# 中国移动云市场
# 深信服 SSL VPN 产品
# 操作手册

SAAS 平台项目组

2018/8/29

# 目 录

# 1.修订目录

| 日期 | 修订者 | 版本号 | 说明 |
|---|---|---|---|
| 2018-3-25 | 阮丘陵 | 1.0 | |
| | | | |
| | | | |

# 2.范围

本文档是SSL VPN系统产品在中国移动公众服务云SAAS平台操作手册。

## 图形界面格式约定

| 文字描述 | 代替符号 | 举例 |
|---|---|---|
| 按钮 | 边框+阴影+底纹 | “确定”按钮可简化为 确定 |
| 菜单项 | 『 』 | 菜单项“系统设置”可简化为『系统设置』 |
| 连续选择菜单项及子菜单项 | → | 选择『系统设置』→『接口配置』 |
| 下拉框、单选框、复选框选项 | [ ] | 复选框选项“启用用户”可简化为[启用用户] |
| 窗口名 | 【】 | 如点击弹出[新增用户]窗口 |
| 提示信息 | “” | 提示框中显示“保存配置成功，配置已修改,需要重启 DLAN 服务才能生效，是否立即重启该服务?” |

## 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 **小心、注意：**提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。

 **警告：**该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。

 **说明、提示、窍门：**对操作内容的描述进行必要的补充和说明。

# 技术支持

用户支持邮箱： support@sangfor.com.cn

技术支持热线电话： 400-630-6430（手机、固话均可拨打）

技术支持论坛： http://bbs.sangfor.com.cn

公司网址： http://www.sangfor.com.cn

# 致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

# 第1章 控制台的使用

## 1.1. 登录 WebUI 配置界面

首次配置设备，需要准备一台 PC，直连或通过二层交换机连接到设备 **ETH0** 接口，通过 Web 界面来配置 VPN 设备。方法如下：

首先为本机器配置一个 IP **10.254.254.100**，掩码配置为 **255.255.255.0**，然后在 IE 浏览器中输入网关的默认登录 IP 及端口，输入 **https:// 10.254.254.254:4430/**，页面如下：

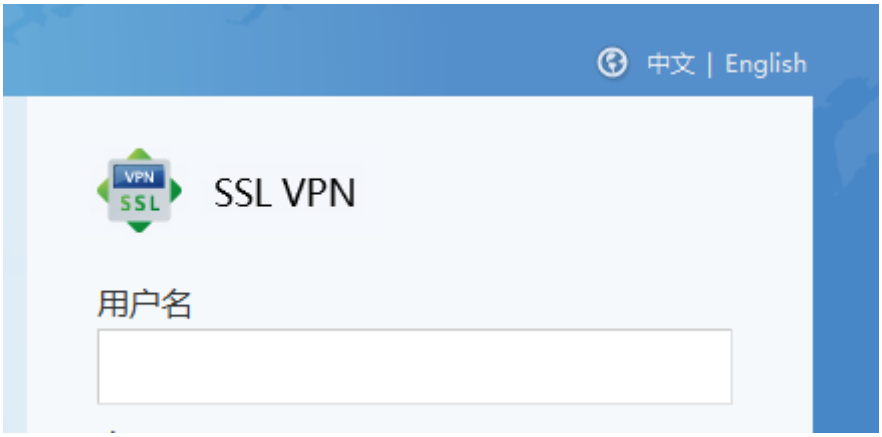

登录页面左树是公司主页面链接。如：


点击相应图片跳转到公司链接了解更多信息。


手机扫描二维码关注公司公共微信，了解公司产品动态。

在登录框输入『用户名』和『密码』，点击登录按钮即可登录 VPN 网关进行配置，默认情况下的用户名和密码均为：admin。

操作系统支持中英文切换，如需切换可点击中文 | English，即显示相应的操作系统。




如果需要查看当前网关的版本号，可点击查看版本，即显示当前硬件的版本信息。

登录 WebUI 配置界面后，可以看到以下配置内容，如下图所示：


『运行状态』：此处可以查看当前设备的运行状态。

『系统设置』：此处可设置设备的序列号、网络配置及各种常见全局性配置。

『SSL VPN 设置』：设置 SSL VPN 相关信息。

『SC 设置』：设置集中管理相关信息。

『IPSEC VPN 设置』：设置 IPSEC VPN 互联信息。

『防火墙设置』：设置设备内置的防火墙规则及策略。

『双机维护』：开启和设置双机功能。

『系统维护』：用来查看日志、备份/恢复设备的配置信息，重启设备/服务或关闭设备。

**注意：所有配置界面中如果有[确定]、[保存]、[配置生效]按钮，则配置完毕后，必须要点击该按钮才能使设置保存并生效，后面的文档不再赘述。**

## 1.2. 运行状态

『SSL VPN 运行状态』里面可以查看『系统状态』,『在线用户』,『告警日志』,『远程应用』。界面如下图所示：


### 1.2.1. 系统状态

在『系统状态』里面可以选择查看相应的模块，包括：『系统信息』,『链路状态』,『网络吞吐量』,『并发用户趋势』,『并发会话数』,『流缓存状态』。

WEBUI 路径：『运行状态』→『SSL VPN 运行状态』→『系统状态』。

界面如下图所示：


点击[选择模块]右边的，在相应的模块前打钩，勾选的模块就会在页面空白处显示。

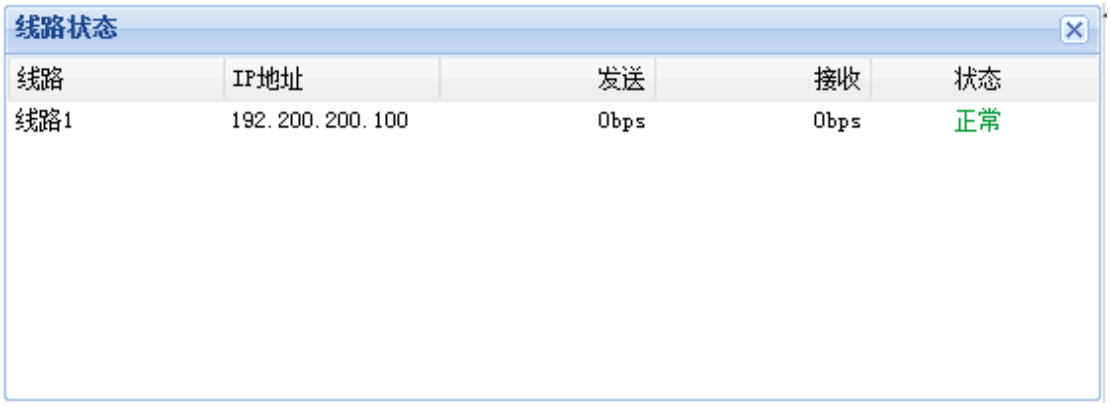
『刷新间隔』，设置页面信息的刷新时间。点击 立即更新 ，则立即更新页面上显示的信息。

『系统信息』，可以查看相应的 CPU 使用记录、在线用户数、锁定用户数、待审批特征

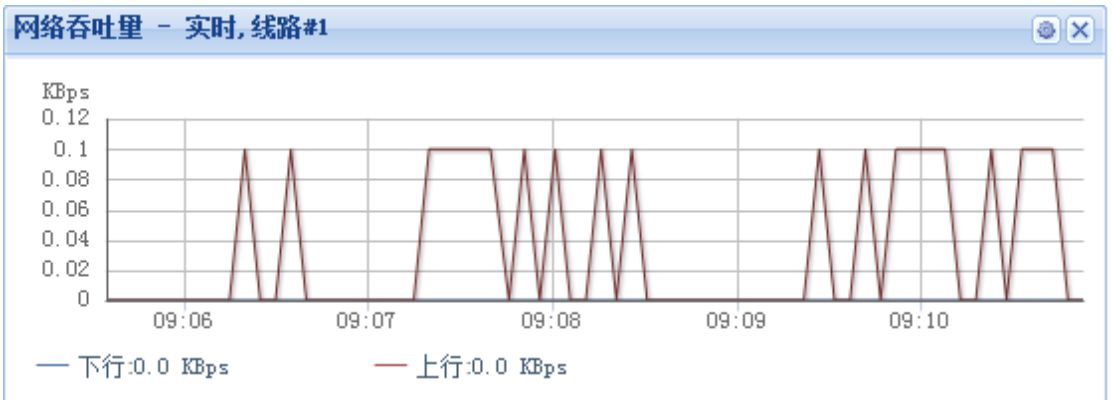
码、SSLVPN 服务状态，点击后面的 查看，可以分别链接到在线用户列表页面、锁定用户列表页面和特征码管理页面。显示如下：


点击 停止服务，停止 SSLVPN 服务。

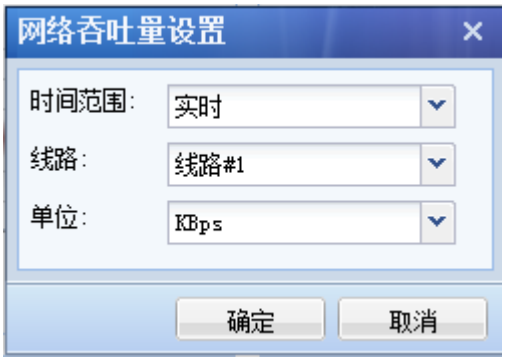
『线路状态』，可以查看所有外网线路的状态信息，并且可以看到相应线路的流速大小。显示如下：




『网络吞吐量』，可以查看线路的流速大小，显示如下：

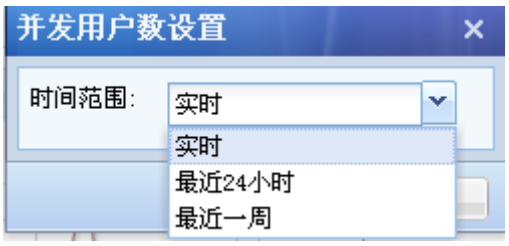


点击右上角图标，选择查看的时间范围（实时；最近 24 小时；最近一周），线路，显示流速的单位。如下图：

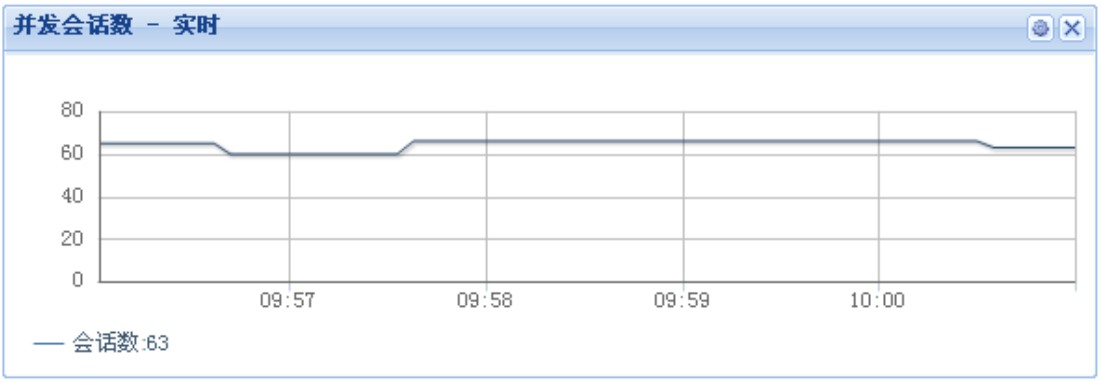



『并发用户趋势』可以查看某个时间段内登录 SSL VPN 的用户数。显示如下：

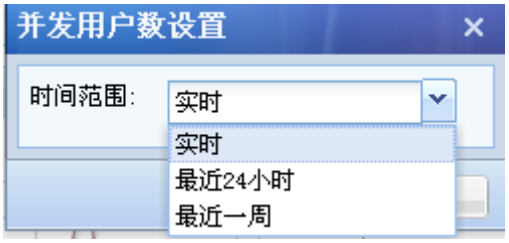

点击左上角的编辑图标，能够选择实时，最近 24 小时，最近一周时间段来显示，显示如下：




『并发会话数』可以查看当前或选择时间段设备发起的并发会话数。显示如下：

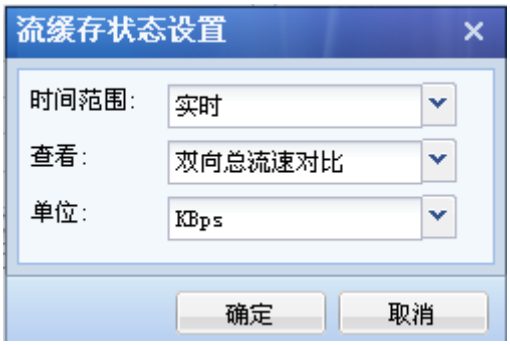



点击左上角的编辑图标，也可以选择实时，最近 24 小时，最近一周时间段来显示会话数，显示如下：




『流缓存状态』，可以查看设备是否启用流缓存，流缓存的加速状态，显示如下：


点击右上角图标选择查看的时间范围（实时；最近 24 小时；最近一周），流速比（总流速比；上行流速比；下行流速比），显示流速的单位。显示如下：

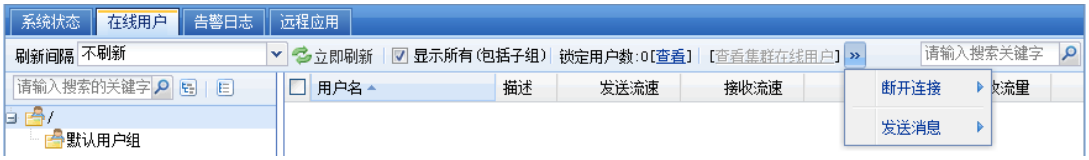



## 1.2.2. 在线用户

在『在线用户』里面可以查看当前登录 SSL VPN 的在线用户，可以查看到相应用户的接收发送流速/流量和接入 VPN 的时间，可以手动将接入的 VPN 用户断开或禁用。

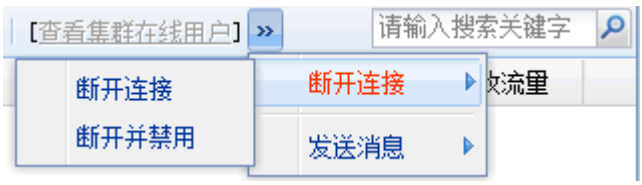
WEBUI 路径：『运行状态』→『SSL VPN 运行状态』→『在线用户』。

界面如下图所示：




『刷新间隔』可以设置页面自动刷新时间，点击 立即刷新 则立即刷新页面信息。

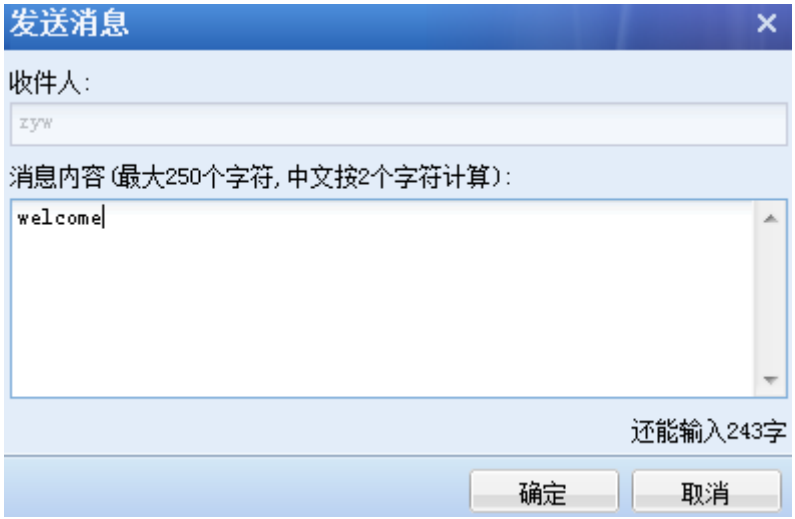
点击 断开连接 可选择[断开连接]或者[断开并禁用]。页面显示如下：



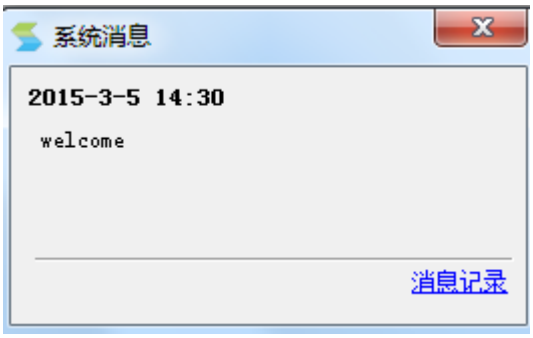

勾选相应的用户，然后点击『断开连接』，该用户则断开 SSLVPN 的连接。如果选择『断开并禁用』，并点击 立即生效，则该用户被断开后将被禁止登录。

点击 发送消息，给 SSL VPN 用户发送相应的信息，可以选择[发送给选中用户]或者[发送给所有用户]，如下图：


选择用户对象后，可设置消息内容，显示如下：




点击 确定 后，SSL VPN 客户端登陆后，在屏幕右下角，会弹出相应消息，显示如下：




## 1.2.3. 告警日志

『告警日志』里面可以查看 SSLVPN 设备的相应告警信息。

WEBUI 路径：『运行状态』→『SSL VPN 运行状态』→『告警日志』。

显示如下：


点击 删除，则可以将选择的告警日志从下面的列表中删除掉。

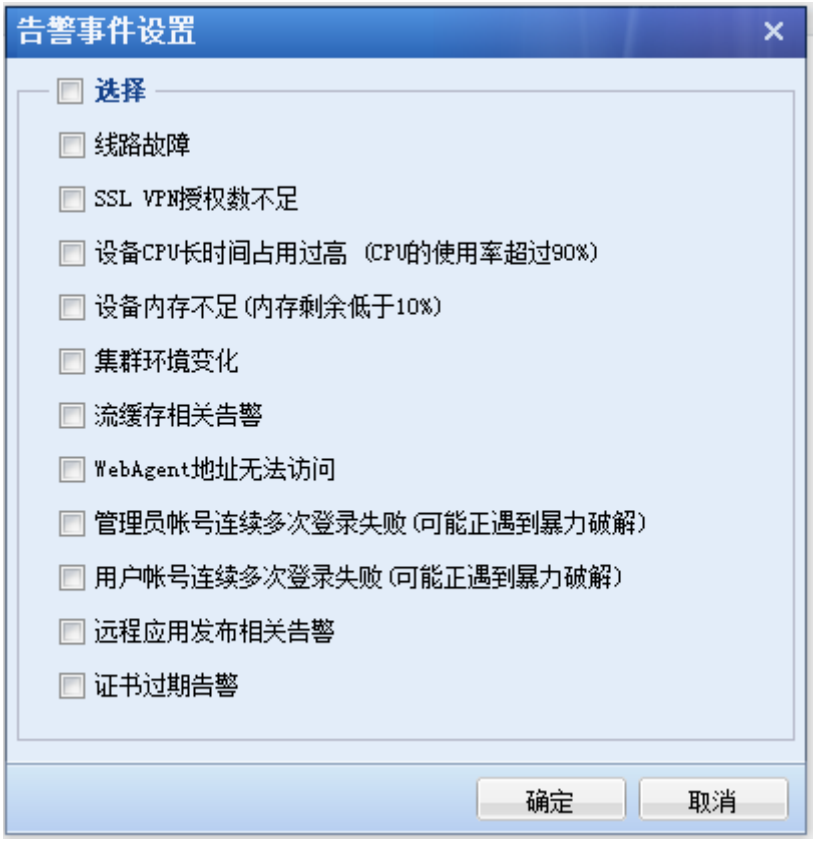
点击 选择，则可以选择[选择当前页]，[选择所有页]，[取消选择]，显示如下：


[选择当前页]，则将该页的日志全部选上，

[选择所有页]，则将所有的日志选上，

[取消选择]，则将之前选择的日志取消掉。

点击 告警事件设置后，可以选择相应的告警信息，显示如下：




『线路故障』当外网线路出现问题时会给指定的邮箱发送邮件告警；

『SSL VPN 授权数不足』SSL VPN 登录用户达到 SSL VPN 用户授权数时，会给指定的邮箱发送邮件告警；

『设备 CPU 长时间占用过高』设备 CPU 长时间过高，120 秒内，平均使用率超过 90%，会给指定的邮箱发送邮件告警，当设备恢复正常也会发送一封邮件；

『设备内存不足』当设备内存不足时，持续 4 分钟，内存低于 10%，会给指定的邮箱发送邮件告警，当恢复正常后，也会发送一份邮件通知设备恢复了；

『集群环境变化』当集群分发器发生变化时，会给指定的邮箱发送邮件告警；

『流缓存相关告警』流缓存相关告警即当流缓存将空间占满时，会给指定的邮箱发送邮件告警；

『WebAgent 地址无法访问』：当 WebAgent 地址无法访问时，会给指定的邮箱发送邮件

告警；

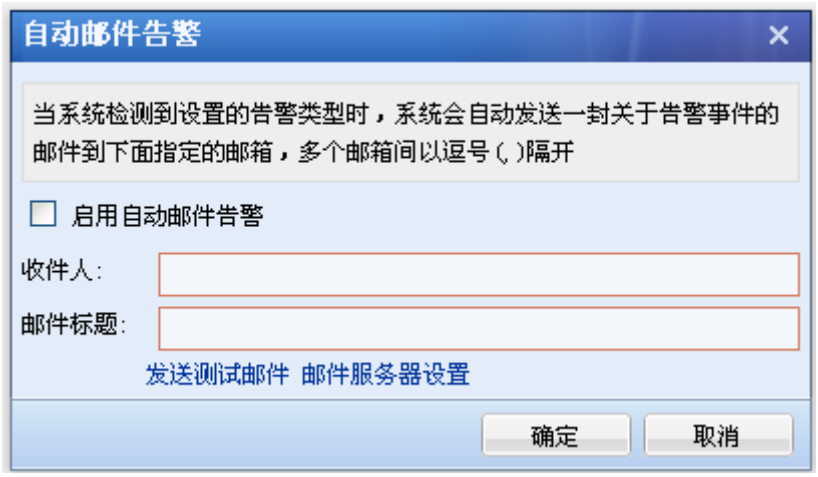
『管理员账号连续多次登录失败』管理员账号连续多次登录失败时，会给指定的邮箱发送邮件告警；

『用户账号连续多次登录失败』SSL 用户账号连续多次登录失败，会给指定的邮箱发送邮件告警；

『远程应用发布相关告警』远程应用发布相关告警即当应用发布出现问题时，会给指定的邮箱发送邮件告警；

『证书过期告警』SSL 证书过期时,会给指定的邮箱发送邮件告警；

点击 自动邮件告警 后，可以勾选[启用自动邮件告警]并设置接收告警的邮件地址和邮件标题。设备会根据设置将告警邮件发送至设置的邮箱，页面显示如下：




点击 发送测试邮件，设备会自动发送一封测试邮件给收件人。

点击 邮件服务器设置，即链接到『邮件服务器』设置页面，详见 3.1.6 章节。

## 1.2.4. 远程应用

在『远程应用』中可以查看 SSLVPN 提供服务器的相应信息和状态。

WEBUI 路径：『运行状态』→『SSL VPN 运行状态』→『远程应用』。

在这里可以看到终端服务器和存储服务器的状态信息，包括服务器名称，服务器地址，服务器类型，CPU，内存，磁盘 I/O，远程应用会话，服务器会话及状态等信息。界面如下图所示：

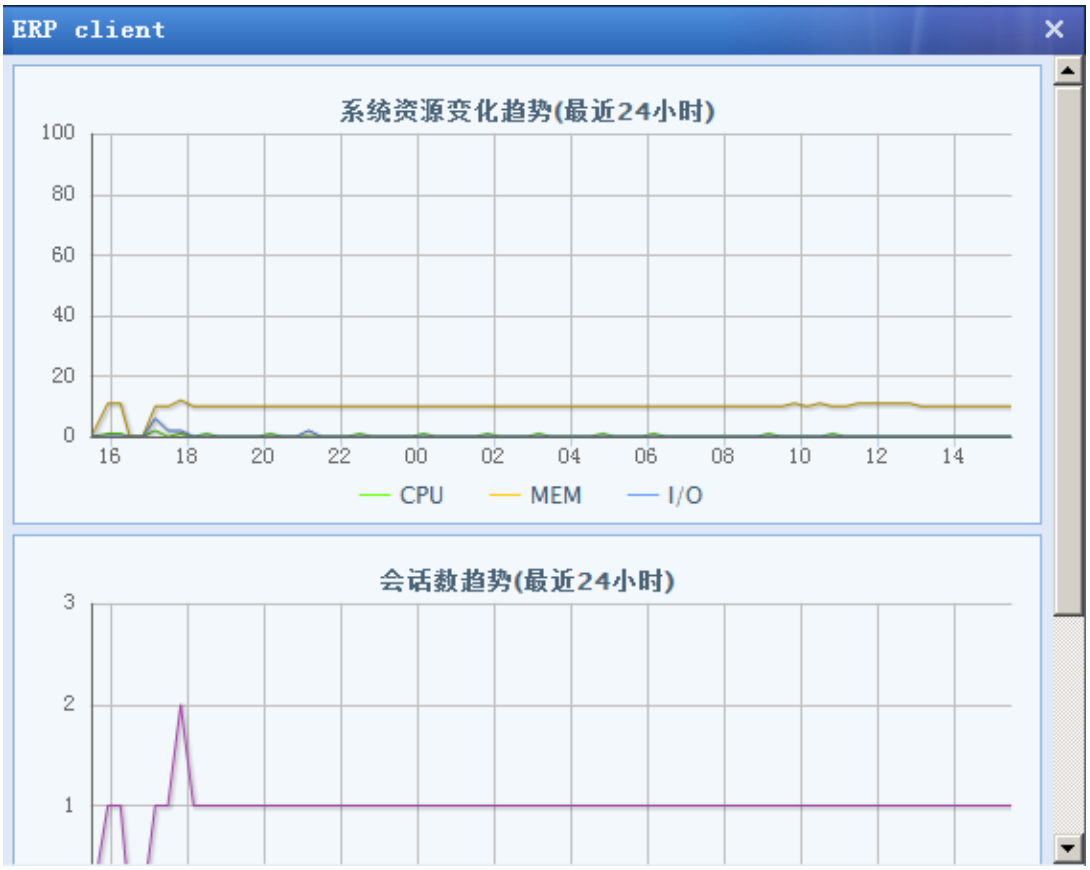

『视图』选择需要查看的状态类型，包括[服务器状态]和[应用程序连接状态]，显示如下：


[服务器状态]显示的是在『SSLVPN 配置』中『终端服务器管理』里面建立的服务器信息，显示其当前状态，如下图：


点击相应的服务器名称，能够查看该服务器上用户的使用情况，显示如下：


在远程应用服务器中，点击运行状态下的 查看，可以查看该服务器的峰值记录，如下

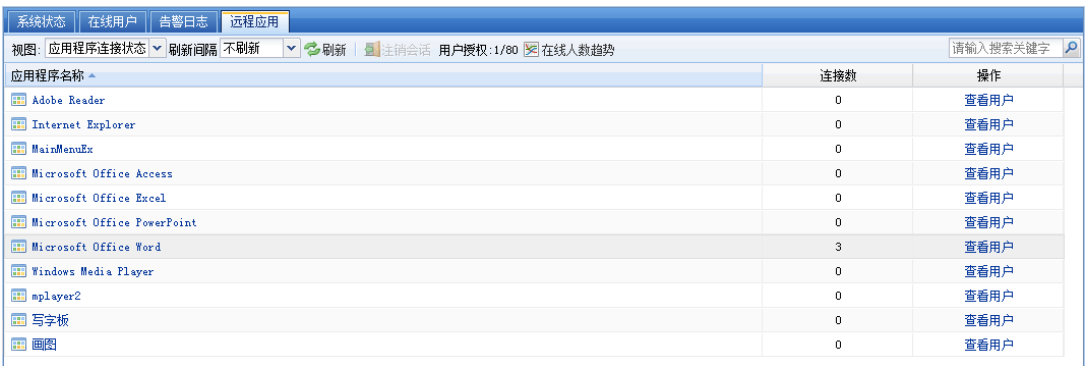
图：




在远程存储服务器中，点击运行状态下的 查看 ，可查看该服务器最近 24 小时的系统资源变化情况，如下图：


勾选相应的用户，点击 注销会话，则将用户访问该服务器的会话注销。

[应用程序连接状态]显示的是在『SSLVPN 配置』中『终端服务器管理』里面启用了的服务并且在资源里面调用后的使用情况，显示如下：




点击相应的应用程序名称或 查看用户 能够查看该应用程序的用户使用情况，显示如下：


勾选相应的用户，点击 注销会话，则将用户使用该应用程序的会话注销。

# 第2章 系统设置

『系统设置』包含『系统配置』,『网络配置』,『时间计划』,『管理员账号』,『SSL VPN 选项』五个大模块。如下图:


## 2.1. 系统配置

『系统配置』里面包含了『序列号管理』,『日期与时间』,『控制台配置』,『外置数据中心』,『设备证书』,『邮件服务器』,『Syslog』,『SNMP』的设置,如下图:


### 2.1.1. 序列号管理

『序列号管理』分为『设备序列号管理』和『模块序列号管理』。 WEBUI

路径:『系统设置』→『系统配置』→『序列号管理』。

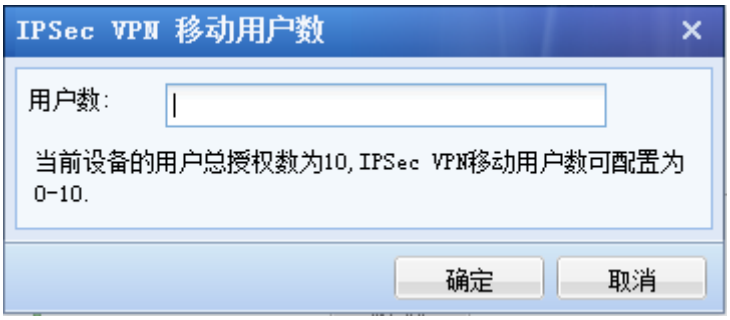
显示界面如下图:


『设备序列号管理』用于填写 SSL 设备的序列号，该序列号控制硬件网关的可用外网线路数量、IPSEC VPN 分支机构数目，SSL VPN 和 IPSEC VPN 移动用户的授权数，跨运营商模块是否启用以及软件版本升级授权。不同的序列号对应着不同线路数量和接入用户数量，填入序列号时，这些授权数会自动生成。

『模块序列号管理』用于填写 SSL 扩展功能的序列号，正确填写序列号后，相应模块的功能就开启了，可以填写的序列号有单点登录序列号，短信认证序列号，流缓存序列号，集群序列号，安全桌面序列号，单边加速序列号，应用发布序列号、应用封装序列号和企业移动管理序列号。

在跨运营商授权码后点击 激活 输入正确的序列号后，即激活跨运营商优化功能。如下图：


SSL VPN 移动用户授权和 IPSEC VPN 移动用户授权可以通用，点击 设置，可手动输入 IPSEC 的移动用户数，设置后，SSL VPN 移动用户数会相应地减少。如下图：




点击相应模块后的 修改 可修改序列号。界面如下图所示：


## 2.1.2. 日期与时间

『日期与时间』用于设定 SSL 设备的系统时间。

WEBUI 路径：『系统设置』→『系统配置』→『日期与时间』。

界面如下图所示：


在日期和时间后面可以自己设置相应的时间，点击保存则将新的设置在设备系统中保存，点击 获取本地时间 则是将设备的时间和登录设备的电脑时间同步，然后再点击 保存，使配置生效。

勾选『自动与时间服务器同步』，选择指定的时间服务器，点击 立即更新 则设备的时间将会从指定的时间同步服务器上同步过来。

点击 取消，取消当前修改。

**注意：修改时间后会重启设备的所有服务！**

## 2.1.3. 控制台配置

『控制台配置』用于设置设备的名称、控制台访问的端口、控制台超时时间以及是否允许远程维护。

WEBUI 路径：『系统设置』→『系统配置』→『控制台配置』。

界面如下图所示：


『设备名称』设备在集群时，用于分辨各设备的标识。

『https 端口』登录设备控制台的 https 端口，默认为 4430。

『http 端口』登录设备控制台的 http 端口，默认为 1000。勾选后，可通过 http 的 1000 端口登录设备控制台。

『超时时间』登录控制台后，在规定的时间内没有对控制台进行操作，即登陆超时，再操作时，需要重新登陆。

『远程维护支持』启用或禁用从外网口对设备控制台进行管理。

点击 保存，保存当前修改。

点击 取消，取消当前修改。

## 2.1.4. 外置数据中心

『外置数据中心』将系统生成的系统日志、用户日志、管理日志、告警日志等同步到外置数据中心服务器。

WEBUI 路径：『系统设置』→『系统配置』→『外置数据中心』。

界面如下图所示：


[启用外置数据中心]勾选即启用外置数据中心；

『数据中心 IP』设置相应的外置数据中心服务器 IP 地址；

『监听端口』即设备和外置数据中心服务器的通信端口，默认为 9501；

『日志同步密码』即设备和外置日志中心服务器同步日志时的密钥，设备与服务器必须相同；

点击 测试，可以测试设备与外置数据中心连接是否正常。

点击 保存，保存当前修改。

点击 取消，取消当前修改。

## 2.1.5. 设备证书

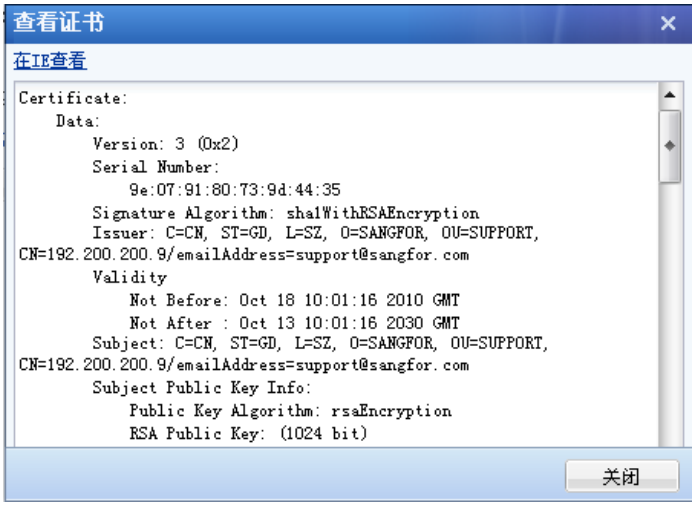
『设备证书』用于配置设备的证书，证书将用于客户端与设备建立 SSL 会话。

WEBUI 路径：『系统设置』→『系统配置』→『设备证书』。

界面如下图所示：


SSL 设备支持国际商用密码标准(RSA)和中国国家密码标准(SM2)，设备证书同时使用这两种密码标准。

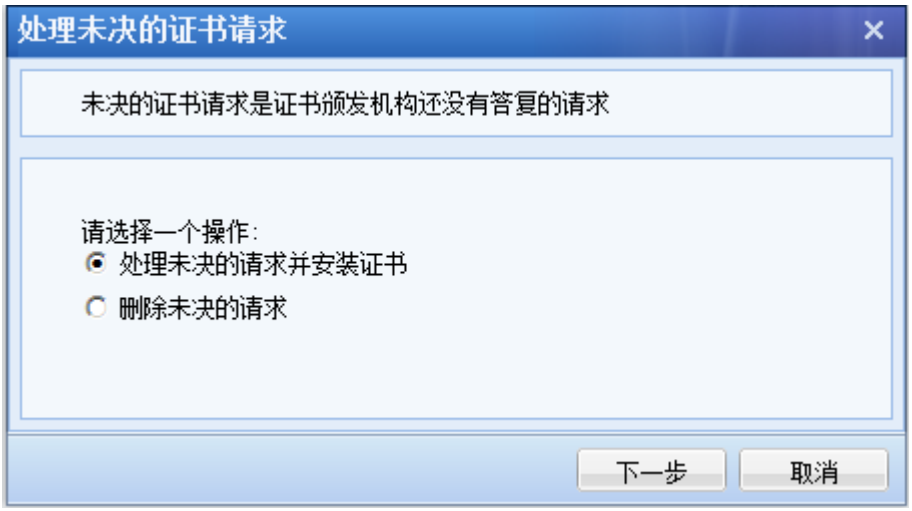
点击 查看 则可以查看设备当前的证书，显示如下：




点击 下载 则可以把设备证书下载下来。点击 更新，则可以重新导入新的设备证书，将之前的设备证书替换掉。点击 证书与 USB-KEY 认证，则会跳转到 3.4.1 章节里面的证书与 USB-KSY 认证，进行设置，后续章节将对此详细介绍。

在[为设备生成一个证书请求]下点击 下载，即新生成一个证书请求，选择证书保存路径保存证书。显示如下：


点击 处理未决的证书请求，可安装证书或删除未决的证书请求。




若选择[处理未决的请求并安装证书]，点击 下一步，需选择需要安装的证书，如下图：


点击 浏览，选择证书，并点击 完成，即完成证书安装。

**注：这里安装的证书格式类型只支持*.crt 或*.cer。**

## 2.1.6. 邮件服务器

『邮件服务器』主要针对设备的 SMTP 服务器的设置，使设备能够对外发送相关的告警邮件。

WEBUI 路径:『系统设置』→『系统配置』→『邮件服务器』。邮件发送支持中英文界面。如下图所示：


『SMTP 服务器地址』填写相应 SMTP 服务器地址，例如 QQ 邮箱的服务器地址为 smtp.qq.com；

『端口号』设置 SMTP 服务器提供服务的端口号；

『身份验证』SMTP 服务器是否需要身份验证，若需要，这在勾上此选项并且填上相应的用户名密码；若不需要，可不勾选。

『用户名』填写发送邮箱的用户名。

『密码』填写发送邮箱的密码。

『发信邮箱』填写发送邮箱的邮件地址。

点击 发送测试邮件，可以测试 SMTP 服务器是否正常，设备上面设置是否正确。

## 2.1.7. Syslog

『Syslog』用于将日志信息同步到 Syslog 服务器上。

WEBUI 路径：『系统设置』→『系统配置』→『Syslog』。


## 2.1.8. SNMP

『SNMP』用于与客户的 SNMP 管理软件或 SNMP 服务器通讯，通过 SNMP 协议管理设备内存信息等。

WEBUI 路径：『系统设置』→『系统配置』→『SNMP』。


## 2.2. 网络配置

『网络配置』包括『部署模式』,『多线路』,『路由设置』,『HOSTS』,『DHCP』,『本地子网』六部分。如下图:

## 2.2.1. 部署模式

部署模式中有两种工作模式可供选择：单臂模式和网关模式。

WEBUI 路径：『系统设置』→『网络配置』→『部署模式』。

界面如下图所示：

选择单臂模式时，需要配置内网接口（LAN 口）IP 地址、子网掩码，默认网关，配置 DMZ 口 IP 地址、子网掩码，配置 DNS。页面如下：


选择网关模式时，不仅需要配置内网接口，同时也必须配置相应的外网线路。页面如下：

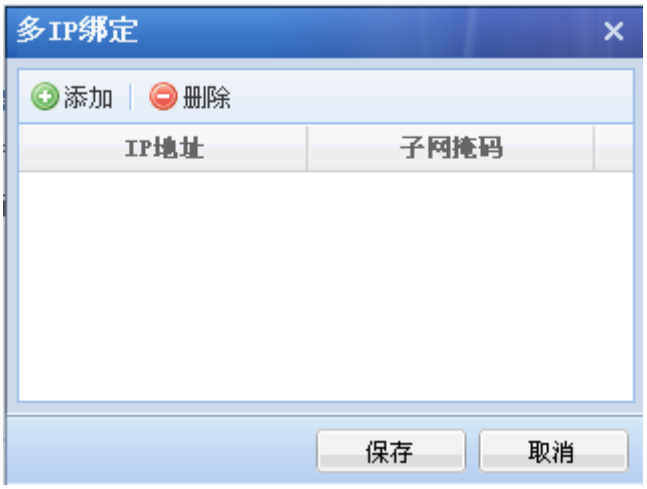

『内网接口』按照实际情况设置相应的地址和子网掩码；

在『外网接口』中，点击相应的线路名称，进入到该线路的编辑页面，显示如下：


勾起[启用该线路]即开启该线路，选择线路类型，可选择[以太网]或[ADSL 拨号连接]。

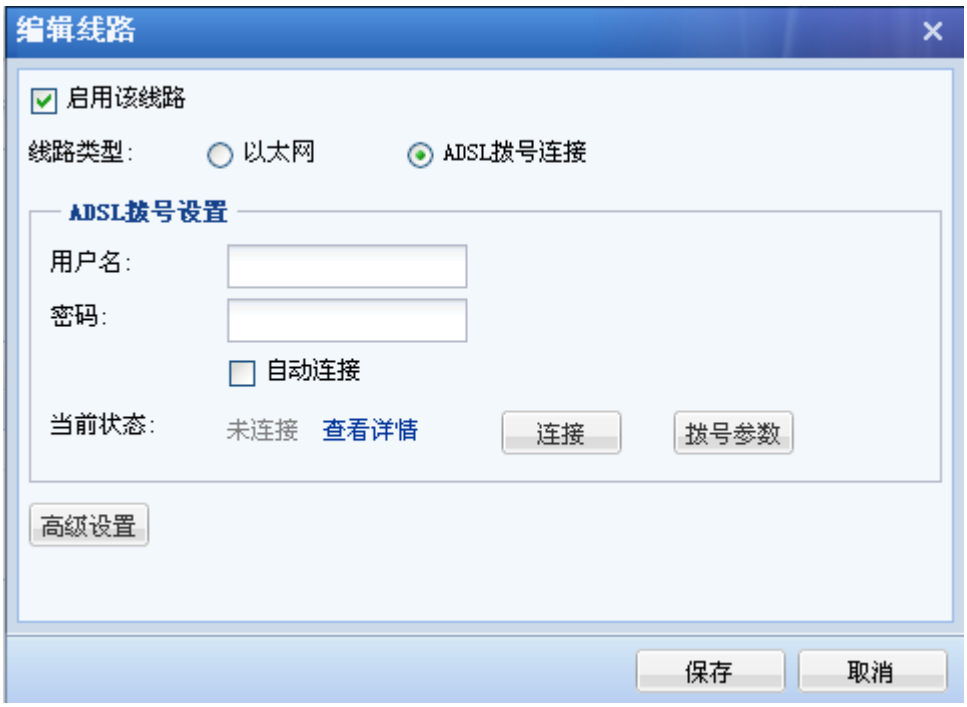
当选择[以太网]时，可以选择[自动获得 IP 地址和 DNS 服务器]，或者手动配置 IP 地址和 DNS 服务器地址，如果自动获取，则设备会从 DHCP 服务器获取相应的 IP 和 DNS 服务器地址。若选择手动配置，那需要配置相应的 IP，掩码，网关和该链路的 DNS 服务器地址。

多 IP 绑定，外网接口为以太网模式下可以启用，在设备外网接口有多个 IP 时，点击 多 IP 绑定 按钮，出现以下对话框，点击 添加，即可为 WAN 口绑定多个 IP，点击 删除，则将之前绑定的 IP 删除。页面如下：

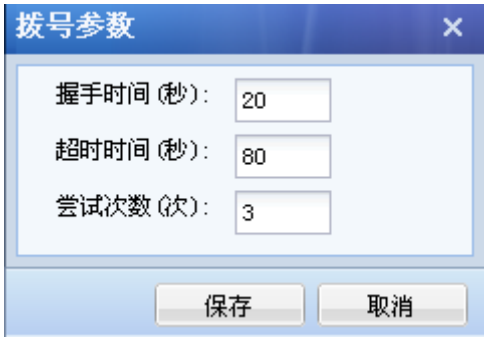



**注意：网关模式部署时 LAN 口，DMZ 口和 WAN 口的地址不能在同一网段。**

当外网线路为 ADSL 拨号时，需在『ADSL 拨号设置』中填写『用户名』和『密码』等信息，勾上[自动连接]，配置完毕点 保存 保存设置，设备将重启所有服务，重新登录后点击 连接，则以后设备再断线后就可以“自动重拨”了。当拨号出现问题的时候可以点击 查看详情，查看相应拨号信息。页面如下：




点击拨号参数可以设置拨号基本参数，一般保持默认即可。显示如下：




## 2.2.2. 多线路

『多线路』，在使用多条 WAN 口线路或者需要在单臂模式下启用多线路功能时，都需要在此处添加“多条线路”，这里可以对线路的信息进行增删和修改。

WEBUI 路径：『系统设置』→『网络配置』→『多线路』。“单臂模式”下的多线路配置页面如下图所示：


“网关模式”下的多线路配置页面如下图所示：


『IPSEC VPN 多线路传输』即在使用 IPSEC VPN 互联时，设置多线路。

勾选[启用 IPSEC VPN 多线路传输]，即开启 IPSEC VPN 多线路传输功能。

在『IPSEC VPN 多线路传输』下点击 新增，设置线路名称， 选择线路和连接模式，若公网有固定的 IP 地址，则勾选[具有固定的 Internet IP]，并配置固定的公网 IP 地址。在『故障检测设置』下设置相应的域名和 DNS 服务器地址，用于检测该线路的通讯状态是否正常。显示如下：


**1.该处设置的 DNS，主要用来检测线路的状态，线路状态是否检测，看是否勾选『启用线路故障检测』。**

**2.以上界面是网关模式下设置 IPSEC VPN 多线路的页面，在单臂模式下界面稍有不同，具体可参考案例集 10.4.4 章节**

『SSL VPN 多线路传输』可配置 SSL VPN 多线路功能。在有多条外网线路，且 SSLVPN 接入也需要使用多线路时，则可以启用该功能来提升 SSL VPN 的传输速度和接入稳定性。

勾选[启用 SSL VPN 多线路]，即开启 SSL VPN 多线路选路功能。启用多线路后，用户登录 SSL VPN 时，将会自动探测，并选择最快的线路接入。SSL 多线路选路里面添加 SSL 多线路信息。SSLVPN 多线路接入方式有两种，一种是 SSL VPN 设备网关模式部署，直接连公网，SSL VPN 用户通过设备的公网地址直接接入。另一种是 SSL VPN 设备放在内网，前面还

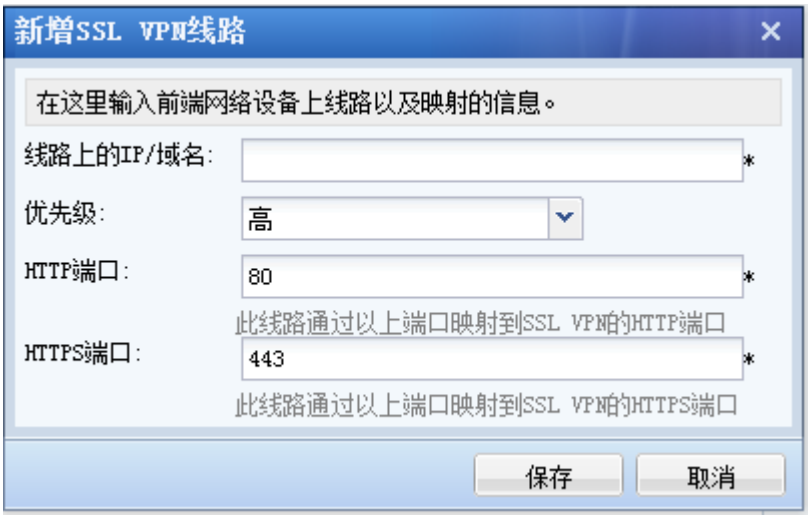
有其它的网关设备，SSL VPN 用户通过前置设备接入。需要在前端设备中将外网地址映射给我们 SSL 设备，显示如下：


点击 设置，设置线路优先级以及支持配置域名消除终端用户接入 SSL 时弹出证书告警框，界面如下：


勾选[消除浏览器安全证书告警]，填写相应线路域名，即可设置终端用户接入 SSL 时，不弹出设备证书告警框。

若选择[SSL VPN 用户通过前置设备接入]，需要添加线路，如下图：


点击 新增，设置线路的 IP/域名，选择优先级和 SSL 接入的端口，如下图：




『线路上的 IP/域名』设置的是外网链路的 IP 地址或者域名，

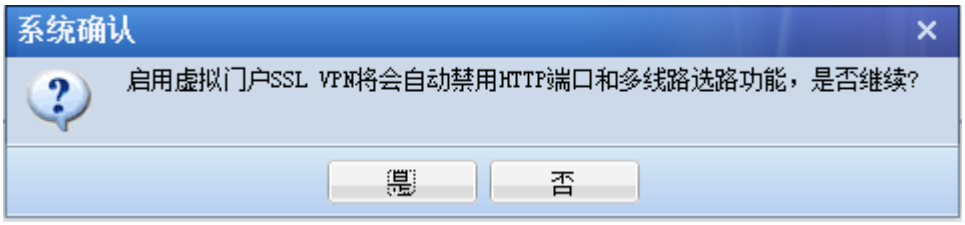
『优先级』设置该链路的等级，优先级高的链路优先被选。

『HTTP 端口』填写前置设备映射给 SSL 设备的 HTTP 端口。

『HTTPS 端口』填写前置设备映射给 SSL 设备的 HTTPS 端口。

**1.SSL VPN 设备以网关模式部署，当开启 SSL 多线路功能时，也需要开启和设置 IPSEC VPN 的多线路，SSL VPN 将引用 IPSEC VPN 里设置的多线路。**

**2.当设备在『系统配置』→『SSLVPN 选项』→『登陆策略』选择虚拟门户时，将禁用 SSL 多线路功能，SSL 多线路传输将无法启用，提示如下：**




**SSL 多线路的具体配置案例，请参考 10.1.3 和 10.1.4 章节**

『多线路-上网数据选择策略』指当 SSL 以网关模式部署，内网用户上网也需要使用多线路选路。用户上网的选路策略分为以下四种，如下图：


[按每条线路的剩余下行带宽优先选择线路]，系统自动根据每条线路的剩余带宽（下行带宽）自动选择剩余带宽较大的线路，充分利用剩余带宽；

[按每条线路的剩余上行带宽优先选择线路]，系统自动根据每条线路的剩余带宽（上行带宽）自动选择剩余带宽较大的线路，充分利用剩余带宽；

[平均分配所有连接到每条线路]，系统把所有的连接平均分配到每条线路，此时不考虑每条线路的剩余带宽；

[优先选择前面的线路（有利于 VPN 部署）]，默认使用最先启用并且是有效的线路，当该线路断线或者不可用时，自动切换到下一条可以使用的线路；

## 2.2.3. 路由设置

对需要 SSL 硬件网关转发的数据（VPN 或非 VPN）及 SSL 硬件本身需要转发的数据进行的路由。『路由设置』主要用于实现两种功能：1、代理多网段上网时添加回包路由。2、访问 VPN 内部多子网时需要设置路由。

WEBUI 路径：『系统设置』→『网络配置』→『路由设置』。

界面如下图所示：


点击 新增，选择[新增路由]和[批量新增路由]，显示如下：


选择[新增路由]，可添加一条路由，如下图：


[目标网段]路由指向的目标地址段。

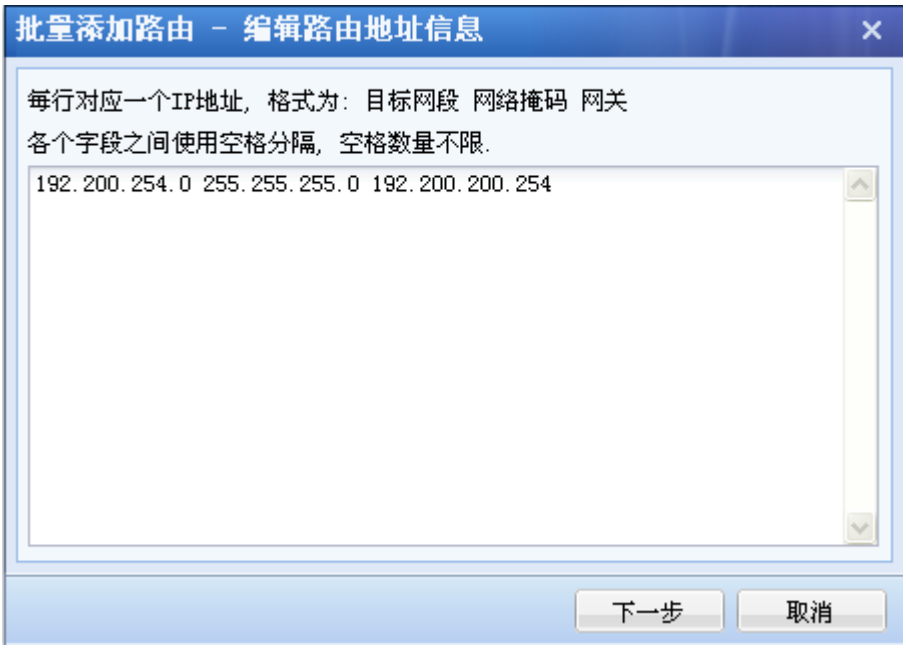
[网络掩码]目标地址段的子网掩码。

[网关]到达目标地址段的下一跳地址。

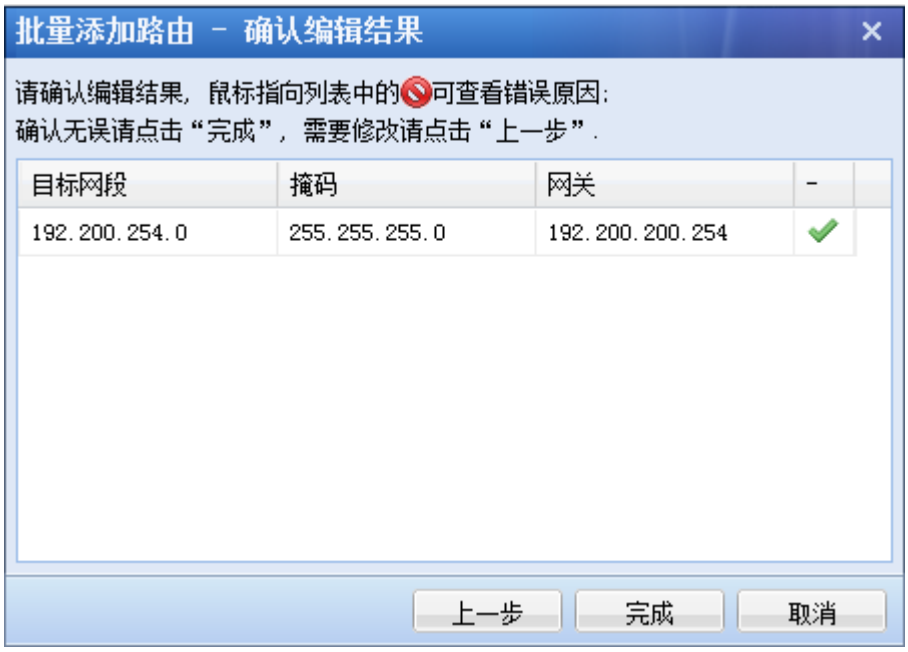
点击 保存并继续添加，可继续添加路由。

点击 保存，即保存配置。

选择[批量添加路由]，可一次性添加多条路由，如下图：




点击 下一步，确认路由信息是否正确，若正确，点击 完成，保存配置。如下图：




## 2.2.4. HOSTS

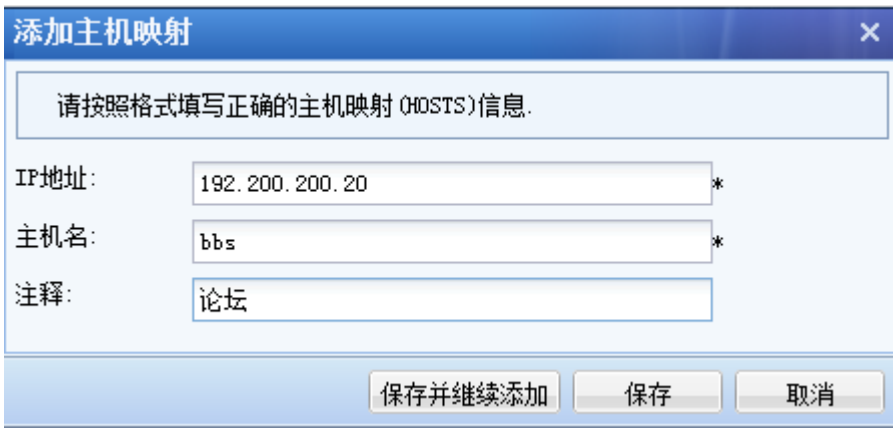
『HOSTS』用于定义 SSL VPN 硬件设备内置的 host 表，以解决 SSL VPN 用户需要通过域名或机器名来访问内网资源的问题，常用于 SSL VPN 设备内网有“域”的情况下。这里可以定义“域名”或“机器名”所对应的主机 IP。

WEBUI 路径：『系统设置』→『网络配置』→『HOSTS』。

界面如下图所示：


点 新增 按钮可选择[新增主机映射]或[批量新增主机映射]。显示如下：

选择[新增主机映射]，弹出【添加主机映射】对话框，如下图所示：

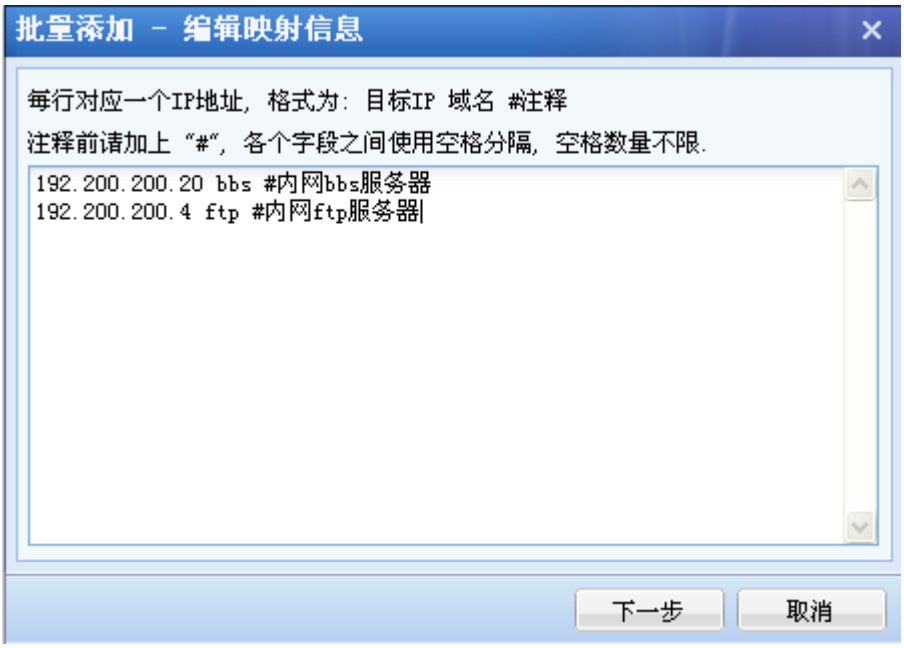



『IP 地址』需要添加映射的 IP 地址。

『主机名』该 IP 对应的主机名称。

『注释』对该 IP 地址对应主机地址的注释。

HOSTS 也可以批量设置，选择[批量新增主机映射]，格式如下：



## 2.2.5. DHCP

在『DHCP』中可以查看『DHCP 状态』和进行『DHCP 设置』。如下图：

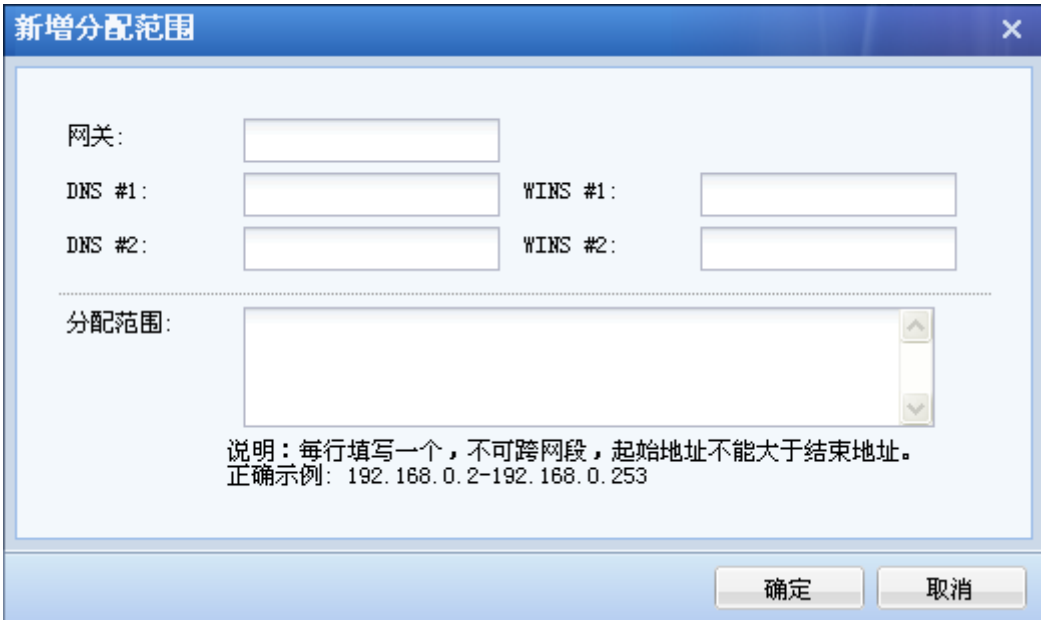

『DHCP 状态』可以查看 DHCP 服务运行状态和地址分配情况。点击 刷新 按钮，可以列出当前已经分配出去的 IP 地址及其所对应的计算机名称，MAC 地址，网口，剩余租期等信息。

选择『DHCP 设置』可以设置 DHCP 分配的信息，如下图所示：


『DHCP 服务』：可选择[启用]或[禁用]。

『地址租期』：设置 DHCP 地址的租用时间。

在分配范围中，点击相应的网络接口，对该接口设置 DHCP 分配，设置需要分配的 IP 网段、网关、DNS 服务器地址。显示如下：




**注意：1、假如内网机器某些电脑设置了固定私网 IP，这里填写的 IP 地址范围不要包含已使用的 IP，以免随机分配 IP 时产生 IP 冲突。**

**2、一般情况下 IP 地址范围不要把末尾为 0 和 255 的地址加上，这两个是网络地址和本网段广播地址。**

『预留 IP 地址』用于设置为某些计算机保留分配固定的 IP，可根据 MAC 地址或计算机名来预留 IP。点击下面的 新增 按钮，出现【新增 DHCP 保留 IP】编辑框，页面如下：

『网络接口』选择相应的 DHCP 的网络接口。

『预留 IP 地址』设置需要预留的 IP 地址，预留给相应 PC。

点击 获取此计算机信息 则可以获取到相应计算机 mac 和计算机名。

[MAC 地址]需要使用预留 IP 地址的电脑的 MAC 地址。设置后，可根据该 MAC 地址来分配预留 IP。

[计算机名]需要使用预留 IP 地址的电脑的计算机名。设置后，可根据该计算机名来分配预留 IP。

## 2.2.6. 本地子网

当 SSL 硬件网关内网有多个子网的情况下，SANGFOR IPSEC VPN 接入用户需要与总部内网的其它子网互访时，需要设置本地子网。

WEBUI 路径：『系统设置』→『网络配置』→『本地子网』。

界面如下图所示：

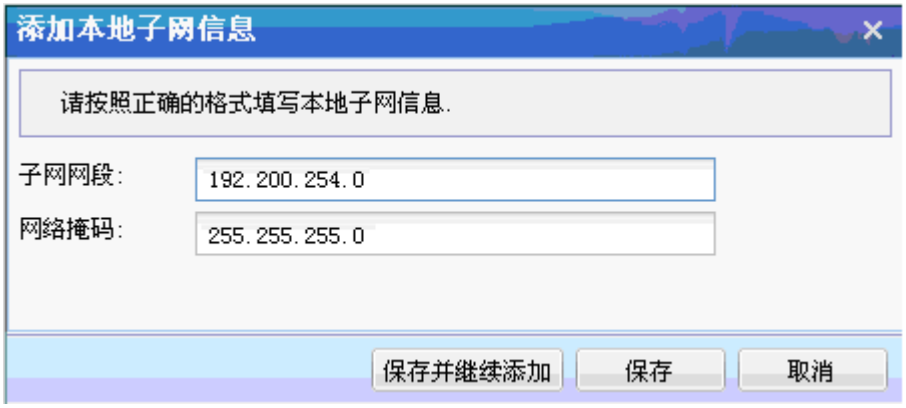

点击 新增，可[选择新增本地子网]或[批量新增本地子网]，如下图：


例，总部有两个子网（192.200.200.x、192.200.254.x），192.200.200.x 为设备 LAN 口所在的网段，192.200.254.x 为内网其它网段，通过在“本地子网”中添加 192.200.254.X，可实现

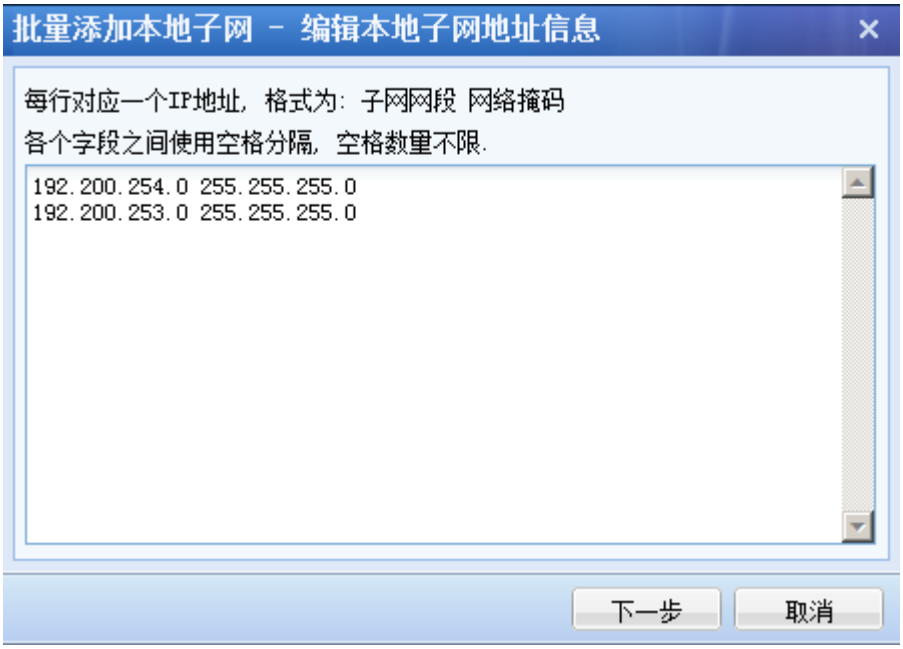
分支、移动用户连上总部后，访问 192.200.254.x 网段。具体配置如下：

点击 新增，选择[新增本地子网]，如下图：


然后填写需要添加的子网网段，并点击 保存，如下图：




当有多个网段需要添加时，可选择[批量新增本地子网]，如下图所示：



**1.这里的『本地子网』仅相当于一种"声明"作用，在此定义的网段，都会被我们的 SANGFOR IPSEC VPN 设备和软件客户端视为 VPN 网段，所有访问这些网段的数据包经过 SANGFOR IPSEC VPN 设备或软件后，都会被封装到 IPSEC VPN 隧道中传输。所以，一般情况下，在『本地子网』里添加了子网网段，都需要配合『系统路由设置』来完成对多子网的访问。**

**2.添加本地子网时，可以包含设备 LAN 口所在的网段，但在实际下发策略时，设备会自动去掉该网段，以保证数据通讯正常。**

## 2.3. 时间计划

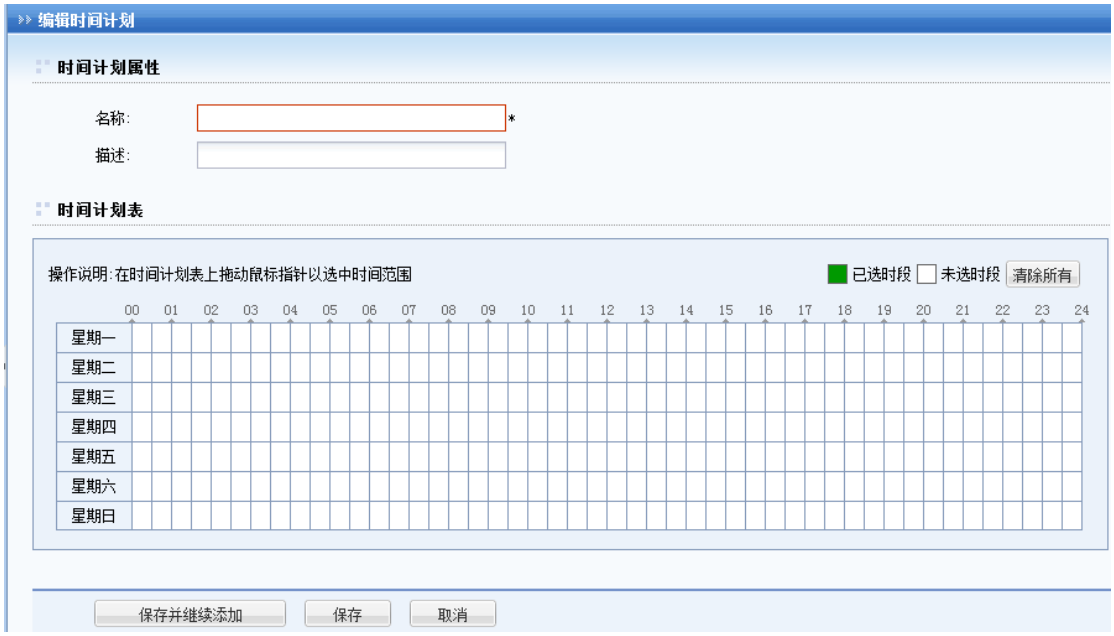
『时间计划』用于定义常用的时间段组合，这些时间组合可在『VPN 有效时间』、『防火墙过滤规则设置』、『用户权限设置』和『端点安全规则』中使用，以设置相应的规则生/失效时间，该时间以设备当前时间为准。

WEBUI 路径：『系统设置』→『时间计划』。

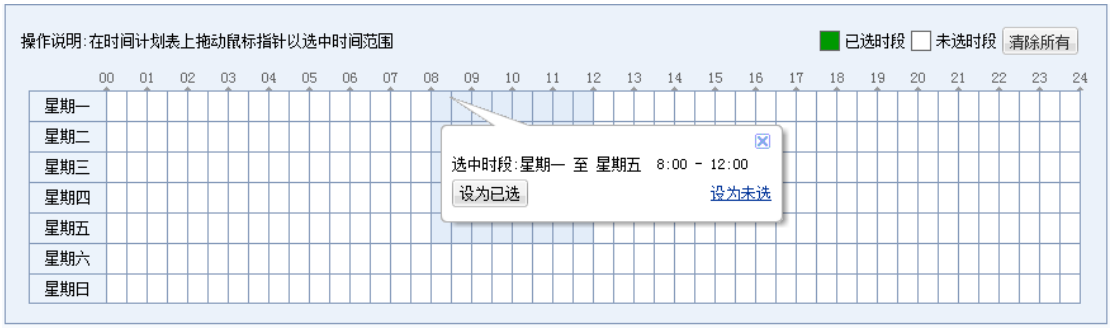
界面如下图所示：


例如需要定义：每周一至周五 8:00-12:00，14:00-18:00 为上班时间，配置方法如下：

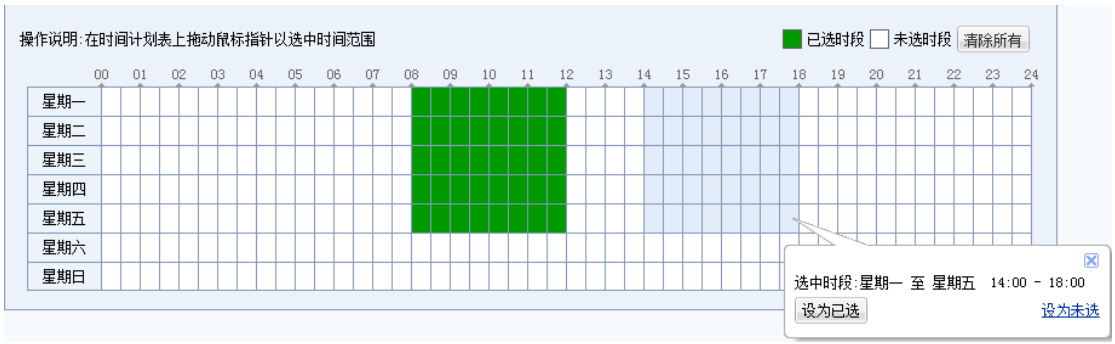
首先在时间计划里面点击 新建，如下图所示：



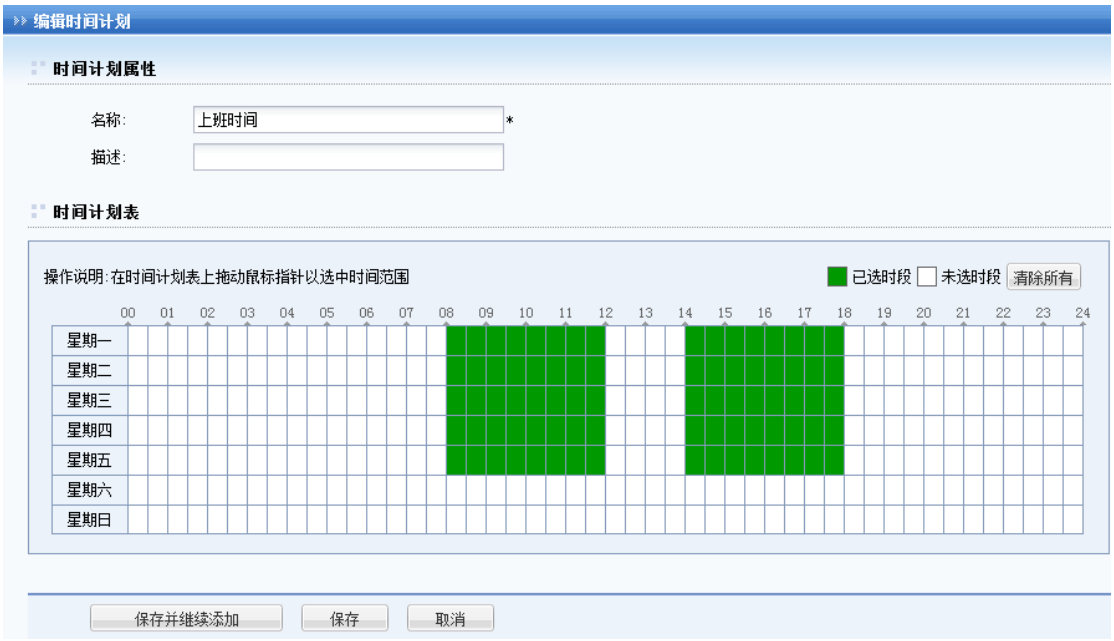

设置名称为“上班时间”，在时间计划表里面选择相应的时间小格，本例中先选中周一至周五 8:00-12:00 的小格，选择时间小格后会弹出选中时段的提示框，选择 设为已选，如下图所示：



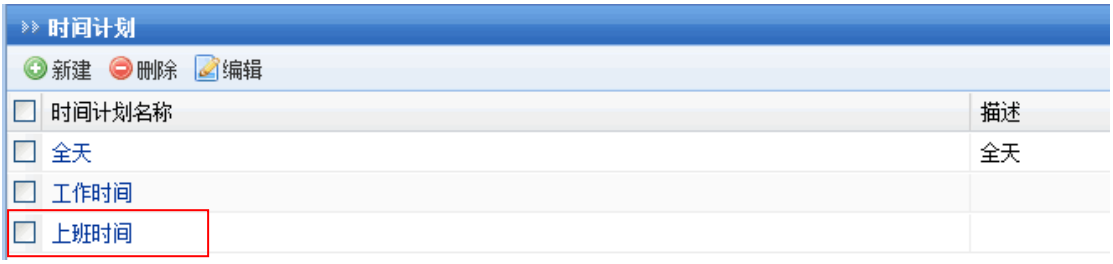

然后用同样的方法选择周一至周五 14：00-18：00 时间段，如下图：



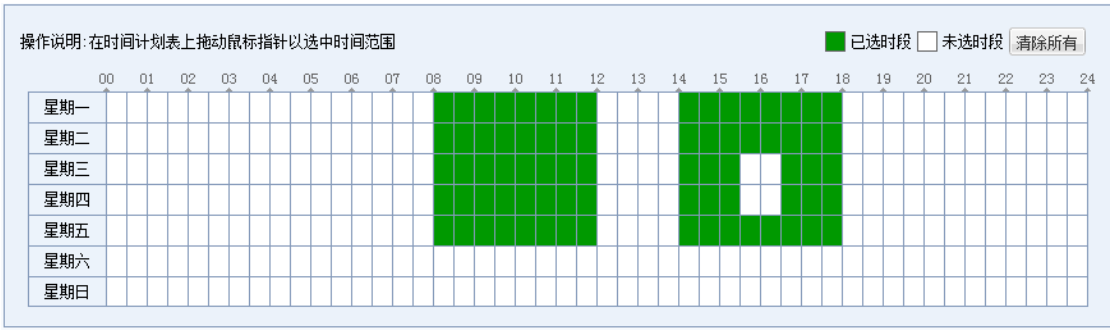
都设置完以后，即完成该例中“上班时间”的定义。




点击 保存 即可。设置完成后显示如下：

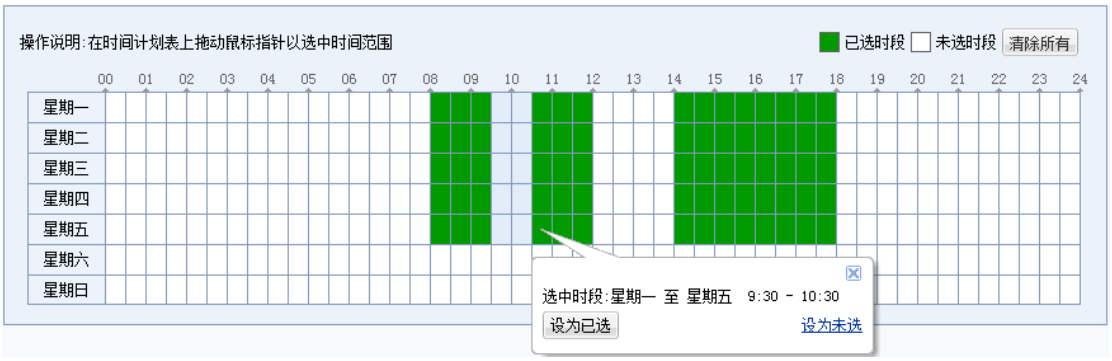



如果在时间计划中，需要删除某一个时间小格，直接点击该绿色小格，变成白色即可。绿色表示“已选时段”，白色表示“未选时段”。如下图所示：




如需在时间计划中删除某一段时间，则勾选该段时间小格，点击 设为未选 即可，如

下图所示：



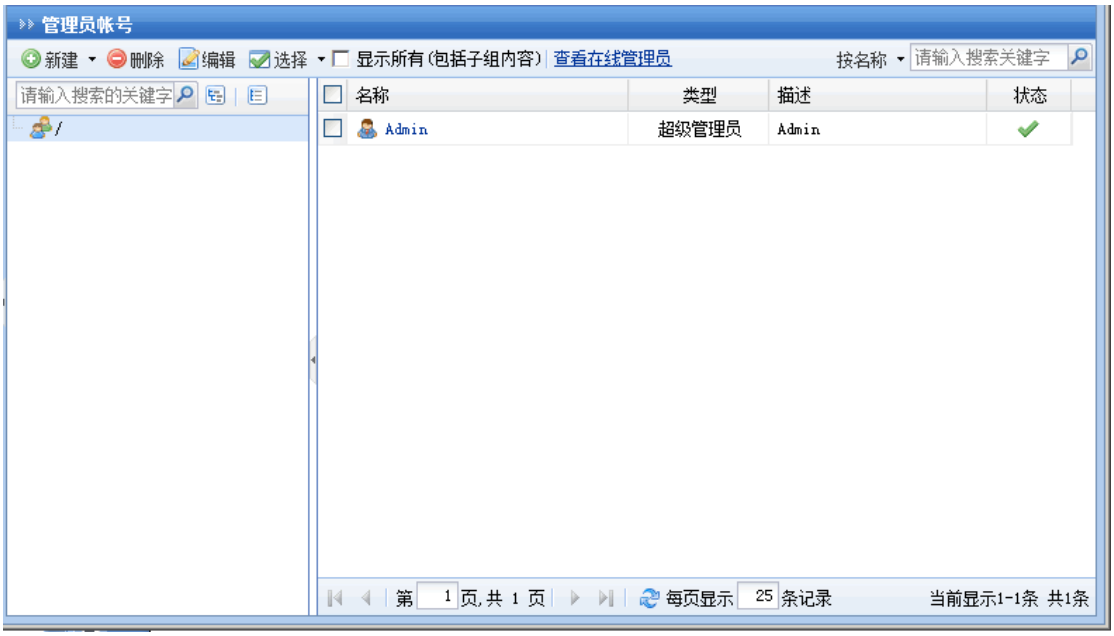

**此处只是定义一个时间计划，然后再在 『VPN 有效时间』、『防火墙过滤规则设置』、『用户权限设置』、『端点安全规则』等设置中来引用该时间计划，引用的时候，只需要选择相应的时间计划名称即可。**

## 2.4. 管理员账号

『管理员账号』用来设置登陆设备的管理员账号和密码等信息，可以把管理员归纳成管理组，并对管理员和管理组分配不同的权限。

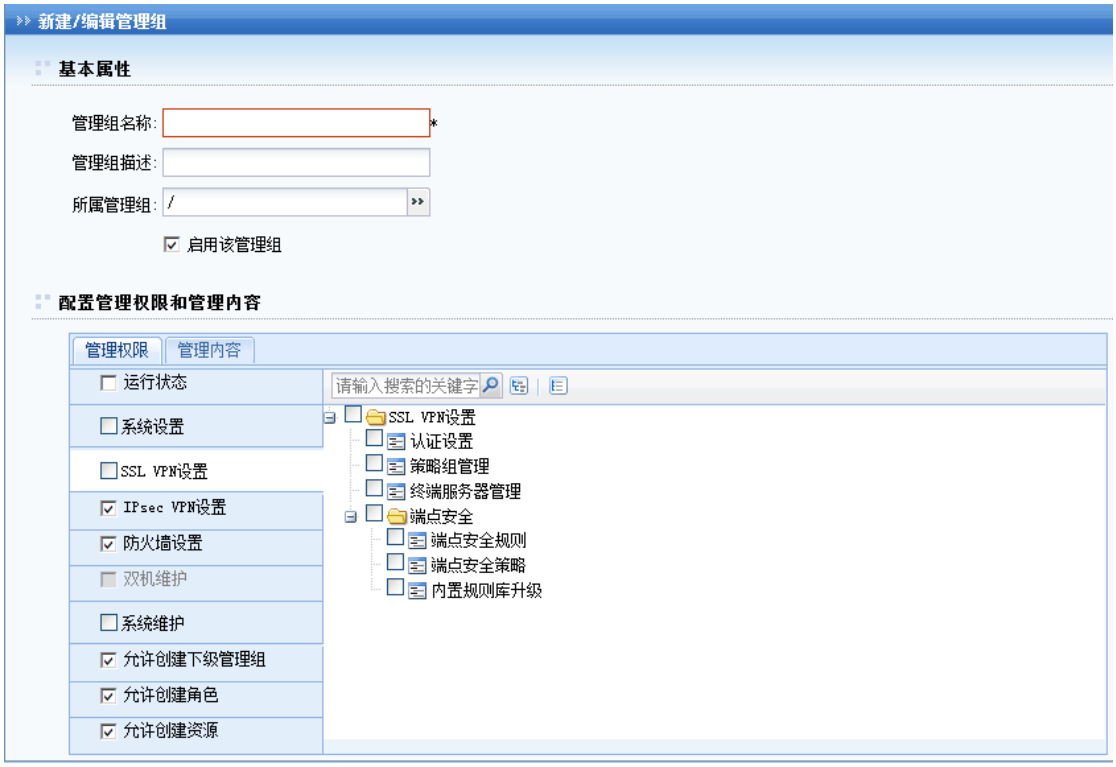
勾选[显示所有（包括子组内容）]即可显示出左边目录树所选中的组及该组下的子组的管理组和管理员信息。

选中管理员或者管理组，点击 编辑，即可对该管理员或管理组进行编辑。点击 删除，即可把选中的管理员或者管理组删除。显示如下：




点击 新建 后会出现[管理员]和[管理组]的选项，显示如下：


选择[管理组]后，可新建一个管理组并设置该管理组的权限。显示如下：

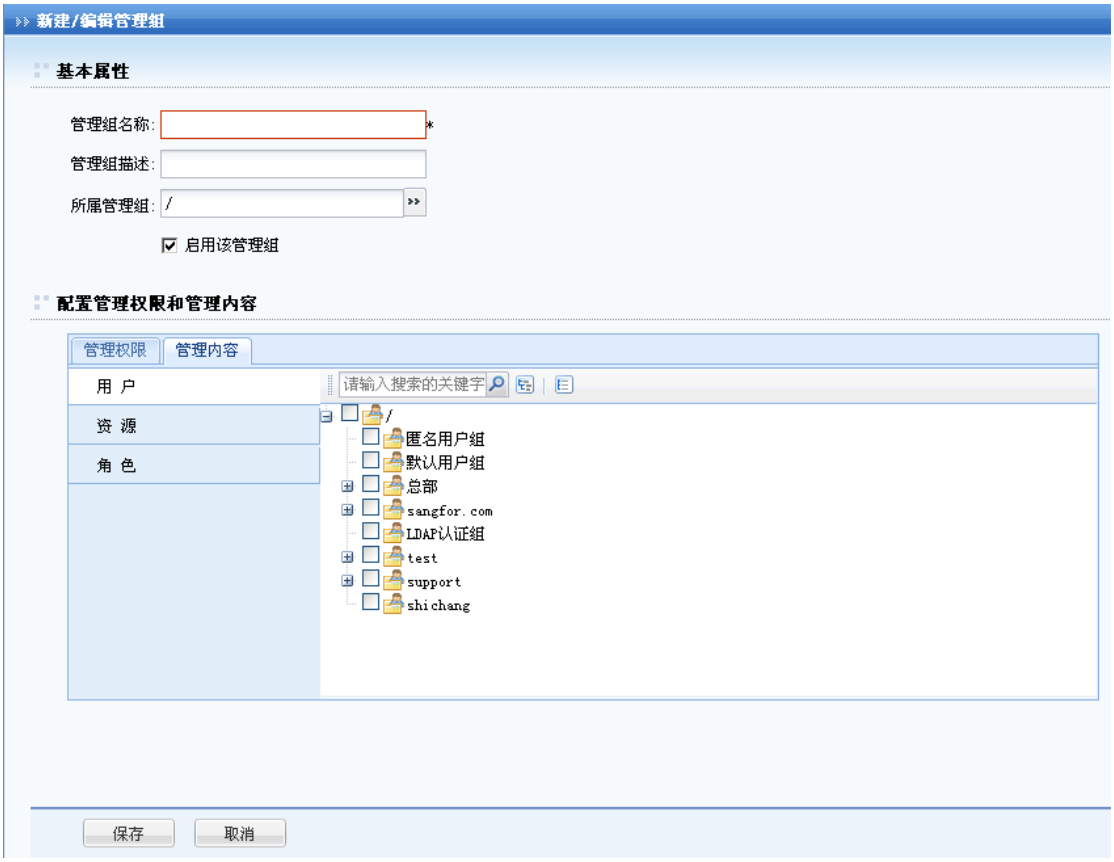



『管理组名称』和『管理组描述』可自定义。

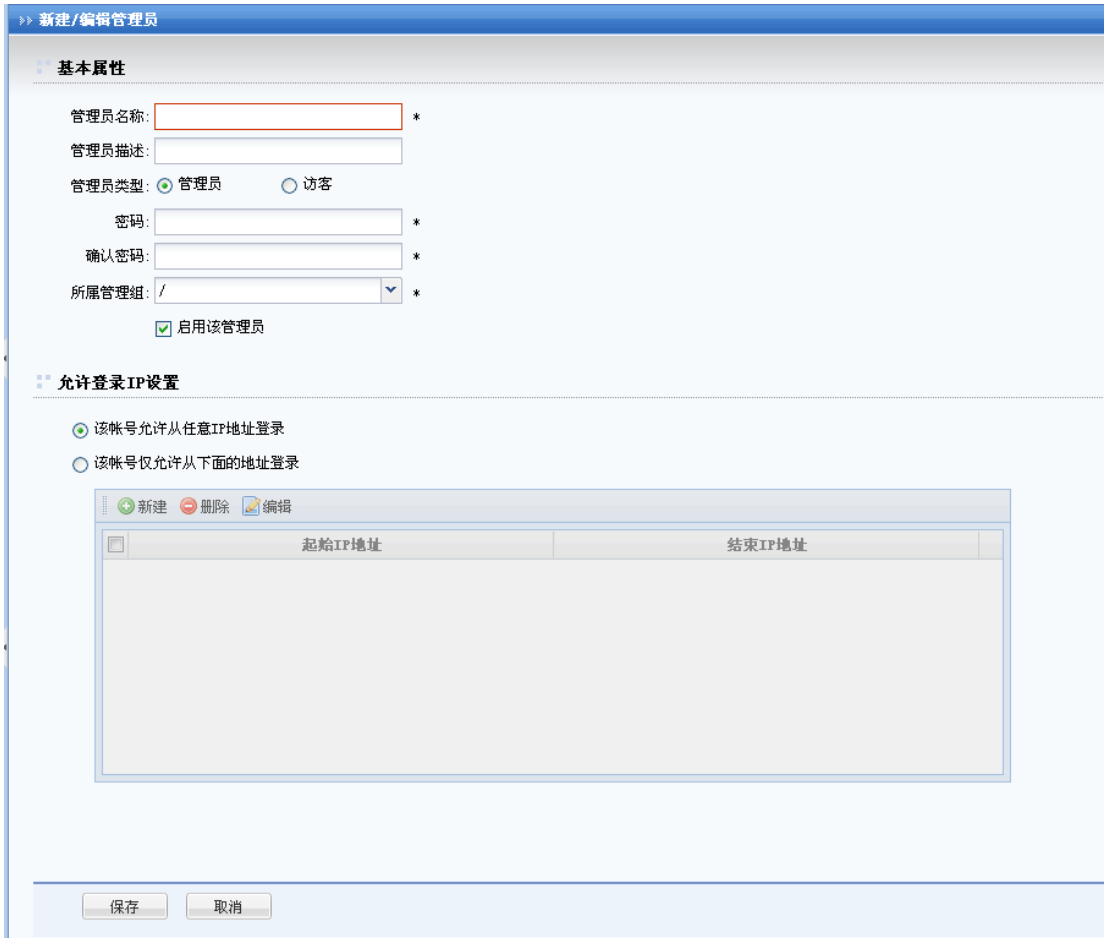
『所属管理组』：选择该管理组所属的组，若是在根组下建管理组，则保持默认即可。

【管理权限】里面可以设置该组成员能够管理设备的权限，只需在相应模块后打勾即可。

选择【管理内容】，即可对该组管理员管理的内容进行限制。包括用户，资源和角色的管理。显示如下：




点击新建 管理员，出现如下设置页面：




『管理员名称』即管理员登录 SSL 设备控制台时所使用的帐号。

『管理员描述』设置该管理员的相关说明信息，可任意填写。

『管理员类型』分为[管理员]和[访客]，管理员对设备配置具有相应组的管理权限；访客只具备只读权限，只能看相应组权限下的设置信息。

『密码』和『确认密码』用于设定管理员登录的密码。管理员密码会自动进行复杂度检测，不能设置简易密码。

『所属管理组』设置此管理员所属的管理组，选择后可匹配相应组的权限。

『允许登录 IP 限制』可以设置使用此管理员帐号登录 SSL 设备的 IP 地址。若设置了登陆 IP 限制，那么在 IP 列表外的地址将不能使用该账号登陆 SSL 设备。

**管理员密码需要同时符合以下策略：**

1. **长度至少为 8 位**
2. **密码中不能包括管理员用户名**
3. **必须包含数字、小写字母、大写字母和特殊字符中的任意两项。**

**注意：下级管理组的管理权限不会比上级管理组还多。即下级管理组的可管理的用户、资源、角色均由上级管理组授权，不会超出这个范围。**

## 2.5. SSL VPN 选项

『SSL VPN 选项』包括『系统选项』、『网络传输优化』、『登录策略』、『集群部署』、『分布式部署』五部分，界面如下图所示：


### 2.5.1. 系统选项

本页面列出了 SSL VPN 常用的基础配置项目，管理员可以在此页面中对常用的配置项目做全局性的配置。包括『接入选项』、『客户端选项』、『虚拟 IP 池』、『内网域名解析』、『单点登录设置』和『资源服务选项』六个标签页。如下图所示：


## 2.5.1.1. 接入选项

『接入选项』用于设置 SSL 设备的登陆端口和登录的方式，是否启用 PPTP/L2TP 接入服务， SSL/TLS 协议设置，webagent 设置以及是否启用防中间人攻击。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『接入选项』。

界面如下图所示：

『用户访问入口』里设置 SSL VPN 服务监听端口。

『HTTPS 端口』设置 HTTPS 的监听端口，默认值为 TCP 443 端口。点击 设置端口 进行 HTTPS 监听端口设置，可设置多个端口。也可以手动输入多个端口，用逗号隔开。

[启用 HTTP 端口]设置 HTTP 的监听端口，默认值为 TCP 80 端口。当在『登录策略』中选择『虚拟门户』时，不能启用 HTTP 端口。

**1.如果更改了这些标准的协议端口，则访问 SSL 登录页面时，需要在主机地址后面加端口来登录，所以，如无必要，请勿修改。**

**2.[启用 HTTP 端口]勾选后，则用户可以通过 http 协议跳转到 https 协议，与 SSL VPN 网关交互，例如访问：http://202.96.137.75可以自动跳转到 https://202.96.137.75。否则只能通过 https 协议交互，如 https://202.96.137.75。**

『PPTP/L2TP 接入设置』里设置 PPTP 和 L2TP VPN 接入功能。

[接入方式]可设置不允许使用 PPTP 和 L2TP 接入，使用 PPTP 接入和使用 L2TP 接入服务。[启用 PPTP 接入服务]勾选后，即开启 PPTP 接入功能。手机用户可通过 VPN 接入并访问 L3VPN 资源。[使用 L2TP 接入服务]勾选后，设置共享密钥，手机用户可通过系统自带的 L2TP VPN 接入并访问 L3VPN 资源。

PPTP/L2TP 接入用户可以选择到 MS ActiveDirectory 认证服务器上认证，前提是还需要在设备上进行如下配置：

1. 点击 LDAP 认证页面，配置一个类型为 MS ActiveDirectory 的认证服务器，使 SSL VPN 设备能够连接到该服务器进行认证。

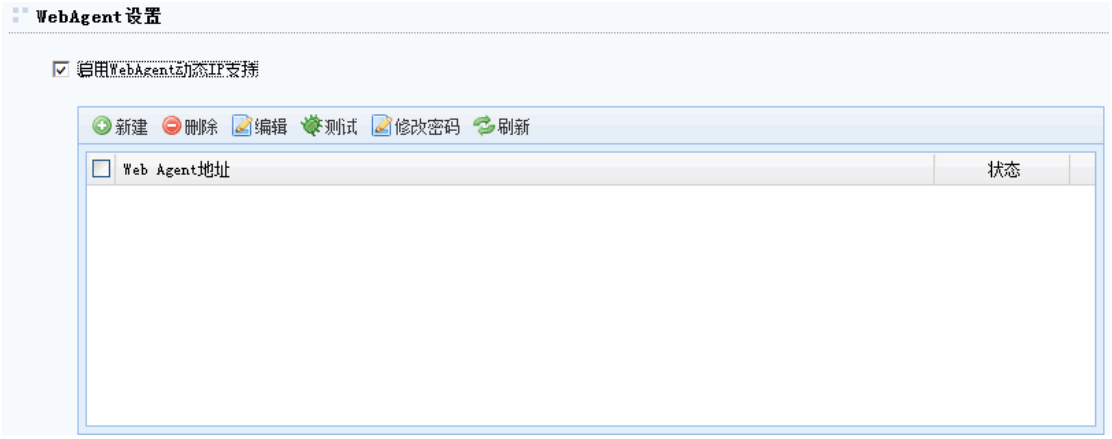
2. 点击 域配置页面，将 SSL VPN 设备加入 MS ActiveDirectory 认证服务器所在的域，才能到域服务器进行认证。

**如果启用 L2TP 接入服务，则自动关闭 SSL 设备的标准 IPSec VPN 用户接入，但是 SANGFOR IPSec VPN 接入不受影响。**

『SSL\TLS 协议设置』该选项设置 SSL VPN 用于数据加密的加密协议算法标准，包括国际商用密码标准(RSA)和中国国家密码标准(SM2)，默认为国际商用密码标准。

『Webagent 设置』当 SSL VPN 网关设备在没有固定公网 IP 的情况下，需要建立 SSL VPN，必须使用 WebAgent 动态寻址。

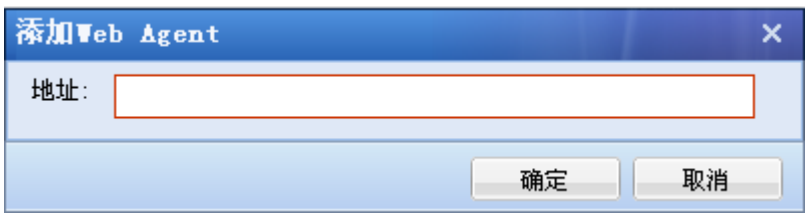
勾选『启用 WebAgent 动态 IP 支持』，即启用 WebAgent 动态寻址功能。可以在这里新增/删或修改 WebAgent，如下图所示：



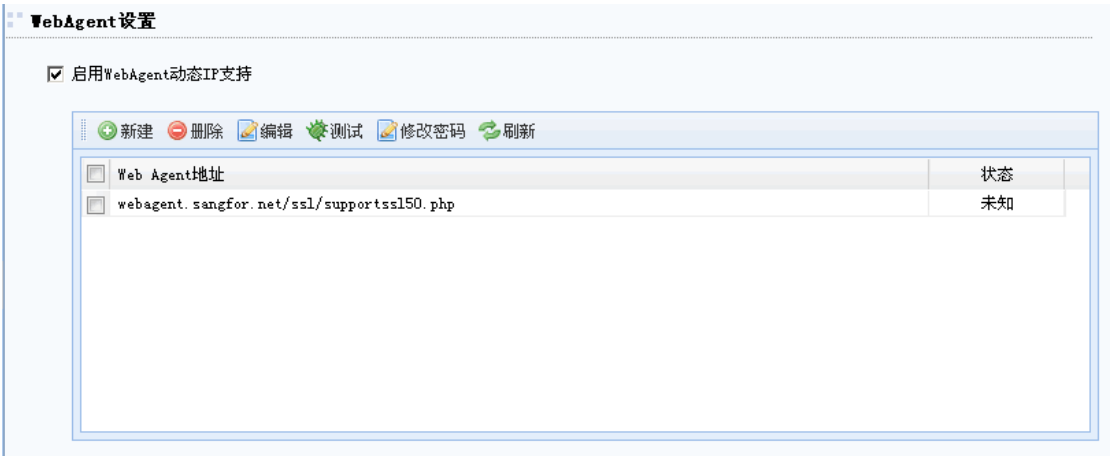

『Webgent 地址』用于显示 Webagent 地址。

『状态』显示当前 Webagent 的状态。

点击 新建 即可新增一条 Webagnet。点击后如下图：




在弹出的输入框中输入申请到的 Webagent 地址，点击 确定 。




勾选相应的 webagent 地址，点击 测试，如果弹出如下框的提示，证明填写正确。


勾选相应的 Webagent 地址，点击 删除 或 编辑 可以进行删除或编辑 webagent 地址。

勾选相应的 Webagent 地址，点击 修改密码 可以设置 Webagent 网页的密码，以防止非法用户往 Webagent 网页更新虚假 IP 地址。

点击 刷新，可以刷新 Webagent 的当前状态。

『防中间人攻击设置』用来防止通信的数据被非法用户篡改和窃取。

『启用防中间人攻击』勾选后，用户登录时强制启用图形校验码，并且会强制安装控件。配置界面如下图所示：

## 2.5.1.2. 客户端选项

『客户端选项』用于设置客户端组件策略以及客户端的功能模块的开启。

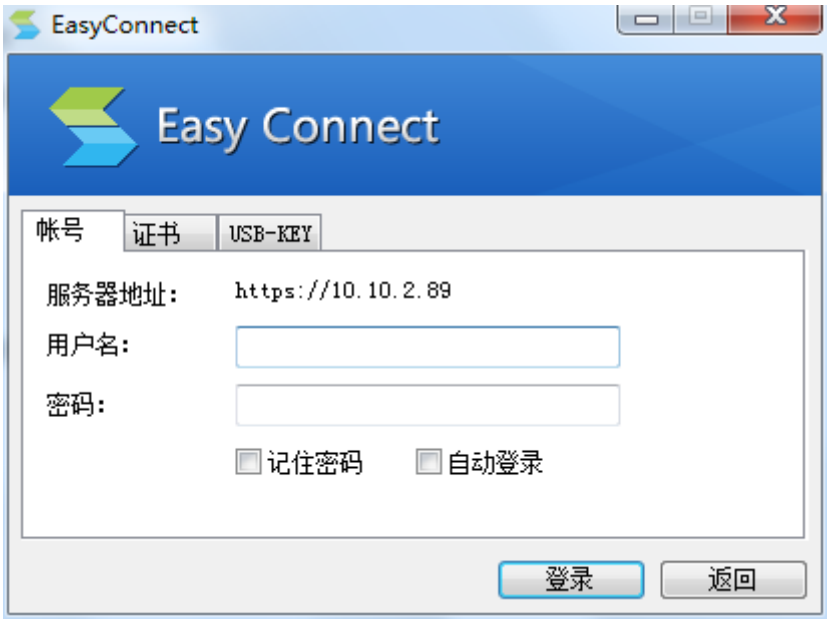
WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『客户端选项』。

界面如下所示：


『启用系统托盘』勾选后客户端登录会在系统托盘处显示 VSP 客户端图标。

『允许客户端保存密码』勾选后客户端登录可以选择是否保存密码。

『允许客户端自动登录』勾选后客户端登录可以选择自动登录，该选项依赖于『允许客户端保存密码』。



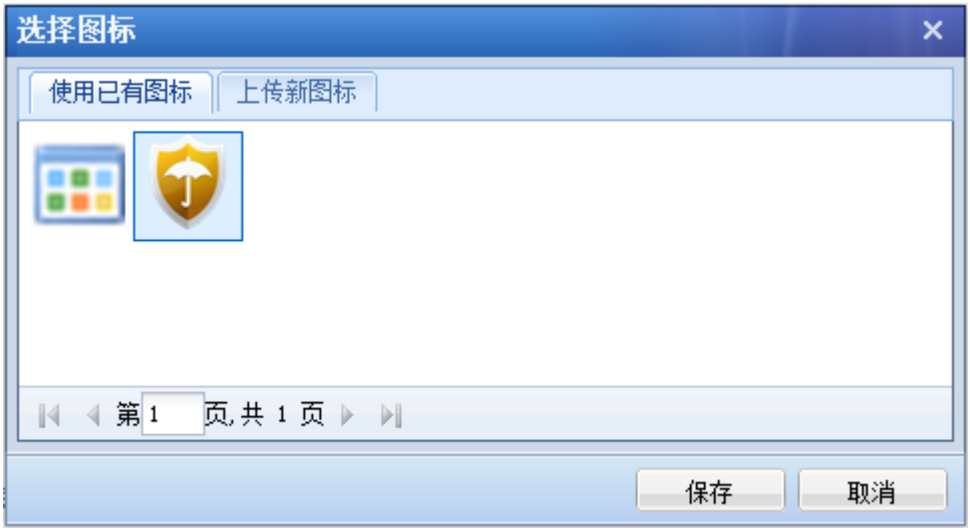

『允许客户端永久在线』连接断开后，会无限次尝试重连，通常用于无人值守的终端。

『自动安装 TCP、L3VPN 应用组件』勾选后客户端登录会自动进行组件安装，否则会提示用户是否安装启用控件。

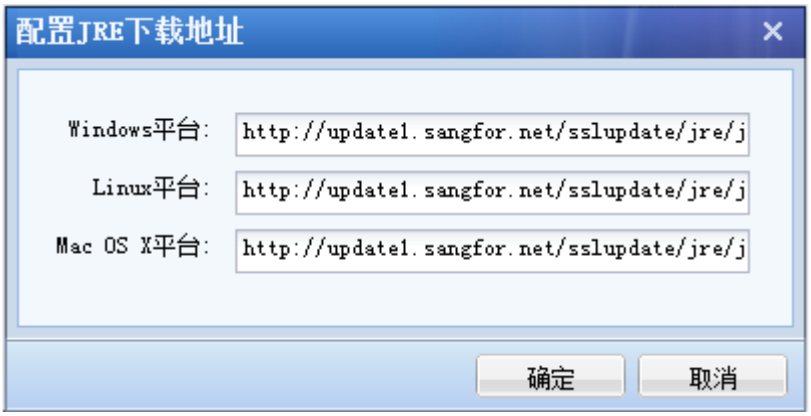
『TCP、L3VPN 服务显示主机地址』勾选后资源页面会显示各资源对应的主机地址，否则只显示资源名称。

『CS 客户端登陆后显示资源列表』勾选后 CS 客户端登陆的用户，登陆成功后会显示关联的资源列表。

『Windows 快捷方式图标』是客户端登录后在桌面自动创建的快捷方式图标，以及系统托盘的图标。点击时可以选择【使用已有图标】或者【上传新图标】。



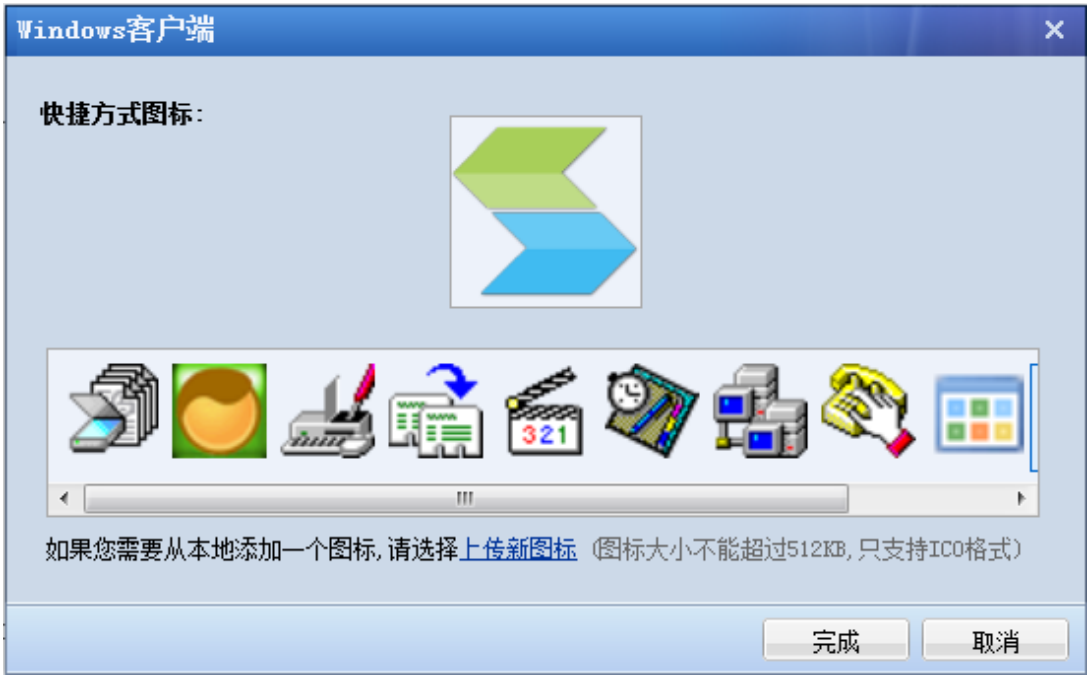

在非 IE 浏览器且非 Google Chrome 浏览器下，用户访问 TCP 应用 ，L3VPN 资源时，需要下载并安装 JRE，点击 配置 JRE 下载地址，弹出编辑框，如图所示：




在『Windows 平台』、『Linux 平台』和『Mac OS X 平台』后面的输入地址，非 IE 浏览器登陆 SSL VPN 时，根据此地址下载 JRE 安装包。

『个性化设置』用于设置各个场景下客户端的自定义设置。包括 Windows 客户端、移动客户端和安全桌面下的设置。

『Windows 客户端』设置用于修改 Windows 客户端的快捷方式图标，如下图：




『移动客户端』用于设定移动客户端（手机、平板等）使用 EasyConnect 登录界面的图片，如下图所示：


『安全桌面』可根据需要来设定安全桌面标题和桌面壁纸，配置页面如下：


[安全桌面标题]用于设置用户启用安全桌面功能后，登录安全桌面的标题。

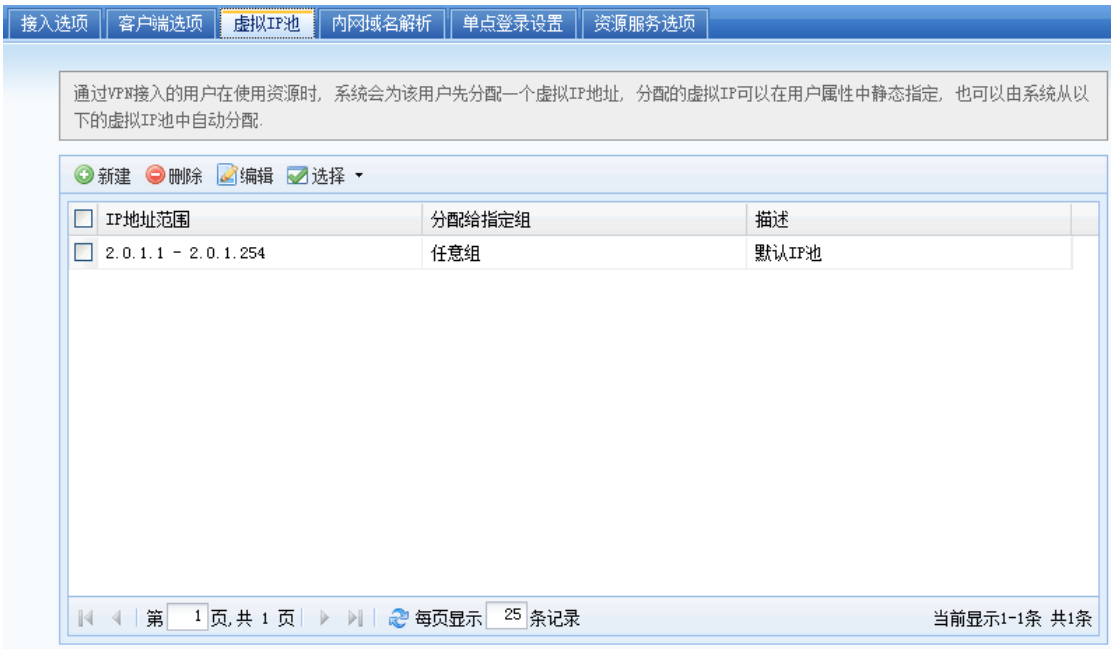
[安全桌面壁纸]用于设置客户使用安全桌面时，在安全桌面内显示的背景图片，若选择[使用电脑桌面壁纸]则生成的安全桌面背景和本地桌面背景一致，也可以选择[用户自定义]，上传相应的.jpg 格式结尾的图片。

### 2.5.1.3. 虚拟 IP 池

此页面设置 SSL VPN 用户登录访问总部资源时使用的虚拟 IP。该 IP 不能够和内网其它地址冲突，建议设置成比较生僻的 IP 段，如保留默认的 2.0.1.1—2.0.1.254 等。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『虚拟 IP 池』。

界面如下所示：



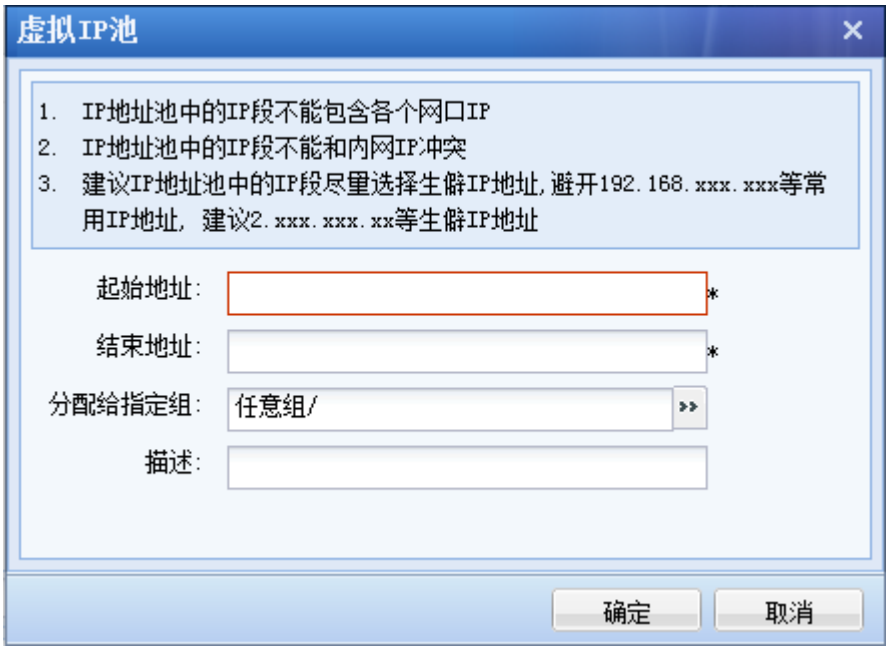

『IP 地址范围』指该虚拟地址池的起始 IP 和结束 IP。

『分配给指定组』是标识该虚拟地址池分配给指定的用户组。

『描述』该 IP 池的相关说明信息，可任意填写。

删除 和 编辑 能够对被勾选上的地址池进行删除和编辑操作。点击 选择 选中所有规则或者取消所有选择。

点击 新建 按钮，出现【虚拟 IP 池】对话框，如下：




**1. IP 地址池中的 IP 段不能包含各个网口的 IP，**

**2.IP 地址池中的 IP 段不能和内网 IP 冲突。**

点击 确定，保存配置。

## 2.5.1.4. 内网域名解析

SSL VPN 支持需要通过内部域名才能访问的资源应用。内网存在此类应用时，一般有一台或多台内网 DNS 服务器，给内网电脑提供内网域名解析服务。通过 SSL VPN 需要访问此类应用时，可以通过『内网域名解析』配置来实现。

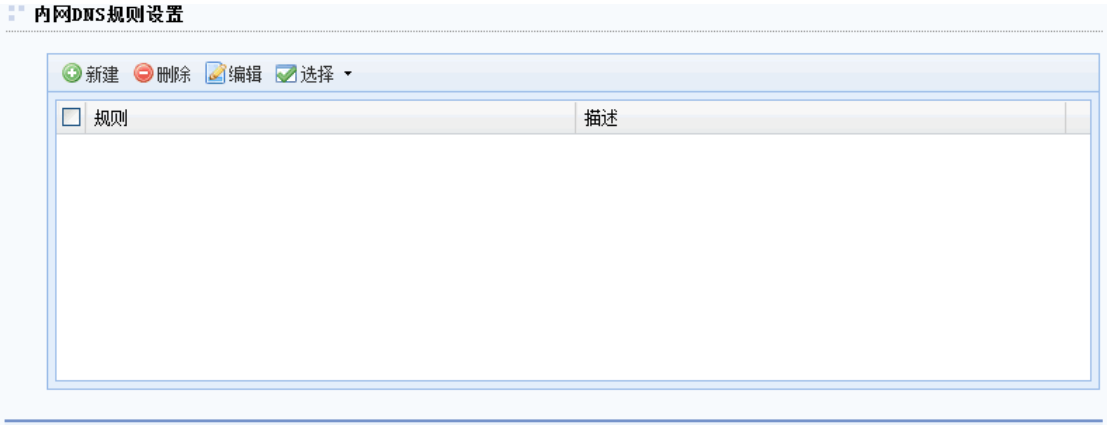
WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『内网域名解析』。

界面如下所示：

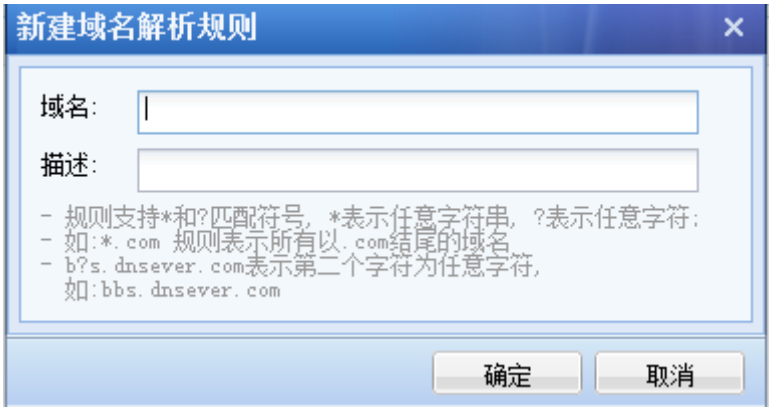

在『内网域名解析』中分别把内网 DNS 服务器的 IP 地址填写在『首选 DNS』和『备份 DNS』上，如果只有一台内网 DNS 服务器，则只需填写『首选 DNS』。然后在 SSL VPN 资源设置下填写资源主机地址或 URL 时以域名方式填写（资源相关的具体设置可参考章节 4.2 资源管理）。客户端访问 SSL VPN 的域名资源时，直接由『内网域名解析』中的 DNS 服务器进行解析。

[接入计算机使用此 DNS 服务器作为首选的 DNS 服务器]即将首选 DNS 和备选 DNS 的地址下发到登录 SSL VPN 的客户端的网卡中的主备 DNS 中。主要应用于当域控制器同时作为内网 DNS 服务器时，登录 SSL VPN 后访问的内网服务器需通过域控制器来认证的情况。

如果没有勾选[接入计算机使用此 DNS 服务器作为首选的 DNS 服务器]，且存在大量的域名应用资源，在设置好『内网域名解析』后，可以进一步采用『内网 DNS 规则设置』处理，界面如下：




点击 新建 出现【新建域名解析规则】对话框：




『域名』在规则列表中需要访问的域名。

『描述』可随意填写便于理解记忆的文字。

点击 确定 保存配置。然后在填写资源主机地址或 URL 时以 IP 方式填写（资源具体设置可参考章节 4.2 资源管理）。客户端访问 SSL VPN 的域名资源时，如果访问的域名符合在此定义的域名规则，将由设备内部的 HOST 表或『内网域名解析』中的 DNS 服务器进行解析，并将解析结果发送给客户端（设备 HOST 具体设置可参考章节 3.2.4）。

勾选相应的域名解析规则，点击 删除 或 编辑，对选中的规则进行删除和编辑操作。点击 选择 选中所有规则或者取消所有选择。

**1.如果资源中使用的地址是内部域名，且内网有专门的 DNS 服务器进行解析，推**

**荐在此添加规则，使得这部分域名的解析请求优先由内网 DNS 服务器解析，否则不要在此添加任何规则！**

**2.此处添加的规则最多支持 100 条；不支持中文域名解析。**

## 2.5.1.5. 单点登录设置

单点登录，也称为 SSO。就是通过用户的一次性认证登录，即可获得需访问系统和应用软件的授权。用户登录 SSL VPN 以后，在使用配置好的单点登录应用程序时，不需要再次手动输入用户名和密码，能够自动完成用户名和密码的输入，并进行登录。管理员可以在『单点登录设置』页面来配置单点登录的服务。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『单点登录设置』。

界面如下所示：


『单点登录设置』：勾选[启用]用户登录后可进行资源的单点登录，勾选『禁用』用户登录后不可进行资源的单点登录。

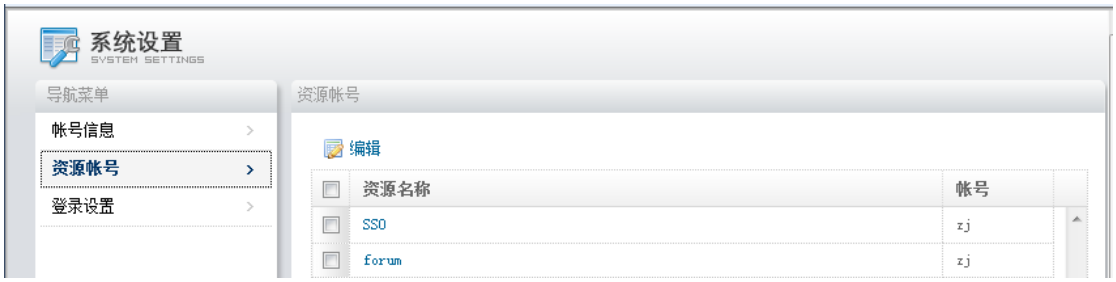
下载单点登配置助手 点击即可下载单点登录配置助手。单点登录配置助手用于在使用自动填表方式时帮助管理员录制单点登录文件。

下载单点登配置文件 点击即可下载单点登录配置文件。在设置好资源的单点登录方式后，需下载此文件使用单点登录配置助手来录制单点登录文件。

点击 浏览，选择录制好的单点登录文件，然后再点击 上传，将录制好的单点登录配置文件上传到设备中。

勾选[允许用户修改单点用户密码]，用户登录 SSL VPN 后可以修改单点登录的用户名和密码。页面如下：


点击 设置 便可出现私人用户设置界面，左边列表中选择『资源账号』，页面如下：



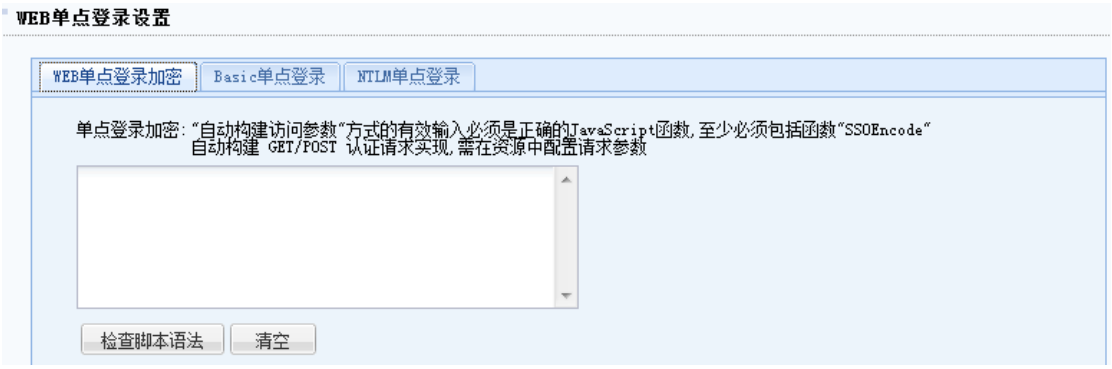

勾选相关的资源，再点击 编辑，弹出编辑框，如下图所示：


在【设置帐号】页面可以修改登录此资源的用户名和密码。点 保存 可以保存设置。

**1.只有私有用户，并且关联了 SSO 资源，才能够在资源列表页面进行 SSO 配置。**

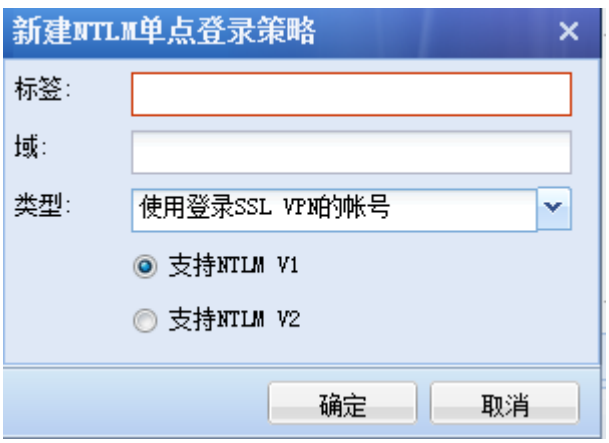
**2.若需要在客户端修改单点登录账号和密码，录制单点登录时，必须选择与 SSL VPN 相同的用户名和密码。**

『WEB 单点登录加密』用于对上传数据进行加密。某些 B/S 应用在登录过程中，客户端需要对上传数据（用户名或密码等）进行加密，服务器再使用相应的算法进行解密。在这里设置正确的 JavaScript 函数，可以满足此类应用。设置页面如下：




『Basic 单点登录』设置 Basic 认证资源的单点登录策略，点击 新增，页面如下：


『NTLM 单点登录』设置 NTLM 认证资源的单点登录策略，点击新增，页面如下：



## 2.5.1.6. 资源服务选项

『资源服务选项』用于设置各类资源的参数及自定义 URL 授权不通过提示页面的信息。包括『WEB 应用』、『TCP 应用』、『L3VPN 应用』以及『其他设置』四个标签页

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『资源服务选项』。

界面如下所示：


**WEB 应用**

『WEB 应用』用于 WEB 应用类型资源的参数的设置和 WEB 服务对象的修正。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『资源服务选项』→『WEB 应用』。

界面如下图所示：

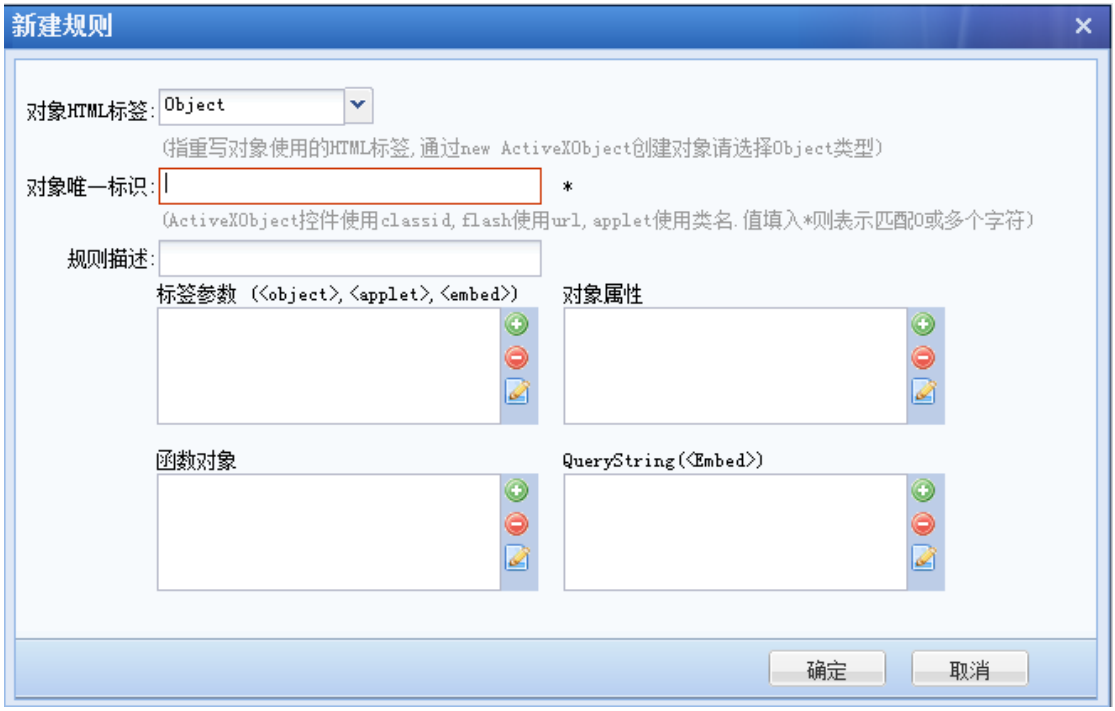

『资源访问模式』设置 SSL 资源的访问模式。

勾选[使用设备的 IP 地址作为源地址]，则客户端是以设备的接口 IP 地址访问服务器资源。

勾选[使用分配的虚拟 IP 地址作为源地址]，则客户端是以分配的虚拟 IP 地址访问服务器资源。（虚拟 IP 设置参考章节 3.5.1.3 虚拟 IP 池）

『WEB 对象修正』修正 WEB 应用服务程序中控件引用资源的路径，例如 Flash，Java Applet 或视频播放器等，使其能正常执行。

点击 新建规则，会出现规则编辑框，如下图所示：




『对象 HTML 标签』选择网页编写技术，支持 Object\Applet\Embed 三种。

『对象唯一标识』即标识该规则的名字。

『规则描述』可任意填写该规则的相关说明信息。

『标签参数』根据要修正的网页代码，填写相应的参数。

『对象属性』根据要修正的网页代码，填写相应的对象属性。

『函数对象』根据要修正的网页代码，填写相应的函数对象。

『QueryString（<Embed>）』根据要修正的网页代码，填写相应的查询字符串。

选中规则，点击 删除 或 编辑，对选中的规则进行删除和编辑操作。点击 选择 选中所有规则或者取消所有选择。

最后点击 保存 并 配置生效。

**TCP 应用**

『TCP 应用』用于 TCP 应用类型资源的参数的设置和开启智能递推。

WEBUI 路径:『系统设置』→『SSL VPN 选项』→『系统选项』→『资源服务选项』→『TCP 应用』。

界面如下图所示:


『资源访问模式』设置 SSL 资源的访问模式。

勾选[使用设备的 IP 地址作为源地址],则客户端是以设备的接口 IP 地址访问服务器资源。

勾选[使用分配的虚拟 IP 地址作为源地址],则客户端是以分配的虚拟 IP 地址访问服务器资源。(虚拟 IP 设置参考章节 3.5.1.3 虚拟 IP 池)

『客户端会话数』用来设置 SSL VPN 客户端 TCP 应用的会话连接数。

[启用资源智能递推]开启或关闭 TCP 应用的智能递推。

智能递推应用背景：有一些网站主页上有很多连接到其他服务器的链接，我们如果要访问这些链接，必须在添加资源的时候把这部分服务器都添加上，否则将无法访问。但是，当遇到这部分服务器很多的情况下，我们添加资源就很难能够添加完全，容易造成资源的漏添加，导致某些资源无法访问。智能递推就是为了解决这类问题而出现的。我们只要将这个网站的主页添加到 TCP 应用中，并将此网站中连接到其他服务器的子链接的 url 添加到智能递推的白名单中，就无需再将这些子链接添加成 TCP 应用，也能够实现对这些资源的访问。

『资源智能递推范围』设置对哪些 URL 地址进行智能递推。

勾选[仅以下地址]则仅对规则列表里面的 URL 地址进行智能递推。

勾选『对以下地址之外的其他地址』则对除规则列表之外的 URL 地址进行智能递推。

点击 新建 可添加 URL 地址，如下图：


勾选规则列表中的 URL 地址，点击 删除 和 编辑，对选中的规则进行删除和编辑操作。点击 选择 可选中所有规则或者取消所有选择。添加完成规则后，如下图所示：


最后点击 保存 并 配置生效。

该处启用智能递推后，在设置 TCP 应用资源时，需要在『其他属性』中勾选『应用智能递推』。

界面如下所示：


**智能递推应用案例**

案例背景：某高校通过部署 SSLVPN 实现用户远程安全接入学校内网，访问图书馆的各种资源。目前，图书馆有一个主页需要提供给用户通过 SSLVPN 进行访问，该图书馆主页的域名是 www.library.com，并且该主页上面有很多访问其他服务器或数据库的链接。

案例需求：用户通过 SSLVPN 可以访问该图书馆主页及其链接的所有其他服务器或数据库。

解决方案：启用智能递推功能。启用智能递推后，只需要在 SSL 设备中添加这个图书馆主页资源（“根资源”），其他镶嵌在这个“根资源”页面上的服务器或数据库（“子资源”）都不需要在 SSL 设备上手动添加。

案例实现配置步骤：

第一步：启用智能递推功能，并添加智能递推范围。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『资源服务选项』→『TCP 应用』。

配置界面如下所示：


勾选[启用资源智能递推]，选择[仅以下地址]并在规则列表中添加需要进行智能递推的 URL 地址，在本案例中填写*.library.*这条 URL 地址，如果图书馆主页中还有其他形式的 URL 链接可以同样加到规则列表里面。

最后点击 保存 并 配置生效 。

第二步：建立图书馆主页资源，类型必须选择 TCP 应用；

WEBUI 路径：『SSL VPN 设置』→『资源管理』。

点击 新建 按钮，再点击 TCP 应用 选项，在弹出页面中编辑图书馆主页资源。

配置界面如下所示：


点击 保存，保存配置

第三步：最后，把“图书馆”这个资源关联给用户，并点击 配置生效。配置完成。

**1.目前智能递推只支持 TCP 应用的 HTTP、HTTPS 应用。**

**2.若有资源启用了智能递推，则用户端在访问该资源时，主页面下的子页面均可以使用智能递推。**

**L3VPN 应用**

『L3VPN 应用』用于 L3VPN 应用类型资源的参数的设置。

WEBUI 路径:『系统设置』→『SSL VPN 选项』→『系统选项』→『资源服务选项』→『L3VPN 应用』。

界面如下图所示：


『资源访问模式』设置 SSL 资源的访问模式。

勾选[使用设备的 IP 地址作为源地址]，则客户端是以设备的接口 IP 地址访问服务器资源。

勾选[使用分配的虚拟 IP 地址作为源地址]，则客户端是以分配的虚拟 IP 地址访问服务器资源。（虚拟 IP 设置参考章节 3.5.1.3 虚拟 IP 池）

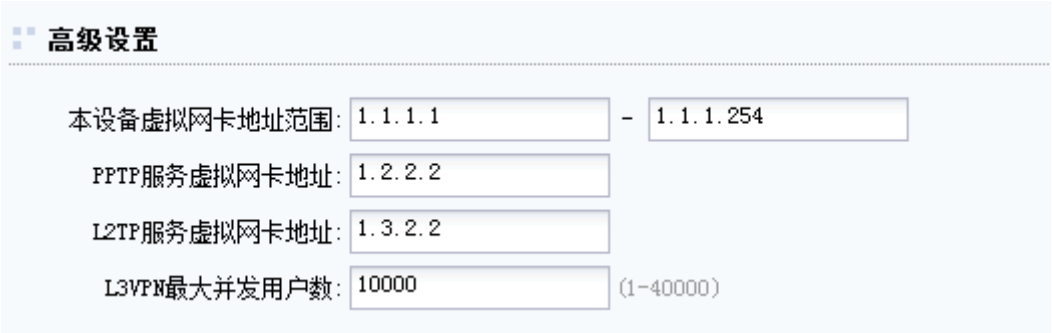
『传输协议选择』选择 L3VPN 应用的传输模式。

勾选[仅使用 TCP]，则在使用 L3VPN 应用的时候，只启用 TCP 隧道进行数据传输。

勾选[自动选择 TCP 或 UDP]，则会优先启用 UDP 隧道进行数据传输。

『UDP 服务端口』使用 UDP 隧道进行数据传输的端口，如果是单臂模式，需要前端网关设备映射端口给 SSL 设备，默认是 442。

点击 高级设置，可对设备虚拟网卡的地址范围，PPTP 服务的虚拟网卡地址，L2TP 服务的虚拟网卡地址和 L3VPN 最大并发用户数进行设置。



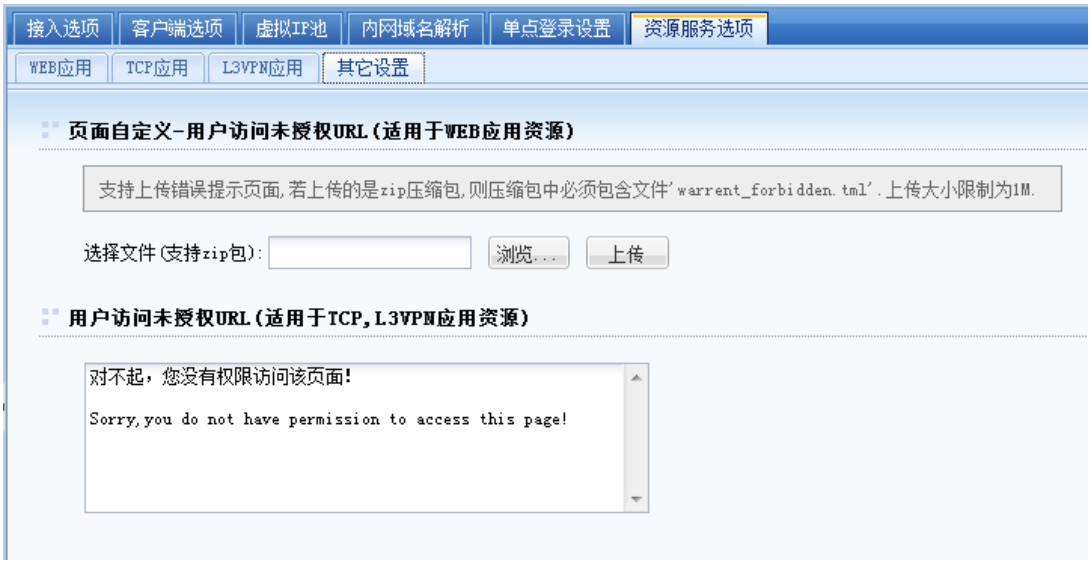

**注意：用户修改高级设置中的参数，有可能对 SSL VPN 性能造成严重影响，一般保留默认值即可。**

**其他设置**

『其他设置』用于设置访问资源时，URL 地址授权不通过的返回页面。（URL 地址授权参考章节 10.6.2.2URL 访问控制配置案例）

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『资源服务选项』→『其他设置』。

界面如下图所示：




点击 浏览 选择制作的页面的压缩包并上传，对 WEB 资源中 URL 地址授权不通过时的返回页面进行修改。

在『用户访问未授权 URL（适用于 TCP，L3VPN 应用资源）』的表中，可自定义 TCP 应用和 L3VPN 应用 URL 地址授权不通过时的返回页面的提示信息。

**1.页面自定义的功能仅支持 WEB 应用资源。**

**2.压缩包中必须包含有“warrant_forbidden.tml”文件，压缩包格式为 zip，且大小要求小于 1M。**

## 2.5.2. 网络传输优化

本页面可配置 SSL VPN 访问优化选项，优化 SSL VPN 的访问速度。包括『远程应用优化』、『传输优化』、『WEB 优化』、『WEB Cache』三个标签页。如下图所示：


### 2.5.2.1. 远程应用优化

WEBUI 路径:『系统设置』→『SSL VPN 选项』→『系统选项』→『网络传输优化』→『远

程应用优化』。

界面如下所示：


[有损压缩设置]启用该选项后，远程应用显示的图像会根据设置的质量等级进行压缩，以提高传输效率。勾选“保持更清晰的文字效果”可以在降低图片质量的时候，保证文字显示效果清晰。

[图像缓存设置]启用该选项后，远程应用会对图像进行缓存，以提高图像滚动的刷新效果，启用该选项会增加服务器的 CPU 使用率。

[动态图像过滤]启用该选项后，对于远程应用中的 FLASH 动画等动态图像会进行过滤，以节省带宽，提高应用的访问速度。

## 2.5.2.2. 传输优化

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『网络传输优化』→『传输优化』。

界面如下所示：


[启用快速传输协议]，在无线网络或网络环境较差的情况下可以使用，有一定的加速效果。

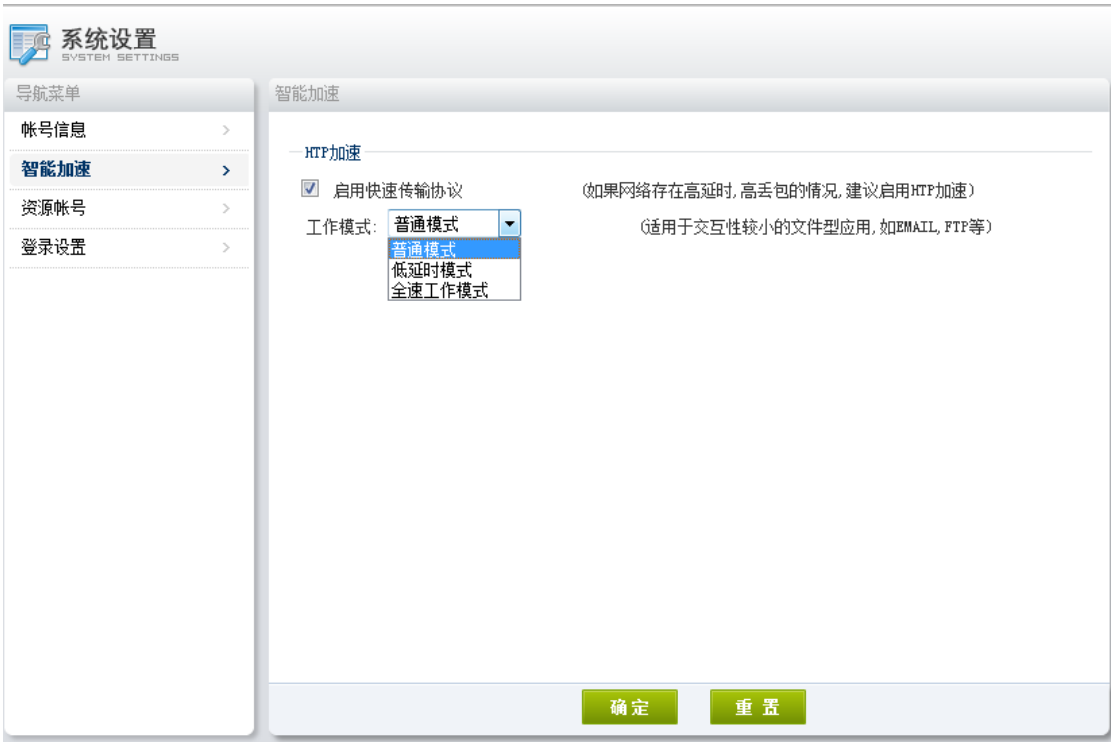
界面如下所示：


点击 高级设置 按钮，可定义启用快速速传输协议的参数。界面如下所示：


在『启用模式』中，勾选[自动选择]，并设置相应的丢包率和延时，则客户端接入 SSL VPN 后会自动测试网络状况，判断是否需要启用快速传输协议传输。丢包率和延迟两个条件，只要符合其中一个条件则启用快速传输协议，一般保留默认值即可。

勾选『手动选择』后，需要在客户端手动开启该功能。

客户端接入 SSL VPN 登录到服务页面，点击右上角的 设置，选择[智能加速]，页面如下：




勾选[启用快速传输协议]按钮，并选择[工作模式]， 最后点击 确定 配置生效。

**『启用快速传输协议』功能只有通过 IE 浏览器访问 SSL VPN 才可以使用（不支持其他浏览器）；只对 “TCP 应用”有效（资源设置可参考章节 4.2.3TCP 应用）；该功能需要通过 UDP 端口（设置可参考章节 3.5.2.1 传输优化实现，在 SSL VPN 网关设备单臂部署时注意在前置防火墙网关把此 UDP 端口映射到 SSL VPN 网关设备上。**

『单边加速设置』用来设置加速基于 TCP 隧道的服务。

勾选[启用单边加速]即开启单边加速功能。如下图：


**单边加速功能需要先在序列号中激才可以选，否则会是灰色不可选状态。**

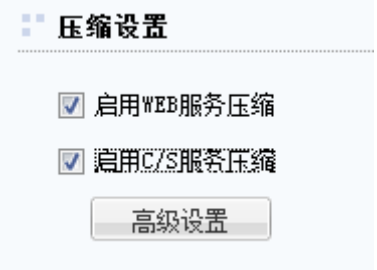
[启用流缓存]即对传输过程中重复数据进行编码压缩，可大大减少传输所需要带宽和时

间。

界面如下所示：


『压缩设置』包括 WEB 服务压缩和 C/S 压缩两种方式。

界面如下所示：




勾选[启用 WEB 服务压缩]，所有 B/S 架构的应在 SSL 隧道传送数据时，数据都会被压缩后再传输。

**该选项只对 WEB 应用资源有压缩效果。**

勾选[启用 C/S 服务压缩]，所有 C/S 架构的应用在 SSL 隧道传送数据时，数据都会被压缩后再传输。

点击 高级设置 按钮，弹出【C/S 服务压缩高级设置】对话框，可设置 C/S 服务压缩算法，可以选择[LZO 算法]或者[GZIP/ZLIB 算法]。

界面如下所示：


**该选项只对“TCP 应用”有压缩效果。**

### 2.5.2.3. WEB 优化

『WEB 优化』是利用 SSL 设备后台资源处理图片来减少公网数据流从而达到加速的效果，主要应用于客户端使用 PDA 或者网络环境很差的 PC 环境。在网络速度较好的环境中建议尽量不要使用。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『网络传输优化』→『WEB 优化』。


在『WEB 优化设置』可设置是否启用 WEB 优化功能，并设置相关的优化参化。

[启用 WEB 优化支持]是 WEB 优化的全局开关，勾选上即可启用 WEB 优化。

[启用图片显示]若不勾选，则禁止资源图片文件显示，从而提高访问速度。

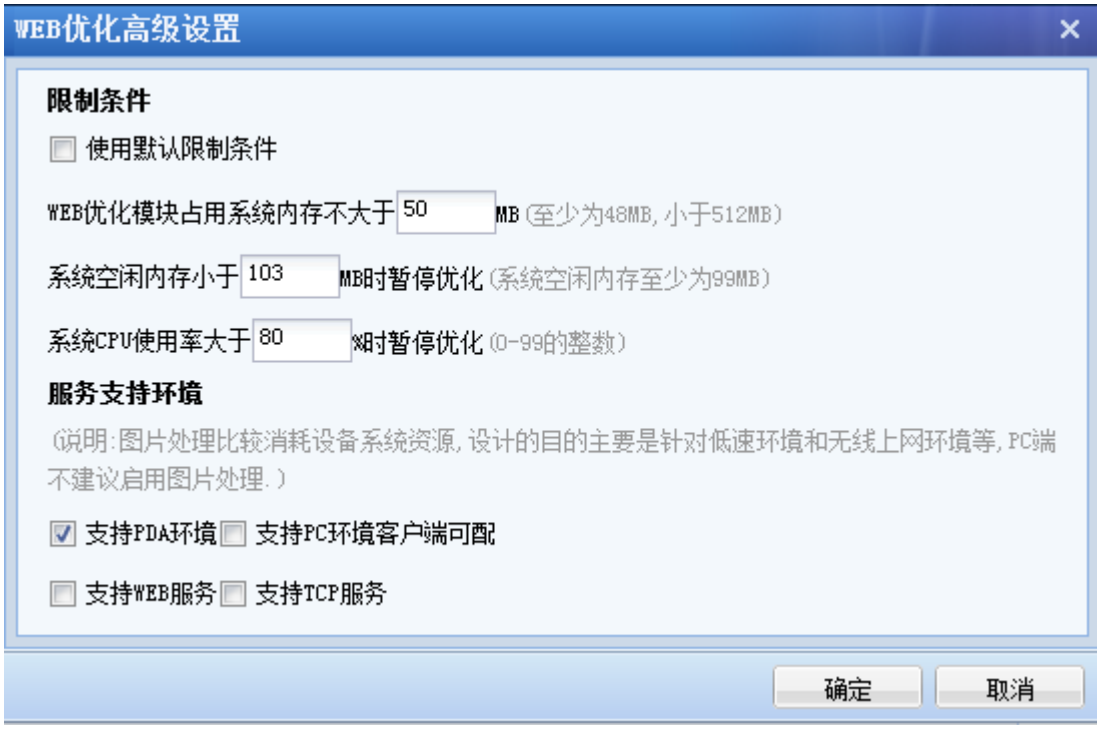
[缩小图片尺寸]勾选后可以缩小图片大小，减少图片数据传输量。

[智能缩小]会根据图片的大小进行动态缩小；也可以选择[强制缩小为原图尺寸的]中填写固定值，把图片按照固定的百分比缩小。

[调整图片质量为]可调整图片的显示质量，调整后会降低图片的质量，达到减少图片数据传输量的目的，只支持 jpg 格式的图片。有 4 种模式可以选择：[智能模糊]、[轻微模糊]、[中等模糊]、[高度模糊]。

**注意：图片格式只支持 jpg、png、gif，且每种格式只能选择一种图片处理策略。**

点击 高级设置，弹出【WEB 优化高级设置】的编辑框，如下图所示：



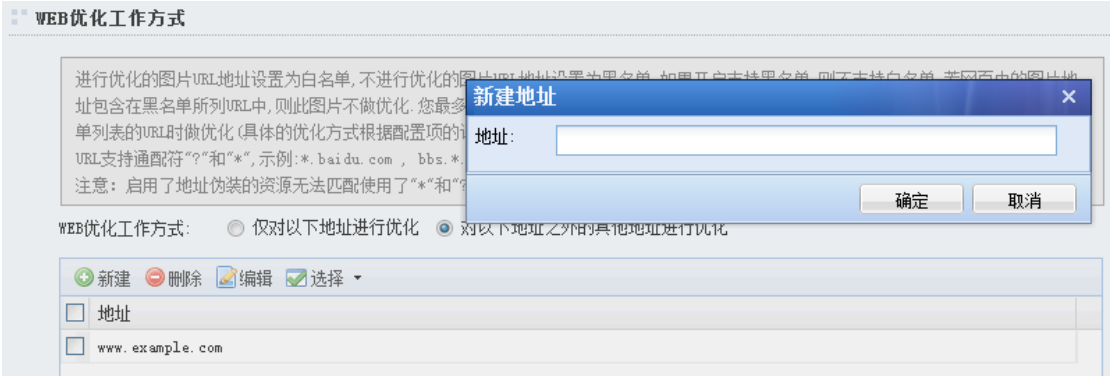

『限制条件』规定了当设备处于何种运行状况下才能运行图片处理，避免设备因图片处理影响其他模块的性能。

勾选[使用默认限制条件]，限制条件将不可配置。建议使用设备默认值。

若需要自定义限制条件，则不勾选，可针对 WEB 优化模块所在系统内存、系统空闲内存、系统 CPU 使用率设置不同的限制值

『服务支持环境』根据接入客户端的网络情况进行 WEB 优化的支持。勾选上相应的选项即可支持相应的环境和需要进行 WEB 优化的资源，包括：[支持 PDA 环境]、[支持 PC 环境客户端可配]、[支持 WEB 服务]、[支持 TCP 服务]。

点击『WEB 优化工作方式』规则列表中的 新建，可以添加需要进行优化的 URL 地址规则。




选中规则，点击 删除 或 编辑，对选中的规则进行删除和编辑操作。点击 选择 选中所有规则或者取消所有选择。

勾选[仅对以下地址进行优化]，将仅对规则列表中的 URL 地址进行 WEB 优化处理。

勾选[对以下地址之外的其他地址进行优化]，将对除规则列表之外的 URL 地址进行 WEB 优化处理。

**最多可以添加 255 条白名单或者黑名单；URL 支持通配符“？”和“*”。**

## 2.5.2.4. WEB Cache

『Web Cache』Web Cache 基于 IE 缓存机制，只要 IE 浏览器一般可以缓存的，就可以利用 Web Cache 对其进行加速（缓存图片，js 脚本，css 等等）。提高用户访问 WEB 页面的响应速度。

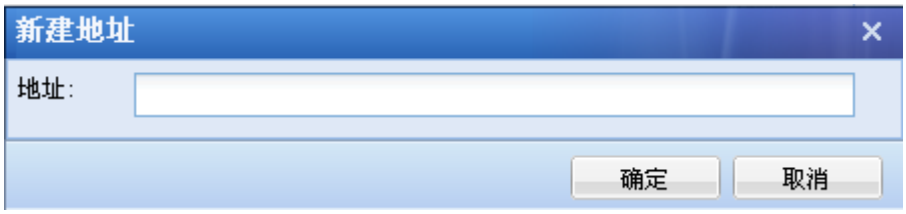
WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『网络传输优化』→『WEB Cache』。


[启用 WEB Cache]启用或者关闭 WEB Cache 功能。

选择[仅对以下地址进行优化]，则只对列表中填写的 URL 地址进行 WebCache 优化处理。

勾选[对以下地址之外的其他地址进行优化]，则对列表中填写的 URL 地址之外的地址，将进行 WebCache 优化处理。

点击 新建，会出现规则编辑框，如下图所示：




在『地址』里填入需要进行 URL 点击 确定 进行保存。

选中规则，点击 删除 或 编辑，对选中的规则进行删除和编辑操作。点击 选择 选中所

有规则或者取消所有选择。

## 2.5.3. 登录策略

『登录策略』可以用来针对不同的用户或用户组设置个性化的登录页面。

### 2.5.3.1. 登录策略

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『登录策略』。

界面如下所示：


[所有用户都使用相同的登录页面]在此处可以针对所有用户使用的登录页面进行全局设置。

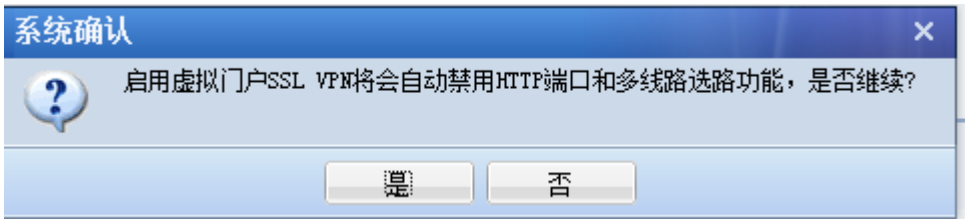
在[页面选择]中选择登陆页面，可选择使用系统自带模板或者用户自定义的模板。

点击 查看缩略图 可以看到当前可以使用的系统模板的缩略图。

界面如下所示：

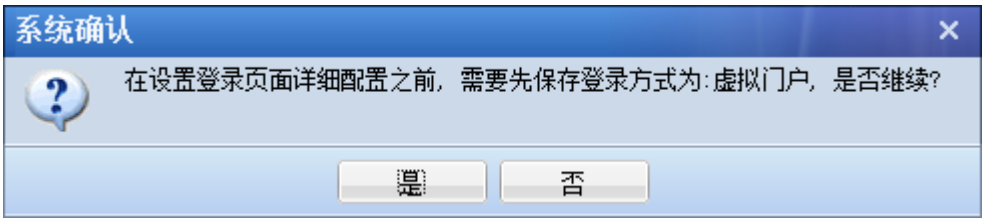

[虚拟门户]可设置允许不同的用户使用多个不同的登录风格及服务页面。

选择[虚拟门户]策略，SSL VPN 的 HTTP 端口和多线路选路功能将不可用，会弹出如下提示：



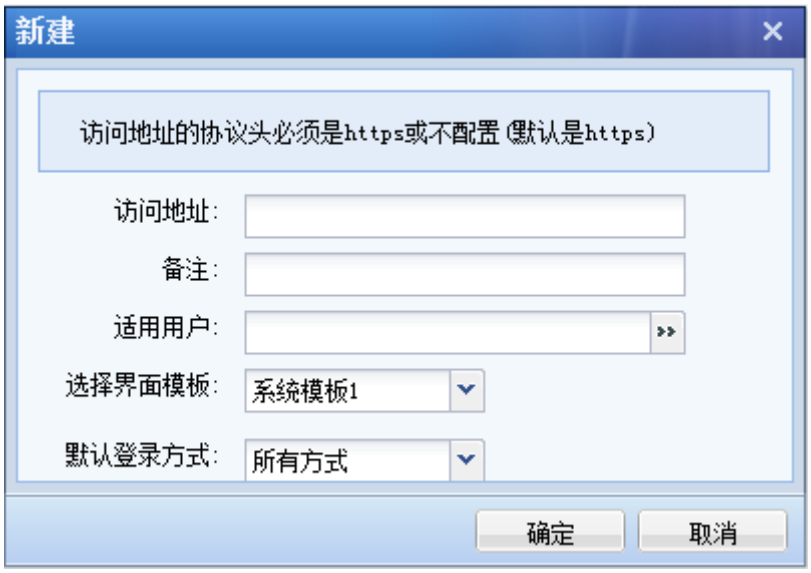

点击 设置 按钮，可以对『虚拟门户』进行详细设置。

界面如下所示：




点击 是 按钮，提交成功后，出现如下图所示的界面：


点击 新建 按钮，如下图所示：

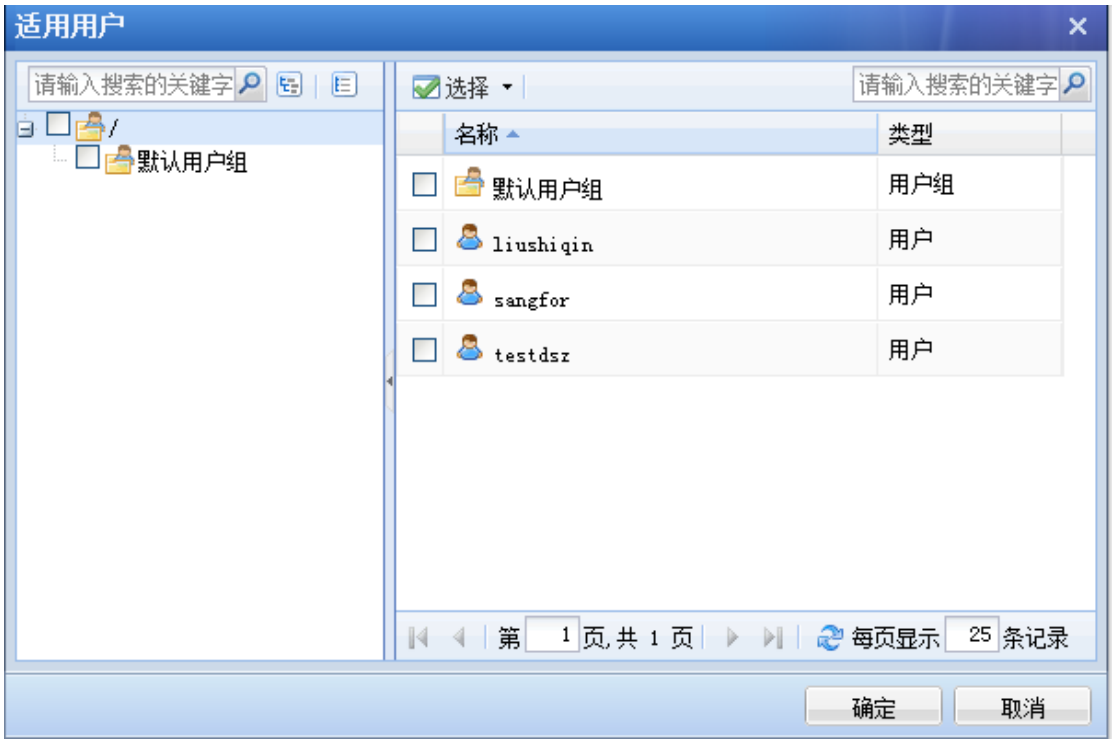



『访问地址』用来填写访问 SSL VPN 登录页面的地址。该地址不能以 http://开头。

『备注』用户填写一些描述信息。

『适用用户』选择关联该条登录策略的用户或者用户组。

点击  图标，如下图所示：



勾选关联的用户或者用户组，点击 确定 按钮，完成。

『选择界面模板』用来选择新建策略应用的登录页面，可以使用系统自带模板，也可以使用用户自定义的模板。

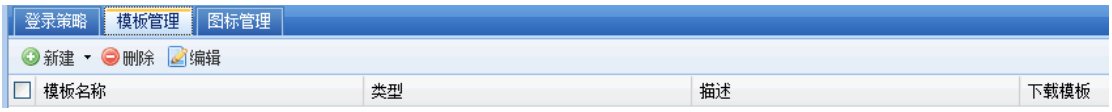
『默认登录方式』用来选择用户默认的登录方式，包括[所有方式]、[密码登录]、[证书登录]和[DKEY 登录]。

## 2.5.3.2. 模板管理

『模板管理』用来设置登录页面的模板，供用户选择使用。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『登录策略』→『模板管理』。

界面如下所示：




点击 新建 按钮，可以选择[以内置页面为模板新建]和[上传自定义页面]。如下图：


选择 [以内置页面为模板新建]就是以系统自带模板为基础来制作新的用户登录模板。

如下图所示：


『模板名称』用来自定义新建模板的名称。

『模板描述』用来添加新建模板的描述信息。

『页面标题』用来自定义新建模板显示的标题信息。

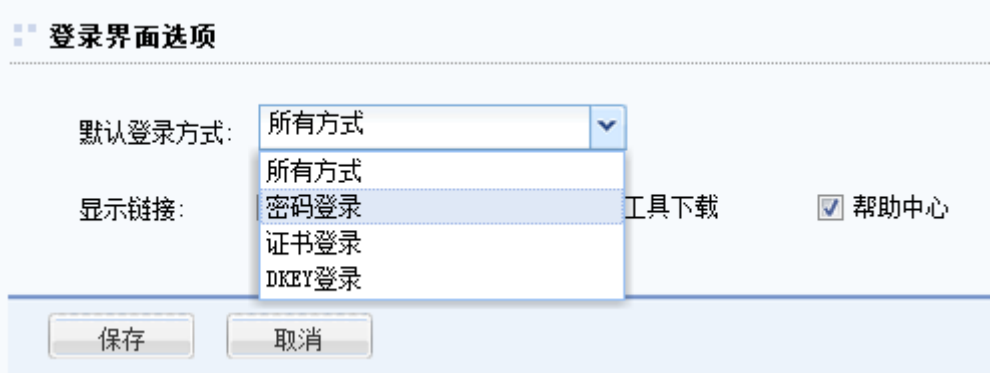
『背景色』用来选择新建模板显示的背景颜色。

『公告信息』可以编写一些公告或者提示信息，支持 HTML，不能超过 1024 个字符。

『登录界面选项』包括默认登录方式设置，以及登录界面显示链接设置。默认登录方式包括【所有方式】、【密码登录】、【证书登录】及【DKEY 登录】等，可选显示的链接包括【客户端组件下载】、【修复工具下载】、【帮助中心】等。

[默认登录方式]可以选择用户默认的登录方式，包括[所有方式]、[密码登录]、[证书登

录]和[DKEY 登录]。如下图：

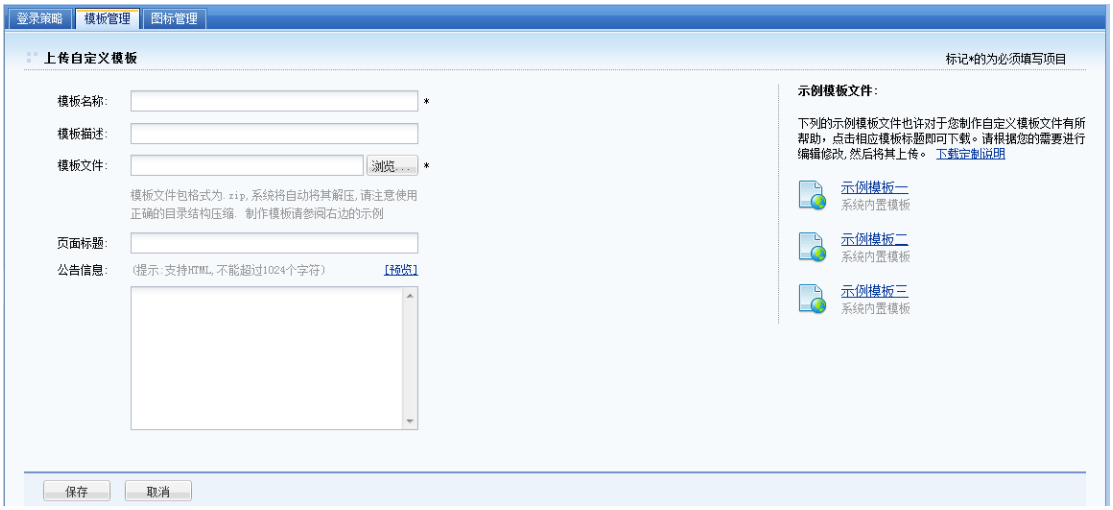



**若系统启用了匿名登录，则无法选择默认登录方式。**

点击 保存 按钮，新建模板设置成功。

选择『上传自定义页面』就是使用客户自己设计的登录页面。

界面如下所示：




『模板名称』用来自定义新建模板的名称。

『模板描述』用来添加新建模板的描述信息。

『模板文件』上传自定义的模板文件，模板文件包格式必须是 ZIP。

『页面标题』用来自定义新建模板显示的标题信息。

『公告信息』可以编写一些公告或者提示信息，支持 HTML，不能超过 1024 个字符。

点击『预览』可以看到预览效果图。

点击 保存 按钮，新建模板设置成功。

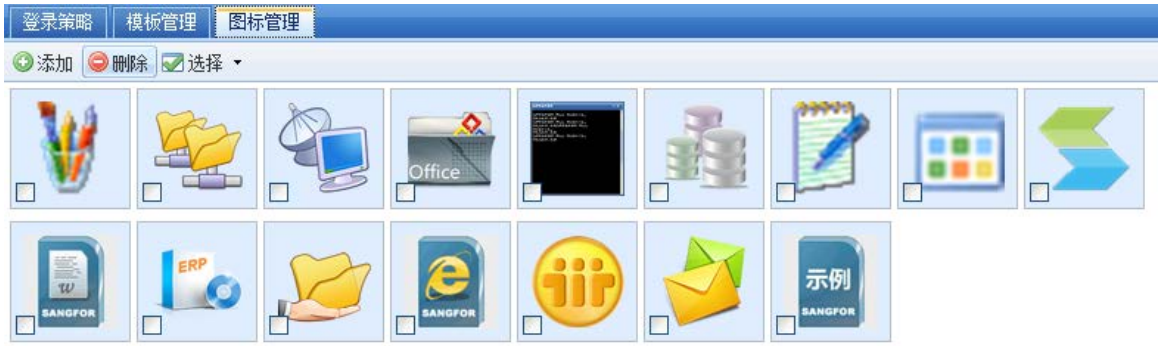
制作模版可以参考右边的示例，设备默认提供三种示例可供参考。

## 2.5.3.3. 图标管理

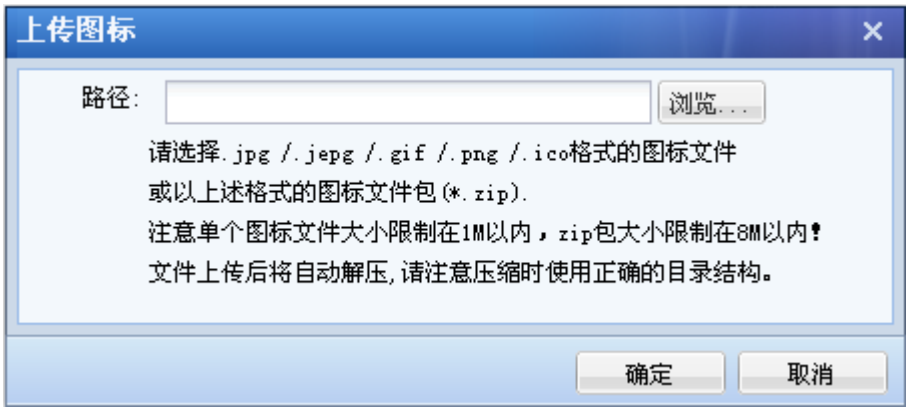
『图标管理』用来管理设备中用到的各种图标信息。

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『登录策略』→『图标管理』。

界面如下所示：




点击 添加 按钮，可以上传新的图标，如下图所示：




勾选图标，点击 删除 按钮，可以删除选中的图标。

点击 选择，可全部选中或取消选择。

## 2.5.4. 集群部署

集群可以使一组相互独立的服务器在网络中表现为单一的系统，并以单一系统的模式加以管理。集群的各个节点（SSL 设备）由一个分发器和一组真实服务器组成，分发器和真实服务器都是 SSL 设备（分发器本身也是一台真实服务器）。网络客户接入 SSL VPN 的时候，会由分发器合理的分配给集群中最空闲的真实服务器为客户提供服务。集群可以达到提高容量和性能的目的，为客户提供更高可靠性的服务。

### 2.5.4.1. 集群中的各元素定义与简介

集群：一组独立的计算机构成的一个松耦合的多处理器系统，通过协调通讯和数据同步实现分布式计算机。

分发器：集群中担任负载均衡器角色的设备。分发器同时也可以是一个真实服务器。

真实服务器：集群中担任真实服务器角色的设备。

节点：分发器和真实服务器的泛称。

集群 IP：集群的对外 IP 地址，外部用户通过这个 IP 来访问 SSLVPN。

集群密码：集群内部通讯密码，使用这个密码对集群内部的通信信息进行加密。

权值：节点性能指标，为 0 时表示不接收服务。

动态加权最小连接调度：各个服务器用相应的权值表示其处理性能。各节点动态地上报自身的权值。加权最小连接调度在调度新连接时尽可能使服务器的已建立连接数和其权值成比例。

## 2.5.4.2. 集群的主要特性

高性能：

1、 新连接会根据“动态加权最小连接”调度到服务节点。

2、 同一 IP 始终调度到同一节点，直到该 IP 与 SSLVPN 断开，新连接才会重新调度到其它节点。

3 、分发器接收请求，然后把请求调度到真实服务器，真实服务器回应用户的请求。

高可用：

1 、节点故障后在心跳（LAN 口发出的信号）超时会被分发器从分发表中清除，只有在该机器接受服务的用户受影响。

2 、新节点加入集群后分发器会把它加入分发表。

3 、分发器故障后会由优先级（优先级一样看性能）最高的机器升级为分发器，只有在分发器接受服务的用户受影响。

服务一致性：

1 、新的节点加入集群会从分发器下载所有配置和数据，与分发器的数据保持一致。

2 、管理员只能登录分发器的控制台进行修改，即使管理员登录到服务节点对 SVPN 也

只有查看权限（除了集群的基本配置的页面配置）。

3、 用户对用户数据（用户密码、HARD ID、手机号）的修改会同步到所有节点。

4 、任何节点数据库的改动都会激发数据校验，校验以分发器为准，如果不同则重新从分发器下载配置和数据库，然后重新启动相关服务。

5 、以下配置和数据不会在集群间同步，只在集群中每个节点单独操作有效：快速配置、网卡设置、日志查看（可以使用日志中心）、序列号、网关运行情况（在节点信息页面中显示）、重启网关（在节点信息页面中有对每个节点的重启）、保存配置和恢复配置、DHCP 状态。

6、没有数据库改动的操作不会进行数据校验，任何节点数据库的改动将会引起所有节点进行数据校验。

7、 时间同步，所有节点的实际以分发器的为准。

信息监控：

1 、分发器上能查看各个节点的资源使用情况，可以控制节点重启 SVPN 或重启服务或重启机器。

2 、分发器上能查看在线用户列表及其所在节点，并有断开某个用户功能。

分发器热插拔：

1 、单个节点：单个节点会在两个心跳间隔内成为分发器。

2 、分发器热插拔：如果分发器故障，那么在两个心跳间隔内拥有最大权值的节点将成为分发器。

3 、分发器的抢夺机制：如果新加入节点被配置成为优先成为分发器，而且是集群内唯一被具有该优先级，那么该节点先成为真实服务器，然后在两个心跳间隔内成为分发器，原来的分发器则降级为真实服务器。

节点热插拔：

1、 节点接入集群：在一个心跳间隔内从分发器下载数据，解压，覆盖原来的数据，重启服务，进行数据校验，通过后校验后正式成为服务器。

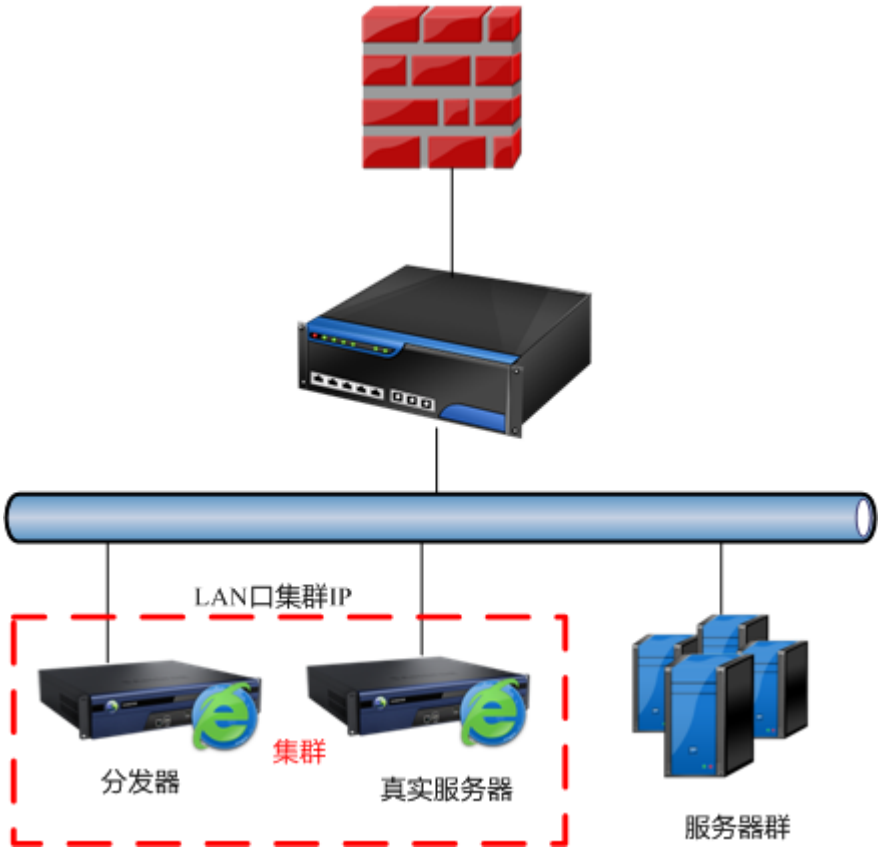
2 、节点故障：在两个心跳间隔内，该节点会被分发器从分发表中剔除。

可靠性：

集群中只要有一台 SSLVPN 网关正常运行，用户即可使用 SSLVPN 的所有服务。使用固定集群 IP 时当某台主机故障后，其该节点上的在线用户会断线，需要重新登录。

## 2.5.4.3. 部署方式

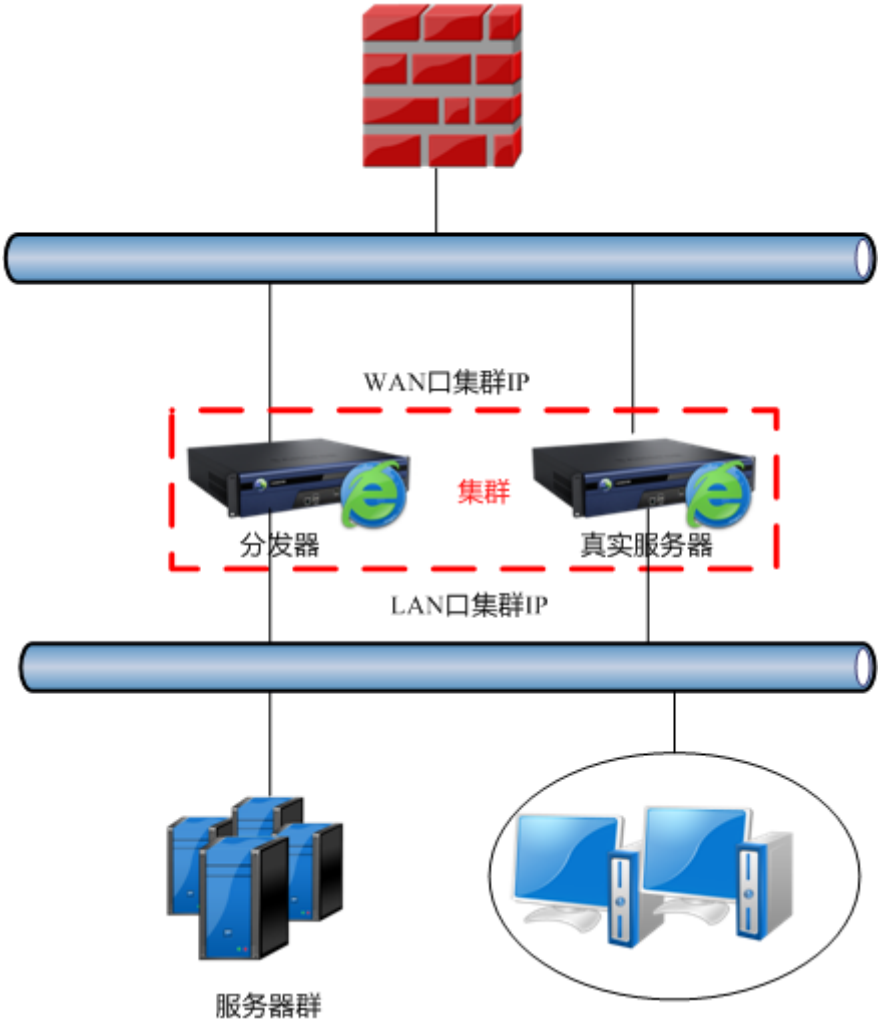
单臂模式部署：集群中各个 SSL 设备的内外网口设置参考章节 3.2.1 部署模式，其他部署与独立设备单臂部署相同。另外还需要在各个 SSL 设备的『集群部署设置』中的『基本配置』里配置相同的 LAN 口集群 IP。




**单臂模式**

**注意：单臂模式部署时，集群中的所有 SSL 设备「内网接口配置」中设置的 LAN 口 IP 和「集群部署设置」里「基本配置」设置的 LAN 口集群 IP 必须在同一个网段。**

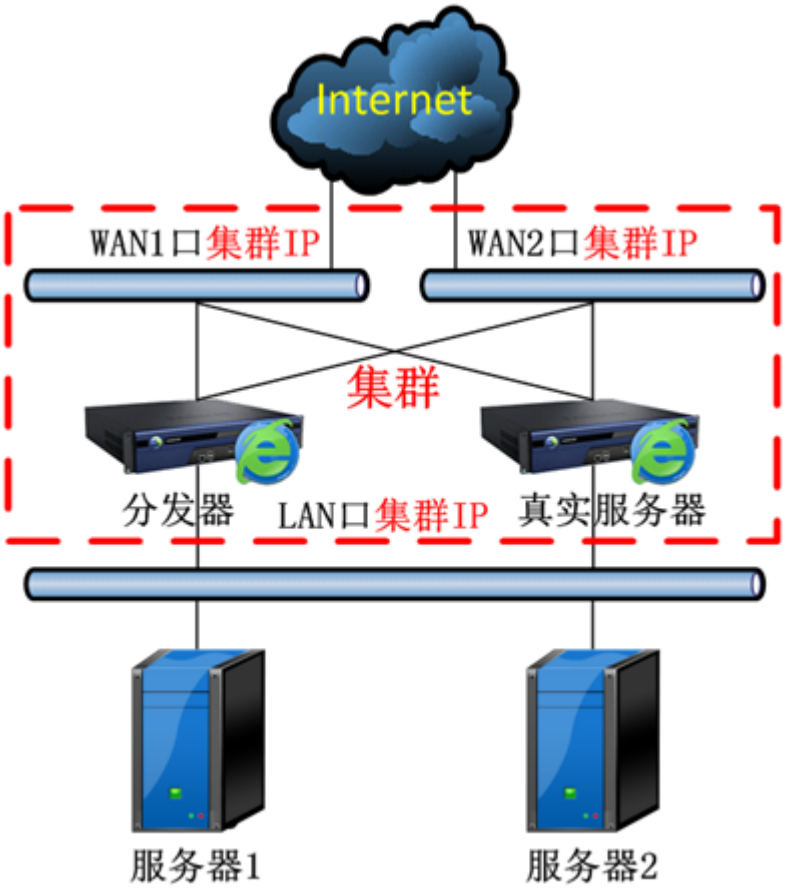
网关模式部署：集群中各个 SSL 设备的内外网口设置参考章节 3.2.1 部署模式，其他部署与独立设备网关部署相同。另外还需要在各个 SSL 设备的『集群部署设置』中的『基本配置』里配置相同的 LAN 口集群 IP 和 WAN 口集群 IP。



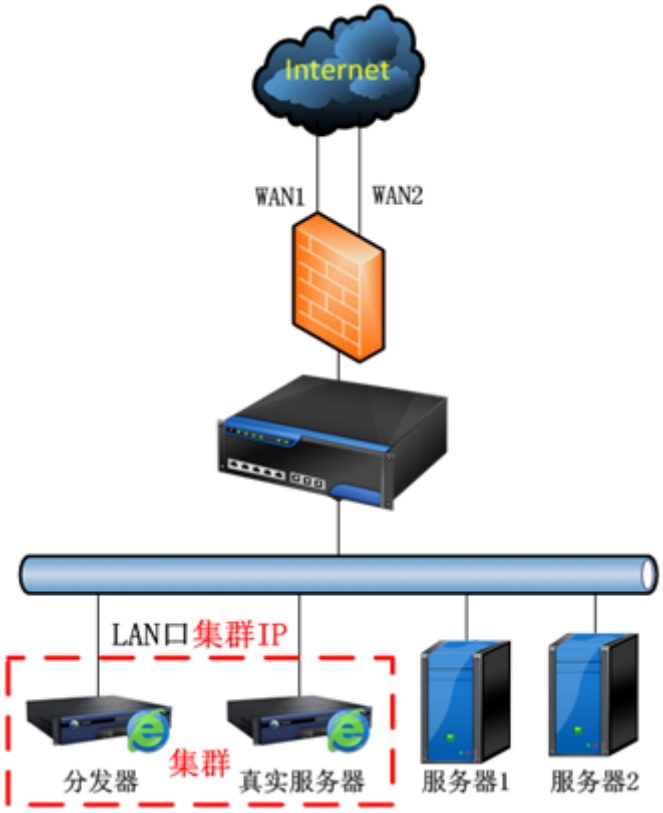

**网关模式**

**注意：网关模式部署时，集群中的所有 SSL 设备『外网接口配置』中设置的 WAN 口 IP 需要在同一个网段，但是和『集群部署设置』中『基本配置』里设置的 WAN 口集群 IP 必须在不同网段。SSL 设备做网关时，若设备是拨号上网的情况，集群不支持。**

多线路模式配置：集群中各个 SSL 设备的内外网口设置参考章节 3.2.1 部署模式，其他部署与独立设备多线路部署相同。需要在各个 SSL 设备的『集群部署设置』中的『基本配置』里配置相同的 LAN 口集群 IP 和 WAN 口集群 IP（有几个 WAN 口就填几个 WAN 口集群 IP）。


Internet
WAN1口集群IP
WAN2口集群IP
集群
分发器
LAN口集群IP
真实服务器
服务器1
服务器2

网关模式多线路




**单臂模式多线路**

**注意：集群中每个节点填写集群 IP 时必须保持一致。**

## 2.5.4.4. 集群部署设置

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『集群部署』→『集群部署设置』。

首先需要在『集群部署』下的『集群部署设置』中进行相应的配置，每台需要加入集群的设备都需要进行这样的配置。操作界面如下：


『集群部署设置』中的『启用集群部署功能』可以开启或关闭 SSL VPN 的集群功能。

『集群部署密钥』处填写该集群的密钥，每台需要加入集群系统的设备必须填写一致。集群密钥以作为分发器的 SSL 设备上设置的集群部署密钥为准。

『分发器选举规则』中可以设置[通过优先级选举分发器]和[优先做为分发器]。

若选[通过优先级选举分发器]，在[优先级别]的下拉框中可选择[自定义]，[高]，[中]，[低]，若选择自定义，则可以在后面填写优先级数字，数字越小，级别越高。集群中所有设备中，优先级越高的设备，则越优先被选为做分发器。

若选择[优先做为分发器]，则该台设备做为分发器，在同一个集群部署环境中，只允许一台设备选择该选项。

『集群 IP 设置』中可以设置各个网口的集群 IP，每一台加入到集群中的 SSL 设备，都必须填写相同的集群 IP。

『LAN 口集群 IP』中设置对外发布的 LAN 口的集群 IP。

『DMZ 口集群 IP』中设置对外发布的 DMZ 口的集群 IP。

『WAN1 口集群 IP』中设置对外发布的 WAN1 口的集群 IP，『WAN1 口掩码』中设置相应的 WAN1 口掩码信息。

『WAN1 口网关』中设置相应的 WAN1 口的网关信息。

**注意：集群 IP 是一组 SSL 设备组成的集群系统对外发布的 IP，集群中的每台设备在『集群 IP 设置』的设置都必须保持一致。**

点 保存 使配置生效。

## 2.5.4.5. 集群部署状态

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『集群部署』→『集群部署状态』。

『集群部署状态』中会显示集群中分发器和真实服务器的各种实时状态信息，包括节点 IP，节点类型，SVPN 运行状态，各个节点的 CPU 使用率，各个节点的授权数，各个节点的在线人数，总在线人数，总授权数。操作界面如下：

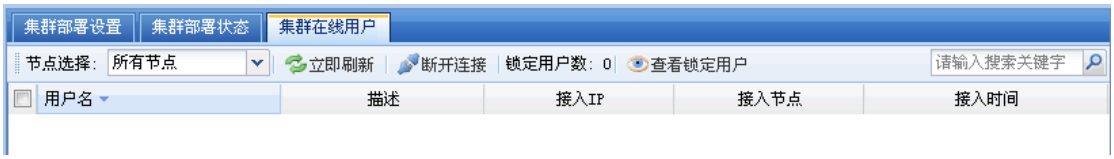

点击 登陆此节点 打开这个节点控制台界面。

## 2.5.4.6. 集群在线用户

WEBUI 路径：『系统设置』→『SSL VPN 选项』→『系统选项』→『集群部署』→『集群在线用户』。

『集群在线用户』中可以查看接入 SSL VPN 的用户名称、接入 IP、接入节点、接入时间，

并可以对接入的用户进行 断开连接 操作。操作界面如下：




『节点选择』可以选择要查询的节点，默认为所有节点。

立即刷新 刷新当前在线用户信息。

断开连接 可以对该用户进行断开 SSL VPN 连接的操作。

锁定用户数 可以查看被锁定的用户数量。

查看锁定用户 可以查看被锁定的用户。

页面右上方的放大镜框中可输入目标用户的关键字，点击放大镜图标，可进行搜索。

## 2.5.5. 分布式部署

WEBUI 路径：在『系统设置』→『SSLVPN 选项』→『分布式部署』。

分布式部署可以对 Internet 中不同地点的设备实现负载均衡。

界面如下所示：


『启用分布式部署』可以开启或关闭 SSL VPN 的分布式部署功能。

『节点名称』节点的名称。点击 检测有效性，则会到 webagent 服务器上验证节点名称是否有效。

『节点类型』用来标识节点的类型。如果勾选[主节点]说明当前配置的节点被定义为[主节点]；若勾选[从节点]说明当前配置的节点被定义为从节点。

『节点描述』用来描述节点。

『虚拟 IP 池同步策略』用来同步各个节点的虚拟 IP 池。

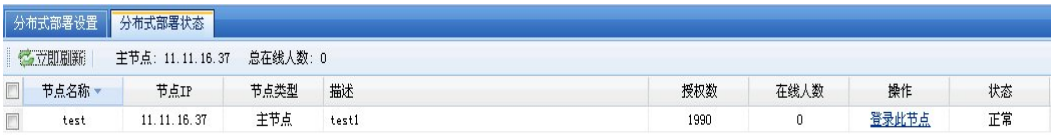
[节点共享虚拟 IP 池配置]即各分布式节点采用相同的虚拟 IP 池设置，适用于绑定 IP 的虚拟 IP 池分配策略。用户登录到不同的分布式部署节点，分配的是绑定的虚拟 IP，该策略不适用于虚拟 IP 动态分配，因其可能导致虚拟 IP 节点间的分配冲突。

[节点独立配置虚拟 IP 池]各分布式节点分别配置不同的虚拟 IP 池段，适用于虚拟 IP 动态分配策略。用户登录到不同的分布式部署节点，分配的是不同的虚拟 IP，不存在虚拟 IP 节点间分配冲突的问题。

点击 虚拟 IP 池设置 可以设置分布式部署中所需用到的虚拟 IP。具体设置参考章节 3.5.1.3 虚拟 IP 池。

点 保存 使配置生效。

『分布式部署状态』中会显示分布式部署中主节点和从节点的各种实时状态信息，包括节点名称，节点 IP，节点类型，描述，授权数，在线人数，状态等。




点击 登陆此节点 打开这个节点控制台界面。

**1.只有启用 WebAgent，才可以启用分布式部署。**

**2.若启用了虚拟门户，则不能启用分布式部署。**

# 第3章 SSL VPN 设置

『SSL VPN 设置』包含『用户管理』、『资源管理』、『角色授权』、『认证设置』、『策略组管理』、『终端服务器管理』、『企业移动管理』、『端点安全』八部分。

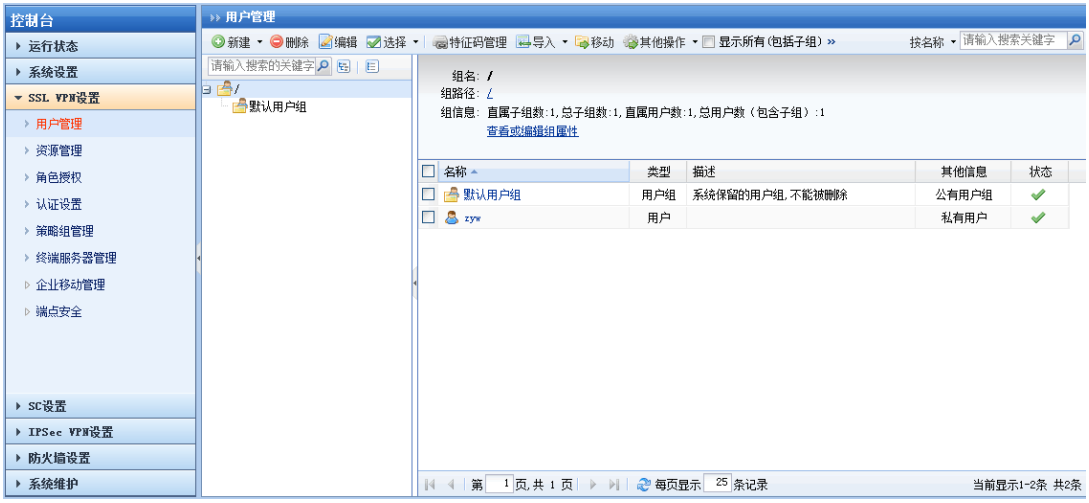
SSL VPN 设置的核心内容是三部分，分别是『用户管理』、『资源管理』和『角色授权』。三者间的关系是：通过“角色”把“用户组”（或“用户”）和“资源”关联起来，“用户组”内的“用户”获得相应“资源”的访问权限。

## 3.1. 用户管理

『用户管理』用于建立 SSL VPN 用户和用户组，SANGFOR SSL VPN 用“组的策略”管理和设置具有相同性质的用户。为了管理具有某些共性的用户以及更符合企业内部管理结构，采用分层的用户组管理用户。

WEBUI 路径：『控制台』→『SSL VPN 设置』→『用户管理』。

界面如下图所示：




在『用户管理』页面，左边为用户组结构树，右边为当前光标停留的用户组中的用户以及下级用户组。勾选[显示所有（包含子组）]，则显示当前用户组下的所有子组以及包含的所有用户。

用户组结构树上方的搜索框中可输入目标用户组的关键字，点击放大镜图标进行搜索，搜索到的用户组在用户结构树中会被高亮显示。

### 3.1.1. 新建用户组

点击 新建 按钮，在下拉框中选择 用户组，弹出【新增用户组】编辑框。

WEBUI 路径：『SSL VPN 设置』→『用户管理』。

界面如下图所示：


『名称』即标识该 SSL VPN 用户组的名字，必须填写。

『描述』可任意填写用户组的相关说明信息。

『所属组』在其下拉框中可选择当前新建用户组所隶属的用户组。/表示根组。

『最大并发用户数』控制该用户组及其下级组可以同时登录的在线用户数。

『账户状态』中勾选[启用]激活该用户组；勾选[禁用]禁用该用户组。

勾选[继承上级用户组关联角色、认证方式和策略组]，当前用户组自动关联上级用户组的角色、认证方法、策略组。

勾选[继承上级用户组认证方式]，当前用户组『认证选项』标签内的功能项与上级用户组一致。

勾选[继承上级用户组策略组』]，当前用户组『接入策略组』标签内的功能项与上级用户组一致。

勾选[继承上级用户组关联角色]，当前用户组自动关联上级用户组的角色。

『认证选项』标签内是用户组的登录认证方式的相关设置。

『账户类型』分为[公有用户组]和[私有用户组]。

[公有用户组]指该用户组中的所有用户账号可以供多人同时使用登录 SSL VPN。

[私有用户组]指该用户组中的所有用户账号仅仅允许一个人使用登录 SSL VPN ，两个人使用时会导致先登录的用户断线。

『多认证方式』分为[同时使用]和[任意一种]两种方式。

[同时使用]是“与”的关系，表示可以多种主要认证同时使用。

[任意一种]是“或”的关系，表示选择任意一种认证方式进行认证。

『主要认证』至少要选一种，『辅助认证』可选可不选。

[用户名/密码]认证，要求该用户组在建立用户账号时，设置用户账号的『名称』和『密码』。

[数字证书/Dkey 认证]，要求该组的用户账号都必须生成数字证书文件或生成 USB-Key（有驱 USB-Key 或无驱 USB-Key）。

[外部认证]，在右边的下拉框中选择该用户账号所在的“外部认证服务器”。用户帐号必

须在所选择的认证服务器上存在。（需要先配置外部认证服务器，外部认证服务器的具体设置可参考 4.4“认证设置”章节）。

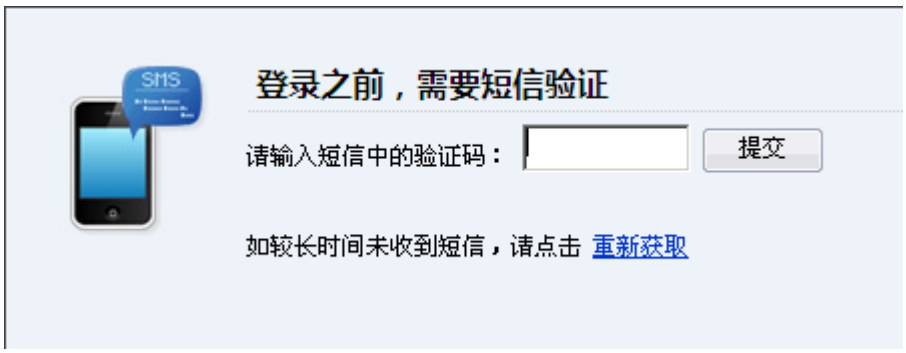
设置如下图所示：


**1.认证服务器必须预先在『认证设置』界面设置完成 LDAP 或 Radius 认证服务器的相关参数。**

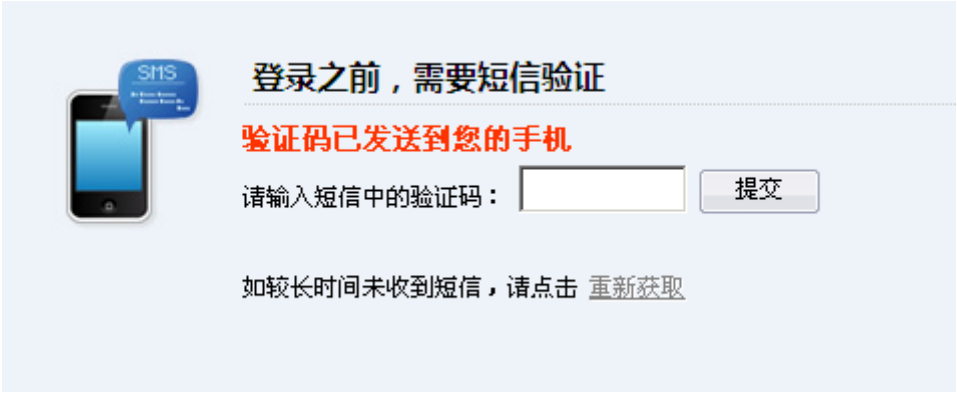
**2. 『用户名/密码』认证和『外部认证』是互斥的关系，二者只能选其一。**

[硬件特征码]把 SSL VPN 用户账号和计算机的部分硬件特性（如网卡、硬盘等）生成的硬件特征码一一绑定。由于硬件特性的唯一性，使得该硬件特征码也是唯一的、不可伪造的。一个用户可以拥有多个特征码，即在同一个账号下，多台符合条件的电脑可以登录。也可以配置成只能拥有 1 个特征码。通过对该硬件特征码的验证，就保障了只有指定的硬件设备才能接入授权的网络，避免了安全隐患。

[短信认证]，要求该用户组在建立用户账号时，必须设置好用户账号的『手机号码』，（手机号码设置请参考 4.1.2 和 4.4 章节）。当用户采用有效的认证方式登录到 SSL 界面后，系统会以短信方式发送一个“校验码”到该用户的手机上，该用户必须输入正确的校验码完成登录。




若收不到短信，可以点击 重新获取 按钮，再次发送认证短信。




**1. 短信认证支持客户端填写手机号码自动提交的方式，认证设置中手机号码为空，“认证方式”勾选短信认证，且配置好短信认证模块即可。**

**2. 每一个用户账号支持填两个手机号码，两个手机号码之间用;隔开。**

**3. 程序内部默认在手机号码前自动带上“86”（中国“国际区号”），若目标手机号为国外号码，必须填写相应国家的“国际区号”（短信认证模块的具体配置，请参照 4.4.2.1“短信认证配置”章节）。**

选择[动态令牌]，在下拉框选择该用户账号所在的“外部认证服务器”，服务器类型必须为“RADIUS 服务器”。用户帐号必须在所选择的认证服务器上存在。（外部认证服务器的具体设置可参考 4.4“认证设置”章节）。如下图所示：


[强制下级组及其用户继承本组认证选项]，可以强制隶属于该用户组的下级用户组及其用户继承本用户组的『认证选项』标签内的所有设置，但是下级用户组能够添加新的认证方式或选择其他外部认证服务器。

通过组合可以有以下的认证方式：

[用户名/密码]＋[短信认证』/[硬件特征码]/[动态令牌]

[数字证书/Dkey 认证]＋[短信认证』/[硬件特征码』/『动态令牌]

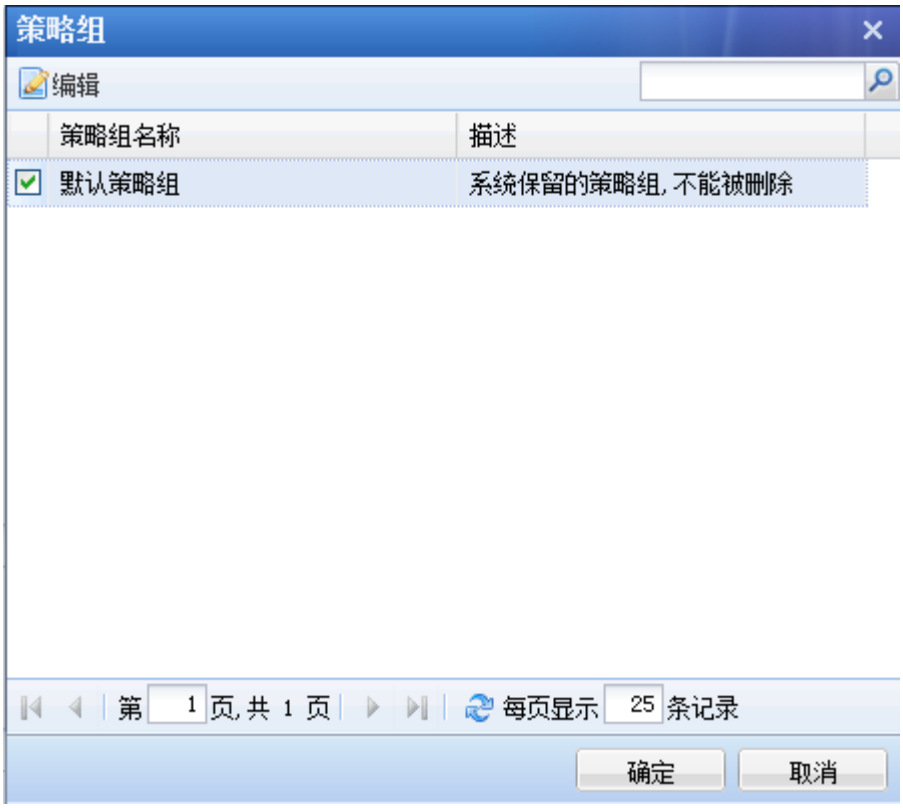
[外部认证]＋[短信认证』/[硬件特征码』/[动态令牌]

[用户名/密码]＋[数字证书/Dkey 认证』＋[短信认证]/[硬件特征码]/[动态令牌]

[外部认证]＋[数字证书/Dkey 认证』＋[短信认证』/[硬件特征码』/[动态令牌]

『接入策略组』用来设置用户使用的各种策略，具体设置可以参考 4.5『策略组管理』章节。


点击  ，弹出【策略组】编辑框，如下图所示：




点击 编辑 按钮，用来修改选中的策略组。

勾选应用的策略组后，点击 确定 ，如下图所示

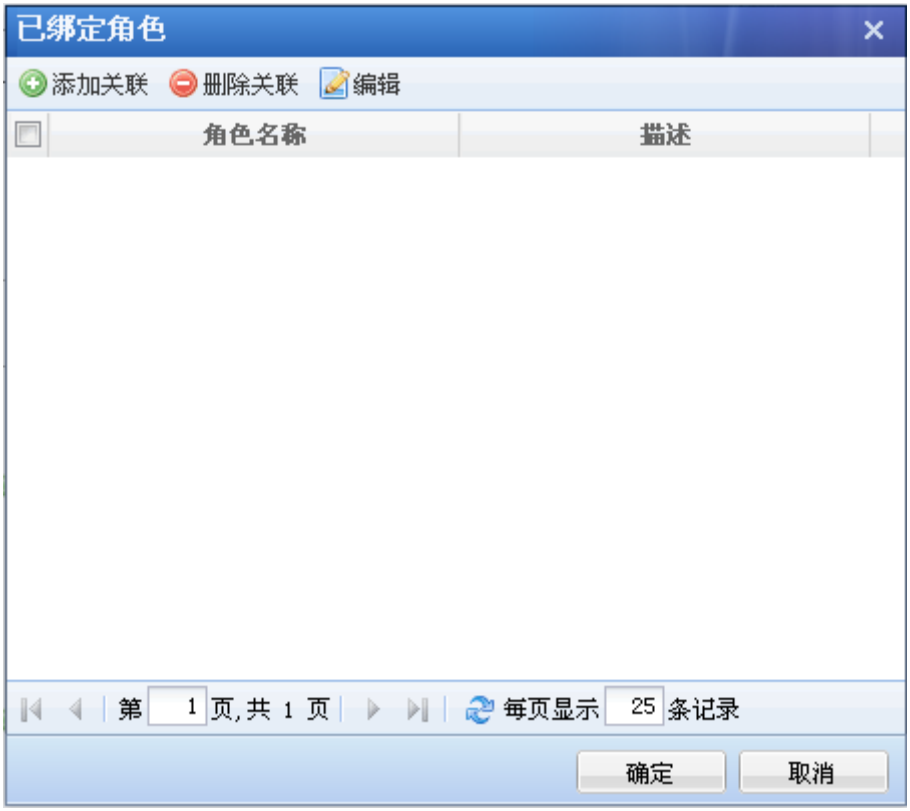

点击 新建策略组并选用 按钮，打开『新建策略组』对话框编辑新策略，编辑完成点击点击 保存 按钮，保存该策略并关联给当前用户组。具体设置可以参考 4.5『策略组管理』章节。

[强制下级组及其用户继承本组策略组]，可以强制隶属于该用户组的下级用户组及其用户继承本用户组所关联『接入策略组』标签内的所有设置。

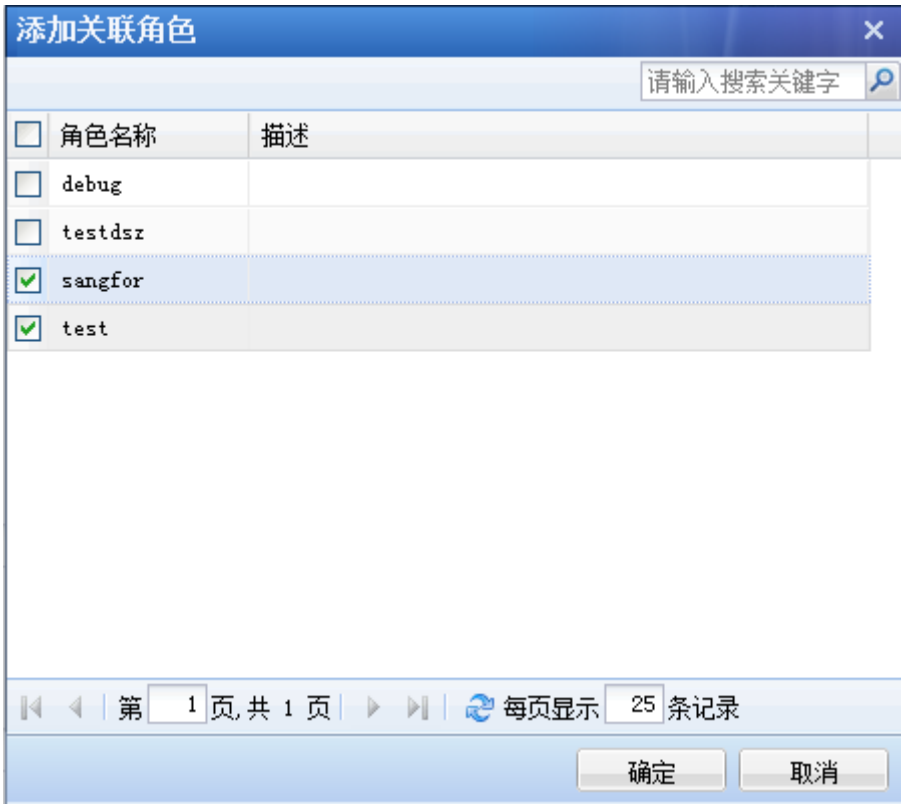
『关联角色』用来选择该用户组所使用的角色，角色的具体设置可以参考 4.3『角色授权』章节。


点击 新建角色并关联 按钮，打开【新建角色】对话框并编辑新角色，编辑完成点击 保存 按钮，保存该角色并关联给当前用户组。具体设置可以参考 4.3『角色授权』章节。

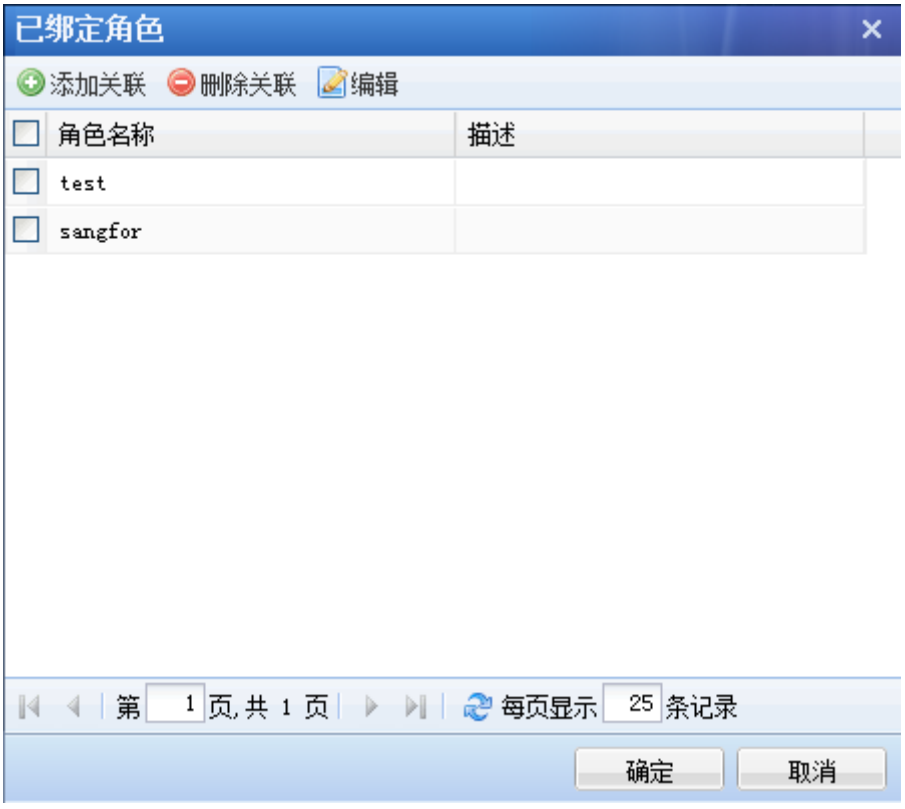
点击 » 为该用户组选择相应的角色，如下图所示：




点击 添加关联 按钮，用来选择需要关联的角色，弹出【添加关联角色】的对话框，如下图所示：




勾选相应的角色，点击 确定，如下图所示：



再点击 确定，如下图所示：


关联角色成功，该用户组关联了两个角色。

点击 保存職继续添加，可继续添加角色。

点击 保存 按钮，保存配置。

**注意：「默认用户组」和「匿名用户组」下不能够新建下级用户组。**

## 3.1.2. 新建用户

WEBUI 路径：『SSL VPN 设置』→『用户管理』。

点击 新建，在下拉框中选择 用户，弹出『新建用户』的操作界面。

界面如下图所示：


『名称』即 SSL VPN 用户登录 VPN 时所使用的帐号。

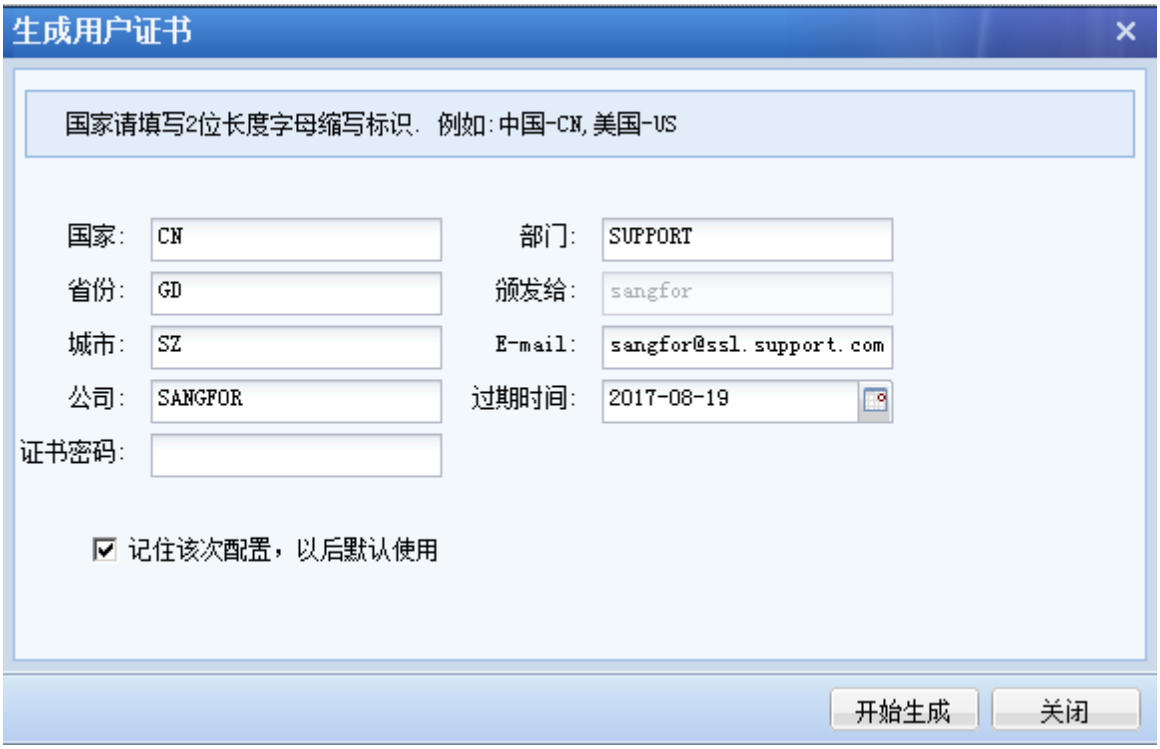
『描述』可任意填写用户的相关说明信息。

『密码』和『确认密码』用于设定 SSL VPN 登录帐号的密码。

『手机号码』用于填写用户的手机号码。

『生成证书』用于给使用内置数字证书认证的用户生成数字证书。若再『SSL VPN 设置』→『认证设置』→『证书与 USB-KEY 认证』里禁用了内置 CA，将弹出如下提示：


若再『SSL VPN 设置』→『认证设置』→『证书与 USB-KEY 认证』里启用了内置 CA，并设置了内置 CA 的相关选项，点击 生成证书 按钮，界面如下图所示：

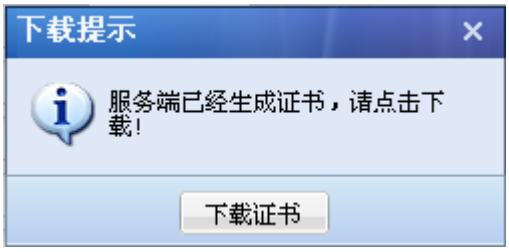



数字证书相关信息中的『国家』、『省份』、『城市』、『公司』、『部门』、『过期时间』、『E-mail』信息存在默认值，可以进行修改。修改后勾选[记住该次配置，以后默认使用]，把当前『证书密码』、『颁发给』除外的所有证书信息作为默认配置保存，后续用户生成数字证书可直接调用该默认配置。

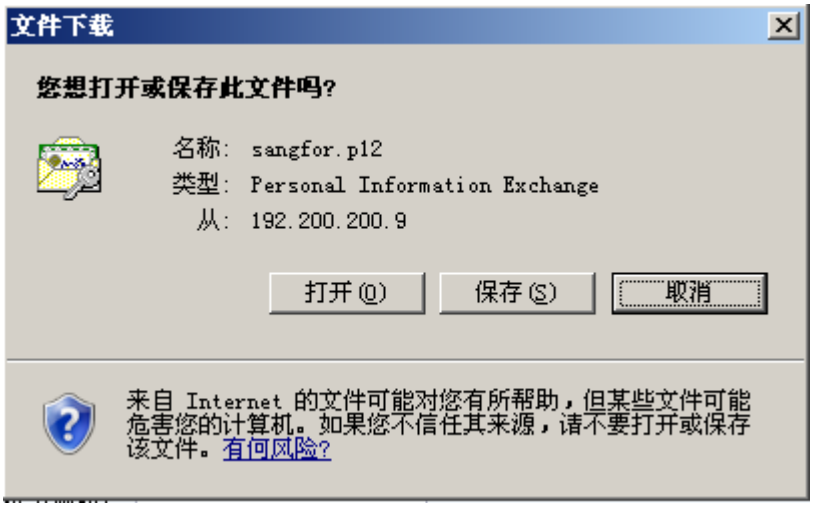
『颁发给』显示的是 SSL 账户名，只读不可更改。

『证书密码』需根据实际情况填写。在用户导入（安装）数字证书到电脑时需要用到，设定后请告知相应的登录用户。

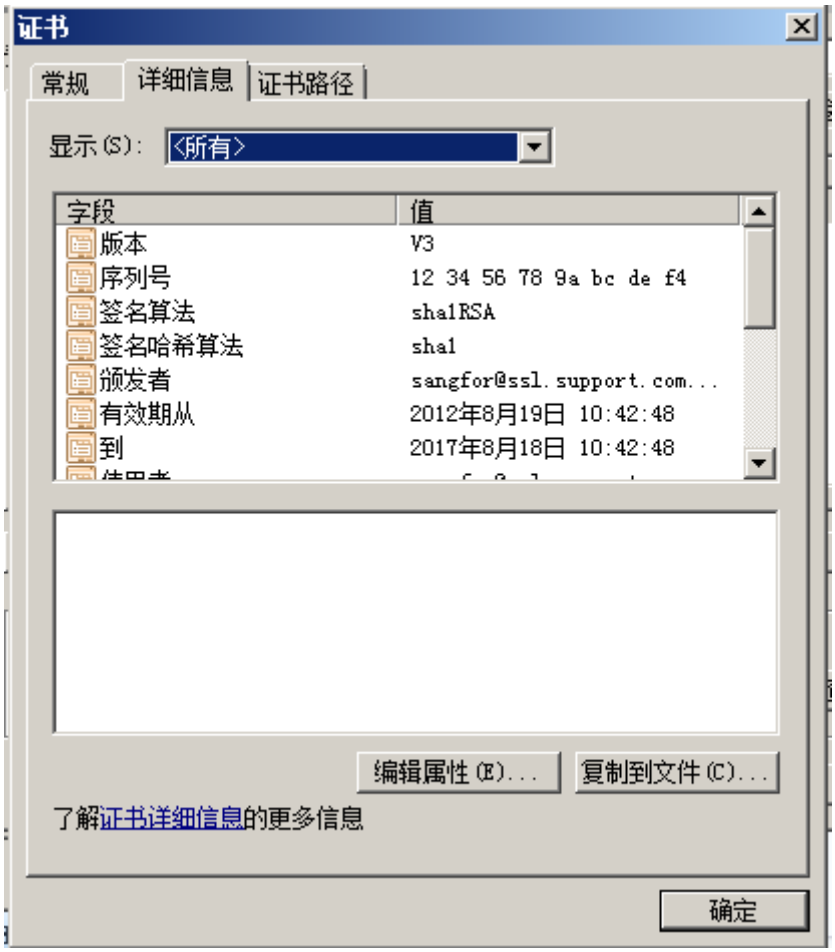
点击 开始生成，则开始生成证书，弹出如下图所示对话框：




点击 下载证书，选择证书的保存路径，会保存为以“.p12”为后缀的数字证书文件。如下图所示：



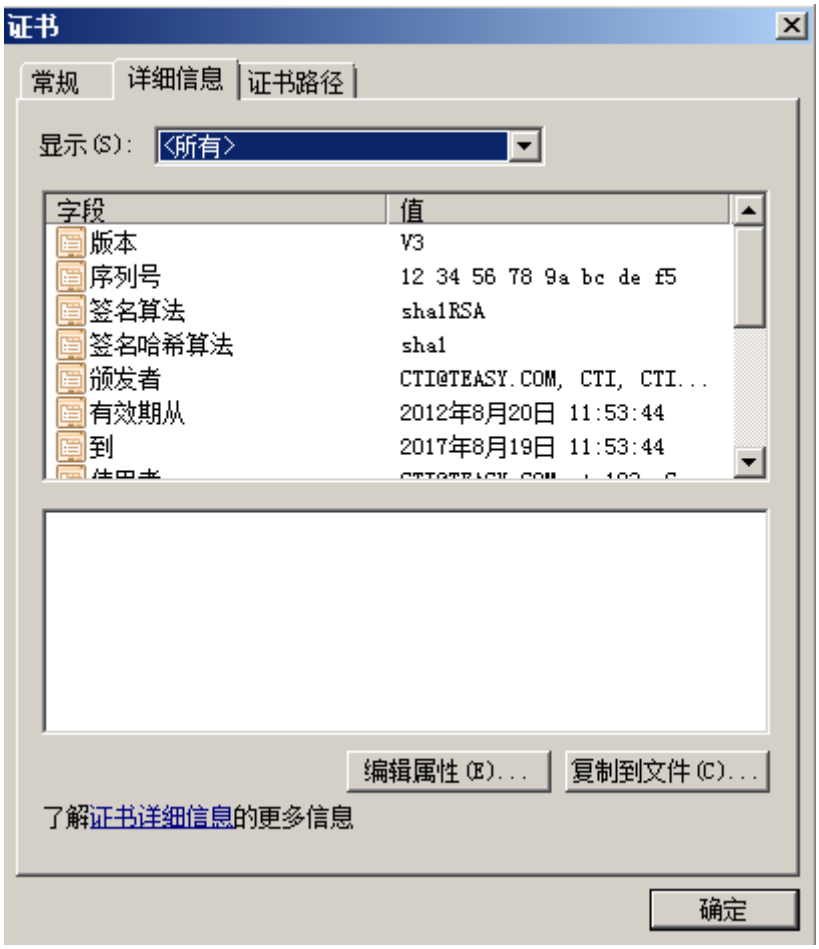

此时，界面上会显示该证书用户的序列号。




『导入证书』用于给使用第三方数字证书认证的用户导入用户证书。点击 导入证书 按钮，界面如下图所示：


选择相应的证书文件，设置证书密码，选择该用户使用的第三方 CA 证书机构，点击确定保存配置。

此时，界面上会显示该证书用户的序列号。




可以将鼠标移至外置 CA，点击后面的编辑图标，更改用户的绑定字段和所属的外置 CA。

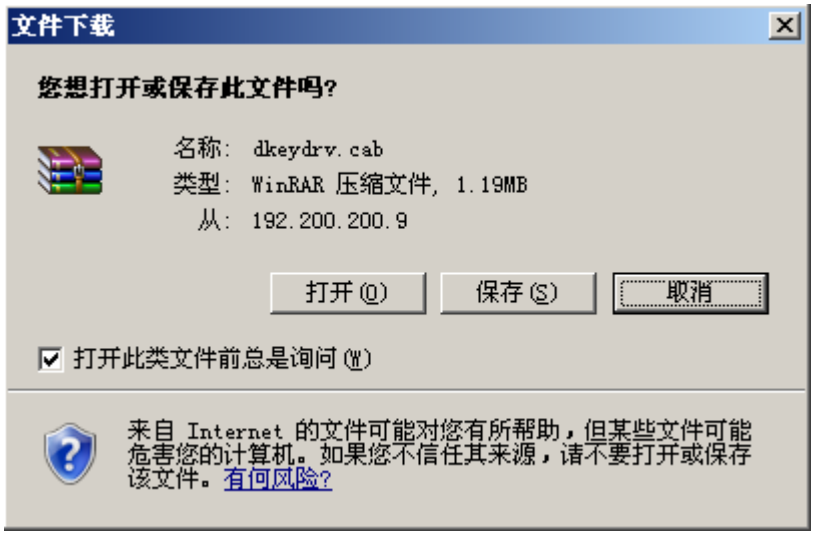

『创建 USB-KEY』用于给使用 DKEY 认证的用户生成 DKEY，可以是有驱 DKEY，也可以是无驱 DKEY。

**注意：“生成 USB-KEY”前，必须先安装证书导入控件和 USB-KEY 驱动。**

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『主要认证』。

如下图所示：


点击 下载安装 USB-KEY 驱动，出现以下界面：

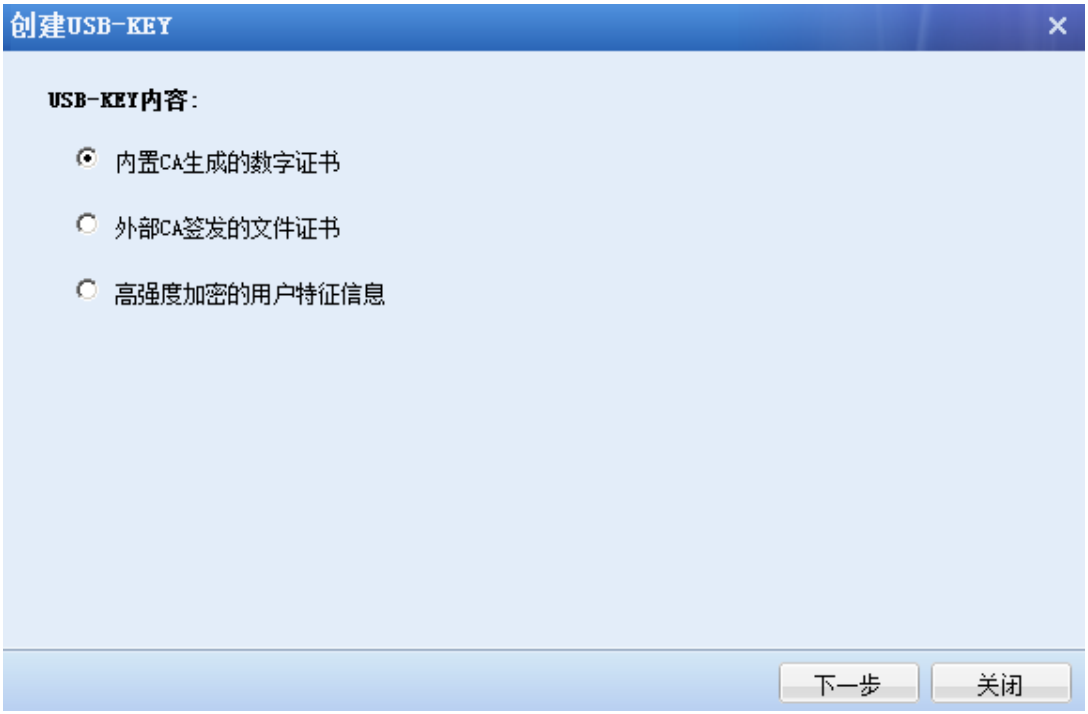



下载后，安装 USB-KEY 驱动。

点击 下载安装导入控件，将文件名为“DKeyImport.exe”的安装包下载后，安装完成。

**注意：安装证书控件时，必须以系统管理员权限登陆系统才可以完整安装。**

点击 创建 USB-KEY 按钮，如下图所示：




[内置 CA 生成的数字证书]需要由设备内置 CA 来签发一张证书，并写入 USB-KEY 中。

[外置 CA 签发的文件证书]需要由第三方 CA 来签发一张证书，并写入 USB-KEY 中。

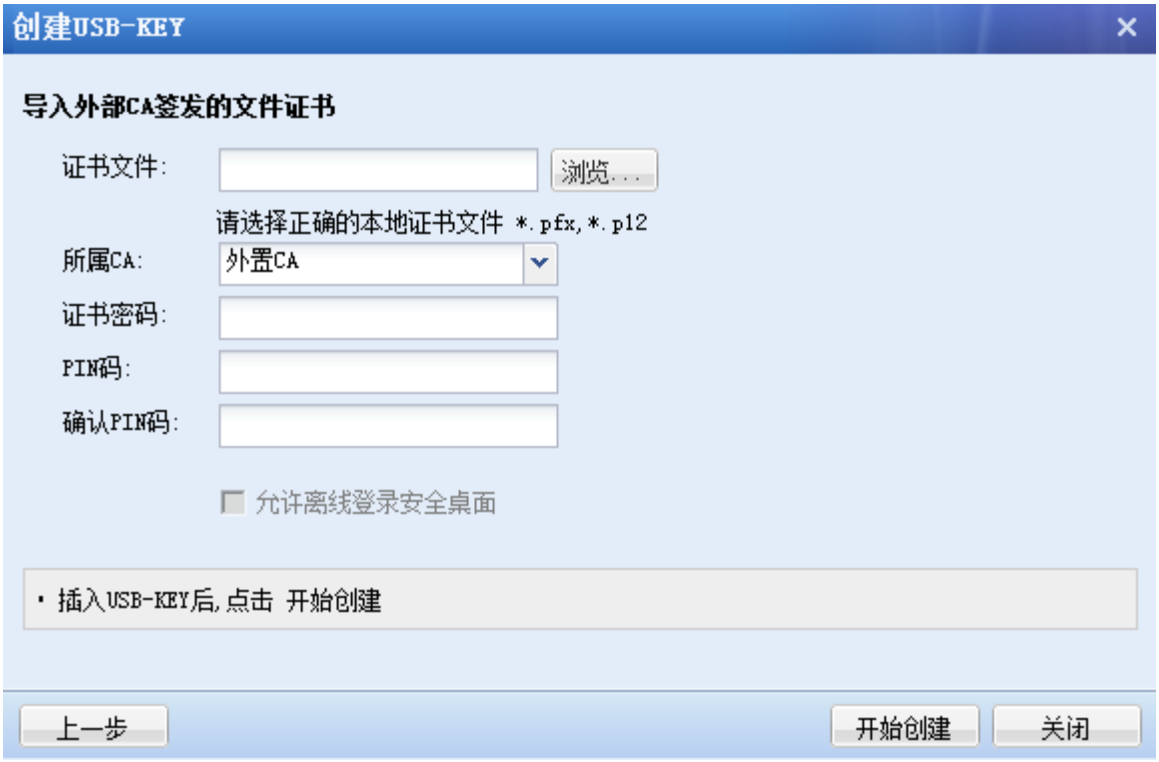
[高强度加密的用户特征信息]中存放的是经高强度加密后的，用来唯一标示该用户的特征信息。登录时，可以根据 USB-KEY 中的信息识别登录用户的身份。

选择[内置 CA 生成的数字证书]，点击 下一步，如下图所示：


输入 DKEY 的 PIN 码，插入 USB-KEY，点击 开始创建，生成证书成功。

**注意：若用户关联了离线访问安全桌面的策略且用户认证 DKEY 和离线登录安全桌面的 DKEY 是同一个 DKEY，还需要勾选上“允许离线登录安全桌面”。**

选择[外置 CA 签发的文件证书]，点击 下一步，如下图所示：




输入证书密码和 DKEY 的 PIN 码，插入 USB-KEY，点击 开始创建，生成证书成功。

**注意：若用户关联了离线访问安全桌面的策略且用户认证 DKEY 和离线登录安全桌面的 DKEY 是同一个 DKEY，还需要勾选上“允许离线登录安全桌面”。**

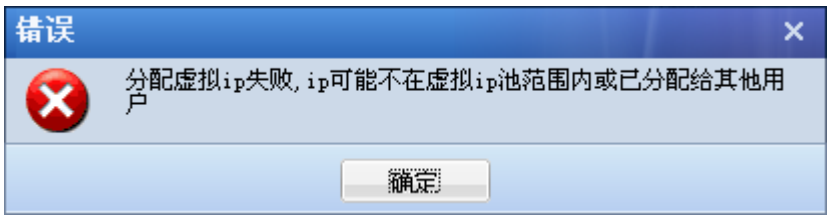
选择[高强度加密的用户特征信息]，点击 下一步，如下图所示：


输入 DKEY 的 PIN 码，插入 USB-KEY，点击 开始创建，生成证书成功。

**注意：若用户关联了离线访问安全桌面的策略且用户认证 DKEY 和离线登录安全桌面的 DKEY 是同一个 DKEY，还需要勾选上“允许离线登录安全桌面”。**

『虚拟 IP』将虚拟 IP 和“当前用户”绑定。可以选择[自动获取]或[手动设置]。

如果选择[自动获取]，则用户登录后自动从虚拟 IP 池中分配一个虚拟 IP；如果选择[手动设置]，则可以点击 获取空闲 IP 按钮，在后面方框中自动出现可以绑定的虚拟 IP；当然也可以手动填写虚拟 IP 地址，如果填写的虚拟 IP 不在虚拟 IP 池内，或者被其他用户绑定，那么在点击 保存 按钮后，会出现如下提示框：



**注意：只有“私有用户”才可以绑定虚拟 IP，**

**“用户”可以单独设置认证方式，缺省情况下“用户”自动继承所在“用户组”的认证方式等属性。**

『过期时间』，包括[永不过期]和[手动设置]两种。

若勾选[永不过期]则该用户一直都可以使用；

若勾选[手动设置]，则在后面的方框中选择日期，如果到了这个时间，那么该用户将被禁用。

『账号状态』，可选择[启用]或[禁用]。

若勾选[启用]则该账号可以正常使用；

若勾选[禁用]，则该账号被禁用，无法使用。

『所属组』可设定该用户属于哪个用户组。

『离线访问』若用户关联了离线访问安全桌面的功能，可以将用户与离线访问安全桌面的 DKEY 进行绑定，则该用户在离线状态下，只能使用指定的 DKEY 访问安全桌面。


点击 绑定 USB-KEY，弹出如下提示：


勾选[继承所属组认证选项和策略组]，当前用户自动关联上级用户组认证选项和接入策略组。

勾选[继承所属接入策略组]，当前用户继承上级用户组的接入策略。

勾选[继承所属组认证选项]，当前用户继承上级用户组的认证策略。

不勾选[继承所属组认证选项和策略组]则当前用户可以独立设置认证方式和接入策略。

『认证选项』和『接入策略组』、『关联角色』标签内的设置项和【新建用户组】页面的一样，此处不再赘述。

完成配置后，点击 保存，最后在『用户管理』页面点击 配置生效，保存配置并生效。

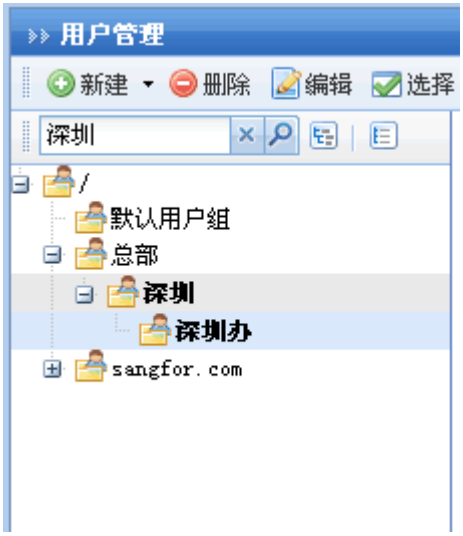
### 3.1.3. 高级搜索

位于界面右上方的搜索框，可[按名称]、[按描述]、[按虚拟 IP]或[按手机号码]来搜索用户，在后面的方框可填入需要搜索的具体内容，点击放大镜图标，会直接显示相关用户的相关信息。


点击 高级搜索 按钮，如下图所示：


可以根据包含关键字、关键字类型、搜索范围、认证类型、过期时间、闲置时间来查询相应的用户。

位于用户组织结构上方的搜索框，可以查找有相应关键字的用户组，如下图所示：




点击用户列表中『名称』标签，即可对用户、用户组进行升降序排列。

点击『列』标签，可根据下拉表的选项进行显示列的筛选，如下图：

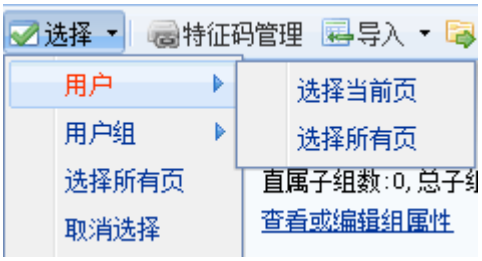

点击『类型』标签，可以选择列出不同类型的用户，方便管理，如下图所示：


点击『类型』、『描述』、『其他信息』、『状态』等标签后的，即可对用户/用户组进行升降序排列。

在【用户管理】界面勾选用户（组），然后点击 删除 按钮即可批量删除用户（组）。

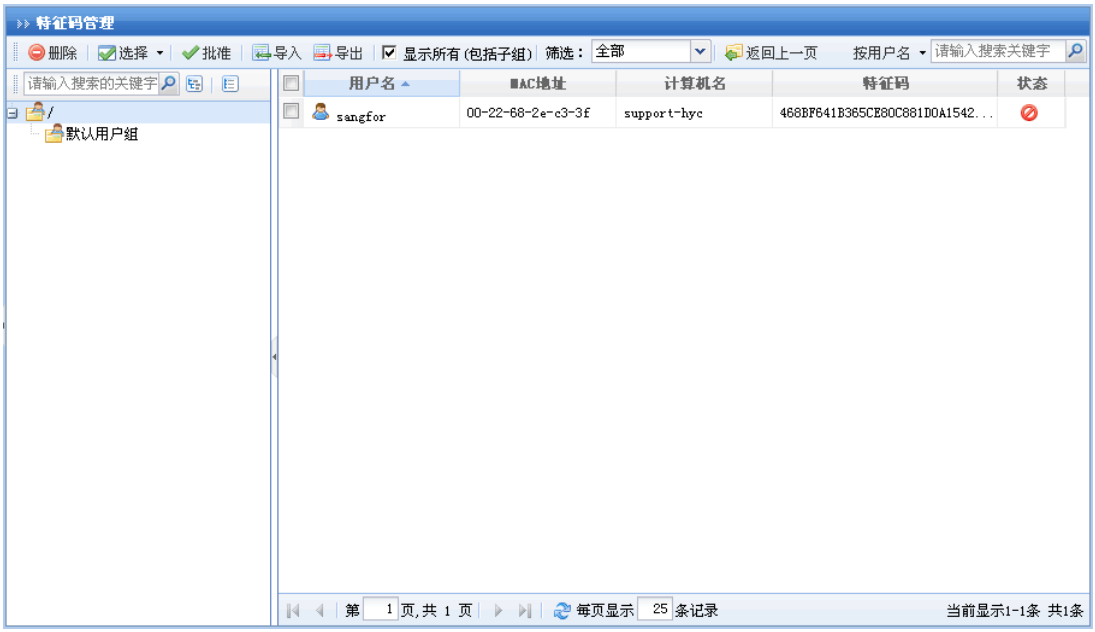
勾选好某个目标用户（组），点击 编辑 按钮，可进入用户（组）信息编辑页面，对目标用户（组）进行修改。

点击 选择 按钮，可以按照用户、用户组选择显示当前页或者所有页上的用户。也可以取消选择，如下图：




## 3.1.4. 特征码管理

点击 特征码管理 按钮，进入【特征码管理】配置页面，如下图所示：

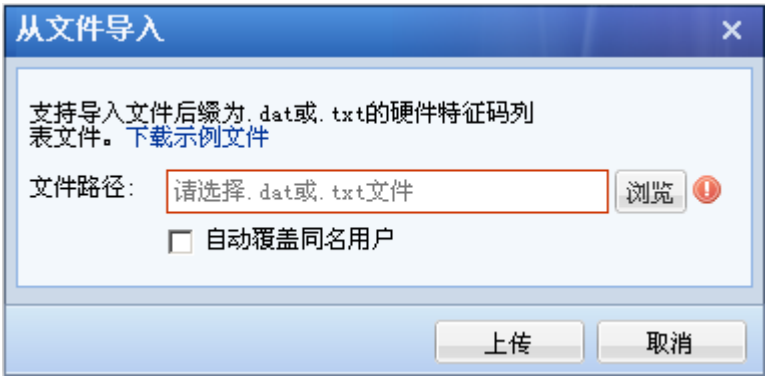



勾选用户，点击 删除 按钮即可批量删除用户特征码。

点击 选择 按钮，可以选择所有用户的特征码或者取消选择。

勾选用户，点击 批准 按钮即可批量审批用户特征码。

点击 导入 按钮，则手动导入用户的硬件特征码，如下图所示：

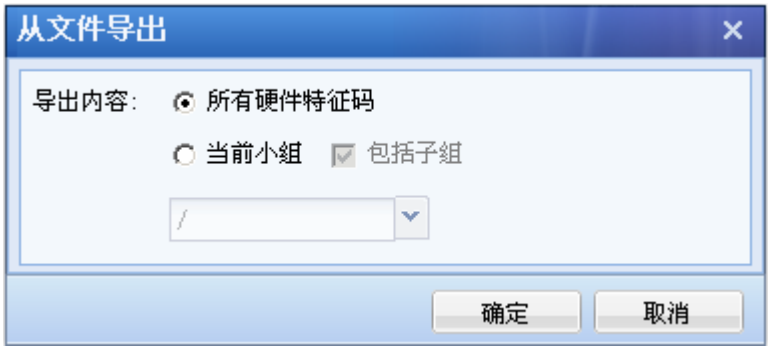



点击 下载示例文件 按钮，可以根据里面的示例格式来编写特征码文件。

勾选[自动覆盖同名用户]，则从文件导入特征码会自动覆盖列表中已有的同名用户的特征码。

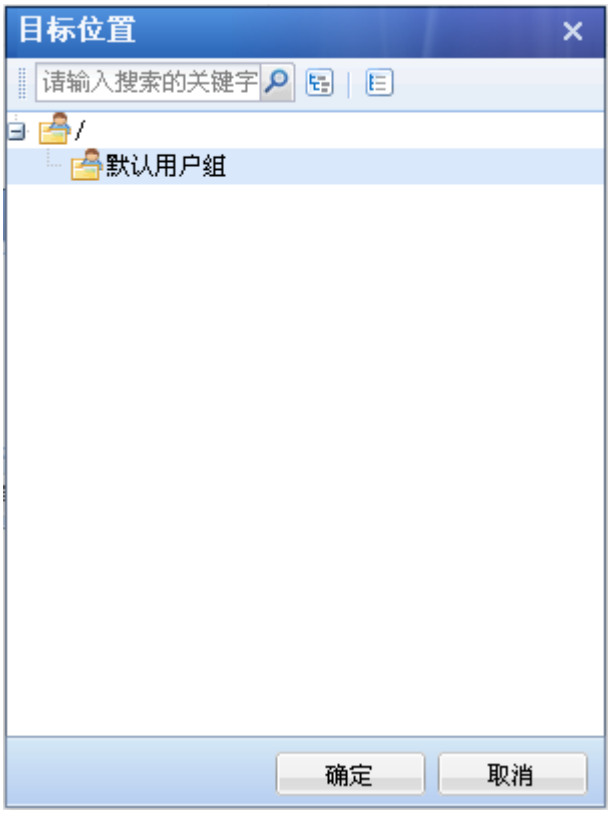
点击 浏览 按钮，选择编辑好的特征码文件，点击 上传 按钮即可。

点击 导出 按钮，则手动将列表中的硬件特征码导出到文件中，如下图所示：

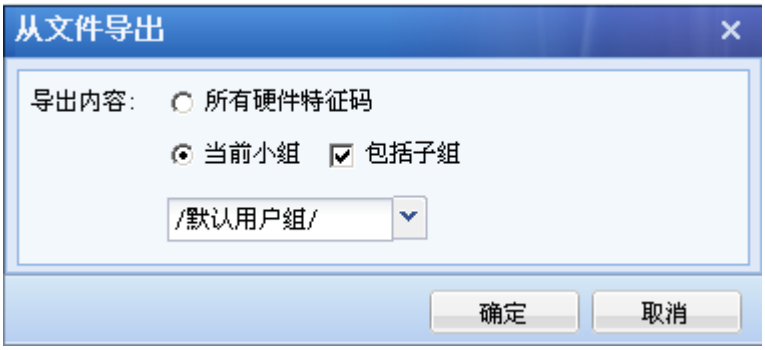



选择[所有硬件特征码]，则点击 确定 按钮，将列表中所有用户特征码全部导出到文件中。

选择[当前小组]，点击下拉框，如下图所示：

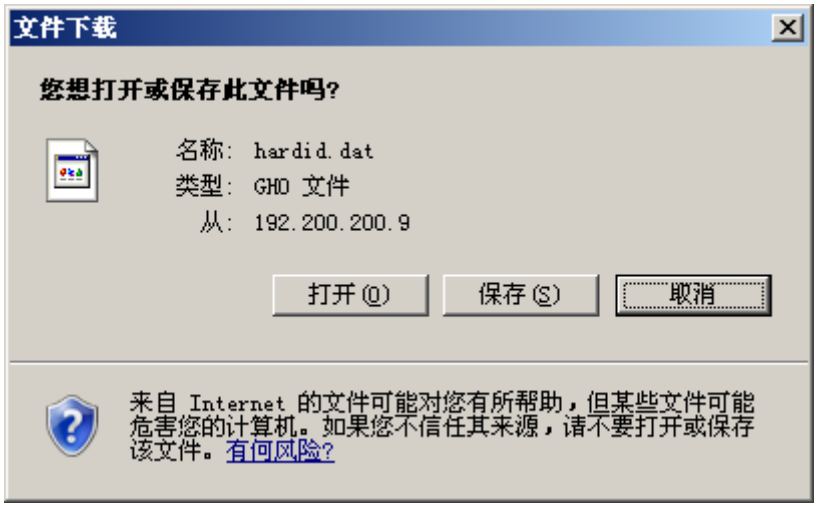



点击导出硬件特征码的用户组，点击 确定 按钮，如下图所示：




点击 确定 按钮，则将选定用户组中的用户的特征码导出到文件中。

如下图所示：




若勾选了[包括子组]，则选定用户组的子组所属用户的特征码也同样被导出。

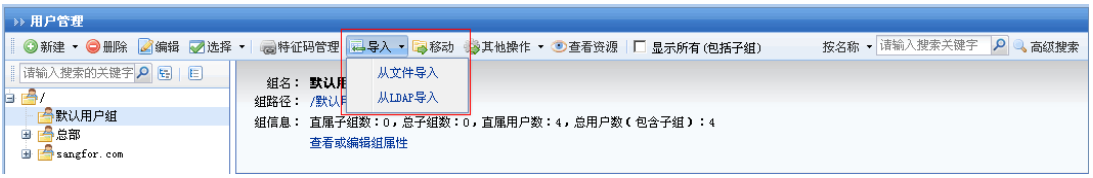
勾选[显示所有（包括子组）]，则在列表中显示所有用户的硬件特征码，否则只显示当前用户组所属用户的硬件特征码。

在『筛选』中，可以分别选择显示[全部]、[已审批]、[未审批]的硬件特征码。

页面右上角的搜索，可以选择[按用户名]或[按计算机名]来搜索相应的硬件特征码。

## 3.1.5. 导入用户

『用户管理』中的『导入』分[从文件导入]和[从 LDAP 导入]两种。




第一种：选择[从文件导入]，如下图所示：


若选择[从文件中（*.csv）导入用户]，如下图所示：

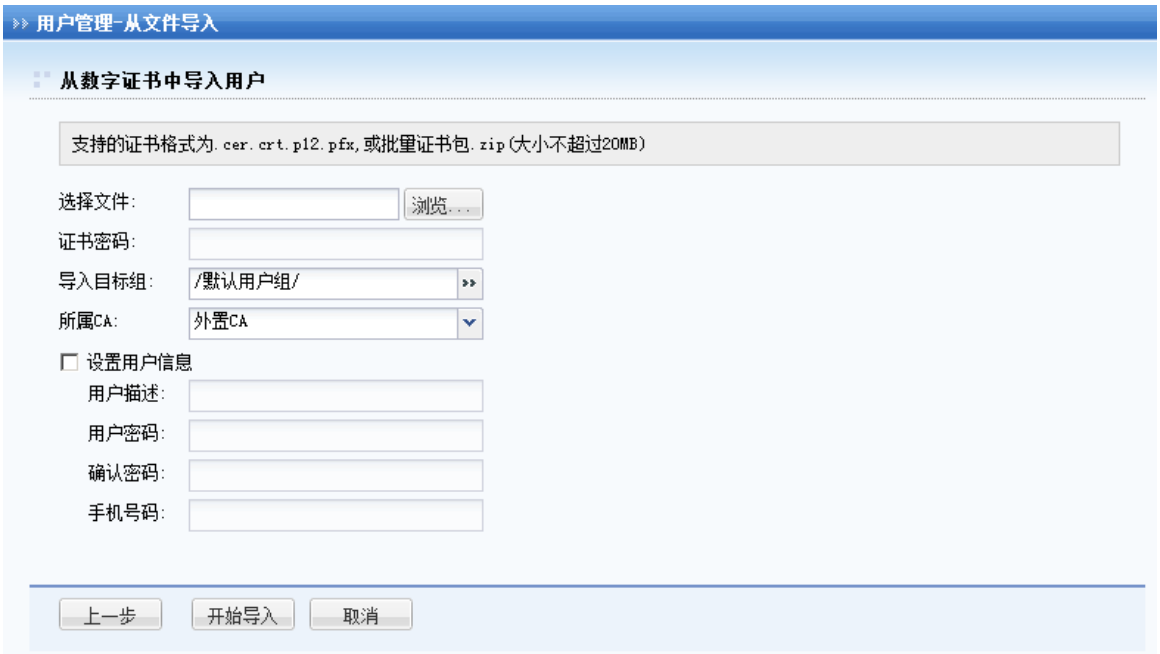
可以通过 csv 文件批量导入用户的账号，支持“用户名”、“所属组路径”、“描述”、“密码”、“手机号码”、“虚拟 IP 地址”等信息的导入，其中“用户名”为必填项，其他均为选填项，点击 下载示例文件，查看编写导入文件的格式。

勾选[未指定用户组的用户导入到]，在下拉框中选择用户组，那么没有在文件中指定用户组的用户就会被导入到该用户组中。

勾选[用户所属组不存在时，自动创建]，如果在本地没有该用户组就会自动创建新用户组；对于本地已存在的用户，若选择继续导入并覆盖已存在用户时，当所导入用户列表中的用户账号和设备用户列表中的原有用户名字冲突（相同），新导入的用户信息会覆盖原有的用户信息；若选择跳过，则不导入该用户。

选择编辑好的文件，点击 下一步，完成。

若选择[从数字证书中导入用户]，如下图所示：




可通过 cer、crt、p12、pfx 后缀的数字证书或批量证书包导入证书用户的账号。

『证书密码』，如果证书有密码，需要填写证书密码。

『导入目标组』选择导入证书用户所属的用户组。

『所属 CA』选择导入证书用户所属的 CA。

勾选[指定用户信息]，需要填写『用户描述』、『用户密码』、『确认密码』、『手机号码』。，导入的证书用户会继承相应的信息。不勾选将采用默认配置，属于默认用户组，描述、密码、手机号码默认为空。

若选择[从文件中（*.xml）导入组织结构]，如下图所示：

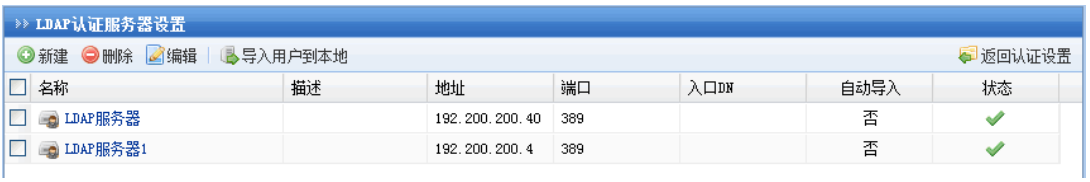

『选择文件』中选择编辑好的文件。

点击 下载示例文件 按钮，可以查看编写格式。

『导入目标组』选择将组织结构导入到当前某个用户组下。

第二种：选择[从 LDAP 导入]，从 LDAP 服务器中导入相应的用户、用户组等信息。

如下图所示：




点击 新建，弹出重新建立一个 LDAP 服务器的界面，具体设置可以参考 4.4『认证设置』中的『LDAP 认证模块』设置。

勾选列表中的 LDAP 服务器，点击 删除，则可以单个或者批量删除 LDAP 服务器。

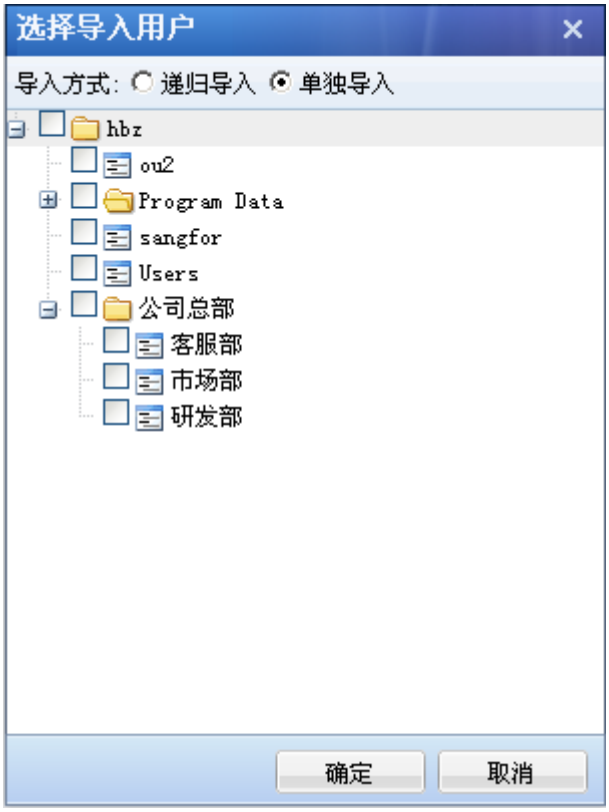
勾选列表中的 LDAP 服务器，点击 编辑，则可以编辑所选择的 LDAP 服务器。

勾选列表中的 LDAP 服务器，点击 导入用户到本地，如下图所示：

『从此 LDAP 服务器导入』显示当前选择的 LDAP 服务器的名称。

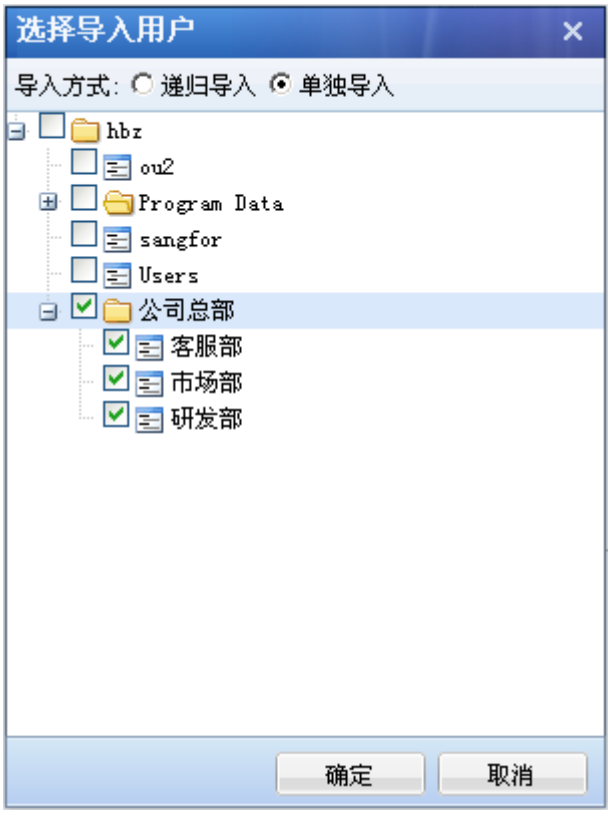
『选择导入用户』显示当前要导入到用户管理列表中的 LDAP 服务器中的用户。

点击 选择导入用户，如下图所示：

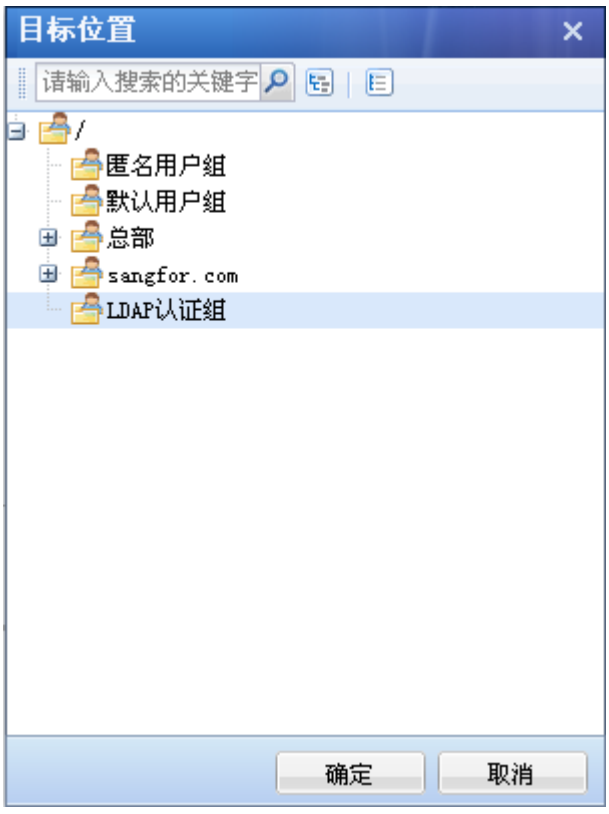



『导入用户』分为两种方式：[递归导入]和[单独导入]。

第一种：选择[单独导入]，勾选需要导入的 LDAP 用户组，如下图所示：




『选择导入到的本地目标组』选择要把 LDAP 中的用户导入到哪个用户组，如下图所示：

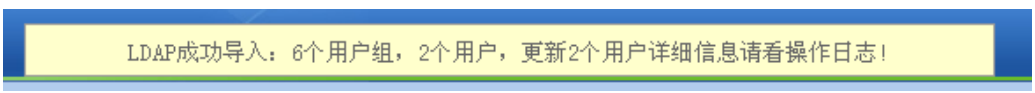


『导入方式』分两种: [复制 LDAP 上的组织结构到目标位置，并导入用户到相应组中]和[所有用户都导入到目标组，忽略 LDAP 上的组织结构]。

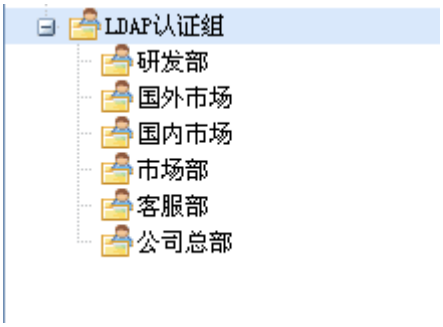
若选择[复制 LDAP 上的组织结构到目标位置，并导入用户到相应组中]，那么将用户导入的同时，即可将勾选中的几个 OU 同步到所选的本地用户组中。

设置完成后，如下图所示：


点击 保存并立即同步，如下图所示：



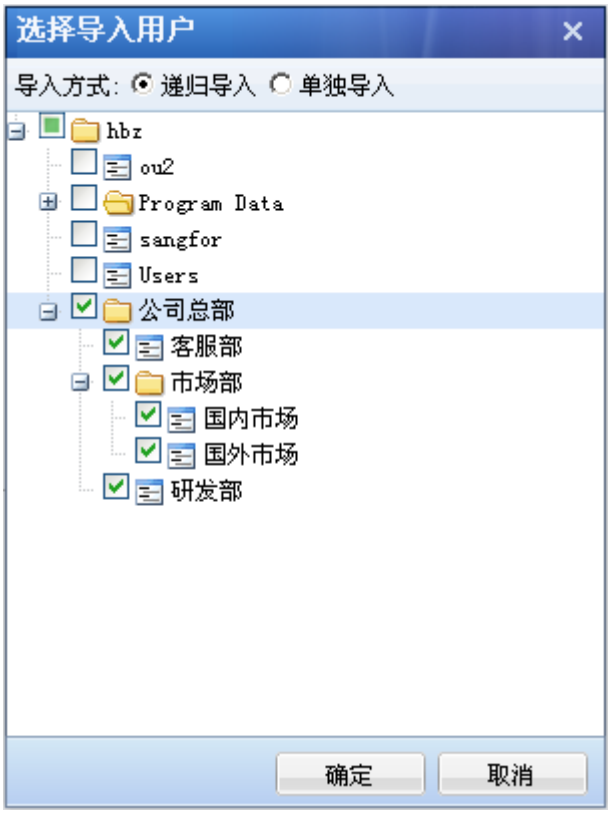

导入成功后，效果如下图所示：



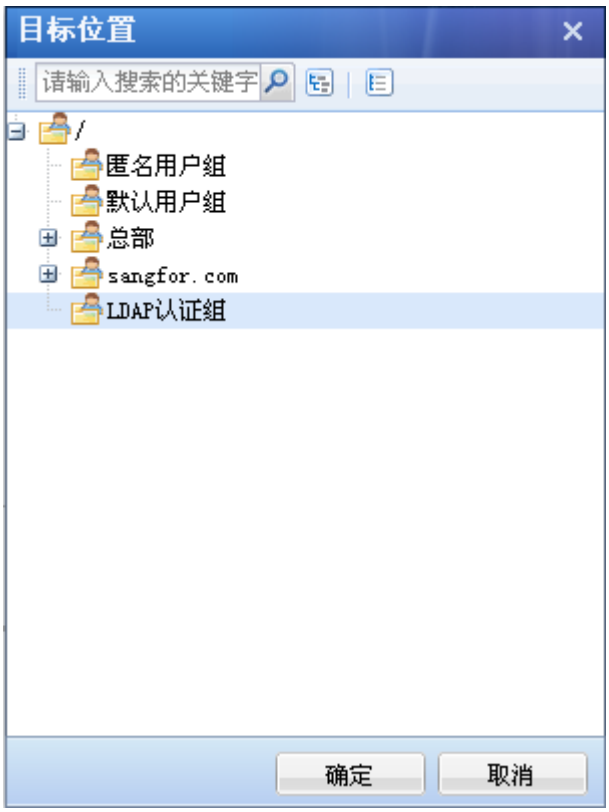

若选择[所有用户都导入到目标组，忽略 LDAP 上的组织结构]，那么就只会将 OU 中的用户导入到指定的本地组中。

第二种：[递归导入]是将 LDAP 中的用户组及其用户按照域中的组织结构导入。

选择[递归导入]，勾选需要导入的 LDAP 用户组，如下图所示：



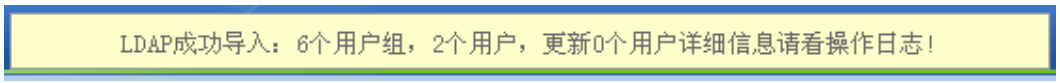

在『选择导入到的本地目标组』中选择要把 LDAP 中的用户导入到哪个用户组，如下图所示：



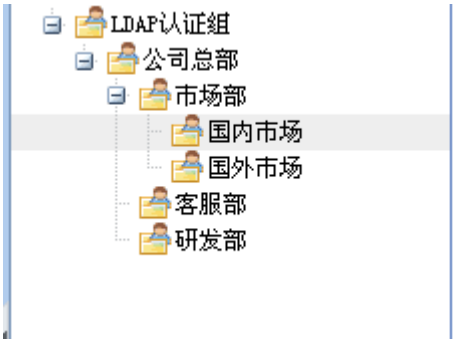

若选择[复制 LDAP 上的组织结构到目标位置，并导入用户到相应组中]，那么将用户导入的同时，即可将勾选中的几个 OU 以及它们之间的组织结构关系同步到所选的本地用户组中。

设置完成后，如下图所示：


点击 保存并立即同步，如下图所示：




导入成功后，效果如下图所示：



若选择[所有用户都导入到目标组，忽略 LDAP 上的组织结构]，那么就只会将 OU 中的用户导入到指定的本地组中。

『本地已经存在的用户』有两种处理方式：[继续导入，覆盖已经存在的用户]和[忽略该用户，不导入本地已存在的用户]。

勾选[继续导入，覆盖已经存在的用户]，若本次导入的用户账号和本地已经存在的用户账号同名，则直接覆盖原有账号。

勾选[忽略该用户，不导入本地已存在的用户]，若本次导入的用户账号和本地已经存在的用户账号同名，则直接忽略该用户，不导入本地。

『自动导入设置』，可以把 LDAP 服务器内所有用户账号自动导入到 SSL VPN 本地用户列表，在设备上生成同名的用户。

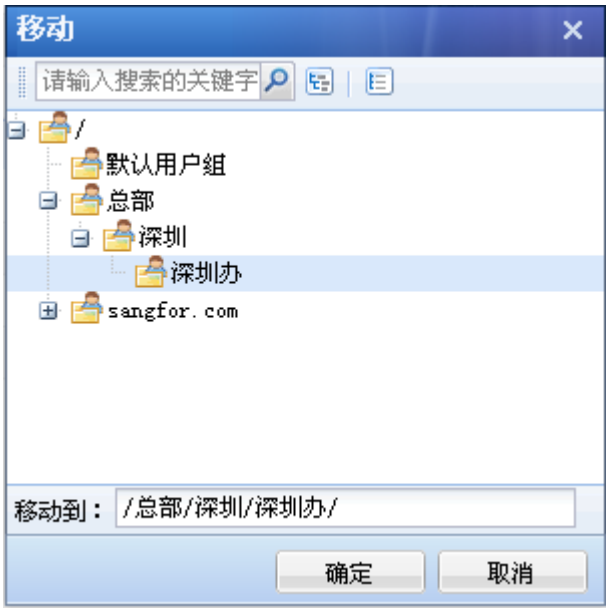
勾选启[用自动导入]，在『自动导入时间间隔』中可以选择“每隔 X 分钟自动导入”或者“定时导入”。点击 操作日志 可以查看自动导入的结果。

如下图所示：


**自动导入可以同时导入用户和用户组。**

『用户管理』中的『移动』功能，可以将列表中选定的用户或用户组移动到其他用户组，

如下图所示：




选择想要移动到的目标用户组，点击 确定 按钮，那么在用户管理列表中选定的用户或用户组就会移动到该用户组。

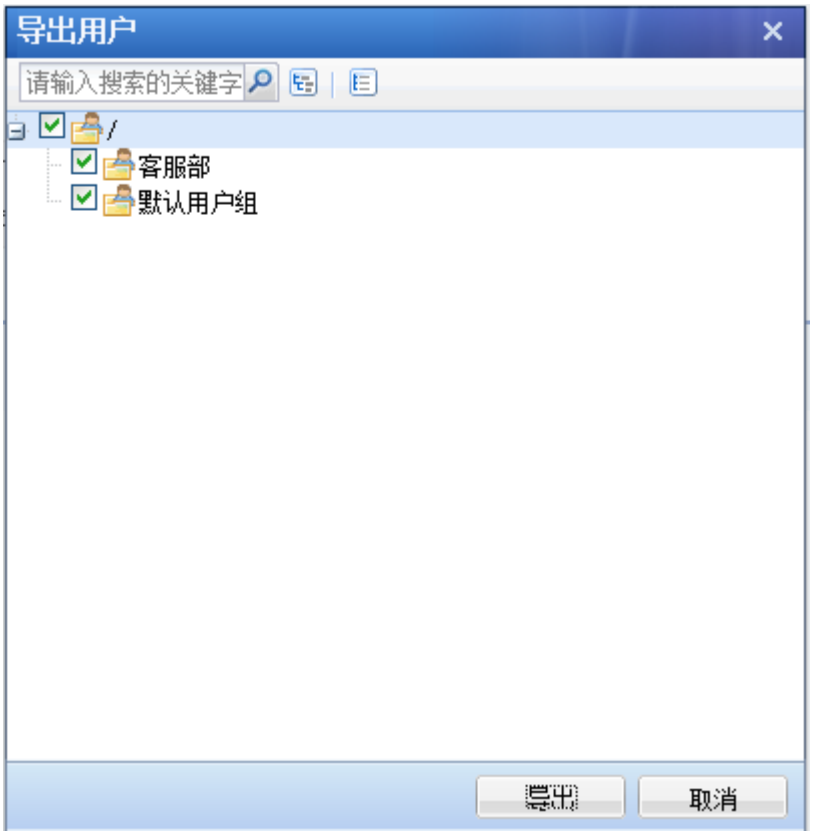
## 3.1.6. 其他操作

『用户管理』中的『其他操作』功能，包括[导出]、[绑定角色]、[从账号设置]、[批量生成证书]、[批量指定 CA]、[批量创建 USB-KEY]、[下载 USB-KEY 驱动]、[下载 USB-KEY 导入控件]。

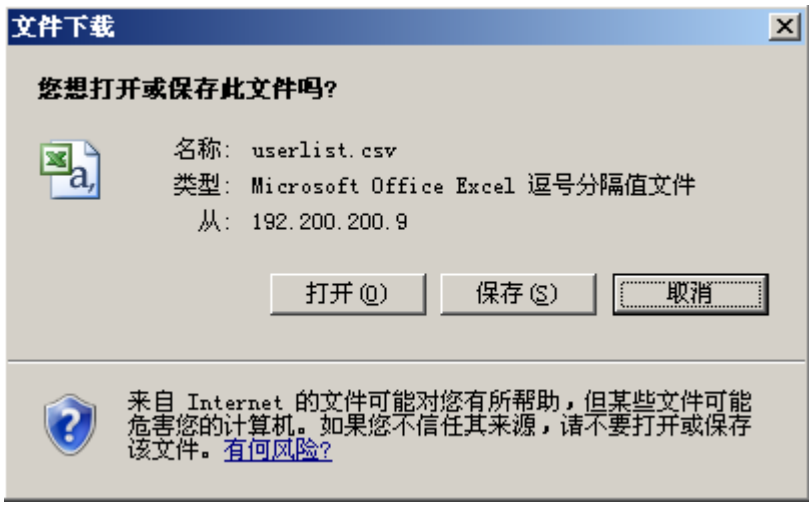
### 3.1.6.1. 导出

点击 导出 按钮，如下图所示：


点击 选择导出内容 按钮会显示出所有的用户组，如下图所示：



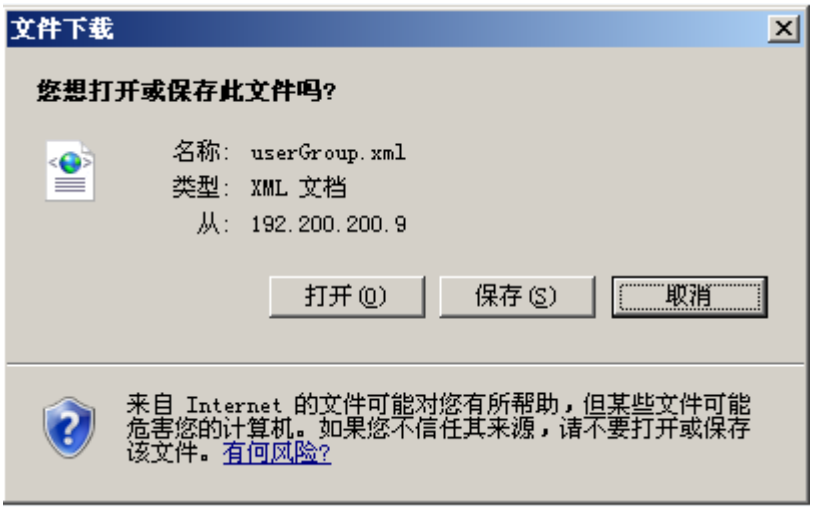

勾选需要导出的用户组，点击 导出 按钮，即可导出后缀为 csv 的文件，如下图所示：




导出信息包含所勾选的用户组中用户的用户名，所属用户组，密码（经过深信服公司研发的私有算法加密），手机号码，虚拟 IP，描述，最近一次登录信息，如下图所示：

| A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|
| #用户名 | 所属组路径 | 密码 | 手机号码 | 虚拟IP地址 | 描述 | 最近一次登陆 |
| zj | /默认用户组 | { 197fba71256ab35f3 } | | | | 2011/11/17 3:01 |
| sangfor | / | { 197fba71256ab35f3 } | | | | 2011/11/17 21:12 |
| liushiqin | / | { 197fba71256ab35f3 } | | | | 2011/11/17 1:48 |
| testdsz | / | { 197fba71256ab35f3 } | | | | 2011/11/17 2:09 |
| debug | / | { 197fba71256ab35f3 } | | | | 2011/11/17 19:53 |
| xxl | / | { 197fba71256ab35f3 } | | | | 2011/11/17 20:15 |
| xxl1 | /客服部 | { 197fba71256ab35f3 } | | | | 从未登陆 |

点击 导出组织架构 按钮，即可导出所勾选的用户组所构成的组织架构，如下图所示：

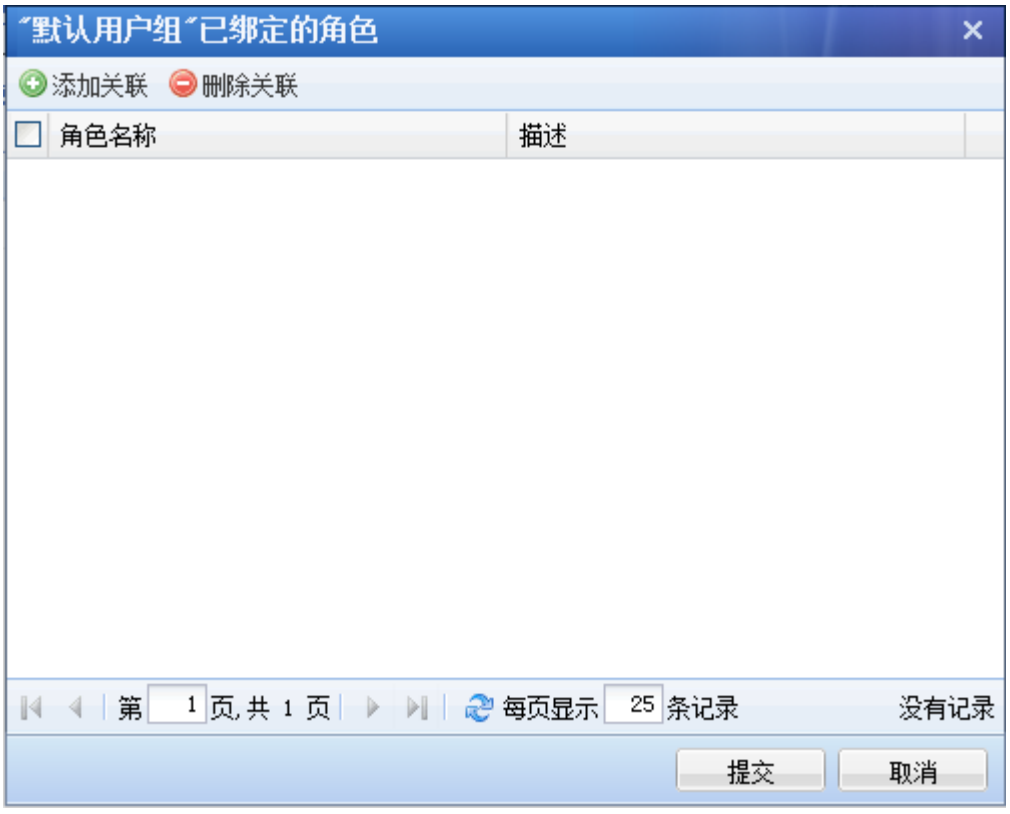



文件打开后显示组织结构信息，如下图所示：

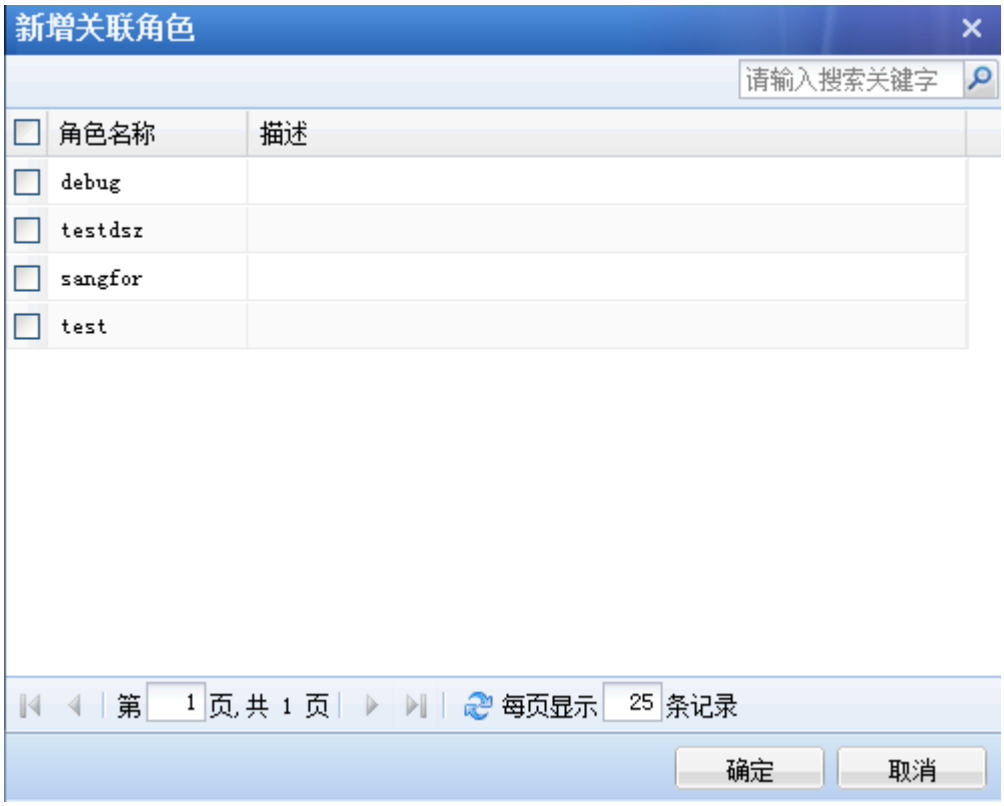
```
<?xml version="1.0" encoding="utf-8" ?>
- <root>
  - <node name="总部" note="">
    - <node name="深圳" note="">
        <node name="深圳办" note="" />
      </node>
    </node>
  - <node name="sangfor.com" note="">
    - <node name="ou2" note="LDAP组映射自动生成用户组">
        <node name="ou4" note="LDAP组映射自动生成用户组" />
      </node>
    - <node name="ou1" note="LDAP组映射自动生成用户组">
        <node name="ou3" note="LDAP组映射自动生成用户组" />
      </node>
    </node>
    <node name="LDAP认证组" note="" />
  </root>
```

### 3.1.6.2. 绑定角色

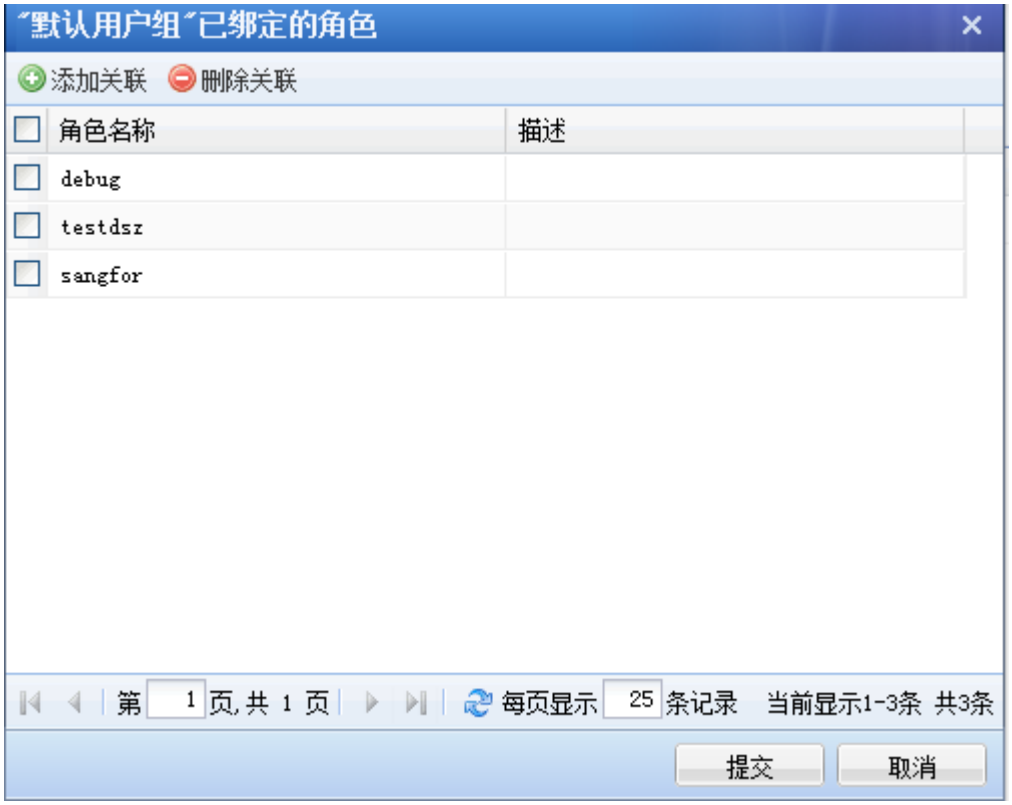
在『用户管理』列表中选择用户或用户组，点击 绑定角色 按钮，在此处可以给用户或用户组关联角色，如下图所示：



点击 添加关联 按钮，会显示出所有在『角色授权』中定义的角色，如下图所示：




勾选角色，点击 确定 按钮，给用户绑定角色成功，如下图所示：

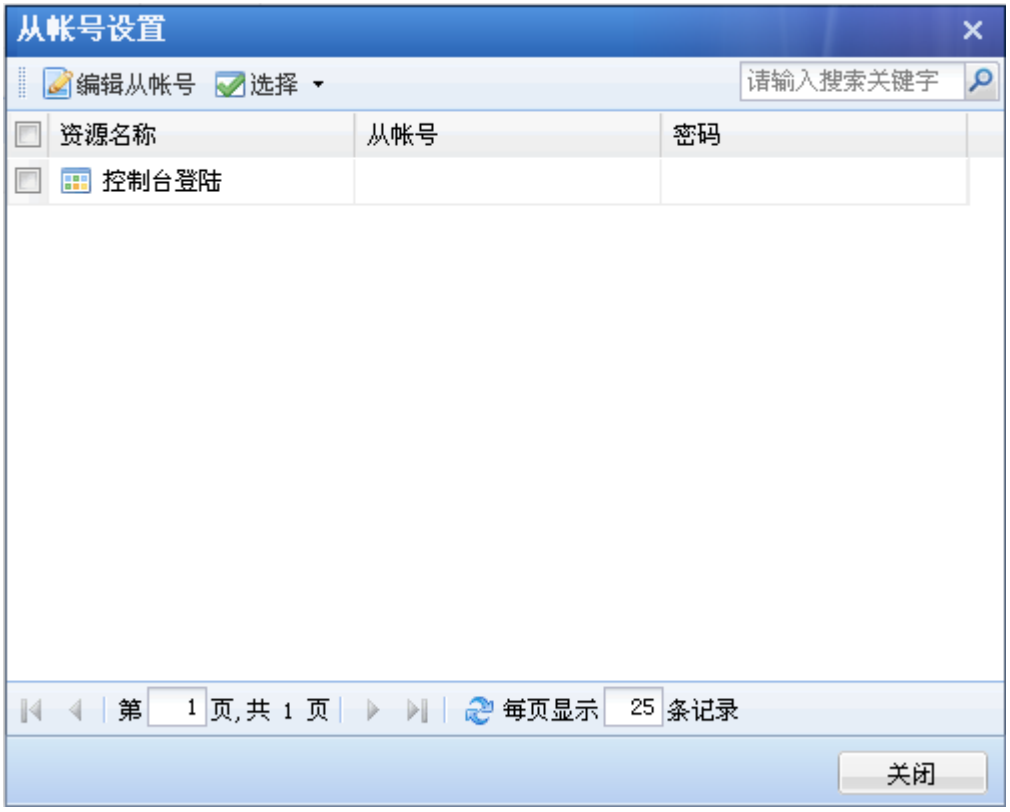



点击 提交 按钮，保存配置。

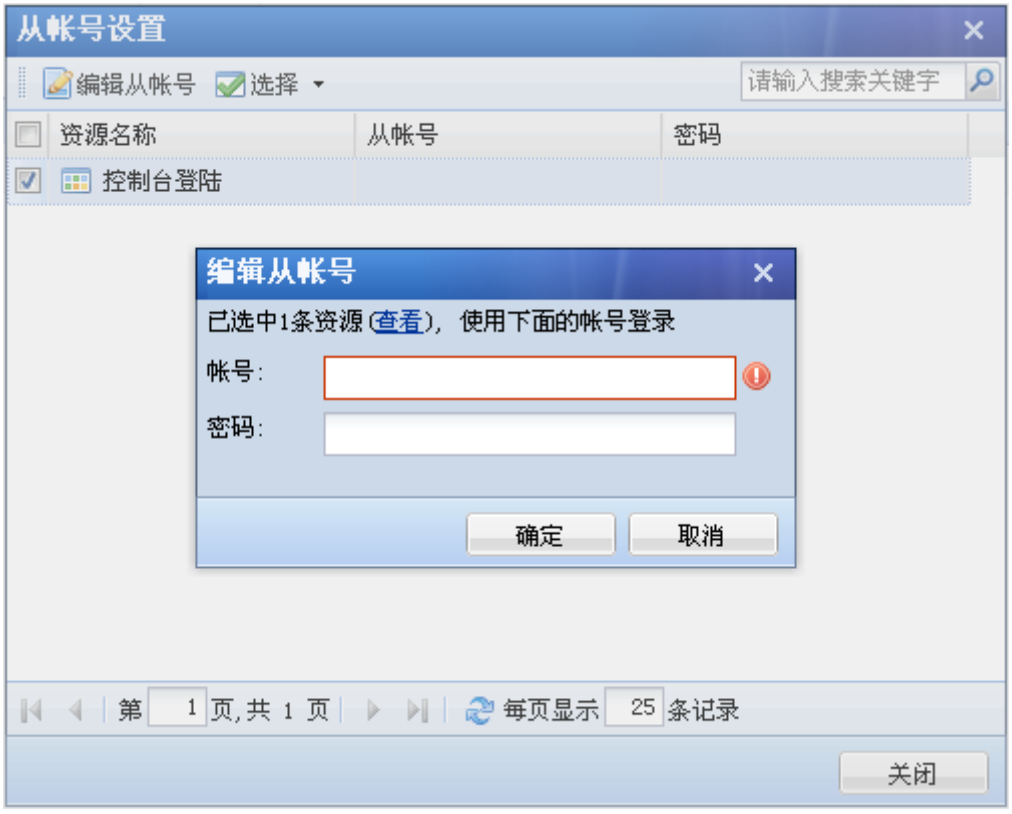
### 3.1.6.3. 从账号设置

[从账号设置]当用户使用启用了单点登录的资源时，用来设置登录应用系统的账号和密码。当用户点击单点登录资源的时候，SSL 设备自动提交从账号设置的账号和密码。

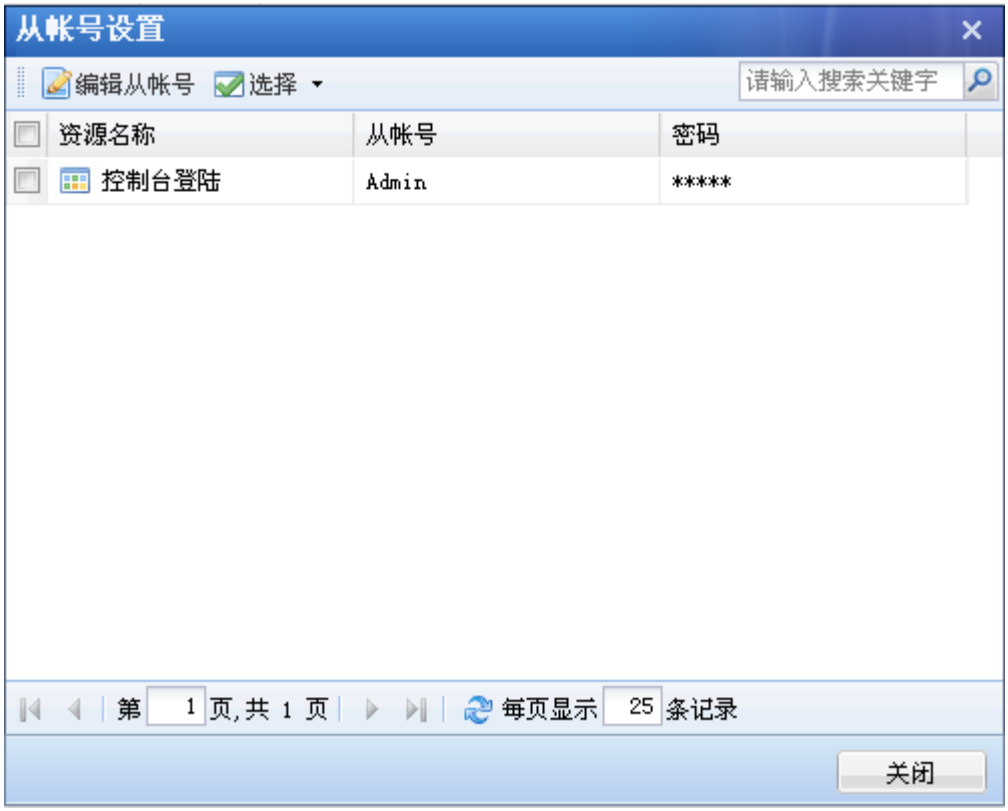
勾选关联了单点登录资源的用户，选择[从账号设置]，弹出【从账号设置】对话框，如下图所示：




勾选资源，点击 编辑从账号 按钮，如下图所示：



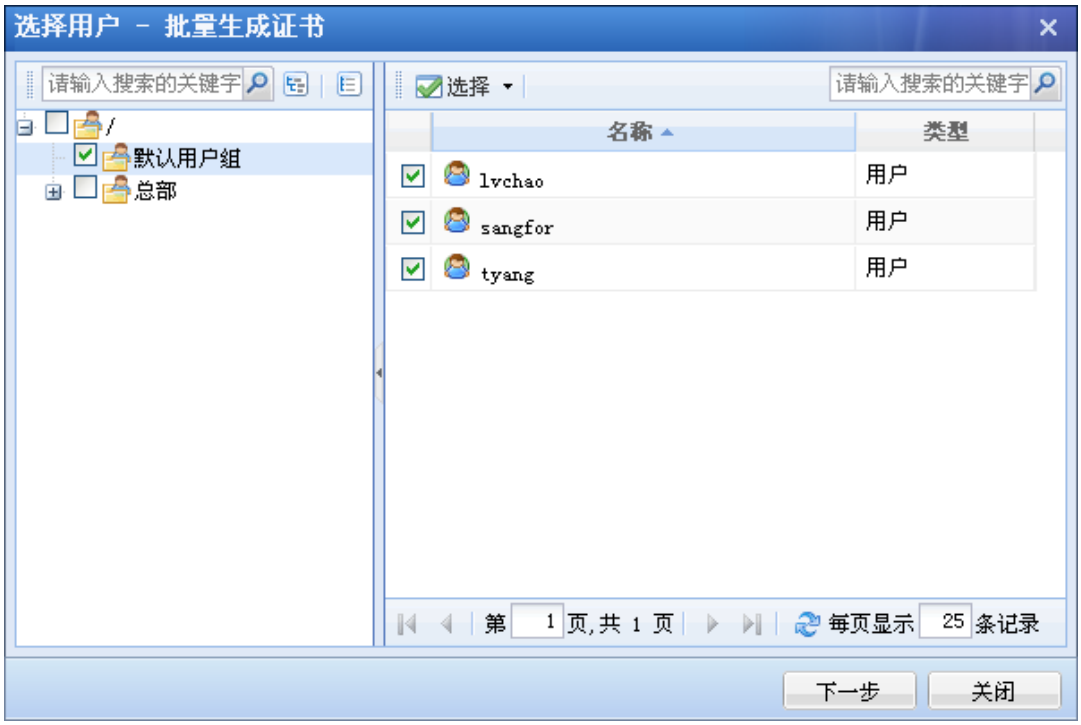
在【编辑从账号】对话框中填写正确的账号和密码，点击 确定 按钮，如下图所示：




点击 关闭 按钮，完成设置，并点击 配置生效 按钮，保存配置。

### 3.1.6.4. 批量生成证书

点击 批量生成证书 按钮，可以同时为多个用户生成证书，如下图所示：

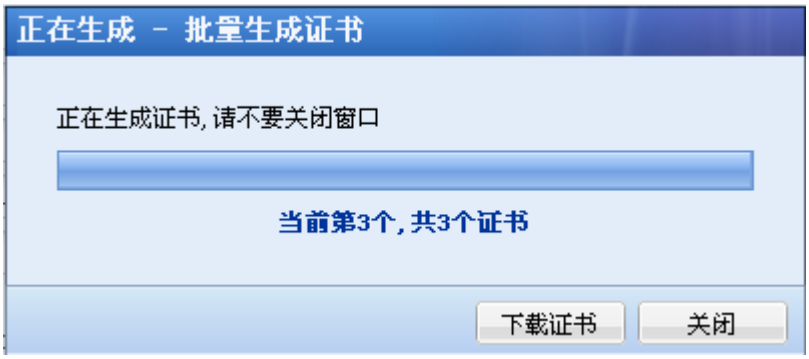



勾选需要生成证书的用户，点击 下一步，如下图所示：

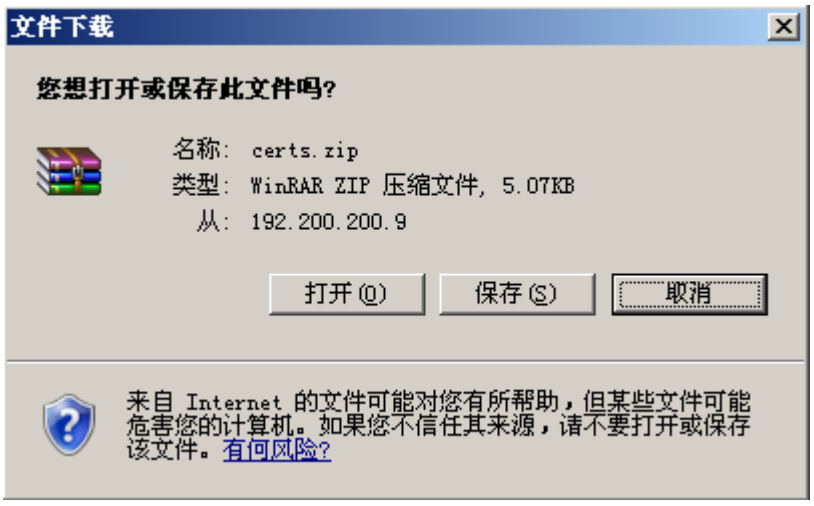

数字证书相关信息中的『国家』、『省份』、『城市』、『公司』、『部门』、『过期时间』信息

存在默认值，可以修改，修改后点击 记住该次设置，以后默认使用，把当前『证书密码』、『颁发给』除外的所有证书信息作为默认配置保存。后续用户生成数字证书可直接调用该默认配置。其中『颁发给』和『E-mail』信息无法编写。『颁发给』显示的是与用户名相同。

点击 开始生成 按钮，按照次序一次生成用户证书，如下图所示：

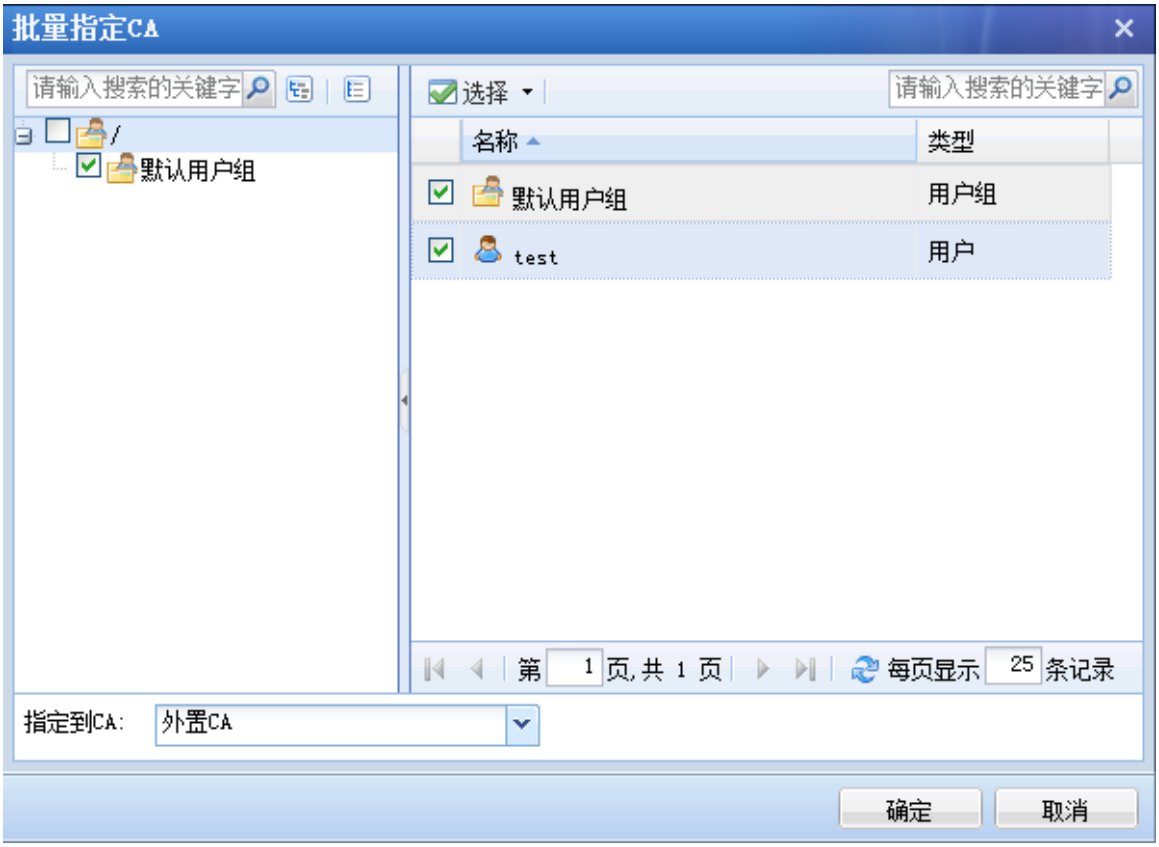



点击 下载证书 按钮，将生成的证书保存下来，如下图所示：




### 3.1.6.5. 批量指定 CA

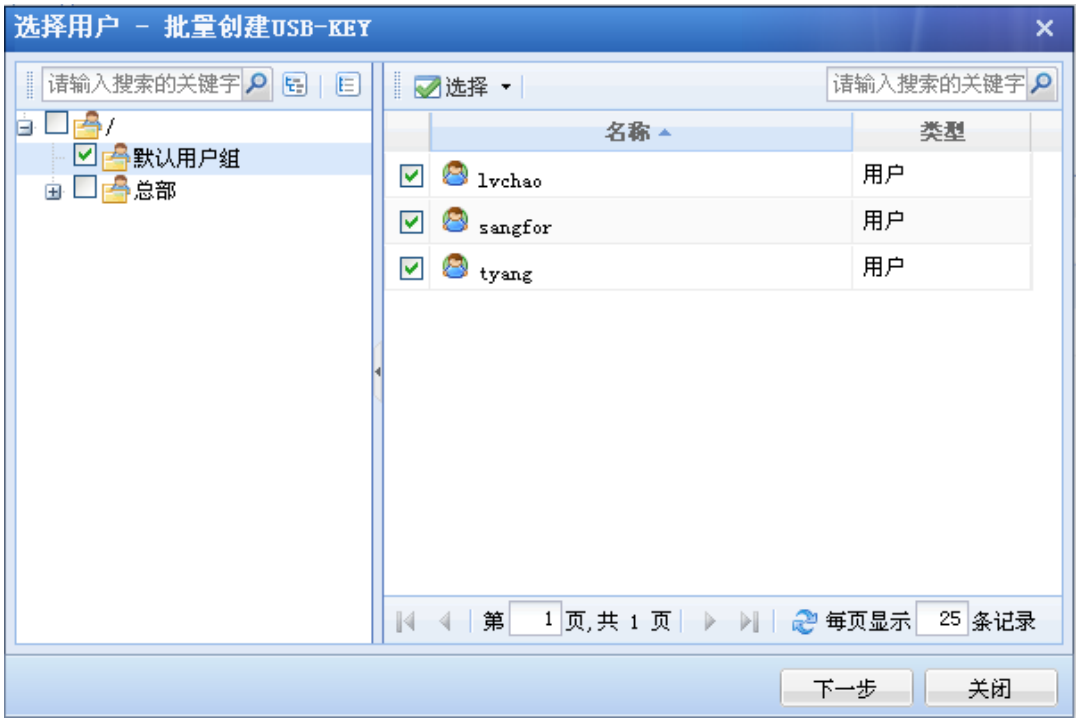
点击 批量指定 CA 按钮，可以同时为多个用户指定所属的第三方 CA，如下图所示：



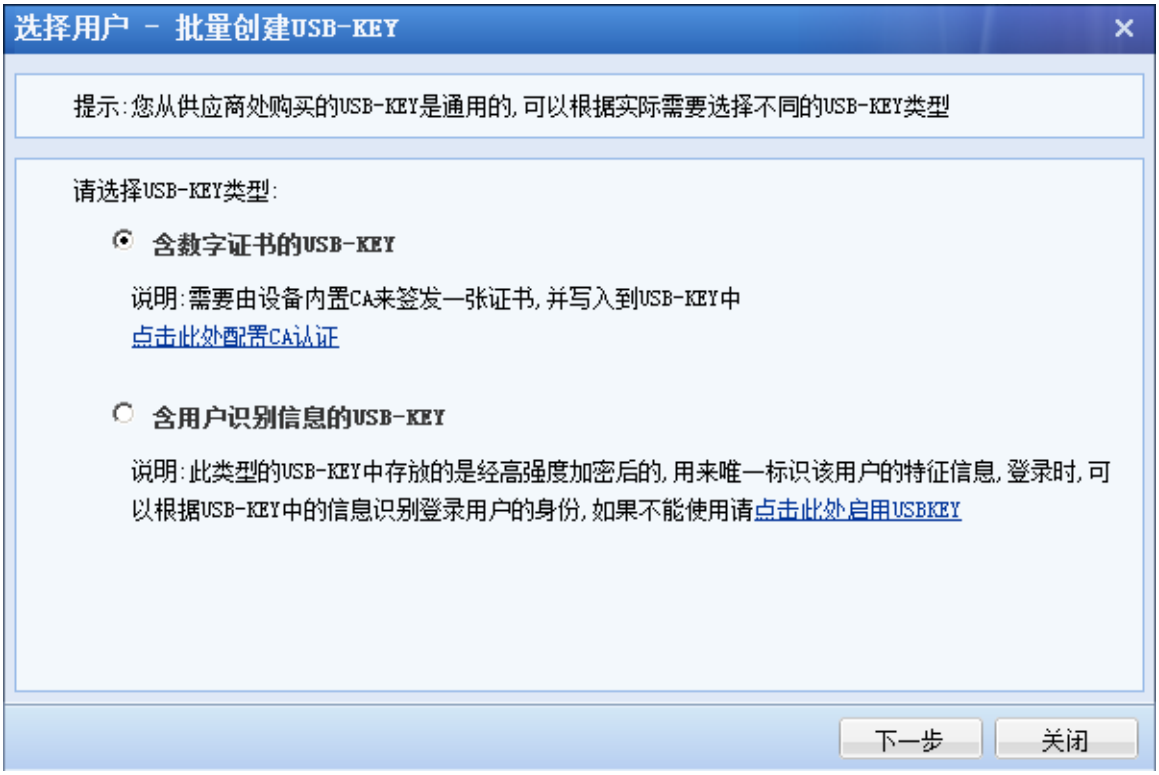

勾选需要指定 CA 的用户，然后选择指定到某个 CA，点击 确定 。

### 3.1.6.6. 批量创建 USB-KEY

点击 批量创建 USB-KEY 按钮，可以同时给多个用户生成 USB-KEY，如下图所示：

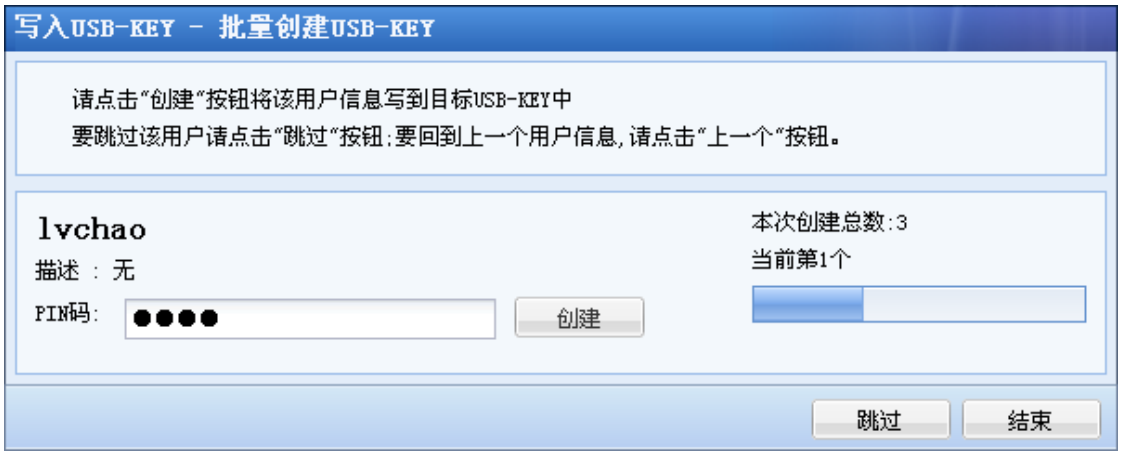



点击 下一步，如下图所示：




点击 下一步，如下图所示：

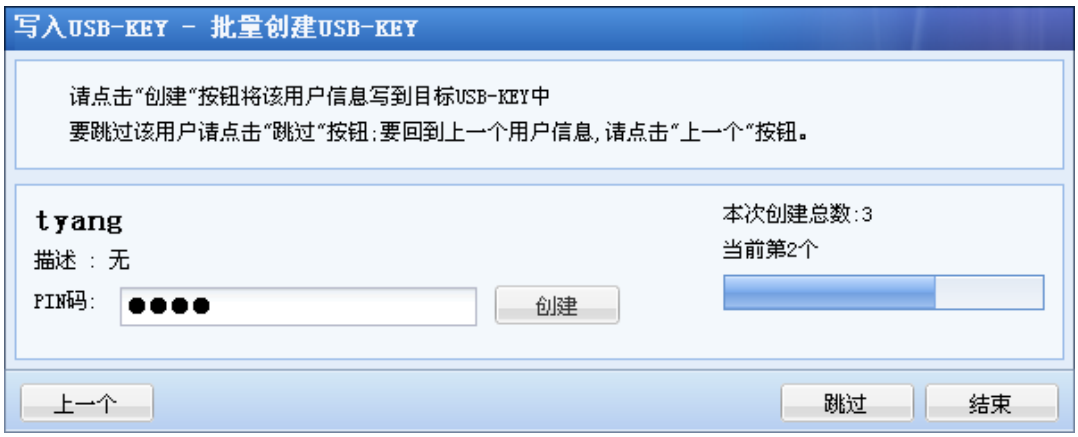

填入默认 PIN 码，点击 开始创建，如下图所示：




插入 USB-KEY，点击 创建 按钮，开始创建证书，将该用户信息写到目标 USB-KEY 中，然后再开始生成下一个用户的 USB-KEY。

如果某一个用户不需要生成 USB-KEY，要跳过该用户请点击 跳过 按钮。

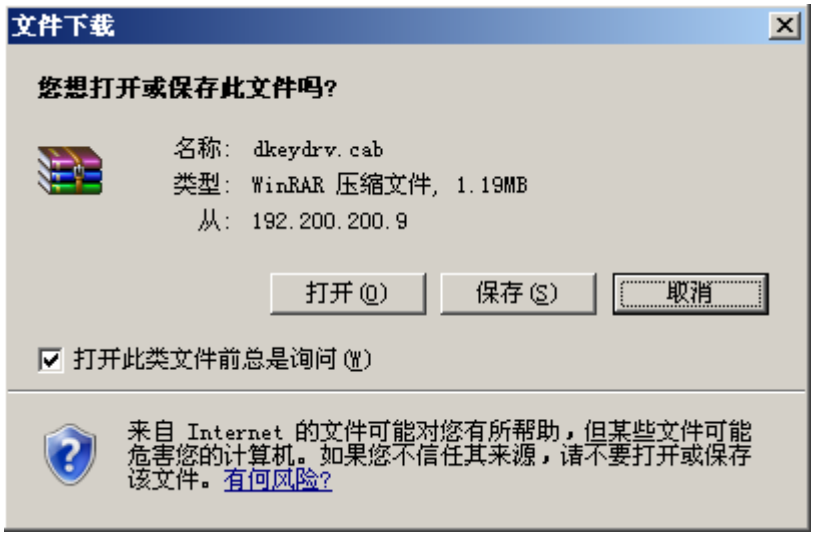
如果要回到上一个用户信息，请点击 上一个 按钮，如下图所示：




如果需要停止设置生成 USB-KEY，则点击 结束 按钮。

### 3.1.6.7. 下载 USB-KEY 驱动

点击 下载安装 USB-KEY 驱动，出现以下界面：



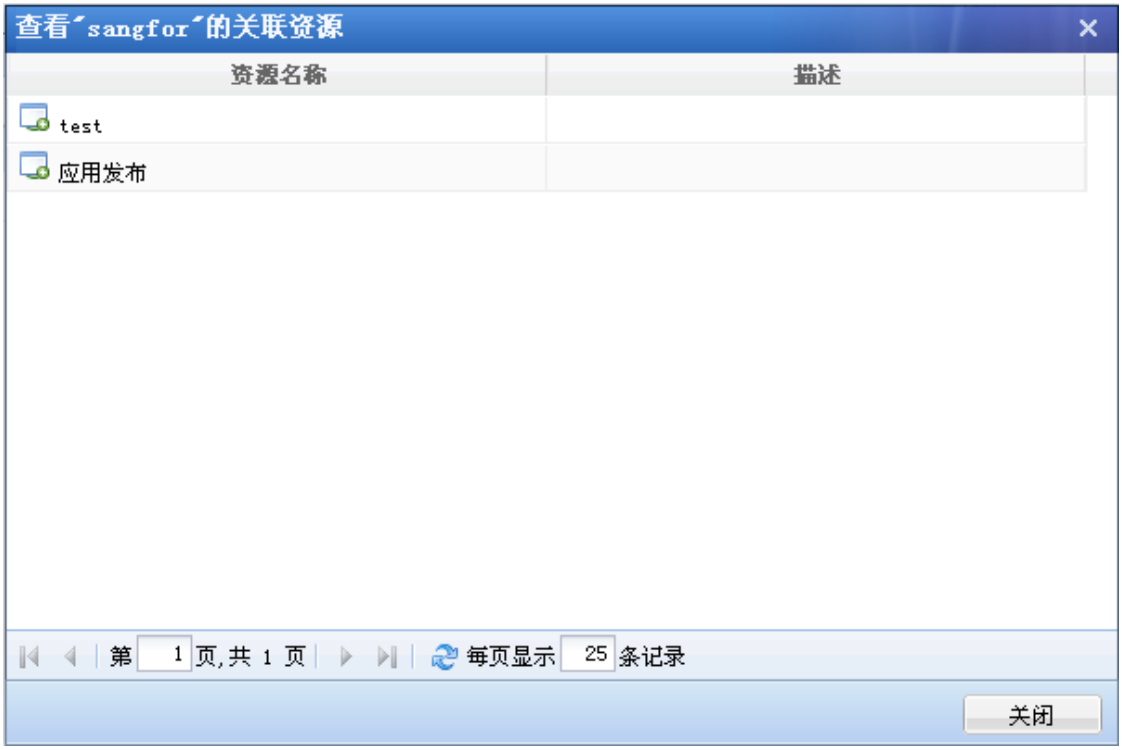

下载后，安装 USB-KEY 驱动。

### 3.1.6.8. 下载 USB-KEY 导入控件

点击 下载安装导入控件，将文件名为“DKeyImport.exe”的安装包下载后，安装完成。

### 3.1.7. 查看资源

在『用户管理』选择某一个用户或用户组，点击 查看资源 按钮，则会显示所关联的资源，如下图所示：




上图中显示用户“sangfor”关联了两个资源“test”和“应用发布”。

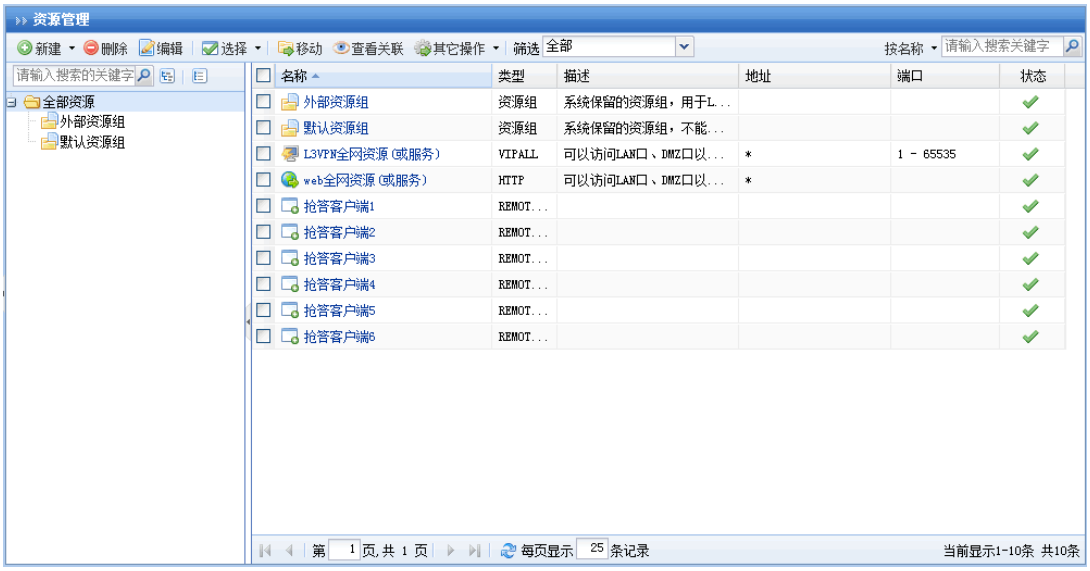
勾选[显示所有（包括子组）]，则会把所有用户都显示到当前页面列表中。

## 3.2. 资源管理

『资源管理』的主要作用是用户定义 SSL VPN 内网的可用资源，包括[WEB 应用]、[TCP 应用]、[L3VPN]和[远程应用]。

WEBUI 路径：『SSL VPN 设置』→『资源管理』。

界面如下图所示：




## 3.2.1. 资源组

为了更好地对资源进行管理、更符合用户使用习惯，以及 SSL VPN 客户端可以更有条理地显示，可以把多个“资源”添加到“资源组”。在资源列表，点击不同的“资源组”显示出该资源组对应“资源”。

WEBUI 路径：『SSLVPN 设置』→『资源管理』→『新建』→『资源组』。

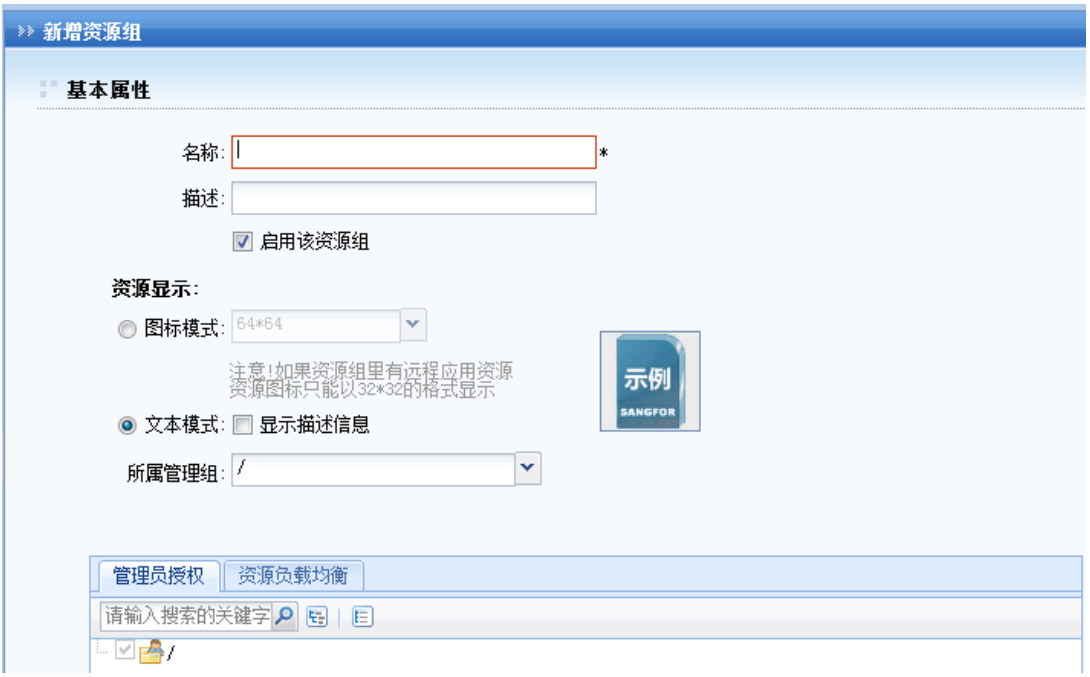
系统默认存在两个资源组，即『外部资源组』和『默认资源组』，界面如下图所示：


『外部资源组』用于 LDAP 绑定资源，只能够修改，不允许删除。

『默认资源组』系统默认保留的资源组，只能够修改，不允许删除。

点击 新建 按钮，选择[资源组]，如下图：


即弹出【新增资源组】对话框，界面如下图所示：




『名称』和『描述』可随意填写便于理解记忆的文字，在『名称』中填写的文字会显示在 SSL VPN 用户成功登录后，出现的“资源组列表”中。

同一个资源组内的资源在“资源组列表”能够以“图标”或“文本”两种方式显示。选择[图标模式]时，在右边下拉框，可设定图标的显示大小，有三种选择：“48*48”、“64*64”、“128*128”。

选择[文本显示]，可勾选右边的[显示描述信息]，在“资源组列表”中显示出该“资源组”内“资源”的描述信息。最后点击 保存（资源图标的具体设置可参考“资源管理”和“图标管理”

章节）。

『所属管理组』即该“资源组”能被哪些管理员编辑和使用。

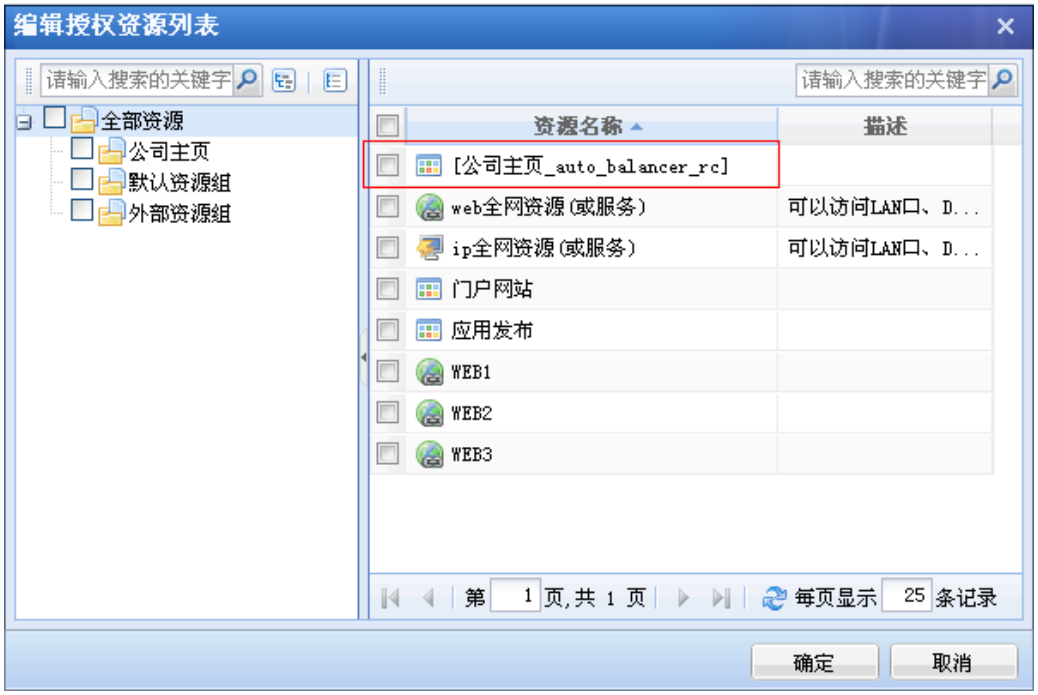
『管理员授权』在这里可以将下级管理员所创建的资源组的拥有权指派给创建该资源组的上级管理员，原来的管理员将无法编辑自己创建的资源组及该资源组里面的资源。

**将下级管理员所创建的资源组的拥有权指派给创建该资源组的上级管理员后，创建该资源的管理员登录控制台后，将无法在资源组和资源页面看见相应的资源组和资源。**

『资源负载均衡』当该资源组有多个相同类型不同 IP 的资源时，可配置资源负载均衡，设备将根据权值选举出来的属于该资源组的资源下发给客户端，实现负载均衡。


『资源负载均衡』的列表中将显示出属于该资源组的资源，在对应的资源后面设置相应的权重（权重范围是 1 至 9，默认为 5）。上图中 WEB1、WEB2、WEB3 都是配置完全相同，仅仅 IP 地址不同的 3 台服务器，权重都是 5。设置完成后，在『角色授权』中会生成一个新

的负载均衡资源，如下图所示：




在角色授权里面将该资源[公司主页_auto_balancer_rc]关联给用户或用户组后，当用户接入 SSLVPN 的时候，前 5 个用户会分得 WEB1 这个资源，接下来登录 SSLVPN 的 5 个用户会会分得 5 个 WEB2 的资源，后面再登录的 5 个用户又分得 WEB3 这个资源，如此循环从而实现 3 个服务器的负载均衡。（将资源组关联给用户或用户组的配置方法可以参考 4.3“角色授权”章节）

用户登录 SSL VPN 后，服务页面显示如下：


点击资源名称即可访问，点击 负载均衡 可以实时更换服务器。

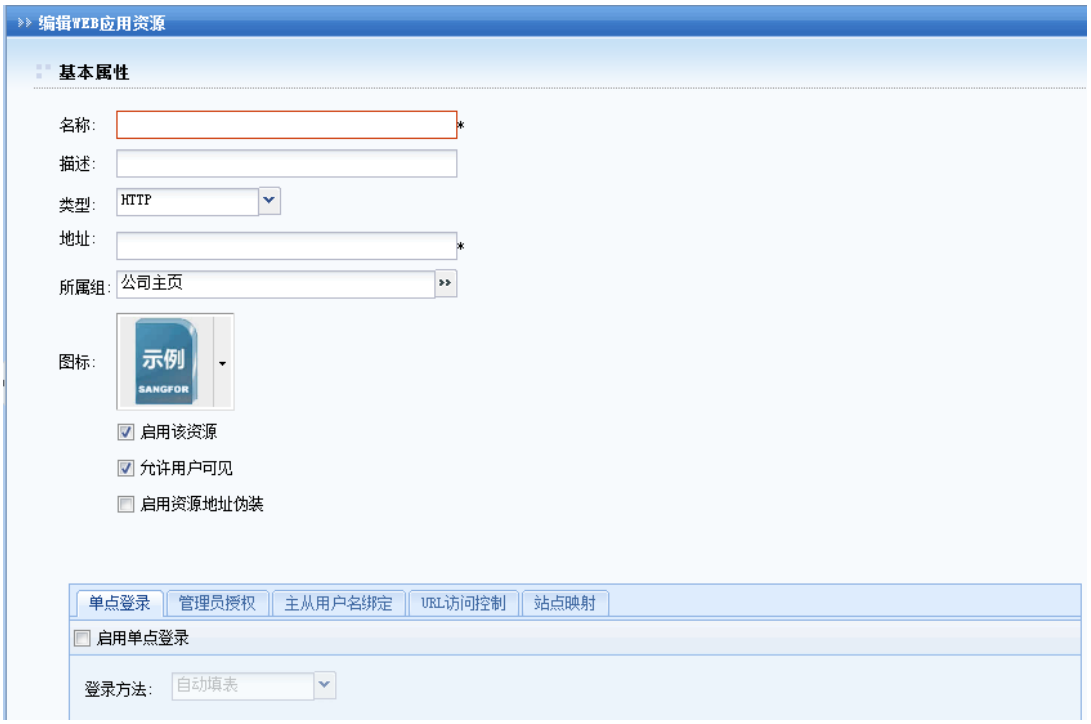
**一个“资源”只能够属于一个“资源组”。最多可建立 100 个“资源组”。**

## 3.2.2. WEB 应用

『WEB 应用』主要用于创建 WEB 类型的资源。

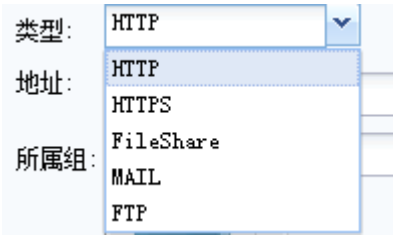
在【资源管理】页面，点击 新建 按钮，如下图：


选择[WEB 应用]，弹出【编辑 WEB 应用资源】对话框，如下图：



『名称』和『描述』可随意填写便于理解记忆的文字，在『名称』填写的文字会显示在 SSL VPN 用户成功登录 SSL VPN 后出现的“资源列表”中。

选择『类型』，包括[HTTP]、[HTTPS]、[FileShare]、[MAIL]和[FTP]。




『地址』填写资源的 IP 地址或者域名。

**1. Http 资源的『地址』不能为空，必须填写相应的 IP 或域名。**

**2.填写“域名”形式时，必须在前面『网络配置』的『HOSTS』中设置“域名”或“主机名”对应的“IP 地址”，也可以通过『系统选项』的『内网域名解析』中设置内网 DNS 服务器解析（系统 host 和内网 DNS 具体设置可参考“host”和“内网域名解析”章节）。**

选择『类型』为[MAIL]时，出现以下对话框：


『地址』填写邮件服务器的 IP，『SMTP 端口』和『IMAP 端口』保留默认即可，『域名』填写邮箱的域名。

**使用该方式收发邮件，要求邮件服务器必须支持“IMAP”协议收邮件。**

选择『类型』为『FTP』时，出现以下对话框：

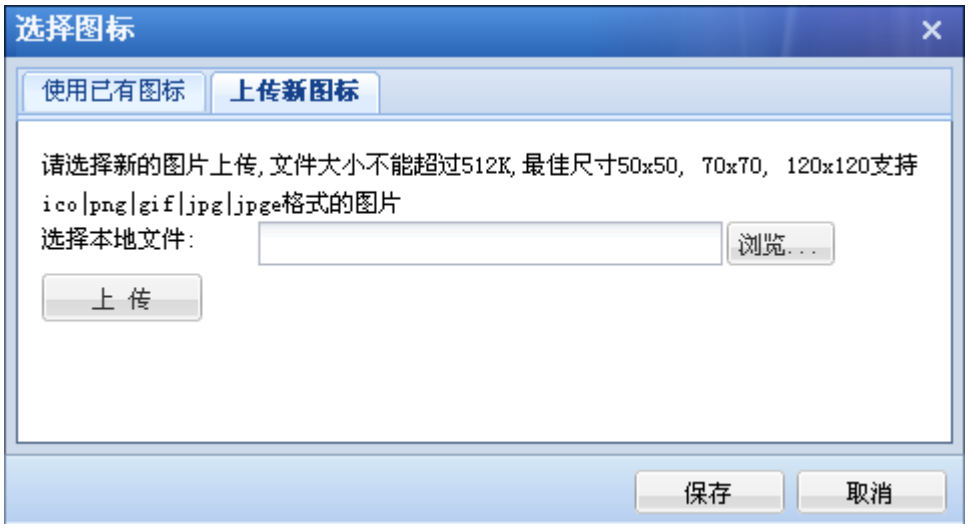

『地址』填写访问该 FTP 服务器的 IP 或域名，『FTP 端口』填写服务器上 FTP 服务的端口（一般保留默认即可）。

**填写“域名”形式时，必须在前面『系统设置』的『HOSTS』管理中设置“域名”或“主机名”对应的“IP 地址”。**

『所属组』后面下拉框可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 4.2.1 章节）。

『图标』选择，在示例图标的右边点击 可选则该资源在“资源列表”中显示的图标，也可以手动上传新的图标。点击下拉框，弹出如下界面：

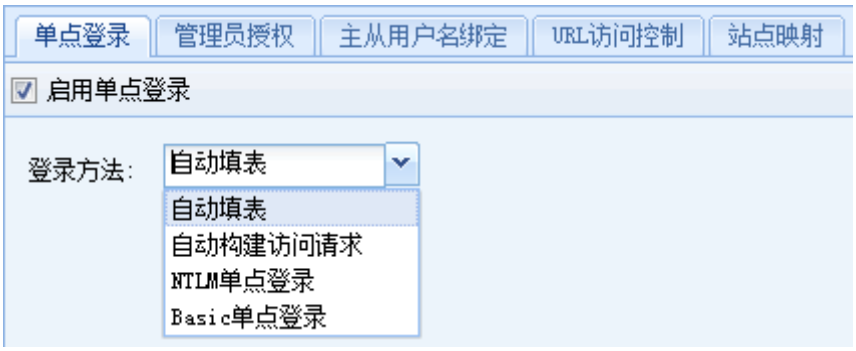

点击 上传新图标 按钮，再点击 浏览 可以把本地的图标上传至 SSL VPN 设备内部，供选择使用。（资源图标的具体设置可参考 3.5.3.3“图标管理”章节）。




如果不勾选[允许用户可见]选项，则登录 SSL VPN 后，在“资源列表”中不显示该资源的信息，但实际上该资源是可用的。

勾选[启用资源地址伪装]，则用户打开资源的时候看不到该资源的真实 IP 地址。

[启用单点登录]勾上后，可以使用“单点登录”方式访问该资源（单点登录的具体设置可参考 3.5.1.5『单点登录配置』章节）。启用单点登录页面如下：




『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。界面如下：


**资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资源列表。编辑权仅属于创建该资源的管理员或其上级管理员。**

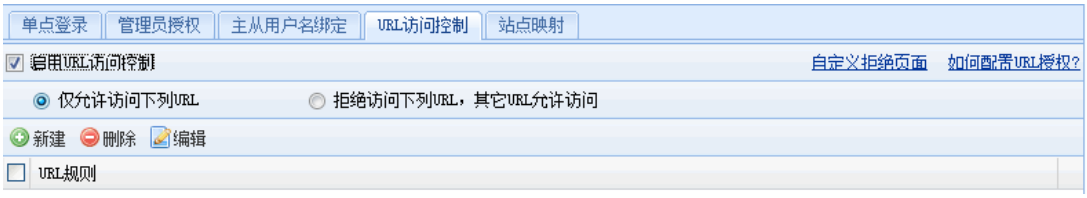
『主从用户名绑定』可实现主从绑定功能，即限制用户登录 SSL VPN 后，只能够使用指定的帐号登录应用资源，使用其他帐号无法登录该应用资源，WEB 应用、TCP 应用、L3VPN 均可实现该功能。界面如下图所示：


勾选[通过数据包解析的用户名绑定认证]，使用数据包解析方式实现。

首先在『数据包格式』后面的下拉框中选择该应用的类型，并根据实际情况填写下方的数据信息。然后在『用户管理』列表页面，对目标用户帐号绑定需要登录应用系统的帐号、密码。

**注意：数据包解析方式不需要启用单点登录功能。**

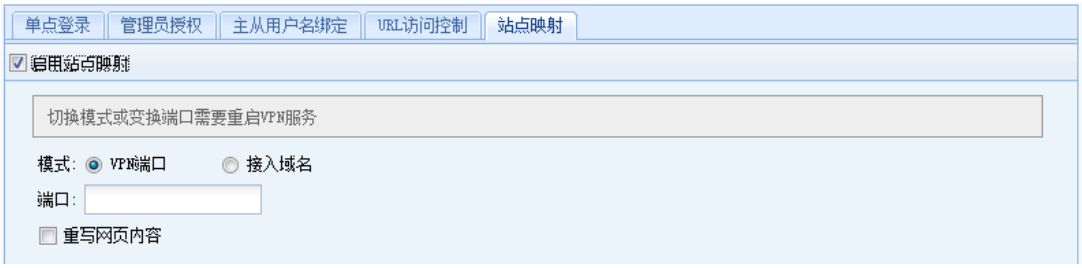
『URL 访问控制』用来设置允许特定用户只能访问特定的 URL 地址，如下图：




可选择[仅允许访问下列 URL]或[拒绝访问下列 URL，其它 URL 允许访问]，点击新建，可添加 URL 地址。


**URL 访问控制支持 WEB 应用中的 HTTP、HTTPS 和 FileShare 三种应用，不支持 mail 和 ftp 类型的应用。**

[站点映射]，即管理员指定解析到 VPN 的接入域名或 VPN 设备的某个端口映射到内网的 Web 资源，SSL VPN 客户端接入 VPN 后使用该公网 URL 访问对应的 http 和 https 类型 Web 资源，即站点映射，也称为 EasyLink 资源，界面如下：




模式中若选择为[VPN 端口]，需要在下面的端口中填入相应的端口号，该端口号不能与设备中使用过的其它端口冲突。

模式中若选为[接入域名]，则该域名必须是 SSL VPN 的公网域名，且要保证 SSL VPN 客户端 PC 可以解析到该域名，通过公网 DNS 解析或者在客户端 PC 上添加系统 HOST 都可以。使用[接入域名]后，SSL 用户不能再使用该地址来接入 SSL VPN。

[重写网页内容]，勾选后，即开启客户端网页修正功能。一般建议开启。

**1.站点映射与地址伪装不能同时开启。**

**2.只有 http、https 类型的可配置 EayLink**

**3.配置了站点映射的资源，在客户端访问的时候，必须通过在资源列表点击链接来访问该资源，不能用重开 IE 手动在 IE 上输入地址访问。**

下面介绍『WEB 应用』的使用：


用户可通过点击服务页面上的链接直接访问，也可以在上面的地址栏中输入 WEB 资源地址来访问。

『WEB 应用』的服务列表中有一项名称为“WEB 全网资源（或服务）”的资源，该资源除了可以修改名字外，不可编辑和删除，可以像其他 L3VPN 一样被关联。相当于设置了『地址』是所有 http 和 https 的『HTTP』类型的『WEB 应用』。关联该资源后，客户端登录 SSL VPN 可以看到一个地址输入框，在此直接输入 URL 访问目标『HTTP』类型资源即可。

**『WEB 应用』支持使用所有浏览器（包括非 IE 核心）访问。**

## 3.2.3. TCP 应用

『TCP 应用』主要用于定义各种类型的 SSL VPN 内网资源，以适应各种各样基于 TCP 协议的应用程序访问 SSL VPN 内网资源的需求。

在『资源管理』页面，点击 新建 按钮，如下图：

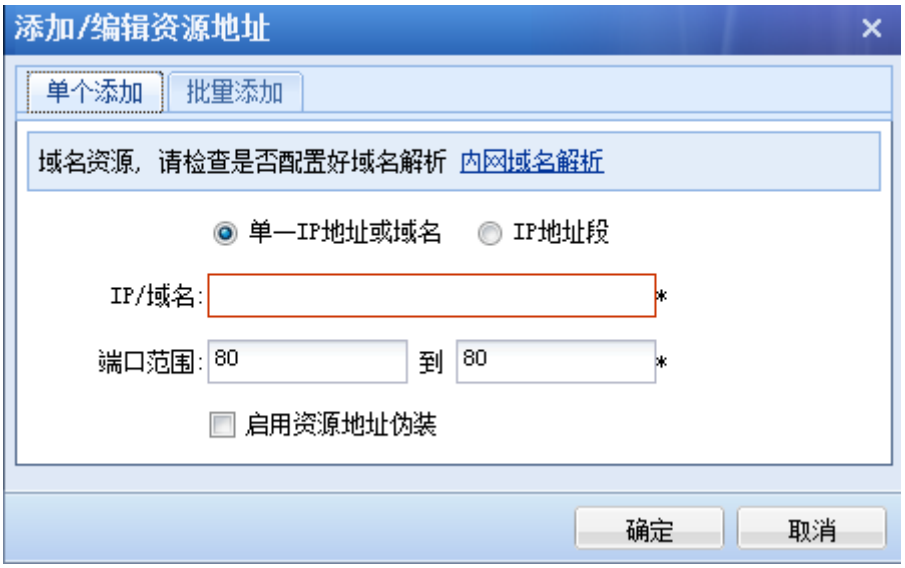
选择[TCP 应用]，弹出【编辑 TCP 应用资源】对话框，设置界面如下：

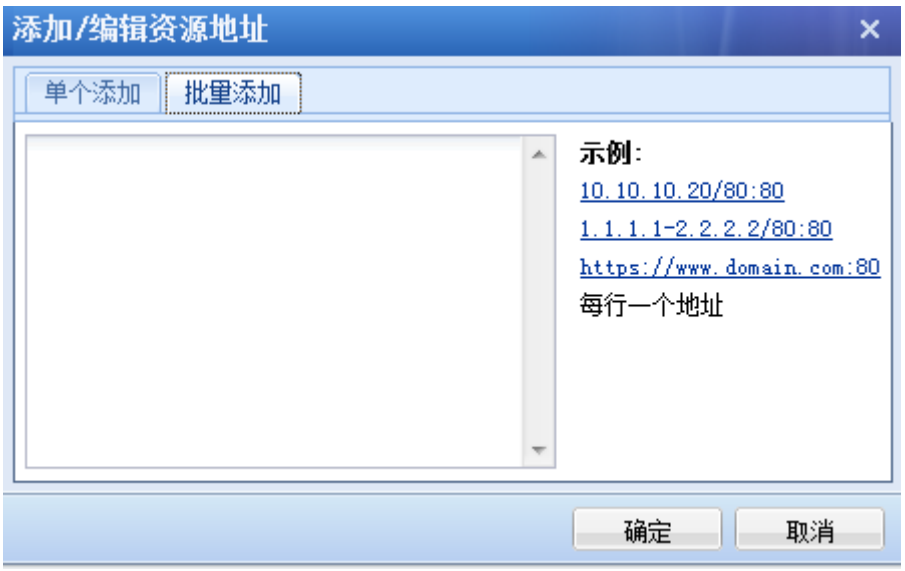

『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 SSL 用户成功登录 SSL VPN 后出现的“资源列表”中。

『类型』选择所建立『TCP 应用』的服务类型，SANGFOR SSL VPN 内置了常用应用服务的定义，直接选择则会在编辑地址的页面中自动填写端口范围，如无所需的类型，可选择底部的[other]，然后自定义该服务所使用的『端口范围』。

『地址』填写提供 TCP 应用的服务器地址，支持『单 IP 或域名』和『IP 段』的形式，

如下图所示：




**以“域名”形式填写时，必须在前面『网络设置』的『HOSTS』中设置“域名”或“主机名”对应的“IP 地址”，也可以通过『内网域名解析』中设置内网 DNS 服务器解析。**

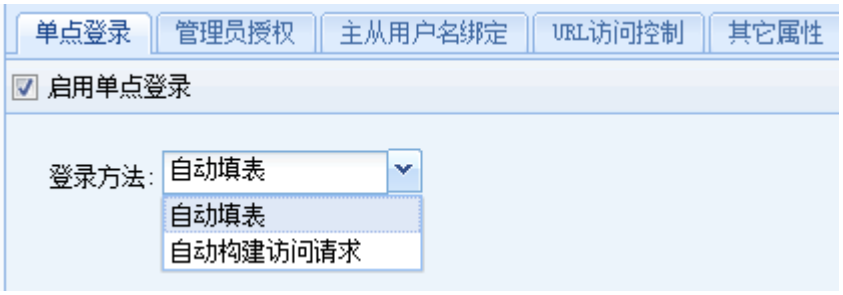
『端口范围』定义该『TCP 应用』提供服务所使用的端口，已预定义好的资源类型一般不需修改，如果『类型』选择了『Other』，则填写该服务所使用的端口。

『所属组』后面下拉框可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资

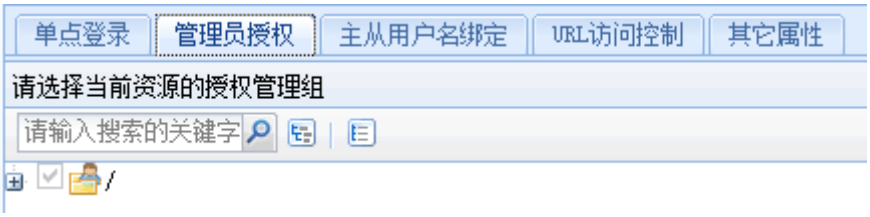
源组的具体设置可参考 4.2.1“资源组”章节）。

如果不勾选[允许用户可见]选项，则登录 SSL VPN 后，在“TCP 应用列表”中不显示该资源的信息，但实际上该资源是可用的。隐藏资源有利于保护内网资源服务器的信息。

[启用单点登录]勾上后，即开启该资源单点登录功能（资源单点登录的具体设置可参考 3.5.1.5『单点登录配置』章节）。配置页面如下：

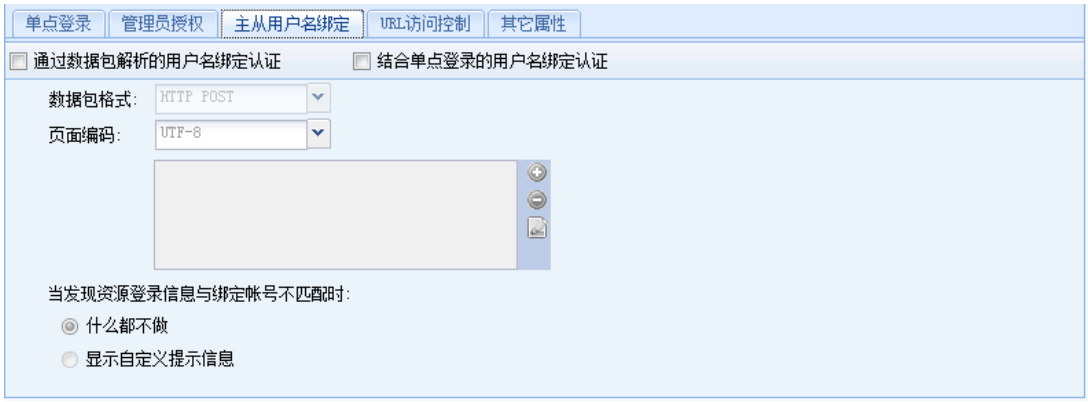



『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。




**资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资源列表。编辑权仅属于创建该资源的管理员或其上级管理员。**

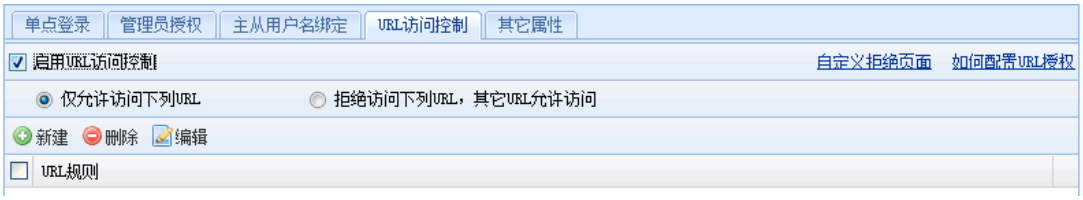
『主从用户名绑定』可实现主从绑定功能，即限制用户登录 SSL VPN 后，只能够使用指定的帐号登录该应用资源，使用其他帐号无法登录该应用资源，WEB 应用、TCP 应用、L3VPN 均可实现该功能。TCP 应用资源可通过以下两种方式实现，界面如下：




勾选[结合单点登录的用户名绑定认证]，使用单点登录方式实现。首先必须对目标资源启用单点登录功能，然后在『用户管理』列表页面，对目标用户帐号绑定需要登录应用系统的帐号和密码。

勾选[通过数据包解析登录的用户名绑定认证]，使用数据包解析方式实现。首先在『数据包格式』后面的下拉框中选择该应用的类型，并根据实际情况填写下方的数据信息。然后在『用户管理』列表页面，对目标用户帐号绑定需要登录应用系统的帐号、密码。

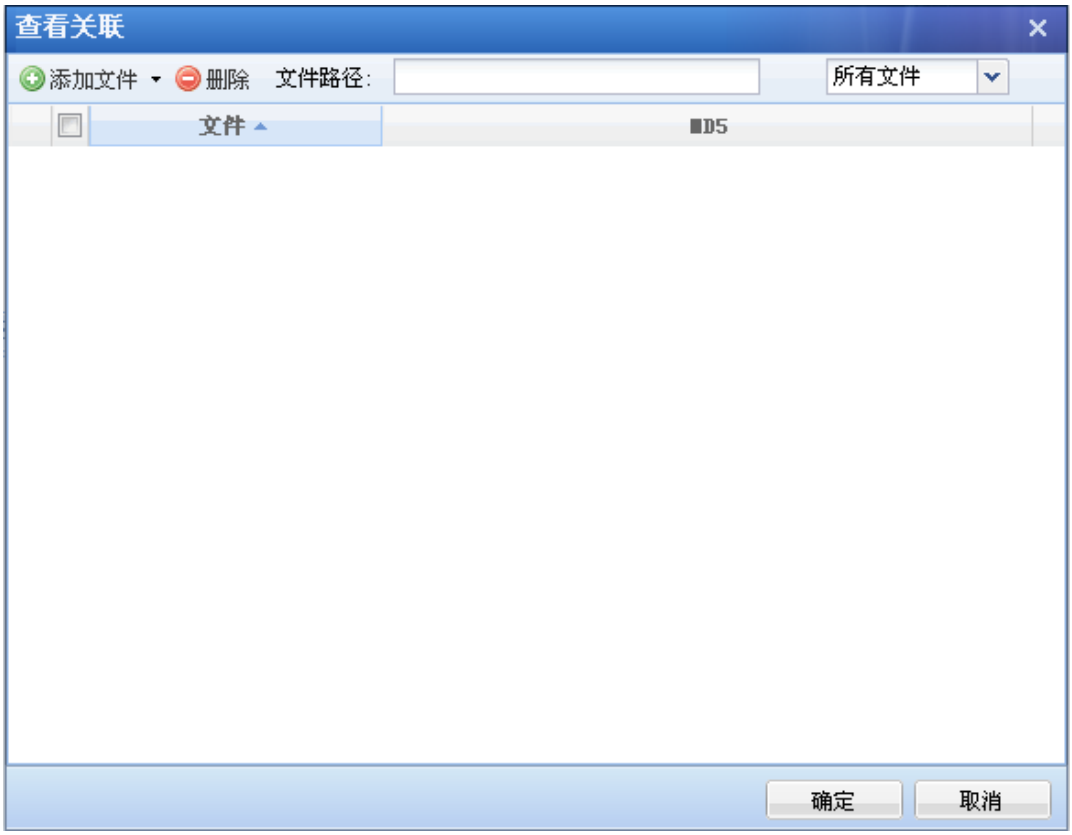
『URL 访问控制』用来设置允许用户只能访问特定的 URL 地址。



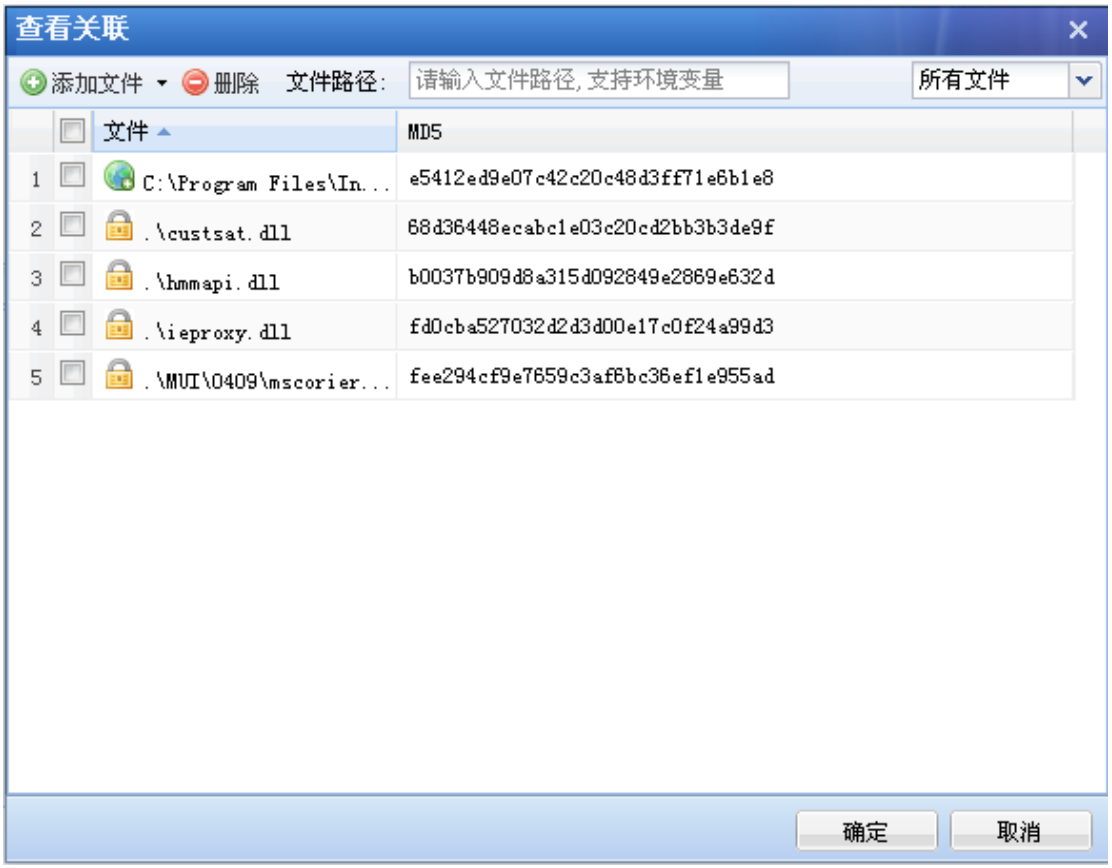

**注意：URL 访问控制只支持 TCP 应用的 HTTP 类型的应用。**

『其他属性』中可以设置对该资源[启用关键文件保护]和[启用智能递推]，如下图所示：


[应用关键文件保护]可以通过锁定使用 Socket 上网的进程所需关键文件，保护用户在访问 SSL VPN 时，所需的关键文件不被改动。如果用户修改过所保护的进程和关键文件，则将无法访问该资源。勾选[应用关键文件保护]后，点击 编辑 进入关键文件保护配置界面。




点击 添加文件，再点击 进程关联文件 按钮，选中想要保护的某个应用程序（必须是 exe 格式），在下面的列表中，显示出该文件所处目录和下级目录下的所有 DLL 文件，显示的信息包括：文件名、MD5 值，如下图所示：




添加文件右边的下拉框可以对列表中的文件根据类型进行过滤显示，默认是显示所有，支持对 dll、exe、pdb 类型过滤。如果需要锁定的文件不在该文件列表中，可以点击添加文件，再点击锁定文件手动添加。添加完成后即可对该进程和列表中勾选上锁定的文件进行锁定，如果用户对该进程或文件修改，则无法访问资源。

删除能够把左边被勾选上的关键文件从列表中删除。

**用户使用资源时，关键文件是被锁定的，不能被“强行”修改。**

[应用智能递推]，主要应用于 WEB 页面中包含子链接的情况，要使用该功能，必须先在『系统选项』中的『资源服务选项』中勾选[启用资源智能递推]。详细可参考 3.5.1.6 章节。

最后确定保存配置即可。

配置生效按钮把当前配置进行保存并生效。

**首次使用『TCP 应用』时计算机会自动安装控件，需要以 administrator 登录系统才可以安装上。若 PC 上有防火墙或杀毒软件，可能会拦挡 PC 安装插件，可先关闭防火墙或杀毒软件。**

## 3.2.4. L3VPN

『L3VPN』主要用于定义、配置和管理各种基于 IP 协议的 SSL VPN 内网资源，以适应各种各样不同协议（TCP/UDP/ICMP）的应用程序访问 SSL VPN 内网资源和内网服务器。

在『资源管理』页面，点击 新建 按钮，如下图：

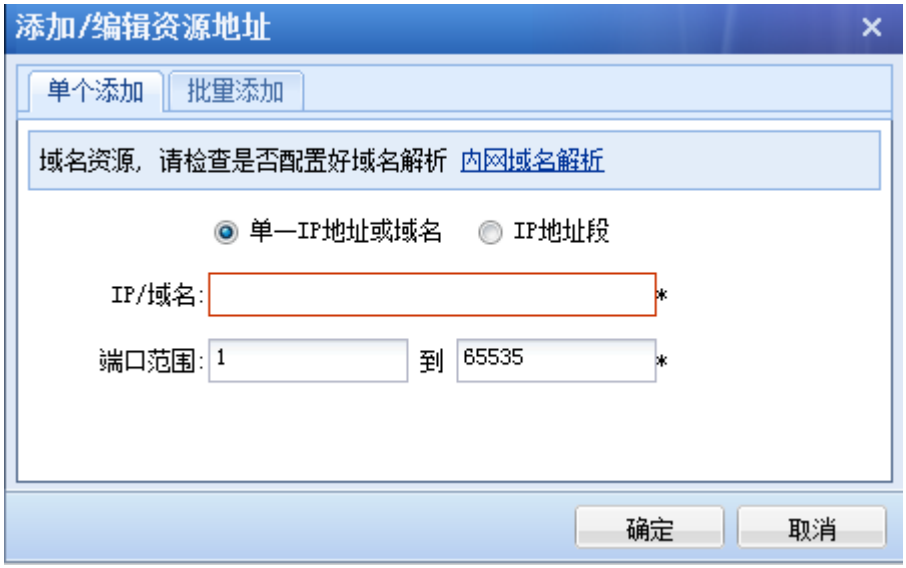

选择[L3VPN]，弹出【编辑 L3VPN 资源】对话框，设置界面如下：

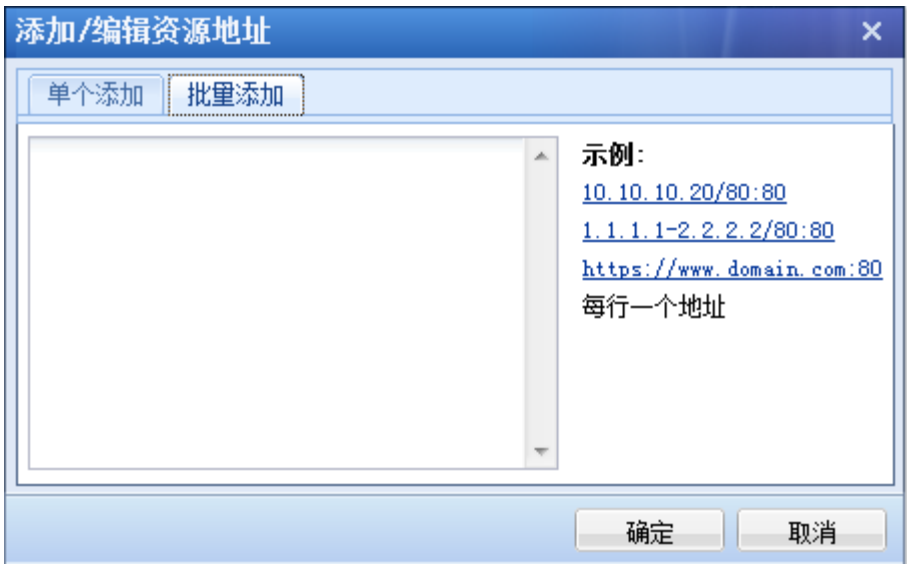

『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 SSL 用户成功登录 SSL VPN 后，出现的“资源列表”中。

『类型』选择该 L3VPN 资源的协议类型，SANGFOR SSL VPN 内置了常用应用服务的定义，直接选择设备会自动识别端口范围和协议，如无所需的类型，可选择『Other』，设置协议，然后自行设定下面的『端口范围』。

若类型选择为[OTHER]，则需要选择『协议』，可选择为 TCP、UDP 或 ICMP，根据定义『L3VPN』所使用的协议进行选择。

『地址』填写提供 L3VPN 服务的服务器地址，支持“单 IP 或域名”和“IP 段”的形式。点击  ，弹出【添加/编辑资源地址】对话框，可单个添加，也可批量添加，如下图：




『端口范围』定义该『L3VPN』所使用的端口，已预定义好的资源类型一般不需修改，如果前面『类型』选择了『Other』，则填写该服务所使用的端口。

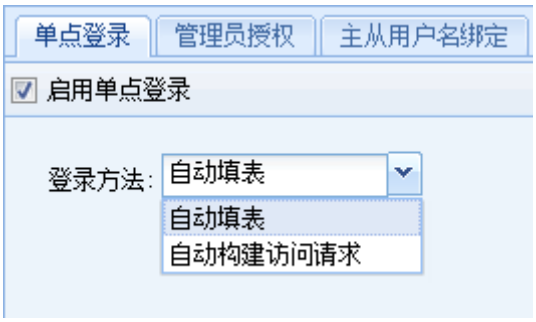
**填写“域名”形式时，必须在前面的『网络配置』中的『HOSTS』中设置“域名”或“主机名”对应的“IP 地址”，也可以通过『内网域名解析』中设置内网 DNS 服务器解析。**

『应用程序路径』此处填写某些 C/S 结构服务可能用到的客户端软件的路径。

如果不勾选[允许用户可见]选项，则登录 SSL VPN 后，在“可用资源列表”中不显示该资源的信息，但实际上该资源是可用的。

『所属组』后面下拉框可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 4.2.1“资源组”章节）。

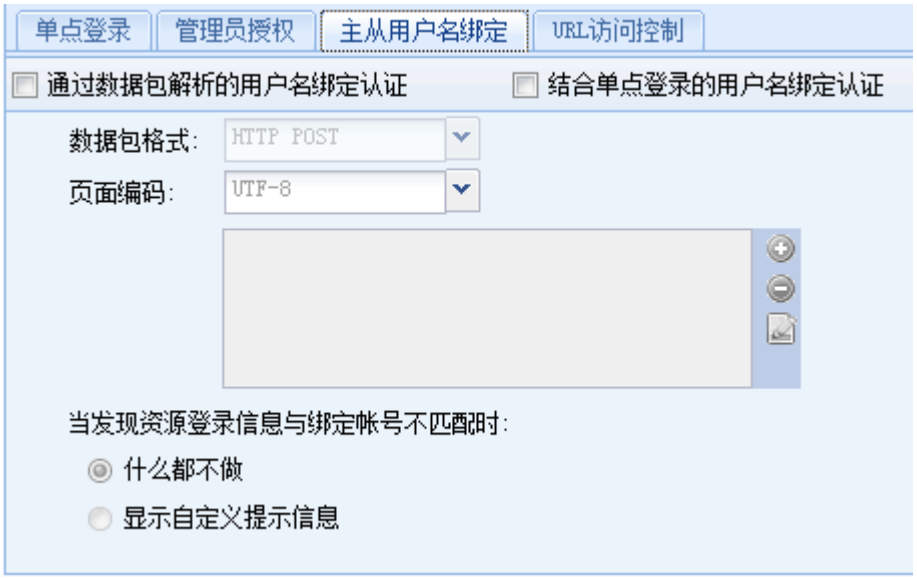
[启用单点登录]勾上后，即开启该资源单点登录功能（资源单点登录的具体设置可参考 3.5.1.5『单点登录配置』章节）。配置页面如下：




『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。


**资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资源列表。编辑权仅属于创建该资源的管理员或其上级管理员。**

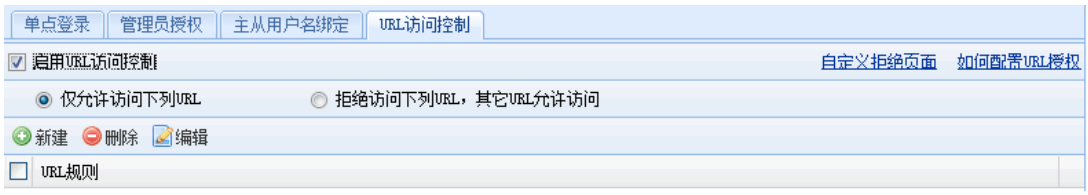
『主从用户名绑定』可实现主从绑定功能，即限制用户登录 SSL VPN 后，只能够使用指定的帐号登录该应用资源，使用其他帐号无法登录该应用资源，WEB 应用、TCP 应用、L3VPN 均可实现该功能。L3VPN 应用资源可通过以下两种方式实现，界面如下：




勾选[结合单点登录的用户名绑定认证]，使用单点登录方式实现。首先必须对目标资源启用单点登录功能，然后在『用户管理』列表页面，对目标用户帐号绑定需要登录应用系统的帐号和密码。

勾选[通过数据包解析登录的用户名绑定认证]，使用数据包解析方式实现。首先在『数据包格式』后面的下拉框中选择该应用的类型，并根据实际情况填写下方的数据信息。然后在『用户管理』列表页面，对目标用户帐号绑定需要登录应用系统的帐号、密码。

『URL 访问控制』用来设置允许用户只能访问特定的 URL 地址。




**注意：URL 访问控制只支持 L3VPN 应用的 HTTP 类型的应用。**

『L3VPN』的资源列表中有一项名称为“L3VPN 全网资源（或服务）”的资源，不可修改和删除，可以像其他 L3VPN 资源一样被用户关联。相当于设置了『主机地址』是 LAN 口和 DMZ 口所在网段，『协议』分别为 TCP、UDP、ICMP，『端口范围』是 1-65535 的三条 IP 服务。

**要使用全网服务访问 LAN 口或 DMZ 口区的非直连网段（中间隔着路由器或交换机等三层设备），需要在『本地子网』中添加需要访问的非直连网段以及在『系统路由设置』添加到相应网段的路由。**

保存 按钮把当前配置进行保存并生效。

**首次使用『L3VPN』时计算机会自动安装虚拟网卡控件，需要以 administrator 登录系统才可以安装上。若 PC 上有防火墙或杀毒软件，可能会拦挡 PC 安装插件，可先关闭防火墙或杀毒软件。**

## 3.2.5. 远程应用

『远程应用』主要用于定义、配置和管理各种基于远程应用服务器的 SSL VPN 内网资源，通过 SSL VPN 来使用内网各种各样的应用程序。

在『资源管理』页面，点击 新建 按钮，如下图：


选择[远程应用]，弹出【编辑远程服务资源】对话框，设置界面如下：


『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 SSL 用户成功登录 SSL VPN 后，出现的“资源列表”中。

『所属组』可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 4.2.1“资源组”章节）。

『图标』，该资源在资源列标中显示的图标。

『应用程序』选择终端服务器提供的应用，点击后面的 选择程序，可以选择已添加好的终端服务器提供服务的应用程序，如下图：


添加终端服务器可以参考 4.6“终端服务器设置”章节。

『工作目录』该应用程序在终端服务器的路径。

『启动参数』用来设置程序启用时可能用到的参数。

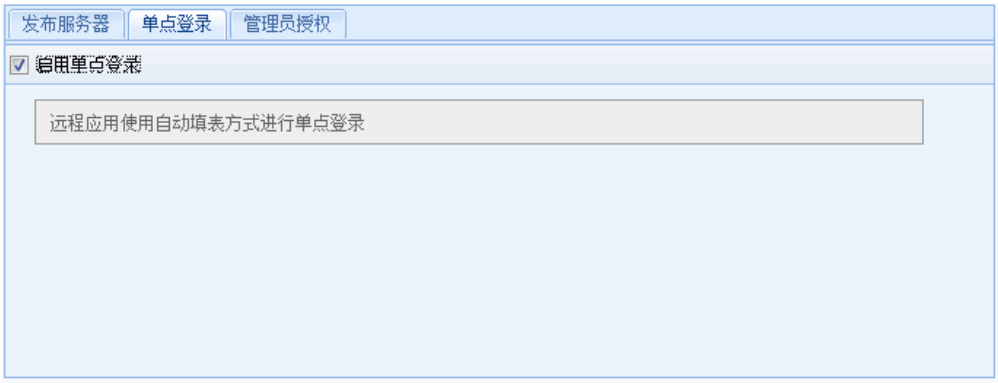
[程序启动后窗口最大化]，勾选上后远程应用发布的程序启动后，窗口直接就最大化。

[单实例模式]勾选上后，如果该用户已经启动了一个远程发布资源，再次点击资源的时候不会重新打开，会直接跳到之前打开的资源窗口上。若该资源关联了不同的启动参数，则不建议使用此选项。

『发布服务器』选择需要发布的终端服务器，配置界面如下图：


勾选服务器名称或者服务器群组，并 保存 配置即可。

『单点登录』用于启用远程应用资源的单点登录。如果勾选[启用单点登录]，同时管理员录制了单点登录信息，那么用户登录 VPN 后，访问相应的远程应用资源，则完成相应的单点登录过程。如下图：

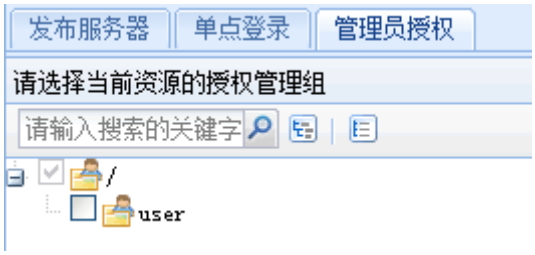



**1.远程应用资源单点登录，仅支持自动填表的方式。**

**2.远程应用单点登录资源，若应用程序选择发布“浏览器”，仅支持发布 IE 内核的浏览器。**

**3.录制远程应用资源单点登录时，仅 “IE”当做BS资源，其它均为CS资源。**

『管理员授权』可将该资源指派给其他管理员，使其他管理员对该资源拥有使用和指派的权限。




**资源指派给管理员后，这部分管理员只具备对该资源的使用权、指派给该管理员的下属管理员的权限，对该资源不具备编辑权，用这部分管理员帐号登录控制台后，只能在角色管理中给用户或者用户组关联指派的资源，无法在资源管理中看见这些资源列表。编辑权仅属于创建该资源的管理员或其上级管理员。**

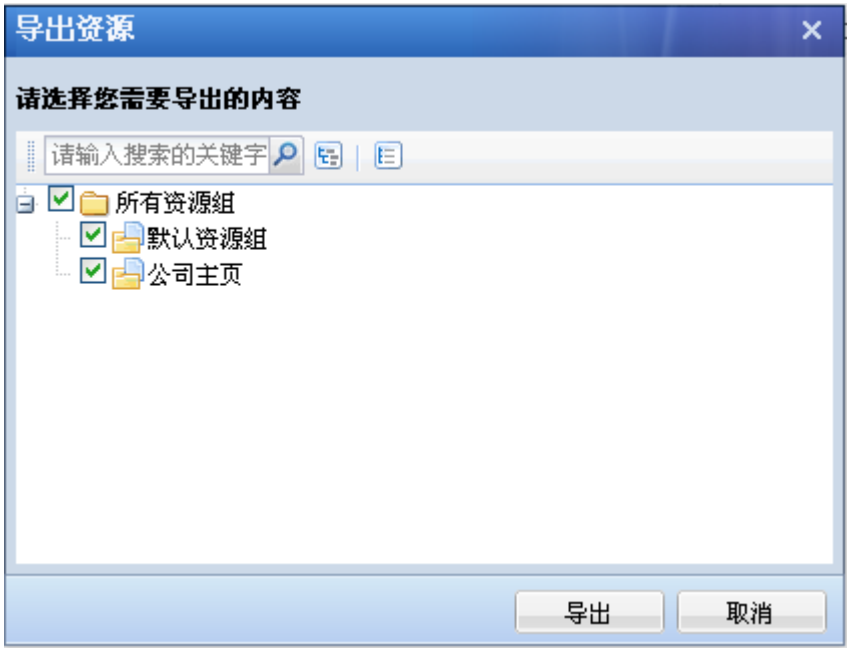
## 3.2.6. 其它操作

其它操作包括『导出资源』、『导入资源』和『资源排序』。WEBUI 路径：『控制台』→『SSL VPN 设置』→『资源管理』→『其他操作』，配置界面如下：


### 3.2.6.1. 导出操作

『导出资源』即将『资源管理』中的资源导出到一个文件中。

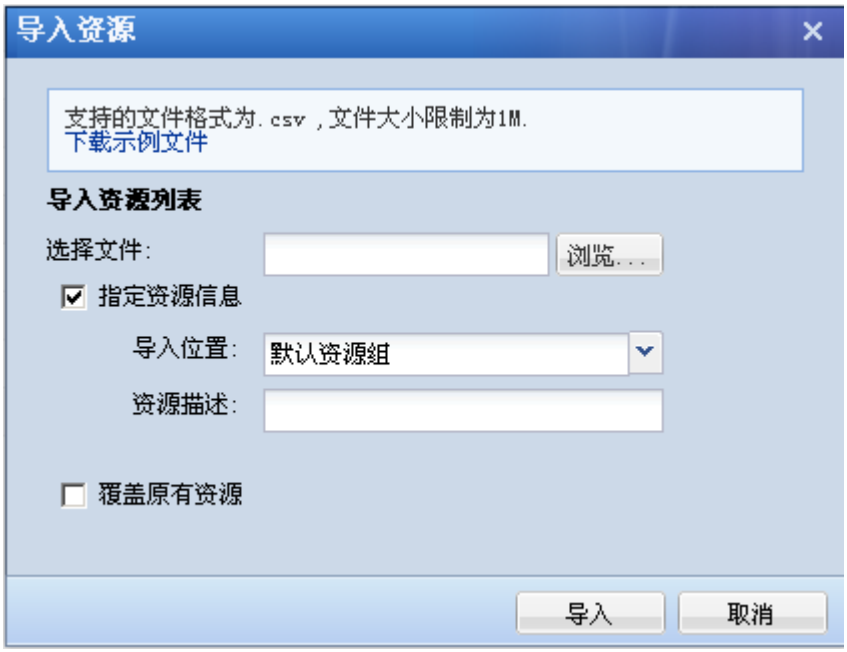
如下图所示：




点击 导出 按钮，将资源保存在默认生成的 rclist.csv 文件中。

### 3.2.6.2. 导入操作

『导入资源』将编辑好的资源通过文件导入到『资源管理』中。




可以通过 下载示例文件 来编辑资源，将编辑完成的.csv 格式的文件导入设备。

通过[指定资源信息]可以将文件中的资源导入到已存的资源组中，还可以指定添加描述信息。

勾选[覆盖原有资源]，若导入的资源名称和原有的资源名称冲突，则覆盖原有资源。

### 3.2.6.3. 资源排序

『资源排序』可以对资源组中的各个资源进行排序。可通过 上移 、下移 、移到底部 或 移到顶部 来调整资源顺序。如下图：


除了上述操作外，在资源管理页面，还可对资源进行 删除 、编辑 、移动 、筛选 等操作：


勾选相应的资源，点击 删除 ，即可删除该资源。

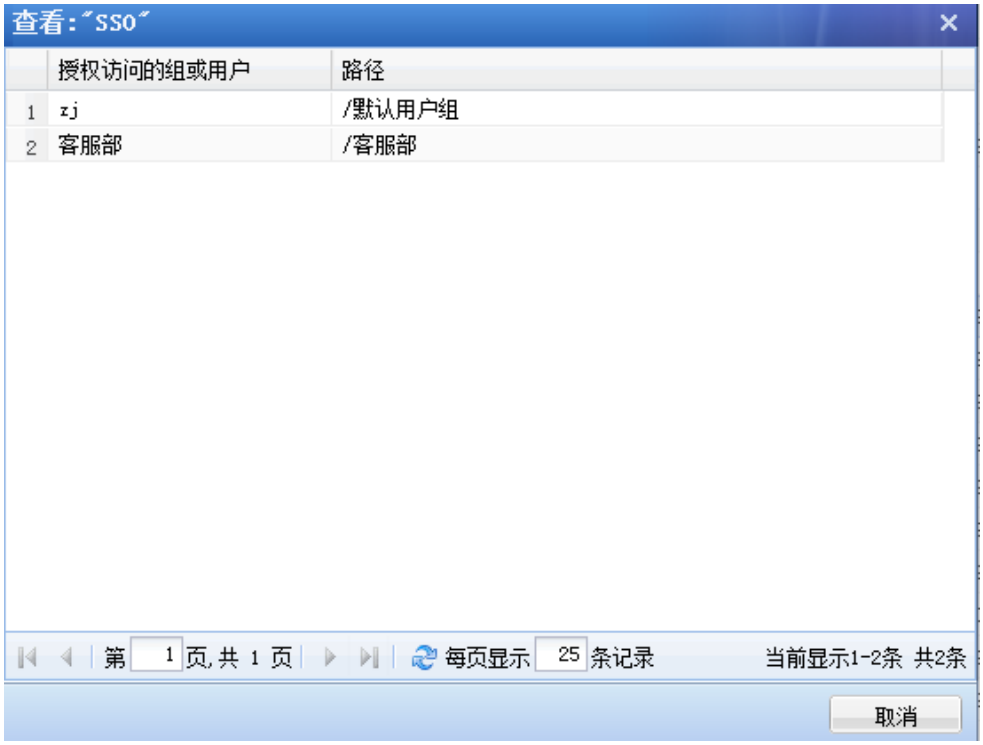
勾选相应的资源，点击 编辑 ，可以该资源进行编辑。

点击 选择 ，可选择当前页或选择所有页的资源，若之前已经选择了资源，也可以取消选择。如下图：

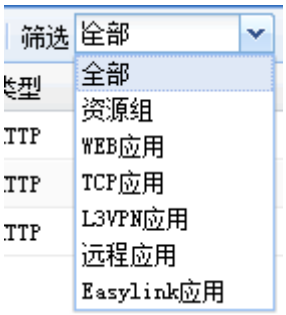

勾选相应的资源，点击 移动，可将选中的资源移动到其它资源组中。

**注：移动的时候，只能移动资源，不能移动资源组。**

勾选相应的资源，点击 查看关联，可以查看该资源被哪些用户关联，如下图：




『筛选』可以根据资源组或资源类型选择显示的资源。可选择显示[全部]、[资源组]、[WEB 应用]、[TCP 应用]、[L3VPN 应用]、[远程应用]、[Easylink]等。



# 3.3. 角色授权

## 3.3.1. 新建角色

『角色授权』是“用户/用户组”和“资源”的中介，SANGFOR SSL VPN 正是通过『角色授权』把 SSL VPN 登录用户/用户组和 SSL VPN 内网资源“关联”起来的。通过角色可以把多个“用户/用户组”、多个资源进行关联，更加有效管理资源和用户组的权限。

WEBUI 路径：『SSL VPN 设置』→『角色授权』。

操作界面如下图所示：


在右上角的输入框内填上需要搜索的目标角色的部分名字，点击即可筛选出符合条件角色，可以按名称、按描述、按关联的用户（组）来查找角色。

『角色名称』显示角色的名称。

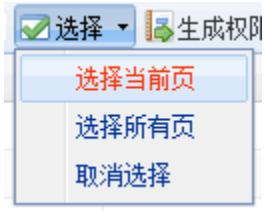
『描述』用来显示角色的描述信息。

『授权给』显示关联了该角色的用户。

点击 编辑，用来编辑勾选的角色。

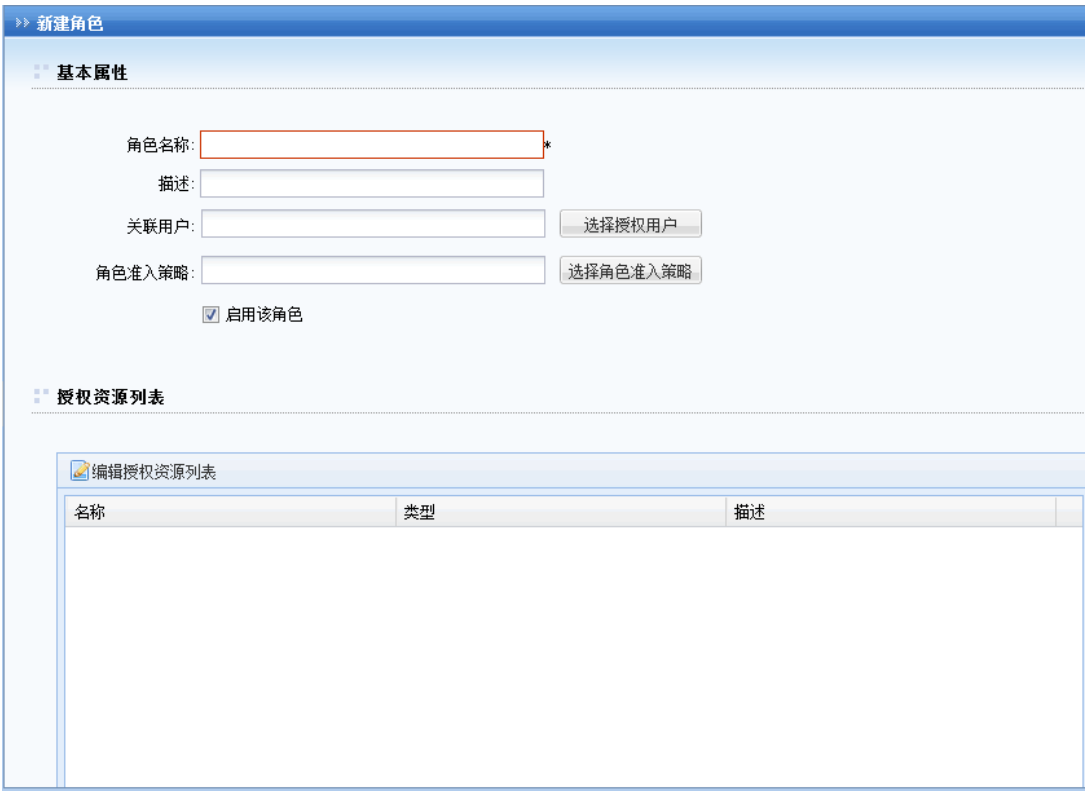
点击 删除，用来删除勾选的角色。

点击 选择，可以选择当前页或选择所有页。




在角色管理页面，点击 新建，可新建角色，如下图：


选择[新建角色]，弹出【新建角色】编辑页面，如下图：



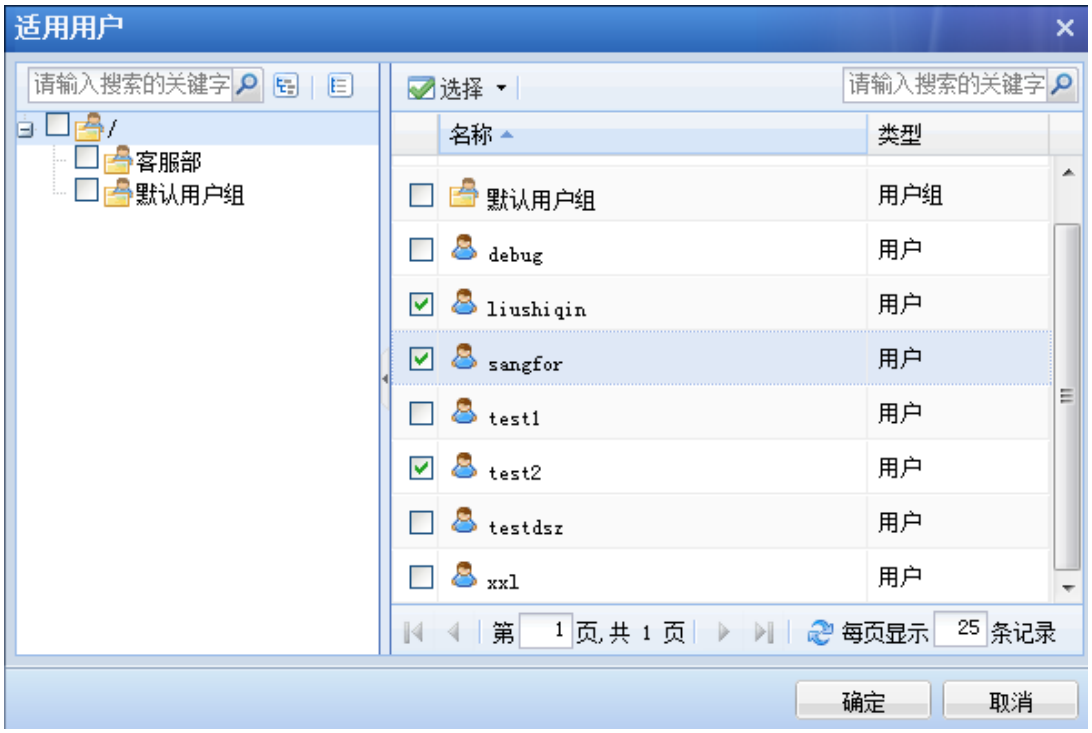
『角色名称』该条角色的名称，自定义即可。

『描述』可随意填写便于理解和记忆的描述语言。

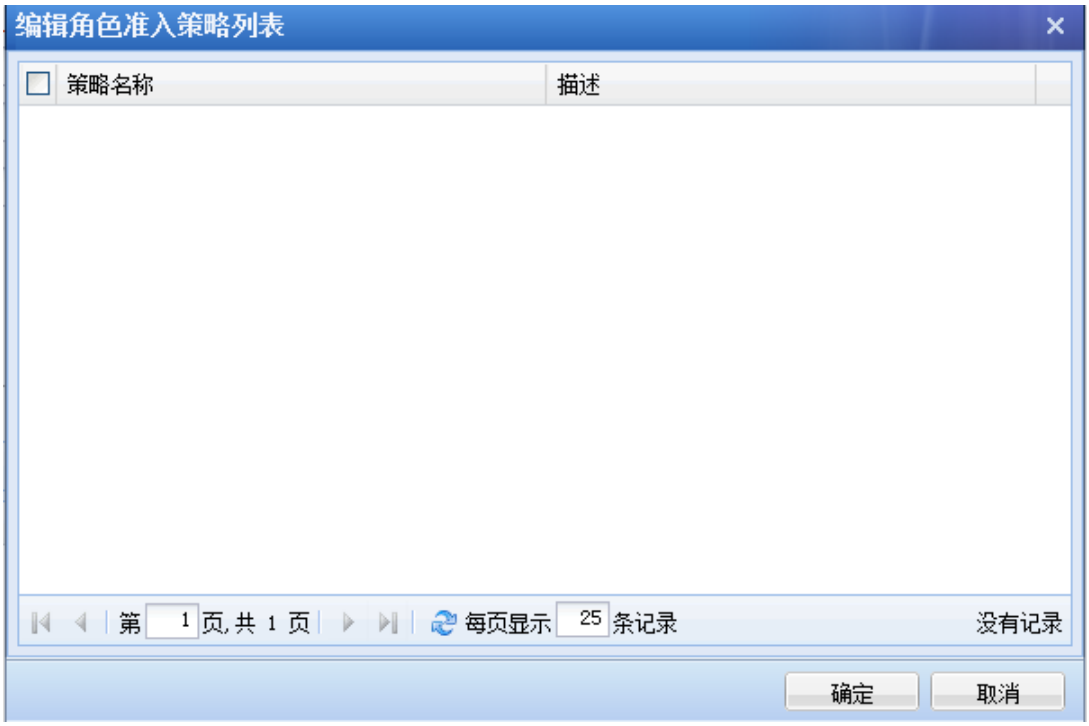
『关联用户』选择关联该条角色的用户或者用户组。

点击 选择授权用户 按钮，下面的列表会列出『用户管理』中所定义好的用户/组（定义用户/组，请参考 4.1 章节），在列表中勾选相应的用户/组，即可完成“用户/组的关联”，属于该角色的用户，会具有访问该角色关联资源的权限。

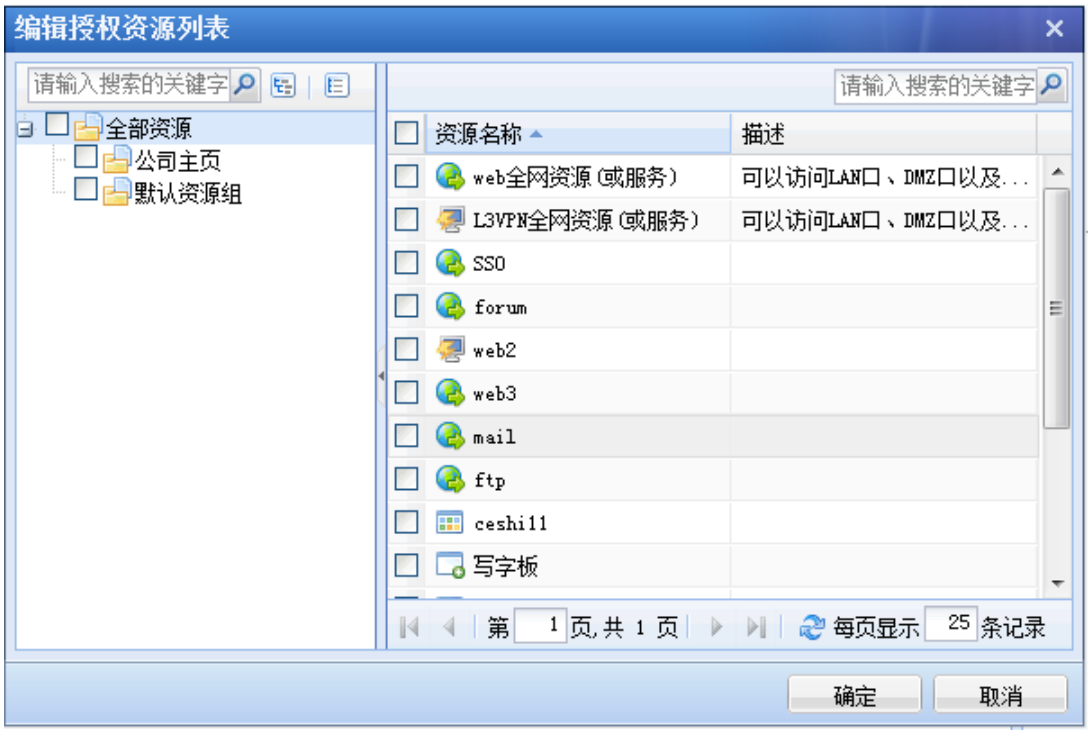
界面如下图所示：




『角色准入策略』，选择该条角色的准入策略，点击 选择角色准入策略，弹出【编辑角色准入策略列表】编辑页面（需要先在准入策略设置中添加好相应的策略后这里才可以选择，准入策略设置请参考 4.7.2 章节）勾选相应的策略即可。若没有准入策略，此处可不配置。

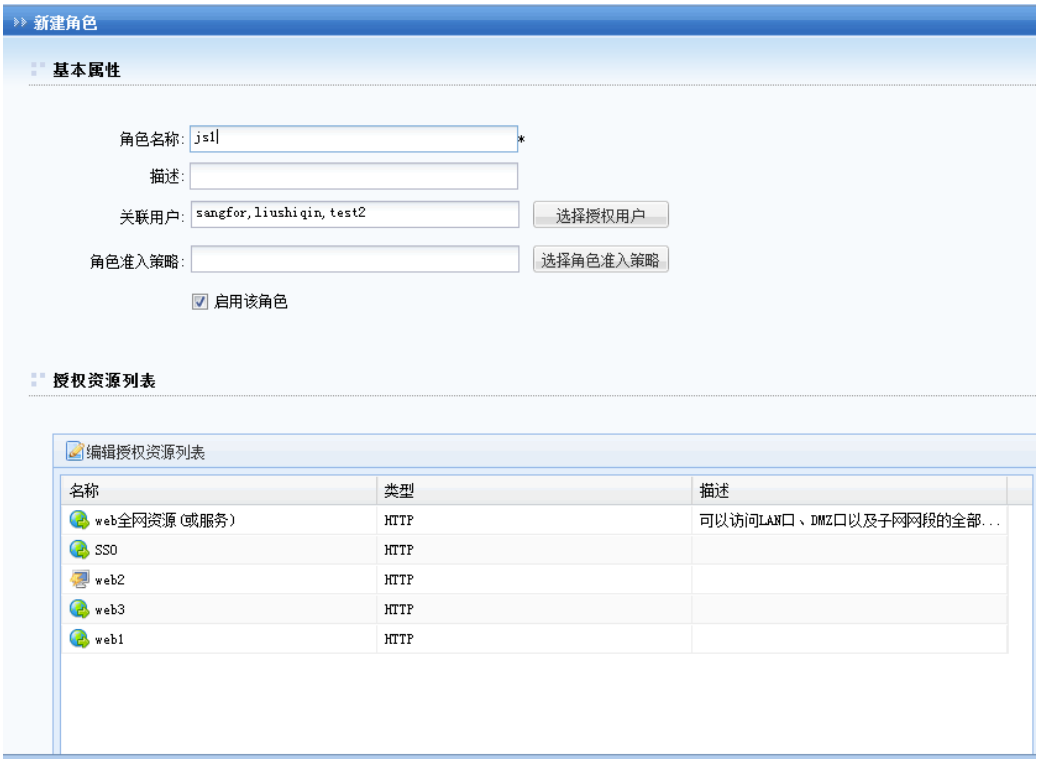



在『授权资源列表』设置中，可以设置该角色需要关联的资源。点击 编辑授权资源列表 按钮，弹出【编辑授权资源列表】页面，选择相应的资源。（资源添加请参考 4.2 章节）界面如下图所示：



选择策略，然后点击 确定 按钮。确定保存。

配置完以后，界面如下：

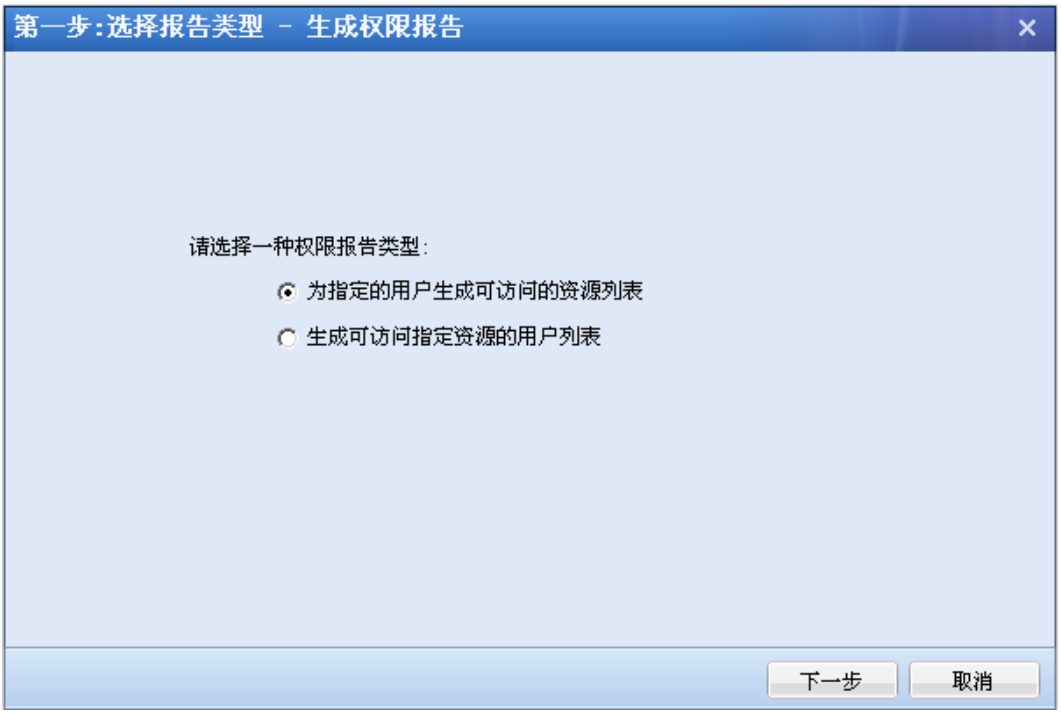



最后点击 保存 并 立即生效，即完成一条角色配置。

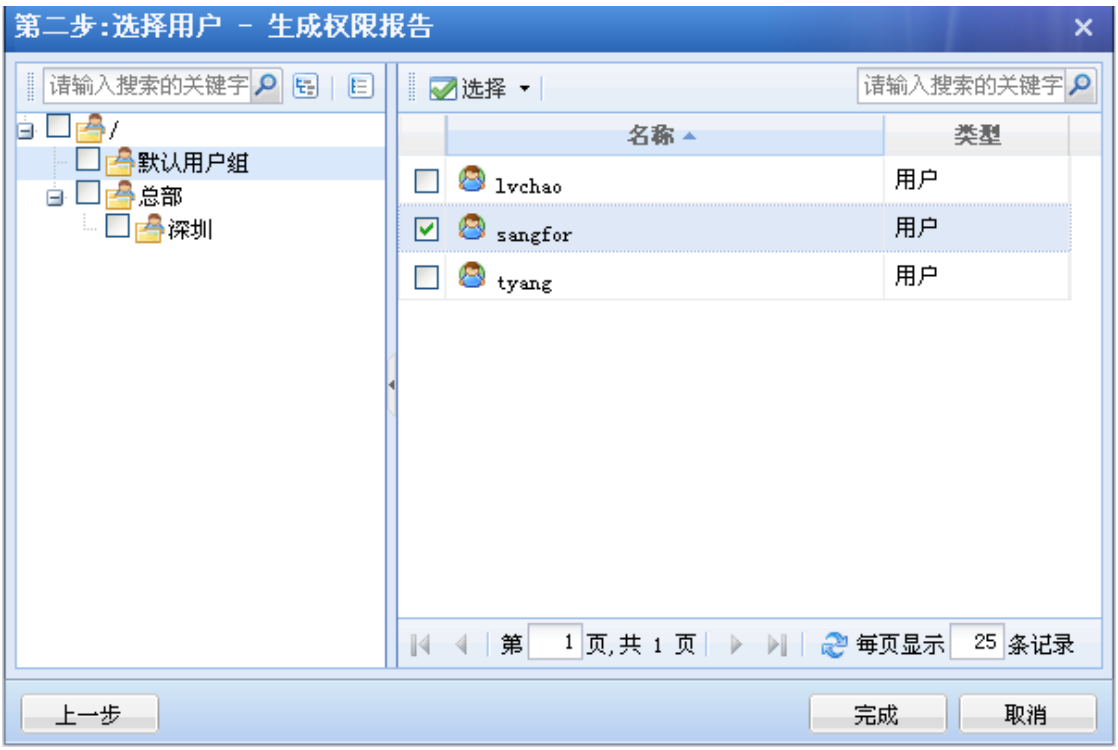
## 3.3.2. 生成权限报告

『生成权限报告』用来生成显示用户可访问资源的报表。

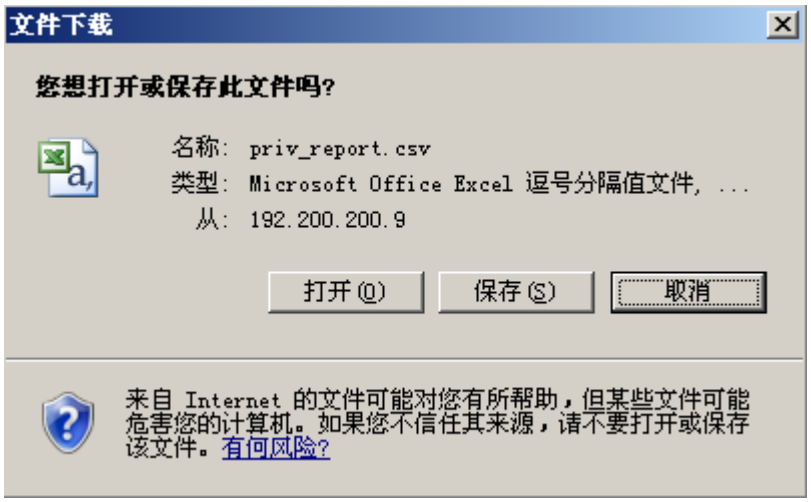
如下图所示：



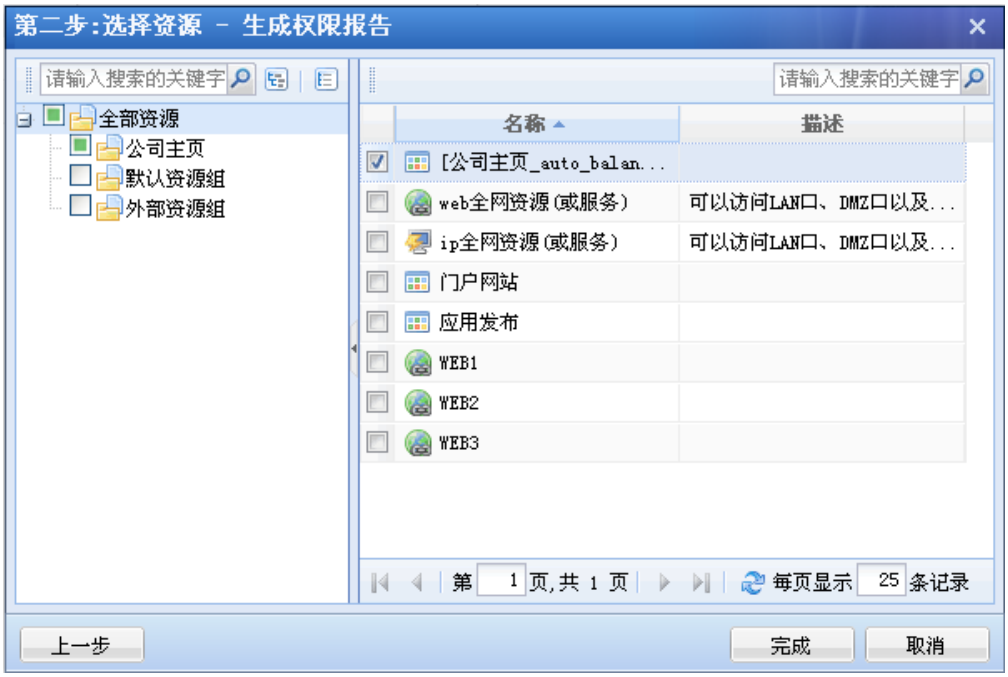

勾选[为指定的用户生成可访问的资源列表]，点击 下一步 按钮，如下图所示：



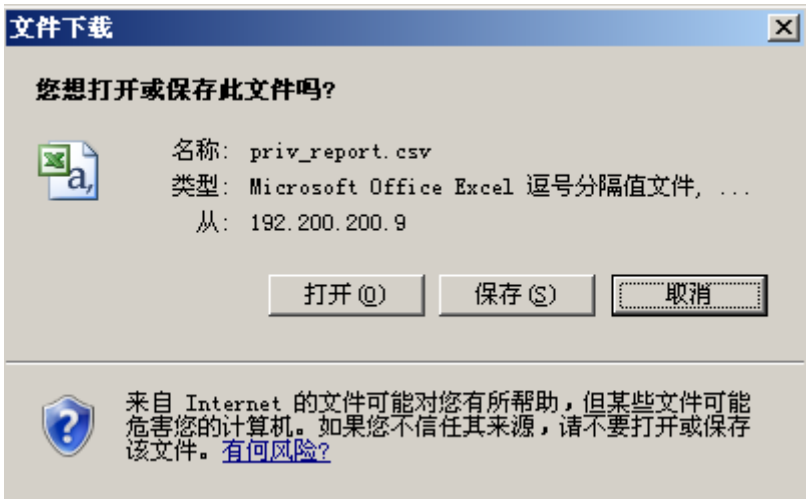

选择用户，点击完成，生成“.csv”格式的文件，如下图所示：




勾选[生成可访问指定资源的用户列表]，点击 下一步 按钮，如下图所示：




选择资源，点击完成，生成“.csv”格式的文件，如下图所示：




## 3.4. 认证设置

『认证设置』包含『主要认证』、『辅助认证』和『认证选项设置』。『认证设置』主要用于配置认证服务器，以及各种认证的相关选项。

WEBUI 路径：『控制台』→『SSL VPN 设置』→『认证设置』。

界面如下图所示：


## 3.4.1. 主要认证

『主要认证』包含『本地密码认证』、『LDAP 认证』、『Radius 认证』、『证书与 USB-KEY 认证』和『域单点登录认证』。

### 3.4.1.1. 本地密码认证

『本地密码认证』设置页面包含『密码安全策略』、『用户名策略』。

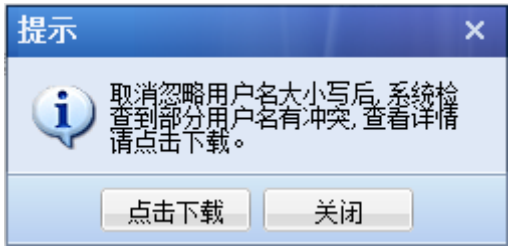
WEBUI 路径：『SSL VPN 设置』→『认证设置』→『主要认证』→『本地密码认证』。页面如下：


点击本地密码认证后面的 设置，弹出【本地密码认证设置】页面，界面如下图所示：


『密码安全策略』用于设置用户的一些密码策略，详细可参见上图。启用密码安全策略

后，用户下次登录会进行密码安全检查，不符合安全策略的会要求修改密码。

『用户名策略』用户登录时，设置是否区分输入用户名的大小写。如果在启用该选项之前，组织结构中已经存大小写不同的相同用户名，则会修改失败并导出同名用户，需要先修改冲突的用户名，再启用该选项。



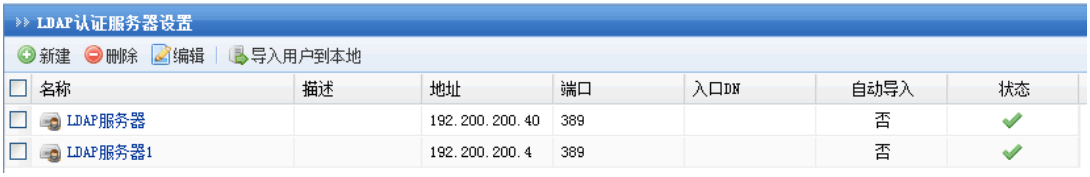

**注意：上述策略只对本地密码认证的用户有效。**

### 3.4.1.2. LDAP 认证

SANGFOR SSL VPN 网关支持使用“LDAP 协议”的第三方的服务器作为认证服务器。『LDAP 认证』就是用于设置 LDAP 外部认证服务器相应参数的。

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『主要认证』→『LDAP 认证』。页面如下：


点击 LDAP 认证后面的 设置，弹出【LDAP 认证服务器设置】页面，界面如下图所示：




点击 新建 可新增一个 LDAP 服务器，弹出 LDAP 外部认证服务器的参数设置界面。配置

如下图：


『服务器名称』和『服务器描述』可随便填写便于记忆的文字。

『服务器地址』用于设置 LDAP 服务器的 IP 地址和所使用的端口，此处可设置多个服务器地址和端口，他们之间是主备关系，第一个服务器为主服务器，其余都为备服务器，当第一个服务器连不上，才尝试连接第二个服务器认证，以此类推。

点击图标，出现服务器 IP 地址和端口的设置页面如下：


点击，可以删除所选的服务器地址。

点击，可以编辑所选的服务器地址。

点击或，可以调整服务器地址的顺序。

『管理员全路径（DN）』和『管理员密码』填写 LDAP 服务器内一个有效的账号和密码，用于读取 LDAP 结构。所填写的帐号一般要以域中 DN 的形式填写。

**该账号在 LDAP 服务器必须有读取用户路径的权限。**

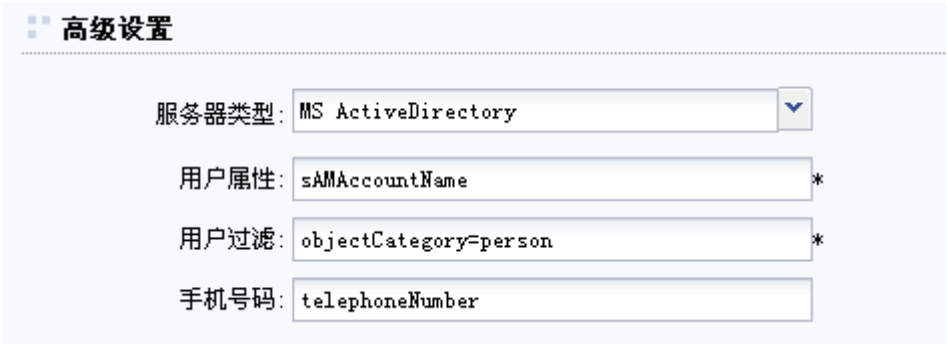
『搜索入口』用于选择需要用于认证的 LDAP 用户账号所在路径。

在所选择用户账号所在路径时，在包含（嵌套）子路径的情况下，若勾选[搜索子树]，该路径下的所有子路径的用户账号都包含进来；若不勾选[搜索子树]，则只包含该路径下的本级用户账号。

『认证超时』当连接到服务器但服务器超过这里所设置的时间仍然没有回应，就认为客户端认证失败。

『是否启用』用于设置是否启用该 LDAP 外部认证服务器。

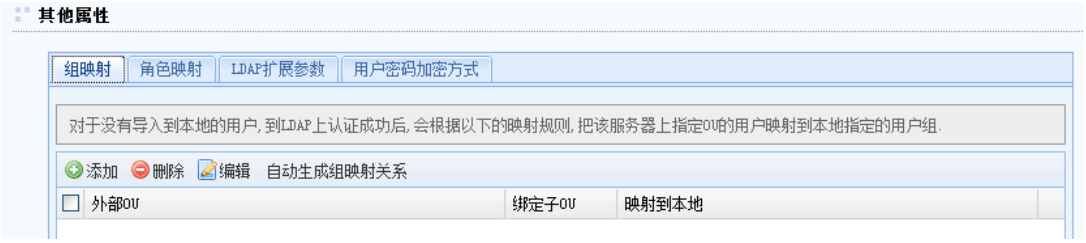
『高级设置』配置如下图：




『高级设置』相关配置，请征询 LDAP 服务器管理员的意见才能进行修改。

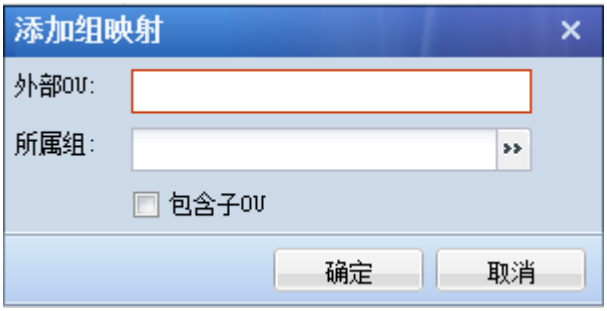
**系统支持普通的 LDAP 协议和支持微软的 MS Active Directory 协议。对于 MS-AD，用户是以属性 sAMAccountName 认证属性，以“objectCategory=person”作为过滤用户账号的条件；对于普通 LDAP 协议，用户是以属性 uid 为认证属性，以“objectclass=person”作为过滤用户账号的条件。用户也可以自定义其他属性来得到用户名和组名称。**

『其他属性』包含『组映射』、『角色映射』、『LDAP 扩展参数』和『用户名密码加密方式』。如下图：




『组映射』针对没有导入到本地的 LDAP 服务器的用户，用于设置将 LDAP 服务器中的 OU 和 SSL VPN 网关本地的用户组绑定起来，那么该 OU 中的用户登录 SSL VPN 之后就会拥有本地被绑定用户组的权限。配置页面如下图：


点击 添加，出现组映射配置页面如下。




『外部 OU』填写需要映射的 OU 在域中的 DN。

『所属组』选择该 OU 所要映射的本地用户组。

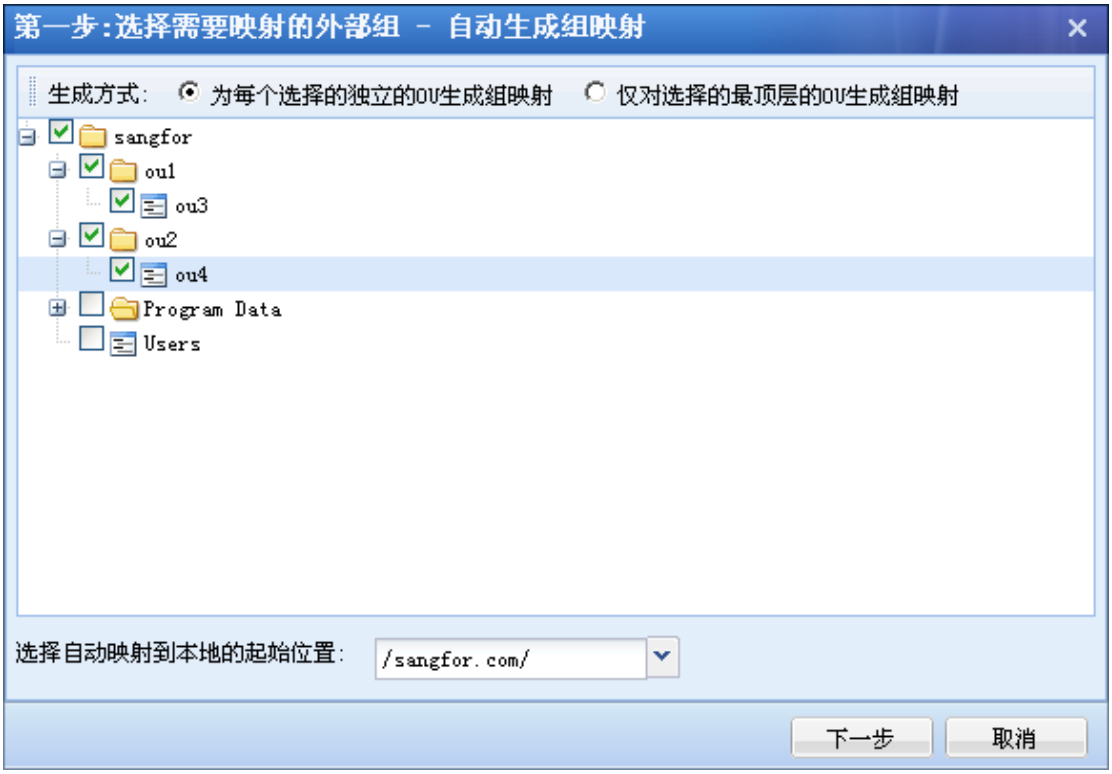
[包含子 OU]用于设置是否包含所选 OU 的子 OU。若勾选[包含子 OU]，则该 OU 下的所有子 OU 的用户账号都包含进来；若不勾选[包含子 OU]，则只包含该 OU 下的本级用户账号。

[如果未设置映射，将其自动映射到目标]用于设置当某个 OU 没有映射到本地用户组的时候，这个 OU 里边的用户认证通过之后自动匹配为那个用户组的用户。

点击 删除，可以删除所选的组映射规则。

点击 编辑，可以编辑所选的组映射规则。

点击 自动生成组映射关系，出现配置页面如下：

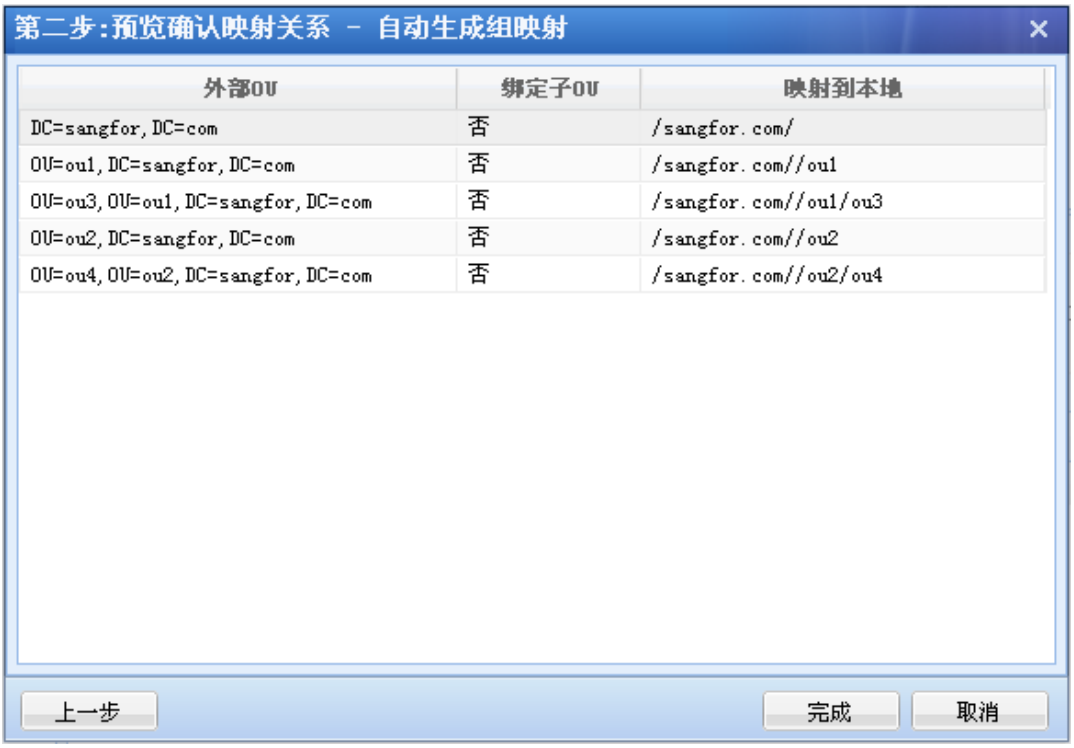



[为每个选择的独立的 OU 生成组映射]用于设置将我们所勾选的所有 OU 都在本地生成一个用户组并自动映射到该组。并且导入之后组织结构不会变化。

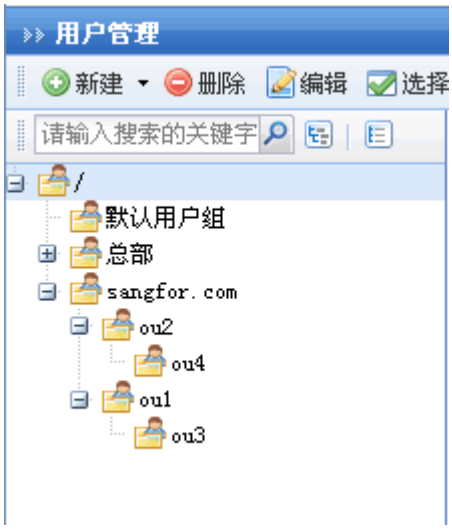
[仅对选择的最顶层的 OU 生成组映射]用于设置只将我们勾选的最上级 OU 在本地生成一个用户组，该 OU 及其下级 OU 都映射到该组。

『选择自动映射到本地的起始位置』用于设置最上级 OU 映射到的本地用户组。

点击 下一步，出现预览映射关系页面如下图：




点击 完成，则在『用户管理』中生成用户组并一一映射，如下图所示：




『角色映射』用于将 LDAP 服务器中的安全组映射到 SSL VPN 网关本地的角色，那么当域中隶属于该安全组的用户通过 SSL VPN 认证之后自动匹配到该角色，获得该角色中绑定资源的访问权限。配置页面如下图：


『是否启用角色映射』用于启用和禁用角色映射功能。

点击 添加，可以添加角色映射规则，配置页面如下图：


『外部安全组』用于设置需要映射的安全组。

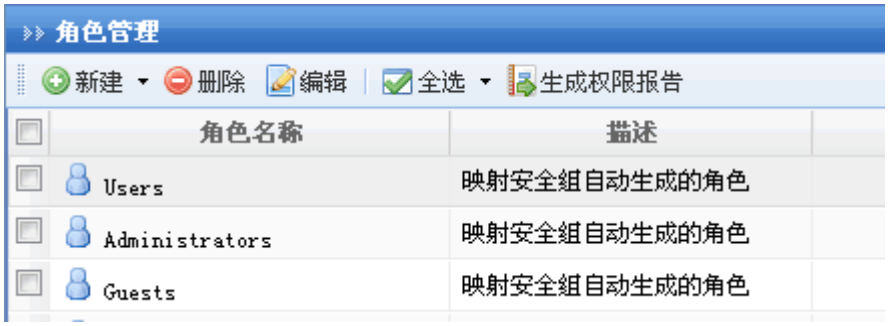
『映射角色』用于设置安全组需要映射到本地的哪个角色。

点击 删除，可以删除所选的角色映射规则。

点击 编辑，可以编辑所选的角色映射规则。

点击 自动生成角色映射关系，出现配置页面如下：


勾选外部安全组，点击 确定，则在本地『角色授权』中自动新建同名的角色并映射，如下图所示：




『LDAP 扩展属性』配置页面如下：


[关联资源的属性列表]用于设置当 LDAP 上用户认证成功后，根据关联资源的属性列表配置的信息，给用户分配相关的资源。

点击  ，弹出【添加关联资源属性】，设置需要关联的属性名。配置页面如下：


点击 确定，将属性名添加至属性列表中。

点击  ，用于删除选中的属性名。

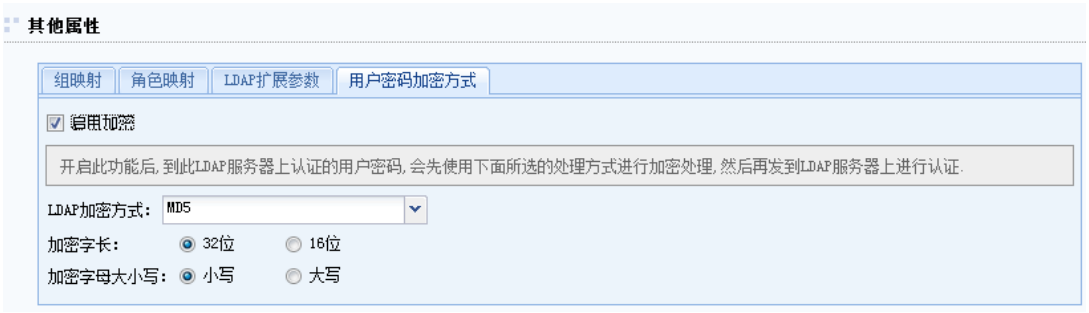
点击  ，用于编辑选中的属性名。

[继承所有上级资源]用于设置当该 LDAP 服务器上用户登录后，除了所绑定的属性的值作为资源下发到资源列表，该用户所属 OU 以及上级的所有 OU 的该属性的值也会作为资源发到资源列表。

勾选[虚拟 IP 属性名]，在右边方框内填写 LDAP 服务器上作为用户账号 IP 地址的属性名字，该 LDAP 服务器上用户登录后，LDAP 服务器返回该属性值到 SSL VPN 设备，用于该 LDAP 账号使用 L3VPN 时下发的虚拟 IP。

**以上『关联资源的属性列表』只对用户列表上不存信息的 LDAP 账号生效，若用户列表存在相应的用户账号，该功能无效。**

『用户名密码加密方式』用于将用户的密码将通过加密处理，再转发到 LDAP 服务器上进行认证。配置页面如下图：




[启用加密]：开启用户密码加密功能。

[LDAP 加密方式]：可选择 MD5 和 SHA1 这两种加密方式。

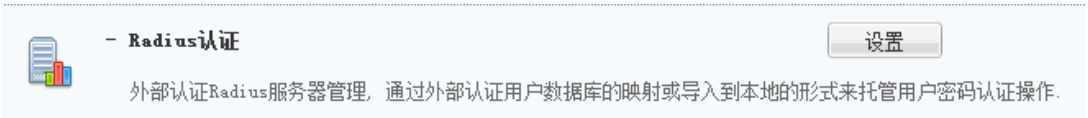
[加密字长]：可选择 32 位或者 16 位。

[加密字母大小写]：可选择将密码转换成小写或者大写。

## 3.4.1.3. RADIUS 认证

SANGFOR SSL VPN 网关支持使用“RADIUS 协议”的第三方的服务器作为认证服务器。『RADIUS 认证』就是用于设置 RADIUS 外部认证服务器相应参数的。

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『主要认证』→『RADIUS 认证』。页面如下：




点击 Radius 认证后面的 设置，弹出【RADIUS 认证服务器设置】页面，如下图：


点击 新建 出现 RADIUS 外部认证服务器的参数设置界面。参数设置页面包含『基本属性』、『RADIUS 扩展属性』、『组映射』。『基本属性』配置如下图：

『服务器名称』和『服务器描述』可随便填写便于记忆的文字。

『服务器地址』用于设置 RADIUS 服务器的 IP 地址和所使用的端口，此处可设置多个服务器地址和端口，他们之间是主备关系，第一个服务器为主服务器，其余都为备服务器，当第一个服务器连不上，才尝试连接第二个服务器认证，以此类推。

点击  ，出现服务器 IP 地址和端口的设置页面如下：


点击  ，可以删除所选的服务器地址。

点击  ，可以编辑所选的服务器地址。

点击  或  ，可以调整服务器地址的顺序。

『认证协议』可选择为[不加密的协议 PAP]、[咨询握手身份验证协议（CHAP）]、[microsoft CHAP]、[microsoft CHAP 2]或[EAP-MD5]，根据实际情况选择。

『共享密钥』、『字符集』、『认证超时』可根据实际情况填写。

『是否启用』用于设置启用或禁用该外部认证服务器。

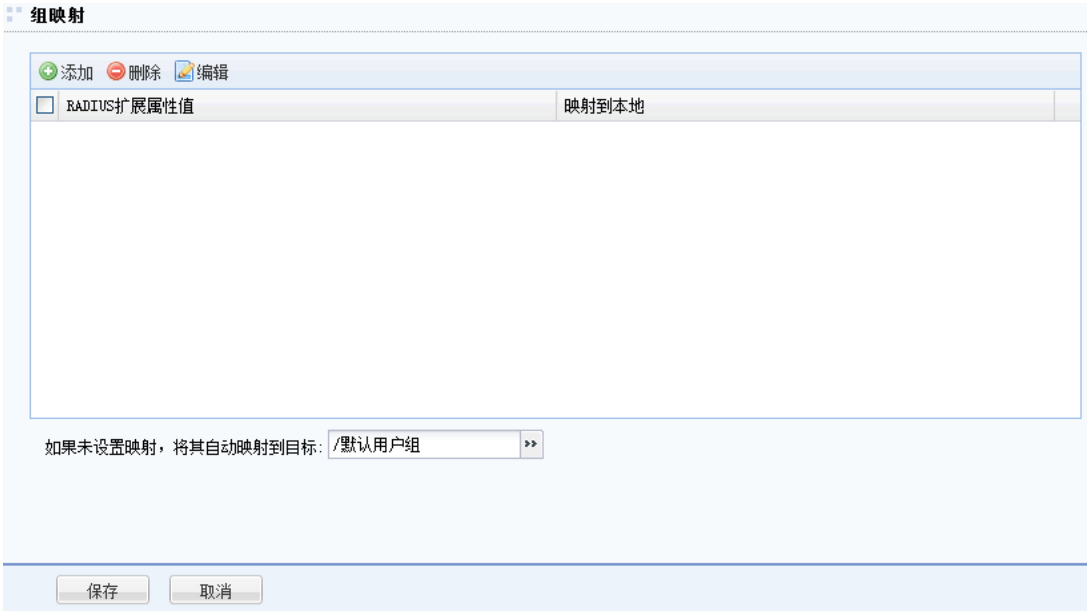
『Radius 扩展属性』配置页面如下图：


勾选『绑定手机号码 ID』，在右边第一个方框内填写 RADIUS 服务器上作为用户账号手机号码的属性 ID，第二方框填写子属性 ID。该 RADIUS 服务器上用户登录后，RADIUS 服务器返回该属性值到 SSL VPN 设备，用于短信认证。

**注：该功能可与短信认证结合使用。**

勾选[绑定虚拟 IP 地址 ID]，在右边第一个方框内填写 RADIUS 服务器上作为用户账号 IP 地址的属性 ID，第二方框填写子属性 ID。该 RADIUS 服务器上用户登录后，RADIUS 服务器返回该属性值到 SSL VPN 设备，用于该 RADIUS 账号使用 L3VPN 时下发的虚拟 IP。

『组映射』用于设置 Radius 的扩展属性值，并映射到本地组，那么当 Radius 认证用户成功认证之后，根据 Radius 中的属性值将用户分配到某个组并拥有访问该组关联资源的权限，配置页面如下图：



点击添加，配置页面如下：


『字段』用于设置 Radius 中的 Class 属性值。

『所属组』用于设置将用户分配到的本地组。

点击 确定，将设置的映射规则添加到映射规则列表。

点击 删除，删除选中的映射规则。

点击 编辑，编辑选中的映射规则。

『如果未设置映射，将其自动映射到目标』用于设置当成功登录 SSL VPN 的用户，找不到对应的组映射规则时，将该用户分配到的本地用户组。

### 3.4.1.4. 证书与 USB-KEY 认证

SANGFOR SSL VPN 不仅支持同时使用内置 CA 和外部 CA 进行认证，还可支持使用多个外部 CA。对于总部部署了 SSL 设备，各个分支接入用户使用不同的第三方 CA 进行认证的情况，大大的增加了 SSL 部署的灵活性。『证书与 USB-KEY 认证』正是用于生成、配置和管理 CA 的数字证书等。

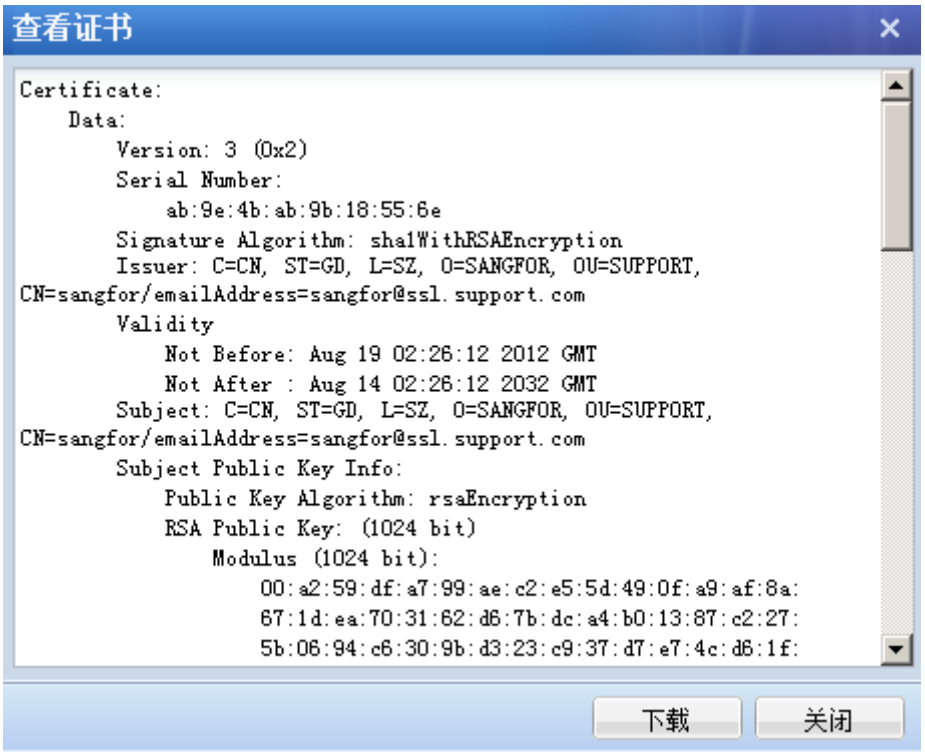
WEBUI 路径：『SSL VPN 设置』→『认证设置』→『主要认证』→『证书与 USB-KEY 认证』。页面如下：

点击 下载安装 USB-KEY 驱动，可以手动安装 USB-KEY 驱动程序。

点击 下载安装导入控件，可以手动安装证导入证书控件。

点击 设置，弹出【证书与 USB-KEY 设置】页面，可启用和禁用内置 CA，配置第三方 CA，查看在线证书和通用 USB 设置等。各部分配置页面如下：


点击内置 CA 的 查看 按钮，查看内置 CA 的根证书，显示如下：




点击内置 CA 的 更新 按钮，设置页面如下图：


选择密钥标准，可以切换 SSLVPN 用于证书认证加密的加密密钥标准，包括国际商用密码标准 RSA 和中国国家密码标准 SM2。RSA 密钥标准的密钥长度可以选择 1024/2048/4096，而 SM2 密钥标准只采用 256 的密钥长度。

输入证书所需的各项信息，点击 完成 生成根证书。

**注意：1.自建 CA 时，国家名为 2 个英文字符。例如：CN。**

**2. 邮件地址不支持中文。**

如果勾选了[更新设备证书]，并选择[使用内置 CA 为设备颁发新证书]，点击 下一步，则出现内置 SSL 证书信息设置页面，如下图：

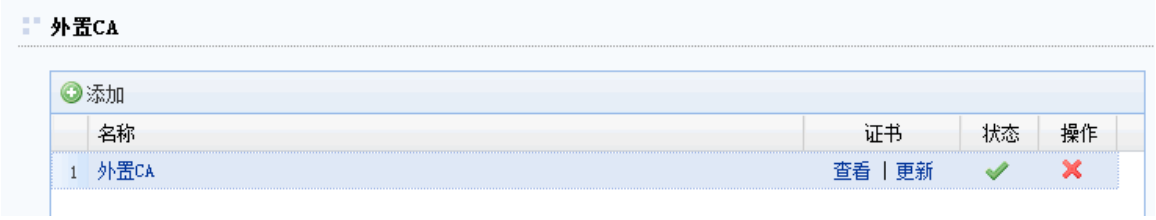

输入证书所需各项信息之后，点击 完成，此时根据所填写根证书及 SSL 证书信息同时生成根证书和 SSL 证书；.

如果勾选了[更新设备证书]，并选择[使用内置 CA 的根证书作为设备证书]，点击 完成，此时生成根证书并将根证书同时作为设备证书。

点击 签发用户证书，生成一个证书，该证书可作为用户证书也可作为服务器证书。

点击外置 CA 的 添加 按钮，添加外置 CA，同时支持 7 个外置 CA 的认证，显示如下：


导入外置 CA 证书并设置 CA 名称，点击 确定 保存。添加成功后，显示如下：




点击证书名称，设置证书相关选项。


[用户名属性] 是指此 CA 签发的证书中，存放用户名的字段；用户名将显示在客户端主界面上，支持使用 CN、Email 前缀和 OID 作为用户名属性。

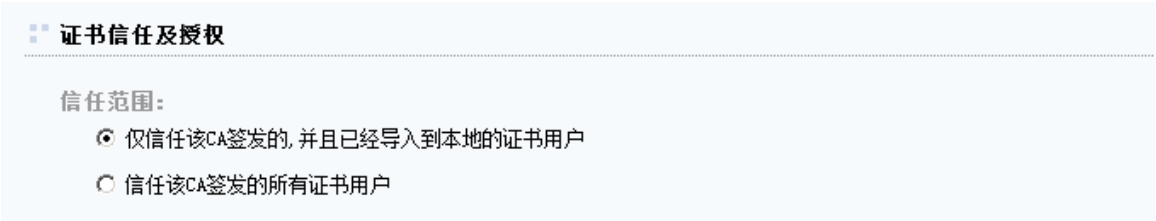
[绑定字段] 指此 CA 颁发的证书导入到本地时，用户所绑定的证书字段。

序列号：证书过期后，CA 会重新签发证书，因为新证书的序列号已改变，必须在本地用户管理中，重新导入新证书；

DN：相比证书序列号，可以避免用户证书更新时需要重新导入证书。选择此选项时，必须保证不同证书的 DN 名是唯一的；

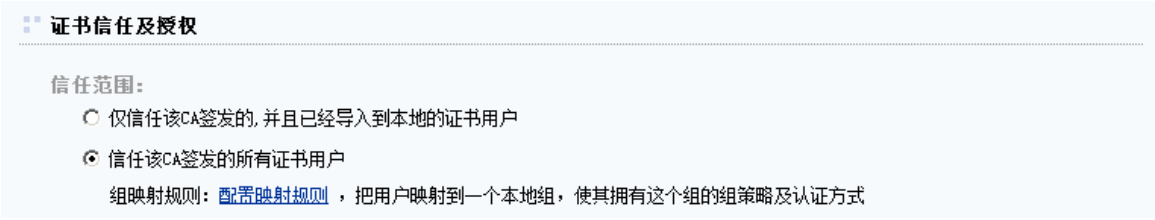
OID：与 DN 类似，通常需要填写存放用户名等唯一标识用户的 OID 属性。

[证书编码]用于设置此证书使用的编码格式。

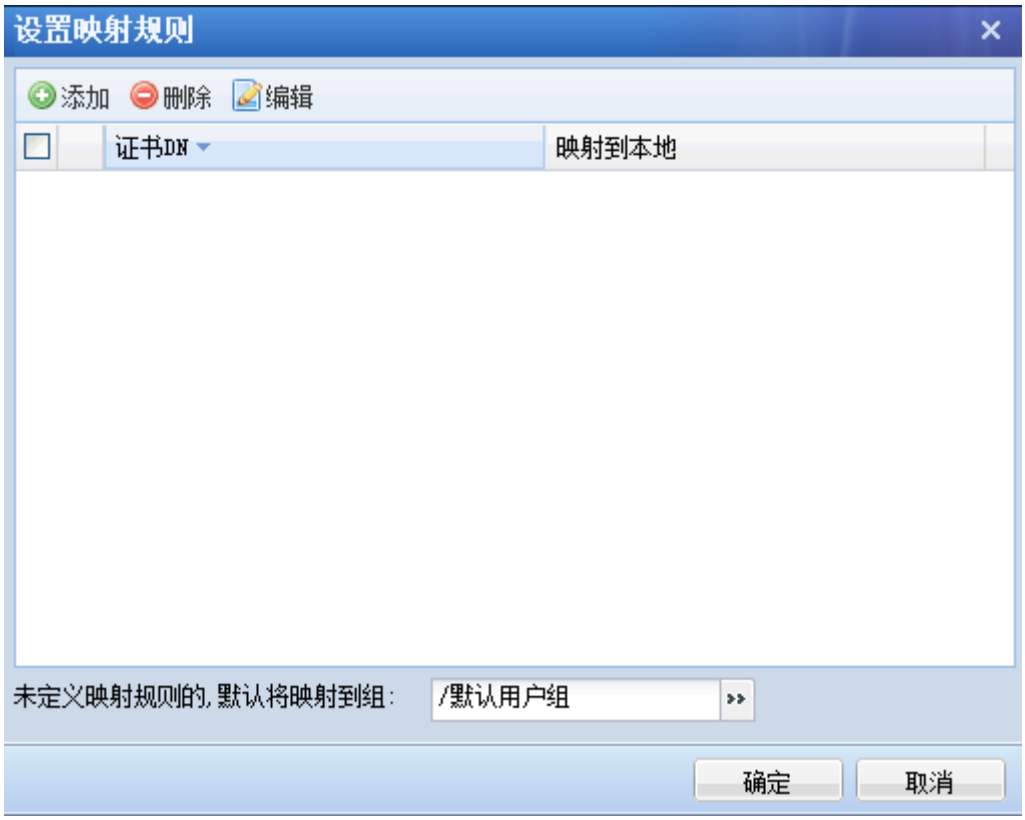


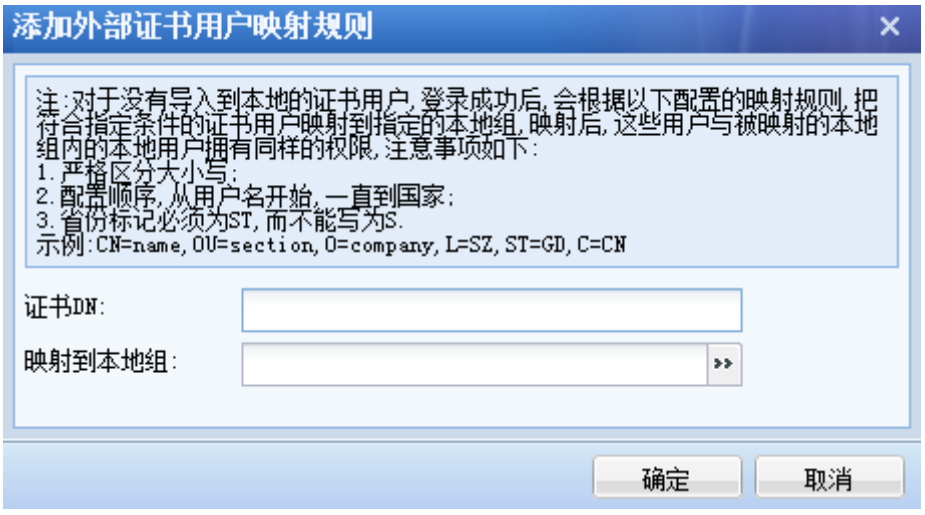

选择『仅信任该 CA 签发的，并且已经导入到本地的证书用户』，则只有当用户证书被导入到 SSL VPN 网关，用户才能通过该用户证书登录 SSL。

选择『信任该 CA 签发的所有证书用户』，则只要是 CA 颁发的有效用户证书，都允许登录 SSL。配置页面如下：




点击 配置映射规则 用于设置将特定某证书 DN 映射到 SSL 本地用户组，使这些证书用户登录 SSL 之后自动分配到该用户组，并拥有该用户组的权限。设置页面如下：



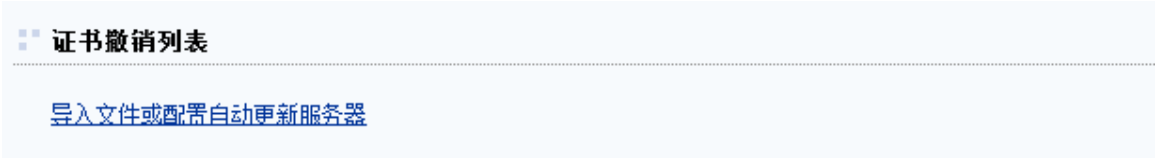

『证书 DN』可以通过证书主题查看。

『映射到本地组』用于设置拥有该字段证书登录后映射到的用户组。

点击 删除，可以删除选中的映射规则。

点击 编辑，可以编辑选中的映射规则。

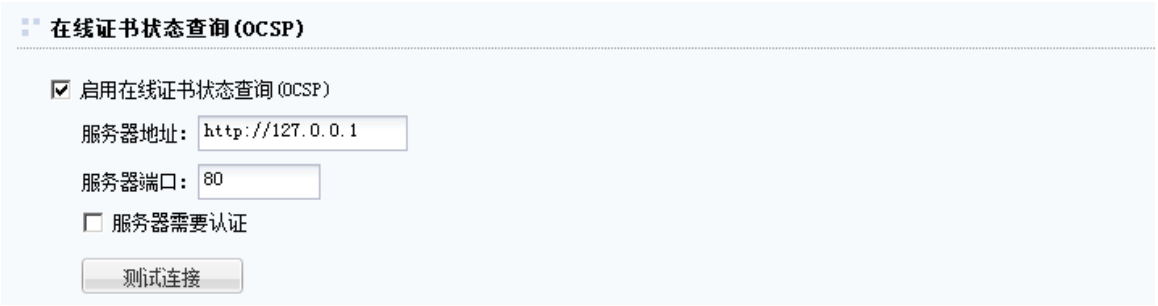
『未定义映射规则的，默认将映射到组』用于设置对于没有做映射规则的证书，登录 SSL 后默认被分配到哪个用户组。




点击 导入文件或配置自动更新服务器，可以手动更新或配置自动更新证书撤销列表，撤销列表支持格式为：*.crl。配置页面如下图：

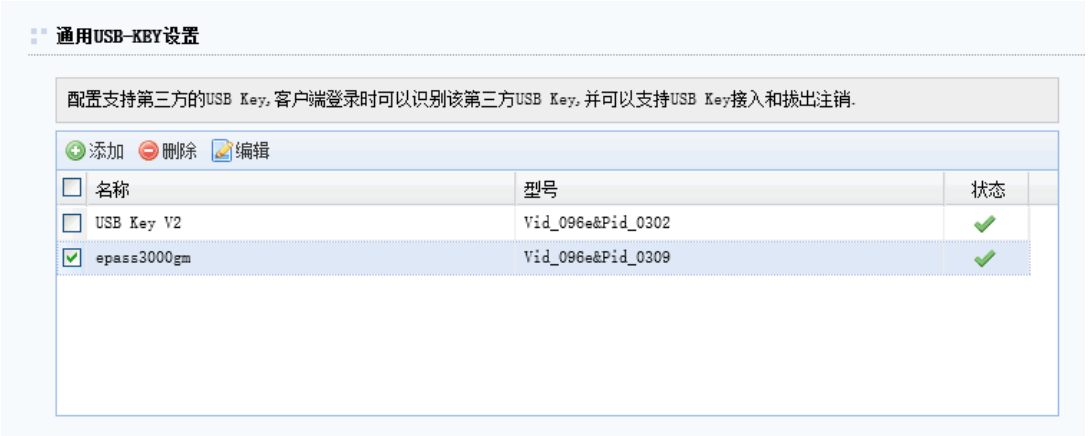

选择相应的证书吊销列表文件进行导入，若选择自动更新配置，则弹出如下界面：


勾选[启用自动更新 CRL]并设置颁发点地址和更新频率。




[在线证书状态查询]用于实时的更新 CA 证书的状态。

『通用 USB-KEY 设置』用于配置支持第三方 USB KEY 的接入和拔出注销，配置好 USB KEY 的型号，当用户登录时，SANGFOR SSL 网关会检测 USB KEY 的型号，假如和我们设置的型号对应，那么当用户将 USB KEY 拔出时，用户将自动注销。配置如下图：




点击 添加，配置页面如下：


『名称』自定义此设置的名称。

『型号』用于设置需要拔出 USB KEY 自动注销用户的 USB KEY 型号。

『动态库文件路径』当添加第三方 KEY 用于支持中国国家密码标准 SM2 的认证加密算法时，需要指定该 KEY 的驱动文件中提供 SM2 加密的函数接口。动态库文件路径即用于设置 SM2 加密函数接口的动态链接库文件的路径。

『是否启用』用于设置对该型号 USB KEY 启用或禁用拔出 KEY 自动注销功能。

点击 确定，保存配置，并将配置添加到列表中。

点击 删除，用于删除列表中的 USB KEY 信息。

点击 编辑，用于编辑列表中的 USB KEY 信息。

### 3.4.1.5. 域单点登录认证

域单点登录认证用于解决客户端 PC 已经登录域的情况下，使用 C/S 登录客户端登录 SSL VPN 时无需再输入用户名及密码，即可自动完成域认证，成功登录 SSL。域单点登录认证只支持客户端方式的登录，不支持网页形式的登录。

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『主要认证』→『域单点登录认证』。页面如下：


点击域单点登录认证后面的 设置，弹出【域单点登录认证设置】页面，如下图：

『域单点登录』勾选[启用]，启用域单点登录功能。

『服务器域名』用来设置 Windows 域的域名。

『域名简称』用来设置 Windows 域的域名简称。

『域控计算机全名』用来设置 Windows 域的域控制器名称。

『域控 IP 地址』用来设置 Windows 域的域控制器的 IP 地址。

『域管理员名』用来设置登录 Windows 域的管理员帐号。

『域管理员密码』用来设置登录 Windows 域的管理员密码。

## 3.4.2. 辅助认证

『辅助认证』包含『短信验证码』、『硬件特征码』、『动态令牌认证』。点击『短信验证码』、『硬件特征码』、『动态令牌认证』的 设置 出现相关认证的设置页面。

### 3.4.2.1. 短信验证码

『短信验证码』即 SSL VPN 用户登录时，输入用户名/密码后，SSL VPN 网关会使用发送短信的方式向该用户的手机号码发送一个动态生成的随机密码，即短信验证码，登录用户必须输入该验证码，才能成功登录 SSL VPN，访问内网资源。

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『辅助认证』→『短信验证码』。页面如下：


点击 设置，弹出【短信认证设置】页面，如下图：


『短信验证码』用于设置启用或禁用短信认证功能。

『绑定手机号码』用于设置是否允许未绑定手机号码的用户登陆时自动绑定手机号码。开启该功能后，管理员无需给每个用户手动设置手机号码，用户管理里的用户只要选择短信认证，手机号码留空，用户登陆时需要自行填写发送短信认证码的手机号码，认证成功后自动给用户绑定该手机号码。

『重新发送间隔』用于设置短信发送间隔时间。

『验证码有效期』用于设定动态密码的有效时间，用户登录 SSL VPN 时，如果输入的动态密码超过了有效时间，则登录失败，需要重新获取验证码。可定义时间为 1－1440 分钟。

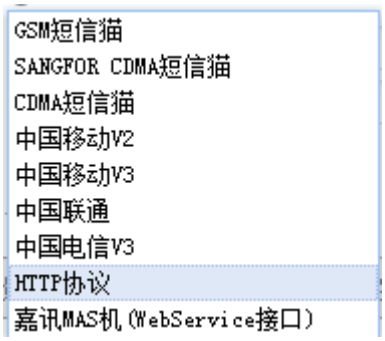
『短信内容』用于设定发送到客户端手机上短信的内容。

点击 恢复初始内容，可以短信的内容恢复为默认值。

『短信验证码发送模块选择』包括[通过设备内置短信模块发送]和[通过安装在外部服务器上的短信模块发送]两种方式。配置如下图：

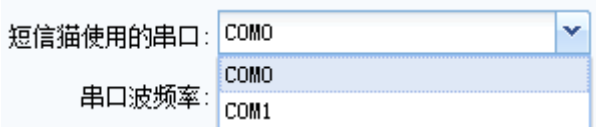

『短信发送参数』用来配置发送短信的参数，配置如下图：


『短信网关类型』用来配置发送短信的网关类型，可以选择通过[GSM 短信猫]（接到短信模块服务器 com 口）、[SANGFOR CDMA 短信猫]、[CDMA 短信猫]、[中国移动 V2]、[中国移动 V3]、[中国联通]、[中国电信 V3]和[HTTP 协议]和[嘉讯 MAS 机(WebService 接口)]的短信网关发送。

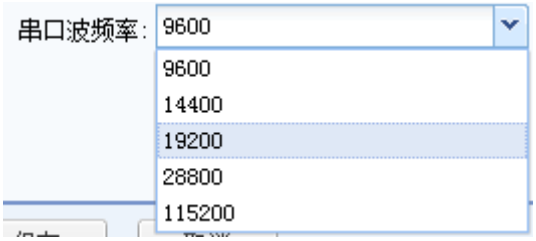



『短信中心』短信猫所对应的运营商的短信中心号码。

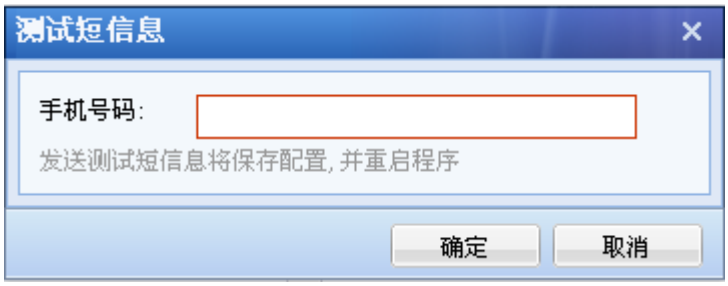
『短信猫使用的串口』即短信猫所使用的串口。可选择[COM0]和[COM1]，如下图：




『串口波频率』SSL VPN 设备和相连的短信猫通讯的波特率，可选择五种波频率，一般用默认的 9600 即可。




点击 发送测试短信息，出现测试短信息的设置页面：




『测试短信息』是用于测试短信猫或者短信网关能否正常发送短信，填入接收短信的手机号码，点击 确定，发送测试短信。

**要配置短信验证码，需要先开通短信认证序列号（可参考 3.1.1“序列号管理”章节）否则会有如下提示：**


**点击 点击这里，可以跳转到『序列号管理』页面。**

**通过设备内置短信模块发送**

[通过设备内置短信模块发送]表示使用 SSL 设备自带的短信中心模块功能。

短信网关类型选择『短信猫』，那么除了 SSLVPN 设备，还需要准备的硬件有短信猫和电话卡。

第一步：将一手机 sim 卡放入短信 Modem 内；

第二步：通过发货时自带的串口线（一端为公头，另一端为母头）将短信猫连接到 SSL VPN 设备后面的 CONSOLE 口上，注意把接口上的旋钮扭紧，确保串口线和短信 Modem 以及串口线和短信服务器接触良好。

第三步：『短信发送参数』中『短信网关类型』选择[GSM 短信猫]。

第四步：『短信发送参数』中『短信中心』为当地短信服务运营商的短信服务号码，例如深圳的为：8613800755500。

第五步：『短信网关配置』中『短信猫使用串口』选择[COM0]。

第六步： 『短信发送参数』中[串口波频率]为 SSL VPN 设备和相连的短信猫通讯的波特率，一般为 9600，可根据所使用的短信 modem 实际参数进行设置。

第七步：点击 保存，配置完成。

如下图所示：


第八步：对用户启用短信认证；

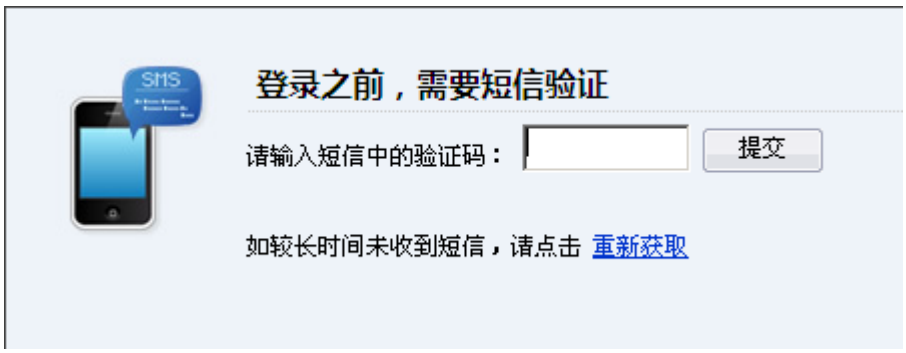
**1. 『账户类型』必须勾为[私有用户]；『辅助认证』必须勾选短信认证；**

**2. 『手机号码』可留空，支持最多填写 2 个。如果手机号码留空的话，必须启用[允许未绑定手机号码的用户登陆时自动绑定手机号码]，用户通过网页登陆时系统会提示填写发送短信验证码的手机号码，如下图所示：**


**3. 启用[允许未绑定手机号码的用户登陆时自动绑定手机号码]，且用户手机号码留空的时候，通过 EC 登录是不会提示填写发送短信验证码的手机号码的，只有通过网页登陆才会提示。**

第九步：登录 SSLVPN。首先输入用户名和密码，点击 登录 按钮，会弹出短信认证的页面。

如下图所示：




输入手机收到的短信检验码，点击 提交 即可。如果没有收到短信，可以点击 重新获取 按钮。

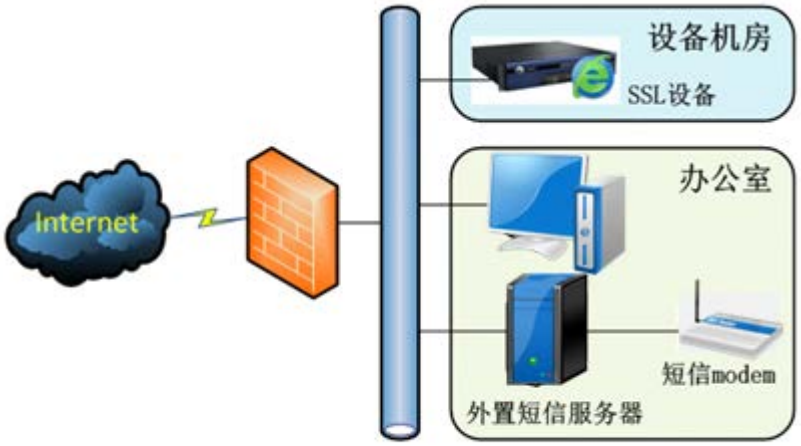

**通过安装在外部服务器上的短信模块发送**

[通过安装在外部服务器上的短信模块发送]即短信模块安装在某一台服务器上，通过短信服务器来发送短信；短信网关类型可以选择[GSM 短信猫] /[CDMA 短信猫]/[SANGFOR CDMA 短信猫]。

以短信猫为例说明『外置短信模块』的使用方法。构建短信服务器只需要一台主板上带有 com 口的电脑，并且安装上深信服公司提供的短信服务软件即可。

支持系统：Windows XP、Windows 2000、Windows 2003，不支持 vista 系统。

外置短信模块结构图：




第一步：将一手机 sim 卡放入短信 Modem 内；

第二步：短信 Modem 通过发货时自带的串口线（一端为公头，另一端为母头）连接到短信服务器（电脑）的 com 口上，注意把接口上的旋钮扭紧，确保串口线和短信 Modem 以及串口线和短信服务器接触良好；

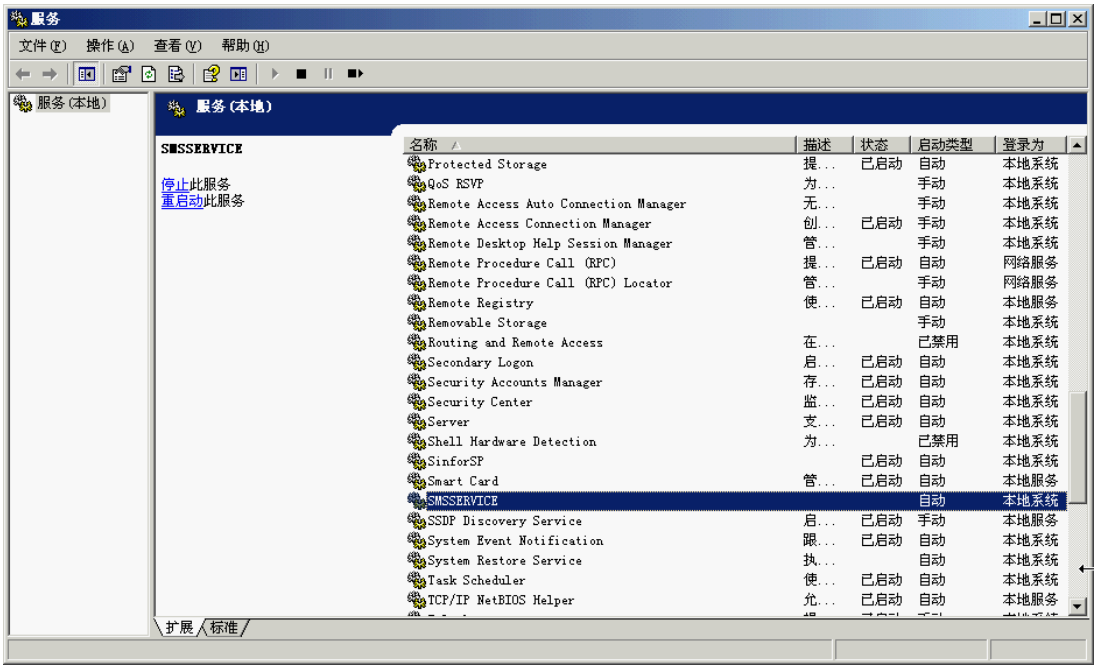
第三步：在短信服务器上安装深信服提供的软件安装包；

第四步：软件安装完成后，短信服务会以系统服务的形式自动运行，短信服务进程为“SMSSP.exe”；

如下图所示：


在服务列表中能够看到短信服务“SMSSERVICE”；

如下图所示：



在系统的“开始”菜单打开短信服务软件的控制台，进行配置


在系统桌面右下角的控制台能够看到当前短信服务的状态，左图为服务正常，右图为服务异常



如果软件安装好后，服务仍然显示停止，一般情况下是由于软件没有安装在系统盘下造成的，请把软件重新安装在默认路径下。

第五步：鼠标右键点击控制台，选择“Config”


在软件服务的监听端口设置对话框里，设置好监听端口（TCP 端口），如果服务器还提供其他服务，可以使用 netstat –na 查看服务器上已监听的端口，要保证设置的端口和这些服务的端口不冲突


如果短信服务器上装有防火墙软件，必须保证防火墙有放通此处设置的短信服务监听端口。

至此“外置短信服务器”设置完毕。

第六步：登录 SSLVPN 设备的控制台，打开『SSLVPN 设置』→『认证设置』→『短信验证码』，配置短信认证信息。

配置如下图所示：


『短信中心地址』填上短信服务器的 IP，必须保证 SSL 设备能够和短信服务器正常通信（SSL 设备能够连通短信服务的监听端口）。

『短信中心端口』填上短信服务软件的监听端口。

『短信网关类型』下拉框，选择[GSM 短信猫]。

『短信中心』填写短信 Modem 上所放入的 sim 卡的短信中心号码，根据 sim 卡的实际情况填写（可咨询 sim 卡的服务提供商）。

『短信猫使用的串口』根据实际情况填写，目前一般电脑只有一个 com 口，选则“0”就可以了，若接到第二个 com 口上，则选择“1”。

『串口波频率』下拉框选择[9600]。

第七步：对用户启用短信认证；

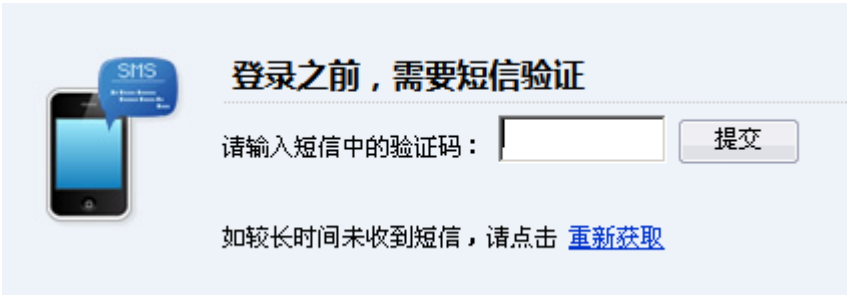

1. **『账户类型』必须勾为[私有用户]；『辅助认证』必须勾选短信认证；**

**2.【手机号码】可留空，支持最多填写 2 个。如果手机号码留空的话，必须启用[允许未绑定手机号码的用户登陆时自动绑定手机号码]，用户登陆时系统会提示填写发送短信验证码的手机号码，如下图所示：**


**3. 启用[允许未绑定手机号码的用户登陆时自动绑定手机号码]，且用户手机号码留空的时候，通过 EC 登录是不会提示填写发送短信验证码的手机号码的，只有通过网页登陆才会提示。**

第八步：登录 SSLVPN。首先输入用户名和密码，点击 登录 按钮，会弹出短信认证的页面。

如下图所示：




输入手机收到的短信检验码，点击 提交 即可。如果没有收到短信，可以点击 重新获取

按钮。

**使用运营商短信网关**

如果网络中已经有中国移动短信网关或者中国联通短信网关，可以和 SSLVPN 结合使用。配置方法如下：

『短信网关类型』中选择[中国移动 V2]/[中国移动 V3]/[中国联通]/[中国电信 V3]。

如果启用『外置短信模块』，『短信模块设置』中『短信中心地址』填写短信模块软件服务器的 IP，『短信中心端口』填写短信模块软件实际监听的端口。

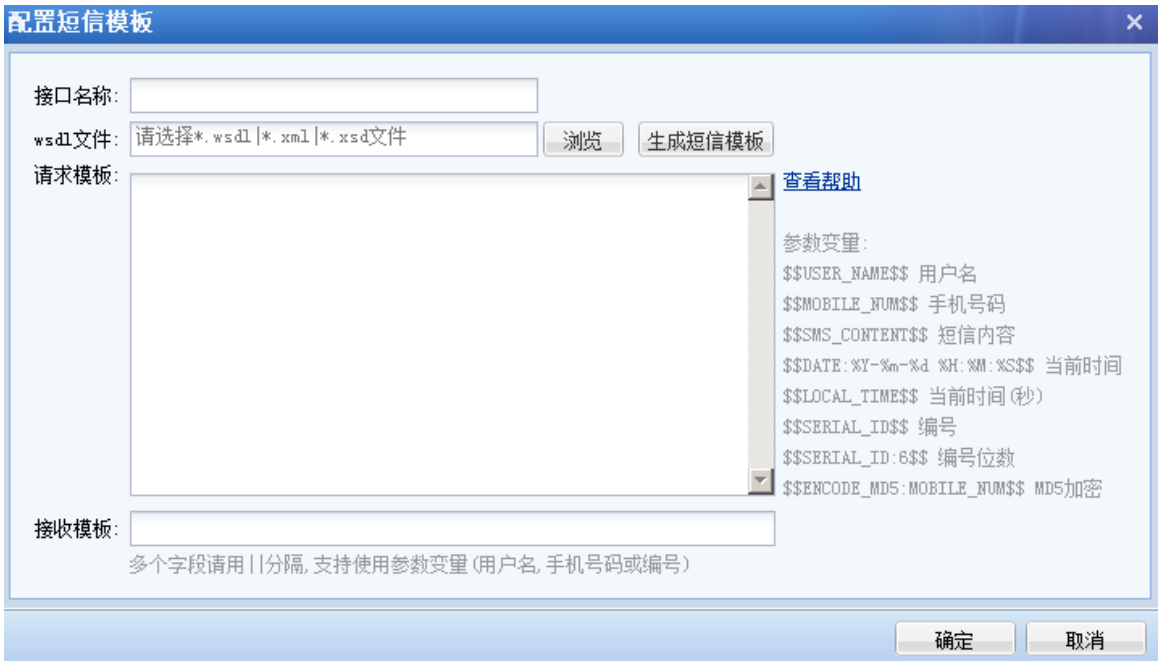
『短信发送参数』中的剩余的『短信网关服务器地址』、『短信网关服务器端口』、『企业代码』、『业务代码』、『SP 接入号』、『网关编号』、『登录帐号』、『登录口令』、『确认口令』信息请按照短信服务提供商提供的相关参数填写。

**使用 webservice 方式发送短信校验码**

SSL VPN 网关设备可以与基于 webservice 的短信平台联动，支持以 webservice 方式发送短信校验码，保障加强短信发送的稳定性。配置界面如下：

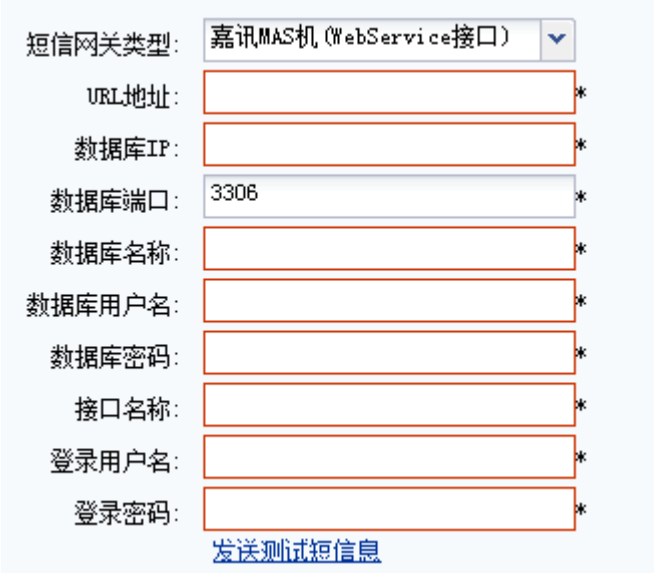

『短信网关类型』中选择 HTTP 协议，设置 webservice 短信网关平台的地址，页面编码方式以及 SOAP 版本和请求类型。

点击 配置短信模板 用于设置短信模板的接口名称等信息。




**使用嘉讯 MAS 机(WebService 接口）发送短信校验码**

SSL VPN 网关设备可以与嘉讯 MAS 机的短信平台联动，支持通过嘉讯 MAS 机发送短信校验码，保障加强短信发送的稳定性。配置界面如下：




[URL 地址]：填写嘉讯 MAS 机的公网地址。

[数据库 IP]：嘉讯 MAS 机采用的数据库的 IP 地址。

[数据库端口]：默认端口是 3306，请根据实际情况填写。

[数据库名称]：填写嘉讯 MAS 机对应的数据库名称。需与管理员确认填写正确的数据库名称。

[数据库用户名]和[数据库密码]：填写嘉讯 MAS 机内部数据库用户名和密码，作用是组成初始化报文发送到嘉讯 MAS 机。需与管理员确认填写正确的数据库用户名和密码。

[接口名称]：Webservice 发送短信的接口名称。

[登陆用户名]：填写嘉讯 MAS 机登陆的用户名。

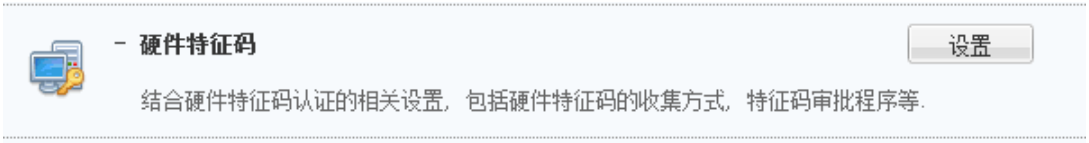
[登陆密码]：填写嘉讯 MAS 机登陆的密码。

### 3.4.2.2. 硬件特征码

『硬件特征码』根据计算机的硬件特性按一定的算法生成的一个序号，由于硬件特性的唯一性，使得该硬件特征码也是唯一的、不可伪造的，所以对于不同的计算机，此序号必然不同。

『硬件特征码』用于对用户的硬件特征码权限进行设置。

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『辅助认证』→『硬件特征码』。页面如下：




点击 设置，弹出【硬件特征码认证设置】页面，如下图所示：


[启用硬件特征码收集]选择此项，则设备只收集用户登录的硬件特征码，但不会启用硬件特征码认证。

[启用硬件特征码认证]选择此项，则开启硬件特征码认证。

『自定义提示信息』提示用户提交硬件特征码时的用语。

[自动审批]勾选此项后，用户提交的硬件特征码不需要管理员手工审批，可自动通过审批。

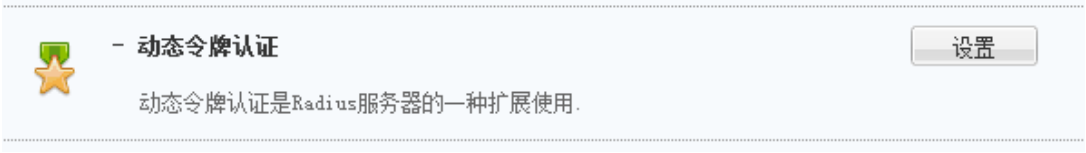
[所有已审核的终端上，允许任意账号登录]勾选此项后，如果某一用户使用的计算机提交了硬件特征码并通过了审批，则其他用户用此计算机登录所提交的硬件特征码可自动通过审批。

点击 保存 使配置生效。

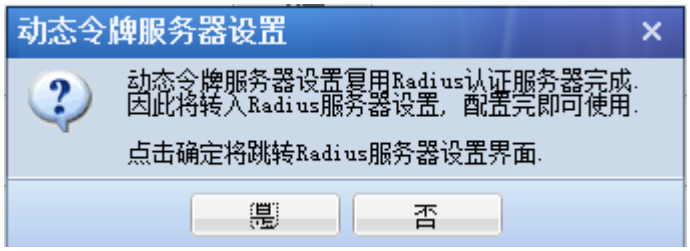
### 3.4.2.3. 动态令牌认证

『动态令牌认证』是 Radius 服务器的一种扩展使用，通过与 Radius 服务器结合并为用户配发动态令牌，通过动态令牌上的动态密码进行登录，由此增加登录的安全性。

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『辅助认证』→『动态令牌认证』。页面如下：




点击动态令牌认证的 设置 按钮，出现动态令牌服务器设置框如下：




点击 是，跳转到 Radius 认证服务器管理页面，详细配置请参照 4.4.1.3 章节。

## 3.4.3. 认证选项设置

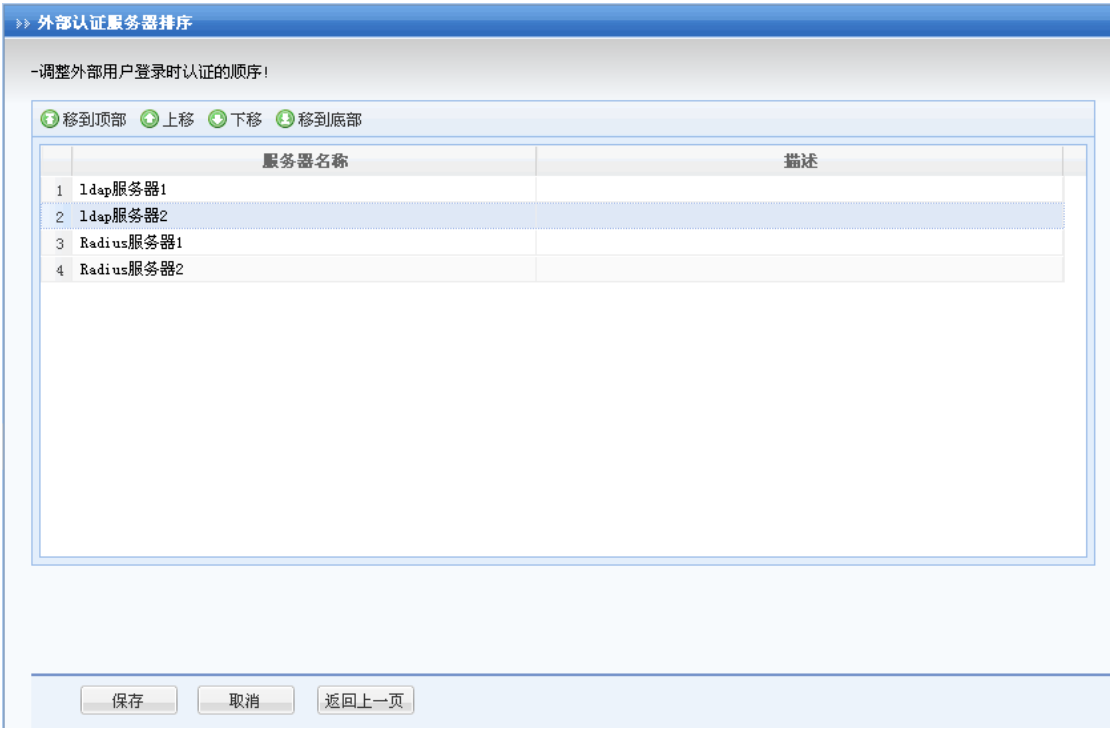
『认证选项设置』包含『LDAP 与 Radius 服务器认证优先级设置』、『密码认证选项』和『匿名登录设置』。

### 3.4.3.1. LDAP 与 Radius 服务器认证优先级设置

『LDAP 与 Radius 服务器认证优先级设置』用于设置用户通过外部服务器中的用户名密码认证时，到各个服务器中认证的优先级。

WEBUI 路径：『SSLVPN 设置』→『认证设置』→『LDAP 与 Radius 服务器认证优先级设置』，页面如下：

点击设置，弹出【外部认证服务器排序】页面，如下图：




【外部认证服务器排序】用于对设置好的 LDAP 和 Radius 服务器进行排序，当外部认证用户登录时，先到第一个服务器中认证，当第一个服务器中无此用户时，再到第二个服务器中认证，以此类推。

选中某台服务器，点击 移到顶部、上移、下移、移到底部，可对服务器进行相应的排序。

点击 保存，完成并保存配置。

## 3.4.3.2. 密码认证选项

『密码认证选项』用于设置当用户通过用户名密码方式认证登录 SSL VPN 时的一些相关选项设置。

WEBUI 路径：『SSLVPN 设置』→『认证设置』→『密码认证选项』，如下图：


点击设置，弹出【密码认证选项设置】页面，包含『用户登录时校验选项』和『防止暴力破解选项』，如下图：


『用户登录时校验选项』的配置页面如下：


勾选[启用软键盘]，可以在 SSL VPN 登录页面启用软键盘和图形校验码，增强登录的安全性。勾选[启用软键盘]并勾选[数字顺序变化]或[字母顺序变化]则每次登录时数字顺序或字母顺序都会改变。如下图所示：

勾选『启用软键盘』，打开登录页面：


点击密码输入框后的小键盘图标，页面如下：


『防止暴力破解选项』是一种安全机制，可设置用户用相同用户名连续输错多少次密码则冻结该用户，该用户在一段时间内将无法登录；或者用户用相同一个 IP 地址连续输错多少次密码，则启用图形校验码或者锁定该 IP 一段时间。配置如下图所示：


图形验证码选项设置中，输入 0 表示强制启用，即默认启用图形验证码；输入小于 3 时，非 Windows 客户端仍然以 3 次为标准。


当客户登录 SSL VPN，连续输错 5 次密码即锁定用户，结果如下图所示。


当设置同 IP 连续输错 64 次密码后启用图形校验码认证，SSL 客户端同一个 IP 连续输错 64 次密码之后，结果如下图所示。


当设置同 IP 连续输错 64 次密码后暂时拒绝同 IP 登录，SSL 客户端同一个 IP 连续输错 64 次密码之后，结果如下图所示。


### 3.4.3.3. 匿名登录设置

『匿名登录设置』可设置用户无需输入账号密码，匿名登录 SSLVPN，并访问相应的资源。

WEBUI 路径：『SSL VPN 设置』→『认证设置』→『认证选项设置』→『匿名登录设置』。如下图：


点击设置，弹出【匿名登陆设置页面】，界面如下所示：

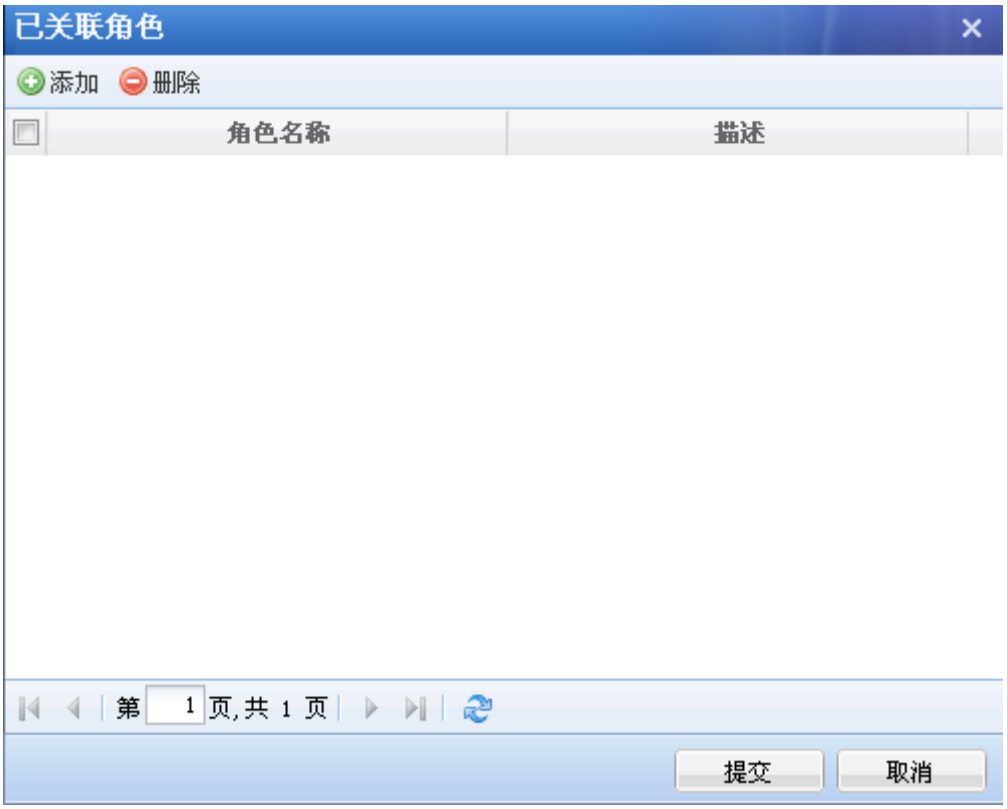
勾选[启用]，登录 SSLVPN 时，即可点击匿名登录的按钮登录 SSLVPN，如下图：


勾选[全部用户都使用匿名账号登录]则用户输入登录 SSLVPN 的地址之后，不会显示我们 SSLVPN 的登录界面，而是直接跳转到资源列表界面（如果对匿名用户启用了默认资源页面则跳转到默认资源页面）。

点击 匿名用户组配置 即可对匿名用户组进行相应的设置。

设置匿名用户组的基本属性，用户组具体配置可以参考 4.1『用户管理』章节，如图：


点击 匿名用户角色授权 即可对匿名用户组关联相应的角色，角色具体配置可以参考 4.3『角色授权』章节，如图：



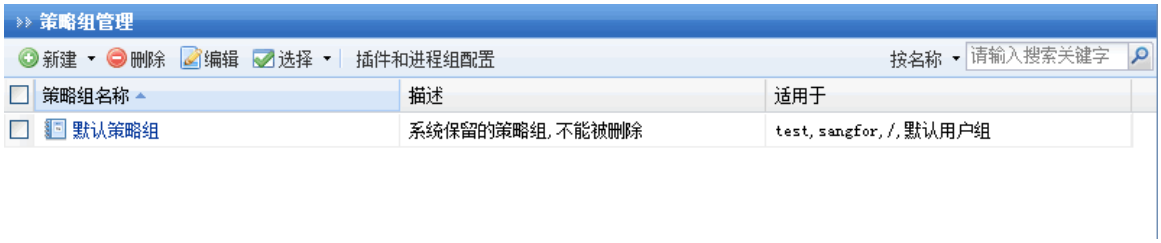

选择[禁用]，禁止用户匿名登录 SSL VPN。

最后点击 保存 并 配置生效。

## 3.5. 策略组管理

『策略组管理』用于配置客户端相关选项、账号控制、安全桌面及远程应用等。

WEBUI 路径：『系统菜单』→『SSL VPN 设置』→『策略组管理』。界面如下图所示：




『策略组名称』显示策略组的名称。

『描述』用来显示策略组的描述信息。

『适用于』显示引用该策略组的用户/用户组。

点击 新建，选择 新建策略组，用来新建策略组。

点击 新建，选择 以所选策略组为模板新建，用来以已经存在的策略组作为模板来新建一个策略组。使用此功能必须要先勾选一个策略组。

点击 删除，用来删除勾选的策略组。

点击 编辑，用来编辑勾选的策略组。

点击 全选，用来选择当前页或所有页的策略，也可以取消选择，如下图：


查询中可选择[按名称]、[按描述]或[按适用范围]来查找策略组。在输入搜索关键字中输入相应的关键字，点击后面的即可。

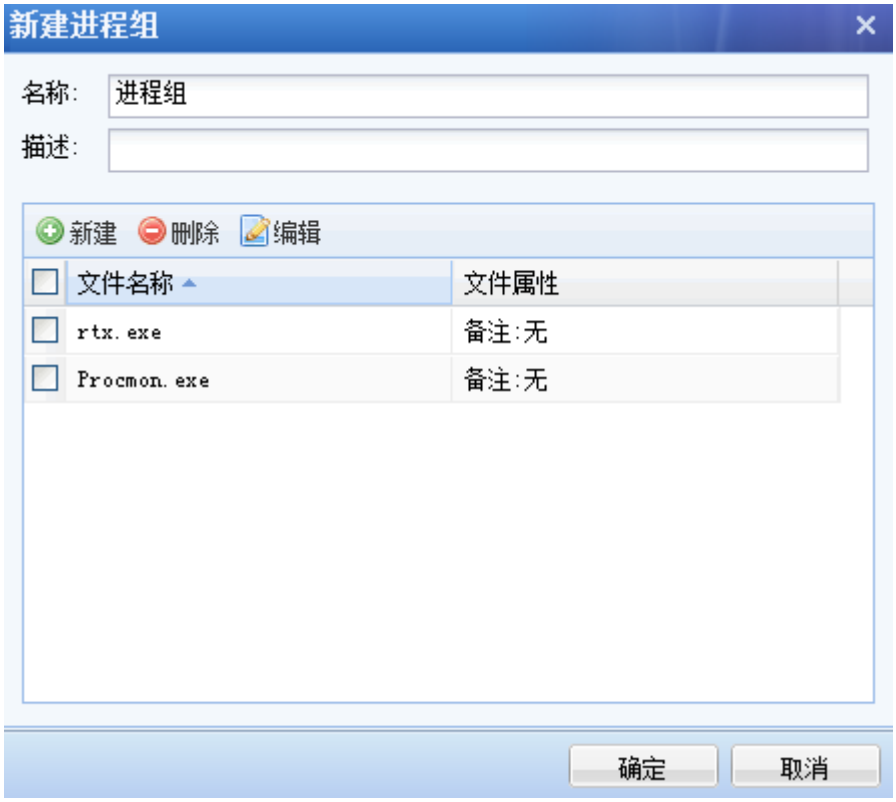
点击 进程和插件组配置 用于设置需要在安全桌面策略组内引用的进程和插件组。

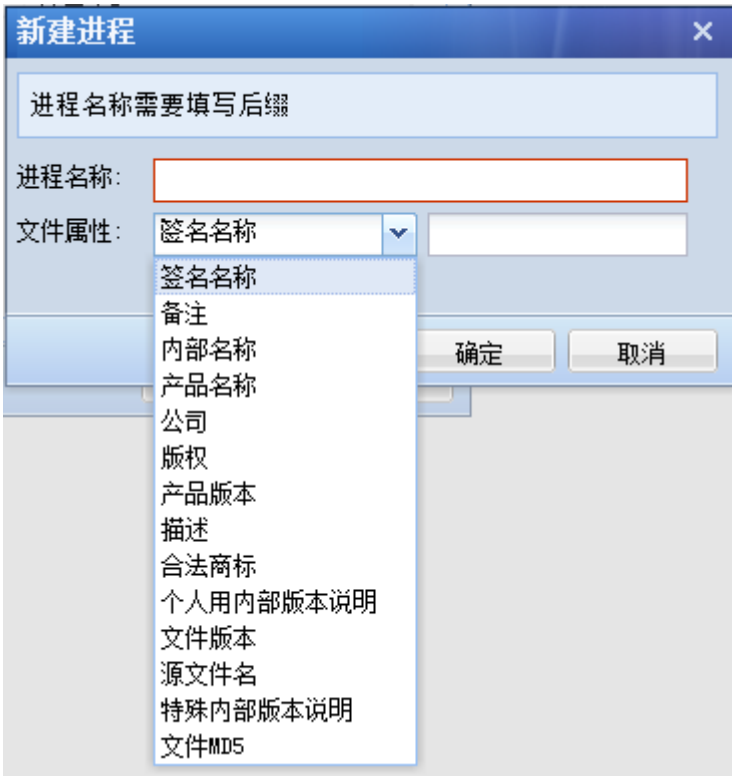

『插件列表』点击 新建 按钮，填写需要在安全桌面内放行的插件名称。


[文件名称]填写插件的名称。

[签名名称]填写插件的签名者。

『进程组列表』点击 新建 按钮，填写需要在安全桌面内放行的进程名称。






点击 新建，选择 新建策略组，弹出【新建策略组】页面。界面如下图所示：


『名称』定义策略组的名称。

『描述』填写策略组的描述信息。

『策略选项』用来设置客户端选项、账号控制、安全桌面、远程应用、远程存储和企业移动管理。

**设置完策略组之后，需要在『用户管理』里将策略组关联给用户或用户组，如果不进行关联的话，即使设置了也是没有作用的。**

## 3.5.1. 客户端选项

『客户端选项』用来设置客户端的相关信息。如下图：


『隐私保护』用来设置用户注销时是否需要自动清除相关的内容，包括[Internet 缓存文件]、[浏览器历史记录]、[保存的表单信息]、[Cookies]，勾选即启用自动清除功能。

『带宽会话设置』用来设置客户端的带宽和会话限制数。

勾选[启用 TCP 应用会话限制]，可以启用对客户端的 TCP 应用进行会话限制，可手动设置限制的会话数，范围是 1-500；不勾选，则不会对客户端的 TCP 应用会话限制。

勾选[启用带宽限制]，可对该客户端访问 SSL VPN 的应用时进行流量控制，用来避免部分客户端使用大下载数据把总部带宽占满，导致后续登录的客户端分配不到足够的带宽，访问速度慢带来的问题。可分别对发送和接收做带宽限制，单位是 KBps，如果填 0 则表示不限制，最小的限制值是 32KBps；不勾选，则不对客户端做带宽限制。

勾选[优先启用流缓存]，可实现客户端接入后利用流缓存功能加快文件下载速度，起到加速效果。不勾选，客户端无法实现加速效果。

**[优先启用流缓存]需要先启用流缓存功能。否则为灰色显示，不可勾选，启用流缓存请查看 3.5.2『网络传输优化』 章节。**

勾选[允许使用 PPTP/L2TP 方式接入]则开启手机用户接入功能。

勾选[启用 SSL VPN 专线]，则用户接入 SSL VPN 后无法访问公网，只允许访问 VPN 服务。不勾选，则既可以访问 VPN 服务，同时也可以访问公网资源。基于 Windows 和 Android 系统的客户端支持 SSL VPN 专线功能。

[每个用户可拥有的硬件特征码个数， 最多限制为]即设置每个用户最多可拥有的硬件特征码的个数，可设置的个数范围是：1-100 个。

完成配置后，点击 保存，最后在策略组管理界面点击 配置生效，保存配置并生效。

取消配置，点击 取消，即取消本次配置。

## 3.5.2. 账号控制

『账号控制』用来设置账号控制选项、超时注销设置、私有用户权限等信息。界面如下图所示：

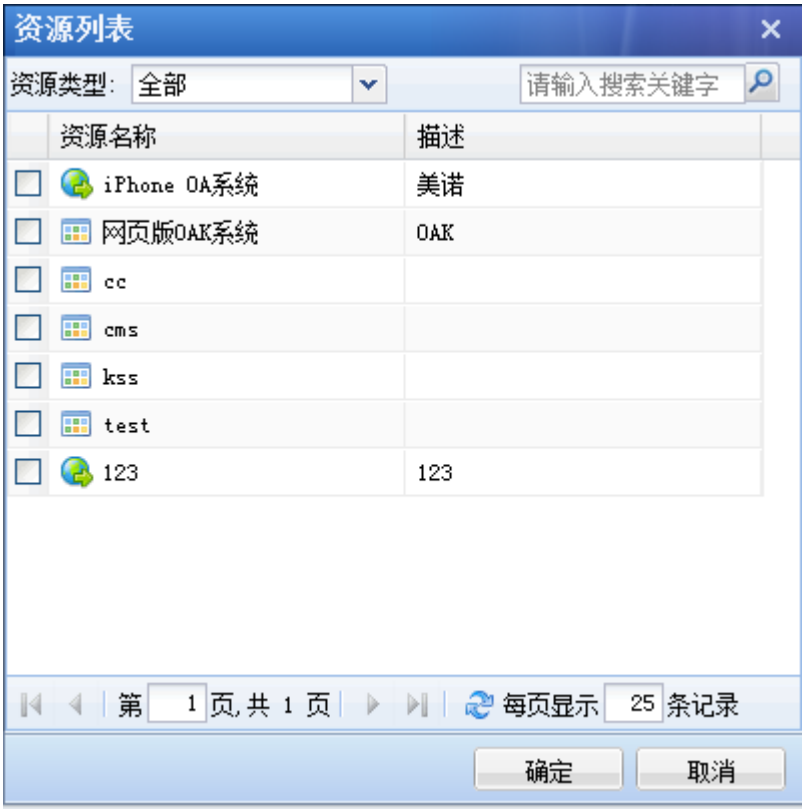

『账号控制选项』用来设置记录用户访问日志、启用系统托盘、用户登录后跳转到指定资源、限制用户可访问时段、用户闲置失效时间、用户超时时间。

[记录用户访问日志]若勾选，可以在外置数据中心记录下该用户访问 SSL VPN 的所有日志。

[启用系统托盘]指对使用该策略的用户启用系统托盘功能（系统托盘的具体设置可参考 3.5.1『系统选项』章节）。

**注意：如果在『系统选项』下启用了系统托盘，是对所有用户全局启用系统托盘，该处启用后在『账号控制』里是默认也启用的，并且无法取消。**

[用户登录后跳转到指定资源]设置用户登录 SSL VPN 后默认跳转到指定的资源，点击[用户登录后跳转到指定资源]后，弹出【资源列表】页面，可选择具体的资源。注：必须先设置好相应的资源（资源的具体设置可参考 4.2『资源管理』章节）。界面如下图所示：

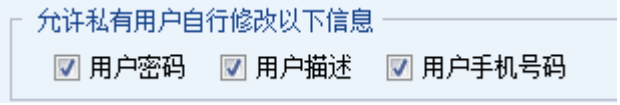



『限制用户可访问时段』用来限制接入 SSL VPN 的时间，点击『限制用户可访问时段』的下拉列表框选择相应的时间。注：必须先设置好相应的时间（时间的具体设置可参考 3.3『时间计划』章节）。

[用户闲置 XX 天后失效]用来设置用户 XX 天没有登录 SSL VPN 后，将账号自动禁用。可以手动设置天数。

[用户如果 X 分钟内未进行任何操作则自动断开连接]用来设置用户超时时间，当用户达到设置的时间未进行过任何操作时，则将用户自动断开连接。设置时间范围 5-43200 分钟。

『允许私有用户自行修改以下信息』用来设置是否允许私有用户修改密码、修改描述和修改手机号码。界面如下图所示：




勾选即允许修改。勾选后，如果用户类型是私有用户，登录 SSLVPN 后，便可以点击资源列表页面右上方的『设置』，左边列表中选择『账号信息』来修改密码、用户描述和手机号码，如下图：

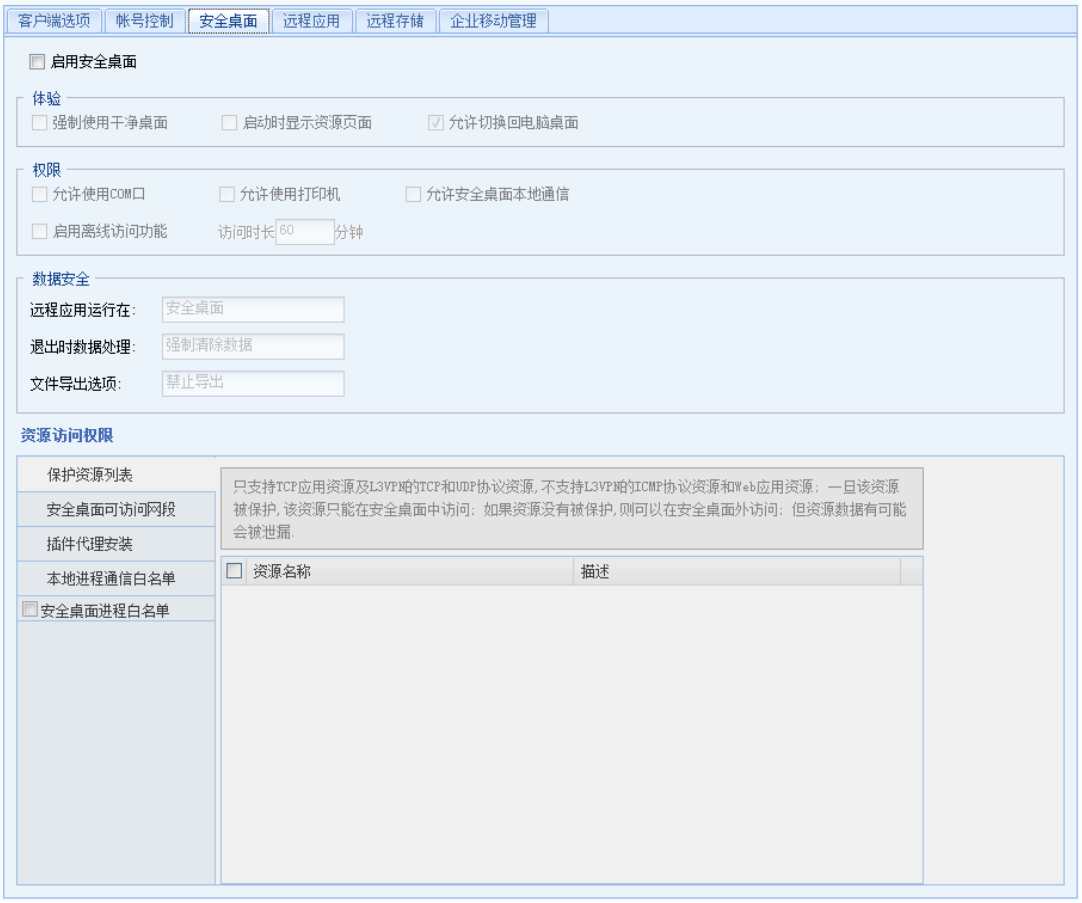

**如果要修改手机号码，必须先对该用户启用短信认证。**

完成配置后，点击 保存，最后在策略组管理界面点击 配置生效，保存配置并生效。

## 3.5.3. 安全桌面

『安全桌面』用于对使用该策略组的用户启用安全桌面。当用户登录 SSL VPN 后，通过安全桌面访问受保护的资源，进一步增强安全性。

界面如下图所示：




勾选[启用安全桌面]即启用安全桌面功能，只有勾选『启用安全桌面』，才能正常使用安全桌面的功能，并对安全桌面功能进行配置。

『体验』用来设置安全桌面的易用性体验。

勾选[强制使用干净桌面]则安全桌面启动后，桌面上只有“我的电脑”等系统图标。不勾选的话，安全桌面启动后，安全桌面的图标和本地桌面的图标一致。

勾选[启动时显示资源页面]则安全桌面启动后，将显示资源页面。

勾选[允许切换回电脑桌面]用于设置允许安全桌面和本地桌面进行切换。

『权限』用来设置用户登录 SSL 后允许在安全桌面中使用的基本功能。包括 [允许使用 COM 端口]、[允许使用打印机]、[允许安全桌面本地通信]、[启用离线访问功能]。

勾选[允许使用 COM 端口]，则用户登录 SSL 后允许在安全桌面中使用计算机的 COM 端

口传输数据；不勾选，则不允许在安全桌面中使用计算机的 COM 端口。

勾选[允许使用打印机]，则用户登录 SSL 后允许在安全桌面中使用计算机连接的打印机；不勾选，则不允许在安全桌面中使用打印机。

勾选[允许安全桌面本地通信]，则用户登录 SSL 后允许在安全桌面和默认桌面之间进行 127.0.0.1 的数据通信；不勾选，则用户登录 SSL 后安全桌面和默认桌面之间无法进行通信。

勾选[启用离线访问功能]，则用户在无法连接到 SSL 的情况下（也就是离线情况下），允许插入有驱和无驱飞天诚信 epass1000nd 类型的 USB KEY 来启动安全桌面，访问保留在安全桌面内的文件。访问安全桌面的时间最长为 60 分钟，当达到允许的时间后，将无法启动安全桌面。不过，允许在接入 SSL 后，插入 DKEY 进行时间充值。

『数据安全』用于设置安全桌面内保留的数据退出时是否保留以及是否允许导出。

[远程应用运行在]用来设置远程应用资源在[默认桌面]下访问还是[安全桌面]下访问。

[退出时数据处理]用来设置退出安全桌面后，安全桌面的数据如何处理。

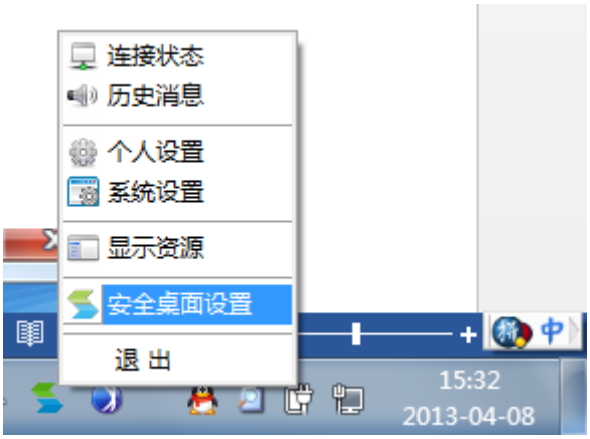
强制清除数据：退出安全桌面后，将清除安全桌面内的所有操作。

强制保留数据：退出安全桌面后，在安全桌面内操作的所有数据保留在安全桌面内。

用户可选择（默认清除）：允许用户自定义退出安全桌面后，安全桌面内的数据操作是否保留，默认是清除的。

用户可选择（默认保留）：允许用户自定义退出安全桌面后，安全桌面内的数据操作是否保留，默认是保留的。

用户在使用安全桌面时，右键点击系统托盘，选择“安全桌面设置”，弹出如下选择框：





用户可以自定义退出安全桌面后是否删除文件。下次重启安全桌面时生效。

[文件导出选项]用来设置保留在安全桌面内的文件，在退出安全桌面后是否允许将文件导出到本地桌面。

禁止导出：不允许将安全桌面内的文件导出到本地桌面。

允许导出（记录文件名）：在启用 SSL 的外置数据中心前提下，才能使用该选项。SSL 外置数据中心将审计用户的导出行为，记录导出文件的文件名、

允许导出（记录文件内容）：在启用 SSL 的外置数据中心前提下，才能使用该选项。SSL 外置数据中心将审计用户的导出行为，记录导出文件的文件名以及文件内容。

允许导出（不审计）：不会记录导出文件的文件名或及文件内容。


外置数据中心安全桌面日志查询结果显示：


『资源访问权限』用来配置用户登录 SSL 后在安全桌面中可以访问的 TCP 应用和 L3VPN 应用。

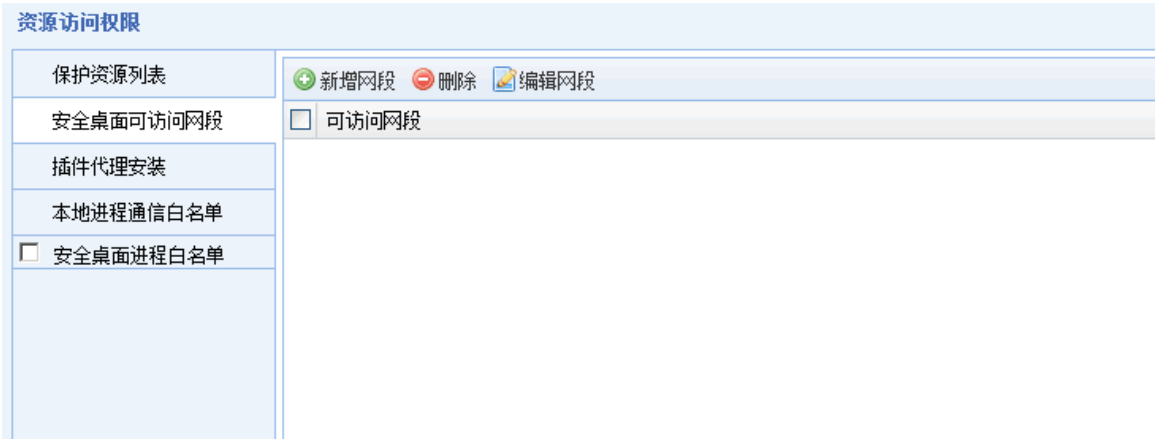
『保护资源列表』用来选择用户登录 SSL 后在安全桌面中允许访问的 TCP 应用和 L3VPN 应用。若勾选，保护资源只允许在安全桌面中访问，不允许在默认桌面中访问；不勾选，则用户登录 SSL 后可以在默认桌面和安全桌面访问。

**如果『保护资源列表』是空的，请先建立需要保护的 TCP 应用资源和 L3VPN 应用资源。**

『安全桌面可访问网段』用来选择用户登录 SSL 后在安全桌面中允许访问的网段。若勾选，则用户登录 SSL 后允许在安全桌面中访问该网段；不勾选，则用户登录 SSL 后不能在安全桌面中访问该网段。

**注意：要让网段限制生效一定要安装 TCP 应用控件，如果使用该组策略的用户只有 WEB 应用资源，可以随意关联一个 TCP 应用来保证能安装上 TCP 应用控件。**

界面如下图所示：




点击 新增网段，添加安全桌面可访问的起始 IP 和结束 IP。

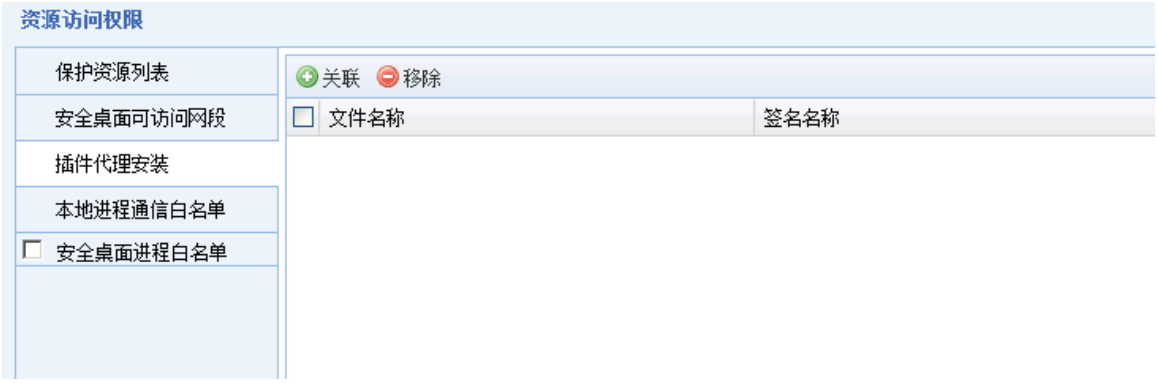
界面如下图所示：

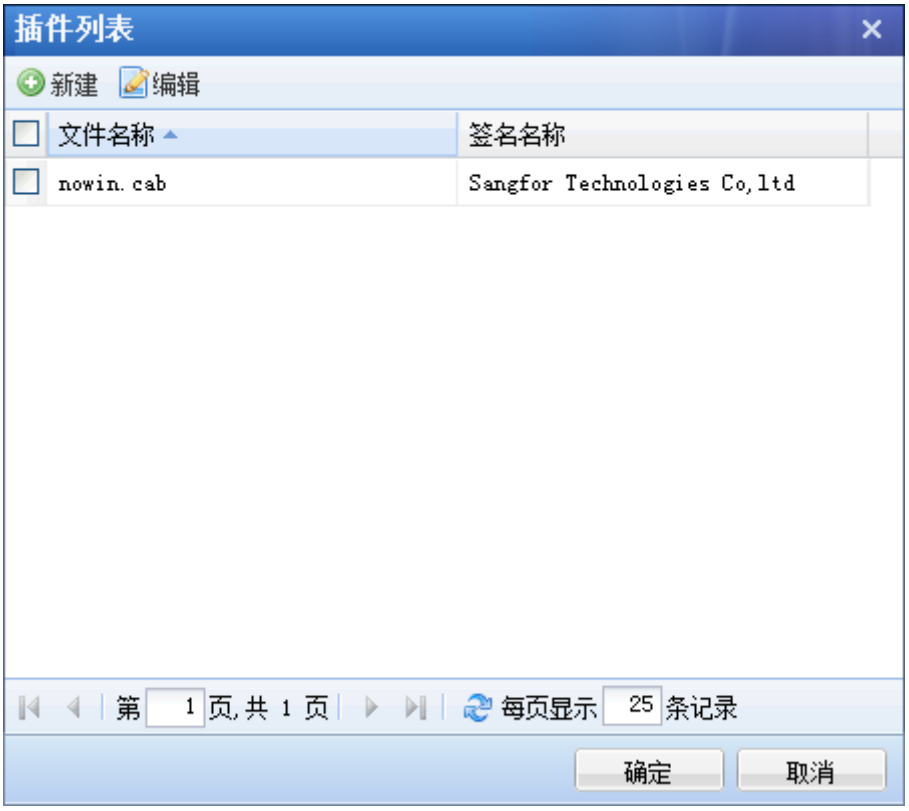

点击 确定，用来保存配置生效。

『插件代理安全』用来选择用户登录 SSL 后在安全桌面中允许安装的插件，因为某些应用程序需要安装插件才能使用，为了让该应用程序在安全桌面内正常允许，需要放通在安全桌面内安装这些插件。点击 关联，选择在策略组里全局设置的插件名称。

**如果『插件列表』是空的，请先在『系统菜单』→『SSL 设置』→『策略组管理』**

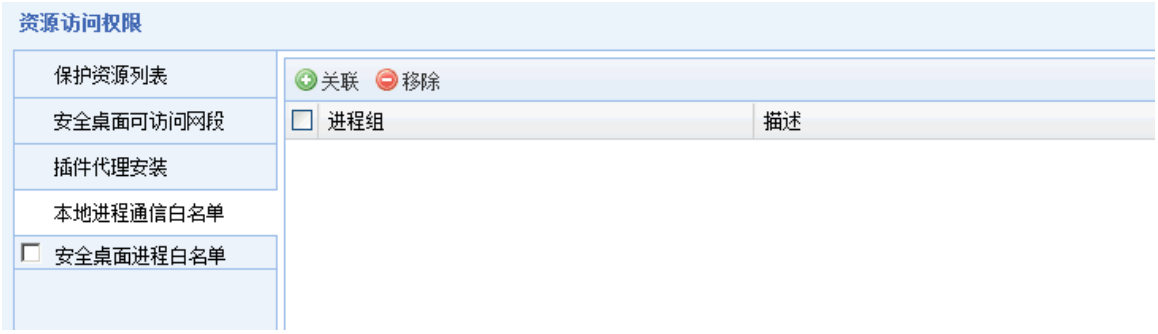
**里点击 插件和进程组配置 配置插件名称。**

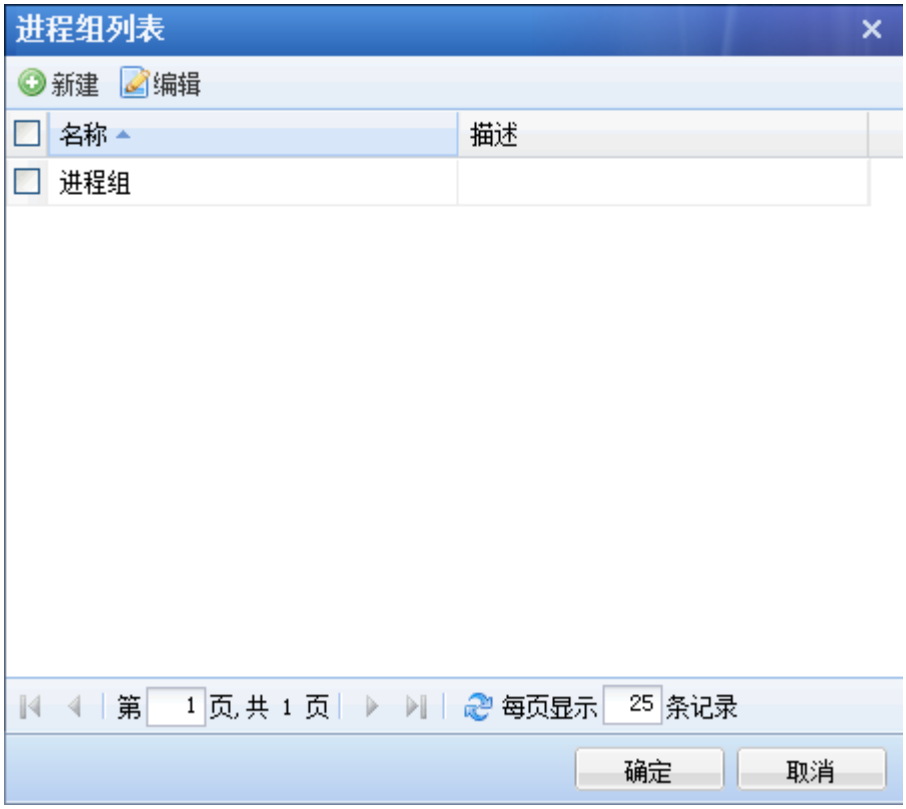



『本地进程通信白名单』用来选择用户登录 SSL 后，允许安全桌面进程与电脑桌面进程之间的 TCP 和 UDP 通讯。点击 关联，选择在策略组里全局设置的进程组。

**如果『进程组列表』是空的，请先在『系统菜单』→『SSL 设置』→『策略组管理』里点击 插件和进程组配置 配置进程组，设置需要放行的进程。**



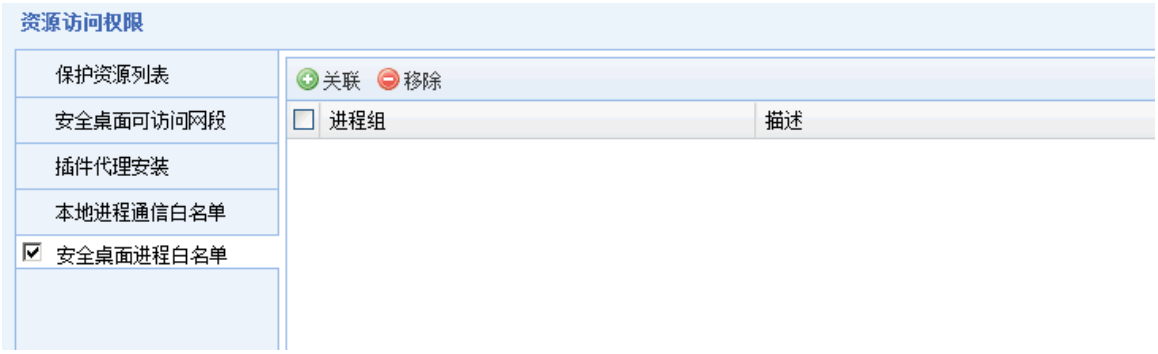



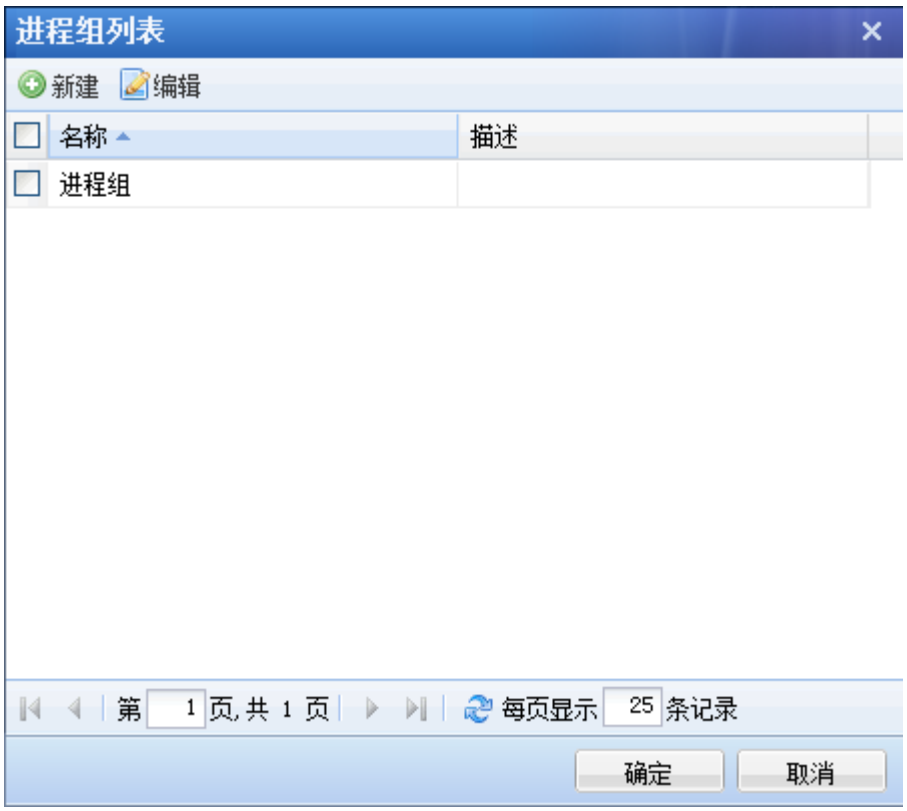

**勾选[安全桌面本地通讯]是全局放开了所有进程安全桌面进程与本地桌面进程之间的 TCP 和 UDP 通讯。而[本地进程白名单]是放开了指定进程在安全桌面与本地桌面之间的 TCP 和 UDP 通讯。**

『安全桌面进程白名单』用来选择用户登录 SSL 后在安全桌面中允许允许的进程，点击关联，选择在策略组里全局设置的进程组。

**如果『进程组列表』是空的，请先在『系统菜单』→『SSL 设置』→『策略组管**

理】里点击 插件和进程组配置 配置进程组，设置需要放行的进程。



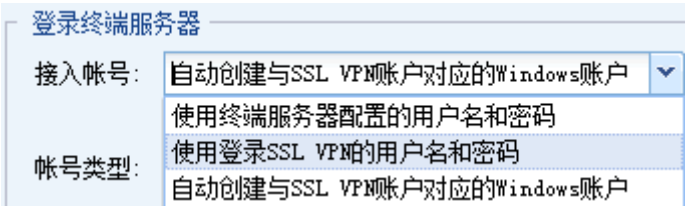




注意：安全桌面只支持 32 位的 Win XP/Win 2003/Win 7/Win 8 系统，以及 64 位的 Win 7/Win 8 系统。

## 3.5.4. 远程应用

『远程应用』用来设置登陆终端服务器、在远程会话中允许使用的设备和资源和远程应用访问权限等信息。如下图：

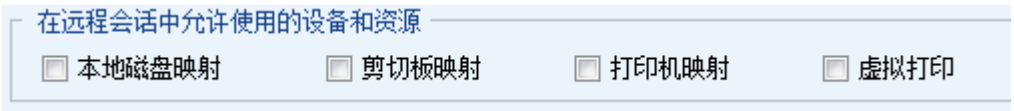

『接入帐号』选择移动用户使用什么样的账号权限登录终端服务器号。如下图：




『账号类型』根据上面选择的账号策略在终端服务器上自动创建的 Windows 账号的类型

『同步选项』，勾选[删除本地用户时，同时删除终端服务器上的账号和存储空间]即当删除了关联该策略组的本地用户时，将该策略组在终端服务器上建立的账号和存储空间一并删。

『在远程会话中允许使用的设备和资源』中，可以选择在远程会话中允许使用的设备和资源。若不勾选，则不允许使用，包括[本地磁盘映射]，[剪切板映射]，[打印机映射]和[虚拟打印]。如下图：



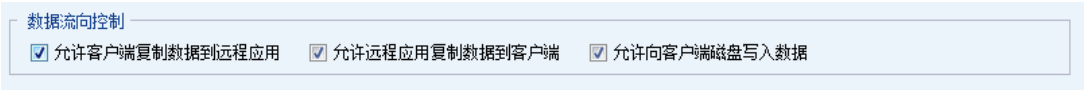
[本地磁盘映射]勾选后，VPN 用户可以在访问远程应用资源时打开或将文档保存到本地磁盘。

[剪切板映射]勾选后，VPN 用户可以使用客户端剪贴板往服务器程序中拷贝内容。

[打印机映射] 勾选后，VPN 用户在服务器上安装打印机驱动以后，可以使用客户端打印机打印远程应用中的文档。

[虚拟打印] 勾选后，VPN 用户可以通过在服务端选择 Sangfor 虚拟打印机，在客户端本地打印机打印文件，且终端服务器无需安装本地打印机驱动。

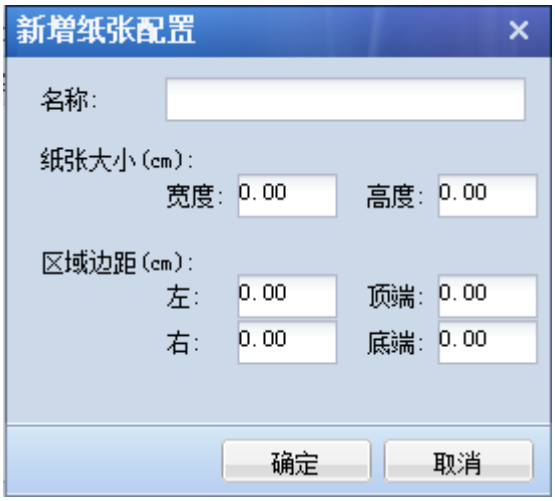
在勾选[剪切板映射]后，[数据流向控制]选项可以配置。可以勾选[允许客户端复制数据到远程应用]、[允许远程应用复制数据到客户端]和[允许向客户端磁盘写入数据]三个选项，实现剪切板数据的控制。




[客户端使用的虚拟打印软件]可以选择 Sangfor PDF Reader、Foxit PDF Reader 和 Adobe PDF Reader 三种，默认选择 Sangfor PDF Reader 打印，打印体验效果较好，支持范围较广。特殊场景下 Sangfor PDF Reader 打印失败时，则使用 Foxit 和 Adobe 打印。若需要使用 Adobe 虚拟打印时，建议安装使用 Adobe 9.4 版本。

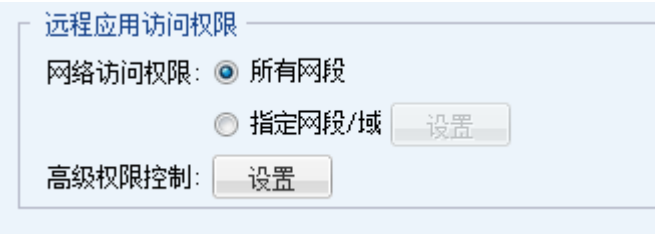

点击 打印纸张配置，如下图所示：


点击新增，新增纸张配置如下图所示：



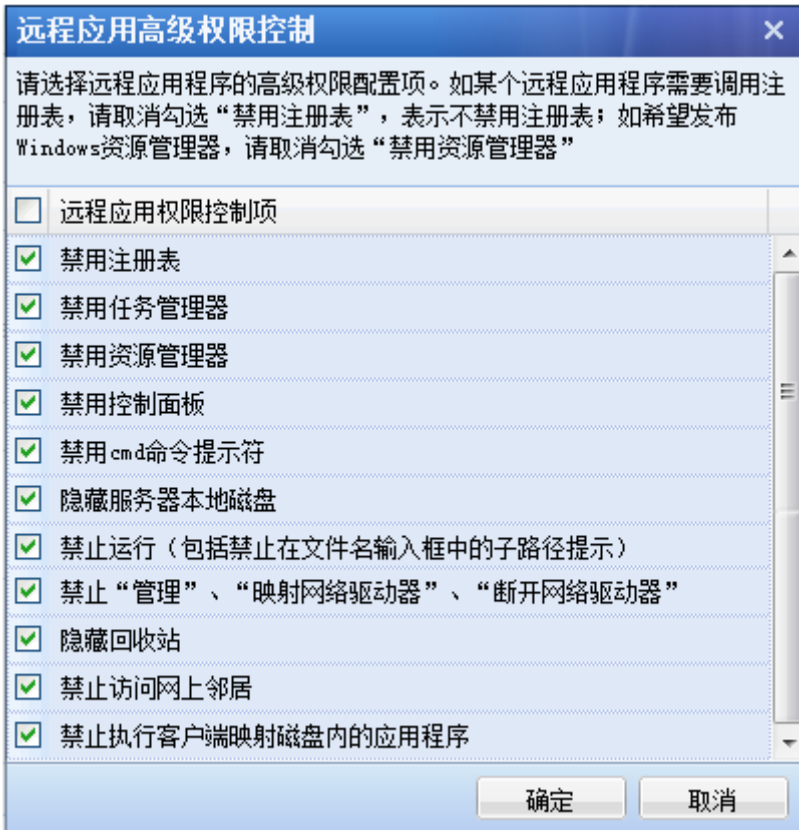

设置纸张大小和区域边距，点击 确认 保存配置。

『远程应用访问权限』为不同用户配置不同的放行网段或者放行域名，对用户关联的所有远程应用的网络访问进行限制。允许访问的网段可选择所有网段或指定某一个网段/域，页面如下：




选择[指定网段/域]，点击设置，可手动配置一段 IP 或指定一个域名，如下图：


[高级权限控制]：选择远程应用程序的高级权限配置项。点击 设置，如下图所示：




## 3.5.5. 远程存储

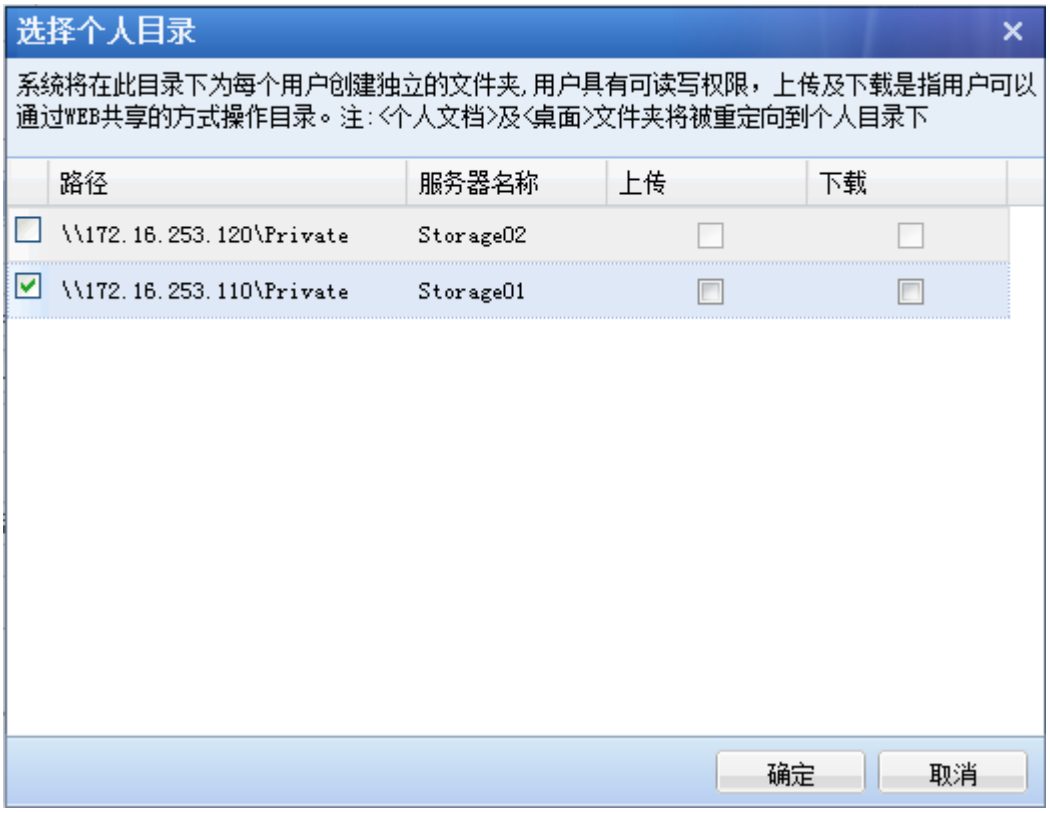
『远程应用』用来设置用户在网络存储服务器上拥有的存储权限，以及 EasyFile 云盘存

储使用到的服务器群组。如下图：

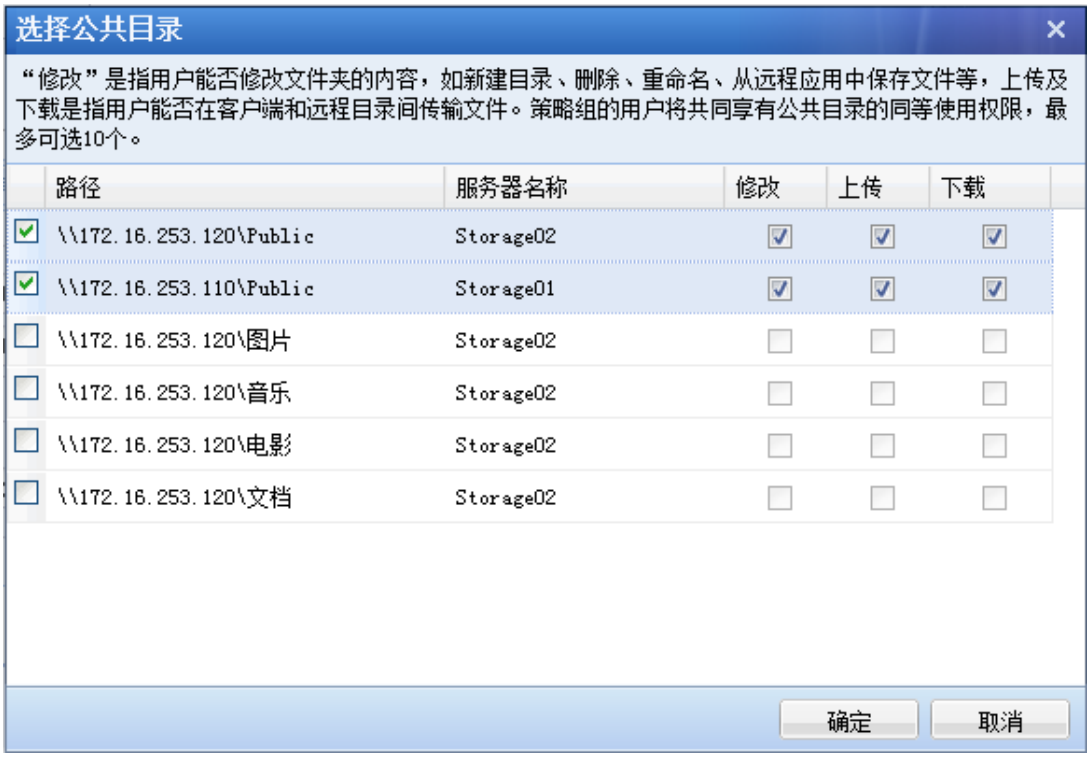

『远程存储目录』用来选择需要在远程服务器上存储文件的目录，包括[个人目录]和[公共目录]。页面如下：


点击后面的  ，可以选择相应的目录，选择之前，需要先在终端服务器管理中添加相应的远程应用存储服务器，详细配置请参考 4.6 章节。

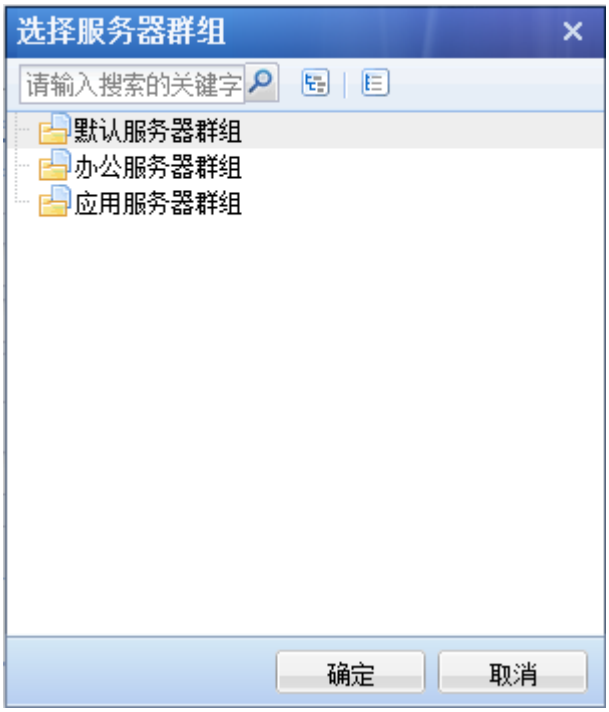
选择个人目录页面如下：




选择公共目录页面如下：




『EasyFile 云盘选项』用于设置移动终端（手机、平板等）打开云盘上的文件时，用哪个服务器群组上的远程应用来打开文件。




以上所有配置完成后，点击 保存，最后在策略组管理界面点击 配置生效，即完成了一条策略组的添加。

**Easylink 资源不支持资源组负载均衡。**

## 3.5.6. 企业移动管理

『企业移动管理』用来管理和设置用户接入 SSL 的移动设备。如下图：


『允许移动设备注册』用于设置是否允许移动设备注册。

『移动设备策略』用于设置安卓和 IOS 设备的策略。

# 第4章 IPSec VPN 设置

## 4.1. 运行状态

此页面可以查看当前的 VPN 连接状态和网络流量信息。页面如下：


点击 分支 NAT 状态 可以查看当前分支 NAT 状态，包括用户名、原子网网段、代理子网网段、网络类型和子网掩码。页面如下：


点击 用户模糊搜索 输入框中输入完整或部分用户名，可以快速找到当前用户的连接情况。


点击 显示选项，可以对显示的列进行筛选。页面如下：


点击 停止服务 可暂时停止 VPN 服务。

## 4.2. 基本设置

『基本设置』用于设置服务端的『Webagent 信息』、『MTU 值』、『最小压缩值』、『VPN 监听端口』等参数，供 VPN 接入用户使用，页面如下：：


Webagent 指动态 IP 寻址文件在 WEB 服务器中的地址，包括『主 Webagent』和『备份 Webagent』。

若服务端为动态 IP，则 Webagent 必须填写为域名形式，一般为以.php 结尾的网页地址（可向深信服科技申请免费的 Webagent 地址，也可以从深信服科技索取 Webagent 文件并自行搭建 Webagent 服务器）。填写完 Webagent 地址后可以点击 测试，查看是否能够连通。

若服务端是固定 IP，请按照“IP 地址:端口”的格式填写，如 202.96.134.133:4009，如果有多条外网线路且均为固定 IP，则可以使用“IP1#IP2: 端口”的格式填写，如 202.96.134.133#58.67.23.22:4009。

点击 修改密码 可以设置 Webagent 网页的密码，以防止非法用户往 Webagent 网页更新虚假 IP 地址。

点击 共享密钥 可以设置 VPN 连接时需要使用的共享密钥，防止非法设备接入。

**如果设置了[Webagent 密码]，一旦遗失该密码则无法恢复，只能联系深信服科技客户服务中心重新生成一个不包含 Webagent 密码的文件并替换原有文件。**

**如果设置了[共享密钥]，则所有 VPN 网点都必须设置相同的[共享密钥]才能相互连接并通信。**

**如果外网有超过 2 条且小于 4 条线路且均为固定 IP，Webagent 可填写成“IP1#IP2#IP3#IP4:4009”格式。**

『MTU 值』用于设置 VPN 数据的最大 MTU 值，默认为 1500，一般建议使用保留值。

『最小压缩值』用于设置启用 VPN 压缩功能时，可压缩的数据包最小值，默认为 100。

『VPN 监听端口』用于设置 VPN 服务的监听端口，缺省为 4009，可根据需要设置。

[修改 MSS]用于设置 UDP 传输模式下 VPN 数据的最大分片，建议勾选。

**『MTU 值』、『最小压缩值』、[修改 MSS]一般情况下请保留默认值，如需设置，**

**请在深信服技术支持工程师的指导下修改。**

[直连]、[非直连]用于设置 VPN 设备与 Internet 的连接方式，如果能直接获得 Internet IP 或者能通过端口映射等方式让 Internet 用户可以访问到设备的 VPN 连接端口，则可设置为[直连]，反之设置为[非直连]。

点击 高级，出现如下界面：


『线程数』用来控制 VPN 设备的最大 VPN 连接个数，默认值 20 可支持 1280 个 VPN 接入。如需修改，请在深信服科技技术工程师的指导下进行修改。

『广播包设置』用来设置是否在 VPN 通道内传递广播包，并且只传递指定端口范围的广播包，尽可能避免 VPN 两边的广播风暴产生。如网上邻居、飞鸽传书等应用，均需要广播包的支持。

『组播设置』用来设置是否在 VPN 隧道内传递组播包，某些视频应用可能需要组播包的支持。

点击 确定，完成服务端的基本设置。

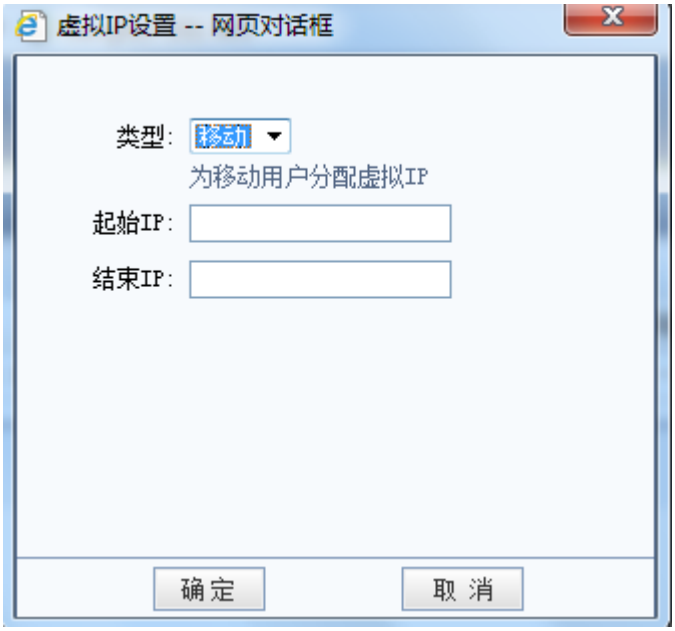
## 4.3. 虚拟 IP 池

『虚拟 IP 池』是指由 SANGFOR VPN 设备指定某一段空闲的 IP 地址作为移动用户接入时的虚拟 IP 地址或者由 SANGFOR VPN 设备指定任意的一段 IP 作为分公司接入后的虚拟 IP 段，解决两个拥有相同网段的分支同时通过 VPN 接入到总部时 IP 冲突的问题。当移动用户接入后，分配一个虚拟 IP 给移动用户，移动用户对总部的任何操作都是以分配的 IP 作为源 IP、移动就像设备上直连的一个网段一样。还可以为接入的移动用户指定 DNS 等网络属性。页面如下：


1、创建移动虚拟 IP 池。

虚拟 IP 池中的 IP 可以是与设备 LAN 口相同网段但空闲 IP 地址，也可以是任意内网没有使用过的其它 IP 地址段。如果使用的是其它网段的 IP 地址，请确保内网服务器有关于这些地址的路由条目交给 SANGFOR VPN 设备，否则会导致移动用户接入服务端后无法正常访问服务端内网服务器。

点击 新增 按钮，出现【虚拟 IP 设置】对话框，选择虚拟 IP 池的类型，设置“IP 池”的起止 IP 即可。页面如下：



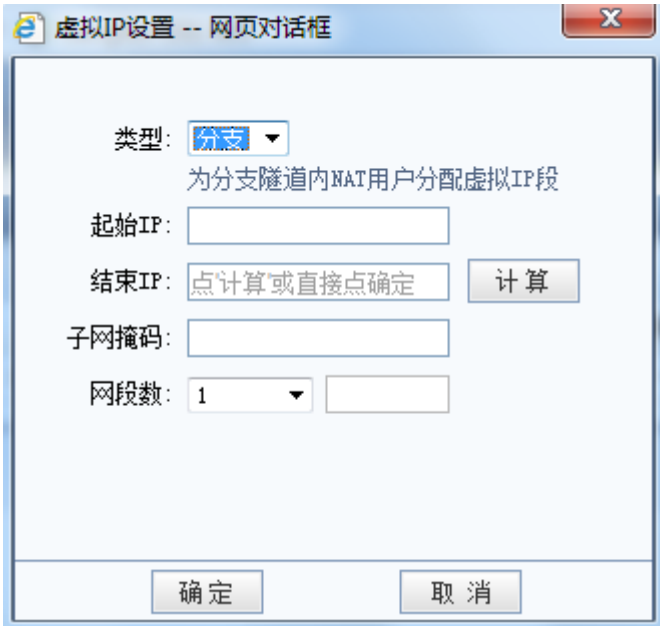

点击 高级 可以设置要分配给移动客户端虚拟网卡上的虚拟 IP 子网掩码、DNS、WINS 服务器等信息，页面如下：


设定移动虚拟 IP 池后，在『用户管理』新建用户，用户类型选『移动』，如果设置虚拟 IP 为 0.0.0.0 表示自动分配虚拟 IP，当移动用户接入后，总部 SANGFOR VPN 网关从虚拟 IP 池中选择一个空闲 IP 分配给移动，也可以为移动用户指定某个固定的虚拟 IP。

**注意：当设置了“虚拟 IP 池”的 高级 选项之后，移动客户端电脑中的虚拟网卡“SANGFOR VPN virtual network adapter”必须设置为自动获取 IP 和 DNS，否则“高级 选项”里面设置的内容不会分配到移动客户端的虚拟网卡上。**

2、创建分支虚拟 IP 池。

分支虚拟 IP 池中的虚拟 IP 段提供给分支接入到总部时将分支的原网段替换成虚拟 ip 池中的一个网段，以解决当两个相同网段的分支同时接入到总部时的内网 IP 冲突问题。设置时设定虚拟 IP 的开始 IP、设定虚拟 IP 的掩码和分支的网段数，点击 计算 可以自动结算出符合要求的结束 IP。页面如下：




『类型』：选择为[分支]。

『起始 IP』：分支虚拟 IP 段的第一个 IP 地址。

『结束 IP』：分支虚拟 IP 段的最后一个 IP 地址。

点击 计算：自动计算虚拟 IP 段的最后一个 IP 地址

『子网掩码』：虚拟 IP 段的子网掩码。与分支端子网掩码保持一致。

『网段数』：需要多少个虚拟 IP 段。

设定分支虚拟 IP 段后，在『用户管理』里新建用户，用户类型选『分支』，然后在『高级/隧道内 NAT 设置』里配置需要转换的分支网段。

## 4.4. 用户管理

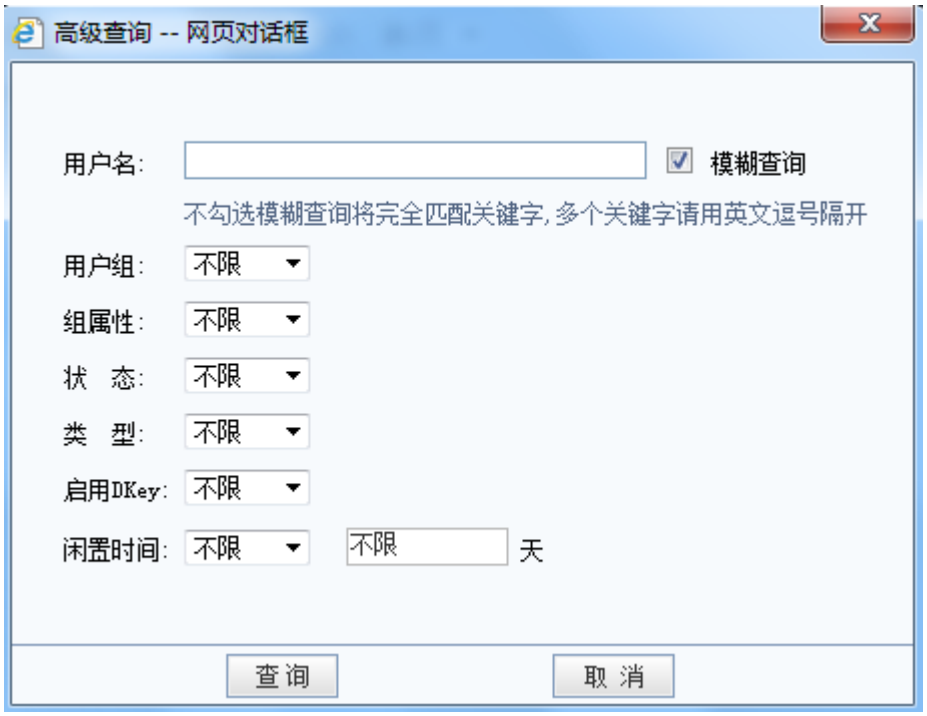
『用户管理』用于管理 VPN 接入账号信息，设置允许接入 VPN 的用户账号、密码、设置账号使用的加密算法、用户的类型（移动或分支）、对用户进行分组并设置组成员的公共属性、是否启用硬件捆绑鉴权或 USB-KEY 认证、设置移动虚拟 IP、账号有效时间、账号的内网权限、组播设置、隧道内流控设置、隧道内 NAT 设置、最后登录时间及最后使用时间等用户策略。页面如下：


点击 检测 USB-Key 将检测当前登录网关控制台的计算机是否插入了 USB-Key，如没有安装 USB-Key 驱动则提示用户是否需要下载，用户可以点击 下载 USB-Key 驱动 直接下载安装。

**注意：生成 USB-Key 前必须安装好 USB-Key 驱动，否则计算机无法识别 USB-Key 硬件，为避免因程序冲突导致 USB-Key 驱动无法正常安装，请在安装过程中关闭第三方杀毒软件、防火墙等程序。**

点击 查询 可对输入的用户名进行查找，以便对查找出来的用户进行编辑操作。查找到的用户会用黄色高亮显示，页面如下：


点击 高级查询 可对查询的用户增加一些过滤条件进行查找，包括用户所属的用户组、组属性（启用/禁用）、用户状态（启用/禁用）、用户类型（移动/分支）、是否启用 DKey（启用/不启用）、用户的闲置时间等等。页面如下：




点击 删除 可对勾选的用户进行删除操作。

点击 新增用户 可依次设置接入账号的『用户名』、『密码』、『描述』、『算法』、『类型』等信息，页面如下：


『认证方式』用于设置用户认证类型，可选本地认证（即硬件设备认证）、LDAP 认证、Radius 认证。

**使用 Radius 认证和 LDAP 认证之前，请先在『LDAP 认证』或『Radius 认证』里设置好对应的认证服务器。**

[使用组属性]用于对用户进行分组，如勾选[使用组属性]，则可激活选择『用户组』设置，选择将该用户加入到某一个用户组并使用这个组的公共属性。

**设置『使用组属性』前请先新增用户组。用户加入用户组后，该用户的『加密算法』、『启用网上邻居』、『权限设置』、『高级』将无法单独设置。**

『启用硬件捆绑鉴权』用于设置基于硬件特性的证书认证，启用后请选择对应此用户的证书文件（*.id）。

[启用 DKEY]用于设置是否对移动用户启用 DKey 认证，启用后请先将 DKey 插入计算机的 USB 接口再点击 生成 DKEY。

[启用虚拟 IP]用于给移动用户分配虚拟 IP。当选择用户类型为“移动”的时候，如果为该用户手动设定好一个虚拟内网 IP 地址（该 IP 必须在虚拟 IP 池范围内），则该用户接入后，会使用这个 IP 作为虚拟的内网 IP 地址。如果虚拟 IP 设置为 0.0.0.0，则系统会自动为该用户从虚拟 IP 池中分配一个内网 IP 地址。

『有效时间』和[启用过期时间]用于设置“接入账号”的有效时间及过期时间。

如 VPN 接入用户需要使用网上邻居服务，则必须勾选[启用网上邻居]。

[启用压缩]用于设置对网关设备与该用户之间传输的数据使用压缩算法进行压缩。

**该设置是 SANGFOR VPN 的独特技术，在低带宽的环境下能有效利用有限带宽，加速数据传输，但并不适用于所有网络环境，实际应用中可根据实际情况进行设置。**

[接入总部后禁止该用户上网]只对移动用户生效。勾选该选项，则可以让移动用户在连通 VPN 后，只能访问服务端 VPN 内网，而不能访问互联网。

[启用多用户登录]用于设置是否允许多个用户同时共用该账号登录 VPN。

[禁止在线修改密码]用于设置移动用户是否能够在连上 VPN 后自行修改移动端登录密码，不勾选表示允许用户自行修改密码。

『权限设置』用于设置用户接入 VPN 后的访问权限，即设置用户只能访问某些服务，默认不做限制。

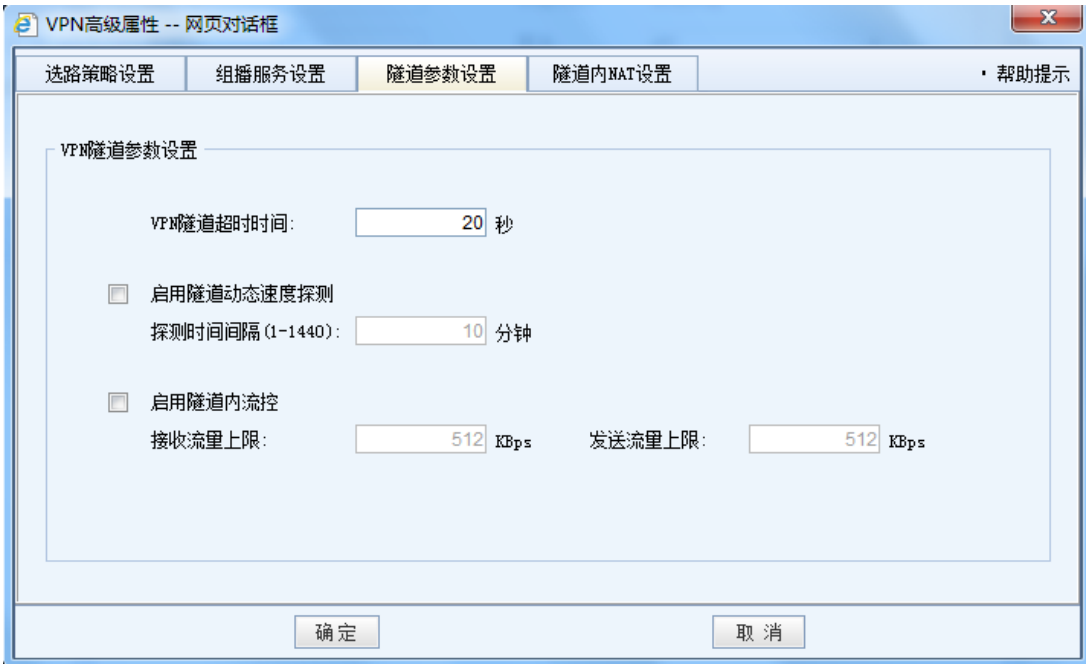
**使用『权限设置』前，请先在『内网服务』处添加所需服务。添加方法请参考 5.9。**

高级用于设置用户接入 VPN 后的一些高级属性，包括启用组播服务、启用隧道内流控、启用隧道内 NAT 等。组播服务主要是满足服务端和分支间有视频等需要组播协议支持的应用需求、隧道内流控主要是避免某个接入的分支 VPN 流量过大的问题、隧道内 NAT 主要是解决两个内网网段相同的分支同时接入到服务端时的地址冲突问题。设置页面如下：


『选路策略设置』请参照章节 5.7 选路策略。

『组播服务设置』请参见章节 5.10 组播服务。

『隧道参数设置』包括了 VPN 隧道超时时间、动态隧道探测、隧道内流控等内容。




『VPN 隧道超时时间』，在网络时延较大、丢包率较高的环境下，SANGFOR VPN 可以针对这些网络设置专门的超时时间，每个隧道的超时时间以服务端配置为准，默认超时时间为 20s，若在较差的网络环境中可适当延长超时时间。

[启用隧道动态速度探测]，在本端或对端拥有多线路情况下有效，此时 SANGFOR VPN 设备将会定时探测多线路里各条线路的延时及丢包情况综合选择最优线路进行数据传输。

[启用隧道内流控]用在多个 VPN 分支或者移动用户接入时，为了避免其中某一个分支或者移动用户将服务端带宽全部占满导致其他分支或者移动用户访问速度变慢，可以针对每个接入的用户分配一个上下行带宽，从而保证所有用户都能得到较理想的访问速度。

**[启用隧道内流控]设置的限制值只是一个范围值，而不是准确值，例如：流控设为 100k，则实际流量会控制在 80-120k 的范围内，在 100k 左右上下小幅波动。**

『隧道内 NAT 设置』：用于对多个冲突的分支网段进行 SNAT 功能，以实现在不修改各个分支的具体网段情况下，各个分支均能接入服务端并和服务端正常通信。


**只有分支类型的用户才能启用隧道内 NAT 功能。**

点击 新增，即可在对话框中输入这条规则所需要匹配原子网网段、代理子网网段、子网掩码，也可以让设备自动从虚拟 IP 池中分配一个 IP 网段，页面如下：


『原子网网段』：分支真实的内网子网网段。

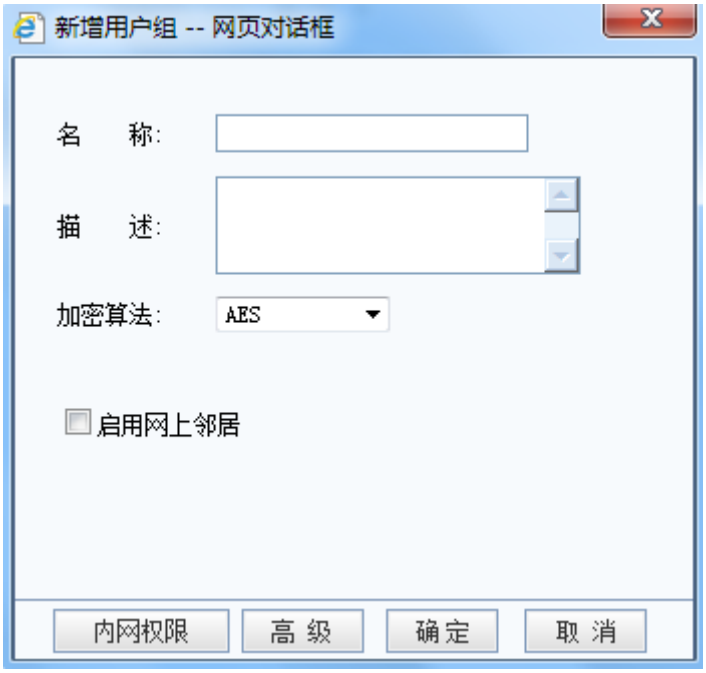
『代理子网网段』：分支转换后的虚拟网段。

『子网掩码』：分支真实的内网子网掩码。

**配置时需要注意子网掩码一定要匹配，隧道内 NAT 只对掩码网段进行 NAT，主机号保持不变。**

**使用 高级 里的隧道内 NAT 功能前，请先在『虚拟 IP 池』添加所需的分支虚拟 IP 网段。**

点击 新增组 可设置用户组名称、描述以及组成员公共属性，页面如下：

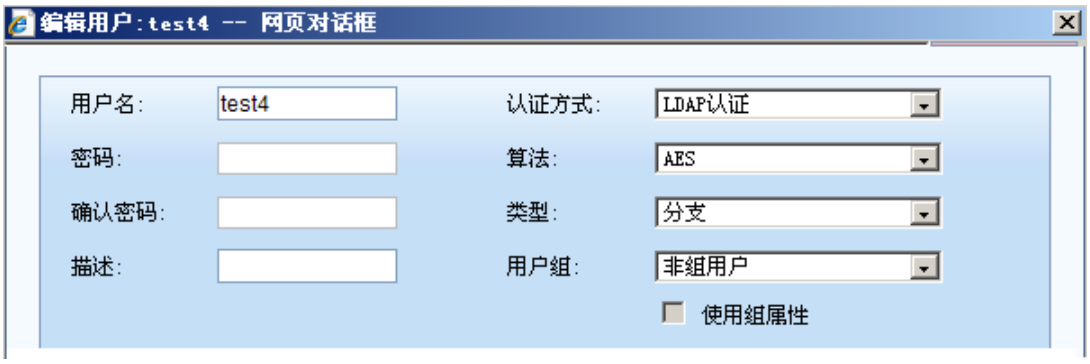



内网权限 和 高级 与 新增用户 里的 内网权限 和 高级 按钮一致，请参见 新增用户 里的对应描述。

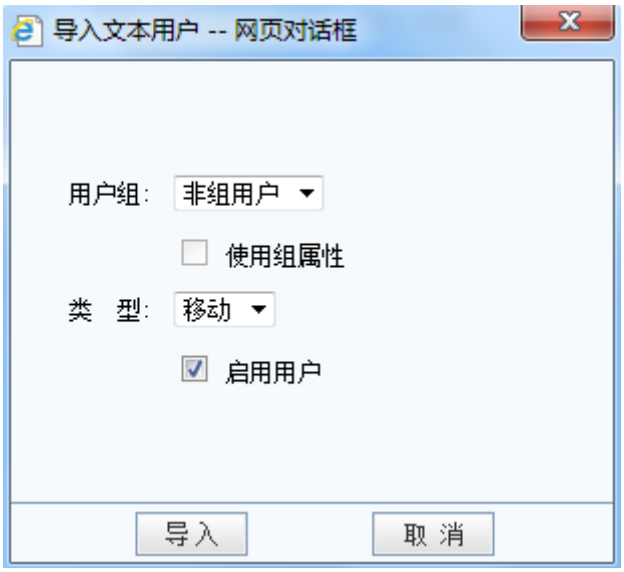
点击导入域用户，可以从 LDAP 服务器中导入用户帐户（导入之前请先在『LDAP 设置』页面中设置好 LDAP 服务器，具体设置请参照 5.13 章节），导入的用户默认使用 LDAP 认证方式且不包含密码，页面如下：

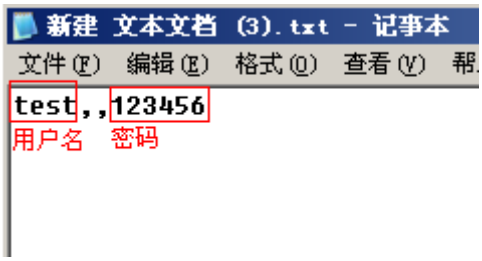

勾选需要导入的用户，选择用户类型是移动用户还是分支用户、是否属于某个用户组、选择加密算法、是否启用压缩及网上邻居等选项后，点击 导入，即可将用户从 LDAP 服务器中导入到 VPN 设备中，页面如下：


| | 名称 | 状态 | 组中用户数 | 类型 | 组属性 | 加密算法 | 虚拟IP | 网上邻居 |
|---|---|---|---|---|---|---|---|---|
| | ⊟非组用户 | | 6 | | | | | |
| ☐ | 域用户:test4 | 启用 | | 分支 | 否 | AES | 禁用 | |
| ☐ | 域用户:test3 | 启用 | | 分支 | 否 | AES | 禁用 | |
| ☐ | 域用户:test2 | 启用 | | 分支 | 否 | AES | 禁用 | |
| ☐ | 域用户:test | 启用 | | 分支 | 否 | AES | 禁用 | |

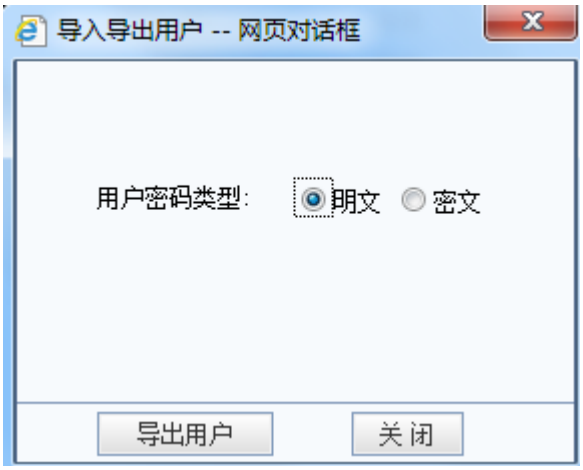



点击 导入文本用户 可以从 TXT 或 CSV 文件中导入用户信息，可以选择选择把用户导入到某个用户组并使用组属性，同时还可以设置导入的用户类型是移动还是分支。TXT 文件的格式为“用户名,,密码”，用户其他信息无法导入。CSV 文件格式同 TXT 文件，把英文逗号换成空列即可。如下图所示：




点击 导出用户 可从设备上将用户导出到本地进行保存，并可选择导出的用户密码是加密还是不加密。页面如下：




## 4.5. 连接管理

如果需要把本端的 SANGFOR 设备接入远端的 SANGFOR 设备，则需要在『连接管理』中进行设置。页面如下：


点 新增 可以添加到一个总部的连接。如下图所示：


『总部名称』和『描述』用于标记连接名称，可以任意填写。

『主/备份 Webagent』用于填写需要连接的总部的对应 Webagent，点 测试 按钮可以测试 Webagent 是否工作正常，结果如下图所示：


**测试请求均是从本机发起的而不是设备发起的。如果 webagent 是用域名形式，**

**测试成功代表该网页存在，否则网页不存在。如果 webagent 采用固定 IP 方式，则测试成功代表填写的 IP:PORT 格式正确。该测试成功并不代表 VPN 就一定能连接成功。**

『传输类型』可选[TCP]或[UDP]，用于决定传输 VPN 数据包的封装类型，默认为[UDP]传输模式。

『共享密钥』、『用户名』和『密码』根据总部提供的接入账号信息来填写。

『跨运营商』功能适用于总部分支采用了不同运营商线路互联经常丢包的情况下。可以选择“低丢包率”、“高丢包率”和“手动设置”。

**注意：跨运营商功能需要通过序列号激活，否则该功能无效。如果是设备和设备之间互连，则双方都需要开启跨运营商功能才能使用，如果是移动用户和设备互连，则只需要设备开启跨运营商功能即可。**

点击 内网权限 ，可以对 VPN 对端进行权限设置，即指定 VPN 对端只能访问本端的哪些服务，页面如下：


设置完以上信息后，勾选[启用]选项即激活该连接。最后点击 确定 按钮保存设置信息。

**1.若需要对启用隧道内 NAT 功能的网点设置内网服务，若在总部设置内网权限，则源 IP 为 NAT 前的网段；若是在分支设置内网权限，源 IP 为 NAT 后的内网权限。**

**2.一旦设置了 VPN 内网权限，不光 VPN 对端访问本端受到限制，本端访问 VPN 对端一样会受到内网权限的控制。因为内网权限只检查数据包的 IP 和端口，不管这个数据包是 VPN 对端主动发起的还是本端主动发起 VPN 对端响应的，只要符合规则条件的数据包都会做相同的处理。**

## 4.6. 隧道间路由

SANGFOR VPN 网关提供了强大的 VPN 隧道间路由功能，通过设置隧道间路由，可轻松实现多个 VPN（软/硬件）之间的互联，真正实现“网状”VPN 网络。


点 新增，可以添加一条隧道间路由，页面如下：


『网络号(源)』：用来设置隧道间路由的源 IP 地址。

『子网掩码(源)』：用来设置隧道间路由的源子网网段。

『网络号(目的)』：用来设置隧道间路由的目的 IP 地址。

『子网掩码(目的)』：用来设置隧道间路由的目的子网网段。

『目的路由用户』：用来选择隧道间路由条目的目的用户（例如，A 跟 B 之间建立了 VPN 连接，使用的是用户“A”，现在 A 想通过 B 访问到 C，则对 A 设备而言，目的路由用户为用户“A”）。

勾选[启用]，则该条隧道间路由生效。

勾选[通过目的路由用户上网]，则所有通过该设备的 Internet 流量都将被发往隧道间路由所指目的路由用户，通过目的路由用户把流量转发至 Internet。

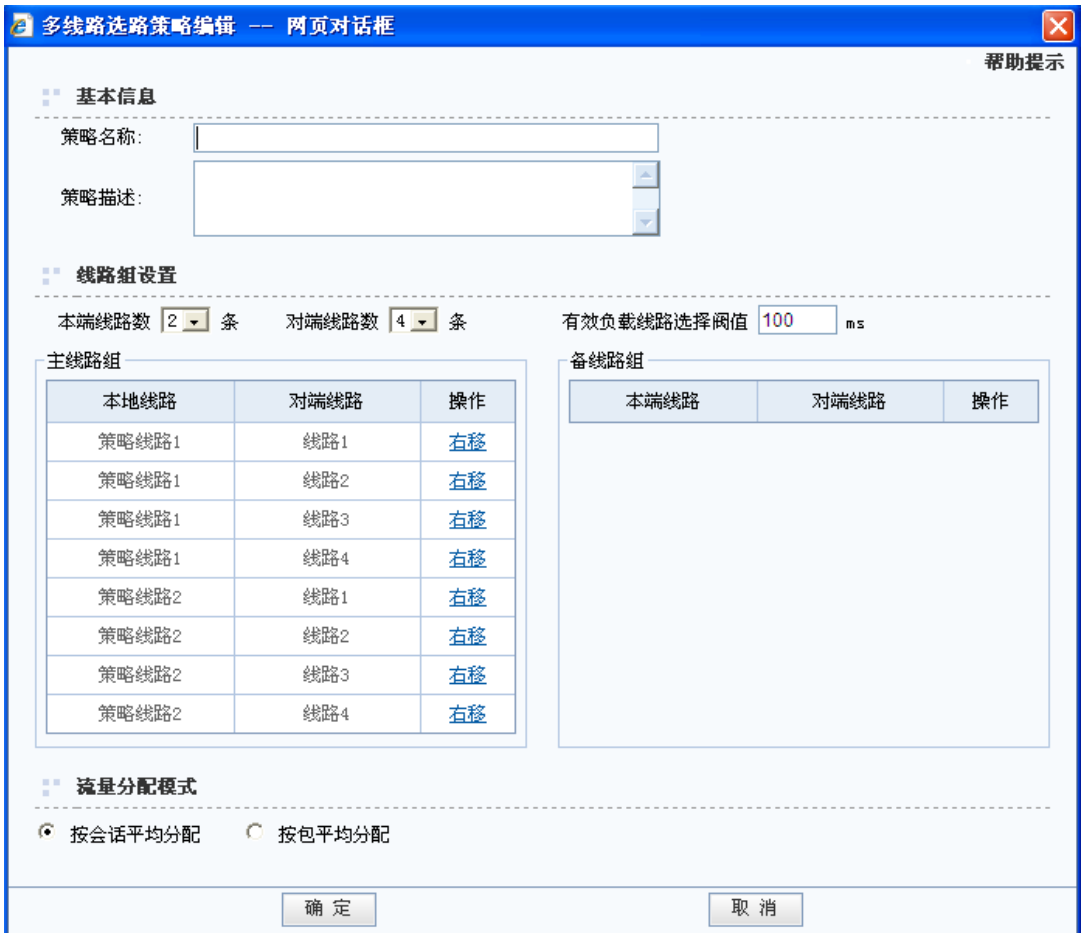
**注意：启用通过目的路由用户上网功能时，VPN 远程接入端设备必须部署为网关模式，服务端设备网关、单臂部署均可。**

勾选[启用路由]，则启用隧道间路由功能

## 4.7. 选路策略

SANGFOR VPN 网关提供了功能强大的 VPN 多线路选路策略，可基于多条线路的连接状况，动态的在多条线路中选择最优线路进行传输，并且可以设置多条线路同时进行传输，既能保证数据始终在连接状态较好的线路上传输，保证数据的传输质量，又能保证数据在多条链路同时传输，提高了线路的利用率。页面如下：


点 新增，弹出【多线路选路策略编辑】页面，页面如下：




『策略名称』：用来定义策略的名称，可以自定义，方便理解记忆就行。

『策略描述』：对策略进行描述，帮助理解。

『本端线路数』：设置本端可用的多线路数目。

『对端线路数』：设置对端可用的多线路数目。

『有效负载线路选择阀值』：用来定义主线路组中判断各条线路连接状况的阀值。如果主线路组中 2 条或多条线路之间的延时差距均小于此阀值，则认为主线路组中这些线路全部都为好线路，数据将同时在这些线路上进行传输；如果主线路组中有线路和其他线路之间的延时差距大于此阀值，则认为该线路为差线路，则数据不从该线路上传输。此阀值只对主线路组内所有线路生效。

『主线路组』：用来定义哪些线路属于主线路组，哪些线路属于备线路组，当主线路组

内的线路连接全部断掉时，VPN 会自动切换到备线路组进行连接，以确保 VPN 连接的可靠性。当主线路中的线路恢复时，VPN 将切回主线路组进行传输，以达到最佳传输效果。

『备线路组』：不属于主线路组的所有其他线路全部属于备线路组。备线路组内的线路是不传 VPN 数据的，只有在主线路组内的全部连接均断开的情况下，才会通过备线路组内的线路进行 VPN 数据的传输。

『流量分配模式』：用来定义主线路组内多条链路同时传输 VPN 数据时的 VPN 流量分配方式，分为[按会话平均分配]和[按包平均分配]。

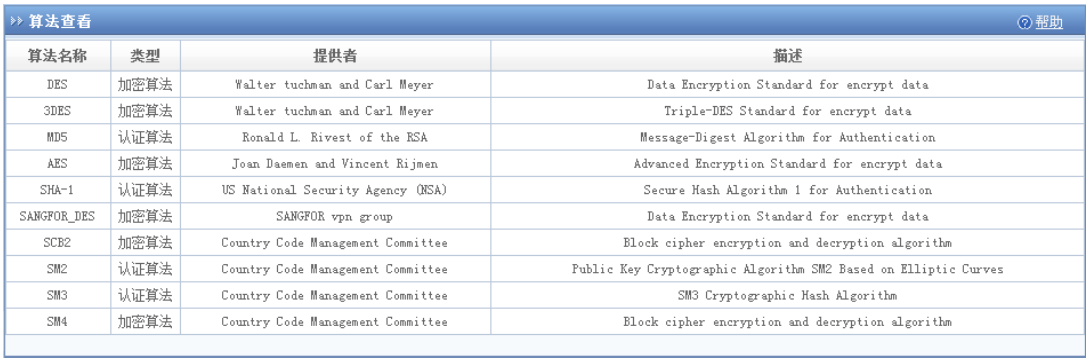
[按会话平均分配]指 VPN 隧道内一个会话始终通过一条链路传输，多个会话才会平均分配到多条链路同时传输。

[按包平均分配]指 VPN 隧道内对每一个 VPN 数据包都平均分配到不同的链路上进行传输。

设置好多线路策略之后，再在『用户管理』里针对不同的用户启用多线路策略即可。

## 4.8. 算法设置

『算法列表设置』提供了对 SANGFOR VPN 支持的数据加密算法进行查看和添加的功能，加密算法会在硬件设备所构建的 VPN 网络中对传输的所有数据进行加密，以保障数据的安全性，页面如下：


算法查看 帮助

| 算法名称 | 类型 | 提供者 | 描述 |
|---|---|---|---|
| DES | 加密算法 | Walter tuchman and Carl Meyer | Data Encryption Standard for encrypt data |
| 3DES | 加密算法 | Walter tuchman and Carl Meyer | Triple-DES Standard for encrypt data |
| MD5 | 认证算法 | Ronald L. Rivest of the RSA | Message-Digest Algorithm for Authentication |
| AES | 加密算法 | Joan Daemen and Vincent Rijmen | Advanced Encryption Standard for encrypt data |
| SHA-1 | 认证算法 | US National Security Agency (NSA) | Secure Hash Algorithm 1 for Authentication |
| SANGFOR_DES | 加密算法 | SANGFOR vpn group | Data Encryption Standard for encrypt data |
| SCB2 | 加密算法 | Country Code Management Committee | Block cipher encryption and decryption algorithm |
| SM2 | 认证算法 | Country Code Management Committee | Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves |
| SM3 | 认证算法 | Country Code Management Committee | SM3 Cryptographic Hash Algorithm |
| SM4 | 加密算法 | Country Code Management Committee | Block cipher encryption and decryption algorithm |

SANGFOR VPN 内置了 DES、3DES、MD5、AES、SHA-1、SANGFOR_DES、SCB2、SM2、SM3、

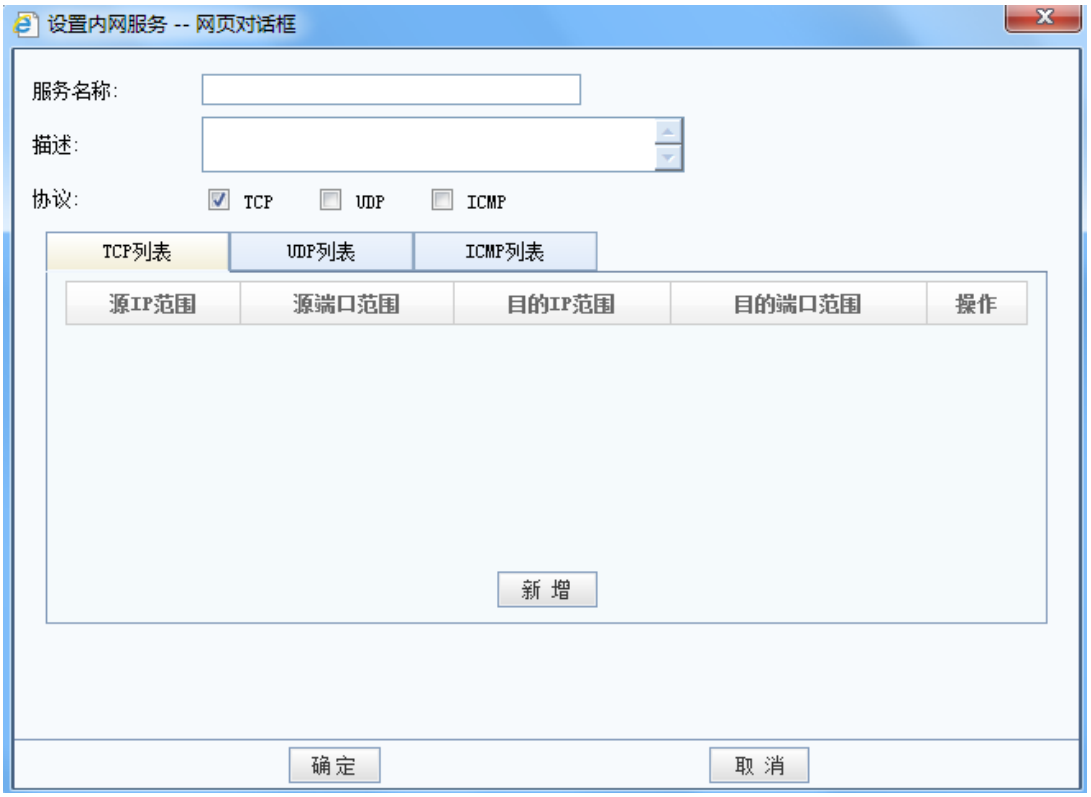
SM4 等多种加密、认证算法，并可以根据客户需要添加其它加密、认证算法，如需添加其它加密、认证算法请联系深信服科技。

**注意：SCB2 为国密办标准加密算法，需要额外采用硬件加密卡进行加密，如果本端和对端设备均没有安装国密办硬件加密卡，则无法使用此加密算法。**

## 4.9. 内网服务

SANGFOR VPN 为接入的 VPN 用户指定相应的访问权限，可以限制分支用户内网的某个 IP、某个移动用户只能访问总部内网的特定计算机的特定服务和与第三方设备互连时设置出入站策略的服务参数。例如：仅允许用户 test 访问总部的 OA 服务器的 80 端口，对 OA 服务器其它服务的访问请求都将被拒绝；仅允许分支用户上海内网的一个 IP 访问总部的 SQL 服务器，分支内网其它 IP 的访问请求将被拒绝等。通过适当的权限设置对服务进行访问授权即可实现 VPN 隧道内的安全管理。页面如下：

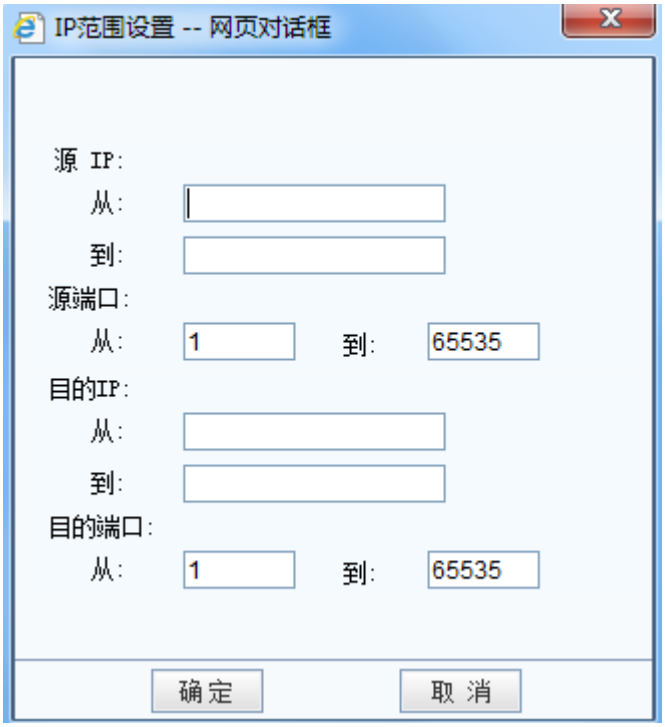

点击新增，弹出【设置内网服务】的网页对话框，如下图：




『服务名称』和『描述』，可自定义。

『协议』：内网服务协议类型，可选择[TCP]、[UDP]、[ICMP]。

选择好协议后，在下面对应的协议列表中，添加 IP 范围和服务端口，点击新增，弹出【IP 范围设置】对话框。如下图：




配置完成后，点击确定，保存配置。

**在这里只是定义内网服，定义好以后，还需要在用户管理中为特定的用户指定权限。缺省状况下系统没有对 VPN 接入用户的访问权限做任何限制。**

## 4.10. 组播服务

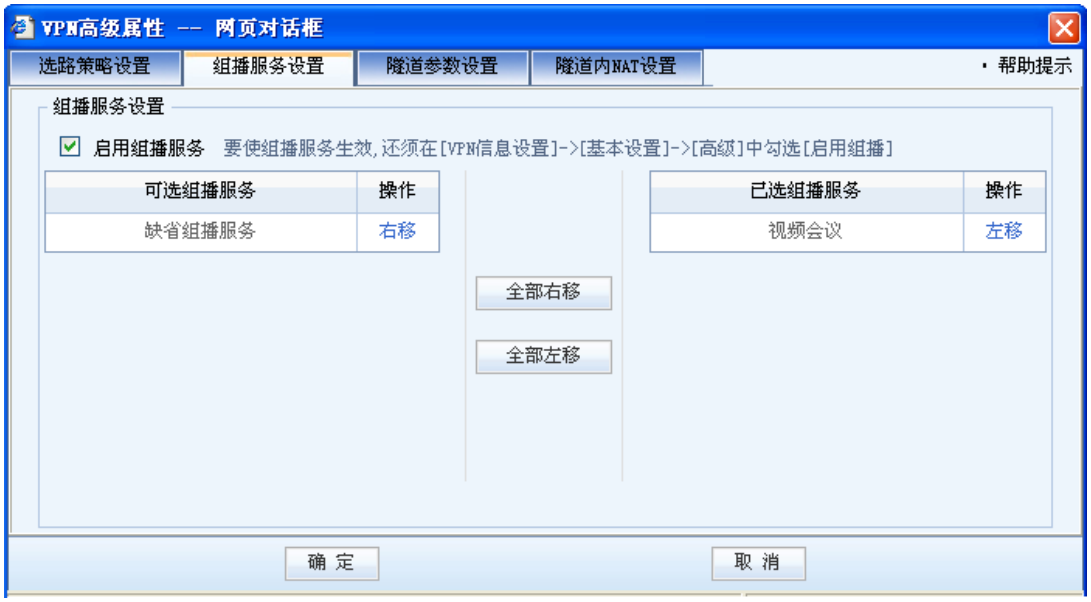
为满足 VOIP 和视频会议等应用，SANGFOR VPN 网关支持组播服务在隧道间传输。在这里可以定义组播的服务，ip 范围是 224.0.0.1-239.255.255.255，端口范围是 1-65535。页面如下：

点击 新增 出现组播服务编辑页面，在这里可以设置组播服务所用的组播地址和端口。页面如下：


点击 新增，添加主播的 IP 和端口号，如下图：

定义好以后，点击 确定 保存，如下图：


然后在『用户管理』新建用户时，在『组播服务』里选择刚定义好的组播服务。页面如下：



# 4.11. RIP 设置

用于设置 SANGFOR VPN 设备通过 RIPv2 协议向其它路由设备通告路由信息，以实现内网路由设备 RIP 路由信息的动态更新。


[启用路由选择信息协议]：是整个动态路由更新功能的开关，激活后，SANGFOR VPN 设备会向所设置的内网路由设备通告已与本端建立 VPN 连接的对端网络的信息（更新其他设备的路由表，添加到 VPN 对端的路由指向 SANGFOR VPN 设备，VPN 连接断开后会通告路由设备删除该路由）。

**设备本身不接收 RIP 路由协议的动态更新，VPN 设备要跟其他启用了 RIP 协议的内网路由器通讯，则需要在 VPN 设备上手动添加静态路由。**

[启用密码验证]：用于设置交换 RIPv2 协议信息时需要验证的密码，可视具体情况进行设置。

『IP 地址』和『端口』：用于设置主动向哪个 IP（路由设备 IP）发布路由更新信息。

[需要触发更新]：勾选后，VPN 设备在路由信息有变化时会触发路由更新信息过程，这时下面设置的 RIP 更新周期参数失效。

[记录日志]：勾选，则 VPN 设备会记录 RIP 路由更新的日志信息。

最后点击 确定 保存配置。

## 4.12. VPN 接口

VPN 接口设置，用于设置 VPN 服务虚拟网卡 IP。页面如下：


“VPN 内网设置”包括 LAN 口和 DMZ 口的 VPN 内网子网掩码设置，“自动同步掩码”是直接使用 LAN 口或 DMZ 口的子网掩码，“自定义掩码”是手动填写 VPN 接口的子网掩码。

“本机 VPN 接口”设置用于设置本端设备的 VPN 接口 IP 地址，可以自动分配或者手动定义 VPN 接口 IP。

**注意：默认情况下请设置为[使用自动分配的 VPN 接口 IP，如果出现 IP 冲突的提示，可改为自定义 IP 并进行设置。**

VPN 接口是 VPN 硬件网关系统的虚拟接口，外观上并不存在对应的真实物理接

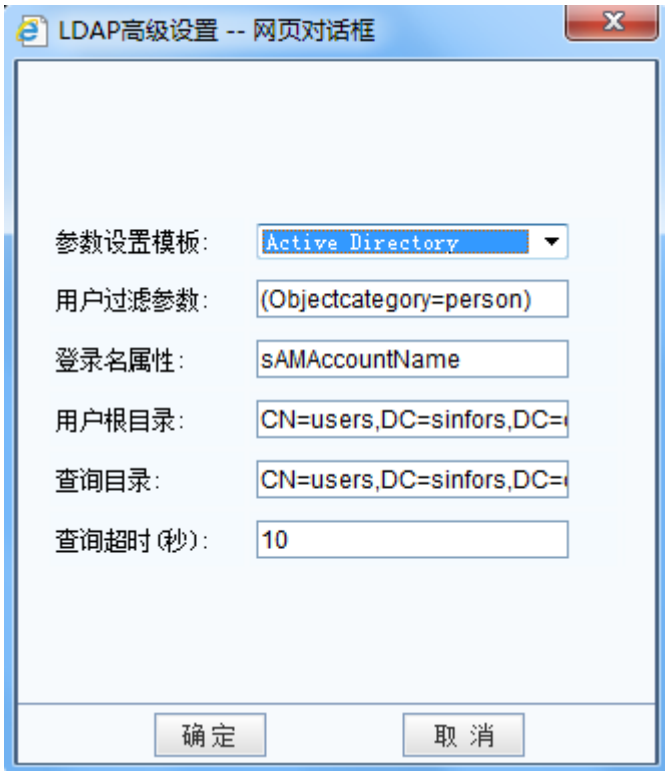
口。

## 4.13. LDAP 设置

SANGFOR VPN 设备的 VPN 服务支持使用第三方 LDAP 认证。如需要启用第三方认证，请在『LDAP 服务器设置』中正确设置第三方 LDAP 服务器信息（包括 LDAP 服务器 IP、LDAP 服务器端口、LDAP 管理员密码），页面如下：

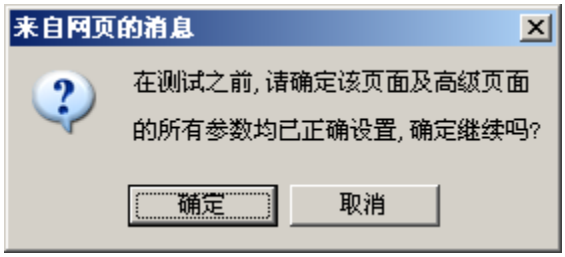

其中，管理员名称需使用域管理员帐号，并且填写完整的格式，例如：“administrator@support.sangfor.com”（不包括引号）

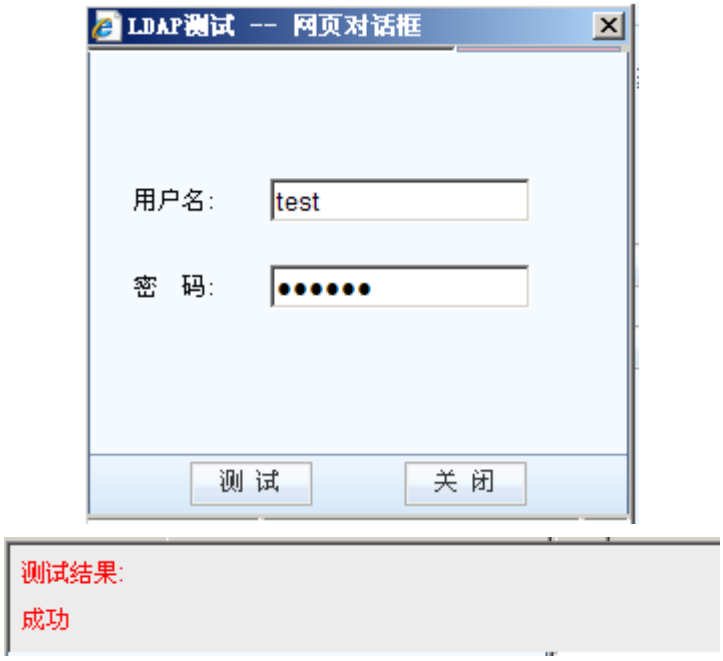
设置好 LDAP 服务器信息后，请点击 高级，显示【LDAP 高级设置】对话框，按照实际需求设置 LDAP 高级信息，页面如下：




『用户过滤参数』和『登录名属性』保留默认值即可，填写好用户根目录及查询目录（用户接入校验时都是使用查询目录来查询并校验的，只有有当查询目录为空的时候才用根目录，导入用户的时候使用用户根目录来导入）。

点击 测试，输入一个域用户名及密码，如果测试通过，则 LDAP 配置正确，页面如下：






点 确定 完成配置。

**LDAP 认证仅支持微软的 AD 和 Novell 的 eDirectory 两种，OpenLDAP 等暂不支持。**

## 4.14. Radius 设置

设置界面如下：

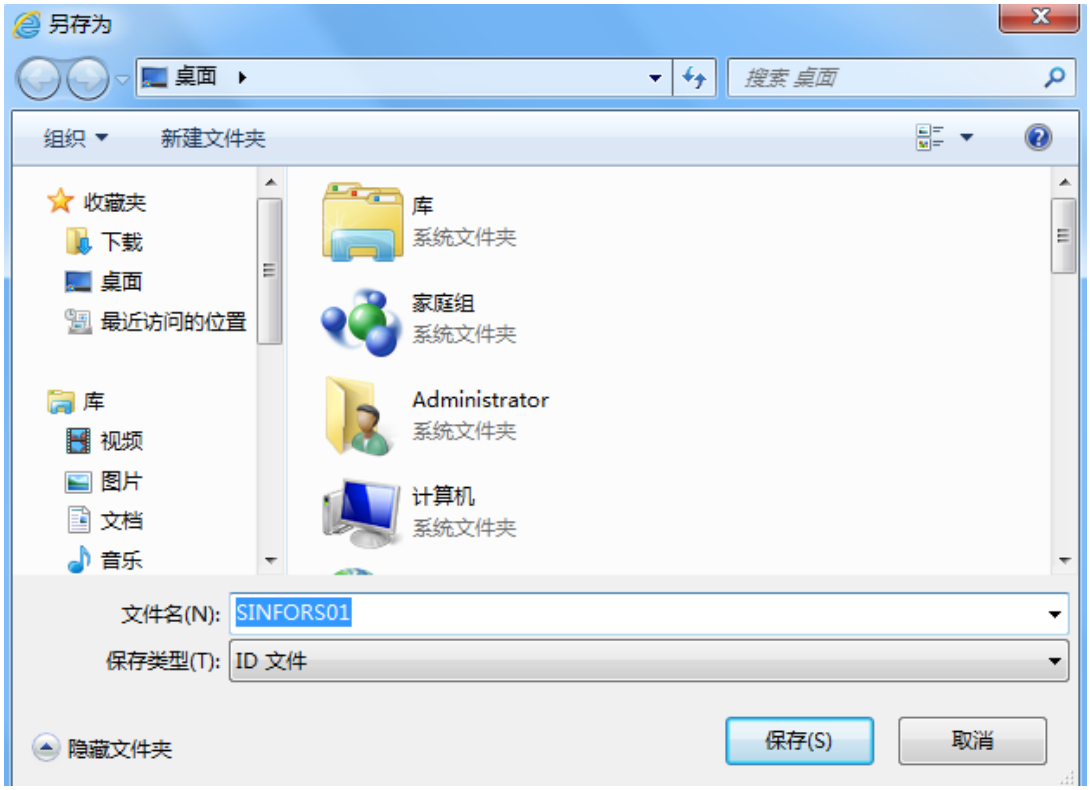
填写『Radius 服务器 IP』、『Radius 服务器端口』、『认证共享密钥』和『Radius 认证协议』。

勾选[启用 Radius 认证]即可。

## 4.15. 生成证书

基于硬件特性的证书认证系统是深信服公司的发明专利之一。SANGFOR SSL VPN 硬件设备和 SANGFOR DLAN VPN 软件一样，都采用了该技术用于不同 VPN 节点之间的身份认证。该证书提取了 SSL VPN 设备或安装 DLAN VPN 软件的计算机的部分硬件特性（如网卡、硬盘等）生成加密的认证证书。由于硬件特性的唯一性，使得该证书也是唯一的、不可伪造的。通过对该硬件特性的验证，就保障了只有指定的硬件设备才能接入授权的网络，避免了安全隐患。页面如下：


点击 生成证书，选择证书保存路径，点击 保存 即可。




证书保存到本地后，还需要将该证书通过某种方式（如电子邮件或 U 盘等）提供给需要接入的站点管理员，由该站点管理员将证书与用户名绑定（即在总部建用户时，启用硬件捆绑鉴权，详见 5.4 章节）。以后该用入接入总部时，会自动验证接入的计算机身份的合法性。

## 4.16. 第三方对接

SANGFOR VPN 硬件网关提供了与第三方 VPN 设备互联的功能，能与第三方的标准 IPSEC VPN 设备建立 VPN 连接。

### 4.16.1. 第一阶段

『第一阶段』用于设置需要与 SANGFOR VPN 网关建立标准 IPSec 连接的对端 VPN 设备的相关信息，也就是标准 IPSec 协议协商的第一阶段。页面如下：


设备列表中的某设备已在出入站策略中使用时，该设备不能被删除或改名。

在右上角输入框中可以搜索设备名称和设备地址。

第三方对接必须固定线路出口，默认为线路 1。单臂多线路部署模式下，出口线路自动使用线路 1。

选择线路出口，点击 新增，显示『设备列表设置』对话框，页面如下：


『设备名称』：可自行定义。

『描述』：可自行定义。

『设备地址类型』：包括对端是固定 IP、对端是动态 IP、对端是固定域名三种。请根据实际情况选择。选择固定 IP，就填写上对端的 IP 地址；选择动态域名，就填写上对端外网绑定的域名。

**注意：标准 IPSEC 不允许连接的双方都是动态 IP，只能允许其中一方为动态 IP。**

『预共享密钥』及『确认密钥』：填入正确的预共享密钥，并确保连接双方采用的都是相同的预共享密钥。

点击 高级，显示『高级选项』对话框，可进行其它高级设置，页面如下：


『ISAKMP 存活时间』：标准 IPSEC 协商的第一阶段存活时间，只支持按秒计时方式。

『重试次数』：当 VPN 故障断开后，重试连接的次数，超过次数还未能连上，则不再主动发起连接，除非有 VPN 流量触发才能再次主动发起连接。

『支持模式』：包括主模式和野蛮模式两种类型。主模式适用于双方均为固定 IP 或者一方固定 IP 一方动态域名方式，并且不支持 NAT 穿透；野蛮模式适用于其中一方为拨号的情况，并且支持 NAT 穿透。

『D-H 群』：设置 Diffie-Hellman 密钥交换的群类型，包括 1、2、5 三种，请与对端设备配置保持一致。

『启用 DPD』：IPSEC 使用 DPD（Dead Peer Detection）功能来检测对端 Peer 是否存活。“DPD 设置”包括检测间隔和超时次数，多次检测超时后，设备会认为对端失效而断开连接。

『ISAKMP 算法列表』包括认证算法和加密算法：

“认证算法”：选择数据认证的 Hash 算法，包括 MD5/SHA-1/SM3 等

“加密算法”：选择数据加密的算法，包括 DES、3DES、AES、SANGFOR_DES 四种。

 **SANGFOR_DES 算法，只有在连接双方都是 SANGFOR 设备时才能使用，与其他厂商设备互联时无法使用。**

 **野蛮模式的身份 ID 有 2 种表达方式，一种为域名字符串（FQDN）格式，可以为任意的网址或者一串字符串；另一种为用户字符串（USER_FQDN），需要是“xxx@xxx.xxx”这种格式。**

## 4.16.2. 第二阶段

『入站策略』用于设置由对端发到本端的数据包规则，策略较多时自动分页显示。可以在右上角搜索策略名称、源 IP、对端设备名称等；其中对于源 IP 是“子网+掩码”的策略，仅搜索的是子网，不搜索掩码。


『入站策略』用于设置由对端发到本端的数据包规则，点击 新增，显示【策略设置】对话框，页面如下：


『策略名称』及『描述』：可自行定义。

『源 IP 类型』：包括单个 IP、子网+掩码两种类型。分别指定对端 VPN 数据的源 IP

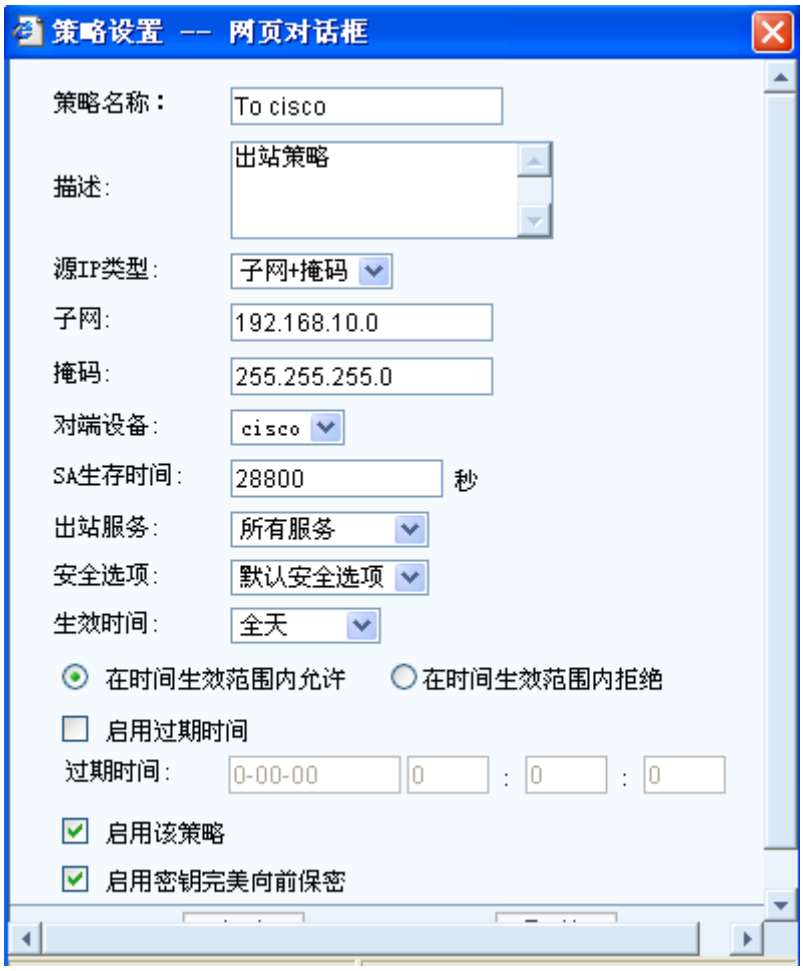
是单个 IP 还是整个网段，并正确填入对端 VPN 数据的源地址。

『对端设备』：该出站策略跟对端哪个设备相关联。

『入站服务』：定义对端哪些类型的服务允许进入 VPN 隧道传输至本端内网。

『生效时间』及『过期时间』：在什么时间范围内，该入站策略有效。

『出站策略』：用于设置从本端发往对端的数据包规则，点击新增，显示【策略设置】对话框，页面如下：




『策略名称』及『描述』：可自行定义。

『源 IP 类型』：包括单个 IP、子网+掩码两种类型。分别指定 VPN 数据的源 IP 是单个 IP 还是整个网段，并正确填入 VPN 数据的源地址。

『对端设备』：该出站策略跟对端哪个设备相关联。

『安全选项』：该出站策略跟哪个安全选项相关联。

『SA 生存时间』：标准 IPSEC 第二阶段协商的存活时间，同样只支持按秒计时。

『出站服务』：定义哪些类型的服务允许进入 VPN 隧道传输至对端内网。

『生效时间』及『过期时间』：在什么时间范围内，该出站策略有效。

**注意：『生效时间』模块，只在连接双方都是 SANGFOR 设备情况下生效，与其他厂商设备互联时无效。**

『启用密钥完美向前保护』：根据对端设备情况而定，如果对端启用了 PFS，则本端也需要勾上此选项，否则不用勾选。

**注意：『出站策略』和『入站策略』中的『出站服务』、『入站服务』和『时间设置』均为 SANGFOR 扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立 VPN 连接的过程中不会协商此类规则。『出站策略』和『入站策略』中策略所对应的源 IP 地址是指『源 IP 类型』和『本/对端服务』中所设置的源 IP 的交集。**

## 4.16.3. 安全选项

『安全选项』用于设置与对端建立标准 IPSec 连接时所使用的安全参数。页面如下：


在建立与第三方设备的 IPSec 连接前，请先确定对端设备采用何种连接策略，包括：使

用的『协议』（AH 或 ESP）、『认证算法』（NULL/MD5/SHA-1/SM3）、『加密算法』（DES、3DES、AES、SANGFOR_DES、SCB2、SM4），点击 新增，添加新的选项，页面如下：


SANGFOR VPN 网关会使用设置好的连接策略与对端协商建立 IPSec 连接。

**『安全选项』中的『加密算法』用于设置标准 IPSec 连接的第二阶段所使用的数据加密算法，如果要与多个采用不同连接策略的设备互联，需要分别将各个设备使用的连接策略添加到『安全选项』中。**

**『出站策略』和『入站策略』中策略所对应的源 IP 地址是指『源 IP 类型』和『本/对端服务』。**

**注意：『出站策略』和『入站策略』中的『出站服务』、『入站服务』和『时间设置』均为 SANGFOR 扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立 VPN 连接的过程中不会协商此类规则。**

**『系统设置』→『SSL VPN 选项』→『系统选项』→『接入选项』页面，开启 L2TP 接入**

**服务后，自动关闭标准 IPSEC VPN 服务，第三方对接模块将隐藏不可见。**

# 第5章 防火墙设置

SANGFOR VPN 硬件网关集成了高性能的企业级状态检测防火墙，能有效保护内部网络免受来自包括 Internet、VPN 连接的其它局域网等多方面的攻击。同时，内置的防 DOS 攻击功能，不仅可以有效防范来自外部网络的 DOS 攻击，对于内网计算机发起的 DOS 攻击，SANGFOR VPN 硬件网关也可以进行防御。

## 5.1. 服务定义

通过网络运行的软件和通信程序使用不同的传输协议和端口，在设定针对这些数据的防火墙规则之前需要先定义其传输协议和端口，页面如下：


例如：需要在 SANGFOR VPN 硬件网关上对 SQL SERVER 服务数据的传输设置规则，首先需要对 SQL SERVER 服务所使用的协议和端口进行定义，点击 新增，出现【防火墙信息编辑】对话框，页面如下：


『服务名称』可自定义（本例中可设置为：SQL）。

『服务定义』选择定义服务的协议类型，本例选择 TCP。

『目标端口』填写提供服务的端口号，本例填写 1433。

点 确定 保存即可完成对 SQL SERVER 服务的定义。

## 5.2. IP 组定义

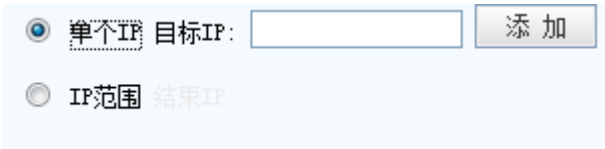
在设定针对特定 IP 的防火墙规则之前需要先定义这些 IP，页面如下：

例如：需要在 SANGFOR VPN 硬件网关上对源 IP 地址为 192.168.1.0/24 数据的传输设置规则，首先需要定义这个 IP 段，点击 新增，出现『防火墙 IP 组编辑』对话框，页面如下：


『IP 组名称』可自定义。

『IP 范围』IP 地址范围，可填单个 IP 或 IP 段，本例填写 192.168.1.1-192.168.1.254。点 确定 保存即可完成对 IP 段的定义。

若选择为单个 IP，则只需要填写一个目标 IP 地址，如下图：




## 5.3. 过滤规则设置

SANGFOR VPN 硬件网关防火墙采用状态检测包过滤技术，可在多个数据传输方向上结

合时间计划实现基于协议类型、源 IP、目的 IP 的数据包过滤。

可设置包括了本机规则和十二个方向的规则设置。如下图：


**所有的 VPN 数据都会经由 VPN 接口传输（例如：本端设备 LAN 接口下的计算机与 VPN 对端计算机的数据通信是经由设备 LAN 接口与 VPN 接口传输），因此防火墙 的过滤规则可以对 VPN 数据进行控制。**

『本机规则』用于设置对本机的防火墙策略。


点击[启用]或[禁用]来开启或禁用本条策略。

点 确定 保存即可完成对本机策略的设置。

『LAN<->DMZ』用于设置 VPN 设备的 LAN 接口与 DMZ 接口之间双向数据传输的防火墙过滤规则。

『DMZ<->WAN』用于设置 VPN 设备的 DMZ 接口与 WAN 接口之间双向数据传输的防火

墙过滤规则。

『WAN<->LAN』用于设置 VPN 设备的 WAN 接口与 LAN 接口之间双向数据传输的防火墙过滤规则。

『VPN<->LAN』用于设置 VPN 设备的 VPN 接口与 LAN 接口之间双向数据传输的防火墙过滤规则。

『VPN<->WAN』用于设置 VPN 设备的 VPN 接口与 WAN 接口之间双向数据传输的防火墙过滤规则（如果 VPN 连接对端在『隧道间路由设置』中设置了以本端作为『目的路由用户』并启用『通过目的路由用户上网』，则在本端可通过设置 VPN<->WAN 的过滤规则实现对分支上网数据的控制）。

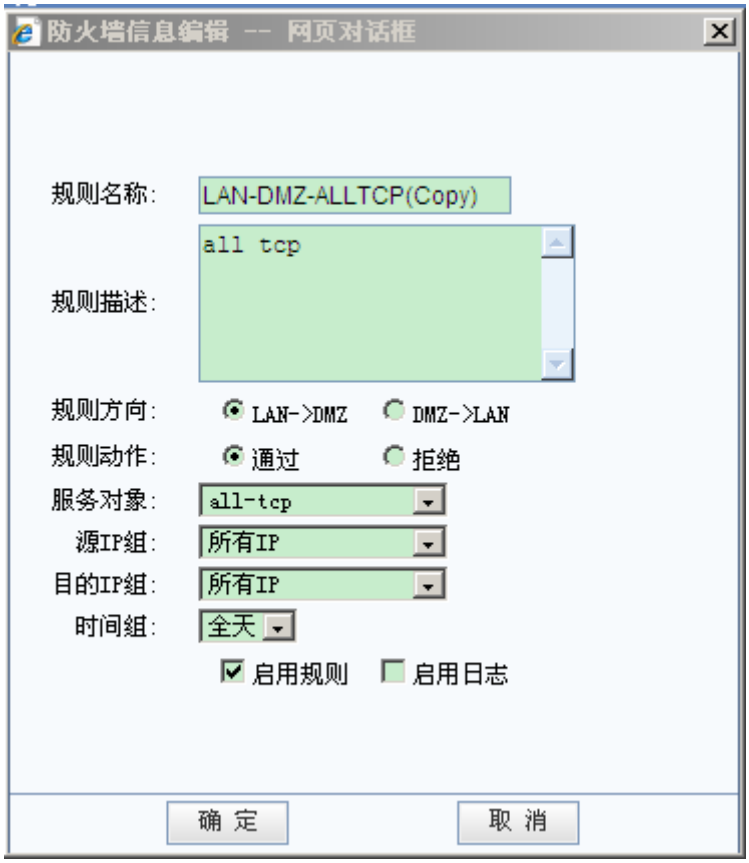
『VPN<->DMZ』用于设置 VPN 设备的 VPN 接口与 DMZ 接口之间双向数据传输的防火墙过滤规则。

下面以 LAN<->DMZ、VPN<->LAN 为例介绍过滤规则设置的一般步骤：

**1、LAN<->DMZ**

用于设置 LAN 口与 DMZ 口之间数据传输的防火墙过滤规则，可根据实际环境设置放行某类服务数据或拒绝某类服务数据。例如要使 LAN 与 DMZ 口之间完全互通并且能够使用 PING 命令进行测试，则需要在两个方向上开放所有的 TCP、UDP 以及 ICMP 过滤规则。页面如下：


设置规则时需要注意数据的方向和动作，页面如下：




『规则名称』自定义规则名称。

『规则方向』设置此规则对哪个方向的数据生效。

『规则动作』设置数据匹配此规则后的执行动作。

『服务对象』设置规则要匹配的服务类型。

『源 IP 组』设置规则要匹配的源 IP 地址。

『目的 IP 组』设置规则要匹配的目的 IP 地址。

『时间组』设置规则生效的时间。

勾[启用规则]选项，则此规则设置完成后立即生效。

勾选[启用日志]选项，则所有匹配此规则的数据包经过设备时日志系统都将记录日志，一般情况下请不要启用，以免系统产生大量日志。

**2、VPN<->LAN**

此界面用于设置 VPN 接口与 LAN 接口之间数据传输的防火墙过滤规则，默认规则已放行了双向的所有 TCP、UDP、ICMP 数据，页面如下：


## 5.3.1. 案例学习

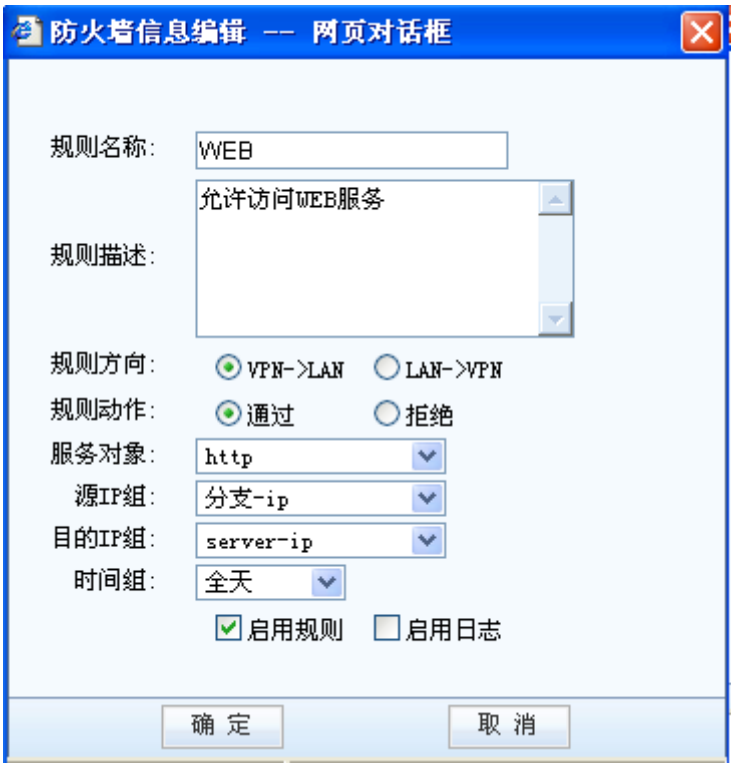
某公司总部只允许接入总部的 VPN 分支（172.16.1.0/24）的其中一部分 IP 地址（172.16.1.100-172.16.1.200）访问总部内网服务器（192.168.10.20）的 WEB 服务，但禁止这一部分 IP 访问同一个总部内网服务器的 SQL SERVER 服务（192.168.10.20）。

设置步骤如下：

1、 新建 IP 组，如下图所示：



2、新建 WEB 服务过滤规则，配置页面如下：




『规则名称』自定义规则名称。

『规则描述』对规则进行描述。

『规则方向』设置为 VPN->LAN。

『规则动作』设置为对此类数据允许。

『服务对象』设置为 HTTP。

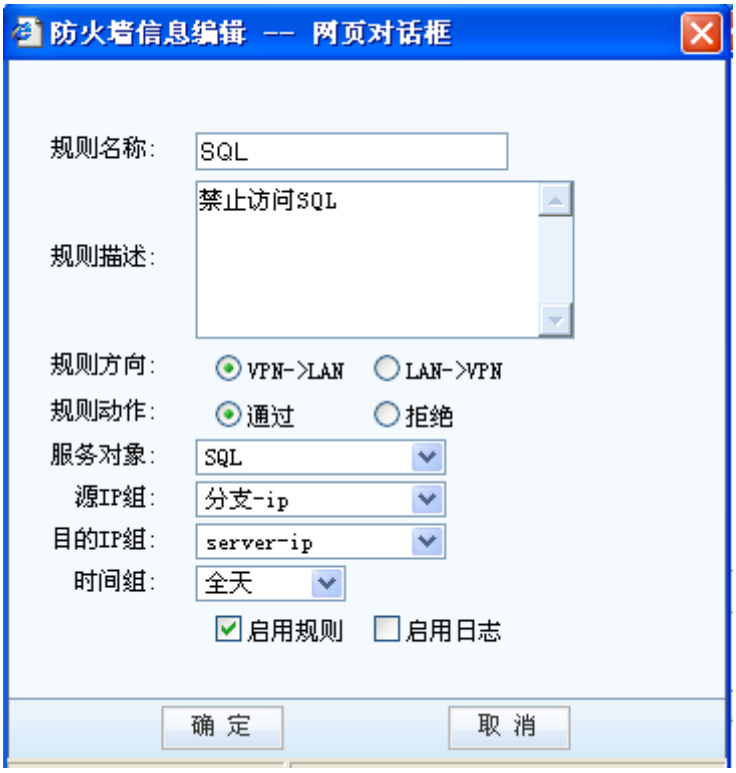
『源 IP 组』设置为分支内网的部分 IP 地址 172.16.1.100-172.16.1.200，即分支-ip。

『目的 IP 组』设置为总部内网的服务器 IP192.168.10.20，即 server-ip。

『时间组』设置规则生效的时间。

勾选『启用规则』选项，确定完成。

3、设置 SQL SERVER 服务过滤规则，页面如下：




『规则名称』自定义为 SQL。

『规则描述』对规则进行描述。

『规则方向』设置为 VPN->LAN。

『规则动作』设置对此类数据拒绝。

『服务对象』设置为 SQL。

『源 IP 组』设置为分支内网的部分 IP 地址 172.16.1.100-172.16.1.200，即分支-ip。

『目的 IP 组』设置为总部内网的服务器 IP192.168.10.20，即 server-ip。

『时间组』设置规则全天生效。

勾选『启用规则』选项，确认完成。

完成上述设置后，即可实现对 VPN 数据的有效过滤。

**其他如限制总部访问分支服务、限制分支通过总部上网的数据等需求都可以通过在相应接口之间设置过滤规则实现。**

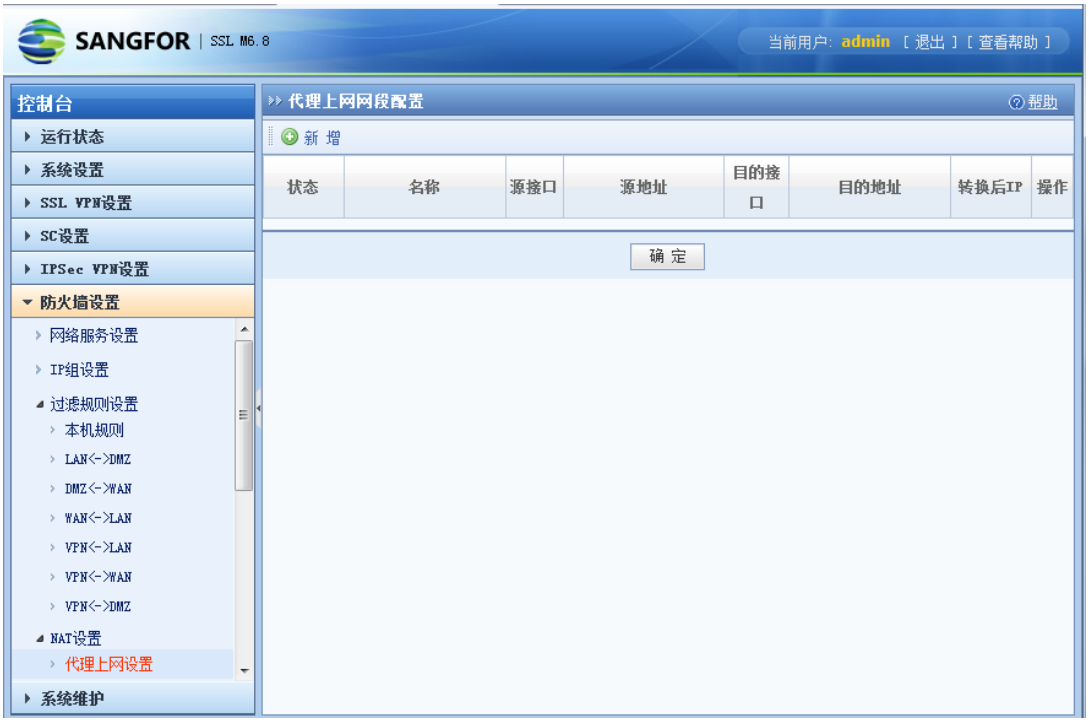
## 5.4. NAT 设置

NAT 设置包括『代理上网设置』、『端口映射设置』、『IP MAC 绑定设置』、『HTTP 端口设置』、『URL 组设置』、『外部服务组设置』、『用户上网权限设置』等内容。

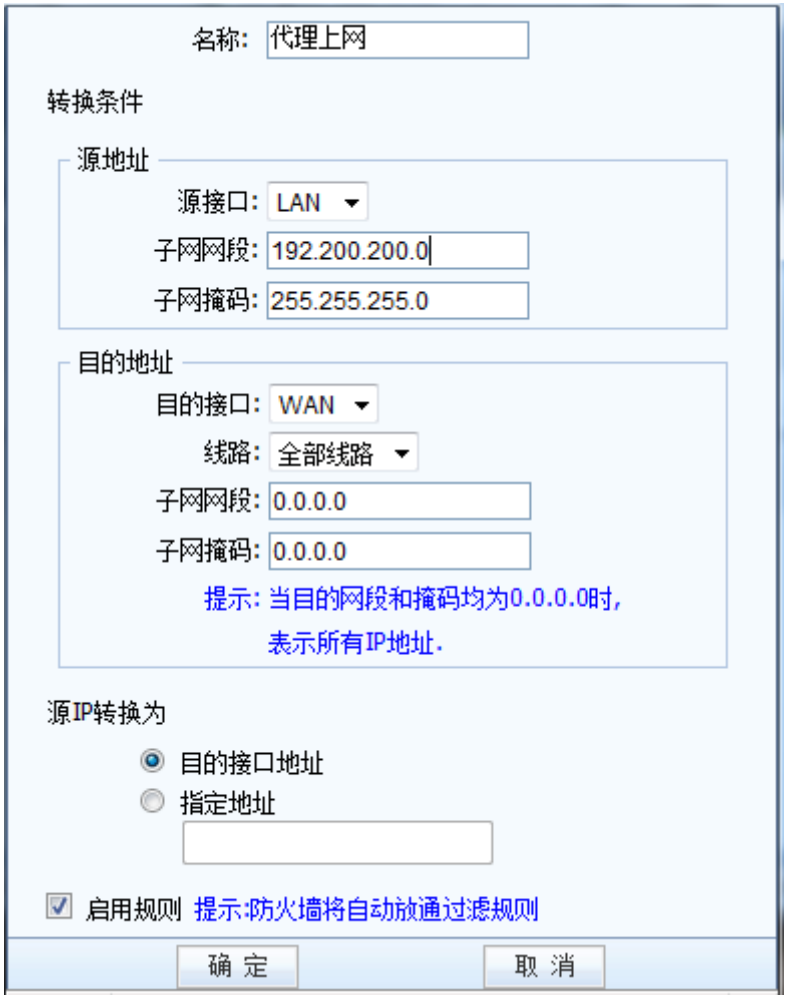
### 5.4.1. 代理上网设置

『代理上网设置』用于设置防火墙代理局域网上网的规则，SANGFOR VPN 硬件网关不仅有基本的 NAT 代理上网功能，还可通过与过滤规则进行配合对内网的上网服务进行控制。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『代理上网设置』。如下图：




设备缺省设置中不包含代理信息，需要手动添加，点击 新增，弹出【代理网段配置编辑】对话框，页面如下：




『名称』用于自定义规则名称

『转换条件/源地址』源接口用于设置数据包的源接口地址，表示从该接口过来的数据会继续往下匹配，可以选择 LAN、DMZ、VPN 三种。子网网段和子网掩码用于设置需要转换的源地址网段。

『转换条件/目的地址』目的接口用于设置数据包的出接口地址，表示从该接口出去的数据会计息往下匹配，可选择 LAN、DMZ、VPN 三种。子网网段和子网掩码用于设置匹配条件，表示数据包的目标 IP 地址在设置的范围内，则可以匹配到该规则。

『源地址转换为』用于设置符合指定条件的数据包转换源地址为“目的接口地址”或者“指定地址”。选择目的接口地址，则会将数据包源地址转换为“目的接口”选择的接口 IP 地址。选择“指定地址”则需要手动设置一个 IP 地址。

勾选『启用规则』，则规则生效，防火墙会自动对应的过滤规则。

## 5.4.2. 端口映射设置

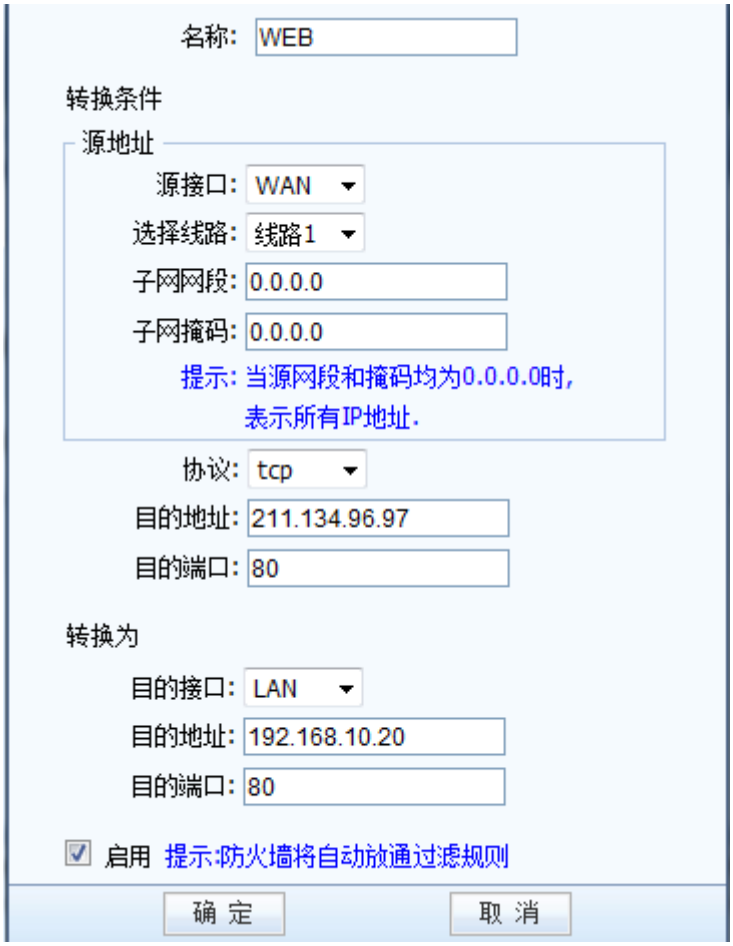
『端口映射设置』用于设置防火墙的 DNAT 规则，如果局域网内的服务器需要向外网提供服务，则需要添加『端口映射设置』。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『端口映射设置』。界面如下图所示：


### 5.4.2.1. 案例学习

内网有一台 IP 为 192.168.10.20 的电脑要对外网提供 Web 服务，所使用的端口为 80，需要通过端口映射将该服务器 80 端口发布至公网，则设置步骤如下：

1、在『端口映射设置』中『新增』一条映射规则。页面如下：




点击 确定 后规则生效，则外网可通过端口映射功能访问到内网提供的 Web 服务。

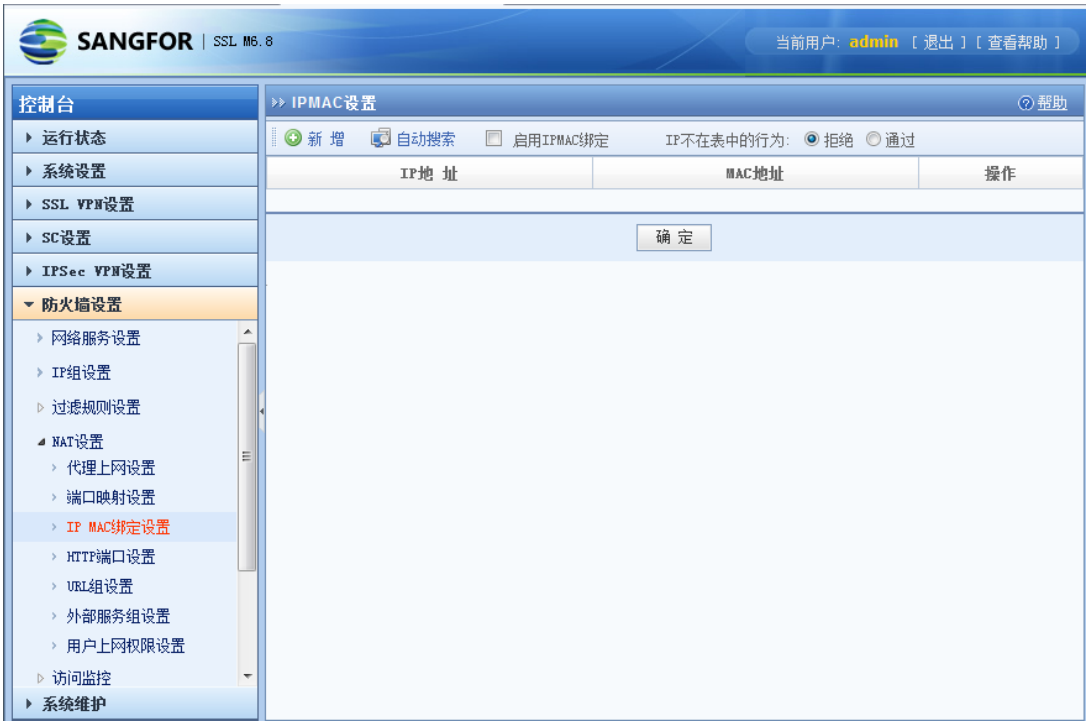
**注意：通过 SANGFOR VPN 硬件设备设置端口映射向外网提供服务的内网服务器，必须是以 VPN 硬件设备作为 NAT 代理上网（网关指向 VPN 设备或上网路由最终指向 VPN 设备），否则端口映射将无法生效。**

## 5.4.3. IP MAC 绑定设置

SANGFOR VPN 系列产品提供了“IP/MAC 绑定”功能，通过此功能可以很方便地得到内网某个 IP 地址所对应的 MAC 地址并将它们绑定在一起，当局域网内部有未知设备接入时，由于在 IP/MAC 绑定表中没有它的记录，未知设备将无法通过 VPN 网关上网。当某个 IP 所对应的 MAC 地址与记录不符时，VPN 网关也将拒绝此 IP 的上网请求，因此 IP/MAC 绑定还可用于限制内部电脑 IP 被人为改动。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『IP MAC 绑定设置』。

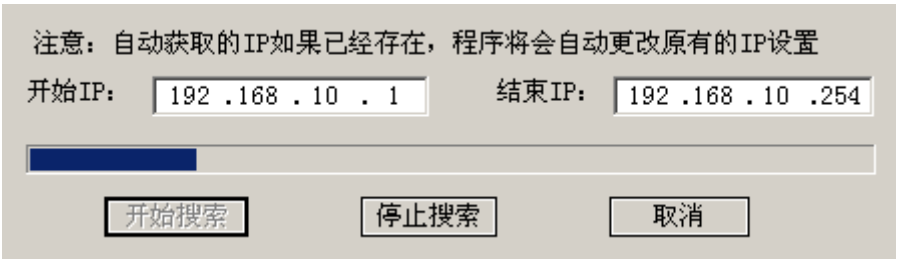
界面如下图所示：




勾选[启用 IP MAC 绑定]即启用 IP-MAC 绑定功能。

点击 新增，手动添加 IP 和 MAC 的对应关系。也可以点击 自动获取 来自动获取 IP 所对应的 MAC 信息。

点击 自动搜索，设置搜索范围，系统将自动在所设置的 IP 范围内搜索存在的计算机的 IP/MAC 信息。


『IP 不在表中的行为』可选为[拒绝]或[通过]，用于设置不匹配 IP/MAC 记录后的操作。

[拒绝]即对不在 IP MAC 列表内的计算机以及列表内 IP MAC 不匹配的计算机禁止上网，对 IP MAC 匹配的计算机依旧允许其上网。

[通过]即对不匹配 IP MAC 记录的计算机以及不在 IP MAC 列表内的计算机允许其上网，在 IP MAC 列表内的计算机如果 IP MAC 匹配正确则允许上网，匹配不正确依旧不允许上网。

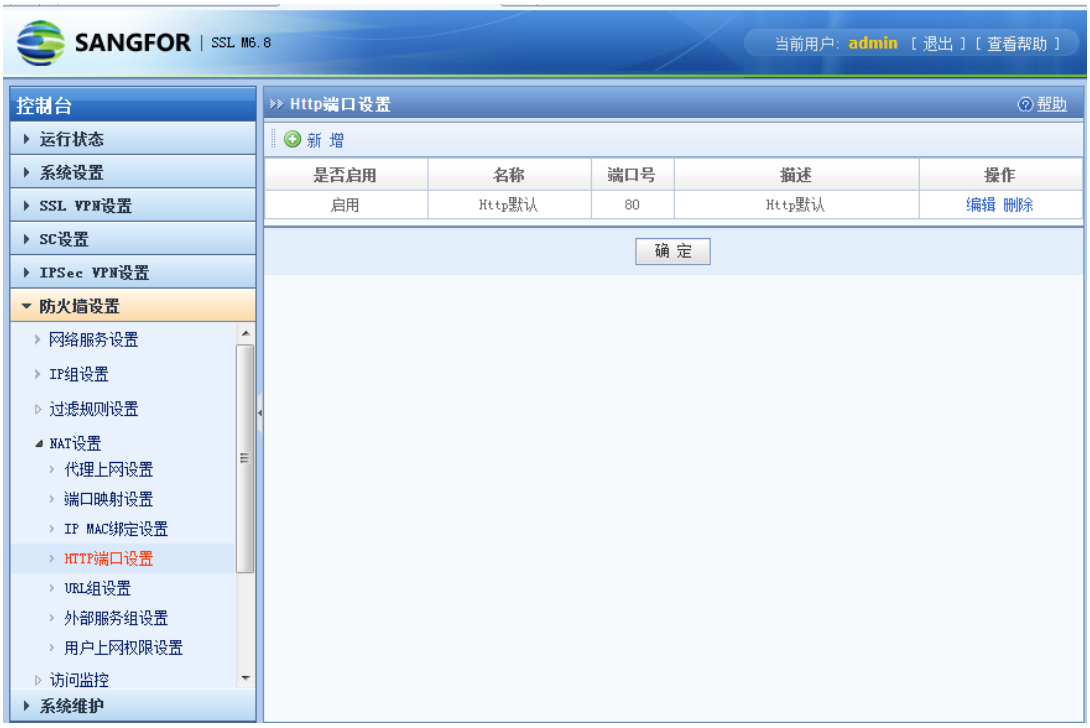
**IP/MAC 绑定功能，不支持内网有三层设备的环境。**

## 5.4.4. HTTP 端口设置

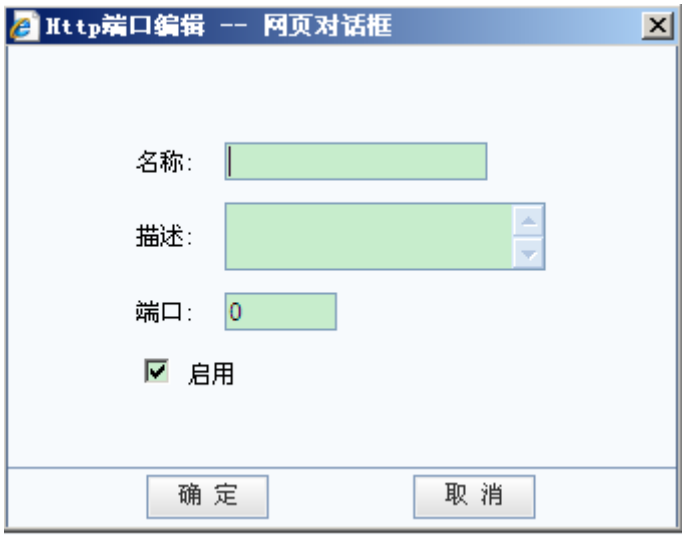
『HTTP 端口设置』用于定义 HTTP 服务的端口，默认设置为 80。这里定义 HTTP 端口为 80 后，当启用[上网权限/启用 URL]记录功能时，VPN 硬件网关会记录通过 80 端口访问的 URL 信息并可对通过 80 端口发出 URL 信息进行过滤，如果需要记录/过滤通过其它端口访问的 URL 信息，则需将相应的端口添加到『HTTP 端口设置』中。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『HTTP 端口设置』。

界面如下图所示：




点击 新增，设置『名称』、『描述』、『端口』，勾选[启用]，完成设置。

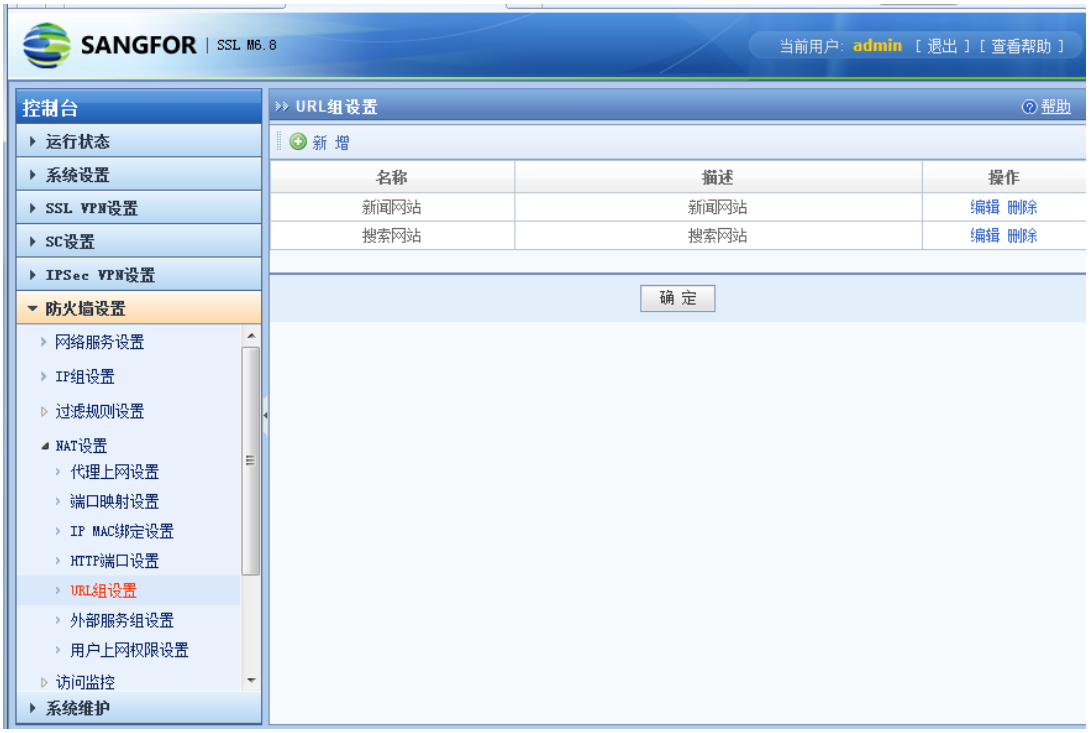



## 5.4.5. URL 组设置

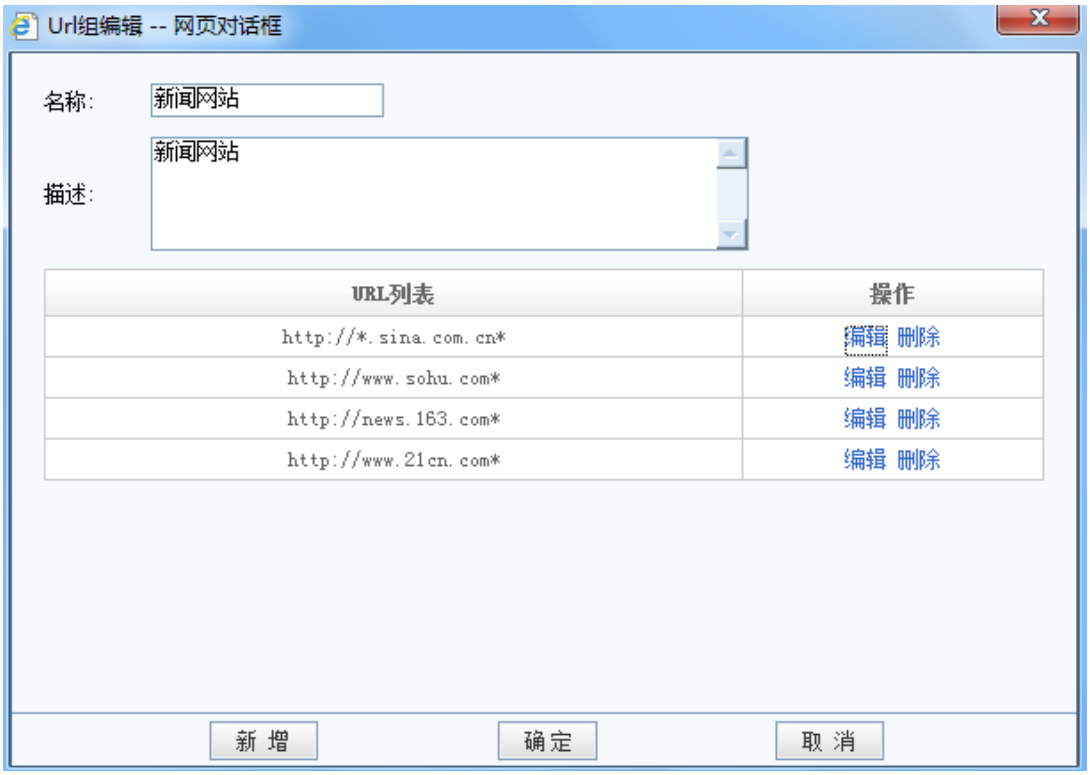
VPN 硬件网关的企业级状态检测防火墙具有“网页地址过滤”功能，可与防火墙配合对局域网用户上网进行管理，使用该功能之前需要先在『URL 组设置』中添加所需的 URL 信息。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『URL 组设置』。

界面如下图所示：




点击上图中 新增 按钮，显示『URL 组编辑』对话框，设置 URL 组『名称』、描述。在点击下图中 新增，将 URL 信息添加到『URL 列表』中（第一个字段支持使用*号匹配），如有需要可添加多个 URL，点 确定 后完成设置，页面如下：

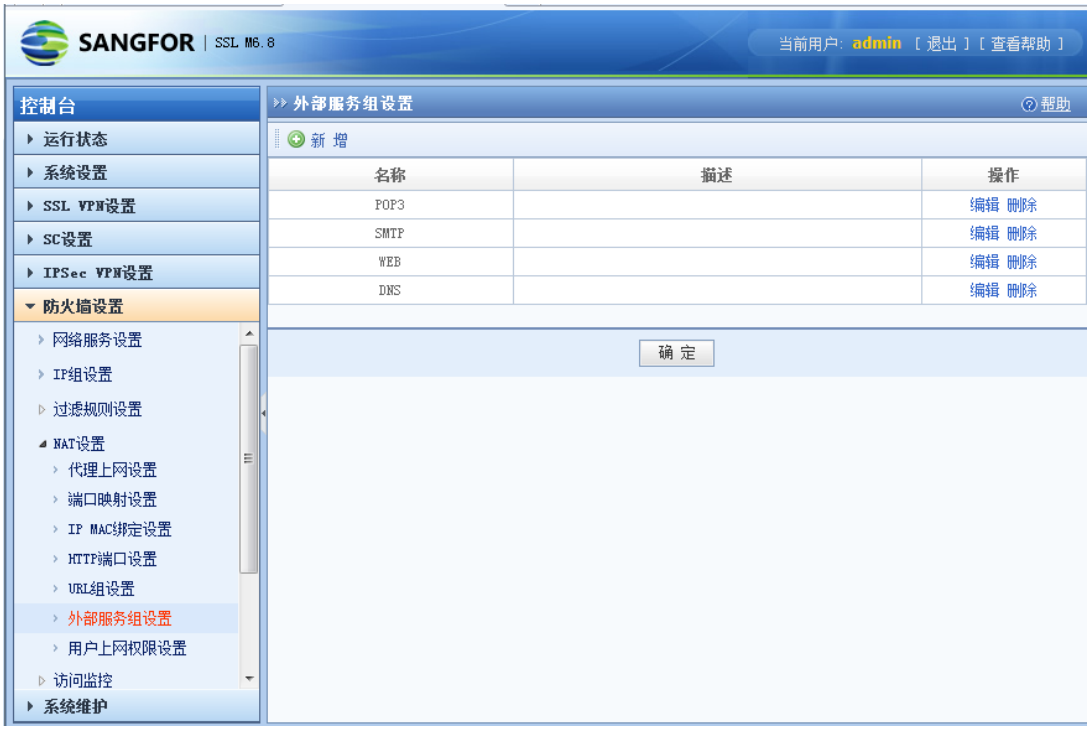



## 5.4.6. 外部服务组设置

默认情况下，内网用户可以访问外网的所有服务，如需在『上网权限设置』中设置内网用户访问外网服务的权限，则需先在『外部服务组设置』中定义相应的服务。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『外部服务组设置』。

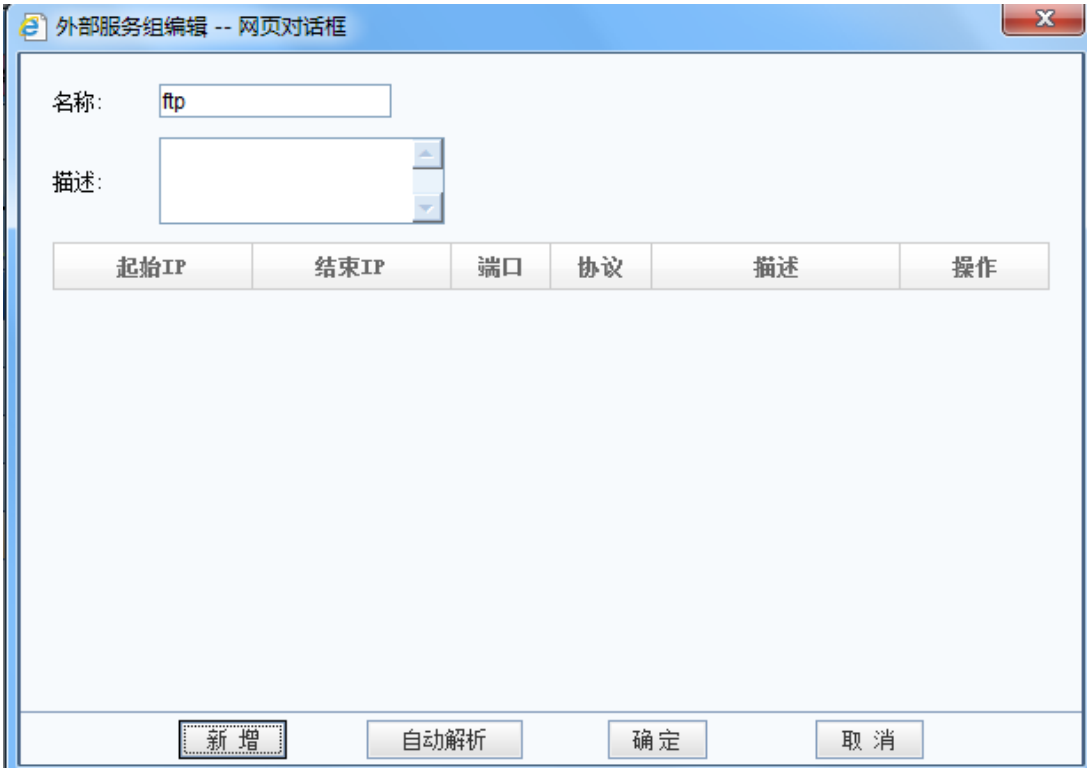
界面如下图所示：




默认配置了 POP3、SMTP、WEB、DNS 四类服务，可自定义其他服务。

例如：要添加 Internet 上 IP 为 202.96.137.75 的服务器提供的 FTP 服务（具体端口号根据软件所使用端口而定），设置方法如下：

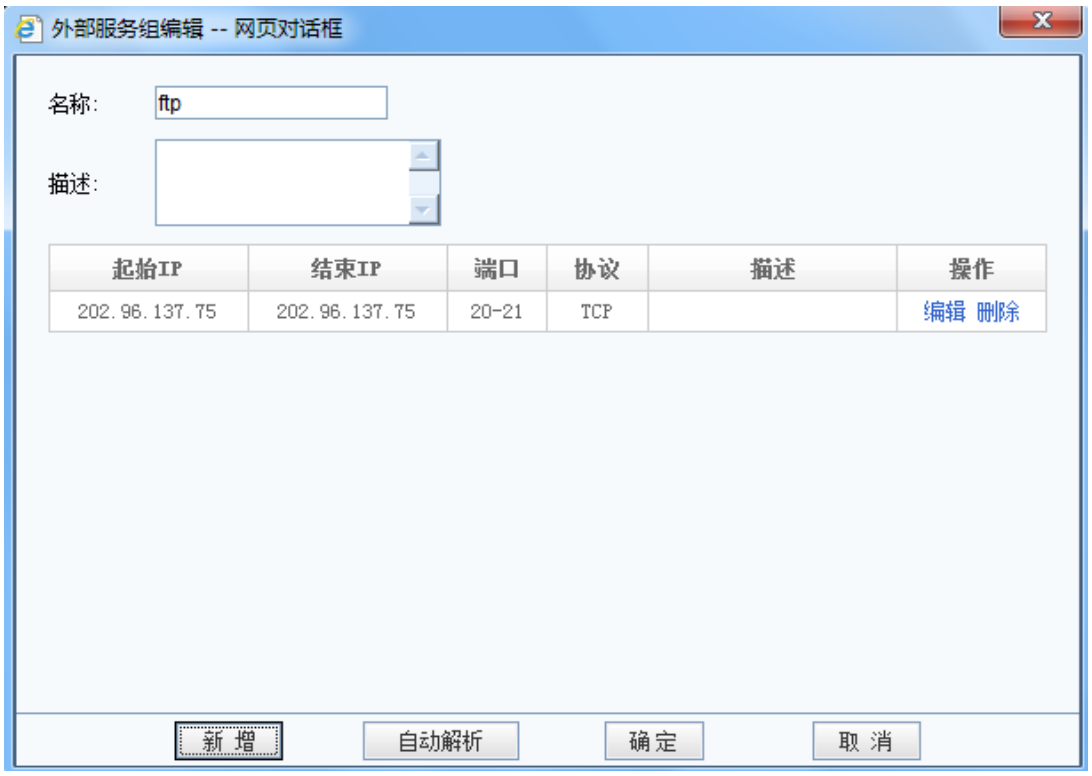
点击 新增，显示『外部服务组编辑』对话框，页面如下：




再点击 新增，设置外网服务器的『起始 IP』、『终止 IP』、『端口号』、『描述』，页面如下：


也可以点击 自动解析 按钮出现以下对话框，填入对应的域名，可以自动解析域名对应的 IP，方便定义外网服务。页面如下：


点击确定，保存配置，如下图：

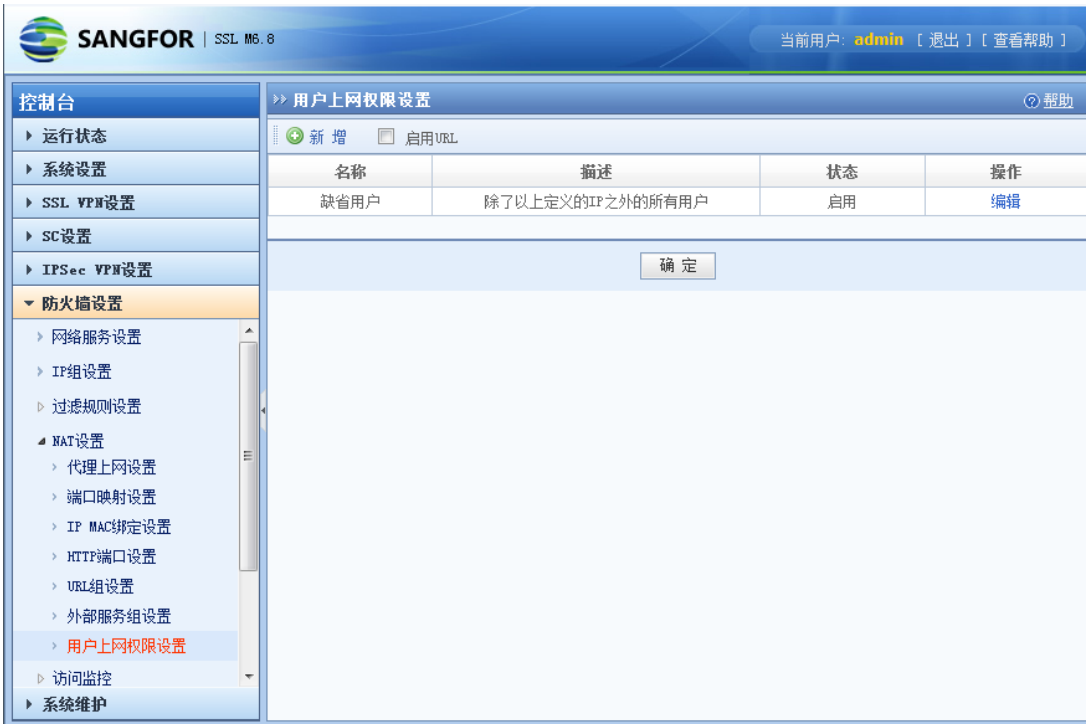


## 5.4.7. 用户上网权限设置

『用户上网权限设置』是防火墙中用于对局域网用户访问外网的权限进行控制而采用的最常用的方法，虽然通过防火墙的过滤规则也可实现，但这两者仍有区别。『过滤规则』是基于对某些 IP 地址和端口的访问控制来实现上网服务的控制，它更注重的是整个网络的安全性。而在控制内网用户上网时，使用『用户上网权限设置』进行控制时会更为方便。

WEBUI 路径：『防火墙设置』→『NAT 设置』→『用户上网权限设置』。

界面如下图所示：




要启用“URL 过滤”及『访问记录』功能，必须勾选[启用 URL]。

点击 新增 出现【上网权限编辑】对话框，

在『IP 组』选项卡下点击 新增，即可在对话框中输入这条规则所要匹配的内网 IP 范围，页面如下：



点击 服务组 选项卡，则可设定该内网 IP 范围内，可以访问外网的哪些服务，页面如下：


在此对当前 IP 组能够访问的外网服务进行设置，默认设置是[缺省允许]，此时局域网用户可访问外网的所有服务。相应的服务请在『外部服务组设置』中添加。

点击『URL 组』选项卡，如下图：


在此可以对当前 IP 组访问的 URL 地址进行设置，默认设置是『缺省允许』，如果要对某

个 URL 组进行拦截只需要把它右移并勾选拒绝即可，相应 URL 信息请在『URL 组设置』中添加。

**防火墙规则匹配均按照从上往下匹配的原则。配置规则的时候，请注意排序。**

## 5.5. 访问监控

### 5.5.1. 流量排名

通过『流量排名』可以直观地查看当前局域网中用户对带宽的使用情况，可分别查看上行和下行流量。

WEBUI 路径：『防火墙设置』→『访问监控』→『流量排名』。

界面如下图所示：


### 5.5.2. 访问记录

『访问记录』用于查看当前局域网用户的 URL 访问记录，点击 刷新状态 可实时刷新访问记录。

WEBUI 路径：『防火墙设置』→『访问监控』→『访问记录』。

界面如下图所示：


**注意：必须在『用户上网权限设置』中勾选『启用 URL』，此处才能看到 URL 访问记录。**

## 5.6. 防 DOS 攻击

防火墙不仅肩负着阻隔 Internet 上的用户对局域网非法攻击的任务，很多时候由于局域网内有电脑中毒，会向网关发送大量的数据包，这样有可能会造成带宽阻塞或者网关死机。SANGFOR VPN 设备内部集成了『防 DOS 攻击』功能，可以监测单位时间内某个 IP 向网关发送了多少数据量，当超过一定值时则 VPN 设备会认为受到此 IP 的 DOS 攻击，并会阻断此 IP 一段时间从而保护自己。页面如下：


勾选[启用防 DOS 攻击]即开启防 DOS 攻击功能。

在『内网网段列表』中添加局域网所包含的网段，当这里为空的时候即表示不检查 IP 地址。当添加了内网网段后，当源 IP 不属于『内网网段列表』所列网段范围之内，则该数据包会被直接丢弃。属于『内网网段列表』范围时，则会进行下面防 DOS 攻击各项设置的计算和探测，以进行相应的处理。

同理，『内网路由器列表』的功能和『内网网段列表』功能类似。

在『排除地址列表』中添加局域网所包含的 IP 地址，当这里为空的时候即表示检查所有 IP 地址。当添加了内网 IP 后，来自这个 IP 地址的攻击不会被防御。

其它选项可根据情况来进行相应设置，包括『最大 TCP 连接数』,『最大 SYN 包数』及『防 DOS 攻击的封锁时间』等。

## 5.7. QOS 级别设置

QoS(Quality of Service，服务质量保证)在网络带宽不足的情况下，通过 QOS 设定来保证一些重要的服务能获得充足的网络带宽。可以设定各优先级能够得到的带宽比例，在网络繁忙时将按照设定的比例来分配网络带宽，保证整个出口线路上，通过防火墙的重要服务能够顺畅进行。


『QoS 优先级别设置』可以设定四个级别占用的带宽比例，以百分比来表示。

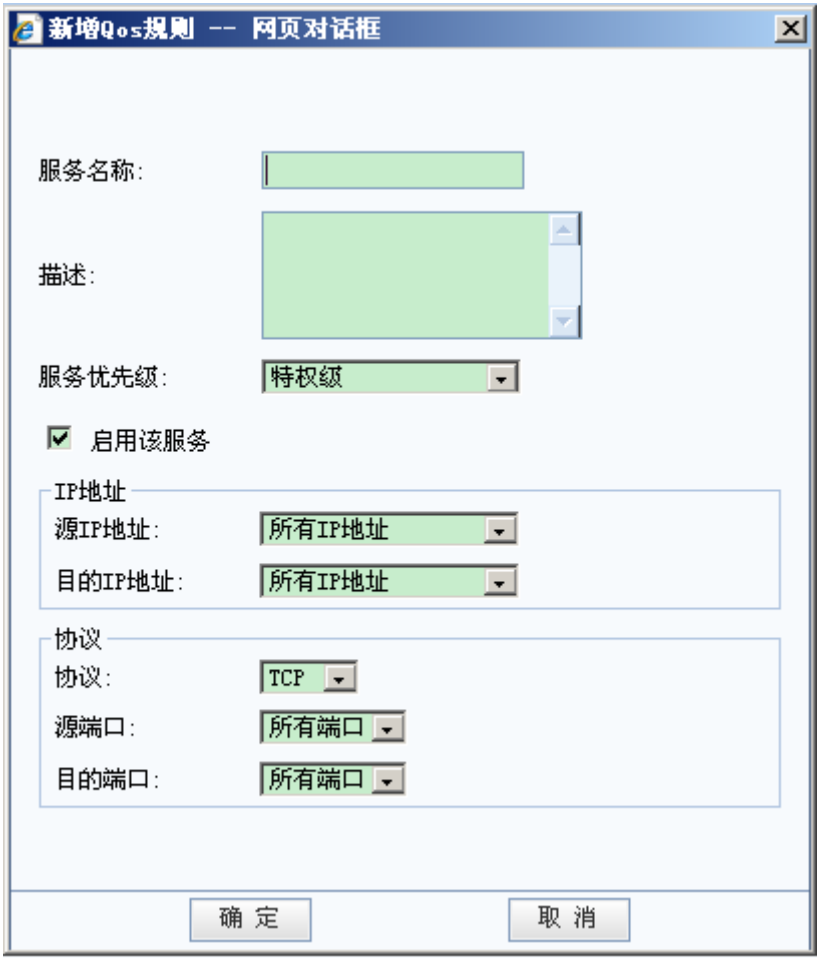
『启用 QoS 功能』是整个防火墙 QoS 功能的开关，勾选即启用了防火墙的 QoS 功能。

# 5.8. QOS 上传规则设置

QoS 上传规则设置是用来把数据业务进行分类，根据 QoS 规则设置所选定的数据投递优先级进行投递，以保证重要数据的及时传输。


设备内置了一项缺省服务定义，只需点击 编辑 按钮，即可设置默认服务的优先等级信息。

点击 新增 按钮，会出现以下【新增 QoS 规则】对话框：




『服务名称』和『描述』可根据喜好填写。

『服务优先级』用于设置该 QoS 规则应用的“优先级”，除了前面『QoS 等级设置』定义的四个等级外，还有一个“特权级”，特权级别可以占用所有带宽。

勾选[启用该服务]即可激活这条 QoS 上传规则。

『IP 地址』用于设置 QoS 规则应用的源及目标 IP，可以设定为“所有 IP 地址”或“指定 IP 地址”。

『协议』用于设置 QoS 规则所对应的服务提供的端口及协议等。

## 5.9. QOS 下载规则设置

QoS 下载规则设置是用来把数据业务进行分类，根据 QoS 规则设置所设定的不同服务

优先级进行投递，以保证重要数据的及时传输。


和 QoS 上传规则相类似，点击 新增 按钮出现如下对话框，以下仅举一例子说明：


以上规则保证了内网从公网 HTTP 服务器 80 端口的下载通讯设定 QoS 级别为特权级别。

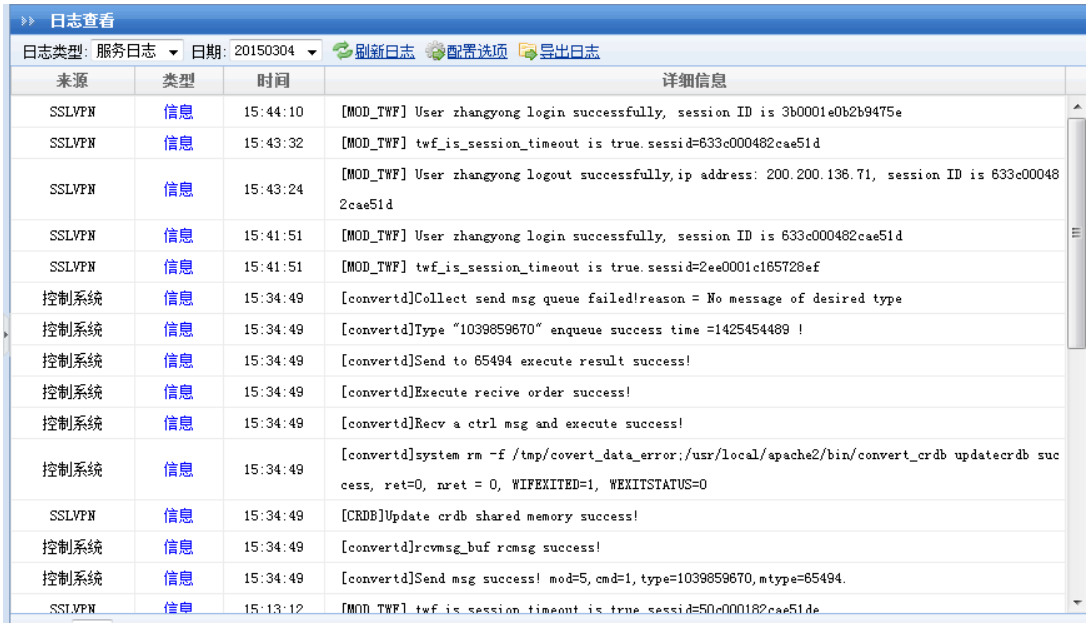
# 第6章 系统维护

『系统维护』包括『日志查看』、『配置备份/恢复』、『重启/重启服务/关机』三部分。

## 6.1. 日志查看

用于查看设备的运行日志及错误提示。运行日志包括了两种类型，一种为服务日志，另一种为管理日志。服务日志可以查看当前设备各种服务运行的信息。选择要查看的日期，会显示相应时间下的日志记录。

WEBUI 路径：『系统维护』→『日志查看』。界面显示如下：

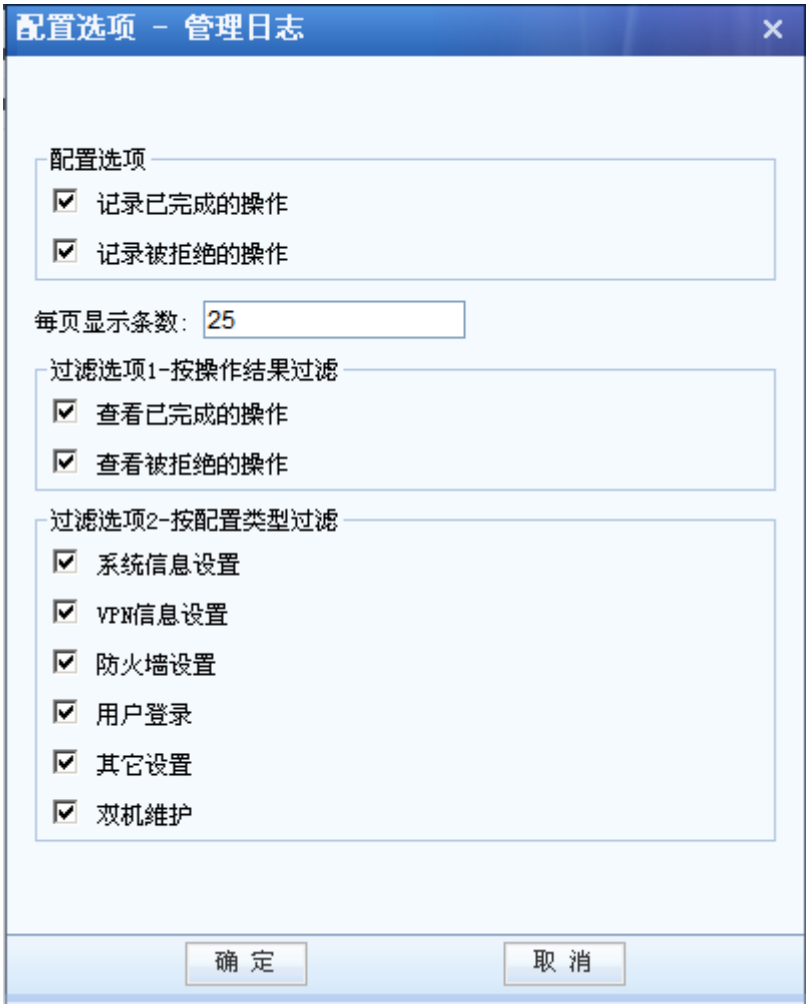



『日志类型』中，默认显示的是[服务日志]，也可以选择[管理日志]，[管理日志]主要用来查看当前设备管理员对设备进行的操作日志信息，如下图：


| | IP地址 | 操作权限 | 操作时间 | 配置类型 | 操作过程 | 操作结果 |
|---|---|---|---|---|---|---|
| Admin | 10.10.2.248 | 管理员 | 23:47:50 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 23:43:51 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 23:35:29 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 23:35:25 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 23:34:18 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 23:04:31 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:53:36 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:46:22 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:32:05 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:31:49 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:20:48 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:19:04 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:17:15 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:14:05 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:13:40 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:09:18 | 用户登录 | 完成 | 用户登录 |
| Admin | 10.10.2.248 | 管理员 | 22:07:13 | 用户登录 | 完成 | 用户登录 |
| 非法用户 | 10.10.2.248 | 非法 | 22:07:02 | 用户登录 | 失败 | 用户注销 |
| Admin | 10.10.2.248 | 管理员 | 22:06:23 | 用户登录 | 完成 | 用户登录 |

在[服务日志]下点 配置选项，可以设置指定查看的系统日志范围。页面如下：


在[管理日志]下点 配置选项，可以设置指定查看的管理日志范围。页面如下：




**注意：VPN 设备最多保留 1 天的日志，超出 1 天的日志将被清空。**

## 6.2. 配置备份/恢复

『配置备份/恢复』用于备份、恢复 VPN 网关设备的配置。

WEBUI 路径：『系统维护』→『配置备份/恢复』。

界面显示如下：


『全局配置备份』标签页，设置备份和还原设备的所有配置。

**通过设备备份 SSL 的全局配置时，会备份 SSL 的序列号，所以，在配置还原 SSL 的全局配置前，注意备份需要还原设备的序列号。**

点击 下载当前配置，可将当前的配置备份到本地 PC 上，以便以后恢复，下载下来的文件格式为.bcf。

点击 开始还原，可将以前备份在本地 PC 上的配置导入设备。

勾选[连续一段时间内没有执行配置备份,则登录控制台时提醒]并设置好『时间间隔』后，系统会以设置的时间为间隔在用户登录控制界面时提醒用户进行备份。

『SSL VPN 配置备份』标签页，设置备份和还原 SSLVPN 的所有配置。

界面显示如下：


点击『下载当前配置』，可将 SSL 模块中的配置下载下来保存在本地 PC 当中。

**注意：这里的下载配置只能下载 SSL 模块的配置，此配置不包含 VPN、系统、防火墙等其它模块的配置。**

『配置还原』功能用于将 SSL 配置恢复到以前保存的配置。点击 浏览，先择以前备份的配置，再点击 开始还原 即可。

『自动备份配置』：设备自动配置最近 7 天的配置，点击相应该配置文件后的 还原配置 可以将 SSL 配置恢复到备份时的状态。

## 6.3. 重启/重启服务/关机

WEBUI 路径：『系统维护』→『重启/重启服务/关机』。

界面显示如下：


关闭设备：将设备安全的关闭。

重启设备：将设备先关闭再重启。

重启所有服务：将当前连接的会话与资源全部释放后，再重启全部服务。

停止 SSL VPN 服务：将 SSLvpn 服务停止。

关于 SSL VPN：显示 SSL VPN 当前版本信以及设置设备自动更新

## 6.3.1. SSL VPN 更新设置

选择是否启用自动更新，如果启用，则会自动下载更新，并安装它们。

WEBUI 路径：『系统维护』→『重启/重启服务/关机』→『关于 SSL VPN』。

点击 更新设置，


选择[启用自动更新]，设备会每隔设定的时间自动去下载可用更新，并安装它们。

选择[关闭自动更新]，设备不再去自动下载更新。

**注：此更新不可用于大版本升级。**

选择[选择体检改善]，允许发送系统质量报告给深信服科技股份有限公司，帮助我们完善 SSL 系统，该报告不会涉及您组织的任何信息。

点击 保存 使当前设置生效。

# 第7章 SSL VPN 客户端使用

本部分主要介绍了 SSL VPN 客户端的安装和使用。

## 7.1. 环境要求

1、客户端计算机已经接入因特网，并且网络通信正常。

2、计算机必须安装浏览器。

3、电脑安装 3721、上网助手等工具，可能会影响正常使用 SSL VPN，可以先卸载。

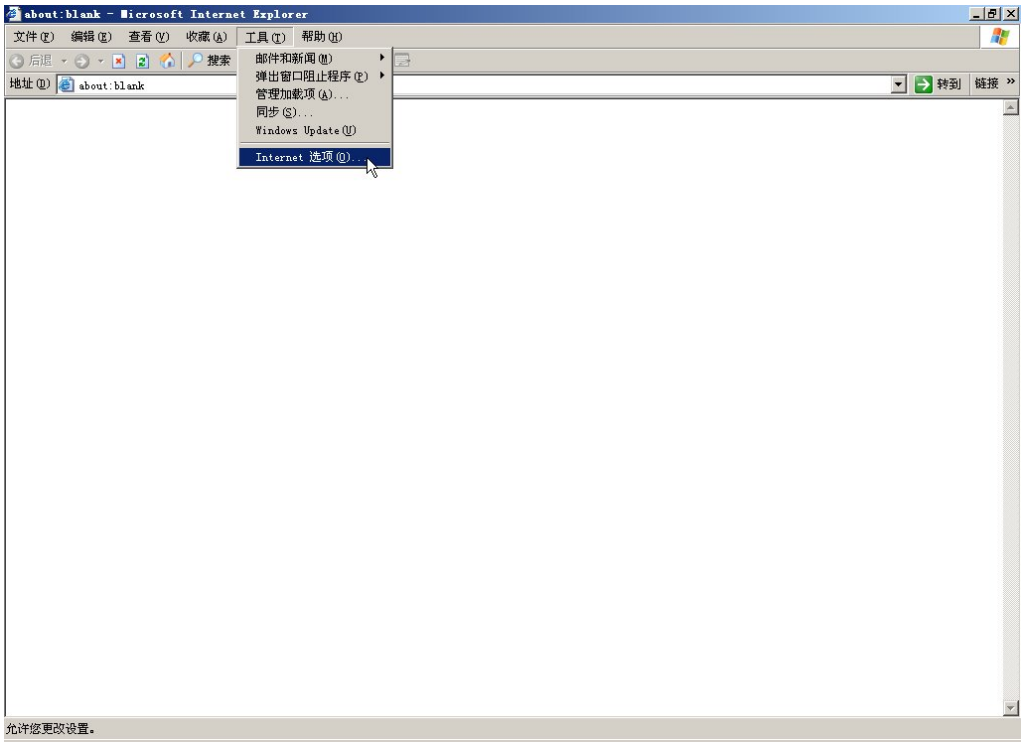
**SSL VPN 客户端支持 Windows 操作系统、Linux 操作系统和 Mac OS X 操作系统，支持苹果，安卓等手机接入；支持多种浏览器。**

## 7.2. 典型使用方法举例

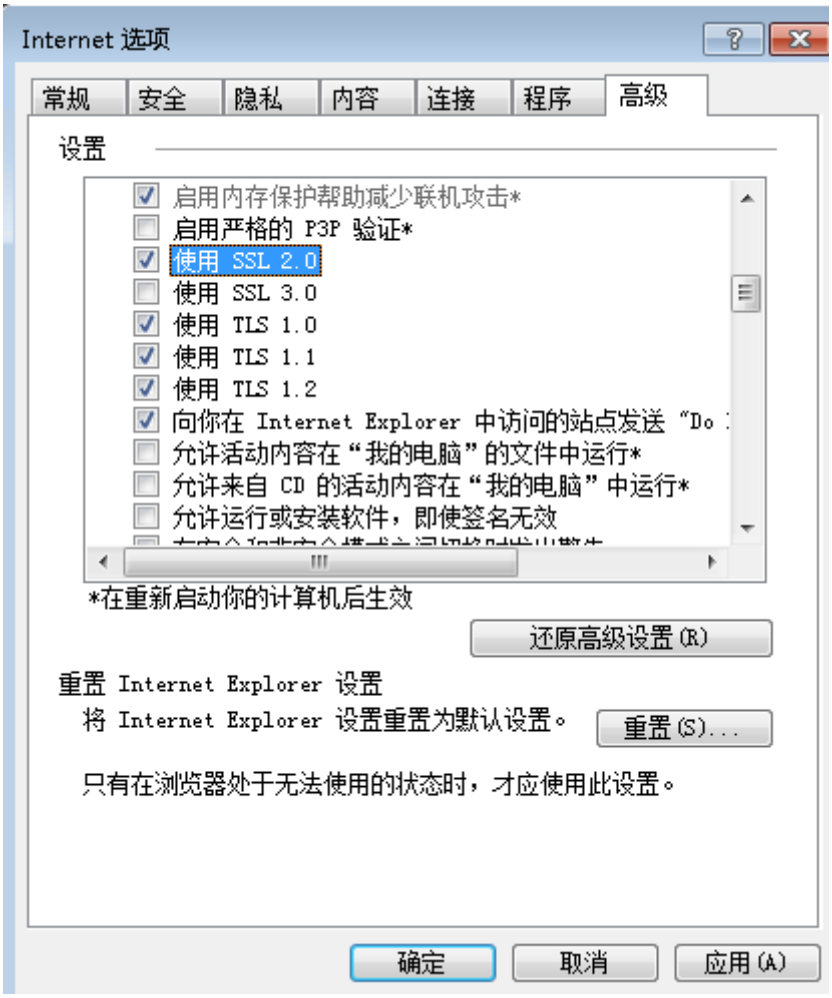
使用 SSL VPN 之前，可能需要对浏览器（例如 IE，以下皆以 IE 作为浏览器来举例）进行必要的设置，步骤如下：

（注：以下所有截图皆以 Windows XP 系统下的 IE 为例，其它操作系统或浏览器，界面可能稍有不同）

打开 IE 中的[工具]－[Internet 选项]，如下图：

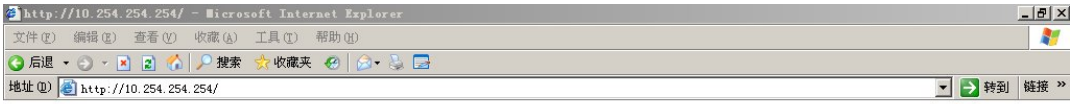


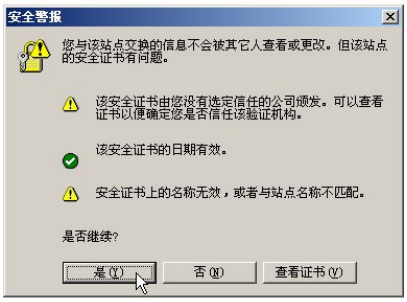

打开 Internet 选项中的[高级]选项卡，勾选[使用 SSL2.0]和[使用 TLS1.0]选项，设置如下图：




设置好 IE 浏览器之后，直接在 IE 地址栏输入 SSL VPN 的登录页面地址来登录 SSL VPN。

访问 SSL VPN 时，会弹[安全警告]，提示需要安装数字证书，如下图所示：

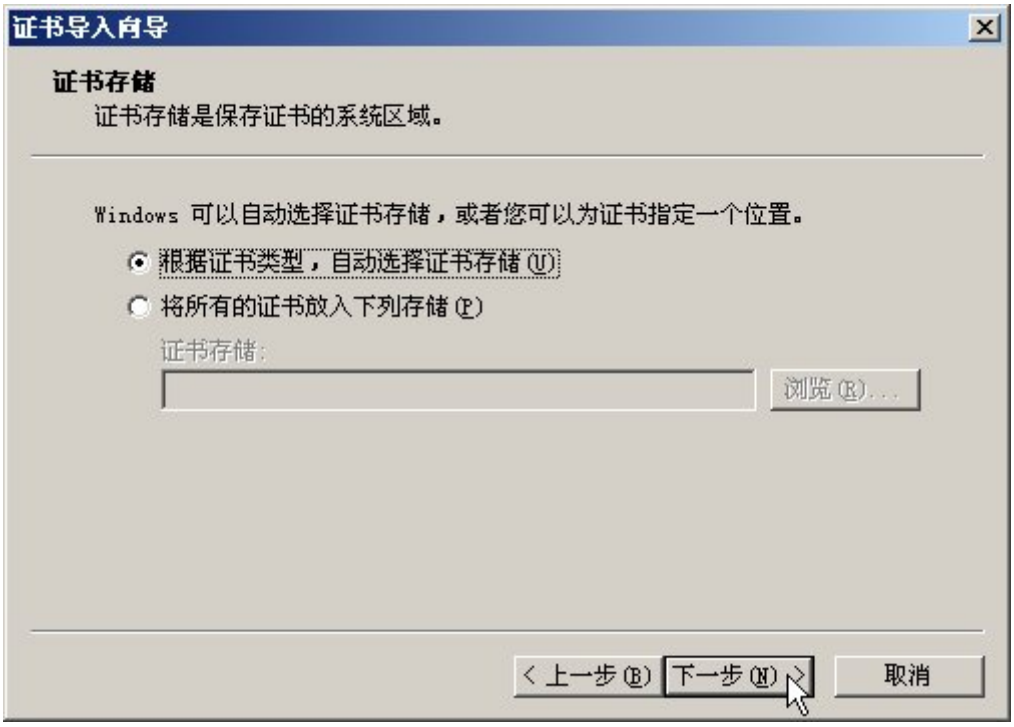


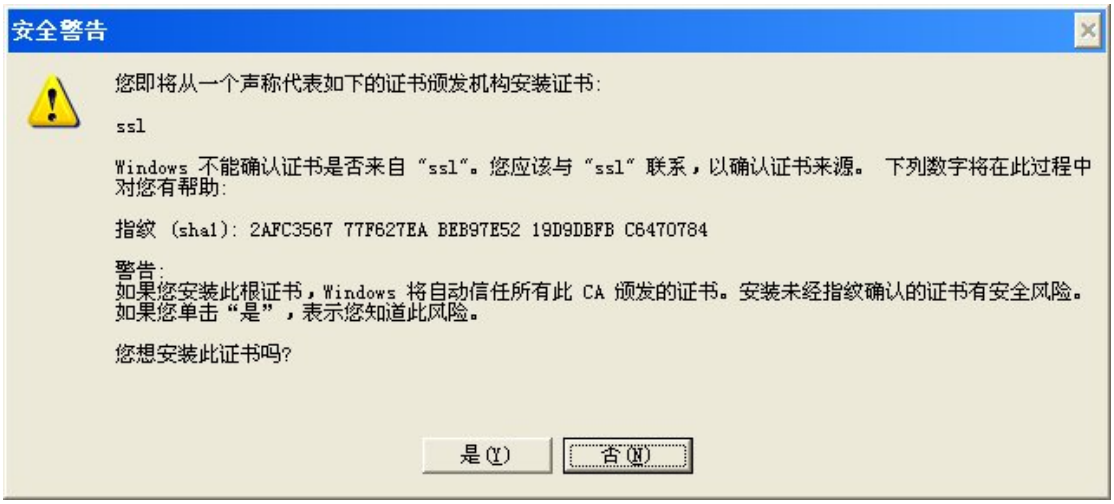


第一次使用时，请点击 查看证书 按钮，以完成“根证书”的安装。查看证书界面如下：


点击 安装证书 按钮，然后 下一步，选择“证书存储”的位置，如下图：



点 下一步，并 完成，会出现[安装证书]的警告框如下，选[是]进行安装。




安装完毕后，会有证书[导入成功]的提示。如下图：


[根证书]的安装一般只在第一次登录时需要安装，安装成功后，下次登录在[安全警报]处，询问是否继续时，直接点[是]即可。

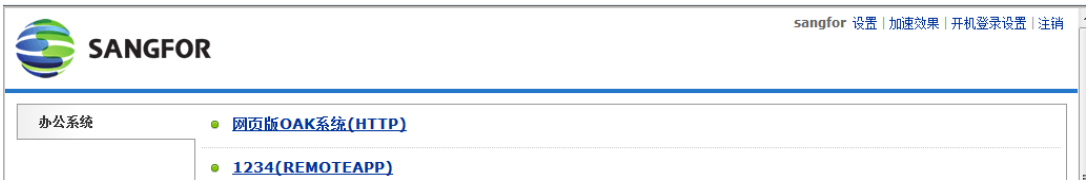
安装好根证书等之后，即进入以下欢迎页面：


输入用户名密码及校验码后，点击 登录，即可登陆 SSL VPN。

『证书登录』连接用于数字证书认证用户登录（数字证书手动安装在 IE 上的用户）。

『USB-Key 登录』用于使用 USB-Key 认证的用户登录（包括有驱 USB-Key 和无驱 USB-Key）。

登录成功后会出现 SSL VPN 资源列表界面如下：

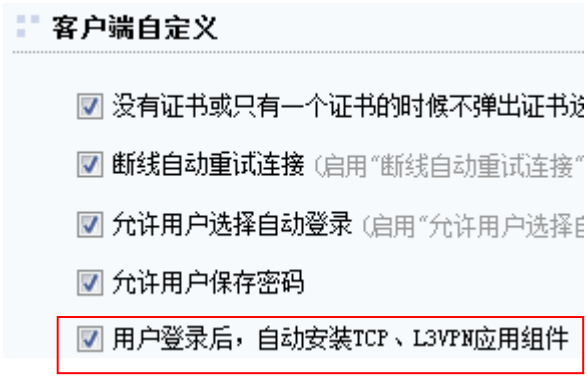



界面会显示该 SSL VPN 用户可用的 SSL VPN 内网资源列表，对于 Web 类型或 B/S 结构的资源，直接点击资源列表中的超链接即可访问，对于其它 C/S 结构的资源，则可直接打开 Client 客户端，通过连接服务器的内网 IP 来访问。

如果登录 SSL VPN 的用户需要访问总部定义好的『TCP 应用』和『L3VPN 应用』，则登录

成功后，会自动安装控件或者需要点击 启用 TCP 服务控件 和 启用 L3VPN 服务控件，如下图所示：

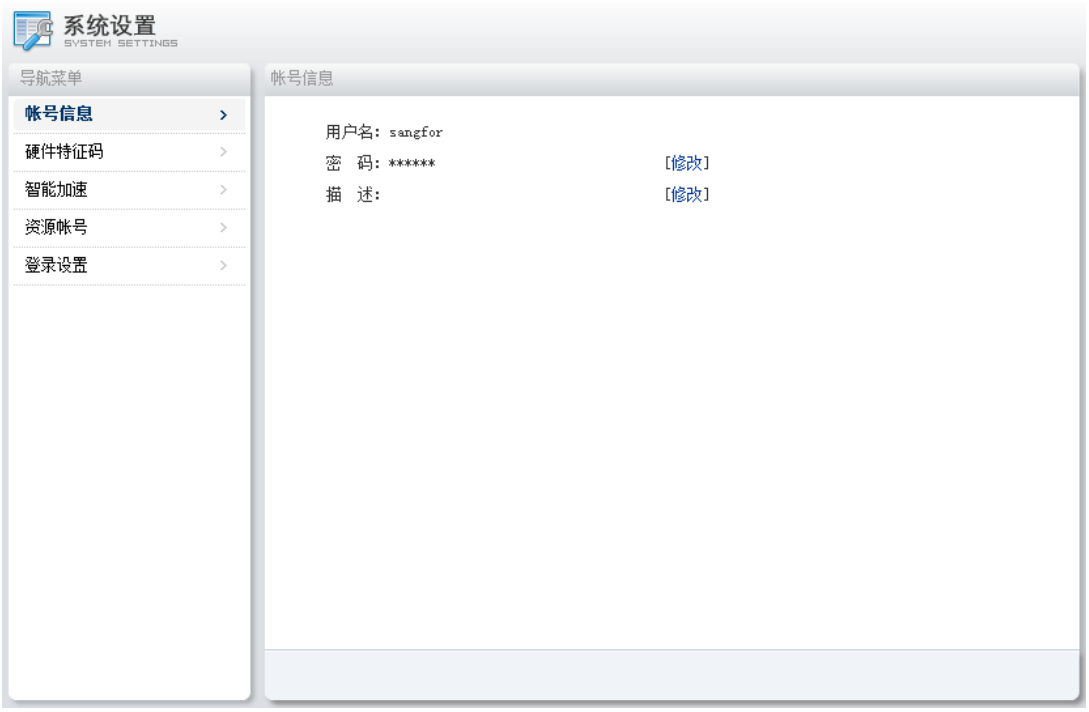

**注：若在『系统设置』→『SSL VPN 选项』→『系统选项』→『客户端选项』，勾选了用户登录后，自动安装 TCP、L3VPN 应用组件，那么 SSL 客户端登陆时，会自动安装上述两个组件。若没有勾选，则需要在上述页面手动安装。如下图：**




至此，完成了一次 SSL VPN 用户登陆的过程。

需要退出 SSL VPN 时，点击右上角的 注销 按钮，即可安全退出 SSL VPN。注销之后，用户将不能访问 SSL VPN 的资源。

资源列表上方的 设置 按钮，可让用户自行修改密码，界面如下：




点击 [修改]，如下图所示：

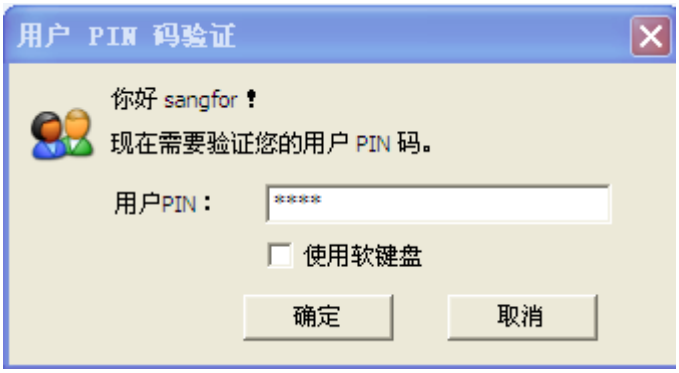

修改后，点击 保存 即可成功修改用户的登录密码。

**『系统设置』下，显示的内容与 SSL VPN 配置有关，请以实际显示的为准。**

对于使用 USB-KEY 的用户登录 SSL VPN 的过程，和普通用户登录稍有不同。

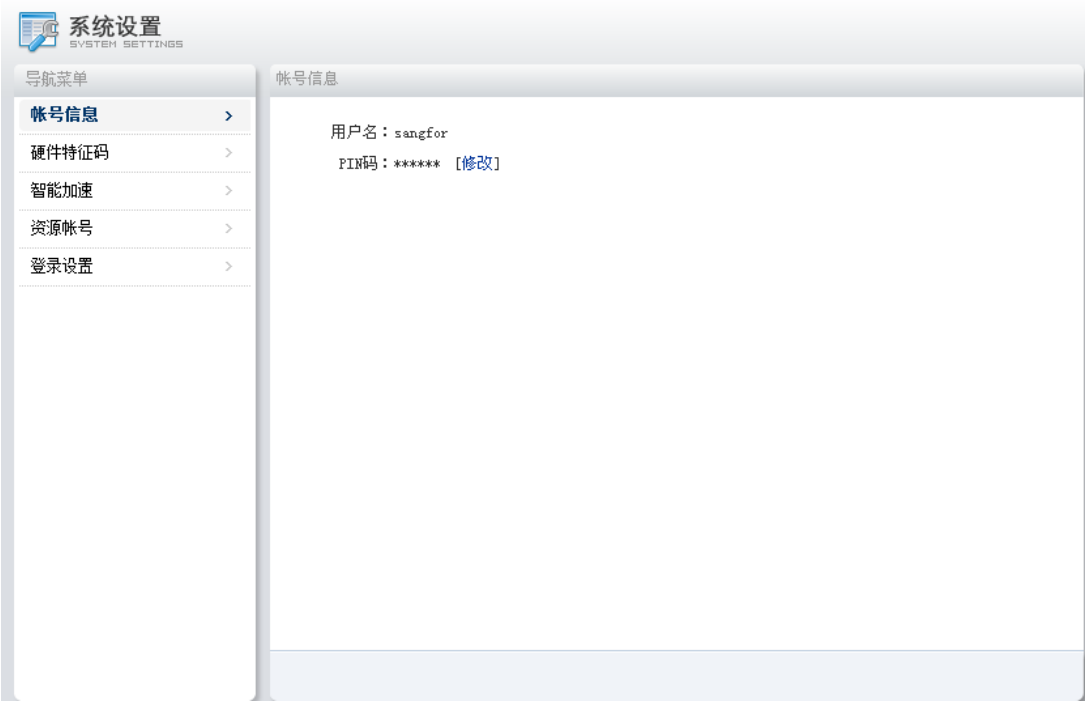
USB-KEY 用户登录时，打开浏览器输入 SSL VPN 登录网址，在登录界面处，插入 USB-Key，点击 USB-KEY 登录 即进入 USB-KEY 用户的登录界面，（或前面直接取消修改 PIN 的操作），

界面如下：

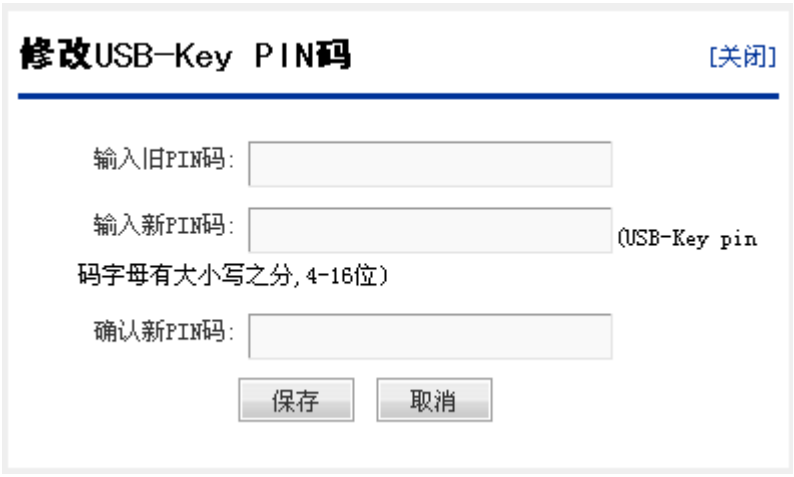



输入用户 USB-Key 的 PIN 码，设备会自动校验客户端信息，校验成功能，即远成 SSL VPN 客户端登陆。

USB-Key 用户登录后，点击资源列表上方的 设置 按钮，可让用户自行修改密码和 USB-Key 的 PIN 码，界面如下：




点击 修改，如下图所示：




输入[旧 PIN 码]和[新 PIN 码]，点击 保存 即修改成功。


**注意：登录 SSL VPN 之后，如果相隔一段时间，没有访问 SSL VPN 内网资源，或者客户端这边没有任何操作，SSL VPN 会超时，自动注销。超时时间设置请参考 4.5 章节。**

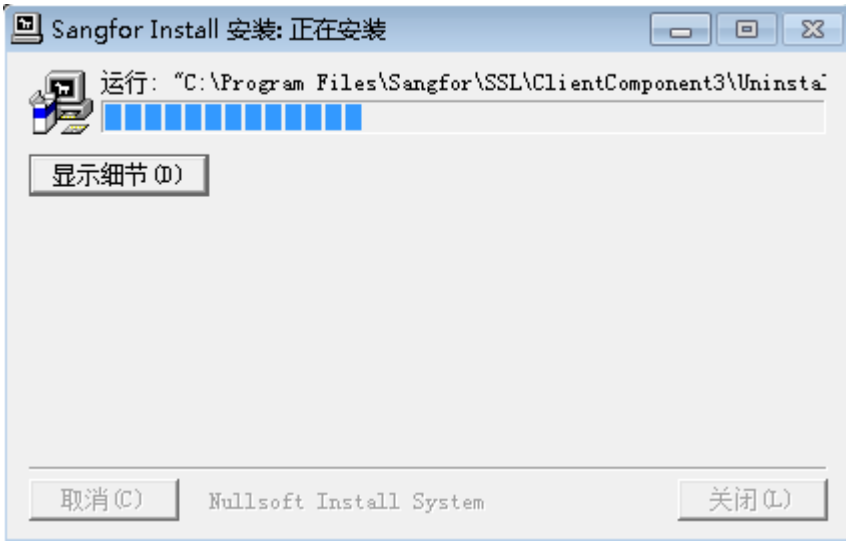
## 7.3. SSL VPN 客户端使用说明

用户通过 IE 登陆了 SSL VPN 后，会自动在电脑上安装 SSL VPN 客户端组件。

在『系统设置』→『SSL VPN 选项』→『系统选项』→『客户端选项』。可选择[由用户手动安装组件]或[自动安装组件]。若选择为手动安装，则在登陆时，会提示：


点击 下载客户端控件，弹出如下图提示：

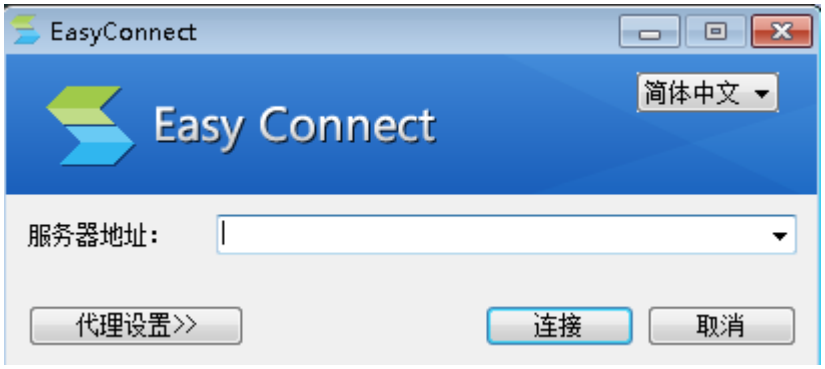

点击 运行，弹出安装界面：




下载并安装完成后，在开始->程序下可以找到如下目录：


**在安装 SSL VPN 组件的过程中，请先关闭本机的防火墙及杀毒软件，否则可能会安装不成功。**

选择[启动客户端]，即打开 SSL VPN 客户端程序，如下图：

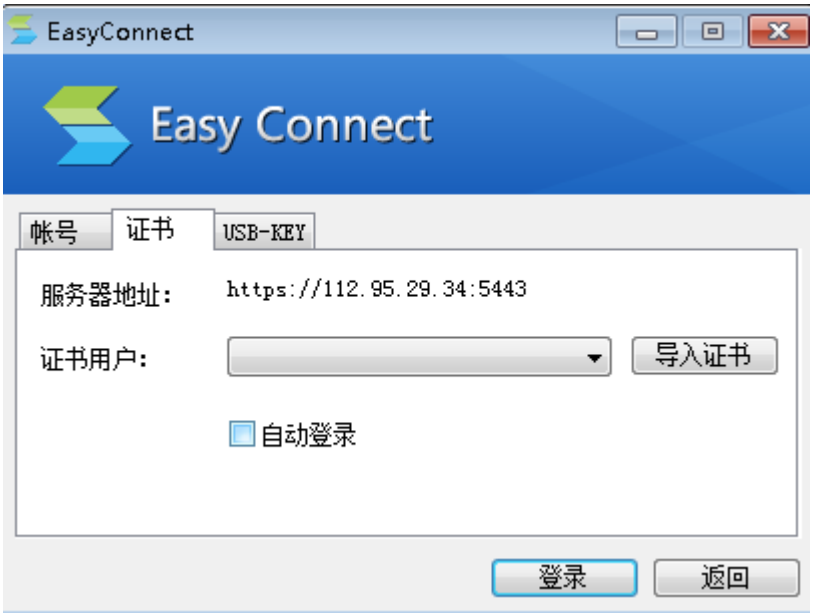



在『SSL VPN 地址』中输入连接 VPN 的地址，点击 连接，弹出【登录 SSL VPN】对话框。若为用户名密码登录，则选择【账号】，并在用户名和密码框中填入对应的“用户名”和“密码”。如下图：


**如果需要，用户可以勾选[记住密码]和[自动登陆]，那么下次点开 SSL VPN 客户端，不需再输一次地址和用户名密码，将自动连接到 SSL VPN。该项选择需要在设备上进行相应**

**的配置，具体可参考 3.5.1.2 章节。**

若为证书登陆，则选择【证书】如下图：




若为 USB-KEY 登陆，则选择为【USB-KEY】，并输入 USB-KEY 的 PIN 码。如下图：


**建立 SSL VPN 用户，请参考 4.1.2 章节。**

按实际情况选择上述中的一种登录方式，成功能登录后，有如下提示：

若在设备里设置了客户端启用系统托盘，则登录后在电脑桌面的右下角显示 SSL VPN 客户端图标，将鼠标移上去，显示 SSL VPN 的流速信息，如下图：


右击该图标，可查看 SSL VPN 状态及对 SSL VPN 进行相关设置，如下图：


**上图中显示的项与 SSL VPN 配置有关，以实际应用中显示的为准。**