上海清算所
综合业务系统会员客户端
数字证书升级改造推广
接入配置手册

2022 年 7 月

1 前置要求

上海清算所综合业务系统会员客户端具备 SSL 加密通信接入能力，分为终端代理软件接入和本地加密网关接入两种方式，会员机构可根据自身情况选择一种方式，完成会员客户端的加密通信接入。

使用加密通信接入前，必须先按照已有流程完成会员客户端的安装，确保 CA 证书安装、hosts 文件配置等环节已按要求完成。

会员客户端使用加密通信接入时，必须使用由 CFCA 提供的专用 UKey 设备，终端操作系统上也必须安装 UKey 设备专用的驱动程序，并按相关流程完成数字证书的申请和下载安装到 UKey 中。

2 开通网络访问

2.1 服务端口

会员客户端需开通网络访问策略来接入上海清算所服务器，具体地址和端口如下：

域名	服务器地址	端口
m1.outter.access.prod.shch.com	191.168.1.160	9000，8090，9222
s1.outter.access.prod.shch.com	191.168.1.176	9000，8090，9222

2.2 设置本地域名

修改 C:\WINDOWS\system32\drivers\etc\hosts 文件，添加以下内容：

191.168.1.160 m1.outter.access.prod.shch.com

191.168.1.176 s1.outter.access.prod.shch.com

如果会员机构内部网络有地址转换，上述 IP 地址应替换为转换后的 IP 地址。**若 hosts 文件中已存在这两个域名的配置可跳过此步骤无需重复配置。**

2.3 网络连通性验证

打开 cmd 窗口下输入以下命令，如果显示无法连接或访问超时，请排查网络问题。

telnet m1.outter.access.prod.shch.com 9222

telnet m1.outter.access.prod.shch.com 9000

```
telnet m1.outter.access.prod.shch.com 8090

telnet s1.outter.access.prod.shch.com 9222

telnet s1.outter.access.prod.shch.com 9000

telnet s1.outter.access.prod.shch.com 8090
```

3 UKey 准备

可根据市场机构需要,进行证书申请时自行选择“新发 UKEY”（由 CFCA 制证）或“不需 UKEY”（由会员机构制证)。

3.1 选择“新发 UKEY”（由 CFCA 制证）

3.1.1 安装 UKey 驱动程序

双击 UKey 驱动的盘符图标或打开 UKey 盘符后双击 UyeeServiceInstall.Enterprise.exe 安装程序，按向导提示点击下一步即可完成安装。

因 CFCA 的 UKey 批次存在差异,驱动程序安装文件及界面风格可能与下文中的说明或图片存在差异,具体以实际获取的为准。

3.1.2 修改 PIN 码

UKey 在第一次使用时需修改 PIN 码，插入 UKey 等系统提示检测到新设备后，在右下角任务栏图标  ，即可显示 UKey 内容。

点击修改 PIN 码后，按提示输入当前 PIN 码和符合要求的新 PIN 码（最短 8 位，最长 16 位，必须含有数字、字母、符号中两种或两种以上组合，字母区分大小写），再点击确定保存。第一次修改时当前 PIN 码为 UKey 的初始 PIN 码：“Cfca123!”。

3.2 选择“不需 UKEY”（由会员机构制证）

会员机构需要自己制证时，经办人将收到“CFCA 企业证书两码”邮件，点击“一键制证链接”，打开 CFCA 制证服务平台页面（请使用 Windows 操作系统+Chrome 浏览器 60 以上版本操作），在“订单详情”页中进行制证操作。插入待制证 Ukey，点击“自

制证”，在弹框中点击“获取 UKey 序列号”后进行一键制证，输入 UKey 密码，验证通过后制证完成。

4 接入方式一：终端代理软件

4.1 代理软件启动步骤

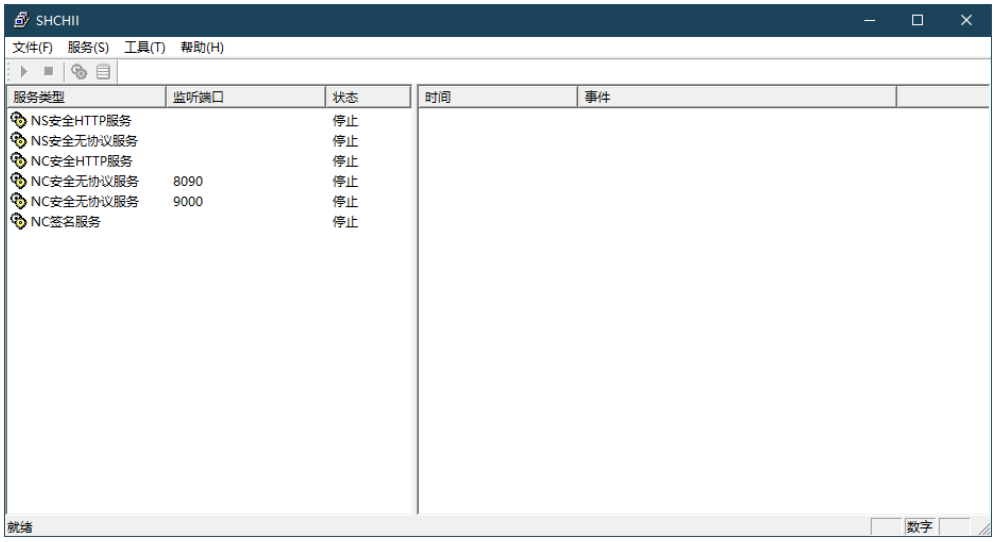
上海清算所提供了在会员终端上运行的加密代理软件用于加密通信接入。

代理软件提供了 2 个版本，压缩包文件名为 BiSafeM1.zip 和 BiSafeS1.zip（详见附件），分别用于上海清算所主数据中心和同城数据中心的接入。两者仅通信配置有差异，功能完全相同，平时可以任选一个使用。若当前线路发生故障无法连通，可以更换启动另外一个版本切换接入线路。后续以 BiSafeM1.zip 为例说明配置启动过程，BiSafeS1.zip 也完全适用。

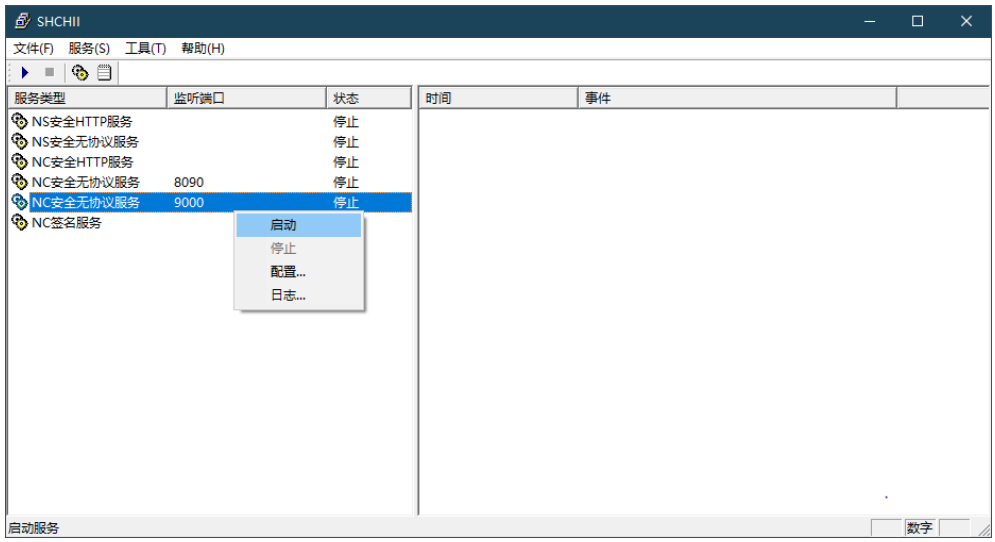
具体过程如下：

1． 将压缩包解压到 D 盘根目录，解压后的目录路径应该为“D:\BiSafeM1”。若目录存在差异变化，需修改代理软件根证书配置，具体步骤见章节 4.3 根证书配置变更。

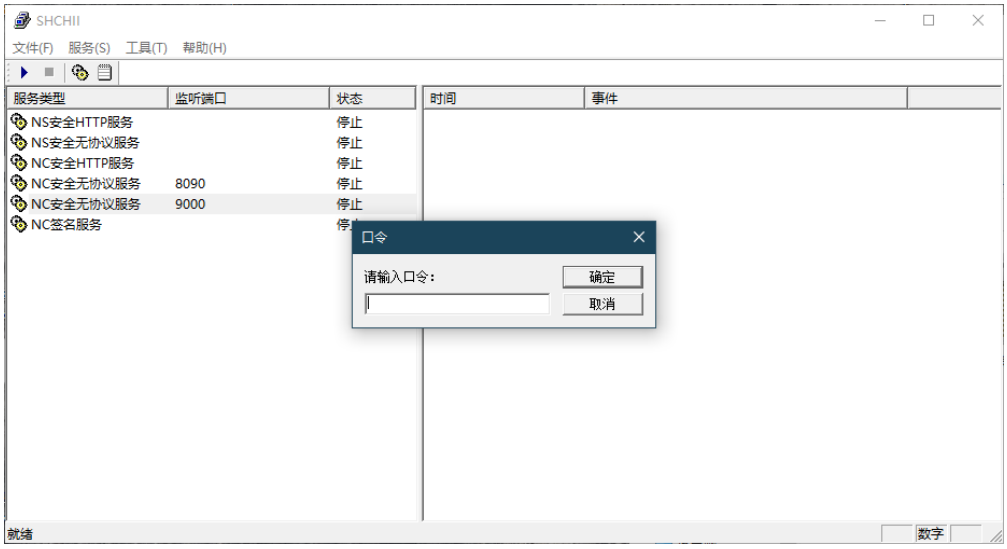
2． **插入 UKey**，双击“D:\BiSafeM1\BiSafe.exe“启动代理软件，启动成功后界面如下：



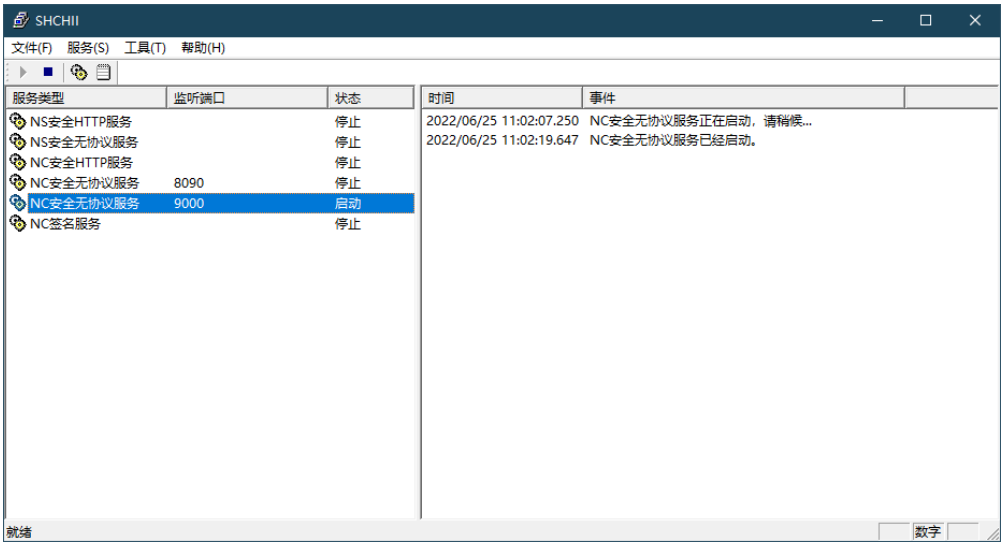
3． 右键点击“NC 安全无协议服务 9000”，在右键菜单中点击启动。



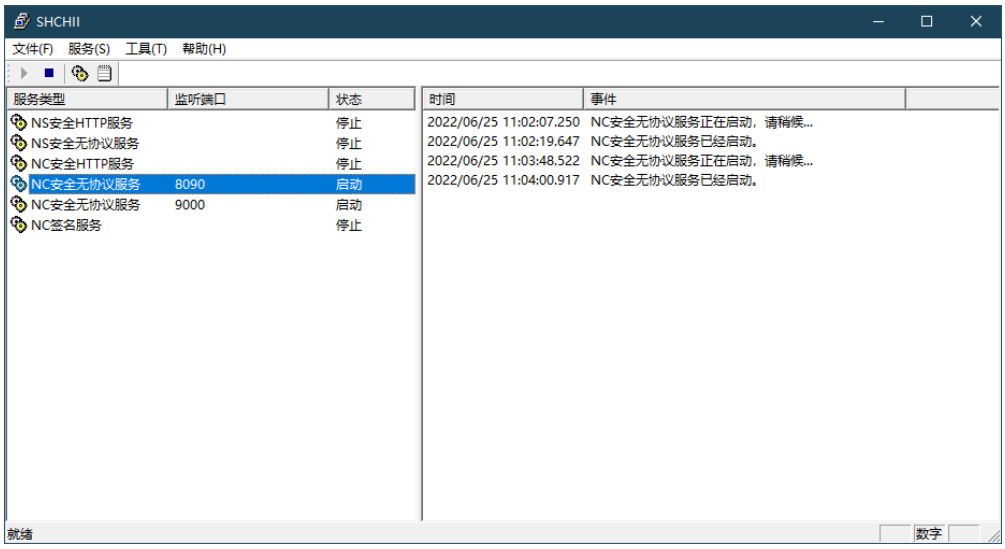
4． 提示输入口令时，输入 UKey 的 pin 码，点击确定按钮继续启动。



5． 等待“NC 安全无协议服务 9000”启动完成，若启动过程有防火墙警告提示请选择允许访问。

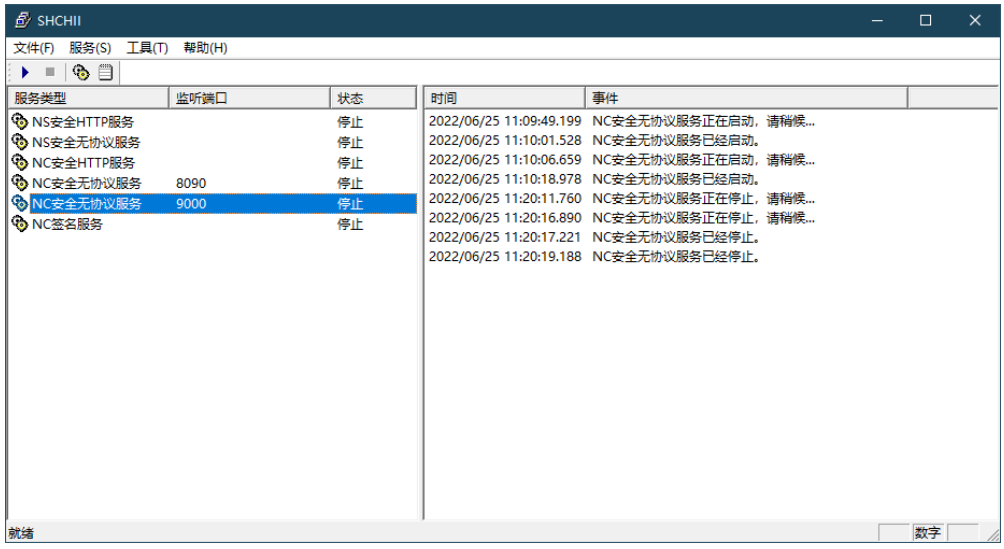


6． 再按相同步骤启动“NC 安全无协议服务 8090”。



7． 至此代理软件启动完成，可以开始启动会员客户端进行操作。

当代理软件使用后，必须先右键点击“NC 安全无协议服务 9000”和“NC 安全无协议服务 8090”，再点击停止菜单项等待 2 个服务完全停止后，再关闭代理软件。



4.2 客户端通信配置

启动会员客户端，在登录界面点击右上角配置图标打开通信配置界面，在设置单选框中选择“代理软件”，再点击确定按钮

保存。如下图：

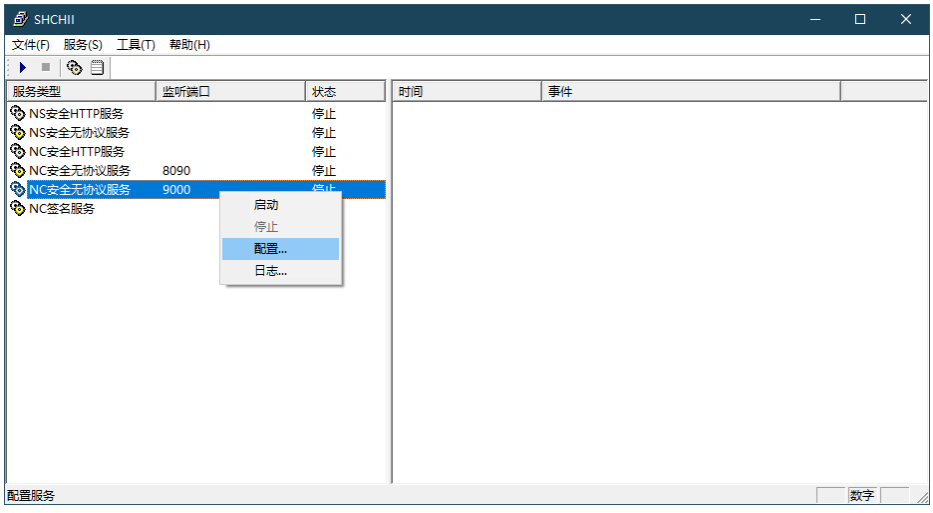
4.3 根证书配置变更

默认情况下不需要修改代理软件根证书配置。当代理软件所在目录路径发生变化，或因其它原因要更换根证书时，则需要对代理软件根证书配置进行修改。具体步骤如下：

1．打开代理软件所在文件目录，确认存在根证书文件CFCA_SM2_OCA1.pem。

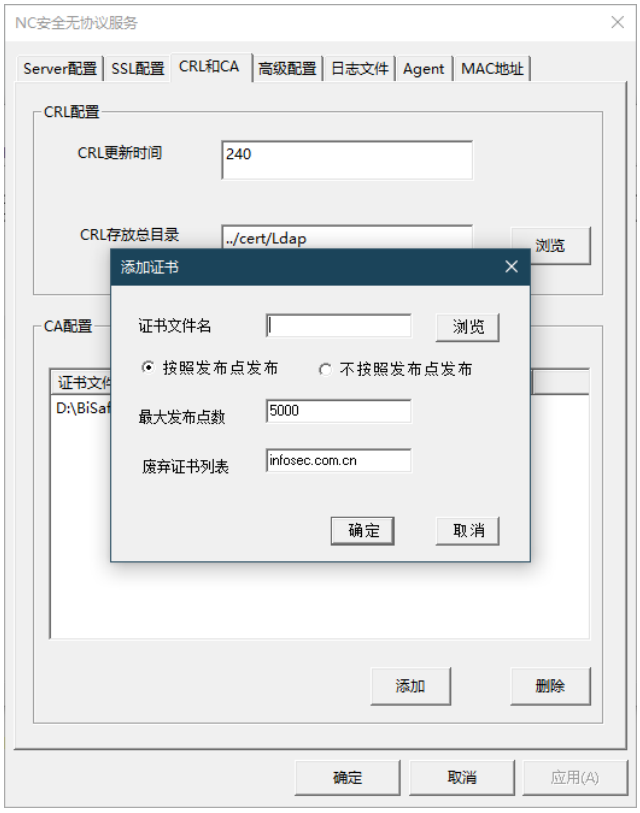
名称	修改日期	类型	大小
cert	2022/6/24 16:11	文件夹	
DownloadCRL	2022/6/24 16:11	文件夹	
nchttps	2022/6/24 16:11	文件夹	
ncnops	2022/6/24 16:11	文件夹	
ncnops1	2022/6/25 10:51	文件夹	
ncsign	2022/6/24 16:11	文件夹	
nshttps	2022/6/24 16:11	文件夹	
nsnops	2022/6/24 16:11	文件夹	
p10gen	2022/6/24 16:11	文件夹	
Aetpkss1.dll	2019/11/1 13:44	应用程序扩展	756 KB
base64.dll	2019/11/1 13:44	应用程序扩展	32 KB
BiSafe.exe	2021/5/10 9:56	应用程序	2,016 KB
CFCA_SM2_OCA1.pem	2015/6/1 16:22	PEM 文件	1 KB
hhpkcs1102.dll	2019/11/1 13:44	应用程序扩展	368 KB
HtPkcs11.dll	2019/11/1 13:44	应用程序扩展	636 KB
libeay32.dll	2019/11/1 13:44	应用程序扩展	1,180 KB
msvcr80.dll	2019/11/1 13:44	应用程序扩展	621 KB
NetInfo.exe	2019/11/1 13:44	应用程序	78 KB
setting.ini	2021/11/9 10:31	配置设置	1 KB
sm2signdyn.dll	2019/11/1 13:44	应用程序扩展	97 KB
src_licenceAPI_win_x86.dll	2019/11/1 13:44	应用程序扩展	160 KB
ssleay32.dll	2019/11/1 13:44	应用程序扩展	272 KB
version	2021/5/6 14:05	文件	1 KB

2．启动代理软件，右键点击“NC 安全无协议服务 9000”，在右键菜单中点击配置。



3．在对话框中选择“CRL 和 CA”配置页，在 CA 配置中选中已有配置项，点击删除按钮删除当前配置。

4．继续点击添加按钮，在新对话框中点击浏览按钮选中步骤 1 中的 pem 文件，再点确定按钮完成保存，关闭配置对话框完成配置变更。

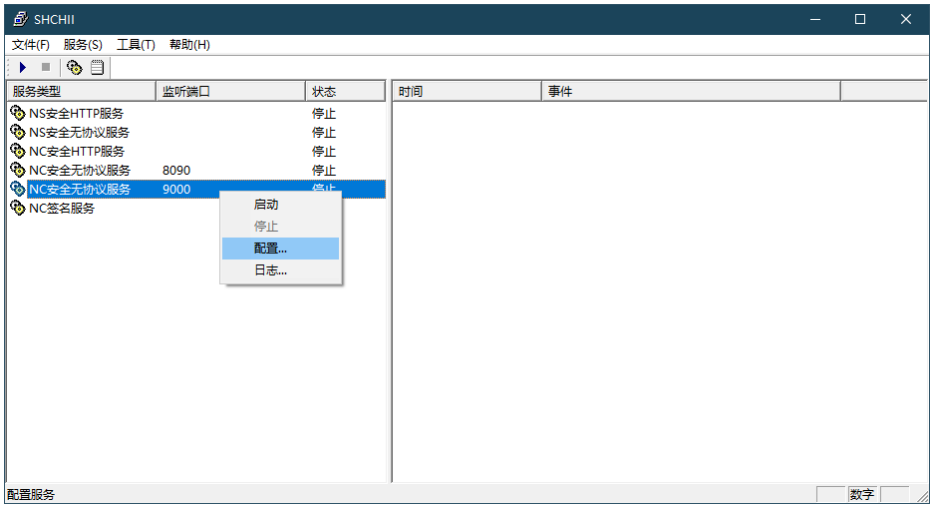


5． 按以上步骤再完成对“NC 安全无协议服务 8090”的配置修改。

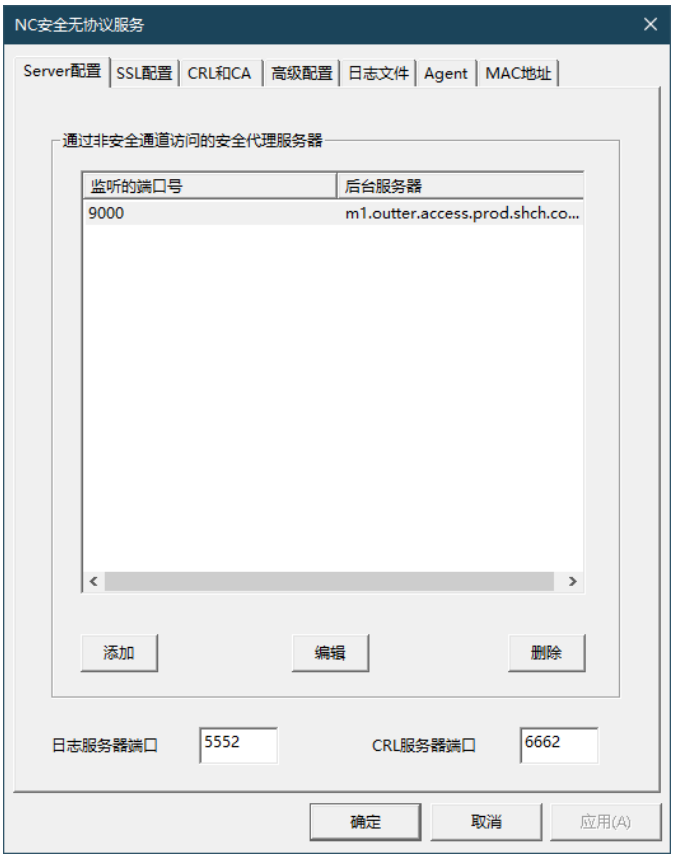
4.4 服务地址配置变更

默认情况下不需要修改代理软件服务地址配置。但若有其它特殊场景需要修改服务地址时，可按以下步骤操作：

1． 启动代理软件，右键点击“NC 安全无协议服务 9000”，在右键菜单中点击配置。



2． 在对话框的”Server 配置”页中选中当前配置项，点击编辑按钮进行修改。



3． 选中已有后台服务配置项，再点击右侧编辑按钮，再在弹出对话框中输入新的后台服务器地址。

注意：请勿修改“监听的 IP 端口号”，保持当前值“9000”。

4． 按以上步骤再完成对“NC 安全无协议服务 8090”的配置修改。

5 接入方式二：本地加密网关

5.1 加密网关配置要求

会员机构需事先自行采购经国家密码管理局认证、符合GMT0025和GMT0028技术标准的加密通信设备，并在设备提供商支持下完成以下网络配置。

上海清算所综合业务系统提供了以下接入地址：

数据中心	IP地址	tcps端口	https端口
主数据中心	191.168.1.160	9000	8090
同城数据中心	191.168.1.176	9000	8090

按上表所述，加密设备上需同时配置一个tcps服务和一个https服务，可同时配置主数据中心和同城数据中心地址实现双活高可用。

tcps服务和https服务的对内服务必须在同一IP上，且端口也必须分别是9000和8090，不可更换为其它端口。例如：

11.22.33.44:9000

11.22.33.44:8090

加密通信设备上必须在全局CA证书列表中，安装以下指定的根证书：

CFCA_CS_SM2_CA.cer

CFCA_SM2_OCA1.cer

根证书文件可从CFCA网站上下载：

（上述页面仅供参考，以 CFCA 实际页面为准）

加密设备的相关通信配置中，SSL 密码套件要求仅配置密码相关算法套件，具体如下：

ECC-SM4-SM3

ECDHE-SM4-SM3

加密设备需安装 CFCA 的数字证书，数字证书申请流程可参见《外部客户端操作手册》的“外部客户端证书管理”章节，证书类型选择“企业高级证书（SM2）”，是否新发 Ukey 选择“否”；数字证书导入设备的具体步骤可咨询设备厂商。

5.2 客户端通信配置

启动会员客户端，在登录界面点击右上角配置图标打开通信配置界面，按下图所示选择相应的加密设置，并在右侧网关地址输入框中输入上一步骤的内部服务 IP 地址，点击确定按钮保存退出，再关闭重启客户端。如下图所示：


设置
国密设置
国密网关
代理软件
*网关地址
11.22.33.44
新增
修改
使用
删除
服务名
地址
使用状态
二代系统（生产）
https://s1.outter.access.prod.shch.com:9222,50|https://m1.outter.acces...
· 使用中
确定
取消

6 客户端启动登录

插入 UKey 后，按常规方式启动会员客户端，可在证书账号下拉框中看到 Ukey 中的证书，选择第一个即可。证书密码暂时不用输入。

在其它输入框中填写正确的账号密码后，点击登录按钮，按提示正确输入UKey的PIN码,点击确认按钮即可完成登录操作。

客户端使用过程中请保持 UKey 插入，使用完成后请及时拔出 UKey 妥善管理。

7 常见问题

7.1 网关连接失败

当登录界面提示“网关连接失败”等异常信息时：

1．检查网络是否通畅

若使用 BiSafeM1 时，执行以下命令探测端口是否能够被打开：

telnet m1.outter.access.prod.shch.com 9000

telnet m1.outter.access.prod.shch.com 8090

若发现探测失败，可更换 BiSafeS1 尝试，或请联系网络支持人员排查网络问题

若使用 BiSafeS1 时，执行以下命令探测端口是否能够被打开：

telnet s1.outter.access.prod.shch.com 9000

telnet s1.outter.access.prod.shch.com 8090

若发现探测失败，可更换 BiSafeM1 尝试，或请联系网络支持人员排查网络问题

2．检查代理软件配置是否正确

如果代理软件未放在指定的默认路径，请按 4.3 章节修改根证书配置；

可停止重启代理软件的两个 NC 安全无协议服务再次尝试登录；

重新获取代理软件程序包，按 4.1 章节步骤重新部署启动代理软件。

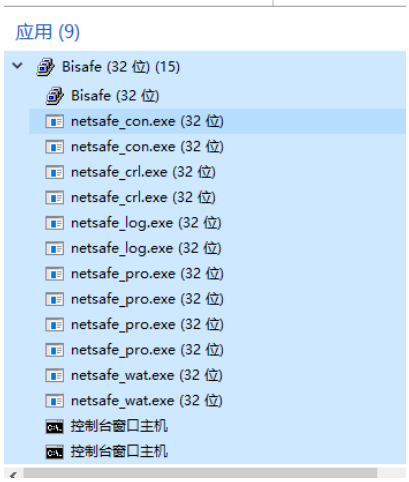
7.2 代理软件服务失败

若代理软件的 NC 安全无协议服务启动失败，

1． 检查代理软件是否被安装在网络磁盘上，代理软件需安装在本地磁盘上启动时才能获取足够的权限；

2． 检查本机的防火墙、杀毒安全软件等是否将代理软件加入了黑名单；

3． 完全关闭代理软件，打开 Windows 任务管理器，若存在残留进程则全部强制结束任务。



8 附件

1．BiSafeM1.zip：终端代理软件（用于接入上海清算所主数据中心）

2．BiSafeS1.zip：终端代理软件（用于接入上海清算所同城数据中心）