安恒网站卫士网页防篡改系统

产品手册



杭州安恒信息技术股份有限公司

二〇二〇年四月 26 日

V1.0 2020-04-26 汪志杰

目录

[1. 产品简介 1](#_Toc40860629)

[2. 登录及添加许可 1](#_Toc40860630)

[3. 密码策略 2](#_Toc40860631)

[4. 首页 3](#_Toc40860632)

[4.1 信息展示 3](#_Toc40860633)

[4.2 用户信息 4](#_Toc40860634)

[5. 资产管理 4](#_Toc40860635)

[5.1 资产编辑 5](#_Toc40860636)

[5.2 资产策略 5](#_Toc40860637)

[5.3 资产详情 6](#_Toc40860638)

[1. 终端详情 6](#_Toc40860639)

[2. 监听端口 7](#_Toc40860640)

[3. 运行程序 7](#_Toc40860641)

[4. 账号信息 8](#_Toc40860642)

[5. 软件信息 8](#_Toc40860643)

[6. 性能监控 8](#_Toc40860644)

[6. 分组标签 9](#_Toc40860645)

[7. 网站防护 9](#_Toc40860646)

[7.1 网页防篡改 9](#_Toc40860647)

[7.1.1 新增规则 9](#_Toc40860648)

[7.1.2 新增子规则 10](#_Toc40860649)

[7.2 网站漏洞防护 11](#_Toc40860650)

[7.3 CC攻击防护 12](#_Toc40860651)

[7.4 网站访问控制 13](#_Toc40860652)

[7.5 网马查杀 14](#_Toc40860653)

[7.6 工具箱 15](#_Toc40860654)

[8. 容器防护 15](#_Toc40860655)

[8.1容器概况 15](#_Toc40860656)

[8.2容器篡改防护 16](#_Toc40860657)

[9. 响应处理 17](#_Toc40860658)

[10. 发布端 (WPT-EE-PRO) 17](#_Toc40860659)

[10.1 发布端管理 17](#_Toc40860660)

[10.2 发布配置 18](#_Toc40860661)

[11. 日志检索 20](#_Toc40860662)

[11.1 日志种类 20](#_Toc40860663)

[11.2 报表 21](#_Toc40860664)

[12. 系统管理 22](#_Toc40860665)

[12.1 个人中心 22](#_Toc40860666)

[12.2 许可证设置 22](#_Toc40860667)

[12.3 离线升级管理 22](#_Toc40860668)

[12.4 添加资产 23](#_Toc40860669)

[12.5 告警配置 23](#_Toc40860670)

[12.6 邮件告警 23](#_Toc40860671)

[短信告警 25](#_Toc40860672)

[SNMPtrap 26](#_Toc40860673)

# 产品简介

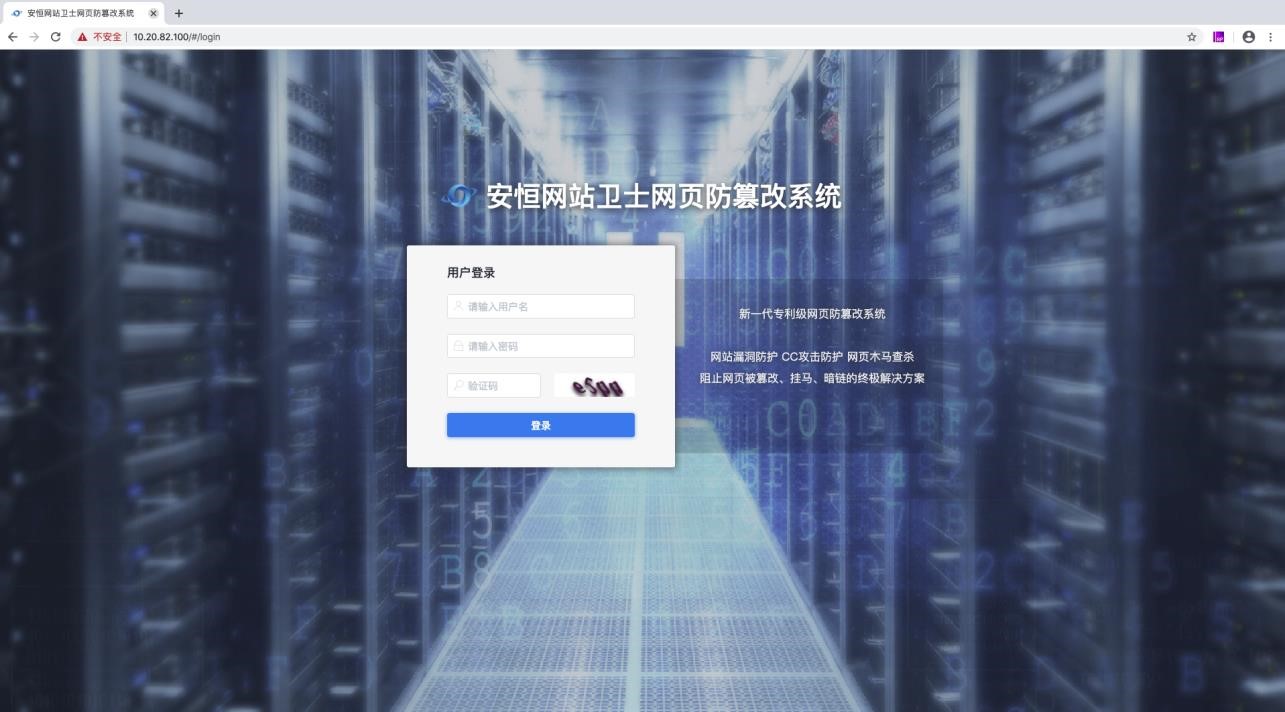
当网站网页被非法篡改后,无论是政府还是企业的网站,其造成的后果都是无法估量的,市场上急需一种应对网页篡改攻击的防网页篡改类的产品,网页防篡改系统应运而生。

安恒网站卫士网页防篡改系统是依托专业的安全团队，凭借雄厚的研发实力，结合多年的技术积累和沉淀，研发出来国内技术最先进、功能最全面、应用最广泛、实施最简单的一款专注于网站内容安全的网页防篡改系统，核心包括 Web 防攻击和文件防篡改功能，产品易安装，占用系统资源低于 3%，支持各类的 Web 服务器，操作系统，数据库，各类网页格式。

网页防篡改系统广泛适用于“政府、金融、运营商、公安、能源、税务、工商、社保、交通、教育” 等门户网站及以互联网为基本的电子商务门户网站。部署网页防篡改系统，可以为网站提供不间断的监控与保护，有效的保障网站的完整性和真实性。

# 登录及添加许可

在管理平台安装完成之后，可通过浏览器【非 Google Chrome 49+、Firefox 35+会导致异常】访问页面查看其是否安装成功。

 步骤 **1** 在浏览器中输入 https://IP。若浏览器版本符合上述要求，则可输入账号密码登录。

步骤 **2** 输入初始用户名密码 admin/Admin123 登录。许可管理页面，根据机器码等信息申请许可【测试用户通过 OA 申请，正式用户通过填写[许可申请表发](https://61.164.47.206:65526/downloads/WPTxksq.xlsx)客服邮箱申请】。得到许可后在此处点击添加许可，导入许可，末尾勿加空格或换行。

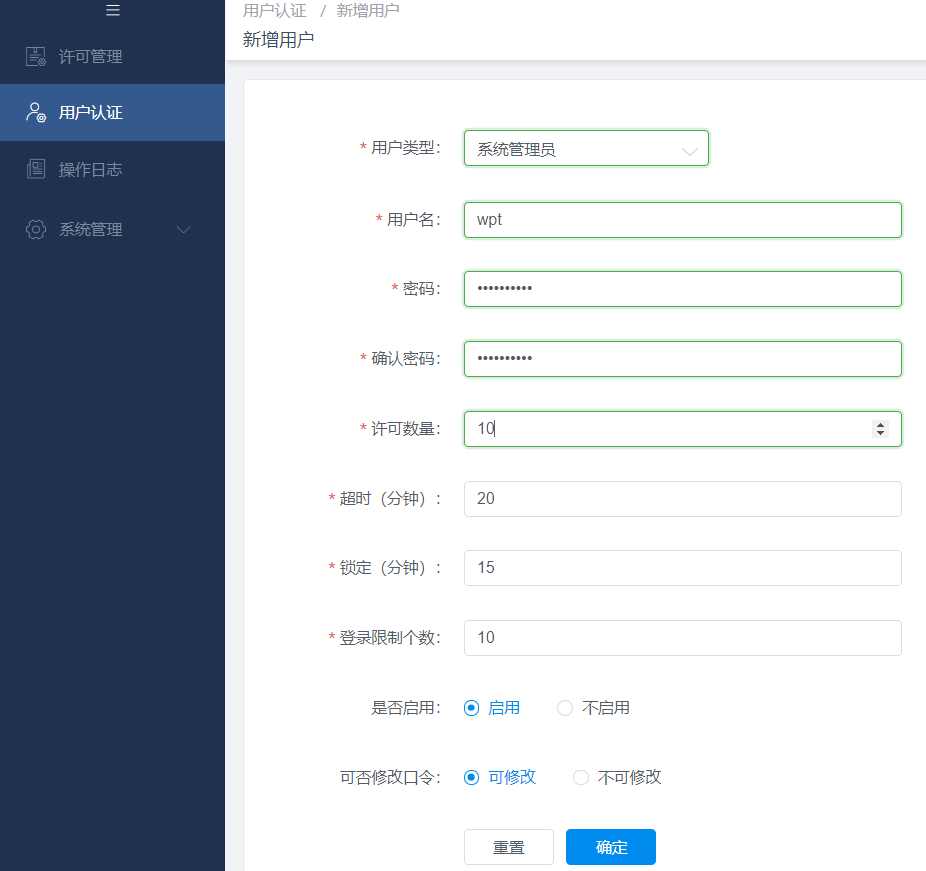


步骤 **3** 点击用户认证，修改初始密码。点击新增，可以选择新增的用户类型，系统默认有四种用户类型，系统管理员、网站管理员、审计管理员、监控管理员。

当用户类型选择系统管理员时需要填写许可数量信息，最大可分配数量不超过 admin 剩余拥有的许可数。

当用户类型选择除系统管理员的其他角色时，需要选择该角色依附的系统管理员。

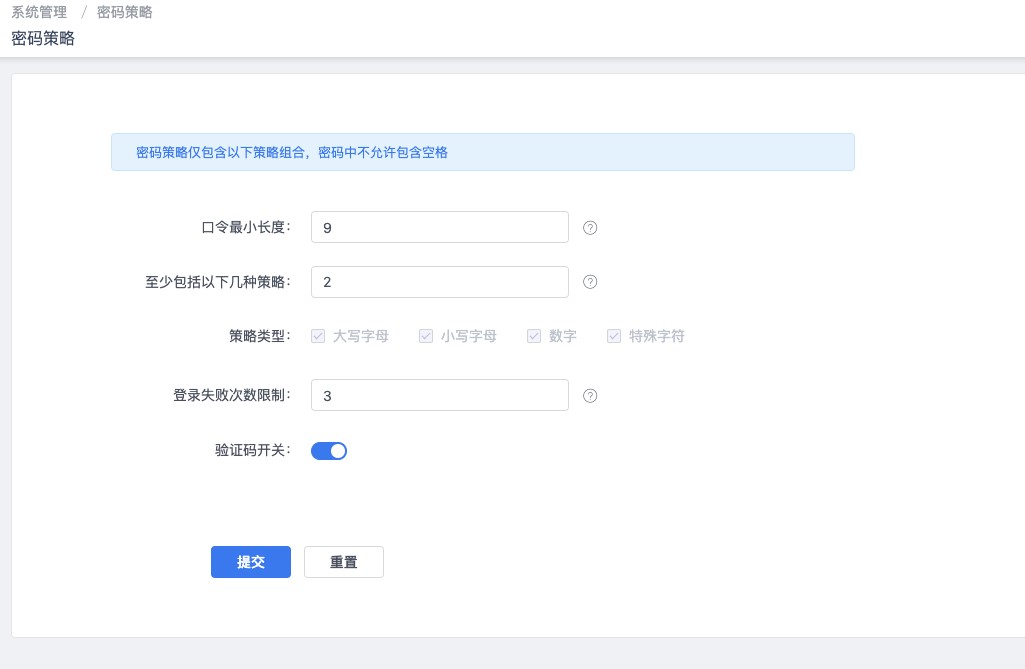
Admin角色可以对其创建的用户角色进行管理，角色之间互斥。



步骤 **4** 右上角选择注销，使用新增的系统管理原用户登录，即可开始下载安装监控端。

# 密码策略

系统管理-密码策略可以设置“口令最小长度”、“口令包含策略类型”、“登录失败次数限制”、验证码开关



# 首页

## 信息展示

使用租户用户名和密码登录，在首页中可查看资产状态、风险资产 TOP5 排行、事件类型占比、管控中心性能、攻击来源区域 TOP5、攻击来源 IP TOP5 等。



## 用户信息

点击右上角“账户名”，在关于中可以查看系统版本、授权等信息；点击“修改密码”可以进行修改密码操作。

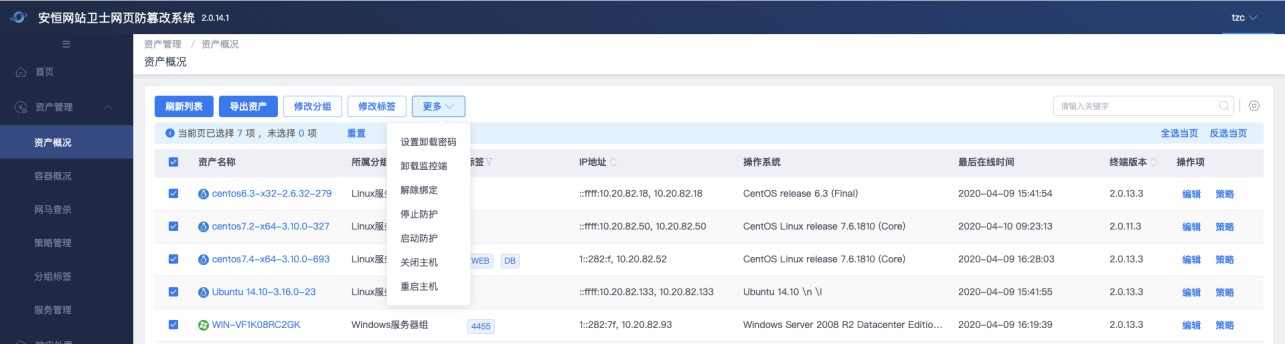


# 资产管理

在资产概况中可以查看所有绑定该中心的服务器信息 。包括名称、分组、标签、IP、操作系统、终端版本等。

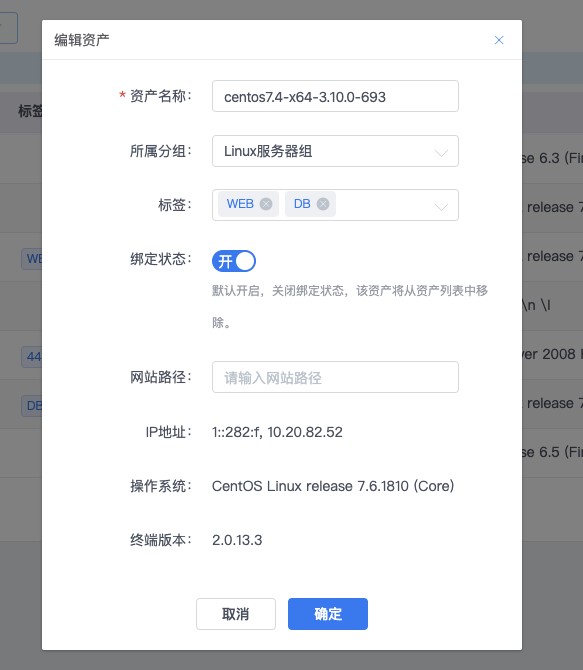


* 点击“导出资产”可将所选资产的概况信息导出。
* 点击“修改分组/标签”可修改所选资产的分组/标签，每个资产必须且只能在一个分组内，可以有多个标签。
* 点击“更多-设置卸载密码/卸载监控端/解除绑定”可对端执行相应操作。
* 点击“更多-停止防护”可关闭所选资产当前所有防护，点击“更多-启动防护”可恢复所选资产关闭防护前的状态。
* 点击关闭/重启主机可以对主机进行批量重启或关闭



## 资产编辑

点击操作项下的“编辑”可编辑资产相关信息，其中绑定状态调整为关，将解绑定该资产，被解绑的资产会从资产列表中删除



## 资产策略

可以按照模板名称的维度和按照资产的维度去查看当前已创建策略模板。

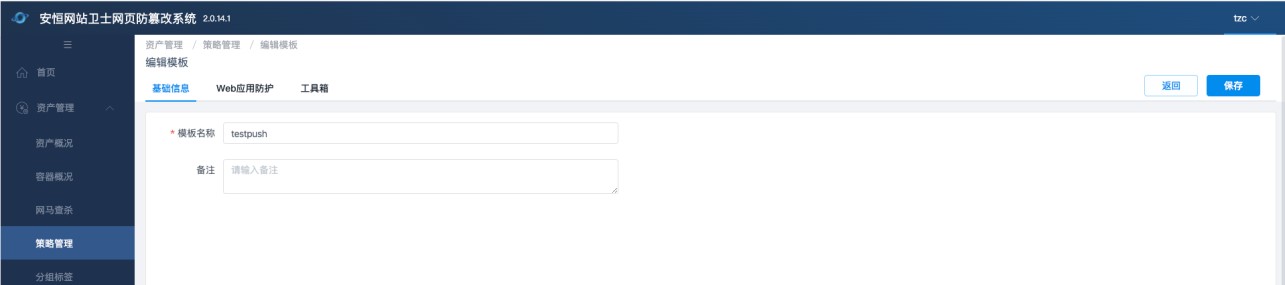
**按模板**

点击“编辑”可查看且配置该策略模板基础信息、Web 应用防护以及工具箱 ，编辑后，点击保存，则策略在所有绑定了该模板的资产中生效。

**按资产**

点击“编辑”则直接查看该资产绑定的策略模板，对策略模板修改后，点击保存，则策略在所有绑定了该模板的资产中生效。

**无论是按资产还是按模板，配置策略的时候都是对模板做修改，保存的时候对所有绑定了该模板的资产都生效，如果想要实现对单独一台资产配置策略，则需要单独为该资产创建一个单独的策略模板。**

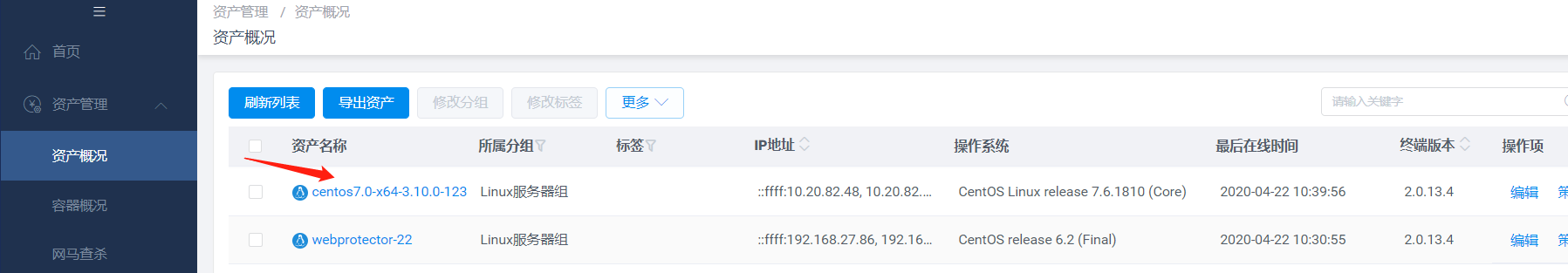


Web应用防护：可根据实际现场需要配置网页防篡改/发布配置/网站漏洞/cc攻击/网站访问控制/网马查杀等功能项，下章节详细介绍



## 资产详情

资产管理—资产概括—资产详情；点击资产名称进入资产详情界面



### 终端详情

在终端详情界面可以对服务器进行重启，查看服务器ip，MAC地址，系统环境信息，网马库更新时间，终端版本等信息



### 监听端口

在监听端口中可以看到系统占用的端口号，网络协议，对应进程，端口绑定ip



### 运行程序

在运行进程中可以看到系统上运行的进程，进程名称，内存占用，cpu使用率，启动参数等信息

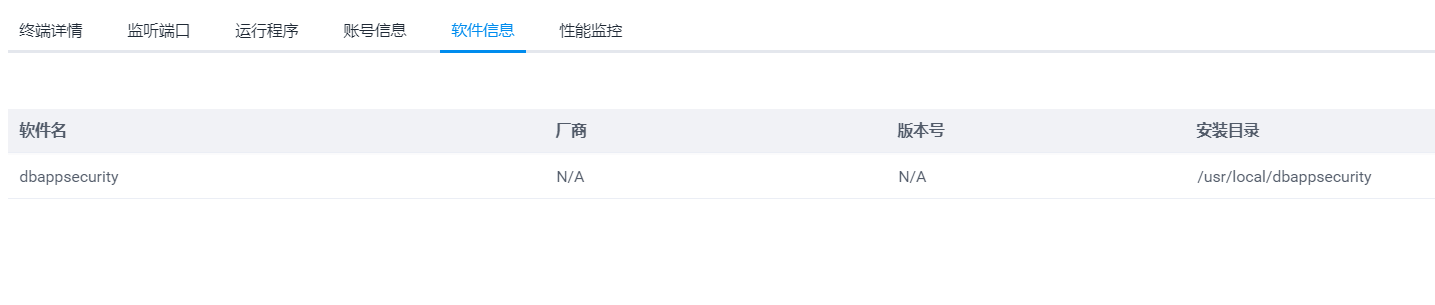


### 账号信息

在账号信息中可以查看到当前系统的账号包括隐藏账号的相关信息

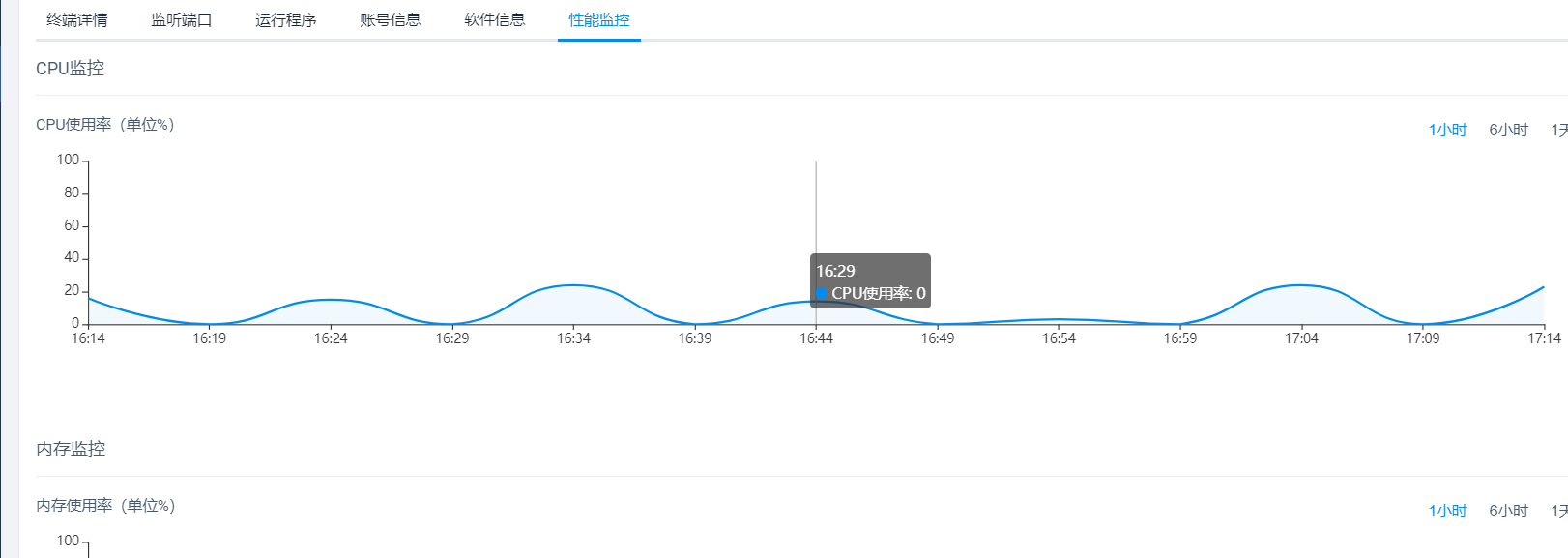
### 软件信息

可以查看该终端上运行的软件，软件厂商，版本号以及软件的安装目录。



### 性能监控

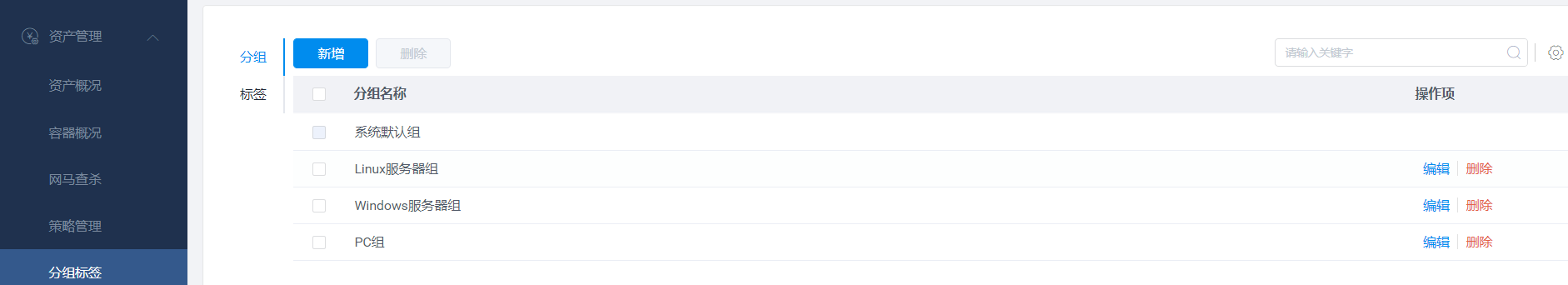
可以查看该终端的 CPU使用率，内存使用率，网络 IO检测，磁盘使用率



# 分组标签

分组：将部署客户端的服务器划分为Linux或者是wins组，在资产界面能对资产服务器进行区分

标签：按需设置，将部署客户端的服务器打上标签以示区分



# 网站防护

## 7.1 网页防篡改

网页防篡改可保护对象设置的目录及子目录下的文件无法被修改，支持例外设置，新增子规则对子目录设置例外。

### 7.1.1 新增规则

\*\*\*注意：黑名单和白名单配合使用时，新增规则父规则是黑名单即阻断并记录，添加子规则才是白名单

1. 保护目录：要保护的目录，支持选择目录或粘贴路径，支持通配符输入，但是一个目录里面只能存在一个”\*”，如/a/\*b/是正确的,但/a/\*b\*a/是错误的，且给文件夹配置通配符要以”/”结尾，如果是文件则不需要以”/”结尾
2. 处理方式：选择仅记录或阻断并记录；
3. 是否启用：选择是否启用该规则



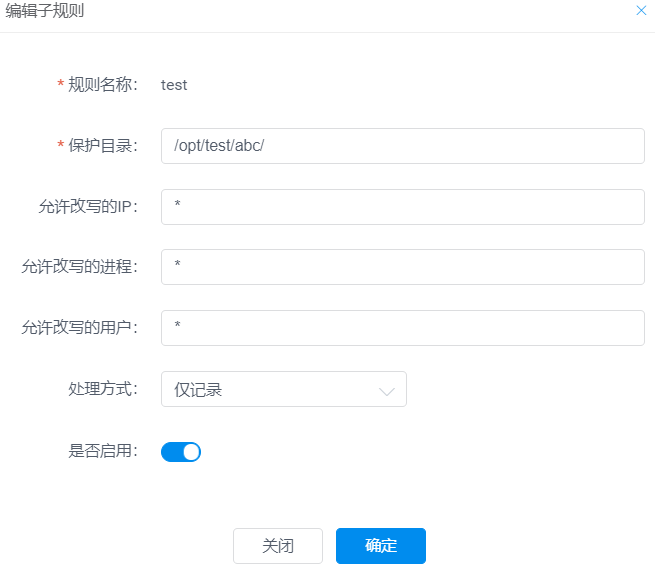
对于已添加的规则，可关闭/启用、重新编辑、删除或新增子规则。



### 7.1.2 新增子规则

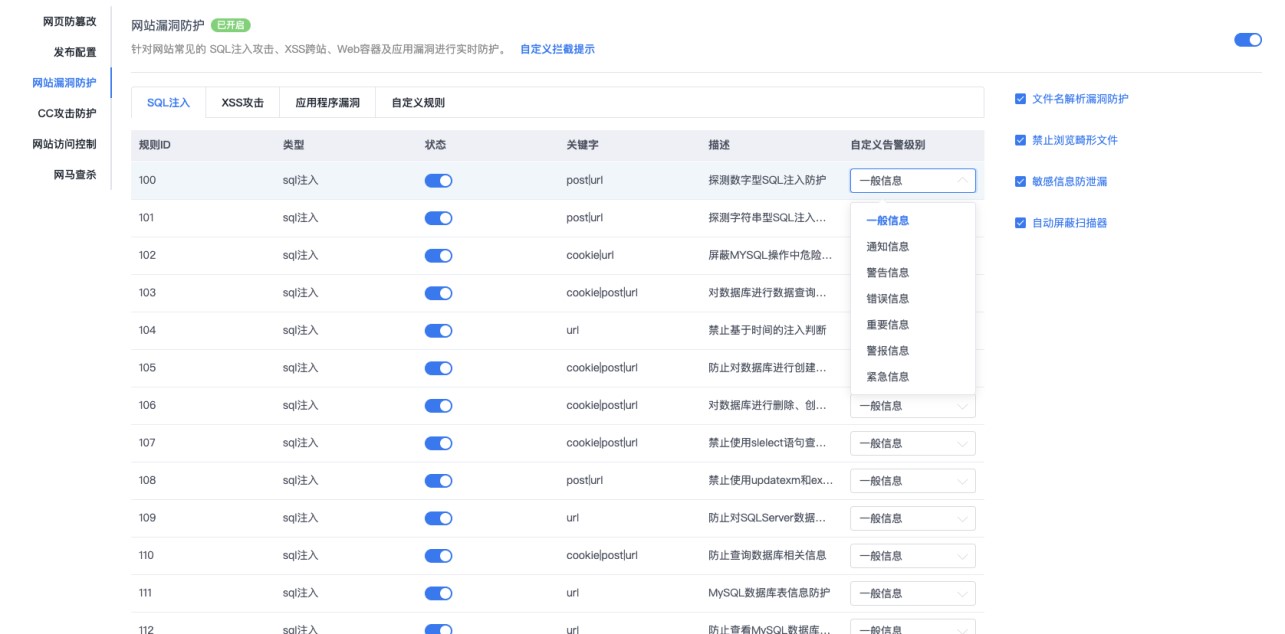
\*\*\*注意：子规则即白名单，优先级最高

1. 保护对象：选择或粘贴规则中保护对象的子目录；
2. 允许改写的 IP：允许改写该对象的 IP，支持填入单个 IP，或多个 IP 用“，”隔开，不支持填入
3. IP 段。允许所有 IP 改写则填\*；
4. 允许改写的进程：允许改写该对象的进程，填写进程名。允许所有进程改写则填\*；
5. 允许改写的用户：输入允许改写该对象的系统用户。允许所有用户改写则填\*；



## 7.2 网站漏洞防护

网站漏洞防护，可对网站常见的 SQL 注入攻击、XSS 跨站、Web 容器及应用漏洞进行实时防护。每条规则都有单独的开关，用户可以对每条防护策略定义告警级别，开启网站漏洞防护后，除“自动屏蔽扫描器” 外，其他规则默认全部开启。



## 7.3 CC攻击防护

智能检测并防御 CC 攻击，保证网站正常服务能力。可调节高、中、低三个防护等级，可自定义拦截提示，三个等级区别如下：

浏览器行为验证说明：当达到规定的访问次数时，如果开启了此选项并且用户是通过浏览器来访问的网站，则说明是正常用户，不会将此 IP 拉黑。这个选项是为了将正常用户和攻击工具、爬虫类程序进行区分。

· 低：最简单验证策略，当单个 IP 规定的时间周期内访问次数达到设置阈值时，自动锁定一段时间。低级别兼容性最好。

·中：对于低级别无法防御的情况（可以自动执行脚本的攻击工具和浏览器无异），可以尝试开启此安全级别，该级别可以智能判断访客的真实性，并且无需访客参与验证，使用了 Cookie、JS 脚本混合验证方式。

· 高：对于长期处于被攻击状态的网站，建议开启高级别模式，高级别模式安全性最高，会在访客首次访问时通过输入一个随机的验证码来确认（图片方式验证码，具有对抗图片识别工具的干扰色），通过验证后浏览无需再次输入验证码。



## 7.4 网站访问控制

网站访问控制可以对一些特定的请求在网站漏洞防护之前直接进行阻断或拦截

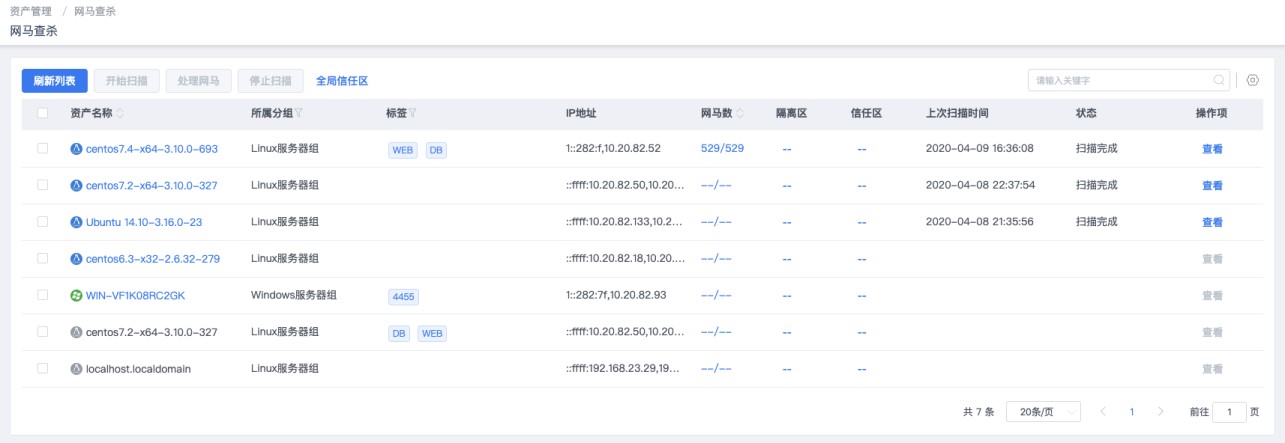
需要先配置Java-WEB防护模块，查看配置文档，注意添加的也没路径不能带http字样



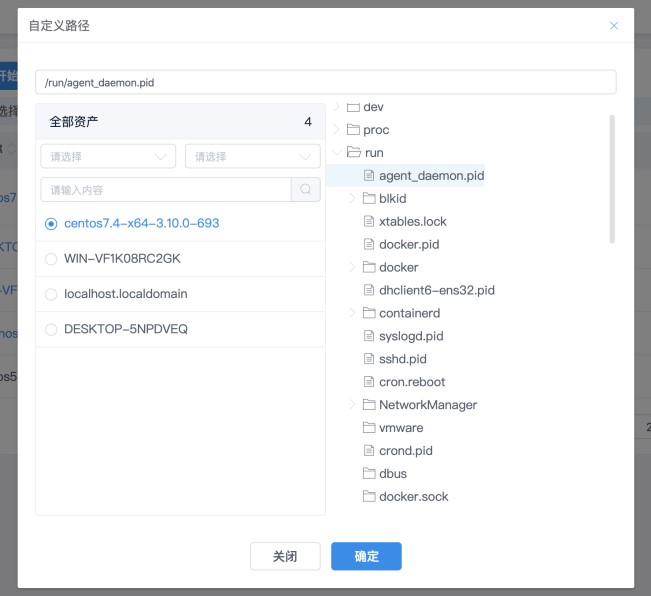


## 7.5 网马查杀

可对单个或者多个资产进行网马查杀或者网马处理

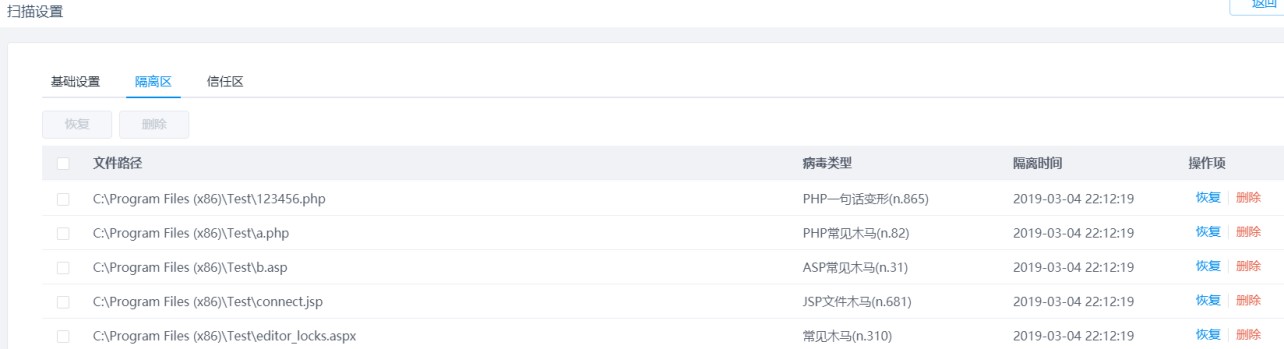


可以对不同的资产设置不同的扫描路径，支持同时对多个资产的多个目录进行网马查杀



设置扫描路径后，检测路径下的网站后门，检测结果可放入隔离区并删除或放入信任区。

隔离区和信任区可在“扫描设置”中查看，隔离区的文件可删除或恢复到原路径下，可将任意指定文件或文件夹添加到信任区下。



## 7.6 工具箱

在工具箱可以监控资产的性能包括，CPU 使用率、内存使用率、网络 IO、磁盘使用率，并且根据业务需求去设置阈值去触发报警。

# 容器防护

## 8.1容器概况

在容器概况可以查看容器名称、镜像、容器ID、容器所在资产、容器创建时间、运行状态、篡改防护状态等信息



点击“查看”可以查看更多容器信息



## 8.2容器篡改防护

容器篡改防护，可以对设置容器目录及子目录内的文件进行篡改防护，支持设置“允许改写的进程”、“放行子目录。

将容器镜像内目录保护后，任何以该镜像创建的容器内的目录都将被保护。目录下的所有目录、文件（包括子目录和文件）都将无法修改。建议将日志目录、缓存目录、数据库目录及网站程序需要写入的目录做放行配置。



# 响应处理

文件推送：可以不用登录服务器后台进行相关操作，在web上上传脚本后直接执行



# 发布端 (WPT-EE-PRO)

## 发布端管理

在发布端管理界面，可以查看当前绑定该中心的所有发布端服务器，包括名称、标签、IP 地址、操作系统、发布服务状态等。



点击“新增”按钮可以下载 windows 系统发布端安装包，或者复制 Linux 命令行去下载安装包。



支持批量对发布端进行卸载、修改标签、解除绑定



点击查看对发布端进行相关配置

首先点击设置，配置发布端服务器得ip；随后点击新增，配置发布目录等信息，开启功能；支持配置发布例外



## 发布配置

批量模板配置：在策略管理->Web 应用防护->发布配置 ，可以对模板进行发布配置，配置生效后，对绑定该模板的资产都生效。



单独资产配置：资产管理-策略管理-web应用防护—发布配置；对该客户端生效



**新增发布策略：**

发布目录：单机选择上一步配置好的发布服务器，选择相应得发布目录

同步删除：按照说明按需选择

同步软连接：按照说明按需选择

同步时机：

* 事件同步：发布目录下文件只要发生改变将立即同步更改过得文件内容
* 定时同步：定时同步发布目录下得文件

网站目录：选择需要同步得网站服务器下得目录；要写真实得路径



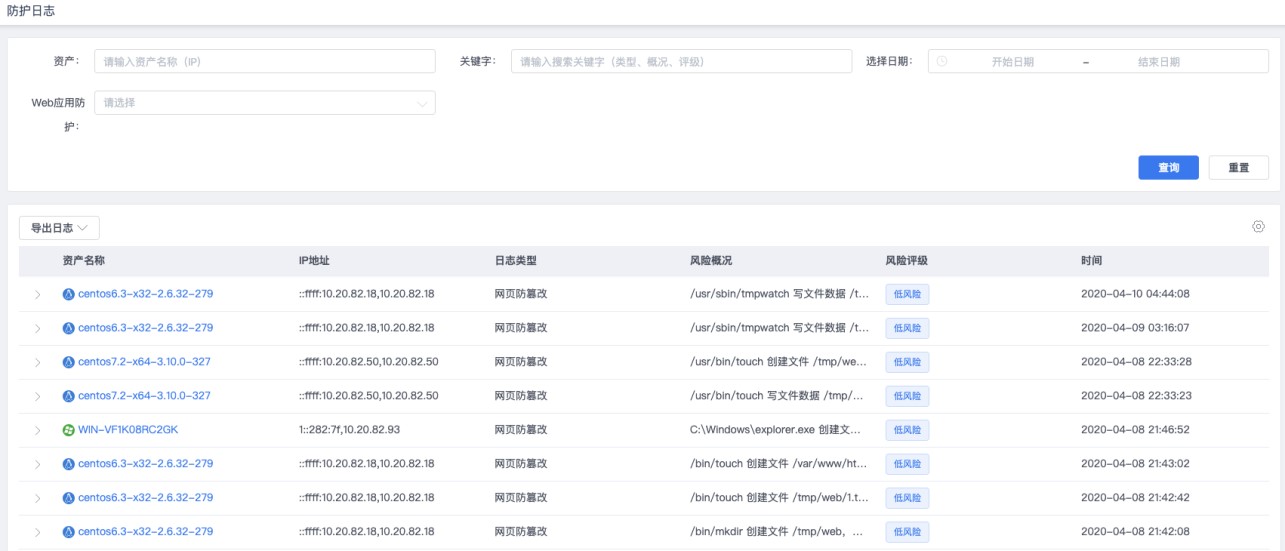
点击确定，开启发布配置，保存



# 日志检索

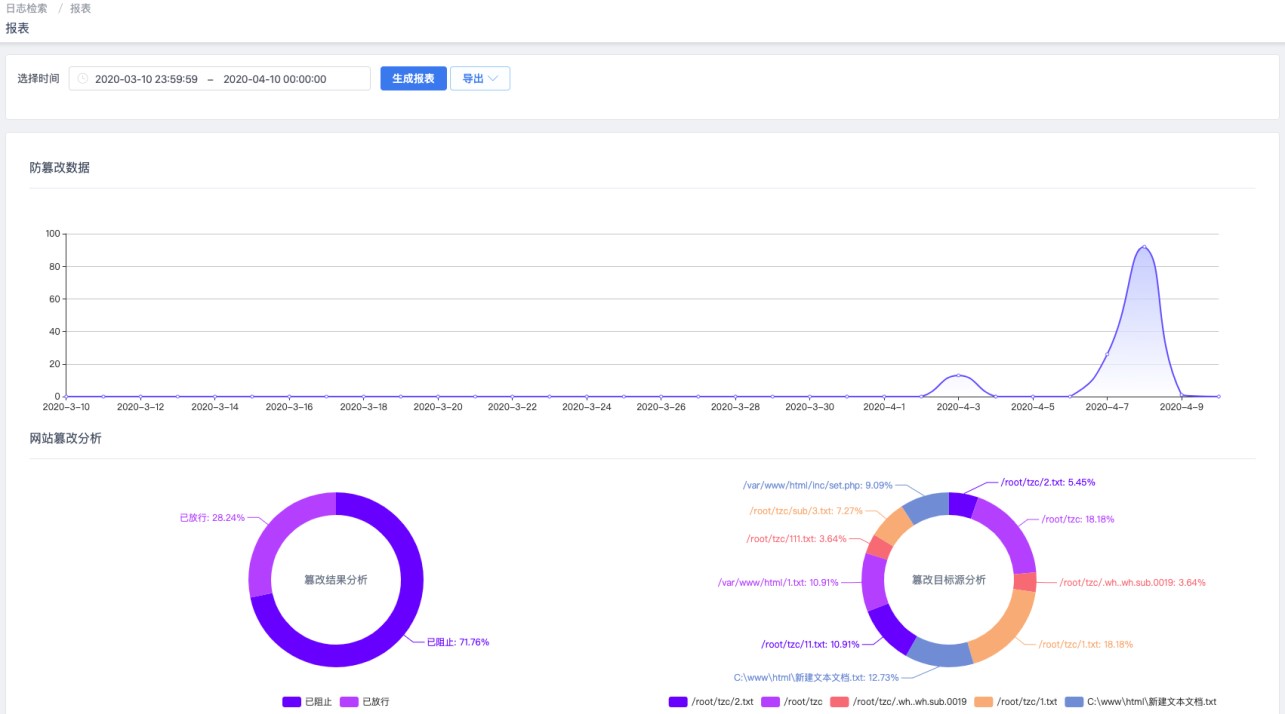
## 日志种类

共有三种类型的日志分别为防护日志、操作日志、运维日志、告警日志、日志均可以根据关键字、日志类型等信息来查询。点击“导出日志”可导出格式为 CSV/Excel 的日志，支持最多导出 10 万条，当前总数超过 10 万条则导出最新的 10 万条。点击资产名，可跳转到相应的配置页面查看详情或更改配置。



## 报表

可以根据时间时间筛选去生成报表，报表里面会从多个维度去详细分析防篡改和防攻击的数据，主要包含篡改防护次数统计、篡改结果分析、篡改目标源分析、篡改源分析、攻击防护次数、高风险资产数据统计以及总体处理结果数据等。报表支持 PDF、HTML、WORD 三种格式的导出。



# 系统管理

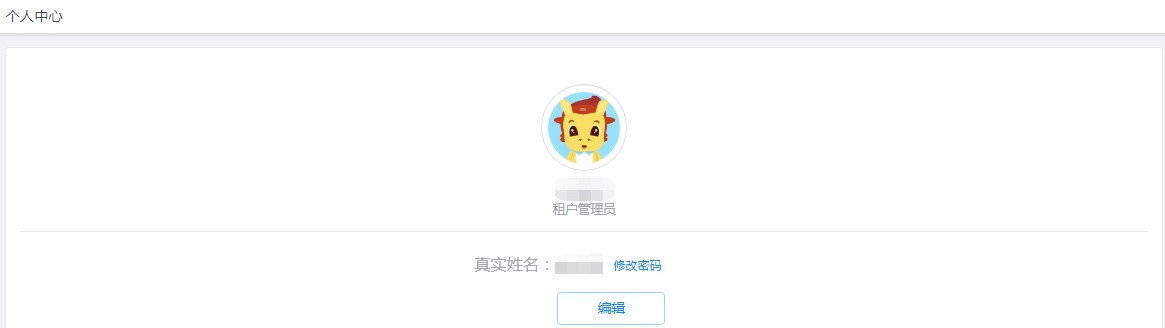
## 个人中心

可修改用户密码

、

修改用户真实姓名

、修改头像。

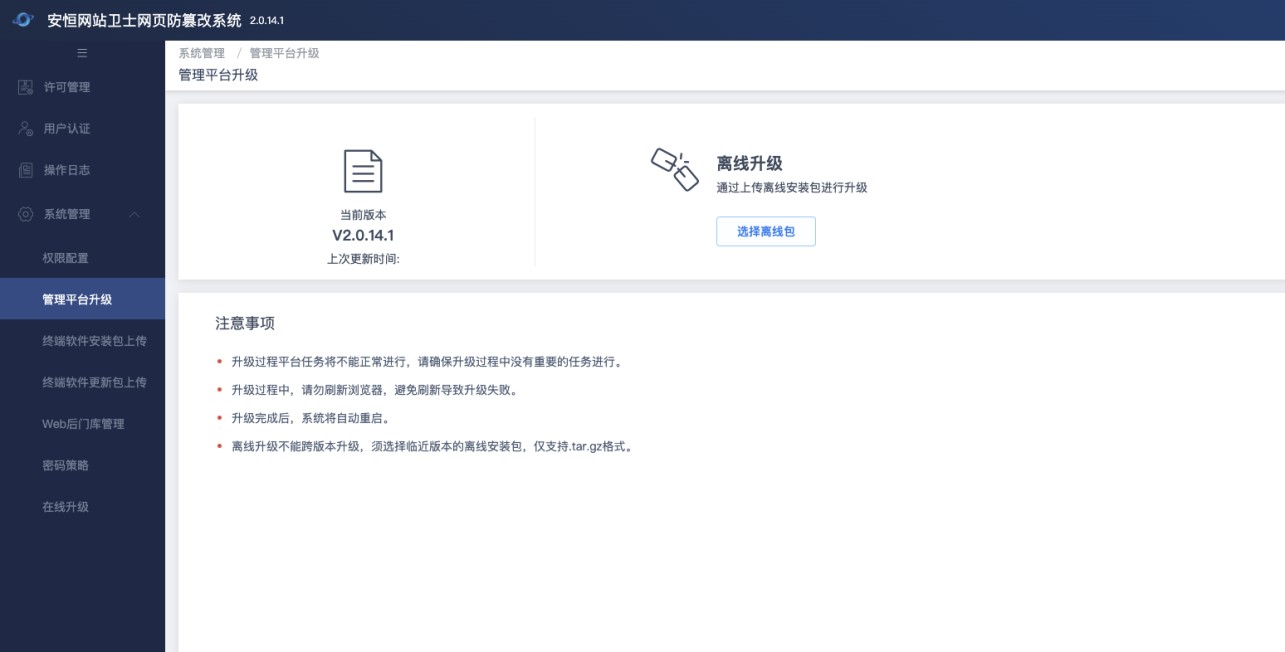


## 许可证设置

查看当前用户的许可信息、添加新的许可信息以及当前用户的机器码。



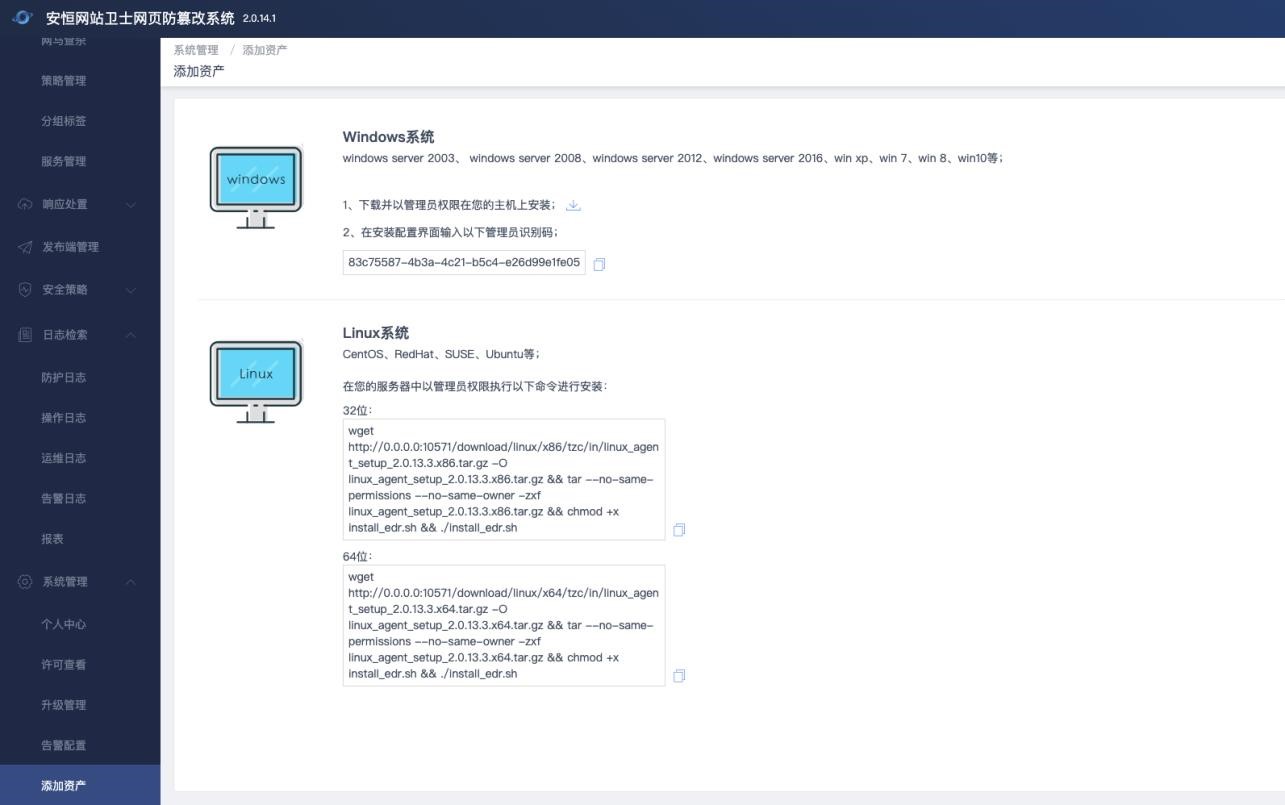
## 离线升级管理

通过 admin 用户登录，上传管理中心、终端软件、Web 后门库、。  再通过租户账号，在“系统设置-升级管理”界面，可升级客户端和病毒库。点击资产名称可跳转到相应资产的配置页面。



## 添加资产

在添加资产页面中，可以查看目前软件所支持的操作系统版本。以及可以在该页面下载客户端安装包。并且可以查看连接管理中心时所需要的管理员识别码（UUID）。



## 告警配置

## 邮件告警

系统管理—告警配置—邮件告警

SMTP服务器地址：mail.dbappsecurity.com.cn

SMTP服务器端口：995

SMTP账号：公司邮箱账号主体如：zhijie.wang

SMTP密码：公司邮箱密码==OA密码

邮箱地址后缀：dbappsecurity.com.cn

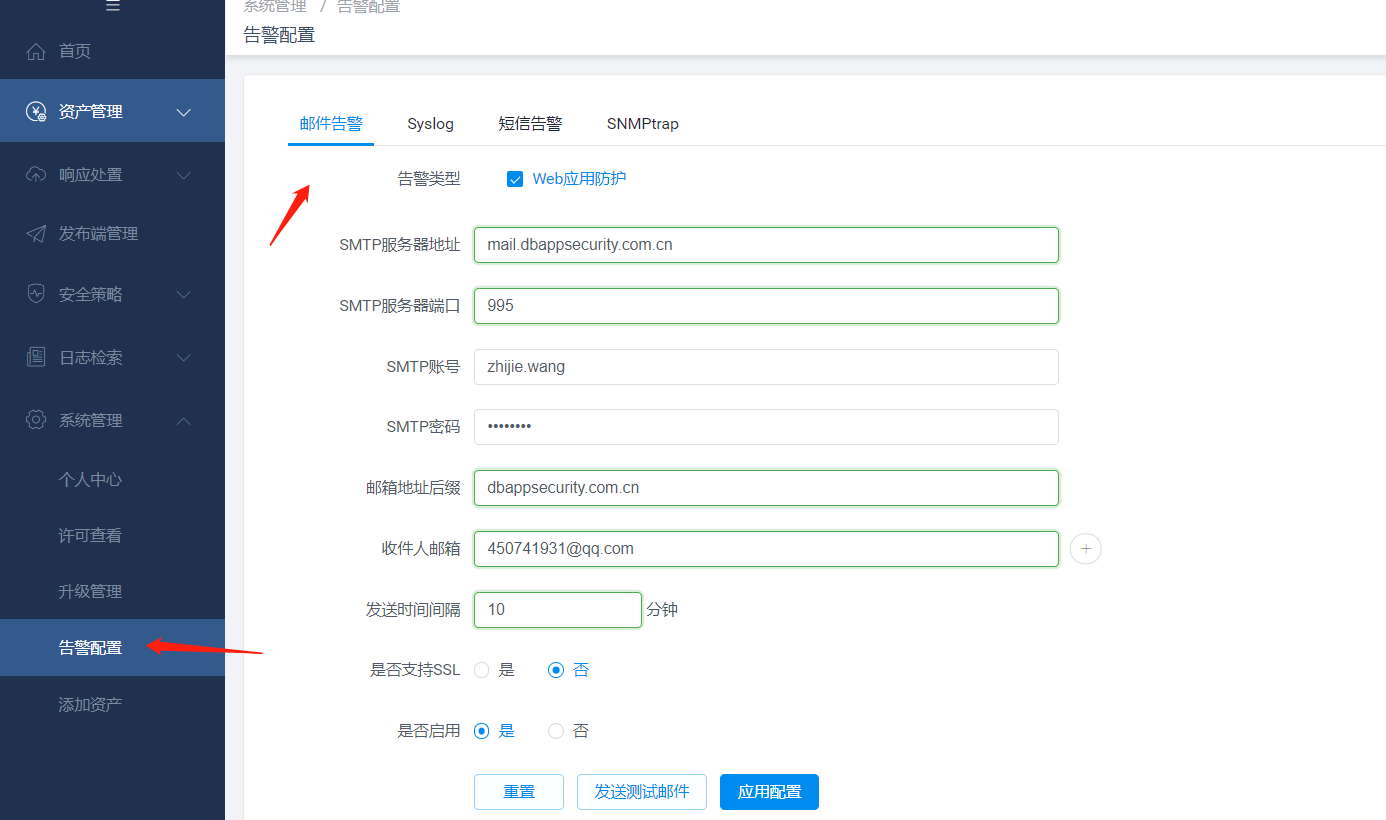
收件人邮箱：可以填写想接收告警邮件的邮箱账户，如：qq邮箱账号，163邮箱账号等

发送时间间隔：按需填写（根据端服务器发送防护日志后得时间计算）

是否支持SSL：要看收件人邮箱是否支持，qq邮箱选择否。如果不知道，就都选择否

是否启用：选择是

填写完配置后，点击应用配置，即可生效，因为安全原因信息保存后，SMTP密码会变为三位数，再次点击发送测试邮件，会提示发送失败，这个属于正常现象



#### syslog

·Syslog 服务器地址：接收 syslog 的服务器 IP；

·Syslog 服务器端口：接收 syslog 的服务器端口；

·是否启用：是否启用 syslog 告警。



### 短信告警

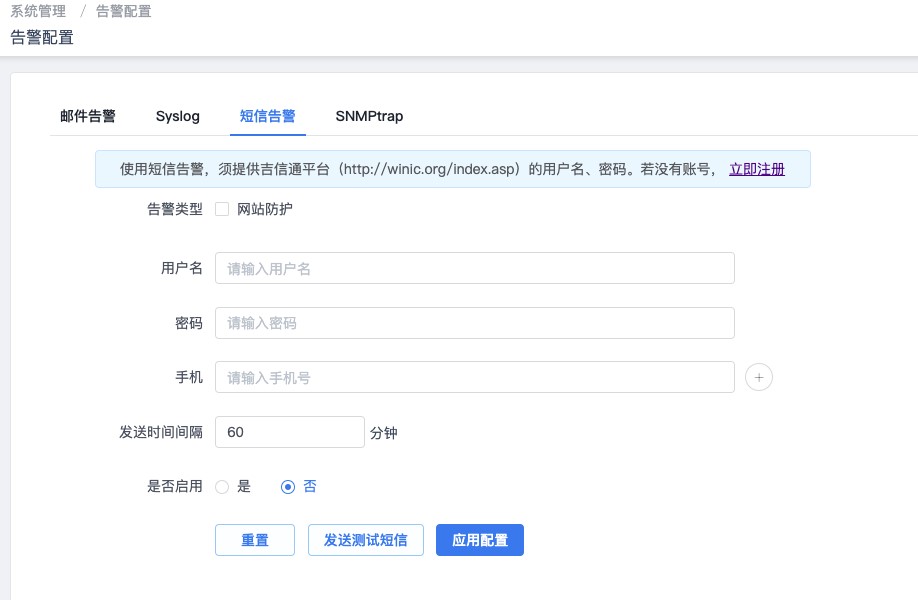
注意：如未注册吉信通平台账号，需先注册。

· 用户名：吉信通注册的账号；

· 密码：对应账号的登录密码；

·手机号：接收告警短信的手机号，可输入多个；

· 发送时间间隔：告警短信发送频率，单位分钟；

·是否启用：是否启用短信告警功能。 

### SNMPtrap

·SNMP服务器地址：部署SNMP服务器的IP

·SNMP服务器端口：SNMP服务器的配置的端口

·是否该功能启用：按需填写

