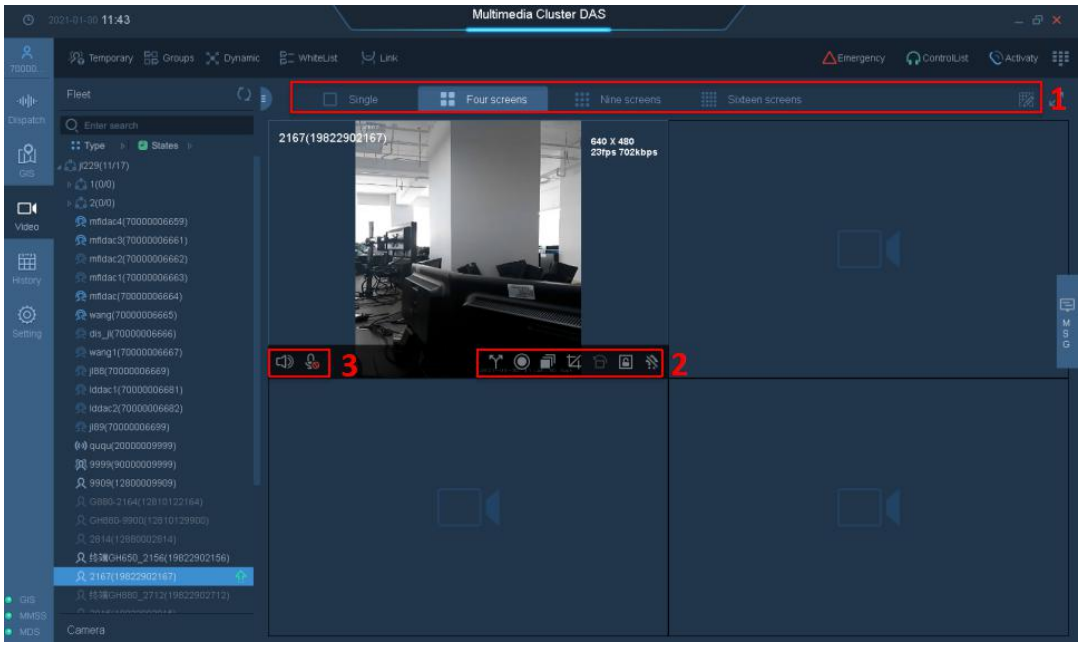


Adjust the number of terminal videos to be displayed on the upper area of the Video interface. Click to customize the display mode.

Move cursor to the toolbar on the bottom of video display window, click to end the Video Pull. Click to capture the video image. Click to capture the video images continuously. Click to record video. Click to distribute the terminal videos.

Click and to control the speaker and microphone of the two-way voice.

Figure 5-30 Toolbar of the video display window

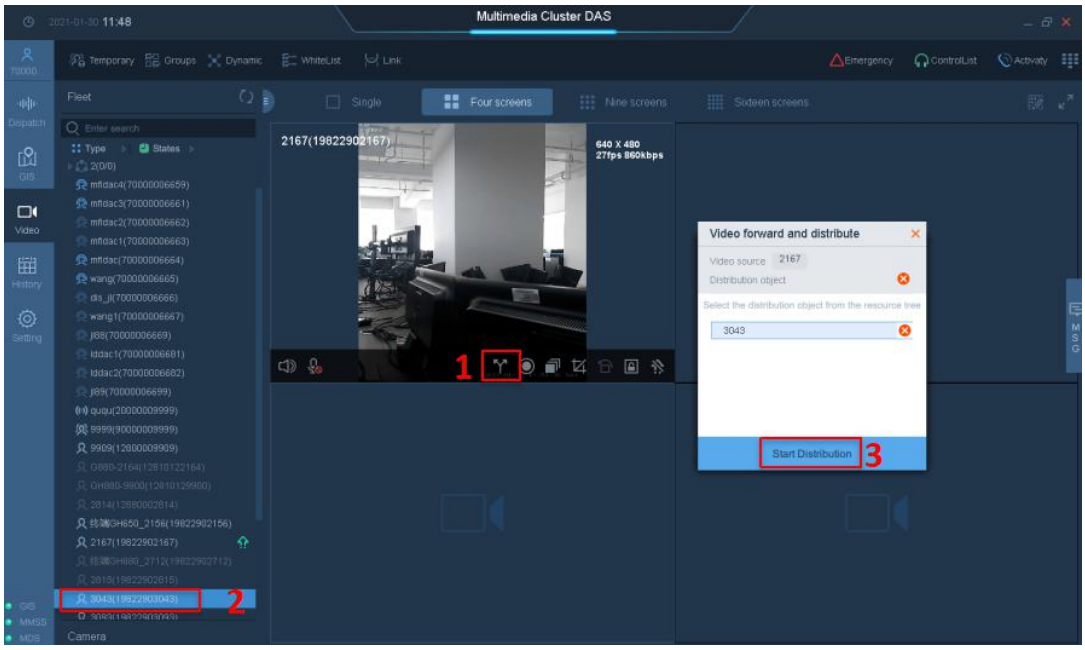


5.1.17 Dispatch Console Initiates Video Distribution

Pull a terminal video to the dispatch console first, and then move cursor to the video display window, the toolbar will be shown. Click  at the video's bottom right corner to open the **Video forward and distribute** page.

Select the users who need to receive video (the users should be registered online) from the user list, and click **Start Distribution** on the page to distribute the pulled video to the specified terminals.
The terminal can end video pull and the video distribution.

Figure 5-31 Dispatch console Initiates video distribution

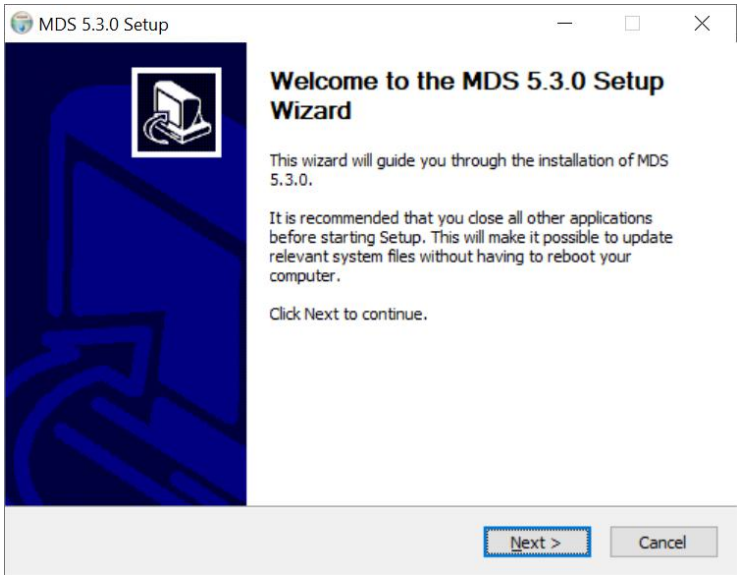


5.2 Operations of Multimedia Dispatch System

The Multimedia Dispatch System (MDS) client supports independent client operations. It's required to install the client before logging.

Install the CS dispatch console client on the dispatching PC. Click the installation file, then click **Next** until the installation is completed, as shown in the following figure.

Figure 5-32 Client Installation of the Multimedia Dispatch System

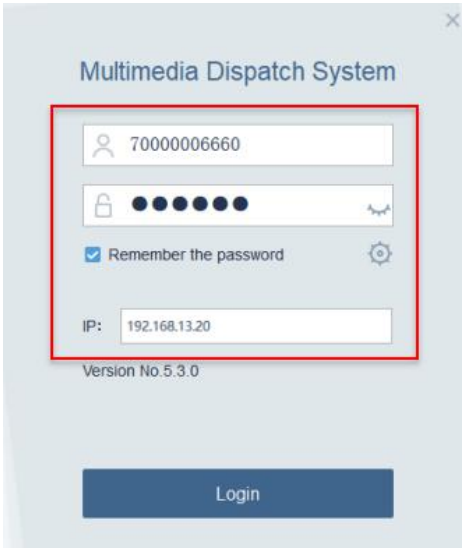


5.2.1 Dispatcher Login

Open the CS dispatch console client. If the the PC has multiple IP addresses, the client will prompt you to select the IP address. Select the correct IP address of PC that accesses with the client, and then turn to the login interface. Input the user name and password on the login interface, then configure the IP address of the server, as the following figure:

IP address of the server, the account and passwords default settings are as follows:
Server IP address: 192.168.13.20
Account/password: 88807558001/666666 (consistent with the OMM account information in the authentication configuration)

Figure 5-33 MDS client logging

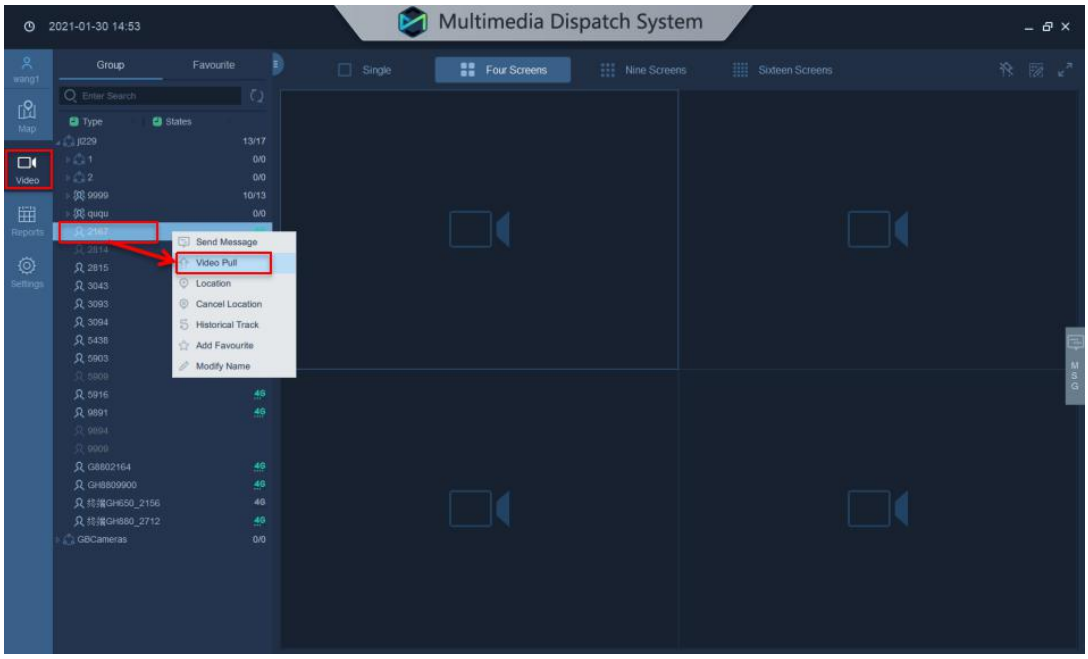


5.2.2 Video Pull

The dispatch console can pull video from cameras and hand-held terminals that access to the system.

Select the user to be pulled in the user list, right click to select **Video Pull** from the shortcut menu as the following figure. You can also pull the end-user video from user list on the Map interface.

Figure 5-34 Operations of the multimedia dispatch video pull



After the video is pulled, the video captured by the user's camera can be viewed on the dispatch console. See the following figure:

Click at the lower right corner of the video window to end the video pull.

Click at the lower right corner of the video window to lock the video angle.

Click at the lower right corner of the video window to automatically rotate the terminal video, that is, the video on the dispatch console is rotated when the terminal rotates.

Click at the lower right corner of the video window to capture the video image.

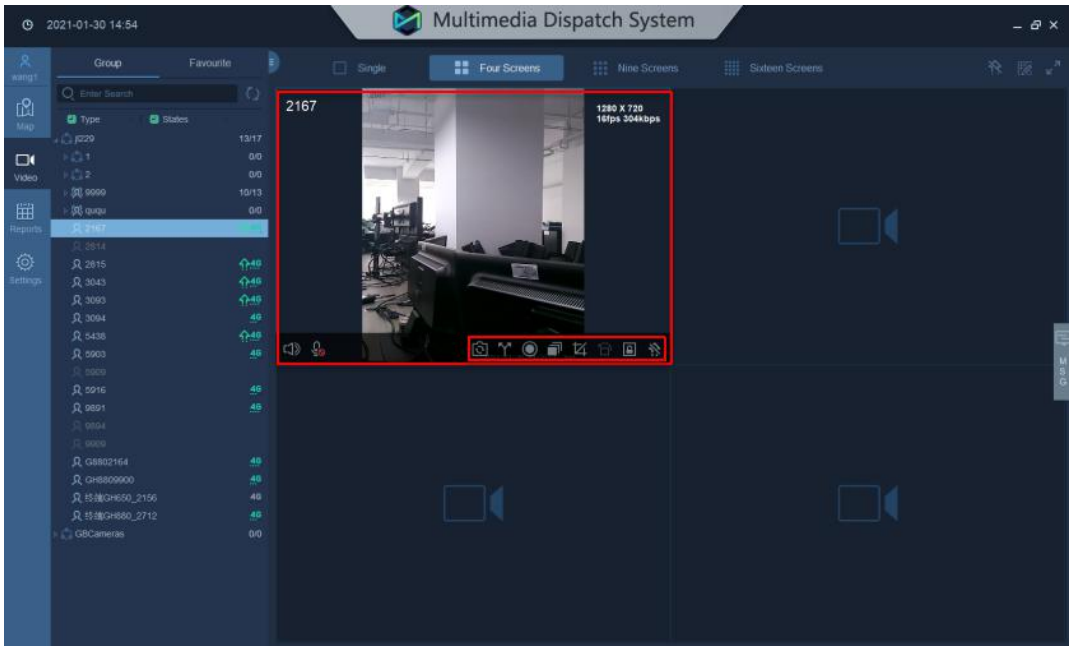
Click at the lower right corner of the video window to capture continuous video images.

Click at the lower right corner of the video window to record the video.

Click at the lower right corner of the video window to distribute terminal video.

Click at the lower right corner of the video window to project the video on the TV wall.

Figure 5-35 Multimedia dispatch video display window

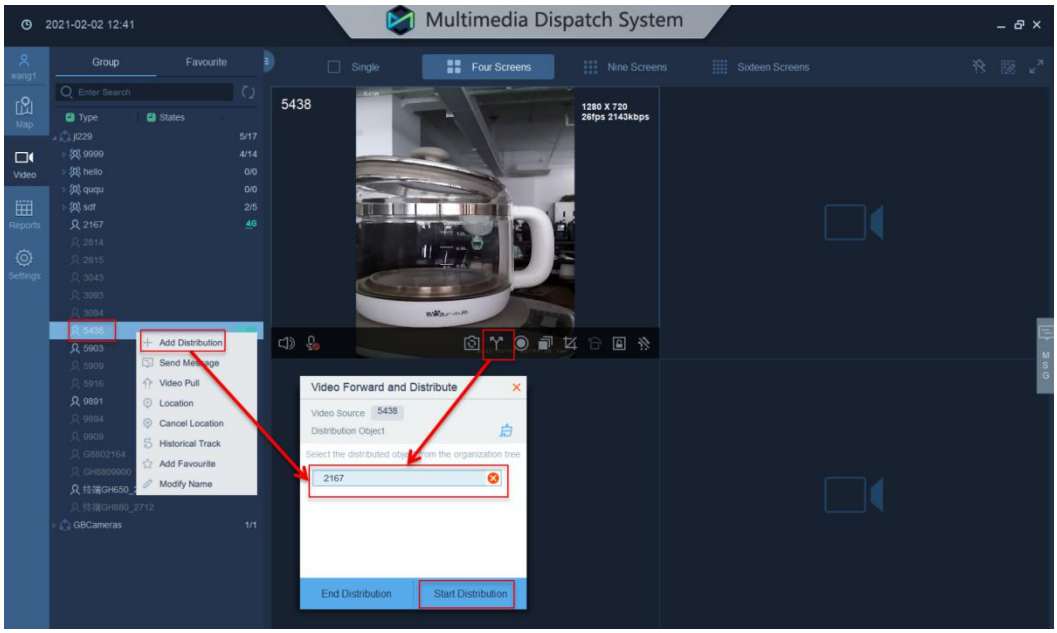


5.2.3 Video Distribution

Dispatch console can distribute the pulled videos to terminals and groups.

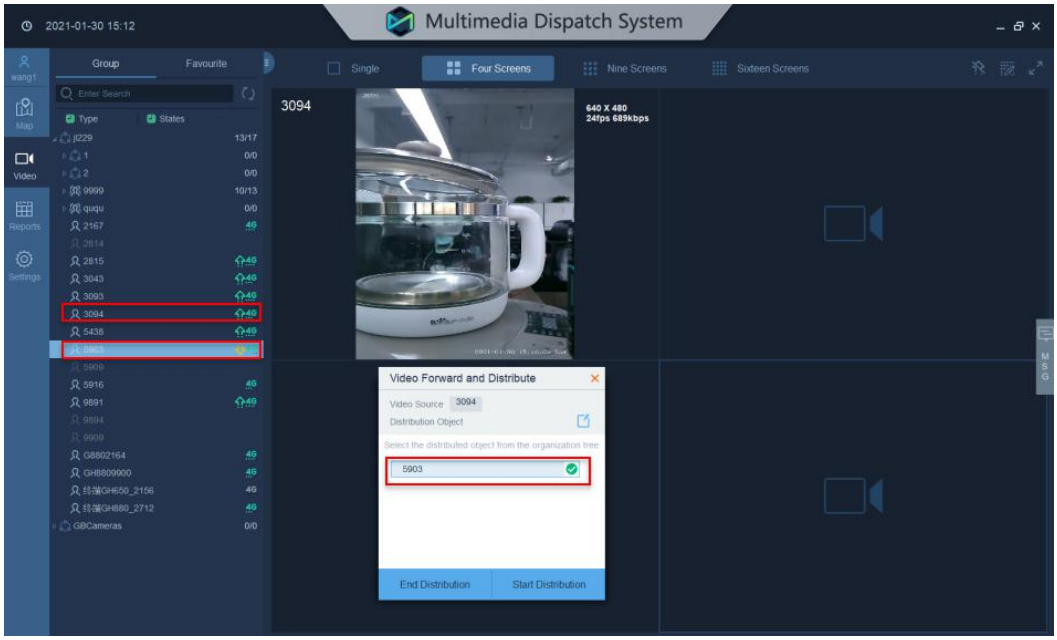
Select a video that has been pulled on the interface of the dispatch console, click on the lower right corner of the window, then the distribution page will pop up. Add the users who need to receive the videos to the distribution page, as the following figure.

Figure 5-36 Multimedia dispatch video distribution



Click **Start Distribution** to distribute the video. For example, after a video is successfully distributed to user 5903, the pull and distribution status will be displayed on both the user list and the distribution list. See the following figure.

Figure 5-37 Video distribution is successful.



After the video is successfully distributed, the screen of terminal will display the video source, as shown below:

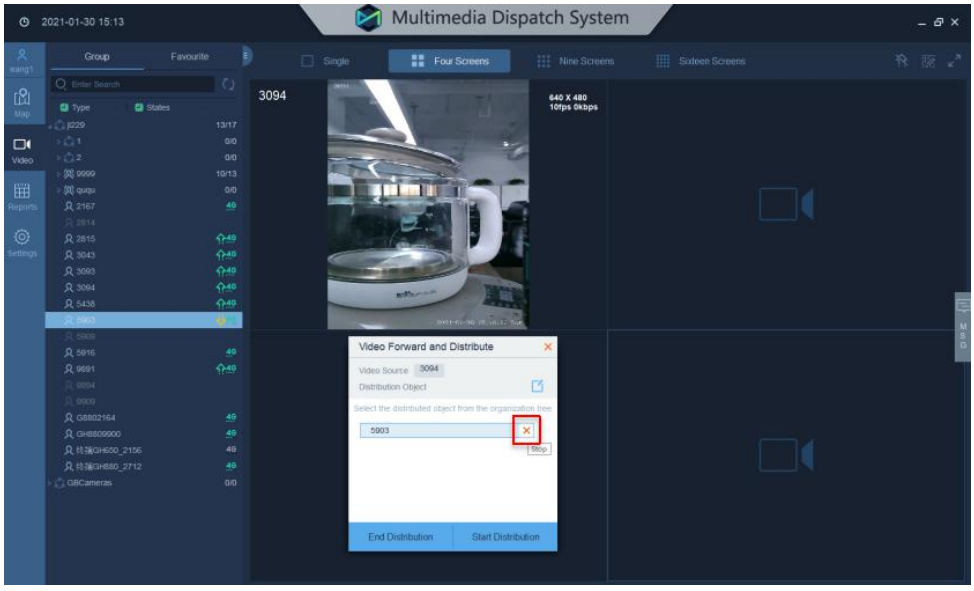
Figure 5-38 Video is distributed to the receiving terminal.

Click **End** on the Terminal who is receiving video to end the video distribution.

Or select the terminal that is distributing videos on the video distribution page of the dispatch console, and click **End Distribution** to end the video distribution, see the following figure.

When ending the pulled video source, the video distribution ends at the same time.

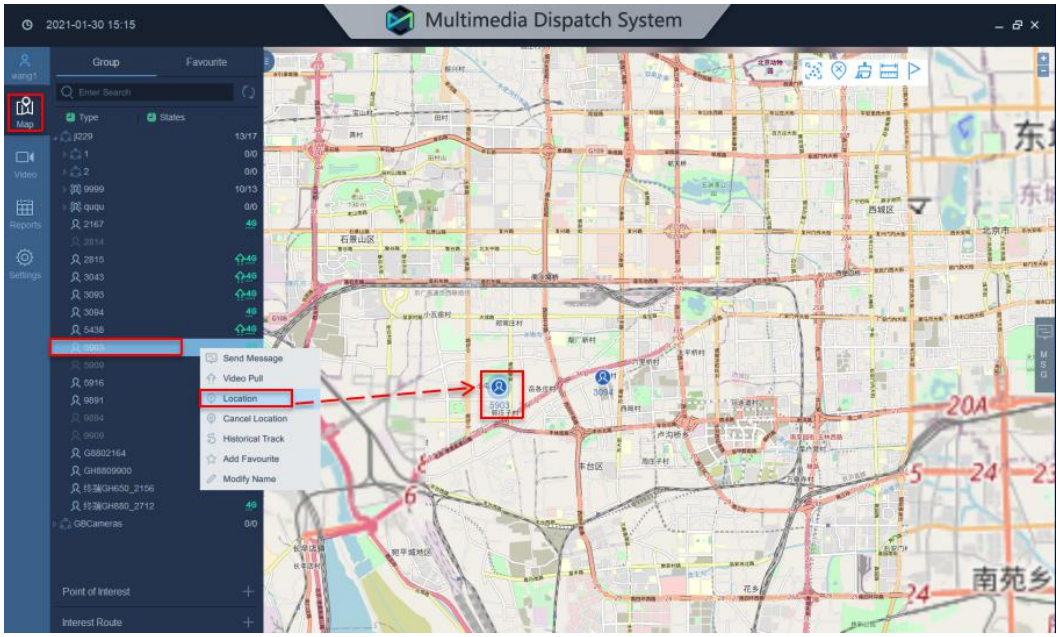
Figure 5-39 Ending video distribution



5.2.4 Location

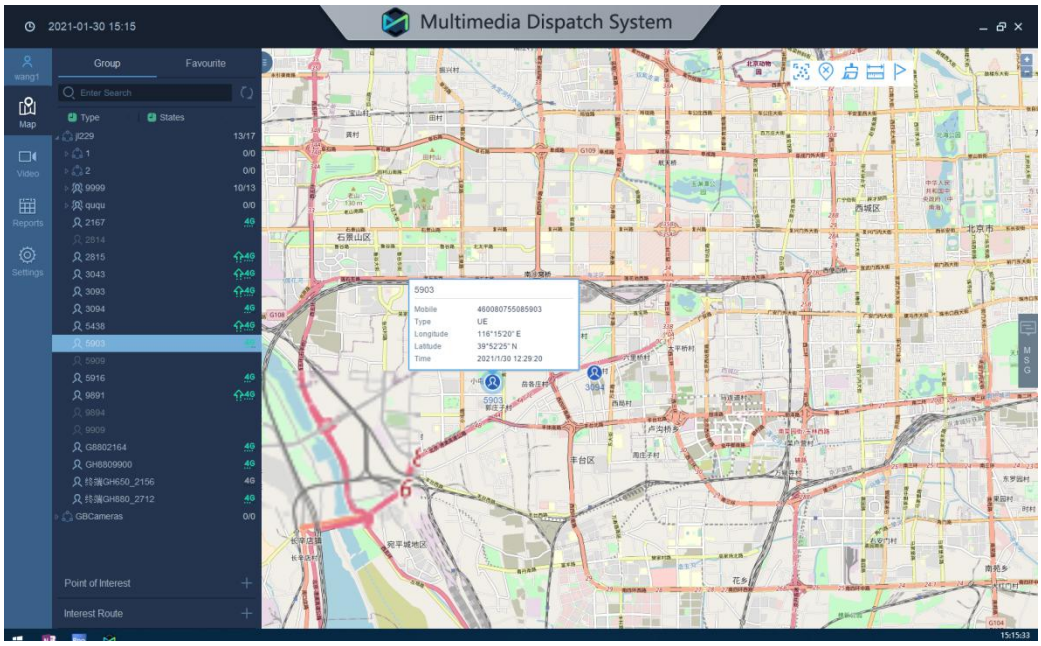
Terminals and groups can be located at the Map interface of the dispatch console. Select the terminal to be located, and select **Location** from the shortcut menu, see the following figure.

Figure 5-40 MDS terminal location operation



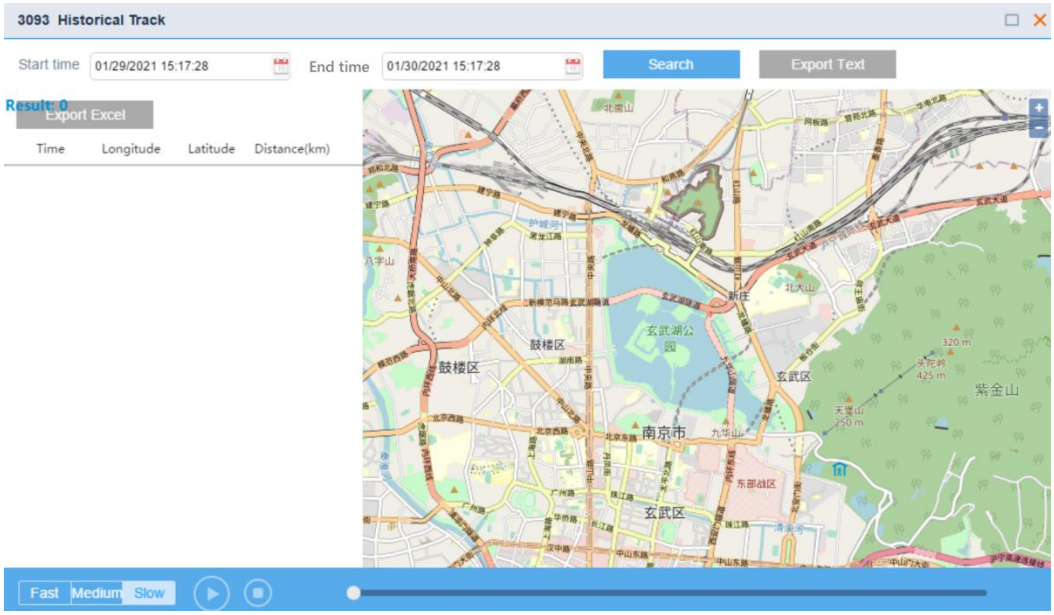
As shown in the above figure, the location of the terminal is displayed clearly on the map. When moving cursor to the terminal, the terminal details will be displayed.

Figure 5-41 MDS location display



Right click the contact list of the terminal and select Historical Track to view the historical track replay of the terminal, as the following figure.

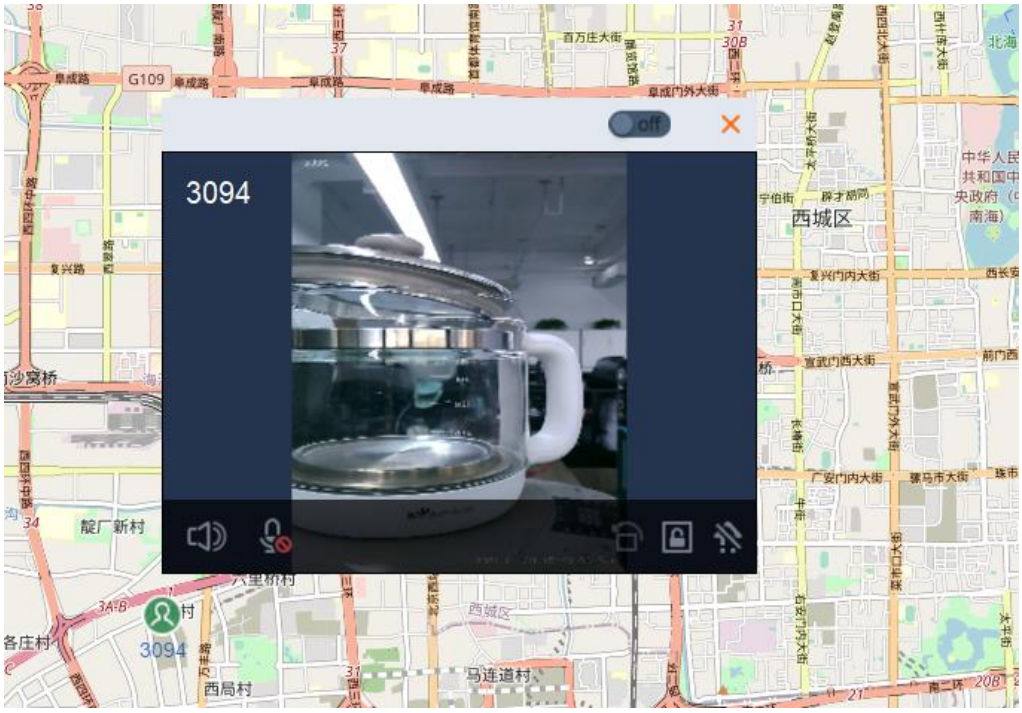
Figure 5-42 Viewing historical track of the terminal



Input the **Start time** and **End time** on the Historical Track page, and click **Search** to query the historical track of the terminal.

Click Video Pull to pull the video, see the following figure.

Figure 5-43 Dispatching the terminal on the Map interface



6 Card Allocation and Number Allocation

6.1 Hand-held Terminal Number Allocation

6.1.1 Login to the unified OMM

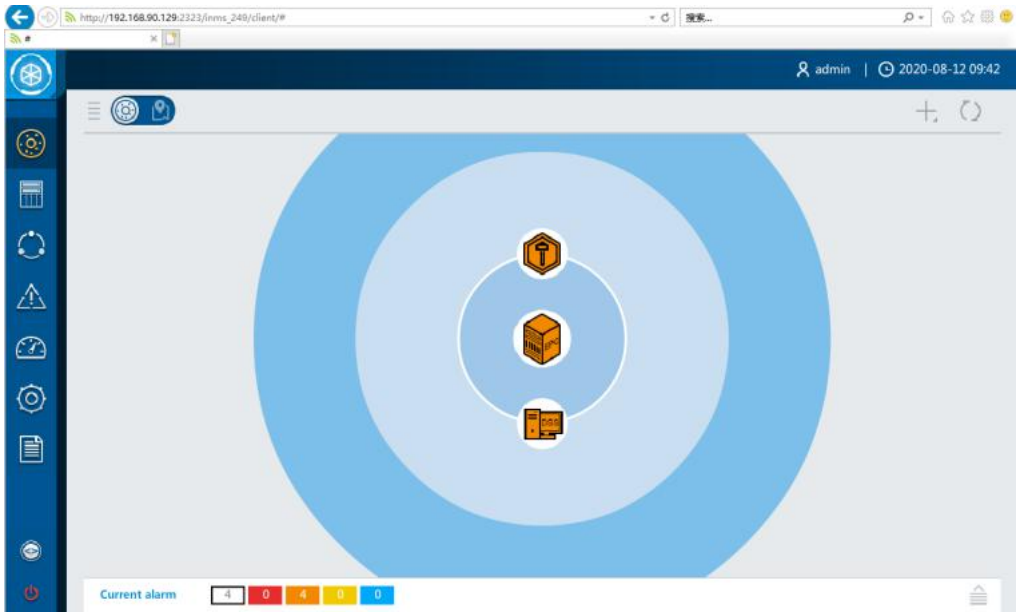
Login to the unified OMM via IE browser (IE 11).

Login address: http://192.168.90.129:2323/inms_ 249/client/#

Login account: admin, password is null.

Note: Different projects may use different login IP addresses, accounts, and passwords. For details, please refer to the project system configuration guide.

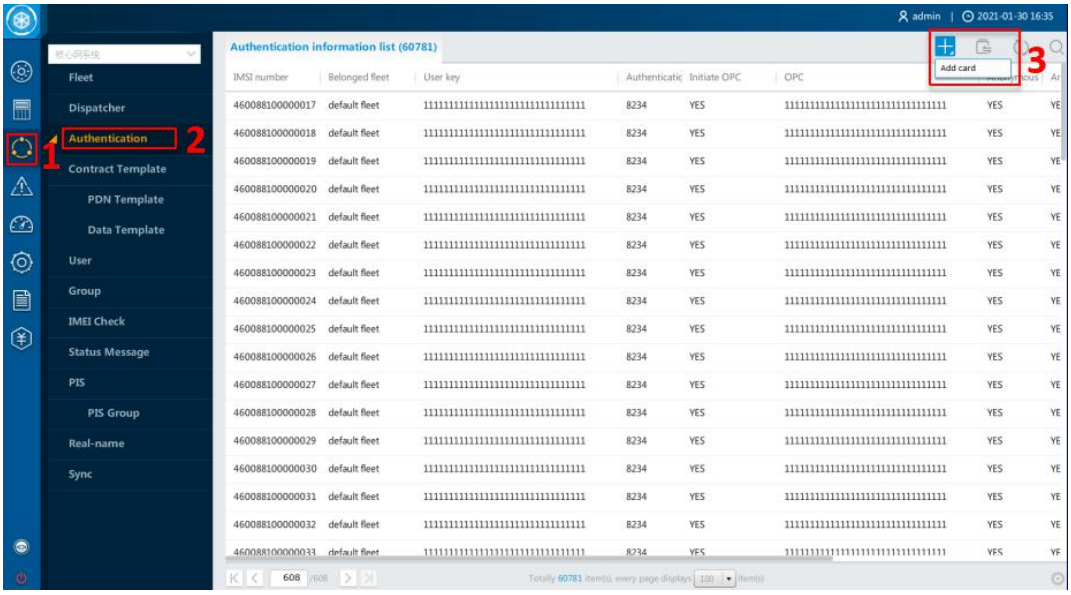
Figure 6-1 Unified OMM interface



6.1.2 User Authentication Information Configuration

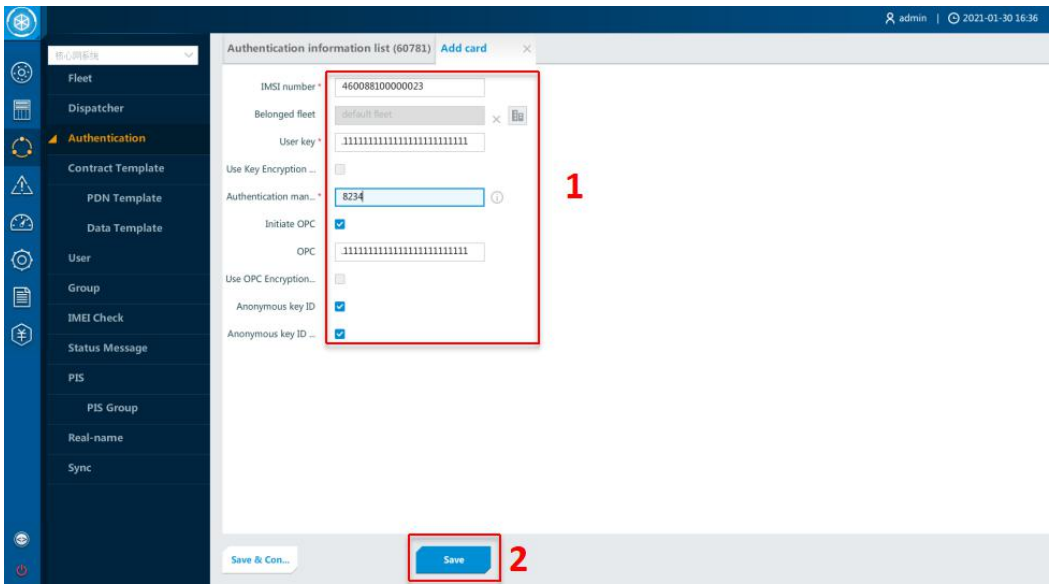
Step1: Click Operation Management , select **Authentication**, and switch to the Authentication information interface. Select **Add card** under the menu to add the user authentication information , see the following figure:

Figure 6-2 Add card



Step 2: Input the IMSI number and SIM card authentication information (User key, Authentication management domain and OPC, can directly copy the existing card information) on the Add card page. Click **Save** to complete operation, as the following figure:

Figure 6-3 Input Add card information

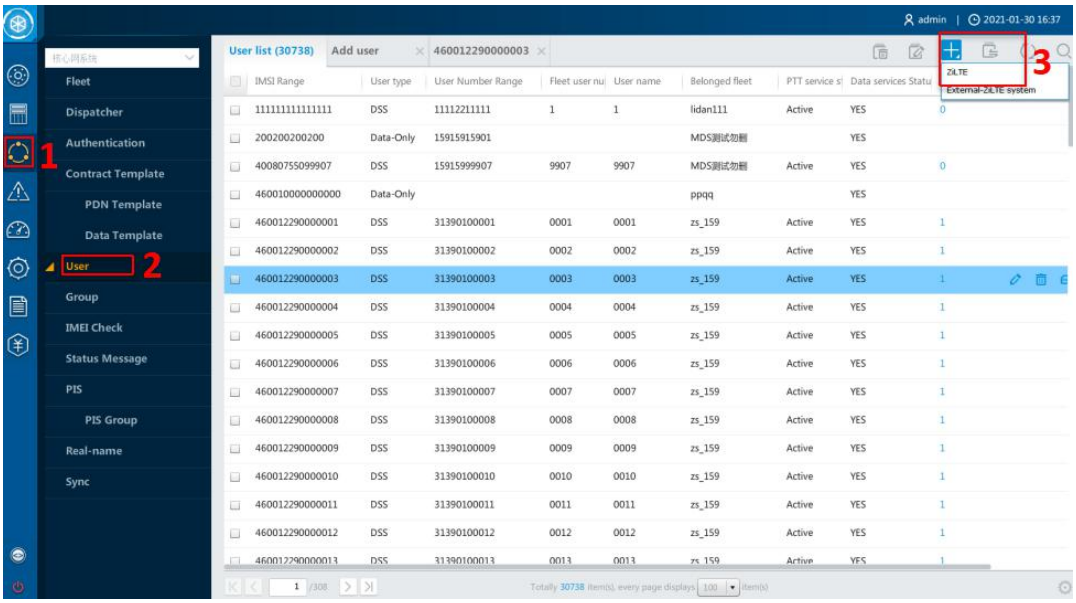


Note: Select the user authentication information to be operated, click and to edit or delete the information.

6.1.3 User Number Allocation

Step 1: Click Operation Management -> User and switch to the user management interface, and select **ZiLTE** under menu on the right to add user:

Figure 6-4 Add user



Step 2: On the pop-up Add user page, input the **IMSI number**, **User number** (beginning with 1880755), tick **Activated data service**, select *iepc.com* as the data service template, tick **Subscribed PTT service**, input **Fleet user number** (recommend the last four digits of IMSI) and User name, and select **Belonged fleet** (by clicking  on the right) for the user. For a vehicle-mounted terminal, tick **Vehicle-mounted terminal** option. Keep the default settings for other parameters, and click **Save**, see the following figure.

Figure 6-5 Input user information-1

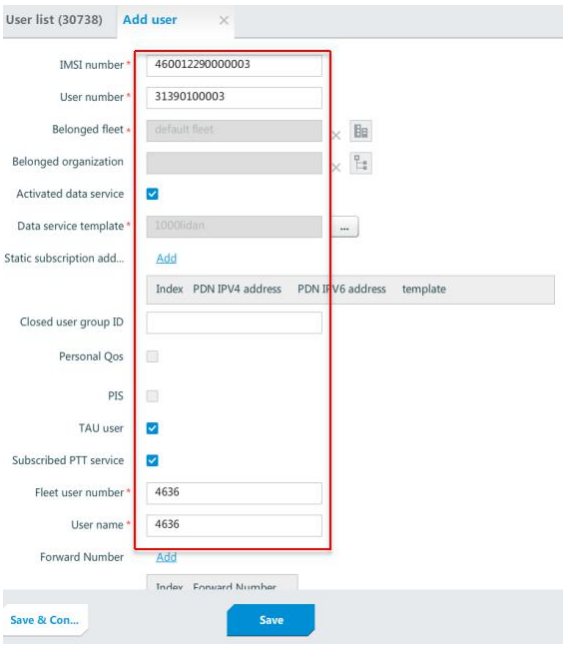
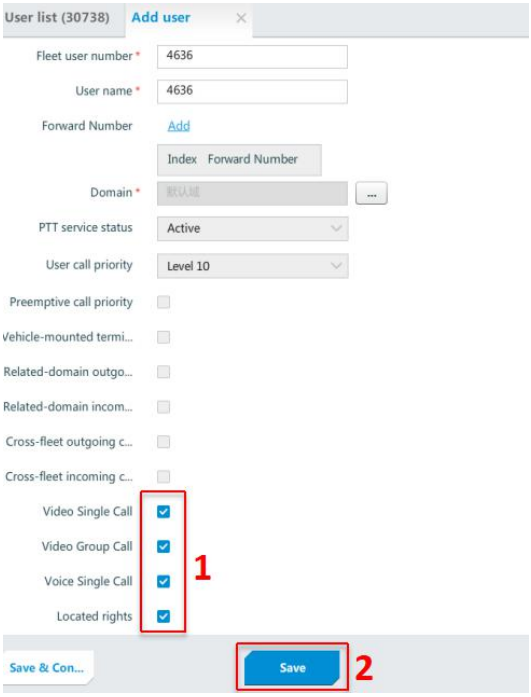


Figure 6-6 Input user information-2

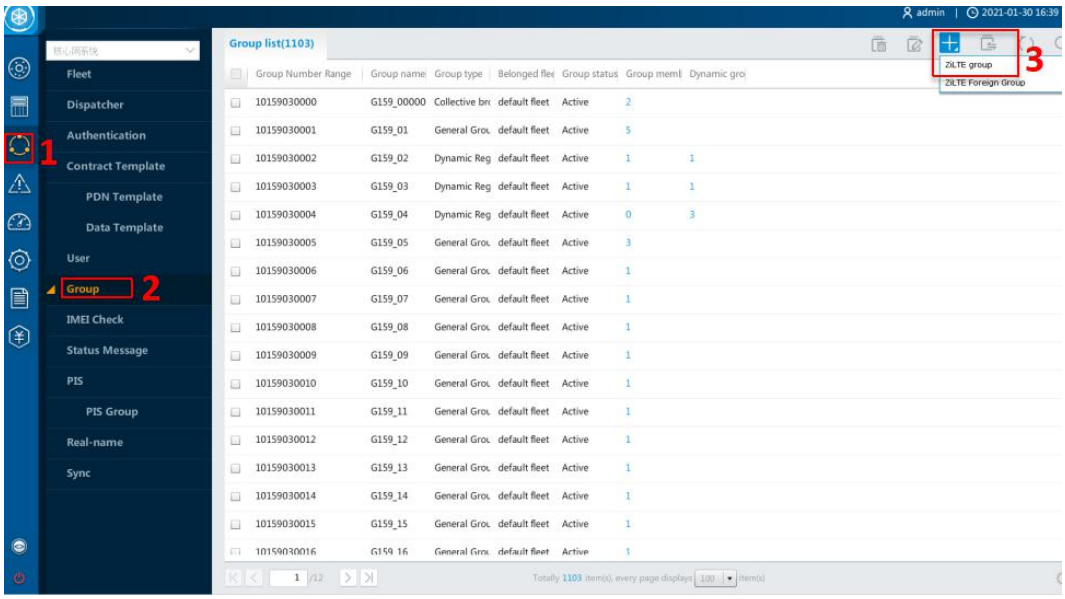


Note: Select the user to be operated, click and to edit or delete the user.

6.1.4 Add Group

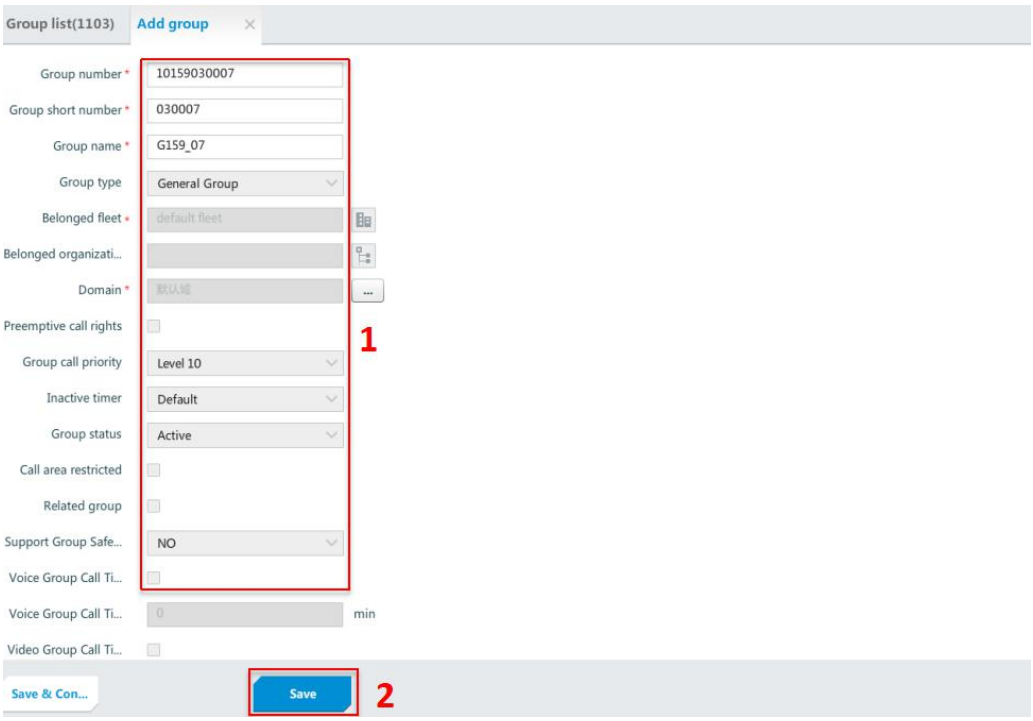
Step1: Click Operation Management  ->Group and switch to the Group management interface, and select **ZiLTE group** under  menu on the right to add group:

Figure 6-7 Add group



Step 2: Input **Group number** (beginning with 6880755), **Group short number**, and **Group name** on the Add group interface. Select **default fleet** (by clicking the  on the right) for the Belonged fleet. Keep the default settings for other parameters, and click **Save**, see the following figure.

Figure 6-8 Group account information setting

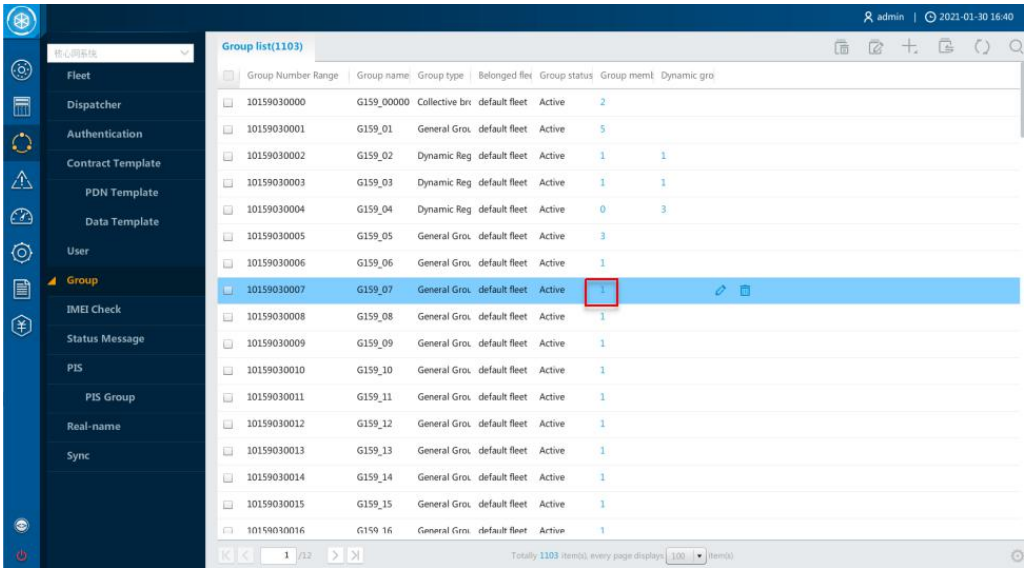


Note: Select the group to be operated, click and to edit or delete the group.

6.1.5 Add group member

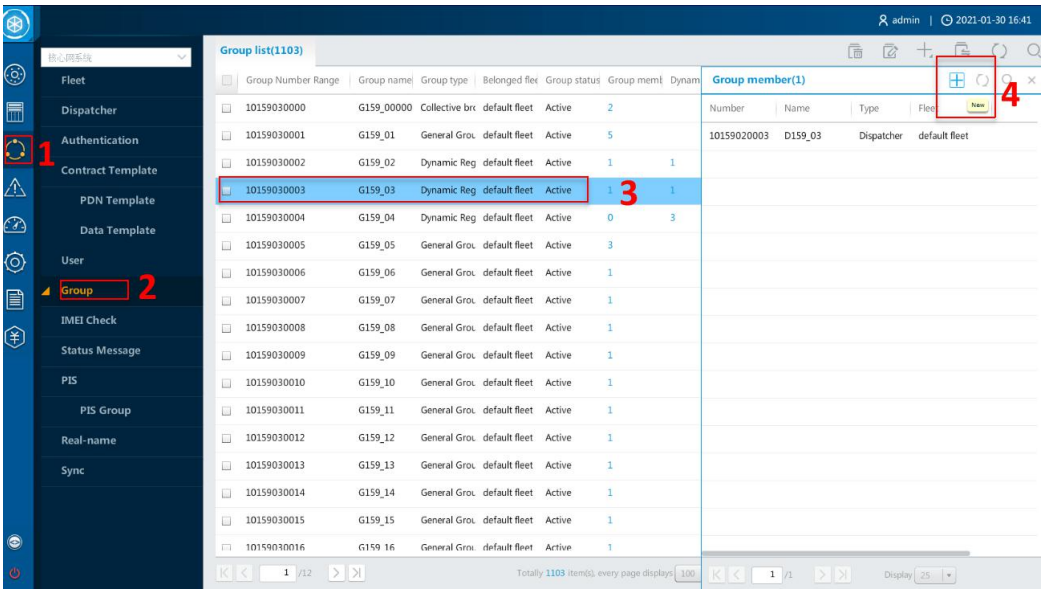
Select the group that need to add group members, and click the number in the **Group member** column, see the following figure.

Figure 6-9 Add group member-1



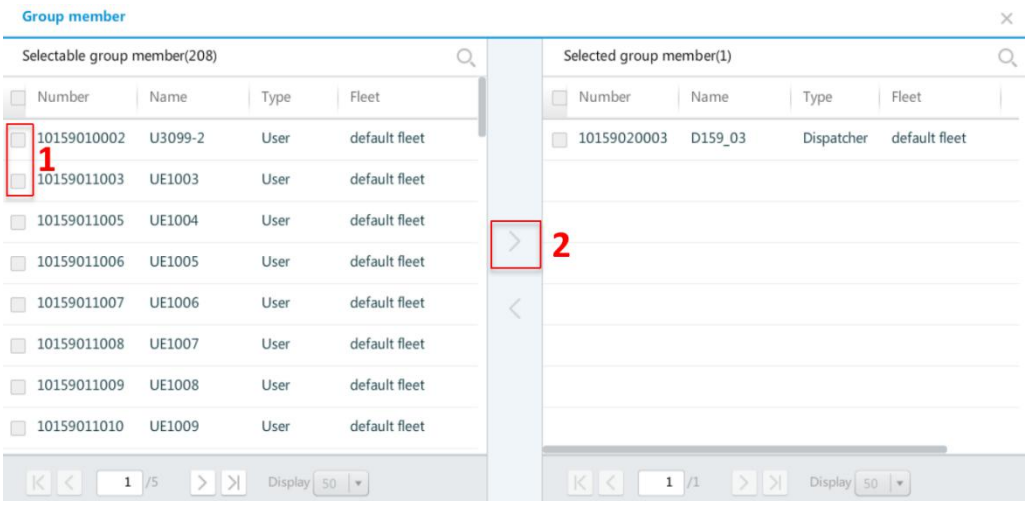
Click on the right of the group member page to display the page for editing group members, see the following figure.

Figure 6-10 Add group member-2



Select the member to be added from the available members list, and click to add the group member, see the following figure.

Figure 6-11 Add group member-3

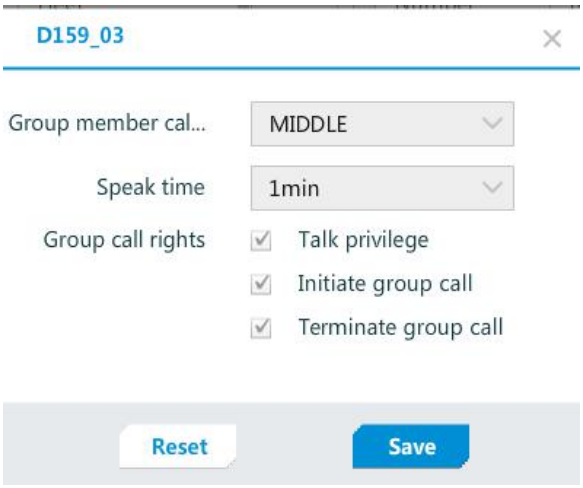


Note: Support add or delete multiple group members.

Note: Select the users to be deleted from the right side, and click to delete the member.

Select the group member to be edited, and click to display the page for editing group member attributes. Modify the information, and click **Save**. The group member attribute will be modified.

Figure 6-12 Modify the group member attribute



6.2 CPE Terminal Number Allocation

6.2.1 Login to the unified OMM

The same as chapter 5.1.1, login to the unified OMM via IE browser (IE 11).

Login address: http://192.168.90.129:2323/inms_ 249/client/#

Login account: admin, password is null.

6.2.2 User Authentication Information Configuration

User authentication information is configured in exactly the same way as described in chapter 5.1.2.

Step1: Click **Authentication** and switch to the Authentication information interface. Select **Add card** under menu on the right to add the user authentication information;

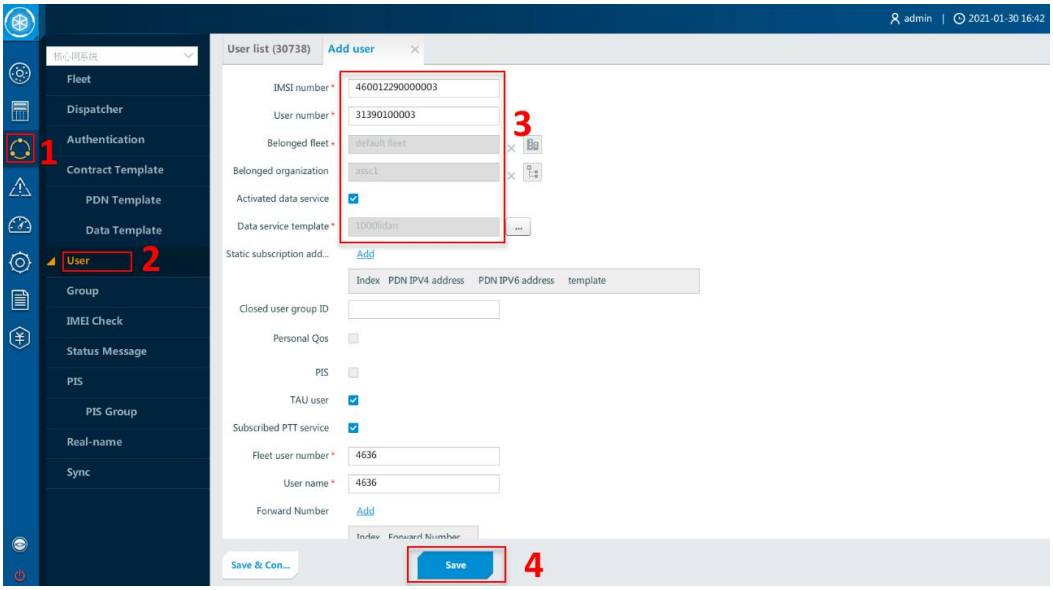
Step 2: Input the IMSI number and SIM card authentication information (User key, Authentication management domain and OPC, can directly copy the existing cards information) on the Add card page. Click Save to complete operation.

6.2.3 User Number Allocation

Step 1: Click Operation Management -> User and switch to the user management interface, select **ZiLTE** under menu on the right to add user. This step is the same as that of hand-held terminal number allocation.

Step 2: Input IMSI number, User number on the interface, select subscription data service and select *cpe.com* as the Data service template. Keep the default settings for other parameters, and click **Save** to add a CPE user information, see the following figure.

Figure 6- 13 Input user information



Note: Select the user to be operated, click and to edit or delete the user.

6.2.4 Login to the LTE Core Network Management Page

Login to the OMM management page of the iEPC (LTE core network) via Web.

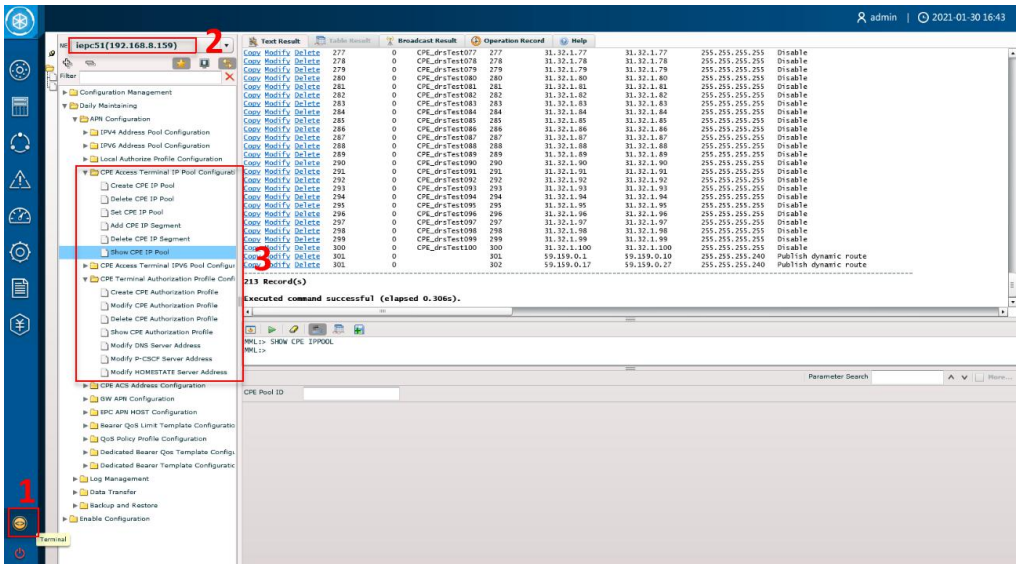
Login address: http://192.168.90.129: 2323/iepc_80/client/#

Login account: admin, the password is null.

Note: Different projects may use different login addresses, accounts, and passwords.

For details, please refer to "access IP address and account/password of the iEPC OMM client " in the system configuration information table.

Figure 6- 14 Enter to expert diagnosis mode on the unified OMM interface.



6.2.5 APN Configuration

The APN configuration mainly include **CPE Access Terminal IP Pool Configuration** and **CPE Terminal Authorization Profile Configuration**.

6.2.5.1 CPE Access Terminal IP Pool Configuration

Login to the iEPC management interface, select from the menu on the left: Daily Maintaining ->APN Configuration ->CPE Access Terminal IP Pool Configuration -> **Show CPE IP Pool**, and click  , the system will display all IP pool configuration information.

Select **Create CPE IP Pool** to add a CPE IP pool. Input the information and click  to execute.

CPE pool ID: Number of the address pool, which must be unique.

VRF ID: Defaults to 0.

Select **Add CPE IP Segment** and add the IP segment information to the corresponding IP pool. Input the information and click  to execute.

Segment ID: The number of the address segment is recommended to be the same as the number of the IP pool added in the previous step.

CPE Pool ID: The same as the address pool ID added in the previous step.

IP Segment Start, IP Segment End, and Mask: Determine the IP pool configuration together. Options:

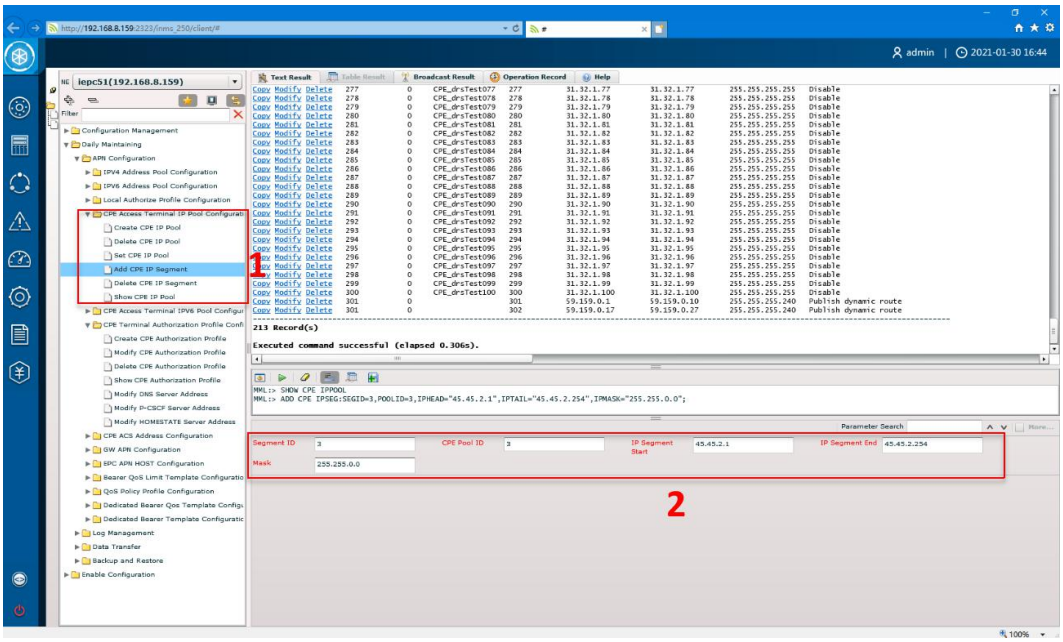
IP Segment Start:45.45.x.1

IP Segment End: 45.45.x.254

Mask: 255.255.0.0

x represents any number of 0-254. The x of the IP Segment Start is the same as the IP Segment End.

Figure 6- 15 Add CPE IP Pool and IP Segment.



Perform **Show CPE IPPool** again to check whether it is added successfully.

6.2.5.2 CPE Terminal Authorization Profile Configuration

Select from the menu on the left: Daily Maintaining ->APN Configuration -> CPE Terminal Authorization Profile Configuration -> Show CPE authorization Profile, and click , the system will display all CPE authorization Profile configuration information.

Select **Create CPE Authorization Profile** and add the CPE authorization information. Input corresponding information and click to execute.

Profile ID: The same as the Profile ID number corresponding to the CPE configured in the GW APN. It is generally set to 1.

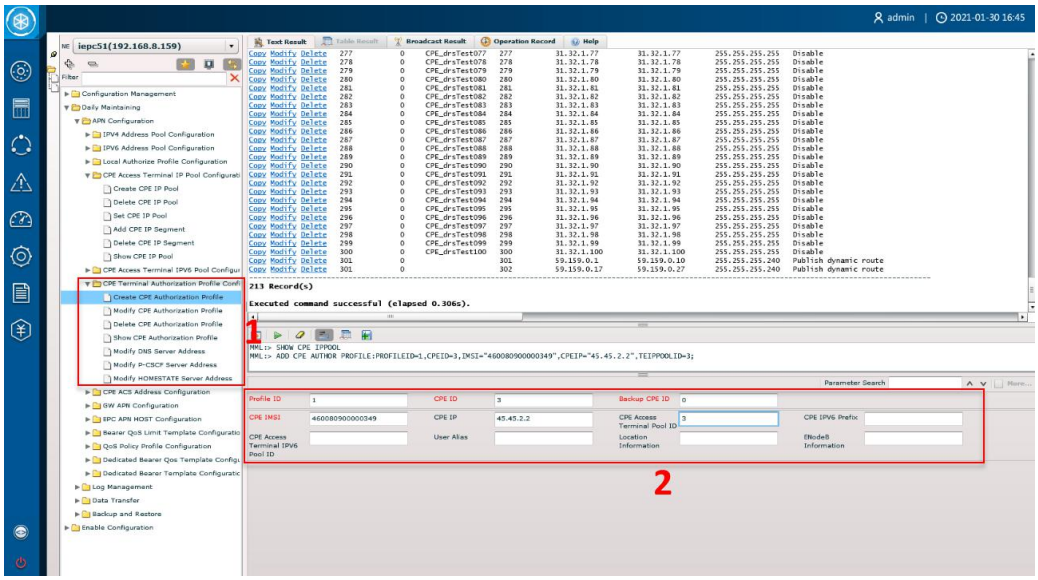
CPE ID: The CPE ID cannot be the same as the existing CPE ID. Recommend to configure the same number as the corresponding pool ID.

CPE IMSI: Input the IMSI number of the SIM card of the CPE to be added.

CPE IP: The IP address used by the CPE to obtain wireless signal, which is the corresponding IP address inside the IP pool (recommend: 45.45.x.2, where x is the IP network segment of the corresponding address pool).

CPE Access Terminal Pool ID: Configure IP pool ID in the CPE Access Terminal IP Pool Configuration .

Figure 6-16 Create CPE Authorization Profile



Perform **Show CPE authorization Profile** again to check whether it is added successfully.

6.2.6 Synchronize Data

Synchronize related data to the system after completing the above steps.

Select from the menu on the left: Daily Maintaining -> Data Transfer -> Synchronize EPC Data, click , and select "Yes" on the pop-up dialog box to complete the configuration data synchronization.

Or directly input SYNC EPC in the command line to synchronize data.

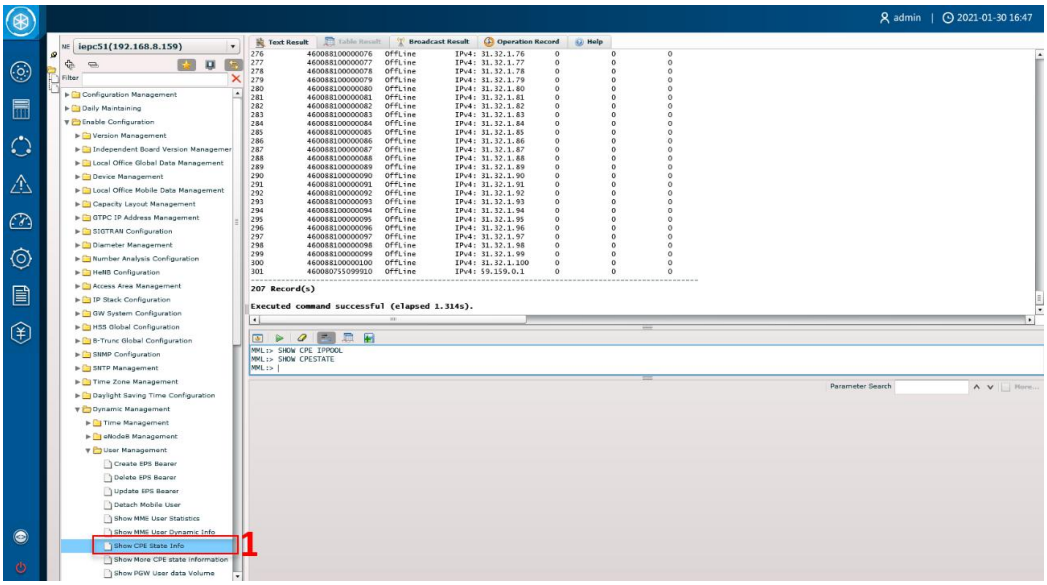
6.2.7 Show CPE Access Status

Select from the menu on the left: Daily Maintaining -> Dynamic Management -> User Management -> Show CPE State Info.

Click and check the CPE access status.

Or, input **SHOW CPESTATE** directly in the command line to check the CPE access status.

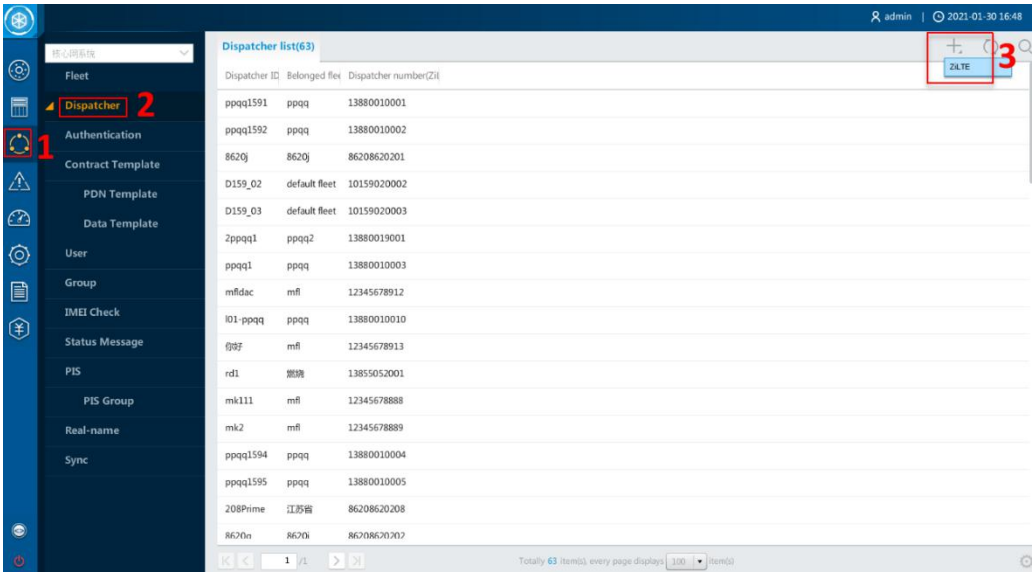
Figure 6-17 Show CPE access status



6.3 Dispatcher Management

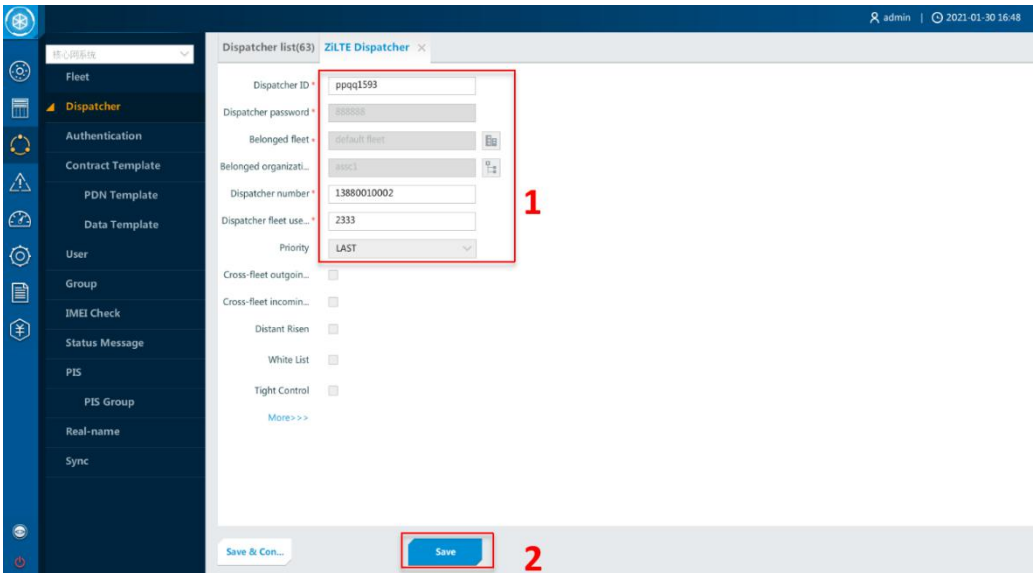
Step1: Select Operation Management -> Dispatcher, switch to the dispatcher management interface. Click + on the right side to show interface of adding a dispatcher.

Figure 6-18 Add dispatcher account



Step2: Input the corresponding information according to the interface requirements (the dispatcher number beginning with 8880755, 11 digits), and click **Save** at the bottom to complete the operation of adding a dispatcher, see the following figure:

Figure 6-19 Setting dispatcher account information



Select the dispatcher to be operated, click and to edit or delete the dispatcher.

7 References

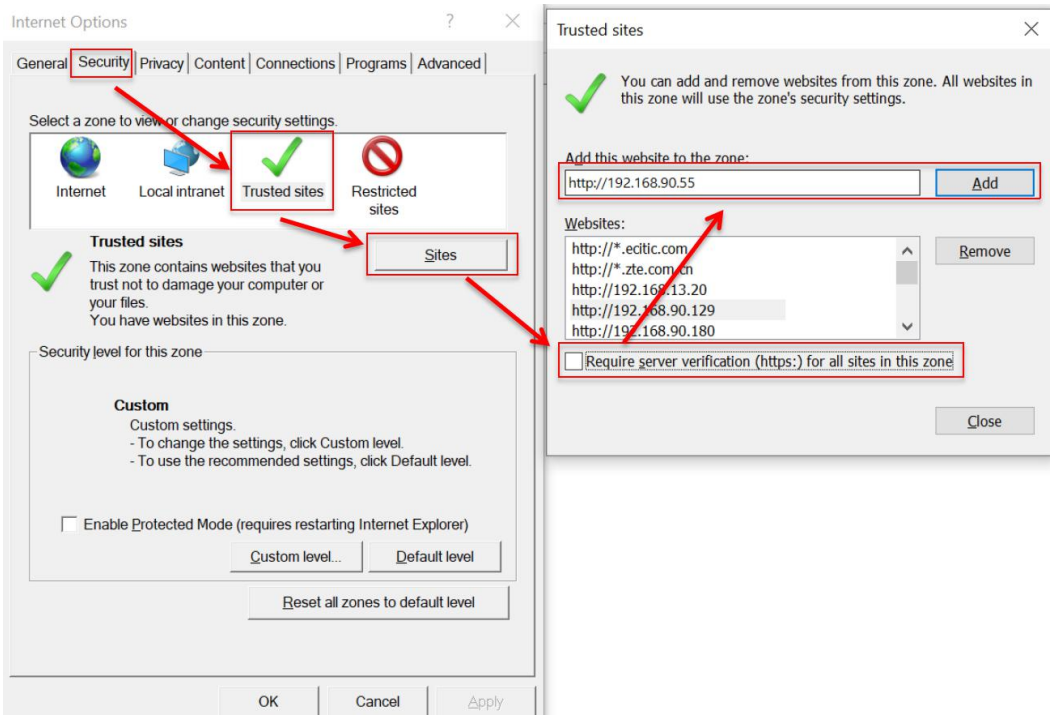
7.1 Manually Add Trusted Sites to the IE Browser

IE 11 (win 7 32-bit operating system) is used for the login and related operations of the dispatch console and OMM of the ZiLTE system. It's required to configure the IE browser when login to the dispatch console for the first time, otherwise, it will fail to login (if cannot login to the dispatch console, please check whether the IE settings have been modified).

Open the IE browser, and select [Tools ->Internet Options] from the toolbar, open the Internet Options dialog box. Select [Security] ->[Trusted sites] ->[Sites], open the Trusted sites page, see the following figure:

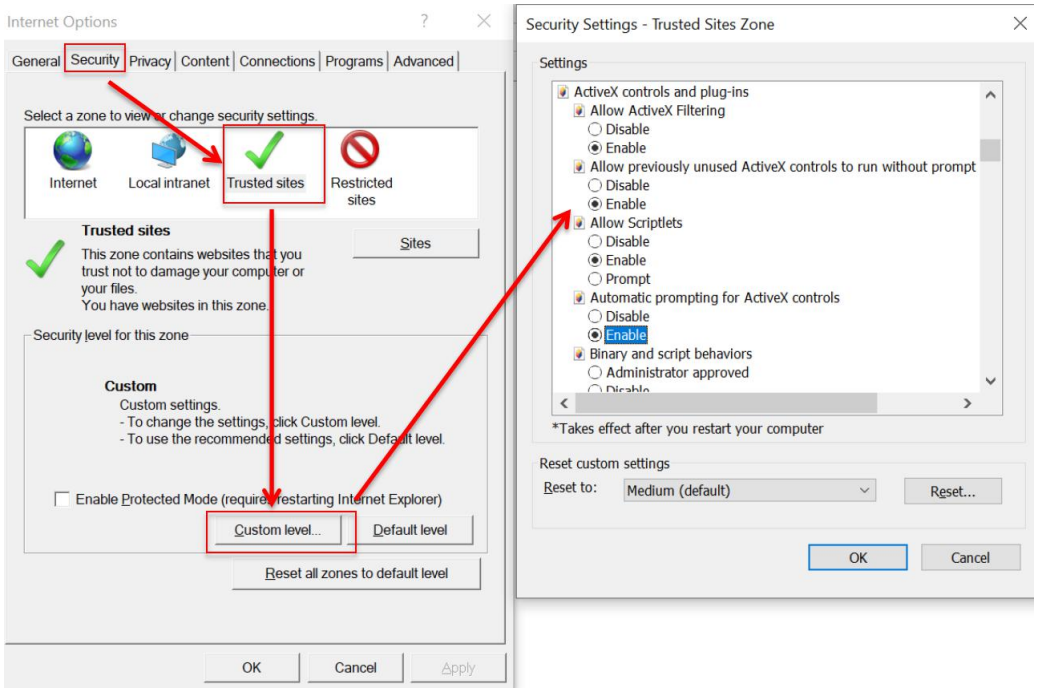
Add the IP address of the dispatch console to the trusted site. For example, take the IP address of the dispatch console as 192.168.90.55. Input **http://192.168.90.55**, remove the check mark from check box of "Require server verification (https) for all sites in this zone" , no server verification is required. Click **Add**, and then click **Close** to exit the settings of trusted sites.

Figure 7-1 Trusted sits setting of the Internet Options



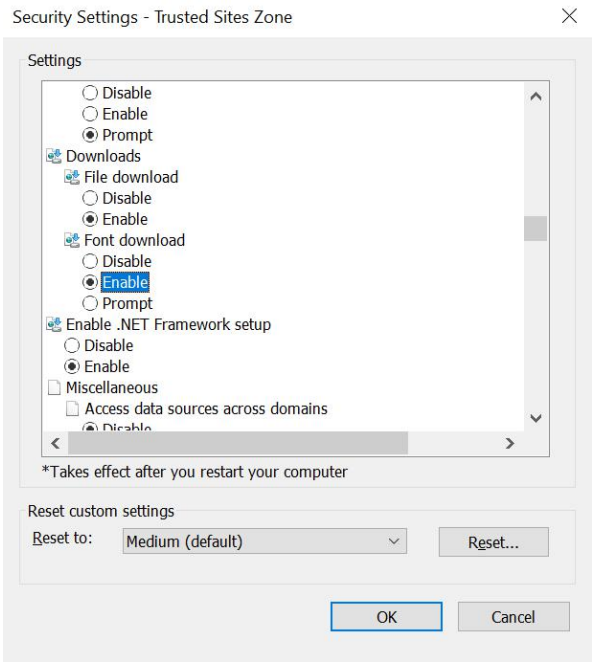
Return to the page of Internet Options [Security], select **Trusted sites** and click **Custom level** to enter the Security Settings - Trusted Sites Zone page to set the security level of the trusted sites. Set all the sub-items under **ActiveX controls and plug-ins** to **Enable**, see the following figures.

Figure 7-2 Security settings of trusted sites-1



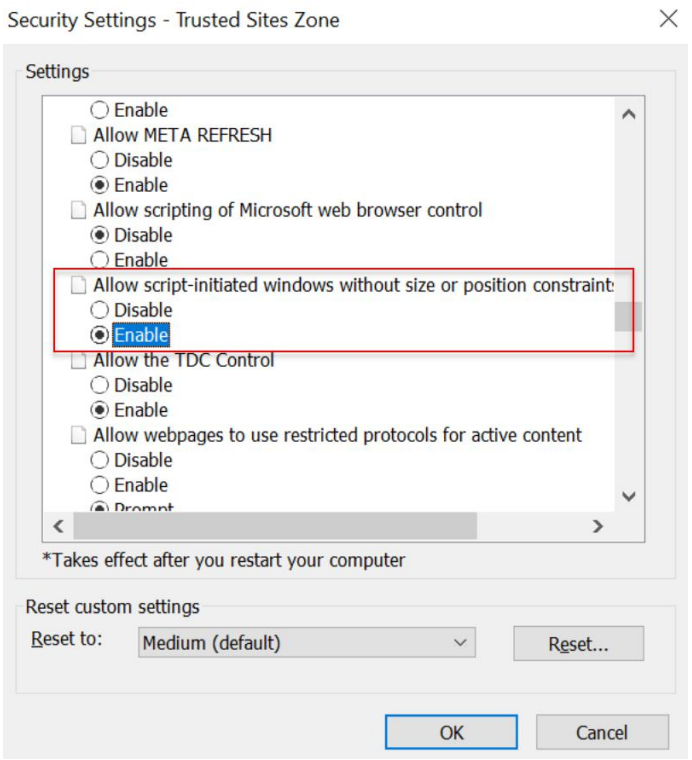
Set all the sub-items under Downloads to **Enable**, see the following figures.

Figure 7-3 Security settings of trusted sites-2



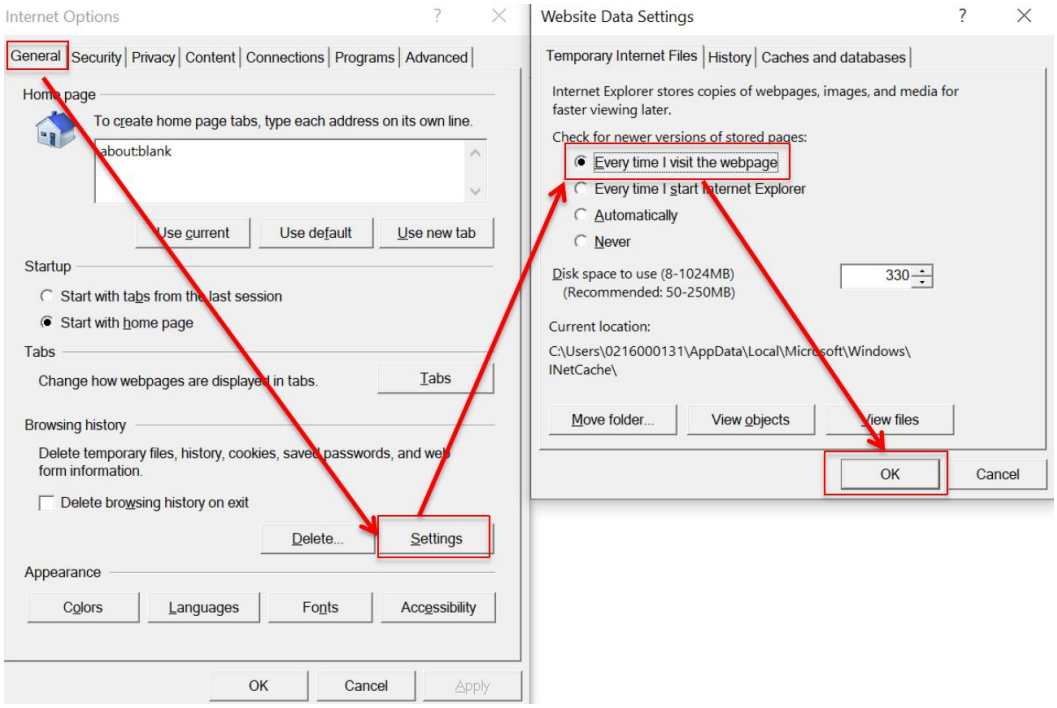
Select Enable for "Allow script-initiated windows without size or position constraints", click OK.

Figure 7-4 Security settings of trusted sites-3



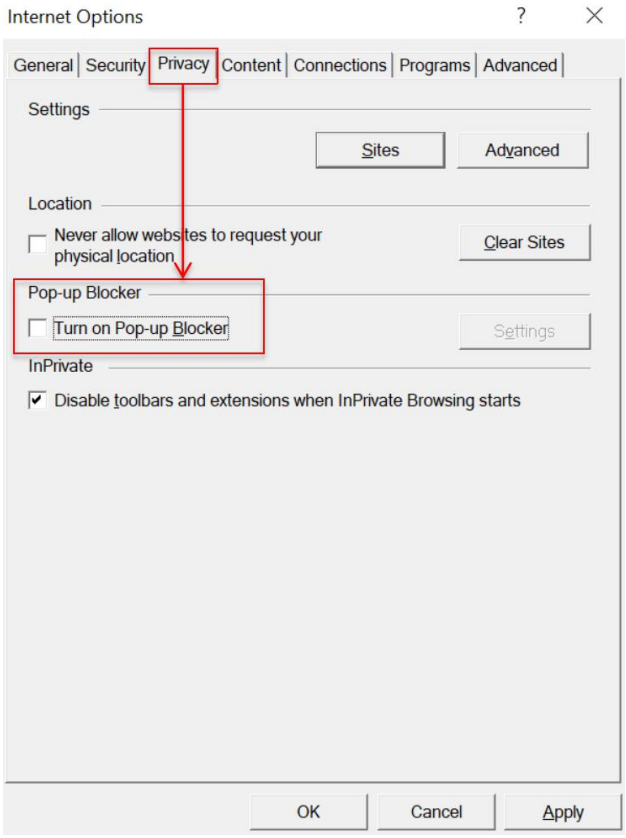
Return to the page of Internet Options [General], and click **Settings** to enter the Temporary Internet Files page. Select [**Every time I visit the webpage**] -> [**OK**], see the following figure.

Figure 7-5 Temporary Internet Files Settings



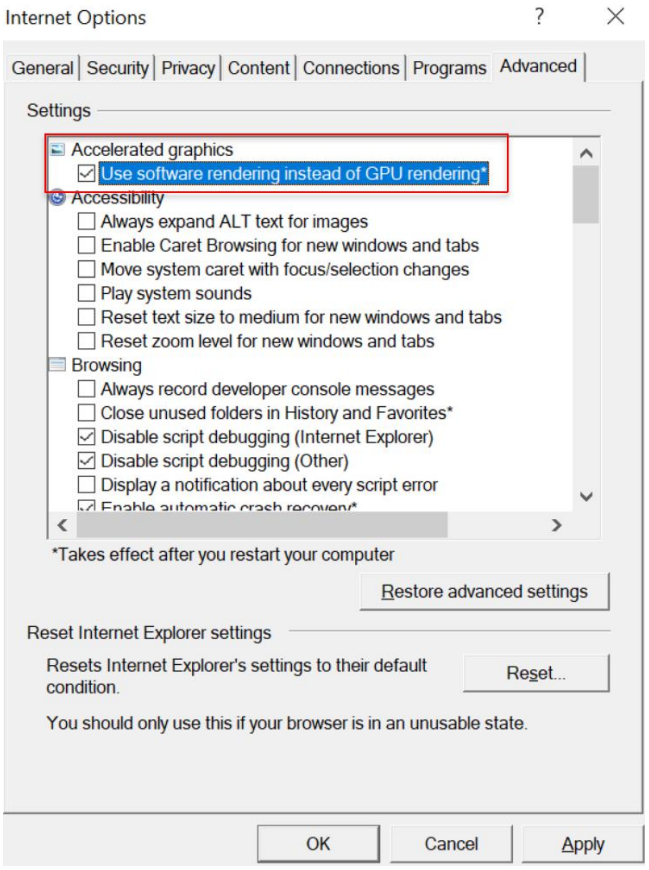
Switch to the page of Internet Options [Privacy], and remove the check mark of "**Turn on Pop-up Blocker**" .

Figure 7-6 Uncheck "Turn on Pop-up Blocker"



Switch to the page of the Internet Options [Advanced] . tick “**Use software rendering instead of GPU rendering**”, click **OK**.

Figure 7-7 Advanced Setting of Internet Option



Restart the IE browser to validate the configuration.

7.2 Appendix A.1.1

7.2.1 Appendix A.1.1.1

Attention

Precautions:

