中安云科 IPSEC/SSL VPN 综合安全网关网关
用户操作手册

中安云科科技发展（山东）有限公司

2023 年 04 月 20 日

目录

1. 手册指南

1.1. 概述

本手册主要介绍中安云科 IPSEC/SSL VPN 综合安全网关网关的使用及维护。其中涵盖了中安云科 IPSEC/SSL VPN 综合安全网关网关所涉及的配置方法及其使用说明。

我们将以提供具体实例的方法来引导使用者安装配置符合自己应用环境的网关。

1.2. 目的

本手册详细描述了如何部署、配置、管理和使用中安云科 IPSEC/SSL VPN 综合安全网关网关，目的是指导用户能正确的管理和使用本产品。

1.3. 适用对象

本手册适用对象为网络管理员、网关实施人员、售前支持人员和技术支持人员，需要具备以下概念知识：

(1) 网络拓扑

(2) 网络地址和路由

(3) 数字证书、VPN、HTTPS

(4) Web 服务器

1.4. 名词解释

虚拟局域网（VPN）：虚拟专用网指的是依靠 ISP（Internet 服务提供商）和其它 NSP（网络服务提供商），在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。

SSL VPN：应用层的一种 VPN，一般以客户端与服务端形式存在，一般用于认证客户端身份和加密应用层数据，例如对 WEB 资源进行访问控制，并对其进行数据加密。

证书认证机构（Certificate Authority）：一个产生和确定公开密钥证书的可靠和可信的第三方机构。它发行数字证书并确保证书的可信性，或证明一个用户和它们的公共密钥的身份。认证机构也可以为实体产生和确定密钥。习惯上又称作认证中心（CA）。

数字证书（Certificate）：数字证书中心签发的用于代表实体身份的一段电文。本手册中涉及代表用户身份的用户证书和代表服务端身份的站点证书（服务器证书）。

LDAP：(Lightweight Directory Access Protocol)是一种轻量级的目录存取协定，提供客户从各个角落连接到目录服务器中。本手册中专指 CA 用于发布证书及黑名单的 LDAP 服务。

黑名单：通常所说的 CRL（Certificate Revoke List），因时间或者安全原因被废除的证书列表，一般发布在 LDAP 上。

2. 环境说明

本章讲述安装中安云科 IPSEC/SSL VPN 综合安全网关网关需要进行的工作和步骤，以及正式配置前的环境准备工作。

2.1. 产品检查

在安装中安云科 IPSEC/SSL VPN 综合安全网关网关之前应对照着产品清单确保所有部件都已存在，并检查所有部件是否完好。如果有任何部件缺少或者损坏，请不要进行安装，应立即与厂商进行联系。

2.2. 默认网络配置

网络接口	用途	出厂接口地址
eth0	管理口	192.168.5.10
eth1	应用口	192.168.6.10
eth2	应用口	192.168.7.10
eth3	应用口	192.168.8.10
…	…	…

注：如果 5 个及以上网口均按照以上结构进行出厂配置

2.3. 环境准备

1）中安云科 IPSEC/SSL VPN 综合安全网关网关产品工作环境：

工作温度：0 ℃--40℃

存储温度：-40℃--70℃

工作湿度：5%--95%RH，不凝结

工作电源：100--240VAC，50-60Hz

2）中安云科 IPSEC/SSL VPN 综合安全网关网关工作时需要以下连接线接入设备：

- 2 根电源线。（连接电源时所需）
- 连接外网口与外部网络的 RJ-45 网线。（接入 WAN 接口时所需）
- 连接内网口与内部服务器网络的 RJ-45 网线。（接入 LAN 接口）
- 连接管理口接口的 RJ-45 网线（接入管理口时所需）

2.4. 开机

确保连接线连接无误后，打开设备后面板的电源开关，开机后会发出刺耳响声，按一下面板后面的红色按钮即可。

启动约为 1 分钟。一旦设备加电，则系统前面板上的指示灯将显示系统的状态：

- 电源灯闪烁显示系统加电成功
- 磁盘灯亮表示正在读取磁盘
- 故障灯亮表示设备故障
- 运行状态灯闪烁表示运行正常

2.5. 关机

关闭中安云科 IPSEC/SSL VPN 综合安全网关网关电源即可。

3. 功能操作使用说明

在使用 VPN 配置管理系统进行管理之前，您需要完成下面的准备工作：

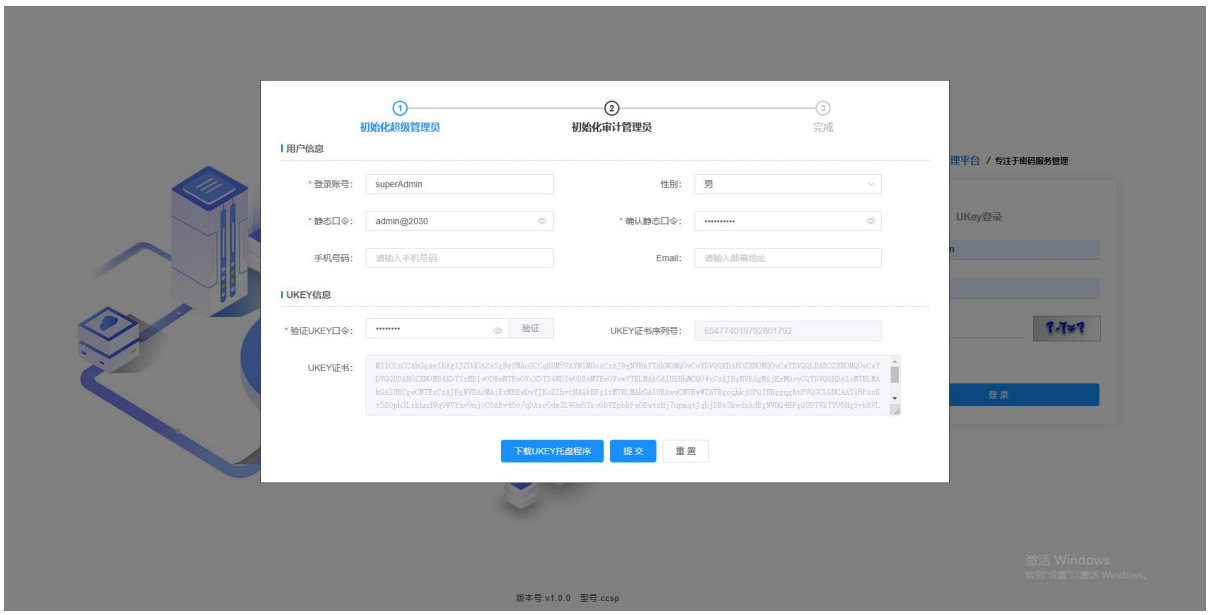
1、将中安云科 IPSEC/SSL VPN 综合安全网关网关开机。

2、使用网线将中安云科 IPSEC/SSL VPN 综合安全网关网关的 NET1(LAN)口，与计算机网卡相连。

3、将本地计算机的 IP 地址设置成与中安云科 IPSEC/SSL VPN 综合安全网关网关 NET1(LAN）口同一子网的地址（默认情况下，NET3 接口 IP 为 192.168.8.10）。

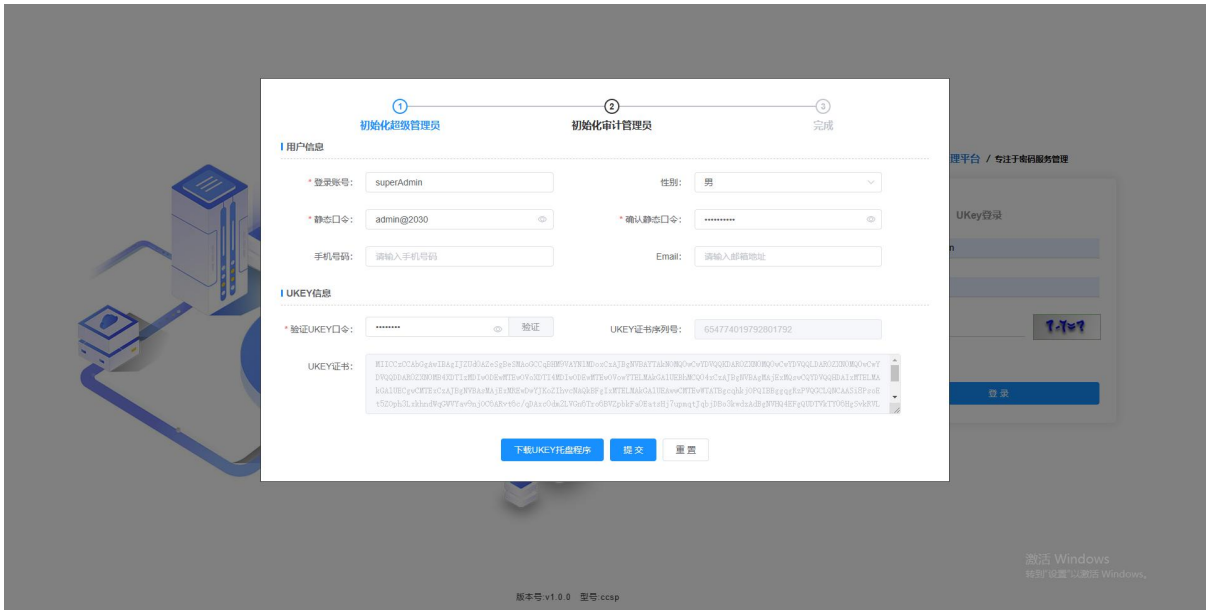
3.1 初始化

在初始化界面和登录页面选择 Ukey 登录界面，点击右下角【下载托盘程序】，即可在浏览器完成下载。下载完成后，解压压缩包，点击安装程序，根据提示安装即可。



3.1.1 初始化系统超级管理员

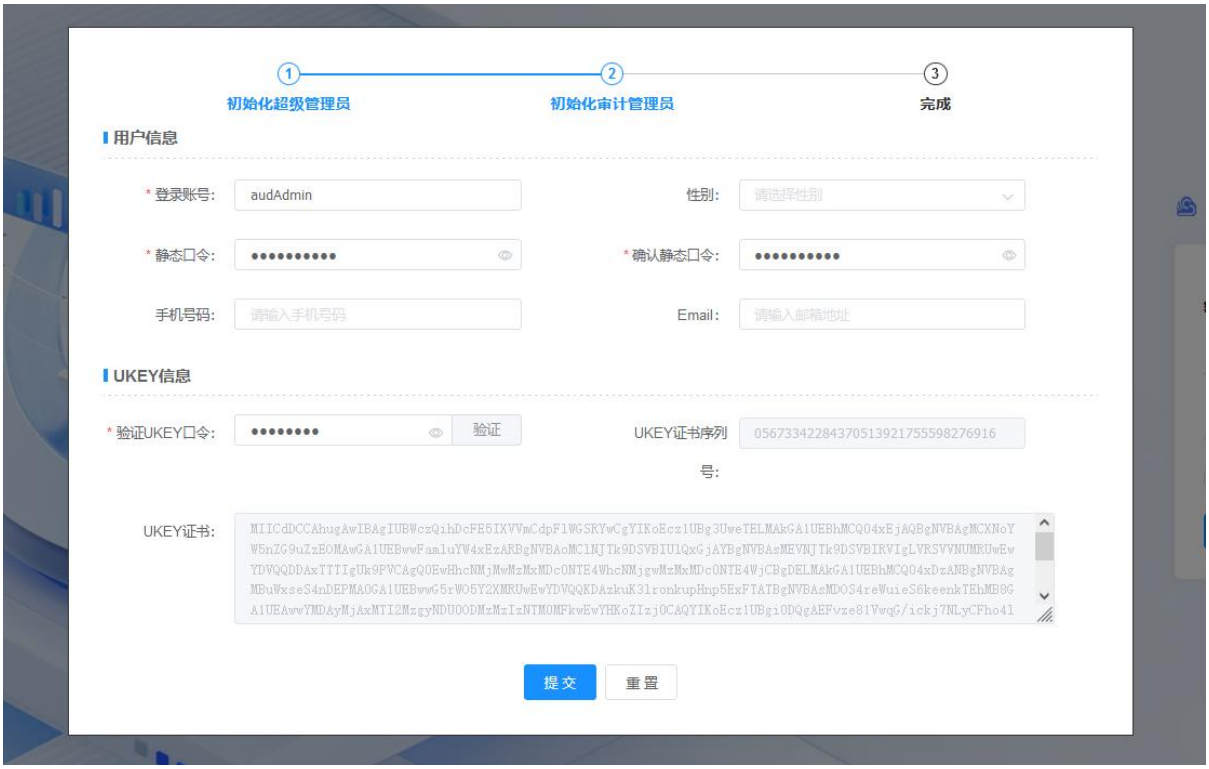
首先初始化系统超级管理员，将超级管理员 UKey 插入计算机的 USB 接口， 按照提示输入两次口令，点击“初始化超级管理员”，初始化成功后自动跳转到下一个页面。



3.1.2 初始化系统审计管理员

初始化完系统的超级管理员之后，会自动跳转到初始化系统审计管理员，初始化方式与

初始化系统超级管理员相同，初始化完毕后，自动跳转登陆界面。



3.2 SSL VPN 登录

管理员有两种登录方式分别是密码登录和 UKey 登录。

密码登录：点击【密码登录】，填写账号、密码、图片验证码，然后点击【登录】按钮，系统验证通过，进入服务器综合安全网关。

UKey 登录：点击【UKey 登录】，插入 Web 页面 Ukey，填写 PIN、密码，然后点击【登录】按钮，系统验证通过，进入服务器综合安全网关。

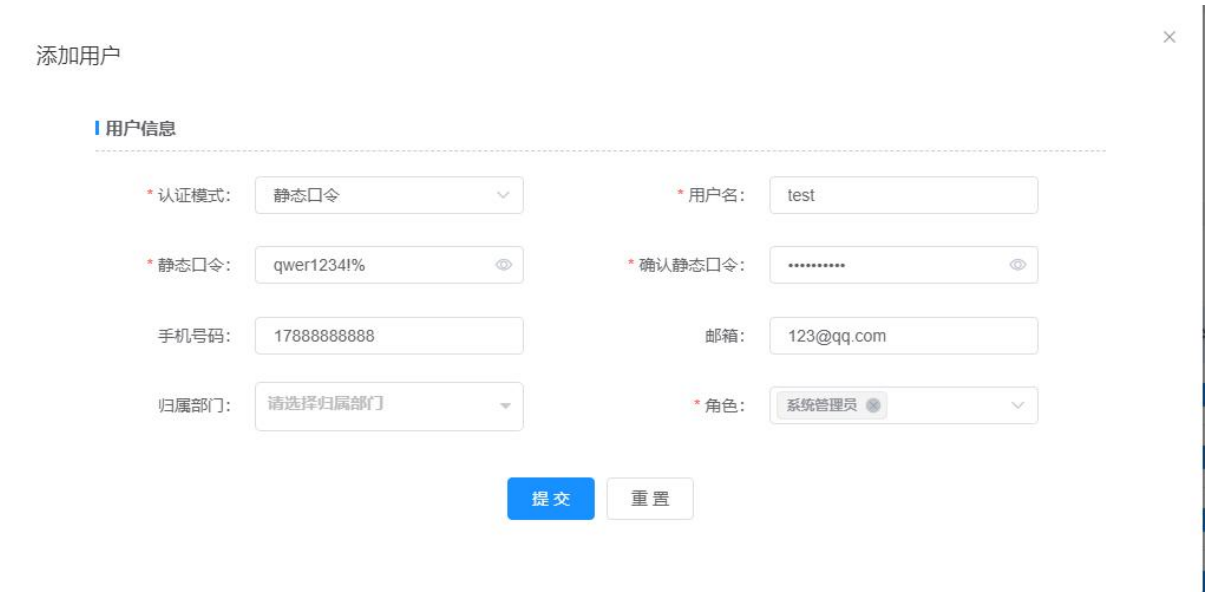
3.3 超级管理员用户

3.3.1 用户管理

管理员管理包括新建管理员、管理员列表。

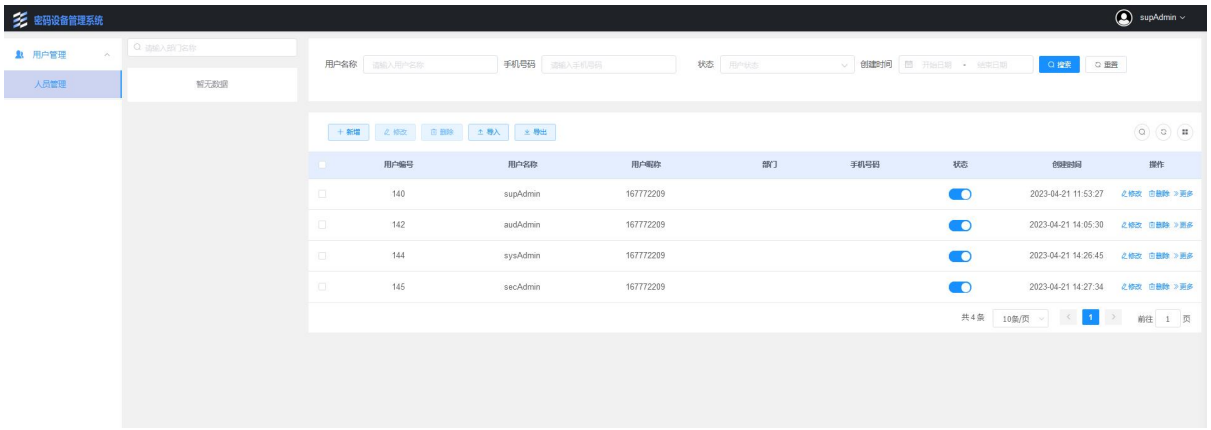
3.3.1.1 新增用户

点击【新增】，管理员类型可以选择系统管理员、系统安全管理员（注：这里新增管理员的时候，已经插在计算机上的超级管理员的 key 不动，直接将新的 key 插到计算机上即可），插入新的 key，选择要生成的管理员类型，输入口令，点击“提交”按钮，管理员生成成功。



3.3.1.2 人员列表

可以在管理员列表中查看生成的管理员，如下图所示。内容包括管理员的登录名、管理员类型、管理员状态。处于正常状态的管理员可以登录，处于锁定状态的管理员不可以登录。对于管理员 key 丢失的情况，我们可以对丢失的 key 的管理员进行锁定操作，以提高系统使用的安全性。



3.4 系统管理员用户

以系统管理员身份登陆 WEB 管理系统，该管理员用户下支持系统管理、系统监控、网口管理、防火墙、运维工具等功能，并支持查看

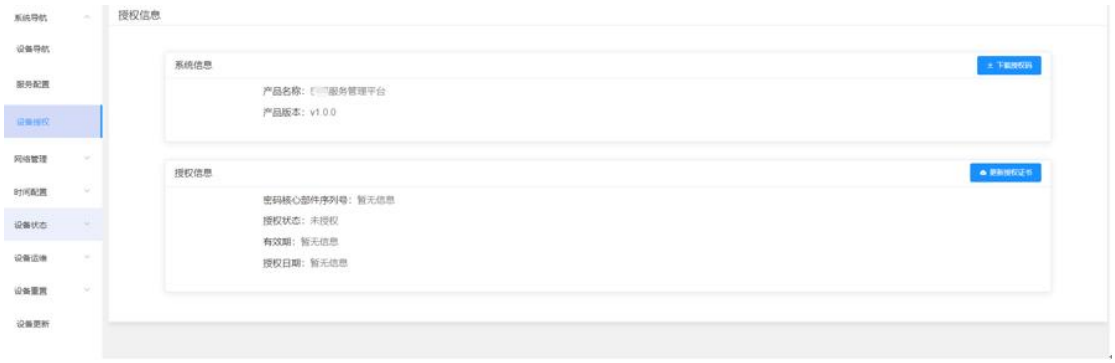
设备基础信息。

3.4.1 设备导航

可以进行系统配置的快捷跳转，以便更方便的进行操作。

3.4.2 设备授权

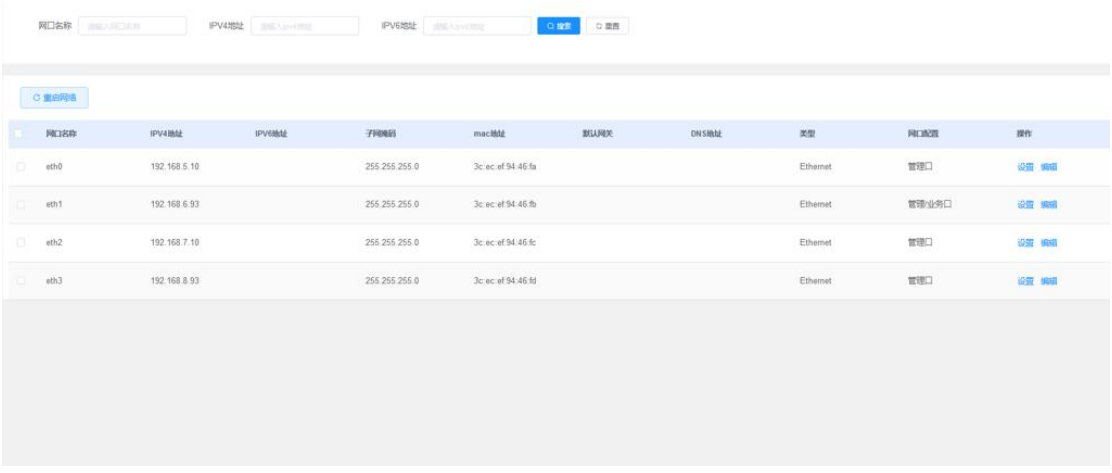
可以查看授权信息，下载授权码和更新授权证书。



3.4.3 网络管理

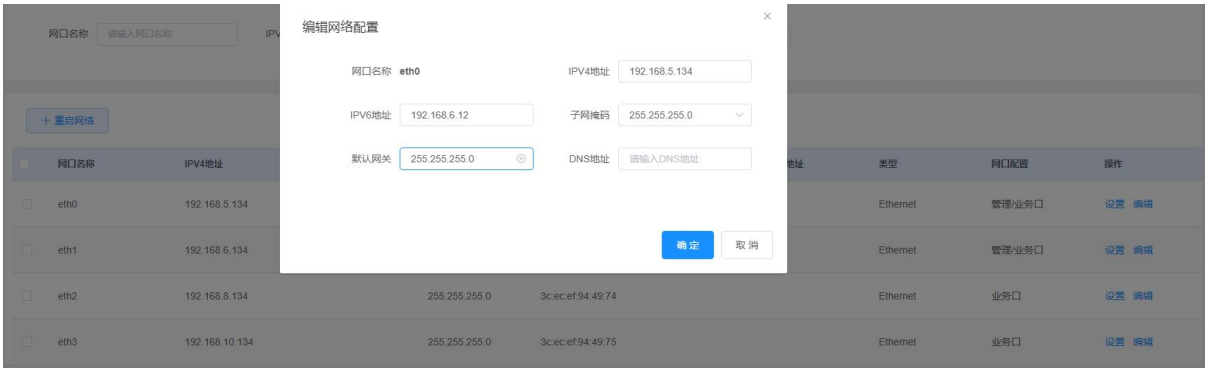
3.4.3.1 网络配置

点击【网络管理】，点击【网络配置】进入到网络配置页面。



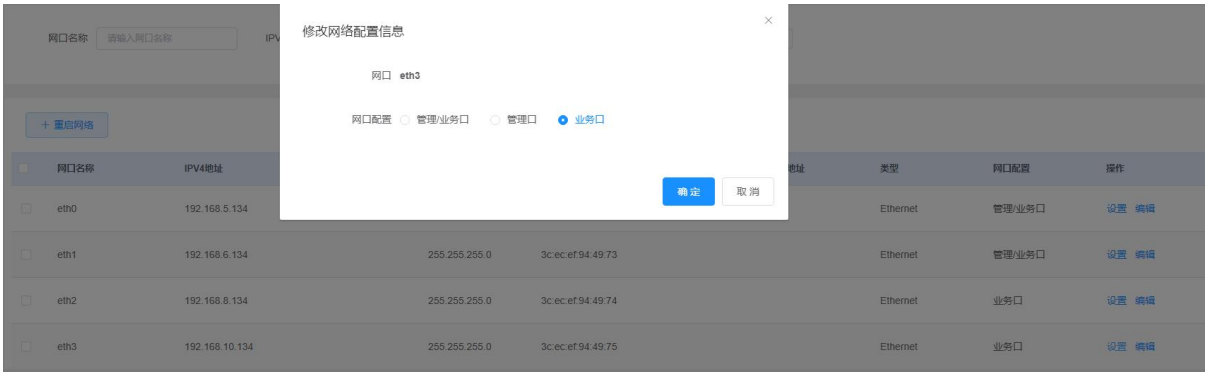
3.4.3.1.1 编辑

点击【编辑】，在弹出的对话框中可修改 IPV4 地址、IPV6 地址、子网掩码、默认网关、DNS 地址，然后【确认】完成编辑。注意每个的格式都要填写正确。点击重启后生效。



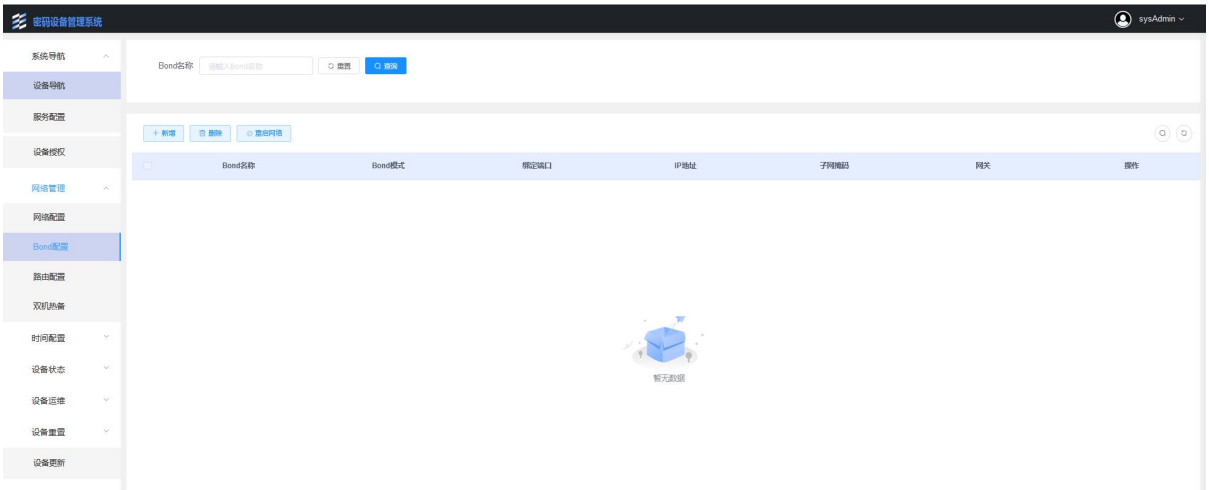
3.4.3.1.2 设置网口类型

点击【设置】，在弹出的对话框中可选择管理口、业务口，然后【确认】完成设置。点击重启后生效。



3.4.3.2 Bond 配置

点击【网络管理】，点击【Bond 配置】进入到 Bond 配置页面。

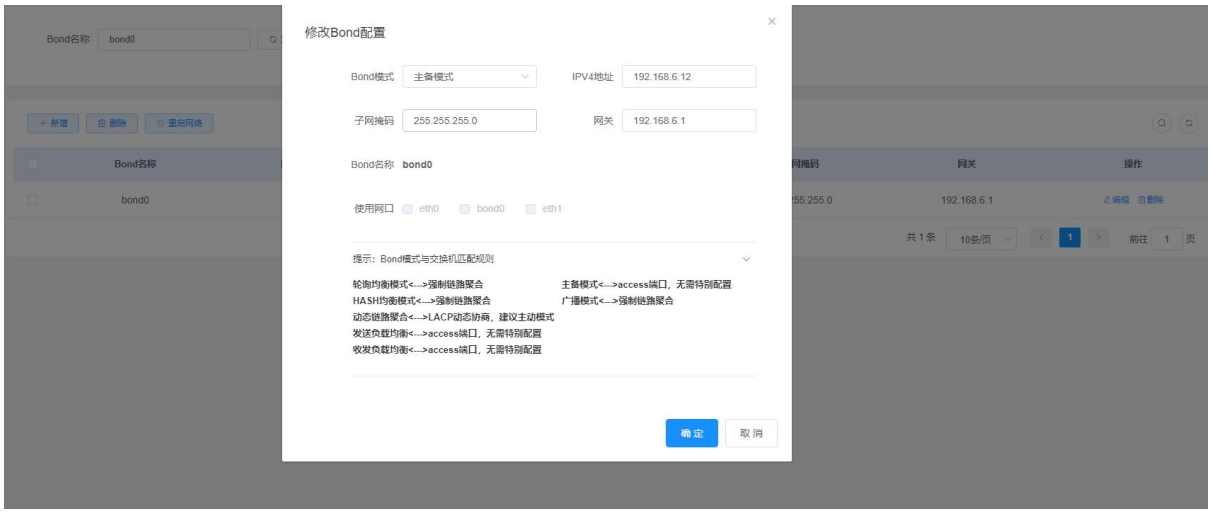


3.4.3.2.1 新增

点击【新增】，在弹出的对话框中选择 Bond 模式、子网掩码，输入 IPV4 地址、网关、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

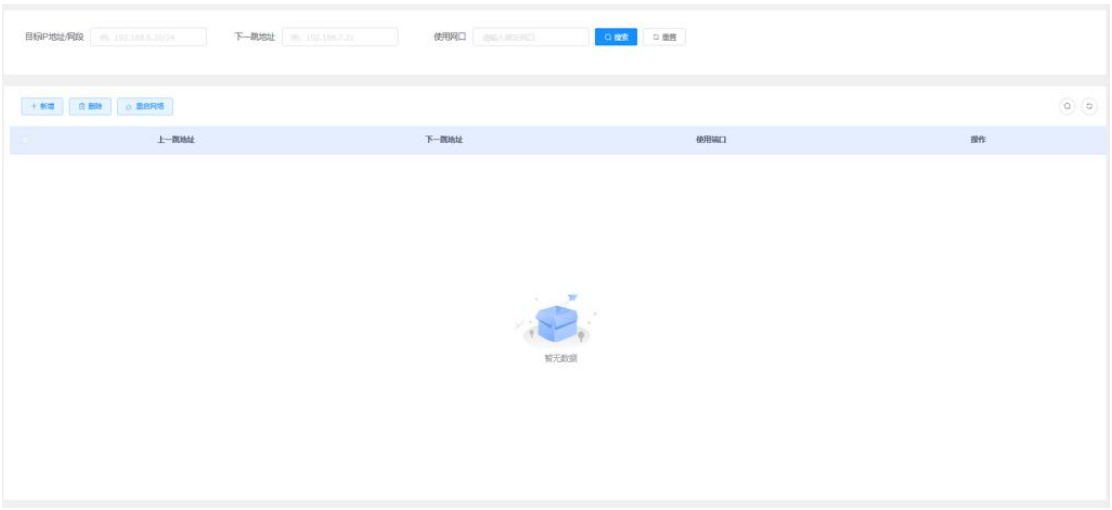
3.4.3.2.2 编辑

点击【编辑】，在弹出的对话框中可修改 Bond 模式、IPV4 地址、子网掩码、网关、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。



3.4.3.3 路由配置

点击【网络管理】，点击【路由配置】进入到路由配置页面。



3.4.3.3.1 新增

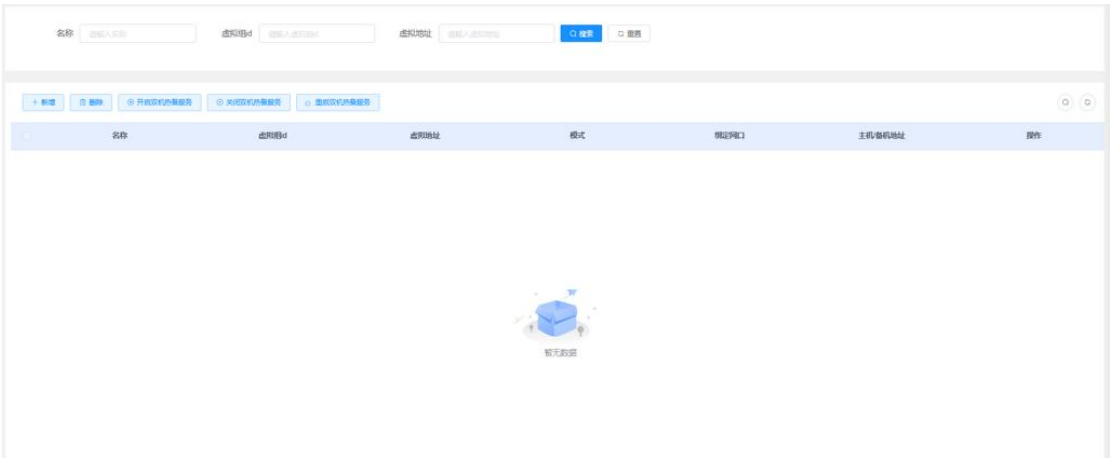
点击【新增】，在弹出的对话框中输入上一条地址、下一条地址、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

3.4.3.3.2 编辑

点击【编辑】，在弹出的对话框中可修改 Bond 模式、IPV4 地址、子网掩码、网关、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

3.4.3.4 双机热备

点击【网络管理】，点击【双击热备】进入到双击热备页面。



3.4.3.4.1 新增

点击【新增】，在弹出的对话框中输入虚拟组 id、虚拟地址、绑定模式、绑定网口、主机地址，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

3.4.3.4.2 编辑

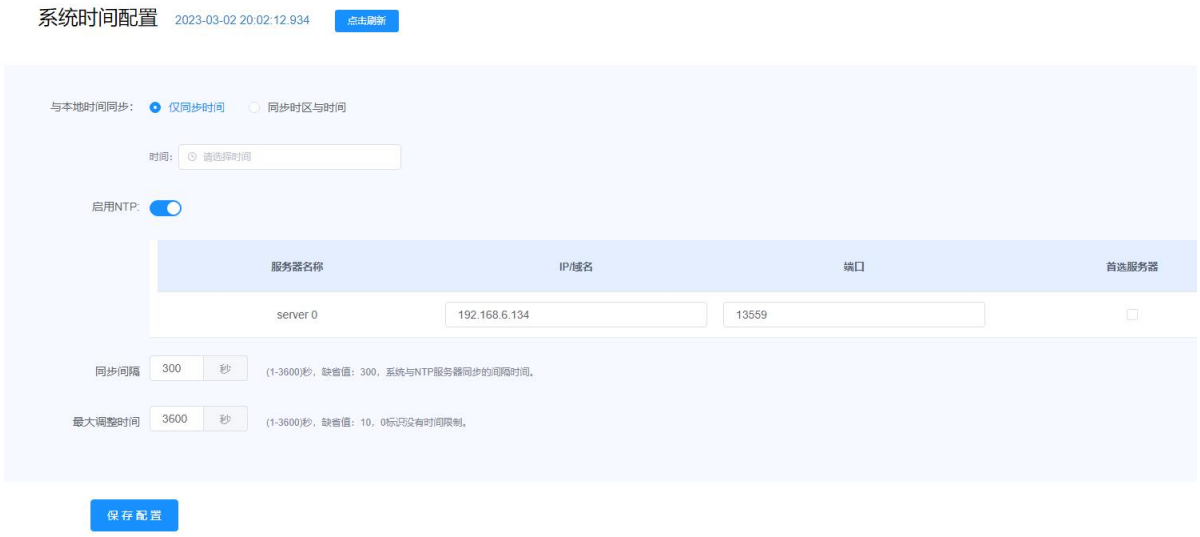
点击【编辑】，在弹出的对话框中可修改虚拟组 id、虚拟地址、绑定模式、绑定网口、主机地址，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。

3.4.4 时间配置

3.4.4.1 系统时间配置

点击【时间配置】，点击【系统时间配置】进入到系统时间配置页面，可以设置当前系

统时间，同步时间服务器上的时间，保证系统时间的精准性。勾选仅同步时间，则时间必须填写。勾选同步时区与时间，则必须填写时区、日期、时间。同步间隔和最大调整时间都得填写，保存配置后，系统时间每相隔指定时间将从 time.windows.com 时间服务器上同步一次。

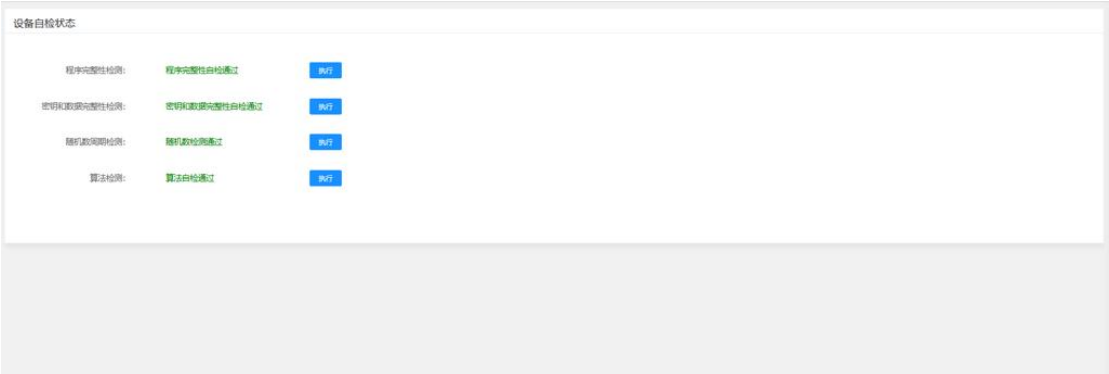


3.4.5 设备状态

设备状态包括【自检状态】和【运行状态】。

3.4.5.1 自检状态

点击【设备状态】，点击【自检状态】进入到自检状态页面。



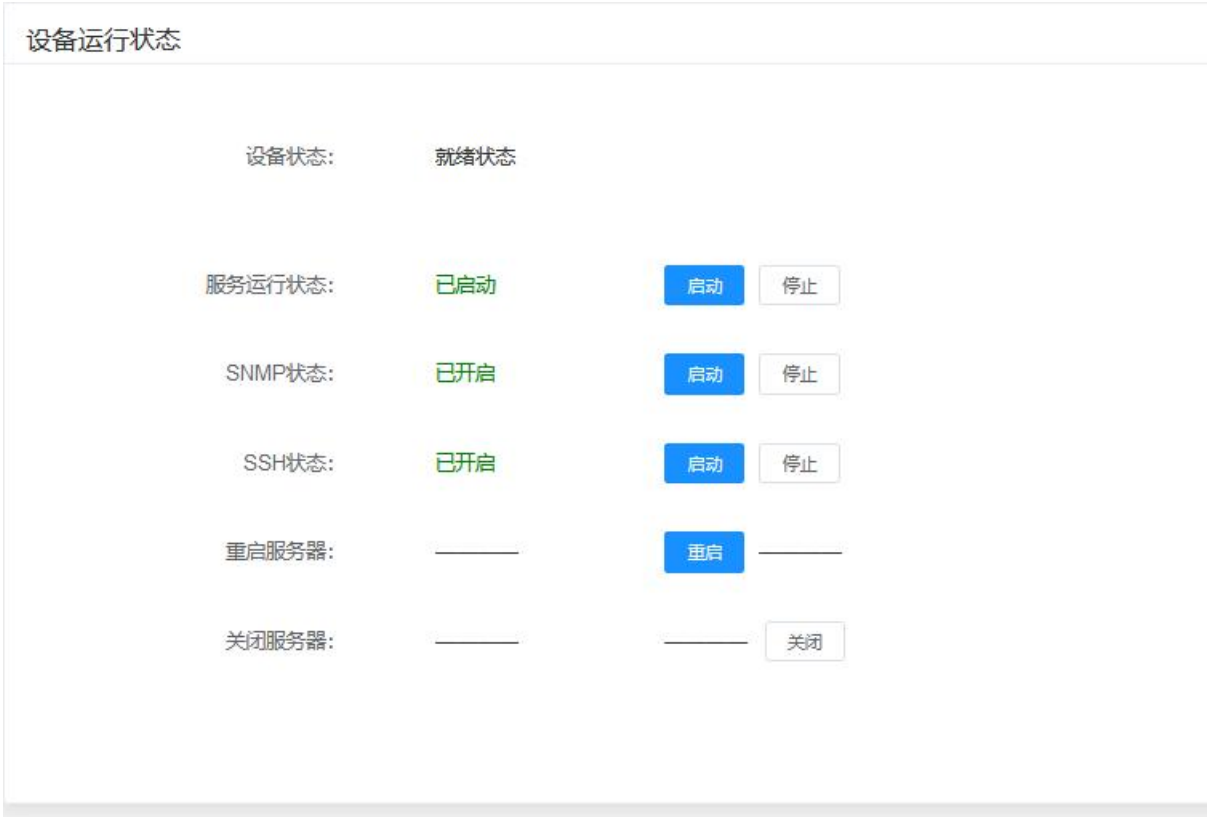
程序完整性检测：检查程序完整性，防止程序中途被篡改，开机会检测，也可手动执行检测。

密钥和数据完整性检测：检测密钥和数据的完整性，防止数据和密钥中途被篡改，开机会检测，也可手动执行检测。

随机数周期检测、算法检测：随机数周期自检检查加密机系统随机数生成机制正常；算法自检检查加密机系统的算法是否正常。

3.4.5.2 运行状态

点击【设备状态】，点击【运行状态】进入到运行状态页面。



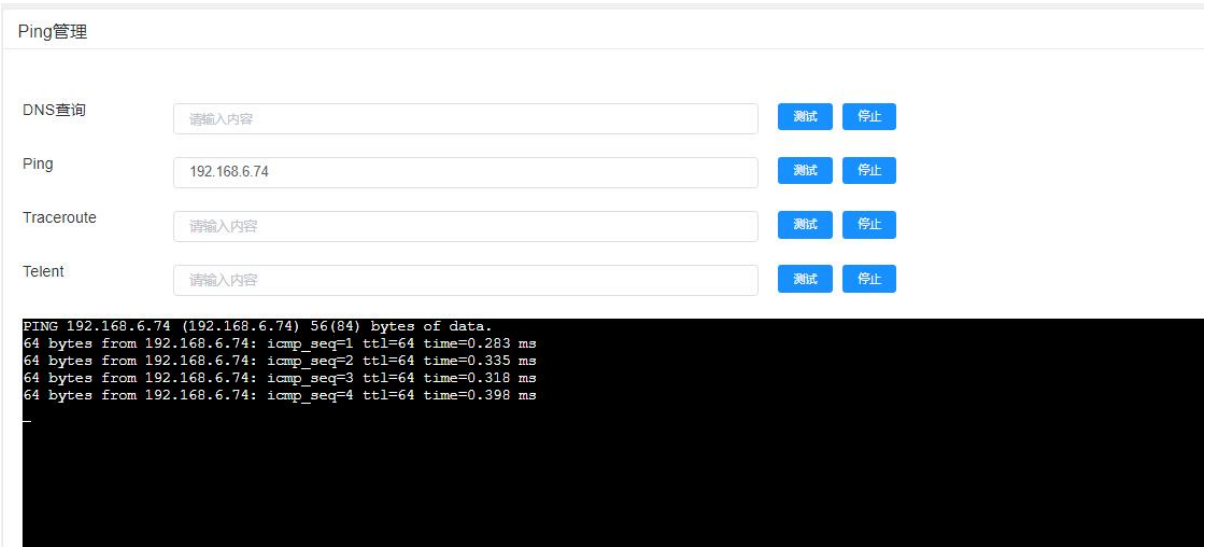
运行状态包括服务状态和关机重启。点击服务状态的【启动】或者【停止】按钮，则会手动开启或者关闭服务。重启表示重新启动综合安全网关服务器，关闭则关闭系统。

3.4.6 设备运维

设备运维包括【运维管理】【SSH 功能】功能。

3.4.6.1 运维管理

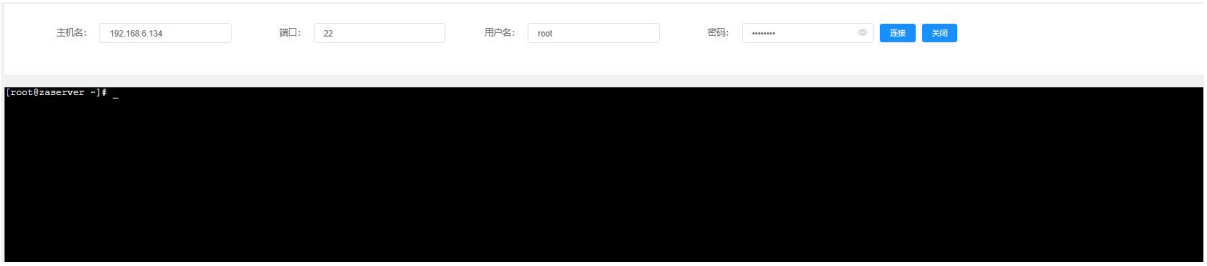
输入地址，点击【连接】。若中断连接，点击【停止】。



3.4.6.2 SSH 功能

点击【设备运维】，点击【SSH 功能】进入到运维管理页面。

输入主机名、端口、用户名、密码，点击【连接】。注意端口号要输入正确。

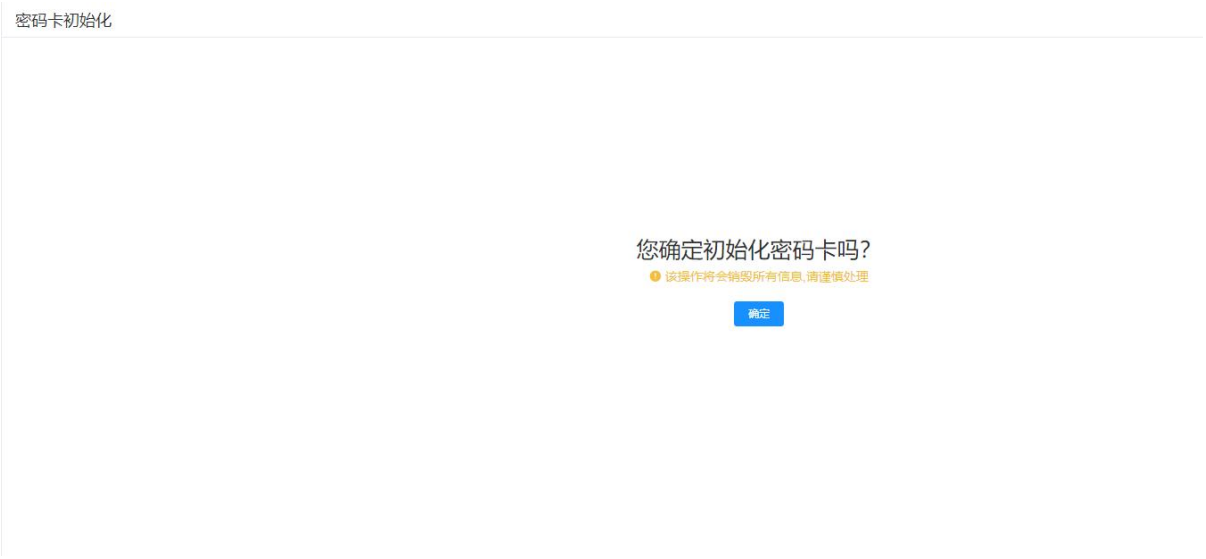


3.4.7 设备重置

设备重置包括【密码卡初始化】【恢复出厂设置】功能。

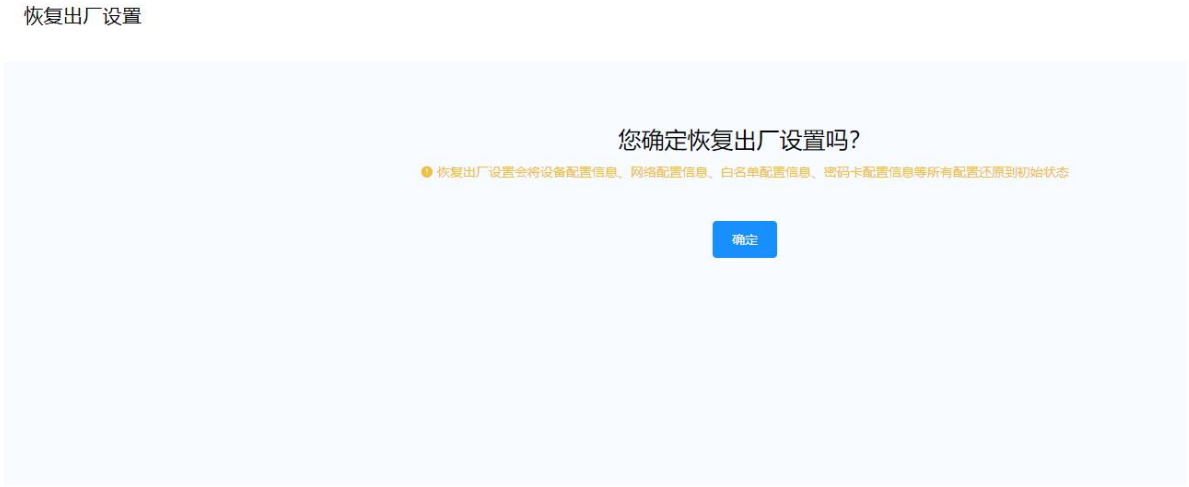
3.4.7.1 密码卡初始化

如果确认初始化，则点击“初始化密码卡”按钮，初始化功能不可逆，请谨慎处理。注意初始化会将全部密钥和密码卡用户信息清空。



3.4.7.2 恢复出厂设置

恢复出厂设置是将系统配置信息、网络配置信息、密码卡信息等所有配置将还原到初始化状态。注意恢复出厂设置会将整个系统重置，请谨慎操作。

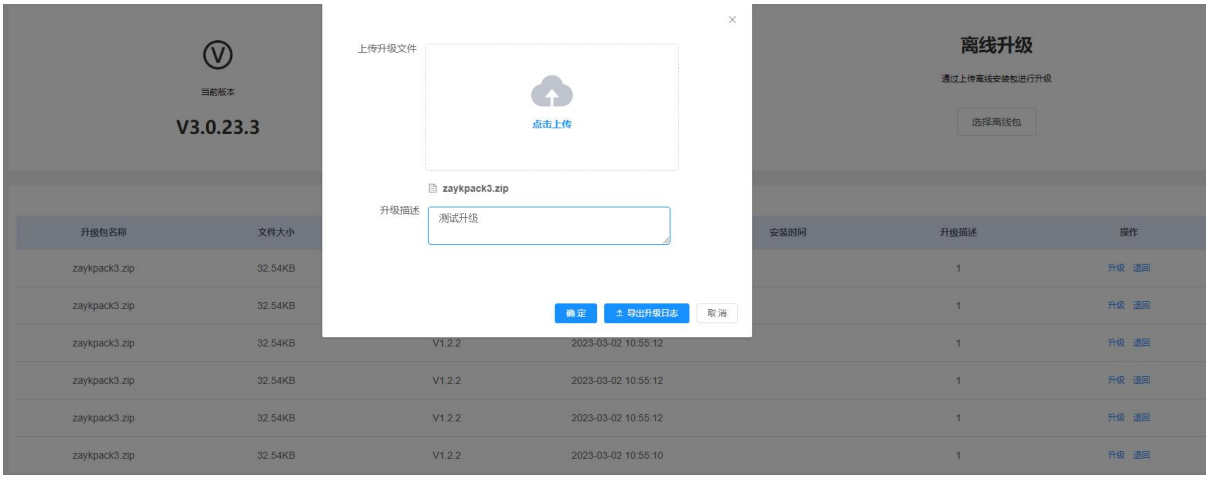


3.4.8 设备更新

点击【设备更新】进入到设备更新界面。

3.4.8.1 离线升级

点击【选择离线包】，然后上传安装包，输入升级描述，点击【升级】。注意升级的版本号会从离线包里面获取。



3.5 安全管理员用户

以安全管理员身份登陆 WEB 管理系统，该管理员用户支持密钥管理、证书管理、隧道服务、用户信息管理、资源管理、网关-客户端模式、系统备份与恢复等配置功能。

VPN 支持隧道代理和客户端两种模式建立 SSL 隧道，使用这两种模式时，需要在安全管理员下进行相关的配置。

1） VPN 服务器证书配置

●依次打开证书管理->设备证书菜单，点击“生成 P10”按钮生成签名 P10 证书请求，然后使用该证书请求到 CA 中心签发证书。

●CA 中心成功下发证书后，根据以下步骤将证书导入到 VPN 设备中。

依次打开证书管理->设备证书菜单，首先，点击“导入根证”按钮，导入 CA 证书对应的跟证书链。然后，点击“导入设备证书”按钮，导入设备证书。

2） 隧道代理模式

点击菜单栏的隧道服务功能菜单，进入隧道服务配置界面，根据界面提示添加隧道代理。

添加成功后，可以使用国密浏览器或国密安全传输中间件，通过该隧道以安全的方式访问被代理的应用资源。

3） VPN 客户端模式

●账号方式拨号登陆

首先，修改客户端认证方式为“账号密码”认证。

依次打开“网关-客户端模式->配置网关”功能菜单，点击编辑按钮，认证方式选择“账号密码”，并根据操作手册说明配置允许用户访问的内网网段信息，确定后保存并重启服务；

然后，新建用户信息。

依次打开“用户信息管理->用户管理”功能菜单，根据操作手册说明新建用户。建立用户成功后，使用新建的用户信进行登陆。登陆后接口访问内网资源。

●账号方式拨号登陆

首先，修改客户端认证方式为“数字证书”认证。

依次打开“网关-客户端模式->配置网关”功能菜单，点击编辑按钮，认证方式选择“数字证书”，并根据操作手册说明配置允许用户访问的内网网段信息，确定后保存并重启服务；

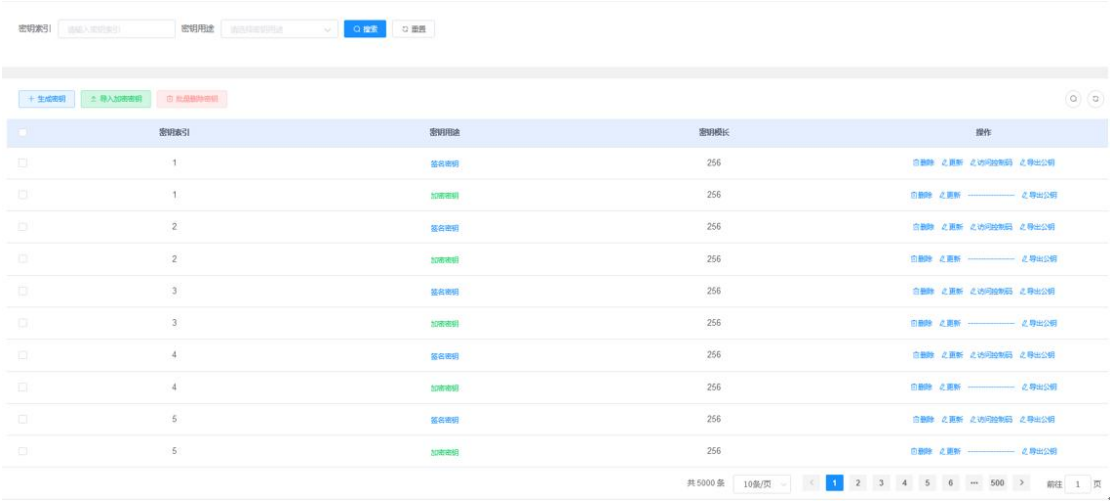
然后通过 VPN 客户端使用 ukey 进行拨号登陆。

详细配置说明，请参考以下功能配置说明。

3.5.1 密钥管理

3.5.1.1 SM2 密钥管理

点击【密钥管理】，点击【SM2 密钥管理】进入 SM2 密钥管理页面。

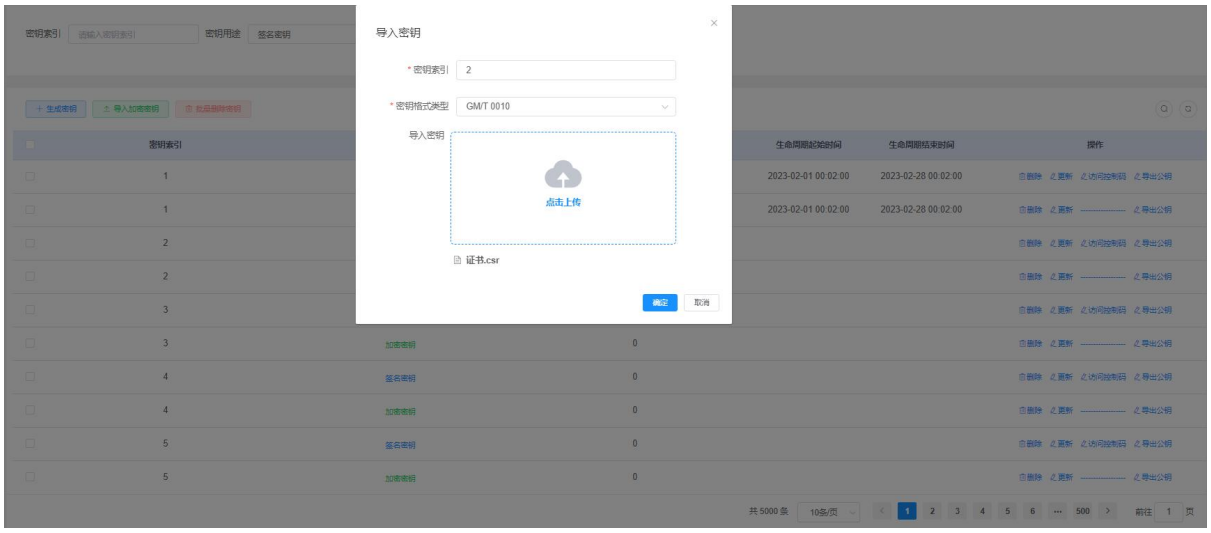


3.5.1.1.1 生成密钥

密钥标签内可输入密钥索引，密钥用途可选择签名密钥/加密密钥/签名和加密密钥，密钥模长 256，点击【生成密钥对】按钮完成指定密钥的生成并安全保存。

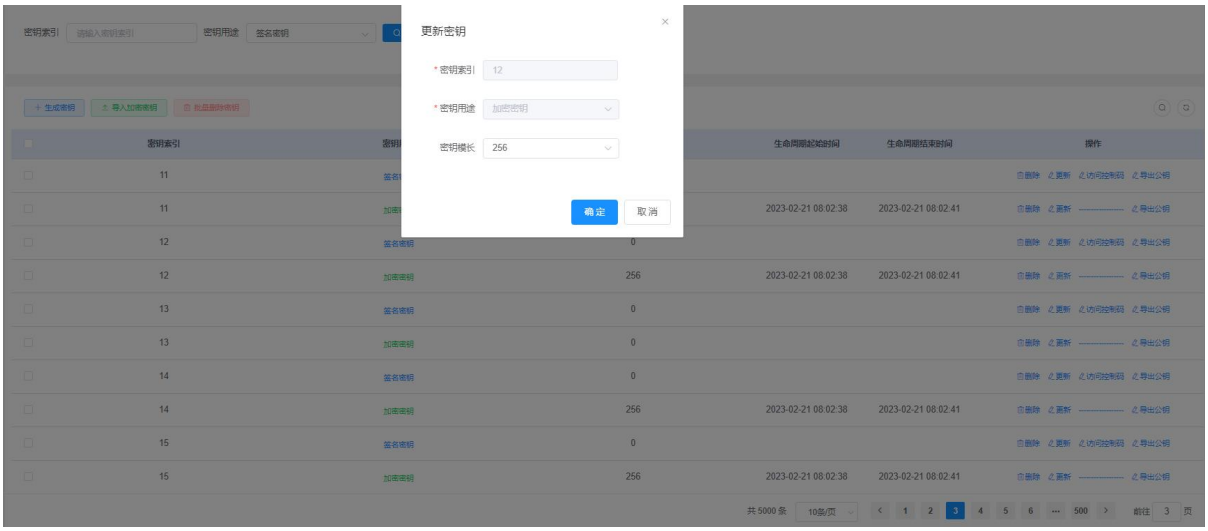
3.5.1.1.2 导入加密密钥

点击【导入加密密钥】，输入密钥索引、选择密钥格式类型、选择文件，点击【确定】。注意证书要上传正确。



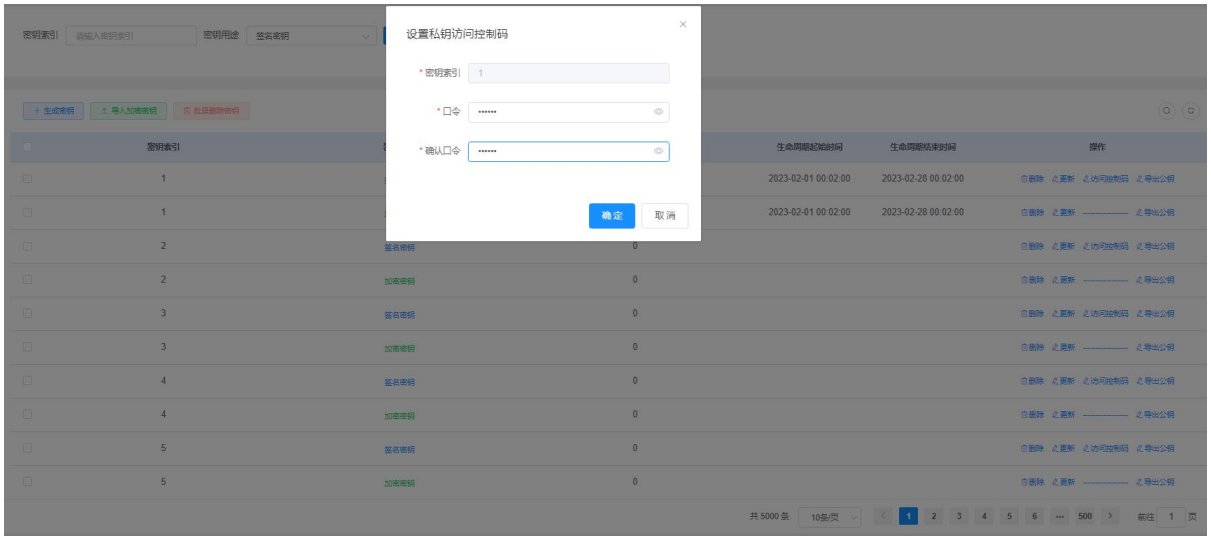
3.5.1.1.3 更新

点击【更新】，在弹出的对话框中选择密钥模长，点击【确定】，修改用户对应的用户密钥模长。



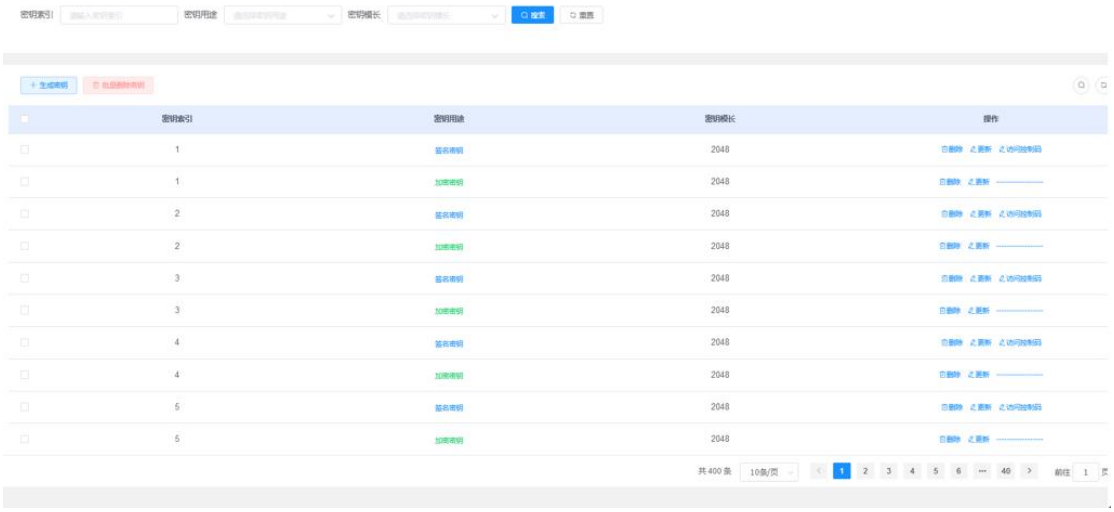
3.5.1.1.4 访问控制码

点击【访问控制码】，在弹出对话框中输入新口令、确认口令，点击【确认】。



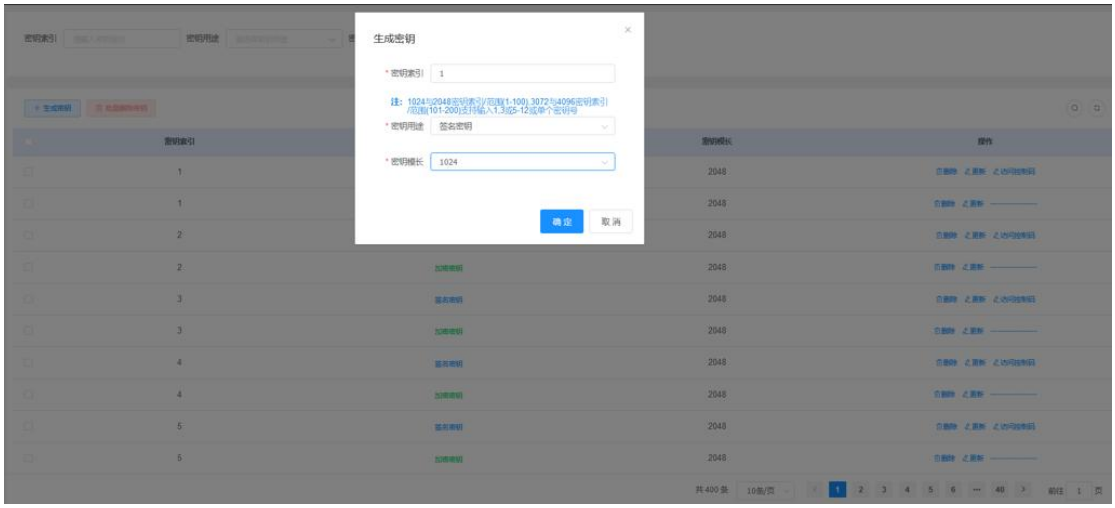
3.5.1.2 RSA 密钥管理

点击【密钥管理】，点击【RSA 密钥管理】进入 RSA 密钥管理页面。



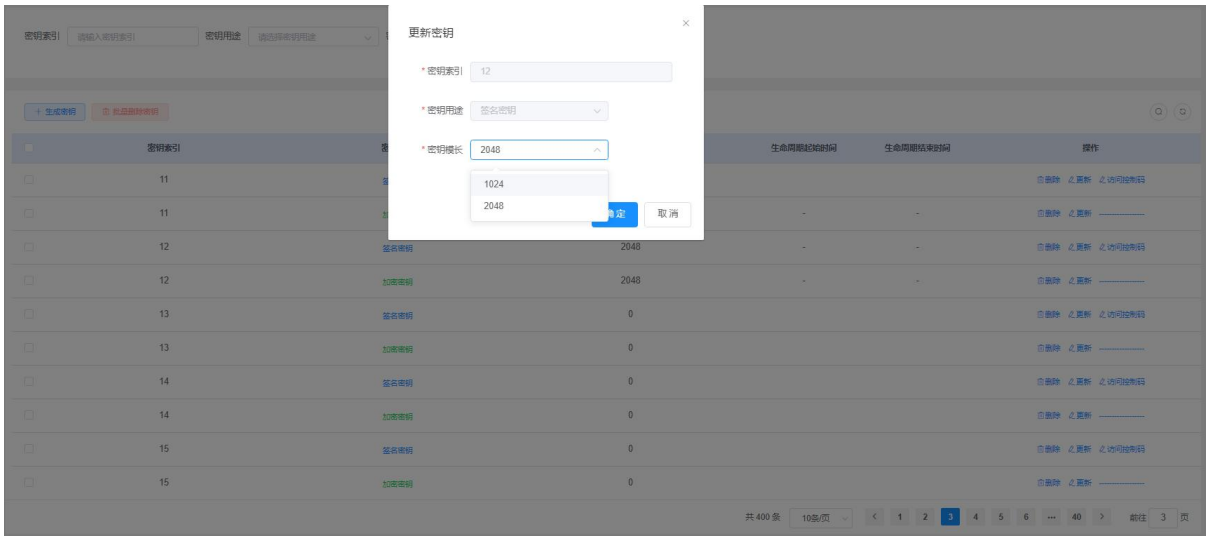
3.5.1.2.1 生成密钥

密钥标签内可输入密钥密钥索引，密钥用途可选择签名密钥/加密密钥/签名和加密密钥，密钥模长 1024，2048，设置生命周期（默认生效时间为当前），配置完成后点击【确定】按钮完成指定密钥的生成并安全保存。



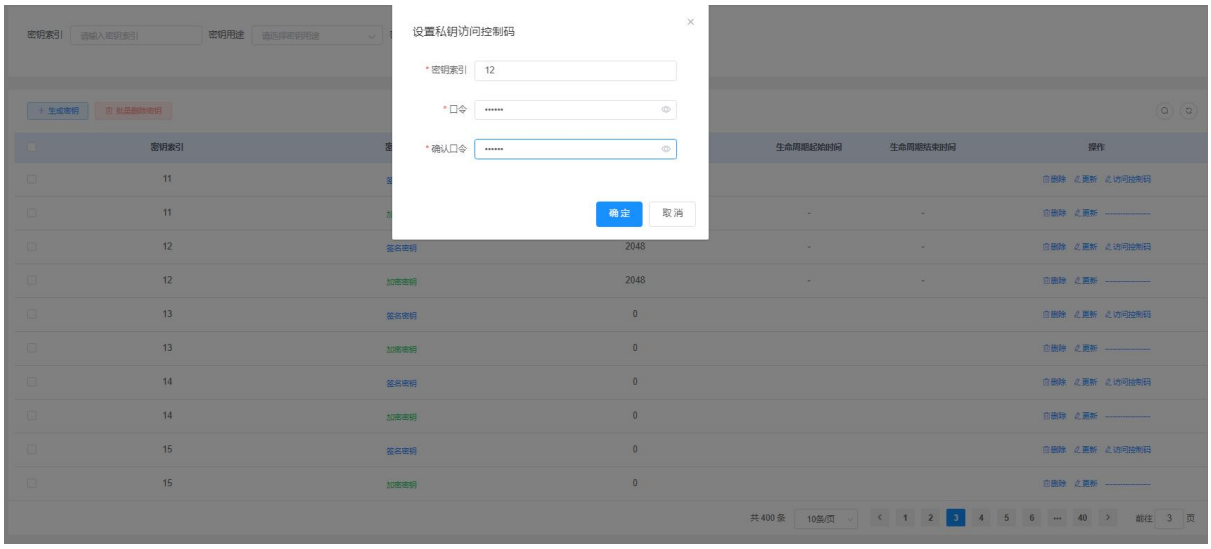
3.5.1.2.2 更新

点击【更新】，在弹出的对话框中选择密钥模长，点击【确定】，修改用户对应的密钥模长。



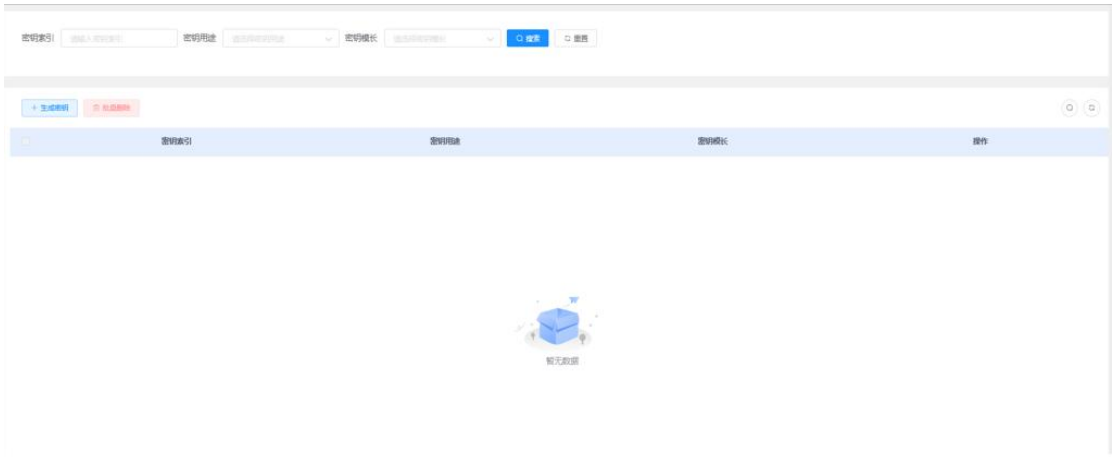
3.5.1.2.3 访问控制码

点击【访问控制码】，在弹出对话框中输入新口令、确认口令，点击【确认】。



3.5.1.3 ECC 密钥管理

点击【密钥管理】，点击【ECC 密钥管理】进入 ECC 密钥管理页面。

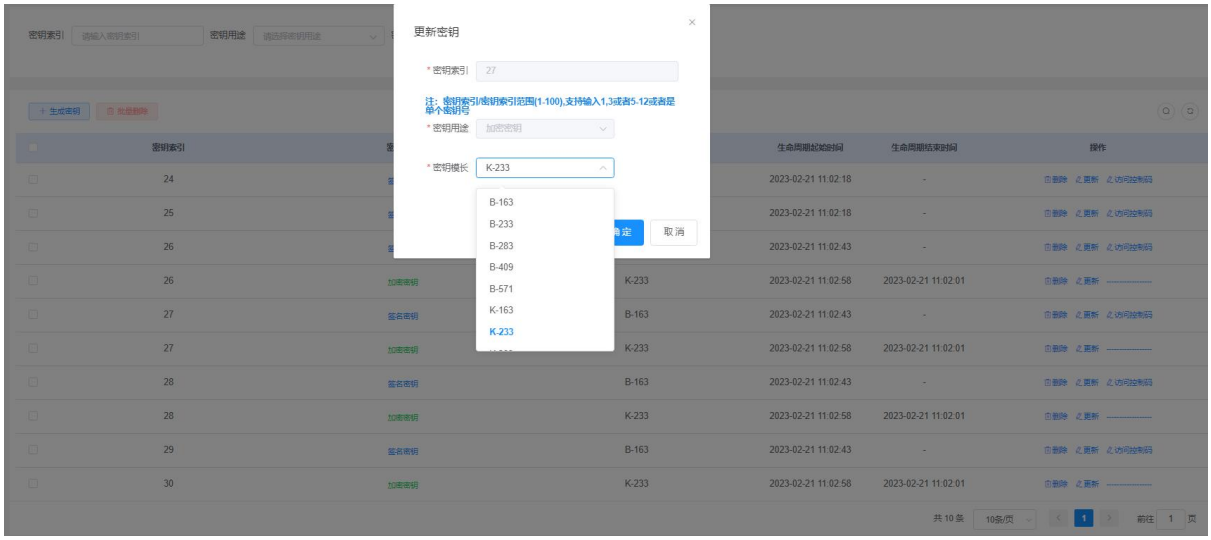


3.5.1.3.1 生成密钥

密钥标签内可输入密钥索引，密钥长度可选择 B-163，B-233，B-283，B-409，B-571，K-163，K-283，K-409，K-571，P-192，P-224，P-256，P-384，P-521，ED25519（默认 P-256）设置生命周期（默认生效时间为当前），配置完成后点击【确定】按钮完成指定密钥的生成并安全保存。

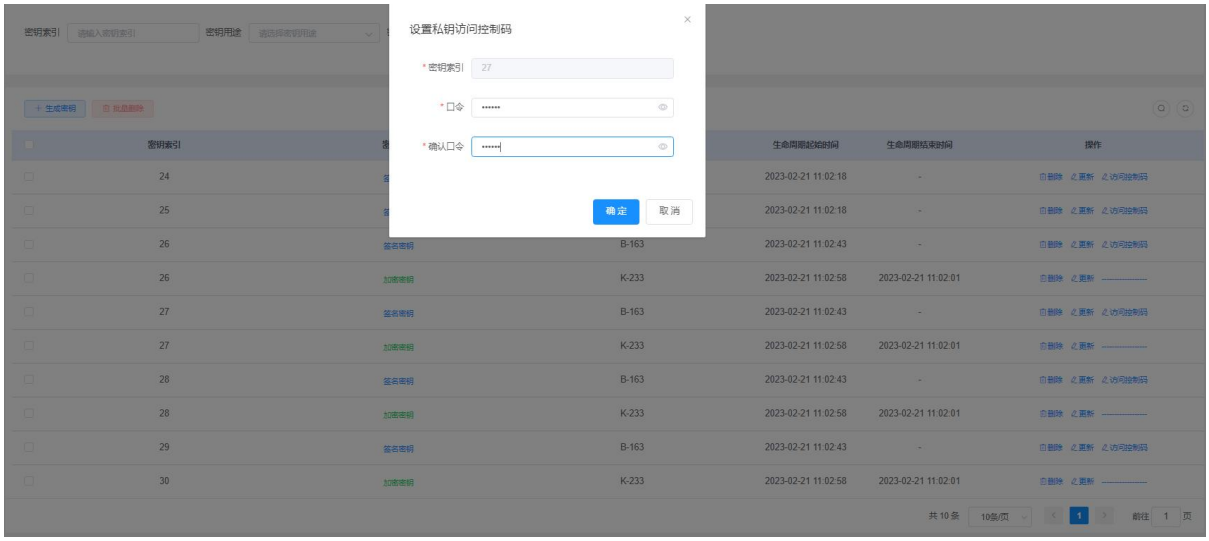
3.5.1.3.2 更新

点击【更新】，在弹出的对话框中选择密钥模长，点击【确定】，修改用户对应的密钥模长。



3.5.1.3.3 访问控制码

点击【访问控制码】，在弹出对话框中输入新口令、确认口令，点击【确认】。



3.5.2 证书管理

3.5.2.1 设备证书

依次点击菜单栏的证书管理-> 设备证书，进入设备证书页面，如下图所示：

1）自签证书

点击自签证书按钮，弹出如下页面，依次添加根证以及设备证书，提示操作成功后表示添加成功，否则添加失败。

2）生成 P10 证书请求

其主要功能为生成 PKCS10 证书请求。在界面中输入证书的主题信息并选择所用密钥 后，点击【生成证书请求】按钮即可生成 PKCS10 格式的证书请求。证书请求的文件内容显示在 PKCS10 文本框中。管理员可以保存 PKCS10 后，去证书机构申请证书，然后导入到签名验签服务器中。

4）导入根证书

点击“导入根证”按钮，弹出导入根证书对话框，选择需要导入的根证书后，点击“导入”，提示操作成功，导入成功，否则导入失败。

6）导入设备证书

点击导入设备证书，弹出导入设备证书对话框，如下图所示，选择证书类型，密钥号，签名证书，加密证书，加密私钥，点击导入，提示操作成功，导入成功，否则导入失败。

3.5.2.2 证书吊销列表

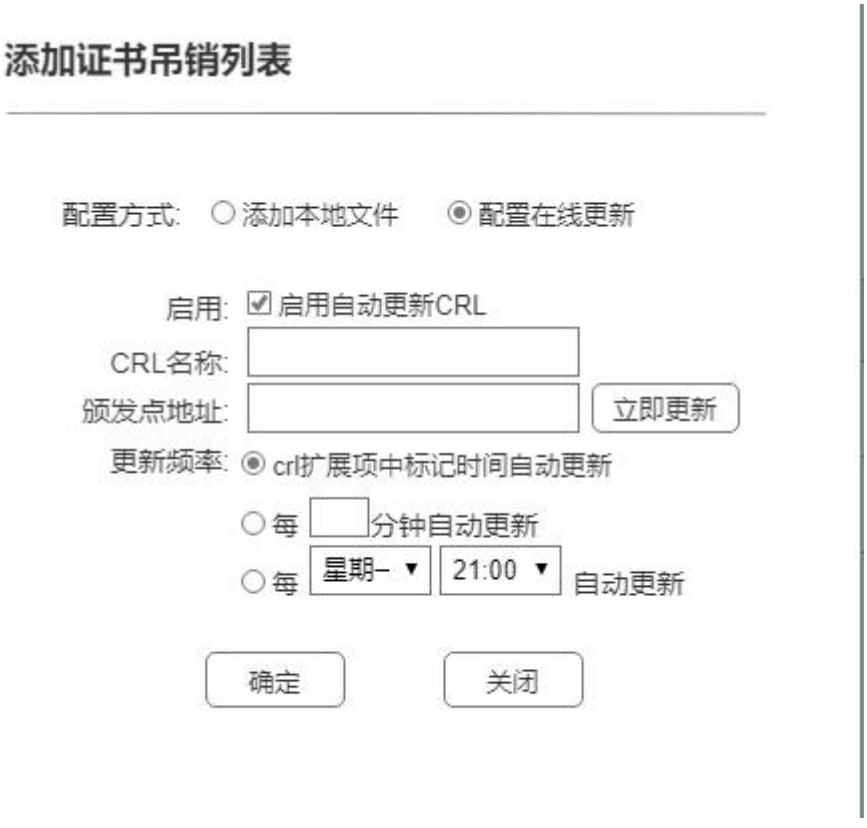
依次点击菜单栏的证书管理→ CRL 管理，进入证书吊销列表页面，如下图所示：

1）添加证书吊销信息

点击添加按钮，弹出添加证书吊销列表对话框：

选择添加本地文件，如下图所示，输入 CRL 名称，以及 CRL 文件，点击确定按钮，提示操作成功，证明添加成功，否则添加失败。

选择配置在线更新,如下图所示，依次输入相关信息后，点击确定按钮。



2）编辑吊销证书信息

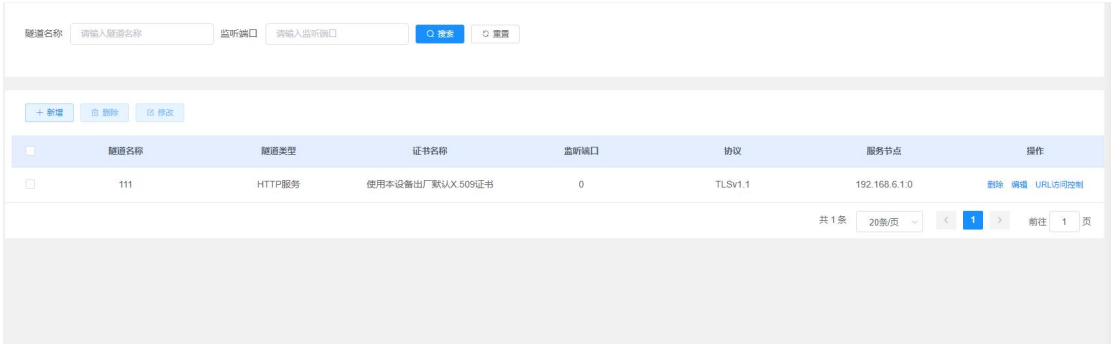
点击编辑按钮，可以修改 CRL 名称及 CRL 文件，或在线更新相关信息。修改完成后，点击确定按钮，进行数据保存，提示操作成功，证明修改成功，否则修改失败。

3）删除吊销证书信息

点击删除按钮，弹出提示框后点击确认，提示操作成功，则删除成功，否则删除失败。

3.5.3 隧道服务

点击菜单栏的隧道服务菜单，如下图所示，进入隧道服务配置界面：



1）新建隧道服务

点击新建按钮，弹出新建隧道服务对话框，如下图所示，包括基本配置，高级配置，其它配置三个配置标签页。其中高级配置，其它配置项的内容为非必输项，根据具体需要选择使用。

基本配置：

●服务名称：该隧道代理的别名，一般用于说明该隧道代理的功

能。

●监听端口：该隧道代理使用的端口号，配置隧道后，使用 VPN 设备地址+监听端口进行方式；

●通道类型：支持国密和国际两种通道类型；

●协议类型：通道类型为国密时，支持国密 SSL 协议；通道类型为国际时，支持国际 TLSv1.0，TLSv1.1，TLSv1.2，TLSv1.3 协议版本；

●国密/国际证书：VPN 设备证书；

●握手策略：支持单向认证，双向认证，单/双向自适应；

●用户根证：双向认证时，该项必填，为客户端证书的根证；

●服务节点：被代理的后端应用服务信息，存在多条时，可实现后端应用的负载均衡；


新建隧道服务
基础配置
高级配置
其他配置
基础信息
* 服务名称
测试服务
* 监听端口
19001
* 通道类型
国密
域名地址
请输入域名地址
* 协议类型
国家密码管理局SSL协议标准v1.1 (GM/T 0024-2014)
国密证书
使用本设备出厂默认X.509证书
* 握手策略
等级0 - 不认证对端证书
用户根证
点击配置用户根证书
* 隧道类型
HTTP服务
TCP服务
FTP服务
UDP服务
服务节点
服务地址
服务端口
权重
操作
192.168.6.113
9000
1
确定
取消

高级配置：


新建隧道服务
基础配置
高级配置
其他配置
HTTP服务高级配置
证书信息透传到应用
开启在线证书状态验（OCSP）
开启内容提换
负载均衡策略配置
IP_HASH
是否启用根据源地址引导流量
重试次数
5
超时时间(秒)
20
代理客户端证书配置
证书配置
注：被代理服务器使用双向认证时，需开启此项
确定
取消

其它配置：


新建隧道服务
基础配置
高级配置
其他配置
连接超时时间(秒)
30
开启防DDOS攻击
开启防sweet32攻击)
开启防host头部攻击
确定
取消

3.5.4 用户信息管理

依次打开用户信息管理->用户管理菜单，进入用户管理操作页面，如下图所示：

3.5.4.1 用户组管理

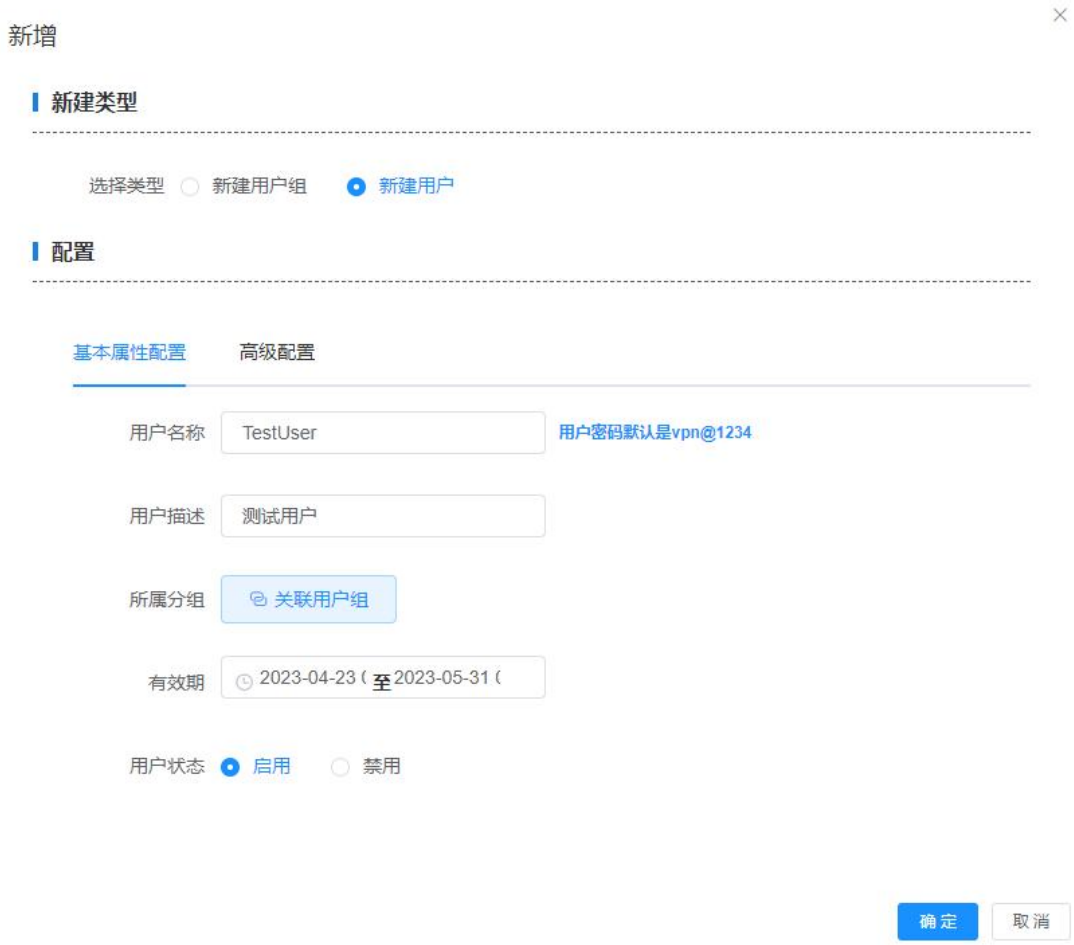
1）新建用户分组

点击“新建”按钮，弹出新建对话框，如下图所示，选择新建用户组。根据页面提示，依次输入用户组相关信息，点击保存后退出。

3.5.4.2 用户管理

1）新建用户

点击“新建”按钮，弹出新建对话框，如下图所示，选择新建用户。根据页面提示，依次输入用户基本属性信息，根据需要配置高级属性信息，点击保存后退出。



3）编辑用户信息

如下图所示，在用户列表中选择需要编辑的用户，点击编辑按钮，可修改用户的基本属性信息和高级属性信息，修改完成点击保存。

3.5.4.3 特征码管理

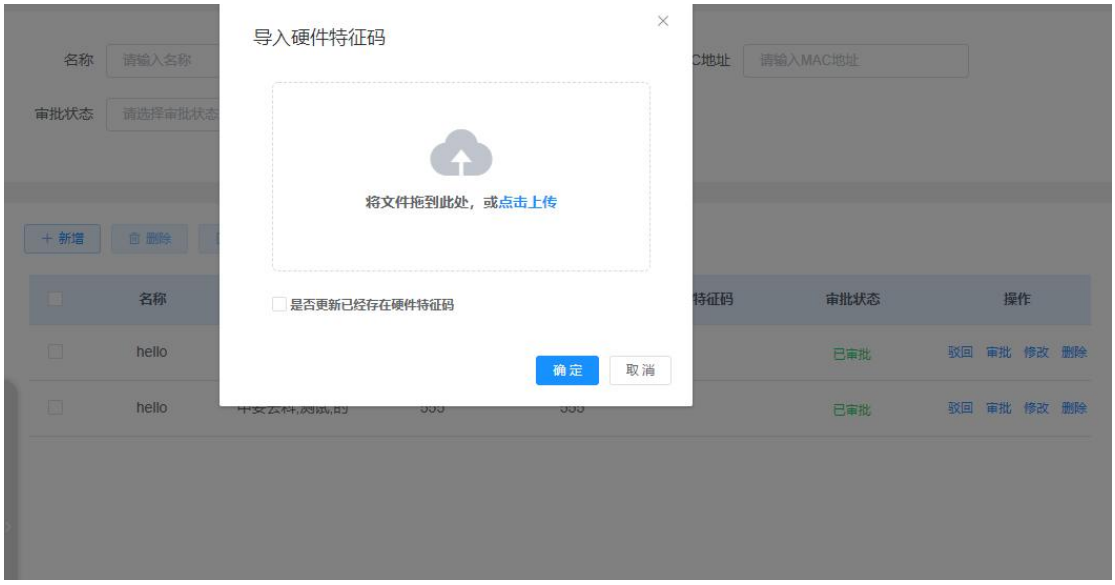
依次打开用户信息管理->特征码管理菜单，进入特征码管理页面，如下图所示：

1） 添加硬件特征码

点击添加按钮，弹出“添加硬件特征码”对话框，如下图所示，根据页面提示，选择用户名，输入计算机名、MAC 地址、硬件特征码等信息后，点击审批按钮。

2） 导入硬件特征码

点击导入按钮，弹出导入硬件特征码对话框，如下图所示。根据界面提示，依次选择硬件特征码信息文件等信息后，点击保存。

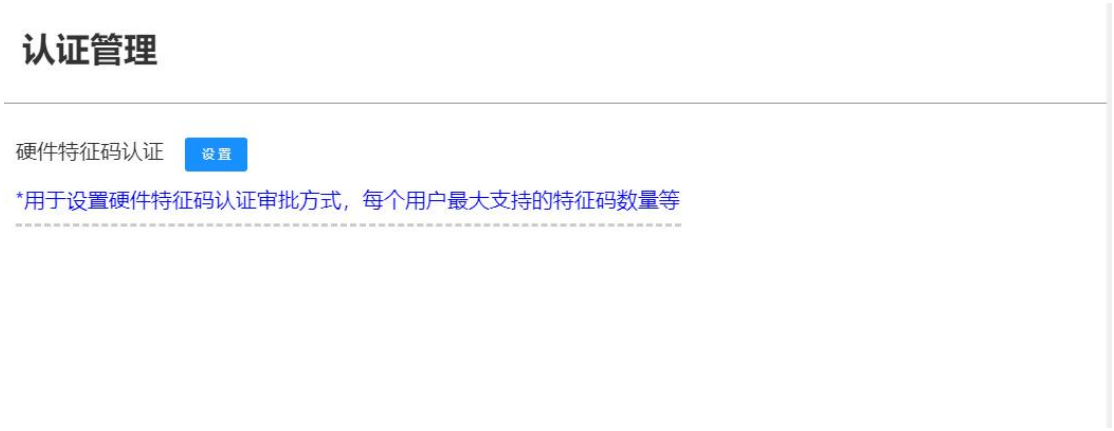


3） 导出硬件特征码

点击导出按钮，弹出导出硬件特征码对话框，如下图所示。根据界面提示，选择需要导出的特征码信息后，点击保存。

3.5.4.4 认证管理

依次打开用户信息管理->认证管理菜单，进入认证管理页面，如下图所示：



1） 硬件特征码认证配置

点击硬件特征码认证的设置功能按钮，弹出特征码认证设置对话框，如下图所示，可设置硬件特征码认证的审批方式，每个用户允许使用的特征码数量。

3.5.5 资源管理

3.5.5.1 资源配置

依次点击菜单栏的资源管理->资源配置功能，进入资源配置页面，如下图所示：

1）新增资源配置

点击“新增”按钮，打开新建资源对话框，如下图所示：

根据界面提示依次输入相关要素，点击确定后保存。

2） 修改资源配置

选择需要修改的资源，点击“编辑”按钮，打开修改资源对话框，如下图所示：

根据界面提示，修改对应的信息后，点击确定后保存。

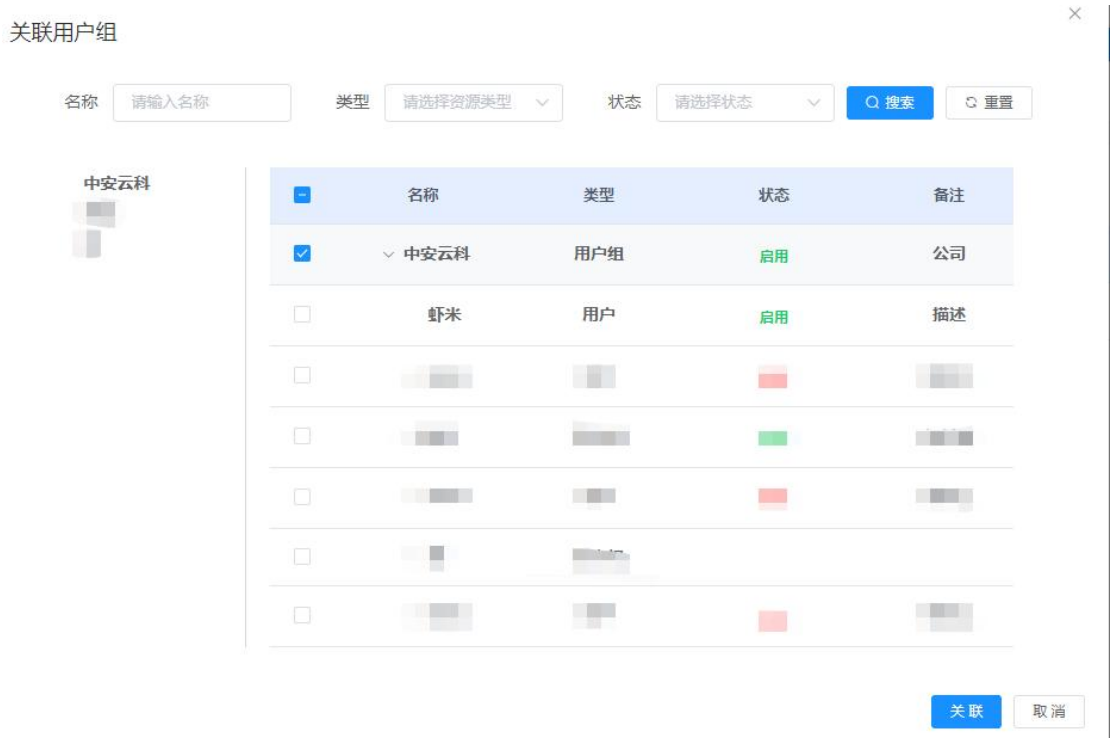
3.5.5.1 资源组管理

依次点击菜单栏的资源管理->资源配置功能，进入资源配置页面，如下图所示：

3.5.5.1.1 新增资源组

点击“新增资源组”按钮，打开新建资源组对话框，如下图所示：

根据界面提示信息，依次输入资源组名称、资源组状态等信息，点击关联用户组按钮，关联用户，如下图所示：



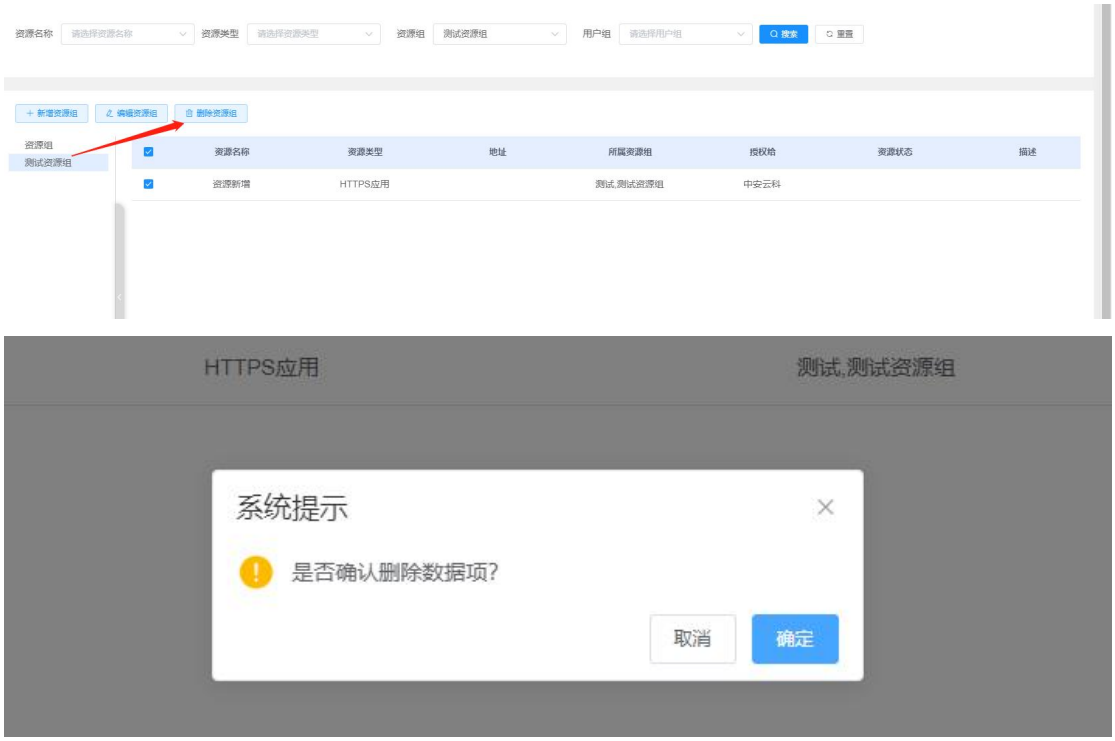
点击关联资源按钮，打开关联资源对话框，为该资源组关联资源，如

下图所示：

相关信息输入完成后，点击确定保存，如下图所示：

3.5.5.1.1 删除资源组

如下图所示，选择需要删除的资源组，点击“删除资源组”按钮，进行资源组的删除。



3.5.6 网关-客户端模式

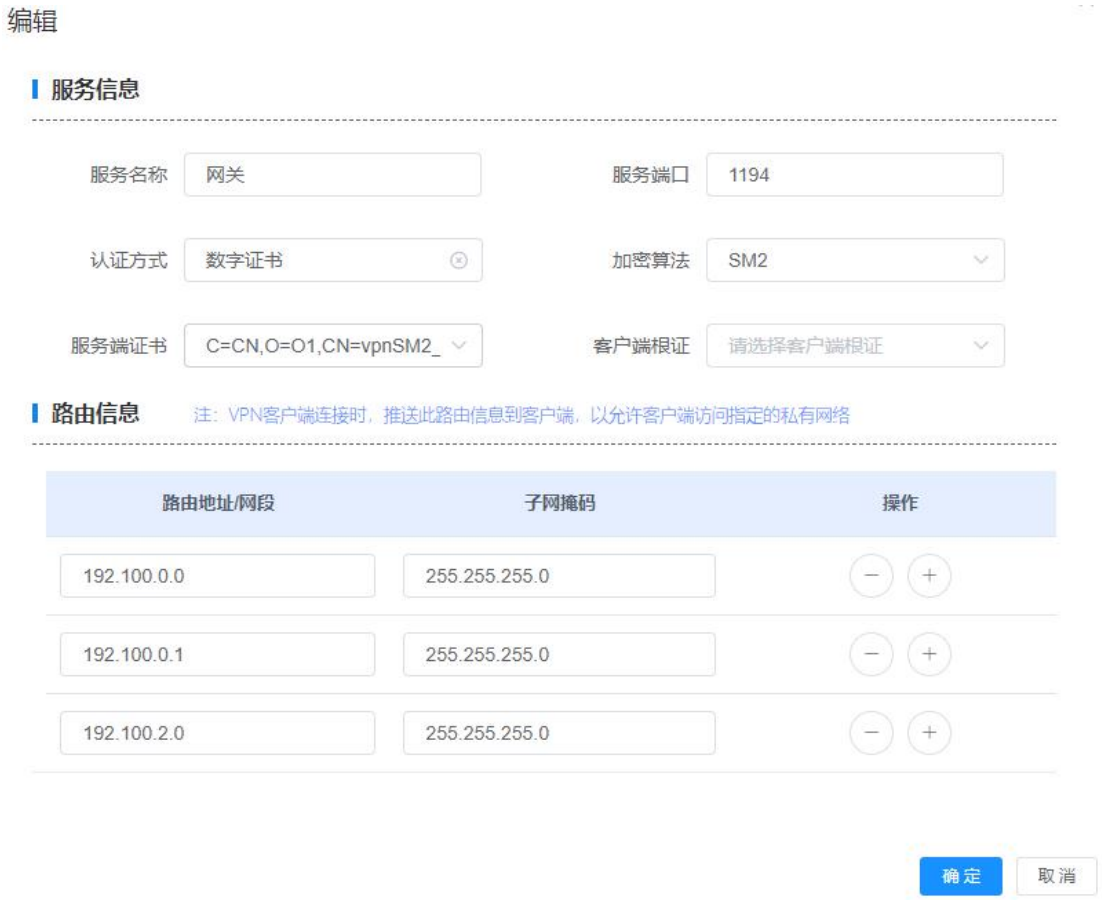
3.5.6.1 配置网关

依次点击菜单栏的网关-客户端模式→配置网关，进入配置网关页面，如下图所示：

1） 修改网关基本配置

点击编辑按钮，弹出修改网关页面，可以修改网关名称、端口号、认证方式、加密算法、修改证书等信息，修改完成后，点击确定按钮，

提示操作成功，表示修改成功，否则修改失败。



3.5.6.2 访问记录

该功能用于查看 VPN 客户端用户的登陆信息。

依次点击菜单栏的网关-客户端模式->访问记录菜单，进入访问记录页面，如下图所示：

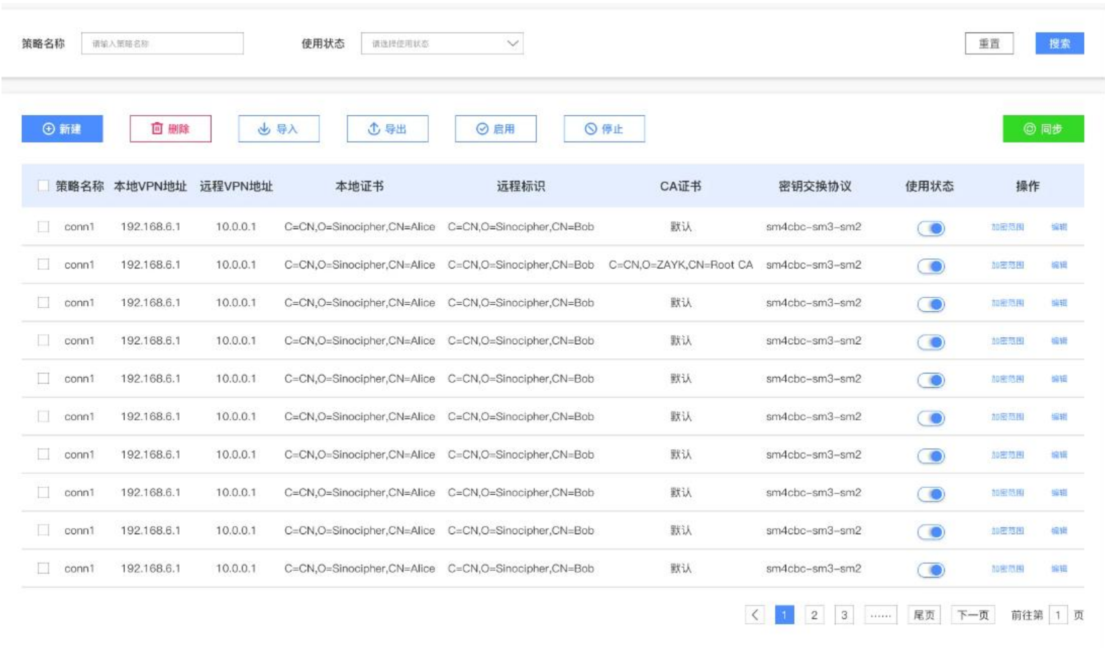
点击导出按钮，可以将访问记录以 Excel 形式导出到本地。

3.5.7 IPSEC 管理

该功能支持 IPSec 服务的策略配置，和加密隧道信息监控。

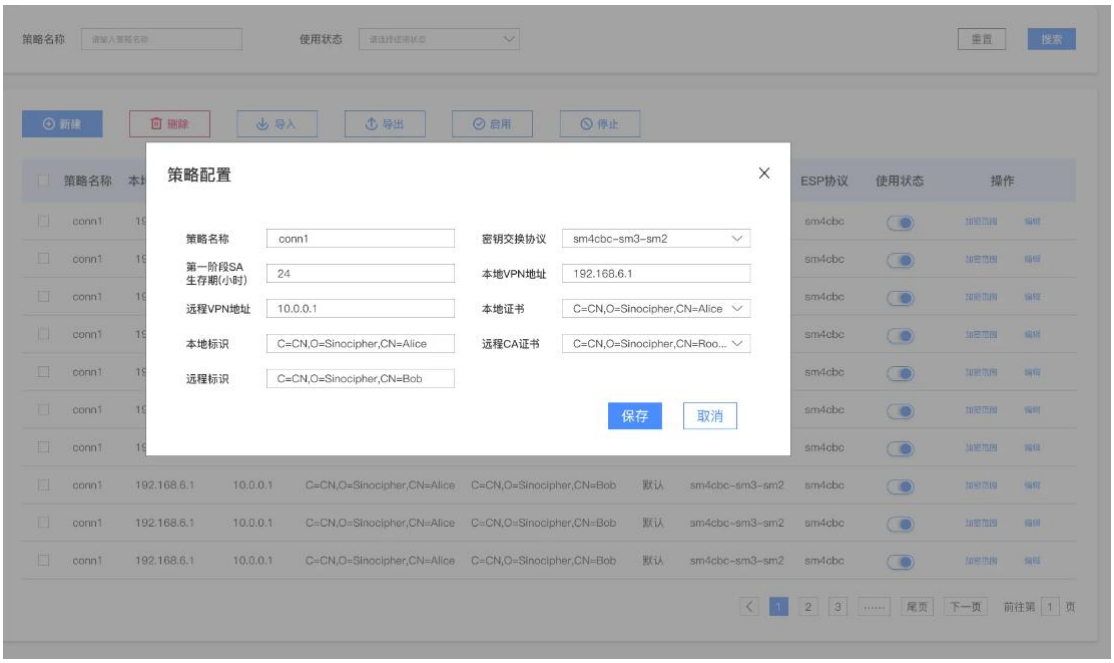
3.5.7.1 策略配置

依次点击菜单栏的 IPSec 管理->策略配置功能菜单，可查看当前配置的 IPSec 隧道信息，如下图所示：



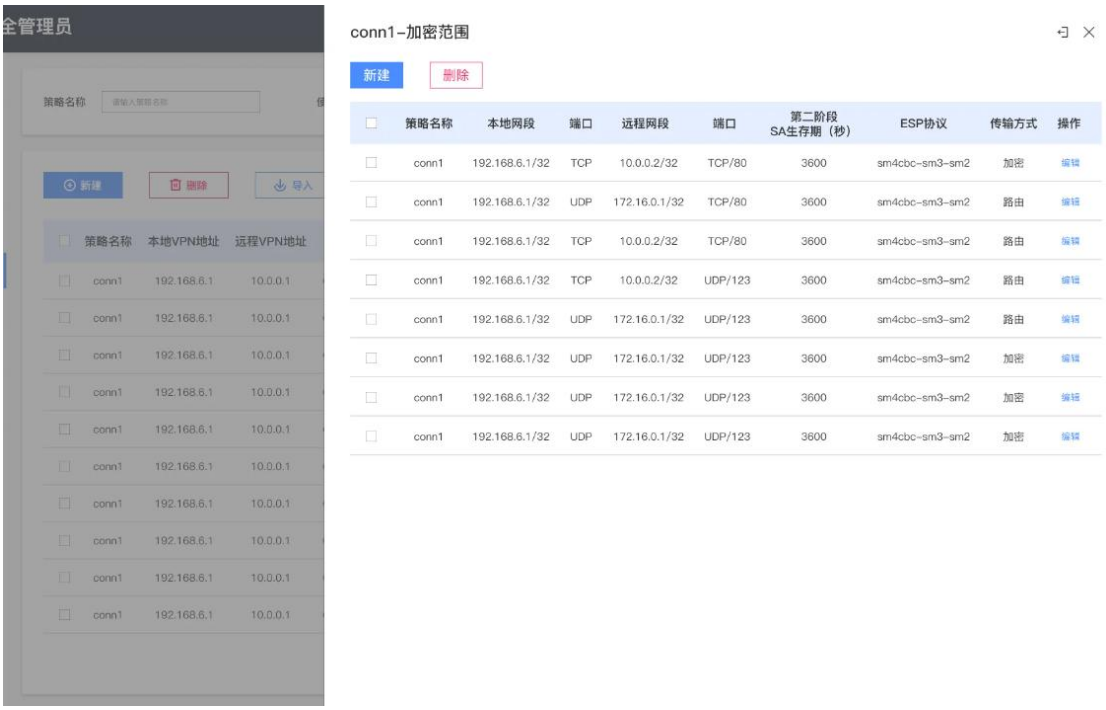
1） 新建策略

点击“新建”按钮，打开策略配置对话框，根据界面提示信息配置策略，如下图所示：



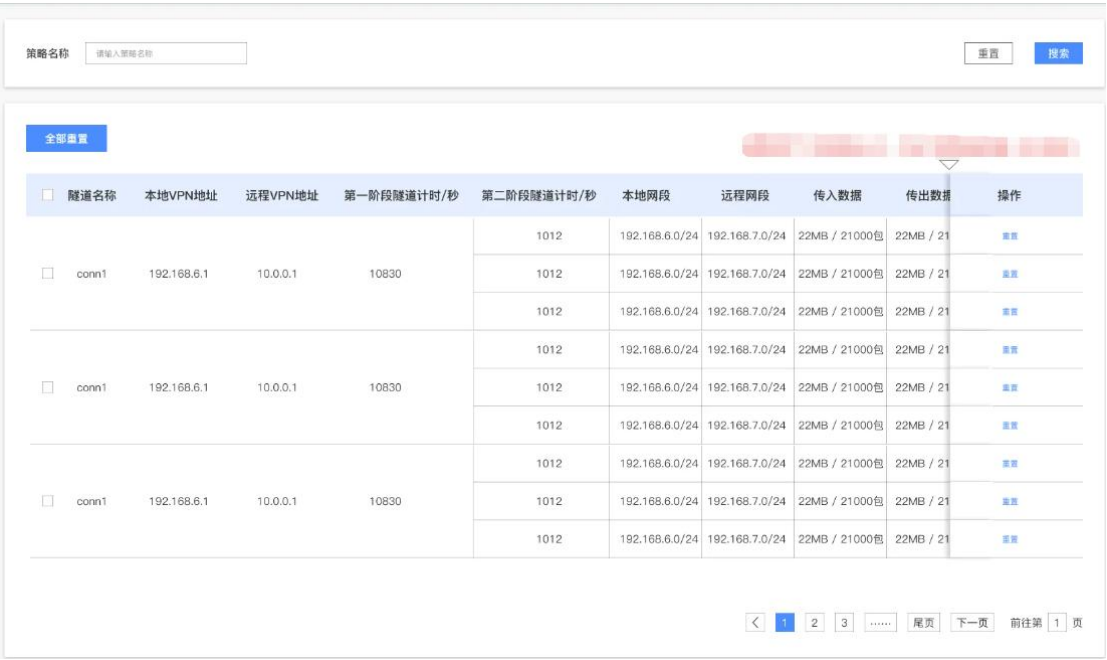
2） 配置加密范围

选择需要配置加密范围的策略，点击“加密范围”按钮，打开加密范围对话框，根据界面提示进行配置即可，如下图所示：



3.5.7.1 隧道监控

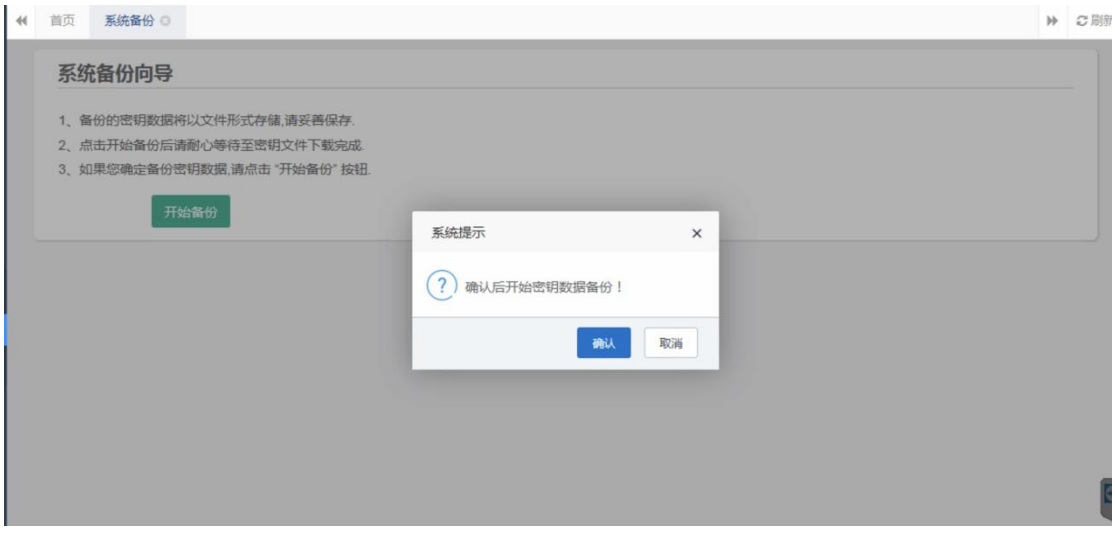
依次点击菜单栏的 IPSec 管理->隧道监控功能菜单，可查看当前配置的 IPSec 隧道信息，如下图所示：



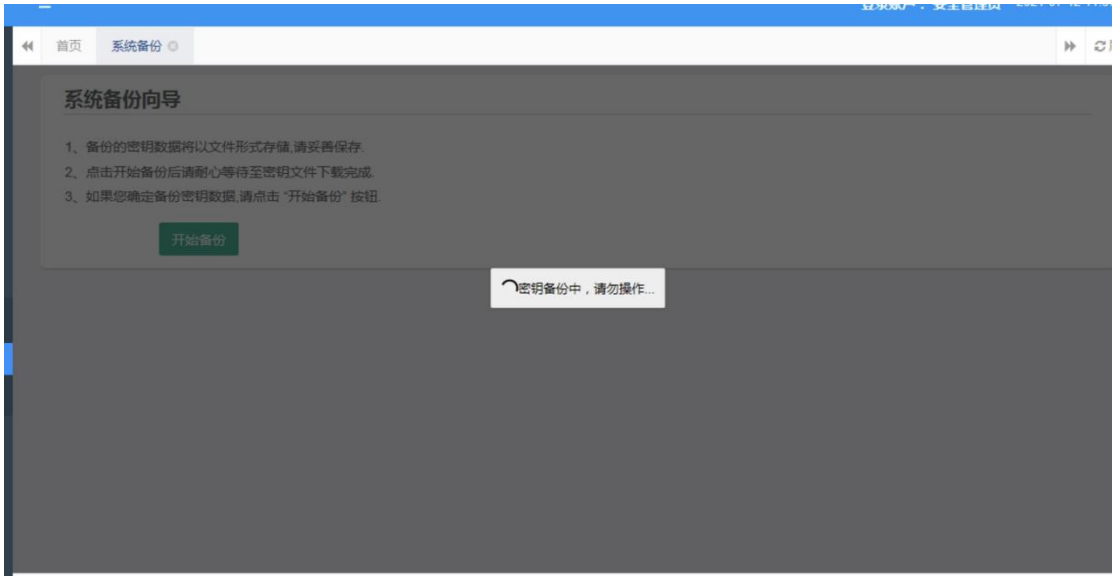
3.5.8 系统备份与恢复

3.5.8.1 系统备份

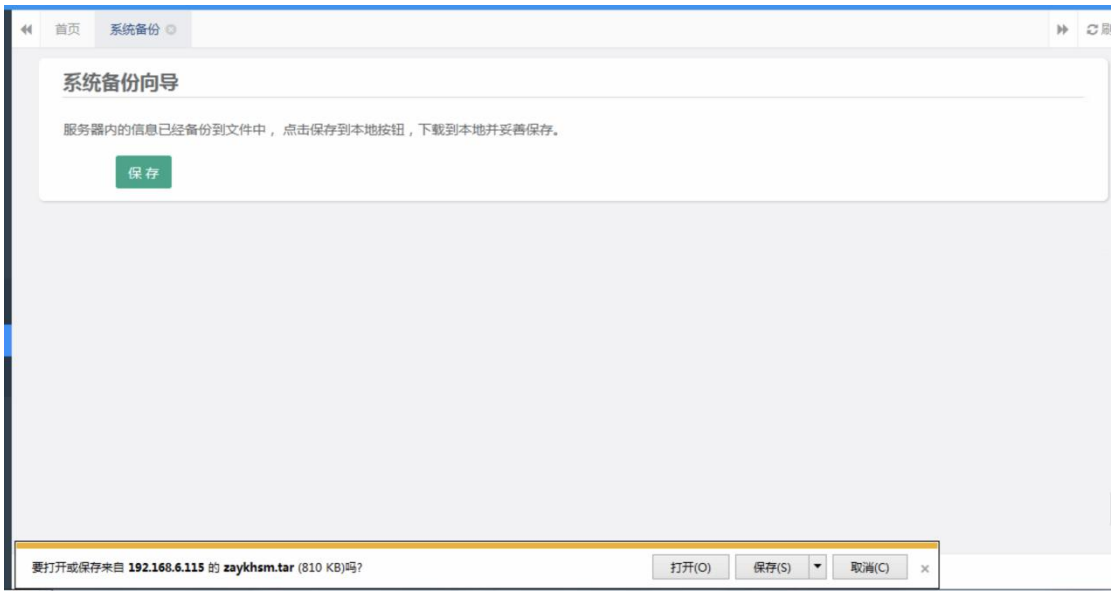
依次点击菜单栏的恢复与备份->系统备份，可对系统中数据以及密钥文件进行备份储存。



点击确认后耐心等待着备份数据完成（会有点慢）。

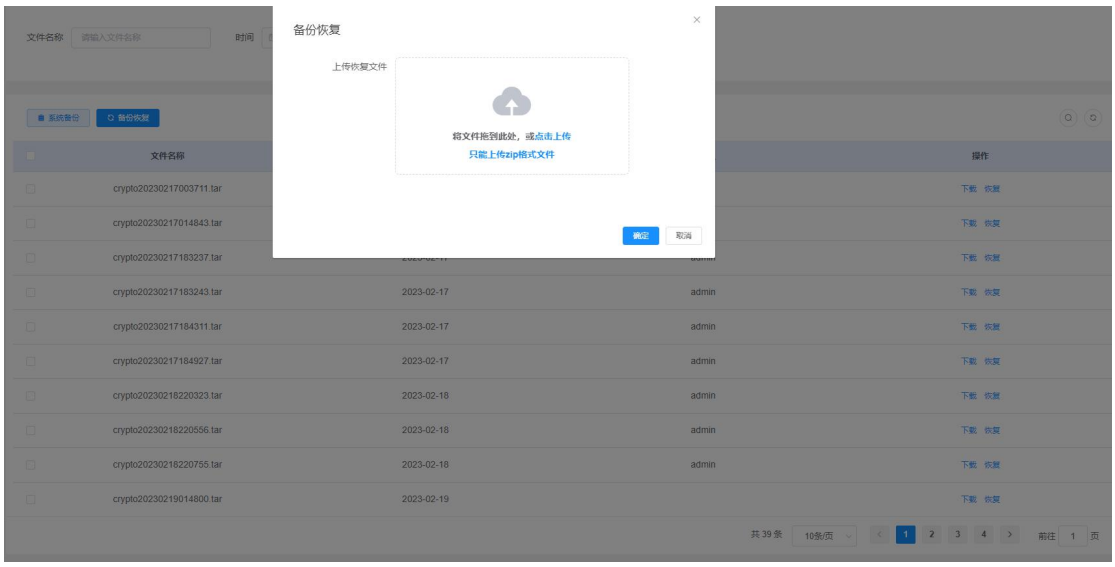


等待数据备份完成后，自动转跳至系统备份文件下载页面，点击保存后可下载备份文件（请妥善保管好备份数据）



3.5.8.2 系统恢复

依次点击菜单栏的系统恢复与备份->系统恢复，可对系统中数据以及密钥文件进行数据恢复，请上传在系统备份中备份的数据后。点击上传



3.6 审计管理员用户

以审计管理员身份登陆 WEB 管理系统，该管理员操作日志、登陆日志、SSL 用户日志的查看、审计、导出功能。

3.6.1 日志管理

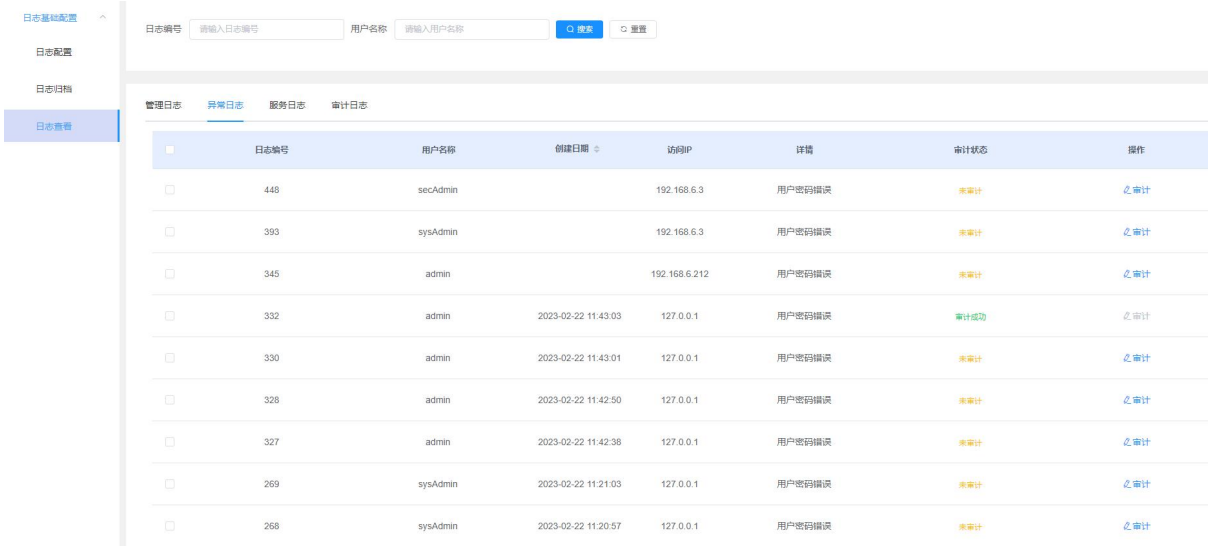
3.5.1.4 日志配置

日志配置页面如下图所示，可以配置日志记录等级，日志记录等级分为“错误、警告、信息、调试”，支持同步 syslog 日志功能，以及配置 syslog 所在服务器的 IP，接口。设置审计日志循环签名周期（小时），设置日志阀值。

3.5.1.5 日志查看

3.5.1.5.1 查看、审计

管理日志、异常日志、服务日志、审计日志，可以根据选择的开始时间、结束时间。日志等级来过滤查询日志，从右侧多选框选择相对应的日志，点击“审计”按钮，即可对选择的日志进行审计。



3.5.1.6 日志归档

3.5.1.6.1 归档和恢复

日志归档和日志恢复直接点击按钮即可，在弹出的对话框点击【确定】，即可完成操作。