

管理员使用手册

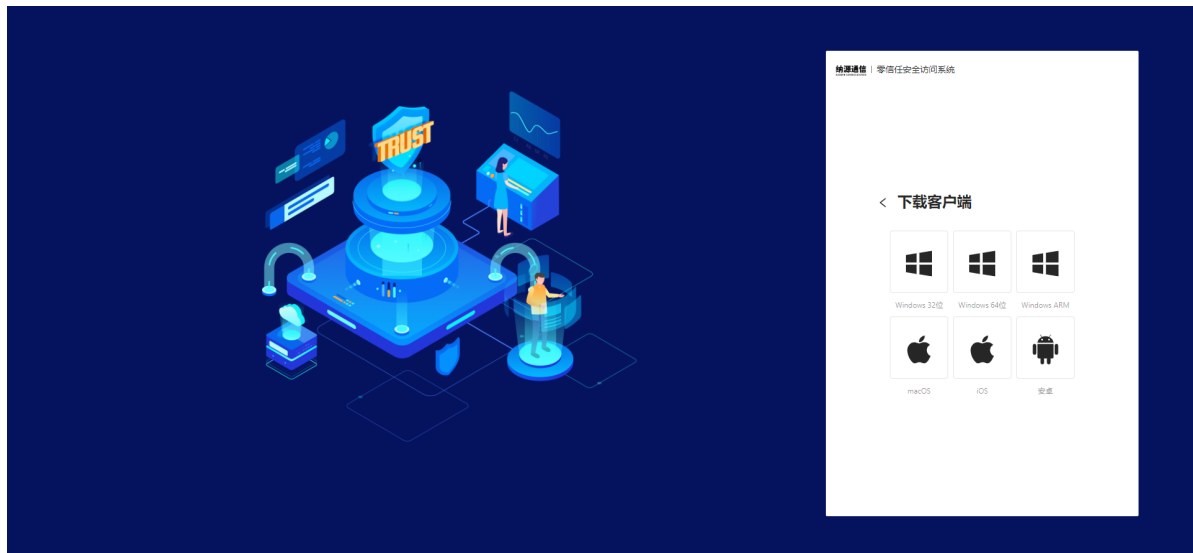
纳源通信零信任安全访问系统采用B/S架构管理，在浏览器中输入<https://IP:3001>访问系统登录界面，默认账号/密码：admin/njny1108

注意：首次登录请务必修改初始化密码

通用功能

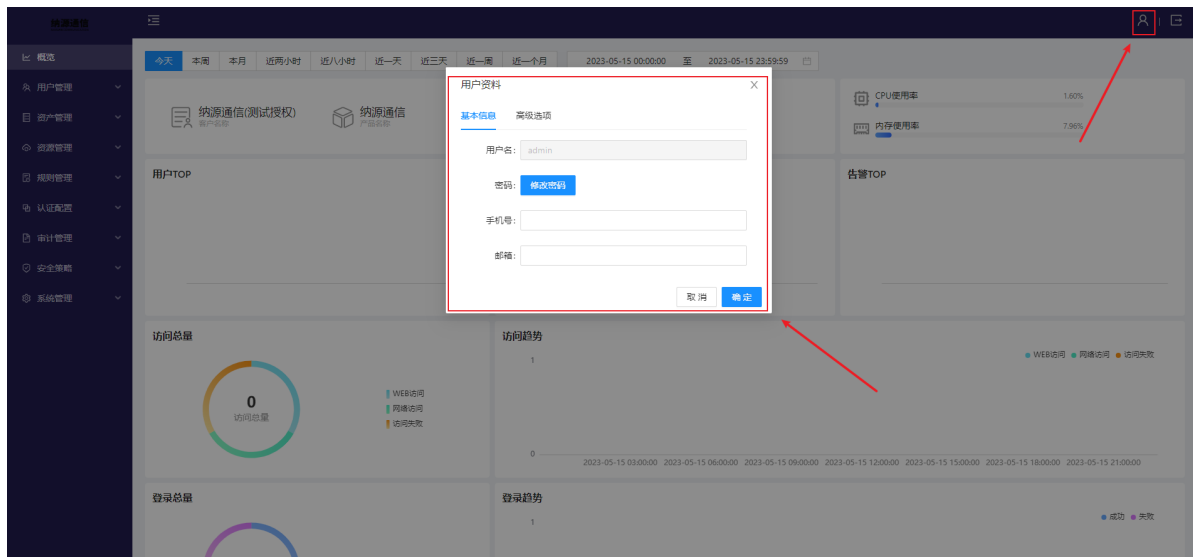
下载客户端

访问管理后台地址，点击 **下载客户端**。



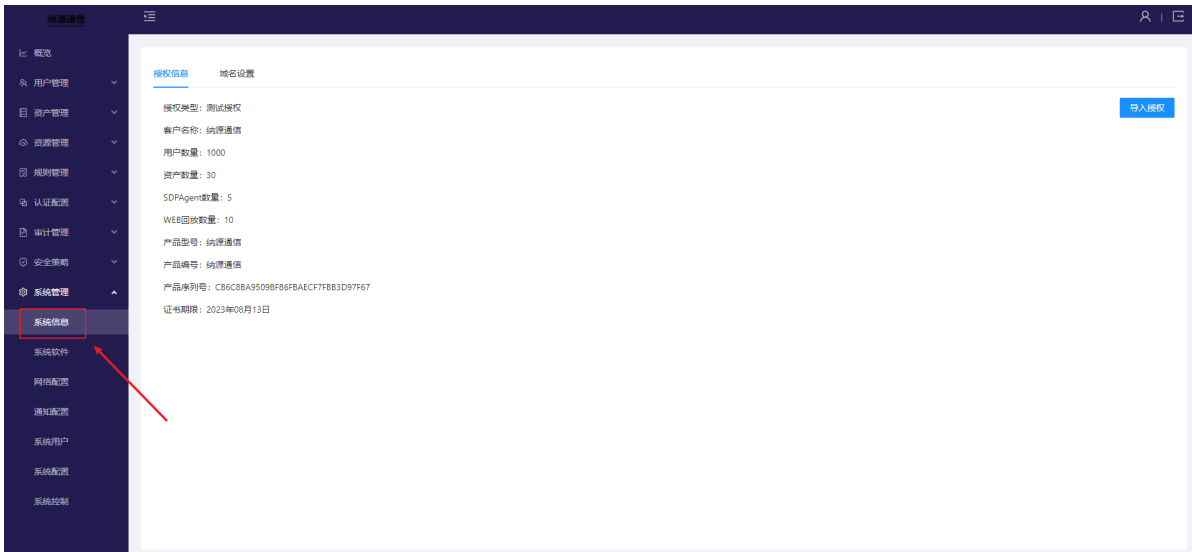
修改管理员资料

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。



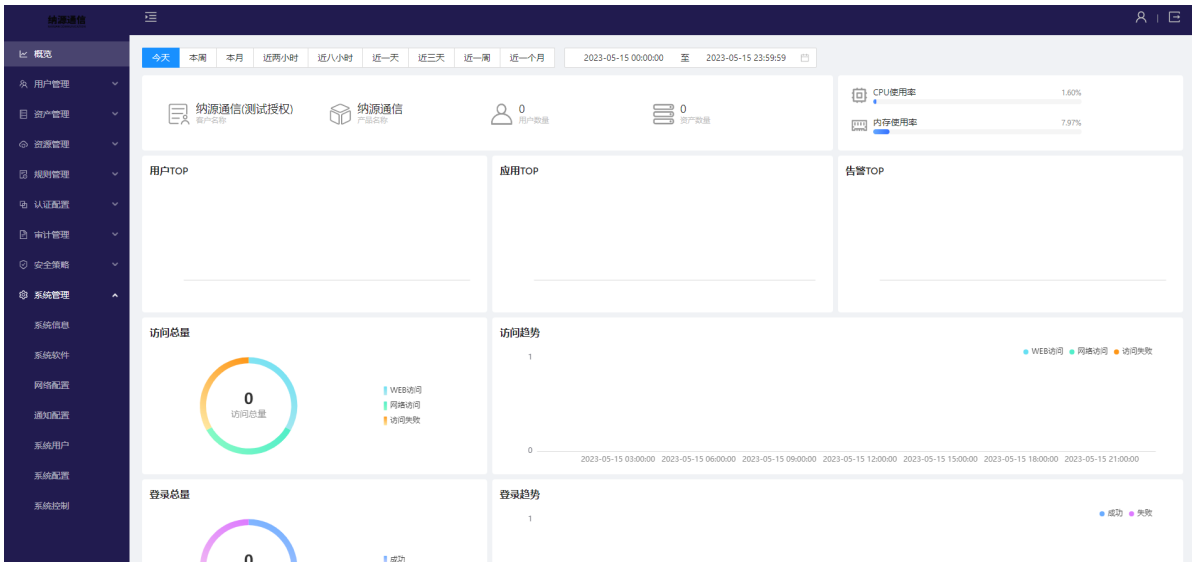
查看系统信息

点击 **系统管理--系统信息**，可查看当前系统信息。



概览

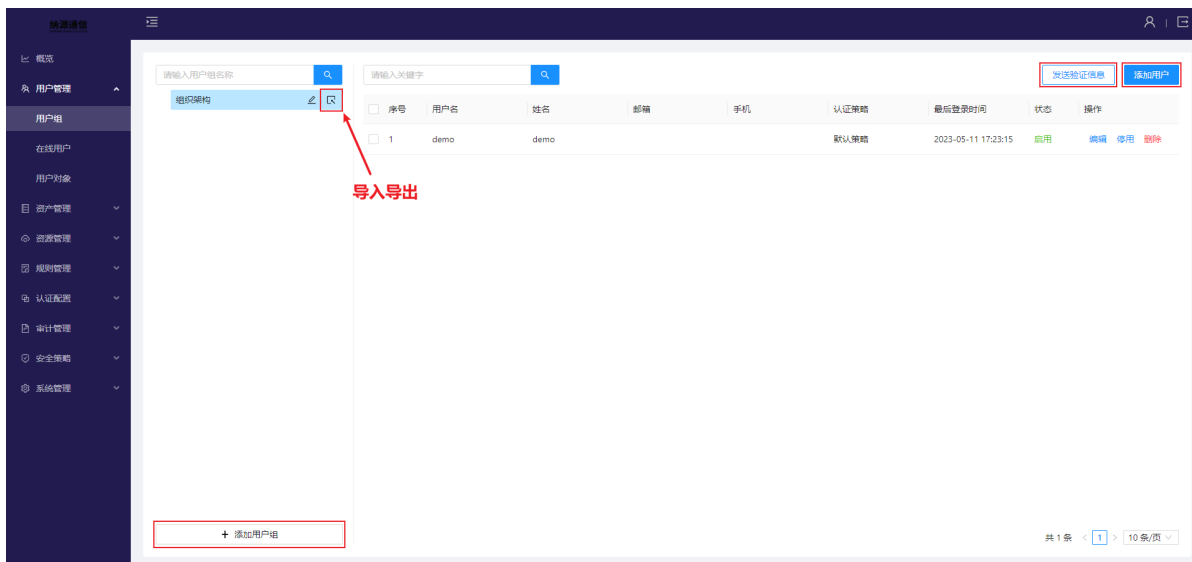
该页面展示系统基本信息，如：系统基本信息、操作系统CPU与内存占用率、用户TOP、应用TOP、告警TOP、访问总量、访问趋势、登录总量、登录趋势。鼠标悬停在各数据模块上，会显示对应的数据详情。



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：

导入导出

X

用户导入

用户导出

AD域/LDAP

钉钉

企业微信

REST-API

导入记录

* 上传文件：

选择文件

下载模版

取消

导入

- 用户导出：选择字段及用户组导出用户信息，如图所示：

导入导出

X

用户导入

用户导出

AD域/LDAP

钉钉

企业微信

REST-API

导入记录

* 导出字段：

全选

手机号

邮箱

所属组

认证策略

高级选项

选择用户组：

取消

导出

- 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：

导入导出

X

用户导入 用户导出 AD域/LDAP 钉钉 企业微信 REST-API 导入记录

认证模块选择:

自动同步: ☐ 启用 (小时)

取消

保存

- 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:

导入导出

X

用户导入 用户导出 AD域/LDAP 钉钉 企业微信 REST-API 导入记录

自动同步: ☐ 启用 (小时)

取消

保存

- 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:

导入导出

X

用户导入 用户导出 AD域/LDAP 钉钉 企业微信 REST-API 导入记录

自动同步: ☐ 启用 (小时)

取消

保存

- 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:

导入导出

X

用户导入 用户导出 AD域/LDAP 钉钉 企业微信 REST-API 导入记录

认证模块选择:

自动同步: ☐ 启用 (小时)

取消

保存

- 导入记录: 展示近20条导入用户信息日志, 如图所示:

当前页面只展示近 20 条记录，更多记录请到审计管理 > 系统日志查看。

时间

导入方式

详情

详情



暂无数据

添加用户

添加用户及相关配置，如图所示：

添加用户

X

基本信息

高级选项

* 用户名：

* 姓名：

* 密码：



* 确认密码：



邮箱：

手机：

* 所属组：

组织架构 x

认证策略：

默认策略



取消

确定

- 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；

添加用户

X

基本信息

高级选项

登录方式: 不限制

登录地区:

登录IP: 

登录系统: 自动识别

唯一登录: ☐ 启用

WEB安全策略: ☐ 启用

客户端安全策略: ☐ 启用

登录时间: ☐ 启用

☒ 允许登录 ☐ 禁止登录

清空选择

[illegible]

取消

确定

- 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：

发送验证信息X

注册类型：

注册码

▼

发送方式：

邮件

▼

* 发送对象：

过期时间：

2

小时

▼

取消

确定

- 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：

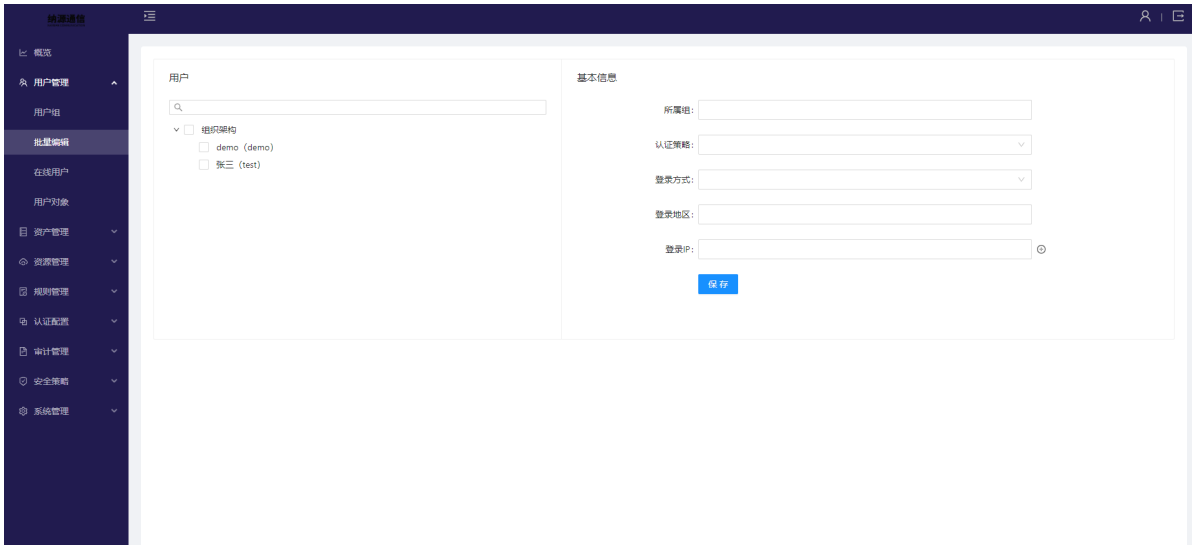
客户端证书绑定码X

JC6ZEduWvv1KIWrUss1PXQi/Xy9XpAuhIIOPGStY9Xihro0mJLGcP5T5SZrKJK/hmRu0BmYd6RNE0Fsx3jFKu5bL1gNhAOuCP29qa2xwQZaYg5eRkTxXN8fCa9Pq1UnLTzTjzb9ovepUCIHnCqI/NT/xpnGEJu2XJ19awNXgVu8JfSuH75KLAsvAhR/seJIXtSkTCt57Mu+FsRtBXry7ghgTvK1oPuPGvo80z3TGi7id3NVTY8/owPnAEbuRQinIF64kSl8bqU8KFg9lxwWAgcTsiBT+rnr0L0oyDa1x5PMTBPr38HI1bZMKoqme/ZxOOiwcoGiV32MS+hiTB9mz7g==

确定

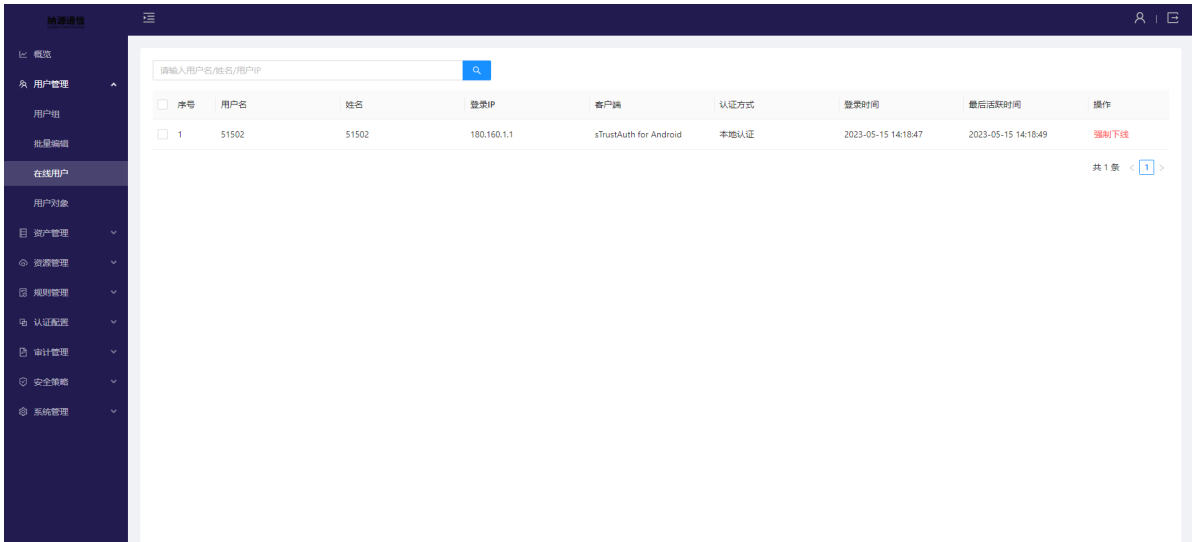
批量编辑

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

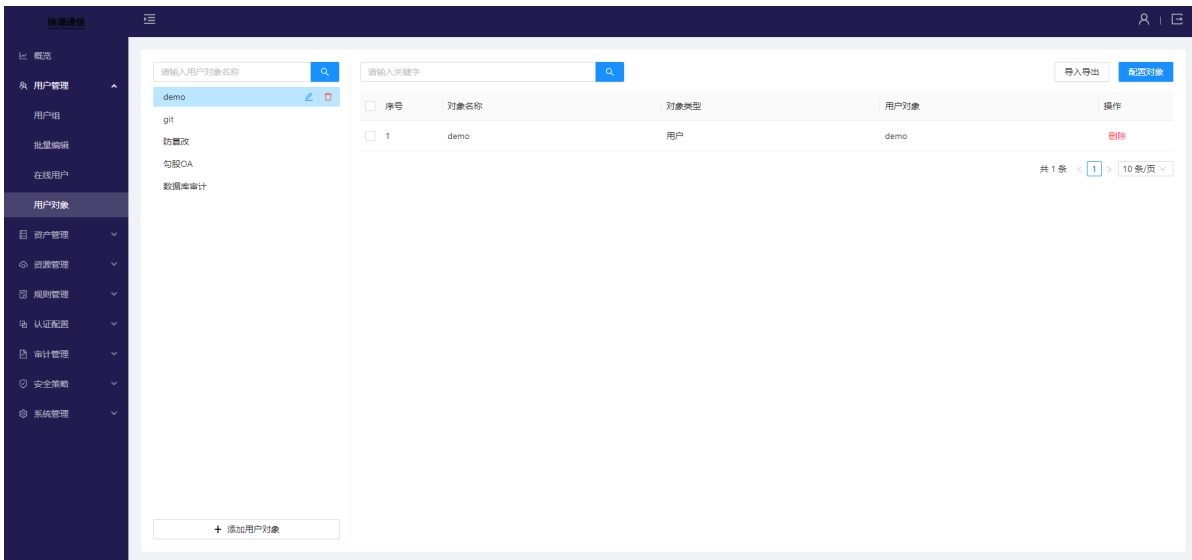
该页面展示当前系统在线用户，如图所示：



- 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：

当前页面只展示近 20 条记录，更多记录请到[审计管理 > 系统日志查看](#)。

时间	导入方式	详情
 暂无数据		

详情

配置对象

添加用户及相关配置，如图所示：

配置对象

X

* 对象名称:

* 用户:

取消

确定

资产管理

资产组

管理资产及资产组，如图所示：

序号	资产名称	资产IP	域名	资产描述	SDP状态	操作
☐	1	数据库审计	192.168.1.221	dba.75.cn	未启用	编辑 删除
☐	2	demo01	192.168.1.234	oa.75.cn	未启用	编辑 删除
☐	3	demo02	192.168.1.38	git.75.cn	未启用	编辑 删除
☐	4	demo03	192.168.1.230	nas.75.cn	异常	编辑 删除
☐	5	demo04	192.168.1.183	tester.75.cn	未启用	编辑 删除

- 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：

导入导出

X

资产导入

资产导出

导入记录

* 上传文件：

选择文件

下载模版

取消

导入

- 资产导出：选择资产组导出资产信息，如图所示：

导入导出

X

资产导入

资产导出

导入记录

* 选择资产组：

取消

导出

- 导入记录：展示近20条导入资产信息日志，如图所示：

导入导出

X

资产导入

资产导出

导入记录

当前页面只展示近 20 条记录，更多记录请到审计管理 > 系统日志查看。

时间	导入方式	详情
----	------	----



暂无数据

添加资产

添加资产及相关配置，如图所示：

基本信息 应用配置 账号配置 访问关系

* 资产名称:

* 资产地址:

资产描述:

SDP控制:

自动检测

▼

SDP端口:

9406

域名:

.75.cn

证书:

公钥

⬆️ 点击上传

私钥

⬆️ 点击上传

取消

确定

- 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；

添加资产X

基本信息应用配置账号配置访问关系

* 应用协议	* 应用端口	应用路径	应用名称	同端口监听	操作
HTTPS	443	/		☒	配置删除
+ 添加应用配置					

取消确定

here192.168.1.183tester.75.cn

- 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；

添加资产X

基本信息应用配置账号配置访问关系

* 账号	* 认证方式	* 绑定应用	操作
admin	密码	HTTPS:443	删除
+ 添加账号配置			

取消确定

adminadministratorrootSSO

- 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；

* 协议	* 类型	* 来源IP	* 来源端口	* 目标IP	* 目标端口	操作
TCP/IP	INPUT		0			删除
+ 添加访问关系						

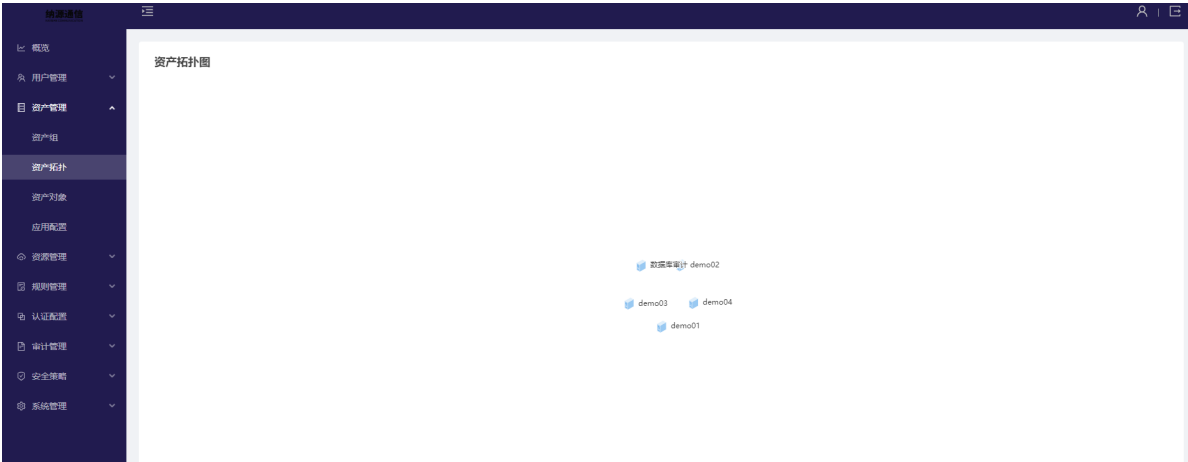
取消

确定

- 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：

序号	对象	类型	资产对象	操作
1	192.168.1.205	资产	demo	删除
2	192.168.1.221	资产	demo	删除

共 2 条 < 1 > 10 条/页

- 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：

导入导出

对象导入

对象导出

导入记录

* 上传文件：

选择文件

下载模版

取消

导入

- 对象导出：选择资产对象导出资产对象信息，如图所示：

导入导出

对象导入

对象导出

导入记录

资产对象：

取消

导出

- 导入记录：展示近20条导入资产信息日志，如图所示：

导入导出

对象导入

对象导出

导入记录

当前页面只展示近 20 条记录，更多记录请到审计管理 > 系统日志查看。

时间	导入方式	详情
2023-04-25 15:50:16	文件	文件导入成功,共导入1个资产对象
2023-04-25 15:48:58	文件	文件导入失败,第2行:不存在的资产.
2023-04-25 15:48:32	文件	文件导入成功,共导入1个资产对象
2023-04-25 15:48:10	文件	文件导入失败,第2行:不存在的资产.
2023-04-25 15:48:04	文件	文件导入失败,第2行:不存在的资产.

共 20 条 < 1 2 3 4 >

配置对象

添加资产及相关配置，如图所示：

配置对象

X

* 对象名称:

demo

▼

* 应用:

数据库审计 (192.168.1.221) x

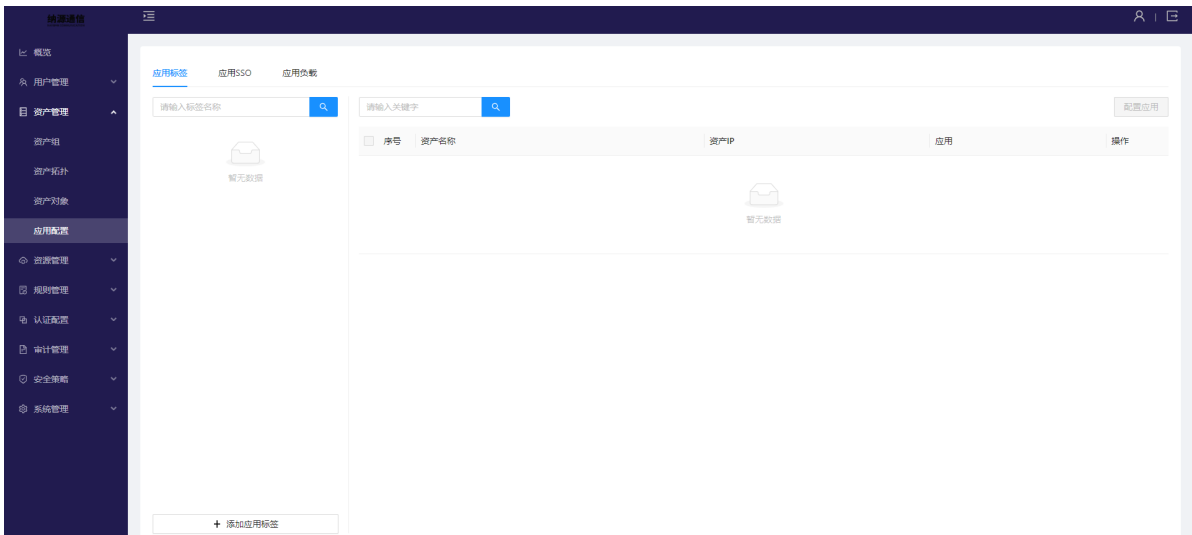
取消

确定

应用配置

应用标签

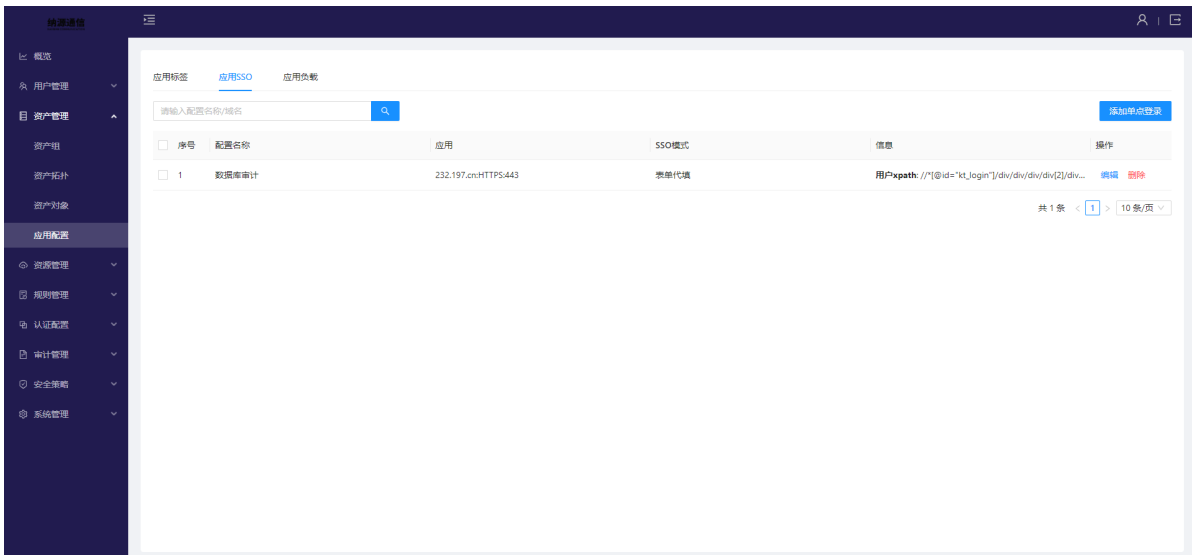
配置管理应用标签，门户中WEB应用以标签分组展示，便于应用分类查找，如图所示：



- 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：

添加单点登录配置



* 配置名称：

* 应用：

SSO模式：

表单代填



用户xpath：

密码xpath：

登录xpath：

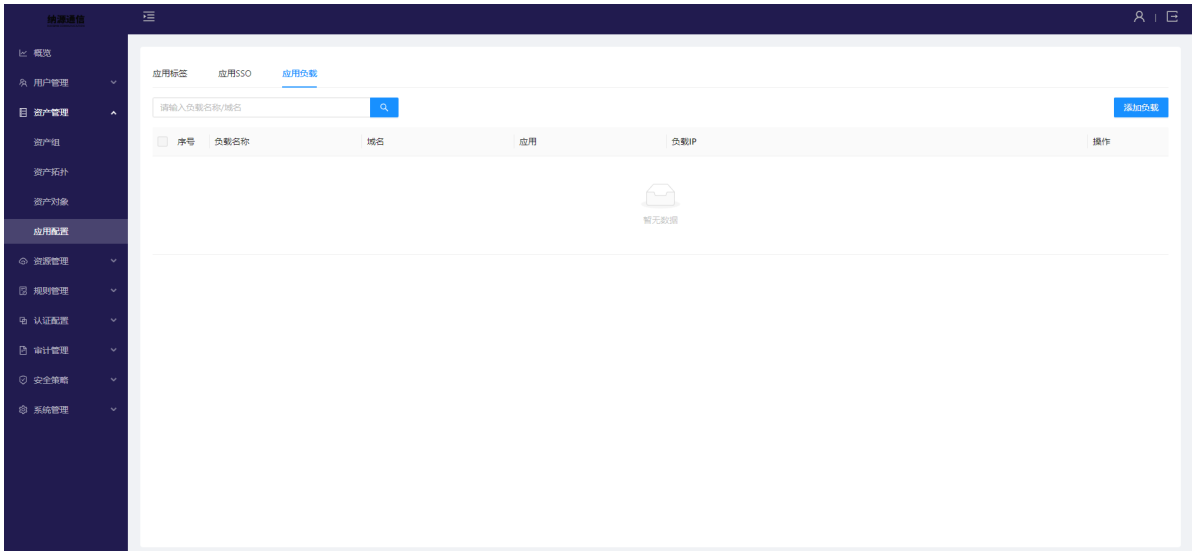
取消

确定

- 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**。

☐	序号	主机名	操作系统	终端类型	绑定用户	MAC地址	最近访问IP	操作
☐	1	M2104K10AC	Android		51502		180.160.1.1	编辑 删除
☐	2	xiaohuo426	Windows		51501		180.160.1.1	编辑 删除
☐	3	M2104K10AC	Android		51110		180.160.1.1	编辑 删除
☐	4	xiaohuo426	Windows		51110		180.160.1.1	编辑 删除
☐	5	xiaohuo426	Windows		51101		180.160.1.1	编辑 删除
☐	6	M2104K10AC	Android		51101		180.160.1.1	编辑 删除
☐	7	M2104K10AC	Android		510222		58.247.23.57	编辑 删除
☐	8	M2104K10AC	Android		510111		58.247.23.57	编辑 删除
☐	9	xiaohuo426	Windows		510111		180.160.1.1	编辑 删除
☐	10	DESKTOP-R11POCA	Windows		51001		180.160.1.1	编辑 删除

共 206 条 < 1 2 3 4 5 ... 21 > 10 条/页

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：

* 主机名:

* 操作系统:

终端类型:

隶属域:

MAC:

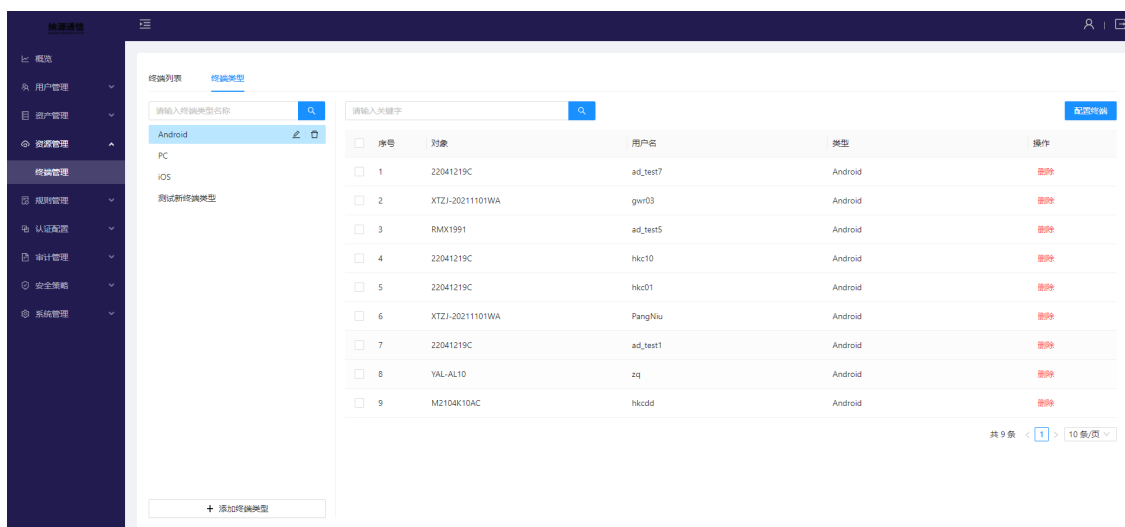
IP:

* 绑定用户:

取消

确定

- 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：

资源管理

概览

用户管理

资产管理

资源管理

规则管理

访问规则

安全规则

认证配置

审计管理

安全管理

系统管理

请输入关键字

Q

导入导出

添加规则

序号	规则名称	描述	状态	操作
1	alis		应用	编辑 停用 删除
2	测试规则		应用	编辑 停用 删除

共 2 条 < 1 > 10 条/页

添加规则

X

基本信息

用户组

用户对象

资产组

资产对象

IP

* 规则名称:

test

X

描述:

请输入

取消

确定

- 规则名称：配置访问规则名称；
- 描述：配置访问规则描述；

添加规则

X

基本信息

用户组

用户对象

资产组

资产对象

IP

Q

组织架构

demo (demo)

张三 (test)

折叠所有

- 用户组：勾选用户组，为所勾选的用户配置权限；

添加规则

X

基本信息

用户组

用户对象

资产组

资产对象

IP

用户对象:

取消

确定

- 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；

Q

√

☐

默认组

折叠所有

>

☐

数据库审计 (192.168.1.221)

>

☐

demo01 (192.168.1.234)

>

☐

demo02 (192.168.1.38)

>

☐

demo03 (192.168.1.230)

>

☐

demo04 (192.168.1.183)

☐

运维

☐

开发

- 资产组：勾选资产，为勾选的用户增加资产权限。

资产对象:

取消

确定

- 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。

授权IP:

IP

IP

IP区间

IP段

请输入

端口:分隔

⊕

取消

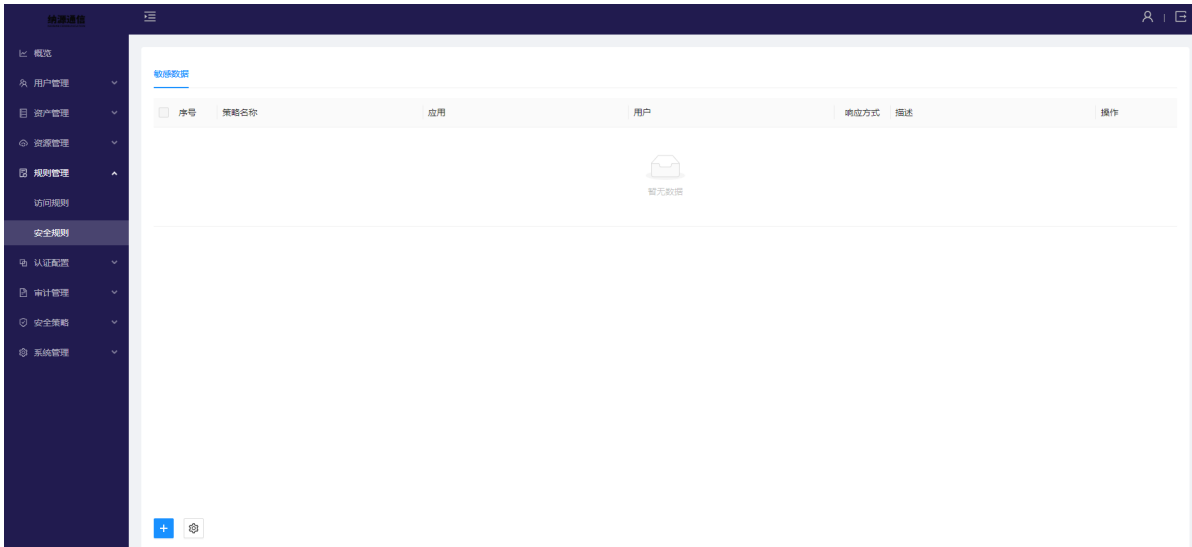
确定

- 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：

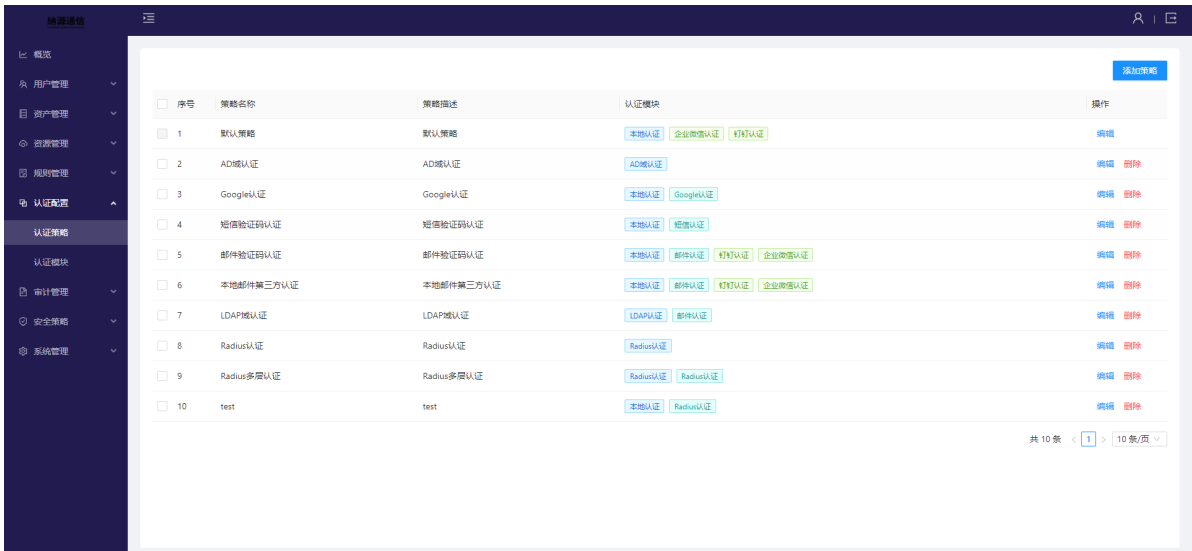


- 告警：配置正则或关键字，触发阈值及周期，并告警；
- 拒绝：配置正则或关键字，触发后拒绝该接口数据请求；
- 替换：配置正则或关键字，触发后替换数据内容；
- 文件类型配置：配置返回接口的文件类型；

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：

添加策略

X

* 策略名称:

策略描述:

基础认证:

▼

动态认证:

▼

SSO认证:

取消

确定

- 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：

序号	模块名称	类型	操作
1	本地认证	默认	编辑
2	钉钉认证	默认	编辑 清空配置
3	企业微信认证	默认	编辑 清空配置
4	LDAP认证	默认	编辑 清空配置
5	AD域认证	默认	编辑 清空配置
6	Radius认证	默认	编辑 清空配置
7	Google认证	默认	编辑
8	短信认证	默认	编辑
9	邮件认证	默认	编辑
10	OAuth2认证	默认	编辑 清空配置
11	REST-API认证	默认	编辑 清空配置

- 本地认证：配置本地密码安全策略，如图所示：

编辑认证模块

X

* 认证模块: 本地认证

* 密码最小长度: 8

密码复杂度: ☐ 启用
☐ 大写字母 ☐ 小写字母 ☐ 数字
☐ 特殊字符

密码锁定策略: ☒ 启用
3 分钟内连续输错 3 次即锁定账户,
1 分钟后解锁

密码过期时间: ☐ 启用
90 天后密码自动过期

密码重复限制: ☒ 启用

取消 确定

- 钉钉认证: 配置钉钉认证模块, 如图所示:

编辑认证模块

X

* 认证模块: 钉钉认证

* 应用程序公钥:

* 应用程序私钥:

* 回调域名地址:

取消 确定

- 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:

* 认证模块: 企业微信认证 ▼

* 企业ID:

* 凭证密钥:

* Schema:

* 登陆接入公钥:

* 回调域名地址:

取消

确定

- 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:

* 认证模块:

LDAP认证



基本信息:

* IP地址:

* 端口号:

* 根标识:

* 用户名:

* 密码:



组织单位:

取消

确定

- 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:

* 认证模块: AD域认证

基本信息:

* IP地址:

* 端口号:

* 根标识:

* 用户名:

* 密码:

组织单位:

取消

确定

- 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:

* 认证模块:

Radius认证

▼

* 地址:

* 端口号:

* 密钥:

取消

确定

- 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：

系统消息

WEB访问

请输入用户名/姓名/登录IP/访问路径

2023-04-15 15:02:00 至 2023-05-15 15:02:00 查询

时间	用户名	姓名	登录IP	登录地区	客户端	认证方式	访问目标	详情	结果	最后活跃时间
2023-05-11 17:21:55	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	https://auth.default.com	访问成功	成功	2023-05-11 17:21:55
2023-05-11 17:19:59	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	https://auth.default.com	访问成功	成功	2023-05-11 17:19:59
2023-05-11 17:12:19	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	https://auth.default.com	访问成功	成功	2023-05-11 17:12:19
2023-05-11 11:56:24	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	https://auth.default.com	访问成功	成功	2023-05-11 11:56:24
2023-05-11 11:38:04	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	https://auth.default.com	访问成功	成功	2023-05-11 11:38:04
2023-05-11 11:33:19	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	https://auth.default.com	访问成功	成功	2023-05-11 11:33:19
2023-05-11 11:00:51	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	https://auth.default.com	访问成功	成功	2023-05-11 11:00:51

共 7 条 < 1 > 10 条/页

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：

快速通告

概览

用户管理

资产管理

资源管理

规则管理

认证配置

审计管理

访问日志

告警日志

登录日志

系统日志

WEB回放

审计回放

安全策略

系统管理

请输入用户名/姓名/登录IP/访问路径/规则名/详情

2023-04-15 15:02:30 至 2023-05-15 15:02:30

查询

时间	用户名	姓名	登录IP	登录地区	客户端	认证方式	访问目标	告警类型	告警规则	输出方式	详情
2023-04-23 17:02:32	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:32	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:31	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:31	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:30	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:30	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:30	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:30	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:30	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:30	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...
2023-04-23 17:02:29	test1	test1	8.201.1.3	上海上海市	Chrome 107.0.0.0 for Windows10	本地认证	https://bt.197.cn8114	敏感数据	告警	syslog	请求接口//匹配内容系统,触发阈值1...

共 223 条 < 1 2 3 4 5 ... 23 > 10 条/页

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：

快速通告

概览

用户管理

资产管理

资源管理

规则管理

认证配置

审计管理

访问日志

告警日志

登录日志

系统日志

WEB回放

审计回放

安全策略

系统管理

请输入用户名/姓名/登录IP/登录地区/详情

2023-04-15 15:06:57 至 2023-05-15 15:06:57

查询

时间	用户名	姓名	登录IP	登录地区	客户端	认证方式	详情	结果	登出时间
2023-05-11 17:23:15	demo	demo	192.168.2.100	内网	sTrustAuth for Android	本地认证	访问成功	成功	
2023-05-11 17:21:54	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	访问成功	成功	2023-05-11 17...
2023-05-11 17:19:58	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	访问成功	成功	2023-05-11 17...
2023-05-11 17:12:18	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	访问成功	成功	2023-05-11 17...
2023-05-11 11:56:23	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	访问成功	成功	2023-05-11 14...
2023-05-11 11:55:45	demo	demo	192.168.2.100	内网	sTrustAuth for Android	本地认证	访问成功	成功	2023-05-11 12...
2023-05-11 11:55:40	demo	demo	192.168.2.100	内网	sTrustAuth for Android	本地认证	用户名或密码错...	失败	
2023-05-11 11:38:03	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	访问成功	成功	2023-05-11 11...
2023-05-11 11:33:18	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	访问成功	成功	2023-05-11 11...
2023-05-11 11:00:49	demo	demo	192.168.2.100	内网	sTrustAuth for Windows	本地认证	访问成功	成功	2023-05-11 11...

共 10 条 < 1 > 10 条/页

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：

溯源通鉴

23

2023-05-15 00:00:00 至 2023-05-15 23:59:59

🔍 查询

概览

用户管理

资产管理

资源管理

规则管理

认证配置

审计管理

访问日志

告警日志

登录日志

系统日志

WEB回放

审计回放

安全策略

系统管理

请输入用户名/登录IP/详情

时间	用户名	登录IP	客户端	功能模块	行为	详情	结果
2023-05-15 14:58:19	admin	8.201.1.1	Chrome 113.0.0.0 for Windows10	认证配置	修改认证策略	添加认证规则test	成功
2023-05-15 14:44:30	admin	8.201.1.1	Chrome 113.0.0.0 for Windows10	应用规则	修改规则	修改规则demo	成功
2023-05-15 14:43:38	admin	8.201.1.1	Chrome 113.0.0.0 for Windows10	应用规则	修改规则	修改规则aalls	成功
2023-05-15 14:43:23	admin	8.201.1.1	Chrome 113.0.0.0 for Windows10	应用规则	修改规则	修改规则aalls	成功
2023-05-15 14:41:19	demo	8.201.1.1	Chrome 113.0.0.0 for Windows10	登录	登录	管理员demo登录	成功
2023-05-15 14:17:14		192.168.1.107	Chrome 113.0.0.0 for Windows10	客户端下载	下载软件	下载软件sTrustAuth_android.apk	成功
2023-05-15 14:17:14			Chrome 113.0.0.0 for Windows10	客户端下载	下载软件	下载软件sTrustAuth_android.apk	成功
2023-05-15 14:17:14		192.168.1.107	Chrome 113.0.0.0 for Windows10	客户端下载	下载软件	下载软件sTrustAuth_android.apk	成功
2023-05-15 14:17:14		192.168.1.107	Chrome 113.0.0.0 for Windows10	客户端下载	下载软件	下载软件sTrustAuth_android.apk	成功
2023-05-15 14:17:14		192.168.1.107	Chrome 113.0.0.0 for Windows10	客户端下载	下载软件	下载软件sTrustAuth_android.apk	成功

共 43 条 < 1 2 3 4 5 > 10 条/页

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。

溯源通鉴

☰

用户管理

资产管理

资源管理

规则管理

认证配置

审计管理

访问日志

告警日志

登录日志

系统日志

WEB回放

审计回放

安全管理

系统管理

概述

用户管理

资产管理

资源管理

规则管理

认证配置

审计管理

访问日志

告警日志

登录日志

系统日志

WEB回放

审计回放

安全管理

系统管理

请输入用户名/姓名/访问目标

2023-04-15 15:12:49 至 2023-05-15 15:12:49

🔍 查询

时间	用户名	姓名	访问目标	操作
2023-05-11 15:35:15	demo	demo	wg.197.cn	查看回放
2023-05-11 15:24:17	demo	demo	wg.197.cn	查看回放
2023-05-11 15:19:36	demo	demo	wg.197.cn	查看回放
2023-05-10 20:56:44	demo	demo	wg.197.cn	查看回放
2023-05-10 20:23:40	demo	demo	bt.197.cn:7700	查看回放
2023-05-10 20:18:14	demo	demo	bt.197.cn:7700	查看回放
2023-05-10 20:11:43	demo	demo	wg.197.cn	查看回放
2023-05-10 20:22:49	demo	demo	wg.197.cn	查看回放
2023-05-10 19:29:35	demo	demo	bt.197.cn:7700	查看回放
2023-05-10 19:22:46	demo	demo	bt.197.cn:7700	查看回放

共 162 条

1

2

3

4

5

...

17

>

10 条/页

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：

时间	用户名	姓名	访问目标	录像状态	操作
2023-04-21 20:11:36	42103	42103	rdp:47.98.238.31:3389	正常	生成录像
2023-04-21 19:43:37	42103	42103	rdp:192.168.1.115:3389	正常	生成录像
2023-04-21 19:41:39	42103	42103	rdp:192.168.1.115:3389	正常	生成录像
2023-04-21 19:41:38	42103	42103	ssh:192.168.1.205:22	正常	生成录像
2023-04-21 15:49:59	gwr	群姐	ssh:192.168.1.205:22	转码完成	下载
2023-04-21 15:49:49	gwr	群姐	ssh:192.168.1.205:22	正常	生成录像
2023-04-21 15:49:42	gwr	群姐	ssh:192.168.1.205:22	正常	生成录像
2023-04-21 13:52:41	42101	42101	rdp:192.168.1.115:3389	正常	生成录像
2023-04-21 13:51:58	42101	42101	ssh:192.168.1.205:22	正常	生成录像
2023-04-21 13:51:34	42101	42101	ssh:192.168.1.205:22	正常	生成录像

安全策略

WEB安全策略

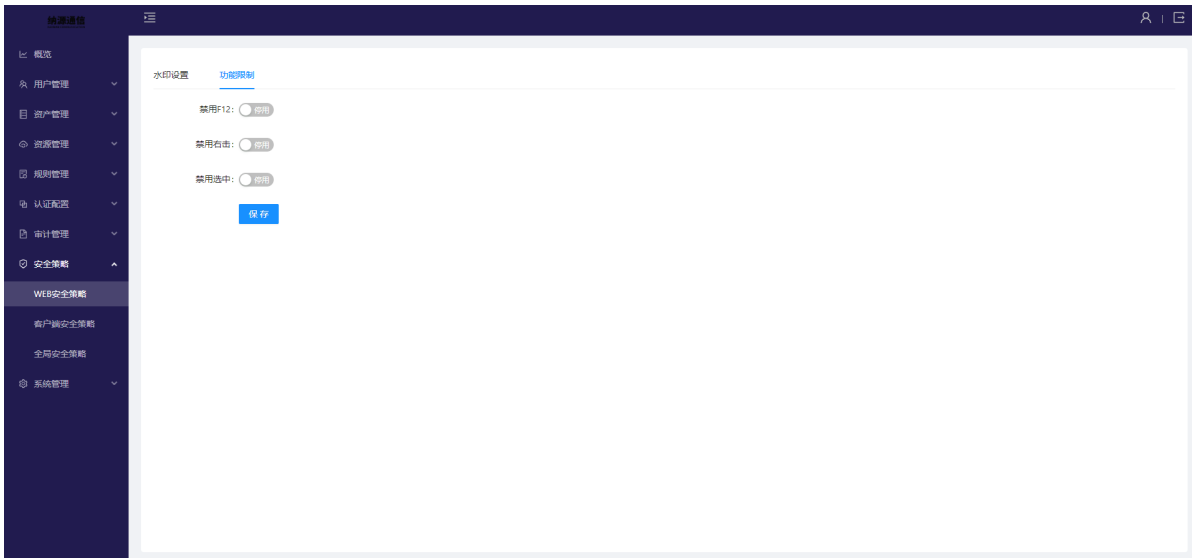
水印设置

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

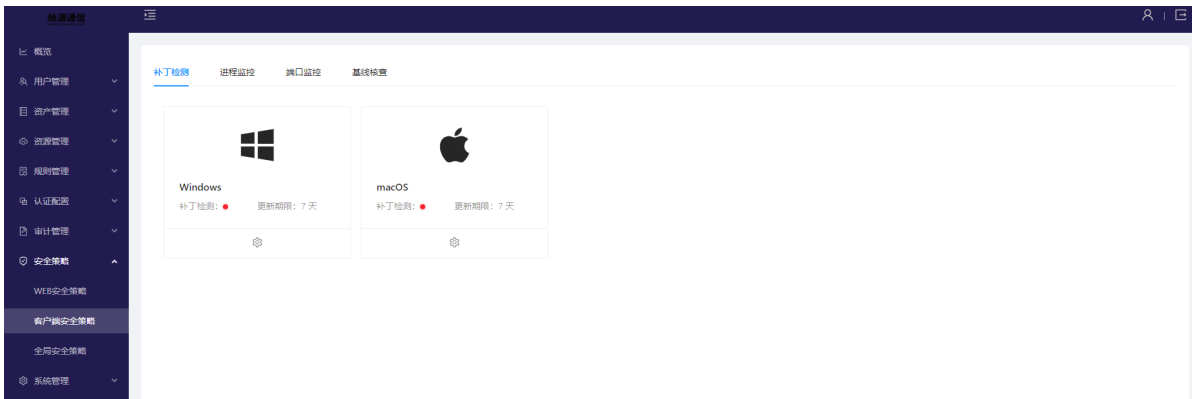
配置WEB应用访问功能限制，如图所示：



客户端安全策略

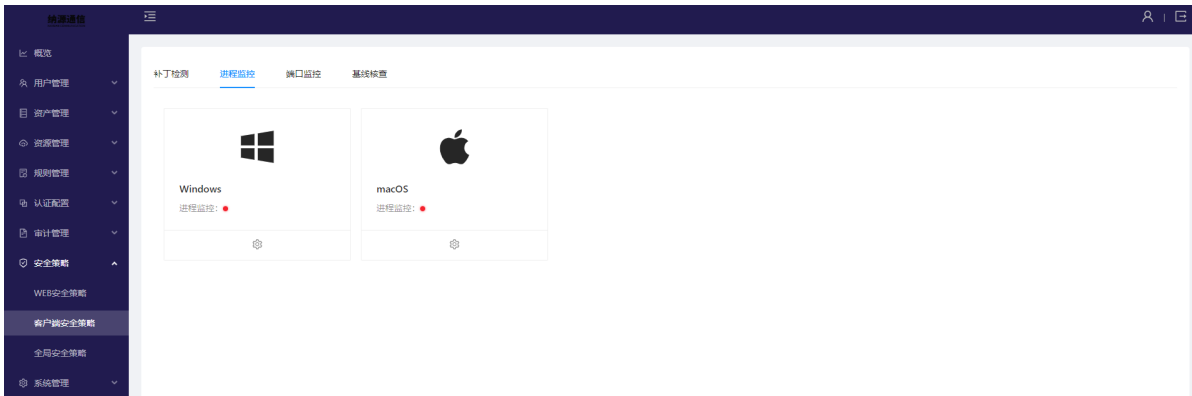
补丁检测

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：



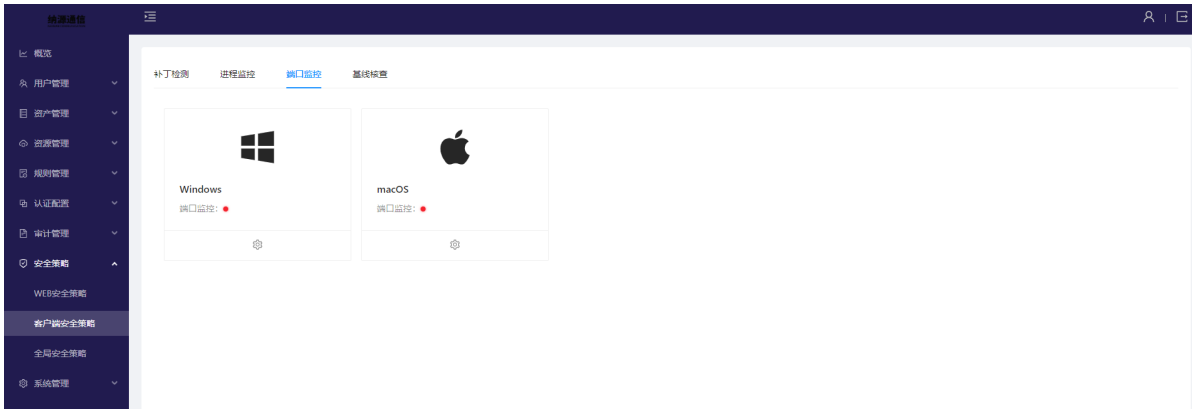
进程检测

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：



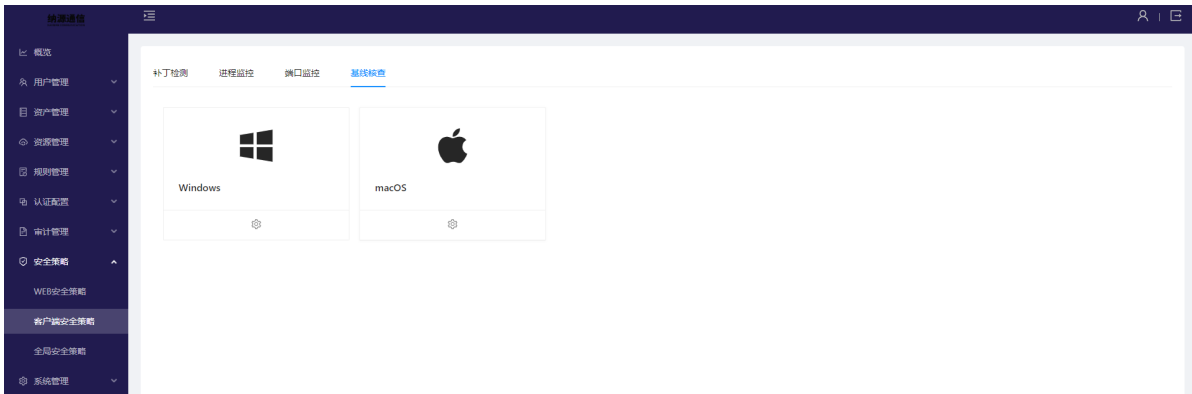
端口检测

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：



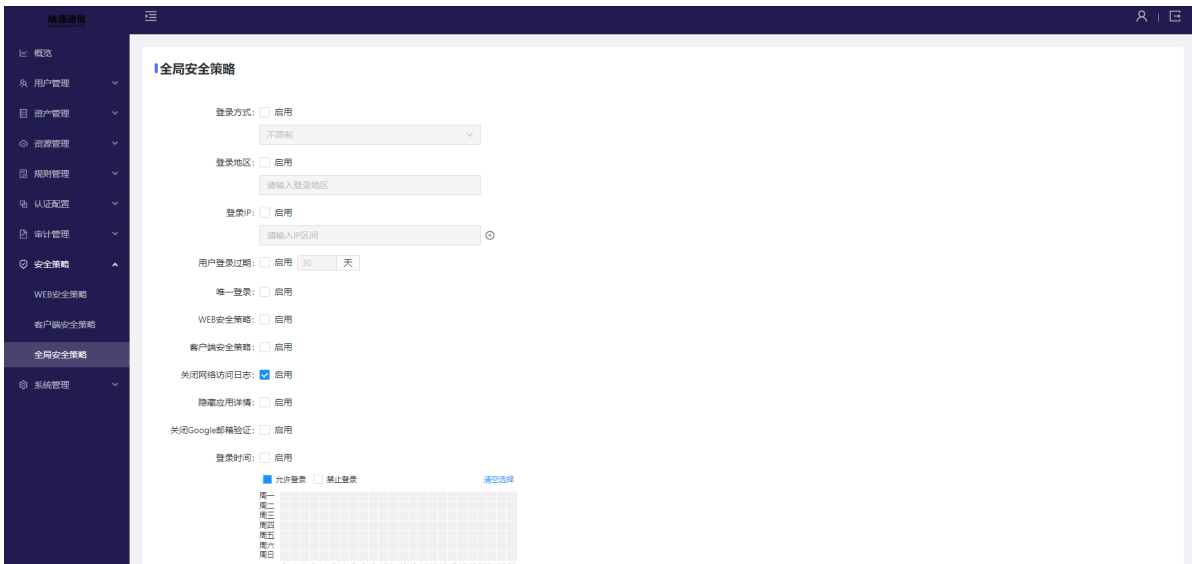
基线核查

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。



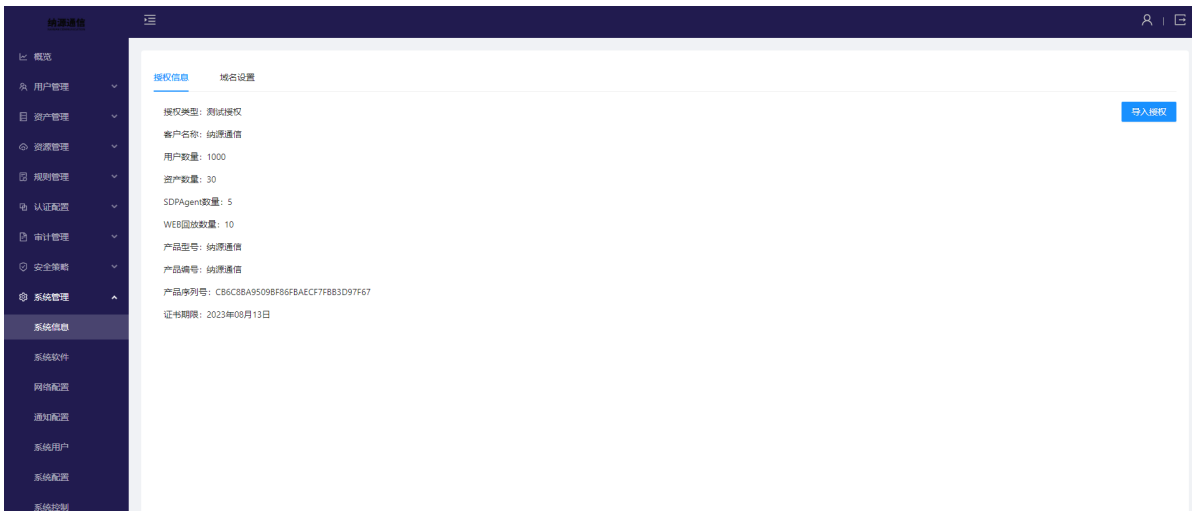
- **登录方式**：配置用户登录方式，默认为不限制；
 - 只允许WEB登录：只允许用户登录WEB门户，不允许通过客户端登录；
 - 强制客户端登录：强制用户只能通过客户端登录，不允许直接登录门户；
- **登录地区**：限制用户登录地区；
- **登录IP**：限制用户登录IP；
- **用户登录过期**：启用后超过设置时长未登录停用用户；
- **唯一登录**：设置唯一登录后，同一账号只能在一台设备上登录；
- **WEB安全策略**：配置用户是否启用WEB安全策略，策略遵循安全策略中的WEB安全策略配置；
- **客户端安全策略**：配置用户是否启用客户端安全策略，策略遵循安全策略中的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

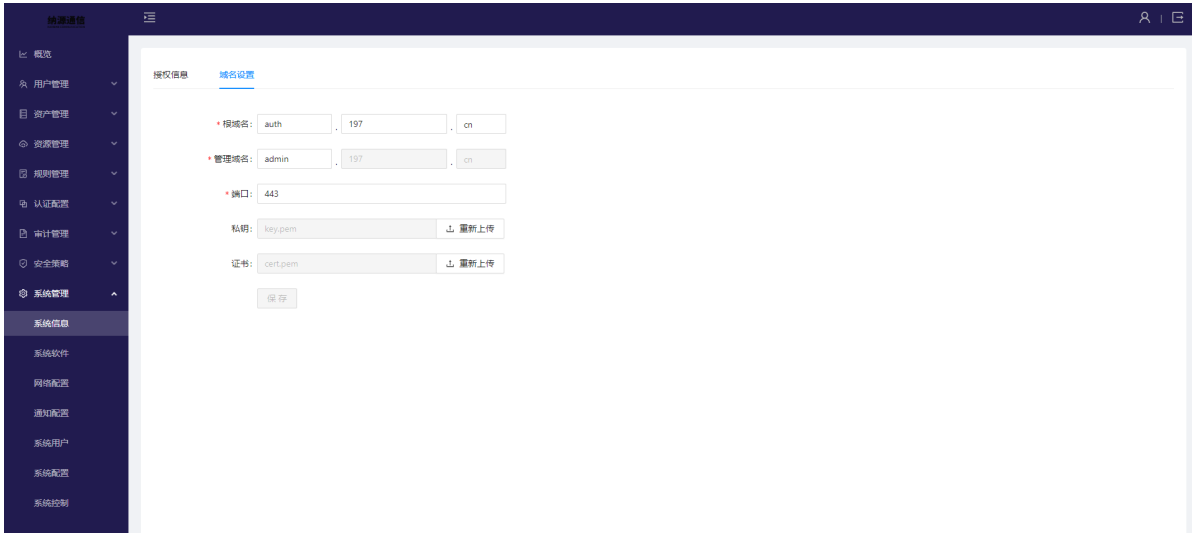
授权信息

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

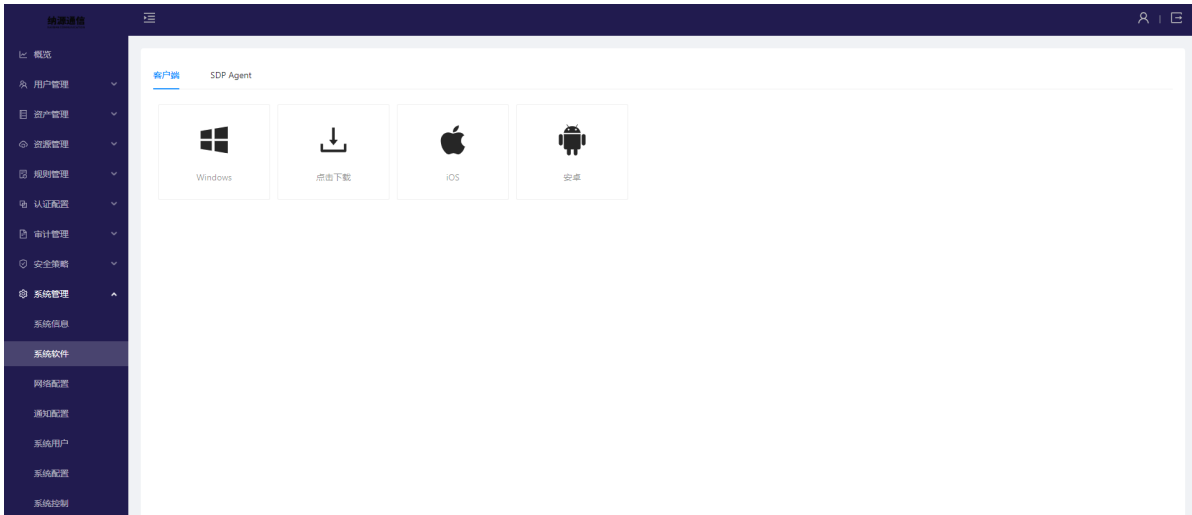
配置系统主域名及门户监听端口及SSL证书，如图所示：



系统软件

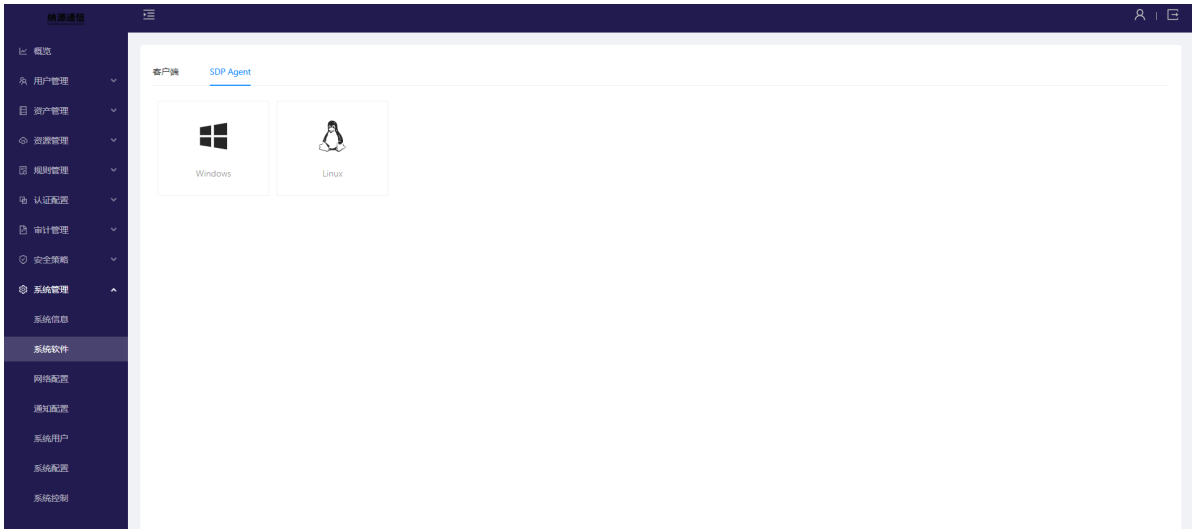
客户端

下载零信任访问客户端，如图所示：



SDP Agent

下载SDP Agent，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：

IPv4配置							
序号	网卡名称	IP地址	子网掩码	默认网关	类型	状态	操作
1	ens192	192.168.1.75	255.255.255.0	192.168.1.254	管理口		编辑

IPv6配置							
序号	网卡名称	IPv6地址	前缀	默认网关	类型	状态	操作
1	ens192				管理口		编辑

路由配置

配置系统静态路由，如图所示：

路由配置					
序号	目标网段	子网掩码	路由地址	网口名称	操作
1	192.168.7.0	255.255.255.0	192.168.1.1	eno1	删除
2	192.168.6.0	255.255.255.0	192.168.1.1	eno1	删除
+ 添加路由配置					

DNS配置

配置系统DNS，如图所示：

DNS配置			
序号	DNS类型	DNS地址	操作
1	私有DNS	8.8.8.8	编辑 删除
2	私有DNS	114.114.114.114	编辑 删除
+ 添加DNS配置			

网络调试

测试网络通信或进行数据抓包，如图所示：

IPv4配置

IPv6配置

路由配置

DNS配置

网络调试

测试方式：

PING

* 目标地址：

qq.com

* 测试时长：

3

秒

检测结果：

```
PING qq.com (61.129.7.47) 56(84) bytes of data.  
64 bytes from 61.129.7.47 (61.129.7.47): icmp_seq=1 ttl=55 time=5.99 ms  
64 bytes from 61.129.7.47 (61.129.7.47): icmp_seq=2 ttl=55 time=5.31 ms  
64 bytes from 61.129.7.47 (61.129.7.47): icmp_seq=3 ttl=55 time=5.97 ms
```

开始检测

通知配置

短信

配置系统短信输出接口，如图所示：

短信

邮件

SYSLOG

接口类型：

阿里短信服务

* 签名：

* 模板：

SM: 56346

* 公钥：

LTAI JbGpSEQ

* 私钥：

Wwjg eugdP3i83SnAy

发送测试短信

保存

清空配置

邮件

配置系统邮件输出接口，如图所示：

短信

邮件

SYSLOG

邮件标题：

应用身份认证

* 邮箱账号：

319144@qq.com

* 邮箱密码：

* 发件服务器：

smtp.qq.com

* 加密方式：

SSL/TLS

* 端口：

587

* 发件人邮箱：

319144@qq.com

发送测试邮件

保存

清空配置

SYSLOG

配置系统SYSLOG输出接口，如图所示：

短信

邮件

SYSLOG

* 服务器地址：

192.168.1.1

* 服务器端口：

514

(1-65535)

* 编码格式：

UTF-8

* 协议类型：

UDP

发送测试信息

保存

清空配置

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。

系统管理

用户管理

资产管理

资源管理

规则管理

认证配置

审计管理

安全策略

系统管理

系统信息

系统软件

网络配置

通知配置

系统用户

系统配置

系统控制

请输入用户名/姓名

添加管理员

序号	用户名	姓名	邮箱	手机	系统角色	最后登录时间	操作
1	admin	admin	87920151@qq.com	17612917750		2023-05-15 16:04:34	
2	demo	demo	xiaohuo0426@163.com	18583023273	审计管理员	2023-05-15 14:42:59	删除
3	test918	test918			配置管理员		删除
4	test924	test924	87920151@qq.com	13512345678	系统管理员	2022-09-21 14:57:06	删除
5	test_radius	test_radius	xiaohuo0426@163.com	18583023273	配置管理员	2023-04-26 12:58:11	删除
6	gwr	群组	87920151@qq.com	17612917750	审计管理员	2023-05-10 11:00:32	删除

共 6 条 < 1 > 10 条/页

可为不同用户添加不同管理员角色，如下图所示：

添加管理员

X

* 管理员角色:

配置管理员

审计管理员

系统管理员

* 用户:

确定

系统配置

时间设置

配置系统时间及NTP服务器，如图所示：

时间设置

超时设置

系统服务

配置备份

系统升级

系统API

连接信息

集群配置

当前时间:

2023-05-15

16:32:59

自动同步:

开启

NTP服务器:

ntp.aliyun.com

同步频率:

一天

时间同步

保存

超时设置

配置系统会话及管理页面超时时间，如图所示：

时间设置

超时设置

系统服务

配置备份

系统升级

系统API

连接信息

集群配置

* 应用会话：

120

秒

* 管理页面：

86400

秒

保存

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：

序号	系统服务	服务端口	访问权限	端口权限	服务状态	操作
1	认证服务	9477	不可配置	开放		编辑
2	WEB管理	3001	组织架构2	开放		编辑
3	网络代理	6668	不可配置	关闭		编辑
4	系统SSH	22	demo	开放		编辑
5	WEB门户	7700.80.8088.8089.8888.443.180.5601.8087.8092.8081.8095.8094.520.8114.8112.8115.8116.28470.801.4436.8117.5.7.22178.81.82	不可配置	开放		编辑

- 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：

序号	日期	文件名	文件大小	操作
1	2023-05-15 00:00:00	1684080000110_sTrust-V1.0.14-2023-05-08	984K	下载 恢复 删除
2	2023-05-14 00:00:00	1683993600108_sTrust-V1.0.14-2023-05-08	984K	下载 恢复 删除
3	2023-05-13 00:00:00	1683907200095_sTrust-V1.0.14-2023-05-08	984K	下载 恢复 删除
4	2023-05-12 00:00:00	1683820800047_sTrust-V1.0.14-2023-05-08	984K	下载 恢复 删除
5	2023-05-06 18:18:03	1683368283437_sTrust-V1.0.13-2023-05-05	924K	下载 恢复 删除
6	2023-04-26 17:10:27	1682500227590_sTrust-V1.0.12-2023-04-24	768K	下载 恢复 删除
7	2023-04-26 17:10:27	1682500227016_sTrust-V1.0.12-2023-04-24	768K	下载 恢复 删除
8	2023-04-26 17:10:26	1682500226489_sTrust-V1.0.12-2023-04-24	768K	下载 恢复 删除
9	2023-04-26 17:10:24	1682500224077_sTrust-V1.0.12-2023-04-24	768K	下载 恢复 删除
10	2023-04-26 17:10:21	1682500221302_sTrust-V1.0.12-2023-04-24	768K	下载 恢复 删除

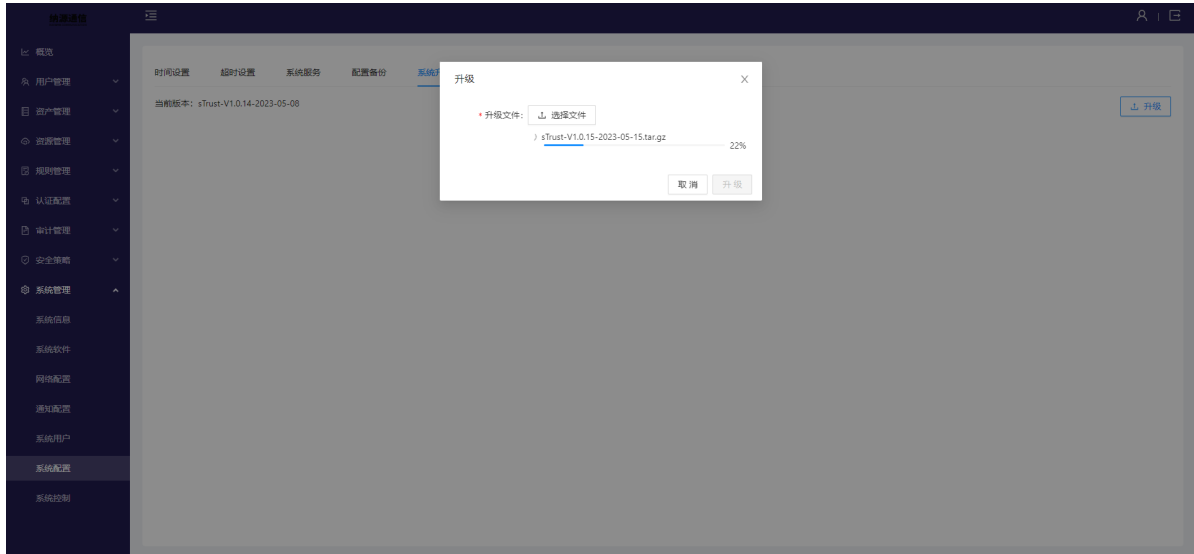
共 262 条 < 1 2 3 4 5 ... 27 > 10 条/页

- 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；

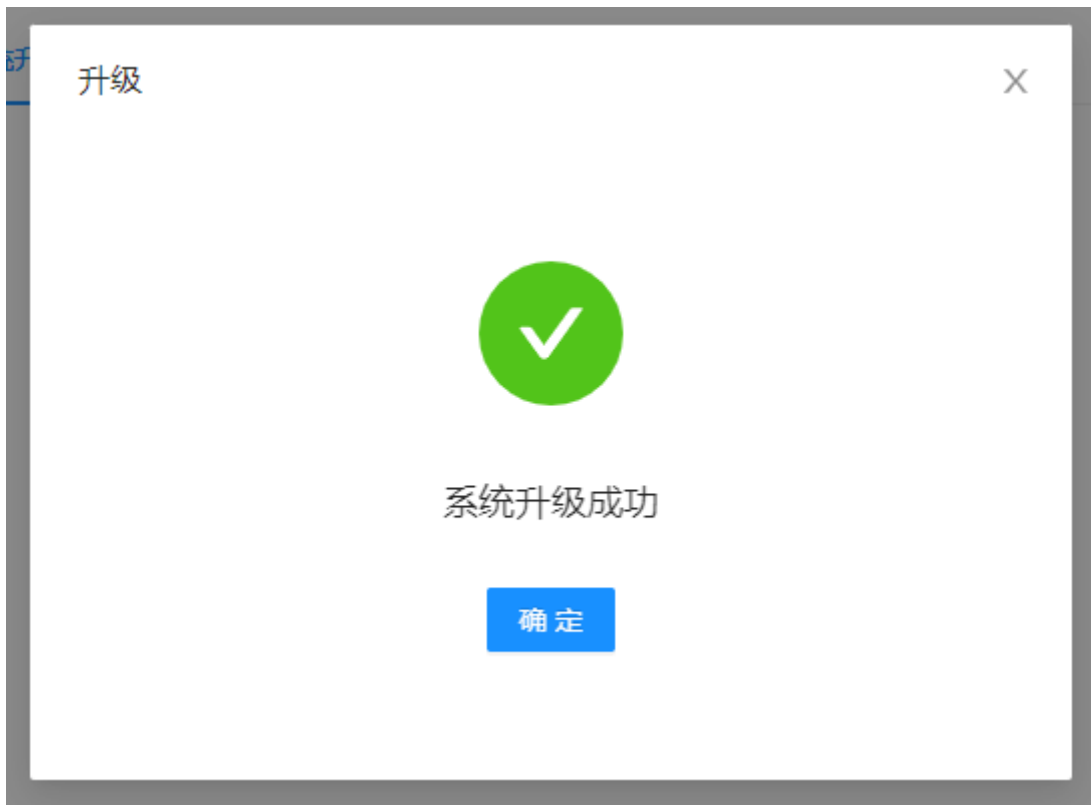
- 应用：仅恢复应用相关配置；
- 配置：自动备份系统配置。

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



升级完成如下图所示：



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：

时间设置	超时设置	系统服务	配置备份	系统升级	系统API	连接信息	集群配置
------	------	------	------	------	-------	------	------

序号	IP	Token	操作
1	192.168.1.110	1a67aa4dc9c1317b16b763	编辑 删除
2	192.168.3.72	c7785c0a9_9a755304d95	编辑 删除
3	192.168.1.107	6d270f978_94ee07dd67	编辑 删除

共 3 条 < 1 > 10 条/页

连接信息

设置服务器连接地址及端口号，如下图所示：

时间设置	超时设置	系统服务	配置备份	系统升级	系统API	连接信息	集群配置
序号	地址				端口	操作	
1	116.233.205.248				9477	编辑	

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：

时间设置

超时设置

系统服务

配置备份

系统升级

系统API

连接信息

集群配置

HA配置:

☐ 开启

VIP:

VRID:

MasterIP:

BackupIP:

Master心跳IP:

Backup心跳IP:

数据库状态:

未同步

磁盘状态:

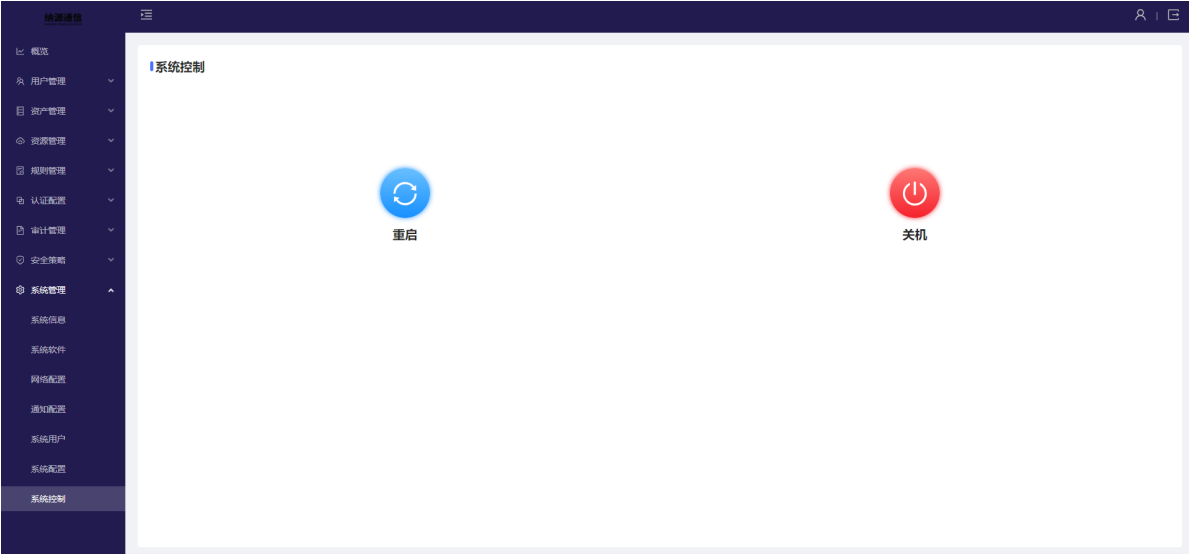
未同步

保存

清空配置

系统控制

控制系统重启或者关机，如图所示：



安全组

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