深证通信工程技术文档

SSCC-FDEP消息传输系统FDAP用户手册

文档编号： **FDEP-FDAP-PUM001**

文档密级： **外部公开**

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

2020年4月

文档信息

文档名称	FDAP 用户手册
说明	
所属项目	金融数据交换平台

修订历史			
日期	版本	修改人员	修改说明
20120725	0.9	研发中心	创建并完成初稿。
20120823	0.91	研发中心	添加 CSV 监控信息
20140328	1.0	研发中心	1. [LOG]中增加 LogDir 的默认配置，并作补充说明。 2. 对 bsmr 启动参数-i 补充说明。 3. 增加 4.5 节接入客户端性能。
20151123	1.1	研发中心	第 4.1 节配置[CurrMR]增加"EkeyExtId"枚举 Ekey 哪个字段，增加"IsSoftCert"是否使用软证书，增加"CAFileName"和"SoftCertFileName"分别表示根证书和用户证书。
20160317	1.2	研发中心	第 4.1 节增加配置[BIZTYPE],每个 app 对应的业务。
20190403	1.3	研发中心	V5 版本新增功能以及注意事项

目 录

图 索 引

表 索 引

1 引言

本文档是金融数据交换平台消息传输系统接入客户端的用户手册，主要介绍金融数据交换平台接入客户端的用户配置、运行和维护等方面的操作以及监控终端功能。

FDAP 是金融数据交换平台消息传输系统的接入客户端(FDEP Access Point)的缩写。

1.1 定义

FDSH：FDEP Switching Hub，金融数据交换平台的交换中枢。

FDSU：FDEP Switching Unit，金融数据交换平台交换单元，FDSH 的构成元素。

FDEAPI：Financial Data Exchange Application Programming Interface，金融数据交换平台客户端应用开发接口。

BSMR：接入客户端的运行程序名称。

MXTerm：监控终端运行程序名称。

2 软件概述

2.1 软件的结构

接入客户端在金融数据交换平台软件架构中的位置如下图所示。金融数据交换平台客户端包括三部分：接入客户端，监控终端以及 API。

金融数据交换平台消息传输系统接入客户端是用以连接金融数据交换平台交换中枢和用户应用的桥梁；监控终端用于监视金融数据交换平台接入客户端的运行状态。

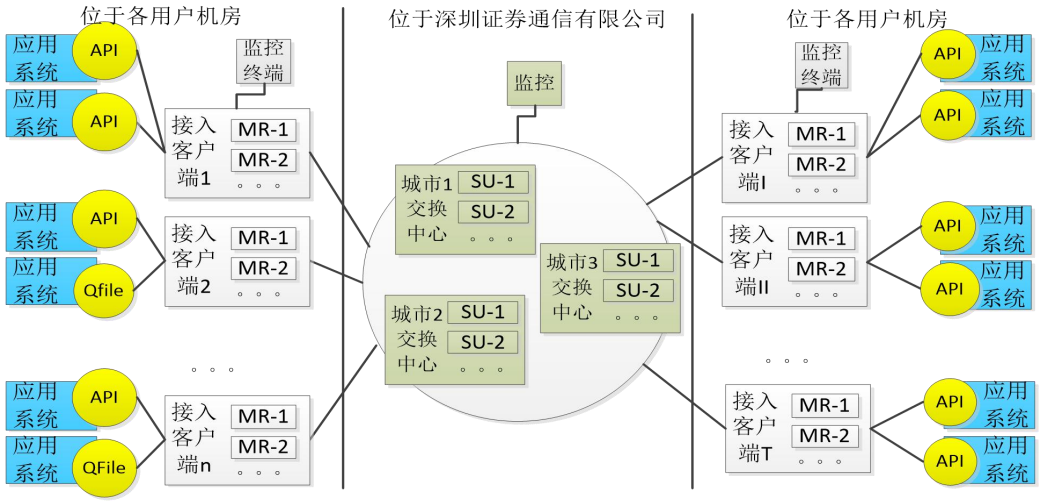


图 1　　金融数据交换平台软件架构

2.2　程序目录结构表

软件为绿色软件，包含文件有。

表 1　　FDAP 程序包

序号	文件名称	说明
1	**bsmr 目录**	**该目录下放置的是金融数据交换平台接入客户端程序**
2	bsmr.exe	金融数据交换平台接入客户端的运行程序
3	cert\sscc.cer	CA 的证书，不能修改
4	ini\mr.ini	配置文件，需要修改
5	ini\spdctrl.db	速度控制指令存储文件，运行期间不可手动删除
6	log\ bsmr_mon_***.csv	用户监空的 CSV 格式文件
7	log\sxdata20190401_*.log	交易日志文件
8	log\bsmr_20190401*.log	运行日志文件

序号	文件名称	说明
1	**mxterm 目录**	**该目录下放置的是金融数据交换平台监控终端**

		程序
2	Mxterm.exe	金融数据交换平台监控终端的运行程序
3	cfg\mxterm.ini	配置文件，按需要修改
4	lang 目录	存放语言包，不可手动删除修改
5	plugin 目录	存放监控终端运行所需插件，不可手动删除
6	qt.conf	QT 插件相关配置文件，不可手动删除
7	*.dll	监控终端运行所需动态库，不可手动删除
8	log\mxterm_20200401_*.log	监控终端运行日志文件

2.3 对硬件的需求

	配置	备注
机型	PC Server	PC Server 适合长时间开机，以及安装到机房机架上。
CPU	主频 3.0G 以上	
内存	4G 以上	
硬盘	150G 以上并进行磁盘镜像	程序本身大小仅 10M 以下，但所产生的日志由于持续增加，会不断消耗磁盘空间。
网卡	双网卡	
USB 接口	至少两个 USB2.0 接口	位于机身后部
电源	建议采用双电源模块	

注：以上配置可根据用户实际情况适当调整。

2.4 对软件的需求

程序	操作系统名称	版本
接入客户端	Microsoft Windows Server 2008 、 Microsoft Windows	

	Server 2012 、 Microsoft Windows 10 、 Microsoft Windows Server 2016、Redhat Enterprise Linux6.8 、 Redhat Enterprise Linux7.5	
监控终端	Windows 7 及以后的 Windows 操作系统、Linux(需带界面操作)	

3 安装与卸载

3.1 安装程序

金融数据交换平台消息传输系统接入客户端为绿色软件，直接拷贝文件到操作系统运行目录即可。

3.2 卸载过程

直接删除目录即可。

4 接入客户端运行说明

4.1 接入客户端运行必须的前提条件

BSMR 软件的运行需要两个前提条件：

(1) 用户必须有深圳证券通信公司颁发的 Ekey 电子证书或者软加密进行登录；

(2) 用户必须正确配置安装后的目录下 ini\mr.ini 文件。如果用户需要运行多个 BSMR，则除[CurrMR]节以外，其他节的配置在多个 MR 上必须一致。

[可以通过深证通提供的配置程序进行配置]

```
[CurrMR]  //本地 mr 配置
"MRName"="MR-1"                    //当前 MR 的名称，必须与以下使用 MR-开头的其中之一匹配
"StartCmd"="-f +wt"                //启动命令，以空格分开，启动参数[-i 安装服务][-u 卸载服务][-h 帮助][+w 打印简易日志][+wt 打印全部日志][-servicename=服务的名称]
"UserID"="SSCC_TEST01"             //用户 ID
"UserPasswd"="123456@abc"          //用户密码[明文]
"UserPasswdCrypt"="2c5189a328e7d87d491e533764170c2a"    //用户密码[密文]，用户可以选择明文或者密文的一种
"Ekey"="/C=CN/CN=SSCC_TEST01"      //电子证书 EKey 的主题名
"EkeyPwd"="111111"                 //电子证书 EKey 的登录密码[明文]
"EkeyPwdCrypt"="948514863abee7c1c9cfe36eb1a826ca"  //电子证书 EKey 的登录密码[密文]，用户可以选择明文或者密文的一种
"EkeyExtId"="1.2.86.100.4.3.2" //读取 Ekey 的字段
//"IsSoftCert"="1"                 //是否使用软证书文件
//"SoftCertFileName"=""            //软证书文件名
"PkgMaxAliveSec"="40"              //消息包在 mr 的保留时间，以秒为单位
"AllowMultiApp"="1"                //是否允许同台机器运行多个 mr 进程
"OnceRecvMsgCount"="1"             //app 以取包方式从 mr 取包，一次最多返回给 app 消息包的个数
"TermName"="termname"              //mrterm 登录的名称
"TermPwd"="termpas"                //mrterm 登录的密码[明文]
"TermPwdCrypt"="9e3f227b69360934ad4ad9ff35e286e8"          //mrterm 登录的密码[密文]，用户可以选择明文或者密文的一种
"AutoBalance"="1"                  //是否自动均衡 app
"BalanceOfFileInstanceId"="0"  //0：默认匹配首个，1:轮询均衡方式，2:原 userid+appid 整数值取模
"TopicPushMode"="0"       //0：默认推送给第一个 applinkid，1：推送所有 applinkid

[SUIPMap] //地址映射，转换前的地址=转换后的地址,如果无 NAT 转换或多线路接入，只需配置左边=右边
"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]//当前 APP 的用户名和密码[明文]
"app1"="1"
"app2"="1"
"app3"="1"
"app4"="1"
"app5"="1"
"app6"="1"
"app7"="1"

[APPINFOCRYPT]//当前 APP 的用户名和密码[密文]
"app1"="bb683b359da5788ad377fa755b6b998d"
"app2"="bb683b359da5788ad377fa755b6b998d"
"app3"="bb683b359da5788ad377fa755b6b998d"
"app7"="bb683b359da5788ad377fa755b6b998d"

[BIZTYPE] //APP 对应的业务类型：0 代表三方存管业务 ，11 代表直销业务，12 代表资金划付业务，13 代表信证报盘业务（证券交易），14 代表电子对账业务，15 代表融资融券业务，16 代表基金盘后业务，17 代表转融通业务，18 代表 B 转 H 业务，19 代表交叉销售业务（金融产品销售），20 代表证券回购业务（报价回购），21 代表个股期权业务（银衍转账），23 代表私募报转业务。新增业务类型大小判断（<128），大于 128 为文件消息，由 api 发文件时填充业务字段。
"app1"="0"
"app2"="11"
"app3"="12"
"app4"="0"
"app5"="0"
"app7"="0"


[MR-1]//交换单元 1 的配置
"Enable"="1"                    //是否使用
"InnerIP"="127.0.0.1"           //交换单元 1 的对内 IP
"ClientIP"="127.0.0.1"          //交换单元 1 对 Client 的 IP
"InnerPort"="3600"              //交换单元之间的通信端口
"TermPort"="3601"               //交换单元与管理终端的通信端口
"ClientPort"="3602"             //交换单元与客户端 API 的通信端口
//"ExpectApp"="app1"
```

```
//"UserMonitorVer"="05.00.20190630" //[版本信息] 与 UserMonitor 同步
//"UserMonitor"="1|app3|5|10,1|app3|5|10"  //其中‘,’为大条目分隔符，‘|’为条目内部分隔符。
//如‘1|app1|2|10’，第一个数字：方式，1 重定向，2csv，3 两者皆有；第二个字串：app 名称；第三个数字：间隔时间；第四个数字：关闭时间。


[MR-2]//交换单元 1 的配置
"Enable"="0"                        //是否使用
"InnerIP"="127.0.0.1"               //交换单元 1 的对内 IP
"ClientIP"="127.0.0.1"              //交换单元 1 对 Client 的 IP
"InnerPort"="4600"                  //交换单元之间的通信端口
"TermPort"="4601"                   //交换单元与管理终端的通信端口
"ClientPort"="4602"                 //交换单元与客户端 API 的通信端口
//"ExpectApp"="app2"
//"UserMonitorVer"="05.00.20190630" //[版本信息] 与 UserMonitor 同步
//"UserMonitor"="1|app3|5|10,1|app3|5|10"  // 其中‘,’为大条目分隔符，‘|’为条目内部分隔符。
//如‘1|app1|2|10’，第一个数字：方式，1 重定向，2csv，3 两者皆有；第二个字串：app 名称；第三个数字：间隔时间；第四个数字：关闭时间。



[LOG]//日志配置
"Level"="0"          //日志级别
"Display"="3"        //打印类型，0 表示不显示也不记录日志；1 表示只在文件中记录日志；2 表示只在屏幕上显示日志（只对控制台程序时有效）；3 表示在文件中记录同时在屏幕上显示日志
"LogDir"="../log"            //日志目录，若以服务方式启动，须配置为绝对路径
"LogName"="../log/bsmr.log" //日志名称
"MaxFileCount"="20"          //最大文件个数
"MaxFileSize"="500000000"    //单个文件最大大小
"MaxSaveDays"="-1"           //日志最长保存天数，-1 表示不启用
```

配置方法说明：

1）以真实的 Ekey 主题名替换"Ekey"="/C=CN/CN=SSCC_TEST01"中的 SSCC_TEST01。

2）[SUIPMap]一节配置地址映射信息，等号左边为交换中枢的真实地址，右边配置经映射后的地址。

3）[APPINFO][APPINFOCRYPT]一节用户可以按照格式自行扩充，增加新的 app。

4）[MR-1]和[MR-2]两节的配置方法类似，其中"Enable"为 1 表示该节配置有效，为 0 表示无效。"InnerIP"和"InnerPort"用于多个 mr 内部通信，在[MR-1]和[MR-2]中不能完全相同；"ClientIP"和"ClientPort"用于对用户程序提供服务，在[MR-1]和[MR-2]中不能完全相同。"TermPort"用于管理中断连接 FDAP 使用。如跨机部署多活 MR 时，IP 地址需配置为实际 IP 递增，不可配置为回环地址。

5）监控方式有 1：重定向，2：CSV 格式，3 两者兼有

6）密码生成方式可以使用 BsmrIniSet 程序或者 mrterm 生成。

4.2 接入客户端运行表

接入客户端程序名称为 bsmr.exe，运行参数如下：

表 2　　BSMR 程序运行表

序号	运行命令	含义
1	bsmr –h	显示运行帮助，将打印可能的运行参数
2	bsmr -i	安装成为服务程序。用户在安装程序时，已经自动替用户安装成了服务程序，所以一般情况下用户不需要使用该选项。若用服务方式启动时配置了-i，在第二次启动前请去掉-i。[Linux 不支持]
3	bsmr -u	卸载服务程序。用户在卸载程序时，已经自动替用户卸载了该服务，所以一般情况下用户不需要使用该选项。[Linux 不支持]
4	bsmr –f	控制台启动，bsmr 默认只能由服务方式启动，如果需要控制台启动，需要添加此参数
5	bsmr +w	写任何交换日志，只记录包头信息.
6	bsmr +wt	写任何交换日志，不仅记录包头信息，也记录包体信息。
7	bsmr	这是错误的运行方式，程序不能在命令行方式下不带参数运行。在这种情况下，程序将首先检测服务，然后将显示用户参数错误，并提示用户是否继续以命令行应用的方式运行。
7	在 Window 服务管理器中启动	这是正常的启动方式。[Linux 不支持]

4.3 接入客户端运行步骤

4.3.1．对 ini\mr.ini 文件进行正确的配置。具体参见 4.1 一节；

4.3.2. 如果是硬加密，在运行该软件的电脑安装该 EKey 的驱动程序，然后在 USB 接口中插入深圳证券通信公司颁发的 Ekey。(在安装驱动时不要插入 Ekey)

4.3.3.1 Window 版本启动程序：手工以服务的方式正常启动金融数据交换平台接入客户端服务。

【注意：启动用户必须为管理员权限用户】手工启动的步骤如下：

(1) 打开“我的电脑----控制面板----管理工具”，然后打开服务；

(2) 找到“SSCC_BSMR”并选中，双击出现属性对话框，在启动参数填写相关的运行参数，然后点击工具条上的“启动”按钮，将启动该软件。默认情况下，该服务是“自动”启动类型，当计算机重新启动时，该软件将随操作系统自动启动，用户可以对此进行修改。

(3) 当软件需要停止运行时，用户也可以在服务管理器中对该服务进行停止。

4.3.3.2 Linux 版本启动程序：

【注意：启动用户必须为 root 用户】直接启动，或者 nohup 后台启动也可以。

4.4 接入客户端停止步骤

4.4.1 Window 版本:

可以通过手工以服务的方式停止金融数据交换平台接入客户端服务。手工停止服务的步骤如下：

(1) 打开“我的电脑----控制面板----管理工具”，然后打开服务；

(2) 找到“SSCC_BSMR”并选中，然后点击工具条上的“停止服务”按钮，将停止该软件。

4.4.2 Linux 版本

Kill 1 [进程 id]

4.5 接入客户端性能

在操作系统 Windows Server 2003 测试（报文大小 1KByte)：

（1）API 有 3 种处理模式，一种是到 BSMR 轮询模式，每秒不低于 500 个，第二种配置 OnceRecvMsgCount 参数，性能为 5000 个/秒，第三种注册下推模式，性能 7000 个/秒；

（2）每个 APP 的处理是单独的线程，不同 APP 可平行扩展。

（2）接入客户端收发数据包性能为 10000 个/秒，数据包大小为 1KB。

4.6 接入客户端运行界面及操作说明

Window 版本以 Windows 服务的方式运行，没有操作界面。

Linux 版本没有操作界面

4.7 接入客户端 Q 文件接口格式

Q 文件用于发送和接收消息，文件为 dbf 格式。

BSMR 收到消息写入接收 dbf 文件，APP 通过文件读取消息。

APP 将消息写入发送 dbf 文件，BSMR 读取文件发送出去。

APP 发送消息的文件名称为 fdep_【日期】_【APP 名称】_send.dbf，例如 fdep_20120725_app20_send.dbf.

APP 接收消息的文件名称为 fdep_【日期】_【APP 名称】_recv.dbf，例如 fdep_20120725_app20_recv.dbf.

其中数据段个数为可配置，详见 MRini

表 3　　Q 文件协议格式

序号	字段名	字段描述	类型	长度	备注
1	ID	记录 ID	N	10	
2	SrcUserID	源用户 ID	C	32	
3	SrcAppID	源 APPID	C	32	

4	DestUsrID	目的用户 ID	C	32	
5	DestAppID	目的 APPID	C	32	
6	PkgID	包 ID	C	64	
7	CorrPkgID	相关包 ID	C	64	
8	UserData1	用户数据 1	C	255	
9	UserData2	用户数据 2	C	255	
10	Flag	标志位	N	3	
11	BizType	业务类型	N	3	
12	Priority	优先级	N	3	
13	SLevel	敏感级	N	3	
14	MsgType	消息类型	C	8	
15	ErrorCode	错误值	N	10	
16	DataLen	消息长度	N	10	
17	Data0	消息内容 0	C	255	
18	Data1	消息内容 0	C	255	
…	…	消息内容			
17+N	DataN	消息内容 N	C	255	
18+N	WTime	写入时间	N	10	hhmmss.ccc [两位小时][两位分钟][两位秒].[三位毫秒]
18+N+1	ReadyFlag	数据准备好标记	C	1	r 为准备好
18+N+2	FdepMark	Fdep 使用扩展字段	C	20	
18+N+3	UserMark	用户使用扩展字段	C	20	


QFileDemo.cpp


dbffile.h


dbffile.cpp

示例：

4.8 接入客户端用户监控

BSMR 提供两种形式用户监控：1 表示重定向方式；2 表示 CSV 文件输出方式。

在配置项

[MR-]

"UserMonitor"="1|E:\UserMonitor.exe|3|5" //用户监控信息接口[监控方式|进程路径|调用间隔秒|过期时间秒]

1 重定向方式：

配置例子：”UserMonitorVer”="05.00.20190630"

配置意思为：05.00.20190630 以后版本采用新的输出格式，较前版本兼容旧格式

配置例子："UserMonitor"="1|E:\UserMonitor.exe|3|5"

配置意思为：使用重定向方式，进程路径为 E:\UserMonitor.exe，每隔 3 秒调用一次，超过 5 的时候自动关闭重定向。

BSMR 根据配置定时调用用户的进程,通过重定向机制发送 FDAP 运行信息给用户进程，用户据此可以定制自己的监控程序。

提供的信息以及调用方式详见示例程序


UserMonitor.cpp

示例:

2CSV 文件方式：

配置例子：”UserMonitorVer”="05.00.20190630"

配置意思为：05.00.20190630 以后版本采用新的输出格式，较前版本兼容旧格式

配置例子：″UserMonitor″=″2||3|″

配置意思为：使用 CSV 文件方式，每隔 3 秒写入文件一次，

CSV文件为log/bsmr_monYYYMMDD.csv

BSMR 根据配置定时将 FDAP 运行信息写入 CSV 格式文件，用户据此可以定制自己的监控程序

表 4　　CSV 协议格式

列信息	具体含义
时间	2-08-25 09:57:23
MR信息	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=

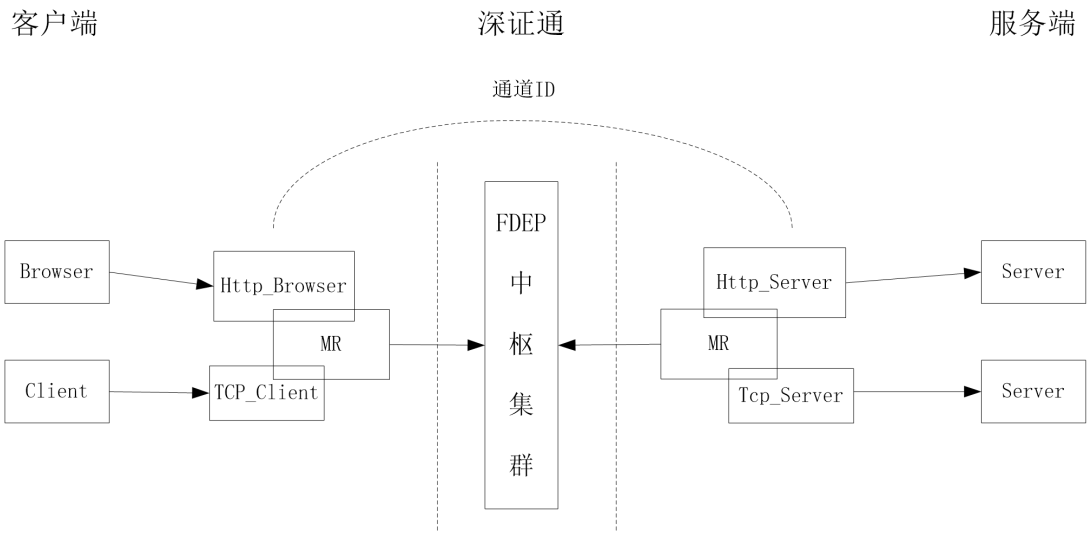
	Mr 的个数|mr 的名称|用户名称|是否已经连接上 SU|机器的 cpu|机器单个最高使用 CPU|总的内存|可用内存|发送包平均速度|接收包平均速度|总共硬盘空间|可用该内存空间|MR 的版本|和 SU 链接 SU 链接的发送网速|普通消息接收包总数|普通消息接收包失败数|普通消息发送总数|普通消息发送失败数|主题消息接收总数|主题消息接收失败数|主题消息发送总数|主题消息发送失败数|文件消息接收总数|文件消息接收成功数|文件消息接收失败数|文件消息发送总数|文件消息发送成功数|文件消息发送失败数|文件消息接收总大小|文件消息接收成功大小|文件消息接收失败大小|文件消息发送总数|文件消息发送成功数|文件消息发送失败数
缓存包信息	MsgQueueCount=2|MrName=MR-1|AppName=app1|Size=0| MrName=MR-1|AppName=app2Size=2 消息包缓存队列个数|缓存队列的 mr 名称|缓存队列的 APP 名称|缓存包个数
APP 信息	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=|TopicRecvCount=|FileSendCount=|FileSendSize=|FileRecvCount=|FileRecvSize= App 个数|mr 名称|app 名称|链接 ID|发送个数|接收个数|连接上 mr 时间|app 的 ip 地址|app 版本|主题消息发送个数|主题消息接收个数|文件消息发送个数|文件消息发送大小|文件消息接收个数|文件消息接收大小
在线用户信息	OnlineUserCount=2|UserID=FTCSTEST1:FTCSTEST100 在线用户个数|用户 id=用户 ID1：用户 ID2
SU 探测信	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 探测结果个数|探测的时间|mr 名称|SU 的 ip 地址|SU 的端口|本地 mr 的 ip 地址|探

息	测的结果 （0 代表成功，1 代表失败）

4.9 接入客户端代理功能

代理功能是对原 FDEP 消息平台进行功能扩展，使客户在向深证通专线环境迁移时，可以直接使用原来的协议（HTTP 或 TCP）接入 FDEP 平台，无需针对 FDEP 协议进行二次开发，实现无缝迁移。

4.9.1 接入客户端代理流程



启动代理功能的准备条件：

1）用户 A 和用户 B 都有向深证通申请成功的各自的用户号 UserID，并且两者申请配有通信关系，并相互约定通信 AppID。

2）用户 A 和用户 B 均参照 4.1，4.2，4.3 节正常配置 ini\mr.ini，并能正常运行接入客户端。（能正常启动后，退出该客户端，这一步只是验证普通 BSMR 是否能正常启动）

3）用户 A 和用户 B 均正确配置代理配置文件 ini\Proxy.ini，并均正常启动代理客户端，代理客户端与深证通中枢连接正常。（正常启动后，BSMR 便可作为代理客户端使用）

HTTP 代理：用户 A 通过浏览器设置代理，代理填入的地址为自己接入客户端 BSMR 的 ini\Proxy.ini 文件中 Http_Browser 模块的监听 IP 地址，端口为监听端口。此时浏览器可与接入客户端 Http_Browser 模块建立连接。连接建立成功

后，该模块通过中枢发送请求给对端（B 用户），对端 Http_Server 模块收到请求后，通过解析请求中携带的目的地址信息，与目的 Server 建立连接，整个通道打通后，进行数据传输。

TCP 代理：用户 A 通过客户端程序向自己的接入客户端 BSMR 中的 TCP_Client 模块发起 TCP 连接，连接建立成功后，该模块通过中枢发送请求给对端（B 用户）BSMR 的 TCP_Server 模块，该模块收到请求后，通过 B 用户端 ini\Proxy.ini 文件中配置的目的地址和端口号与 Server 建立 TCP 连接，整个通道打通后，进行数据传输。

4.9.2 代理功能配置

除了接入客户端运行必须的前提条件外（4.1 章节），要启动代理功能，用户必须正确配置安装后的目录下的 ini\Proxy.ini 代理配置文件：

其中代理配置文件 ini\Proxy.ini 中的 AppID 不能和 ini\mr.ini 中[APPINFO]字段的任何 AppID 相同；

如果同一用户运行多个 BSMR，则主备 BSMR 的代理配置文件中的 AppID 也都不能相同；

代理模块配置部分必须包含 Type 类型，表示代理类型。

```
[HttpB1]                    ///代理模块，根据真实 AppID 修改
"Type"="HTTP_Browser"  ///代理类型是 HTTP 浏览器端代理
"ListenIP"="127.0.0.1"  ///代理监听地址
"ListenPort"="7001"  ///代理监听端口
"TimeOutSec"="180"  ///超时等待时间，默认为 180s=3min，通道超过该时间没有数据传输，则断开连接
"PoolThreadCount"="4"    ///线程池数目，默认为 1
"MaxAcceptCount"="1000"  ///服务器最大连接数，默认为 1000
"BizType"="0"   ///业务类型，根据真实业务类型修改
"RecvSpeedCtrlKbps"="10240"   ///浏览器传输限速，默认值 10Mbps

[HttpS1]    ///代理模块，根据真实 AppID 修改
"Type"="HTTP_Server"  ///代理类型是 HTTP 服务器端代理
"TimeOutSec"="180"   ///超时等待时间，默认为 180s=3min，通道超过该时间没有数据传输，则断开连接
"PoolThreadCount"="4"  ///线程池数目
```

```
"MaxConnCount"="1000"   ///最大发起连接数
"BizType"="0"   ///业务类型，根据真实业务类型修改
"RecvSpeedCtrlKbps"="10240" ///服务器端传输限速，不配取默认值 10Mbps 带宽

[TcpC1]   ///代理模块，根据真实 AppID 修改
"Type"="TCP_Client"    ///代理类型是 TCP 客户端代理
"ListenIP"="127.0.0.1"  ///TCP 客户端代理监听地址
"ListenPort"="7003"     ///TCP 客户端代理监听端口
"DestUserID"="userTest"  ///对端用户 UserID
"DestAppID"="#PortMap1"   ///对端用户 AppID
"TimeOutSec"="180"   ///超时等待时间，默认为 180s=3min，通道超过该时间没有数据传输，则断开连接
"PoolThreadCount"="4"    ///线程池数目
"MaxAcceptCount"="1000"   ///服务器最大连接数
"BizType"="0"  ///业务类型，根据真实业务类型修改
"RecvSpeedCtrlKbps"="10240"  ///服务器端传输限速，不配取默认值 10Mbps 带宽

[TcpS1]    ///代理模块，根据真实 AppID 修改
"Type"="TCP_Server"   ///代理类型是 TCP 服务器端代理
"ServerAddr"="127.0.0.1:7001"   ///目的地址和端口
"TimeOutSec"="180"  ///超时等待时间，默认为 180s=3min，通道超过该时间没有数据传输，则断开连接
"PoolThreadCount"="4"     ///线程池数目
"MaxConnCount"="1000"   ///最大发起连接数
"BizType"="0"   ///业务类型，根据真实业务类型修改
"RecvSpeedCtrlKbps"="10240" ///服务器端传输限速，不配取默认值 10Mbps 带宽

[HostMap]    ///浏览器输入的地址对应的对端用户 UserID 和 AppId
"www.sscc.com.cn"="DestUserID:DestAppID"

[DNS]   ///域名解析地址，浏览器输入的域名对应的 Ip 地址
"www.sscc.com.cn"="10.10.10.16   ,   10.10.10.20"

[FilterAddr]   ///过滤的一些网址
"FilterUrl"="oa.sscc.com"
"FilterUrl"="www.firefox.com"
```

配置方法说明：

1）配置几个 AppID 就表示该 BSMR 客户端有几个代理模块；

2）四种类型的代理，可以根据需要只配置其中一种或多种，也可以每

种只配置一个或多个。

3）如果只作为 TCP 代理，则[HostMap]、[DNS]、[FilterAddr]字段内容可缺省，这三个字段只用于 HTTP 代理功能。

4）如果缺少该配置文件则作为普通 BSMR 接入客户端运行，无代理功能；但如果有该配置文件，但配置有误，则整个 BSMR 不能正常启动。

4.9.3 接入客户端 TCP 代理

TCP 代理有两种类型：TCP_Client 和 TCP_Server，相互通信的两个用户，如果一个接入客户端作为 TCP_Client，那么对端必须配置 TCP_Server 代理模块。

两种代理模块的配置，参看 4.9 节。

TCP_Client：

1）需监听客户端的连接，所以必须配置客户端监听端口 ListenPort，而 ListenIP 可以填客户端 IP，也可以缺省，缺省情况下默认端口号全网监听。

2）需配置对端用户的 UserID 和 AppID 才能和对端通信。

TCP_Server:

需配置目的地址 IP 和端口号。

例如，如果 A 用户的 TCP_Client 配置如下

```
[TcpC1]   ///代理模块，根据真实 AppID 修改
"Type"="TCP_Client"     ///代理类型是 TCP 客户端代理
"ListenIP"="127.0.0.1"   ///TCP 客户端代理监听地址
"ListenPort"="7003"      ///TCP 客户端代理监听端口
"DestUserID"="BUserID"   ///对端用户 UserID
"DestAppID"="TcpS1"      ///对端用户 AppID
"TimeOutSec"="180"    ///超时等待时间 180s=3min，通道超过该时间没有数据传输，则断开连接
"PoolThreadCount"="4"     ///线程池数目
"MaxAcceptCount"="1000"    ///服务器最大连接数
"BizType"="0"  ///业务类型，根据真实业务类型修改
"RecvSpeedCtrlKbps"="10240"  ///服务器端传输限速，不配取默认值 10Mbps 带宽
```

连接该代理，客户端需填该模块的 IP 和端口号

那么 B 用户的 TCP_Server 配置如下：

```
[TcpS1] ←///代理模块，根据真实 AppID 修改
"Type"="TCP_Server"   ///代理类型是 TCP 服务器端代理
"ServerAddr"="127.0.0.1:7001"   ///目的地址和端口
"TimeOutSec"="180"  ///超时等待时间 180s=3min，通道超过该时间没有数据传输，则断开连接
"PoolThreadCount"="4"      ///线程池数目
"MaxConnCount"="1000"   ///最大发起连接数
"BizType"="0"   ///业务类型，根据真实业务类型修改
"RecvSpeedCtrlKbps"="10240" ///服务器端传输限速，不配取默认值 10Mbps 带宽
```

该代理模的 ServerAddr 字段需知道服务器的监听 IP 和端口，才能通过读取该字段的配置连接上服务器

4.9.4 接入客户端 HTTP 代理

HTTP 代理有两种类型：HTTP_Browser 和 HTTP_Server，相互通信的两个用户，负责接收和转发浏览器端信息的接入客户端作为 HTTP_Browser，用于发起连接到 Web 服务器请求资源的接入客户端作为 HTTP_Server。使用 HTTP 代理模式来进行网页访问，配置了 HTTP_Browser 模块，必须确保正在访问的网页所对应的 Web 服务器有已经配置了 HTTP_Server 模块的接入客户端连通。

两种代理模块的配置，参加 4.9.2 节。

HTTP_Browser：

1）需监听浏览器的连接，所以必须配置监听端口 ListenPort，而 ListenIP 可以填接入客户端所在机器的 IP，也可以缺省，缺省情况下默认端口号全网监听。

2）必须在[HostMap]节点内容配置域名所对应的对端用户的 UserID 和 APPID。

HTTP_Server:

Web 服务器以域名向外提供服务时，配置 HTTP_Server 模块的接入客户端所运行的机器本地无法获取域名对应的 Web 服务器 IP 地址时，需要手动[DNS]节点内容，把域名和 IP 地址映射起来。

举个例子，A 用户使用 IE 浏览器访问网址 abc.com，abc.com 的 Web 服务器

是B用户管理，那么，A用户想要使用接入客户端的HTTP代理功能访问abc.com，B 用户也要接入 FDAP 系统，A 用户和 B 用户分别拿到他们自己的 UserID 为 UserA 和 UserB，在 A 用户端进行配置 ：

```
[HTTPB1]  //当前 APPID 名称为“#Proxy1”
"Type"="HTTP_Browser"    //当前配置的类型是代理浏览器端
"ListenIP"="10.10.160.14"  //代理监听的地址，默认为本机 IP
"ListenPort"="7004"        //代理浏览器类型必填字段，代理监听端口
"TimeOutSec"="300"         //超时时间，单位秒，默认为 180s
"PoolThreadCount"="4"      //线程池数量，默认为 1
"MaxAcceptCount"="20000"   //最大连接数，默认为 1000
"BizType"="0"              //业务类型，必填字段
"RecvSpeedCtrlKbps"="5120"  //限速，单位 Kbps，选填范围[200-10240]，默认 10M

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

在 B 用户端进行配置：

```
[HTTPS1]  //当前 APPID 名称为“#Proxy2”
"Type"="HTTP_Server"    //当前配置的类型是代理 Web 服务器端
"TimeOutSec"="300"      //超时时间，单位秒，默认为 180s
"PoolThreadCount"="1"   //线程池数量，默认为 1
"MaxConnCount"="1000"   //最大连接数，默认为 1000
"BizType"="0"           //业务类型，必填字段
"RecvSpeedCtrlKbps"="5120"  //限速，单位 Kbps，选填范围[200-10240]，默认 10MKbps
```

```
[DNS]    //选配部分
"abc.com."="10.10.10.16"
```

其他相关配置说明：

HTTP_Browser 端配置必须包含[HostMap]节点内容，存放将要访问的域名所在的 BSMR 代理 UserID 和 AppID 映射，统一格式为：“域名”=“DestUserID：DestAppID”

【注意】一个网站存在重定向时，重定向到不同的域名，需要把新的域名也添加到[HostMap]中。

示例如下：

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

访问 abc.com，Web 服务器返回了重定向 30x，重定向到新的地址 def.com，那么 def.com 所映射的对端 UserID 和 APPID 也要配置到[HostMap]节点中。

HTTP_Browser 端配置可选配置[FilterAddr]，过滤不需要发起访问的网址域名，统一格式为：“FilterUrl”=“url”

示例如下：

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

HTTP_Server 端配置可选配置[DNS]，配置域名映射的真正 IP 地址，没有该节点或者在该节点找不到 DNS 转换时，从本机 Host 文件中寻找。

配置示例如下：

```
[DNS]
```

```
//可配置多个 IP 地址作为域名映射，BSMR 软件随机选取一个进行连接
"www.sscc.com.cn"="10.10.10.16     ,   10.10.10.20"
```

Proxy.ini 填写正确后，根据 4.3 接入客户端运行步骤启动，浏览器配置 HTTP 代理功能，代理的 IP 地址和端口在 Proxy.ini 中代理浏览器端配置节点中查找。

5 监控终端运行说明

5.1 监控终端功能

监控终端主要功能是监视接入客户端程序的运行状况、连接的队列和用户、以及接入客户端与交换中枢的连接状态。

监控终端是作为客户端运行的，可以在任何合适的地点接入进行监控，与其中一个服务端通过 TCP 进行通信。

5.2 监控终端的启动

监控终端提供 Windows 平台界面程序以及 Linux 平台界面程序。

Windows 下的程序启动方法：鼠标双击 MxTerm.exe 文件即可启动。

Linux 下的程序启动方法：执行 MxTerm.sh 脚本即可启动。

5.3 监控终端的停止

监控终端是一个标准的界面程序，程序的停止方法：鼠标点击窗口右上角的关闭按钮，程序就退出。

5.4 监控终端的操作说明

按照 5.2 说明启动软件后运行。软件登录界面如下：

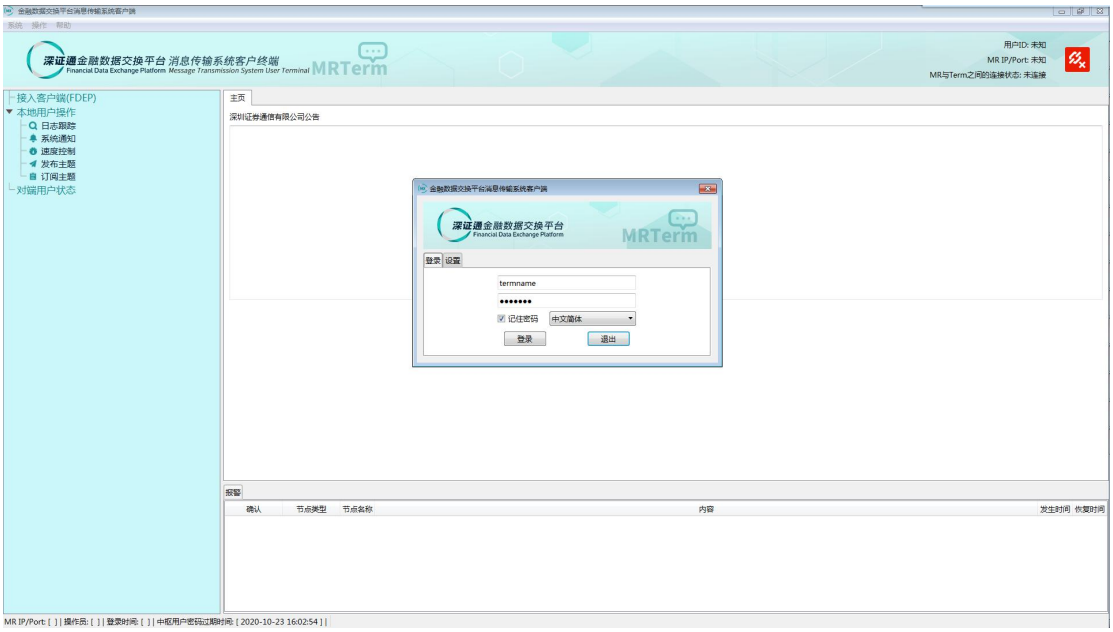


图 2　　监控登录界面

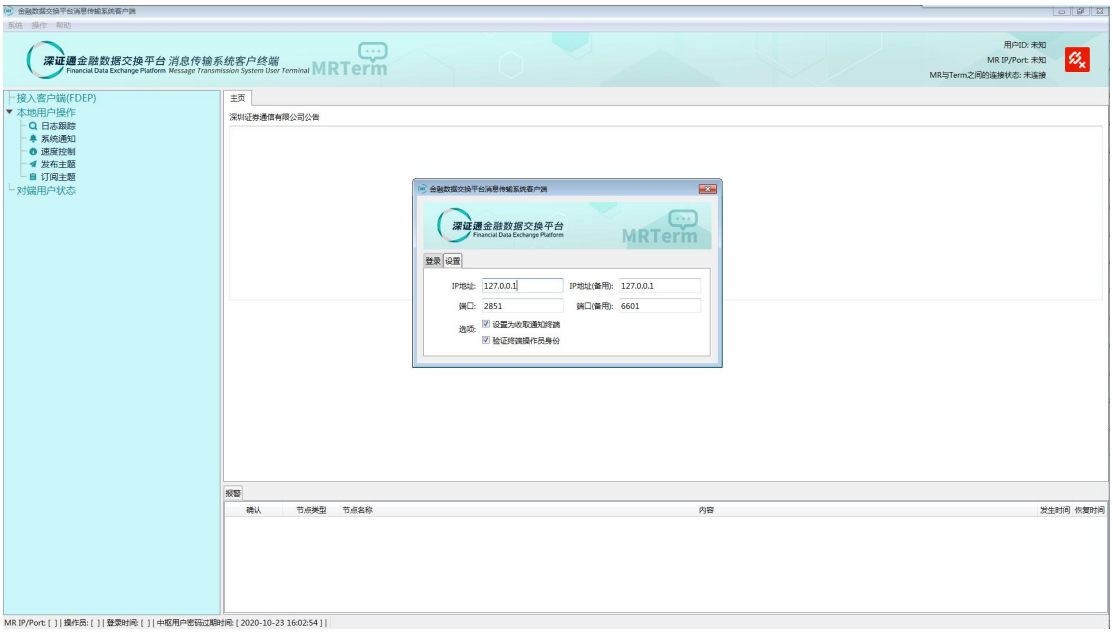


图 3　　监控终端登录地址栏界面

在登录对话框中输入接入客户端的 IP 地址和端口，用户名和密码，即可连接接入客户端。登录对话框设置 Tab 页提供两组接入客户端 IP 地址和端口，连接顺序是监控终端从第一组地址开始尝试连接，连接不上会尝试第二组，第二组再连接不上又重新尝试第二组，循环重试直到连接成功。如果部署的接入客户端只有一个，那么两组地址可以填成相同的。

连接上接入客户端后，就可以通过打开左树上的各个节点，可以查看各个

AP 节点下的队列以及连接的客户端的情况；选中各个节点，右上边查看接入客户端的状态。右下角为报警信息。

在监控终端连接上接入客户端以后，如果意外断开，则监控终端会自动重连接入客户端。

登录之后，监控终端主界面如下图所示。

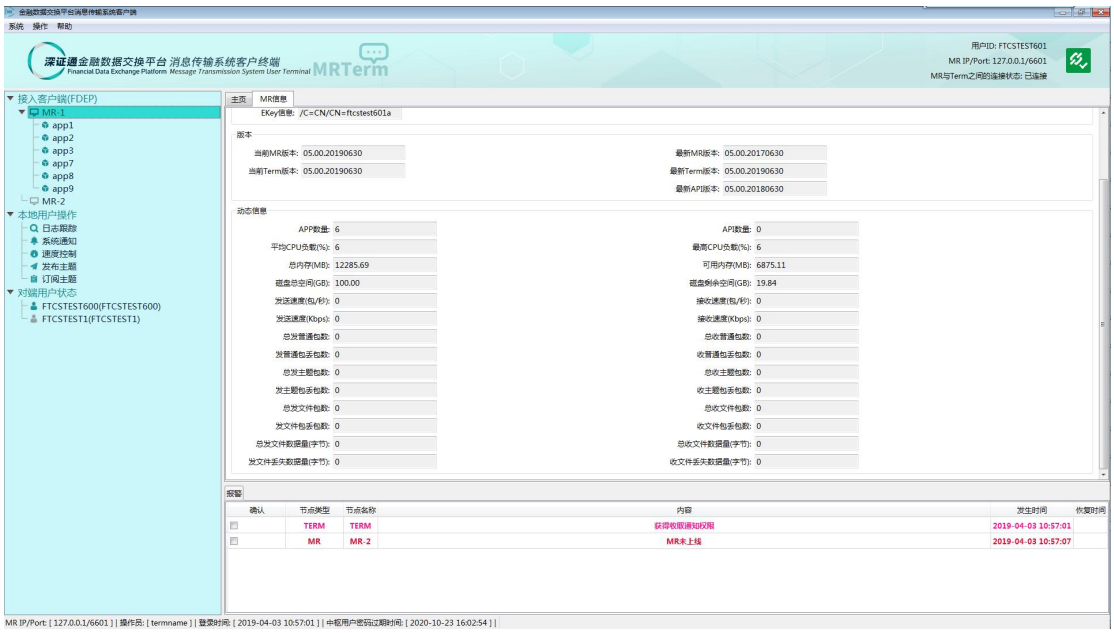


图 4　　监控终端主界面

分别点击各个节点，在右侧的面板中可以看到各个节点的详细信息。

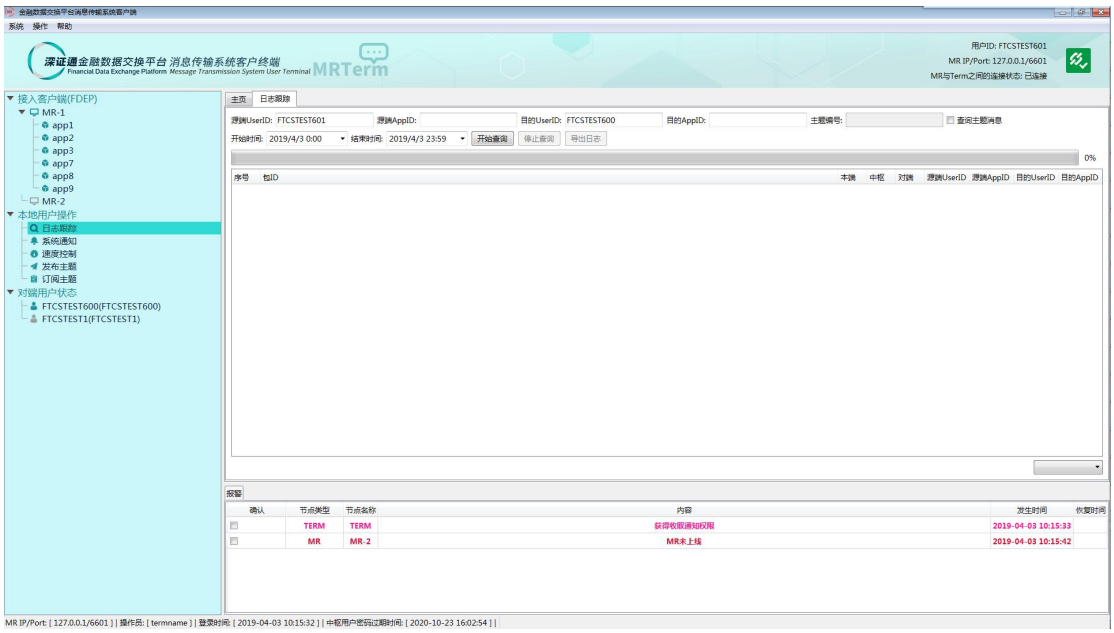


图 5　　日志搜索界面

输入搜索关键字，日志日期，点击开始查询，可以显示相应交换日志的搜索结果

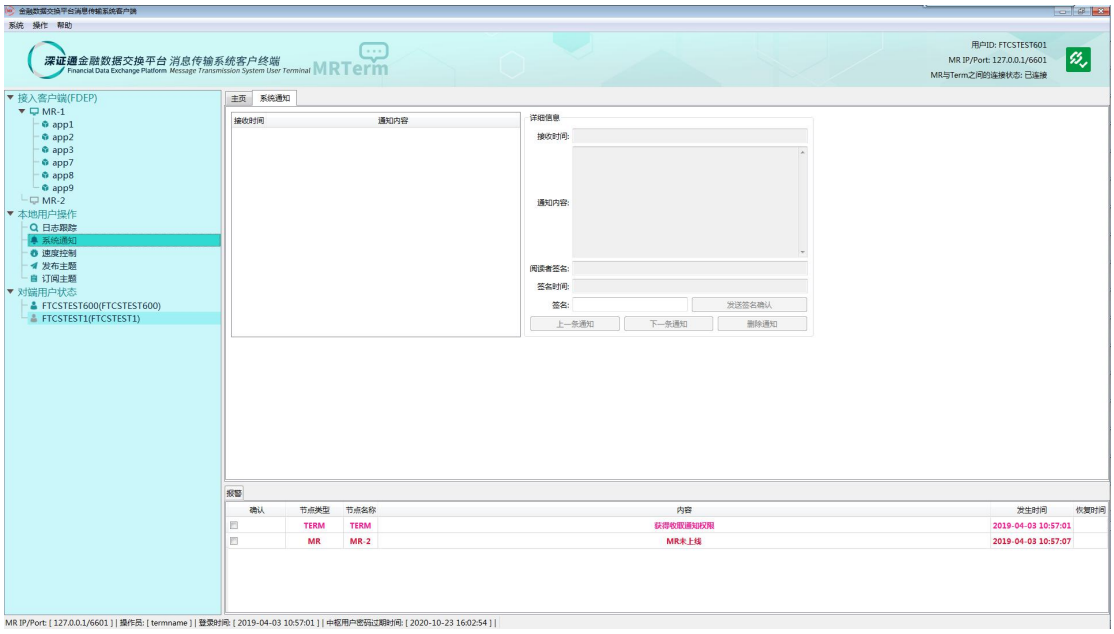


图 6　　系统通知界面

MxTerm 可以接收深证通发送的系统通知，同时允许多个 MxTerm 设置为收发通知终端，可以在登陆界面设置，或者【操作】菜单下【请求通知权限】。

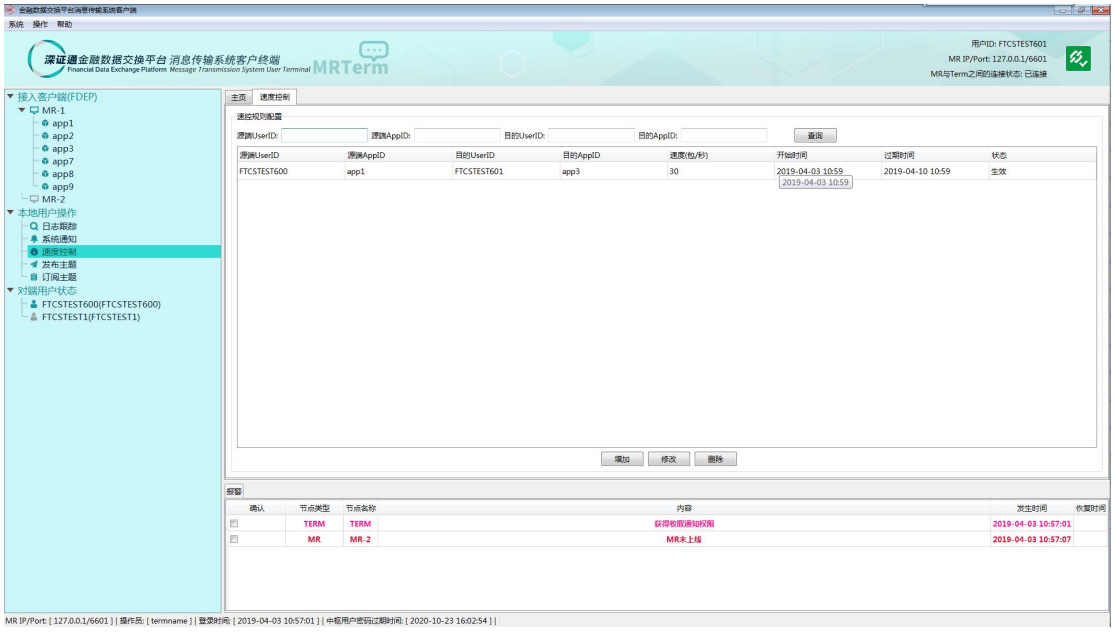


图 7　　速度控制界面

MxTerm 点击左菜单栏速度控制，可添加修改删除相应速控规则指令，查询本地添加的速控指令和对端限速的速控指令。

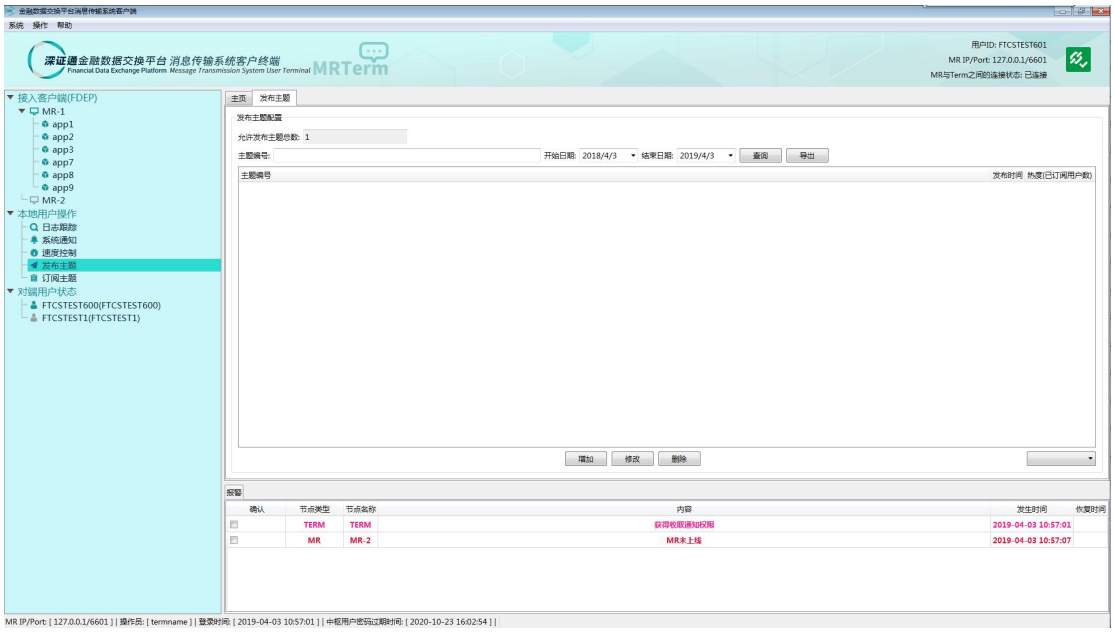


图 8　　发布主题界面

MxTerm 点击左菜单栏发布主题，可以查询、添加、修改、删除主题。

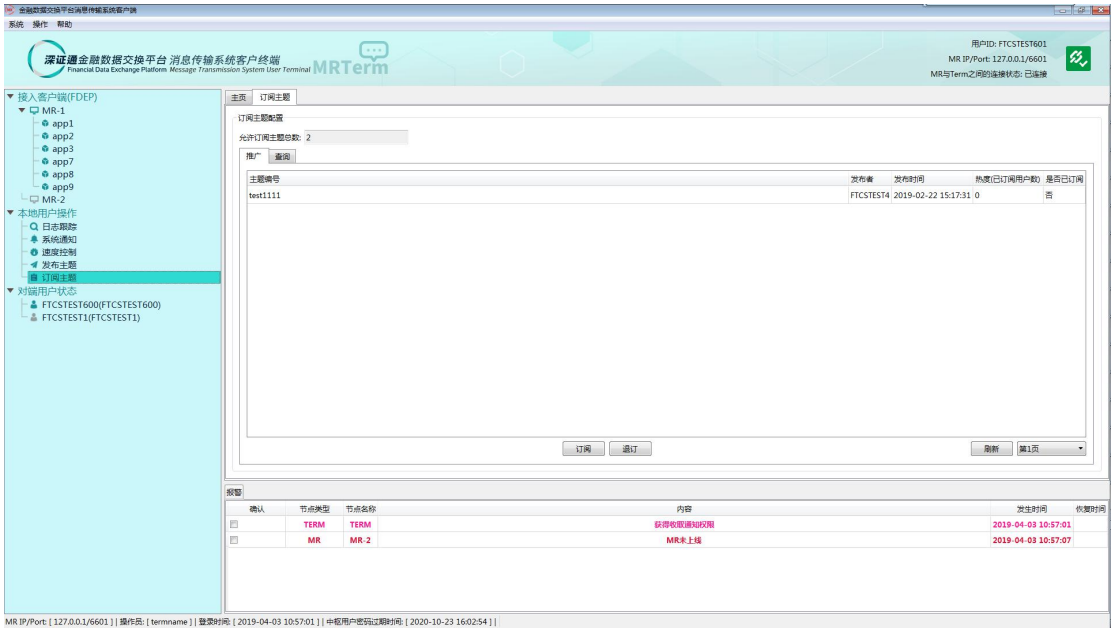


图 9　　订阅主题

MxTerm 点击左菜单栏订阅主题，可以订阅、退订、查询主题。

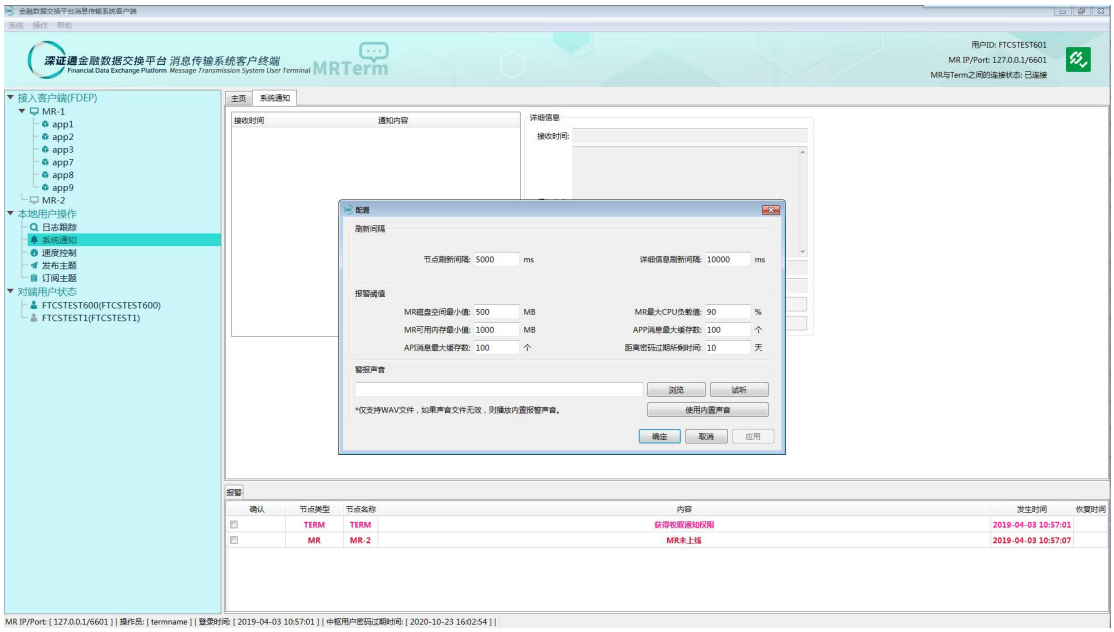


图 10　　监控终端配置界面

MxTerm 可点击【操作】菜单下【配置】，可以配置 MxTerm。

6　备份解决方案

接入客户端是深证通提供的，运行在用户端的消息传输前置机。每个用户可以部署一个或多个 bsmr 软件，它们组成一组，称为接入客户端。由于部署的多个 bsmr 软件之间具有相互热备的能力，因此，推荐用户部署两个 bsmr 软件。

接入客户端的部署方式如下图 11　所示，图中是部署由两个 bsmr 软件，即 MR-1 和 MR-2 的示意图。

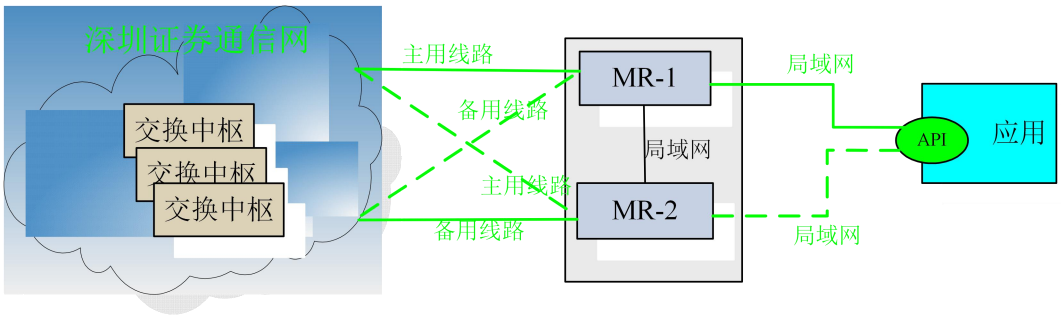


图 11　　接入客户端的部署方式

应用备份：部署两个 bsmr 软件，当任意一个 bsmr 软件发生故障或机器硬件

宕机时，另一个 bsmr 软件可以自动接替故障的 bsmr 而进行正常工作，用户的软件不需要任何操作。

网络备份：从图 11　可以看出，位于用户端的 MR-1 和 MR-2 到交换中枢的网络链路建议是一主一备两条。这样，当万一一条线路发生故障时，bsmr 软件可以从主备其中的任意一条线路进行连接，而正常工作，用户端的软件也不需要任何操作。

备份准备事项，如采用硬件加密，需准备 2 个 Ekey，分插在应用所部署的不同机器上；如果是软加密，需确保 mr.ini 中的 Ekey 字段不一样。

应用备份时，两个 bsmr 软件的配置文件中配置段需要修改的地方如下：

序号	所在配置段名称	字段名称	配置内容
1	[CurrMR]	"MRName"	本 bsmr 软件的名称，一般使用 MR-1 和 MR-2 的命名方式，两个 bsmr 软件的配置文件中此字段值不能相同。
2	[CurrMR]	"Ekey"	如果为硬加密，两个 bsmr 的配置文件中，此字段值填写“/C=CN/CN=****”，打*号部分分别填写两个 Ekey 号码(在 Ekey 上有个标签注明)；如果为软加密，此字段值填写两个文件证书名称。
3	[CurrMR]	"EkeyPwd"	相对应的 EKey 登录密码或文件证书密码[明文]
4	[CurrMR]	"EkeyPwdCrypt"	相对应的 EKey 登录密码或文件证书密码[密文]（实际配置中，3、4 只需配置一项）

7　Ekey 更换操作

7.1　准备条件

更换 Ekey 的准备条件：

(1)已申请到新的硬件 Ekey，准备好新的 Ekey；

(2)选择证券交易闭市后，关闭现有 bsmr 程序，拔掉旧 Ekey。

(3)执行以下更换 Ekey 的操作步骤。

7.2 操作步骤

序号	操作名称	操作说明
1	确保新 Ekey 驱动已经安装好	确保 Ekey 驱动程序已经安装。如果没有，请安装 Ekey 附带光盘中的驱动程序。（如果该机器之前已安装过该类型 Ekey 的驱动，就不用执行本步骤）
2	插入 Ekey	插入 Ekey 到指定机器的 USB 接口。此时可以在 Ekey 的令牌管理器中看到 Ekey 证书在工作中状态，表明新 Ekey 能够正常工作，驱动也安装成功。
3	修改 mr.ini 配置文件	找到深证通 FDAP 程序文件夹，打开 mr.ini 配置文件，修改第三行“Ekey”=“/C=CN/CN=****”。打*号部分填写目前机器上插入的 Ekey 号码(在 Ekey 上有个标签注明)
4	申请开通该 Ekey	电话通知深证通运行热线：0755-83182222，申请开通证书 Ekey，并告知新和旧 Ekey 的主题名。深证通将配合更改相关配置，以便用户可以连接
5	重启 mr 程序	启动 mr 程序的快捷方式，用 mrterm 监控 mr 程序的连接状态。

7.3 常见故障

1. **故障一：**Ekey 驱动安装成功后，插入 Ekey 到指定机器的 USB 接口。此时在 Ekey 的令牌管理器中没有正在工作中的 Ekey 号。

解决办法：该现象表明新 Ekey 无法识别，请尝试将 Ekey 插入到新的 USB 接口，或者检查 Ekey 是否接触不良。如果故障仍然存在，说明 Ekey 可能存在问题，请把新 Ekey 邮寄到我公司更换。

2. **故障二：**更换新的 Ekey 后，启动 bsmr 程序，bsmr.log 日志中提示到 SU 的通信连接一会儿成功，马上又断开，不停地这样重复。

解决办法：该现象表明深证通还未为该用户配置好该 Ekey，也即中枢端软件认为该 Ekey 非法。这种情况下，可以致电深证通运维热线，申请开通证书。

7.4 回退步骤

如果 Ekey 更换不成功，请按照以下步骤进行回退处理：

序号	回退操作名称	回退操作说明
1	确保旧 Ekey 驱动已经安装好	如果该机器之前已安装过需要回退的旧 Ekey 的驱动，就不用执行本步骤。如果没有，需要安装 Ekey 附带光盘中的 Ekey 驱动程序
2	插入旧 Ekey	插入旧 Ekey 到指定机器的 USB 接口。此时可以在 Ekey 的令牌管理器中看到旧 Ekey 证书在工作中状态，表明旧 Ekey 能够正常工作，驱动也安装成功。
3	修改 mr.ini 配置文件	找到深证通 FDAP 程序文件夹，打开 mr.ini 配置文件，修改第三行“Ekey”=“/C=CN/CN=****”。打*号部分填写目前机器上插入的旧 Ekey 号码(在 Ekey 上有个标签注明)
4	申请开通旧 Ekey	电话通知深证通运行热线：0755-83182222，申请更改回旧 Ekey，并告知新和旧 Ekey 的主题名。深证通将配合更改相关配置，以便用户可以连接
5	重启 mr 程序	启动 mr 程序的快捷方式，用 mrterm 监控 mr 程序的连接状态。

8 日常维护

8.1 日常维护

FDAP 程序在运行过程中，一般不需要进行手工维护。但是每隔一段时间应该查看一下程序所在的磁盘占用空间是否已满。因为程序在运行过程中，将产生交换日志和运行日志，当这些日志占用空间太大时，应当及时清除或移到其它磁盘下。建议每天开市之前把 FDAP 程序重启一下，即便是不重启也请查看一下 FDAP 程序是否运行正常。

8.2 关于日志的说明

FDAP 程序在使用过程中，可以产生运行日志并记入日志文件。日志目录为<installdir>\log 目录。日志文件采用日期时间格式，文件名为

bsmr_20190401_000000.log 、 bsmr_20190401_080800.log 、 bsmr_20190401_090900.log 、 … … 、 bsmr_20190401_235959.log 。 其 中 bsmr_20190401_235959.log 是最新的日志文件，bsmr_20190401_00000.log 是最旧的日志文件，即根据时间递增。每个日志文件最大约 50MB，更早的日志文件根据最大保存天数将自动被删除。

日志配置文件\ini\mr.ini 可以控制 FDAP 服务端日志的产生和输出。文件格式如下：

```
[LOG]
"LockType"="1"
"Level"="0"
"Display"="3"
"LogDir"=""
"LogName"="../log/bsmr.log"
"MaxFileSize"="50000000"
"MaxSaveDays"="10"                    // 日志最长保存天数
```

Level 表示日志的级别，其取值范围是 0 至 10，缺省值为 0。0 级日志信息最少，只报告错误和重要的运行信息，这也是正式运行时设置的级别；10 级日志信息最多，包括所有的错误、警告和信息，一般只在程序调试错误时使用。其它常用的级别还有 1 和 5，其信息量中等。

Display 表示日志输出的方式，其取值范围是 0 至 3，缺省值为 1。0 表示不显示也不记录日志；1 表示只在文件中记录日志；2 表示只在屏幕上显示日志（只对控制台程序时有效）；3 表示在文件中记录同时在屏幕上显示日志。

如果配置文件不存在，或者里面少配置了某个参数，则相应参数采用缺省值。

该配置文件可以在使用 FDAP 程序运行过程中动态修改，修改后 30 秒内生效。

9 故障排除指引

问题 1：服务端程序启动失败。

解决方法：可以通过查看安装目录下的\log 目录下的日志文件，找出失败的原因。大多数情况下，启动失败都是因为没有 EKey 引起的，有时也可能是在配置的端口监听失败引起的。

问题 2：监控终端无法连接接入客户端程序，或连接失败。

解决方法：请查看连接的接入客户端的 IP 和端口是否正确。

问题 3：在监控终端看到与交换中枢的连接状态不正常。

解决方法：请检查接入客户端的配置文件是否正确，如果修改了配置，请重新启动接入客户端程序。

10 建议

1、每天开市之前把FDAP程序重启一下，即便是不重启也请查看一下FDAP程序是否运行正常。

11 注意事项

1、BSMR 运行期间不能手动删除*.db 文件，误删除时需清理临时*.db 后重新启动 BSMR。

2、手动删除交易日志，需重新启动 BSMR。

3、修改系统时间，需清理交易日志，并重启 BSMR。

4、跨机部署多活 BSMR 时，mr.ini 配置 Mr 的 ip 地址时需填写实际 ip 地址，不能填写回环地址。

深圳证券通信有限公司

2020 年 4 月