Technical Document of Shenzhen Securities Communication Co., Ltd.

User's Manual for SSCC-FDEP Message Transfer System FDAP

Document No.: FDEP-FDAP-PUM001

Security Classification: For public use

深圳证券通信有限公司
SHENZHEN SECURITIES COMMUNICATION CO.,LTD.

April, 2020

Document Information

Document Name	FDAP User's Manual
Note	
Project to which it belongs	Financial Data Exchange Platform

Revision History			
Date	**Version**	**Revised by**	**Description**
20120725	0.9	R&D Center	Created and completed the first draft.
20120823	0.91	R&D Center	Added CSV monitoring information
20140328	1.0	R&D Center	1. Added the default configuration of LogDir in [LOG], and provided a supplementary explanation. 2. Added supplementary explanation of bsmr startup parameter -i. 3. Added Section 4.5 Access Client Performance.
20151123	1.1	R&D Center	Added "EkeyExtId" to Section 4.1 Configuration [CurrMR] to enumerate field of Ekey, added "IsSoftCert" whether to use soft certificate, and added "CAFileName" and "SoftCertFileName" to indicate the root certificate and user certificate, respectively.
20160317	1.2	R&D Center	Added configuration [BIZTYPE] in section 4.1, the service corresponding to each app.
20190403	1.3	R&D Center	Added new features and precautions to V5

Contents

Figure Index

Table Index

1 Introduction

This document is a user manual for the financial data exchange platform message transfer system access client. It mainly introduces the user configuration, operation, and maintenance operations of the financial data exchange platform access client, and the functions of monitor terminal.

FDAP is an abbreviation of FDEP Access Point for the message transfer system of financial data exchange platforms.

1.1 Definition

FDSH: FDEP Switching Hub, a switching hub for financial data exchange platform.

FDSU: FDEP Switching Unit, financial data exchange platform switching unit, a constituent element of FDSH.

FDEAPI: Financial Data Exchange Application Programming Interface, application development interface for financial data exchange platform client.

BSMR: name of the running program of access client.

MXTerm: name of the running program of monitor terminal.

2 Software Overview

2.1 Software structure

The position of the access client in the software architecture of financial data exchange platform is shown in the following figure. The financial data exchange platform client includes three parts: access client, monitor terminal, and API.

The access client of financial data exchange platform message transfer system is a bridge used to connect the financial data exchange platform exchange hub and user applications; the monitor terminal is used to monitor the operating status of access client of financial data exchange platform.

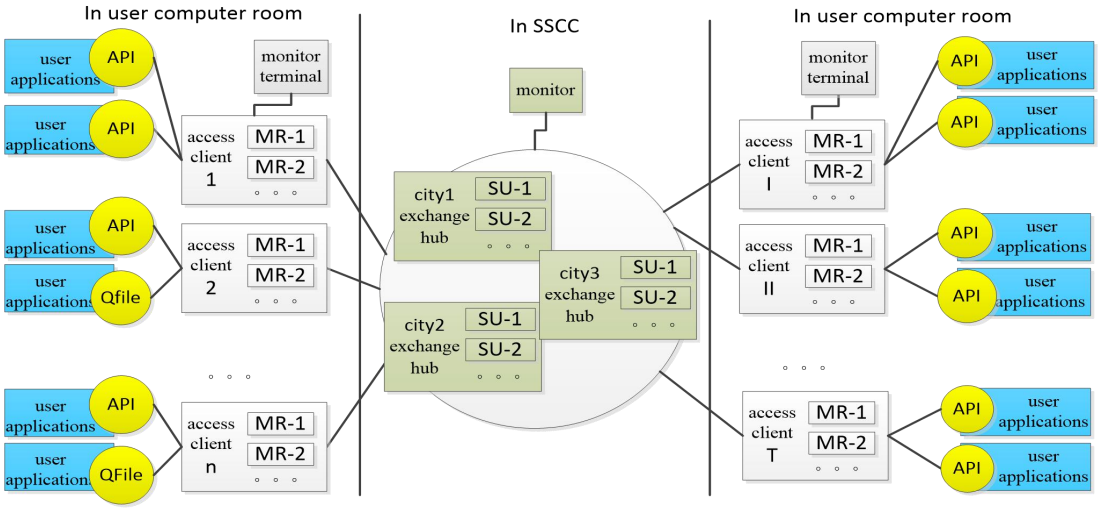


Fig. 1 Software architecture of financial data exchange platform

2.2 Structure table of program directory

The software is green software, including files.

Table 1 FDAP program package

No.	File name	Description
1	**Bsmr directory**	**Financial data exchange platform access client program and monitor terminal program are saved in this directory.**
2	bsmr.exe	Run program of financial data exchange platform access client
3	cert\sscc.cer	CA certificate cannot be modified
4	ini\mr.ini	Configuration file shall be modified
5	ini\spdctrl.db	Speed control instruction storage file, cannot be deleted manually during operation
6	log\ bsmr_mon_***.csv	CSV format file for user monitoring
7	log\sxdata20190401_*.log	Transaction log file
8	log\bsmr_20190401*.log	Running log file

No.	File name	Description

1	**Mxterm directory**	**Financial data exchange platform monitor terminal program are saved in this directory.**
2	Mxterm.exe	Run program of financial data exchange platform monitor terminal program
3	cfg\mxterm.ini	Configuration file,cannot be deleted or modified manually
4	lang directory	Language packs are saved here,cannot be deleted manually
5	plugin directory	The plugins needed to run monitor terminal program are saved here,cannot be deleted manually
6	qt.conf	QT plugin configuration file,cannot be deleted manually
7	*.dll	Dynamic library for monitor terminal program,cannot be deleted manually
8	log\mxterm_20200401_*.log	Running log file for monitor terminal program

2.3 Requirements for hardware

	Configuration	Comments
Model	PC Server	PC Server is suitable for long-time startup and installation on machine room rack
CPU	Main frequency above 3.0G	
Memory	Above 4G	
Hard Disks	Above 150G and disk mirroring	The size of the program itself is only less than 10M, but eht generated logs will continue to consume disk due to continuous incurease
Ethernet cards	Dual NIC	
USB Interfaces	At least two USB2.0 interfaces	At the rear of the machine
Power	Dual power module is recommended	

Note: the above configuration can be adjusted according to the actual situation of the user.

2.4 Requirements for software

Program	Operating system name	Version
access client programs	Microsoft Windows Server 2008、Microsoft Windows Server 2012、Microsoft Windows 10、Microsoft Windows Server 2016 、 Redhat Enterprise Linux6.8 、 Redhat Enterprise Linux7.5	
monitor terminal program	Windows 7 and later operating systems of Windows 、 Linux(Interface required)	

3 Installation and Uninstallation

3.1 Installation procedure

The financial data exchange platform message transfer system access client is green software, and files can be copied directly to the operating system's operating directory.

3.2 Uninstall process

Just delete the directory.

4 Instructions for Operating Access Client

4.1 Prerequisites for access client operation

Two prerequisites are necessary for operating BSMR software:

(1) The user must have an Ekey electronic certificate or soft encryption issued by Shenzhen Securities Communications Company for login;

(2) The user must correctly configure the ini\mr.ini file in the directory after installation. If the

user has to run multiple BSMRs, the configuration of other sections except the [CurrMR] section must be consistent on multiple MRs.

[It can be configured through the configuration program provided by Shenzhen Securities Communication]

```
[CurrMR]    //Current MR information, this line cannot be modified
"MRName"="MR-1"                    //The name of current MR must match one of the MR-beginnings listed below. For details, see [MR-1]
"StartCmd"="-f +wt"                //Start parameter， separated by spaces.[-i(Install service)][-u(Uninstall service)][-h(Help)][+w(Print simple log)][+wt(Print all log)][-servicename=Service name]
"UserID"="SSCC_TEST01"             //User ID
"UserPasswd"="123456@abc"          //User password[plaintext]
"UserPasswdCrypt"="2c5189a328e7d87d491e533764170c2a"    //User password[ciphertext]，users can choose one of plaintext or ciphertext
"Ekey"="/C=CN/CN=SSCC_TEST01"      //Topic name of e-certificate EKey
"EkeyPwd"="111111"                 //Login Password for EKey[plaintext]
"EkeyPwdCrypt"="948514863abee7c1c9cfe36eb1a826ca"    //Login Password for EKey[ciphertext]，users can choose one of plaintext or ciphertext
"EkeyExtId"="1.2.86.100.4.3.2"     //Read Ekey's fields
//"IsSoftCert"="1"                 //Whether to use soft certificates file
//"SoftCertFileName"="FTCSTEST01.pfx"    //Soft certificates file name
"PkgMaxAliveSec"="40"              //FDAP Maximum live time in the queue for packets received by FDAP, in seconds
"AllowMultiApp"="1"                //The same machine allows multiple MRs to be started
"OnceRecvMsgCount"="1"             //The maximum number of packets returned by the APP when fetching packets from MR
"TermName"="termname"              //Login name for MxTerm
"TermPwd"="termpas"                //Login password for MxTerm[plaintext]
"TermPwdCrypt"="9e3f227b69360934ad4ad9ff35e286e8"    //Login password for MxTerm[ciphertext],users can choose one of plaintext or ciphertext
"AutoBalance"="1"                  //Auto Balance App
"BalanceOfFileInstanceId"="0"      //File message instance number matching mode, 0: match
```

the first one by default, 1: polling equalization mode, 2: modulo after checksum.
"TopicPushMode"="0" //Topic message push, 0: push to the first applinkid by default, 1: push all applinkid

[SUIPMap] //IP address mapping information,address before conversion = address after conversion, if there is no NAT conversion or multi-line access, just configure left = right
"172.100.1.10:7001"="172.100.1.10:7001"
"172.100.11.10:7001"="172.100.11.10:7001"
"172.100.1.11:7001"="172.100.1.11:7001"
"172.100.1.12:7001"="172.100.1.12:7001"
"172.100.1.13:7001"="172.100.1.13:7001"
"172.100.1.14:7001"="172.100.1.14:7001"
"172.100.11.11:7001"="172.100.11.11:7001"
"172.100.11.12:7001"="172.100.11.12:7001"
"172.100.11.13:7001"="172.100.11.13:7001"
"172.100.11.14:7001"="172.100.11.14:7001"
"172.100.43.11:7001"="172.100.43.11:7001"
"172.100.43.12:7001"="172.100.43.12:7001"

[APPINFO]//Username and password of the current app[plaintext]
"app1"="1"
"app2"="1"
"app3"="1"
"app4"="1"
"app5"="1"
"app6"="1"
"app7"="1"

[APPINFOCRYPT]//Username and password of the current app[ciphertext]
"app1"="bb683b359da5788ad377fa755b6b998d"
"app2"="bb683b359da5788ad377fa755b6b998d"
"app3"="bb683b359da5788ad377fa755b6b998d"
"app7"="bb683b359da5788ad377fa755b6b998d"

[BIZTYPE] //Corresponding business types of APP: 0 represents three-party depository business, 11 the direct sales business, 12 the funds transfer business, 13 the securities offer business (securities trading), 14 the electronic reconciliation business, 15 the financing and securities loan business, 16 the after-hours business of the fund, 17 the transfer financing business, 18 the B to H business, 19 the cross-selling business (financial product sales), 20 the securities repurchase business (quotation repurchase), and 21 the individual stock options business (bank-derivative transfer), 23 the private equity report transfer business. Judgment of newly added business type size (<128). If it is greater than 128, it is a file message, the business field is filled when the file is sent by the api.

"app1"="0"

"app2"="11"

"app3"="12"

"app4"="0"

"app5"="0"

"app7"="0"

[MR-1] //Configuration of Switching Unit 1

"Enable"="1" //Enable or not

"InnerIP"="127.0.0.1" //Inner IP of Switching Unit 1

"ClientIP"="127.0.0.1" //Client IP for Switching Unit 1

"InnerPort"="3600" //Communication port between switching units

"TermPort"="3601" //Communication port between switching unit and management terminal

"ClientPort"="3602" //Communication port between the switching unit and the client API

//"ExpectApp"="app1"

//"UserMonitorVer"="05.00.20190630" //[Version Infotmation] Synchronize with UserMonitor

//"UserMonitor"="1|app3|5|10,1|app3|5|10" //User monitoring information interface [monitoring method |Process path |Call interval in seconds |Expiration time in seconds], see section 4.8 Access Client User Monitoring for details。

```
[MR-2]                  //Configuration of Switching Unit 2
"Enable"="0"                        //Enable or not
"InnerIP"="127.0.0.1"               //Inner IP of Switching Unit 2
"ClientIP"="127.0.0.1"              //Client IP for Switching Unit 2
"InnerPort"="4600"                  //Communication port between switching units
"TermPort"="4601"     //Communication port between switching unit and management terminal
"ClientPort"="4602"     //Communication port between the switching unit and the client API
//"ExpectApp"="app2"
//"UserMonitorVer"="05.00.20190630"     //[Version Infotmation] Synchronize with UserMonitor
//"UserMonitor"="1|app3|5|10,1|app3|5|10"       //User monitoring information interface [monitoring method |Process path |Call interval in seconds |Expiration time in seconds]

[LOG]//日志配置
"Level"="0"                 //Log level
"Display"="3"               //Printing type, 0 means no log is displayed or recorded; 1 means log is only recorded in file; 2 means log is only displayed on screen (only valid for console program); 3 means log is recorded in file and displayed on screen
"LogDir"="../log"           //The log directory, if started as a service, must be configured as an absolute path.
"LogName"="../log/bsmr.log"       //Log name
"MaxFileCount"="20"               //Maximum file count in the day
"MaxFileSize"="500000000"       //Maximum size of single file
"MaxSaveDays"="-1"              //Maximum save days of log，-1 means disable
```

Configuration method description:

1) Replace SSCC_TEST01 in "Ekey" = "/C=CN/CN=SSCC_TEST01" with the real Ekey topic name.

2) The [SUIPMap] section configures the address mapping information. The real address of the switching hub is configured on the left side of the equal sign, and the mapped address is

configured on the right side.

3) [APPINFO] [APPINFOCRYPT] users can expand by themselves and add new apps.

4) The configuration method of [MR-1] and [MR-2] sections is similar, where "Enable" is 1, indicating that the configuration of this section is valid, and 0 indicates that it is invalid. "InnerIP" and "InnerPort" are used for multiple mr internal communications, and cannot be exactly the same in [MR-1] and [MR-2]; "ClientIP" and "ClientPort" are used to provide services to user programs in [MR -1] and [MR-2] cannot be exactly the same. "TermPort" is used to manage the disconnected use of the FDAP. When multi-active MR is deployed across machines, the IP address must be configured as the actual IP increment, and cannot be configured as a loopback address.

5) Monitoring methods include 1: redirection, 2: CSV format, and 3 both.

6) The password can be generated using the BsmrIniSet program or mrterm.

4.2 Access client run chart

The name of the access client program is bsmr.exe, and the operating parameters are as follows:

Table 2 BSMR program run chart

No.	Run command	Meaning
1	bsmr –h	It shows run help and may print run parameters
2	bsmr -i	Installed as a service program. When the user installs the program, it has been automatically installed as a service program for the user, therefore users generally should not use this option. If -i is configured during service startup, remove -i before the second startup. [not supported by Linux]
3	bsmr -u	Uninstall the service program. When the user uninstalls the program, the service has been automatically uninstalled for the user, therefore users generally should not use this option. [not supported by Linux]
4	bsmr –f	Started by console. bsmr can only be started by service mode by default, if you need to start by console, you need to add this parameter
5	bsmr +w	Write any exchange log, only record header information.
6	bsmr +wt	Write any exchange log, not only record the packet header information, but also the packet body information.

No.	Run command	Meaning
7	bsmr	This is the wrong way of running. The program cannot be run in the command line mode without parameters. In this case, the program will first detect the service, then display user parameter errors and prompt the user to continue running as a command line application.
7	Start in Window Service Manager	This is the normal startup method. [not supported by Linux]

4.3 Operating steps of access client

4.3.1. Configure the ini \mr.ini file correctly. For details, see section 4.1.

4.3.2. If it is hard encryption, install the drive program of the EKey on the computer running the software, and then insert the Ekey issued by Shenzhen Securities Communication Co., Ltd. into the USB interface. (Do not insert Ekey when installing the driver)

4.3.3.1 Window version startup program: Manually start the financial data exchange platform access client services in a service mode.

[Note: The startup user must be an administrator user] The steps for manual startup are as follows:

(1) Open "My Computer ---- Control Panel ---- Management Tools", and then turn on the service;

(2) Find "SSCC_BSMR" and select it. Double-click to display the property dialog box, fill in the relevant operating parameters in the field Startup Parameters, and then click the "Start" button on the toolbar to start the software. By default, the service is of the "automatic" startup type. When the computer restarts, the software will start automatically with the operating system and users can modify it.

(3) To stop running software, the user can also stop the service in the service manager.

4.3.3.2 Linux version startup program:

[Note: The startup user must be the root user] Start directly, or start in the nohup background.

4.4 Steps to stop access client

4.4.1 Window version:

It is permitted to manually stop the financial data exchange platform access client services by using services. To manually stop the service:

(1) Open "My Computer ---- Control Panel ---- Management Tools", and then turn onn the service;

(2) Find "SSCC_BSMR" and select it, and then click the "Stop Service" button on the toolbar to stop the software.

4.4.2 Linux version

Kill 1 [Process id]

4.5 Performance of access client

Test on the operating system Windows Server 2003(Message size 1KByte):

(1)API has three processing modes, one is to bsmr polling mode,no less than 500 per second, the second is to configure parameter OnceRecvMsgCount ,with performance of 5000 per second, and the third is to register push-down mode, with performance of 7000 per second.

(2)Processing each APP relates to the separate thread, and different APPs can be extended in parallel.

(3) The data packets received and sent by the access client is 10,000 per second, with the size of 1KB.

4.6 Access client operation interface and operation instructions

The Windows version runs as a Windows service and has no user interface.

Linux version does not have a user interface

4.7 Interface format of access client Q file

Q files are used to send and receive messages. The files are in dbf format.

The BSMR receives the message and writes to the dbf file received, and the APP reads the

message through the file.

The APP writes the message to the dbf file sent, and the BSMR reads the file and sends it out.

The file name of the message sent by the APP is fdep_ [date] _ [APP name] _send.dbf, such as fdep_20120725_app20_send.dbf.

The file name of the message received by APP is fdep_ [date] _ [APP name] _recv.dbf, such as fdep_20120725_app20_recv.dbf.

The number of data segments is configurable, see MRini for details.

Table 3 Q file protocol format

No.	Field name	Description	Type	Length	Remark
1	ID	Record ID	N	10	
2	SrcUserID	Source user ID	C	32	
3	SrcAppID	Source APPID	C	32	
4	DestUsrID	Destination user ID	C	32	
5	DestAppID	Destination APPID	C	32	
6	PkgID	Package ID	C	64	
7	CorrPkgID	Correlated package ID	C	64	
8	UserData1	User data 1	C	255	
9	UserData2	User data 2	C	255	
10	Flag	Flag bit	N	3	
11	BizType	Business type	N	3	
12	Priority	Priority	N	3	
13	SLevel	Sensitivity level	N	3	
14	MsgType	Message type	C	8	
15	ErrorCode	Error value	N	10	
16	DataLen	Message length	N	10	
17	Data0	Message content 0	C	255	
18	Data1	Message content 0	C	255	
…	…	Message content			
17+ N	DataN	Message content N	C	255	
18+ N	WTime	Write time	N	10	hhmmss.ccc [Two-bit, hour][Two-bit, minute][Two-bit, second].[Three-bit, ms]
18+	ReadyFlag	Data prepares flag	C	1	R means ready

N+1					
18+ N+2	FdepMark	Fdep uses extension field	C	20	
18+ N+3	UserMark	User uses extension field	C	20	

Example:

4.8 User monitoring by access client

BSMR provides two forms of user monitoring: 1 means redirection; 2 means CSV file output.

In the configuration item

[MR-]

"UserMonitor"="1|E:\UserMonitor.exe|3|5" //User monitoring information interface [monitoring method |Process path |Call interval seconds | expiration time seconds]
1 Redirection method:

Configuration example: "UserMonitorVer" = "05.00.20190630"

The meaning of the configuration is: 05.00.20190630 and later versions employs the new output format, and the previous version is compatible with the old format

Configuration example: "UserMonitor" = "1 | E: \ UserMonitor.exe | 3 | 5"

The configuration means: use the redirection method, the process path is E: \ UserMonitor.exe, and it is called every 3 seconds, and the redirection is automatically turned off when it exceeds 5.

BSMR periodically calls the user's process according to the configuration, and sends the FDAP operation information to the user process through the redirection mechanism. The user can customize own monitoring program accordingly.

See the sample program for the information provided and how to call it

UserMonitor.cpp

Example:

2. CSV file mode:

Configuration example: "UserMonitorVer" = "05.00.20190630"

The meaning of the configuration is: 05.00.20190630 and later versions employs the new output format, and the previous version is compatible with the old format

Configuration example: "UserMonitor" = "2 || 3 |"

Configuration means: use CSV file method, write the file every 3 seconds,

CSV file is log/bsmr_monYYYMMDD.csv

BSMR writes the FDAP operation information to a CSV format file according to the configuration timing. Users can customize their own monitoring procedures accordingly.

Table 4 CSV protocol format

Line message	**Specific meaning**
Time	2-08-25 09:57:23
MR message	MrCount=1|MonitorVersion=1|MrName=MR-1|UserID=FTCSTEST3|Link2su=0|Cpuload=4 |MaxSingleCpuload=5|MemTotalMB=246859|MemAvailMB=178544 |SwitchInSpeedPerSec=0|SwitchOutSpeedPerSec=0|TotalDiskGB=2929 |FreeDiskGB=1245|Version=04.00.20120701|RecvSpeedKbps=731 |SendSpeedKbps=0|RecvTotal=|RecvFailed=|SendTotal=|SendFailed=|TopicRecvTotal=|TopicRecvFailed=|TopicSendTotal=|TopicSendFailed=|RecvFileTotal=|RecvFileSucess=|RecvFileFailed=|SendFileTotal=|SendFileSucess=|SendFileFailed=|RecvFileTotalSize=|RecvFileSucessSize=|RecvFileFailedSize=|SendFileTotalSize=|SendFileSucessSize=|SendFileFailedSize= Mr's number | mr name | user name | connected to SU or not| cpu of the machine | the highest CPU of single machine |total memory |available memory |average speed of sending packets |average speed of receiving packets |total hard disk space |available memory space | MR version | sending network speed of SU link |Total number of ordinary message receive packets |Number of ordinary message failed received packets | Total number of ordinary

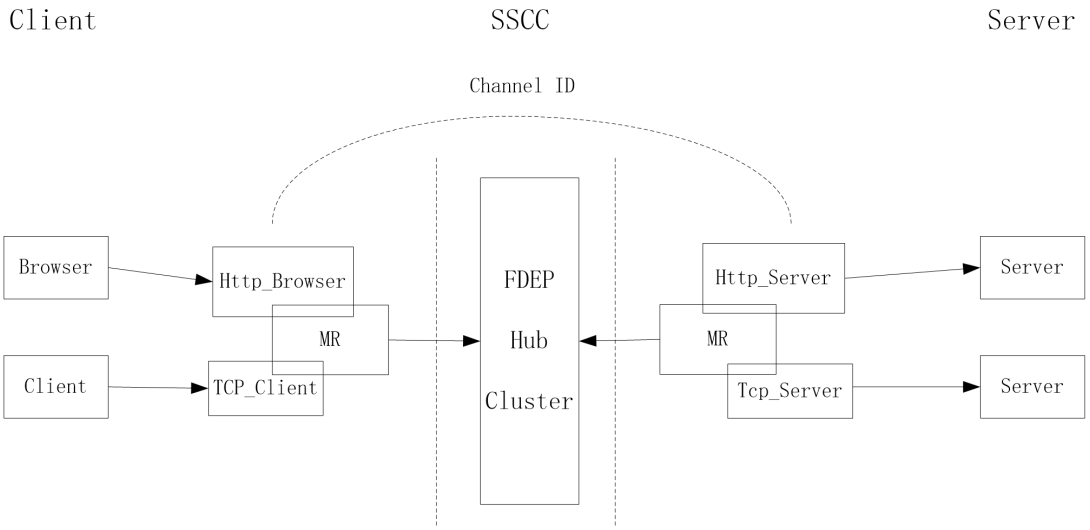
Line message	Specific meaning
	message sent |Number of ordinary message failed to send | Total message received | Total number of message failed to receive | Total number of topic message sent| Number of topic message failed to send| Total number of file message received | File message successfully received | Number of file message failed to receive | Total number of file message sent | Number of file message successfully sent | Number of file message failed to send | Total size of file messages received | Size of file message successfully received | Size of file message failed to receive | Total number of file message sent | Number of file message successfully sent | Number of file message failed to send
Cache packet information	MsgQueueCount=2|MrName=MR-1|AppName=app1|Size=0| MrName=MR-1|AppName=app2Size=2 Number of message cache queues | mr name of cache queue | APP name of cache queue | number of cache packages
APP message	AppCount=2|MrName=MR-1|AppName=app20|LinkID=QFILE_LINKUUID |SendCount=90|RecvCount=85|ConTime=2012-08-23 16:53:35|ClientIp=|Version=|MrName=MR-1|AppName=app6 |LinkID=05000000|SendCount=640|RecvCount=640|ConTime=2012-08-23 16:53:36|ClientIp=10.10.22.39|Version=04.00.20120701||TopicSendCount=|T opicRecvCount=|FileSendCount=|FileSendSize=|FileRecvCount=|FileRecvSiz e= App number | mr name | app name | link ID | sending number | receiving number | connecting mr time | app ip address | app version | number of topic message sent | number of topic message received| number of file message sent |size of file message sent | number of file message received | size of file message received
Online user information	OnlineUserCount=2|UserID=FTCSTEST1:FTCSTEST100 Number of online users | User id = User ID1: User ID2
SU detection information	TcpSnifferCount=1|TestTime=2012-08-25 09:31:27|MrName=MR-1|SuIP=10.10.24.41|SuPort=7001|MrIp=10.10.22.185 |Result=0 Number of detection results | Time of detection | mr name | IP address of SU | Port of SU | IP address of local mr | Detection result (0 means success, 1 means failure)

4.9 Proxy function by access client

The proxy function is to extend the function of the original FDEP message transfer system,so that customers can directly access the FDEP message transfer system by using

the original protocol when migrating to special line environment of SSCC,without secondary development for the fdep protocol,so as to realize seamless migration.

4.9.1 Access client proxy process



Preparation conditions for starting proxy function：

1） Both user A and user B have their own UserID that have been successfully applied to SSCC,and they are provided with communication relationship and mutually agreed communication.

2）Both user A and user B correctly configure ini\mr.ini according to section 4.1，4.2，4.3 ,and can normally access client.(Exit the client after normal startup,this step is only to verify whether the normal BSMR can be started normally)

3）User A and user B configure ini\Proxy.ini correctly,and can startup proxy client correctly,the connection between proxy client and SSCC hub is normal(After normal startup,BSMR can be used as a proxy client)

HTTP proxy：User A sets the proxy through the browser.The address filled in by the proxy is listening IP address of the Http_Browser module in the ini\Proxy.ini of the BSMR client,and the port is the listening port.At this time,the browser can establish a connection with Http_Browser module of the access client.After the connection is established successfully, the module sends the request to the peer(User B) through the hub,after the peer Http_Server module receives the request,it establishes the connection with the destination server by

analyzing the destination address information carried in the request.After the whole channel is opened,data transmission is carried out.

TCP proxy：User A initiates a TCP connection to the TCP_Client module in BSMR through the client.After the connection is established successfully,he module sends the request to the peer(user B) through the hub,after the peer TCP_Server module receives the request,it establishes the connection with the destination server through the destination address and port configured in ini\Proxy.ini file of client.After the whole channel is opened,data transmission is carried out.

4.9.2 Proxy function configuration

In addition to the prerequisites necessary for the access client to run(chapter 4.1),to enable the proxy function,the user must correctly configure the ini\Proxy.ini configuration file:

Where the AppID in proxy configuration file ini\Proxy.ini cannot be the same as any AppID in the [APPINFO]filed in ini\mr.ini.

If multiple BSMRs are run by the same user,the AppID in the proxy configuration file of the primary and standby BSMR cannot be the same.

The proxy module configuration section must contain the [Type] ,which represents the proxy type.

```
[HttpB1]                          ///proxy module,modify according to true AppID
"Type"="HTTP_Browser"             ///proxy type is HTTP browser proxy
"ListenIP"="127.0.0.1"            ///proxy listening IP address
"ListenPort"="7001"               ///proxy listening port
"TimeOutSec"="180"                ///Timeout wait time,default value is 180s=3min，if no
data is transmitted over this time ,disconnect
"PoolThreadCount"="4"             ///Number of thread pool，default value is 1
"MaxAcceptCount"="1000"           ///Maximum number of connections to server,default
value is 1000
"BizType"="0"                     ///Business type，modify according to true business type
"RecvSpeedCtrlKbps"="10240"   ///Browser transmission speed limit,default 10Mbps
```

```
[HttpS1]                          ///proxy module,modify according to true AppID
"Type"="HTTP_Server"              ///proxy type is HTTP browser proxy
"TimeOutSec"="180"                ///Timeout wait time,default value is 180s=3min，if no data
is transmitted over this time ,disconnect
"PoolThreadCount"="4"             ///Number of thread pool
"MaxConnCount"="1000"             ///Maximum number of initiated connections
"BizType"="0"                     ///Business type，modify according to true business type
"RecvSpeedCtrlKbps"="10240" ///Browser transmission speed limit,default    value is
10Mbps

[TcpC1]                           ///proxy module,modify according to true AppID
"Type"="TCP_Client"               ///proxy type is TCP client proxy
"ListenIP"="127.0.0.1"            ///TCP proxy listening IP address
"ListenPort"="7003"               ///TCP proxy listening port
"DestUserID"="userTest"           ///peer user's UserID
"DestAppID"="#PortMap1"           ///peer user's AppID
"TimeOutSec"="180"                ///Timeout wait time,default value is 180s=3min，if no data is
transmitted over this time ,disconnect
"PoolThreadCount"="4"             ///Number of thread pool
"MaxAcceptCount"="1000"           ///Maximum number of connections to server
"BizType"="0"                     ///Business type，modify according to true business type
"RecvSpeedCtrlKbps"="10240" ///Browser transmission speed limit,default    value is
10Mbps

[TcpS1]                           ///proxy module,modify according to true AppID
"Type"="TCP_Server"               ///proxy type is TCP client proxy
"ServerAddr"="127.0.0.1:7001"     ///Destination IP address and port
"TimeOutSec"="180"                ///Timeout wait time,default value is 180s=3min，if no data is
transmitted over this time ,disconnect
"PoolThreadCount"="4"             ///Number of thread pool
"MaxConnCount"="1000"             ///Maximum number of initiated connections
"BizType"="0"                     ///Business type，modify according to true business type
```

```
"RecvSpeedCtrlKbps"="10240" ///Browser transmission speed limit,default value is 10Mbps

[HostMap]       ///The peer user's UserID and AppId corresponding to the address entered by the browser
"www.sscc.com.cn"="DestUserID:DestAppID"

[DNS]           ///Domain name resolution address,IP address corresponding to thedomain name entered by the browser
"www.sscc.com.cn"="10.10.10.16,10.10.10.20"

[FilterAddr]    ///URLs filtered
"FilterUrl"="oa.sscc.com"
"FilterUrl"="www.firefox.com"
```

Configuration method description：

Configuring several AppIDs means that the BSMR client has several proxy modules；

Four types of proxy, one or more of which can be configured as needed,or one or more of each type.

If only used as a TCP proxy，[HostMap]、[DNS]、[FilterAddr]field content can be defaulted ,and these three fields are only used for the HTTP proxy function.

If this profile is missing,it will run as a normal BMSR access client without proxy function,but if it is available and configured incorrectly,the whole BSMR will not startup properly.

4.9.3 Access client TCP proxy

There are two types of TCP proxy:TCP_Client and TCP_Server,two users communicating with each other,if an access client is TCP_Client then the other end must configure TCP_Server proxy module。

Configuration of the proxy modules ,see section 4.9.

TCP_Client：

1） You need to listen on client connections.so you must configure the client listening port [ListenPort],and [ListenIP] can either fill in the client IP or default,default port for network-wild listening.

2）To communicate with the peer user,you need to configure the UserID and AppID of the peer user。

TCP_Server:

You need to configure destination IP address and port.

For example,if user A's TCP_Client configuration is as follows:

```
[TcpC1]   ///proxy module,modify according to true AppID
"Type"="TCP_Client"    ///proxy type is TCP client proxy
"ListenIP"="127.0.0.1"  ///TCP proxy listening IP address
"ListenPort"="7003"     ///TCP proxy listening port
"DestUserID"="BUserID"  ///peer user's UserID
"DestAppID"="TcpS1"     ///peer user's AppID
"TimeOutSec"="180"      ///Timeout wait time,default value is
180s=3min, if no data is transmitted over this time ,disconnect
"PoolThreadCount"="4"    ///Number of thread pool
"MaxAcceptCount"="1000"       ///Maximum number of initiated
connections
"BizType"="0"  ///Business type, modify according to true business
type
"RecvSpeedCtrlKbps"="10240"     ///Browser transmission speed
limit,default value is 10Mbps
```

To connect to the proxy,the client needs to fill in the IP and port of the module

Then user B's TCP_Server configuration is as follows:

```
[TcpS1]     ///proxy module,modify according to true AppID
"Type"="TCP_Server"   ///proxy type is TCP server proxy
"ServerAddr"="127.0.0.1:7001"   ///Destination IP address and port
"TimeOutSec"="180"    ///Timeout wait time,default value is
180s=3min, if no data is transmitted over this time ,disconnect
"PoolThreadCount"="4"     ///Number of thread pool
"MaxConnCount"="1000"   ///Maximum number of initiated connections
"BizType"="0"   ///usiness type, modify according to true business
type
"RecvSpeedCtrlKbps"="10240"   ///Browser transmission speed
limit,default value is 10Mbps
```

The [ServerAddr] field of the proxy module needs to know the server's listening IP and port to connect to the server by reading its configuration.

4.9.4 Access client HTTP proxy

There are two types of HTTP proxy:HTTP_Browser and HTTP_Server,two users communicating with each other,the access client responsible for receiving and forwarding browser-side information acts as HTTP_Browser,and the access client used to initiate requests for resources connected to web server acts as HTTP_Server.Use HTTP proxy mode for web page access,configure HTTP_Browser module,you must ensure that the web server corresponding to the web page you are visiting has access client connectivity configured with HTTP_Server module.

Configuration of the proxy modules ,see section 4.9.2

HTTP_Browser：

1） You need to listen on client connections.so you must configure the client listening port [ListenPort],and [ListenIP] can either fill in the client IP or default,default port for network-wild listening.

2） The UserID and APPID of the peer user corresponding to the domain name must be configured in node[HostMap].

HTTP_Server:

When the web server serves as a domain name,and the machine running the access client that configures the HTTP_Server module is unable to obtain the IP address of the web server corresponding to the domain name locally,it is necessary to fill in [DNS]node manually to map the domain name to the IP address.

For example,if user A uses IE browser to access web address abc.com,and web server of abc.com is managed by user B,then user A wants to access abc.com using HTTP proxy function of access client,user B also needs to intervene in FDAP system,User A and user B get their own UserID ,then configure it in user A:

```
[HTTPB1]    //current APPID is "#Proxy1"
"Type"="HTTP_Browser"      //proxy type is HTTP browser proxy
```

```
"ListenIP"="10.10.160.14" //proxy listening IP address，default is local IP
"ListenPort"="7004"          //proxy listening port,mandatory field
"TimeOutSec"="300"           //Timeout wait time,default value is 180s
"PoolThreadCount"="4"        //Number of thread pool，default value is 1
"MaxAcceptCount"="20000"     //Maximum number of connections to server,default to 1000
"BizType"="0"                ///Business type,mandatory field
"RecvSpeedCtrlKbps"="5120"   //Browser transmission speed limit,default 10Mbps,range[200-10240]

[HostMap]
"abc.com"="UserB:HTTPS1"
```

Configure in user B：

```
[HTTPS1]   ///current APPID is“#Proxy2”
"Type"="HTTP_Server"     //proxy type is HTTP server proxy
"TimeOutSec"="300"       //Timeout wait time,default value is 180s
"PoolThreadCount"="1"    //Number of thread pool，default value is 1
"MaxConnCount"="1000"    //Maximum number of initiated connections
"BizType"="0"            //Business type,mandatory field
"RecvSpeedCtrlKbps"="5120"   //Browser transmission speed limit,default 10Mbps,range[200-10240]

[DNS]     //Optional section
"abc.com."="10.10.10.16"
```

Other related configuration instructions：

The HTTP_Browser configuration must contain[HostMap]node content,which stores BSMR proxy UserID and AppID mappings for the domain name to be accessed,in a uniform format of ：“domain name”=“DestUserID：DestAppID”

【Note】When a website is redirected to a different domain name ,you need to add the new domain name to the[HostMap]。

For example：

```
[HostMap]
"abc.com"="UserB:HTTPS1"
"def.com"="UserB:HTTPS1"
```

When you visit abc.com,the web server returns redirection 30x to the new address def.com,then the peer UserID and APPID mapped by def.com are also configured in [HostMap]node

Configure Optional section[FilterAddr] of HTTP_Browser to filter domain names that do not initiate access,in a uniform format of ：“FilterUrl”=“url”

For example：

```
[FilterAddr]
"FilterUrl"="www.firefox.com"
```

Configure Optional section[DNS] of HTTP_Server,configures the true IP address of the domain name mapping,look in the local Host file if there is no nodes or if the DNS transformation is not found at that node.

For example：

```
[DNS]
//Multiple IP addresses can be configured as domain name mappings,and BSMR software will randomly selects one to connect to
"www.sscc.com.cn"="10.10.10.16 , 10.10.10.20"
```

After the Proxy.ini is filled correctly,startup according to the chapter 4.3 Operating steps of

access client,browser configures HTTP proxy function,proxy IP address and port are found in proxy browser configuration node in Proxy.ini

5 Instructions for Running Monitor Terminal

5.1 Functions of monitor terminal

The main function of the monitor terminal is to monitor the running status of the access client program, the connected queues and users, and the connection status of access client and switching hub.

The monitor terminal operates as a client, and can be accessed at any suitable location for monitoring, and communicate with one of the server by TCP.

5.2 Starting monitor terminal

The monitor terminal provides Windows platform interface program and Linux platform interface program.

Program startup method under Windows: Double-click the MxTerm.exe file to start.

Program startup method under Linux: Run the MxTerm.sh script to start.

5.3 Stopping monitor terminal

The monitor terminal is a standard interface program. The method of stopping the program: click the Close button in the upper right corner of the window with the mouse, and exit the program.

5.4 Operating instructions for monitor terminal

Follow the instructions in 5.2 to run the software. The software login interface is as follows:

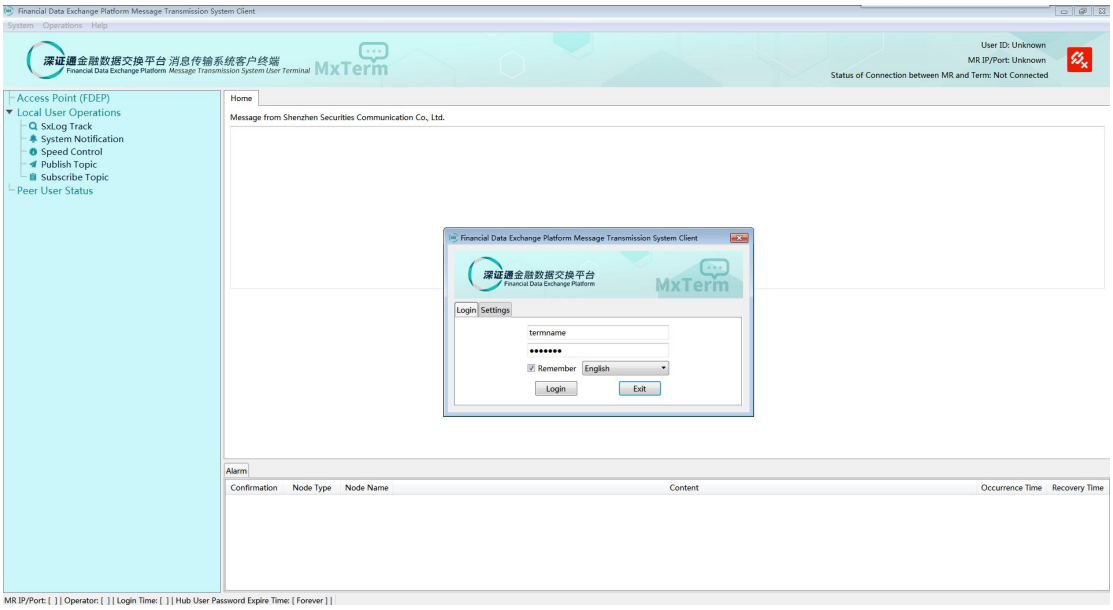


Fig. 2 Monitor login interface

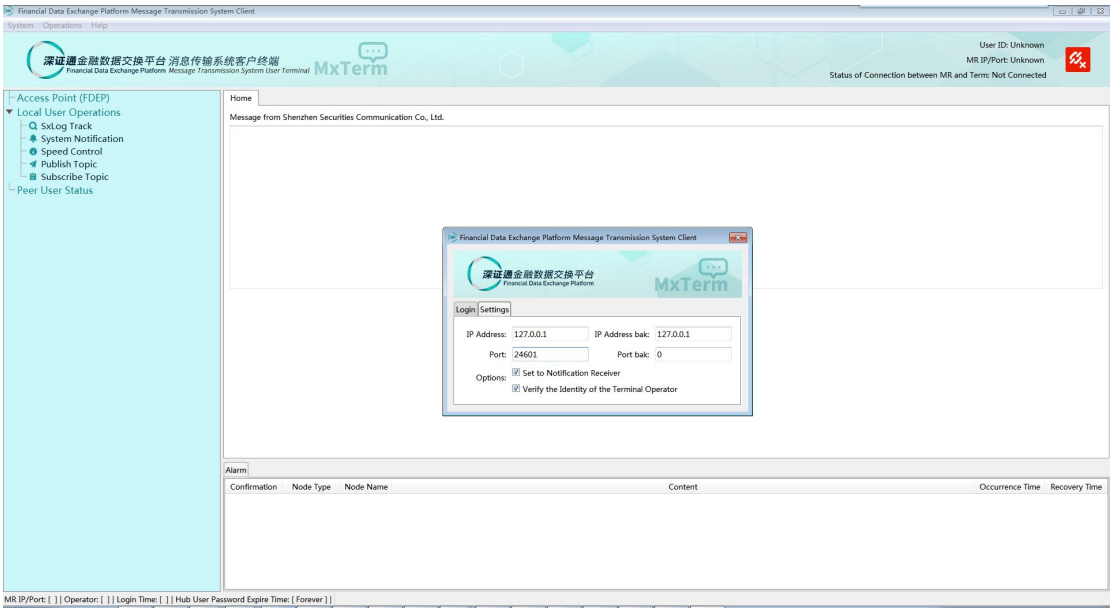


Fig. 3 Monitor terminal login address bar interface

Enter the IP address and port, username and password of the access client in the login dialog box to connect to the access client. The tab page of the login dialog provides two sets of client IP addresses and ports. The connection order is that the monitor terminal attempts to connect from the first set of addresses. The second set will be tried if the first connection is not available. Try the second set and try again cyclically until the connection is successful. If only one access client is deployed, the two sets of addresses can be identical.

After connecting to the access client, you can view the queue under each AP node and the

status of the connected client by opening each node on the left tree; select each node and check the status of the access client on the upper right. The lower right corner provides the alarm message.

If, after the monitor terminal is connected to the client, the monitor terminal disconnects unexpectedly, the monitor terminal will automatically reconnect to the client.

After login, the main interface of the monitor terminal is shown in the figure below.

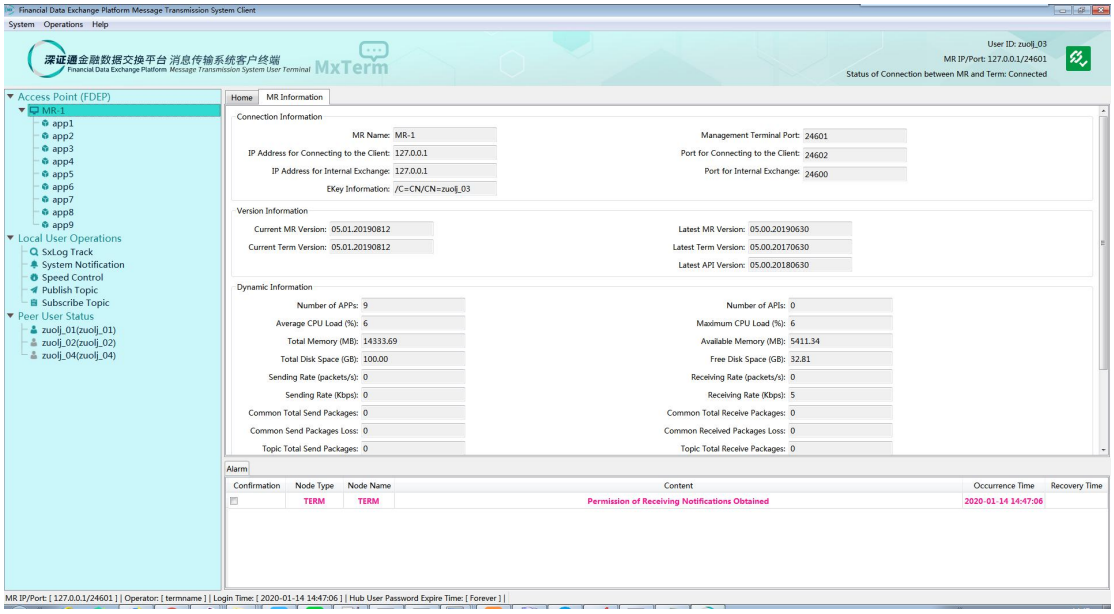


Fig. 4 Monitor terminal main interface

Click each node separately, and you can see the detailed information of each node in the right panel.

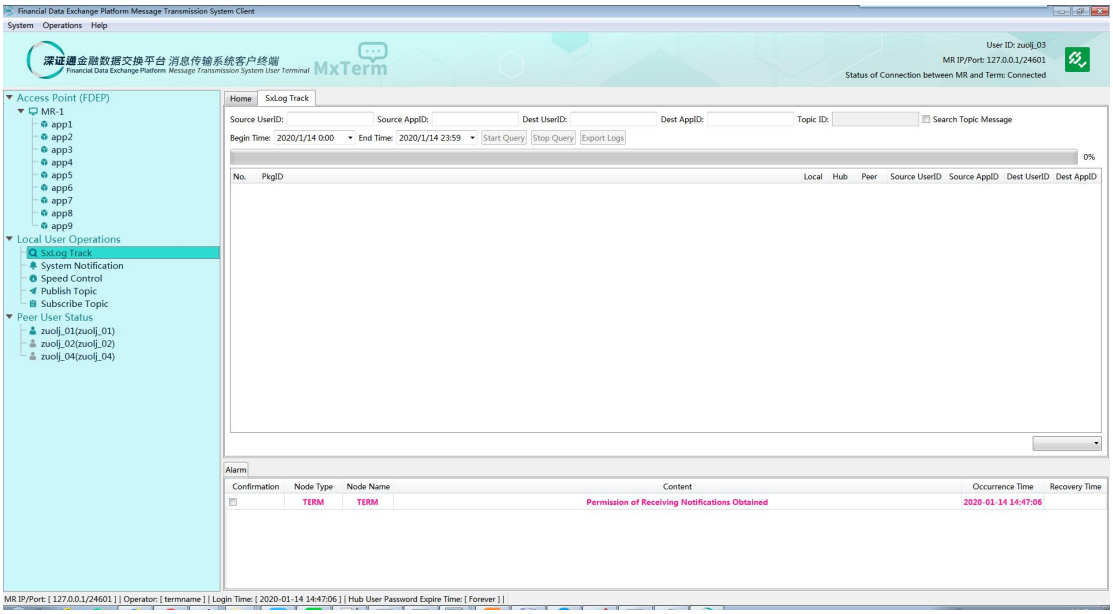


Fig. 5 Log search interface

Enter the search keywords, log dates, and click to start the query. The search results of the corresponding exchange logs can be displayed.

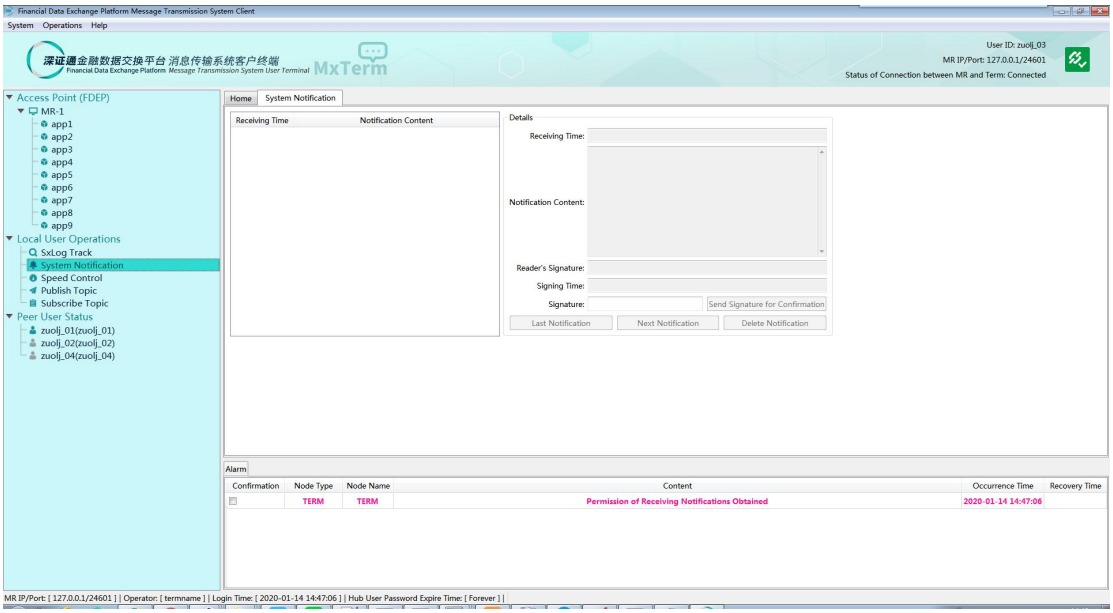


Fig. 6 System notification interface

MxTerm allows for receiving system notifications sent by Shenzhen Securities Communication Co., Ltd and in addition, multiple MxTerms can be set as sending and receiving notification terminals. You can set them on the login interface or [Request Notification Permission] under the [Operation] menu.

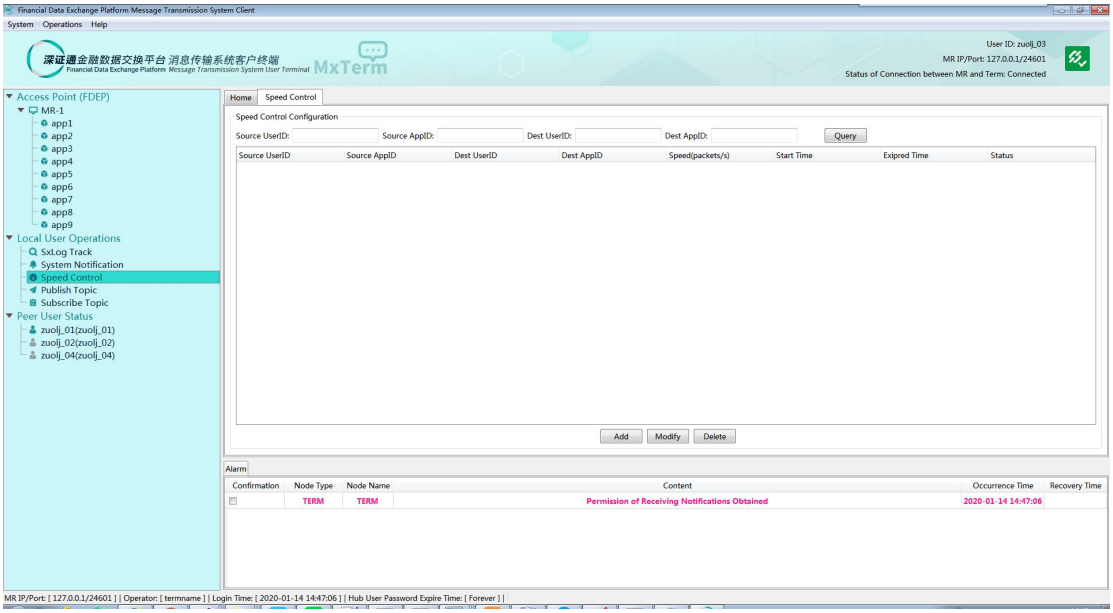


Fig. 7 Speed control interface

For MxTerm, clicking the left menu bar Speed Control, you can add, modify and delete the corresponding speed control rule instructions, query the speed control instructions added locally and the speed control instructions of the opposite end.

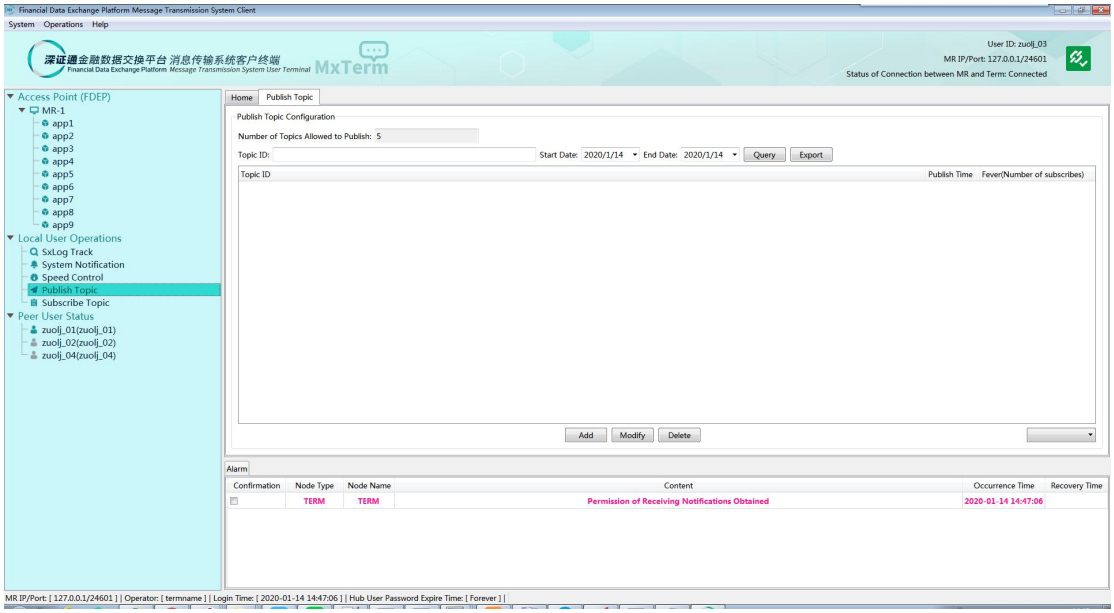


Fig. 8 Publishing topic interface

For MxTerm, clicking on the left menu bar to publish topics, you can query, add, modify, and delete topics.

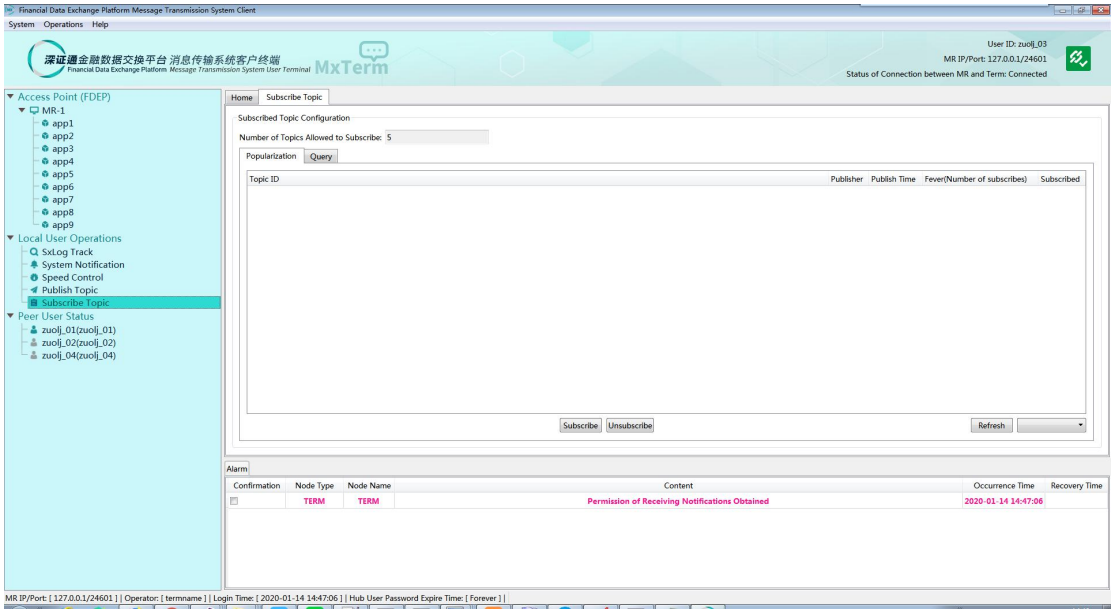


Fig. 9 Topic subscription

For MxTerm, clicking the left menu bar to subscribe to topics, you can subscribe, unsubscribe, and query topics.

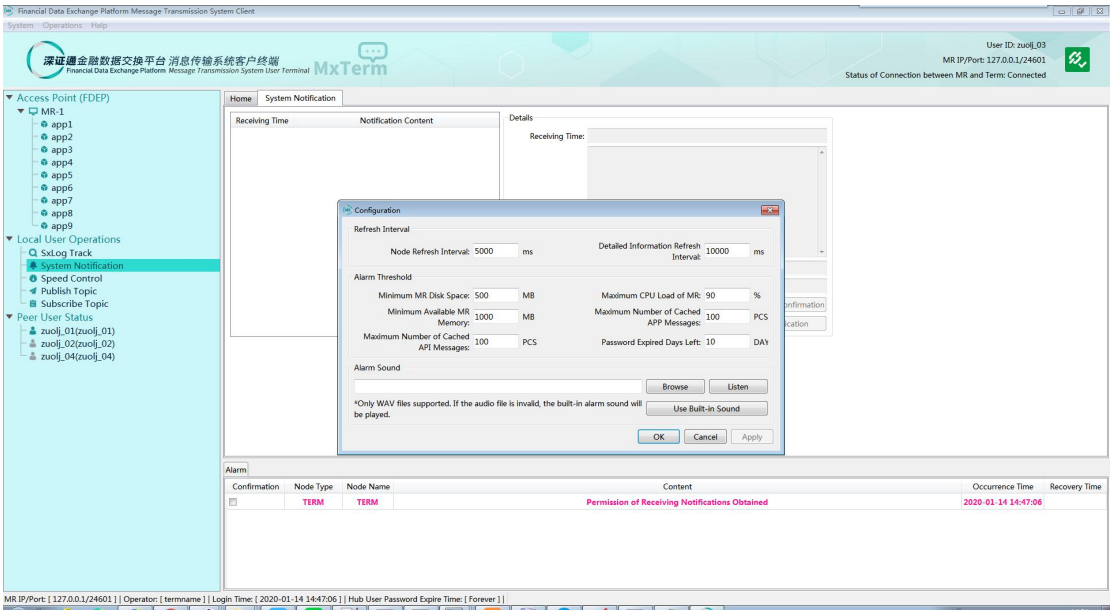


Fig. 10 Monitor terminal configuration interface

For MxTerm, click [Configure] under the [Operation] menu to configure MxTerm.

6 Backup solution

The access client is provided by SSCC and runs as a front-end of the message transfer system on the client-side. Each user can deploy one or more bsmr software, which is called access client. It is recommended that users deploy two bsmr software because the multiple bsmr software has the capability of hot standby with each other .

The deployment of the access client is shown in figure 11 below, which is a schematic diagram of the deployment by two bsmr software,named MR-1 and MR-2.

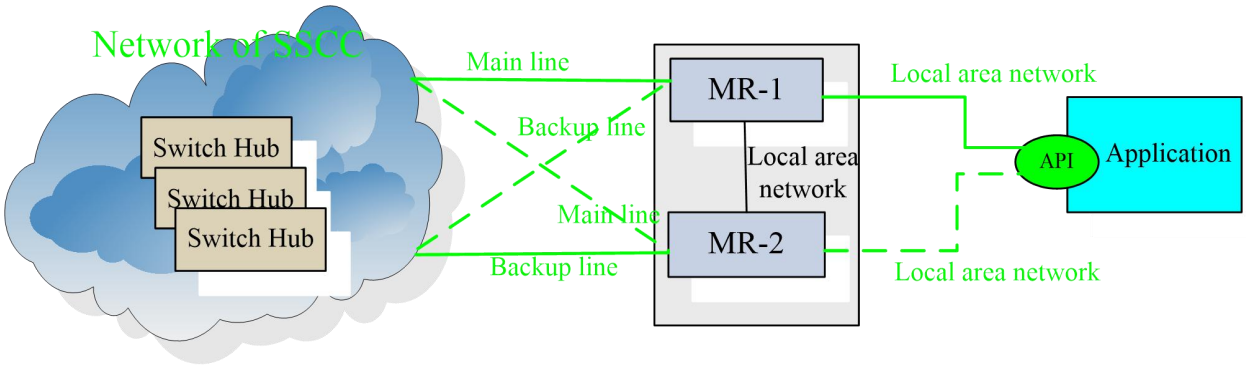


Fig. 11 Deployment mode of access client

Application Backup: Deploy two bsmr software, when any bsmr software fails or the machine hardware goes down, the other bsmr software can automatically replace the failed bsmr and work normally, and the user's software does not need any operation.

Network Backup: It can be seen from Figure 11 that the network link between MR-1 and MR-2 located at the user end and the switching center is recommended to be one active and one standby. In this way, in case of a line failure, bsmr software can be connected from any of the main and standby lines, and it works normally, and the software of the user does not need any operation.

For backup preparation, if hardware encryption is used, two Ekeys need to be prepared and inserted into different machines of application deployment; if software encryption is used, make sure the Ekey field in mr.ini is different.

When application backup, the configuration segments in the configuration files of the two bsmr software need to be modified as follows:

No.	Configuration segment name	Field name	Configuration content
1	[CurrMR]	"MRName"	The name of this bsmr software, generally uses the naming method of MR-1 and MR-2. The value of this field in the configuration file of the two bsmr software cannot be the same.
2	[CurrMR]	"Ekey"	If it is hard encryption, in the configuration files of the two bsmr, the value of this field is filled in "/C=CN/CN=****", fill the number of Ekey inserted on the current machine(there is a label on Ekey) to the '***'; if soft encryption is used, fill in two file certificate names respectively into this field.
3	[CurrMR]	"EkeyPwd"	Corresponding Ekey login password or file certificate password[plaintext].
4	[CurrMR]	"EkeyPwdCrypt"	Corresponding Ekey login password or file certificate password[ciphertext].

7 Replacement operation of Ekey

7.1 Prepare conidtions

Prepare conditions for replacing Ekey:

(1) The new hardware Ekey has been applied, and the new Ekey is ready;

(2) When the stock market close, close the existing bsmr program and unplug the old Ekey;

(3) Follow the steps to replace the Ekey;

7.2 Operation steps

No.	Operation name	Operation instructions
1	Make sure the new Ekey driver is installed	Make sure the Ekey driver is installed. If not, install the driver in the CD that came with Ekey. (Do not perform this step if the machine has previously installed this type of Ekey driver)
2	Insert the Ekey	Insert Ekey insto the USB interface of the specified machine. At this time, you can see the working status of Ekey Certificate in token manager of Ekey, indicating that the new Ekey can work normally and the driver has been installed successfully.
3	Modify the mr.ini configuration file	Locate the SSCC FDAP program folder, open the mr.ini configuration file, and modify the third line "Ekey"="/C=CN/CN=****", fill the number of Ekey inserted on the current machine(there is a label on Ekey) to the '***'.
4	Apply to open the Ekey	Call the SSCC operation hotline:0755-83182222, apply for the activation certificate Ekey, and inform the subject names of new and old Ekey. SSCC will cooperate to change the relevant configuration so that user can connect.
5	Restart the mr program	Start the shortcut of mr program, and use mxterm to monitor the connection status of mr program.

7.3 Common faults

If the Ekey is not replaced successfully, please follow the steps below to rollback

1. **Fault 1:** After the Ekey driver is installed successfully, insert the Ekey into the USB interface of the specified machine. At this time, there is no working number in Ekey's token manger.

   Solution: This phenomenon indicates that the new Ekey cannot be recognized. Please try to insert the Ekey into the new USB interface or check if the Ekey is not properly touched. If the fault still exists, it means there may be a problem with Ekey. Please mail the new Ekey to our company for replacement.

2. **Fault 2:** After replacing the new Ekey, start the bsmr program. The bsmr.log indicates that communication connection to SU succeeds for a while, then disconnects immediately.

   Solution: This phenomenon shows that SSCC has not configured the Ekey for the user, that is, the central software considers the Ekey illegal. In this case, you can call the SSCC operation hotline to apply for the certificate.

7.4 Rollback steps

If the Ekey is not replaced successfully, please follow the steps below to rollback:

No.	Rollback operation name	Rollback operation instructions
1	Make sure the old Ekey driver is installed	If the machine has previously installed the driver of the old Ekey that needs to be rollback, do not perform this step. If not, install the driver in the CD that came with Ekey.
2	Insert the old Ekey	Insert the old Ekey into the USB interface of the specified machine. At this time, you can see the working status of old Ekey Certificate in token manager of Ekey, indicating that the old Ekey can work normally and the driver has been installed successfully.
3	Modify the mr.ini configuration file	Locate the SSCC FDAP program folder, open the mr.ini configuration file, and modify the third line "Ekey"="/C=CN/CN=****", fill the number of old Ekey inserted on the current machine(there is a label on Ekey) to the '***'.
4	Apply to open the old Ekey	Call the SSCC operation hotline:0755-83182222, apply for change back to the old Ekey, and inform the

		subject names of new and old Ekey. SSCC will cooperate to change the relevant configuration so that user can connect.
5	Restart the mr program	Start the shortcut of mr program, and use mxterm to monitor the connection status of mr program.

8 Daily Maintenance

8.1 Daily maintenance

FDAP program generally do not require manual maintenance during operation, but every once in a while, you should check to see if the disk space occupied by the program is full, because the program will generate exchange logs and running logs during the running process. When these logs take up too much space, they should be cleared or moved to other disks in time. It is recommended that the FDAP program be restarted every day before the market opens. Even if it is not restarted, please check whether the FDAP program is running normally.

8.2 Instructions about log

During the use of the FDAP program, an operation log can be generated and recorded in a log file. The log directory is the <installdir>\log directory. The log file is in the date and time format. The file names are bsmr_20190401_000000.log, bsmr_20190401_080800.log, bsmr_20190401_090900.log, ..., bsmr_20190401_235959.log. Among them, bsmr_20190401_235959.log is the latest log file, and bsmr_20190401_00000.log is the oldest log file, that is, it is incremented according to time. Each log file is approximately 50MB in maximum, and older log files are automatically deleted based on the maximum number of days to be saved.

The log configuration file \ini\ mr.ini can control the generation and output of the FDAP server log. The file format is as follows:

```
[LOG]
"LockType"="1"
"Level"="0"
"Display"="3"
"LogDir"=""
"LogName"="../log/bsmr.log"
```

```
"MaxFileSize"="50000000"
"MaxSaveDays"="10"                    // Maximum save days of log
```

Level indicates the log level. The value ranges from 0 to 10. The default value is 0. The level 0 log has the least information and only reports errors and important operating information. This is also the level set during formal operation. The level 10 log information has the most information, including all errors, warnings, and messages, is generally only used when debugging a program. Other commonly used levels are 1 and 5, which are moderately informative.

Display indicates the log output mode. The value ranges from 0 to 3, and the default value is 1. 0 means no log is displayed or recorded; 1 means log is only recorded in file; 2 means log is only displayed on screen (only valid for console program); 3 means log is recorded in file and displayed on screen

If the configuration file does not exist, or a parameter is not configured in it, the corresponding parameter adopts the default value.

This configuration file can be dynamically modified during the use of the FDAP program, and it takes effect within 30 seconds after modification.

9 Guidance for Trouble Removal

Problem 1: The server program fails to start.

Solution: You can find the cause of the failure by looking at the log files in the \log directory under the installation directory. In most cases, the startup failure is caused by the absence of EKey, and sometimes may be caused by failure to listen on the configured port.

Problem 2: The monitor terminal cannot connect to the client program, or the connection fails.

Solution: Check whether the IP and port of the connected access client are correct.

Question 3: It is found on the monitor terminal that the connection with the switching hub is abnormal

Solution: Check whether the configuration file of the access client is correct. If the configuration is modified, restart the access client program.

10 Recommendation

1. Restart the FDAP program before the market opens every day. Even if it is not restarted, please check whether the FDAP program is running normally.

11 Precautions

1. The *.db file cannot be manually deleted during the BSMR operation, and the temporary *.db must be cleaned up and restarted after the accidental deletion.

2. Manually delete the transaction log, restart BSMR.

3. Modify the system time, clear the transaction log and restart BSMR.

4. When deploying multi-active BSMR across machines, IP address of Mr configured by mr.ini should be the actual ip address instead of the loopback address.

Shenzhen Securities Communication Co., Ltd.

April 2020