中安云科安全认证网关
用户操作手册

中安云科科技发展（山东）有限公司

2022 年 9 月

目录

1. 手册指南

1.1. 概述

本手册主要介绍中安云科安全认证网关的使用及维护。其中涵盖了中安云科安全认证网关所涉及的配置方法及其使用说明。

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安全认证网关，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

2. 环境说明

本章讲述安装中安云科安全认证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. 配置环境

1. JDK 1.8 或 JDK 11 及以上，建议使用 JDK 1.8
2. MYSQL 5.7.34 及以上
3. Redis x64 3.2 及以上
4. MinIO

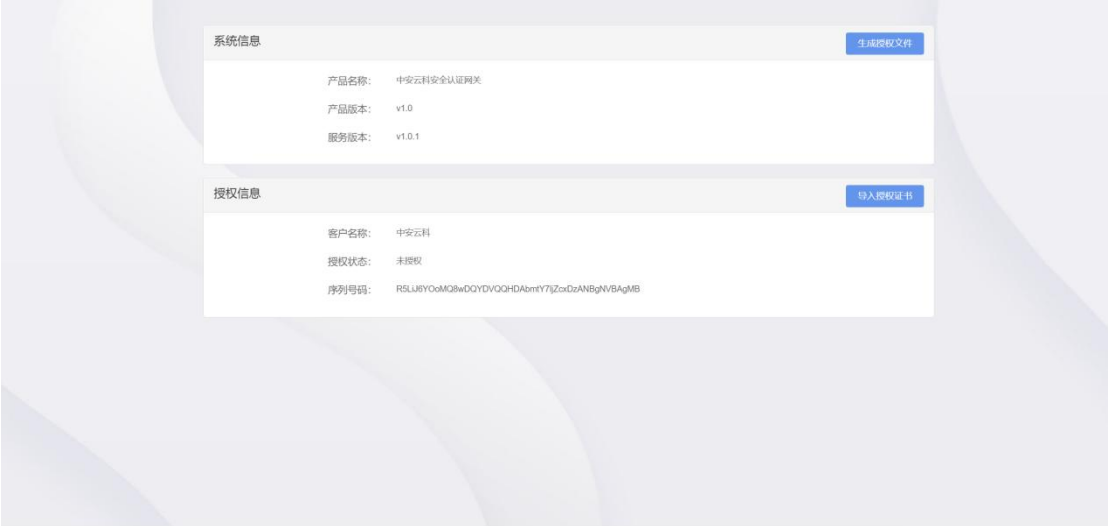
3. 功能操作使用说明

3.1 设备管理

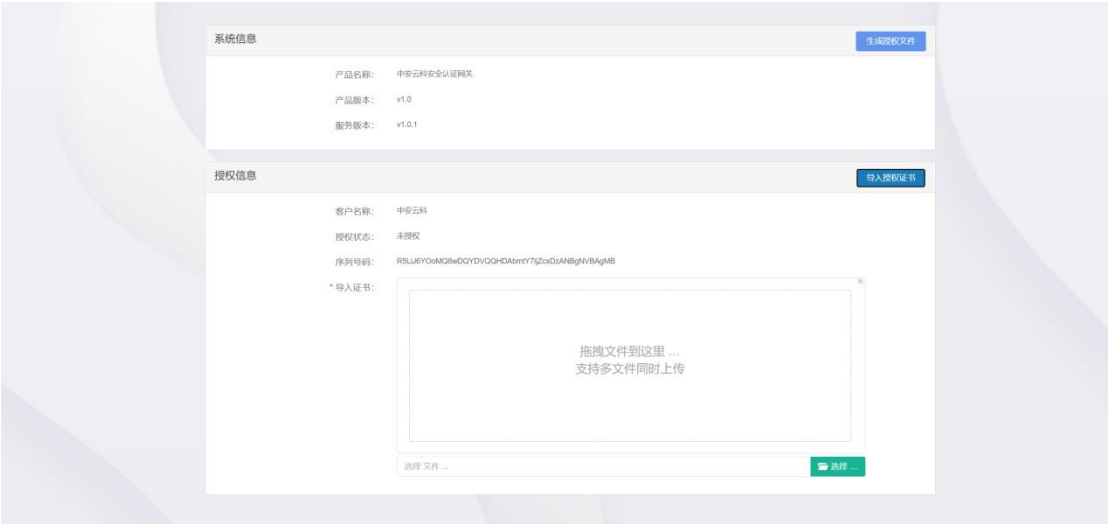
3.1.1. 设备授权码

首次访问中安云科安全认证网关会进入上传设备授权码页面，需要上传合法的授权码证书才能进入到设备初始化界面。

1.首先需要点击生成授权文件，下载授权码。



2.点击导入授权证书，将下载的授权文件交给管理人员，由管理人员将此文件解析成授权证书，导入验证成功后进入初始化页面。



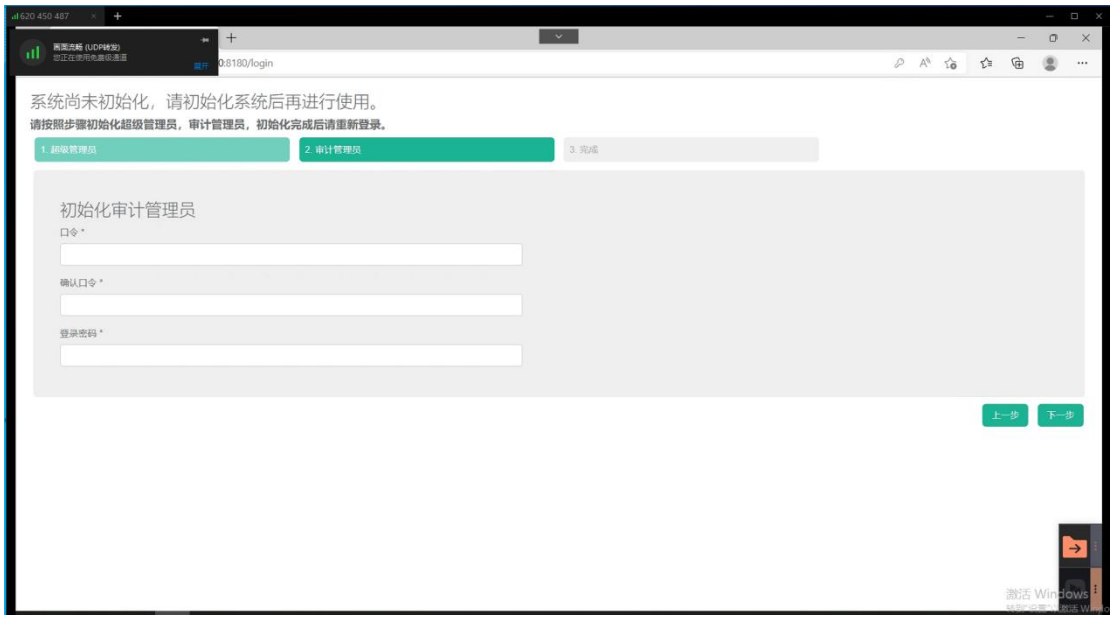
3.1.2. 设备初始化

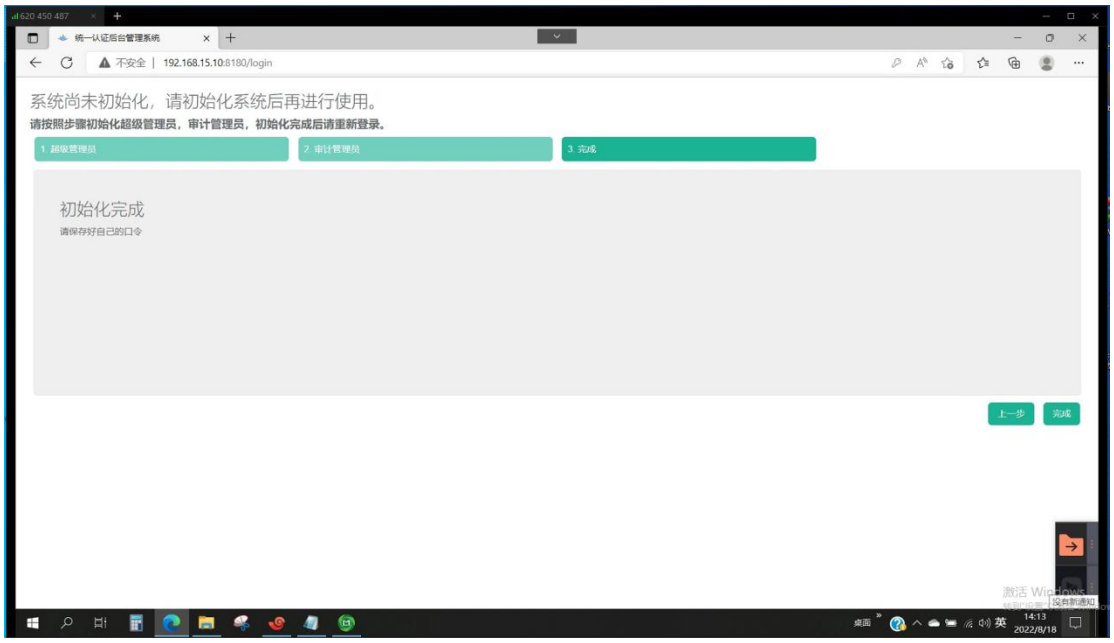
上传设备授权码成功后进入初始化页面、需要对超级管理员及审计管理员及设备完成初始化操作。

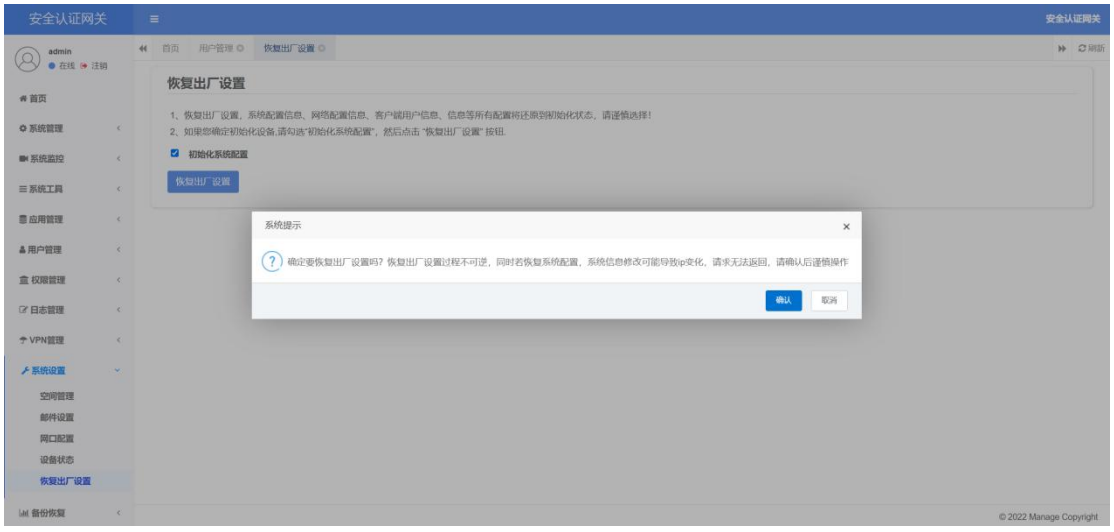
初始化管理员时需要插入已经导入证书的 UKEY，并保证托盘程序正常运行，完成初始化操作自动跳转登录页面。

说明：页面中的口令、确认口令为验证 UKEY 口令（默认 111111）。登录密码为设置平台登录密码。

初始化全部内容后，您可以登录超级管理员，若进行恢复出厂设置操作，将使安全认证网关重新进入未初始化状态。

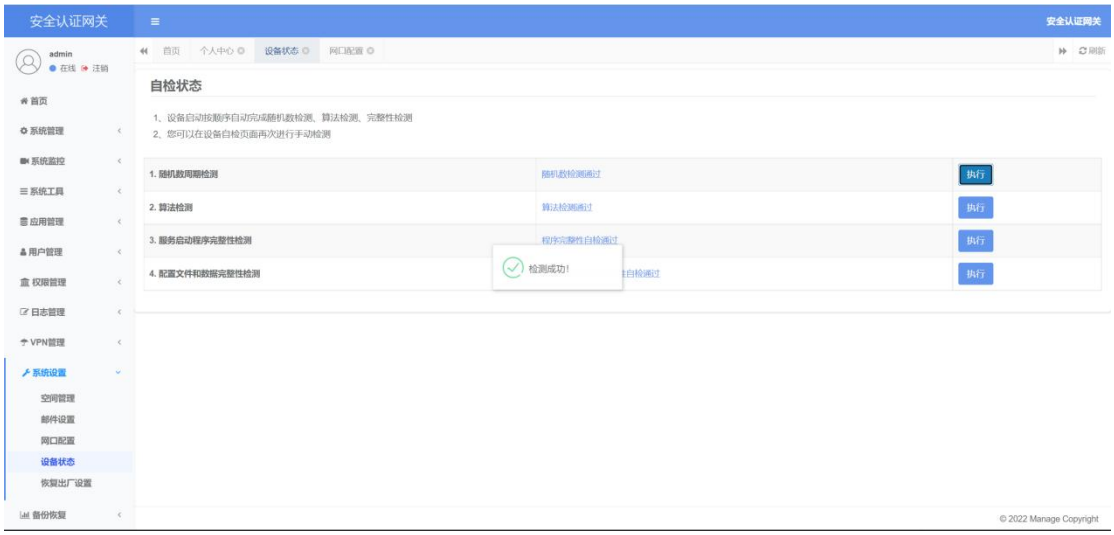

系统尚未初始化，请初始化系统后再进行使用。
请按照步骤初始化超级管理员，审计管理员，初始化完成后请重新登录。
1. 超级管理员
2. 审计管理员
3. 完成
初始化审计管理员
口令 *
确认口令 *
登录密码 *
上一步
下一步


统一认证后台管理系统
不安全 | 192.168.15.10:8180/login
系统尚未初始化，请初始化系统后再进行使用。
请按照步骤初始化超级管理员，审计管理员，初始化完成后请重新登录。
1. 超级管理员
2. 审计管理员
3. 完成
初始化完成
请保存好自己的口令
上一步
完成


安全认证网关
admin
首页
用户管理
恢复出厂设置
恢复出厂设置
1、恢复出厂设置，系统配置信息、网络配置信息、客户端用户信息、信息等所有配置将还原到初始化状态，请谨慎选择！
2、如果您确定初始化设备,请勾选"初始化系统配置"，然后点击"恢复出厂设置"按钮.
初始化系统配置
恢复出厂设置
系统提示
确定要恢复出厂设置吗？恢复出厂设置过程不可逆，同时若恢复系统配置，系统信息修改可能导致ip变化，请求无法返回，请确认后谨慎操作
确认
取消
© 2022 Manage Copyright

3.1.3. 设备自检

安全认证网关拥有设备自检功能。设备启动按顺序自动完成随机数检测、算法检测、完整性检测，登录后也可以在设备自检页面再次进行手动检测。

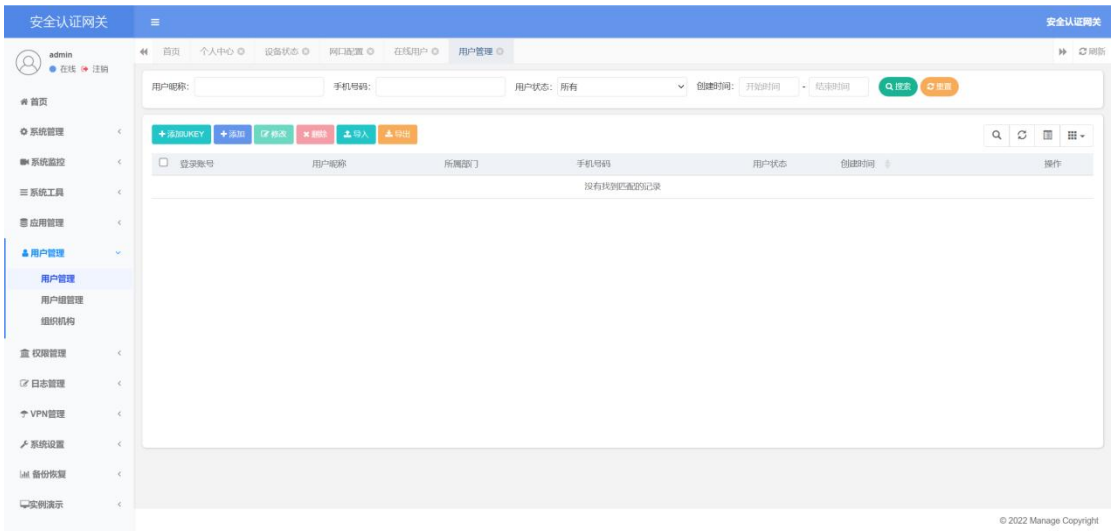


3.2 管理功能

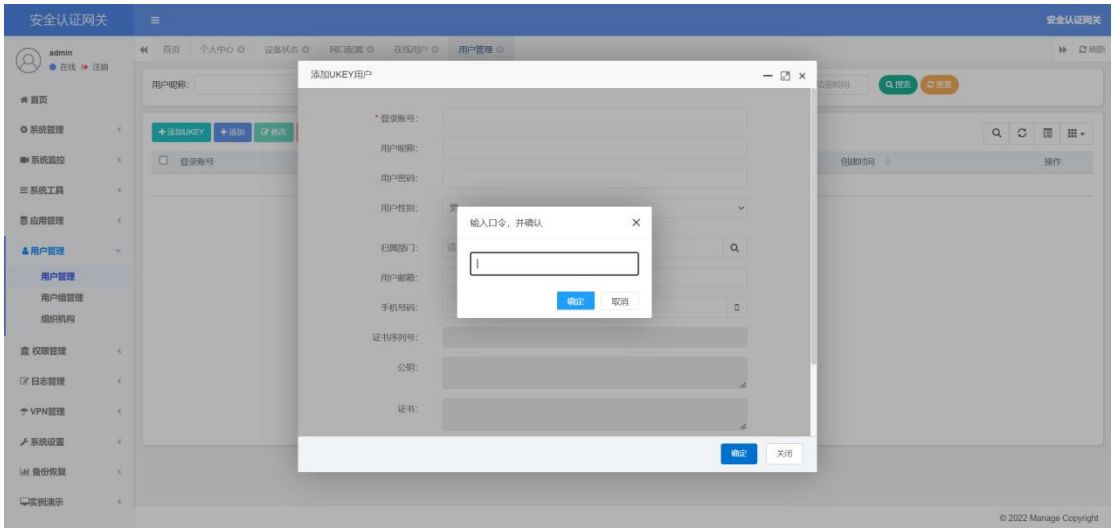
3.2.1. 用户管理

安全认证网关用户管理包含：

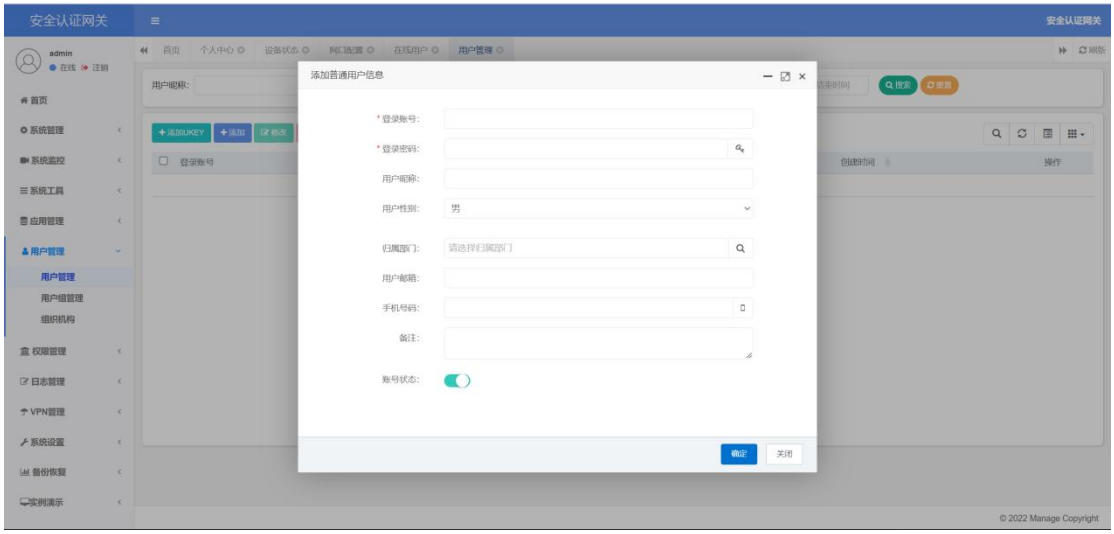
1. 普通用户管理，包含对用户的增删改查、导入、导出功能，其中普通用户的新增分为 UKEY 新增用户与普通新增用户，使用 UKEY 新增注册的用户，可以通过 UKEY 进行登录，普通新增的用户则只可以使用静态口令进行登录。
2. 用户组管理，包含增删改查、对用户的分组、对用户取消分组功能。
3. 组织机构管理，包含组织机构增删改查功能，在维护用户信息时可以绑定在此维护的组织机构信息，用户组织机构存在关联关系，则此组织机构无法删除。

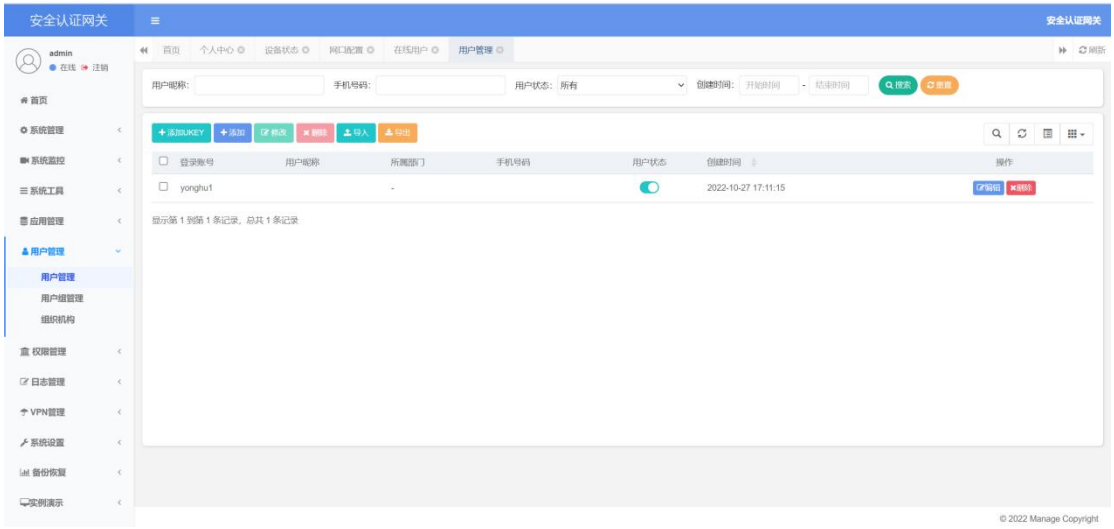


新增绑定 UKEY 用户，在验证口令阶段，拔下管理员 UKEY,换上即将新增用户的 UKEY,验证成功后拔下当前 UKEY,重新插上管理员 UKEY 完成保存操作。

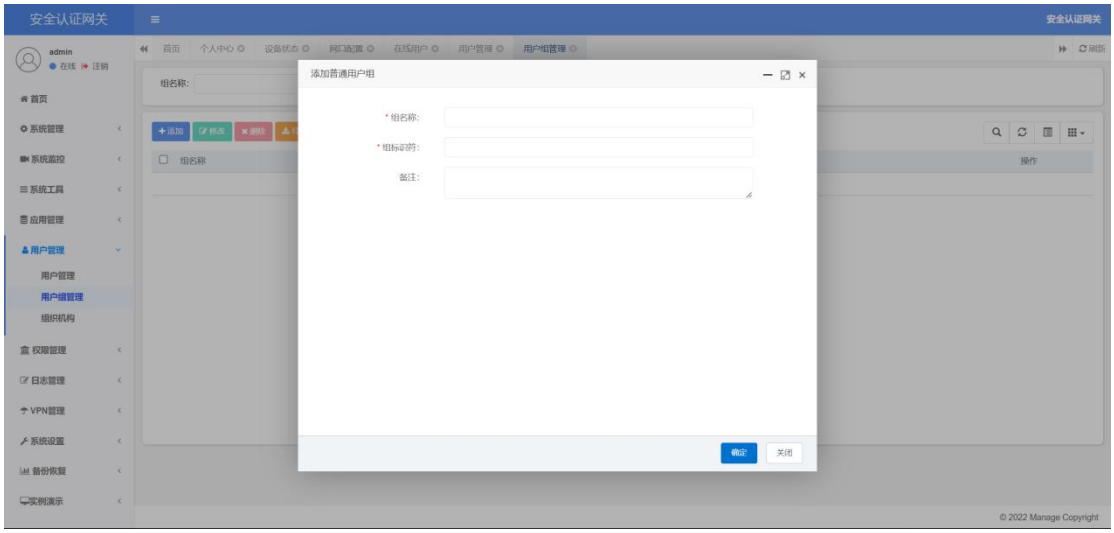


新增普通用户

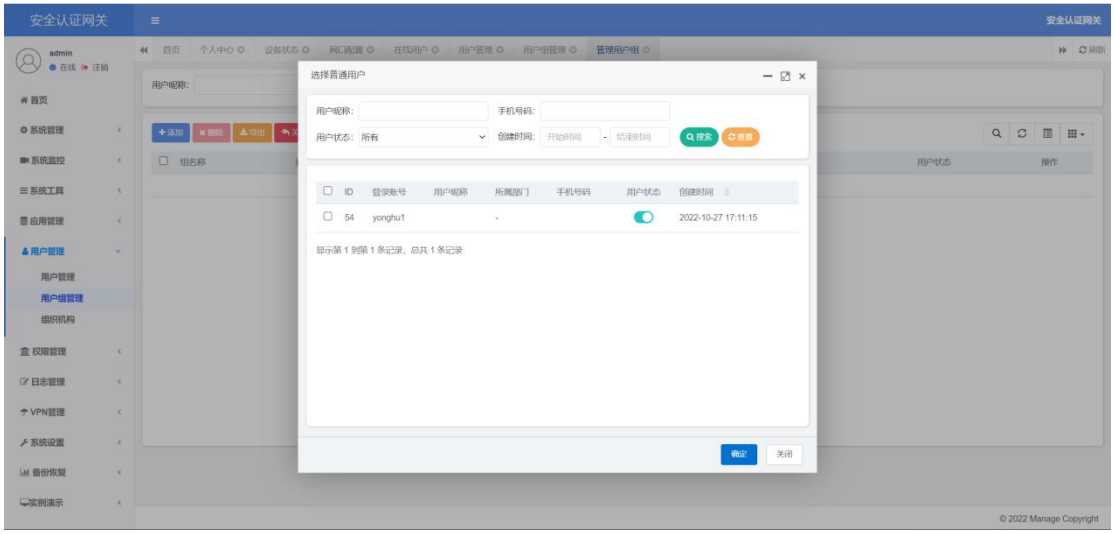




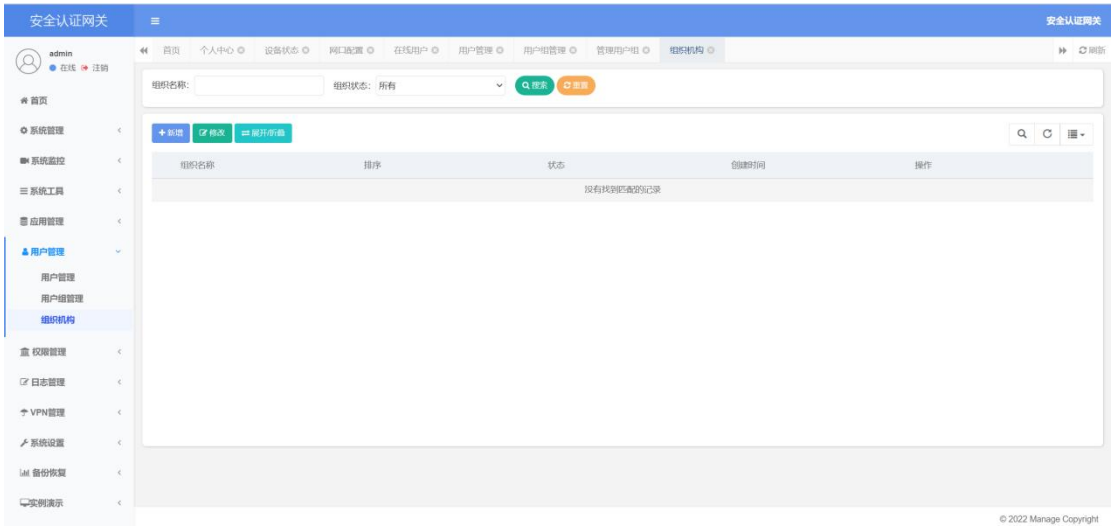
新增用户组



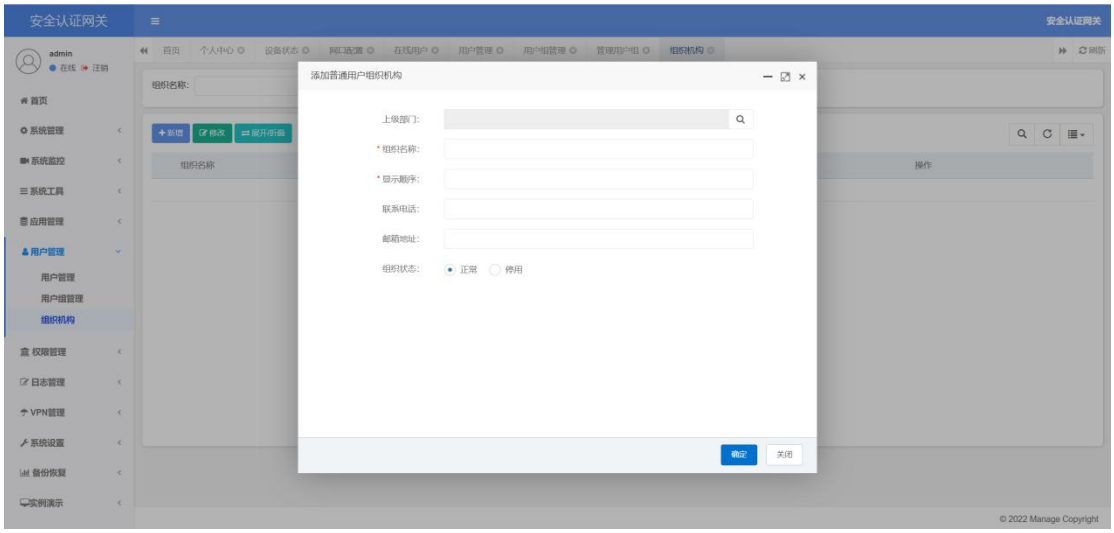
为用户组添加人员



组织机构



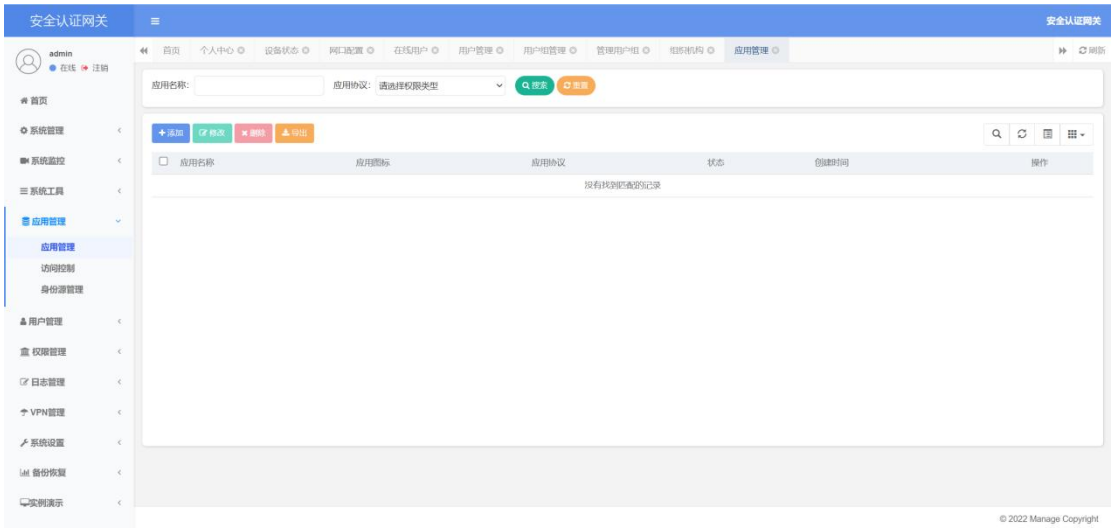
新增组织机构



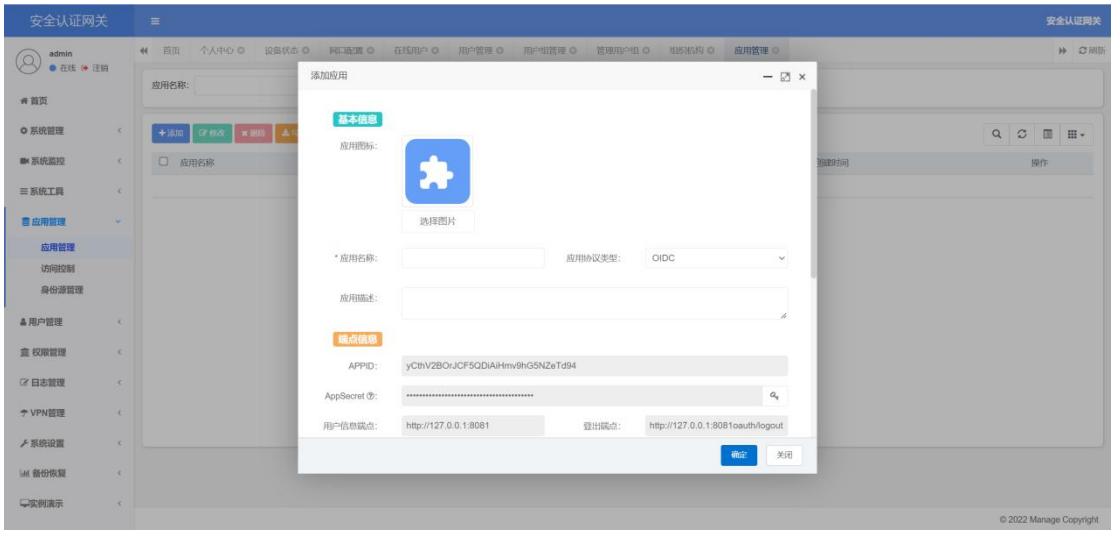
3.2.2. 应用管理

安全认证网关可以对需要保护的应用进行管理，能对应用信息进行增删改查。采用 OIDC 登录协议、支持 WEB 应用类型。

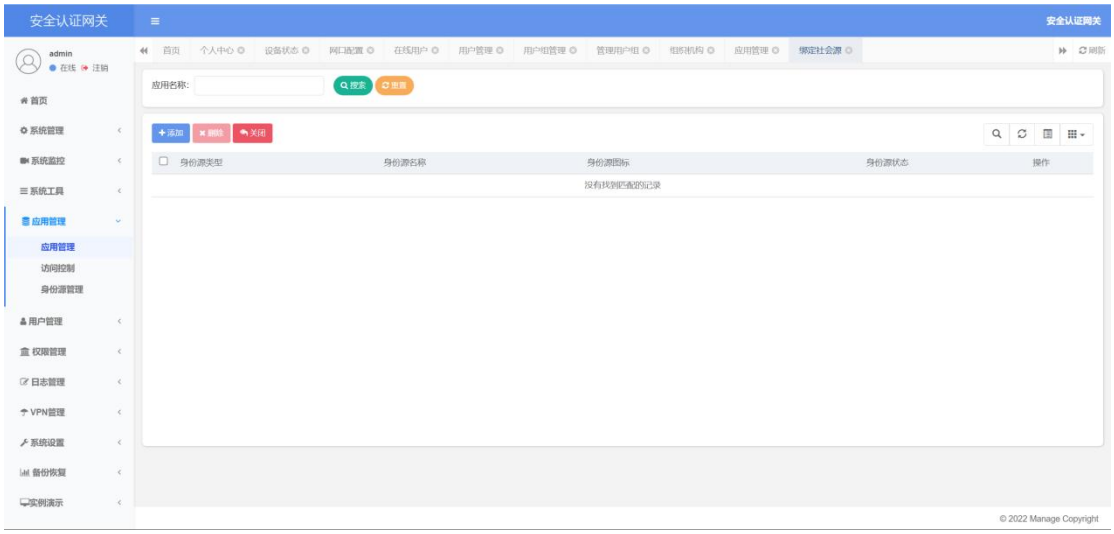
在更多操作中应用可以进行绑定身份源与登录配置，来自定义用户的登录方式。（身份源详细操作见身份源管理）



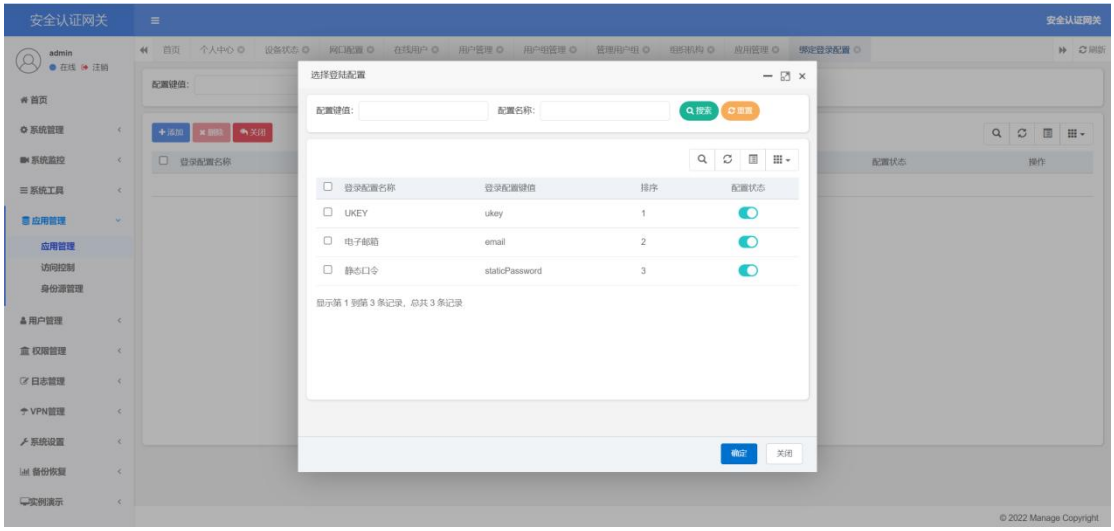
新建应用



为应用绑定社会源（社会源相关介绍与操作见 3.2.5）



为应用绑定登录方式（登录方式在字典中维护）

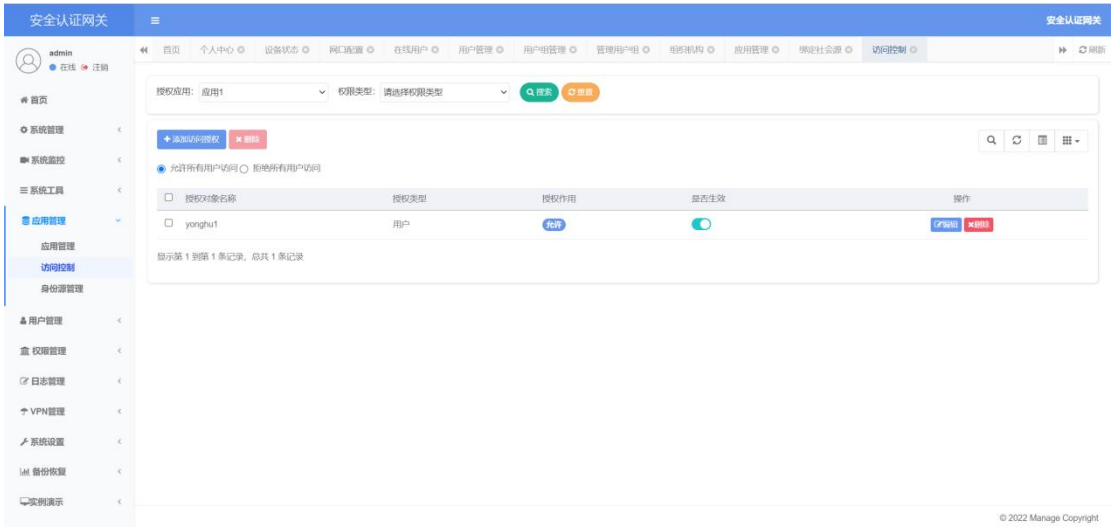


3.2.3. 访问控制

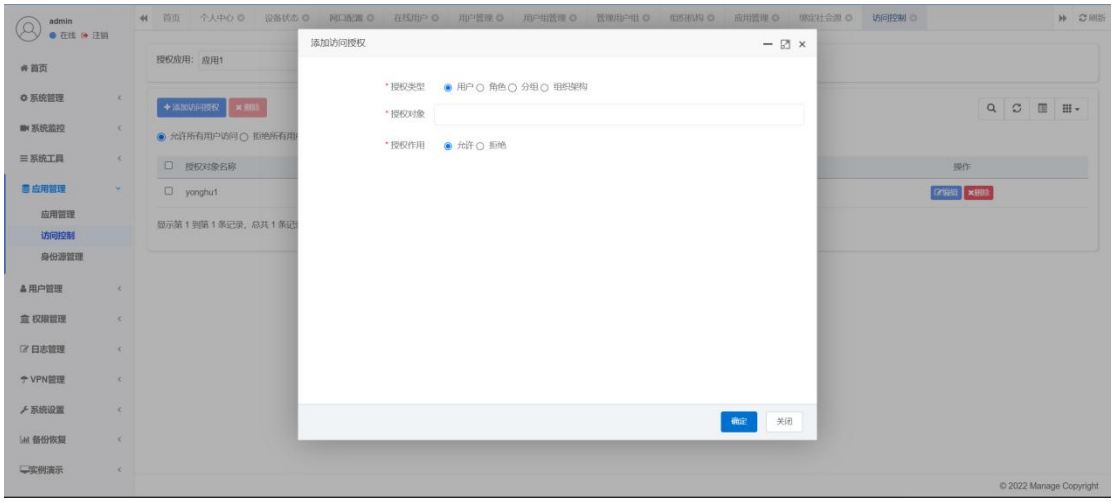
安全认证网关访问控制包括对应用的访问控制和对资源的访问控制。

对于应用的访问控制，可以采用黑名单的方式，也可以采用白名单的方式。当应用默认允许所有用户访问时，配置的黑名单对用户进行访问限制，对不在黑名单没有访问限制。当应用默认禁止所有用户访问时，配置的白名单内的用户没有访问限制。对不在白名单的其他用户有访问限制。

对于资源的访问控制，采用白名单的配置方式。用户使用客户端代理软件与安全认证网关建立 SSL 连接后，安全认证网关利用相应的访问控制模块和信息传递配置技术，当用户所在角色、用户所在组织有配置资源访问权限时，用户可以访问资源，否则用户不可访问资源。选择需要进行访问控制的应用进行自定义配置。



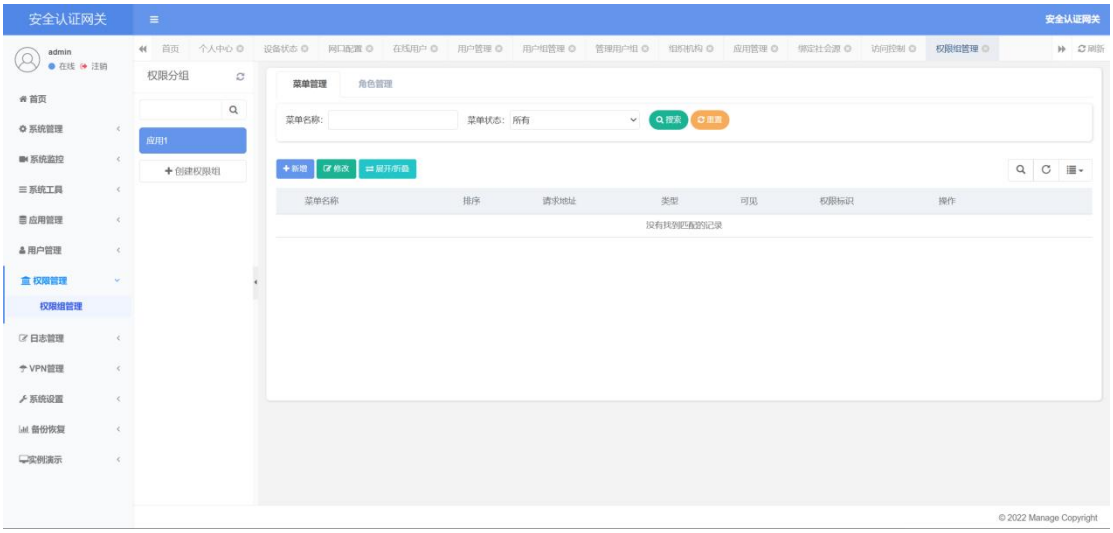
可以选择指定用户、角色、分组、组织机构进行访问控制配置



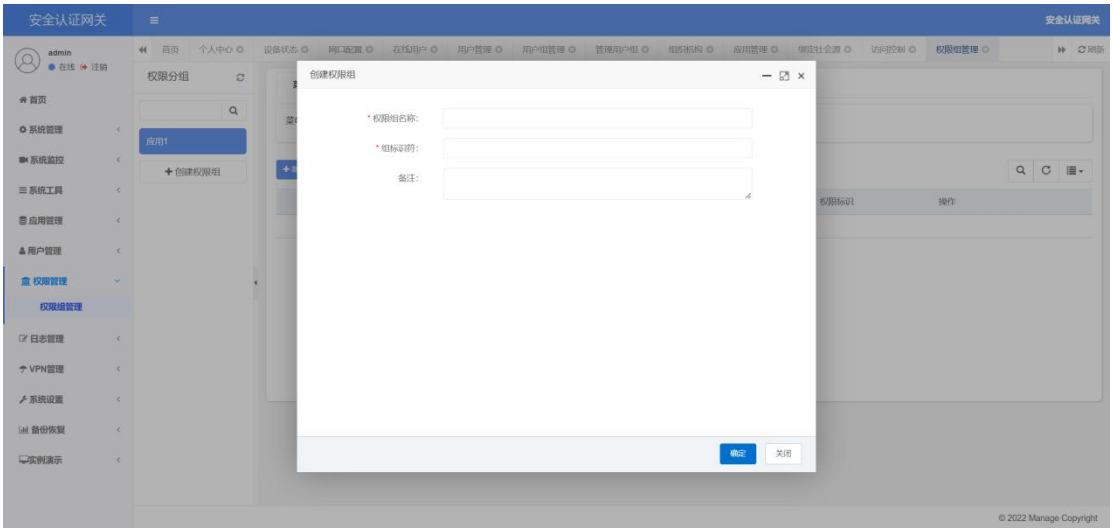
3.2.4. 权限组管理

安全认证网关对应用的访问控制和对资源的访问控制是基于权限组管理而言的，权限组作为一个特殊的隔离单位包含了资源、角色的配置，一般操作顺序为：建立权限组→建立资源菜单→建立角色并为所建立的角色绑定资源菜单→为角色分配用户或组织机构。

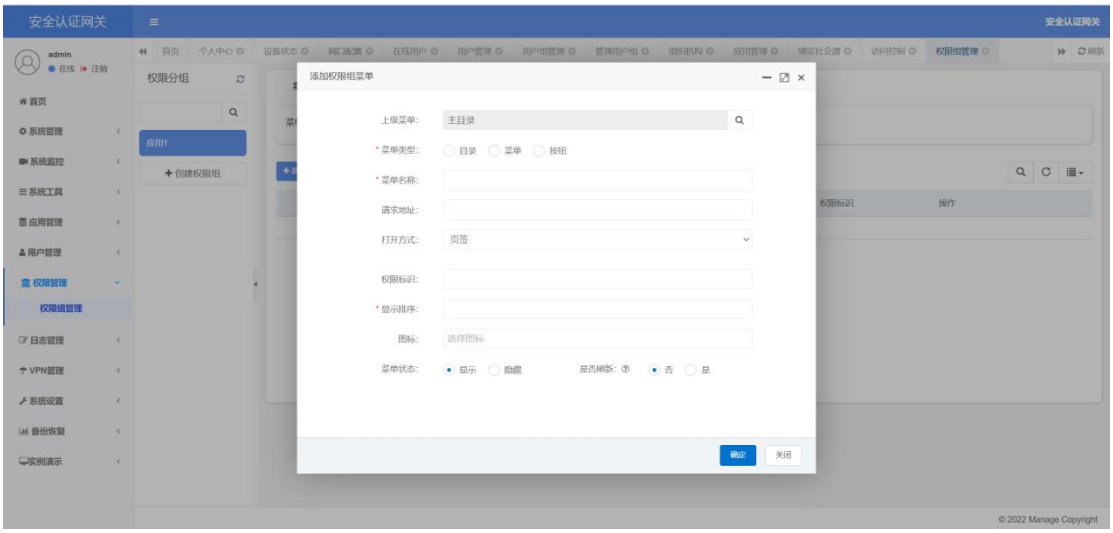
权限组和应用也可以是存在直接绑定关系的，管理员在创建应用的时候会自动创建一个与此应用关联的权限组，并且此权限组不能直接删除，只有在删除应用时才能删除此权限组。

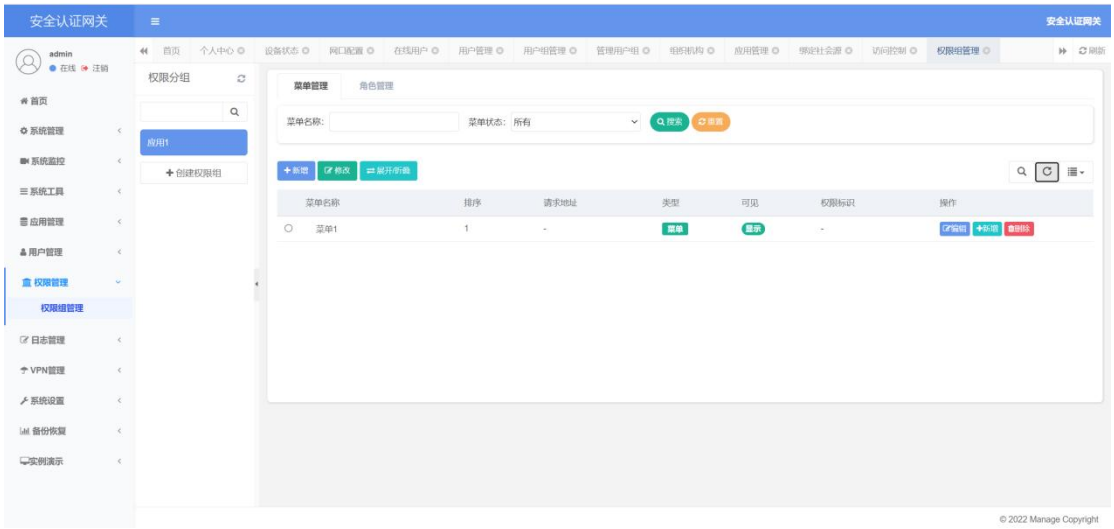


创建权限组

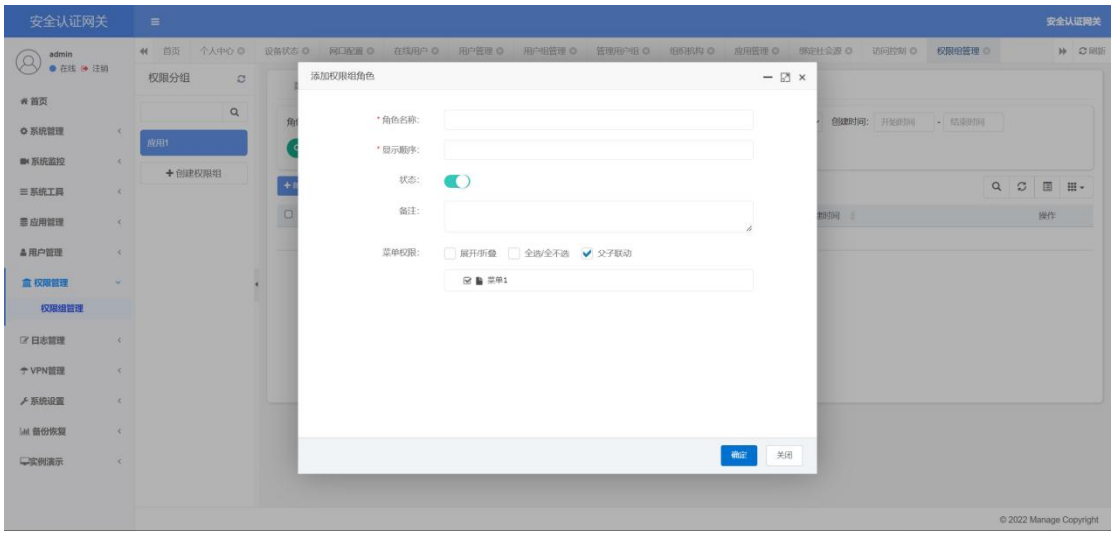


创建资源菜单

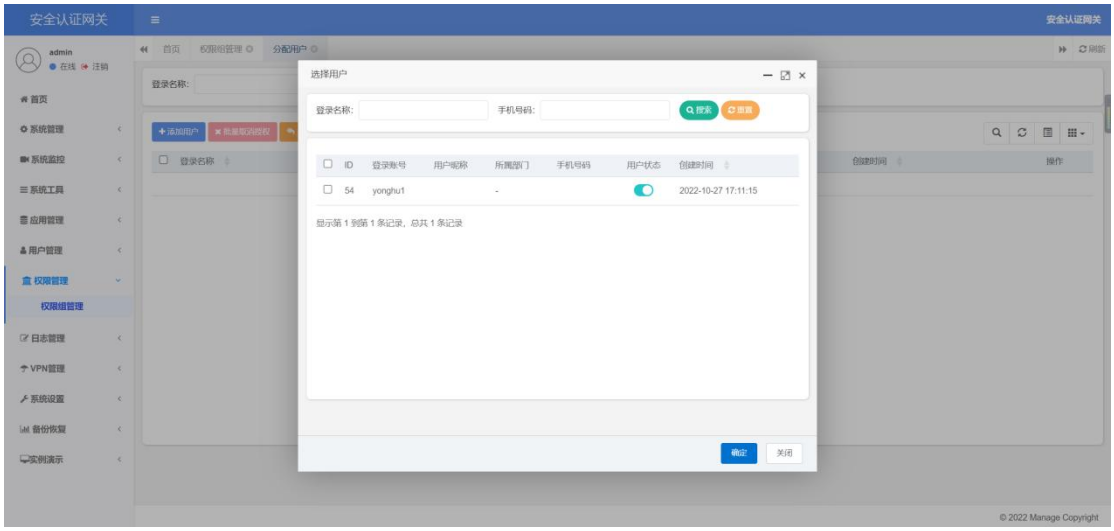




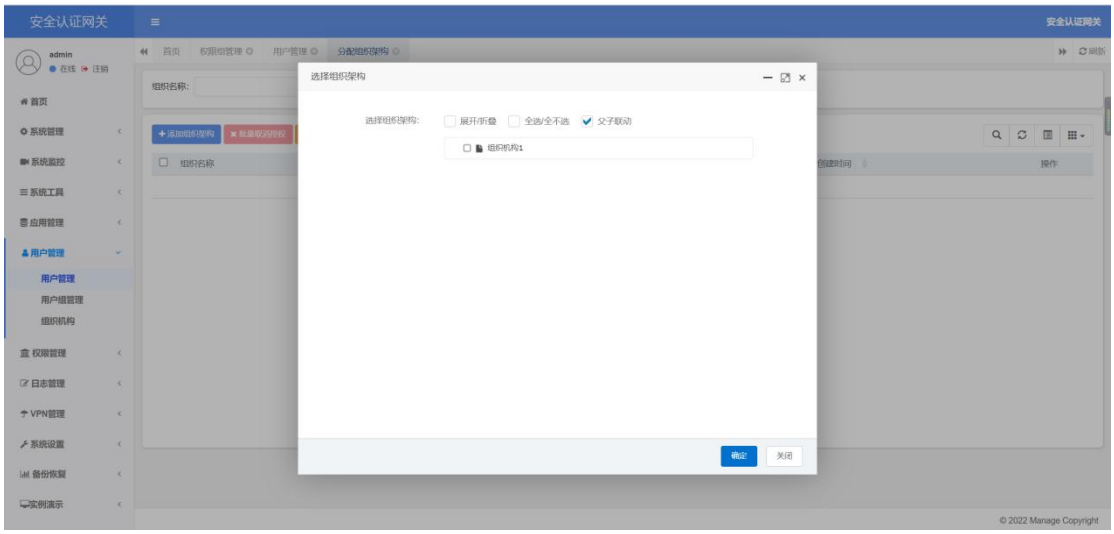
创建角色并绑定资源菜单



为角色分配用户



为角色分配组织机构

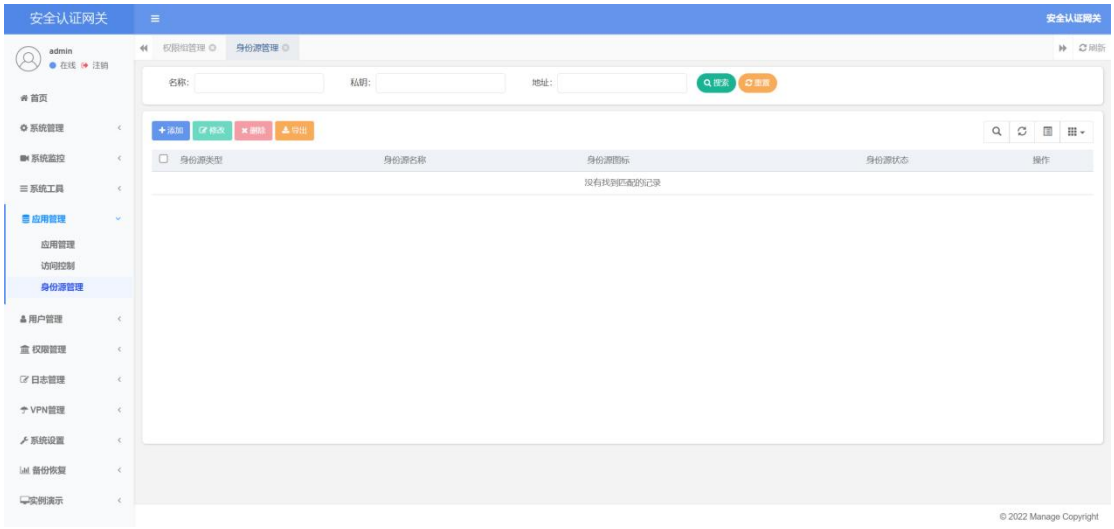


3.2.5. 身份源管理

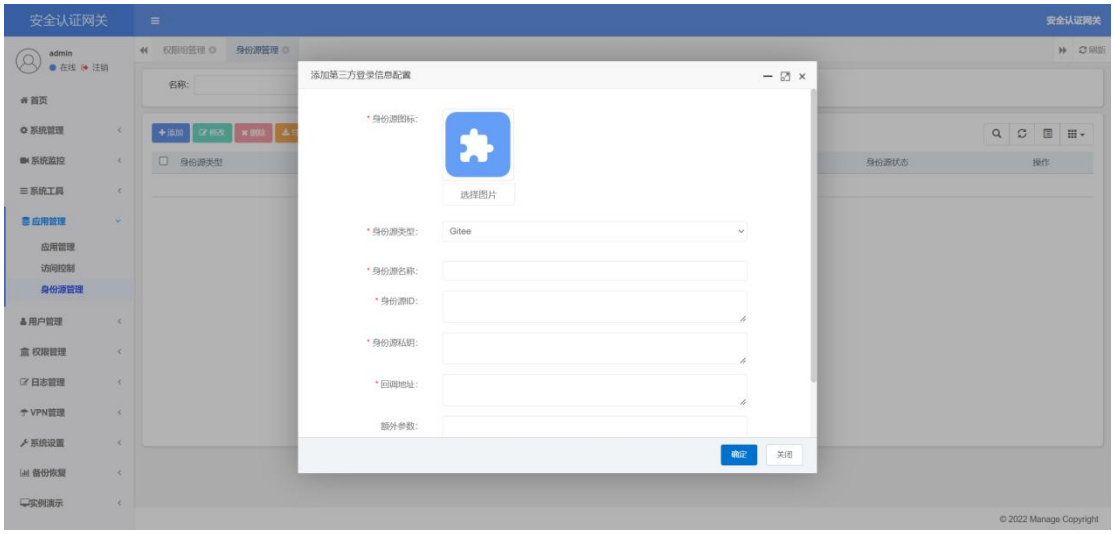
安全认证网关支持在管理端配置身份源登录应用信息，具体流程如下：

1.选择适合的身份源登录，例如 QQ、百度、微信等，注册对应平台的开发者账号，将平台信息配置到身份源对应的开发者平台中。

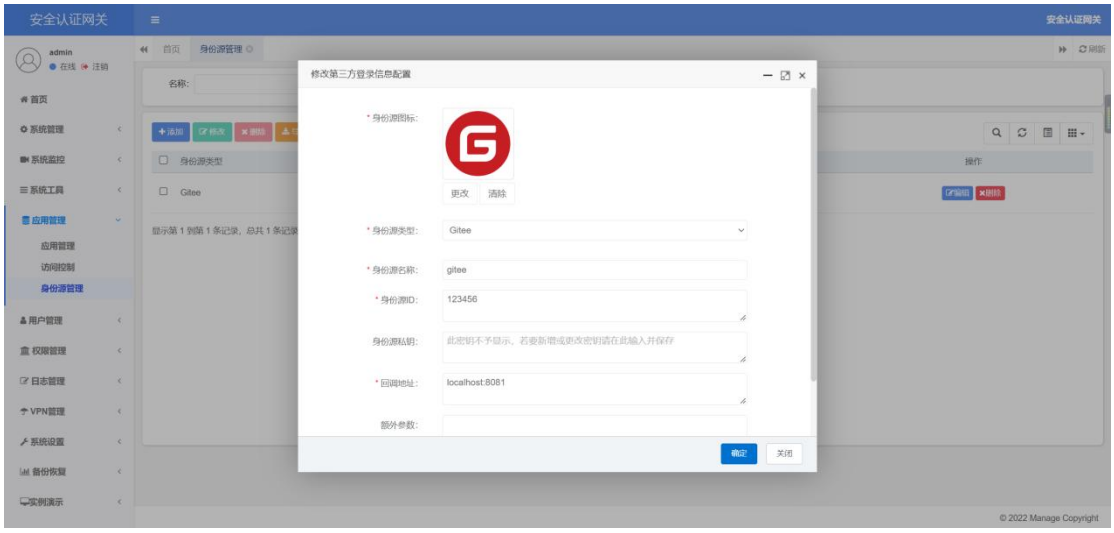
2.在安全认证网关管理平台进行配置，创建身份源完成后，身份源应用私钥会进行加密然后保存，并不会直接显示在配置信息里，如果需要修改私钥，可以直接填入新的私钥并保存。



新建身份源（身份源类型在字典中维护）



编辑身份源



3.2.6. 管理员管理

1、管理员创建、修改对登录密码强度进行规范、长度必须大于 8 位。

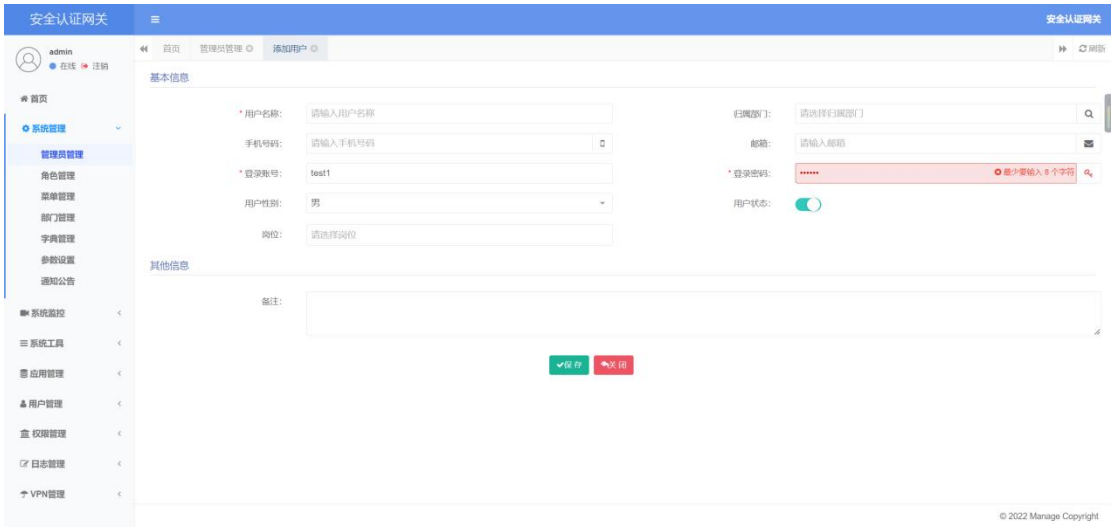
2、管理员登录采用双重认证、认证 UKEY 的 PIN 和登录密码。

3、管理员登录失败对密码错误次数进行计数、达到 5 次管理员账户将被锁定。

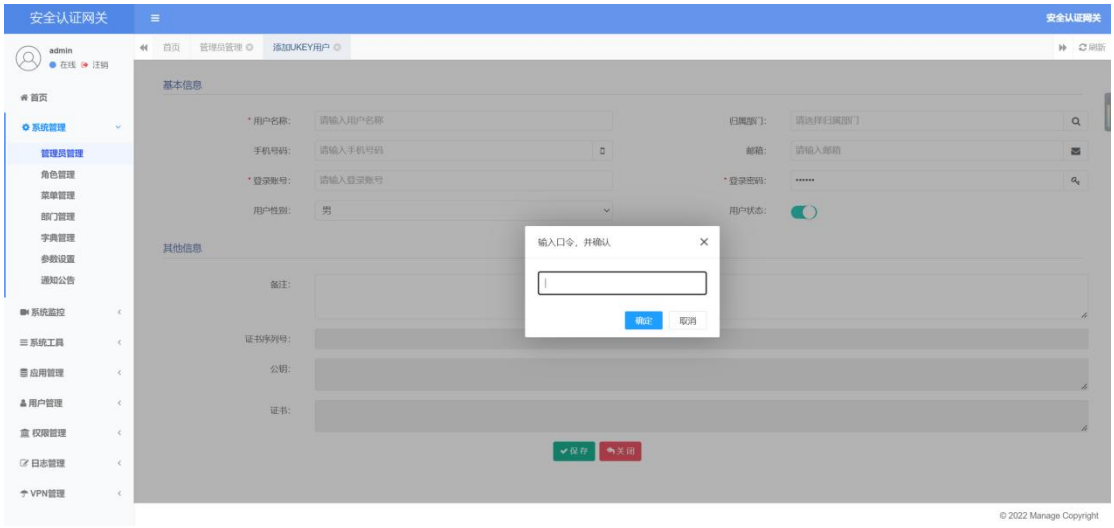
4、登录进行 UKEY 信息校验、硬件检测失败及 UKEY 信息失败将禁止登录。

5、为确保安全的授权访问，管理员必须使用代理软件，通过远程管理口，与安全认证网关建立 SSL 连接认证后，方可进行配置管理操作。其中 SSL 协议遵循《GM/T 0024-2014 SSL VPN 技术规范》，可以保证管理员与安全认证网关之间建立安全的加密通道，同时可基于 SM2 证书对于管理员和安全认证网关进行双向证书认证，并基于证书属性分配不同权限的配置管理操作。网关与远程用户终端和远程管理终端进行 SSL 协商时，安全认证网关会验证用户证书有效性，包括证书有效期、根证书验证以及证书撤销列表验证。

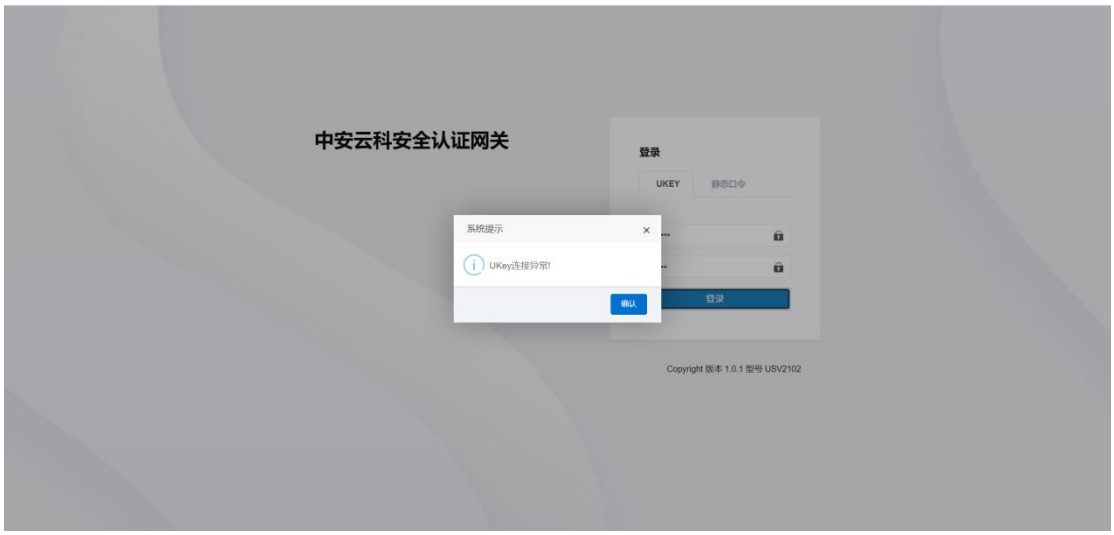
新增管理员



新增绑定 UKEY 管理员

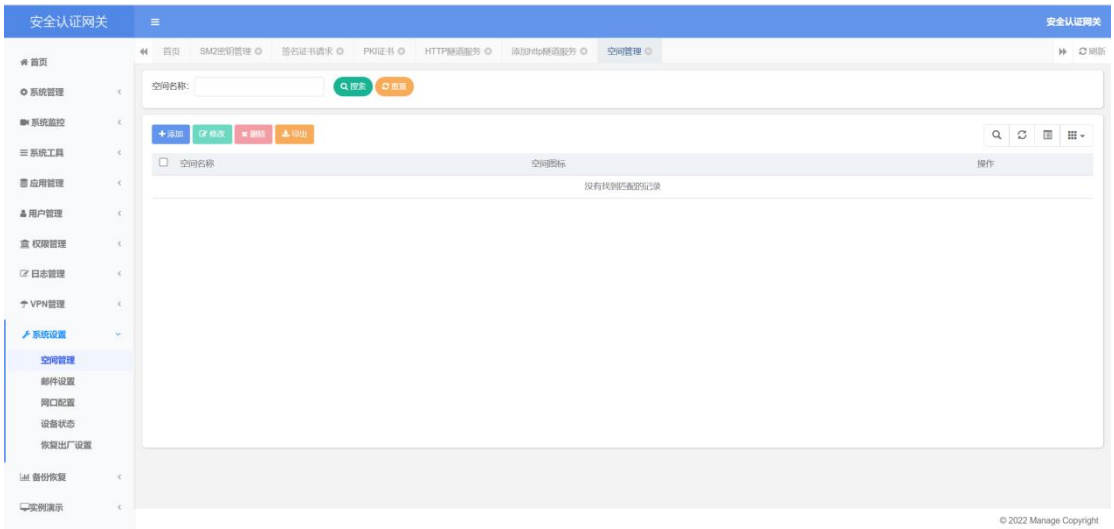


管理员登录时验证

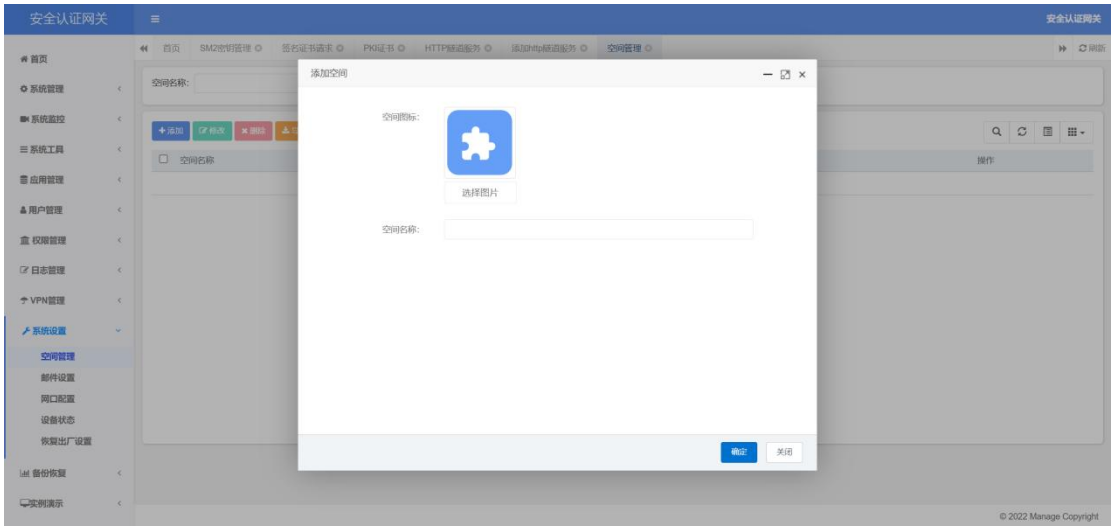


3.2.7. 空间管理

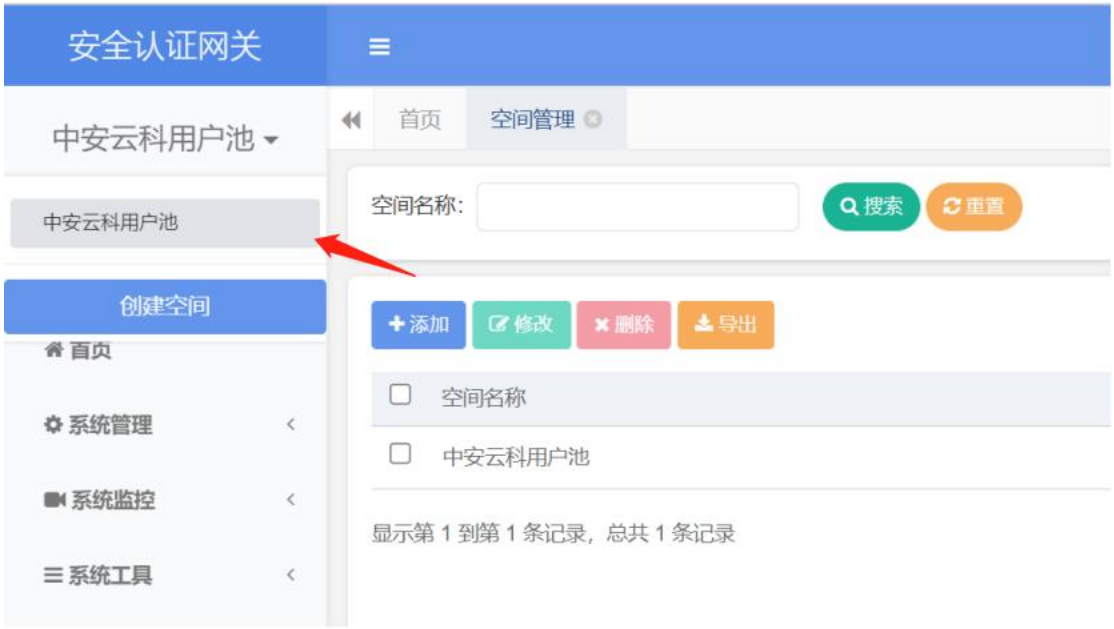
中安云科安全认证网关系统以用户空间隔离用户信息，每个用户空间用于一个完全独立的用户目录和应用等目录，您可以在管理界面管理指定用户空间的用户与应用等信息。



创建用户空间

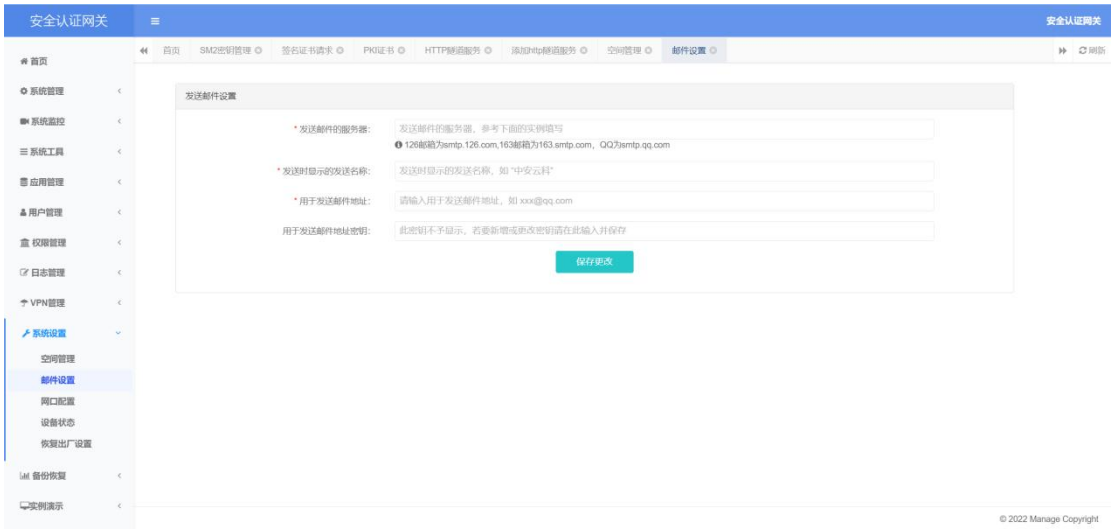


切换用户空间



3.2.8. 邮件配置

邮件配置用于用户端登录、绑定、解绑账号时发送邮件账户的配置，例如配置发送邮件的服务器、发送时显示的发送人名称、用于发送邮件的邮箱地址。



如何配置邮件信息？（这里使用 QQ 邮箱为例）

1. 进入 QQ 邮箱，在页面首部找到设置

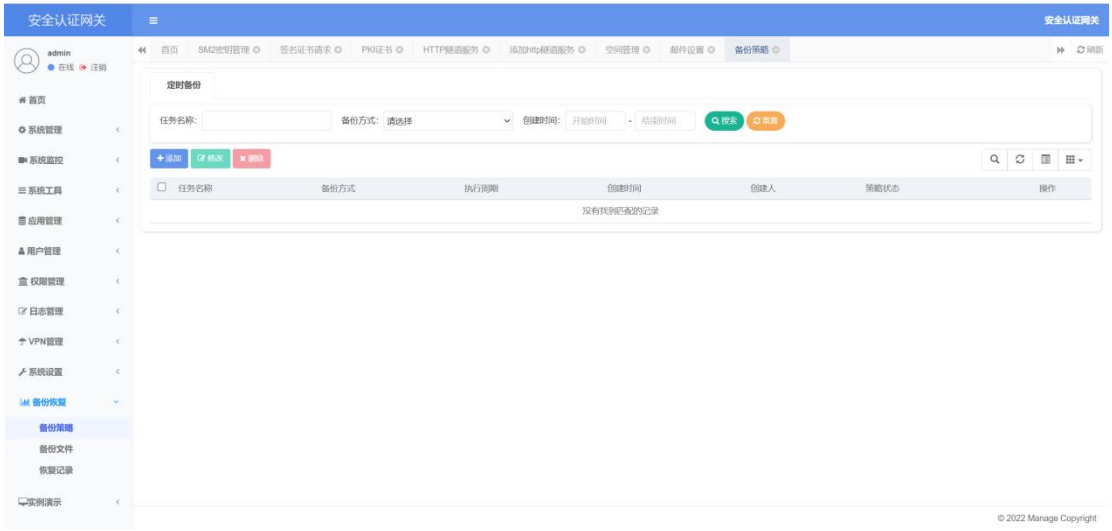
2. 开启 POP3/SMTP 服务

3.生成授权码，将授权码牢记，并填入 ’用于发送邮件地址密钥 ‘ 中保存

3.2.9. 备份恢复

备份恢复主要用于日常使用中的数据备份策略和数据丢失时的数据恢复功能，便于更安全可靠的使用此系统，您可以在备份策略中创建日常所需的备份策略，创建的策略会在您指定的时间段内备份数据，以防止系统因数据丢失而导致的损失。

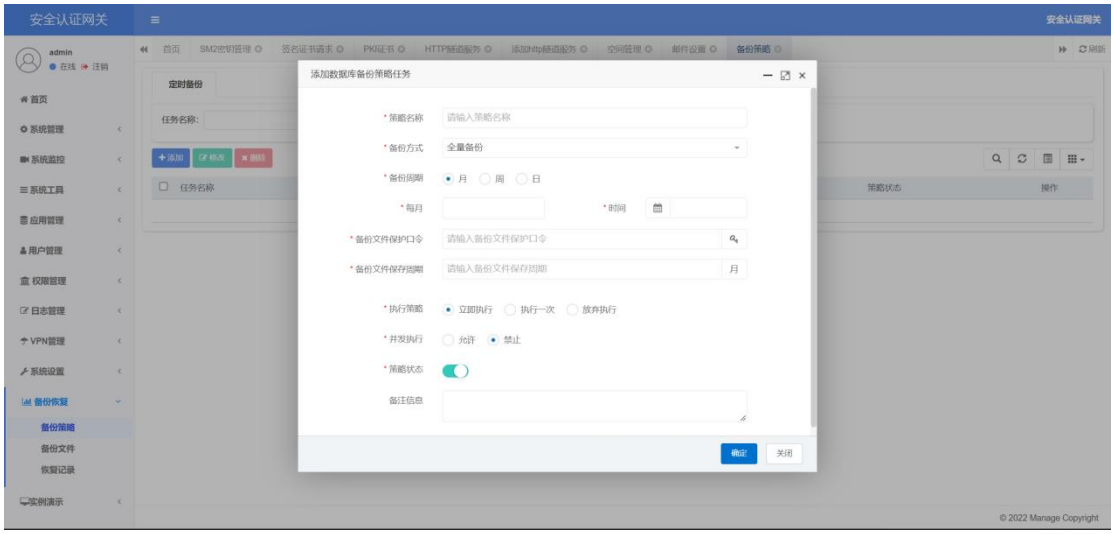
备份策略列表



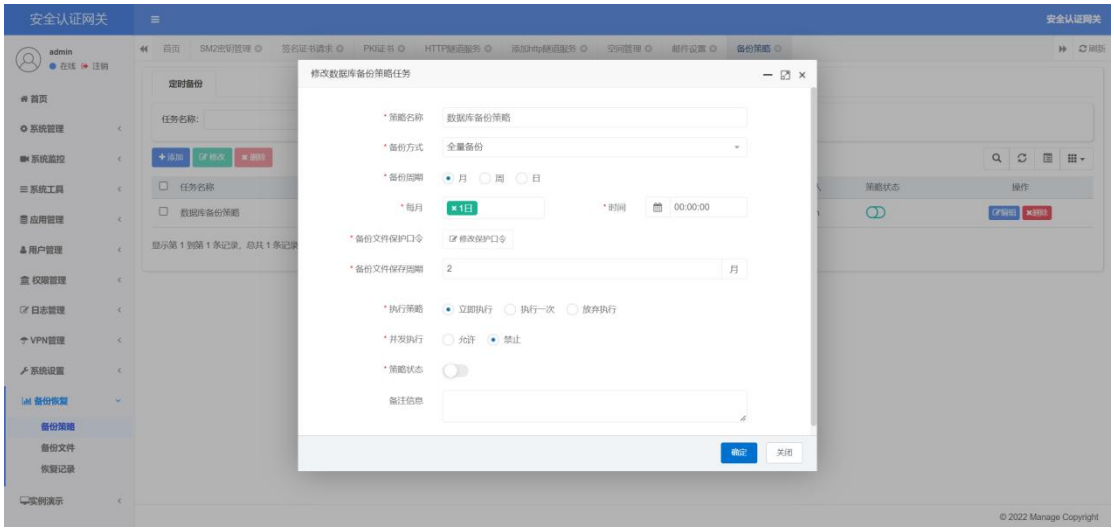
创建备份策略：

1. 您可以按每月，每周，或每日定时执行您创建的备份策略任务，在创建任务时，您需要设置一个保护口令和保存周期。
2. 在执行此备份策略任务时会创建备份文件，在您下载这个文件并想用这个文件进行数据恢复时需要用到您设置的保护口令，否则不能进行恢复。
3. 保存周期按月设置，在您设置完成后，生成的备份文件会在您设置的周期到期后删除。

创建数据库备份策略任务

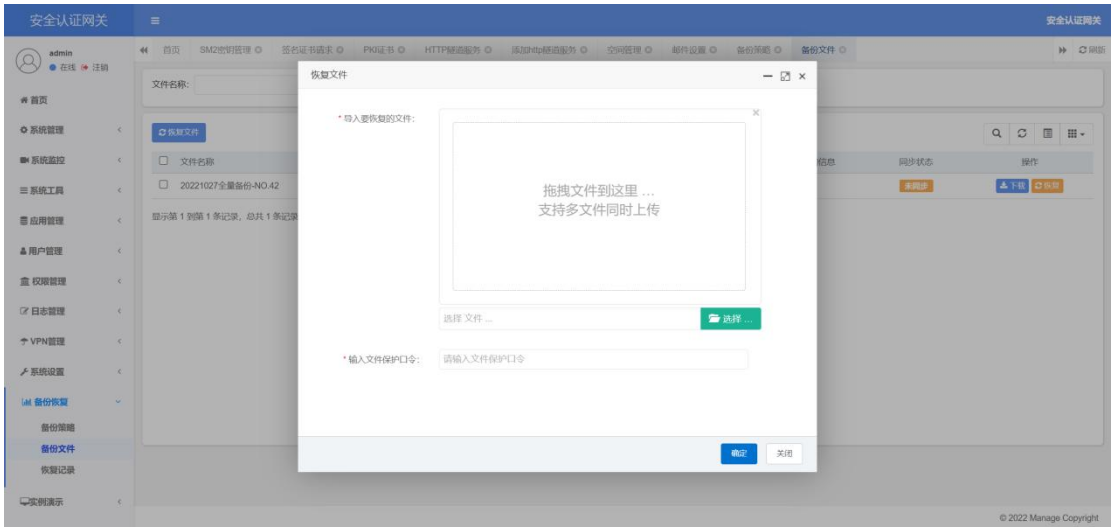


修改数据库备份策略任务（修改保护口令需要用到原口令）

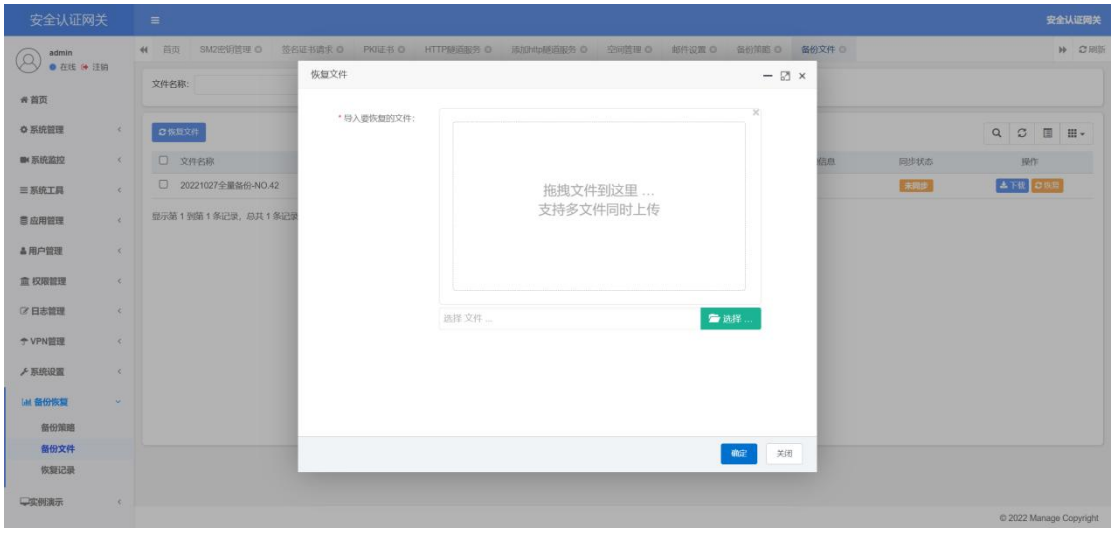


备份文件：

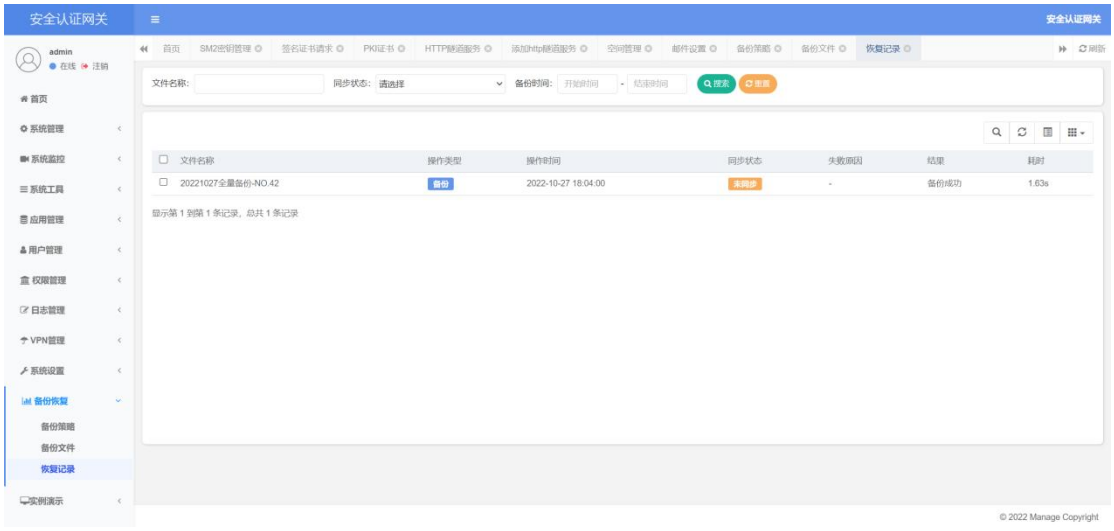
1. 备份策略任务到时间开始执行时，会生成加密过的备份文件，您可以在备份文件或备份恢复记录中看到执行的任务文件信息。
2. 在备份文件中，如果需要恢复数据，首先点击列表中的下载按钮，将加密过的文件下载，然后点击恢复按钮，上传刚才下载的文件并输入保护口令。



恢复文件不需要口令（列表头部的'恢复文件'按钮）需要上传没被加密过的 .SQL 文件



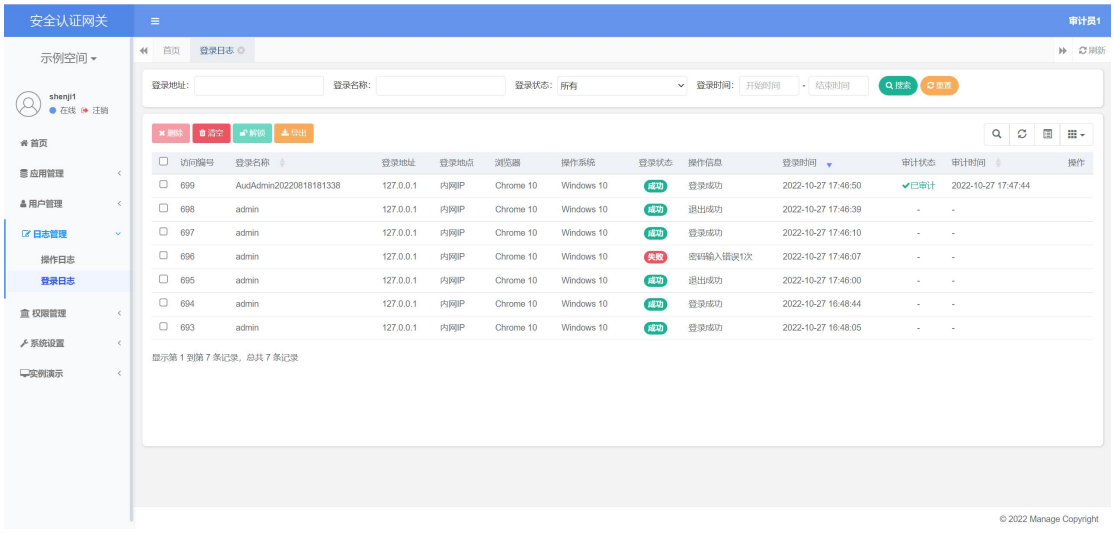
备份与恢复记录



3.2.10. 信息审计

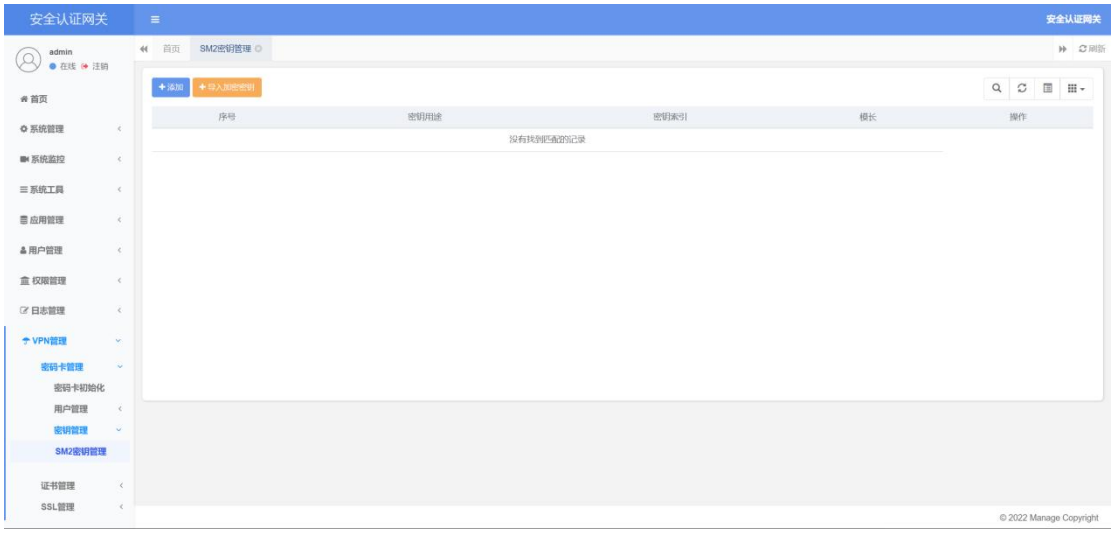
安全认证网关记录用户登录信息及操作信息。

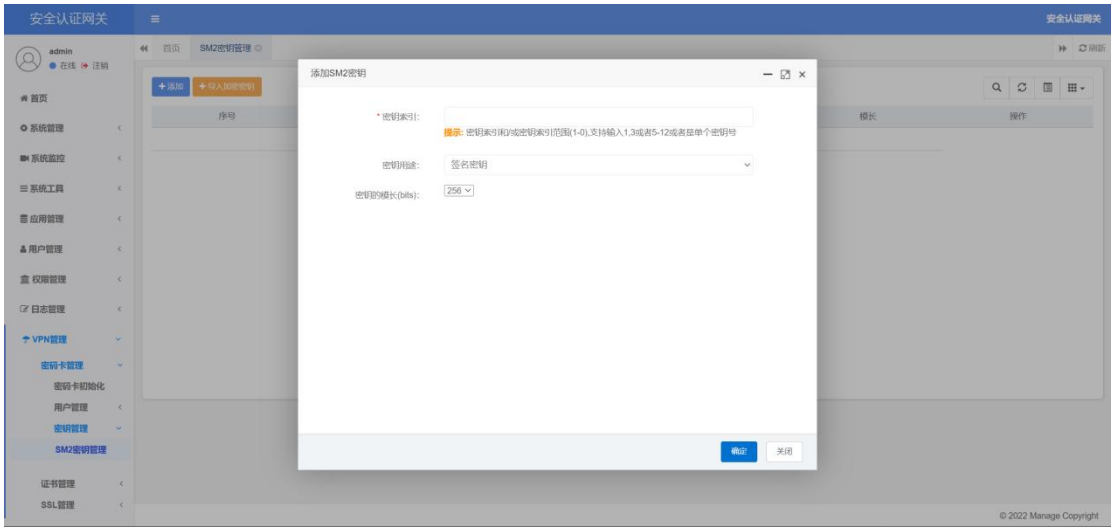
用户通过访问后，安全认证网关能够对用户访问信息进行详细记录，记录结果符合GM/T 0026-2016《安全认证网关产品规范》中 7.1.6 要求，记录信息包括：时间、用户 IP、用户证书信息、时间类型、访问资源、访问结果、错误原因、成功或失败标识。



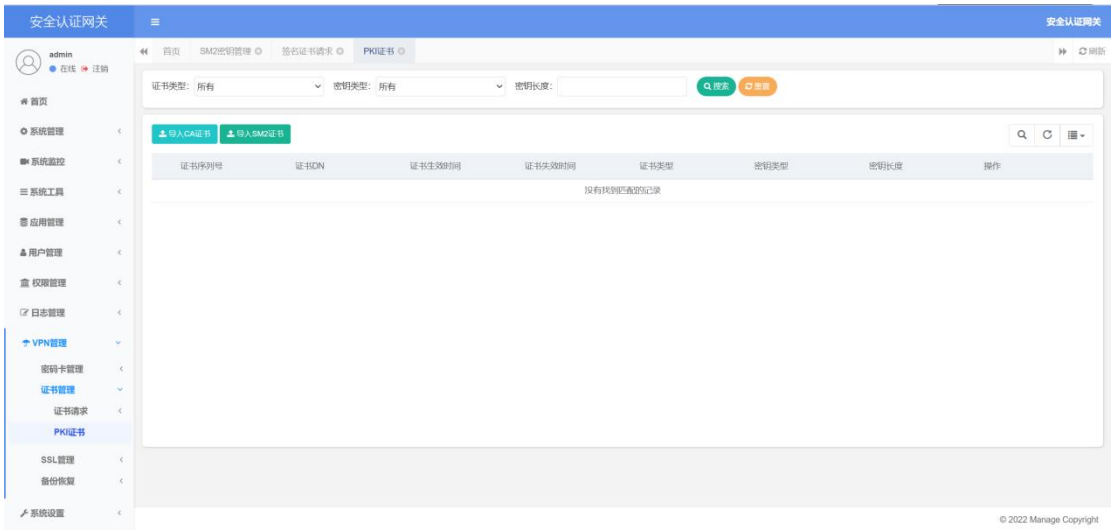
3.2.11. 密钥安全

安全认证网关对密钥信息、证书信息进行管理，密钥可以初始化和更新、证书信息拥有申请证书请求、导入、删除等功能。




安全认证网关
admin
首页
SM2密钥管理
添加SM2密钥
* 密钥索引:
密钥用途:
签名密钥
密钥的模长(bits):
256
确定
关闭
© 2022 Manage Copyright


安全认证网关
admin
首页
SM2密钥管理
签名证书请求
申请方式:
离线申请
* 名称(CN):
邮箱(E):
* 国家(C):
CN
省(ST):
市(L):
县(L):
组织机构代码(T):
* 组织(O):
* 部门(OU):
密钥:
-----请选择密钥-----
生成的PKCS10:
© 2022 Manage Copyright


安全认证网关
admin
首页
SM2密钥管理
签名证书请求
PKI证书
证书类型:
所有
密钥类型:
所有
密钥长度:
搜索
重置
导入CA证书
导入SM2证书
证书序列号
证书DN
证书生效时间
证书失效时间
证书类型
密钥类型
密钥长度
操作
没有找到匹配的记录
© 2022 Manage Copyright

3.2.12. 管理安全

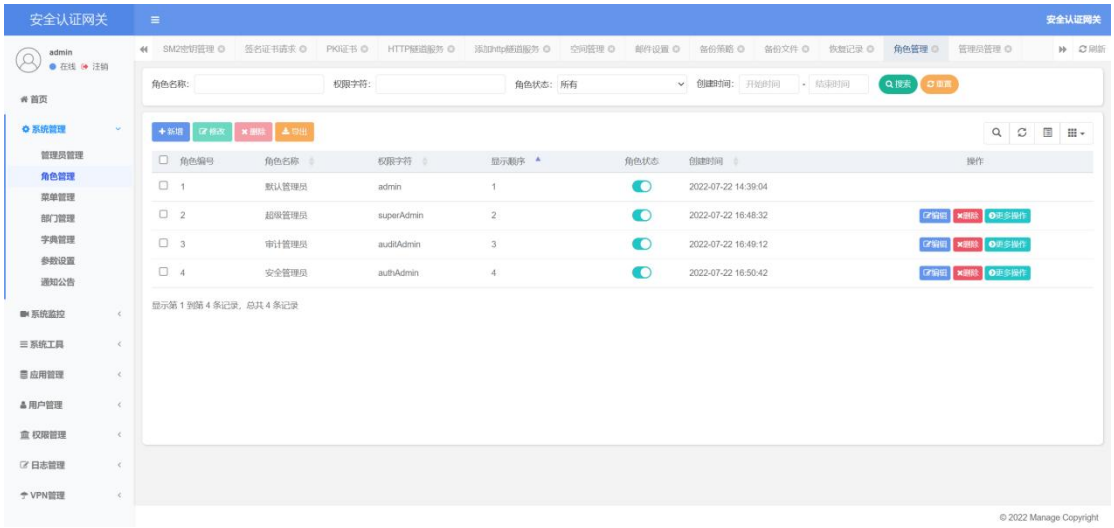
3.2.12.1. 分权管理

安全认证网关具有分权管理功能，包括超级管理员、审计管理员、安全管理员。

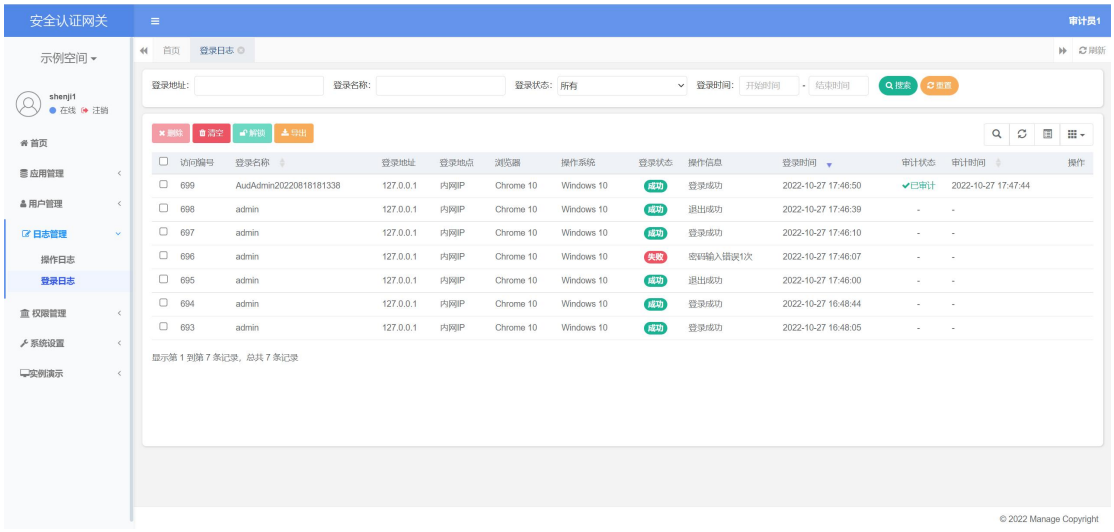
1、超级管理员，拥有管理员人员信息管理、平台参数管理、密钥管理、证书管理、SSL管理、设备管理等功能。

2、审计管理员权限包括日志管理，包含信息审计功能。

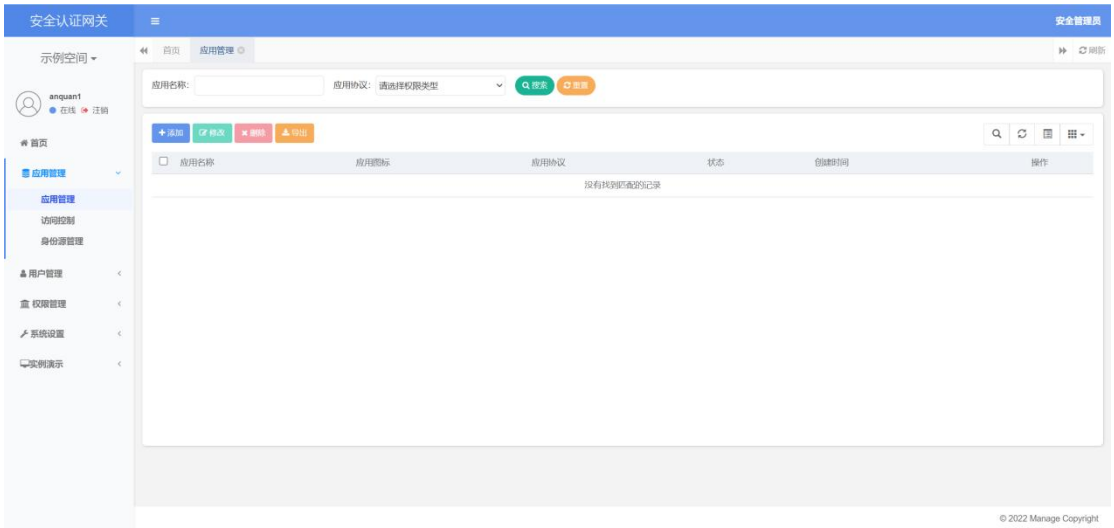
3、安全管理员包含应用管理功能、用户管理功能和权限管理功能。

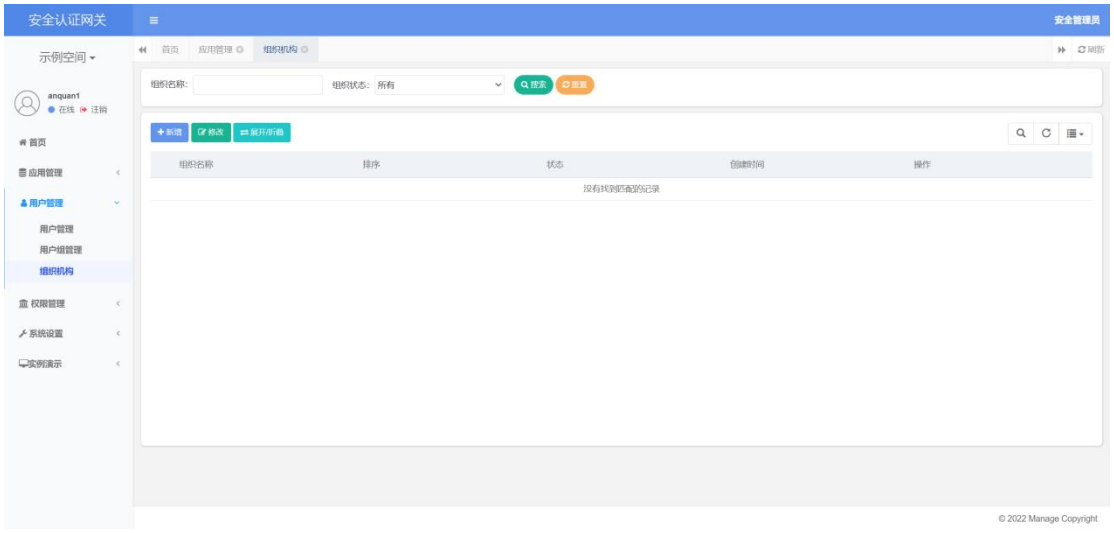


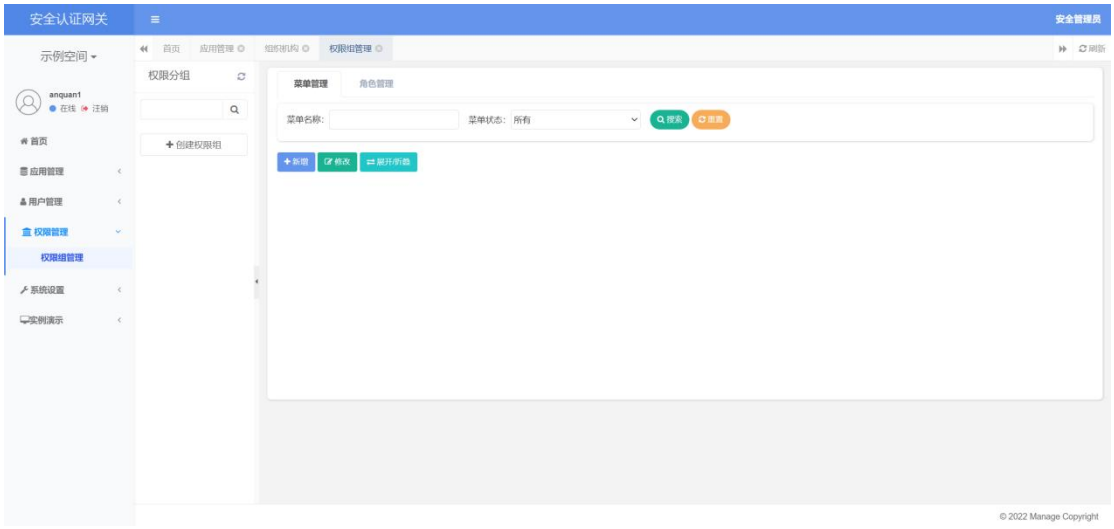
审计管理员权限：



安全管理员权限：







3.2.12.2. 管理员登录安全

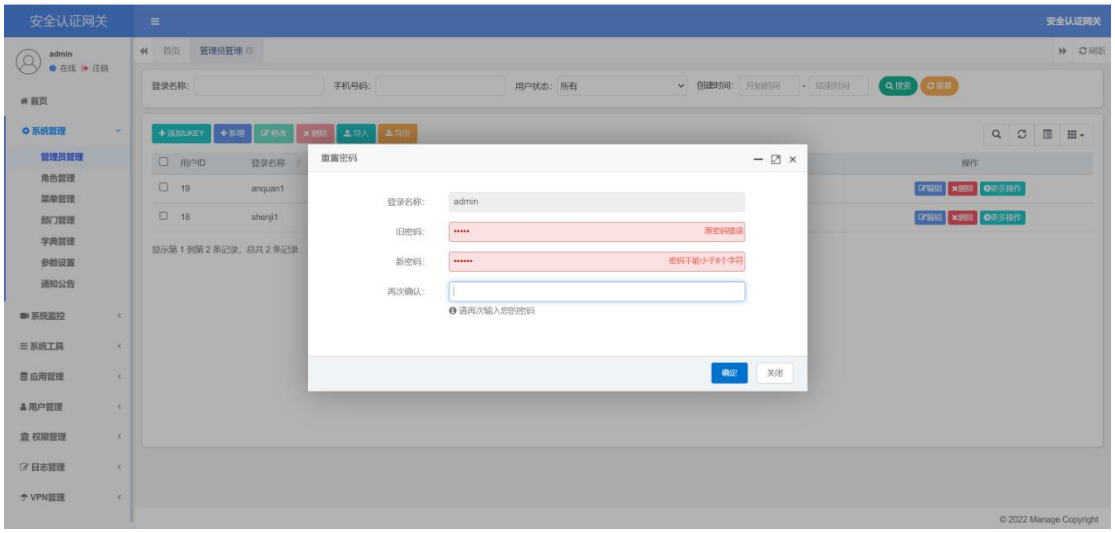
安全认证网关管理员登录安全规范如下：

1、管理员初始化及创建、修改对登录密码强度进行规范、长度必须大于 8 位。

2、用户登录采用双重认证、认证 UKEY 的 PIN 和登录密码。

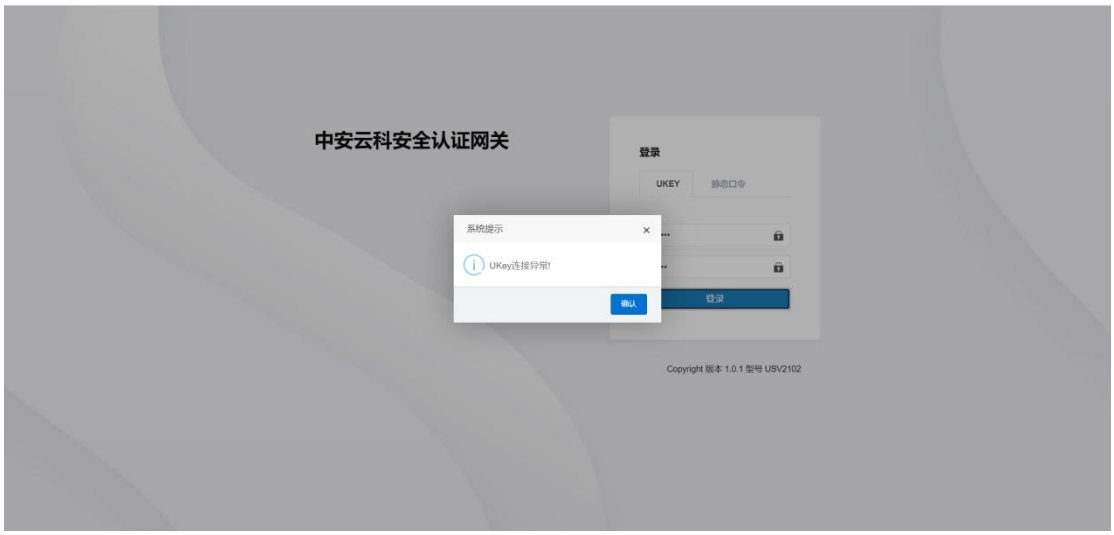
3、用户登录失败对密码错误次数进行计数、达到 5 次管理员账户将被锁定。

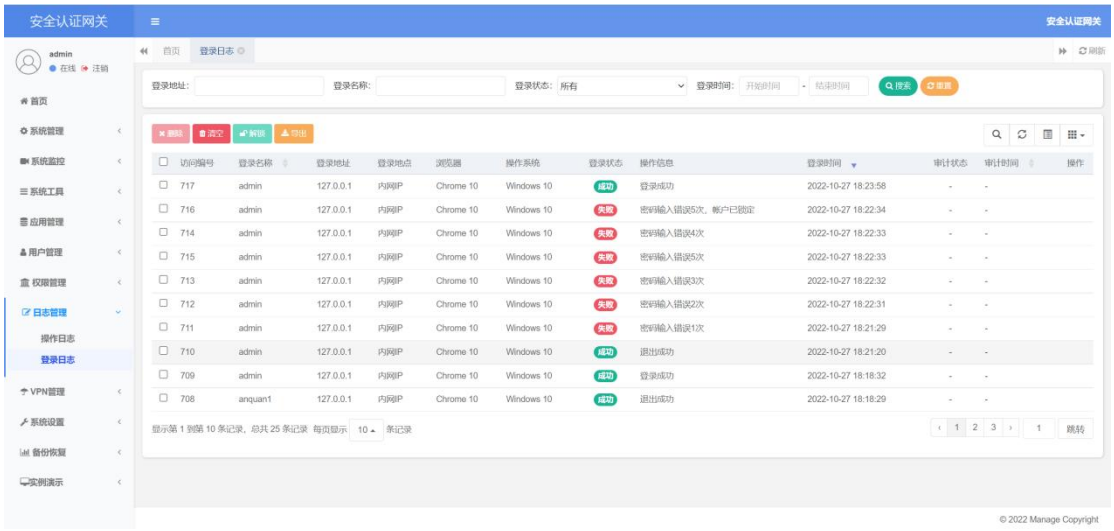
4、登录进行 UKEY 信息校验、硬件检测失败及 UKEY 信息失败将禁止登录。


安全认证网关
admin
首页
管理员管理
登录名称:
手机号码:
用户状态:
所有
创建时间:
重置密码
登录名称:
admin
旧密码:
新密码:
再次确认:
确定
关闭
© 2022 Manage Copyright


中安云科安全认证网关
登录
UKEY
静态口令
admin
用户不存在/密码错误 [密码输入错误1次]
登录
还没有账号? 立即注册
Copyright 版本 1.0.1 型号 USV2102

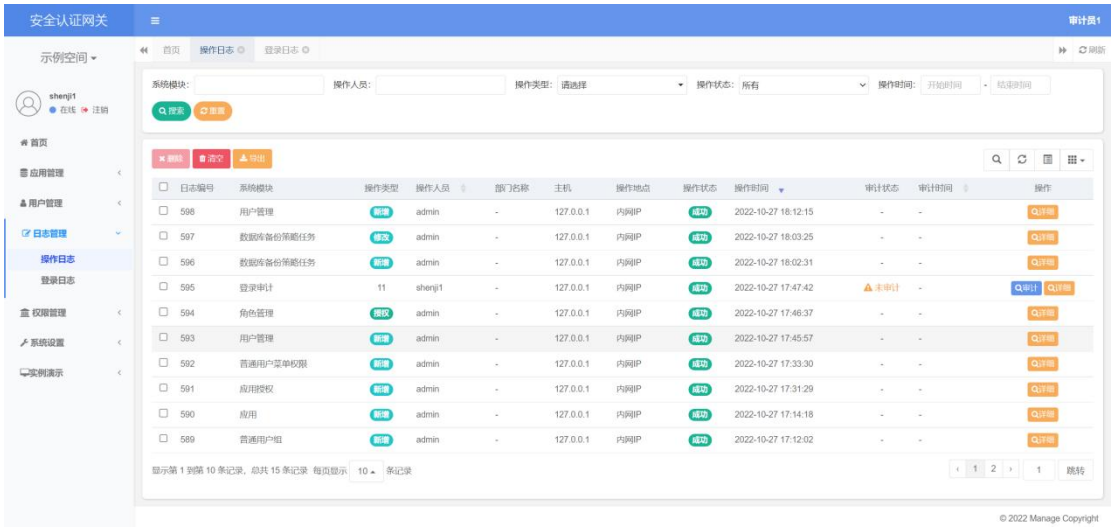

中安云科安全认证网关
登录
UKEY
静态口令
admin
密码输入错误5次，帐户已锁定
登录
还没有账号? 立即注册
Copyright 版本 1.0.1 型号 USV2102

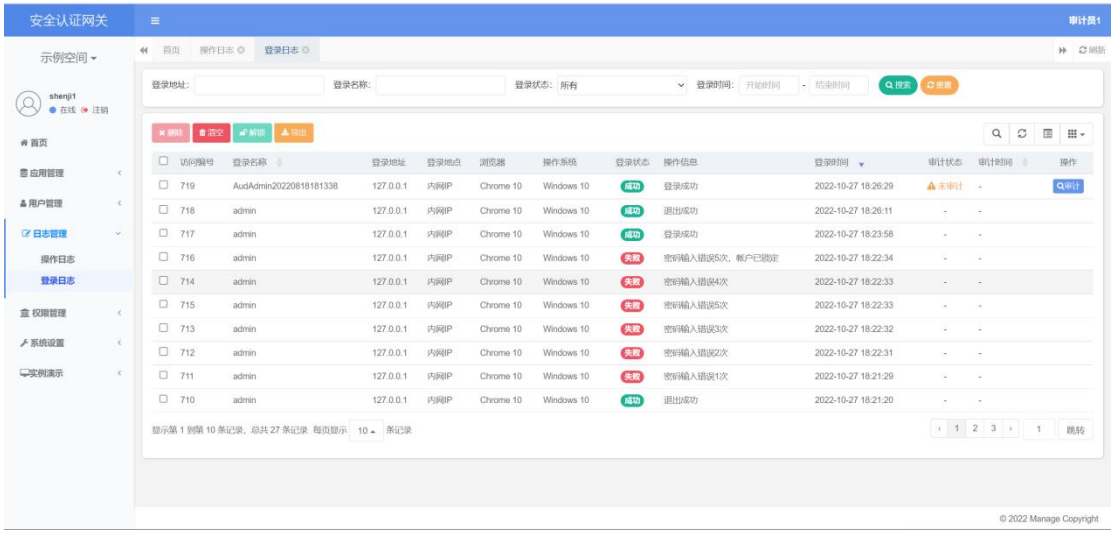




3.2.13. 日志管理安全

安全认证网关具有日志管理功能，审计管理员拥有查看、删除、导出日志等权限。日志记录操作时间、操作人员、操作内容及事件、操作结果等详细信息、日志可以审计。



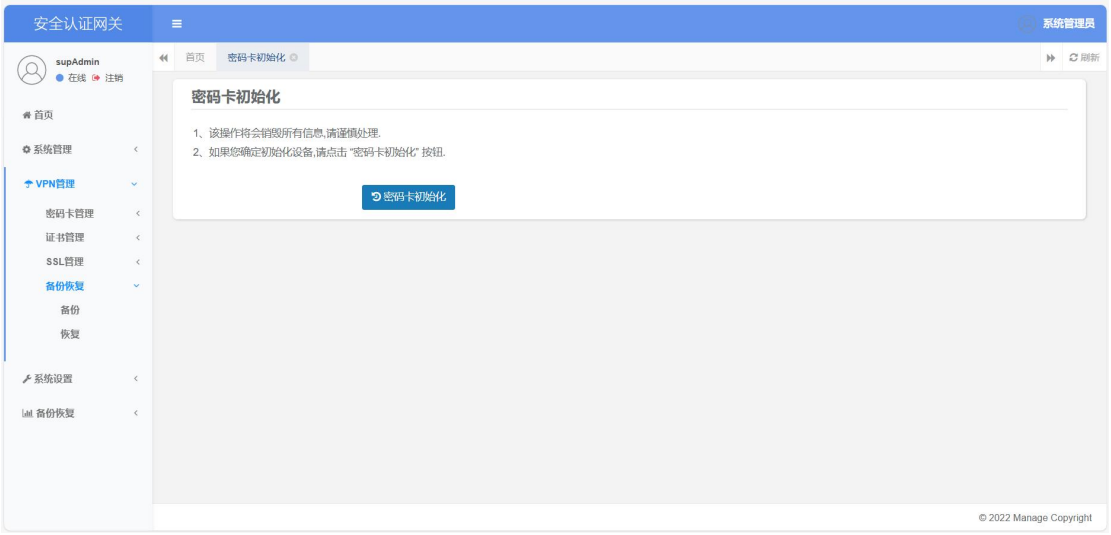


3.2.14. VPN 管理

安全认证网关具有隧道代理功能，使用具有国密认证证书的密码卡管理密钥，使用 VPN 功能，可以便捷的为应用系统提供 SSL 隧道代理功能。

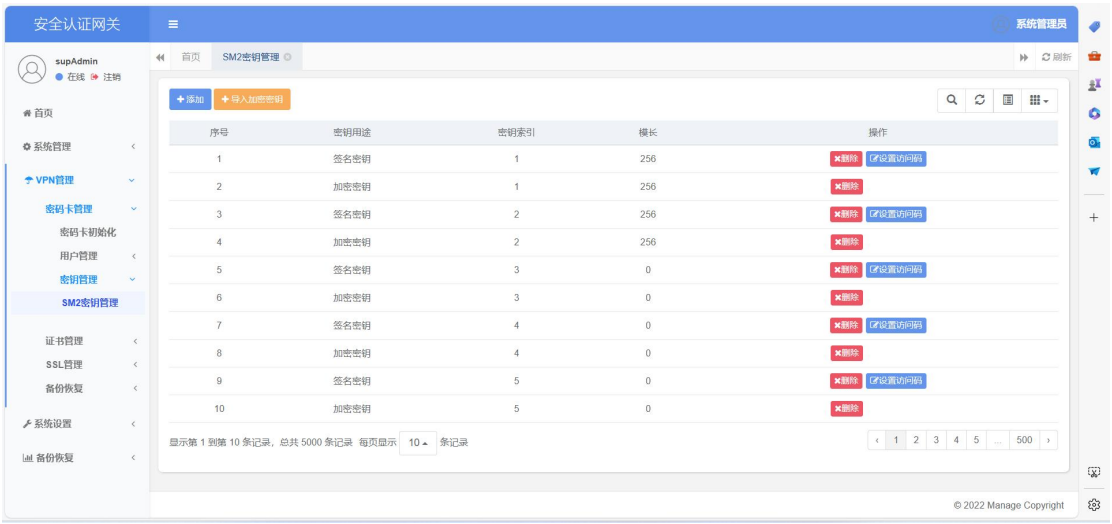
1.密码卡管理-初始化密码卡

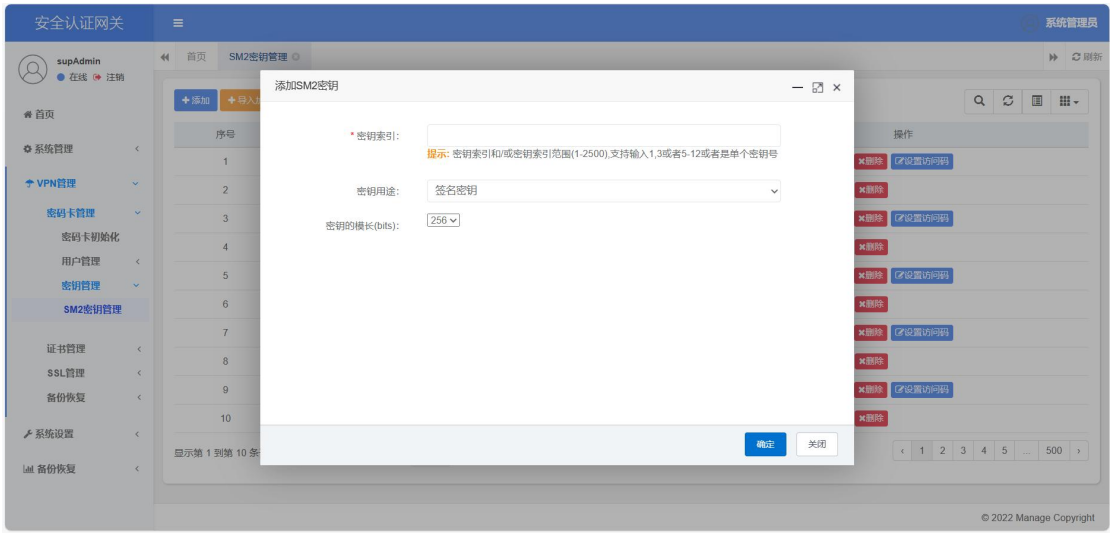
系统初次访问，登录超级管理员进入密码卡初始化页面，点击密码卡初始化，完成密码卡初始化，初始化完成后，密钥重置，可进入密钥管理创建密钥。

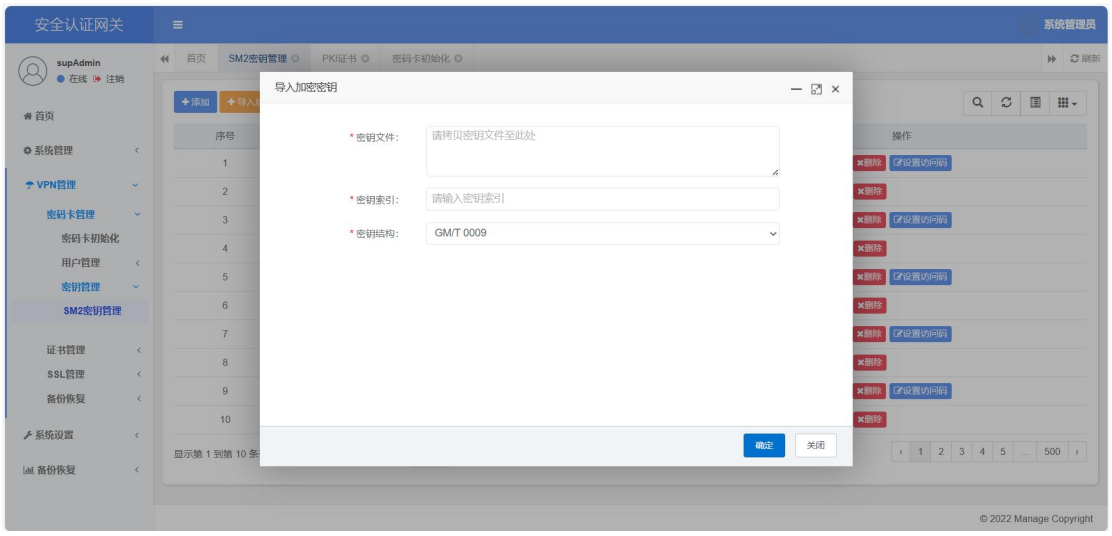


3.密码卡管理-密钥管理

安全认证网关支持国密 SM2 密钥，可以点击添加创建签名密钥与加密密钥，另外加密密钥可外部导入。密钥管理中的密钥用于申请证书。





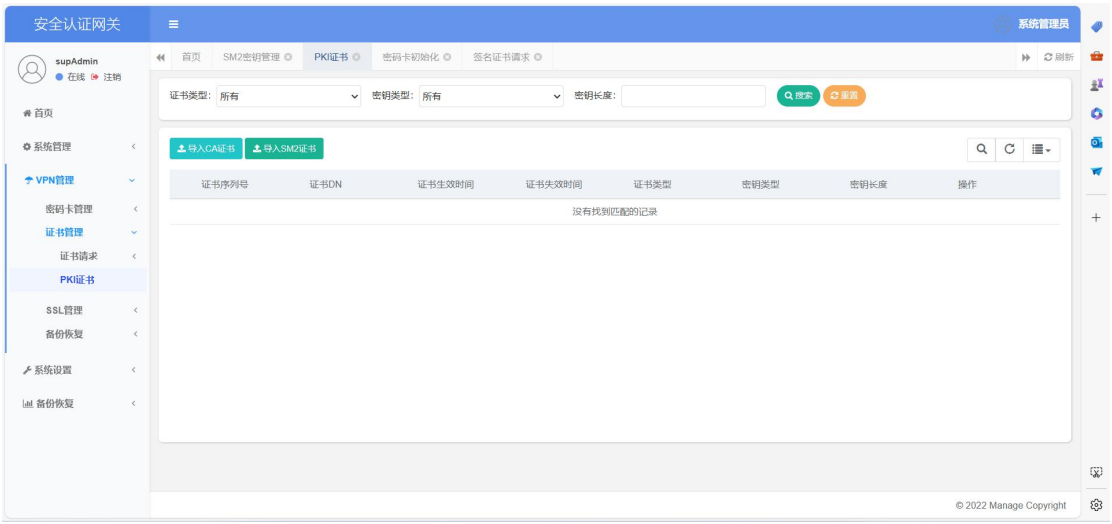


4.证书管理-证书请求（P10）

安全认证网关支持生成签名密钥证书请求和加密密钥证书请求，证书请求需要选择已存在的密钥才能生成，证书请求是 CA 系统的证书申请凭证，获取证书请求后，可以在 CA 系统下载证书。

5.证书管理-PKI 证书

PKI 证书模块用于管理用户证书，用户可以在此页面选择“导入 CA 证书”按钮导入对应根证书，选择“导入 SM2 证书”导入用户证书，需要注意的是，在导入用户证书前，需要先导入根证书。PKI 证书可以用于创建 HTTP 隧道服务

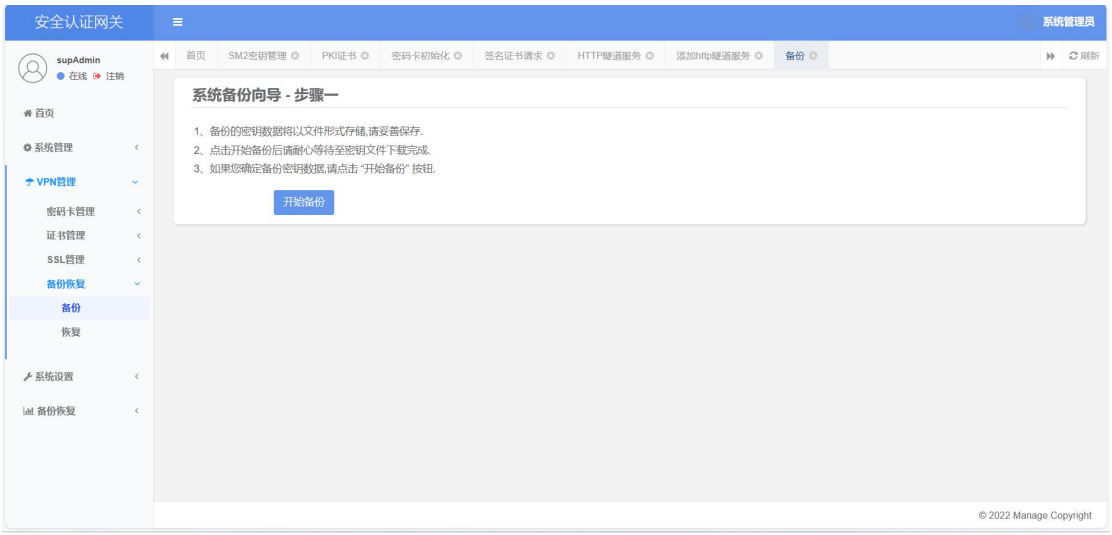


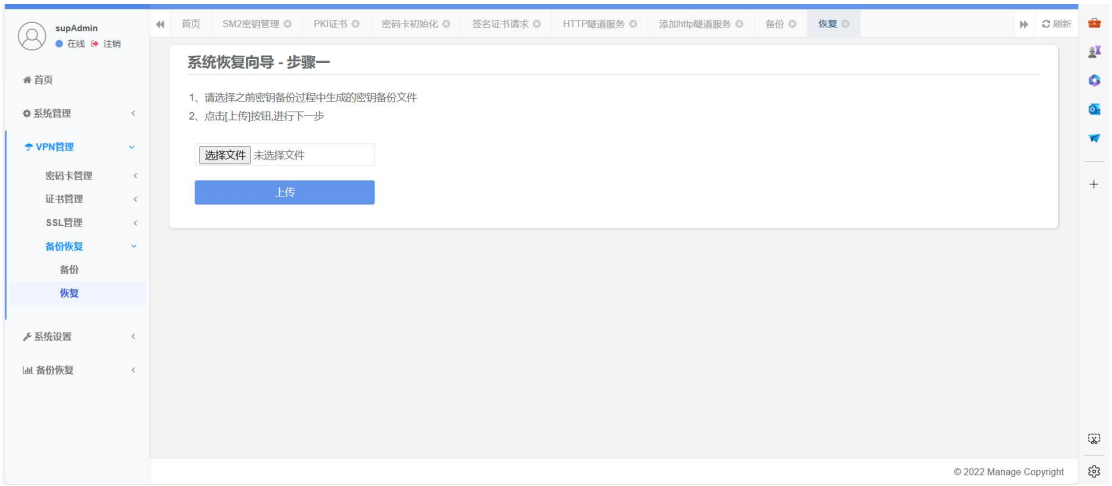
6.SSL 管理-HTTP 隧道服务

HTTP 隧道服务，可使用安全认证网关对应用系统进行代理，统一使用安全认证网关 IP 管理应用系统，在 HTTP 隧道服务，监听端口为安全认证网关为应用系统新开放的端口，代理 HTTP 服务器为应用系统本身的 ip/域名或端口，应用系统可以选择自己配置的证书，也支持使用系统默认的软证书。配置完成后，点击保存，使用安全认证网关开放的新地址也可访问对应应用系统。

7.备份-恢复

密码卡数据可以备份恢复功能完成离线数据保存，用于灾备情况下的密钥备份与恢复。



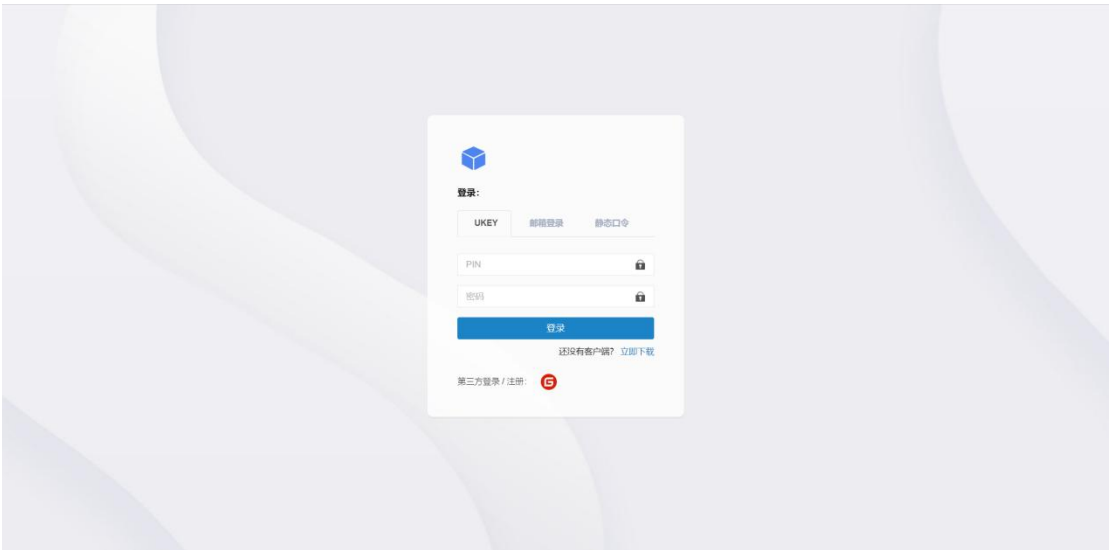


3.3 用户端功能（门户）

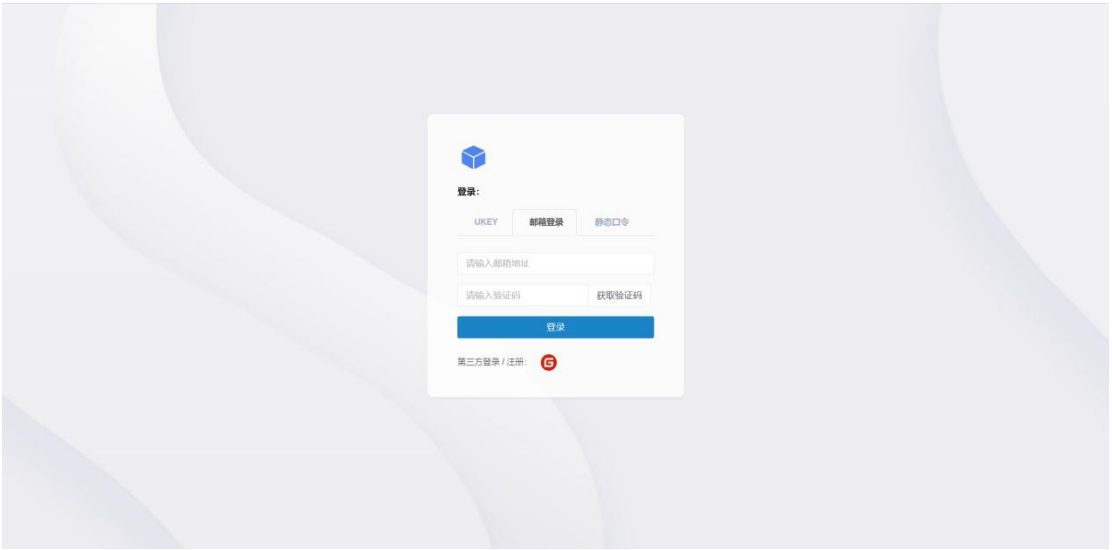
3.3.1. 用户登录

用户端登录方式分为 UKEY 登录、邮箱登录、静态口令登录、第三方登录。

1.UKEY 登录：UKEY 登录需要管理员注册带有 UKEY 登录的用户信息，如果没有 UKEY 客户端，可以点击下载客户端，将注册码交给管理员进行 UKEY 注册。注册后，管理员添加绑定 UKEY 的用户信息，添加完成后，用户即可使用绑定 UKEY 的账户进行登录。

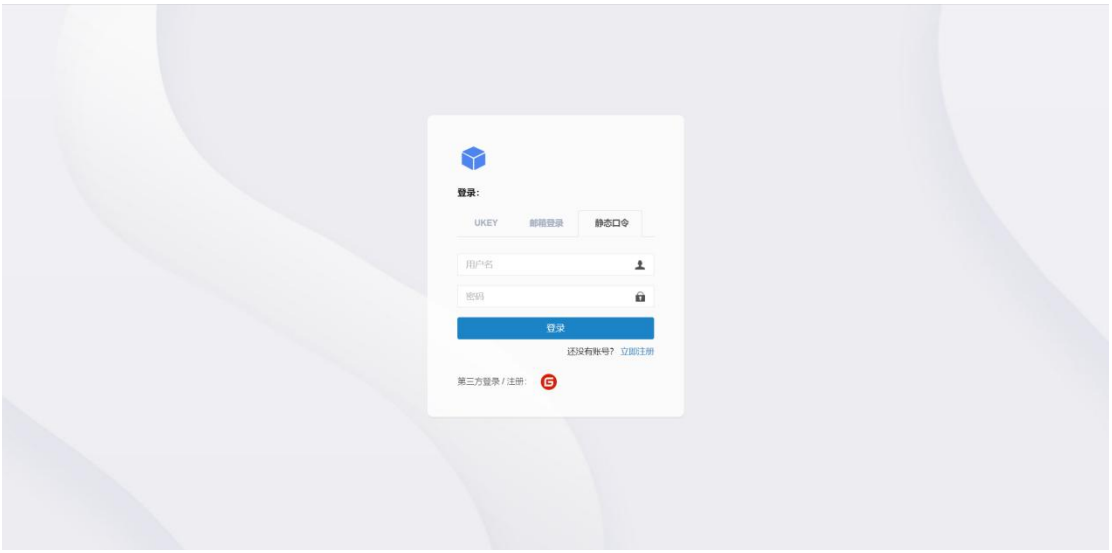


2.邮箱登录：邮箱登录需要输入合法的邮箱账户，点击获取验证码，获取后填入点击登录。

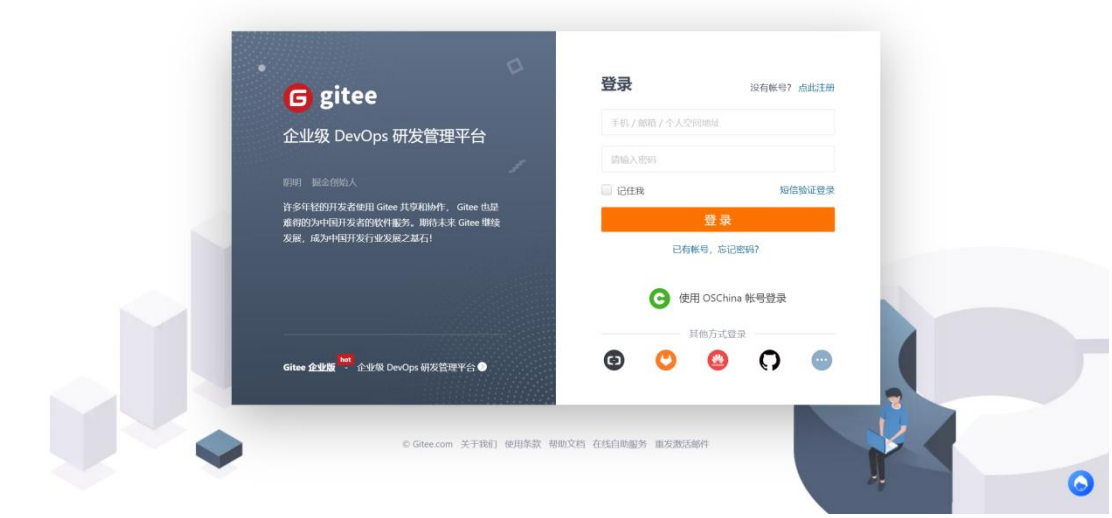


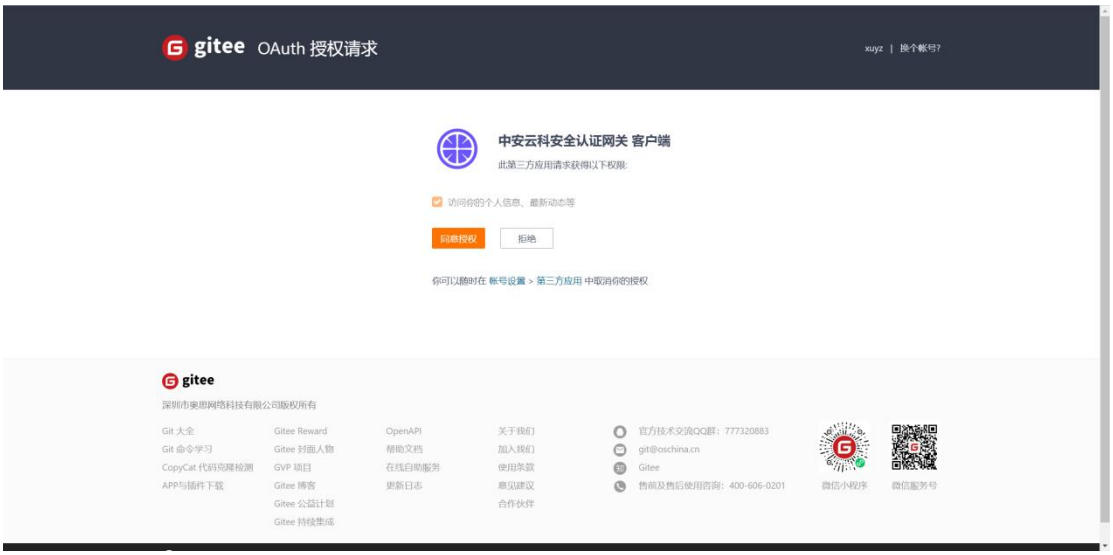
如果您的邮箱地址未绑定平台账户，则需要注册，注册完毕后即可使用这个邮箱地址登录平台。

3.静态口令登录



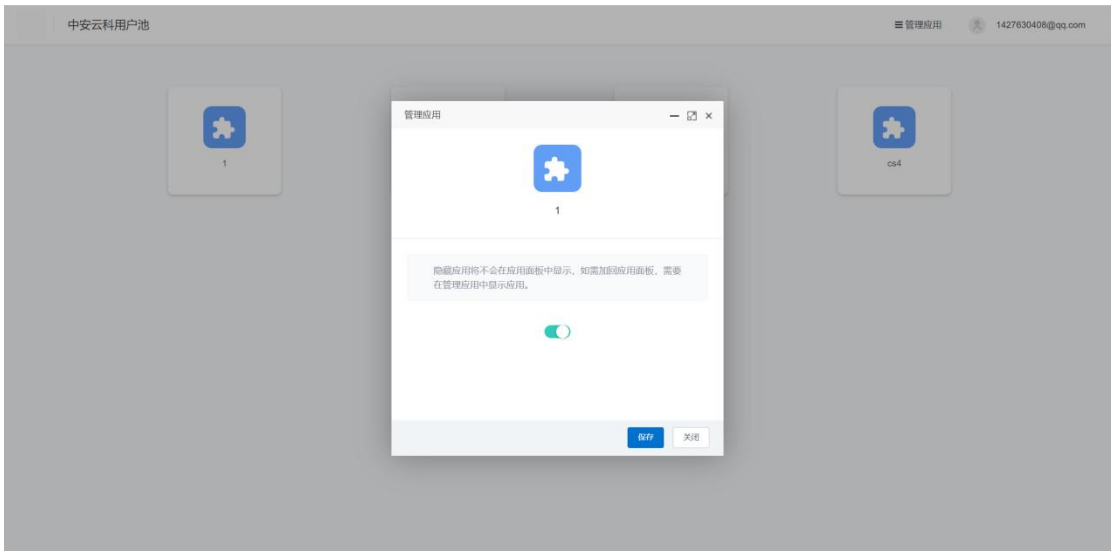
4. 第三方登录：可以使用平台配置的第三方社会源进行登录，与邮箱登录类似，如果这个第三方账户未绑定平台账户，则需要注册，注册完毕后即可使用这个第三方账户进行登录。以 git 为例：

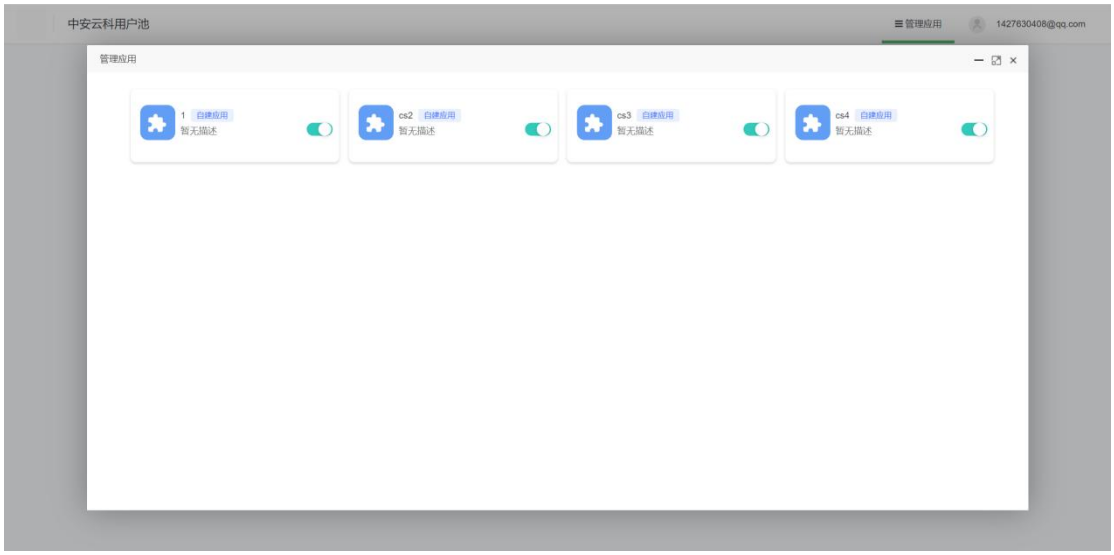




3.3.2. 管理应用

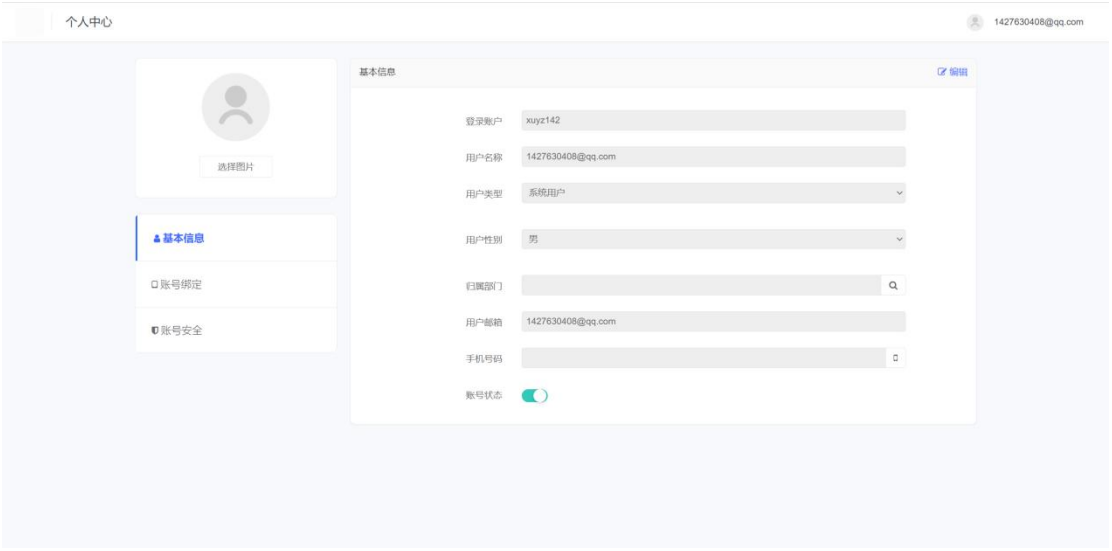
用户的管理应用只能操作应用的隐藏与显示



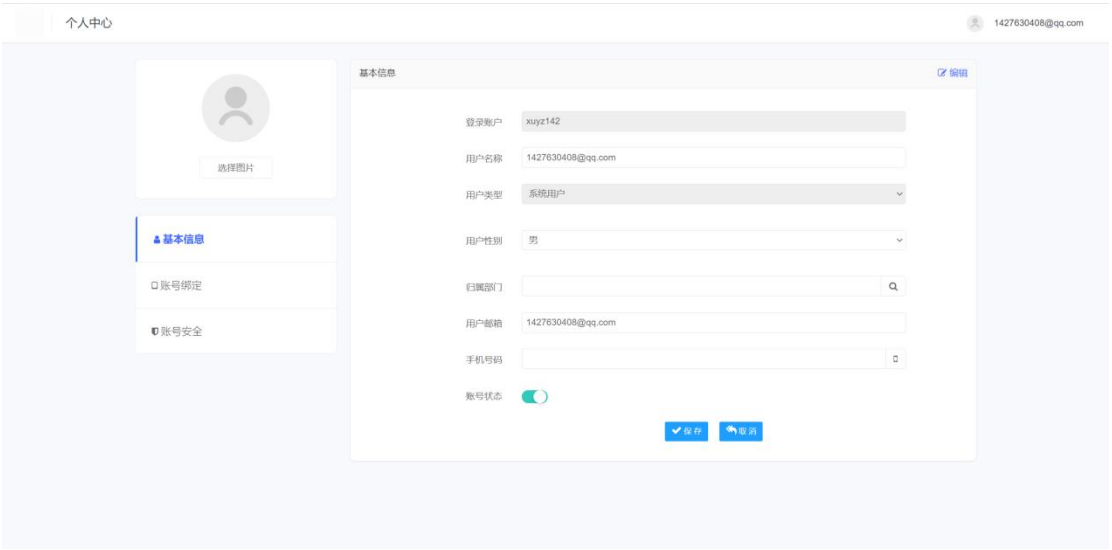


3.3.3. 个人中心

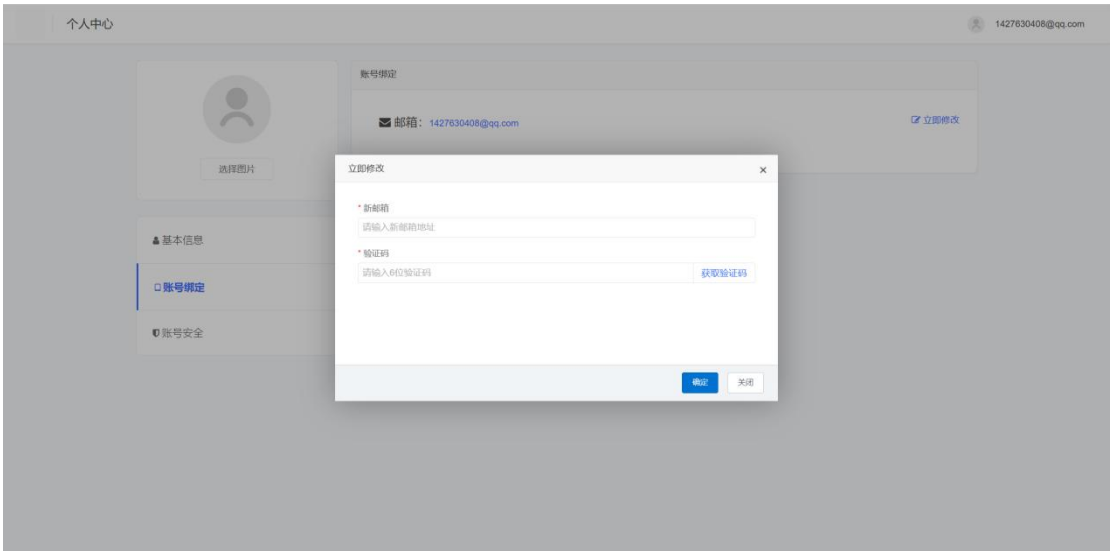
用户端的个人中心提供了个人信息编辑、账号绑定、账号安全等功能



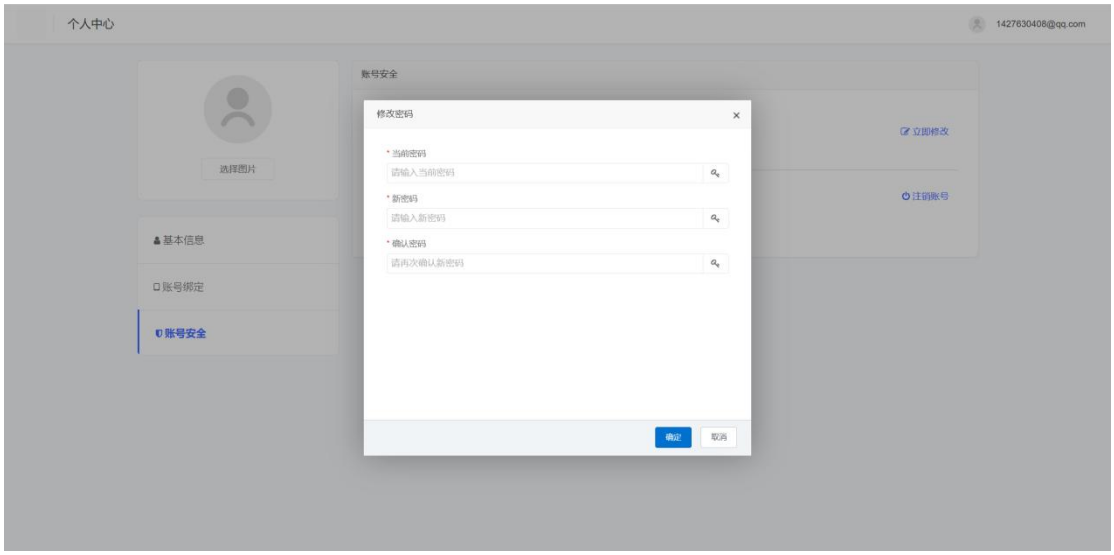
1.修改个人信息



2.账号绑定邮箱



3.修改密码


个人中心
1427630408@qq.com
选择图片
基本信息
账号绑定
账号安全
账号安全
立即修改
注销账号
修改密码
当前密码
请输入当前密码
新密码
请输入新密码
确认密码
请再次确认新密码
确定
取消