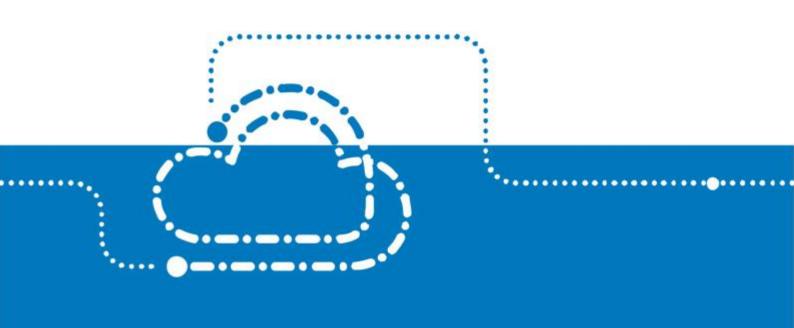


ZXIMCU PT01 P200 Portable Emergency Command System Operation Manual



Version update instruction

Version	Date	Author	Auditor	Remark
1.0	2021-01-19			

© 2021 Copyright Caltta Technologies Co.,Ltd. All rights reserved Copyright statement:

The copyright of this document belongs to Caltta Technologies Co.,Ltd. Text contains proprietary information owned by Caltta Technologies Co.,Ltd., without the written permission of Caltta Technologies Co.,Ltd., any unit or individual shall not use or leak any document and Figures, this document contains tables, Figure, data and other information. The information in this document contains the development progress of Caltta Technologies Co.,Ltd. products and technology will continue to update, Caltta Technologies Co.,Ltd. would not notice such information updates. Privacy Policy:

Caltta Technologies Co.,Ltd. is a global leader in trunking communications and information technology, the company has committed to complying with appropriate regulations to personal data security. In order to protect it, a lot of essential security technical measures should be taken such as anonymous, data encryption.

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

1 OVERVIEW	.1
2 ZXIMCU PT01 P200 VERSION 3.0	1
2.1 INTRODUCTION OF ZXIMCU PT01 P200 VERSION 3.0	. 1
2.2 ZXIMCU PT01 P200 CONNECTION OPERATION	.4
3 NETWORK ARCHITECTURE INTRODUCTION	7
4 DISPATCHING PC CONFIGURATION	.8
4.1 IP ADDRESS SETTING	.8
4.2 IE 11 BROWSER SETTING	.9
5 TRUNKING SERVICES OPERATIONS 1	10
5.1 OPERATIONS OF DAS UNIFIED DISPATCH CONSOLE1	0
5.1.1 DISPATCH CONSOLE INSTALLATION1	-
5.1.2 DISPATCH CONSOLE LOGIN 1	1
5.1.3 DISPATCH CONSOLE INTERFACE INTRODUCTION1	3
5.1.4 DISPATCH CONSOLE INITIATES A HALF-DUPLEX VOICE PRIVATE CALL 1	9
5.1.5 DISPATCH CONSOLE INITIATES A FULL-DUPLEX VOICE PRIVATE CALL.2	20
5.1.6 DISPATCH CONSOLE INITIATES A FULL-DUPLEX VIDEO PRIVATE CALL.2	20
5.1.7 DISPATCH CONSOLE INITIATES A VOICE GROUP CALL	21
5.1.8 DISPATCH CONSOLE INITIATES A VIDEO GROUP CALL	21
5.1.9 SENDING SMS AND MMS2	22
5.1.10 FORCED RELEASE AND FORCED INSERTION BY THE DISPATCHER 2	22
5.1.11 DYNAMIC REGROUP2	23
5.1.12 TEMPORARY GROUP CALL	24
5.1.13 EMERGENCY CALL	25
5.1.14 DISPATCH CONSOLE LOCATION	25
5.1.15 FRAME SELECT AND DISPATCH ON THE MAP	27
5.1.16 DISPATCH CONSOLE INITIATES VIDEO PULL	28
5.1.17 DISPATCH CONSOLE INITIATES VIDEO DISTRIBUTION	30
5.2 OPERATIONS OF MULTIMEDIA DISPATCH SYSTEM	31
5.2.1 DISPATCHER LOGIN	32



5.2.2 VIDEO PULL	32
5.2.3 VIDEO DISTRIBUTION	
5.2.4 LOCATION	37
6 CARD ALLOCATION AND NUMBER ALLOCATION	39
6.1 HAND-HELD TERMINAL NUMBER ALLOCATION	
6.1.1 LOGIN TO THE UNIFIED OMM	39
6.1.2 USER AUTHENTICATION INFORMATION CONFIGURATION	40
6.1.3 USER NUMBER ALLOCATION	41
6.1.4 ADD GROUP	44
6.1.5 ADD GROUP MEMBER	45
6.2 CPE TERMINAL NUMBER ALLOCATION	47
6.2.1 LOGIN TO THE UNIFIED OMM	47
6.2.2 USER AUTHENTICATION INFORMATION CONFIGURATION	47
6.2.3 USER NUMBER ALLOCATION	48
6.2.4 LOGIN TO THE LTE CORE NETWORK MANAGEMENT PAGE	
6.2.5 APN CONFIGURATION	49
6.2.6 SYNCHRONIZE DATA	51
6.2.7 SHOW CPE ACCESS STATUS	51
6.3 DISPATCHER MANAGEMENT	52
7 REFERENCES	54
7.1 MANUALLY ADD TRUSTED SITES TO THE IE BROWSER	-
7.2 APPENDIX A.1.1	59
7.2.1 APPENDIX A.1.1.1	59



Figure Index

Figure 2-1	ZXIMCU PT01 P200 MPU	1
Figure 2-2	ZXIMCU PT01 P200 RRU	2
Figure 2-3	ZXIMCU PT01 P200 Power Line	3
Figure 2-4	ZXIMCU P200 device	4
Figure 2-5	Connection between MPU and RRU with the the power line	4
Figure 2-6	Connection of the feeder and antenna	4
Figure 2-7	Connection of GPS antenna	5
Figure 2-8	Power switch and indicator light	6
Figure 2-9	Connection of the dispatch console	6
Figure 3-1	System Network Architecture	7
Figure 4-1	Adding Route	9
Figure 4-2	Download plug-in and script on the OMM interface	9
Figure 4-3	Trusted site script setting of IE browser	
Figure 5-1	Downloading client and plug-ins of the dispatch console	11
Figure 5-2	Selecting dispatch console local IP address	11
Figure 5-3	Login interface of the dispatch console	12
Figure 5-4	Dispatch console interface	13
Figure 5-5	Dispatch console interface layout	14
Figure 5-6	Add user to dispatching operation area	15
Figure 5-7	Remove user from dispatching operation area	15
Figure 5-8	Sound channel selection	16
Figure 5-9	User call attribute setting	16
Figure 5-10	Group call attribute setting	17
Figure 5-11	Dispatcher call attribute setting	17
Figure 5-12	GIS interface of the dispatch console	
Figure 5-13	Video dispatch interface	19
Figure 5-14	Dispatch console initiates a half-duplex voice private call	19
Figure 5-15	Dispatch console initiates a full-duplex voice private call	
Figure 5-16	Dispatch console initiates a full-duplex video private call	20
Figure 5-17	Dispatch console initiates a voice group call	21
Figure 5-18	Dispatch console initiates a video group call	
Figure 5-19	Sending SMS and MMS	

Figure 5-20	Forced release by the dispatcher	23
Figure 5-21	Forced insertion by dispatcher	23
Figure 5-22	Dynamic regroup	24
Figure 5-23	Temporary group call	25
Figure 5-24	Emergency call	25
Figure 5-25	Dispatch console location operation	26
Figure 5-26	Map interface display and operation	27
Figure 5-27	Frame select on the map	27
Figure 5-28	Frame select and dispatch on the map	
Figure 5-29	Dispatch console initiates a video pull	29
Figure 5-30	Toolbar of the video display window	30
Figure 5-31	Dispatch console Initiates video distribution	31
Figure 5-32	Client Installation of the Multimedia Dispatch System	31
Figure 5-33	MDS client logging	
Figure 5-34	Operations of the multimedia dispatch video pull	33
Figure 5-35	Multimedia dispatch video display window	34
Figure 5-36	Multimedia dispatch video distribution	35
Figure 5-37	Video distribution is successful	35
Figure 5-38	Video is distributed to the receiving terminal	36
Figure 5-39	Ending video distribution	36
Figure 5-40	MDS terminal location operation	37
Figure 5-41	MDS location display	
Figure 5-42	Viewing historical track of the terminal	
Figure 5-43	Dispatching the terminal on the Map interface	39
Figure 6-1	Unified OMM interface	40
Figure 6-2	Add card	40
Figure 6-3	Input Add card information	41
Figure 6-4	Add user	42
Figure 6-5	Input user information-1	43
Figure 6-6	Input user information-2	43
Figure 6-7	Add group	44
Figure 6-8	Group account information setting	45
Figure 6-9	Add group member-1	45
Figure 6-10	Add group member-2	46
Figure 6-11	Add group member-3	46
Figure 6-12	Modify the group member attribute	47



Figure 6-13	Input user information	48
Figure 6-14	Enter to expert diagnosis mode on the unified OMM interface	49
Figure 6-15	Add CPE IP Pool and IP Segment	50
Figure 6-16	Create CPE Authorization Profile	51
Figure 6- 17	Show CPE access status	52
Figure 6-18	Add dispatcher account	52
Figure 6-19	Setting dispatcher account information	53
Figure 7-1	Trusted sits setting of the Internet Options	54
Figure 7-2	Security settings of trusted sites-1	
Figure 7-3	Security settings of trusted sites-2	
Figure 7-4	Security settings of trusted sites-3	
Figure 7-5	Temporary Internet Files Settings	
Figure 7-6	Uncheck "Turn on Pop-up Blocker"	58
Figure 7-7	Advanced Setting of Internet Option	

1 Overview

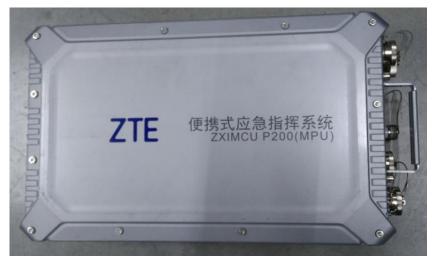
This manual covers introduction and operating instruction of Caltta LTE Emergency Command System, which includes configuration and operation methods for MDS, core network, base station, terminals and peripheral supporting products. Please select the corresponding operation steps according to the actual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

2 ZXIMCU PT01 P200 Version 3.0

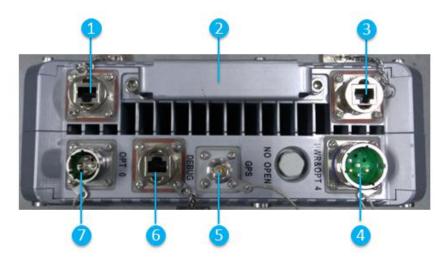
2.1 Introduction of ZXIMCU PT01 P200 Version 3.0

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



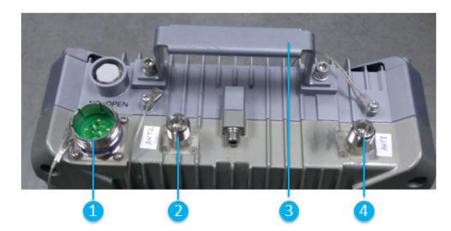




- 1) Network Interface 1: used for connecting with dispatch console or backhaul device
- 2) Handle: convenient to carry
- 3) Network Interface 2: used for connecting with dispatch console or backhaul device
- 4) Optoelectronic Input Interface: connect with RRU via power line.
- 5) CPS Antenna Interface: 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

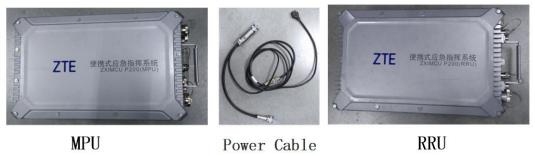
- 2) B Connector , Waterproof connector with small size diameter, connect to MPU
- 3) C Connector : Triangle plug, connect to external power supply



2.2 ZXIMCU PT01 P200 Connection Operation

Step 1: Take out the device as shown below

Figure 2-4 ZXIMCU P200 device



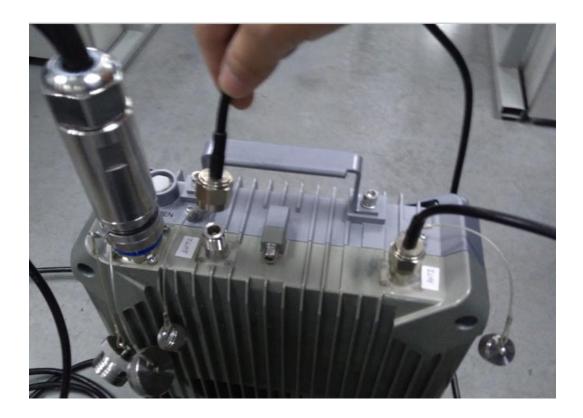
Step 2: Connect the A connector of the power line to RRU, connect B connector to MPU, and tighten them up



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.

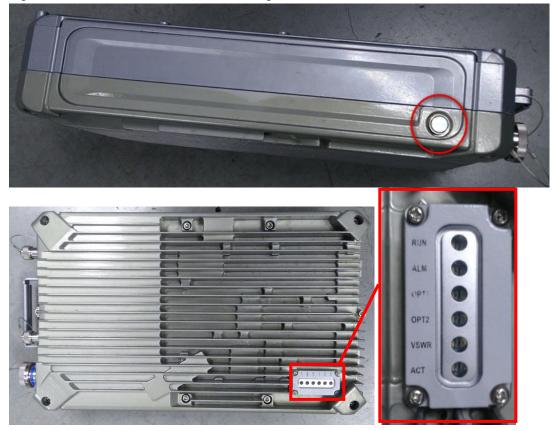
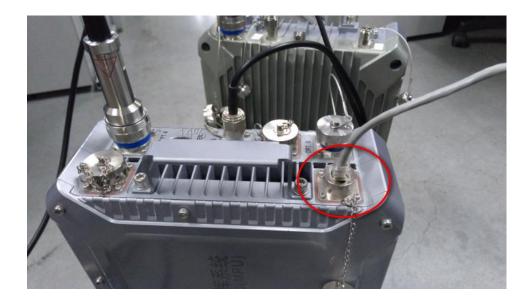


Figure 2-8 Power switch and indicator light

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 AlI-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:

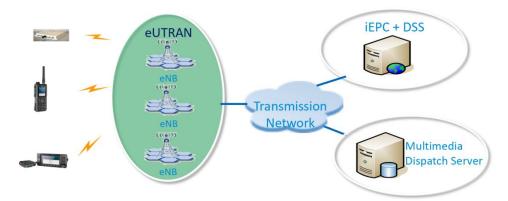


Figure 3-1 System Network Architecture

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

Administrator: Command Prompt

```
operable program or batch file.
C:\Users>
C:\Users>
C:\Users>route add 45.45.0.0 mask 255.255.0.0 192.168.13.80 -p
```

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.

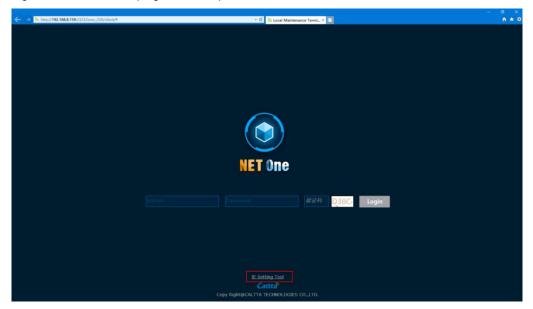


Figure 4-2 Download plug-in and script on the OMM interface

Script setting of IE trusted site:

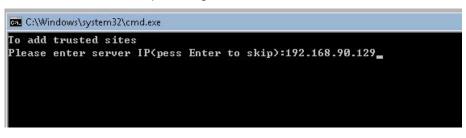
Extract the following compressed package (or the batch file downloaded from the OMM), open Internet Explore11 to set up the script:





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.



调度台客户端	Download Client	
VC2013_x32	Download	
dotNetFx45_Full_x86_x64	Plug-ins	

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





2	् dis(01	
ł		••••	***
	veri	ficatio	
	Remem	ber password	Ó
Se	rver IP:	192.168.13.21	
Ва	ckup IP:		
ME	OS IP:	192.168.13.20	
Ver	sion:V8.6(0.40.B12	
		Login	

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

0 2	227-01-28 19:15	1	Multimedia Cluster DAS	/			- 8 X
X) Temporary 뜸을 Groups 💥 Dynamic 🚊 WhiteList 🖂 Link				Emergency	G ControlList	
	Facet (*) Q: Enter stanto Q: Enter st		() UE993399 ()	UE992328		Controllat	Querrany III
• Cus • MMSSS • MDS	(2) C1158 C410150000005) (2) C1159 C410150000005) (2) (2) C1150 C4101500000013) (2) (2) C1152 C4101500000013) (2) (2) (2) C1152 L510150000014) (2)						

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.

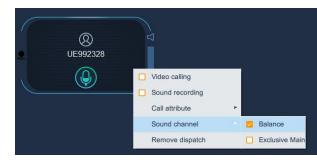
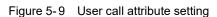


Figure 5-8 Sound channel selection

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.





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.



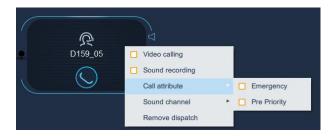
Figure 5-10 Group call attribute setting

	R			r.
	UE992328	Video calling		
REC		Sound recording		
K		Call attribute		Full duplex
		Sound channel	۴	Emergency
		Remove dispatch		Pre Priority
				Ambience Control

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

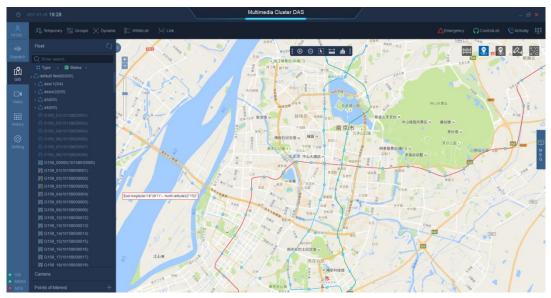


5.1.3.3 General Operations of GIS Dispatch

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.

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

(Q) UE992328	 Video calling Sound recording Call attribute 	- Rec	(UE992328	(2) UE992328	B
	Sound channel Remove dispatch		00:00:00	00:00:22	

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 .



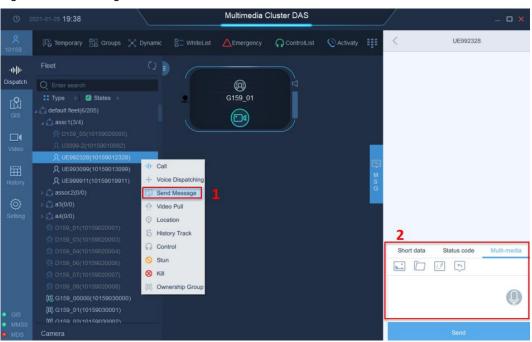
Figure 5-18 Dispatch console initiates a video group call



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.





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

\mathscr{P}_{0} Temporary		₿⊒ WhiteList			
Start Time					2
19:44:23	Normal Call	Group call	UE992328(新1.4G基站(G159_01	୬ ଲେକ୍ 🖉

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 is 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

🎊 Temporary	📴 Groups 🔀 Dynamic	₿ — WhiteList			ControlList 🚫 Activ	vity
Start Time						
19:44:23	Normal Call		UE992328(新1.4G基站	G159_01	، حر ک	<u>1</u> 23

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



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

Number Name	10159030001 G159_01	
Permanent	member(5)/Dynam	nic member(New add:0/To
© D159_0	÷	Permanent member
UE9999	11	Permanent member
	28	Permanent member
UE9923		

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 Click Click Temporary 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 \bowtie on the right side of the member.

Click Save 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.



Temporary group	×
Please enter a temporary group name	7
Selected member(0)	-
User Number User Name	-
Cancel Save	

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 it 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

No Temporary 🔤 Groups 💥 Dynamic	c 1 mute		G ControlList
Start Time		Call Duration	
19:51:17	UE992328	00:00:09	9

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.

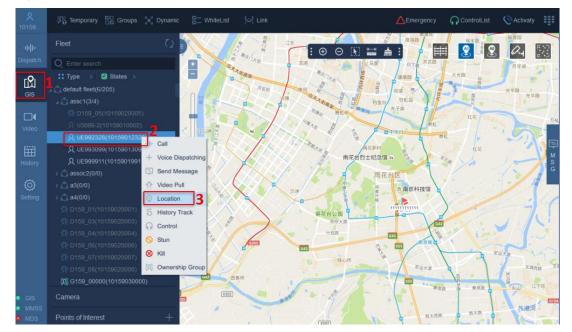


Figure 5-25 Dispatch console location operation

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 0 to end the location. Click 0 to display the moving path of the terminal. Click 1 to pull the terminal video. Click 1 to send a message. Click 1 to initiate a voice call.



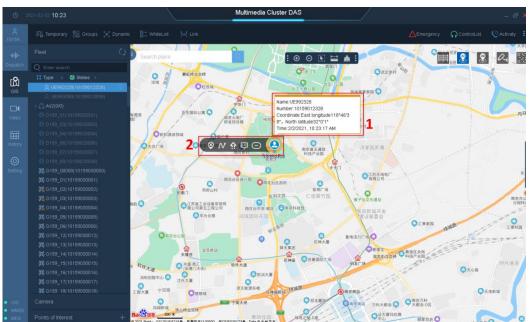


Figure 5-26 Map interface display and operation

5.1.15 Frame Select and Dispatch on the Map

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

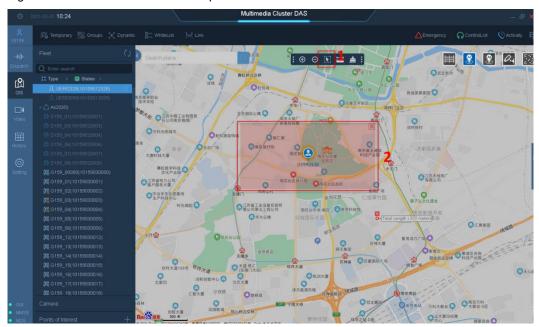


Figure 5-27 Frame select on the map

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

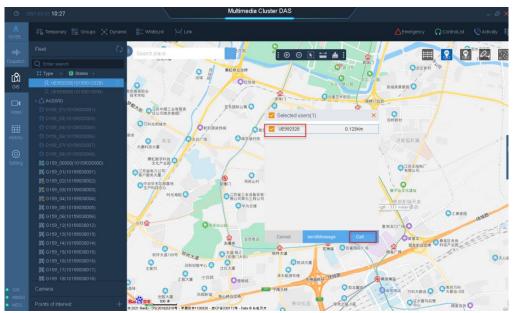


Figure 5-28 Frame select and dispatch on the map

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.



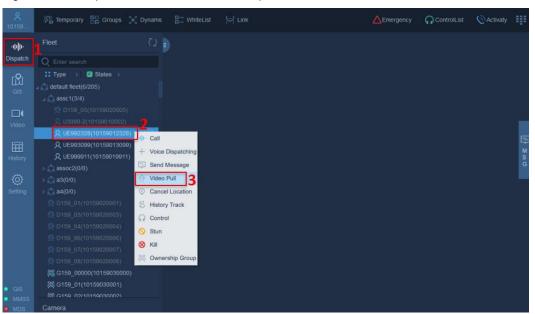


Figure 5-29 Dispatch console initiates a video pull

Adjust the number of terminal videos to be displayed on the upper area of the Video interface. Click is 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 it 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.



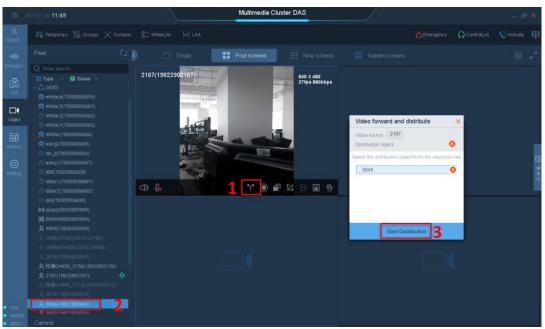


Figure 5-31 Dispatch console Initiates video distribution

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)

8	7000006660	
6		1
I	Remember the password	0
IP:	192.168.13.20	
Vers	ion No.5.3.0	



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.

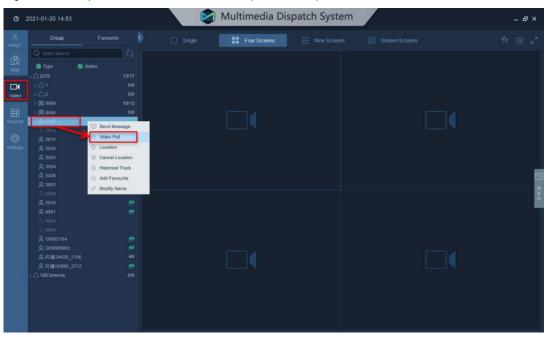


Figure 5-34 Operations of the multimedia dispatch video pull

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 I 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 I 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.

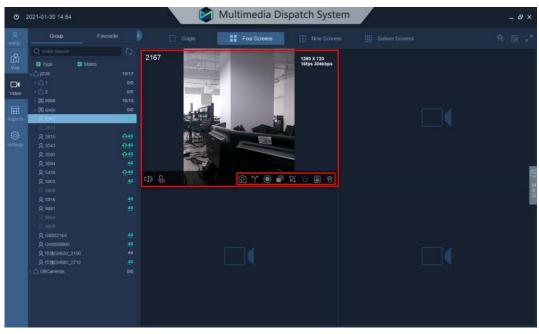


Figure 5-35 Multimedia dispatch video display window

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 \square 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.

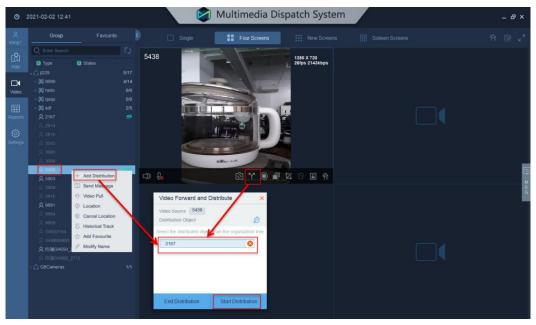


Figure 5-36 Multimedia dispatch video distribution

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.

0	2021-01-30 15:12			Multimedia Dis	patch System	- 8 ×
A wangt	Group					
Atanga Mago Video Reports Settingo	Q. Enter Sourch ■ Type B state ↓ State A state	() es 13/17 000 000 19/13 000 19/14 合理 合理 合理 の 合理 の	994		640 X 480 Skips Gerkops](
	R 9909 R 9916 R 9904 R 9904 R 9905 R	00 99 99 99 99	Vde Distr Seinci	eo Forward and Distribute o Source 3004 titution Object the distribution depict and Distribution Start Distribution	0	

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.

0	2021-01-30 15:13			Multimedia Dis	patch System	- @ ×
Rang1	Group			Four Screens		18 💀 🖉
Lap Map	Q Enter Search I type I Sta 1029			1 1	640 X 480 10fps 0kbps	
video	- C 1 - C 2 - St 0000					
Beports ©						
Settings		수49 수49 수49			f	
	Ω 5094 Ω 5438 Ω 5400	ር <u>ቀ</u> በ ተደ		and the second s		Ę
		40 1740	Video 5	Forward and Distribute	×	ů
	Я свероть Я сневозно Я сневозно Я намонного_2126 Я намонного_2126		Select th	e disinitiated object from the organiz	stop	
			End	Distribution Start Distri	buban	

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.

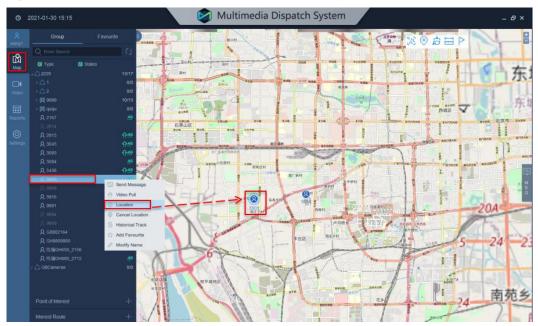


Figure 5-40 MDS terminal location operation

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.

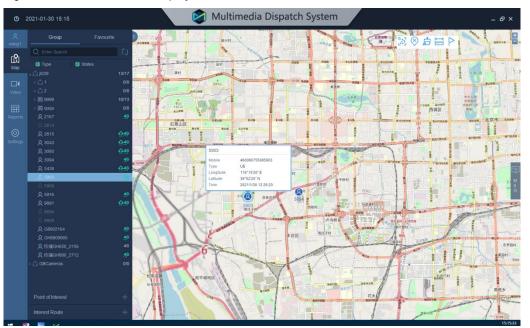


Figure 5-41 MDS location display

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

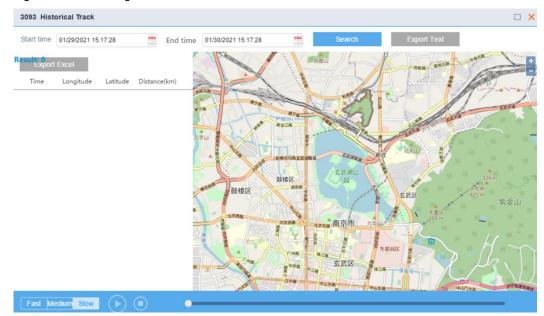


Figure 5-42 Viewing historical track of the terminal

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

Click 1 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

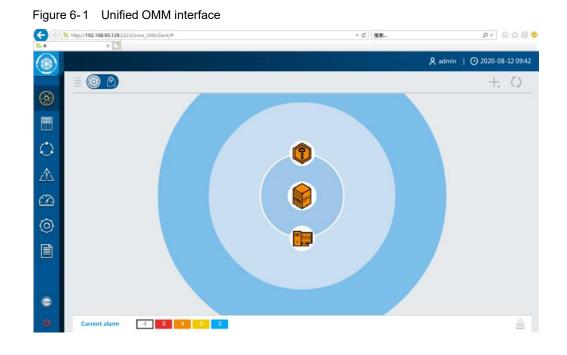
Login to the unified OMM via IE browser (IE 11).

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.





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:

							🞗 admi	in 🖸	2021-01-	30 16:35
-1	81.周系战 · ·	Authentication in	formation list (50781)				÷	G (20
	Fleet	IMSI number	Belonged fleet	User key	Authenticatio	Initiate OPC	OPC	Add care	d	nous Ar
	Dispatcher	460088100000017	default fleet		8234	YES		111	YES	YE
ſ	Authentication 🥊 🄈	460088100000018	default fleet		8234	YES	111111111111111111111111111111111111111	111	YES	YE
c	ontract Template	460088100000019	default fleet		8234	YES	111111111111111111111111111111111111111	111	YES	YE
	PDN Template	460088100000020	default fleet		8234	YES	111111111111111111111111111111111111111	111	YES	YE
	Data Template	460088100000021	default fleet	111111111111111111111111111111111111111	8234	YES	111111111111111111111111111111111111111	111	YES	YE
	Iser	460088100000022	default fleet	111111111111111111111111111111111111111	8234	YES	111111111111111111111111111111111111111	111	YES	YE
		460088100000023	default fleet		8234	YES		111	YES	YE
	roup	460088100000024	default fleet	111111111111111111111111111111111111	8234	YES	111111111111111111111111111111111111111	111	YES	YE
IM	EI Check	460088100000025	default fleet	111111111111111111111111111111111111111	8234	YES	111111111111111111111111111111111111111	111	YES	YE
Sta	itus Message	460088100000026	default fleet	111111111111111111111111111111111111111	8234	YES	111111111111111111111111111111111111111	111	YES	YE
PI	5	460088100000027	default fleet		8234	YES	111111111111111111111111111111111111111	111	YES	YE
	PIS Group	460088100000028	default fleet		8234	YES	111111111111111111111111111111111111111	111	YES	YE
Re	al-name	460088100000029	default fleet		8234	YES	111111111111111111111111111111111111111	111	YES	YE
sj	/nc	460088100000030	default fleet		8234	YES	111111111111111111111111111111111111111	111	YES	YE
		460088100000031	default fleet	111111111111111111111111111111111111111	8234	YES	111111111111111111111111111111111111111	111	YES	YE
		460088100000032	default fleet	111111111111111111111111111111111111111	8234	YES	111111111111111111111111111111111111111	111	YES	YE
		460088100000033	default fieet		8234	YES		111	YES	YF
		K < 608 /6	IC C II	Totally 60781 item	(d), every page displa	vs 100				0

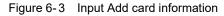
Figure	6-2	Add	card
iguic	0-2	Auu	caru

All rights reserved



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:

			🎗 admin 🔿 2021-01-30 16:36
	. 杨心明系统 🔷	Authentication information list (60781) Add card ×	
٢	Fleet	IMSI number * 46008810000023	
	Dispatcher	Belonged fleet default fleet: × Eu	
0	Authentication	User key*	
	Contract Template	Use Key Encryption	
Δ	PDN Template	Authentication man* 8234 🕜	
	Data Template	Initiate OPC	
0	User	OPC 111111111111111111111111111111111111	
	Group	Use OPC Encryption	
	IMEI Check	Anonymous key ID 🔽	
۲	Status Message	Anonymous key ID	
	PIS		
	PIS Group		
	Real-name		
	Sync		
۲			
		Save & Con Save 2	
U			



Note: Select the user authentication information to be operated, $\operatorname{click}^{\swarrow}$ and $\overline{\operatorname{Im}}$ 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
riguic 0-+	/ 100 0301

ſ	桥心周系统 ~	User	list (30738) Ad	d user \times	460012290000003	×				6 2	t G	0	2
	Fleet	0	IMSI Range	User type	User Number Range	Fleet user nu	User name	Belonged fleet	PTT service s	Data services Statu	ZiLTE External-ZiLTE	E system	_
	Dispatcher		111111111111111	DSS	11112211111	1	1	lidan111	Active	YES	ō		
1	Authentication		200200200200	Data-Only	15915915901			MDS测试勿删		YES			
	Contract Template		40080755099907	DSS	15915999907	9907	9907	MDS测试勿删	Active	YES	0		
	PDN Template		460010000000000	Data-Only				ppqq		YES			
	Data Template		460012290000001	DSS	31390100001	0001	0001	zs_159	Active	YES	1		
	User 2		460012290000002	DSS	31390100002	0002	0002	zs_159	Active	YES	1		
ŕ			460012290000003	DSS	31390100003	0003	0003	25_159	Active	YES	1	0	
	Group		460012290000004	DSS	31390100004	0004	0004	zs_159	Active	YES	1		
	IMEI Check	•	460012290000005	DSS	31390100005	0005	0005	zs_159	Active	YES	1		
	Status Message		460012290000006	DSS	31390100006	0006	0006	zs_159	Active	YES	1		
	PIS		460012290000007	DSS	31390100007	0007	0007	zs_159	Active	YES	1		
	PIS Group		460012290000008	DSS	31390100008	0008	0008	zs_159	Active	YES	1		
	Real-name		460012290000009	DSS	31390100009	0009	0009	zs_159	Active	YES	1		
	Sync		460012290000010	DSS	31390100010	0010	0010	zs_159	Active	YES	1		
			460012290000011	DSS	31390100011	0011	0011	zs_159	Active	YES	1		
			460012290000012	DSS	31390100012	0012	0012	zs_159	Active	YES	1		
			460012290000013	DSS	31390100013	0013	0013	75 159	Active	YES	1		

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**

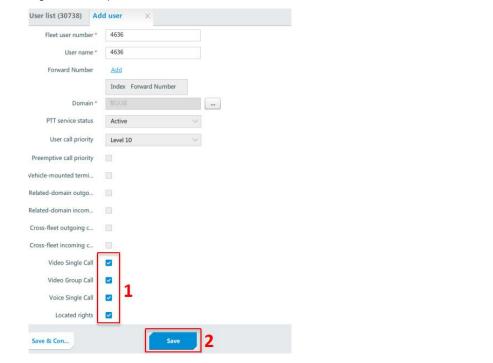
(by clicking ¹ on the right) for the user. For a vehicle-mounted terminal, tick **Vehicle-mounted terminal** option. Keep the default settings for other parameters, and click **Save**, see the following figure.



IMSI number *	460012290000003]
User number *	31390100003	
Belonged fleet *	default fieat.	× B:
Belonged organization		×
Activated data service		
Data service template *	1000lidan	
static subscription add	Add	
	Index PDN IPV4 address PDN I	FV6 address template
Closed user group ID		
Personal Qos		
PIS		
TAU user		
Subscribed PTT service		
Fleet user number*	4636	
User name *	4636	
Forward Number	Add	1
	Index Forward Number	

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 the menu on the right to add group:

f	他心间系统 ~	Grou	ıp list(1103)							6	2 🛨 🖪 🕻
Ì	Fleet		Group Number Range	Group name	Group type	Belonged flee	Group status	Group meml	Dynamic gro		ZiLTE group ZiLTE Foreign Group
	Dispatcher		10159030000	G159_00000	Collective bro	default fleet	Active	2			
1	Authentication		10159030001	G159_01	General Grou	default fleet	Active	5			
4	Contract Template		10159030002	G159_02	Dynamic Reg	default fleet	Active	1	1		
	PDN Template		10159030003	G159_03	Dynamic Reg	default fleet	Active	1	1		
	Data Template		10159030004	G159_04	Dynamic Reg	default fleet	Active	0	3		
	User		10159030005	G159_05	General Grou	default fleet	Active	3			
	Group 2		10159030006	G159_06	General Grou	default fleet	Active	1			
ľ	IMEI Check		10159030007	G159_07	General Grou	default fleet	Active	1			
			10159030008	G159_08	General Grou	default fleet	Active	1			
	Status Message		10159030009	G159_09	General Grou	default fleet	Active	1			
	PIS		10159030010	G159_10	General Grou	default fleet	Active	1			
	PIS Group		10159030011	G159_11	General Grou	default fleet	Active	1			
	Real-name	12	10159030012	G159_12	General Grou	default fleet	Active	1			
	Sync		10159030013	G159_13	General Grou	default fleet	Active	1			
			10159030014	G159_14	General Grou	default fleet	Active	1			
			10159030015	G159_15	General Grou	default fleet	Active	1			
		- E	10159030016	G159 16	General Gros	default fleet	Active	1			

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 the right) for the Belonged fleet. Keep the default settings for other parameters, and click **Save**, see the following figure.



Group list(1103)	Add group X	
Group number *	10159030007	
Group short number *	030007	
Group name *	G159_07	
Group type	General Group	
Belonged fleet •	default fleet	Be
Belonged organizati		
Domain *	默认验	
Preemptive call rights		1
Group call priority	Level 10 🗸	1. The second
Inactive timer	Default 🗸	
Group status	Active 🗸	
Call area restricted		
Related group		
Support Group Safe	NO 🗸	
Voice Group Call Ti		
Voice Group Call Ti	0	min
Video Group Call Ti		
Save & Con	Save	2

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.

()			🞗 admin 😋 2021-01-30 16:40
		Group list(1103)	
0	Fleet	Group Number Range Group name Group type Belonged flet Group status Group memt Dynamic gro	
	Dispatcher	10159030000 G159_00000 Collective brr default fleet Active 2	
0	Authentication	10159030001 G159_01 General Grou default fleet Active 5	
	Contract Template	International Interna International International<	
	PDN Template	10159030003 G159_03 Dynamic Reg default fleet Active 1 1	
	Data Template	10159030004 G159_04 Dynamic Reg default fleet Active 0 3	
0	User	10159030005 G159_05 General Grout default fleet Active 3	
		10159030006 G159_06 General Grout default fleet Active 1	
	droup	🔲 10159030007 G159_07 General Grou default fleet Active	
¥	IMEI Check	10159030008 G159_08 General Grou. default fleet Active 1	
	Status Message	10159030009 G159_09 General Grou. default fleet Active 1	
	PIS	10159030010 G159_10 General Grou default fleet Active 1	
	PIS Group	10159030011 G159_11 General Grou default fleet Active 1	
	Real-name	10159030012 G159_12 General Grou default fleet Active 1	
	Sync	10159030013 G159_13 General Grou default fleet Active 1	
		10159030014 G159_14 General Grou. default fleet Active 1	
		10159030015 G159_15 General Grou. default fleet Active 1	
0		10159030016 G159-16 General Gros. default fleet Active 1	
		K K I /12 X I Totally 1103 item(s), every page displays 100 × item(s)	

Figure 6-9 Add group member-1



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

\circledast											R adn	in 😋 2021-01-30 16:41
	核心网系统	Group list(1103)									6 2	+_ E () Q
<u>(</u>	Fleet	Group Number Range	Group name	Group type	Belonged flee	Group status	Group memb	Dynam	Group mem	ber(1)		⊞ Q 9 ×
	Dispatcher	10159030000	G159_00000	Collective bro	default fleet	Active	2		Number	Name	Туре	Flee
ि	Authentication	10159030001	G159_01	General Grou	default fleet	Active	5		10159020003	D159_03	Dispatcher	default fleet
	Contract Template	10159030002	G159_02	Dynamic Reg	default fleet	Active	1	1				
⚠	PDN Template	10159030003	G159_03	Dynamic Reg	default fleet	Active	- 3	1				
A.	Data Template	10159030004	G159_04	Dynamic Reg	default fleet	Active	0	3				
\odot	User	10159030005	G159_05	General Grou			3					
	⊿ Group 2	10159030006	G159_06	General Grou			1					
Ē	IMEI Check	10159030007	G159_07	General Grou			1					
¥	Status Message	10159030008	G159_08	General Grou			1					
		10159030009	G159_09	General Grou			1	_				
	PIS	10159030010	G159_10	General Grou			1					
	PIS Group	10159030011	G159_11	General Grou		Active	1					
	Real-name	10159030012	G159_12	General Grou			1					
	Sync	10159030013	G159_13	General Grou			1					
		10159030014	G159_14	General Grou		Active	1					
0		10159030015	G159_15	General Grou	default fleet	Active	1					
		ID159030016	G159 16	General Grou			1					
C		K < 1 /12 >	K		Totall	y 1103 item(s), e	very page displa	lys 100	K < 1		> Displa	/ 25 +

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.

Group member										\times
Selectable group n	nember(208)			Q		Selected group m	ember(1)			Q
Number	Name	Туре	Fleet			Number	Name	Туре	Fleet	
10159010002	U3099-2	User	default fleet			10159020003	D159_03	Dispatcher	default fleet	
10159011003	UE1003	User	default fleet							
10159011005	UE1004	User	default fleet	ſ	~	-				
10159011006	UE1005	User	default fleet	l	2	2				
10159011007	UE1006	User	default fleet							
10159011008	UE1007	User	default fleet							
10159011009	UE1008	User	default fleet							
10159011010	UE1009	User	default fleet							
	/5 > >	Display 50				K < 1	/1 >>	Display 50	•	

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.

Group member cal	MIDDLE
Speak time	1min
Group call rights	Talk privilege
	Initiate group call
	🗹 🛛 Terminate group ca

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 H 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.

					🞗 admin 🕥 2021-01-30 16:42
	核心网系统 🗸	User list (30738) Add	l user X		
0	Fleet	IMSI number *	460012290000003		
	Dispatcher	User number *	31390100003	3	
\bigcirc	Authentication	Belonged fleet +		× Bu	
	Contract Template	Belonged organization		×	
	PDN Template	Activated data service			
	Data Template	Data service template *	1000lidan		
\odot	⊿ User 2	Static subscription add	Add		
	Group		Index PDN IPV4 address P	DN IPV6 address template	
	IMEI Check	Closed user group ID			
¥	Status Message	Personal Qos			
	PIS	PIS			
	PIS Group	TAU user	v		
	Real-name	Subscribed PTT service	~		
		Fleet user number *	4636		
	Sync	User name *	4636		
		Forward Number	Add		
6			Index Forward Number	_	
ø		Save & Con	Save	4	

Figure 6-13 Input user information

Note: Select the user to be operated, $click^{2}$ and \overline{m} 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.

									🞗 admi	n 🖸 2021-01-30 16:4
Ne iepc51(192.168.8.159)		Table Result			Operation F					
	Copy Modify Delete Copy Modify Delete	277 278	0	CPE_drsTest077 CPE_drsTest078	277 278	31.32.1.77 31.32.1.78	31.32.1.77 31.32.1.78	255.255.255.255	Disable	
	Copy Modify Delete	279	ö	CPE_drsTest079	279	31.32.1.79	31, 32, 1, 79	255.255.255.255	Disable	
- Filter X	Copy Modify Delete	280	0	CPE_drsTest080	280	31.32.1.80	31.32.1.80	255.255.255.255	Disable	
Configuration Management	Copy Modify Delete	281	0	CPE_drsTest081	281	31.32.1.81	31.32.1.81	255.255.255.255	Disable	
	Copy Modify Delete	282 283	0	CPE_drsTest082 CPE_drsTest083	282 283	31.32.1.82 31.32.1.83	31.32.1.82 31.32.1.83	255.255.255.255	Disable	
V Doily Maintaining	Copy Modify Delete	284	0	CPE_drsTest084	284	31. 32.1.84	31. 32.1.84	255.255.255.255	Disable	
The APN Configuration	Copy Modify Delete	285	0	CPE_drsTest085	285	31.32.1.85	31.32.1.85	255.255.255.255	Disable	
IPV4 Address Pool Configuration	Copy Modify Delete	286	0	CPE_drsTest086	286	31.32.1.86	31.32.1.86	255.255.255.255	Disable	
IPV6 Address Pool Configuration	Copy Modify Delete	287 288	0	CPE_drsTest087	287	31.32.1.87	31.32.1.87	255.255.255.255	Disable	
	Copy Modify Delete	289	0	CPE_drsTest088 CPE_drsTest089	289	31.32.1.88 31.32.1.89	31.32.1.88 31.32.1.89	255.255.255.255	Disable	
Local Authorize Profile Configuration	Copy Modify Delete	290	0	CPE_drsTest090	290	31.32.1.90	31.32.1.90	255.255.255.255	Disable	
V CPE Access Terminal IP Pool Configurati	Copy Modify Delete	291	0	CPE_drsTest091	291	31.32.1.91	31.32.1.91	255.255.255.255	Disable	
Create CPE IP Pool	Copy Modify Delete	292	0	CPE_drsTest092	292	31.32.1.92	31.32.1.92	255.255.255.255	Disable	
	Copy Modify Delete	293 294	0	CPE_drsTest093 CPE_drsTest094	293	31.32.1.93 31.32.1.94	31.32.1.93 31.32.1.94	255.255.255.255 255.255.255.255	Disable	
Delete CPE IP Pool	Copy Modify Delete	295	0	CPE_drsTest094 CPE_drsTest095	294	31. 32. 1. 94	31. 32. 1. 94	255.255.255.255	Disable	
Set CPE IP Pool	Copy Modify Delete	296	0	CPE_drsTest096	296	31.32.1.96	31.32.1.96	255.255.255.255	Disable	
Add CPE IP Segment	Copy Modify Delete	297	0	CPE_drsTest097	297	31.32.1.97	31.32.1.97	255.255.255.255	Disable	
Delete CPE IP Segment	Copy Modify Delete	298 299	0	CPE_drsTest098 CPE_drsTest099	298 299	31.32.1.98 31.32.1.99	31.32.1.98 31.32.1.99	255.255.255.255 255.255.255.255	Disable Disable	
	Copy Modify Delete	300	0	CPE_drsTest100	300	31. 32. 1. 99	31.32.1.99	255,255,255,255	Disable	
Show CPE IP Pool	Copy odify Delete	301	0	Cra_dratest200	301	59.159.0.1	59.159.0.10	255.255.255.240	Publish dynamic route	
CPE Access Terminal IPV6 Pool Configur	Conv. bdify Delete	301	0		302	59.159.0.17	59.159.0.27	255.255.255.240	Publish dynamic route	
The CPF Terminal Authorization Profile Confi										
v 🗁 CPE Terminal Authorization Profile Confi	213 Record(s)									
Create CPE Authorization Profile										
	213 Record(s)									
Create CPE Authorization Profile	213 Record(s)	successful					****			
Create CPE Authorization Profile Modify CPE Authorization Profile Delete CPE Authorization Profile	213 Record(s)									
Create CPE Authorization Profile Modify CPE Authorization Profile Delete CPE Authorization Profile Show CPE Authorization Profile	213 Record(s) Executed command	successful								
Create CPE Authorization Profile Modify CPE Authorization Profile Delete CPE Authorization Profile	213 Record(s) Executed command	successful								
Create CPE Authorization Profile Modify CPE Authorization Profile Delete CPE Authorization Profile Show CPE Authorization Profile	213 Record(s) Executed command	successful								
Create CPE Authorization Profile Modify CPE Authorization Profile Delete CPE Authorization Profile Brow CPE Authorization Profile Modify DNS Server Address	213 Record(s) Executed command	successful								
Create CPE Authorization Profile Modify CPE Authorization Profile Center CPE Authorization Profile Detec CPE Authorization Profile Detec CPE Authorization Profile Modify DNS Server Address Oxfolf P-CSCP Server Address	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful							Parameter Search	^ v
Create CFR Authorization Profile Modif CFR Authorization Profile Oxford CFR Authorization Profile Oxford CFR Authorization Profile Modif / POST Server Address Modif / POST Server Addre	213 Record(s) Executed command	successful								
Create CTR Autorization Public CTR Autorization Public CTR Autorization Public CTR Autorization Public CTR Autorization Public Modify PGS Second Autorization Modify PGS Tarter Address CTR ACS Address Configuration P CTR ACS Address Configuration	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Ceste CFR Authorization Putifie Delete CFR Authorization Putifie Delete CFR Authorization Putifie Delete CFR Authorization Putifie Modify PCCSC Server Address Modify PCCSC Server Address C CFR ACti Address Configuration C CFR ACti Addre	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Create CTR Autorization Public CTR Autorization Public CTR Autorization Public CTR Autorization Public CTR Autorization Public Modify PGS Second Autorization Modify PGS Tarter Address CTR ACS Address Configuration P CTR ACS Address Configuration	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Ceste CFR Authorization Putifie Delete CFR Authorization Putifie Delete CFR Authorization Putifie Delete CFR Authorization Putifie Modify PCCSC Server Address Modify PCCSC Server Address C CFR ACti Address Configuration C CFR ACti Addre	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Conce CF A Morecession Public Media CF A Morecession Public Detail Viol Server Advects Detail Viol	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Const. CTR. Autorization: Public Defa: CTR. AUTO: Configuration Public Defa: CTR. All Configuration Public Defa: Autor Transfer Scientification Public Defa: Autor Transfer Science De	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Conce CF Autorsson Pulle Delta CF Autorsson E GF Autorsson E G	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Const. CTR. Autorization: Public Defa: CTR. AUTO: Configuration Public Defa: CTR. All Configuration Public Defa: Autor Transfer Scientification Public Defa: Autor Transfer Science De	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Conce CF Autorsson Pulle Delta CF Autorsson E GF Autorsson E G	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Greate CFF, Authorstein mhrile Greate CFF, Authorstein Malanz Greate CFF,	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								
Conce CF A Morecession Public Media CF A Morecession Public Conce CF A Morecession Conc	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful					-			
Greate CFF, Auforstation Public delse Version Public Public delse Version Public Public delse Version Public Public delse Version Public	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful					_			
Greate CFF, Auforstation Public delse Version Public Public delse Version Public Public delse Version Public Public delse Version Public	213 Record(s) Executed command (S NHL:> SHOW CPE IPR ML:>	successful								

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 **IP**, 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 let 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.

€ →	http://192.168.8.159:2323/inms_250/client/#			- C 🔊 =	×		- 0 × n★0
(🞗 admin 🖸	2021-01-30 16:44
	Its Lepc51(192.168.8.159) V Confountion Management Daily Management V MC Confountion V MA defease that Confountion P) VPC Addeese that Confountion P)	Test Result Tolke term Tolke term	It Droadcast Result It 0 CPE_drsTset07 CPE_drsTset07 0 CPE_drsTset07 CPE_drsTset08 0 CPE_drsTset08 CPE_drsTset08	8 278 31, 32, 1, 7 9 279 31, 32, 1, 7 0 280 31, 32, 1, 6 11 281 31, 32, 1, 6 12 282 31, 32, 1, 6 13 283 31, 32, 1, 6 14 284 31, 32, 1, 6 15 285 31, 32, 1, 6 16 266 31, 32, 1, 6 17 287 31, 32, 1, 6	$\begin{array}{cccccccccccccccccccccccccccccccccccc$.35, 235 0 (sub)e .255, 235 0 (sub)e	
		Copy Hodify Delete 289 Copy Hodify Delete 290 Copy Hodify Delete 290 Copy Hodify Delete 291 Copy Hodify Delete 292 Copy Hodify Delete 293 Copy Hodify Delete 294 Copy Hodify Delete 296 Hozy Hodify Delete 296 Hozy Hodify Delete 296	0 CPE_dnsTest09	19 289 31, 32, 1, 4 00 290 31, 32, 1, 4 11 291 31, 32, 1, 5 12 292 31, 32, 1, 5 13 231 32, 1, 5 14 294 31, 32, 1, 5 15 295 31, 32, 1, 5 16 296 31, 32, 1, 5 16 296 31, 32, 1, 5 16 296 31, 32, 1, 5 16 296 31, 32, 1, 5 17 297 31, 32, 1, 5 18 298 31, 32, 1, 5	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	235.255 Disable 235.255 Disable 235.255 Disable 235.255 Disable 235.255 Disable 235.255 Disable 235.255 Disable 235.255 Disable 235.255 Disable	
0	Gleba CFE ID Segment Show CFE IP Pool CER Access Terminal TWV6 Pool Configu CE Terminal Authorization Profile Configu Create CPE Authorization Profile	Copy Modify Delete 299 Copy Modify Delete 300 Copy Modify Delete 301 Copy Modify Delete 301 213 Record(s) Executed command successi	0 CPE_drsTest10 0 0	0 300 31.32.1.1 301 59.159.0 302 59.159.0	100 31.32.1.100 255.255 1 59.159.0.10 255.255 17 59.159.0.27 255.255	235.255 Disable 235.255 Disable 235.240 Publish dynamic route 235.240 Publish dynamic route	10
¥	Modify CPE Authorization Profile Belea CPE Authorization Profile Show CPE Authorization Profile Modify DNS Server Address Modify DNS Forces Farver Address	ML:> SHOW CPE IPPOOL MML:> ADD CPE IPSEG:SEGID=3,		L",IPTAIL="45.45.2.254",IP			• •
	Modify HOMESTATE Server Address					Parameter Search	A V Dire
	CPL ACL: Advass: Configuration Configur		CPE Pool 1D	3	19 Septem Start 2	ID Segment End 45.43.2.254	
©	▶ 🚰 Backup and Restore ▶ 🎦 Enable Configuration						

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 *let* to execute.

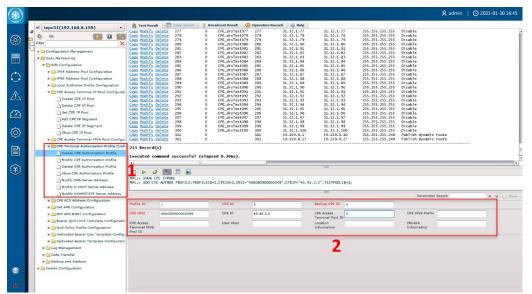
Profile ID: The same as the Profile ID number corresponding to the CPE configured in the GW APN. It is generally set to 1.

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 .





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

					🞗 admin	🕑 2021-01-30 16:47
-	NE iepc51(192.168.8.159)	🙀 Text Result 🕅 Table Result 🏋 B	oadcast Result 🛛 🙆 Operation Record	😡 Help		
	9	276 460088100000076 OffLine		0 0		
(<u>;</u>)	🖕 🗢 🛛 🚺 🖬	277 46008810000077 OffLine 278 46008810000078 OffLine		0 0		
	Filter X	279 460088100000079 OffLine	IPv4: 31.32.1.79 0	0 0		
	Configuration Management	280 46008810000080 OffLine 281 46008810000081 OffLine		0 0		
	► Daily Maintaining	281 46008810000081 OffLine 282 46008810000082 OffLine		0 0		
IIII		283 46008810000083 OffLine	IPv4: 31.32.1.83 0	0 0		
	V Configuration	284 46008810000084 OffLine 285 46008810000085 OffLine		0 0		
\bigcirc	▶ 🗁 Version Management	286 460088100000086 OffLine	IPv4: 31.32.1.86 0	0 0		
	Independent Board Version Managemer	287 460088100000087 OffLine 288 460088100000088 OffLine		0 0		
	Local Office Global Data Management	289 46008810000089 OffLine		0 0		
	Device Management	290 460088100000090 OffLine	IPv4: 31.32.1.90 0	0 0		
	Local Office Mobile Data Management	291 460088100000091 OffLine 292 460088100000092 OffLine		0 0		
	Capacity Layout Management	293 46008810000093 OffLine	IPv4: 31.32.1.93 0	0 0		
0	GTPC IP Address Management	294 460088100000094 OffLine 295 460088100000095 OffLine		0 0		
(\mathcal{I})	SIGTRAN Configuration	295 46008810000095 OffLine 296 46008810000096 OffLine		0 0		
-		297 46008810000097 OffLine	IPv4: 31.32.1.97 0	0 0		
	Diameter Management	298 46008810000098 OffLine 299 46008810000099 OffLine		0 0		
\bigcirc	Number Analysis Configuration	300 460088100000100 OffLine	IPv4: 31.32.1.100 0	0 0		
~	► 📴 HeNB Configuration	301 460080755099910 OffLine	IPv4: 59.159.0.1 0	0 0		
	Access Area Management	207 Record(s)				
	▶ 🚞 IP Stack Configuration	Executed command successful (elap				
	GW System Configuration	executed command successful (elap	sed 1.3145).			
(¥)	▶ 📴 H55 Global Configuration	and the second se				1.1
(Ŧ)	▶ 🛅 8-Trunc Global Configuration	💽 🕨 🥒 📰 🗮 🖬				
	SIMP Configuration	MML:> SHOW CPE IPPOOL MML:> SHOW CPESTATE				
	SNTP Management	MRL:>				
	▶ 🔄 Time Zone Management				Parameter Search	the complete
	▶ C Daylight Saving Time Configuration				Parameter search	∧ ∨ [_] Here
	v 🗁 Dynamic Management					
	► Ci Time Management					
	Ol eNode8 Management					
	Viser Management					
	Create EPS Bearer					
	Delete EPS Bearer					
	Dupdate EPS Bearer					
	Detach Mobile User					
	Show MME User Statistics					
\odot	Show MME User Dynamic Info	1				
0	Show CPE State Info					
16	Show More CPE state information					
Q	Show PGW User data Volume					

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.

()					& admin ⊙ 20	021-01-30 16:48
	核心同系统 🗸	Dispatcher I	ist(63)			- 0 2 0
0	Fleet	Dispatcher ID	Belonged flee	Dispatcher number(Zil	2	LTE
	⊿ Dispatcher 2	ppqq1591	ppqq	13880010001		
	Authentication	ppqq1592	ppqq	13880010002		
	Contract Template	8620j	8620j	86208620201		
	PDN Template	D159_02	default fleet	10159020002		
	Data Template	D159_03	default fleet	10159020003		
\odot	User	2ppqq1	ppqq2	13880019001		
		ppqq1	ppqq	13880010003		
	Group	mfidac	mfl	12345678912		
¥	IMEI Check	l01-ppqq	ppqq	13880010010		
0	Status Message	们动于	mfl	12345678913		
	PIS	rd1	燃烧	13855052001		
	PIS Group	mk111	mfl	12345678888		
	Real-name	mk2	mfl	12345678889		
	Sync	ppqq1594	ppqq	13880010004		
		ppqq1595	ppqq	13880010005		
		208Prime	江苏省	86208620208		
0		8620n	8620i	86208620202		
Ø		K K	1 /1 >		Totally 63 item(s) every page displays 100 + item(s)	O

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:

۲						🞗 admin 🕐 2021-01-30 16:48
	核心网系统 🖌	Dispatcher list(63)	ZiLTE Dispatcher ×			
0	Fleet	Dispatcher ID •	ppqq1593	1	7	
	Dispatcher	Dispatcher password *	555555			
\odot	Authentication	Belonged fleet •	default fleet	Ee		
	Contract Template	Belonged organizati	asse1	0		
⚠	PDN Template	Dispatcher number *	13880010002		1	
	Data Template	Dispatcher fleet use*	2333		-	
\odot	User	Priority	LAST			
Ê	Group	Cross-fleet outgoin				
	IMEI Check					
€	Status Message	Distant Risen				
	PIS	White List				
	PIS Group	Tight Control				
	Real-name	More>>>				
	Sync					
0		Save & Con	Save		2	
Q			Jave		2	

Figure 6-19 Setting dispatcher account information

Select the dispatcher to be operated, click and \overline{m} 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.

Internet Options	? × Trusted sites	×
General Security Privacy Content Connections Programs Ac Select a zone to view or change security settings.	Add this website to the zone:	websites from this zone. All websites in e's security settings.
Internet Local intranet Trusted sites Restricted sites	http://192.168.90.55	Add
Trusted sites This zone contains websites that you trust not to damage your computer or your files. You have websites in this zone. Security level for this zone	http://*.editic.com http://*.zte.com/cn http://192.169.13.20 http://192.168.90.129 http://191.168.90.180	s:) for all sites in this zone
Custom Custom settings To change the settings, click Custom level To use the recommended settings, click Defaul Enable Protected Mode (requires restarting Internet Exp Qustom level Defau	lorer)	Close
Reset all zones to defau OK Cancel	Apply	

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.

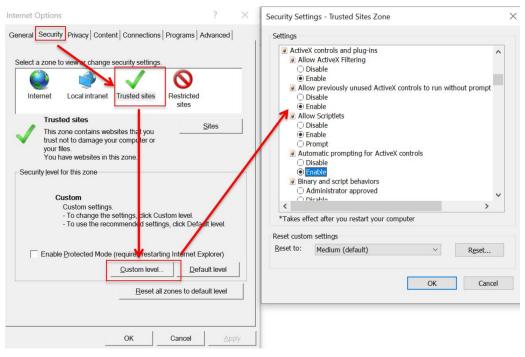


Figure 7-2 Security settings of trusted sites-1

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

Figure 7-3 Security settings of trusted sites-2



-			
	Disable		
	nable		
	Prompt		
Down			
	download		
	Disable		
	Inable		
	t download		
	Disable		
	Enable Prompt		
	• .NET Framework setup		
() Ena			
Misce			
	ess data sources across doma	ains	
Local Control of the second	Disablo	2015	
<			>
*Takes ef	fect after you restart your con	nputer	
Reset custo	m settings		
	Medium (default)	~	Reset
Reset to:	Mediulii (deidult)		

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

Figure 7-4 Security settings of trusted sites-3

OF	nable		
-	W META REFRESH		^
_	Disable		
~ -	nable		
-	w scripting of Microsoft web l	prowser control	
	Disable		
. O E	Enable		
	ow script-initiated windows wit	thout size or positi	on constraint
0	Disable		
	Enable		
	ow the TDC Control		
~ ~	Disable		
() E	Inable		
-			
	w webpages to use restricted	protocols for activ	e content
Allo	ow webpages to use restricted Disable	protocols for activ	e content
	ow webpages to use restricted Disable Enable	protocols for activ	re content
	ow webpages to use restricted Disable	protocols for activ	
	ow webpages to use restricted Disable Enable		~
Alla O E O E *Takes ef	ow webpages to use restricted Disable Enable Dromet		~



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.

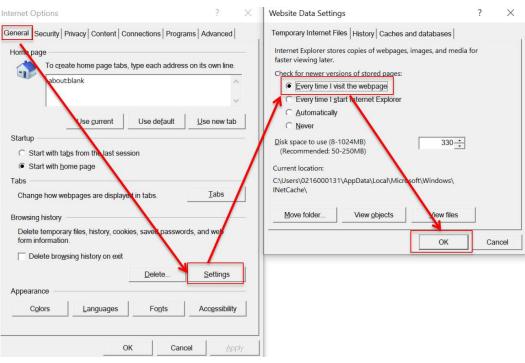


Figure 7-5 Temporary Internet Files Settings

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



-	acy Content Connections	Programs Advanced
Settings	Sites	Advanced
Location		
Never allow webs physical location	tes to request your	<u>C</u> lear Sites
Pop-up Blocker		
Turn on Pop-up <u>B</u> I InPrivate	locker	S <u>e</u> ttings
InPrivate	nd extensions when InPrivate	
InPrivate		

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.



Accelerated of a second sec	raphics		1	^
Use softw	are rendering instead of	GPU rendering*		
S Accessibility			-	
	pand ALT text for image			
	aret Browsing for new wi em caret with focus/sele			
	m sounds	outri onanges		
_ , ,	t size to medium for new	windows and tabs		
Reset zoo	om level for new windows	and tabs		
Browsing				
	cord developer console r	0		
	ised folders in History an cript debugging (Internet			
	cript debugging (Other)	Explorely		
	notification about every	script error		0
C Enable a	itomatic crash racovan/*		>	
1	ter you restart your comp	outer		
Takes encor a	tor you restart your comp			
		Restore advance	ed setting	gs
anot Internet Fuel	orer settings			
eset internet Expi	Explorer's settings to the	ir default	Re <u>s</u> et	
	Explorer o ootango to the			
Resets Internet I condition.	use this if your browser is	s in an unusable st	ate	

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



Precautions: