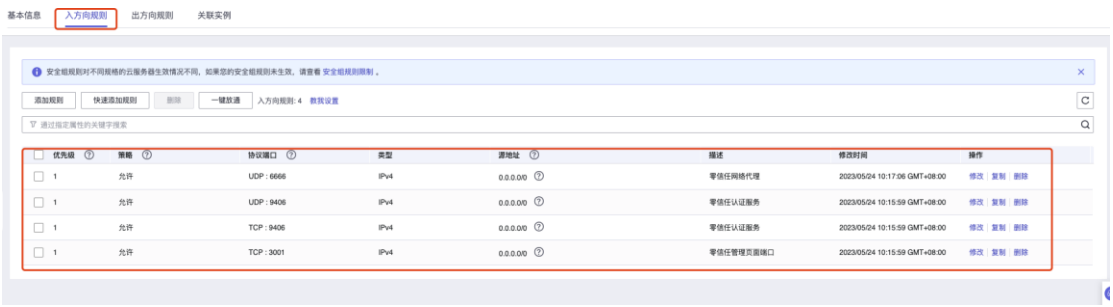
管理员使用手册

环境准备

根据零信任使用需要的协议端口为零信任云主机创建安全规则

协议	端口号	用途
TCP+UDP	9406	认证服务
UDP	6666	网络代理
TCP	3001	web 管理面板



零信任使用需要一个系统盘>=40G 和一个数据盘>=100G

系统登录

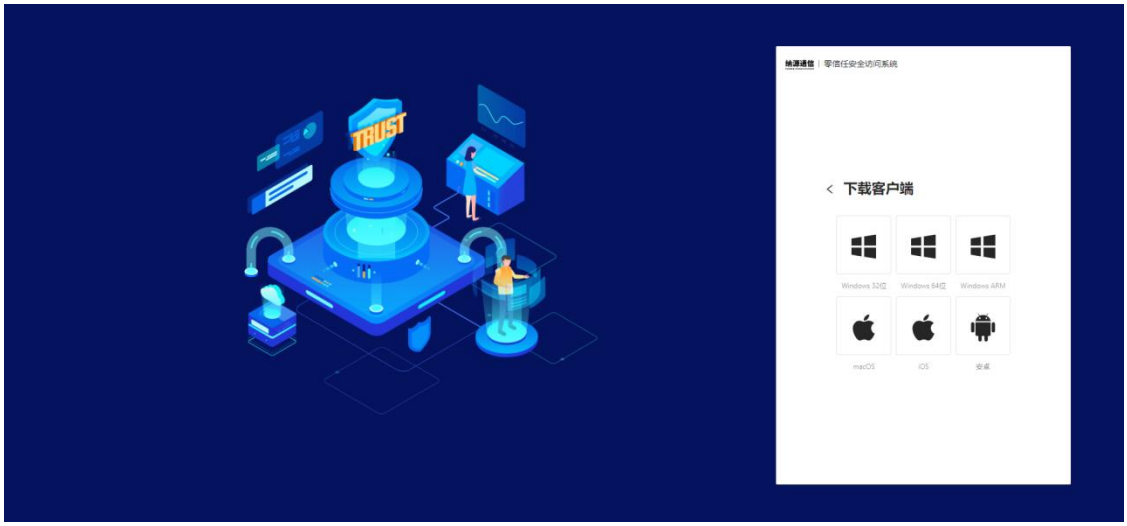
纳源通信零信任安全访问系统采用 B/S 架构管理，在浏览器中输入 https://IP:3001 访问系统登录界面，默认账号/密码：admin/njny1108

注意：首次登录请务必修改初始化密码

通用功能

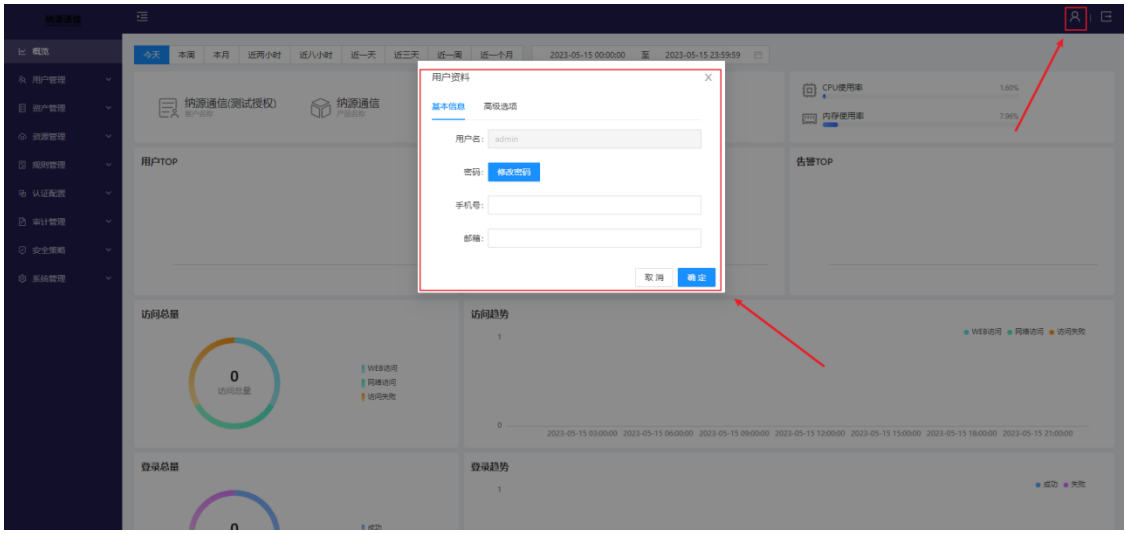
下载客户端

访问管理后台地址，点击 **下载客户端**。



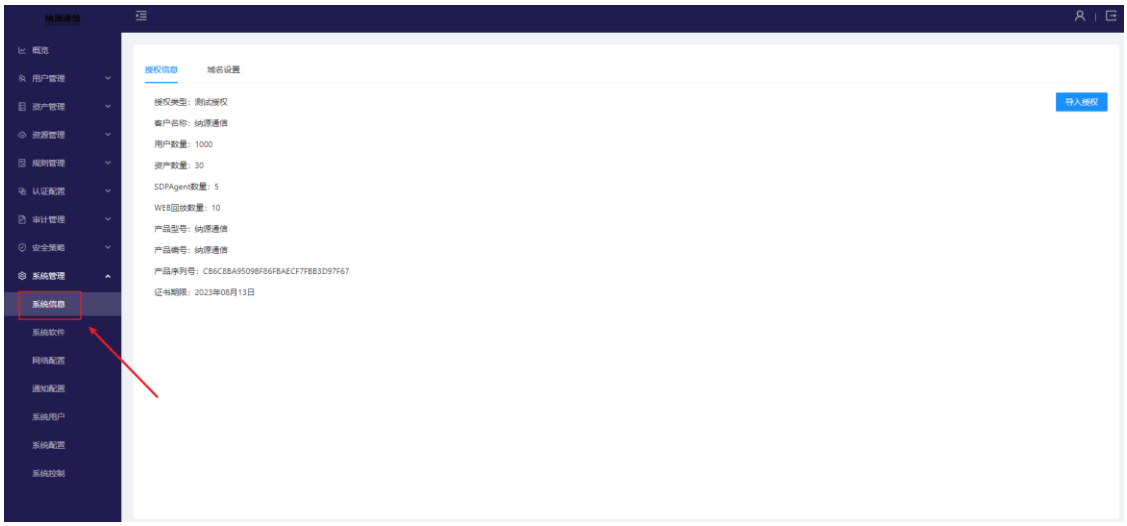
修改管理员资料

登录账号后，点击右上角 **小人** 图标，修改密码、手机号、邮箱、登录 IP、Google 验证信息。



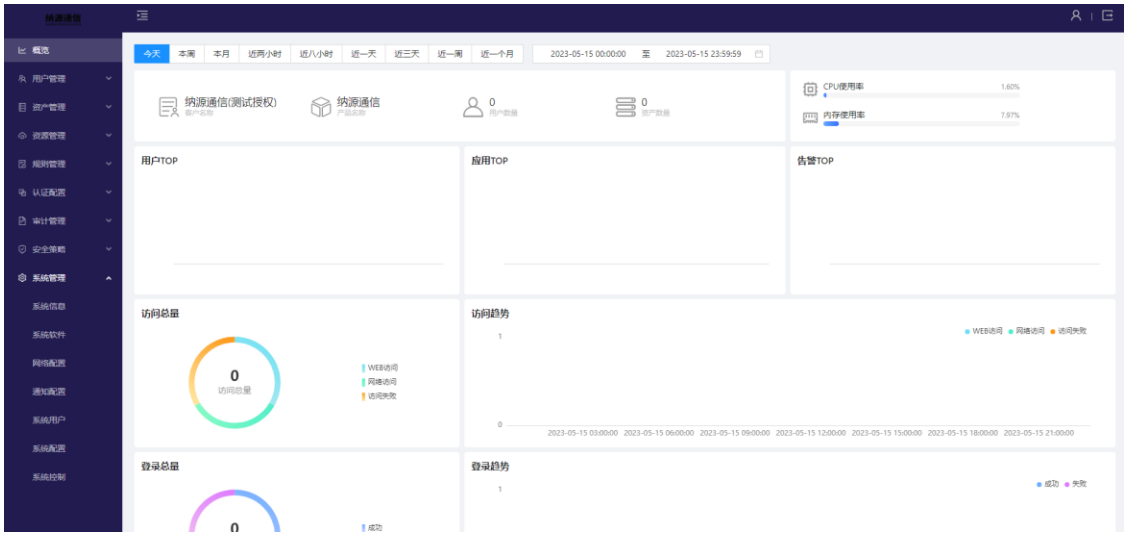
查看系统信息

点击 **系统管理--系统信息**，可查看当前系统信息。



概览

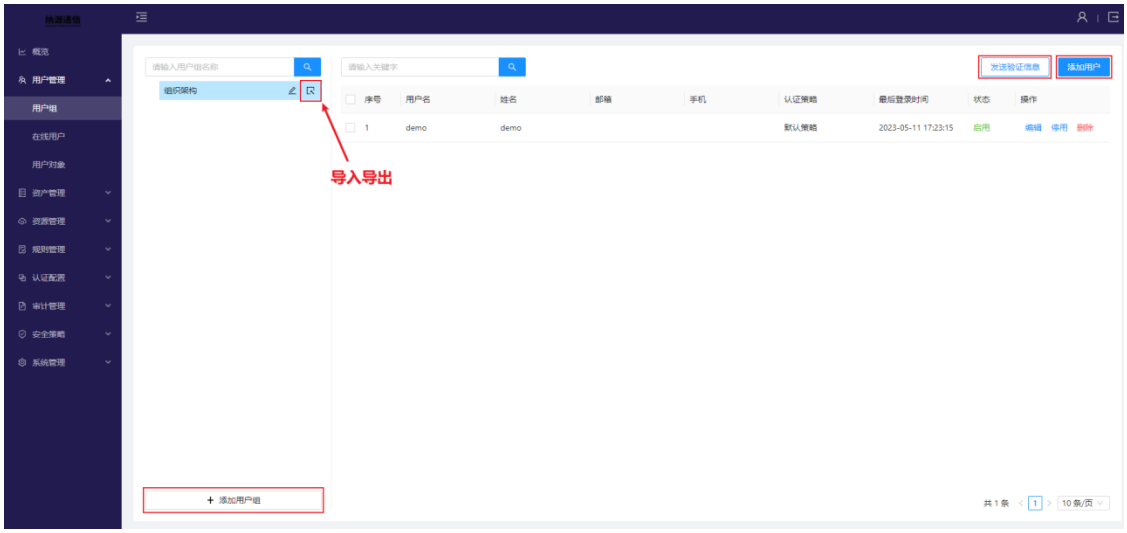
该页面展示系统基本信息，如：系统基本信息、操作系统 CPU 与内存占用率、用户 TOP、应用 TOP、告警 TOP、访问总量、访问趋势、登录总量、登录趋势。鼠标悬停在各数据模块上，会显示对应的数据详情。



用户管理

用户组

添加用户及用户组，如图所示：

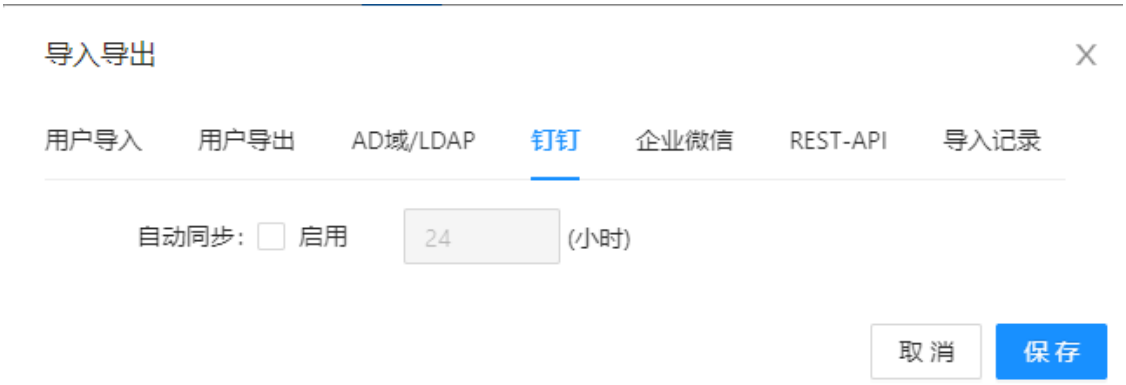


- 添加用户组：可在当前选择组下添加用户组，用户组支持多级管理；
- 导入导出：点击组织架构导入图标，可批量导入/导出及自动同步其他认证系统用户；
  - 用户导入：根据下载模板批量导入用户信息，如图所示：

  - 用户导出：选择字段及用户组导出用户信息，如图所示：

- AD 域/LDAP：选择认证模块同步用户信息及自动同步周期，如图所示：

- 钉钉：根据钉钉认证模块配置同步用户信息及自动同步周期，如图所示：



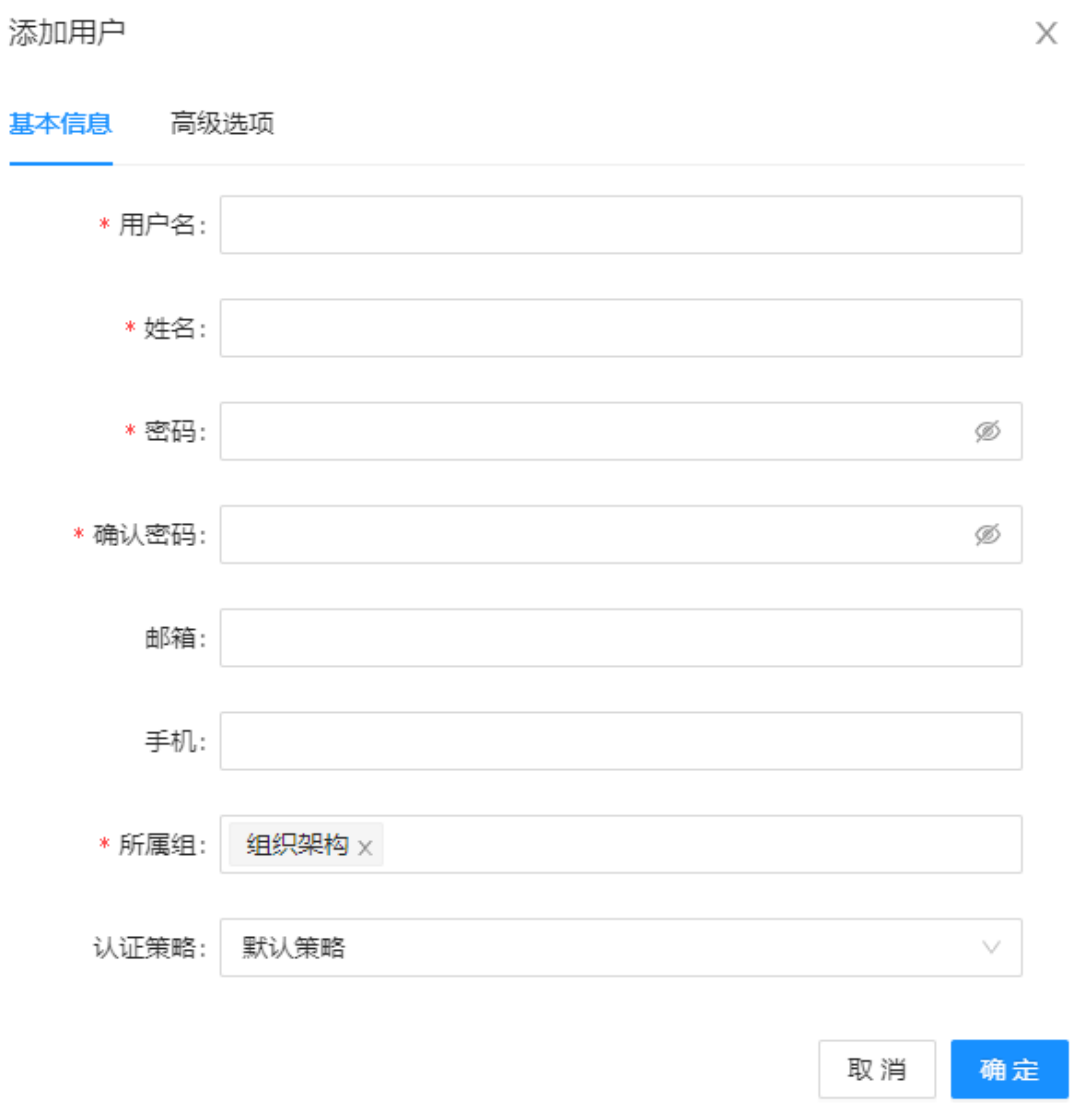
- 企业微信：根据企业微信认证模块配置同步用户信息及自动同步周期，如图所示：

- REST-API：选择认证模块同步用户信息及自动同步周期，如图所示：

- 导入记录：展示近 20 条导入用户信息日志，如图所示：

添加用户

添加用户及相关配置，如图所示：



- 用户名：配置用户登录用户名，添加后默认不可编辑，从钉钉及企业微信导入用户名可编辑；
- 姓名：配置用户登录姓名，本地用户默认可编辑，从其他认证系统导入姓名不可编辑；
- 密码：配置用户登录密码，密码策略遵循本地认证模块的密码策略；
- 确认密码：确认用户登录密码；
- 邮箱：配置用户邮箱；

- 手机：配置用户手机号码；
- 所属组：配置用户所属组，用户可以属于多个组；
- 认证策略：配置用户认证策略；

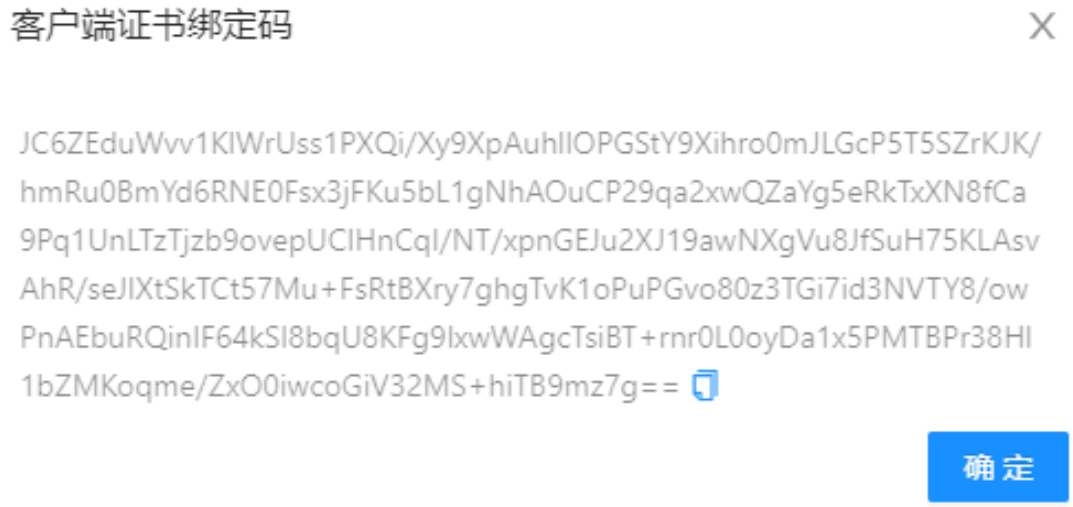
- 登录方式：配置用户登录方式，默认为不限制；

  - 只允许 WEB 登录：只允许用户登录 WEB 门户，不允许通过客户端登录；
  - 强制客户端登录：强制用户只能通过客户端登录，不允许直接登录门户；
- 登录地区：限制用户登录地区；
- 登录 IP：限制用户登录 IP；
- 登录系统：限制用户登录终端，默认为自动识别；
  - 不限制：不限制用户登录终端数量；
  - 自动识别：给予用户一台终端登录名额，并自动识别其终端信息；
  - 其他：给予用户一台终端登录名额，并限制其终端系统类型与 HOSTNAME；
- WEB 安全策略：配置用户是否启用 WEB 安全策略，策略遵循安全策略中的 WEB 安全策略配置；
- 客户端安全策略：配置用户是否启用客户端安全策略，策略遵循安全策略中的客户端安全策略配置；
- 登录时间：配置用户允许与禁止的访问时间。

用户注册码

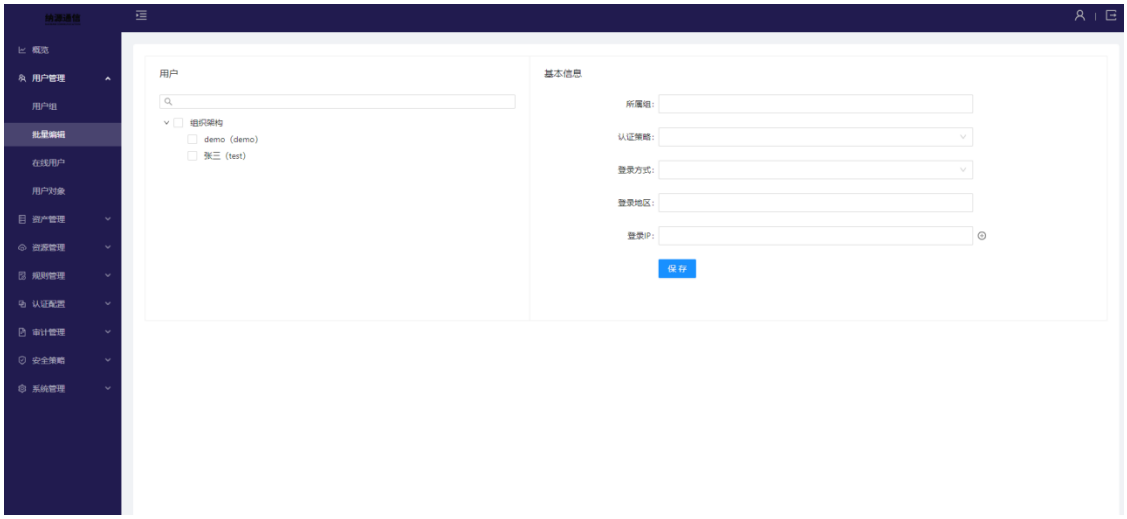
【发送验证信息】中可通过邮件发送或生成用户客户端注册码，如图所示：

- 邮件发送：选择用户及用户组发送其客户端注册码；
- 生成文本：生成用户客户端注册码，如图所示：



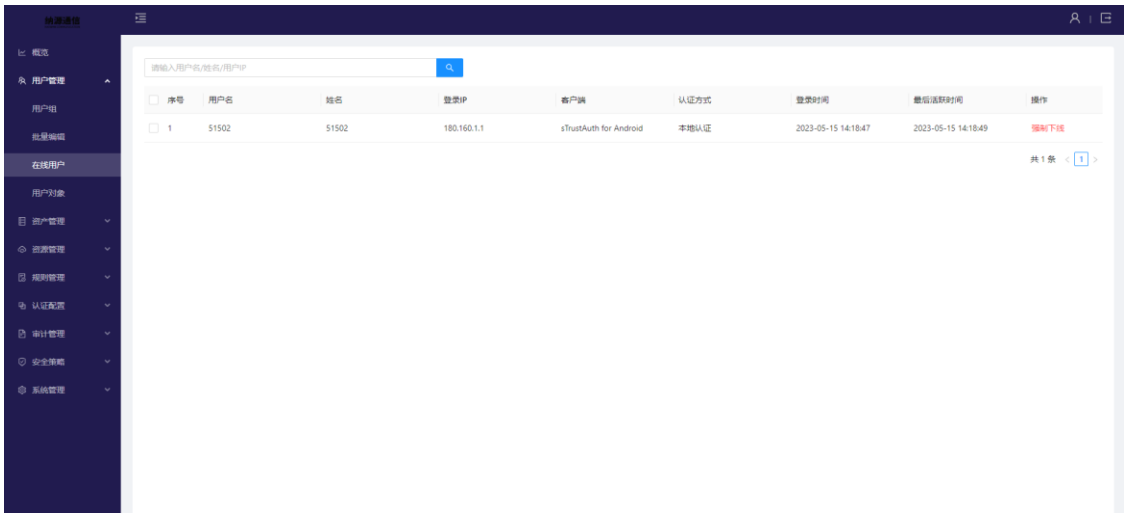
批量编辑

该页面可对用户进行批量编辑操作。批量修改用户**所属组、认证策略、登录方式、登录地区、登录 IP**，点击保存完成编辑操作，如图所示：



在线用户

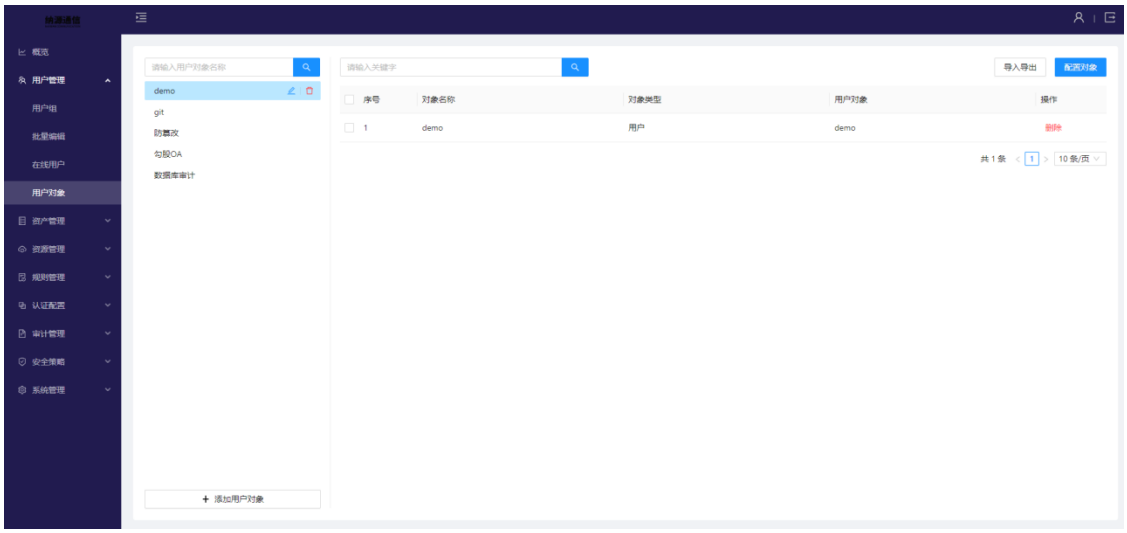
该页面展示当前系统在线用户，如图所示：



- 强制下线：中断当前登录的用户，可批量选择强制下载。

用户对象

管理用户及用户组，如图所示：



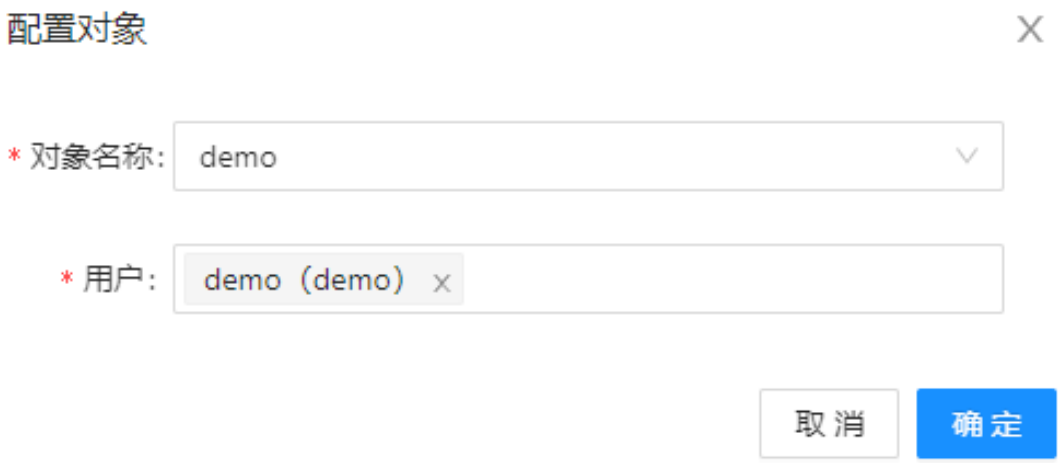
- 添加用户对象：可在当前选择对象下添加用户对象，用户对象支持多级管理；
- 导入导出：点击导入导出按钮，可批量导入/导出系统用户对象；
  - 对象导入：根据下载模板批量导入对象信息，如图所示：

  - 对象导出：选择用户对象导出用户对象信息，如图所示：

- 导入记录：展示近 20 条导入用户信息日志，如图所示：

配置对象

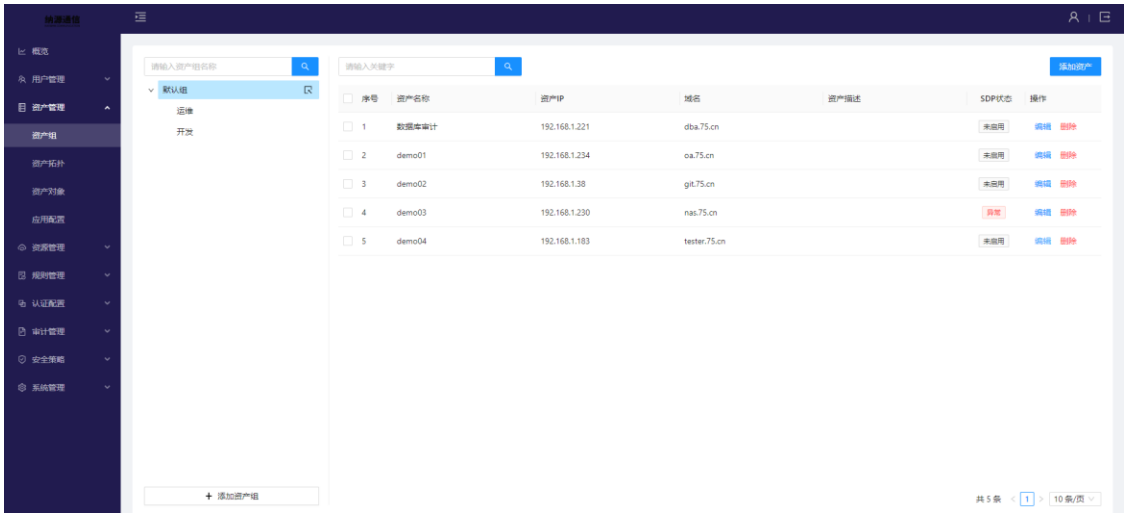
添加用户及相关配置，如图所示：



资产管理

资产组

管理资产及资产组，如图所示：



- 添加资产组：可在当前选择组下添加资产组，资产组支持多级管理；
- 导入导出：点击默认组导入图标，可批量导入/导出资产信息
  - 资产导入：根据下载模板批量导入资产信息，如图所示：

- 资产导出：选择资产组导出资产信息，如图所示：

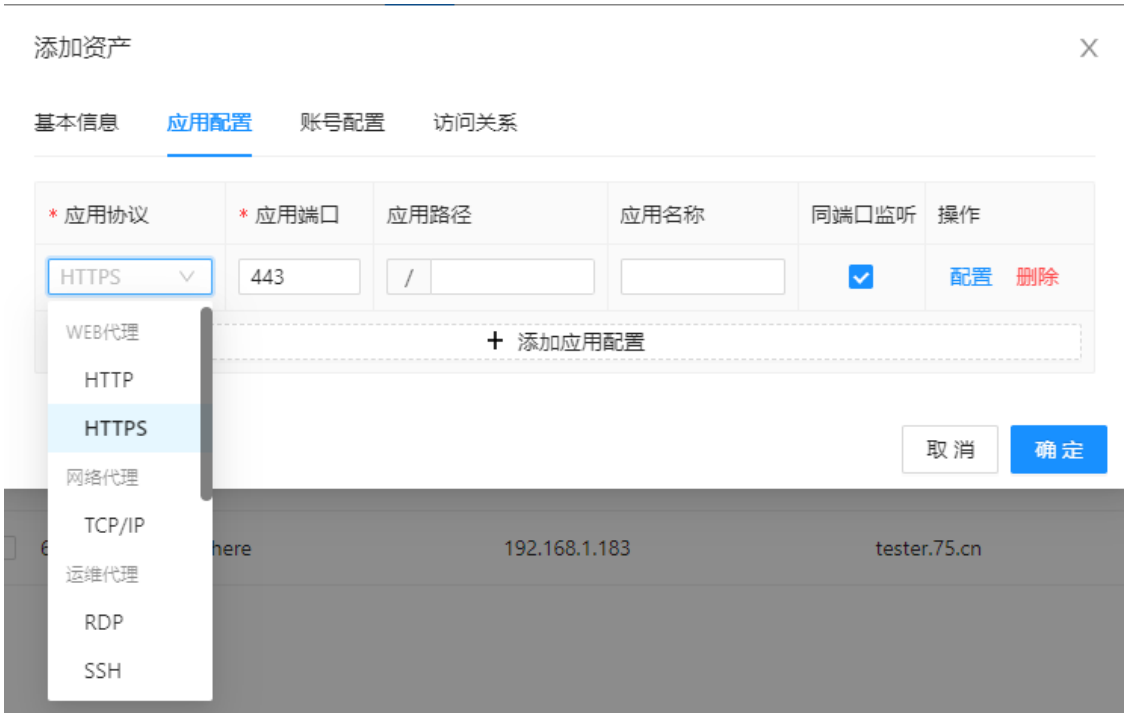
- 导入记录：展示近 20 条导入资产信息日志，如图所示：

添加资产

添加资产及相关配置，如图所示：

- 资产名称：配置资产名称；
- 资产 IP：配置资产 IP；
- 资产描述：配置资产描述；
- SDP 控制：远程控制 SDPAgent，SDPAgent 启用后默认将拒绝所有连接请求，并启用 SPA 认证机制；
  - 自动检测：自动检测 SDPAgent 状态，并将检测到的状态显示在 SDP 状态中；
  - 启用：启用 SDPAgent，启动成功 SDP 状态显示为正常；
  - 停用：停用 SDPAgent，停用成功 SDP 状态显示为停用；
  - 不检测：不再检测 SDPAgent 状态，SDP 状态显示为未启用；

- 域名：配置资产域名，添加 WEB 应用必须配置域名；
- 证书：上传域名公钥及私钥；
- 所属组：配置资产所属组，只能属于一个资产组；



- 添加应用：配置资产下相关应用；
- 应用协议：选择应用对应协议；
  - 网络代理：客户端登录后可连接的网络应用；
  - WEB 代理：需要通过域名访问的 WEB 应用；
- 应用端口：配置应用对应端口，网络代理应用可配置 0 代表所有端口；
- 应用名称：配置应用名称，应用在门户中以该名称，仅限 WEB 代理应用配置；
- 应用标签：配置应用标签，应用在门户中以标签分类展示，仅限 WEB 代理应用配置；

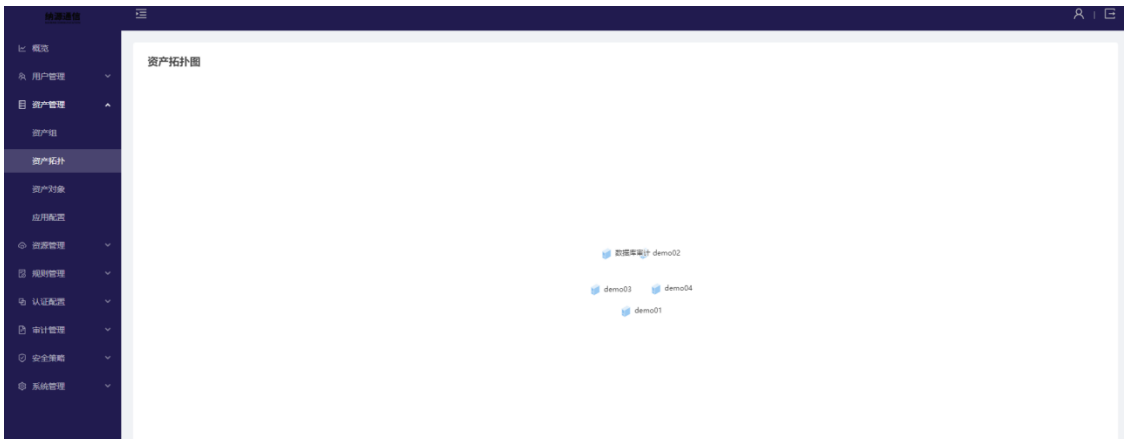
- 添加账号：配置应用相关账号，仅限 WEB 代理应用配置；
- 账号：配置应用账号，SSO 账号为当前登录用户账号；
- 认证方式：配置应用账号密码，如果不需要密码可以选择无需密码，SSO 账号一般配置为无需密码；
- 绑定应用：配置应用账号绑定的 WEB 代理应用；

- 添加访问关系：配置该资产允许被访问的白名单 IP，仅限于 SDPAgent 安装后生效；
- 协议：配置来源访问协议；

- 来源 IP：配置来源访问 IP；
- 来源端口：配置来源访问端口，0 为不限制；
- 目标端口：访问该资产的目标端口，0 为不限制；

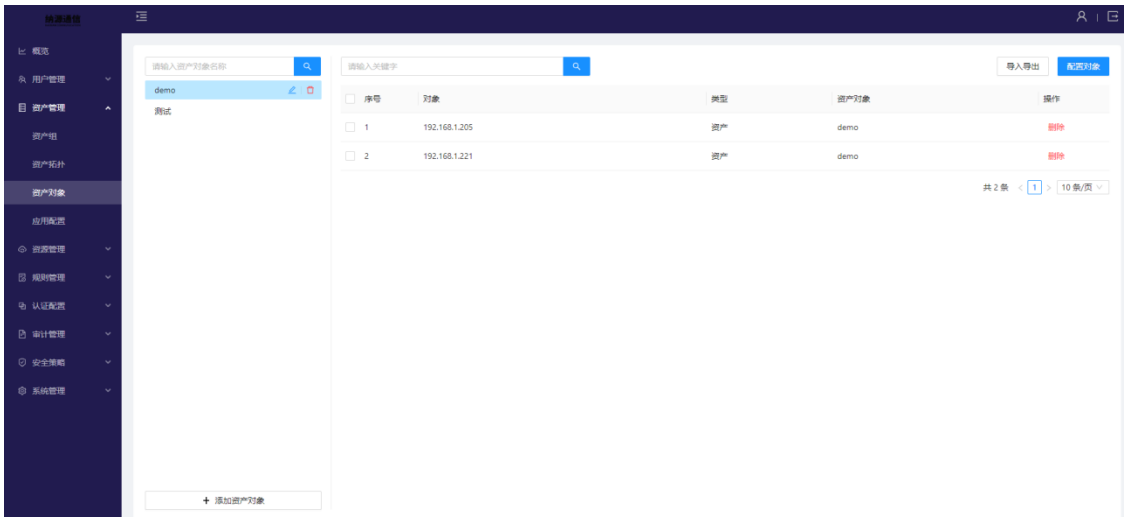
资产拓扑

对系统资产生成资产拓扑图，方便查看所拥有的资产。如图所示：



资产对象

管理资产及资产组，如图所示：



- 添加资产对象：可在当前选择资产下添加资产对象，资产对象支持多级管理；
- 导入导出：点击导入导出按钮，可批量导入/导出系统资产对象；
  - 对象导入：根据下载模板批量导入资产信息，如图所示：

  - 对象导出：选择资产对象导出资产对象信息，如图所示：

  - 导入记录：展示近 20 条导入资产信息日志，如图所示：

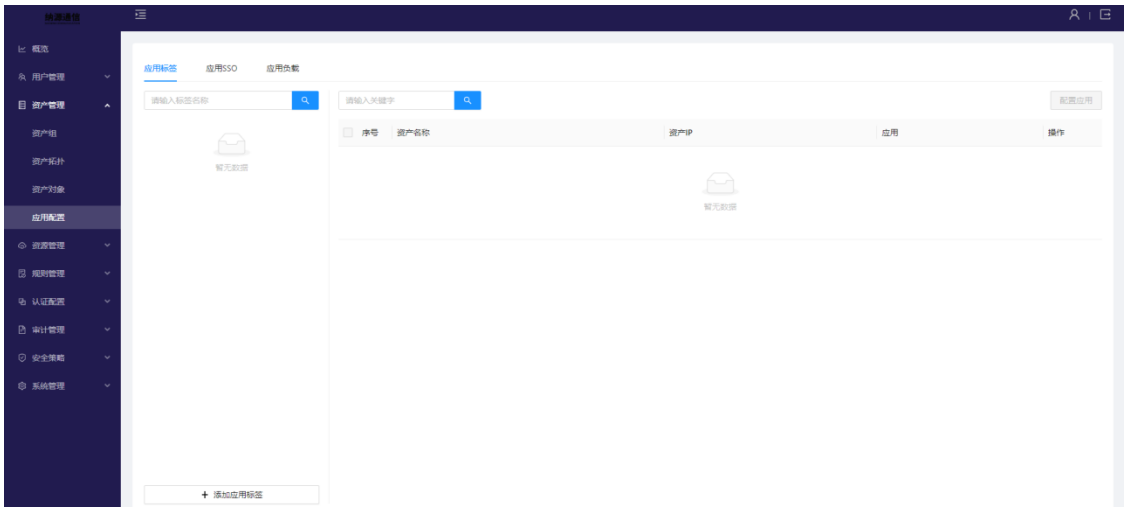
配置对象

添加资产及相关配置，如图所示：

应用配置

应用标签

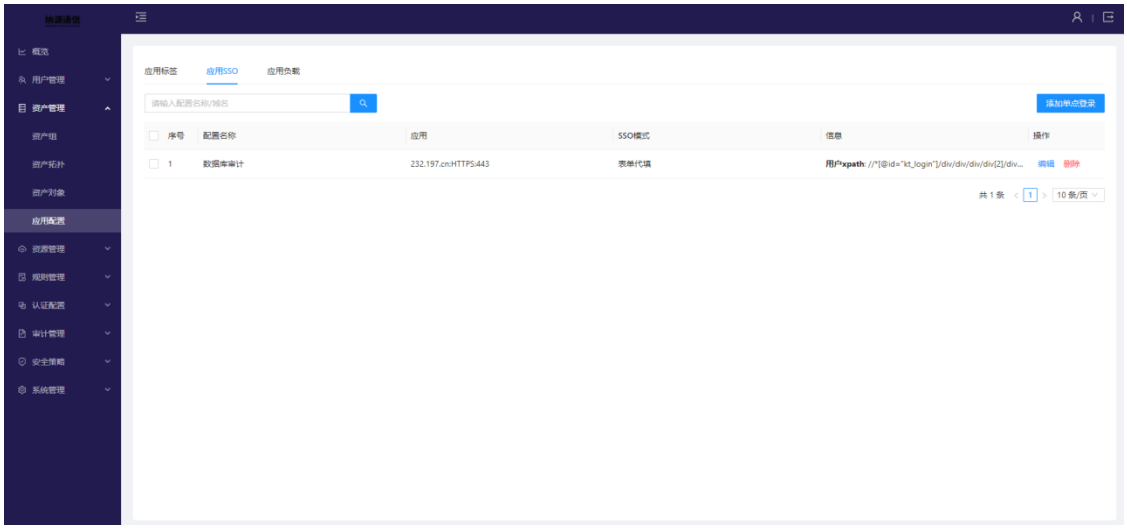
配置管理应用标签，门户中 WEB 应用以标签分组展示，便于应用分类查找，如图所示：



- 添加应用标签：添加一个应用标签类型；
- 配置应用：配置该标签下的应用，仅限 WEB 代理应用配置；

应用 SSO

配置 WEB 应用账号的单点登录，如图所示：

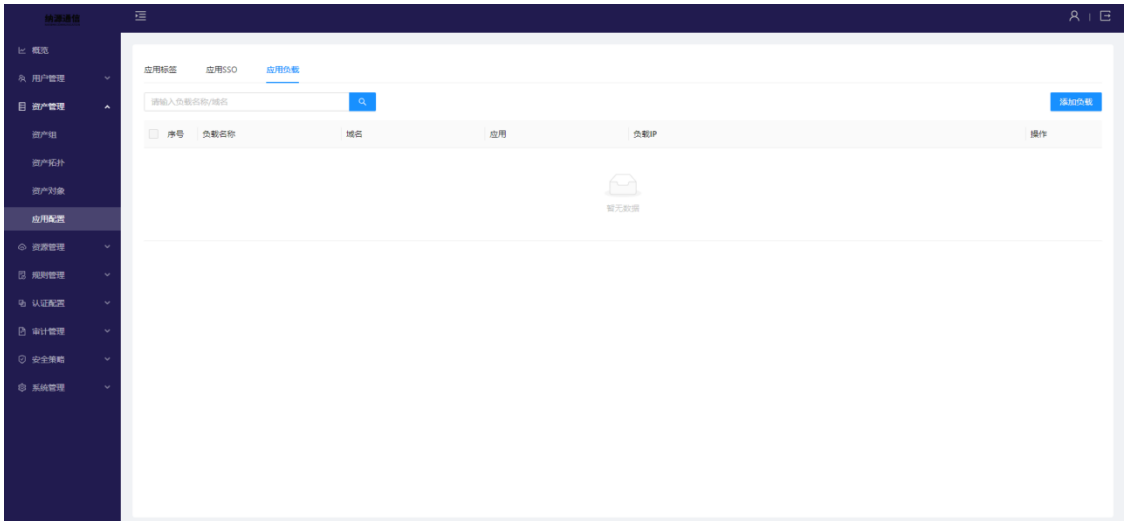


- 表单代填：配置表单相应元素值，如图所示：

- Oauth2.0：添加后会为该应用生成单独的密钥，被登录的应用系统向本系统 API 接口发送密钥进行认证；

应用负载

配置 WEB 应用负载均衡，根据 `ip-hash` 算法进行轮询，如图所示：

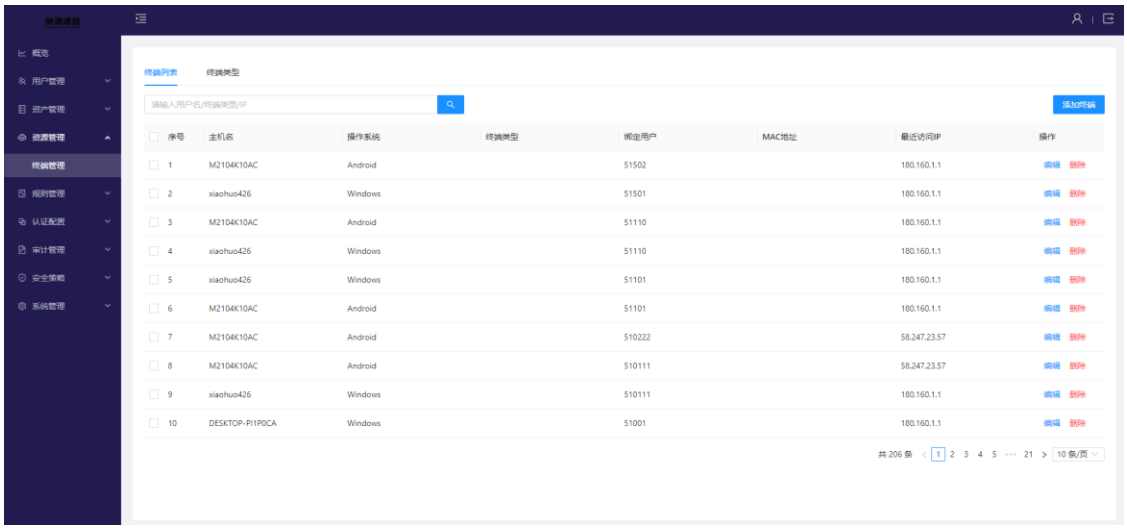


- 负载名称：配置应用负载名称；
- 主域名：选择应用负载主域名；
- 应用：选择应用协议；
- 负载 IP：配置负载 IP；

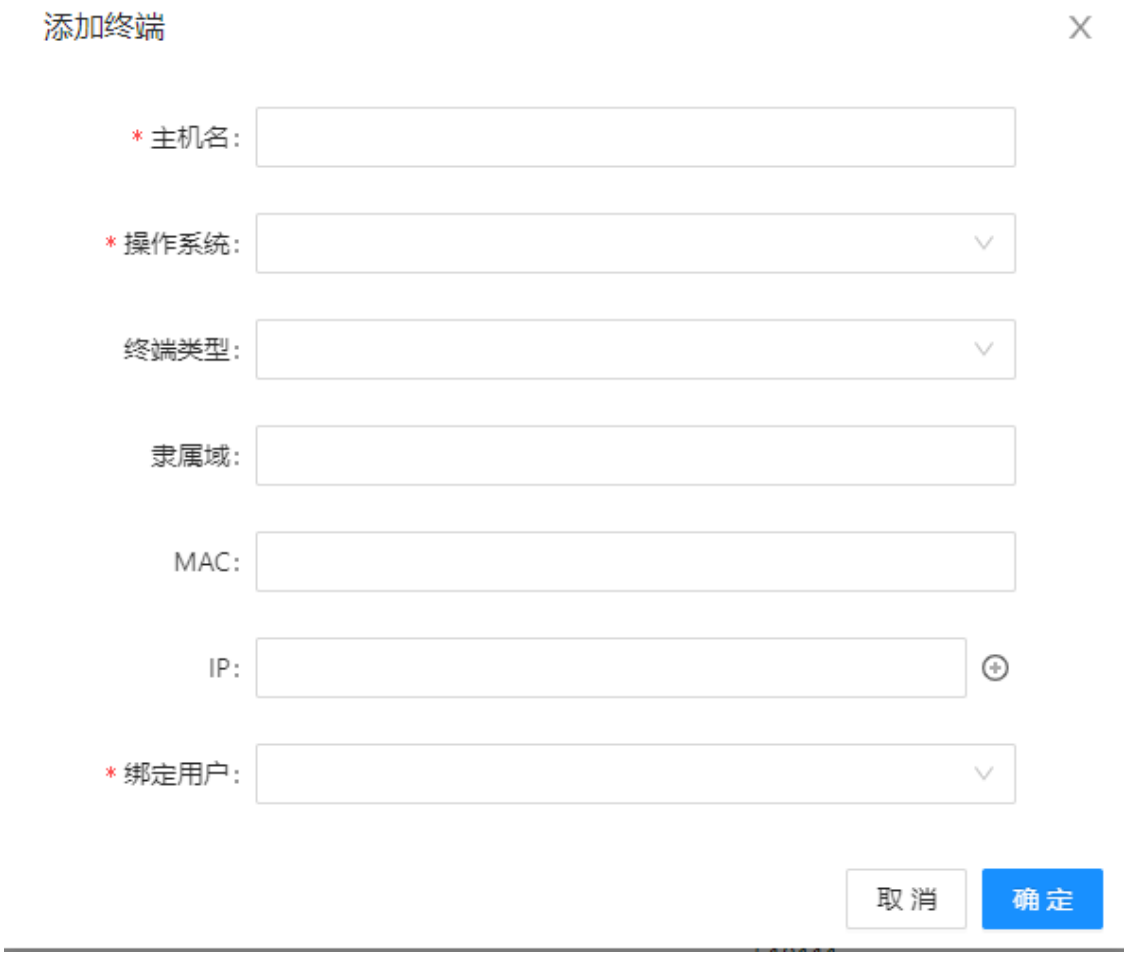
资源管理

终端管理

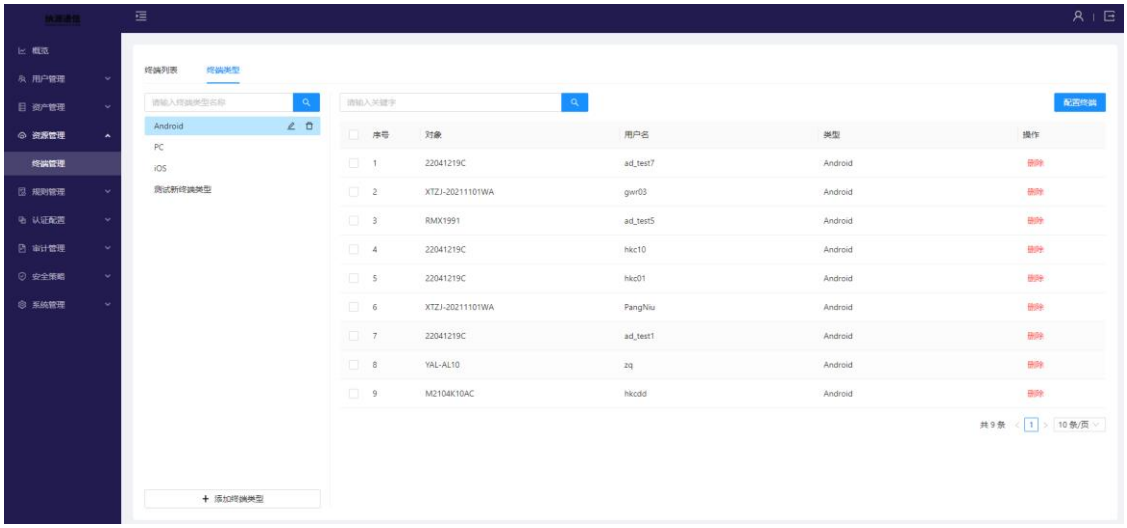
- 终端列表：展示登录客户端的终端设备的**主机名、操作系统、终端类型、绑定用户、MAC 地址**以及**最近访问 IP**。



添加/编辑终端：对终端列表中的设备进行编辑操作用来限制登录设备。填写操作设备的主机名，选择操作系统及终端类型，设置隶属域、MAC 地址、IP 同时绑定用户，登录账号如不满足设置的规则就会无法进行登录。如下图所示：



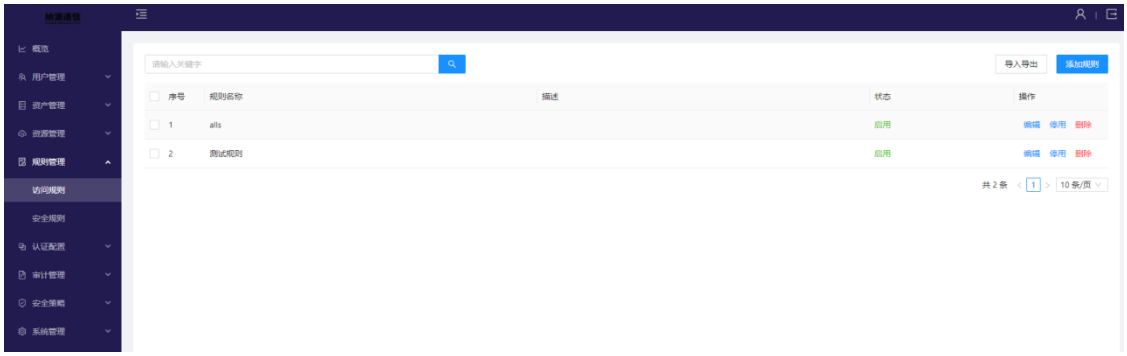
- 终端类型：可添加终端类型标签，对不同的终端设备进行分类编辑操作。



规则管理

访问规则

配置管理用户与资产的访问规则，如图所示：

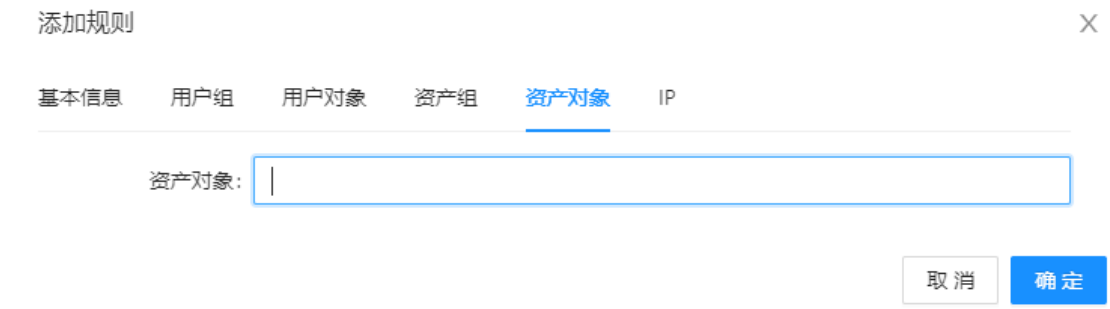


- 规则名称：配置访问规则名称；
- 描述：配置访问规则描述；

- 用户组：勾选用户组，为所勾选的用户配置权限；

- 用户对象：勾选为用户对象，组下新增用户、应用及账号均继承组配置权限；

- 资产组：勾选资产，为勾选的用户增加资产权限。



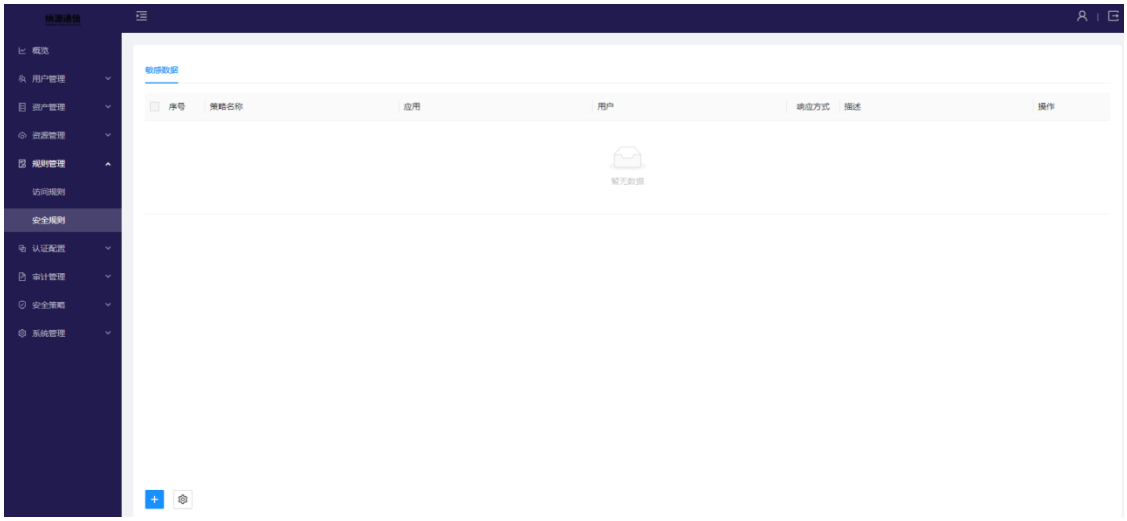
- 资产对象：勾选为资产对象，勾选的用户拥有组下所有资产权限。

- IP：填写 IP，为所属用户增加 IP 权限。可进行选择填写 **IP/IP 区间/IP 段**

安全规则

敏感数据

配置 WEB 应用访问 API 接口审计，当 API 接口返回数据关键字被命中则触发规则，如图所示：

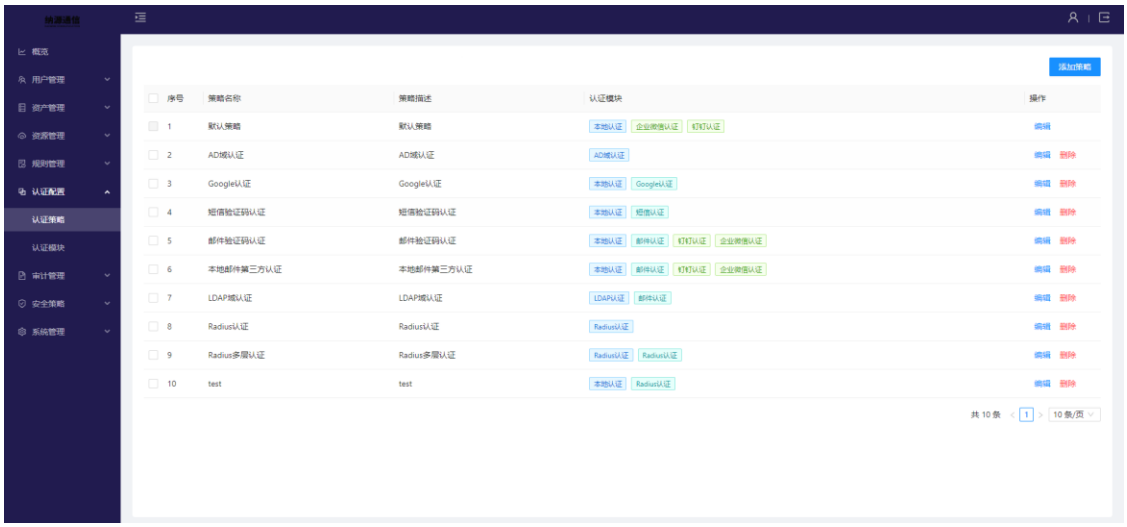


- 告警：配置正则或关键字，触发阈值及周期，并告警；
- 拒绝：配置正则或关键字，触发后拒绝该接口数据请求；
- 替换：配置正则或关键字，触发后替换数据内容；
- 文件类型配置：配置返回接口的文件类型；

认证配置

认证策略

配置管理认证策略，如图所示：



添加策略

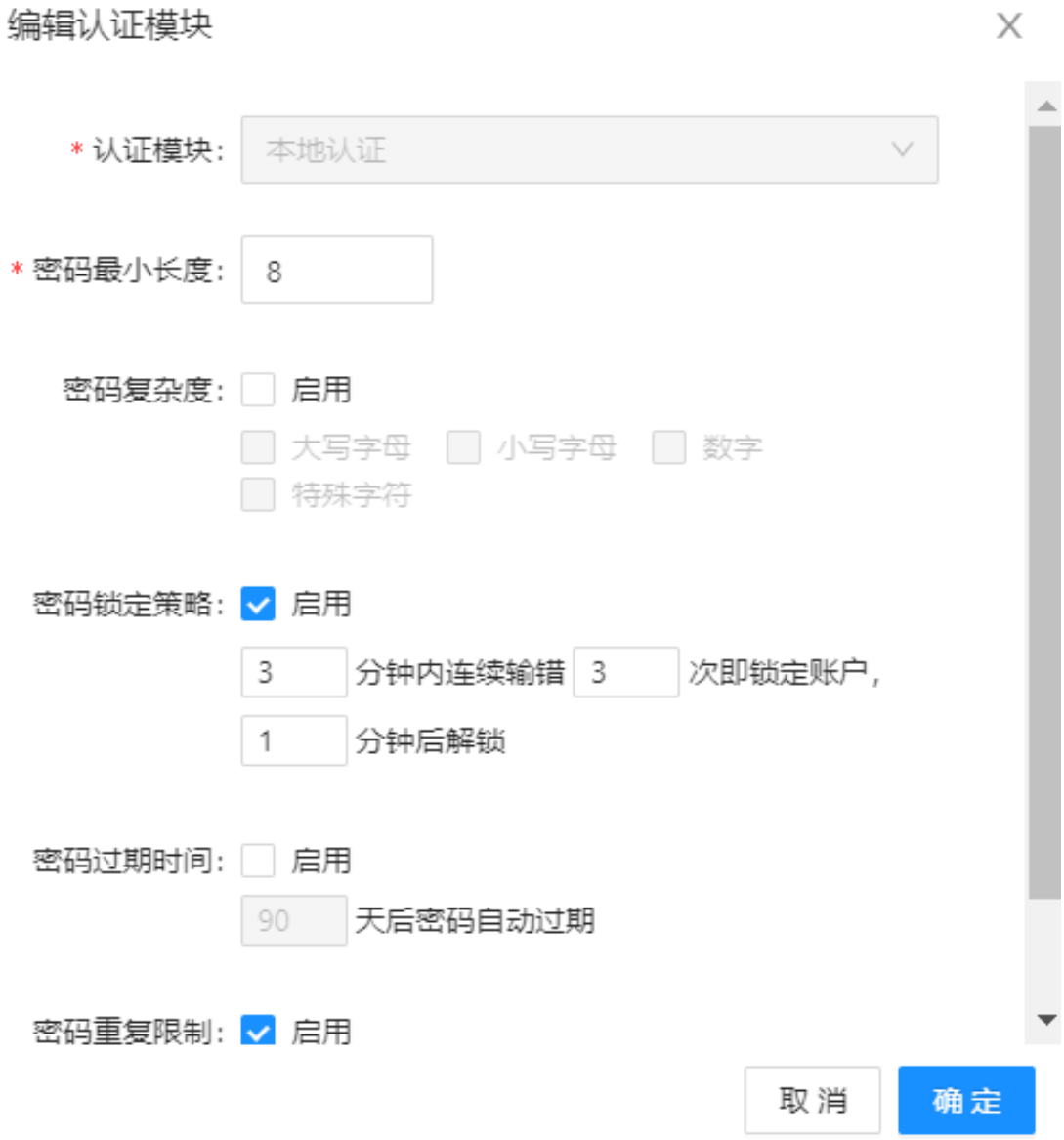
添加认证策略，如图所示：

- 策略名称：配置认证策略名称；
- 策略描述：配置认证策略描述；
- 基础认证：配置基本认证模块，包含本地认证、AD 域认证、LDAP 认证及 Radius 认证；
- 动态验证：配置动态认证模块，包含 Google 验证器、短信、邮件；
- 强身份认证：配置强身份认证模块，包含钉钉、企业微信；

认证模块

配置管理认证模块，如图所示：

- 本地认证：配置本地密码安全策略，如图所示：



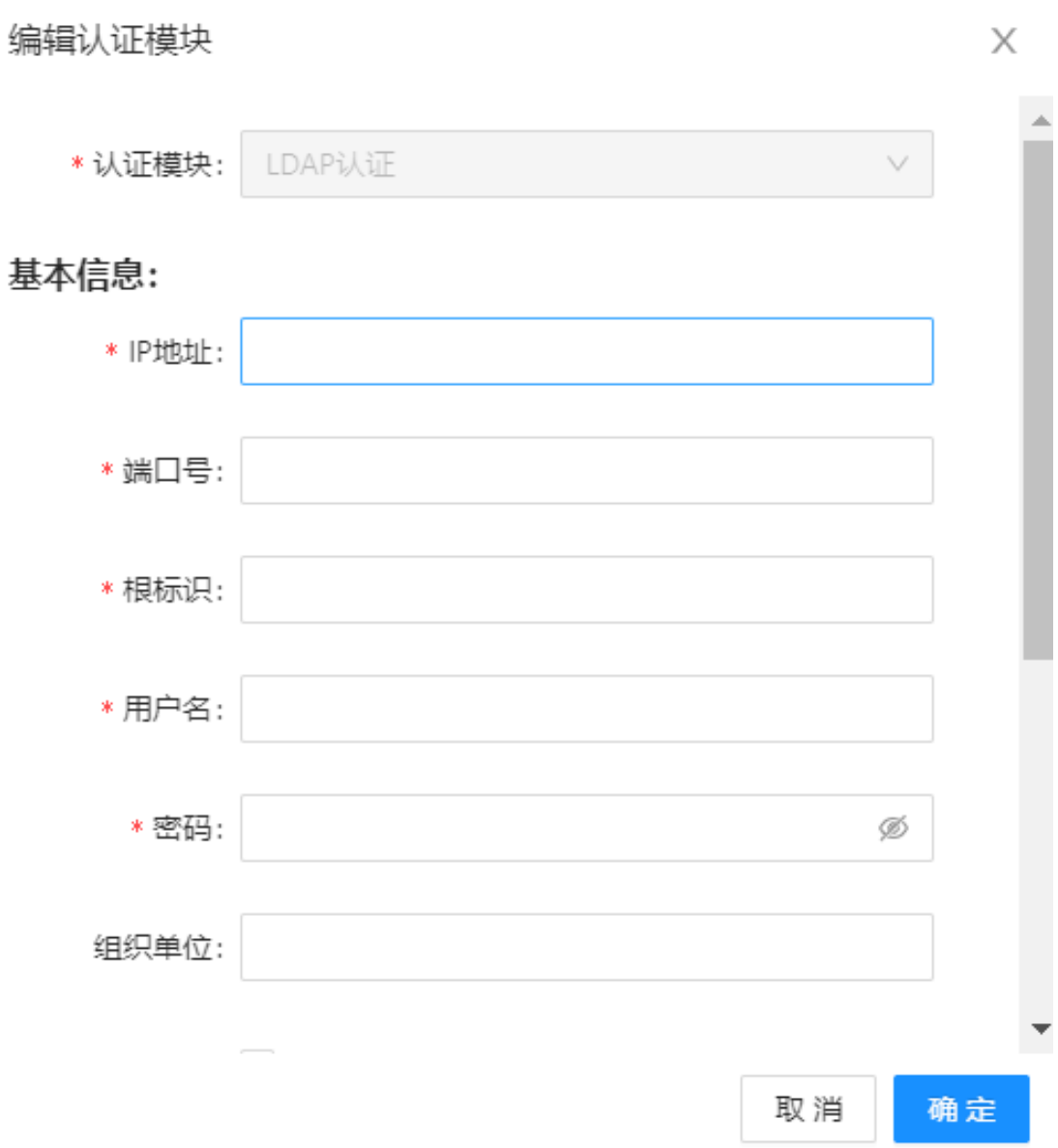
- 钉钉认证：配置钉钉认证模块，如图所示：

- 应用程序公钥：钉钉开发者平台对应应用 AppKey；
- 应用程序私钥：钉钉开发者平台对应应用 AppSecret；
- 回调域名地址：https://零信任网关域名/api/get-code

- 企业微信认证：配置企业微信认证模块，如图所示：

  - 企业 ID：企业微信开发者平台我的企业中的企业 ID；
  - 凭证密钥：企业微信开发者平台对应应用 Secret；
  - Schema：企业微信开发者平台对应应用，企业微信授权登录中的 schema；
  - 登陆接入公钥：企业微信开发者平台对应应用 AgentId；
  - 回调域名地址：企业微信开发者平台对应应用，企业微信授权登录中设置零信任网关域名:端口；

- LDAP 认证：配置 LDAP 认证模块，如图所示：



- IP 地址：配置 LDAP 服务器地址；
- 端口号：配置 LDAP 服务器端口，缺省为 389；
- 根标识：配置 LDAP 根标识；
- 用户名：配置 LDAP 登录用户信息；
- 密码：配置 LDAP 登录用户密码；

  - 组织单位：配置同步的组，不指定 OU 即同步全部；
  - SSL/TLS：是否启用 SSL/TLS；
  - 用户名：同步用户对应的用户名字段；
  - 姓名：同步用户对应的姓名字段；
  - 邮箱：同步用户对应的邮箱字段；
  - 手机：同步用户对应的手机字段；
- AD 域认证：配置 AD 域认证模块，如图所示：

  - IP 地址：配置 AD 域服务器地址；

- 端口号：配置 AD 域服务器端口，缺省为 389；
  - 根标识：配置 AD 域根标识；
- 用户名：配置 AD 域登录用户信息；
  - 密码：配置 AD 域登录用户密码；

- 组织单位：配置同步的组，不指定 OU 即同步全部；
  - SSL/TLS：是否启用 SSL/TLS；
- 用户名：同步用户对应的用户名字段；
  - 姓名：同步用户对应的姓名字段；
- 邮箱：同步用户对应的邮箱字段；
  - 手机：同步用户对应的手机字段；
- Radius 认证：配置 Radius 认证模块，如图所示：

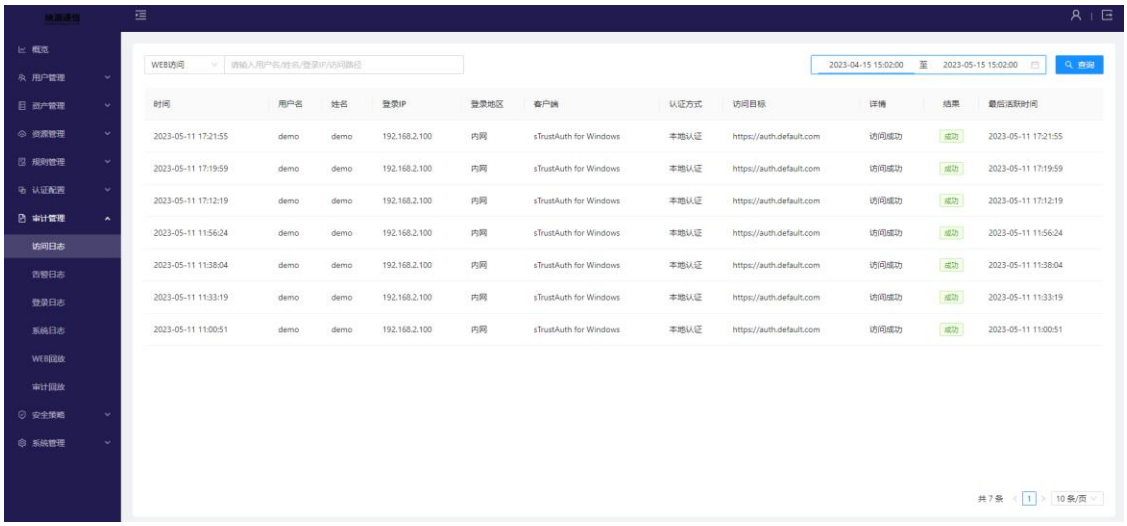
  -
  -
  - 地址：配置 Radius 服务器地址；
- 端口号：配置 Radius 服务器端口，缺省为 1812；
  - 密钥：配置 Radius 服务器密钥；

- Google 认证：无需配置；
- 短信认证：无需配置，短信发送根据通知配置中的设置；
- 邮件认证：无需配置，邮件发送根据通知配置中的设置；

审计管理

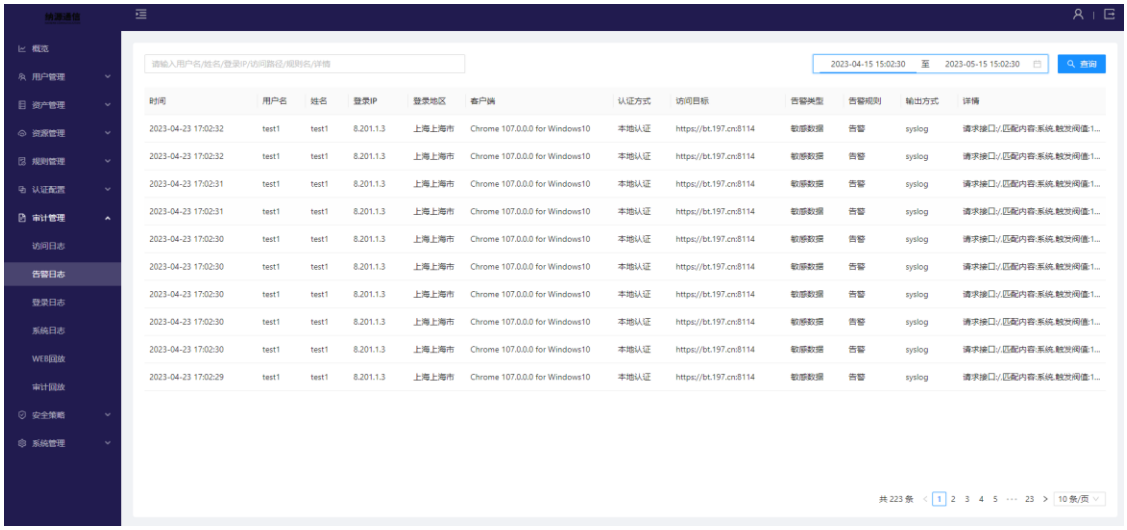
访问日志

可查询所有 **WEB/网络**应用的访问日志，包括访问**时间、用户名、姓名、登录 IP、登录地区、客户端、认证方式**等，如图所示：



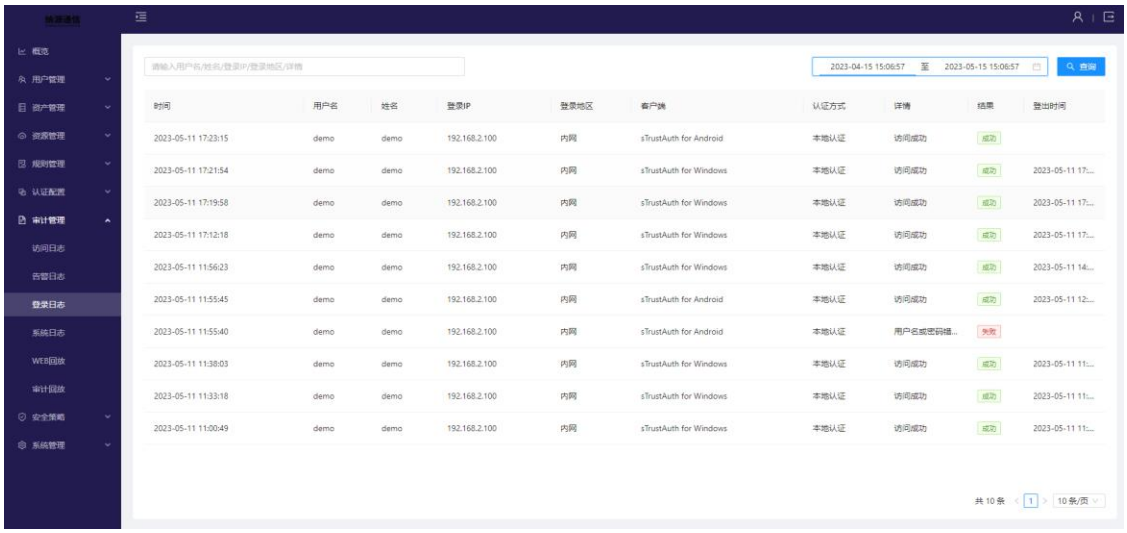
告警日志

可查询所有 WEB 安全策略敏感数据触发告警日志，如图所示：



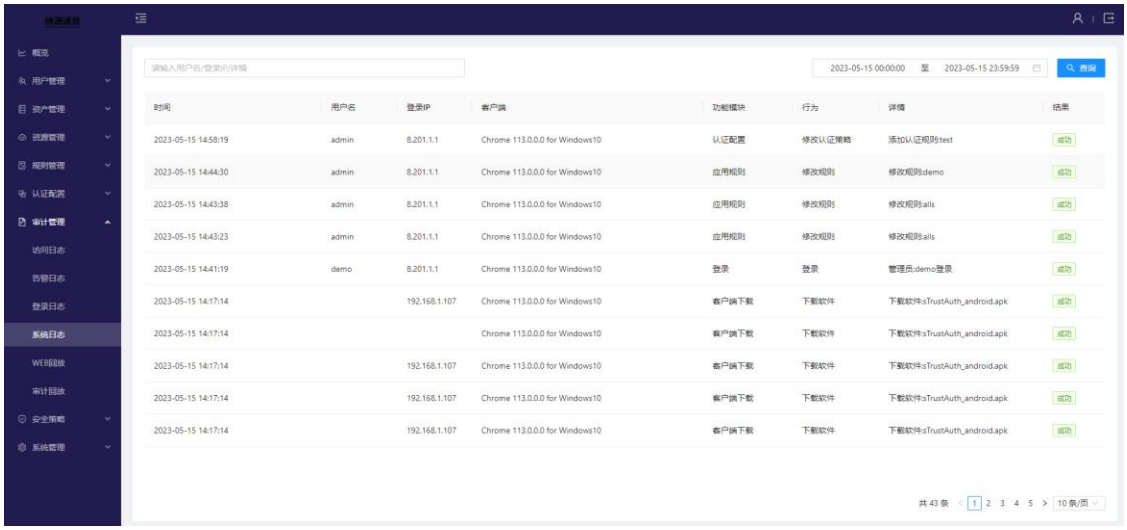
登录日志

可查询系统用户登录的详细日志，包括访问**时间、姓名、登录 IP、登录地区、客户端、认证方式**等。如下图所示：



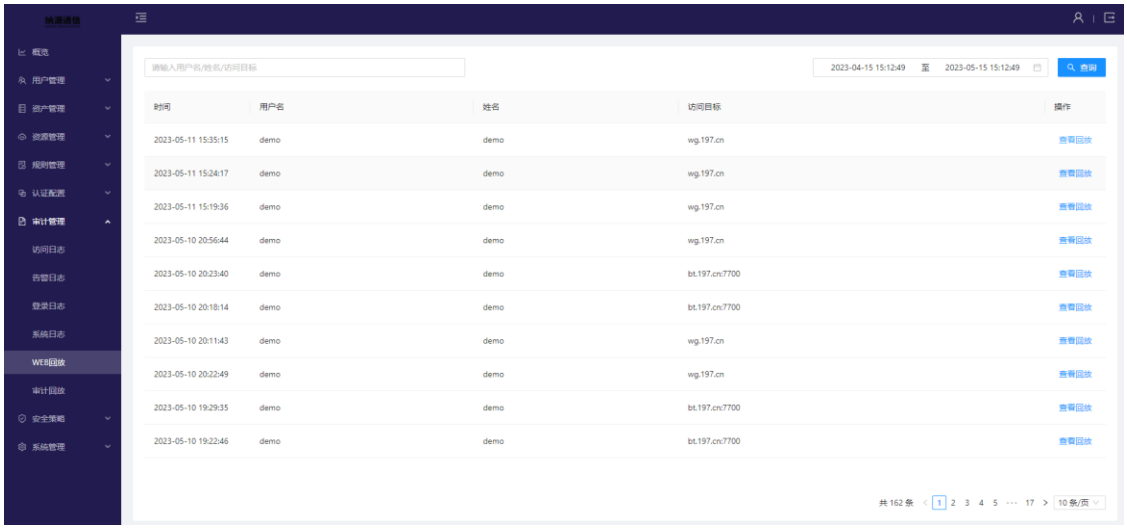
系统日志

可查询该系统的系统相关日志，包括用户操作行为，软件下载详情以及系统更新日志等。如下图所示：



WEB 回放

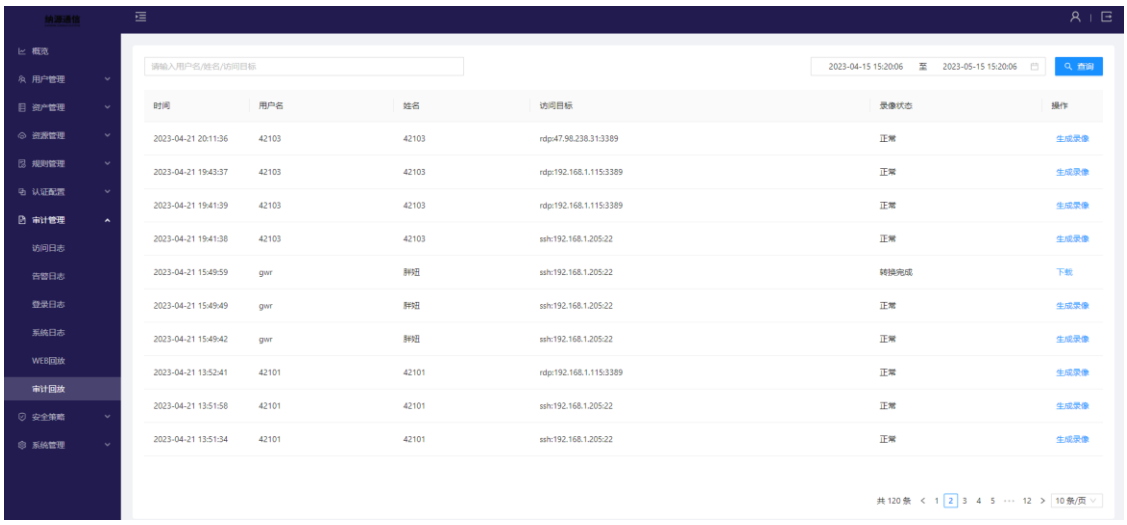
可查询用户浏览器操作回放，用户在设置了开启 **web 回放**功能的页面时，会记录下用户的操作行为并保存为回放可进行随时查看。



点击查看回放，可查看用户的操作记录。并可以设置播放速度 **1X/2X/4X/8X** 速度播放。同时可以跳过静止画面(此按钮需要在未进入静止画面前开启才会生效)。

审计回放

可查询用户操作并生成录像，同时支持下载到本地进行查看。如下图所示：

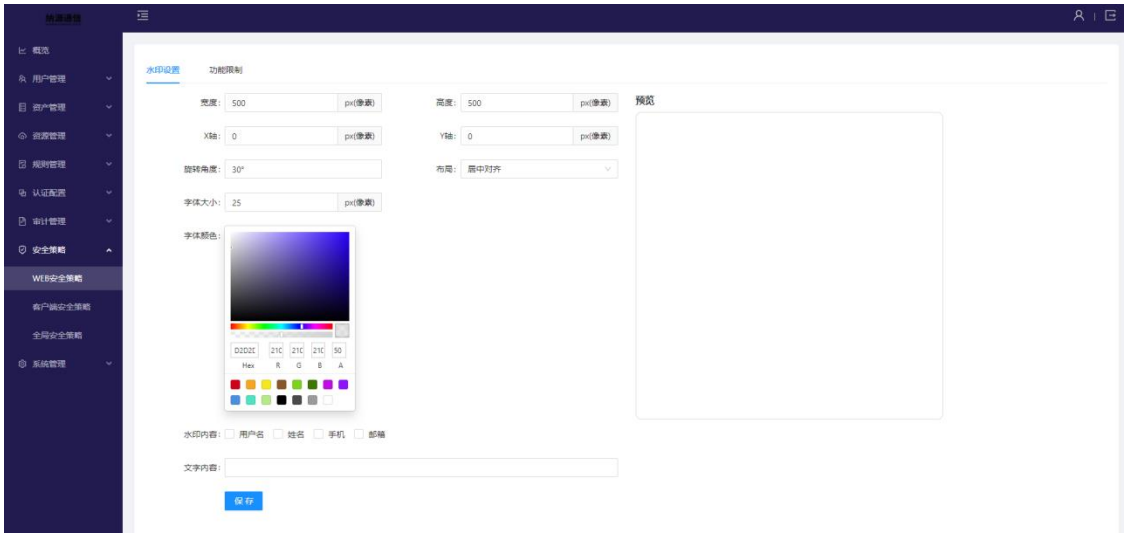


安全策略

WEB 安全策略

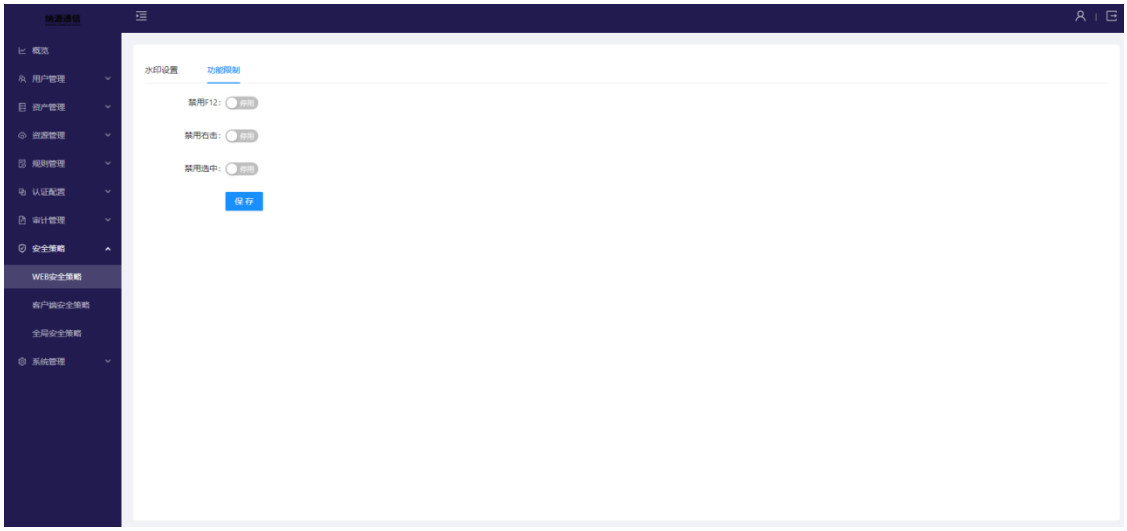
水印设置

配置 WEB 应用访问水印的像素，文字内容，字体大小、颜色、角度，如图所示：



功能限制

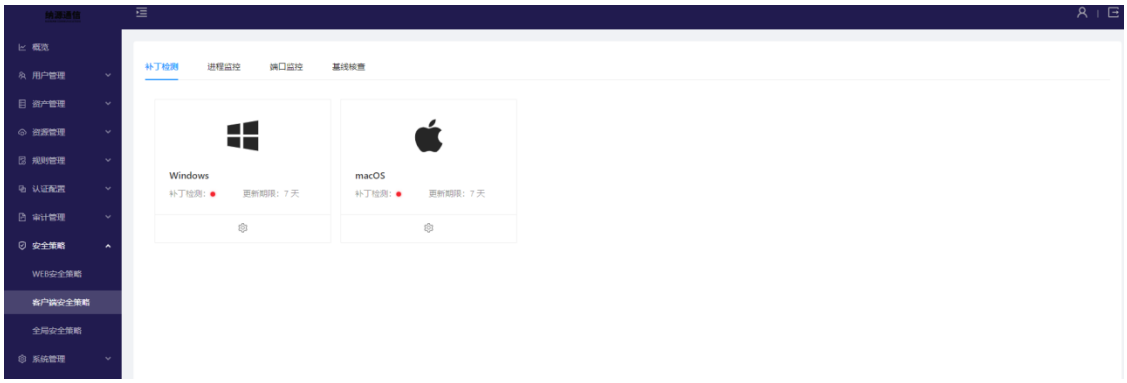
配置 WEB 应用访问功能限制，如图所示：



客户端安全策略

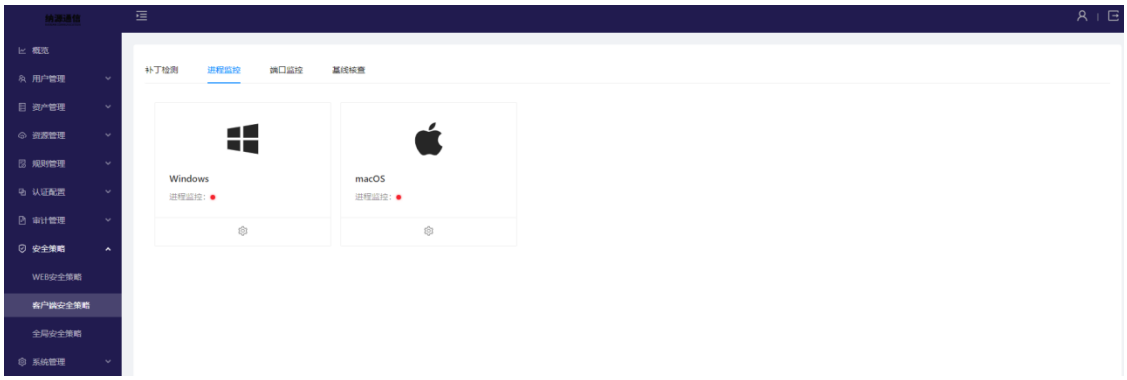
补丁检测

配置客户端补丁安全策略，检测客户端连接终端系统补丁状态，补丁未更新则不允许连接访问，如图所示：



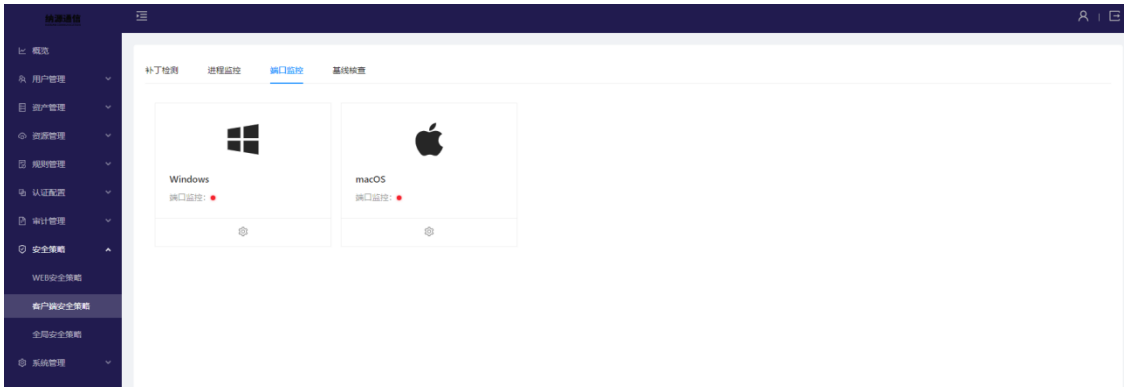
进程检测

配置客户端进程安全策略，检测客户端连接终端系统进程，未按照策略开启相关进程则不允许连接访问，如图所示：



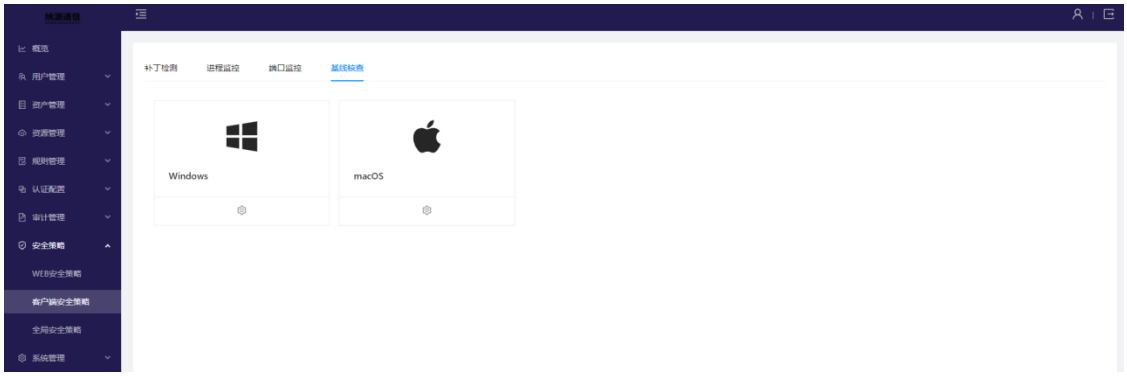
端口检测

配置客户端端口安全策略，检测客户端连接终端系统端口，如若有开启策略相关端口则不允许连接访问，如图所示：



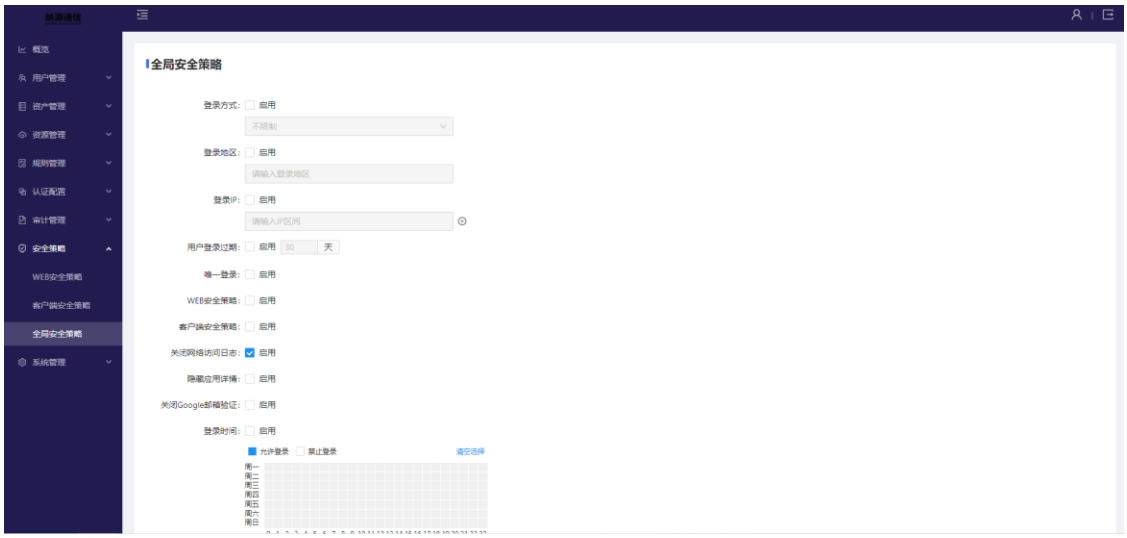
基线核查

配置客户端基线安全策略，检测客户端的最低安全要求，包括服务和应用程序设置、操作系统组件的配置、权限和权利分配、管理规则等。



全局安全策略

全局安全策略开启，针对系统所有用户立刻生效。



- **登录方式**：配置用户登录方式，**默认**为**不限制**；
  - 只允许 WEB 登录：只允许用户登录 WEB 门户，不允许通过客户端登录；
  - 强制客户端登录：强制用户只能通过客户端登录，不允许直接登录门户；
- **登录地区**：限制用户登录地区；
- **登录 IP**：限制用户登录 IP；
- **用户登录过期**：启用后超过设置时长未登录停用用户；
- **唯一登录**：设置唯一登录后，同一账号只能在一台设备上登录；
- **WEB 安全策略**：配置用户是否启用 WEB 安全策略，策略遵循安全策略中的 WEB 安全策略配置；
- **客户端安全策略**：配置用户是否启用客户端安全策略，策略遵循安全策略中的客户端安全策略配置；
- **关闭网络访问日志**：启用后，关闭网络访问日志，**审计管理/访问日志**中网络访问不在进行记录；

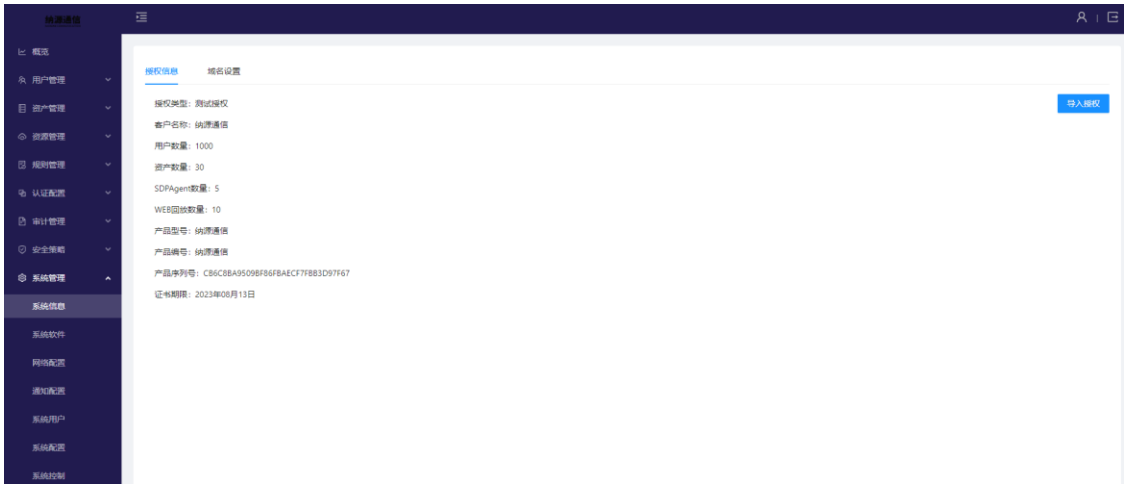
- **隐藏应用详情**：启用后，应用隐藏不可见，可通过域名进行访问，客户端所有应用中不可见；
- **关闭 Google 邮箱验证**：启用后，登录 **Google 认证**账号不在需要**邮箱/短信**验证；
- **登录时间**：配置用户允许与禁止的访问时间。

系统管理

系统信息

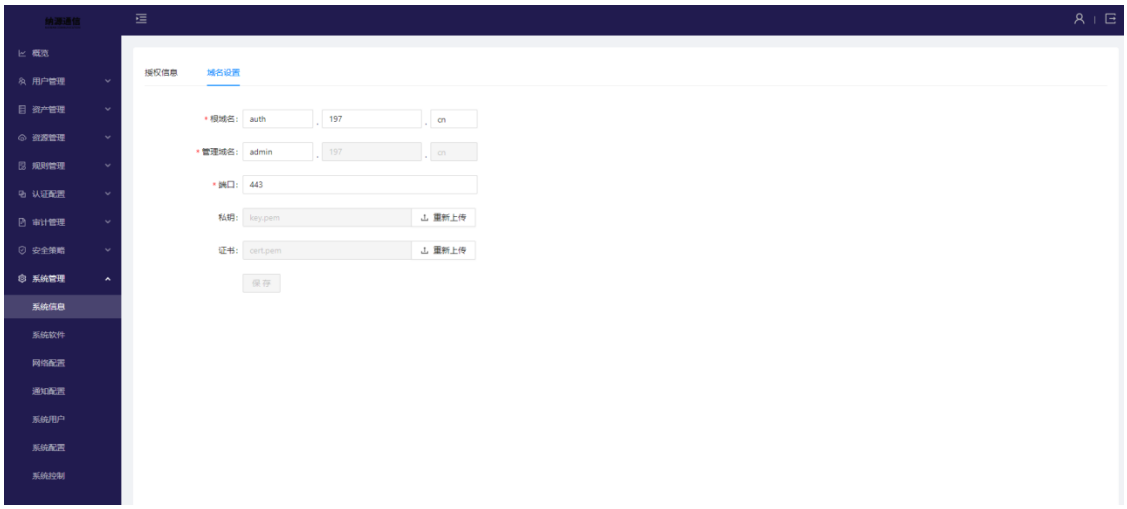
授权信息

显示当前系统授权信息，导入授权，文件向管理员索取，如图所示：



域名设置

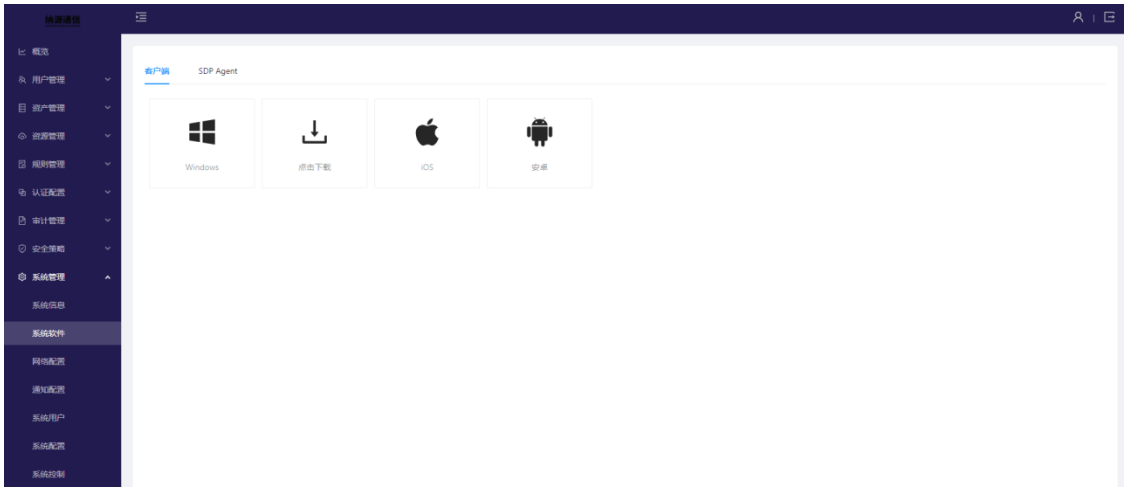
配置系统主域名及门户监听端口及 SSL 证书，如图所示：



系统软件

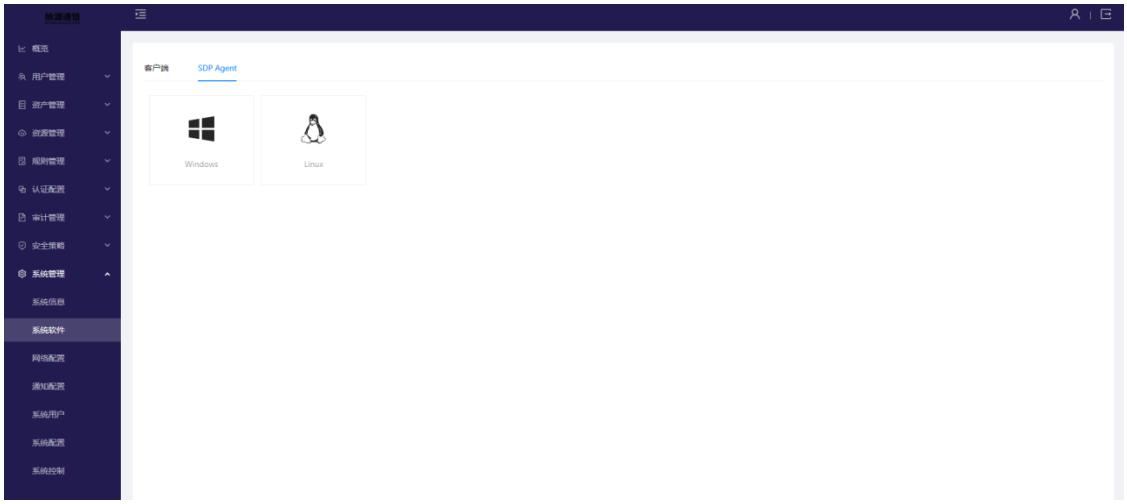
客户端

下载零信任访问客户端，如图所示：



SDP Agent

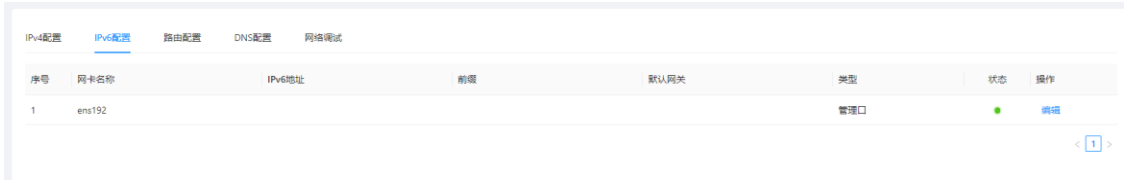
下载 SDPAgent，如图所示：



网络配置

IPv4/IPv6 配置

配置系统网口 IP 及默认网关，如图所示：



路由配置

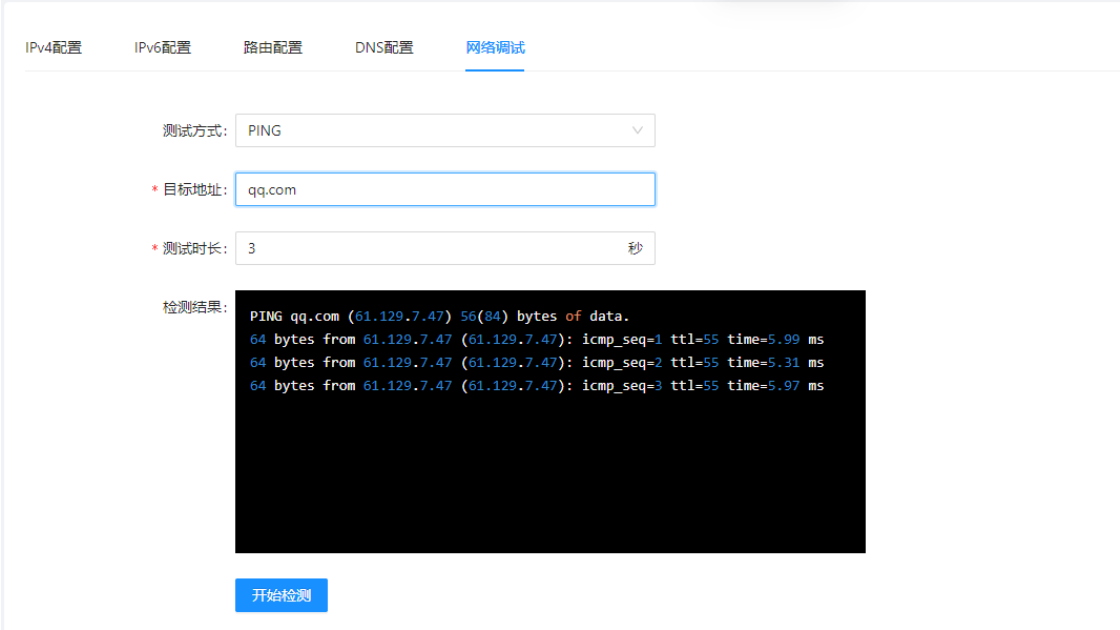
配置系统静态路由，如图所示：

DNS 配置

配置系统 DNS，如图所示：

网络调试

测试网络通信或进行数据抓包，如图所示：



通知配置

短信

配置系统短信输出接口，如图所示：

邮件

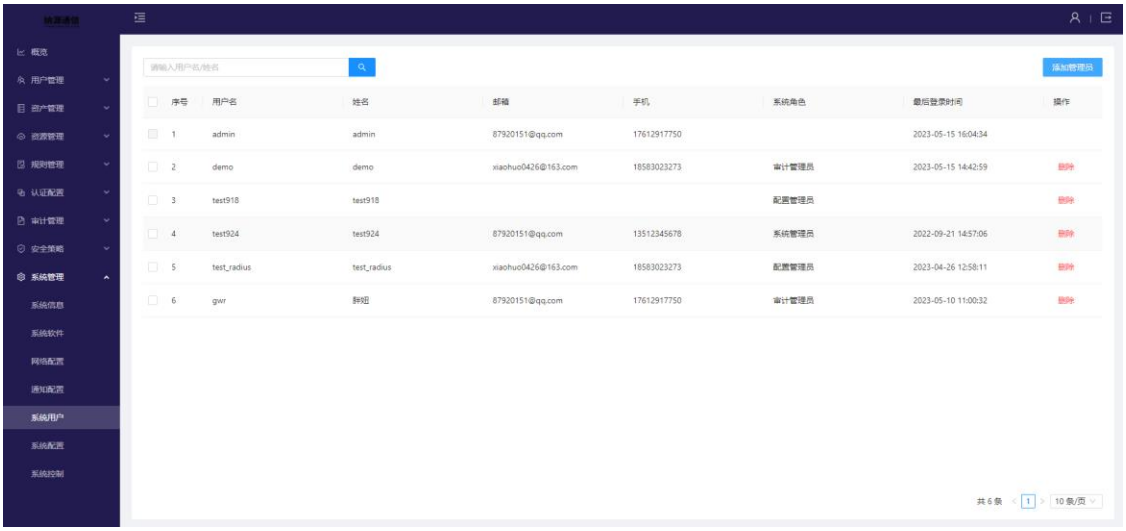
配置系统邮件输出接口，如图所示：

SYSLOG

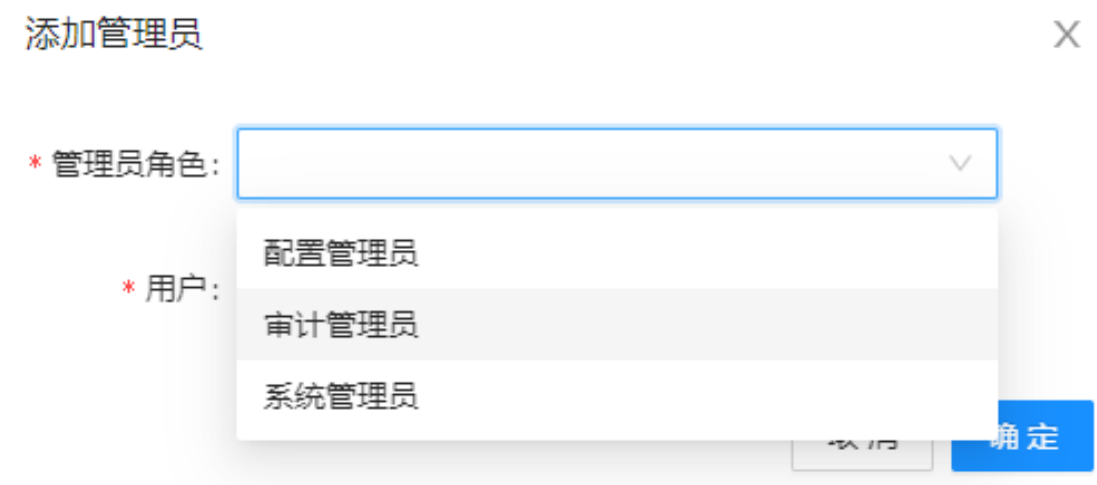
配置系统 SYSLOG 输出接口，如图所示：

系统用户

设置系统用户，系统用户登录客户端后，不影响管理系统正常使用。



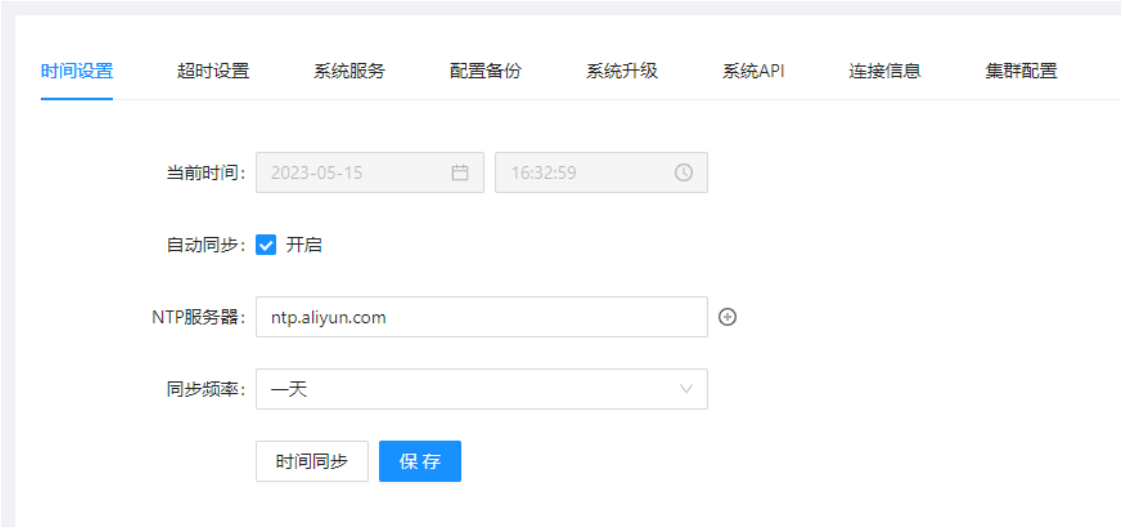
可为不同用户添加不同管理员角色，如下图所示：



系统配置

时间设置

配置系统时间及 NTP 服务器，如图所示：



超时设置

配置系统会话及管理页面超时时间，如图所示：

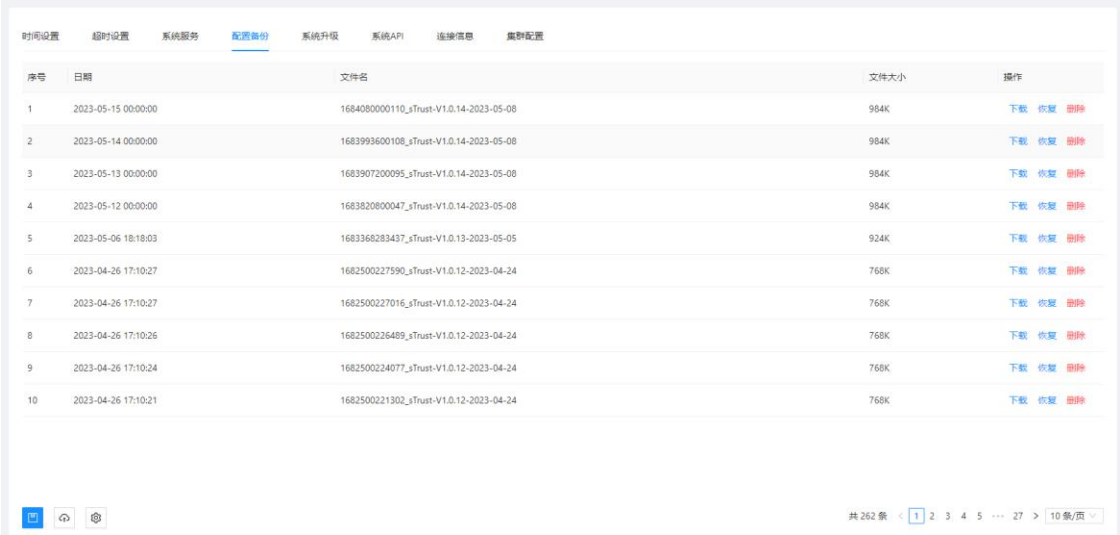
系统服务

查看系统服务状态及设置其端口与访问权限，如图所示：

- 访问权限：设置系统服务访问权限；
  - 开放：允许直接访问服务端口；
  - 关闭：不允许直接访问服务端口；

配置备份

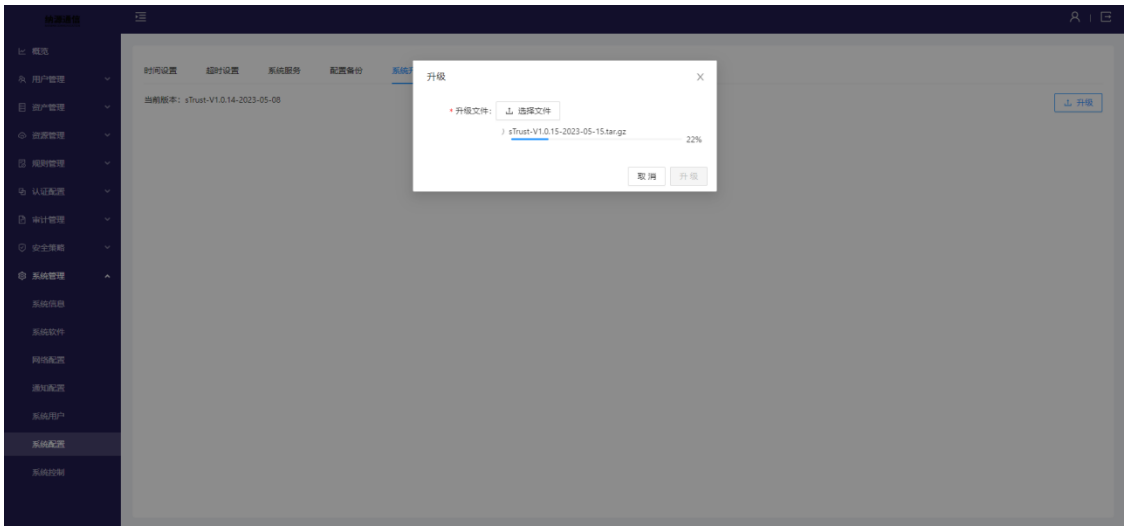
备份系统配置及恢复系统配置，如图所示：



- 备份：立即备份当前系统配置信息；
- 恢复：恢复配置文件，可选择响应恢复内容；
  - 系统：恢复系统所有配置，会涉及服务重启；
  - 网络：恢复系统网络配置；
  - 应用：仅恢复应用相关配置；
- 配置：自动备份系统配置。

系统升级

查看当前系统版本或进行系统升级。升级包向管理员索取，上传升级包进行升级操作。如下图所示


升级
升级文件：
选择文件
sTrust-V1.0.15-2023-05-15.tar.gz
22%
取 消
升 级
当前版本：sTrust-V1.0.14-2023-05-08
升级

升级完成如下图所示：


升级
系统升级成功
确 定

系统 API

对外开放的 API，可对用户、资产、访问规则进行修改。如下图所示：

连接信息

设置服务器连接地址及端口号，如下图所示：

集群配置

集群配置用于确保零信任产品的连续可用性和可靠性。如下图所示：

系统控制

控制系统重启或者关机，如图所示：