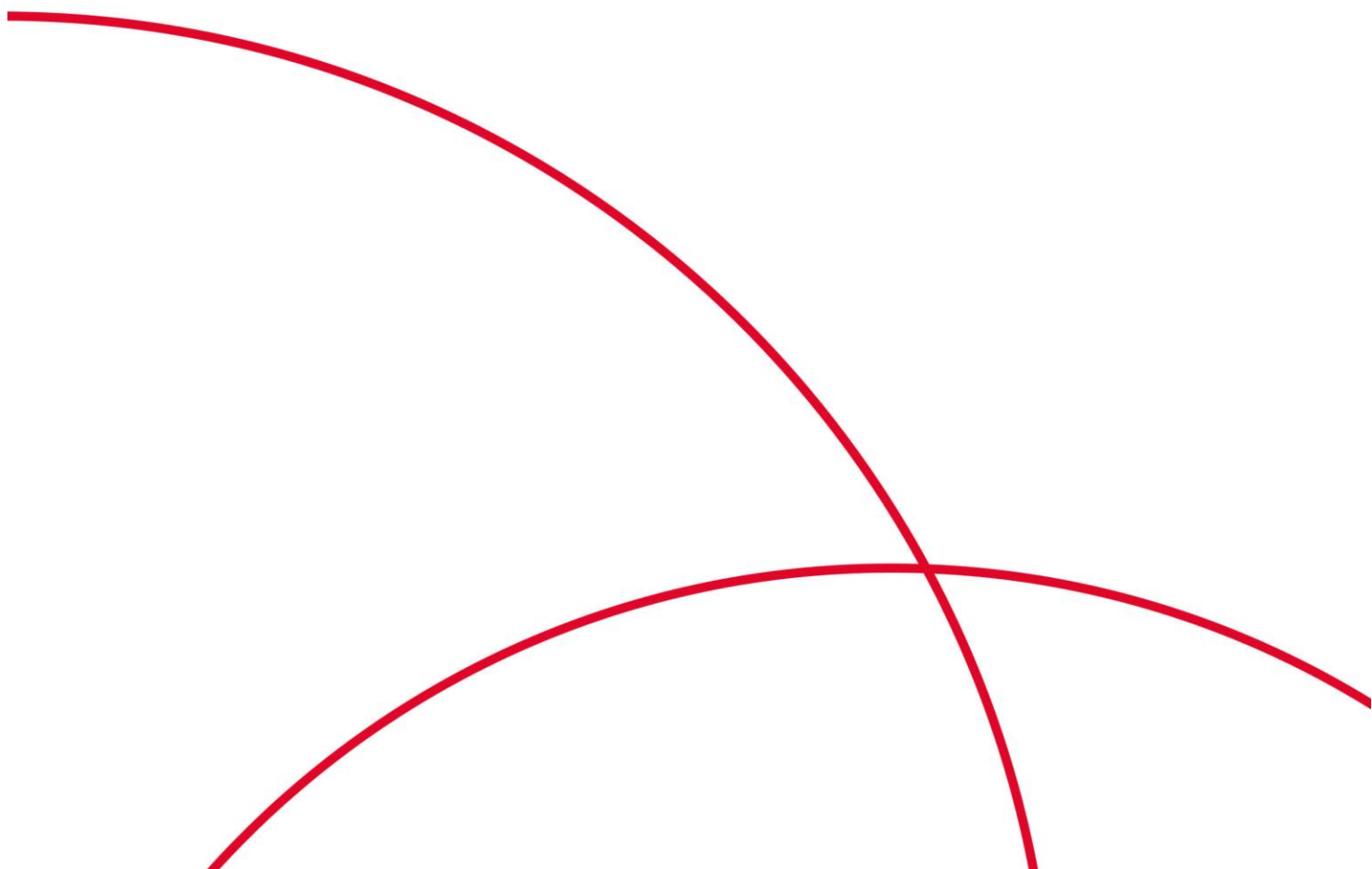




天翼云·SSL VPN

管理员手册

天翼云科技有限公司



第 1 章 前言.....	3
第 2 章 系统管理.....	3
2.1 设备登录.....	3
2.2 管理员配置.....	4
2.2.1 修改管理员密码.....	4
2.2.2 创建二级管理员.....	4
2.3 系统基本信息配置.....	7
2.3.1 授权信息.....	7
2.3.2 系统时间.....	7
2.3.3 控制台配置.....	8
2.3.4 设备配置备份与恢复.....	8
第 3 章 SSL VPN 配置.....	9
3.1 用户管理.....	9
3.1.1 批量导入用户.....	9
3.1.2 手动创建用户.....	11
3.2 资源管理.....	13
3.2.1 手动创建资源.....	13
3.3 角色授权.....	15
3.4 内网域名解析设置.....	15
3.5 其他设置.....	17
3.5.1 密码安全策略.....	17
3.5.2 开启防暴力破解选项.....	18

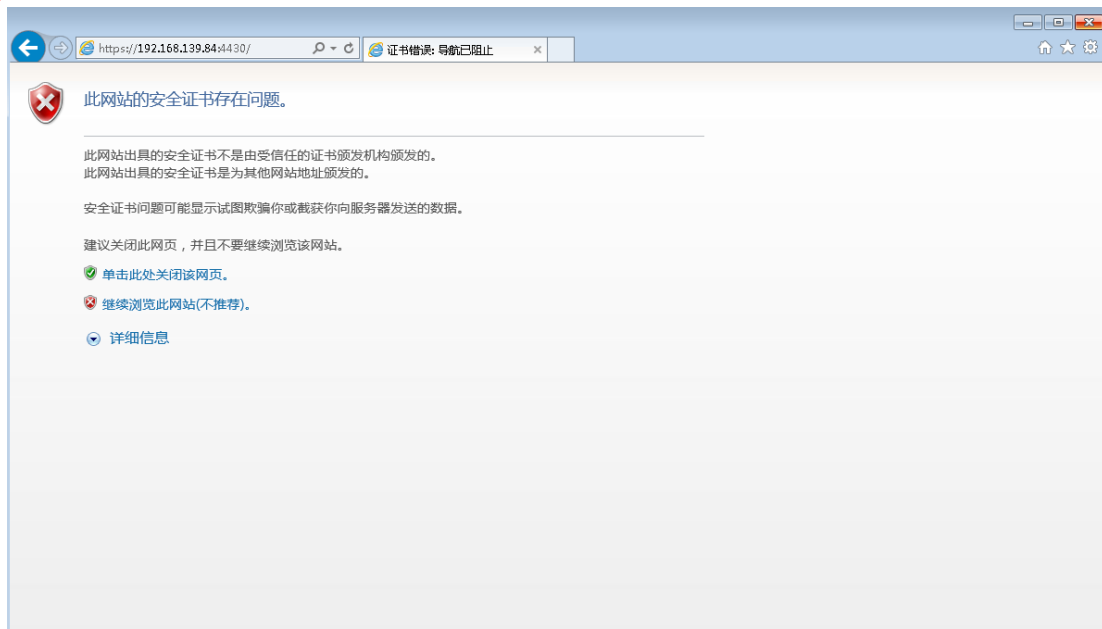
第1章 前言

本手册用于讲解 SSL VPN 常见功能操作方法，为管理员提供日常策略维护指导。

第2章 系统管理

2.1 设备登录

首先确保本机从网络可以访问到设备管理 IP 地址，然后在浏览器中输入网关的 IP 及端口 <https://192.x.x.x:4430>。出现一个如下图的安全提示：

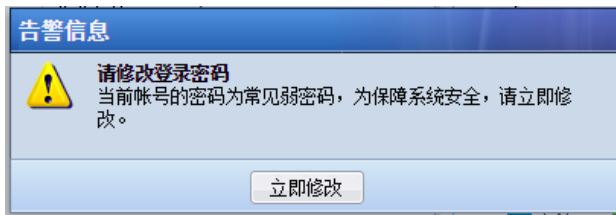


点击 <继续浏览此网站(不推荐)> 后出现以下的登录界面：



在登陆框输入『用户名』和『密码』，点击<登录>按钮即可登录 SSL VPN 设备进行配置，默认情况下的用户名和密码均为 admin。

如果用户密码过于简单,则会被检测为弱密码,在控制台的处理为:登录后检测为弱密码则提示修改密码,则会弹出如下提示:



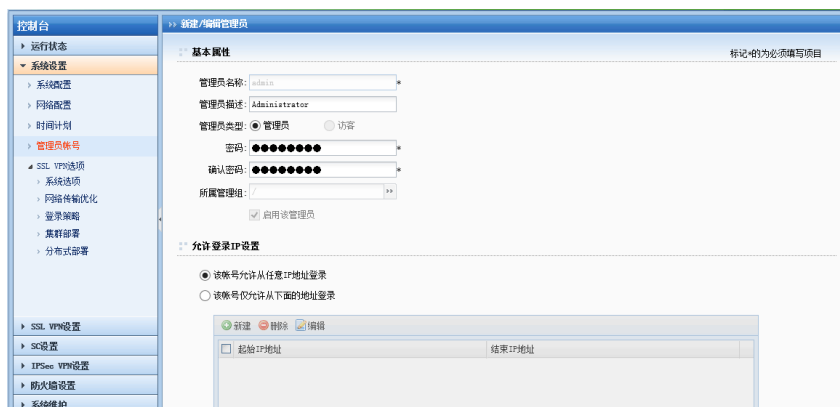
2.2 管理员配置

在『系统设置』-『管理员账号』页面，可修改 admin 管理员密码、删除管理员账号以及创建二级管理员。

2.2.1 修改管理员密码

管理员账号页面找到 admin 管理员，直接点击<编辑>，设置新密码即可修改 admin 账号的密码信息。

注：admin 账号只可修改密码，不可删除。

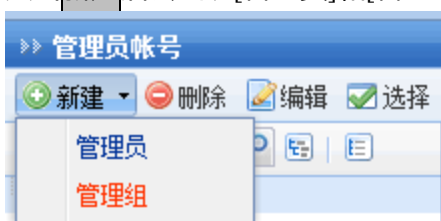


2.2.2 创建二级管理员

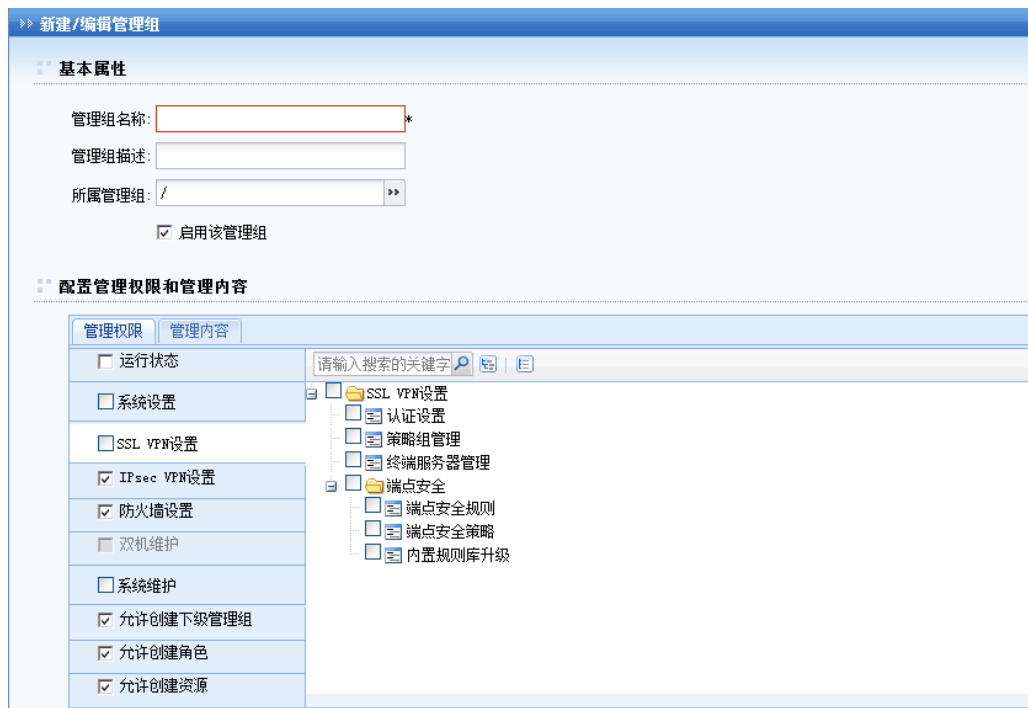
在管理员账户页面，可以创建二级管理员，设置不同的管理员可以管理不同的用户、资源以及角色等内容。

创建管理组

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：



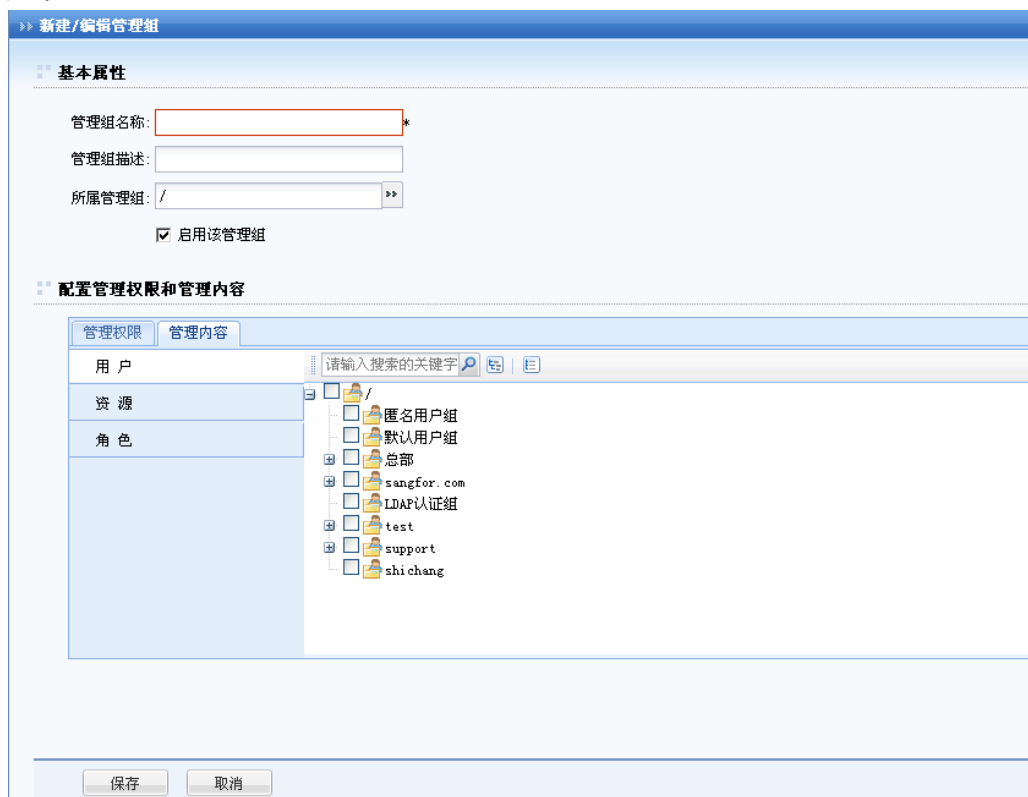
『管理组名称』和『管理组描述』可自定义。

『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：



创建管理员

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。

注：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；
- (4) 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。

2.3 系统基本信息配置

2.3.1 授权信息

在『系统设置』-『系统配置』-『序列号管理』页面，可以查看设备当前的授权信息。



2.3.2 系统时间

『系统设置』-『系统配置』-『日期与时间』用于设定 SANGFOR 设备的系统时间。可以直接在界面上修改时间，也可以选择<自动与时间服务器>进行时间的同步。

注：设备日志记录的时间与系统时间相关，请注意确保设备系统时间的准确性，手动获取本地时间和系统时间会重启设备，请勿工作时间操作。



2.3.3 控制台配置

『系统设置』 - 『系统配置』 - 『控制台配置』用于设定 SSL 设备的设备名称、WEBUI 管理页面端口、超时时间以及远程维护支持选项。



注：为设备安全考虑，一般情况下建议禁用远程维护支持。

2.3.4 设备配置备份与恢复

『系统维护』 - 『配置备份/恢复』用于将设备已有的配置下载保存，或者是将已备份的配置文件恢复到设备中。



SSL 的配置包含全局配置和 SSL VPN 配置，都是点击<下载当前配置>进行下载，两者的区别是：

全局配置：包含 SSL 设备系统配置、网络配置、SSL VPN 设置、IPSEC VPN 配置以及防火墙设置等设备全部配置信息。导入全局配置时，设备需要重启。

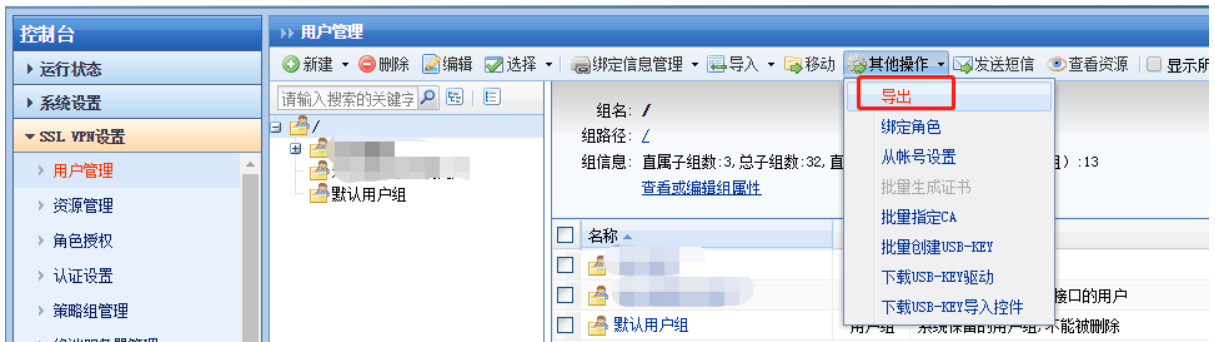
SSL VPN 配置：仅包含 SSL VPN 设置和 SSL VPN 选项的配置。导入 SSL VPN 配置时，设备仅重启 SVPN 相关服务。

第3章 SSL VPN 配置

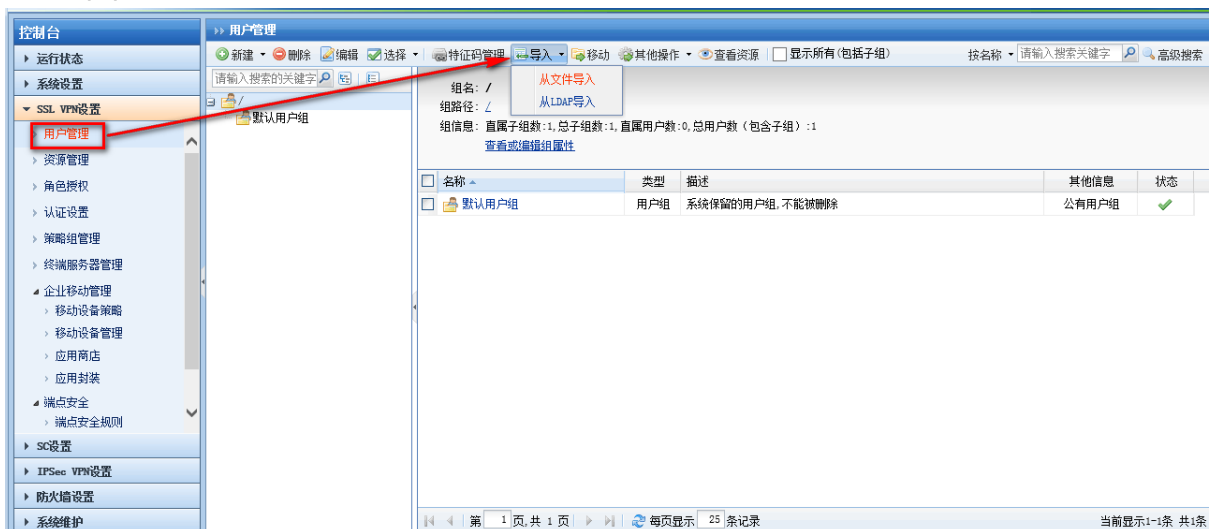
3.1 用户管理

3.1.1 批量导入用户

先在用户管理中创建模板用户，然后点击『其他操作』→『导出』，点击『选择导出内容』选择模板用户，导出模板 csv 文件，编辑 csv 文件，按照模板用户格式中添加其他用户信息。



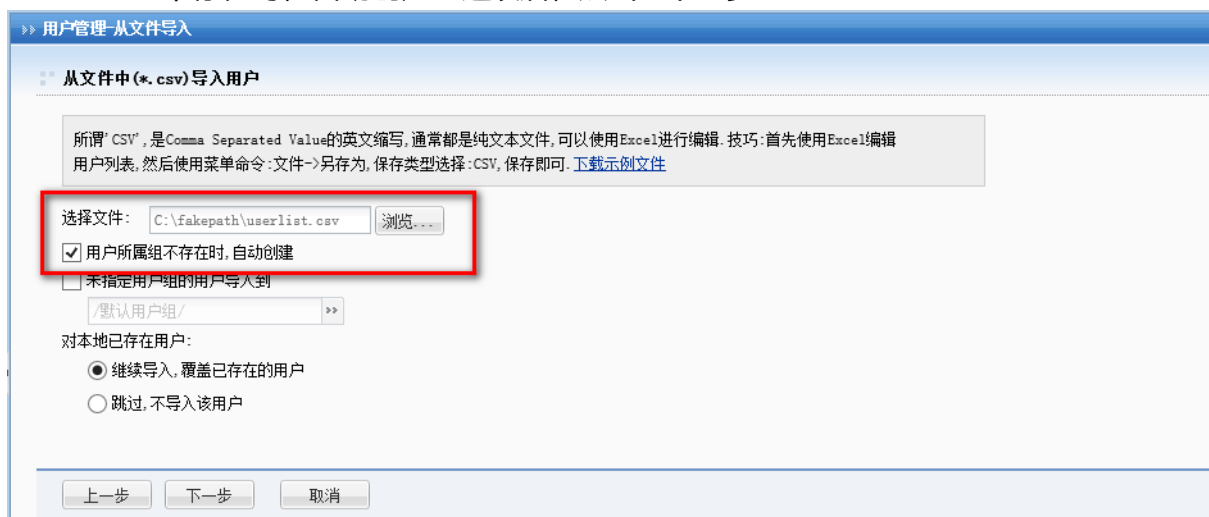
(1) 点击『SSLVPN 设置』→『用户管理』，点击『导入』→『从文件导入』；



(2) 选择“从文件中(*.csv)导入用户”，点击“下一步”；



(3) 在“选择文件”处，选择编辑好的用户信息表 csv 文件，同时勾选“用户所属组不存在时，自动创建”选项后，点击“下一步”



(4) 确认需要导入的用户信息没有问题后，点击“开始导入”。

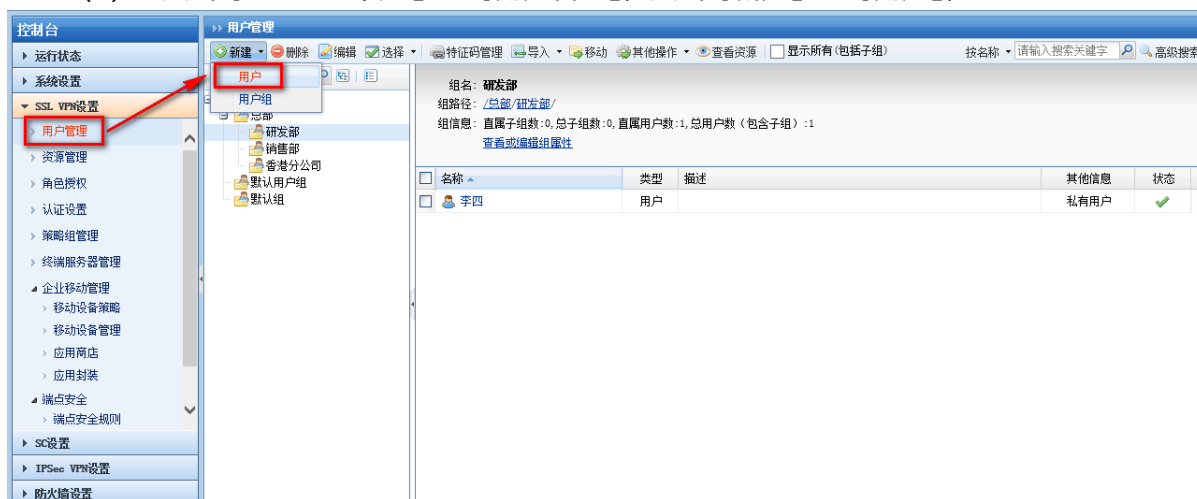


(5) 导入成功后，在用户管理页面可以看到导入成功的用户组以及相关用户。



3.1.2 手动创建用户

(1) 点击『SSLVPN 设置』→『用户管理』，点击『新建』→『用户』；



(2) 设置用户名、密码以及用户所属组后点击“保存”即可。

>> 新建用户

基本属性

名称: testuser X *

描述: _____

密码: ●●●●●●

确认密码: ●●●●●●

手机号码: _____

所属组: /总部/销售部 >>

继承所属组认证选项和策略组

继承所属组接入策略组

继承所属组认证选项

认证选项

账户类型: 公有用户 私有用户

主要认证

用户名/密码

数字证书/Dkey认证

外部认证 _____

多认证方式: 同时使用 任意一种

辅助认证

硬件特征码

短信认证

动态令牌 _____

接入策略组

策略组选用: 默认策略组 >>

关联角色

关联角色: _____ [新建角色并关联](#)

数字证书/USB-KEY: 无

虚拟IP: 自动获取 手动设置 0.0.0.0

过期时间: 永不过期 手动设置 2021-11-02

账户状态: 启用 禁用

离线访问: 接入策略未启用离线访问

所属组信息在点击新建用户时，可提前选择指定组，则新建的用户会自动选择该组。

>> 用户管理

新建 删除 编辑 选择 特征码管理 导入 移动 其他操作 查看资源 显示所有(包括子组) 按名称 请输入搜索关键字 高级搜索

请输入搜索关键字

组名: 销售部

组路径: /总部/销售部/

组信息: 直属子组数:0, 总子组数:0, 直属用户数:2, 总用户数(包含子组):2

[查看或编辑组属性](#)

名称	类型	描述	其他信息	状态
testuser	用户		私有用户	✓
王五	用户	销售同事	私有用户	✓

注:

- (1) 用户或用户组导入成功后，缺省会继承上级组的组属性，如果需要调整用户组的认证方式和账户类型，可单独编辑用户或用户组进行修改，如下图:

修改用户组

基本属性

名称: 总部 *

描述:

所属组: /

最大并发用户数: 0 (0表示不限制)

账户状态: 启用 禁用

继承上级用户组关联角色、认证方式和策略组

继承上级用户组认证方式

继承上级用户组策略组

继承上级用户组关联角色

认证选项

账户类型: 公有用户组 私有用户组

主要认证

用户名/密码

数字证书/Dkey认证

外部认证

多认证方式: 同时使用 任意一种

辅助认证

硬件特征码

短信认证

动态令牌

(2) 公有用户和私有用户的区别:

公共用户: 该类型账户允许多人同时登陆, 用户登录后不可修改自己的密码等属性, 公有用户不可选择证书认证和短信认证。

私有用户: 私有用户同一时间仅允许同一用户在线, 本地密码认证的私有用户可在登录后修改自己的密码、手机号码、描述等信息。

3.2 资源管理

3.2.1 手动创建资源

- (1) 在『资源管理』页面, 点击新建按钮, VPN 设备提供三种四种类型资源可选, 为支持移动终端 VPN 直连业务系统, 本次资源全部选择 L3VPN 类型, 如下图:



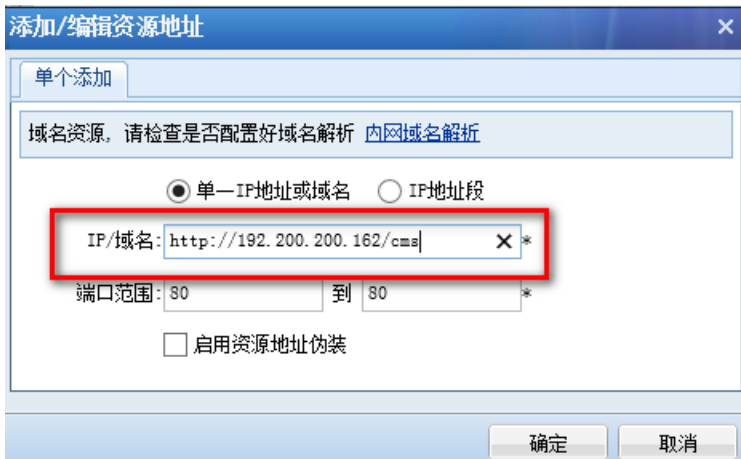
(2) 选择一种应用类型，如[L3VPN]，弹出『编辑 L3VPN 资源』对话框，设置界面如下：



(3) 设置资源名称，设备预定义了一些资源类型，如果没有可选择 Other 即可，选择协议类型以及地址，保存立即生效即可。

注：

- (1) 非必要场景（无插件），不建议使用 web 应用添加资源。
- (2) HTTP 类型的系统，如果访问地址有带文件路径，在创建资源时，地址列表应该填写带 HTTP 前缀的完整路径，如下图：



(3) 资源类型说明：

WEB 应用：支持无任何插件的 WEB 资源，建议仅对移动终端开放。

TCP 应用：支持 TCP 协议的业务，如果没有移动终端接入需求，大部分 TCP 协议的应用建议使用该类型的资源，如 HTTP、FTP 等。

L3VPN：使用隧道支持全 IP 协议，支持 TCP、UDP、ICMP 等应用，支持 Android4.0，IOS9.0 以上版本的移动终端的 VPN 接入，如需考虑移动终端接入，建议使用该类型资源。

远程应用：需借助 Windows server 搭建终端服务器，可发布服务器上的应用程序访问内网系统。

3.3 角色授权

『角色授权』是“用户/用户组”和“资源”的中介，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。

例如，研发部仅允许访问公司门户和知识管理系统，销售部可以访问公司门户和 CRM 系统等禁止外发上网策略配置，具体配置如下：

(1) 在『SSL VPN 设置』→『角色授权』，点击新建角色。



(2) 在新建角色页面，『关联用户』处选择授权用户，例如关联研发部，『授权资源列表』处编辑资源授权列表，关联公司门户和知识管理系统两个资源。



3.4 内网域名解析设置

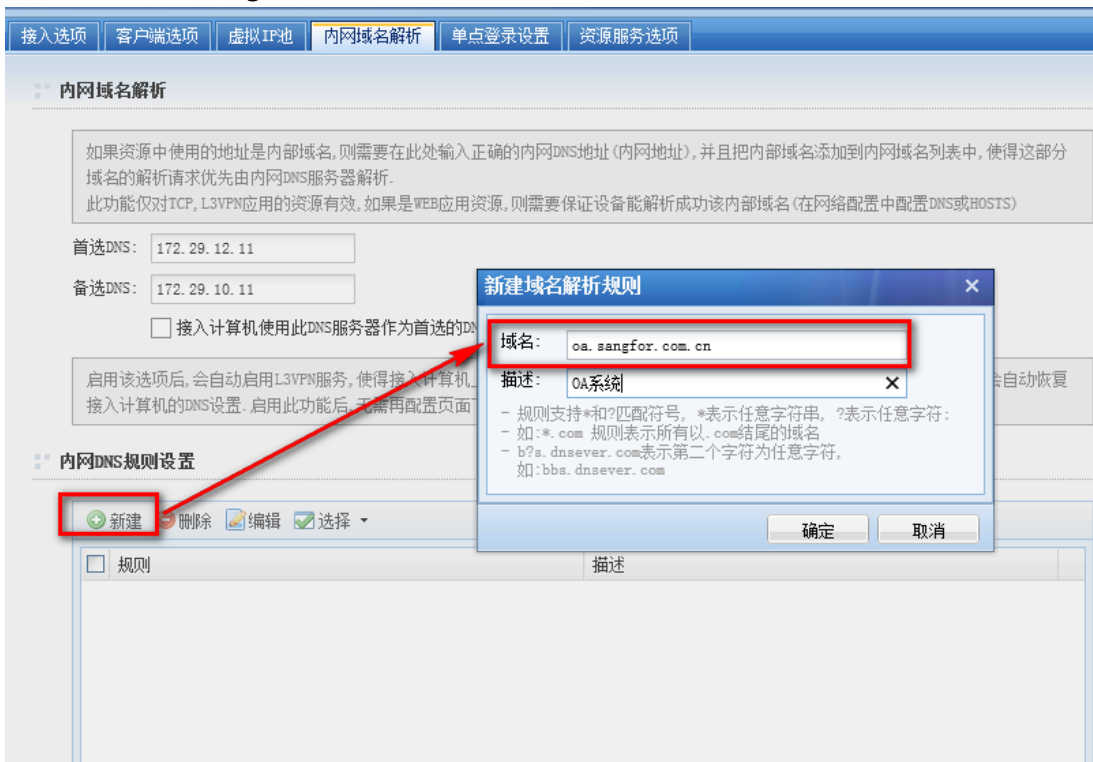
SSL VPN 支持需要通过内部域名才能访问的资源应用。内网存在此类应用时，一般有一台或

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

- (1) 在『系统设置』→『SSL VPN 选项』→『系统选项』，选择『内网域名解析』选项卡，在首选和备选 DNS 处设置客户的内网 DNS 服务器地址，如下图内网 DNS 为 172.29.12.11 和 172.29.10.11。



- (2) 在此页面『内网 DNS 规则设置』处，将定义资源的域名全部在此处添加，如 oa.sangfor.com.cn。



注:

- (1) 此处添加的规则最多支持 100 条；不支持中文域名解析

- (2) 添加内网 DNS 规则后，对应域名的解析请求，会优先走内网 DNS 解析，未通过 VPN 发布的域名，请不要在此添加任何规则！

3.5 其他设置

3.5.1 密码安全策略

密码安全策略可以要求用户必须修改初始密码，并且满足密码复杂度要求。

- (1) 在『认证设置』→『主要认证』→『本地密码认证』设置页面



- (2) 勾选“启用密码安全策略”，并开启响应复杂度要求。



3.5.2 开启防暴力破解选项

防暴力破解可以避免恶意用户暴力破解 SSL 账号，入侵内网系统。

(1) 在『认证设置』→『认证选项设置』→『密码认证选项』设置页面



控制台

- 运行状态
- 系统设置
- SSL VPN设置
 - 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
 - 移动设备策略
 - 移动设备管理
 - 应用商店
 - 应用封装
 - 端点安全
 - 端点安全规则
 - 端点安全策略
 - 内置规则库升级
- SC设置
- IPSec VPN设置
- 防火墙设置

认证设置

数字证书与CA中心, 创建证书及证书申请等. > 下载安装USB-KEY驱动 > 下载安装USB-KEY导入控件

域单点登录认证 设置
以实现域用户在客户端的自动登录, L2TP/PPTP的AD域认证和或安装控件功能.

辅助认证

短信验证码 设置
在用户登录时结合短信验证码进行认证准入的相关设置, 包括短信发送接口, 验证码信息格式等内容.

硬件特征码 设置
结合硬件特征码认证的相关设置, 包括硬件特征码的收集方式, 特征码审批程序等.

动态令牌认证 设置
动态令牌认证是Radius服务器的一种扩展使用.

认证选项设置

LDAP与Radius服务器认证优先级设置 设置
当配置了多个LDAP与Radius认证服务器时, 将依据该配置项中所设置的顺序优先级进行用户认证.

密码认证选项 设置
用户登录时密码输入选项与防暴力破解登录的相关设置, 对本地密码认证和LDAP认证以及Radius认证同时生效.

匿名登录设置 设置
匿名登录权限设置与角色授权设置.

(2) 勾选防暴力破解选项下的三个选项。



密码认证选项设置

用户登录时校验选项

启用软键盘 (防止木马记录键盘输入信息)
 字母键随机变化 数字键随机变化

防止暴力破解选项

连续登录错误 次, 启用图形验证码 (输入0表示强制启用; 小于3时, 非windows客户端仍然以3次为标准)

同名用户登录连续出错 (1-32)次后锁定用户 (30-1800)秒后恢复正常状态 (仅针对本地用户有效)

同IP用户登录连续出错 (64-2048)次后拒绝同IP登录, 并在 (30-1800)秒后恢复正常状态

1. 登录连续出错是指两次登录错误间隔在45秒之内;
 2. 同名用户登录连续出错次数设置范围为1至32次;
 3. 同IP用户登录连续出错次数设置范围为64至2048次;
 4. 恢复正常状态时间值设置范围为30至1800秒, 0表示永久锁定, 需管理员手动释放.

保存 取消