

# 360 终端安全管理系统 操作手册

适用版本：10.0.0.07300/12.0.0.07100

# 版权声明

©2021-2022 360 公司 保留所有权利

本文档所有内容均为 360 公司独立完成，未经 360 公司作出明确书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形状）对本文档的任何部分进行复制、修改、存储、引入检索系统或者传播。

# 前言

## 文档概述

本手册主要描述 360 终端安全管理系统 V10.0 业务简述及操作步骤。通过阅读本手册，用户可以了解本系统客户端的业务功能使用方法及操作步骤，帮助用户理解和使用。

## 读者对象

本手册的阅读对象包括：产品经理、文档工程师、技术支持、用户等。

## 修订记录

版本	修订时间	编制者	审核者	修订内容
v3.6	2022-04-22			更新 6000 版本内容
v3.7	2022-05-07			补充准入内容
V3.8	2022-06-22			更新 6100 版本内容
V3.9	2022-09-15			补充工具大全内容，调整内容格式
V4.0	2022-10-31			更新 6200 版本内容
V5.0	2023-5-10			更新 7000 版本内容
V5.1	2023-7-31			更新 7100 版本内容
V5.2	2023-9-21			更新 7300 版本内容

# 目 录

1.	360 终端安全管理系统简介 .....	1
1.1.	产品简介 .....	1
1.2.	部署场景 .....	1
2.	使用前准备 .....	2
2.1.	登录系统 .....	2
2.2.	授权导入 .....	2
2.2.1.	证书获取—申请序列号 .....	2
2.2.2.	生成授权证书 .....	2
2.2.3.	管控中心导入证书 .....	4
2.3.	安装客户端 .....	6
	Windows/Winserver 客户端 .....	6
	Linux 客户端 .....	7
3.	控制中心首页 .....	8
4.	资产管理 .....	11
4.1.	资产总览 .....	11
4.2.	终端管理 .....	14
4.2.1.	终端概况 .....	14
4.2.2.	终端策略 .....	24
4.2.3.	终端升级 .....	51
4.2.4.	终端交互 .....	56
4.2.5.	终端详情 .....	62
5.	实时对抗 .....	77
5.1.	实时防御 .....	77
5.1.1.	风险总览 .....	77
5.1.2.	实时防御管理 .....	77
5.1.3.	策略设置 .....	78



5.1.4.	1 日志分析 .....	80
5.2.	勒索防护 .....	82
5.2.1.	勒索总览 .....	82
5.2.2.	勒索管理 .....	82
5.2.3.	勒索风险日志 .....	83
5.2.4.	系统多因素认证 .....	83
5.2.5.	策略设置 .....	87
6.	病毒查杀 .....	89
6.1.	基本概念 .....	89
6.1.1.	快速扫描 .....	89
6.1.2.	全盘扫描 .....	89
6.1.3.	强力扫描 .....	89
6.1.4.	宏病毒扫描 .....	89
6.1.5.	隔离区 .....	89
6.1.6.	信任区 .....	89
6.2.	风险总览 .....	90
6.3.	查杀管理 .....	90
6.3.1.	主机查杀 .....	90
6.3.2.	按终端统计 .....	90
6.3.3.	按项目统计 .....	93
6.4.	策略设置 .....	95
6.4.1.	病毒查杀 .....	95
6.4.2.	安全区 .....	103
6.5.	MD5 与路径库 .....	108
7.	漏洞管理 .....	109
7.1.	基本概念 .....	109
7.1.1.	智能忽略 .....	109
7.2.	系统漏洞管理 .....	109
7.2.1.	漏洞风险概览 .....	109
7.2.2.	漏洞视图统计 .....	110

7.2.3.	终端视图统计.....	113
7.2.4.	策略设置.....	115
7.2.5.	系统漏洞日志.....	121
7.3.	补丁文件管理.....	123
7.4.	停服系统管理.....	124
7.5.	无补丁漏洞免疫.....	125
8.	数据保护.....	129
8.1.	数据操作审计.....	129
8.1.1.	功能入口.....	129
8.1.2.	Windows 终端策略配置.....	129
8.1.3.	日志记录.....	131
8.1.4.	注意说明.....	131
8.2.	数据打印审计.....	131
8.2.1.	功能入口.....	132
8.2.2.	Windows 终端策略配置.....	132
8.2.3.	国产通用桌面机终端策略配置.....	133
8.2.4.	日志记录.....	134
9.	外设管理.....	136
9.1.	外设总览.....	136
9.2.	外接设备管控.....	137
9.2.1.	外设库.....	137
9.2.2.	外设控制.....	138
9.2.3.	外设控制日志.....	139
9.3.	移动存储管控.....	140
9.3.1.	设备列表.....	140
9.3.2.	设备注册.....	141
9.3.3.	设备审批.....	142
9.3.4.	设备控制.....	143
9.3.5.	设备控制日志.....	144
9.4.	外设使用审计.....	145

9.4.1.	功能入口.....	145
9.4.2.	Windows 终端策略配置.....	146
9.4.3.	国产通用通用桌面机策略配置.....	147
9.4.4.	日志记录.....	148
10.	上网管理.....	149
10.1.	外联管控.....	149
10.1.1.	违规外联管控.....	149
10.1.2.	境外连接监测.....	153
10.1.3.	网络出口管理.....	154
10.2.	强制隔离.....	154
10.2.1.	终端隔离状态.....	154
10.2.2.	智能隔离日志.....	156
10.2.3.	智能隔离策略.....	156
10.3.	典型场景.....	159
11.	软件管理.....	161
11.1.	基本概念.....	161
11.1.1.	软件管家.....	161
11.1.2.	应用软件.....	161
11.2.	软件管理.....	161
11.2.1.	软件使用分析.....	161
11.2.2.	终端视图.....	162
11.2.3.	软件视图.....	163
11.2.5.	软件管理策略.....	165
11.3.	软件管家.....	170
11.3.1.	软件市场.....	170
11.3.2.	软件定制.....	173
11.3.3.	软件设置.....	174
11.3.4.	软管报表.....	175
11.4.	分发管理.....	176
11.4.1.	软件分发.....	176

---

11.4.2. 文件分发.....	177
11.5. 进程管理.....	180

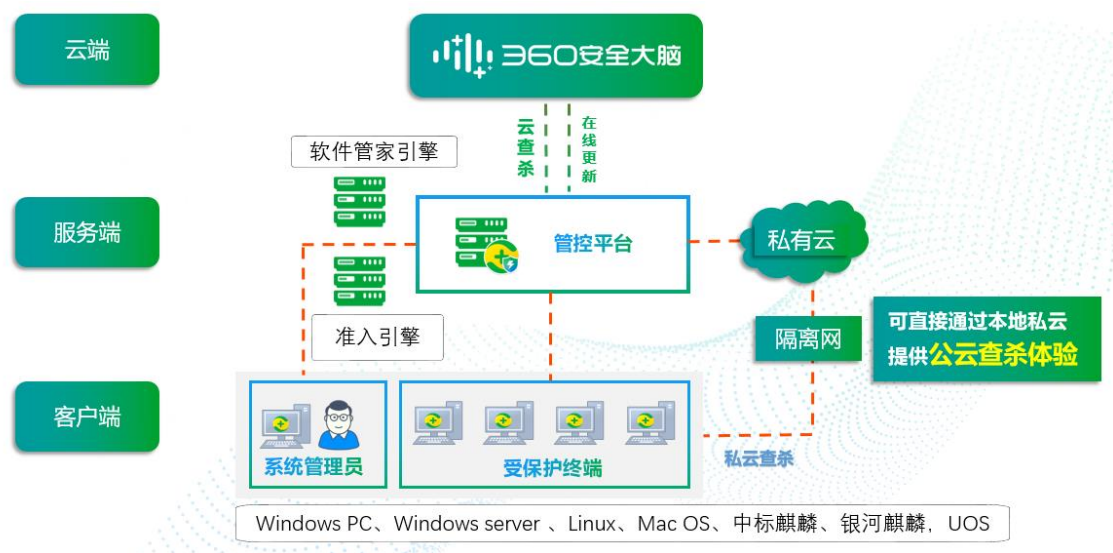
# 1. 360 终端安全管理系统简介

## 1.1. 产品简介

360 终端安全管理系统是在 360 安全大脑极致赋能下，以云计算、大数据、人工智能等新技术为支撑，以可靠服务为保障，集高级威胁发现（EDR）、防病毒、漏洞防护、停服加固、终端合规管控、终端准入（NAC）、终端审计、数据安全、主机加固（CWPP）管理于一体的企业级安全产品，能同时兼容传统与信创终端统一管理、全面保障政企终端安全。

360 终端安全管理系统具备模块化特性，具备单平台多品类能力，也可根据不同的安全诉求提供相应的安全模块组合、灵活交付；360 终端安全管理系统可与 360 体系的安全大脑、云盘、零信任等产品进行集成、联动，实现体系化的安全管理。

## 1.2. 部署场景



## 2. 使用前准备

### 2.1. 登录系统

http://IP:8081/dist 登录管控中心首页，输入用户名和初始密码。

用户名：eppadmin

初始密码：pass-abcd-1234



### 2.2. 授权导入

#### 2.2.1. 证书获取—申请序列号

请联系授权管理平台生成对应序列号。

#### 2.2.2. 生成授权证书

- (1) 访问 360 产品授权服务平台进行授权激活操作：<https://epp.360.cn>



(2) 第一次登录，需进行注册，点击最下方蓝色按钮【注册】，弹出注册页面，填写用户信息。

用户信息：序列号，企业名称，行业，电话，邮箱，密码，确认密码；


### 授权系统注册

已有授权账户? 点击这里 [登录](#)

公司名称*	行业*
<input type="text"/>	<input type="text"/>
公司联系人*	公司联系电话*
<input type="text"/>	<input type="text"/>
公司联系人邮箱*	分销商名称
<input type="text"/>	<input type="text"/>
分销商联系人	分销商联系电话
<input type="text"/>	<input type="text"/>
密码*	确认密码*
<input type="password"/>	<input type="password"/>

基本序列号/单机序列号 [导入](#) (支持导入txt文件格式，使用英文逗号分隔每组序列号)

0160000

 注意：请牢记服务号及密码

(3) 注册完成后，登录到系统中。

1) 点击【证书申请】



2) 在证书申请页面, 填写申请信息, 进行提交。

申请信息: 基本序列号, 经销商名称, 经销商电话, 联系人, 产品名称, logo;

证书申请

\* 基本序列号 请输入或选择

产品名称 请输入

logo

上传照片

取消 提交

3) 提交后, 系统将激活产品, 生成 license 证书, 点击页面中的【证书下载】进行下载。

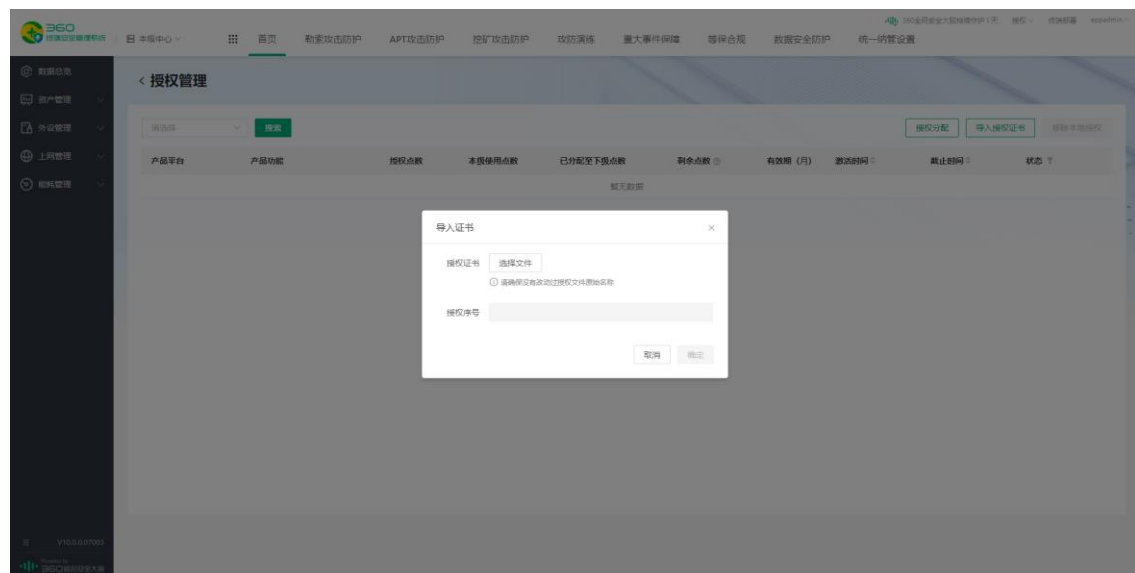
序列号	产品类型	类型	产品名称	Logo	序列号生成时间	证书申请时间	特征码	密钥	解密码	用户名	操作
	360终端安全管理软件	基本	—	—	2021-04-07 15:37:31	2021-04-07	—	—	—		查看详情 证书下载

## 2.2.3. 管控中心导入证书

管控中心首页 <http://管理中心 IP:8081/dist>, 在右上角菜单栏, 点击 授权\授权管理, 进入到授权管理界面。







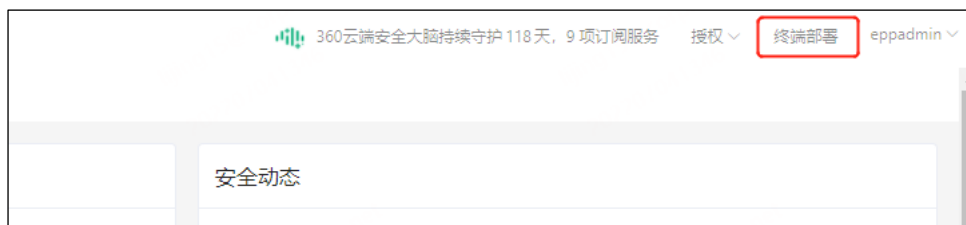
选择授权文件后提交，完成后刷新页面：

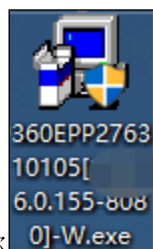
产品平台	产品功能	授权点数	本设备使用点数	已分配至下级点数	剩余点数	有效期 (月)	激活时间	截止时间	状态
金平台	私有云服务	-	-	-	-	11	2022-06-14	2023-05-14	正常
金平台	威胁情报服务	-	-	-	-	11	2022-06-14	2023-05-14	正常
金平台	多级管控	-	-	-	-	11	2022-06-14	2023-05-14	正常
Windows	漏洞管理	1111	245	0	866	11	2022-06-14	2023-05-14	正常
Windows	资产管理	1111	832	0	279	11	2022-06-14	2023-05-14	正常

## 2.3. 安装客户端

### Windows/Winserver 客户端

首页> 终端部署，找到对应的客户端安装包点击【下载】





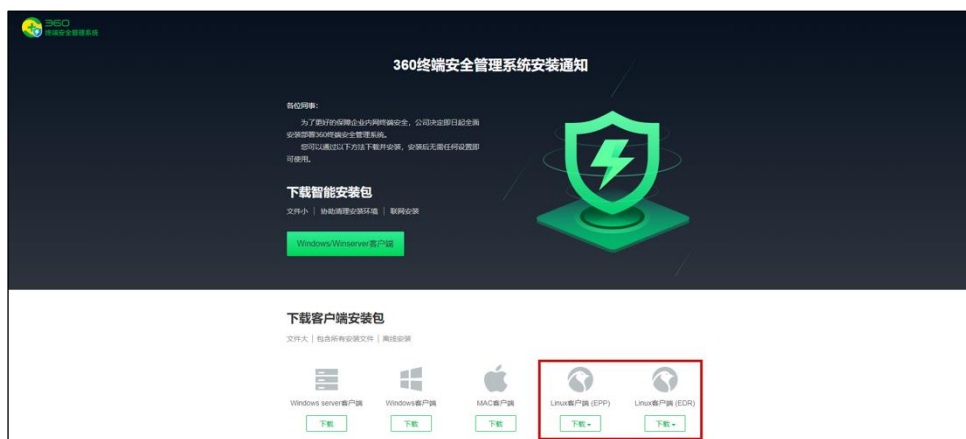
客户端安装文件如下，不要更改文件名称

双击执行安装文件即可。

说明：如果客户端已经安装其他杀毒软件，需要先卸载并重启后再执行安装。

## Linux 客户端

(1) 下载客户端：下载步骤与 windows 客户端下载步骤类似，找到对应的安装包，点击【下载】



(2) 安装包 rpm -ivh +包名或双击运行安装

```
[root@localhost zhangyg]# ll
total 34556
-rwxrw-rw-. 1 zyg zyg 35384417 Mar 23 01:54 360epp-server-10.0.0.0001-redhat.x86_64.rpm
[root@localhost zhangyg]# rpm -ivh 360epp-server-10.0.0.0001-redhat.x86_64.rpm
Preparing...
package 360epp-server-10.0.0.0001-redhat.x86_64 is already installed
[root@localhost zhangyg]#
```

说明：如果执行安装的时候报错，则包名的这个地方添加\试试

```
rpm -ivh --force 360epp-server-10.0.0.1001-redhat.x86_64\10.209.213.159_8080\).rpm
```

## 3. 控制中心首页

管控中心首页，直观展示全网整体的安全状况。依托安全体检，为全网终端安全状态快捷体检和检查结果分析；引入云端情报能力，支持云脑情报查询和热点时间推荐等。增加基础和业务模块的数据分析和可视化展示，帮助管理员了解全网安全状态。具体包括：

- (1) 安全体检分析：支持对全网终端进行一键体检，同时对全网安全体检健康度进行分析，对异常项进行统计展示
- (2) 云脑情报：将 360 威胁情报中心搜索入口嵌入首页中，供管理员快捷发起云脑情报搜索。
- (3) 热点事件：展示最新的热点时间，支持查看详情
- (4) 终端设备总量：终端发现的设备数量总和。即：已注册终端+未注册终端+手动添加设备总和
- (5) 已安装终端：管控当前接入的所有终端(包括在线、离线)总和
- (6) 累计查杀病毒：系统上线起，所有终端病毒查杀次数累计值，即“处理成功”+“添加信任”类型的病毒日志总量。
- (7) 累计漏洞修复：系统上线起，所有终端漏洞修复次数累计值，即“已修复”漏洞日志总量。
- (8) 待修复漏洞数：当前系统中终端待修复漏洞数的统计，支持跳转处理
- (9) 累计对抗拦截：系统上线起，所有终端主防日志总和
- (10) 终端概况：对用户侧已安装客户端的设备终端进行分析统计，同时按 OS 平台进行统计分析，帮助用户了解资产的操作系统分布情况。
- (11) 设备类型分布：对用户侧本级中心全网发现的设备，按类型进行统计分析，帮助用户了解资产的类型分布情况。同时，对 TOP10 的设备类型进行排名。
- (12) 安全事件播报：此模块用于对当前全网终端最新发生的安全事件进行发现，以时间轴方式滚动播报，方便用户及时了解最新的安全事件动态，及时进行干预、处置操作。
- (13) 告警事件看版：展示前系统最新的告警事件内容，可设置查看仅高危告警或全部告警。
- (14) 病毒类型统计：对系统所发现的病毒类型进行统计分析
- (15) 发现病毒最多的终端 Top10：支持对终端感染病毒数量进行分析，根据终端感染的病

## 病毒数进行 top 排行统计

(16) 感染终端最多的病毒：支持对病毒感染终端的情况进行分析，根据病毒感染终端数进行 top 排行统计

(17) 病毒查杀趋势：支持对全网终端的病毒查杀事件进行分析，绘制趋势分布，包括清除成功、清除失败、未处理、添加信任。

(18) 漏洞修复趋势：支持对全网终端的漏洞修复事件进行分析，绘制趋势分布，包括已修复、未修复、已忽略。

(19) 违规外联分布：支持对全网终端的违规外联事件进行分析，绘制趋势分布

(20) 服务器资源状况：此功能用于帮助用户对当前管控中心的服务器运行情况进行监控，对服务器 CPU 使用率、内存占用率、磁盘使用率等进行在线监控，当服务器性能异常或产生压力时及时直观的提醒用户。

(21) 终端系统：分析、统计当前系统中使用较多的操作系统，进行 top 排行统计

(22) 终端品牌：分析、统计当前系统中使用较多的终端品牌，进行 top 排行统计

(23) 终端浏览器：分析、统计当前系统中使用较多的终端浏览器，进行 top 排行统计

(24) CPU 类型：分析、统计当前系统中使用较多的 CPU 类型，进行 top 排行统计

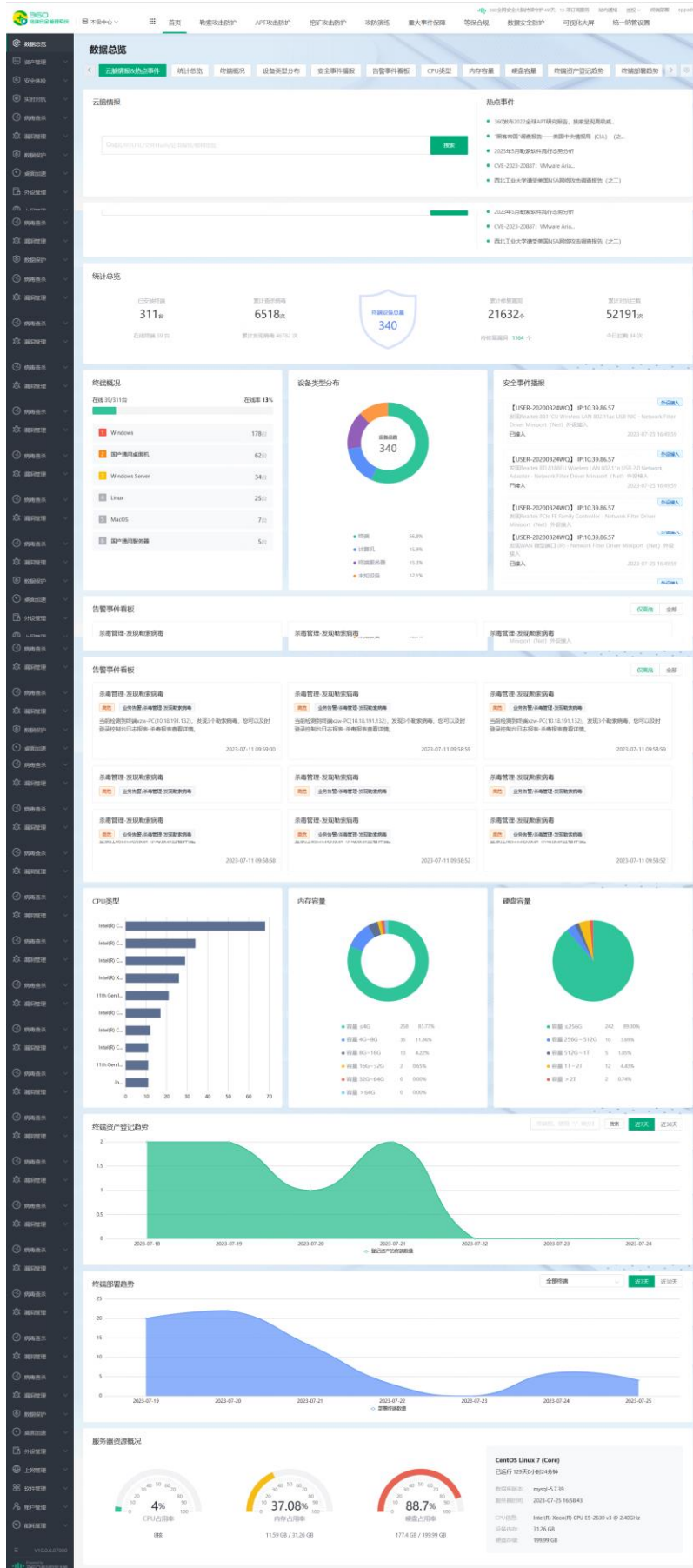
(25) 内存容量：分析、统计当前终端设备所使用的内存容量情况，按照不同的容量区间做分布统计

(26) 硬盘容量：分析、统计当前终端设备所使用的硬盘容量情况，按照不同的容量区间做分布统计

(27) 终端资产登记趋势：对当前网内终端，每天发生的资产登记行为做统计，绘制趋势分布

(28) 终端部署趋势：对当前网内每天新部署的终端设备数量做统计，绘制趋势分布

点击上侧场景导航：**首页** > **数据总览**，展示系统首页相关数据详情：



## 4. 资产管理

### 4.1. 资产总览

资产总览作为“资产管理”功能的首页，主要实现对资产信息的可视化，帮助用户更直观地了解资产总体情况，更有效得出对资产的理解或判断。

点击左侧导航：**资产管理** > **资产总览**可以查看资产总览模块的可视化视图，其下包含资产总览视图模块的锚点定位以及各视图模块的数据展示。





主要包含：

1. 终端设备统计：对用户侧本级中心全网发现的终端设备（计算机、服务器、打印机等），按类型进行统计分析，帮助用户了解资产的类型分布情况。
2. 终端资产统计：对用户侧本级中心全网终端资产（软件资产、进程资产、启动项、账户资产等），按类型进行统计分析，帮助用户了解资产分布情况。
3. 风险资产事件统计：基于用户侧本级中心全网发现的风险资产事件列表，按风险类型进行统计。
4. 风险终端设备 top5：基于用户侧本级中心全网发现的风险资产事件，按终端做风险事件统计的聚合，对关联风险事件数最多的终端 top 统计。
5. 高危端口开放 top5：基于用户侧本级中心全网发现的风险资产事件，从端口维度对日志统计做聚合，统计哪些高危端口被终端开放的多。
6. 发现风险事件最多的分组 Top5：基于用户侧本级中心全网发现的风险资产事件，按终端分组做风险事件统计的聚合，对关联风险事件数最多的终端 top 统计。
7. 资产风险事件播报：对当前全网终端设备最新检测发生的资产风险事件进行发现，以时间轴方式滚动播报，方便用户及时了解最新的风险事件动态，及时进行干预、处置操作。
8. 终端设备分布：基于用户侧本级中心全网发现的终端设备，以分组角度，按终端设备类型进行设备数量统计。
9. 设备类型分布：对用户侧本级中心全网发现的设备，按类型进行统计分析，帮助用户了解资产的类型分布情况。同时，对所有的设备类型进行排名。
10. 操作系统分布：对用户侧已安装客户端的设备终端进行分析统计，同时按 OS 平台进行统计分析，帮助用户了解资产的操作系统分布情况。
11. 软件应用 top5：对用户侧本级中心全网终端软件资产，按安装终端数进行 top5 统计，帮助用户了解哪些软件被终端安装的多。
12. 开放端口 top5：对用户侧本级中心全网终端软件资产，按开放终端数进行 top5 统计，帮助用户了解哪些端口被终端开放的多。
13. 账户资产 top5：对用户侧本级中心全网终端软件资产，按使用终端数进行 top5 统计，帮助用户了解哪些账号被终端使用的多。
14. 终端资产趋势：基于用户侧本级中心全网发现的终端设备，以终端设备总量和风险终端维度，绘制终端发现趋势和风险发现趋势。
15. 风险资产事件趋势：基于用户侧本级中心全网发现的风险资产事件日志，按每天的

风险事件总数绘制时间周期范围内的风险事件趋势，帮助用户了解发现趋势和哪类风险事件较多。

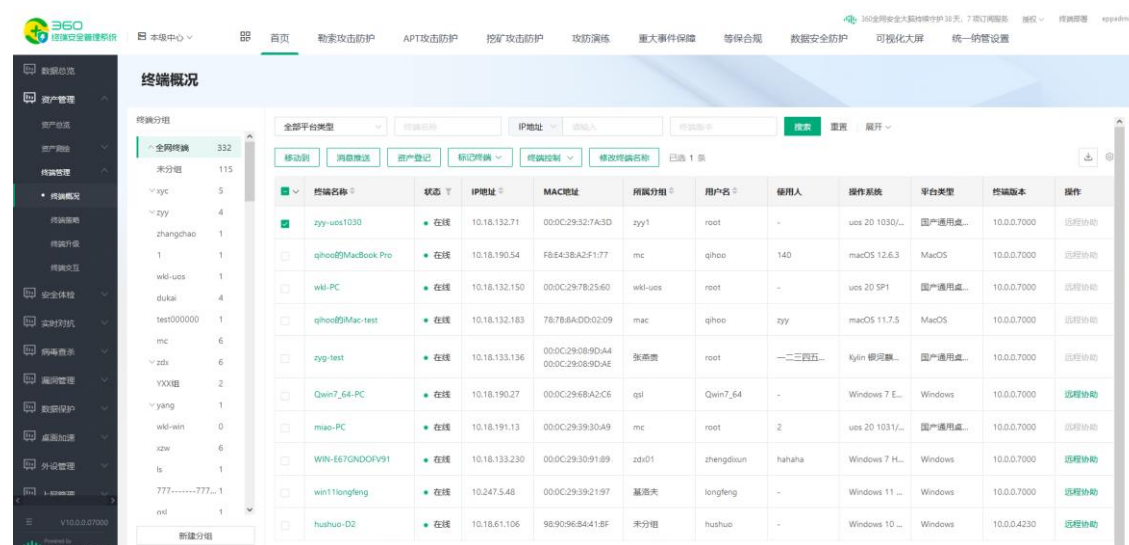
## 4.2. 终端管理

### 4.2.1. 终端概况

全网授权的终端概况展示了所有终端的基本情况，包括计算机基础信息：终端在线信息、计算机名、登录用户、IP 地址、所在分组、操作系统等。可以根据关键词、状态、操作系统、浏览器信息进行筛选，终端信息可以批量导出 csv 和 excel。

表格中每个单元格有一个初始加载时的宽度，若对初始宽度不满意支持手动调整。列表头处支持手动调整列表字段宽度，管理员可通过鼠标在列表头处左右拖拽调整列表字段列宽度。

点击左侧功能导航：**资产管理** > **终端管理** > **终端概况**，进入终端概况列表界面。

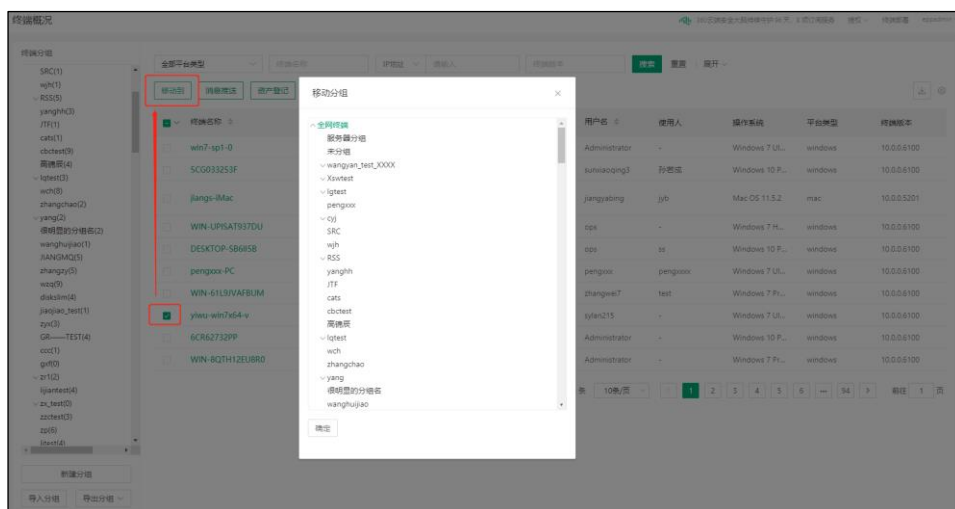



**说明：**列表中如果存在固定的首列或尾列，则固定列不支持调整宽度；列表调整宽度后不进行持久化。

#### 4.2.1.1. 转移分组

在终端列表中，选择一个或者多个终端，点击【**移动分组**】按钮，可以将目标终端移动到目标的分组下。

选择需要调整组的终端，点击**移动到》选择分组》**点击确定。



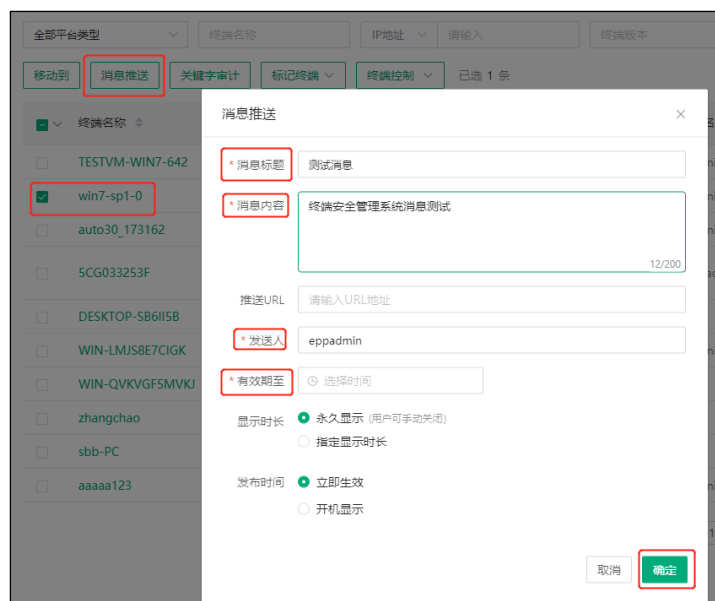
 说明：管理中心操作过程中，均可以通过点击全网终端后进行操作对象的改变，如下图：

终端名称	状态	IP地址	MAC地址	所属分组	用户名	使用人	操作系统	平台类型	终端版本
win7-spl-0	在线	10.16.16.93	00:0C:29:47:D0:DA	zhangheng	Administrator	-	Windows 7 UL...	windows	10.0.0.6100
auto30_173162	在线	10.16.16.29	00:0C:29:2F:C4:00	未分组	Administrator	-	Windows 10 P...	windows	10.0.0.6100
SCG033253F	在线	10.18.133.8	00:0E:C6:DA:97:91	RD_group	sunwiaoqing3	-	Windows 10 P...	windows	10.0.0.6100
DESKTOP-SB685B	在线	10.254.142.91	4CE8:8D:66:F8:13	未分组	ops	ss	Windows 10 P...	windows	10.0.0.6100
WIN-1MJS8E7CIGK	在线	10.19.1.5	00:0C:29:42:1B:19	未分组	Administrator	-	Windows 7 UL...	windows	10.0.0.6100

## 4.2.1.2.消息推送

在终端列表中，选择一个或者多个终端，点击**【消息推送】**按钮，可以对目标终端发送消息。

- 推送消息



- 客户端的消息窗口



### 4.2.1.3.资产登记

在终端列表中，选择一个或者多个终端，点击【资产登记】按钮，可以对目标终端进行资产登记提醒。

- 登记提醒

选择需要提醒的终端，点击资产登记。

**终端概况**

终端分组: 全部平台类型 终端名称 IP地址 终端版本 搜索 重置 展开

移动到 消息推送 资产登记 标记终端 终端控制 修改终端名称 已选 1 条

终端名称	状态	IP地址	MAC地址	所属分组	用户名	使用人	操作系统	平台类型	终端版本	操作
zyy-uos1030	在线	10.18.132.71	00:0C:29:32:7A:3D	zyy1	root	-	uos 20 1030/...	国产通用桌...	10.0.0.7000	远程协助
qihoo的MacBook Pro	在线	10.18.190.54	F8:E4:3B:A2:F1:77	mc	qihoo	140	macOS 12.6.3	MacOS	10.0.0.7000	远程协助
wkl-PC	在线	10.18.132.150	00:0C:29:7B:25:60	wkl-uos	root	-	uos 20 SP1	国产通用桌...	10.0.0.7000	远程协助
qihoo的Mac-test	在线	10.18.132.183	78:7B:8A:DD:02:09	mac	qihoo	zyy	macOS 11.7.5	MacOS	10.0.0.7000	远程协助
zyy-test	在线	10.18.133.136	00:0C:29:08:9D:A4 00:0C:29:08:9D:AE	张燕燕	root	一二三四五...	Kylin 银河麒麟...	国产通用桌...	10.0.0.7000	远程协助
Qwin7_64-PC	在线	10.18.190.27	00:0C:29:6B:A2:C6	qsl	Qwin7_64	-	Windows 7 E...	Windows	10.0.0.7000	远程协助

## ● 客户端提示



## ● 客户端资产登记

360 终端安全管理系统

360安全大脑持续守护 8 天

常规设置 资产信息 实名信息 实时防护 引擎设置 病毒扫描 漏洞修复

**资产登记**  
请尽快完成资产登记!

资产类型: 请选择资产类型

资产用途: 请选择资产用途

归属部门: 请选择归属部门

使用人: 请填写使用人

手机: 请填写手机

邮箱: 请填写邮箱

备注: 请填写备注

请输入备注

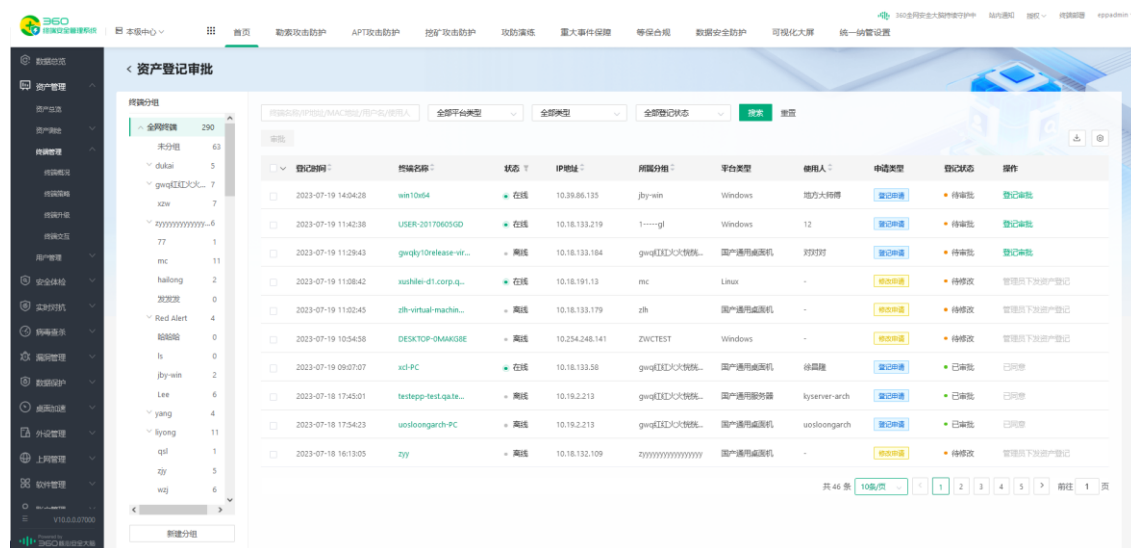
ip地址: 请填写ip地址

取消 保存

## 1) 资产登记审批

为提升资产登记模块登记信息的可靠性，资产登记新增了审批流程。终端用户在客户端填写资产登记信息提交后，会在管控中心生成一条资产登记申请信息，管理员完成审批后，终端资产登记状态才为“已审批”状态。

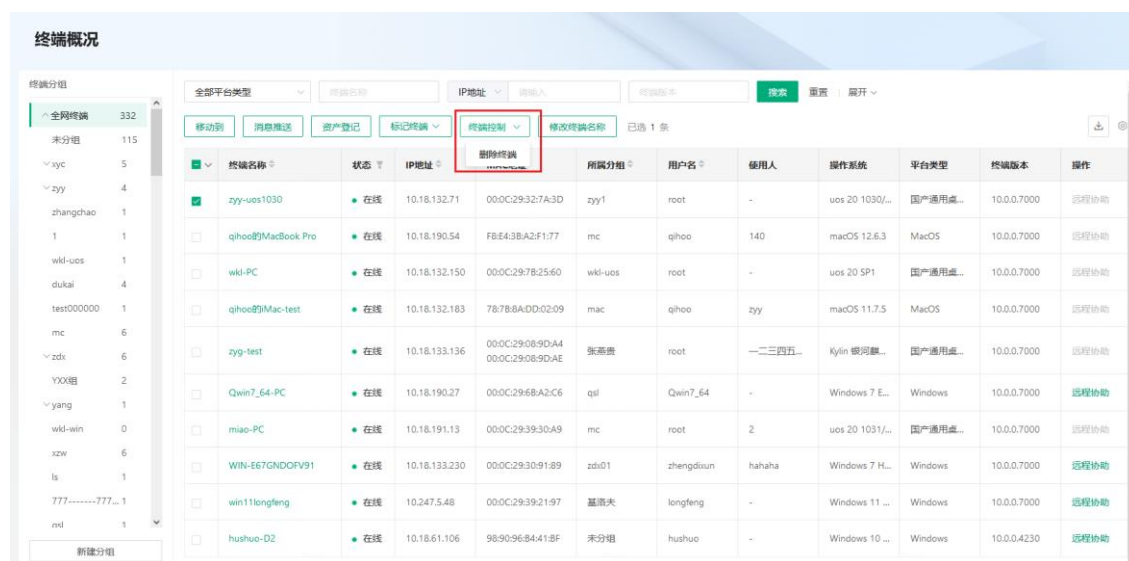
已审批状态的终端，不允许用户自行编辑修改，当有修改诉求时，需向管理员发起资产修改的审批流，管理员完成审批后，方可进行修改。



## 4.2.1.4.删除终端

管理员可对离线客户端进行手动删除，删除后该终端的授权将会被回收，被删除终端再次连接管控时，恢复该终端的数据展示。

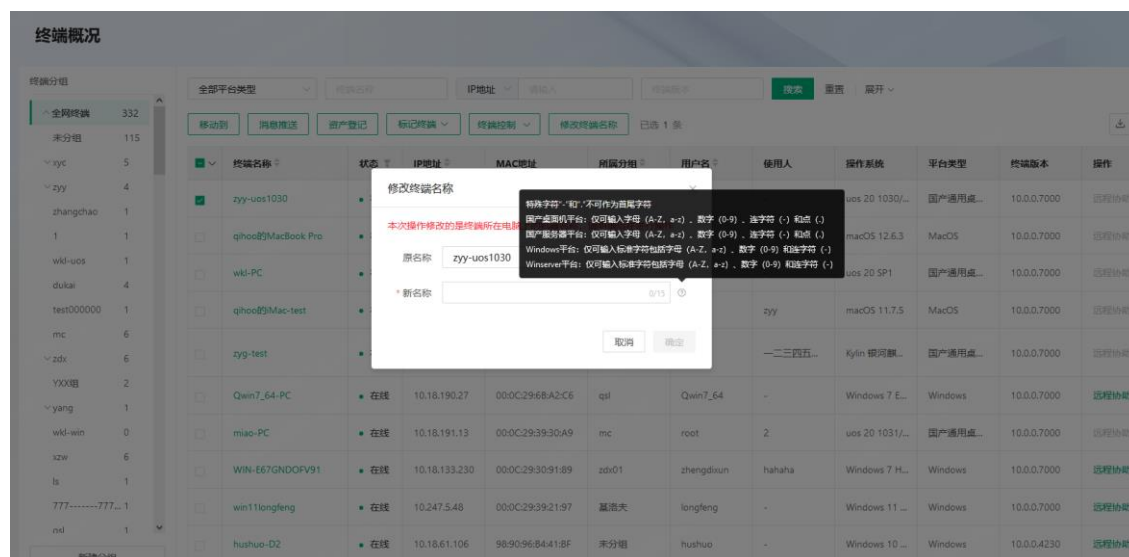
在终端列表中，选择一个或者多个离线终端，点击【删除终端】按钮，可以对目标终端进行删除。



#### 4.2.1.5.修改终端名称

管理员可对终端的计算机名称进行手动修改。

在终端列表中，选择一个终端，点击【修改终端名称】按钮，通过相关配置说明，完成对目标终端计算机名的修改。

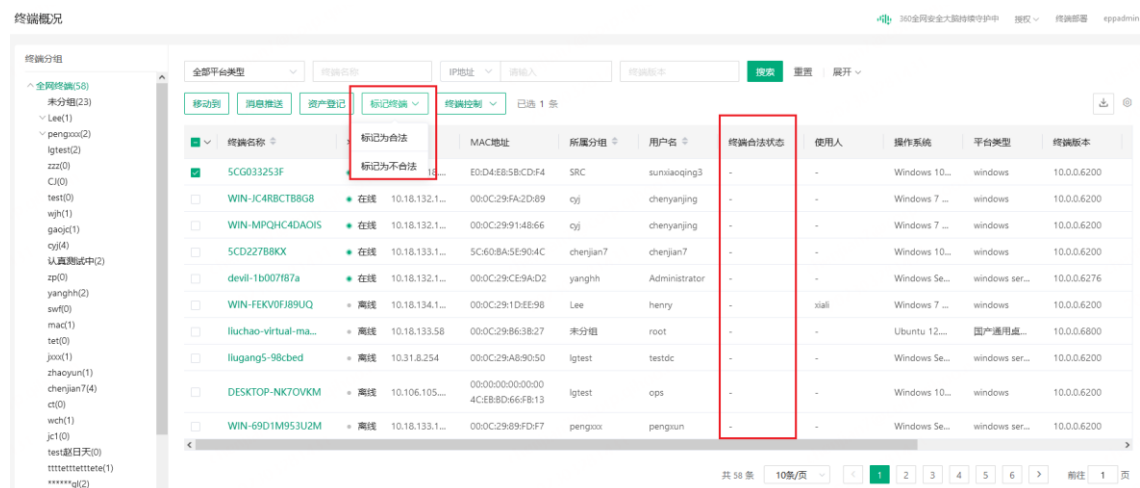


#### 4.2.1.6.标记终端

管理员可对终端的合法状态进行标记，辅助准入管理。

在终端列表中，选择一个或多个终端，点击【标记终端】按钮，对终端进行合法/非法标记。





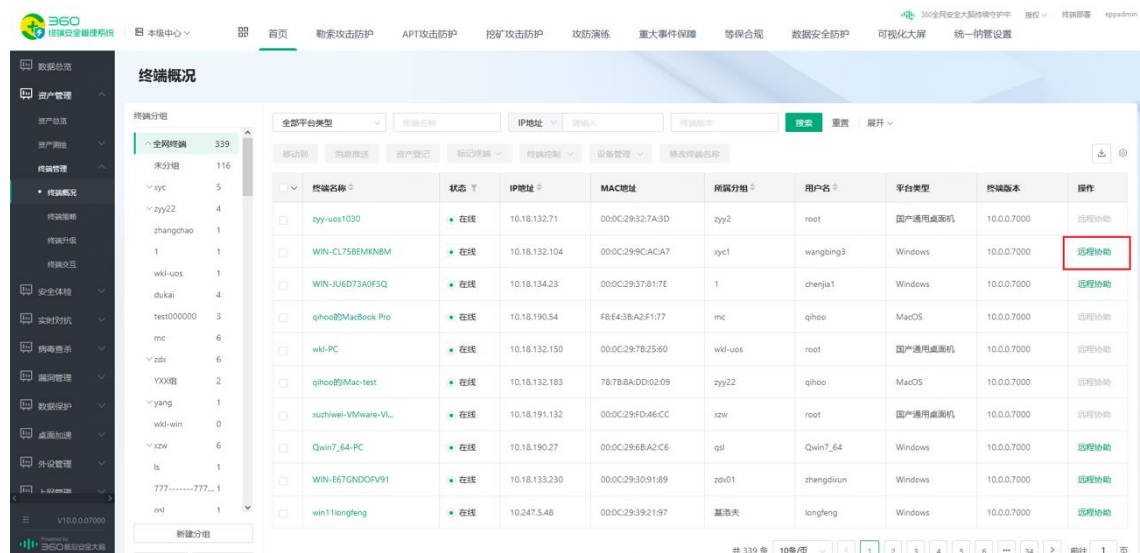
## 4.2.1.7.远程协助

提供远程协助快捷入口，支持快捷对终端执行远程协助。

在终端列表中，对某一个终端，点击【远程协助】按钮，进入该终端的远程协助界面进行远程操作。

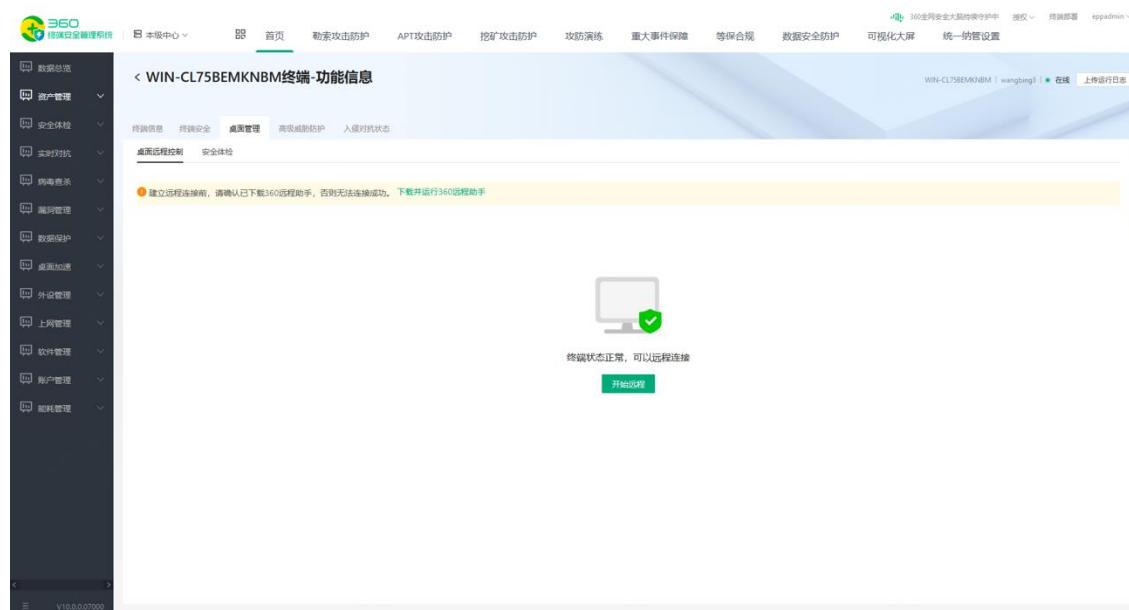
### 1) 远程协助入口

可对 Windows、Winserver、国产通用桌面机类型的设备，发起远程协助。



### 2) 发起远程协助界面





### 3) 远程协助配置界面

管理人员可配置是否需要终端用户确认、以及所使用的连接方式：

桌面远程控制设置

1、在国产终端上登录控制中心，无法对Windows终端进行远程协助。  
2、国产终端选择“发送控制中心本地文件”后，文件将被发送到客户端桌面上的“upload”文件夹中。

终端IP

10.39.86.179

通知方式

☒ 终端同意后执行远程控制
 ☐ 直接执行远程控制

连接方式

☒ 直连
 ☐ 引擎中转
 ☐ 引擎双向中转

远控理由

远程调试

4/20

取消

确定

#### a) 通知方式

- 选择“直接执行远程控制”时，不需要填写远控理由，在网络可连通的情况下，可直接与终端建立远程连接。
- 选择“终端同意后执行远程控制”时，远控理由为必填项，客户端会出现弹窗提示。仅在终端用户同意远程的情况下，才会建立连接。

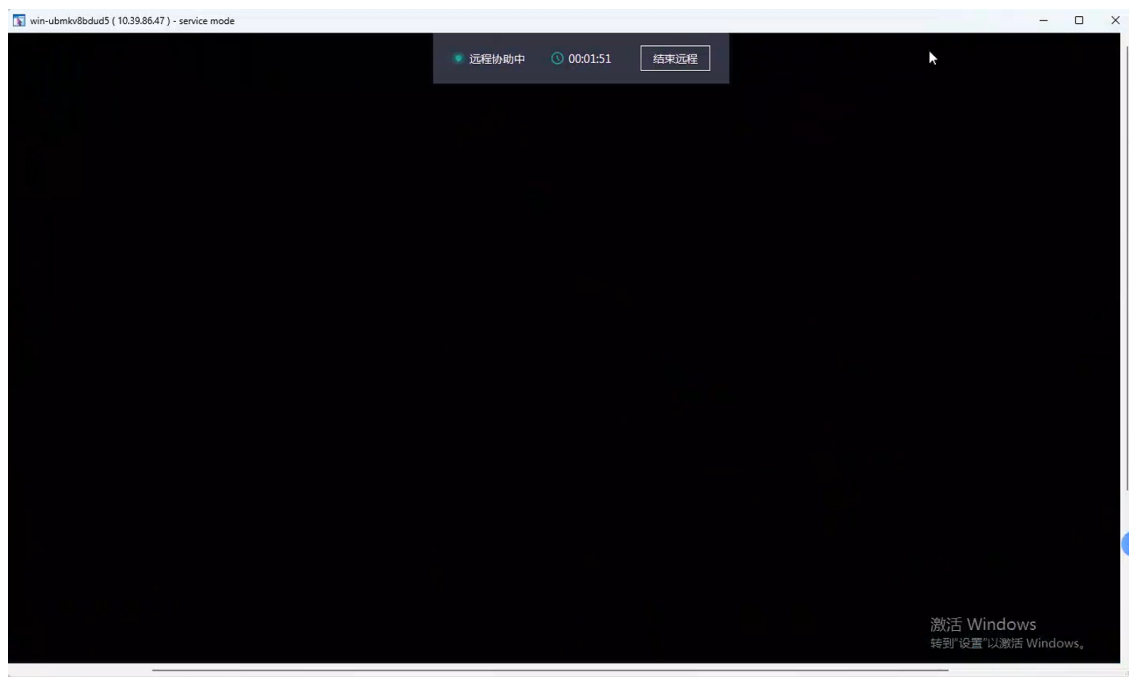


b) 连接方式

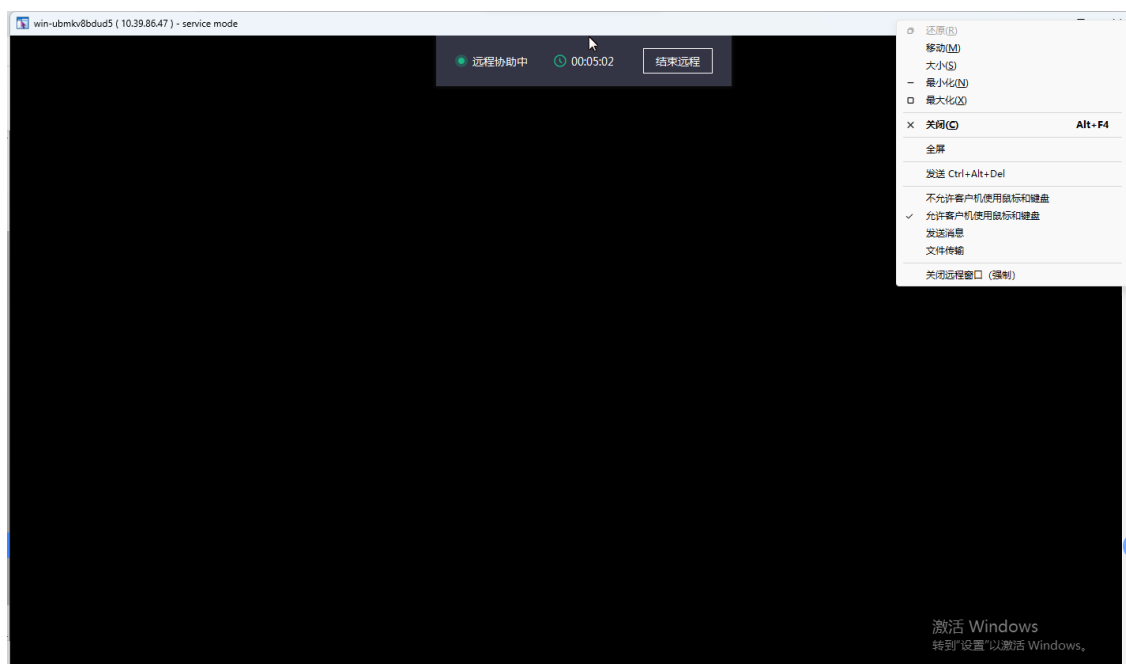
- i. 直连：适用于主控端与被控端网络可连通的环境；
- ii. 引擎中转：适用于主控端与被控端网络不可连通，但控制中心可与主控端和被控端网络连通的环境；
- iii. 引擎双中转：适用于主控端与被控端网络不可连通，并且主控端处于 NAT 网络。但制中心可与主控端和被控端网络连通的环境；

4) 被控端远程效果

a) Windows/Winserver 终端

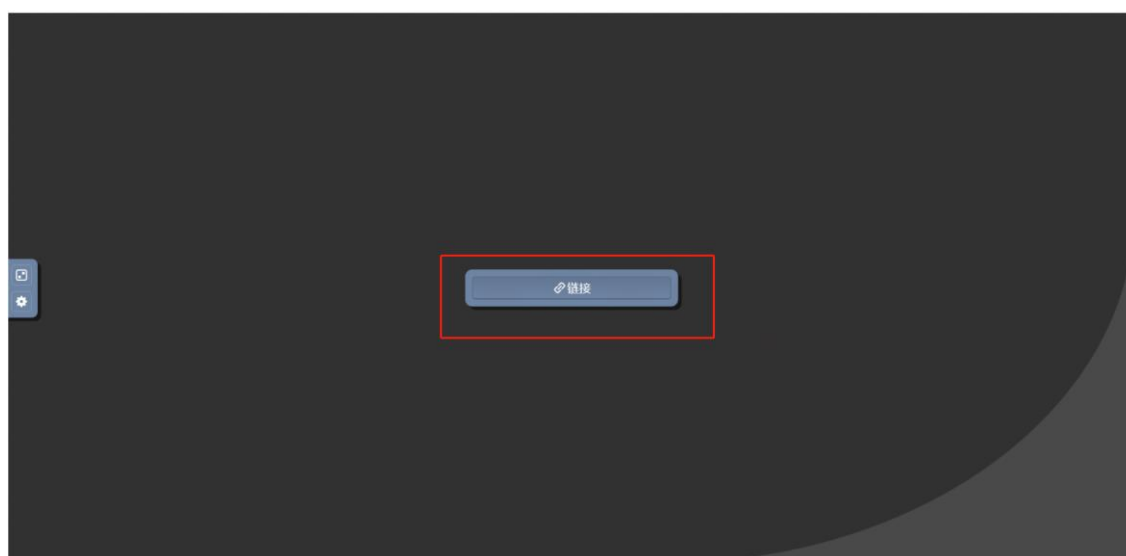


在远程窗体上边栏右键，即调出协助功能项：



b) 国产通用桌面机

点击界面中的【链接】按钮，即可进入远程协助界面。





说明：对于 windows 和 winserver 终端，建立远程连接前，需要先下载 360 远程助手。

## 4.2.2. 终端策略

### 4.2.2.1. 基本设置

#### 4.2.2.1.1. Windows 平台

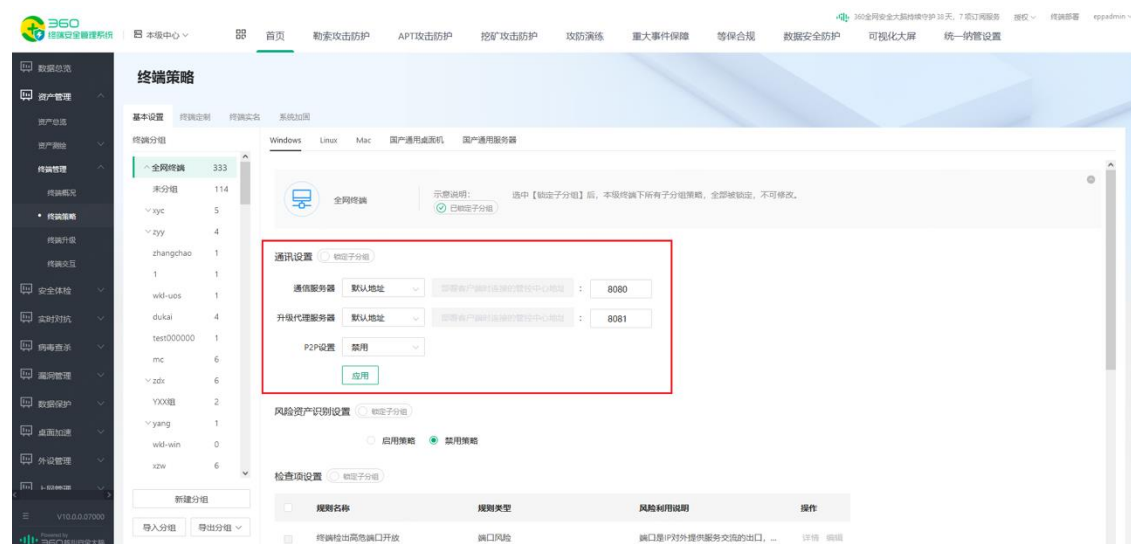
点击左侧功能导航：资产管理〉终端管理〉终端策略〉基本设置〉Windows，进入策略配置界面。

#### 5) 通讯设置

通信服务器：设置内外网 IP、域名，通信生效。

升级代理服务器：设置内外网 IP、域名，客户端升级等功能正常。

支持双网卡环境，因多子网设备连接管控，请使用“默认地址”功能。



## (1) 客户端设置

支持固定密码和动态密码。动态密码每个用户的密码均不同，且每个用户的密码也会随着时间的变化而变化。密码只在一段时间内对某个终端生效。

选择固定密码时，后方出现密码输入框；选择动态密码时，自动隐藏后方密码输入框。支持同时使用固定密码和动态密码。

客户端设置

卸载密码

☐ 固定密码
 

卸载密码

☐ 动态密码
 

应用

退出密码

☐ 固定密码
 

退出密码

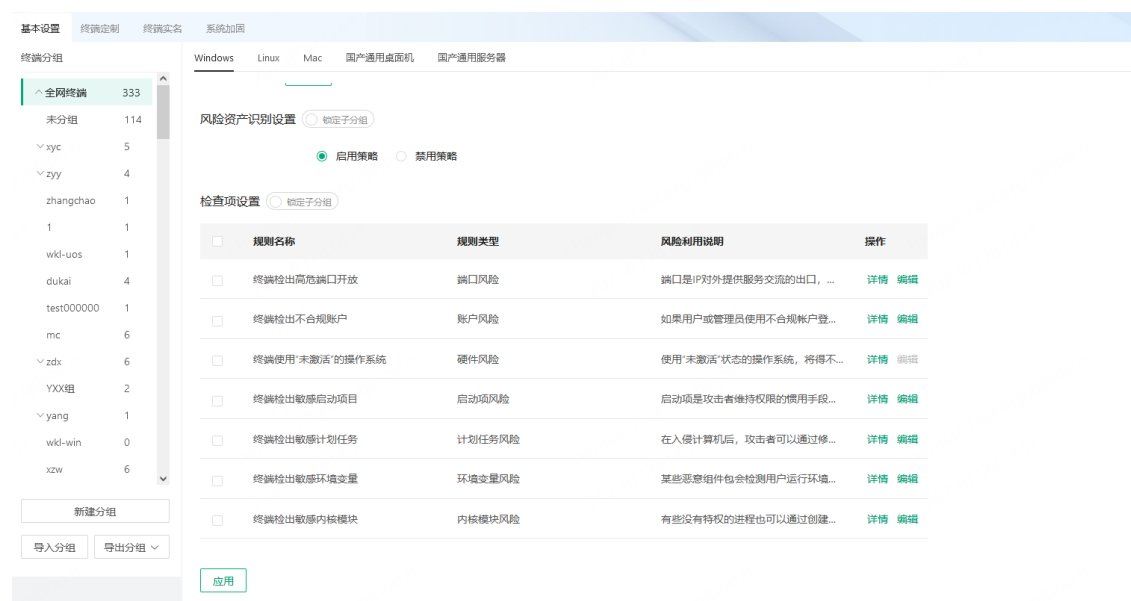
☐ 动态密码
 

应用

说明：6200 版本之前（不包括）的客户端仅支持固定密码；若管控下发动态密码策略，需向管理员获取固定密码；升级后可使用动态密码。

## (2) 风险资产识别设置

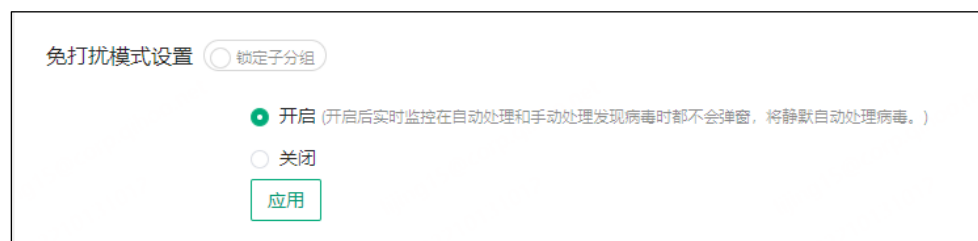
客户端根据策略规则发现风险资产并上报给服务端，支持的风险识别规则有端口风险、账户风险、硬件风险、启动项风险、计划任务风险、环境变量风险、内核模块风险等



### (3) 免打扰模式设置

基本设置中支持免打扰模式设置，免打扰模式开启后，实时监控在自动处理和手动处理发现病毒时都不会弹窗，将静默自动处理病毒；免打扰模式关闭，重启逻辑开启。

客户端扫描到部分病毒时，需要重启彻底清除，并弹窗提示。



### 4.2.2.1.2. Linux 平台

点击左侧功能导航：资产管理〉终端管理〉终端策略〉基本设置〉Linux，进入策略配置界面。

### 6) 通讯设置

通信服务器：设置内外网 IP、域名，通信生效。

升级代理服务器：设置内外网 IP、域名，客户端升级等功能正常。



## 7) 客户端设置

支持固定密码，后方出现密码输入框；

### 4.2.2.1.3. 国产桌面机

点击左侧功能导航：资产管理〉终端管理>终端策略〉基本设置>国产桌面机，进入策略配置界面。

## 8) 通讯设置

通信服务器：设置内外网 IP、域名，通信生效。

升级代理服务器：设置内外网 IP、域名，客户端升级等功能正常。

## 9) 客户端设置

支持固定密码和动态密码。动态密码每个用户的密码均不同，且每个用户的密码也会随着时间的变化而变化。密码只在一段时间内对某个终端生效。

选择固定密码时，后方出现密码输入框；选择动态密码时，自动隐藏后方密码输入框。支持同时使用固定密码和动态密码。

密保密码：设置防止终端修改客户端管控中心地址密码，全局生效

客户端设置
○ 锁定子分组

卸载密码 ②

☐ 固定密码

请输入6-32位字符

☐ 动态密码

应用

退出密码 ②

☐ 固定密码

请输入6-32位字符


☐ 动态密码

应用

管控连接保护

☐ 开启密保后，终端修改管控中心地址需输入以下设置的正确密码

应用

 说明：6200 版本之前（不包括）的客户端仅支持固定密码；若管控下发动态密码策略，需向管理员获取固定密码；升级后可使用动态密码。

## 10) 自我保护设置

国产通用桌面机支持终端“自我保护”功能，为防止信创客户端驱动故障导致系统蓝屏死机，可以通过该功能统一开启或关闭客户端驱动。

该功能有两个开关，“360 自我保护”开关用来开启/关闭客户端的进程保护驱动，还能设置客户端关闭驱动的权限；通过“360 主动防御”开关用来开启/关闭进程管理驱动。

自我保护设置
○ 锁定子分组

360自我保护设置

☒ 开启360自我保护 (防止客户端进程被擅自结束)

☒ 允许客户端修改自我保护设置

360自我保护设置

.....

360主动防御设置

☒ 开启360主动防御 (关闭后进程策略将会失效)

应用

## 11) 带宽设置

设置最大上传速度、最大下载速



带宽设置
☐ 锁定子分组

默认带宽限制

最大上传速度
10240 KB/s

最大下载速度
10240 KB/s

定时带宽设置
 (最多可添加10条定时策略)

时间段	带宽限制	操作
-----	------	----

## 12) 联系管理员

设置姓名、邮箱、电话

联系管理员
☐ 锁定子分组

姓名

电话

邮箱

## 13) 时间同步

设置管控平台时间同步、NTP 时间同步

时间同步
☐ 锁定子分组

☒ 开启
☐ 关闭

☒ 管控平台时间同步
☐ NTP时间同步

最长同步间隔
 分钟

### 4.2.2.1.4. 国产服务器

点击左侧功能导航：资产管理>终端管理>终端策略>基本设置>国产桌面机，进入策略配置界面。

## 14) 通讯设置

通信服务器：设置内外网 IP、域名，通信生效。

升级代理服务器：设置内外网 IP、域名，客户端升级等功能正常。

通讯设置

☐ 锁定子分组

通信服务器

默认地址

部署客户端时连接的管控中心地址

:

8080

升级代理服务器

默认地址

部署客户端时连接的管控中心地址

:

8081

应用

## 15) 客户端设置

支持固定密码和动态密码。动态密码每个用户的密码均不同，且每个用户的密码也会随着时间的变化而变化。密码只在一段时间内对某个终端生效。

选择固定密码时，后方出现密码输入框；选择动态密码时，自动隐藏后方密码输入框。支持同时使用固定密码和动态密码。

密保密码：设置防止终端修改客户端管控中心地址密码，全局生效

客户端设置

☐ 锁定子分组

卸载密码

☐ 固定密码

请输入6-32位字符

☐ 动态密码

应用

退出密码

☐ 固定密码

请输入6-32位字符


☐ 动态密码

应用

管控连接保护

☐ 开启密保后，终端修改管控中心地址需输入以下设置的正确密码

应用

 说明：6200 版本之前（不包括）的客户端仅支持固定密码；若管控下发动态密码策略，需向管理员获取固定密码；升级后可使用动态密码。

## 16) 带宽设置

设置最大上传速度、最大下载速



带宽设置 ☐ 锁定子分组

默认带宽限制

最大上传速度  10240 KB/s

最大下载速度  10240 KB/s

定时带宽设置  (最多可添加10条定时策略)

时间段	带宽限制	操作
-----	------	----

## 17) 联系管理员

设置姓名、邮箱、电话



联系管理员 ☐ 锁定子分组

姓名

电话

邮箱

## 18) 时间同步

设置管控平台时间同步、NTP 时间同步



时间同步 ☐ 锁定子分组

☒ 开启 ☐ 关闭

☒ 管控平台时间同步 ☐ NTP时间同步

最长同步间隔  分钟

## 4.2.2.2. 终端定制

### 4.2.2.2.1. Windows 平台

点击左侧功能导航：资产管理>终端管理>终端策略>终端定制>Windows，进入策略配置界面。

## 19) 终端界面定制

可自定义客户端系统图标，包括系统托盘、桌面快捷方式、开始菜单、任务栏等系统图标使用；

可自定义客户端界面内图标，包括客户端首页及部分弹窗界面内图标使用；

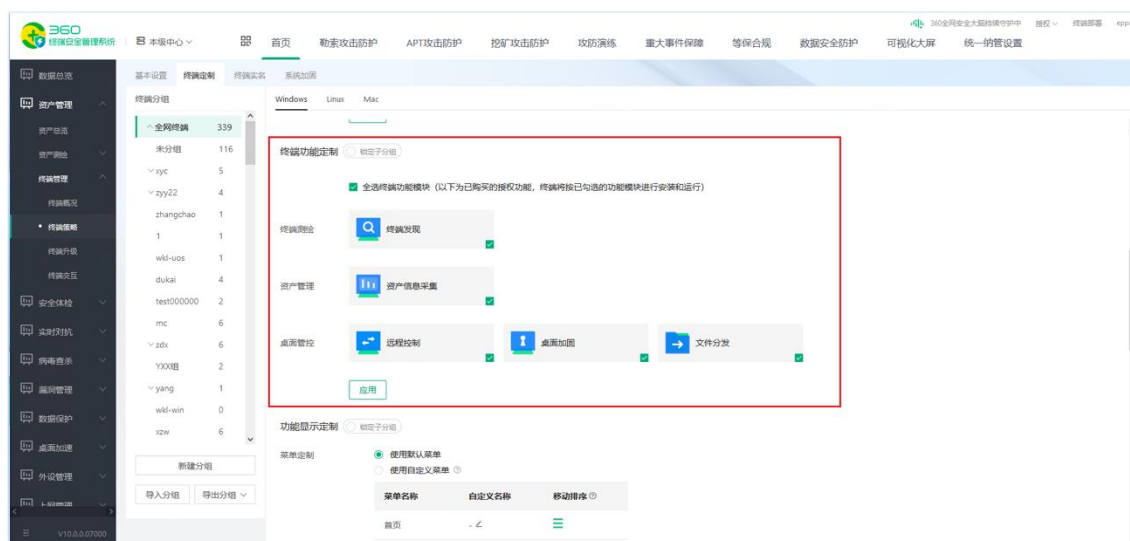
可定制客户端首页主图、客户端首页文案（文字）。



## 20) 终端功能定制

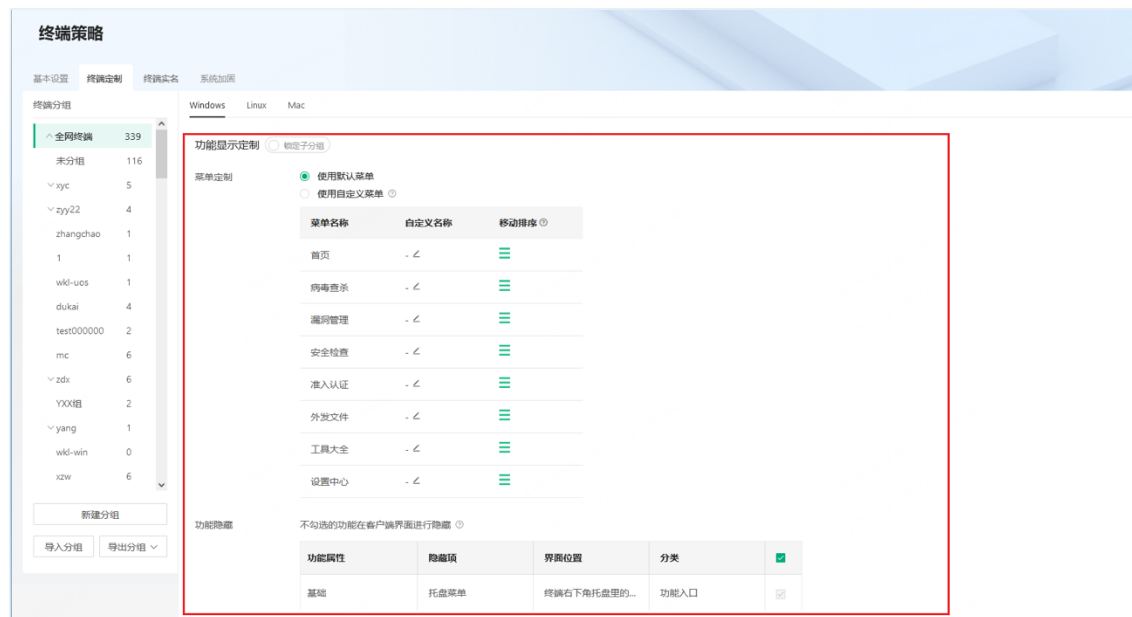
客户端功能支持模块化，管理员可配置客户端安装的功能模块。

根据下发的授权功能，客户端安装/卸载对应的功能。



## 21) 功能显示定制

可对客户端功能菜单名称和位置进行自定义；对客户端版权信息、设置项等内容进行自定义。



#### 4.2.2.2.2. Linux 平台

点击左侧功能导航：资产管理>终端管理>终端策略>终端定制>Linux，进入策略配置界面。

#### 22) 终端功能定制

客户端功能支持模块化，管理员可配置客户端安装的功能模块。

根据下发的授权功能，客户端安装/卸载对应的功能。



#### 4.2.2.2.3. Mac 平台

点击左侧功能导航：资产管理〉终端管理〉终端策略〉终端定制〉Mac，进入策略配置界面。

## 23) 终端界面定制

Mac 平台的客户端能够自定义产品 logo、产品名称和首页主图。管理员需完成终端界面定制策略并下发应用后，该分组下的终端将会根据策略约束完成相应 logo/品名/主图的替换显示。



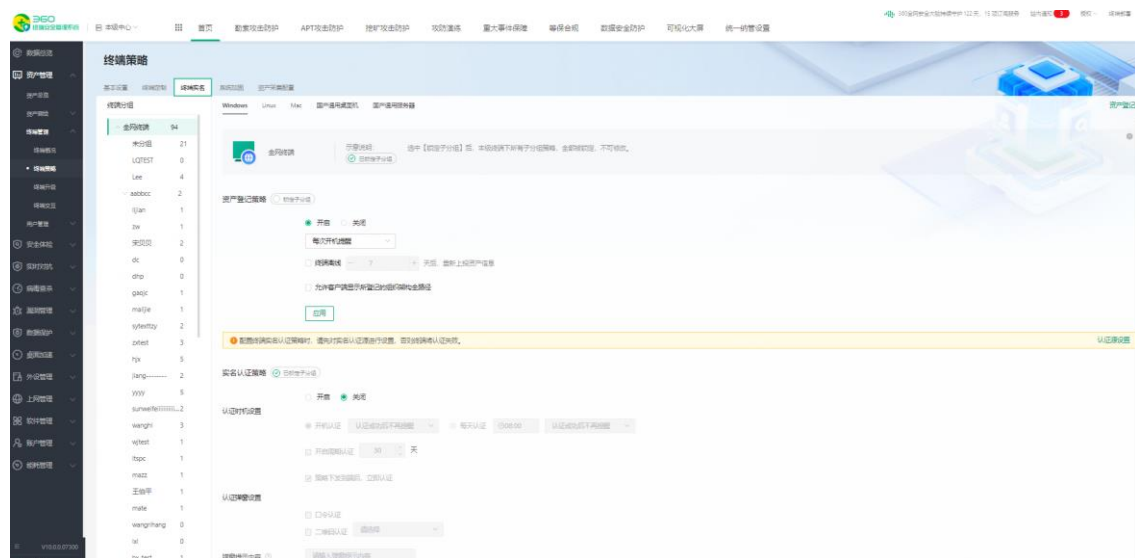
## 4.2.2.3. 终端实名

### 4.2.2.3.1. Windows 平台

点击左侧功能导航：资产管理〉终端管理〉终端策略〉终端实名〉Windows，进入策略配置界面。

#### (1) 资产登记策略

资产登记策略开启，终端将根据策略配置进行弹窗提示。支持终端离线 xx 天后，重新上报资产信息。



## (2) 实名认证策略

Windows 支持实名认证功能，支持从 LDAP 等第三方认证源同步组织架构、用户信息到终端分组中；支持（Windows 终端）进行周期认证、开机认证；支持终端入域后自动认证；支持不认证禁用电脑，禁用后支持密码逃生；支持认证后在管控中心实现人机绑定；自动调整终端到对应分组；自动关联显示从第三方认证源中同步过来的用户属性信息。

1) 认证开关：支持选择开启或关闭，管理员可根据需求下发策略。默认关闭，关闭后不再进行实名认证，实名认证配置选项禁用配置且功能不生效。

2) 认证时机设置：

认证时机设置主要是完成对客户端弹窗时机的配置。支持两种周期性认证时机，默认选中“开机认证-认证成功后不再提醒模式”。

A. 开机认证：

认证成功后不再提醒：客户端未完成实名认证前，每次开机（启动 360epp 进程）即弹框（实名认证弹窗）；

每次开机都认证：此模式下，终端（无论是否已认证）在每次开机时，需将客户端认证状态置为“未认证”并向服务端反馈，而后强制弹窗进行认证。若认证成功，则向管控反馈认证状态及认证用户信息；若认证失败或关闭弹窗不做认证，则保持该终端为“未认证”状态。

B. 每天认证：

认证成功后不再提醒：客户端未完成实名认证前，每天 X 点弹窗认证。弹窗的具体时间可配置；

每天定时认证：此模式下，终端（无论是否已认证）在每天的 X 时，需将客户端认证状态

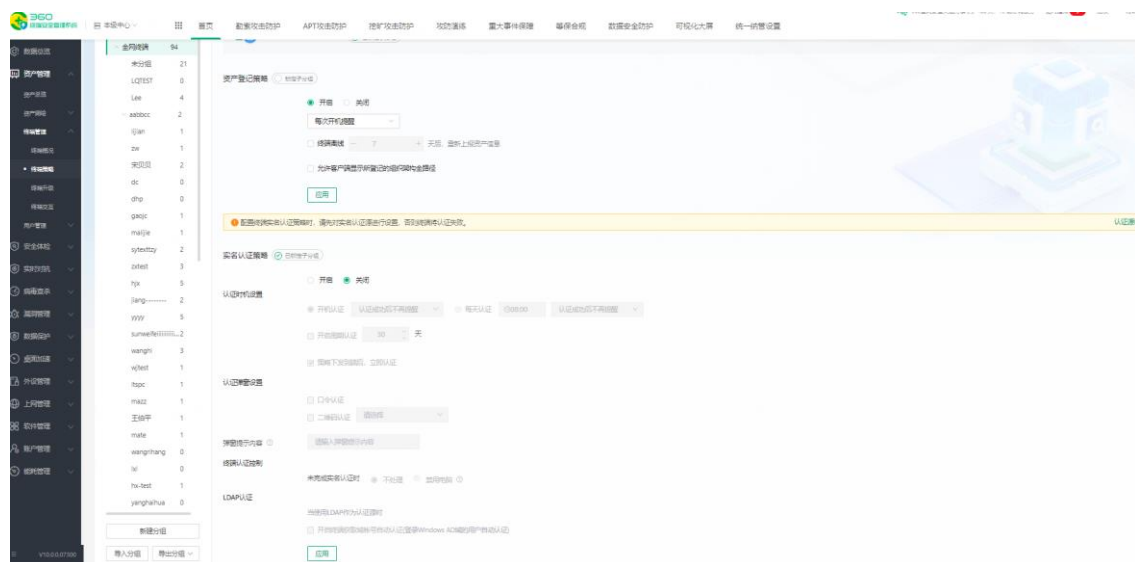
置为“未认证”并向服务端反馈，而后强制弹窗进行认证。若认证成功，则向管控反馈认证状态及认证用户信息；若认证失败或关闭弹窗不做认证，则保持该终端为“未认证”状态。

### 3) 终端认证控制：

支持对于未完成实名认证的终端，制定相应的管理措施。例如不处理和禁用电脑等措施；支持逃逸密码进行逃生。

支持选择未完成认证的处理方式，默认选中“不处理”方式。选择“不处理”模式时，若客户端未完成实名认证，仍可正常使用客户端和终端，认证弹窗可关闭。选择“禁用电脑”模式时，若客户端未完成实名认证，实名认证窗口强制置顶锁屏，只允许终端用户具备完成实名认证相关的操作和能力；完成实名认证后，自动解除控制，终端恢复正常使用。

点击【应用】按钮后，完成策略的保存和应用执行。



### 4.2.2.3.2. Linux 平台



支持 Linux 资产登记设置。





点击左侧功能导航：**资产管理**〉**终端管理**〉**终端策略**〉**终端实名**〉**Mac**，进入策略配置界面。

支持 Mac 平台的客户端能够进行资产登记。资产登记策略与 Windows 平台策略一致，管理员可配置策略开关、登记提醒时机和资产登记有效期。管理员完成策略配置下发应用到客户端后，终端根据弹窗提示进行资产登记和资产信息查看。

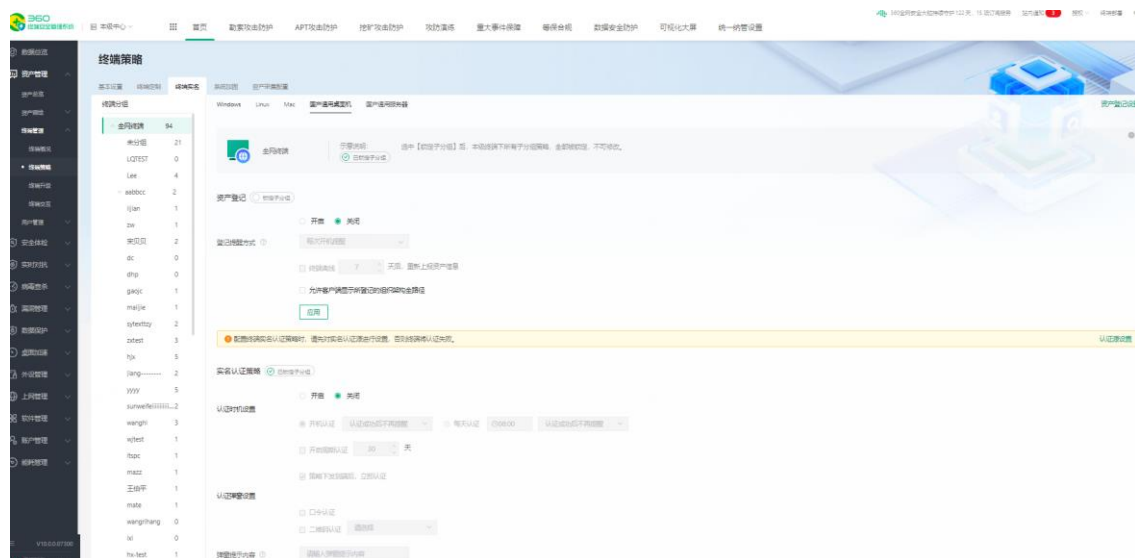


#### 4.2.2.3.4. 国产桌面机

点击左侧功能导航：**资产管理**〉**终端管理**〉**终端策略**〉**终端实名**〉**国产桌面机**，进入策略配置界面。

##### (1) 资产登记策略

管理员可配置策略开关、登记提醒时机和资产登记有效期。管理员完成策略配置下发应用到客户端后，终端根据弹窗提示进行资产登记和资产信息查看。



##### (2) 实名认证策略

信创支持实名认证功能，支持从 LDAP 等第三方认证源同步组织架构、用户信息到终端分组中；支持进行周期认证、开机认证；支持认证后在管控中心实现人机绑定；自动调整终端到对应分组；自动关联显示从第三方认证源中同步过来的用户属性信息。

1) 认证开关：支持选择开启或关闭，管理员可根据需求下发策略。默认关闭，关闭后不再进行实名认证，实名认证配置选项禁用配置且功能不生效。

2) 认证时机设置：

认证时机设置主要是完成对客户端弹窗时机的配置。支持两种周期性认证时机，默认选中“开机认证-认证成功后不再提醒模式”。

#### C. 开机认证：

认证成功后不再提醒：客户端未完成实名认证前，每次开机（启动 360epp 进程）即弹框（实名认证弹窗）；

每次开机都认证：此模式下，终端（无论是否已认证）在每次开机时，需将客户端认证状态置为“未认证”并向服务端反馈，而后强制弹窗进行认证。若认证成功，则向管控反馈认证状态及认证用户信息；若认证失败或关闭弹窗不做认证，则保持该终端为“未认证”状态。

#### D. 每天认证：

认证成功后不再提醒：客户端未完成实名认证前，每天 X 点弹窗认证。弹窗的具体时间可配置；

每天定时认证：此模式下，终端（无论是否已认证）在每天的 X 时，需将客户端认证状态置为“未认证”并向服务端反馈，而后强制弹窗进行认证。若认证成功，则向管控反馈认证状态及认证用户信息；若认证失败或关闭弹窗不做认证，则保持该终端为“未认证”状态。

点击【应用】按钮后，完成策略的保存和应用执行。

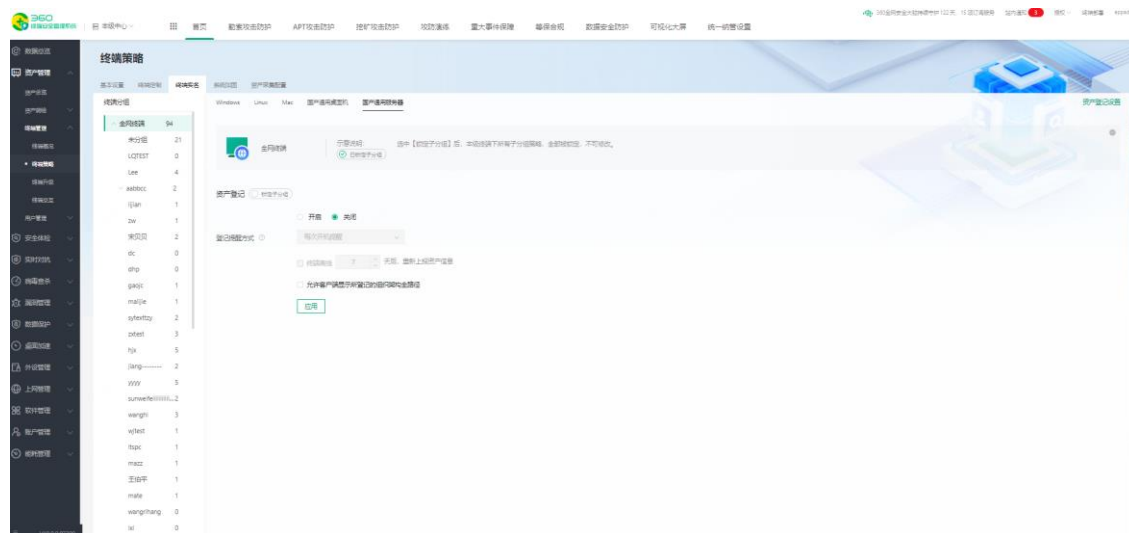
The screenshot shows the '实名认证策略' (Real-name Authentication Strategy) configuration page. At the top, there are radio buttons for '开启' (Enabled) and '关闭' (Disabled), with '开启' selected. Below this is a dropdown menu for '认证方式' (Authentication Method) set to '每次开机提醒' (Remind every time the machine starts). There are also checkboxes for '终端离线' (Terminal Offline) and '允许客户端显示所登记的组织架构全路径' (Allow client to display the full path of the registered organizational structure), both currently unchecked. An '应用' (Apply) button is visible. A yellow warning bar states: '配置终端实名认证策略时，请先对实名认证源进行设置，否则终端将认证失败。' (When configuring the real-name authentication strategy for the terminal, please set the real-name authentication source first, otherwise the terminal authentication will fail). The main configuration area is titled '实名认证策略' and includes a '锁定子分组' (Lock sub-group) button. It has radio buttons for '开启' (Selected) and '关闭'. Under '认证时机设置' (Authentication Timing Settings), there are three options: '开机认证' (Selected) with a dropdown '认证成功后不再提醒' (No reminder after successful authentication), '每天认证' (Daily authentication) with a time picker '08:00', and '认证成功后不再提醒' (No reminder after successful authentication). There is also a checkbox for '开启周期认证' (Enable periodic authentication) set to '30' days. A checked checkbox '策略下发到端后，立即认证' (Authenticate immediately after policy is pushed to the terminal) is present. Under '认证弹窗设置' (Authentication Popup Settings), there are checkboxes for '口令认证' (Password authentication) and '二维码认证' (QR code authentication), both unchecked. At the bottom, there is a text input field for '弹窗提示内容' (Popup prompt content) and an '应用' (Apply) button.

#### 4.2.2.3.5. 国产服务器

点击左侧功能导航：资产管理〉终端管理〉终端策略〉终端实名〉国产服务器，进入策略配置界面。

## (1) 资产登记策略

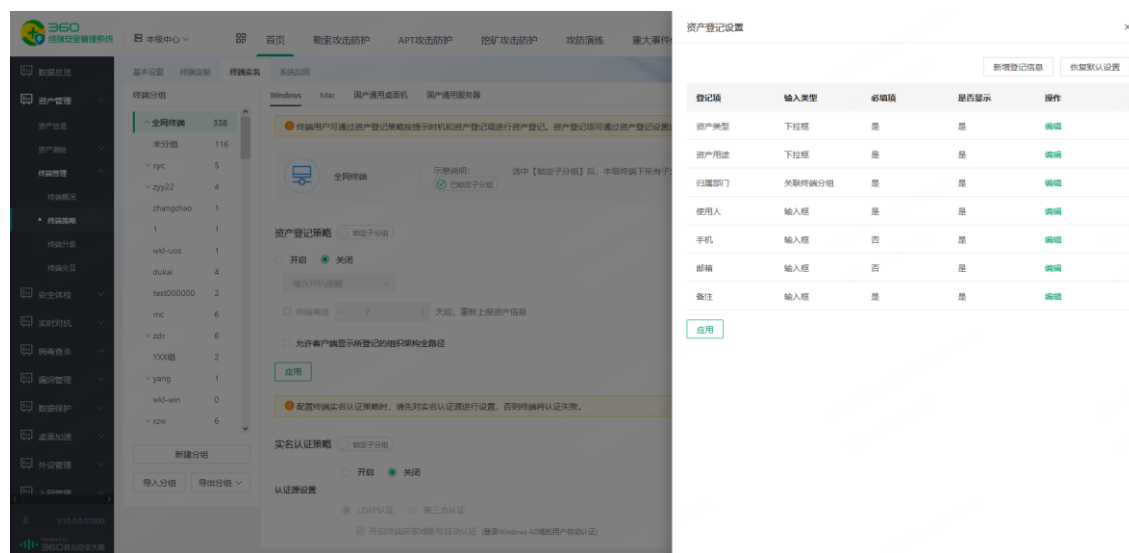
管理员可配置策略开关、登记提醒时机和资产登记有效期。管理员完成策略配置下发应用到客户端后，终端根据弹窗提示进行资产登记和资产信息查看。



### 4.2.2.3.6. 资产登记设置

点击左侧功能导航：**资产管理**〉**终端管理**〉**终端策略**〉**终端实名**，进入策略配置界面，点击“资产登记”设置，抽屉显示设置页面。

#### (1) 资产登记项



该页面提供默认字段作为缺省，管理员可根据需要自行配置资产登记所需字段

登记项	输入类型	必填项	是否显示	操作
资产类型	下拉框	是	是	编辑
资产用途	下拉框	是	是	编辑
归属部门	关联终端分组	是	是	编辑

添加登记信息

\* 登记项名称

是否必填项

☒ 是 ☐ 否

客户端显示

☒ 显示 ☐ 不显示

输入类型

☒ 输入框 ☐ 下拉框

取消

确定

### (2) 资产登记提醒

支持对终端资产登记时的提示信息进行设置，方便终端用户填写时，作为参照信息或登记要求。

### (3) 资产登记审批

系统提供自动审批和手动审批两种审批模式，默认为自动审批模式，不需管理员干预。当管理员有强管控的诉求时，可转为手动审批模式，对资产登记信息进行管控。

360

终端安全管理系统

本级中心

首页

勒索攻击防护

APT攻击防护

挖矿攻击防护

攻防演练

重大事件

数据总览

资产管理

终端策略

终端实名

终端加固

终端防护

终端检测

终端响应

终端修复

终端迁移

终端备份

终端还原

终端升级

终端卸载

终端重装

终端迁移

终端备份

终端还原

终端升级

终端卸载

终端重装

终端策略

终端实名

终端加固

终端防护

终端检测

终端响应

终端修复

终端迁移

终端备份

终端还原

终端升级

终端卸载

终端重装

资产登记设置

新增登记项

你默认设置

登记项	输入类型	必填项	是否显示	操作
资产类型	下拉框	是	是	编辑
资产用途	下拉框	是	是	编辑
归属部门	关联终端分组	是	是	编辑
使用人	输入框	是	是	编辑
手机	输入框	否	是	编辑
邮箱	输入框	否	是	编辑
备注	输入框	是	是	编辑
423	输入框	是	是	编辑 删除
243	输入框	是	是	编辑 删除

应用

登记提醒设置

☒ 开启 ☐ 关闭

登记提醒---请及时填写/修改资产信息-会实时弹窗提醒用户

应用

登记审批设置

☒ 自动审批 ☐ 手动审批

应用

## 4.2.2.3.7. 实名认证源设置

点击左侧功能导航：资产管理>终端管理>终端策略>终端实名，进入策略配置界面，点击“认证源设置”，抽屉显示设置页面。

### (1) 认证源开关

实名认证源的开关控制，默认为关闭状态。

## （2）认证源选择

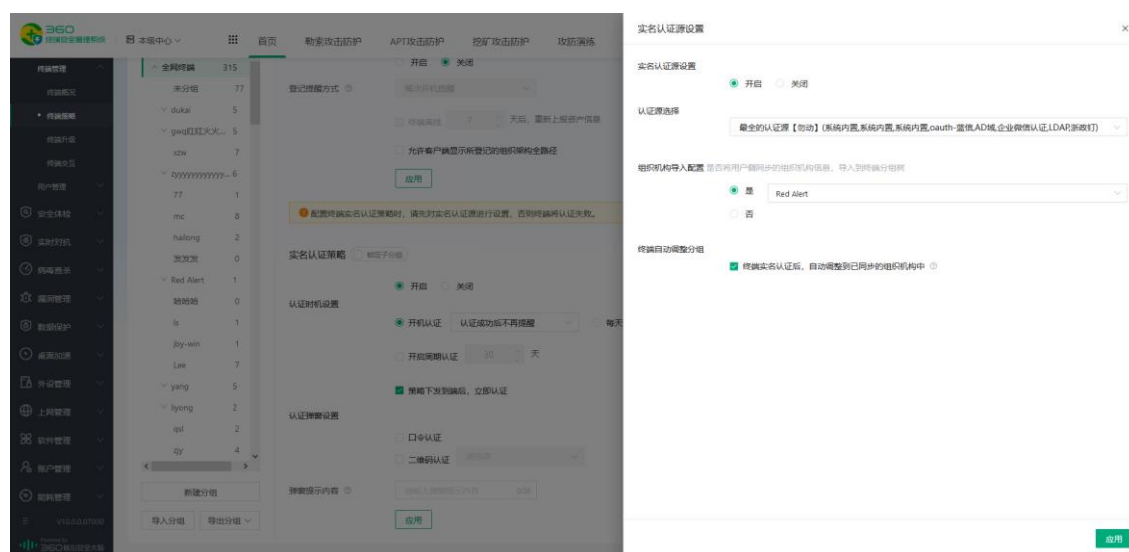
对接用户管理-身份认证模块，从中选取实名认证需要的认证源，客户端发起认证后，通过身份认证服务向选中的认证源发起认证。

## （3）组织机构导入

支持将从第三方同步的组织机构，导入到终端分组树中。

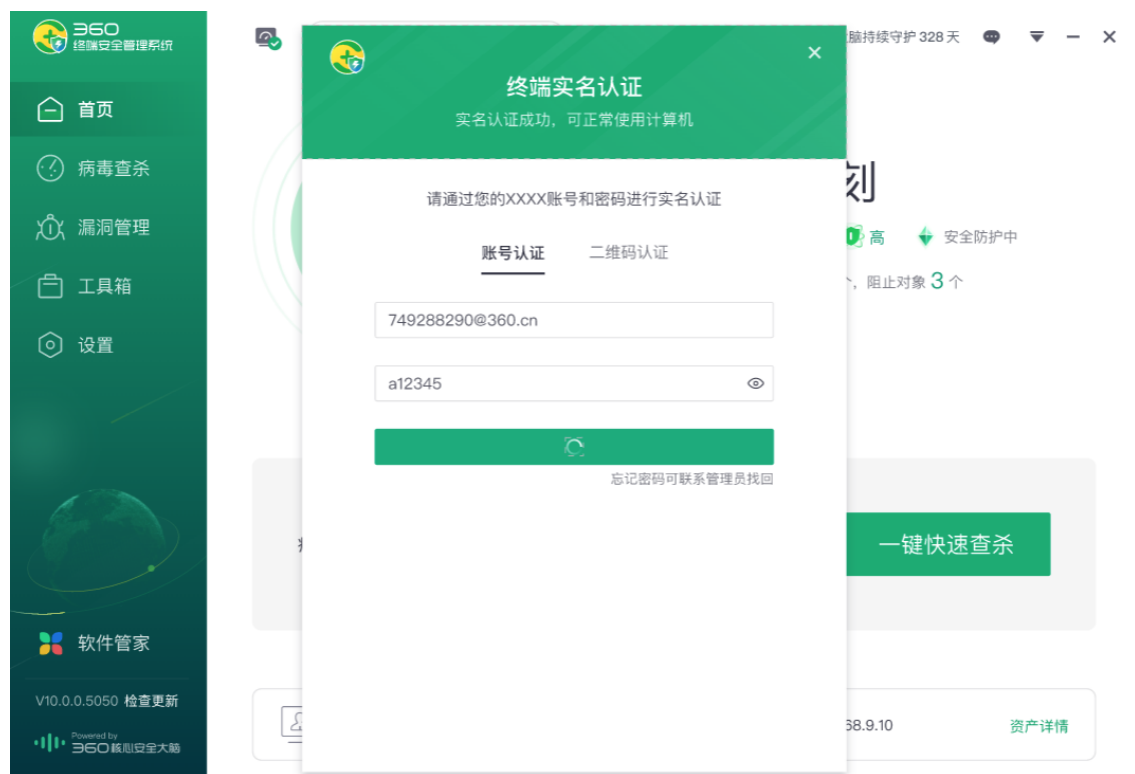
## （4）自动调整分组

支持终端完成实名认证后，自动将分组挪到已导入的组织机构下。



### 4.2.2.3.8. 客户端实名认证

客户端依托分组策略，触发实名认证，进行相关认证操作。发起认证后，通过认证服务，将用户提交的认证信息进行校验，认证完成后进行结果查看。



#### 4.2.2.3.9. 客户端资产登记

客户端依托分组策略或管理员下发，触发资产登记，进行相关登记操作。终端用户在客户端填写资产登记信息提交后，会在管控中心生成一条资产登记申请信息，管理员完成审批后，终端资产登记状态才为“已审批”状态。

已审批状态的终端，不允许用户自行编辑修改，当有修改诉求时，需向管理员发起资产修改的审批流，管理员完成审批后，方可进行修改。

[illegible]

点击左侧功能导航：资产管理>终端管理>终端策略>系统加固>Windows，进入策略配



### (1) 账户密码策略

开启密码复杂度“不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分，至少有六个字符长，包含以下四类字符中的三类字符：英文大写字母（A 到 Z）、英文小写字母（a 到 z）、10 个基本数字（0 到 9）、非字母字符（例如！、#、¥、%）”检查；

帐户密码策略

☐ 锁定子分组

帐户安全

☐ 开启

☒ 关闭

☐ 帐户锁定阈值

0

次无效登录 (0则永不锁定)

☐ 帐户锁定时间

0

分钟 (0则一直锁定直到管理员解除锁定)

☐ GUEST帐户状态

禁用

☐ 提升帐户权限

禁止

☐ 增加/删除账号

禁止

☐ 本地管理员帐户状态

启用

②

密码安全

☐ 开启

☒ 关闭

☐ 密码长度最小值

7

个字符 ②

☐ 密码最长使用期限

42

天 ②

☐ 密码最短使用期限

0

天 (0则可随时更改密码)

☐ 强制密码历史

24

个记住的密码

☐ 密码复杂性要求

禁用

(在更改或创建密码时执行)

☐ 用可还原的加密方法存储密码

禁用

---

45

弱口令检测
☐ 开启
☒ 关闭

☒ 启用内置弱密码库 (将按照系统内置的万级弱密码库进行检测)

☐ 启用自定义弱密码库

当密码不符合要求时
请选择
(终端重启后开始检查)

终端提示信息
系统检测到您当前登录账号密码不符合要求, 为保障系统安全, 请您重新设置密码。

## (2) 屏保壁纸策略

屏幕保护：设定屏幕保护，保护终端安全。

屏保壁纸策略：管理可以对终端桌面壁纸进行设置。

屏保壁纸策略
☐ 锁定子分组

☐ 开启
☒ 关闭

☒ 启用屏幕保护设置

等待时间
10
分钟后进入屏保

☐ 在恢复时显示登录屏幕

上传屏保文件

☒ 壁纸状态
不限制壁纸

## (3) 控制面板策略

支持开启或禁用用户账户、添加/删除程序、网络共享中心、个性化、管理工具、日期和时间等；支持开启或禁用安全模式，可设置安全模式登录密码。

控制面板策略
☐ 锁定子分组

☐ 开启
☒ 关闭

☐ 用户帐户
禁用

☐ 添加/删除程序
禁用

☐ 网络共享中心
禁用

☐ 个性化
禁用

☐ 管理工具
禁用

☐ 日期和时间
禁用

☐ 安全模式
禁用

## (4) 本地安全策略

支持开启或禁用组策略编辑器、注册表编辑器、阻止添加打印机、关闭系统还原、系统共享、用户共享、任务管理器、账户自动登录、远程修改注册表、远程协助、远程桌面、系统防

防火墙、U 盘自动播放等本地安全策略；支持开启或禁用终端审核策略，审核内容包括审核策略更改、审核登录事件、审核对象访问、审核进程跟踪、审核目录服务访问、审核特权使用、审核系统事件、审核账户登录事件、审核账户管理等。

本地安全策略 ☐ 锁定子分组

☐ 开启 ☒ 关闭

<input type="checkbox"/> 组策略编辑器	禁用	<input type="checkbox"/> 注册表编辑器	禁用
<input type="checkbox"/> 阻止添加打印机	禁用	<input type="checkbox"/> 关闭系统还原	禁用
<input type="checkbox"/> 系统共享	禁用	<input type="checkbox"/> 用户共享	禁用 (终端将不可主动发布共享文件夹)
<input type="checkbox"/> 任务管理器	禁用	<input type="checkbox"/> 帐户自动登录	禁用 (终端需输入用户名和密码才可登录)
<input type="checkbox"/> 远程修改注册表	禁用	<input type="checkbox"/> 远程协助	禁用
<input type="checkbox"/> 远程桌面	禁用	<input type="checkbox"/> 系统防火墙	禁用 可能造成安全威胁!
<input type="checkbox"/> U盘自动播放	禁用	<input type="checkbox"/> 终端审核策略	审核内容设置

## (5) 浏览器安全策略

可设置 IE 浏览器的 Internet 安全级别、本地安全级别设置，可禁止使用 IE 代理。

浏览器安全策略 ☐ 锁定子分组

☐ 开启 ☒ 关闭

<input type="checkbox"/> Internet安全级别	中高	(适用于大多数网站，下载潜在不安全内容前提示。)
<input type="checkbox"/> 本地安全级别	中低	(适用于本地网络上的网站，大多数内容运行没有提示，除了没有提示外，其他与中等级别安全级相同。)
<input type="checkbox"/> 代理设置	禁止使用代理	

## 4.2.2.4.2. 国产桌面机

管理员可以对全网终端账户密码进行管控，设置帐户密码、帐户安全、密码安全、弱口令、自定义弱密码、锁屏、壁纸。

点击左侧功能导航：**资产管理》终端管理>终端策略》系统加固>国产桌面机**，进入策略配置界面。

### (1) 帐户密码

开启密码复杂性，桌面加固策略下发到信创客户端，策略生效（包括账户安全、密码安全、弱口令提醒）；关闭密码复杂性要求，桌面加固策略下发到信创客户端，桌面加固所有设置都不再生效；

### (2) 账户安全

开启账户安全，系统开启输入账号错误次数、锁定时间、是否可添加删除账号，都响应策略设置；关闭账户安全策略，系统开机输入错误密码锁定次数和时间已经是否能添加删除账号不再受管控控制；

### (3) 密码安全

开启密码安全，修改或者新建系统账号时，密码最小长度、密码有效期限、不能使用 X 个历史密码都响应管控设置值；关闭密码安全，修改或者新建系统账号时，密码可任意设置，不再受管控控制；

### (4) 弱口令

开启弱口令提醒策略，当信创系统密码命中弱密码库时，开机会在右下角提醒弱密码；关闭弱口令提醒，开机不会有弱密码弹窗；

### (5) 自定义弱密码

设置自定义弱密码，信创系统密码符合自定义弱密码规则会在开机时弹窗提醒；删除自定义弱密码管控响应正常；

### (6) 锁屏

可设置终端在指定时间范围内，没有操作，即进入锁屏状态。

### (7) 壁纸

设置终端显示的壁纸，所设置的壁纸将按照填充模式做展示。

Windows 国产通用桌面机 国产通用服务器

帐户密码

☐ 锁定子分组

☐ 密码复杂性要求 (在更改或创建密码时执行)

1、密码不能包含用户的帐户名  
 2、至少六个字符，且最少含以下四类中的三类字符：大写字母、小写字母、数字（0到9）、非字母字符（如！#%）

帐户安全

☐ 锁定子分组

帐户锁定阈值  次无效登录

帐户锁定时间  分钟

☒ 允许增加删除帐号

密码安全

☐ 锁定子分组

最小长度  位

最长使用期限  天

强制密码历史  个记住密码

弱口令

☐ 锁定子分组

☒ 弱口令密码检测 (用户登录时检测)

☒ 启用自定义弱密码库

☒ 当密码不符合要求时仅消息提示

自定义弱密码

☐ 锁定子分组

弱密码	添加时间	管理员	操作
暂无数据			

壁纸策略

☐ 锁定子分组

壁纸设置 ☒ 开启 ☐ 关闭

上传壁纸

示例壁纸

锁屏策略

☐ 锁定子分组

锁屏设置 ☒ 开启 ☐ 关闭

终端  分钟内无操作时，进入锁屏状态。

#### 4.2.2.4.3. 国产服务器

管理员可以对全网终端账户密码进行管控，设置帐户密码、帐户安全、密码安全、弱口

令、自定义弱密码。

点击左侧功能导航：**资产管理》终端管理>终端策略》系统加固>国产桌面机**，进入策略配置界面。

#### (1) 帐户密码

开启密码复杂性，桌面加固策略下发到信创客户端，策略生效（包括账户安全、密码安全、弱口令提醒）；关闭密码复杂性要求，桌面加固策略下发到信创客户端，桌面加固所有设置都不再生效；

#### (2) 账户安全

开启账户安全，系统开启输入账号错误次数、锁定时间、是否可添加删除账号，都响应策略设置；关闭账户安全策略，系统开机输入错误密码锁定次数和时间已经是否能添加删除账号不再受管控控制；

#### (3) 密码安全

开启密码安全，修改或者新建系统账号时，密码最小长度、密码有效期限、不能使用 X 个历史密码都响应管控设置值；关闭密码安全，修改或者新建系统账号时，密码可任意设置，不再受管控控制；

#### (4) 弱口令

开启弱口令提醒策略，当信创系统密码命中弱密码库时，开机会在右下角提醒弱密码；关闭弱口令提醒，开机不会有弱密码弹窗；

#### (5) 自定义弱密码

设置自定义弱密码，信创系统密码符合自定义弱密码规则会在开机时弹窗提醒；删除自定义弱密码管控响应正常；

帐户密码

已继承策略

自定义策略

☐ 密码复杂性要求 (在更改或创建密码时执行)

1、密码不能包含用户的帐户名

2、至少六个字符，且最少含以下四类中的三类字符：大写字母、小写字母、数字（0到9）、非字母字符（如！#%）

帐户安全

已继承策略

自定义策略

帐户锁定阈值

5

次无效登录

帐户锁定时间

3

分钟

☒ 允许增加删除帐号

密码安全

已继承策略

自定义策略

最小长度

6

位

最长使用期限

90

天

强制密码历史

3

个记住密码

弱口令

已继承策略

自定义策略

☒ 弱口令密码检测 (用户登录时检测)

☒ 启用自定义弱密码库

☒ 当密码不符合要求时仅消息提示

自定义弱密码

已继承策略

自定义策略

## 4.2.3. 终端升级

### 4.2.3.1. 升级管理

点击左侧功能导航：资产管理〉终端管理>终端升级〉升级管理 tab，进入管理界面。

360

终端安全管理系统

首页

勒索攻击防护

APT攻击防护

挖矿攻击防护

攻防演练

重大事件保障

等保合规

数据安全防护

可视化大屏

统一纳管设置

360全网安全大脑管理中心

帮助

我的设备

退出系统

数据总览

资产管理

资产分类

资产扫描

终端管理

终端升级

终端日志

安全体检

实时扫描

病毒查杀

漏洞管理

数据保护

桌面运维

补丁管理

上网管理

软件管理

帐户管理

终端升级

升级管理

升级策略

升级设置

升级日志

终端分组

全部终端 339

未分组 116

zyx 5

zyz2 4

zhangchao 1

1 1

wk1-uos 1

dulali 4

test000000 2

mc 6

zdx 6

YXX组 2

yang 1

wk1-win 0

xzw 6

新建分组

导入分组

导出分组

终端名称

状态

操作系统

主程序版本

漏洞库版本

病毒库时间

zyx-uos1030

在线

国产通用桌面机

10.0.0.7000

2022-12-26

2023-03-23

WIN-CL758EMKN8M

在线

Windows

10.0.0.7000

2022-10-25

2023-02-10

WIN-JURD73A0FSQ

在线

Windows

10.0.0.7000

2022-10-25

2023-02-10

qhoo的Macbook Pro

在线

MacOS

10.0.0.7000

-

2022-9-5

wk1-PC

在线

国产通用桌面机

10.0.0.7000

2022-12-26

2023-03-16

qhoo的Mac-text

在线

MacOS

10.0.0.7000

-

2022-9-5

Qwin7\_64-PC

在线

Windows

10.0.0.7000

2022-10-25

2023-02-10

miao-PC

在线

国产通用桌面机

10.0.0.7000

2022-12-26

2023-03-23

WIN-667GNDQV91

在线

Windows

10.0.0.7000

2022-10-25

2022-02-10

win11hongfeng

在线

Windows

10.0.0.7000

2022-10-25

2023-02-10

- （1）版本查看：查看客户端主程序、补丁库版本及病毒库时间。
- （2）下发升级指令：支持客户端【立即升级主程序】、【立即升级病毒库】、【立即升

级漏洞库】。



终端病毒库支持离线下载更新：管控中心的**终端管理》升级管理**，病毒库每次更新时自动生成一个离线病毒库文件供管理员下载，同时客户端离线病毒库升级入口，满足客户端离线升级的需求。



## 4.2.3.2. 升级策略

### 4.2.3.2.1. Windows 平台

点击左侧功能导航：**资产管理》终端管理>终端升级》升级策略>Windows**，进入策略配置界面。

根据实际环境及需求设置终端升级的策略，内网升级支持通过管控升级和通过升级服务器升级，二者至少勾选一个升级通路，拖动排序可调整升级优先级。



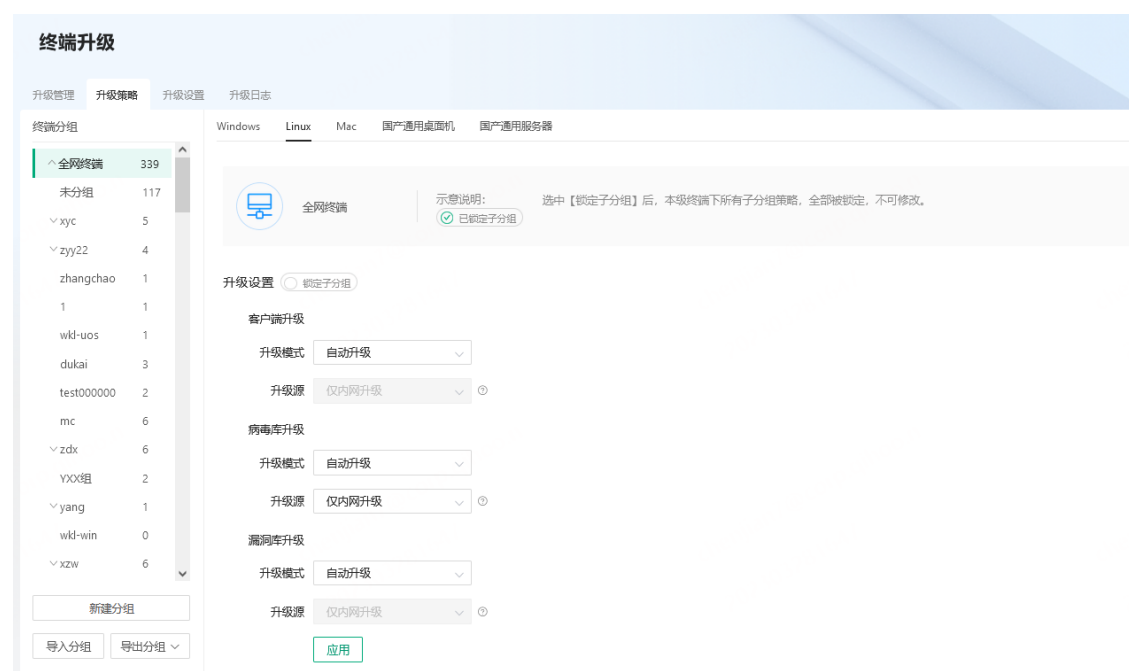
### 4.2.3.2.2. Linux 平台

点击左侧功能导航：**资产管理》终端管理>终端升级》升级策略>Linux**，进入策略配置界



面。

根据实际环境及需求设置终端升级的策略。



### 4.2.3.2.3. Mac 平台

点击左侧功能导航：资产管理〉终端管理>终端升级〉升级策略> Mac，进入策略配置界面。

根据实际环境及需求设置终端升级的策略，内网升级支持通过管控升级和通过升级服务器升级，二者至少勾选一个升级通路，拖动排序可调整升级优先级。



#### 4.2.3.2.4. 国产桌面机

点击左侧功能导航：**资产管理》终端管理>终端升级》升级策略> 国产桌面机**，进入策略配置界面。

根据实际环境及需求设置终端升级的策略，内网升级支持通过管控升级和通过升级服务器升级，二者至少勾选一个升级通路，拖动排序可调整升级优先级。

升级设置

客户端升级

升级模式

自动升级

升级源

仅内网升级

病毒库升级

升级模式

自动升级

升级源

仅内网升级

漏洞库升级

升级模式

自动升级

升级源

仅内网升级

内网升级通路配置(至少勾选一个升级通路，拖动排序可调整升级优先级)

升级通路	操作
<input checked="" type="checkbox"/> 通过管控升级	
<input checked="" type="checkbox"/> 通过升级服务器升级	

终端名称	通讯地址	终端下载地址	状态	是否使用	备注
epp201v.epp.shyc2.qi...	10.213.246.227	10.213.246.227:36690	在线	<input type="checkbox"/>	-

#### 4.2.3.2.5. 国产服务器

点击左侧功能导航：**资产管理》终端管理>终端升级》升级策略> 国产服务器**，进入策略配置界面。

根据实际环境及需求设置终端升级的策略，内网升级支持通过管控升级和通过升级服务器升级，二者至少勾选一个升级通路，拖动排序可调整升级优先级。

升级设置

客户端升级

升级模式

自动升级

升级源

仅内网升级

病毒库升级

升级模式

自动升级

升级源

仅内网升级

漏洞库升级

升级模式

自动升级

升级源

仅内网升级

内网升级通路配置(至少勾选一个升级通路, 拖动排序可调整升级优先级)

升级通路	操作
<input checked="" type="checkbox"/> 通过管控升级	
<input checked="" type="checkbox"/> 通过升级服务器升级	

终端名称	通讯地址	终端下载地址	状态	是否使用	备注
epp201iv.epp.shyc2.qi...	10.213.246.227	10.213.246.227:36690	在线	<input type="checkbox"/>	-

## 4.2.3.3.升级设置

允许管理员对客户端程序版本、病毒库、补丁库进行灰度升级控制, 允许选择部分分组的客户端先升级。灰度升级优先, 未在灰度设置的组将不进行自动升级。

点击左侧功能导航: **资产管理》终端管理>终端升级》升级设置**, 进入客户端升级配置界面。

360

终端安全管理系统

本级中心

首页

勒索攻击防护

APT攻击防护

挖矿攻击防护

攻防演练

重大事件保障

等保合规

数据安全防护

可视化大屏

统一纳管设置

数据总览

资产管理

终端管理

终端升级

安全体检

实时对抗

病毒查杀

漏洞管理

数据保护

桌面加速

外设管理

终端升级

升级管理

升级策略

升级设置

升级日志

终端范围包括Windows、国产通用机、Mac、Linux终端, 仅允许选中的终端进行升级。

客户端病毒库灰度升级

开启灰度升级

升级的终端

至少勾选一个分组

测试天数

15

天

批次	升级的终端	所属分组	测试天数(天)	操作
1	xyc	全网终端/xyc	<div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>5</div> <div>6</div> <div>7</div> <div>8</div> <div>9</div> <div>10</div> <div>11</div> <div>12</div> <div>13</div> <div>14</div> <div>15</div>	编辑 删除

测试策略

2

天

全网计算机将在13天6小时18分后升级到最新版本

客户端程序灰度升级

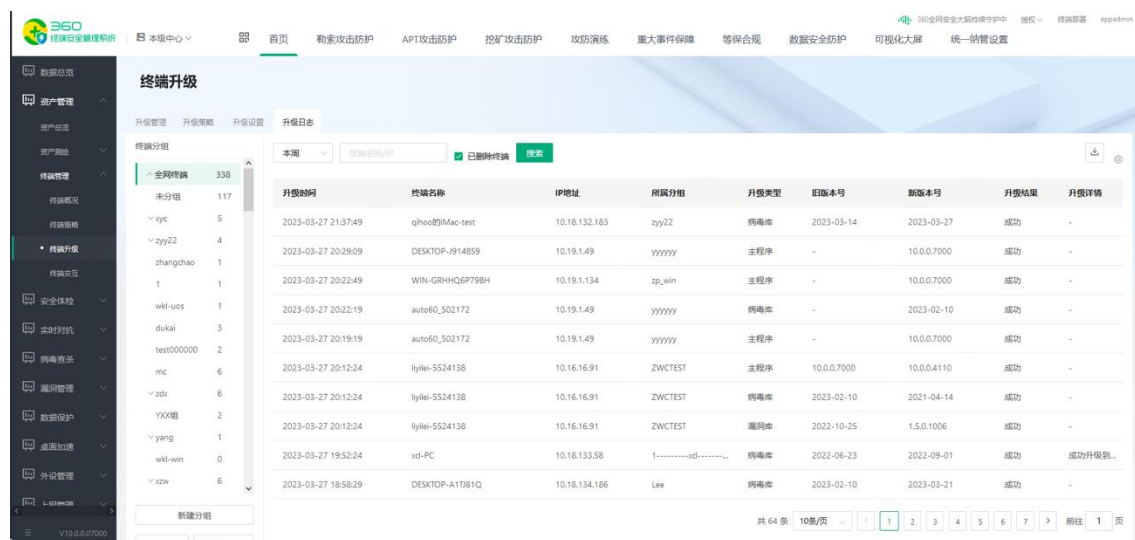
开启灰度升级

## 4.2.3.4.升级日志

服务端记录终端升级日志详情，包括升级类型和升级结果等。

点击左侧功能导航：**资产管理》终端管理>终端升级》升级日志**，进入客户端升级日志界面，查看升级日志。

默认一周的终端升级日志，管理员可以调整时间段进行查看，可以导出 CSV 或 Excel 报表。



## 4.2.4.终端交互

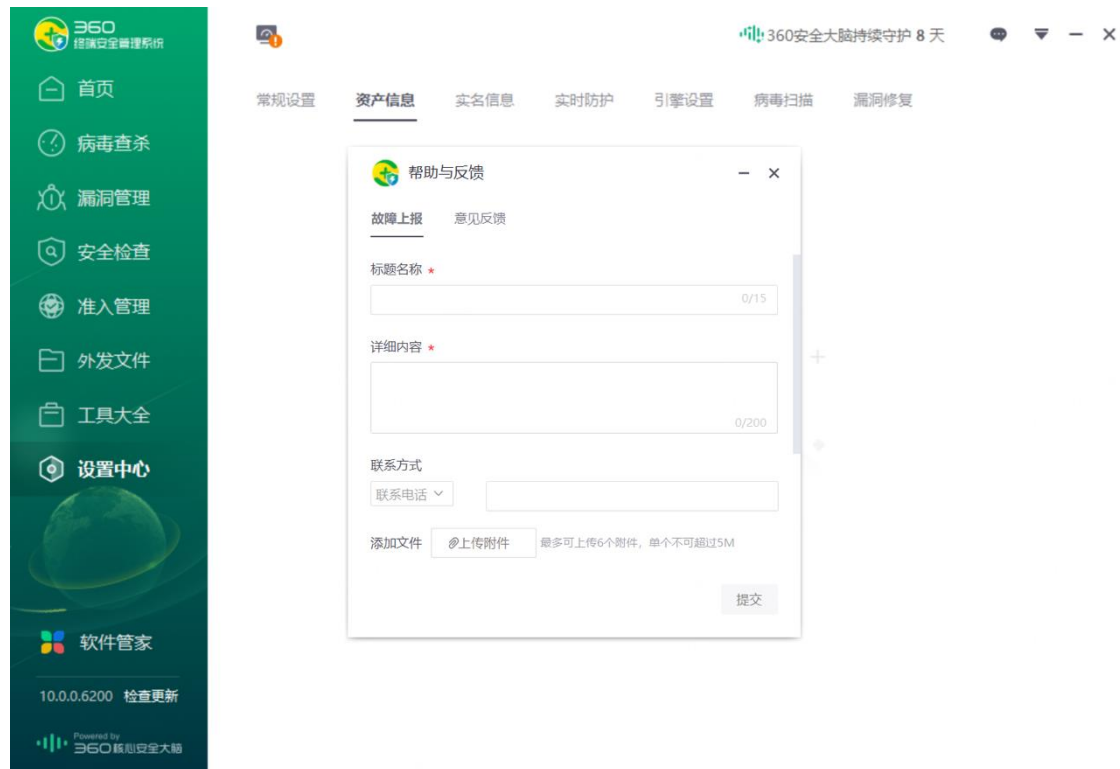
### 4.2.4.1.故障上报

终端用户可在客户端对终端故障进行上报，管理员在服务端查阅客户端上报的故障信息进行处置及反馈。

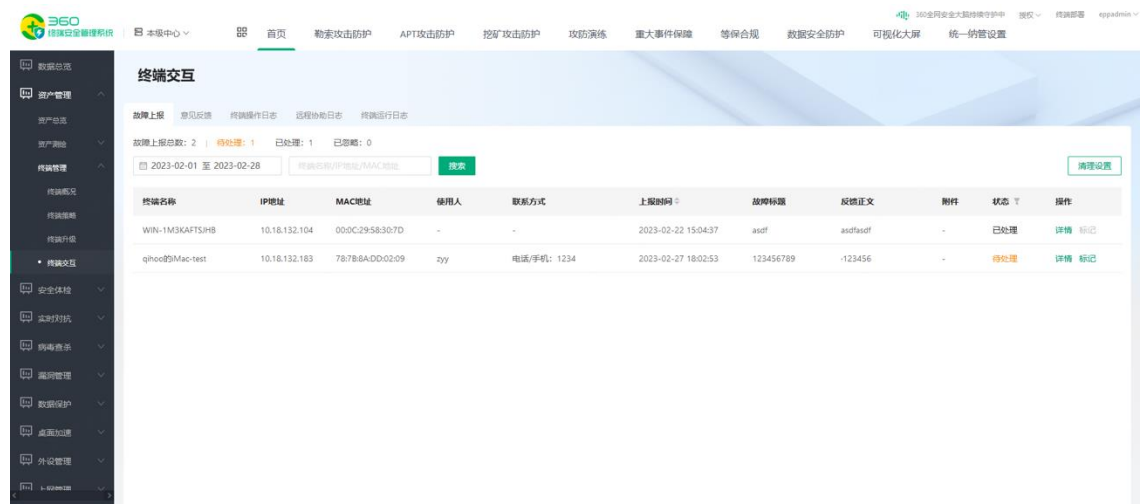
点击左侧功能导航：**资产管理》终端管理>终端交互》故障上报**，进入页面进行查阅和处置。

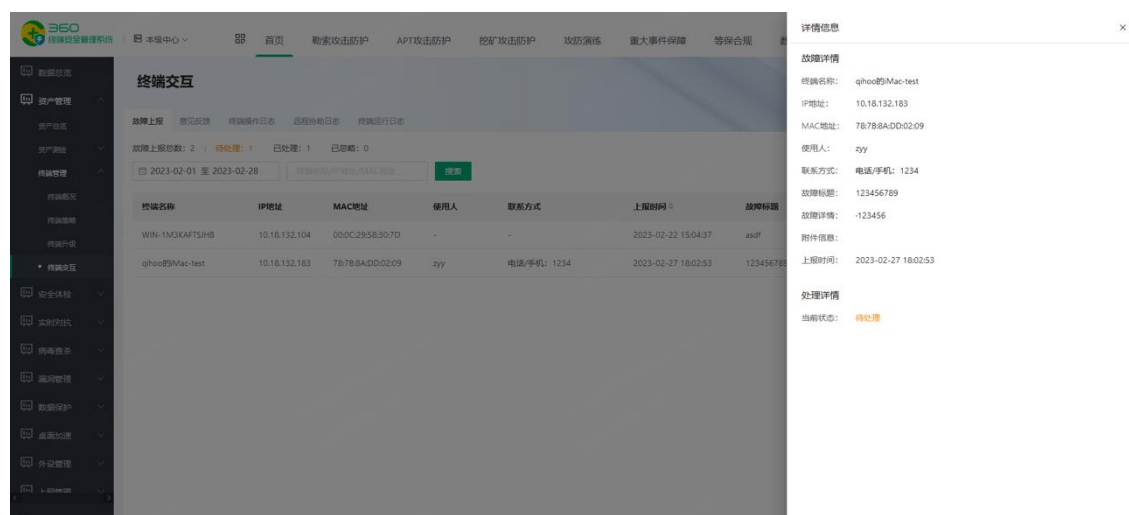
支持展示故障上报总数、待处理数量、已处理数量和已忽略数量。支持按时间查看和模糊搜索反馈信息。可根据需求设置自动清理 XX 天前上报的故障信息。

#### (1) 客户端上报



## (2) 服务端查阅处理





### (3) 自动清理



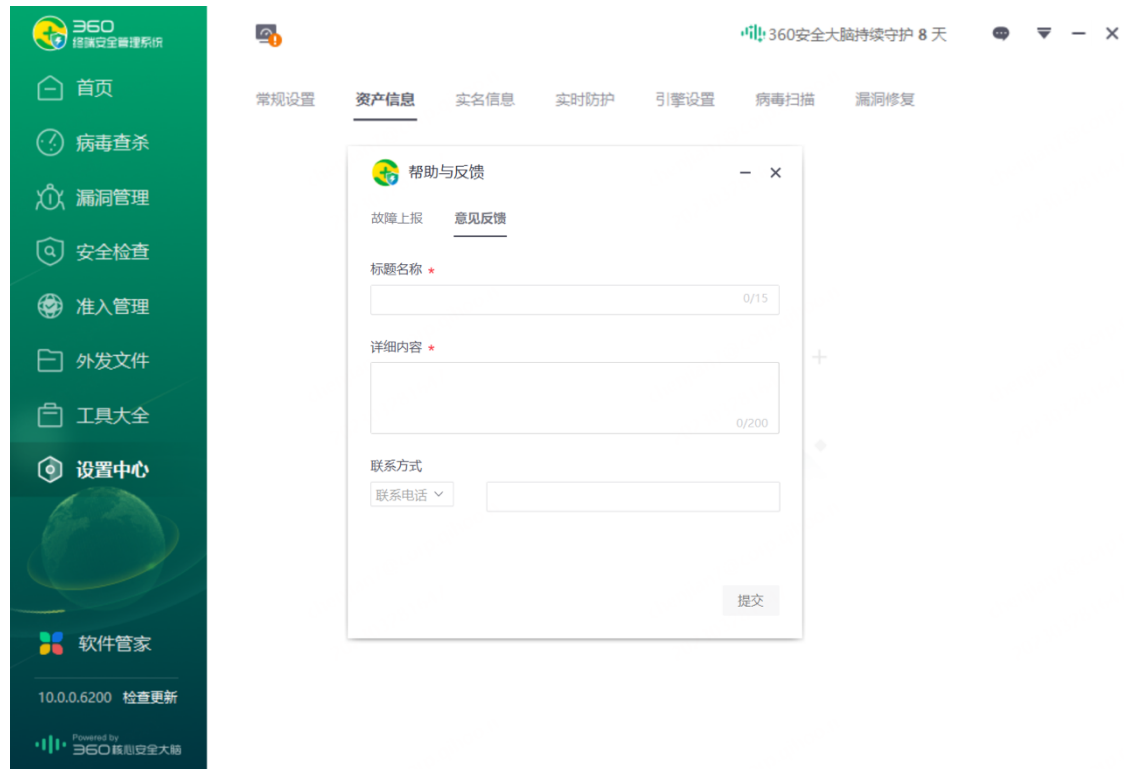
## 4.2.4.2. 意见反馈

终端用户可在客户端对意见反馈进行上报，管理员在服务端查阅客户端上报的意见反馈信息并进行处置及反馈。

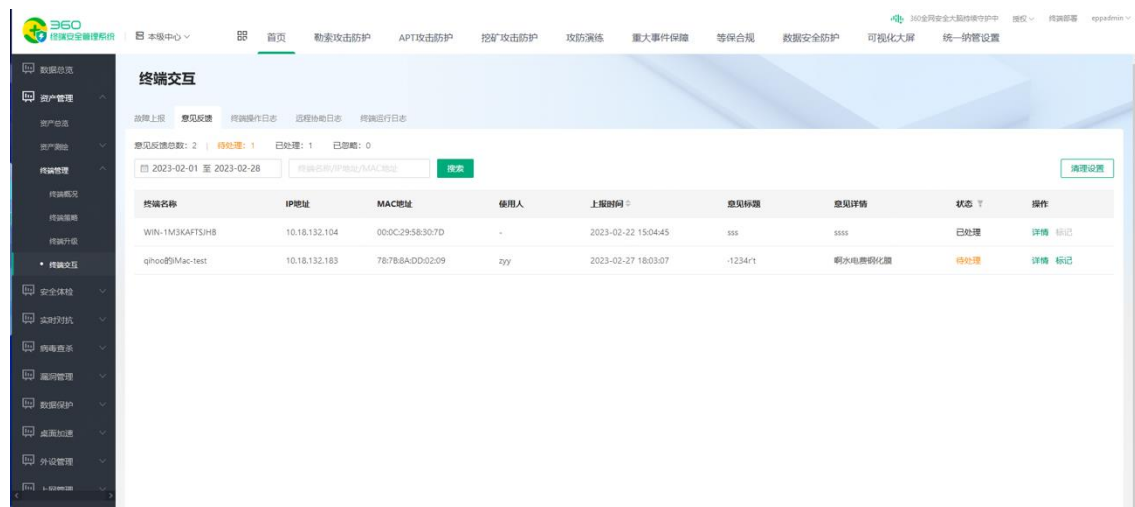
点击左侧功能导航：**资产管理》终端管理>终端交互》意见反馈**，进入页面进行查阅和处理。

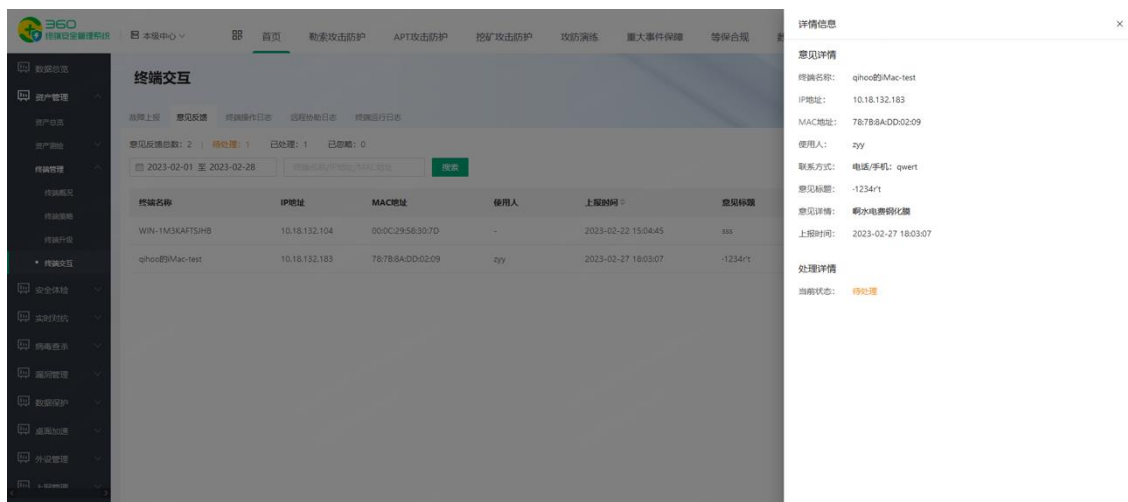
支持展示意见反馈总数、待处理数量、已处理数量和已忽略数量。支持按时间查看和模糊搜索反馈信息。可根据需求设置自动清理 XX 天前上报的意见反馈信息。支持查看单点详情。

### (1) 客户端上报



## (2) 服务端查阅处理

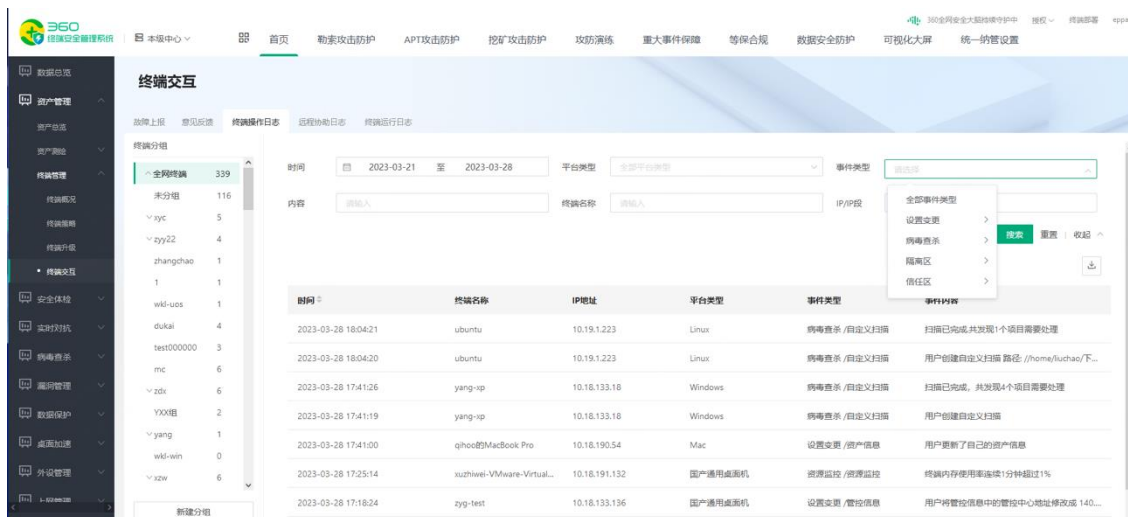




### 4.2.4.3.终端操作日志

客户端的操作行为会上报给服务端，服务端可查看客户端的操作行为日志，包括客户端对隔离区、信任区的操作以及客户端安装卸载日志等。

点击左侧功能导航：**资产管理**〉**终端管理**〉**终端交互**〉**终端操作日志**，进入页面进行查阅和处理。



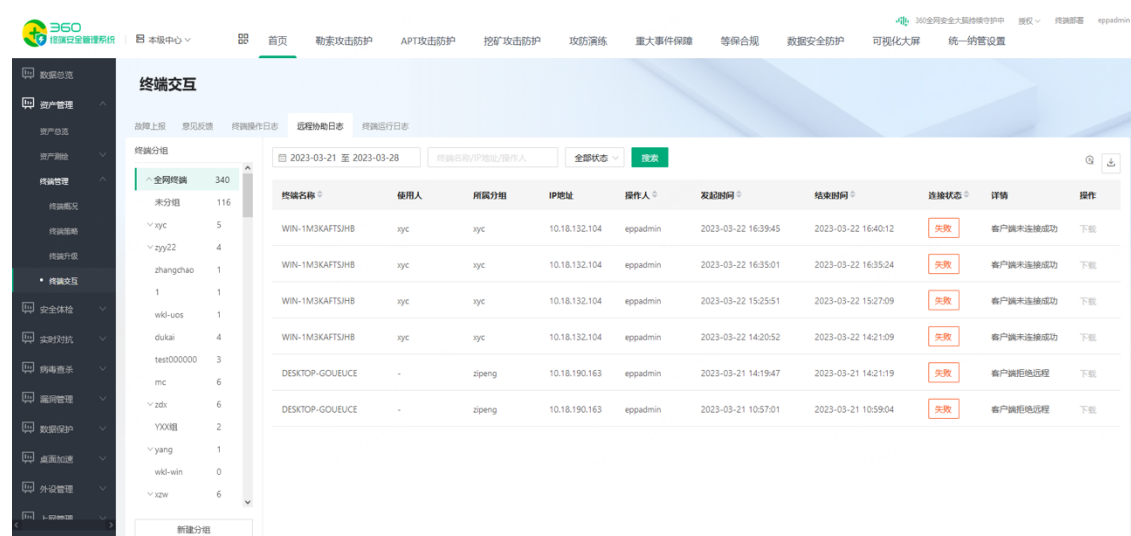
### 4.2.4.4.远程协助日志

服务端对客户端的远程协助控制行为会进行录屏上报给服务端，服务端可查看对客户端的远控过程以及远程记录。

点击左侧功能导航：**资产管理**〉**终端管理**〉**终端交互**〉**远程协助日志**，进入页面进行查阅



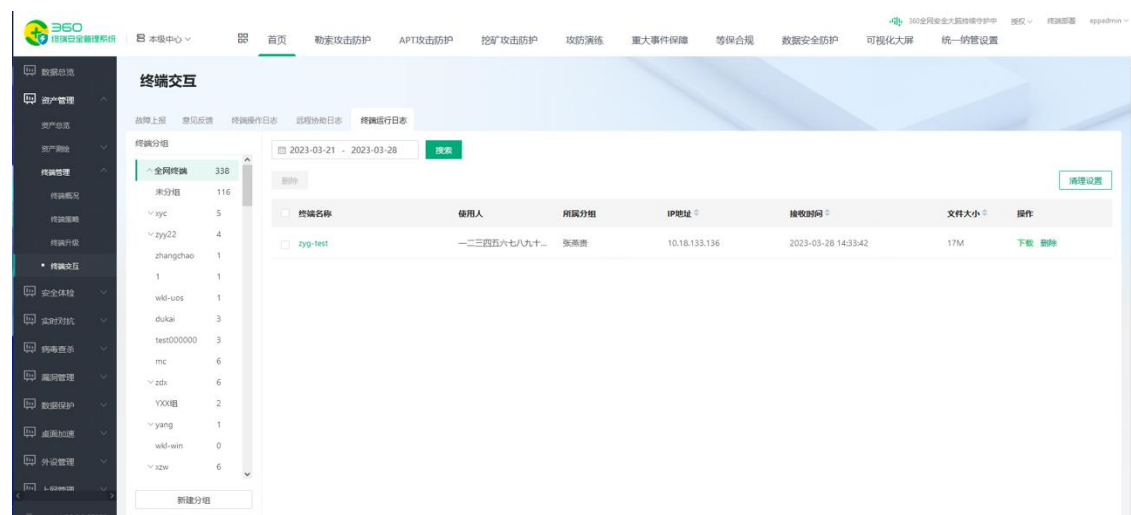
和处理。



## 4.2.4.5. 终端运行日志

在单个终端详情页面下发命令收集终端日志信息后，在终端运行日志也可下载日志查看。

点击左侧功能导航：**资产管理**〉**终端管理**〉**终端交互**〉**终端运行日志**，进入页面进行查阅和处理。



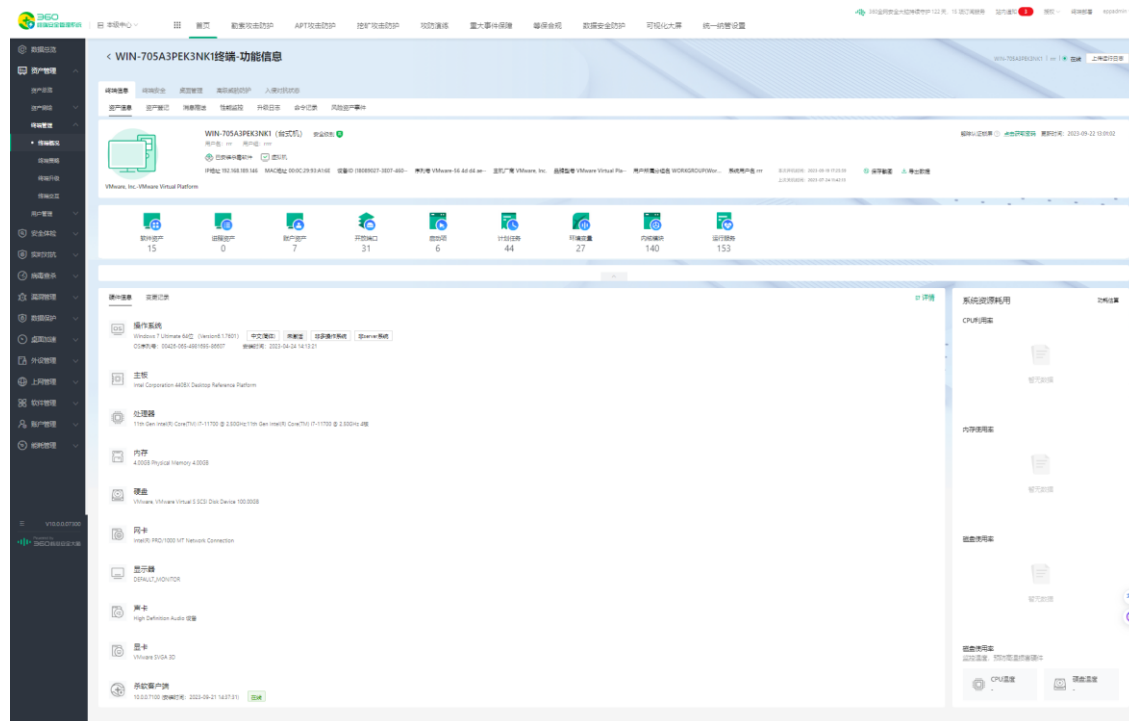
## 4.2.5. 终端详情

### 4.2.5.1. 终端信息

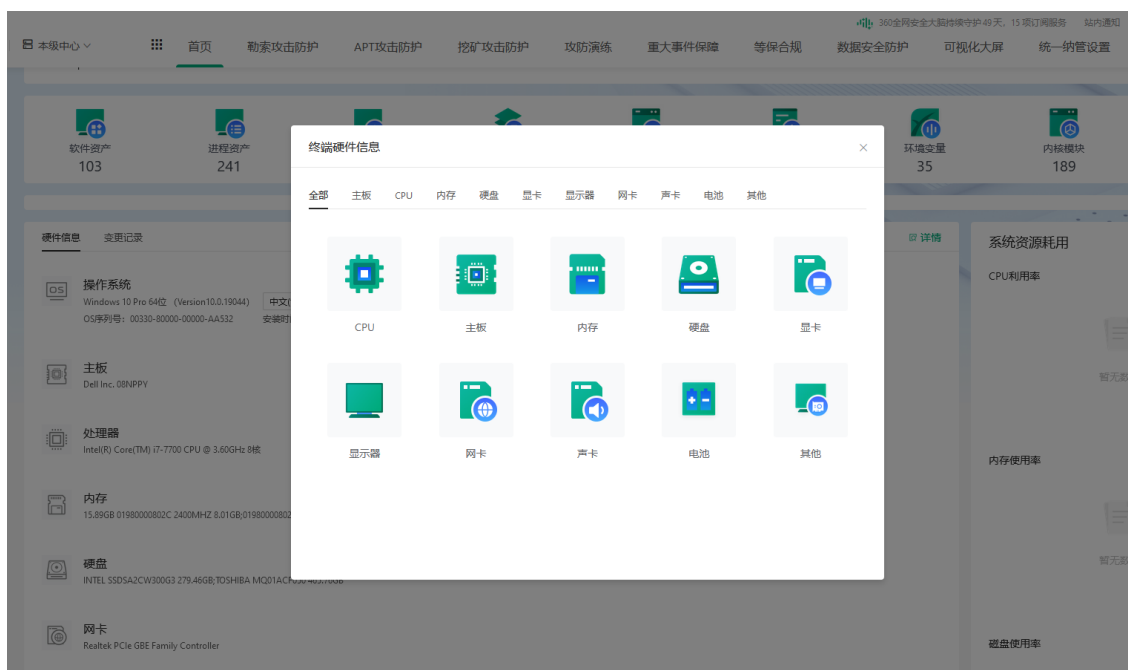
#### 4.2.5.1.1. 资产信息

展示具体某个终端的设备信息和资产信息（包括软件、进程、账户、计划任务等）以及相关的一些基础信息。同时，支持以资产维度，展示此终端的资产信息，并执行相关操作指令。

点击左侧功能导航：**资产管理>终端管理>终端概况>终端详情>终端信息**，查看资产信息。

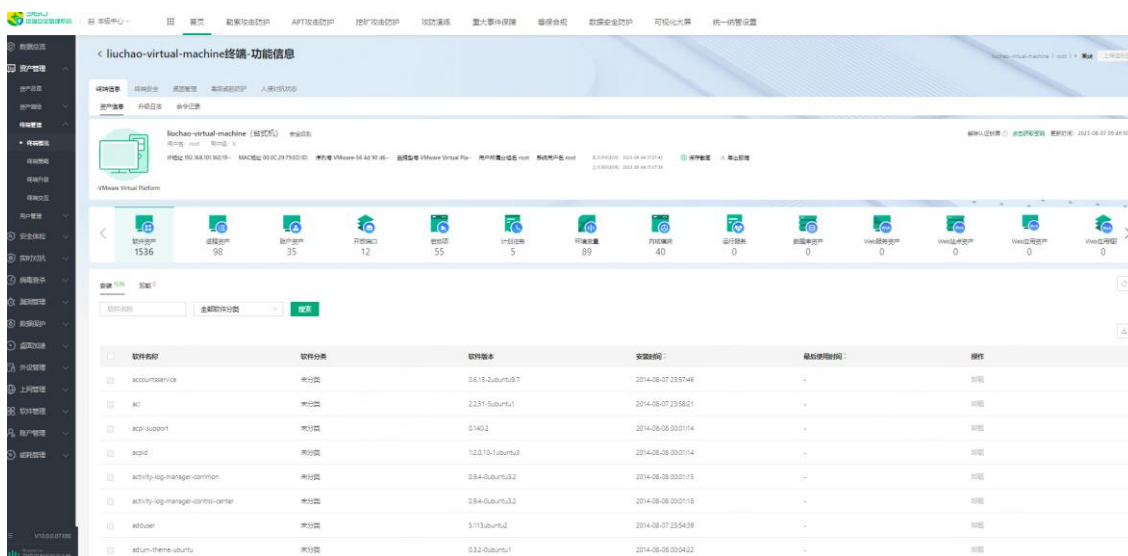


支持硬件详情信息的采集和展示。

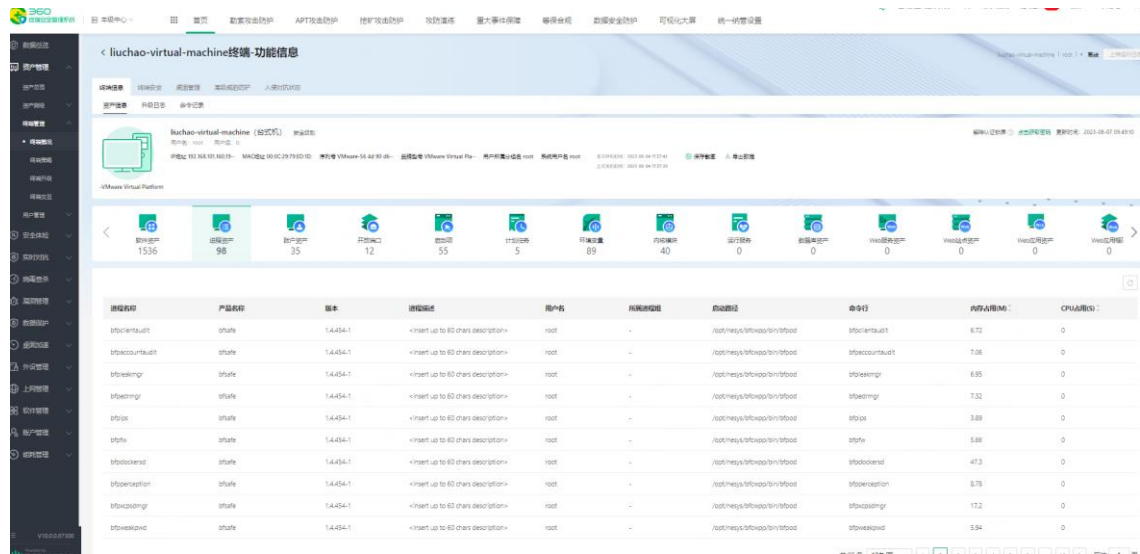


## (1) 软件资产

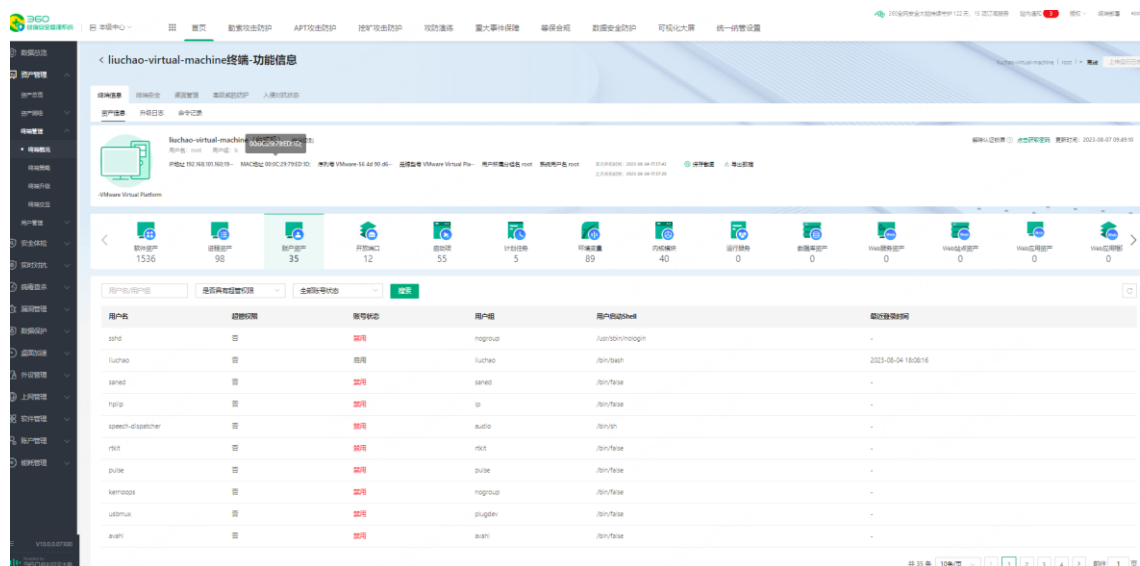
展示所安装的软件信息，支持对终端软件进行远程卸载。



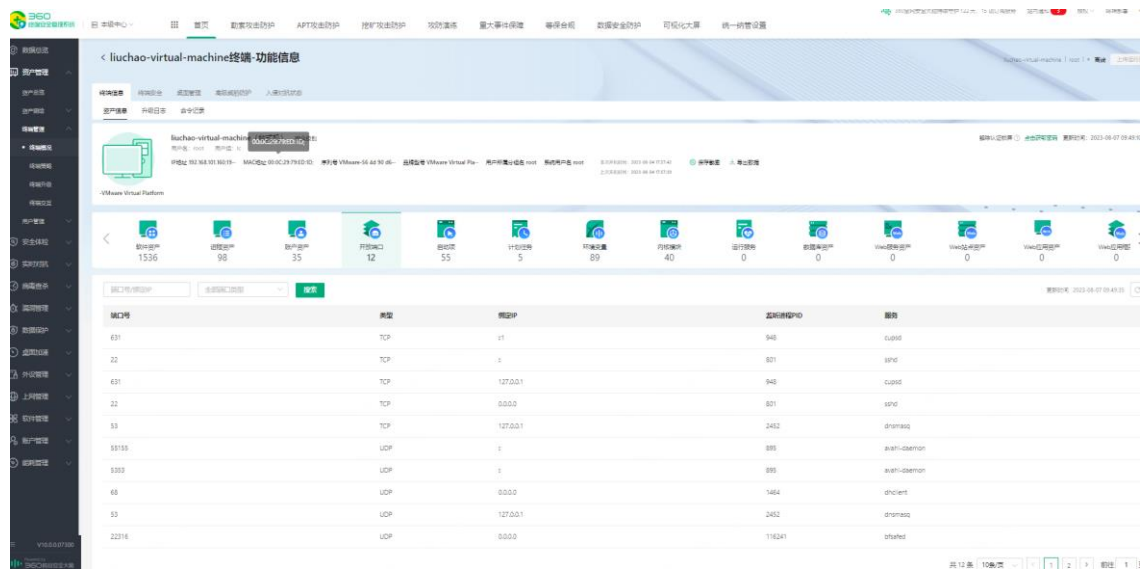
## (2) 进程资产



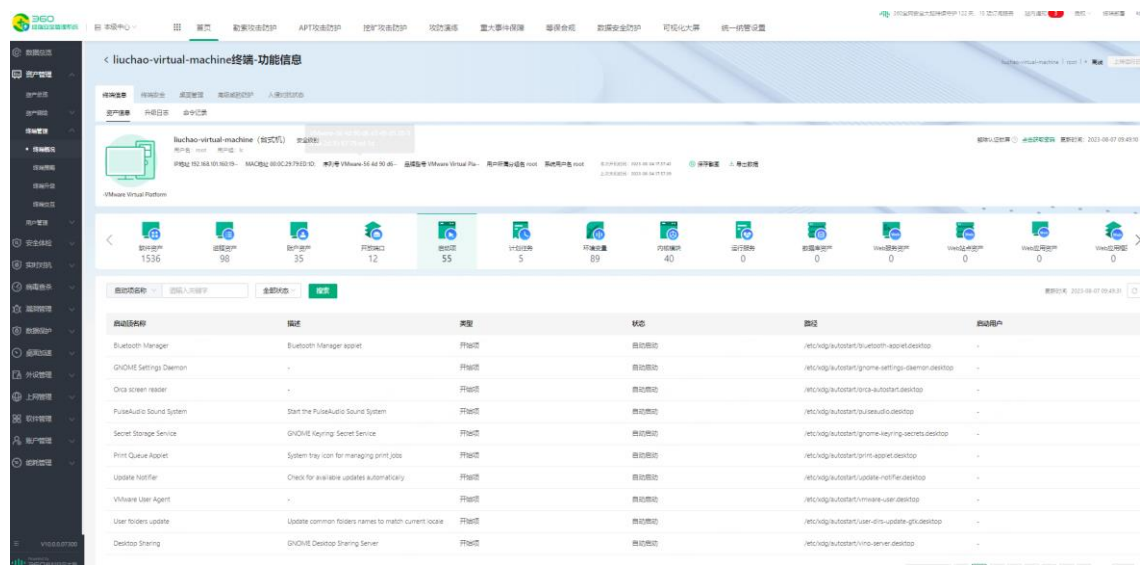
### (3) 账户资产



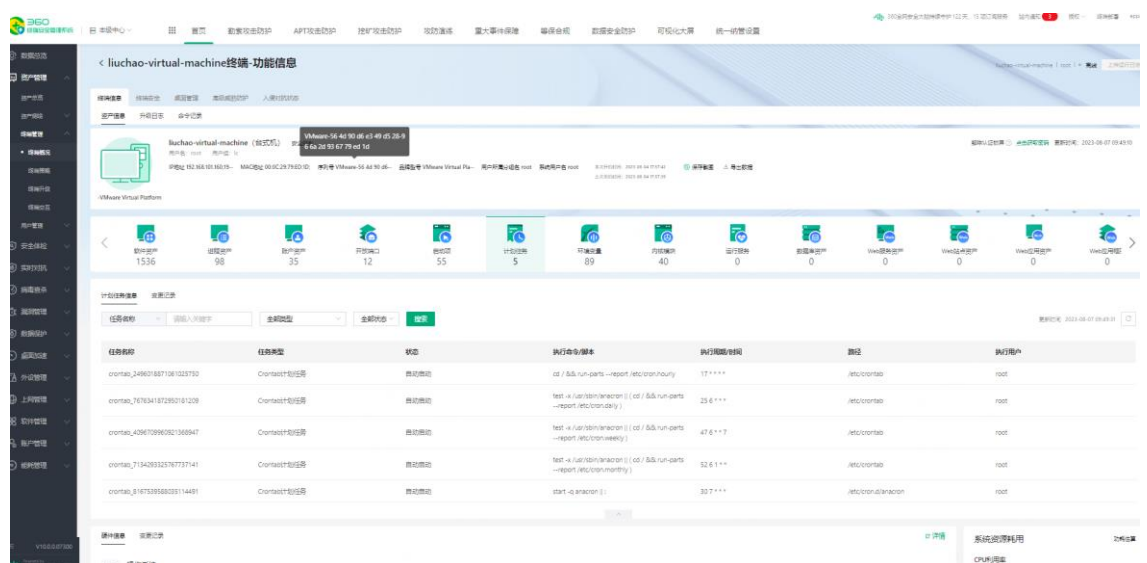
### (4) 开放端口



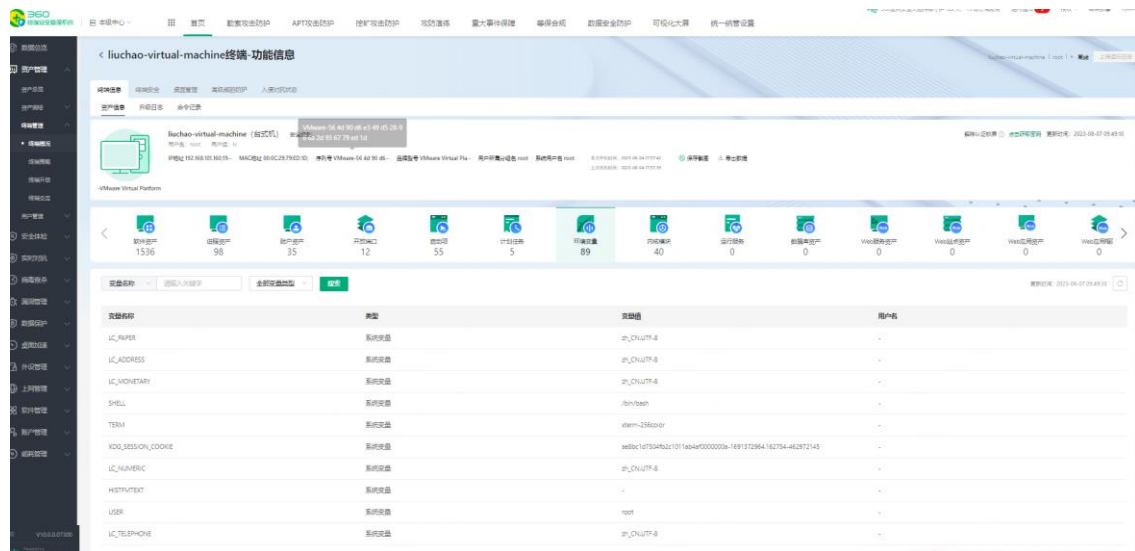
## (5) 启动项



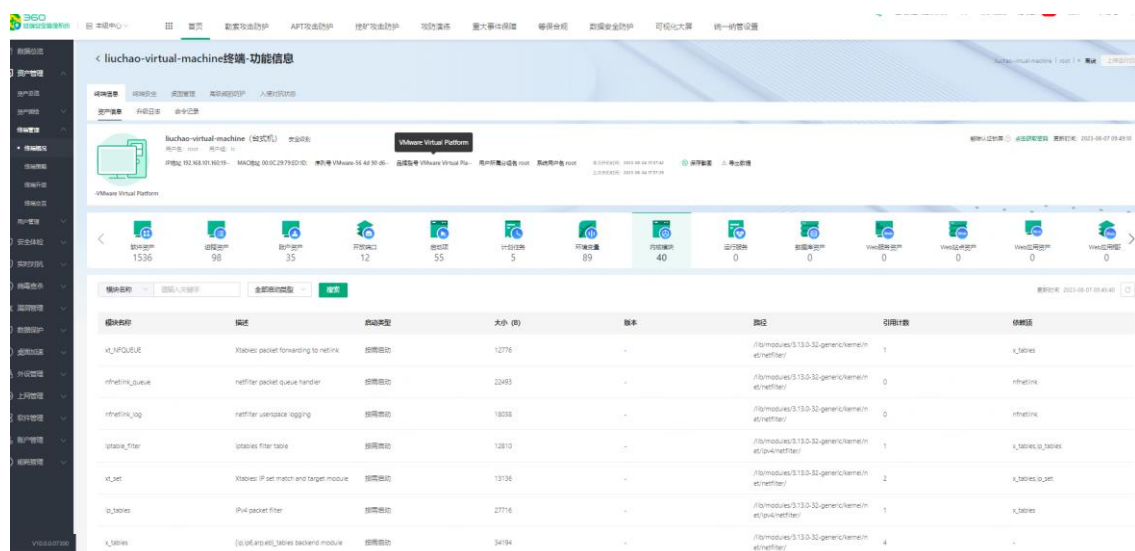
## (6) 计划任务



### (7) 环境变量

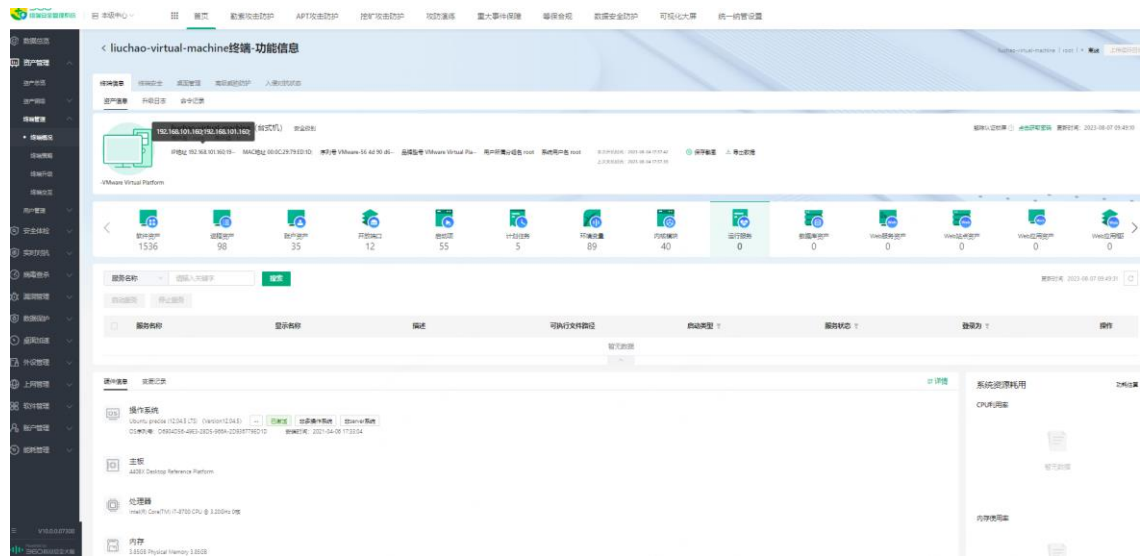


## (8) 内核模块

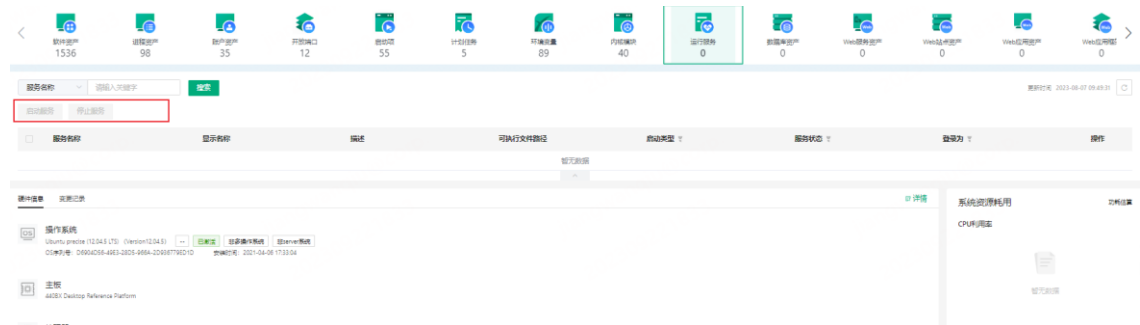


### (9) 运行服务

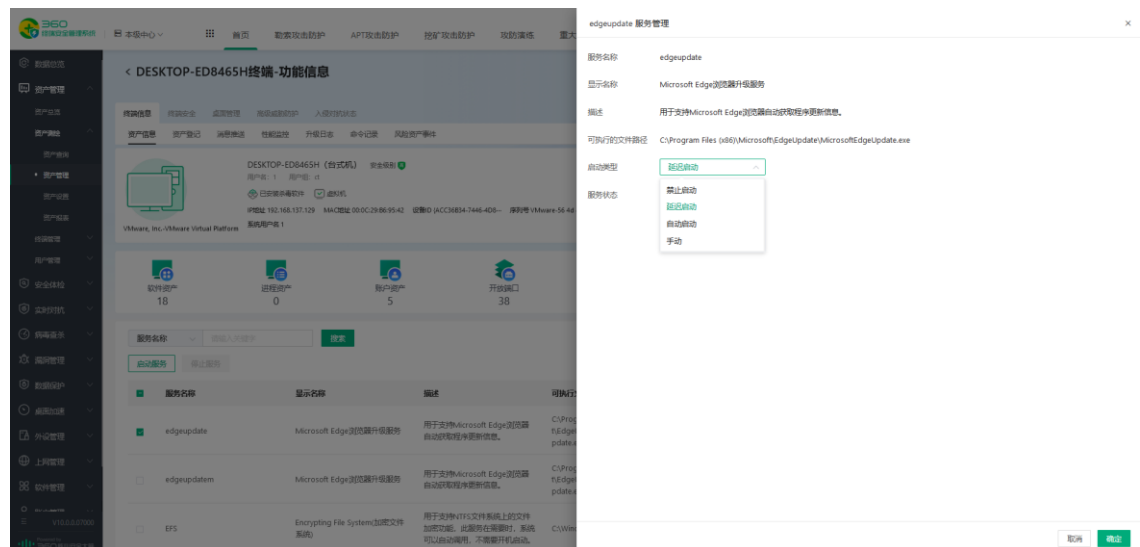
支持管理员在控制台修改服务的启动类型（自动/手动/延迟/禁止）以及对服务进行启停操作。



## 1) 启停服务

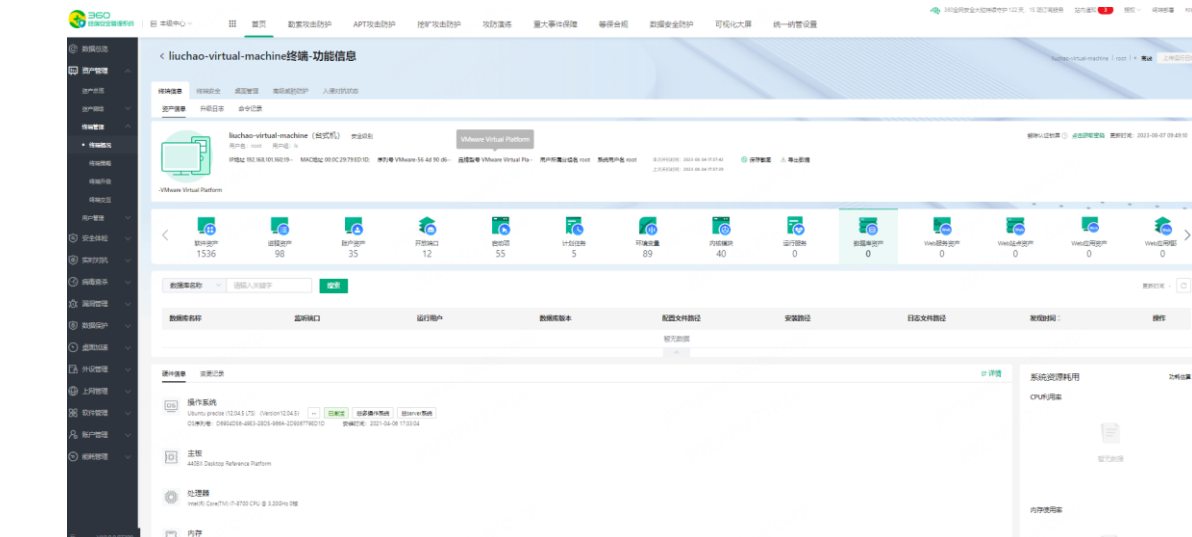


## 2) 启动类型设置

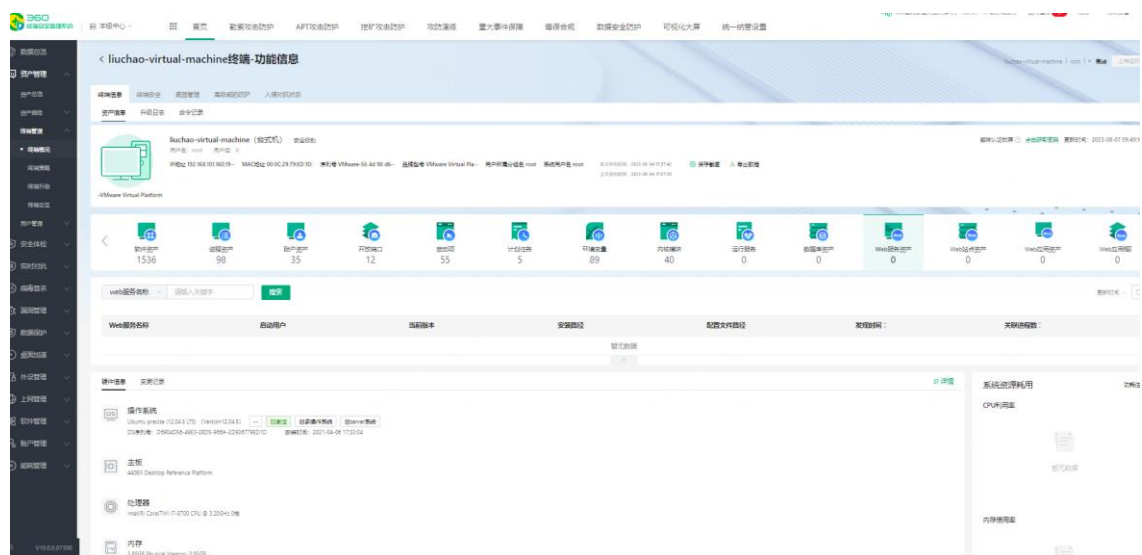


## (10) 数据库资产

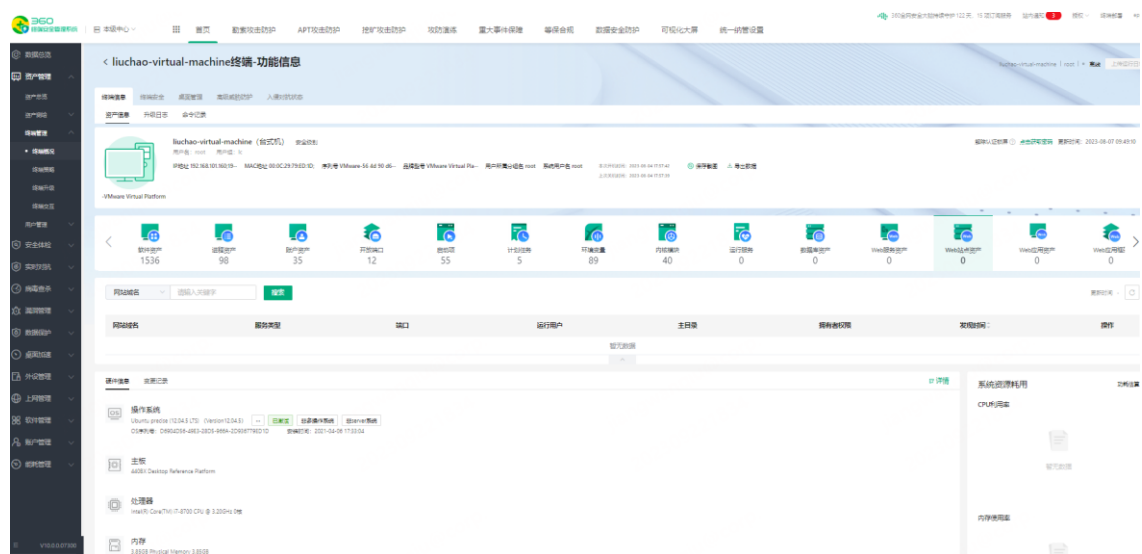




(11) web 服务资产

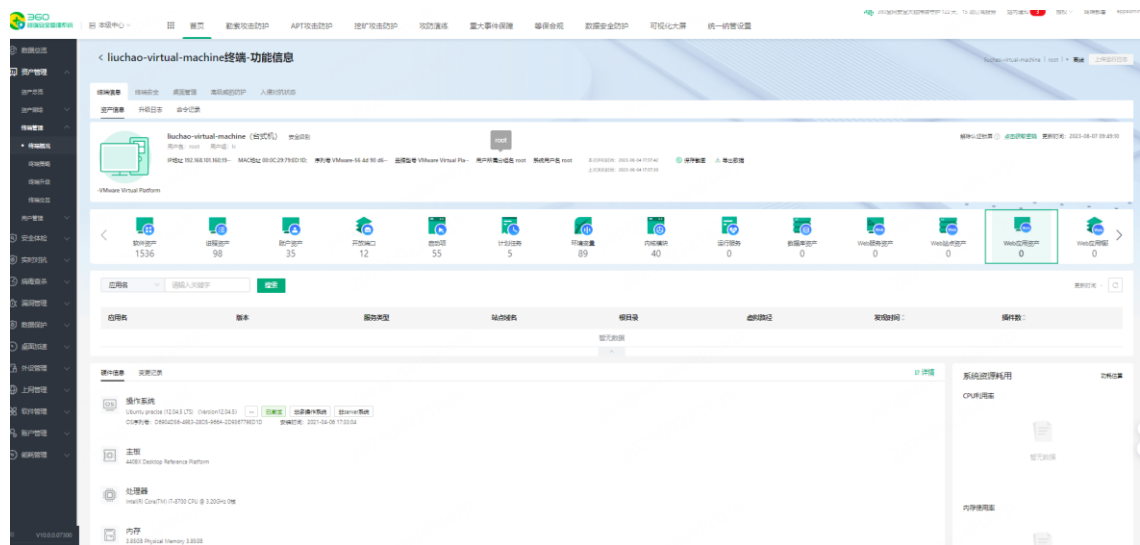


(12) web 站点资产

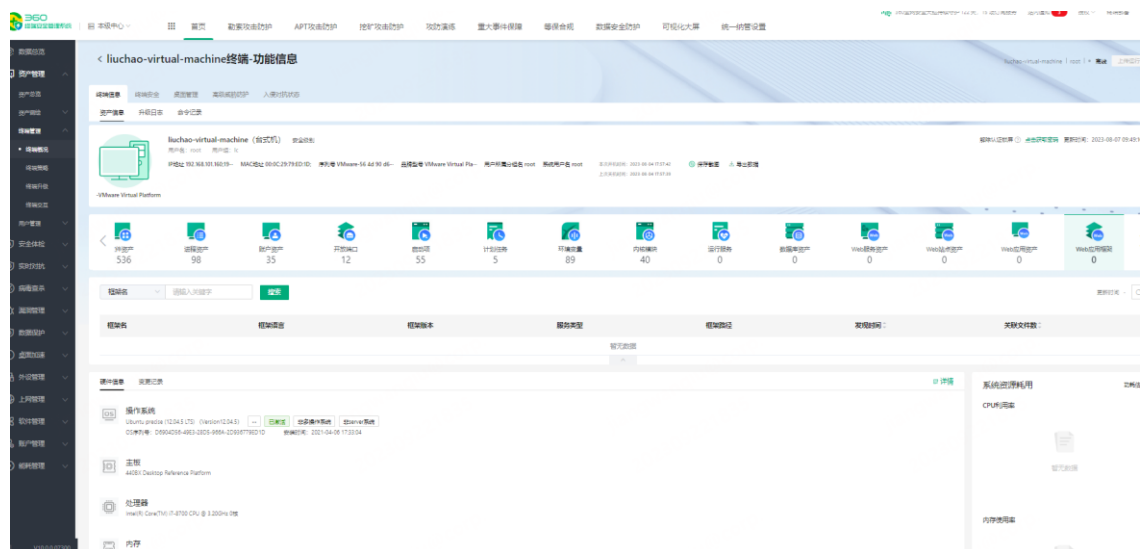




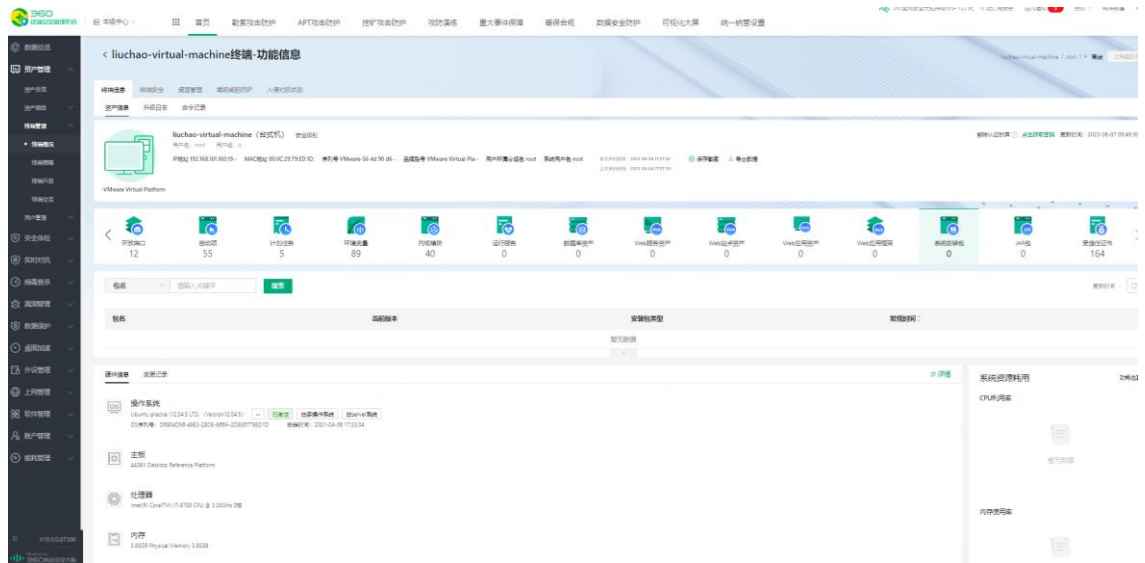
## (13) web 应用资产



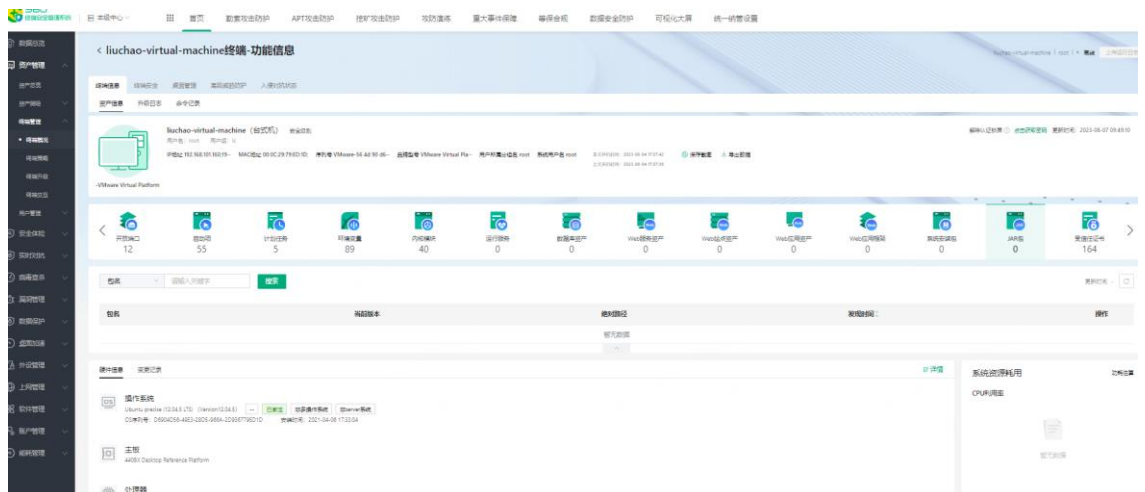
## (14) web 应用框架资产



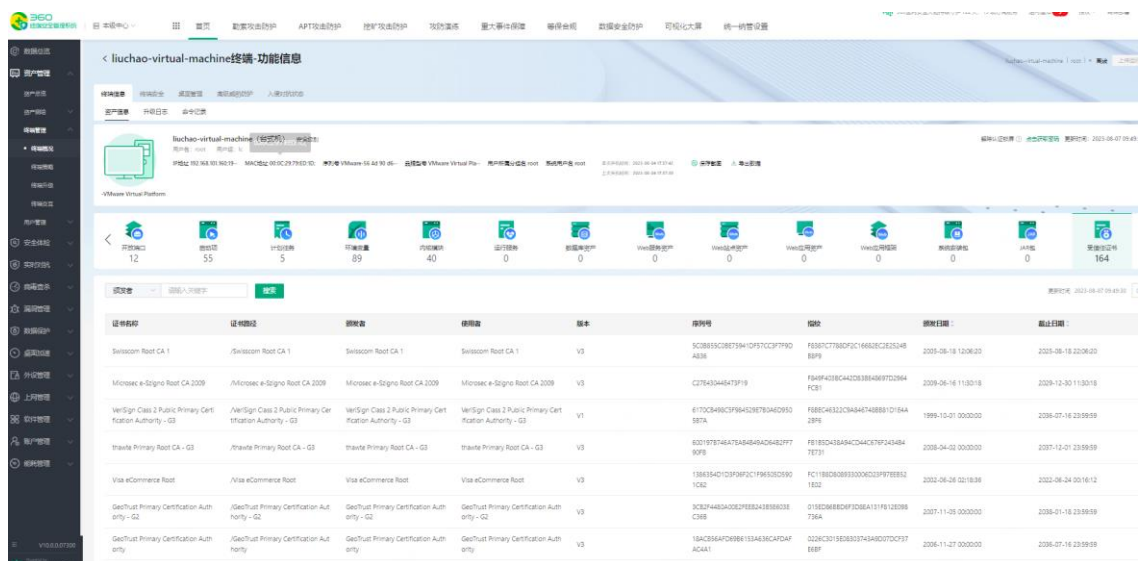
## (15) 系统安装包资产



## (16) jar 包资产



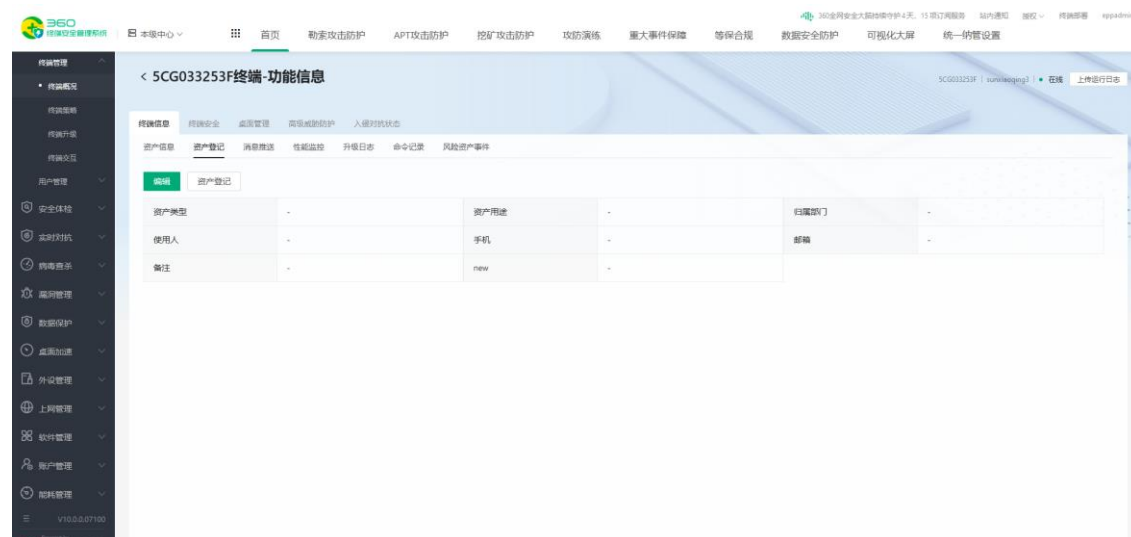
## (17) 受信任证书



### 4.2.5.1.2. 资产登记

展示终端的资产登记信息，支持管理员编辑修改和重新登记。

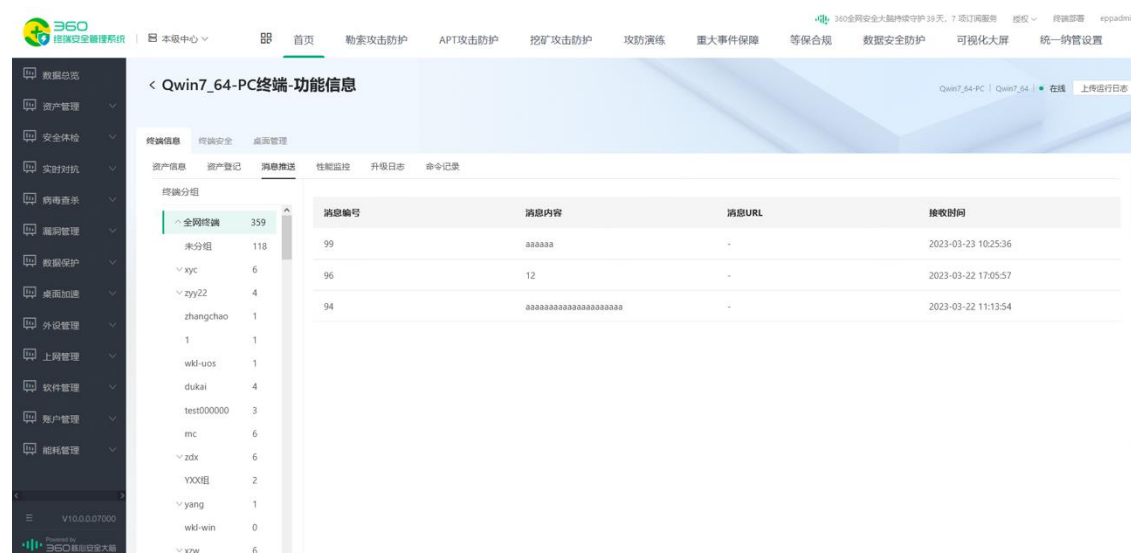
点击左侧功能导航：资产管理>终端管理>终端概况>终端详情>终端信息>资产登记，查看客户端登记的资产信息。



#### 4.2.5.1.3. 消息推送

展示给终端推送的消息记录。

点击左侧功能导航：资产管理>终端管理>终端概况>终端详情>终端信息>消息推送，查看客户端推送的消息记录。



#### 4.2.5.1.4. 性能监控

展示终端的性能状况，包括显示“当前状态”和“持续状态”，类型支持 CPU 温度、CPU 使用率、内存使用率、硬盘容量、硬盘温度、硬盘 I/O 占用率、网络监控数据。

点击左侧功能导航：资产管理>终端管理>终端概况>终端详情>终端信息>性能监控



#### 4.2.5.1.5. 升级日志

展示此终端的升级日志详情。

点击左侧功能导航：资产管理>终端管理>终端概况>终端详情>终端信息>升级日志，查看客户端升级记录。

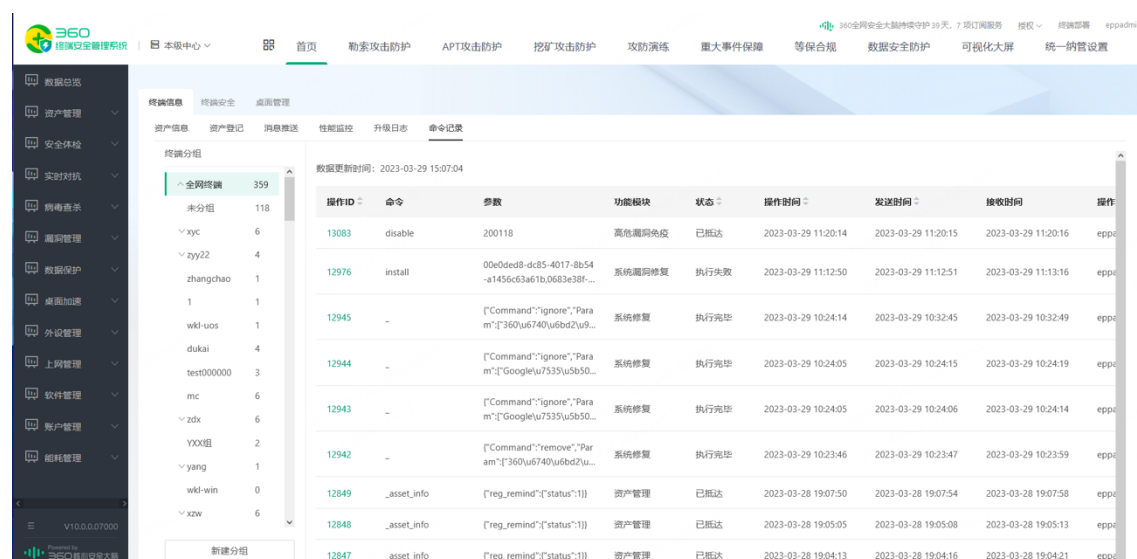
The screenshot shows the 'Qwin7\_64-PC' terminal's upgrade log page. The left sidebar is the same as the previous screenshot. The main content area shows '终端信息' (Terminal Information) with tabs for '终端安全' and '桌面管理'. Under '升级日志' (Upgrade Log), there is a table with the following columns: '升级时间' (Upgrade Time), '终端名称' (Terminal Name), 'IP地址' (IP Address), '使用人' (User), '所属分组' (Group), '旧版本号' (Old Version), '新版本号' (New Version), '升级类型' (Upgrade Type), and '升级结果' (Upgrade Result).

升级时间	终端名称	IP地址	使用人	所属分组	旧版本号	新版本号	升级类型	升级结果
2023-03-06 16:42:56	Qwin7_64-PC	10.18.190.27	fa	qtl	10.0.0.6270	10.0.0.7000	主程序	成功
2023-02-22 16:15:41	Qwin7_64-PC	10.18.190.27	fa	qtl	-	10.0.0.6270	主程序	成功
2023-02-22 16:15:01	Qwin7_64-PC	10.18.190.27	fa	qtl	-	2022-10-25	漏洞库	成功

#### 4.2.5.1.6. 命令记录

展示管控向此终端发送的命令记录情况。

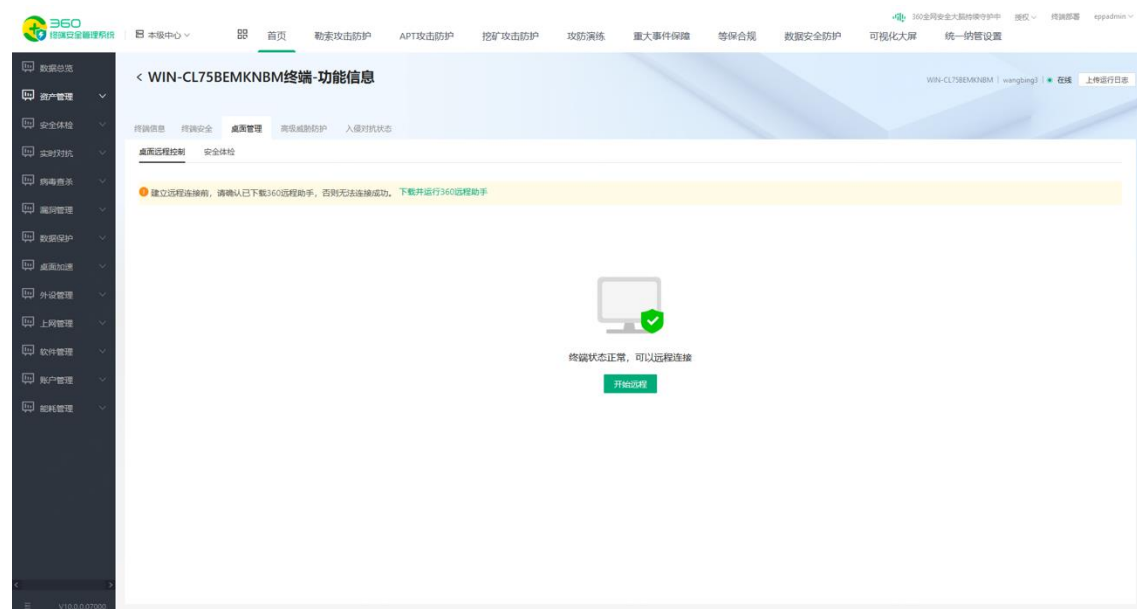
点击左侧功能导航：资产管理>终端管理>终端概况>终端详情>终端信息>命令记录，查看向客户端发送的命令记录。



## 4.2.5.2. 桌面管理

### 4.2.5.2.1. 远程协助

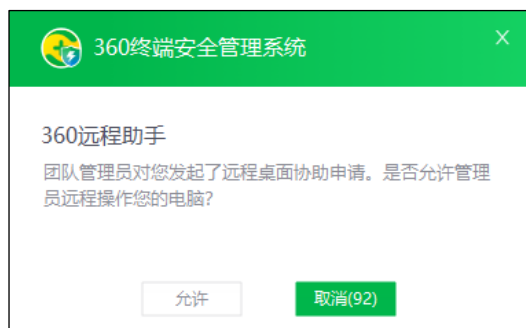
点击左侧功能导航：资产管理>终端管理>终端概况>终端详情>桌面管理>远程协助，对终端发起远程协助。



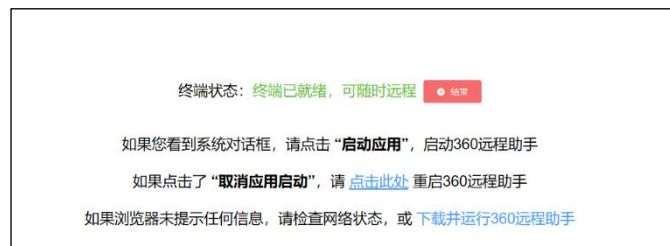
用户配置时，选择：终端同意后执行远程控制，远控理由为必填项，客户端会出现弹窗提示：



在客户端弹出的远程协助界面点击【确定】

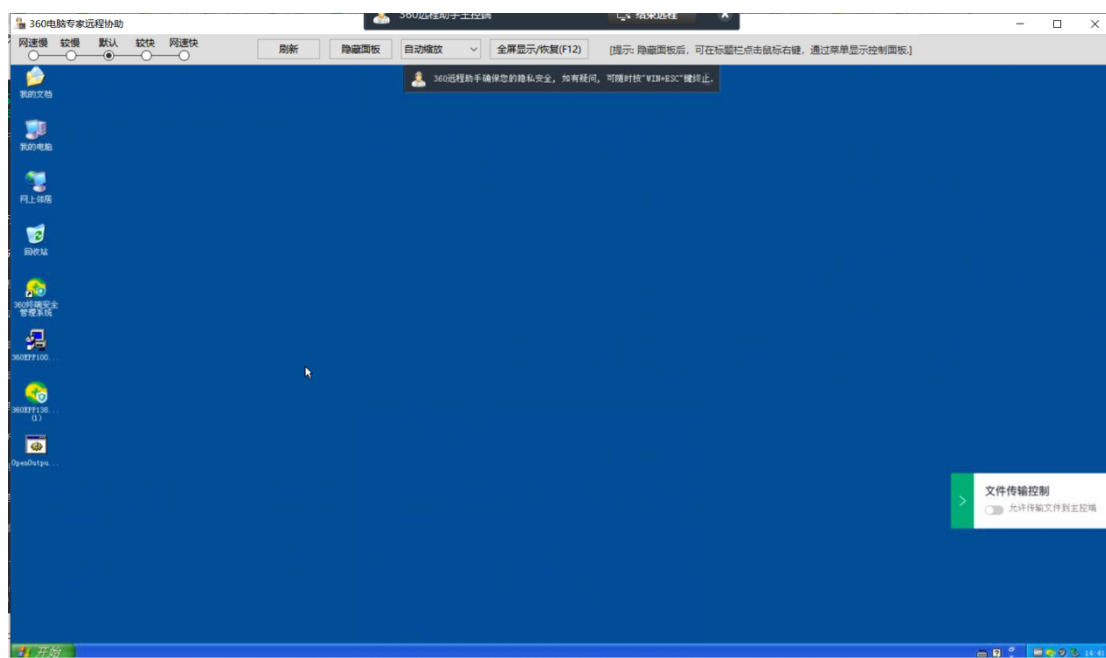


管理中心点击启动应用，首次需要下载 360 远程助手



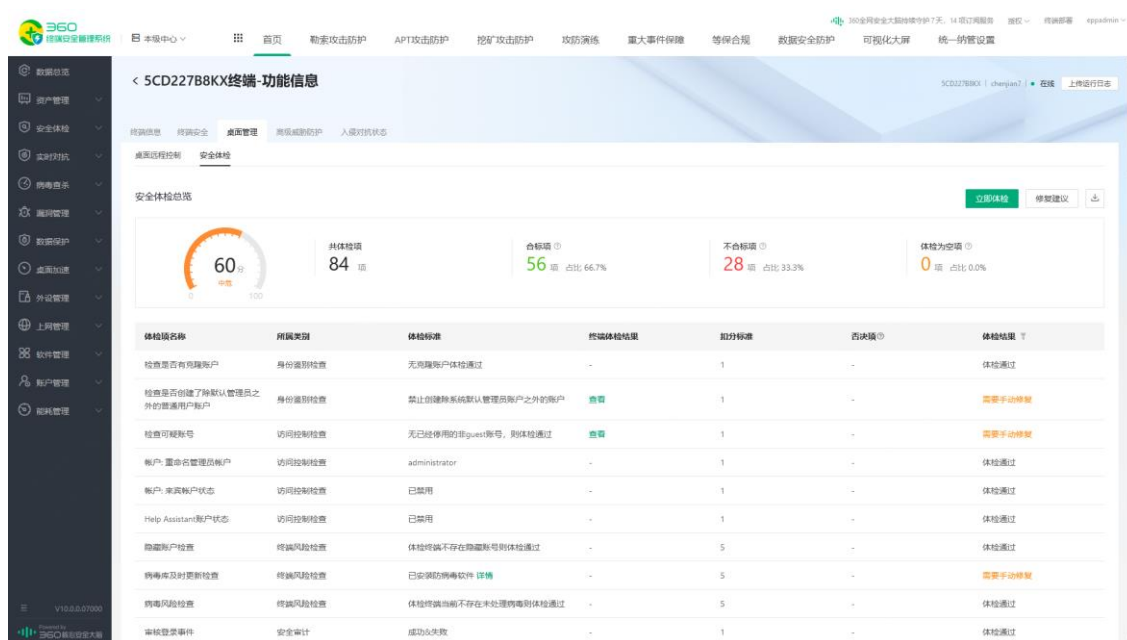
点击上方的开启远程





#### 4.2.5.2.2. 安全检查

点击左侧功能导航：资产管理>终端管理>终端概况>终端详情>桌面管理>安全检查，可查看此终端的安全检查情况。



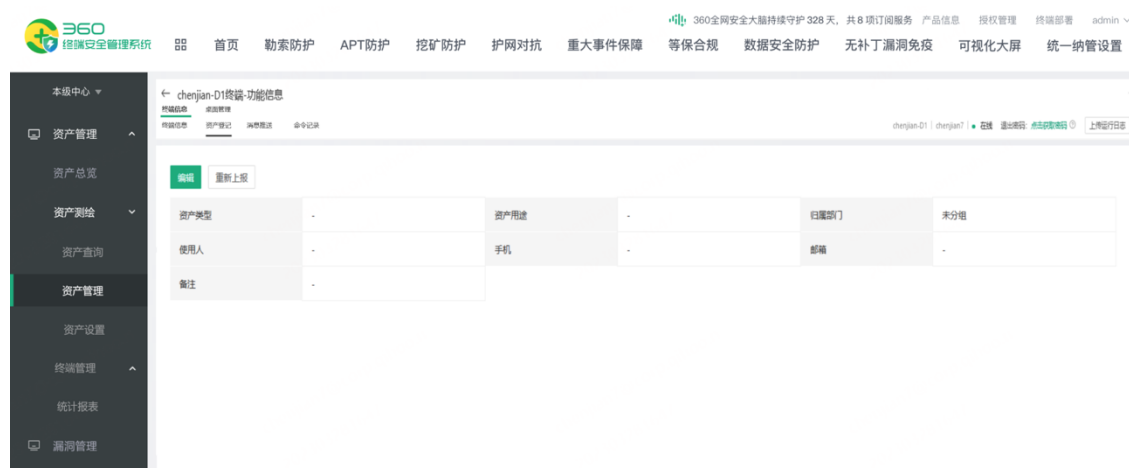
#### 4.2.5.3. 卸载/退出密码

可查看此终端名称、用户名、状态、卸载密码、退出密码。此处显示的相关密码，由终端策略配置决定。若此终端配置的策略为动态口令，则显示对应卸载密码、退出密码的动态口



令，如只配置了某一个动态口令，则只显示配置为动态口令的对应密码。会显示 tip “动态密码每天更新一次，使用动态密码时，请终端设备的日期保持和服务端一致。当前服务器日期：2022-10-09”。如策略配置为使用固定密码，则不显示此行以及 tip 图标。

点击左侧功能导航：**资产管理>终端管理>终端概况>终端详情>终端信息**，查看退出/卸载密码。



#### 4.2.5.4.上传运行日志

可点击“上传运行日志”按钮，对终端下发指令，对其运行日志进行采集。

点击左侧功能导航：**资产管理>终端管理>终端概况>终端详情>终端信息**，点击按钮，完成指令下发。





## 5. 实时对抗

### 5.1. 实时防御

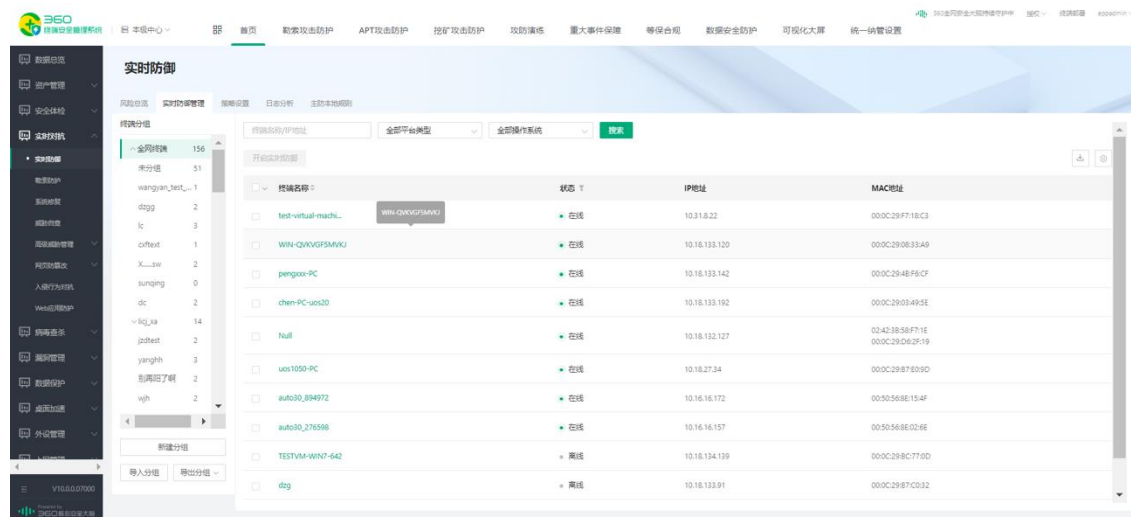
#### 5.1.1. 风险总览

点击左侧功能导航：**实时对抗**》**实时防御**》**风险总览**进行查看，包括勒索病毒拦截次数，挖矿病毒拦截次数，拦截横向渗透次数，拦截黑客入侵次数，拦截漏洞入侵次、拦截钓鱼邮件次数、拦截账号爆破次数、拦截木马病毒次数、拦截病毒驻留次数、拦截盗取凭证次数等重点关注信息，以及其它事件统计和趋势图等。



#### 5.1.2. 实时防御管理

点击左侧功能导航：**实时对抗**》**实时防御**》**实时防御管理**进行查看，在此界面可以批量开启实时防御功能。

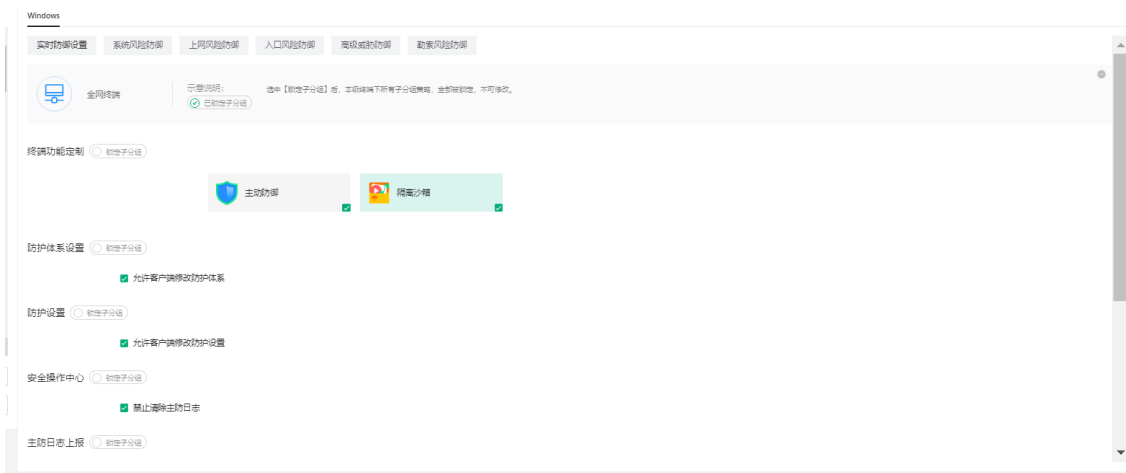


### 5.1.3.策略设置

点击左侧功能导航：**实时对抗** > **实时防御** > **策略设置**，主要区分为实时防御设置，系统风险防御、上网风险防御、入口风险防御、高级威胁防御以及勒索风险防御。

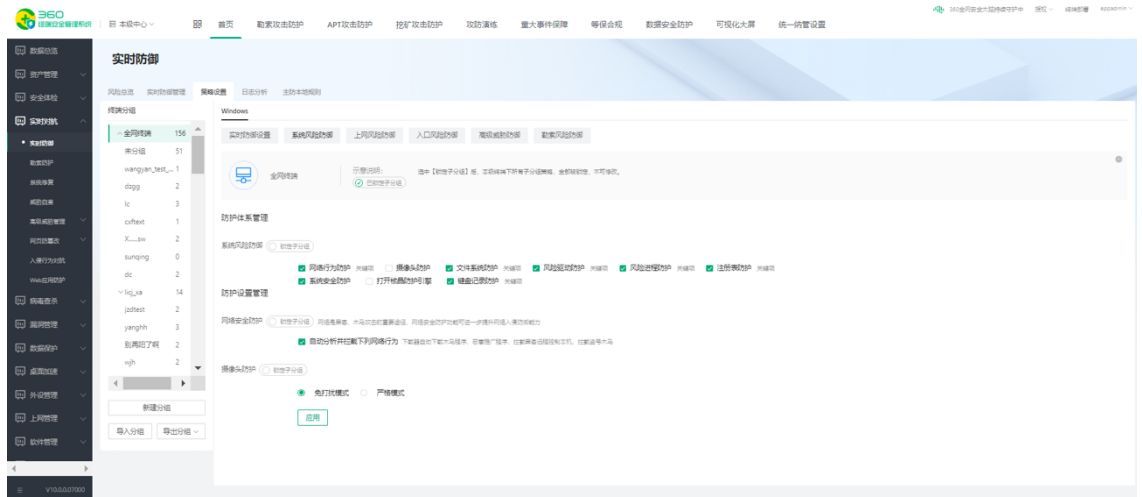
#### ● 基本设置

此页面支持对实时防御的一些基础策略进行配置，包括模块化下发，主防日志上报等。



#### ● 系统风险防御

此页面支持对进程，注册表和驱动等相关系统风险策略进行配置。



## ● 上网风险防御

此页面支持对网页安全、网购安全、搜索安全和邮件等上网安全的策略进行配置。



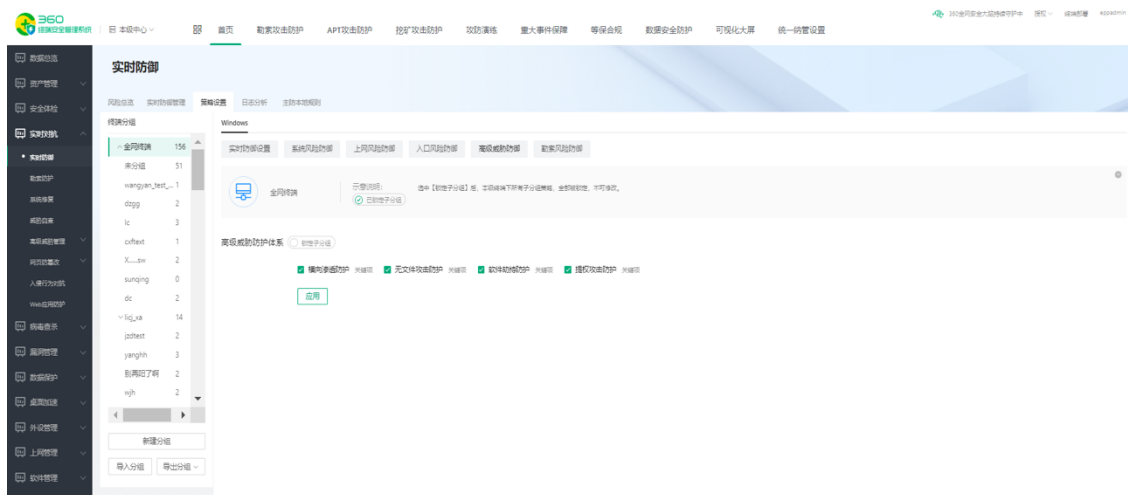
## ● 入口风险防御

此页面支持对聊天、下载和安全等入口相关的策略进行配置。



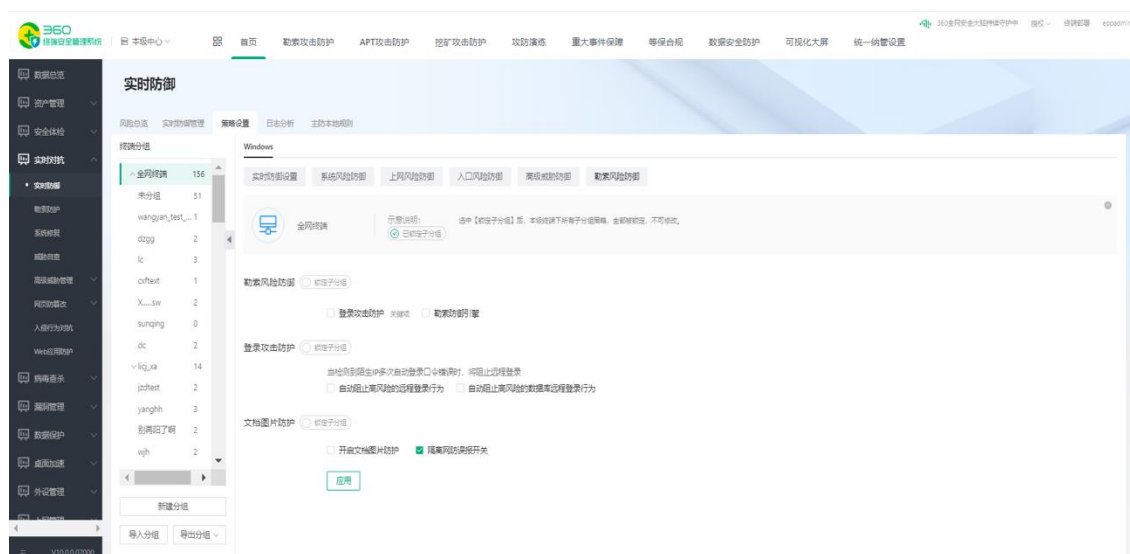
## ● 高级威胁防御

此页面横向渗透防护、无文件攻击防护、软件劫持防护和提前攻击防护等高级威胁相关的策略进行配置。



## ● 勒索风险防御

此页面支持对登录攻击防护和勒索防护引擎相关的勒索防护策略进行配置。

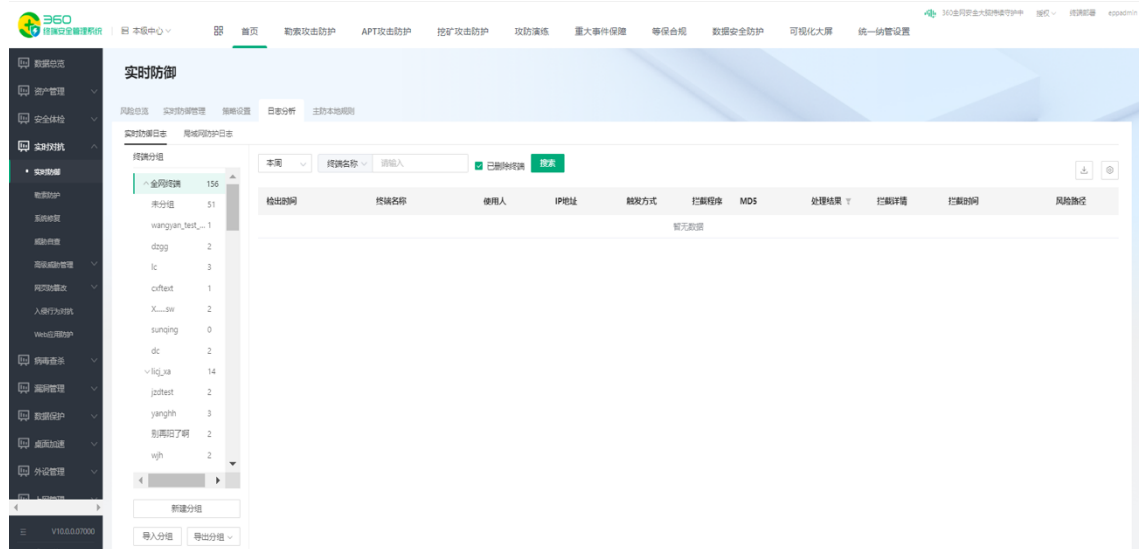


### 5.1.4.1 日志分析

点击左侧功能导航：**实时对抗** > **实时防御** > **日志分析**，可以查看实时防御日志好局域网防护日志。

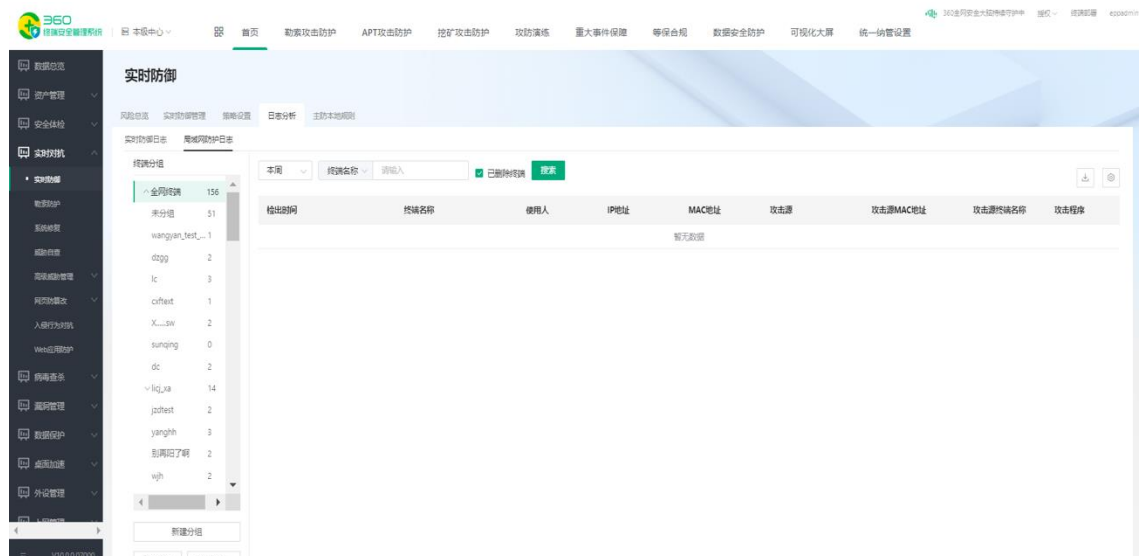
## 6.2.4.1.实时防御日志

默认查看一周日志，管理员可以自定义时间段查看实时防御日志，可导出报表。



## 6.2.4.2.局域网防护日志

默认查看一周日志，管理员可以自定义时间段查看局域网防护详情。可导出报表。



## 5.2. 勒索防护

### 5.2.1. 勒索总览

勒索防护支持拦截 VNC 攻击，远程登录成功，拦截 RPC 攻击，拦截 TELNET 攻击，拦截 SMB 攻击，拦截 FTP 攻击，拦截 TOMCAT 暴力破解的攻击拦截。

RPC、VNC、Telnet 是常用于远程连接的协议，其中 RPC 可能被用于爆破攻击 Windows 的账号和密码。

Tomcat: web 服务器，可能被用于爆破 web 服务器管理后台的账号和密码。

SMB、FTP: 分别是网络文件共享和文件传输协议。

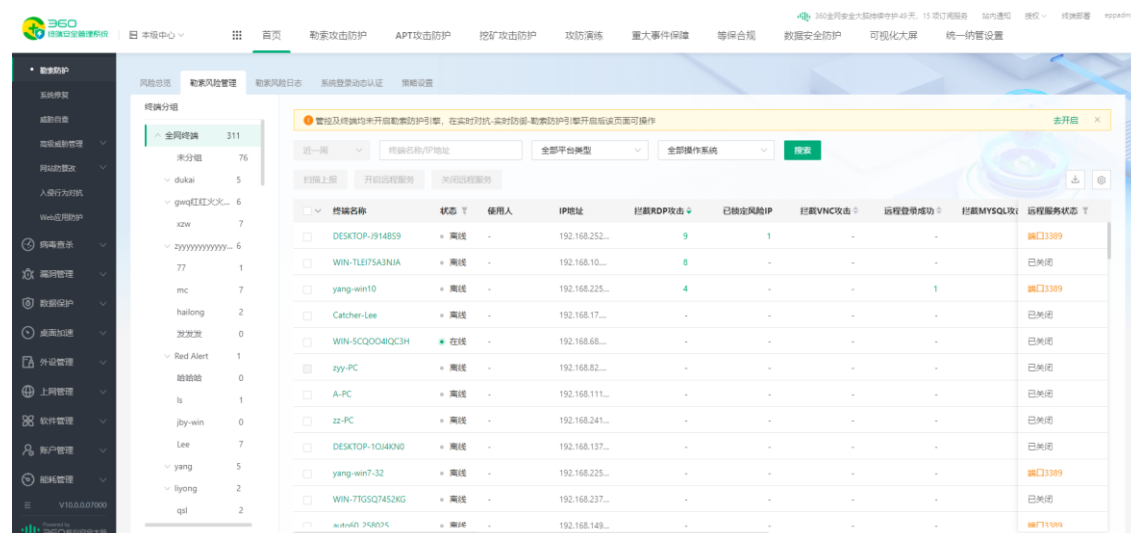


### 5.2.2. 勒索管理

点击右侧功能导航：**实时对抗》勒索防护》勒索管理**

以终端为维度显示勒索防护相关信息。列表展示：终端名称、状态、拦截 VNC 攻击，远程登录成功，拦截 RPC 攻击，拦截 TELNET 攻击，拦截 SMB 攻击，拦截 FTP 攻击，拦截 TOMCAT、锁定 ip、弱密码账号、弱密码软件、远程服务状态。

支持“扫描上报”、“开启远程服务”、“关闭远程服务”功能，支持导出列表数据至 excel、csv。

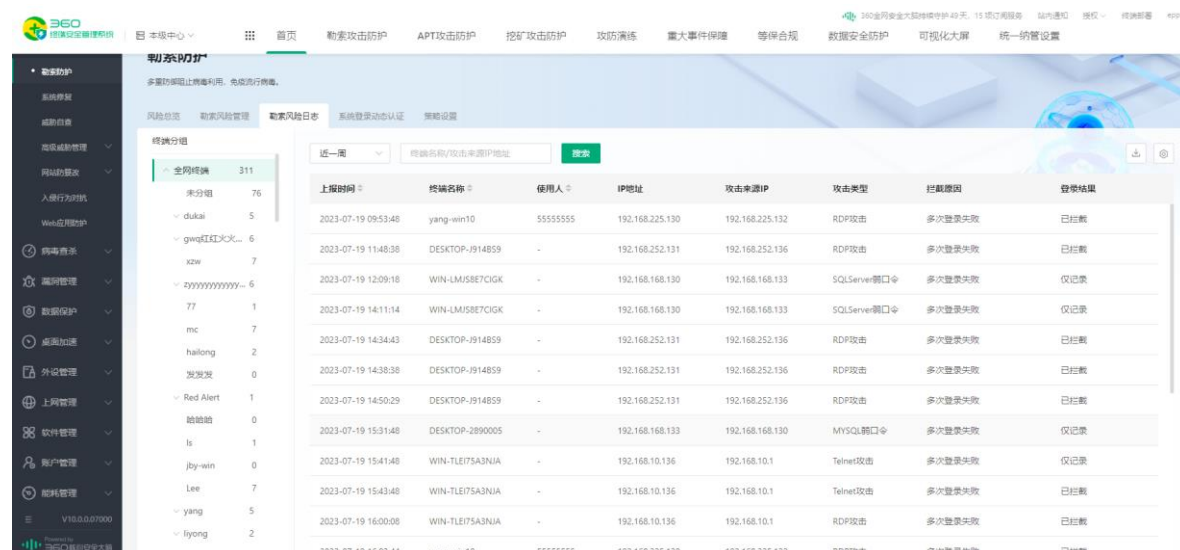


终端动态认未开启防护策略的终端，需先开启对应的防护策略：

**实时对抗〉实时防御〉策略设置〉勒索风险防御：**开启相关的系统防护体系和系统防护设置开关。

## 5.2.3. 勒索风险日志

默认查看近一周日志，管理员可以自定义时间段查看勒索风险日志，可支持导出报表。



## 5.2.4. 系统多因素认证

作为企业内访问控制的第一道防线，单一的身份认证方式已经不足以抵挡内外部勒索、暴力破解等各类威胁，而将系统多因素认证可以极大的提高终端安全性。

## 6.3.2.1.服务端

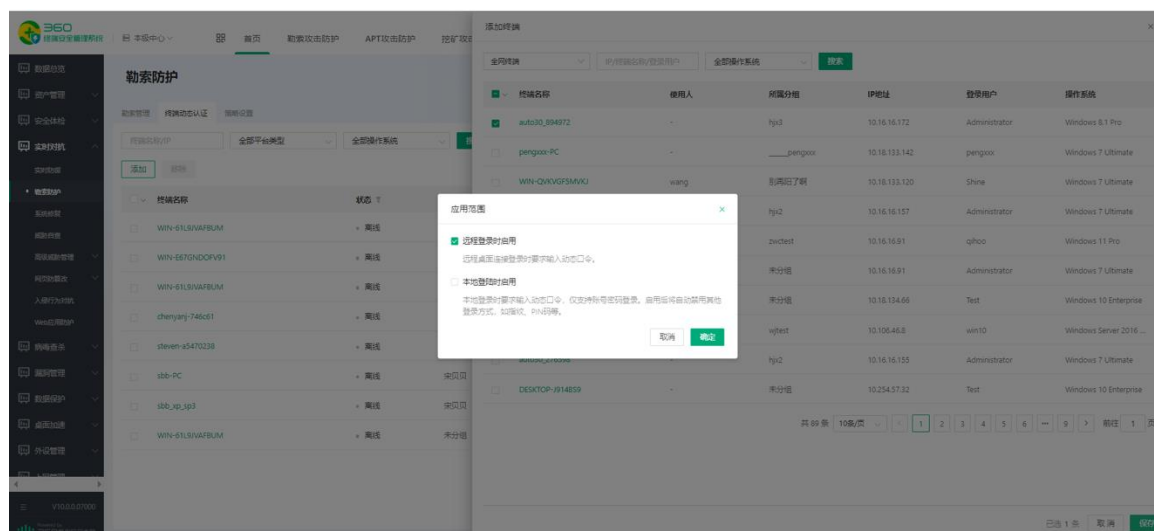
点击功能导航：实时对抗〉勒索防护〉终端动态认证，支持对系统本地登录和远程登录进行多因素认证。

以终端为维度显示系统多因素认证相关信息。列表展示：终端名称、状态、所属分组、ip地址、MAC地址等（可根据设备显示列表展示内容），支持导出列表数据至 excel、csv：



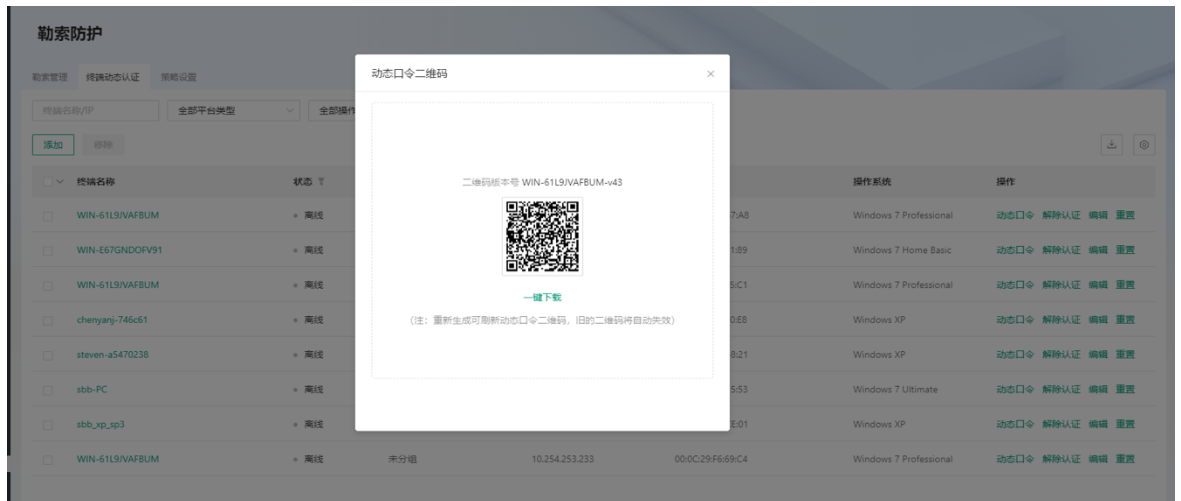
### ● 添加认证终端

选择相应的终端和应用范围，点击确认生效。

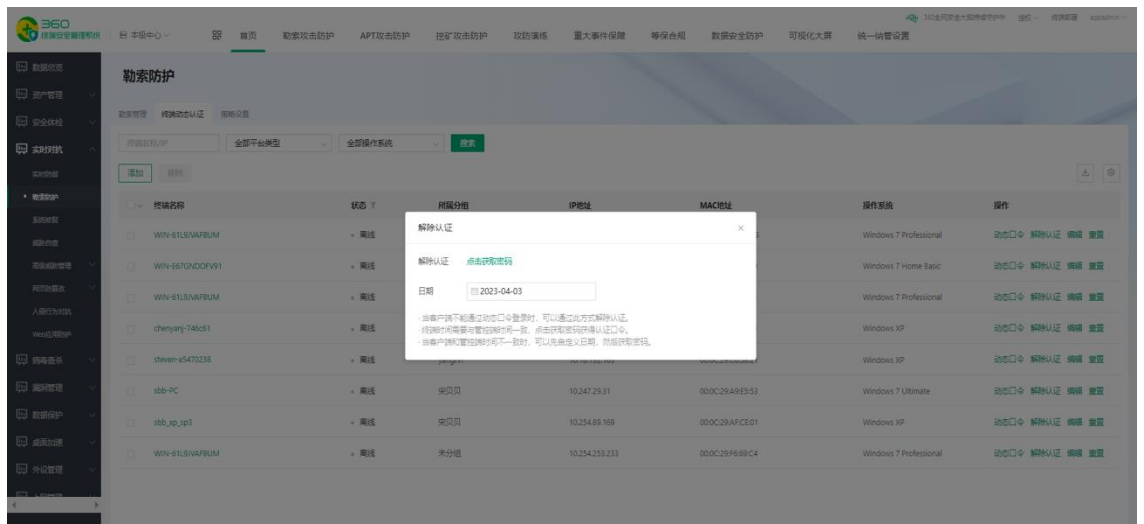


添加终端成功后，管理员点击“动态口令”按钮，获取口令二维码。然后将二维码发送至终端用户，用户使用“360 终端安全动态口令认证”小程序扫描该二维码即可。

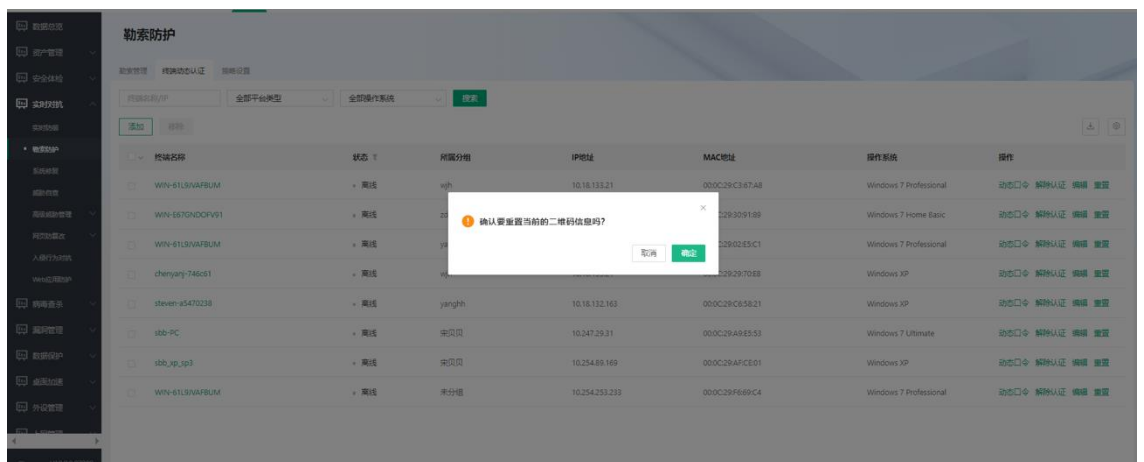




## ● 解除认证

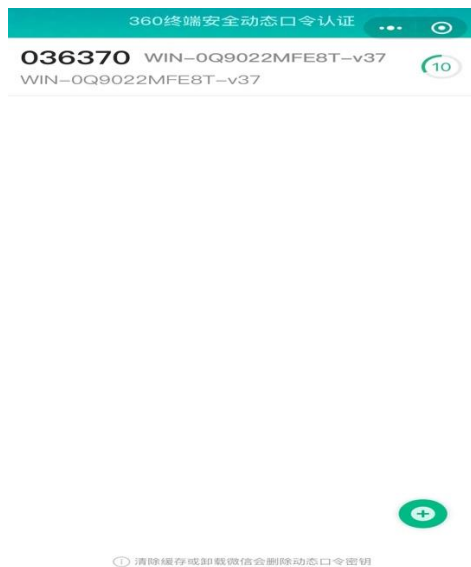


## ● 重置多因素认证

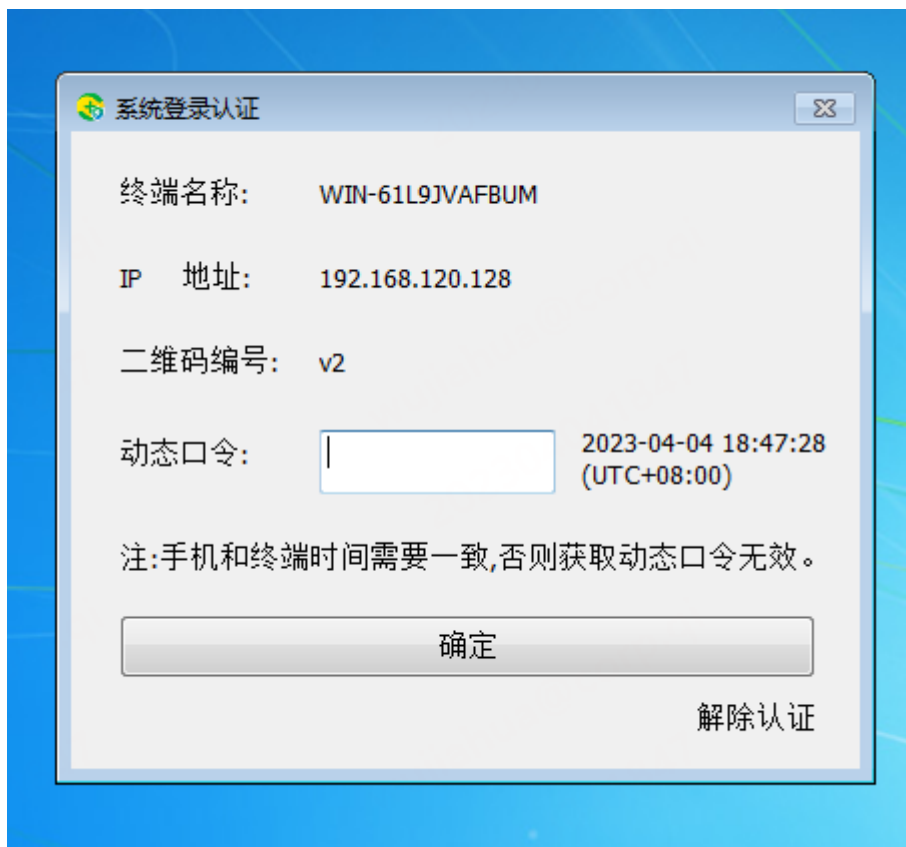


### 6.3.2.2.客户端

微信搜索 360 终端安全动态口令认证，并通过管理员处获得的二维码进行绑定。



当开启系统多因素认证功能后，无论是本地还是远程登录用户计算机时，都将弹出动态口令安全认证窗口。若用户设置了计算机密码，则该弹窗将在用户输入正确的账户密码后弹出；如果用户未设置计算机密码，则该弹窗开机直接弹出。用户需再次输入正确的动态口令才可登录计算机。



#### 备注:

当客户端多因子认证不通时, 建议通过管理员重新生成二维码重新绑定或者解除认证。  
如果仍然不通过时可以通过管控端移除, 重启客户端重新添加。

### 5.2.5. 策略设置

点击功能导航: **实时对抗》勒索防护》策略设置**, 支持对购买的功能进行模块化安装和卸载。

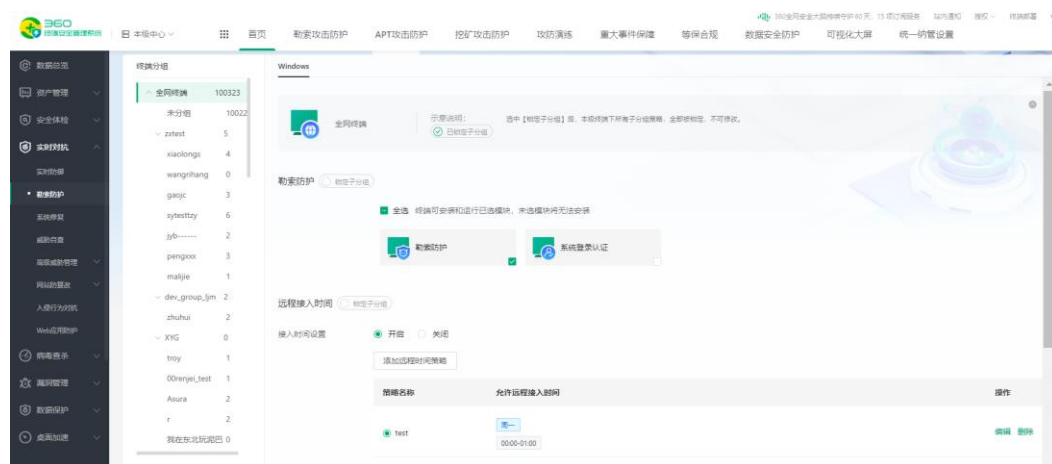
#### 风险 IP 和境外 IP 拦截

勒索防护支持自定义配置同一 IP 暴力破解登录的次数和时间限制, 客户端按照自定义的次数和时间段进行配置。



## 勒索防护增强，支持远程登陆使用限制

勒索防护支持按照时间段来限制远程桌面的登录时间，只有策略配置时间范围内才能远程登录，其它时间禁止登录



## 勒索防护增强，暴力破解次数、自动封禁可配置

勒索防护支持自定义配置同一 IP 暴力破解登录的次数和时间限制，客户端按照自定义的次数和时间段进行配置。



## 6. 病毒查杀

### 6.1. 基本概念

#### 6.1.1. 快速扫描

**快速扫描：**扫描耗时短，有效扫描随系统自启动运行的风险文件。主要扫描系统常被利用的位置，包含注册表启动项、桌面、开始菜单、快速启动栏、系统关键目录等。

#### 6.1.2. 全盘扫描

**全盘扫描：**全面扫描计算机，包含快速扫描内容以及所有硬盘文件，清理磁盘中木马病毒更彻底。

#### 6.1.3. 强力扫描

**强力扫描：**通过选择 扫描模式+终端信任区+引擎数量 对终端进行检测扫描。

#### 6.1.4. 宏病毒扫描

**宏病毒扫描：**宏病毒扫描是 360 公司推出 Office 宏病毒扫描“专杀”，可全面查杀寄生在 Excel、Word 等文档中的 Office 宏病毒

#### 6.1.5. 隔离区

**隔离区：**恢复区是终端病毒文件被隔离后，本地备份保存的功能，此时病毒文件加密备份在系统硬盘上，可随时恢复回来。当在恢复区中执行删除操作后，该文件才彻底从硬盘上删掉

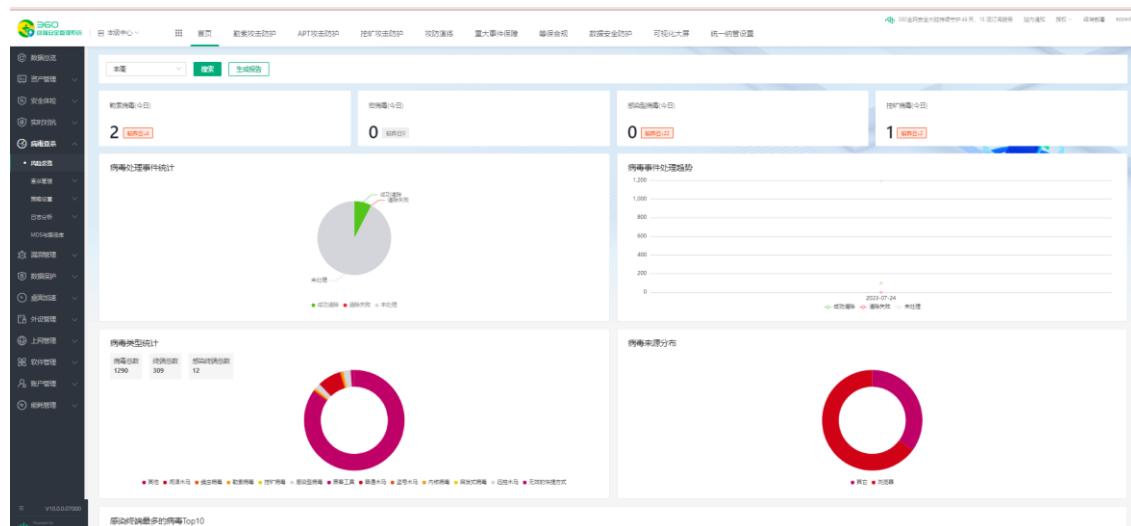
#### 6.1.6. 信任区

**信任区：**信任区是终端加白的一种机制，当发现自己正常软件被误报为黑时，通过添加信任的操作避免文件被查杀。

## 6.2. 风险总览

点击左侧功能导航：病毒查杀〉高风险总览

风险总览支持对客户关注感染性病毒，挖矿病毒，勒索病毒和宏病毒，病毒来源以及其它病毒事件统计进行可视化展示。



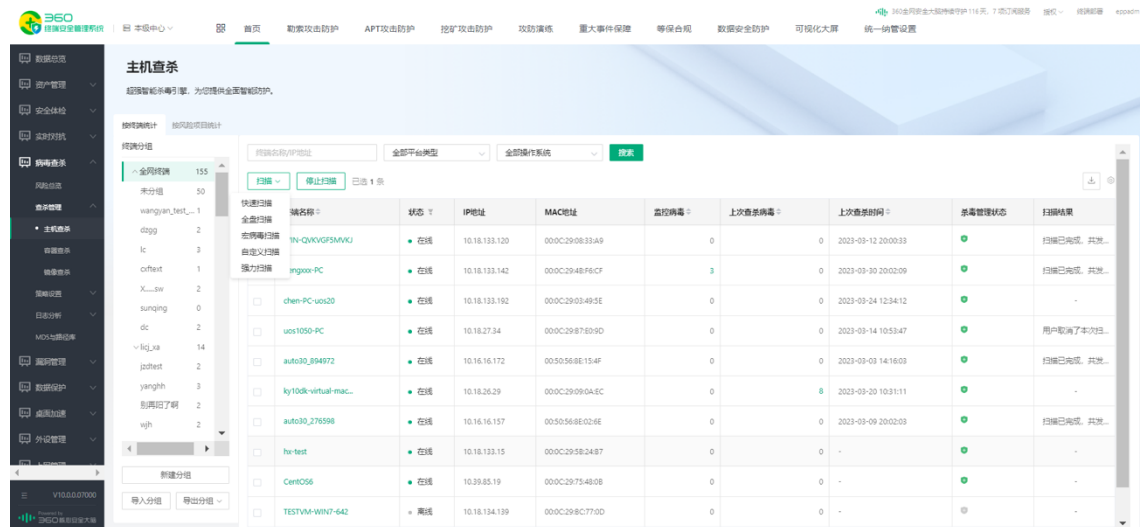
## 6.3. 查杀管理

### 6.3.1. 主机查杀

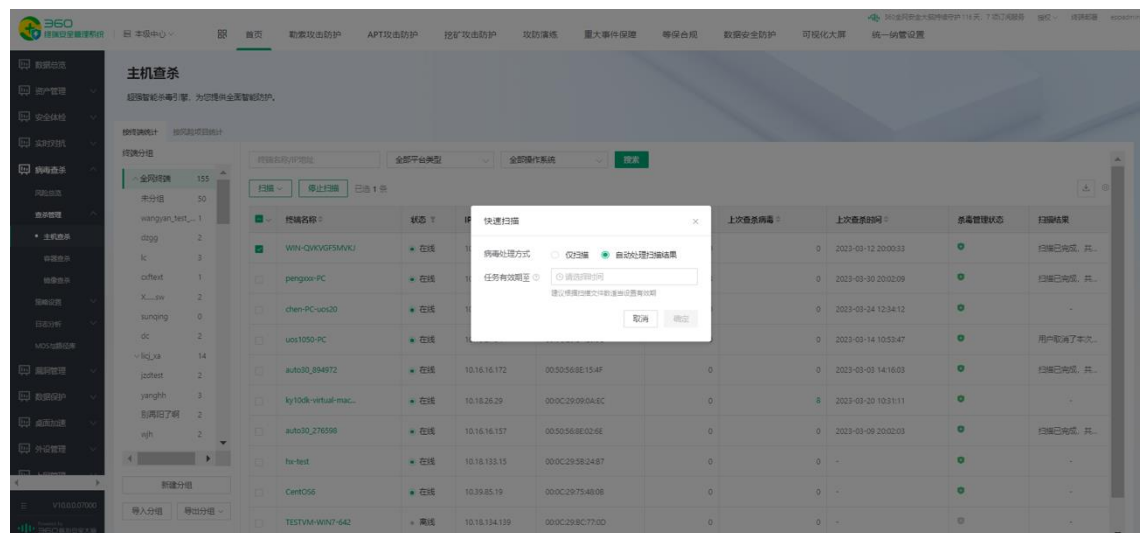
点击左侧功能导航：病毒查杀〉查杀管理〉主机查杀

### 6.3.2. 按终端统计

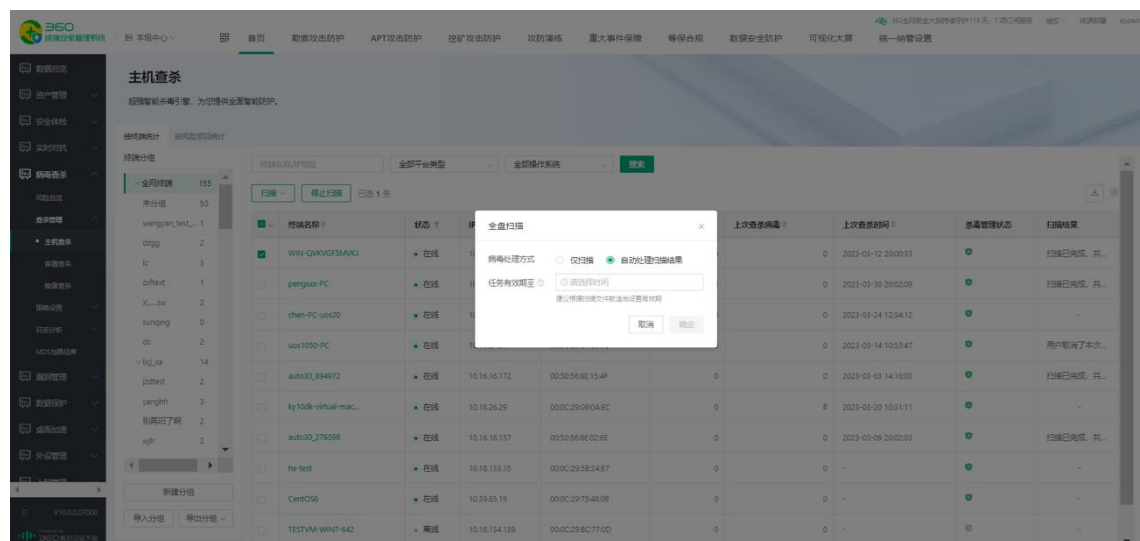
点击左侧功能导航：病毒查杀〉查杀管理〉主机查杀〉按终端统计



## 快速扫描



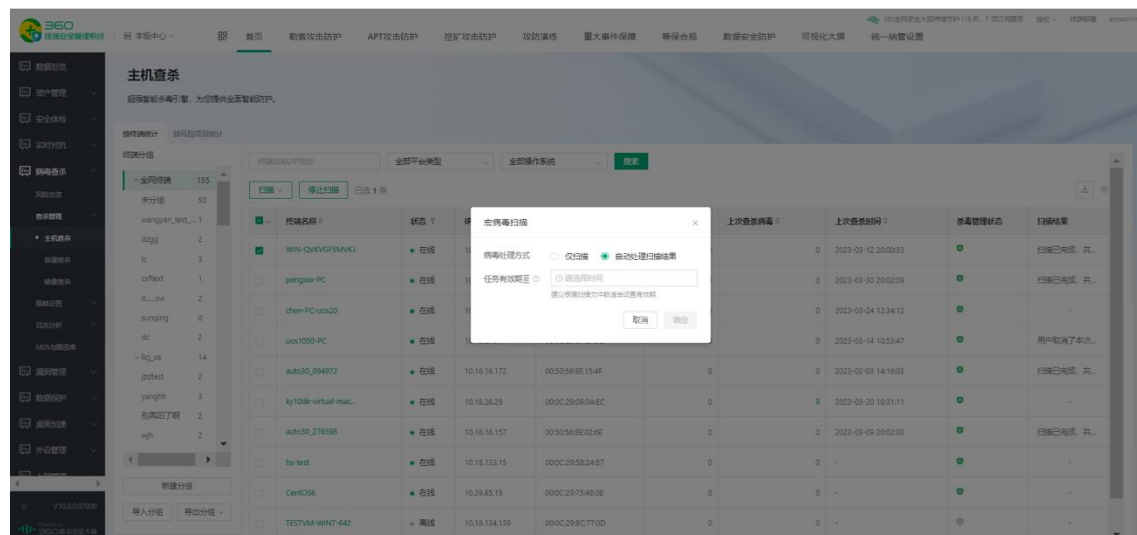
## 全盘扫描



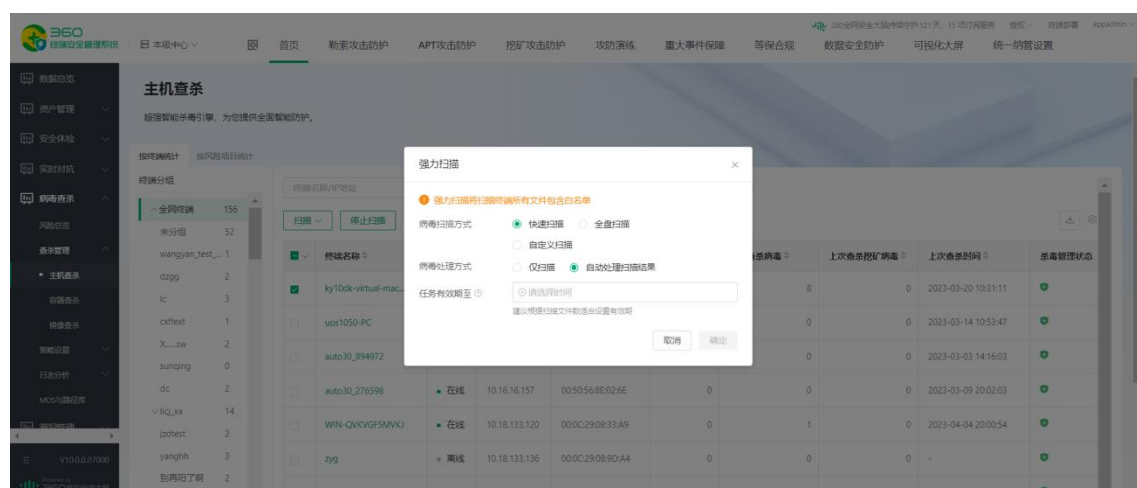
## 自定义扫描



## 宏病毒扫描



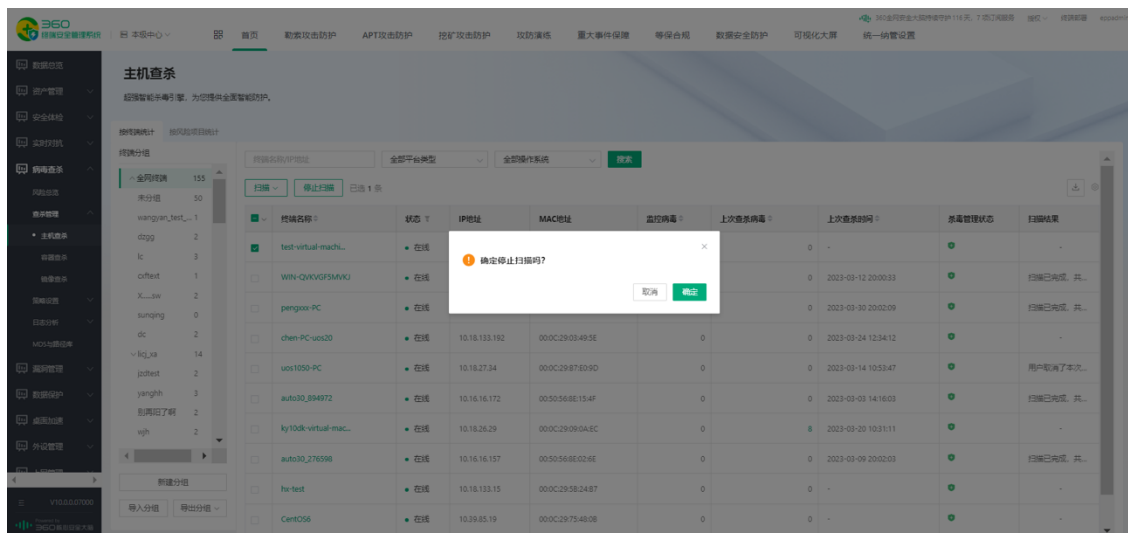
## 强力扫描



## 停止扫描

支持停止客户端正在进行的病毒扫描。





### 6.3.3. 按项目统计

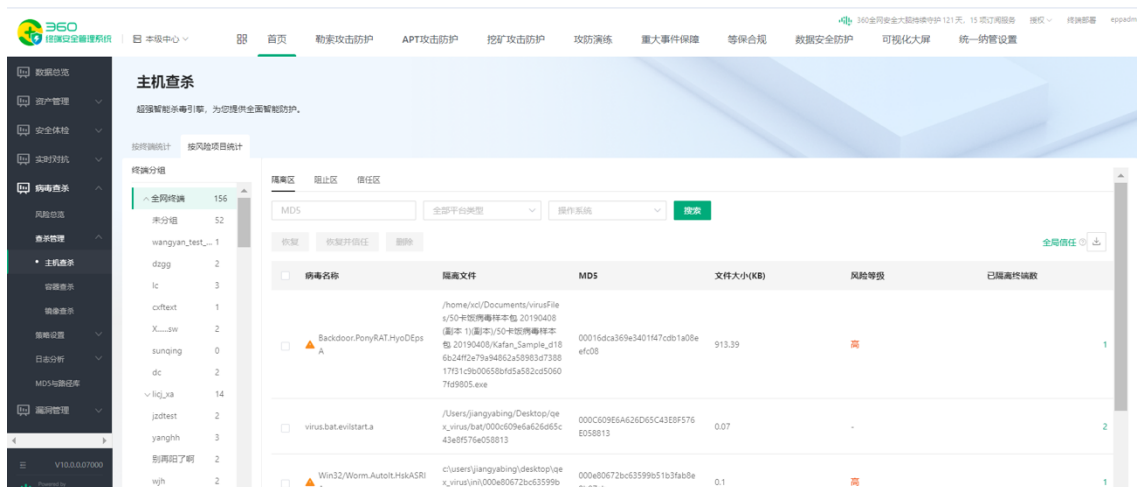
点击左侧功能导航：病毒查杀〉查杀管理〉主机查杀〉按项目统计

#### ● 隔离区

显示当前终端分组的隔离区信息，可以按 MD5、平台类型、操作系统进行搜索，并可以按照当前搜索条件的结果进行导出。

恢复功能，选中病毒，恢复隔离区病毒（注意：恢复病毒 MD5 相同的所有病毒）

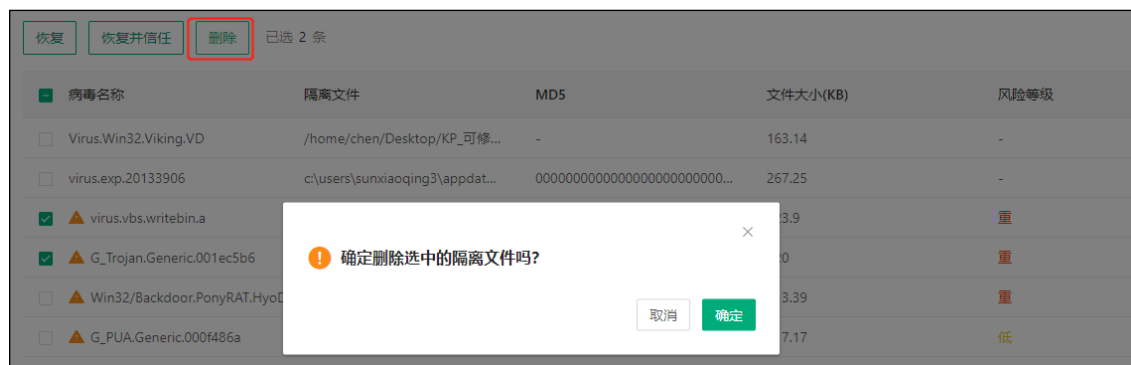
恢复并信任功能，选中病毒，恢复隔离区病毒并加入信任区（注意：恢复并信任病毒 MD5 相同的所有病毒）



## 恢复并信任



删除功能，选中病毒，隔离区删除（注意：病毒 MD5 相同的所有病毒被删除）



## ● 阻止区

显示当前终端分组的阻止区信息，可以按 MD5、平台类型、操作系统进行搜索，并可以按照当前搜索条件的结果进行导出（注：此功能为 windows 客户端特有）



阻止的效果展示：



移除功能，移除阻止区所选的 URL（注意：MD5 相同的 URL 被移除阻止区）

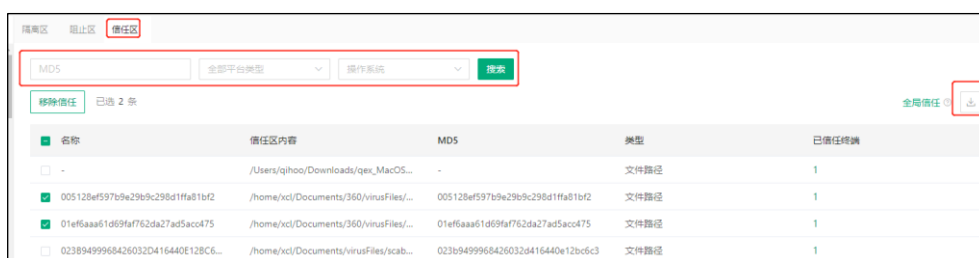


添加信任功能，信任阻止区的所选的 url，（注意：信任 MD5 相同的 URL）

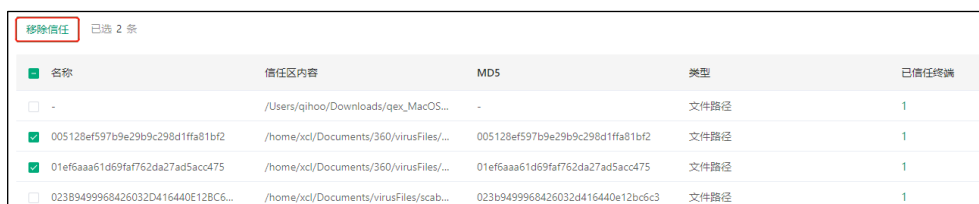


## ● 信任区

显示当前终端分组的信任区信息，可以按 MD5、平台类型、操作系统进行搜索，并可以按照当前搜索条件的结果进行导出



移除信任功能，选中病毒，信任区移除病毒（注意：病毒 MD5 相同的所有病毒都被移除信任区）

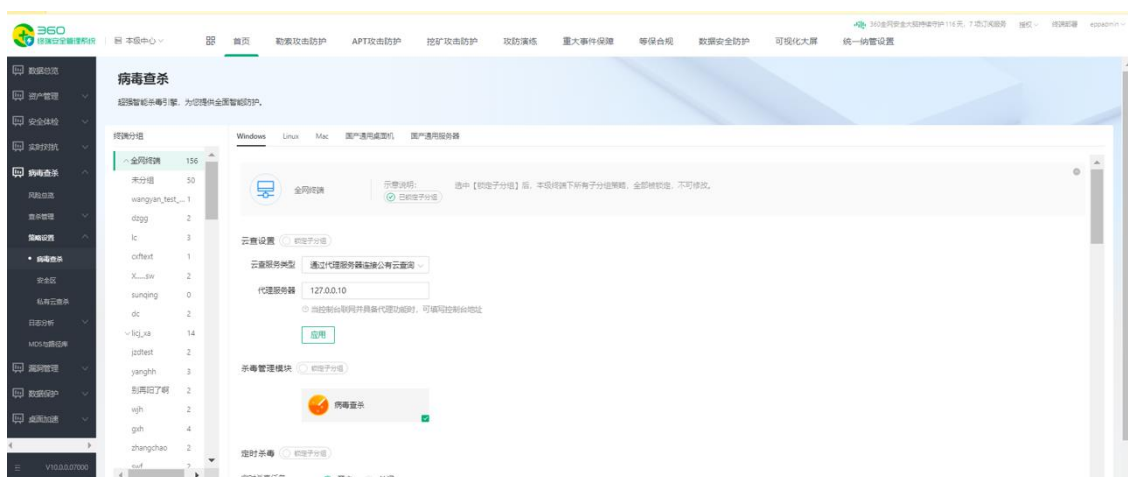


## 6.4. 策略设置

### 6.4.1. 病毒查杀

点击左侧功能导航：病毒查杀》策略设置》病毒查杀，支持 Windows、Linux、Mac、国

产桌面机和国产服务器的病毒查杀策略设置。



## 6.4.1.1.Windows

点击左侧功能导航：病毒查杀》策略设置》病毒查杀》Windows

### (1) 云查设置



### (2) 定时杀毒

设置定期每天或每周或每月指定时间刻进行快速扫描、全盘扫描、自定义和宏病毒。其中，定时任务增加最大扫描时长选择项，当客户端杀毒扫描时间超过最大时长，停止扫描任务并上报相关病毒日志。



### (3) 上报设置

设置隔离区、阻止区、信任区定时上报时间段。

杀毒状态上报

☐ 锁定子分组

杀毒状态上报任务

☒ 开启
 ☐ 关闭

时间上报间隔

10

分钟

#### (4) 扫描设置

管理员可以对扫描模式、扫描性能、压缩包扫描、扫描内容进行设置。

增加扫描网络驱动器开关，默认开启，客户端查杀扫描时对网络映射驱动器进行扫描，关闭后，查杀扫描时跳过网络映射驱动器。

增加性能自定义配置入口，配置完成后客户端扫描性能受此开关影响。

扫描设置

☐ 锁定子分组

☒ 防感染模式
 ☒ 扫描时允许终端用户暂停、停止扫描任务
 ☒ 扫描网络映射驱动器

病毒扫描资源占用

☐ 速度最快 (扫描速度最快, 但可能影响性能)
 ☒ 性能最佳 (资源占用低, 但扫描速度稍慢)
 ☐ 自定义

压缩包扫描设置

最大扫描

1

层压缩包

跳过大于

5

MB 的压缩包

扫描内容设置

☐ 扫描时, 跳过系统修复相关的内容

支持跳过大文件



#### (5) 多引擎设置

支持云查杀引擎、Behavioral 脚本引擎、QVM II 人工智能引擎。管理员可配置云查询引擎的模式，共 4 种，分别为直接连接到公有云查询、通过代理服务器（管控中心）连接到公有云查询、直接连接私有云查询，可以选择关闭云查询服务。管理员可关闭 Behavioral 脚本引

擎、QVM II 人工智能引擎，可允许客户端修改设置。

多引擎设置 ☐ 锁定子分组

☒ 允许客户端修改设置

引擎	病毒查杀	实时防护
云查杀引擎	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
QVM II 人工智能引擎	<input type="checkbox"/>	<input type="checkbox"/>
Behavioral脚本引擎	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

#### (6) 未知文件防误杀设置

开启后将减少未知文件误杀，但会降低安全防护能力

未知文件防误杀设置 ☐ 锁定子分组

☒ 开启未知文件防误杀 (开启后将减少未知文件误杀，但会降低安全防护能力)

#### (7) 病毒查杀设置

管理员可设置客户端是否可修改查杀设置，以及发现病毒时的处理方式。支持设置扫描文件类型，可设置全部文件或仅程序和文档。

病毒查杀设置 ☐ 锁定子分组

☒ 允许客户端修改设置

发现病毒时处理方式 ☒ 手动处理，由终端用户选择处理方式  
☐ 自动处理，并将原始文件在隔离区备份

需要扫描的文件类型 ☐ 扫描所有文件  
☒ 仅扫描程序和文档文件

#### (8) 安全操作中心

安全操作中心 ☐ 锁定子分组

病毒扫描 ☒ 允许客户端修改自动清理设置  
☒ 自动清理30天前记录  
☐ 禁止清空日志 (开启后所有日志被保留，将占用客户端存储空间)

实时防护 ☒ 允许客户端修改自动清理设置  
☒ 自动清理30天前记录  
☐ 禁止清空日志 (开启后所有日志被保留，将占用客户端存储空间)

#### (9) 保护等级

保护等级：管理员可根据实际需求设置终端文件监控级别，高、中、低三级，系统默认中级。

保护等级

☐ 锁定子分组

防护等级设置

☒ 允许客户端修改设置

☐ 高 监控文件的所有操作方式，对电脑性能有一定影响

☒ 中 监控文件的执行与写入，极少影响电脑性能

☐ 低 只监控文件执行，不影响电脑性能

#### (10) 实时防护设置

管理员可设置是否允许客户端修改设置：

支持实时防护监控所有文件/仅程序和文档，管理员可以对扫描文件格式进行选择，所有文件或者仅程序和文档。

可设置发现病毒时的处理方式，分手动处理和自动处理两种模式。

实时防护设置

☐ 锁定子分组

发现病毒时处理方式

☒ 允许客户端修改设置

☒ 手动处理，由终端用户选择处理方式

☐ 自动处理，并将原始文件在隔离区备份

需要监控的文件类型

☐ 仅监控程序和文档文件

☒ 监控所有文件

#### (11) 实时防护弹窗模式

实时防护弹窗模式

☐ 锁定子分组

☒ 手动关闭拦截弹窗时，文件不能执行

☐ 手动关闭拦截弹窗时，文件执行并临时添加信任

#### (12) 未知样本鉴定

未知样本鉴定：终端发现可疑威胁，本地引擎无法判断时，将文件生成 MD5 值，发送到互联网云端进行检测判定；默认进行“勾选”：

未知样本鉴定

☐ 锁定子分组

☒ 允许客户端修改设置

☐ 参加文件云安全计划，将未知样本上传到云端鉴定中心进行安全鉴定

应用

### 6.4.1.2.Linux

点击左侧功能导航：策略中心〉终端策略〉Linux〉杀毒管理

#### (1) 云查设置

根据用户部署模式可配置云查询模式，包括直接连接到公有云查询、通过代理服务器连接到公有云查、直接连接私有云查询（需采购私有云模块）。

## (2) 定时杀毒

设置定期每天或每周或每月指定时间进行快速扫描、全盘扫描和自定义扫描。其中，定时任务增加最大扫描时长选择项，当客户端杀毒扫描时间超过最大时长，停止扫描任务并上报相关病毒日志。

## (3) 扫描设置

管理员可以对扫描模式、扫描性能、压缩包扫描、扫描内容进行设置。

支持防感染模式开启/关闭设置。扫描到感染型病毒时，进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件；

支持扫描网络影射驱动器开关设置，默认开启，客户端查杀扫描时对网络映射驱动器进行扫描，关闭后，查杀扫描时跳过网络映射驱动器；

支持病毒扫描资源占用性能选择，可设置病毒扫描资源占用模式配置，速度最快将不限制扫描时 CPU 资源的占用，程序进行动态自行调整，最快完成扫描。性能最佳表明 CPU 资源低占用扫描，扫描时间会稍微长；

支持压缩包扫描开关设置，默认关闭状态，不对压缩包进行解压扫描，打开后，客户端扫描时对压缩包进行解压缩扫描。

支持对内存病毒进行扫描，对运行的病毒进行扫描查杀，发现病毒后支持结束进程和隔



离文件的处置。

扫描设置 ☐ 锁定子分组

☒ 防感染模式

☒ 扫描时允许终端用户暂停、停止扫描任务

☒ 扫描网络映射驱动器

☐ 内存扫描

病毒扫描资源占用 ☐ 速度最快 (扫描速度最快, 但可能影响性能)

☒ 性能最佳 (资源占用低, 但扫描速度稍慢)

☐ 自定义

压缩包解压扫描设置 ☐ 开启 ☒ 关闭

最大扫描  层压缩包

跳过大于  MB 的压缩包

#### (4) 多引擎设置

支持鲲鹏引擎、QEX 脚本查杀引擎、QVM 查杀引擎、EAV 引擎。管理员可以根据自己的电脑配置及查杀需求对其进行调整。

多引擎设置 ☐ 锁定子分组

内含多个领先的查杀引擎, 已经默认为您选择了最佳组合, 您也可以根据自己的电脑配置及查杀需求对其进行调整。

☒ 鲲鹏引擎 ☒ QEX脚本查杀引擎 ☐ QVM查杀引擎 ☒ EAV引擎

#### (5) 病毒查杀设置

支持设置扫描文件类型, 可设置全部文件或仅程序和文档;

支持对发现病毒时对病毒的处理方式进行设置

病毒查杀设置 ☐ 锁定子分组

发现病毒时处理方式 ☒ 手动处理, 由终端用户选择处理方式

☐ 自动处理, 并将原始文件在隔离区备份

☐ 仅上报但不处理

☐ 自动处理, 并将病毒清除

☐ 自动处理, 并将原始文件删除

需要扫描的文件类型 ☐ 扫描所有文件

☒ 仅扫描程序和文档文件

跳过大于  MB 的文件

## (6) 实时防护

支持允许客户端修改设置，最大扫描压缩包大小；支持设置监控文件类型，可设置全部文件或仅程序和文档；支持对病毒处理方式选择“仅上报但不处理”、“由系统自动处理”和“由用户选择处理”。

实时防护设置
○ 锁定子分组

文件系统实时防护
☒ 开启
☐ 关闭（降低系统消耗）

发现病毒时处理方式
☒ 手动处理，由终端用户选择处理方式
☐ 自动处理，并将原始文件在隔离区备份
☐ 仅上报但不处理
☐ 自动处理，并将病毒清除
☐ 自动处理，并将原始文件删除

跳过大于

2

MB 的文件

需要监控的文件类型
☒ 仅监控程序和文档文件
☐ 监控所有文件

防护等级设置
☐ 高 监控文件的所有操作方式，对电脑性能有一定影响
☐ 中 监控文件的执行与写入，极少影响电脑性能
☒ 低 只监控文件执行，不影响电脑性能

可疑行为防护
☐ 开启可疑行为检测与防护（勒索防护）

## (7) 防护压缩包设置

支持设置监控压缩包的扫描层数，最大扫描压缩包大小；支持设置监控文件类型，可设置全部文件或仅程序和文档。

防护压缩包设置
○ 锁定子分组

监控压缩包设置
☐ 开启
☒ 关闭

最大扫描

2

层压缩包

跳过大于

1

MB 的压缩包

## (8) 病毒溯源

支持开启病毒溯源设置

病毒溯源 ☐ 锁定子分组

开启后会占用一定的空间和性能，同时开启实时防御的文件系统防护，恶意邮件防护，聊天安全防护，下载病毒查杀项。

☒ 开启 ☐ 关闭

应用

## 6.4.2. 安全区

点击左侧功能导航：病毒查杀〉策略设置〉安全区



### 6.4.2.1. Windows

(1) 支持隔离区自动清理设置。

支持设置存储空间上限。鼠标 hover 时，悬浮显示：“上限范围：1-100 之间的整数，设置的存储上限小于终端隔离区已用空间时，若开启了文件的自动清理，则会触发自动清理机制”。

隔离文件自动清理机制分为两种，为单项选择。A. 已达上限 90%时，自动清理隔离区中超过“XX 天/周/月/年”的文件；选择该项时，可设置时长，按天、按周、按月、按年；则当隔离区存储空间已达上限 90%时，清除隔离区中超过设置天数的全部隔离文件，默认值为 1 年；B. 已达上限 90%时，自动清理隔离区文件至存储空间剩余上限的“XX”%；选择该项时，则当隔离区存储空间已达上限 90%时，按照隔离文件的发现时间倒序清理隔离区中的隔离文件；（默认填写值为 20%，取值范围 1~100），清理至隔离区剩余可用空间大小为设置的存储空间上限的 XX%。

**隔离区** ☐ 锁定子分组

☐ 禁止清空、恢复和删除隔离区内容 (开启后所有文件被保存, 将占用客户端存储空间)

设置存储空间上限  GB

☒ 隔离文件自动清理

☒ 已达上限90%时, 自动清理隔离区中超过  天的文件

☐ 已达上限90%时, 自动清理隔离区文件至存储空间剩余上限的  %

## (2) 上报设置

上报内容包含隔离区、阻止区和信任区, 上报时间可选 1/3/7/15 天, 为避免终端集中上报造成带宽压力, 客户端将在设置的时间周期内, 随机进行上报, 默认时间为 3 天。

**上报设置** ☐ 锁定子分组

上报内容包含隔离区、阻止区、信任区

上报时间 客户端每隔  天, 自动向服务器上报一次数据

## (3) 全局信任区

首先在 MD5 与路径库页面进行添加, 输入要加白的 MD5 值。

**MD5与路径库**

超强智能引擎引擎, 为您提供全面智能防护。

MD5与路径库

MD5与路径库

MD5与路径库

MD5	路径	添加时间	操作人	备注	操作
-	c:\system32	2023-04-07 09:05:06	espadmin	测试数据	编辑
-	c:\test.exe	2023-04-07 09:05:06	espadmin	测试数据	编辑
-	/home/test/	2023-04-07 09:04:33	espadmin	-	编辑
e4a4238a3b3232323232323232323232	-	2023-04-05 15:02:30	espadmin	测试数据	编辑
-	c:\test.exe	2023-04-05 15:02:30	espadmin	测试数据	编辑
-	123456	2023-03-28 14:44:04	espadmin	-	编辑

然后再全局信任区点击【添加】

**全局信任区** ☐ 锁定子分组

☐ 禁止终端用户管理文件和路径白名单

☐ 客户端显示管控添加文件和路径白名单

MD5与路径白名单

同时, 支持添加文件后缀白名单, 增加同类后缀文件不再会被杀毒和主防报出病毒。

白名单信任区 ☐ 锁定子分组

文件后缀白名单

添加文件后缀白名单会使白名单中的同类文件脱离病毒防护的保护，请慎重添加！

文件后缀如.doc，每次添加一个

添加

#### (4) 全局黑名单

### 6.4.2.2.Mac

#### (1) 隔离区

支持设置存储空间上限。鼠标 hover 时，悬浮显示：“上限范围：1-100 之间的整数，设置的存储上限小于终端隔离区已用空间时，若开启了文件的自动清理，则会触发自动清理机制”。默认值为 20。

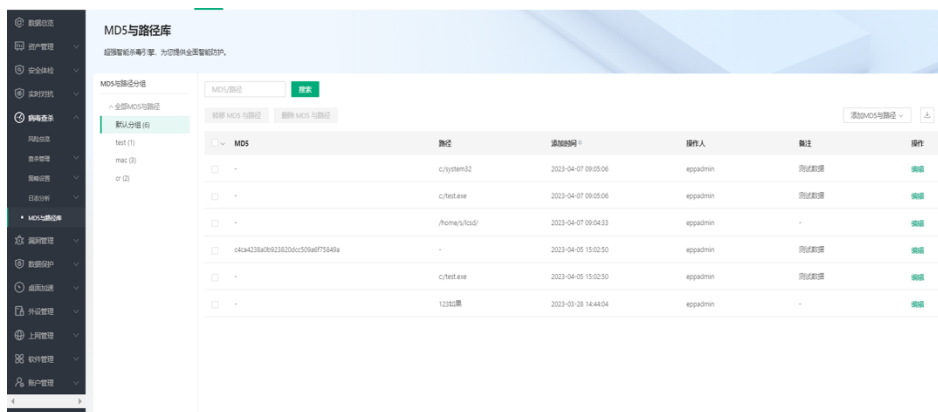
隔离文件自动清理机制分为两种，为单项选择。

A. 已达上限 90%时，自动清理隔离区中超“XX 天”的文件；选择该项时，可按天设置时长；则当隔离区存储空间已达上限 90%时，清除隔离区中超过设置天数的全部隔离文件，默认值为 1 年；

B. 已达上限 90%时，自动清理隔离区文件至存储空间剩余上限的“XX”%；选择该项时，则当隔离区存储空间已达上限 90%时，按照隔离文件的发现时间倒序清理隔离区中的隔离文件；（默认填写值为 20%，取值范围 1~100），清理至隔离区剩余可用空间大小为设置的存储空间上限的 XX%。

#### (2) 全局信任区

首先在 MD5 与路径库页面进行添加，输入要加白的 MD5 值。



然后再全局信任区点击【添加】



同时，支持添加文件后缀白名单，增加同类后缀文件不再会被杀毒和主防报出病毒。

白名单信任区 ☐ 锁定子分坦

文件后缀白名单

添加文件后缀白名单会使白名单中的同类文件脱离病毒防护的保护，请慎重添加！

文件后缀如.doc，每次添加一个

添加

## 6.4.2.3.Linux

### (1) 隔离区

支持设置存储空间上限。鼠标 hover 时，悬浮显示：“上限范围：1-100 之间的整数，设置的存储上限小于终端隔离区已用空间时，若开启了文件的自动清理，则会触发自动清理机制”。默认值为 20。

隔离文件自动清理机制分为两种，为单项选择。

A. 已达上限 90%时，自动清理隔离区中超“XX 天”的文件；选择该项时，可按天设置时长；则当隔离区存储空间已达上限 90%时，清除隔离区中超过设置天数的全部隔离文件，默认值为 1 年；

B. 已达上限 90%时，自动清理隔离区文件至存储空间剩余上限的“XX”%；选择该项时，则当隔离区存储空间已达上限 90%时，按照隔离文件的发现时间倒序清理隔离区中的隔离文件；

（默认填写值为 20%，取值范围 1~100），清理至隔离区剩余可用空间大小为设置的存储空间上限的 XX%。

**隔离区** ☐ 锁定子分组

☐ 禁止清空、恢复和删除隔离区内容（开启后所有文件被保存，将占用客户端存储空间）

设置存储空间上限  GB <sup>①</sup>

☒ 隔离文件自动清理

☒ 已达上限90%时，自动清理隔离区中超过  天的文件

☐ 已达上限90%时，自动清理隔离区文件至存储空间剩余上限的  %

## (2) 全局信任区

首先在 MD5 与路径库页面进行添加，输入要加白的 MD5 值。

**MD5与路径库**

超强智能病毒引擎，为您提供全面智能安全防护。

MD5与路径分组

☐ 删除 MD5 与路径 ☐ 删除 MD5 与路径

<input type="checkbox"/> MD5	路径	添加时间	操作人	备注	操作
<input type="checkbox"/> -	c:\system32	2023-04-07 09:03:06	appadmin	测试数据	<input type="button" value="编辑"/>
<input type="checkbox"/> -	c:\test.exe	2023-04-07 09:03:06	appadmin	测试数据	<input type="button" value="编辑"/>
<input type="checkbox"/> -	/home/ty/fcd/	2023-04-07 09:04:33	appadmin	-	<input type="button" value="编辑"/>
<input type="checkbox"/> 64c4c23a3b3232323232323232323232	-	2023-04-05 15:02:30	appadmin	测试数据	<input type="button" value="编辑"/>
<input type="checkbox"/> -	c:\test.exe	2023-04-05 15:02:30	appadmin	测试数据	<input type="button" value="编辑"/>
<input type="checkbox"/> -	123路路	2023-03-28 14:44:04	appadmin	-	<input type="button" value="编辑"/>

然后再全局信任区点击【添加】

**全局信任区** ☐ 锁定子分组

☐ 禁止终端用户管理文件和路径白名单

☐ 客户端显示管控添加文件和路径白名单

MD5与路径白名单

<input type="checkbox"/> MD5	路径	备注
------------------------------	----	----

## (3) 上报设置

上报内容包含隔离区、阻止区和信任区，上报时间可选 1/3/7/15 天，为避免终端集中上报造成带宽压力，客户端将在设置的时间周期内，随机进行上报，默认时间为 3 天。

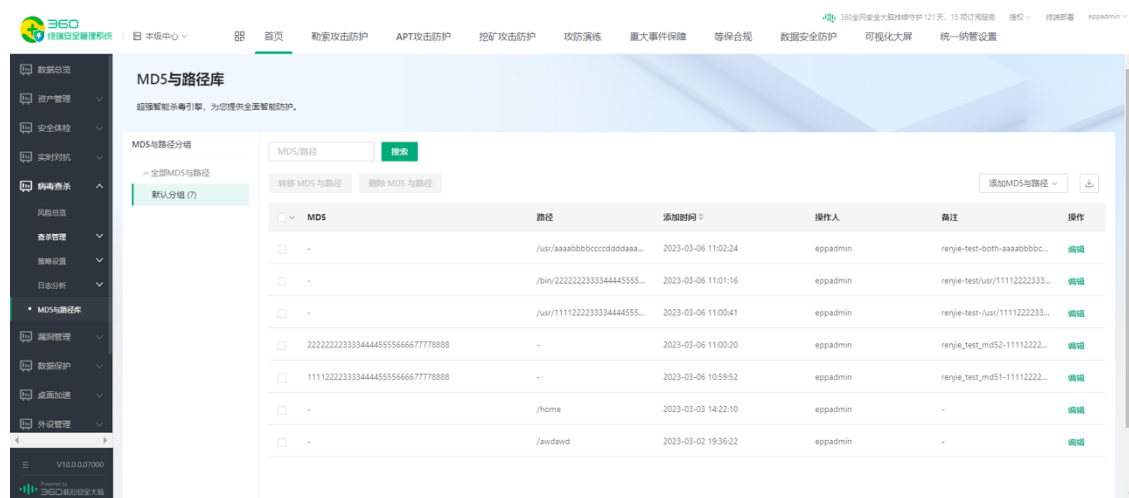
**上报设置** ☐ 锁定子分组

上报内容包含隔离区、阻止区、信任区

上报时间 客户端每隔  天，自动向服务器上报一次数据 <sup>②</sup>

## 6.5. MD5 与路径库

点击左侧功能导航：**病毒查杀 > MD5 与路径库**



支持在识库内添加、编辑、删除 MD5 与路径。同时，可以对 MD5 与路径创建 MD5 与路径组，对 MD5 与路径组进行添加、修改、删除操作。添加完成的 MD5 组，可以在策略黑/白名单中选择 MD5 与路径使用。





## 7. 漏洞管理

### 7.1. 基本概念

#### 7.1.1. 智能忽略

当补丁修复时出现三次修复失败情况，客户端将会自定把该补丁设置成为自动忽略项，不会对该补丁进行再次安装。

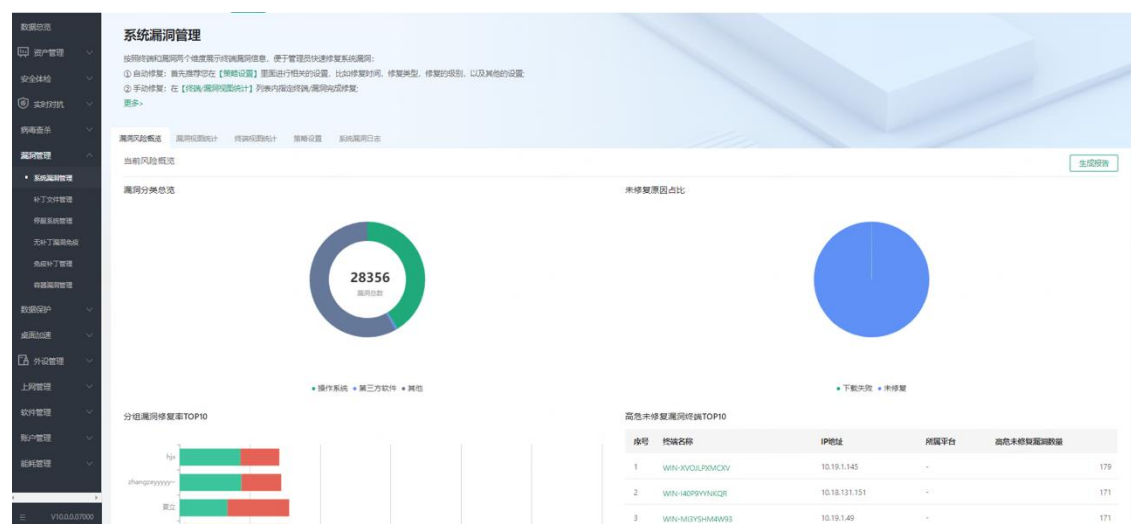
### 7.2. 系统漏洞管理

#### 7.2.1. 漏洞风险概览

点击左侧功能导航：漏洞管理——系统漏洞管理——漏洞风险概览

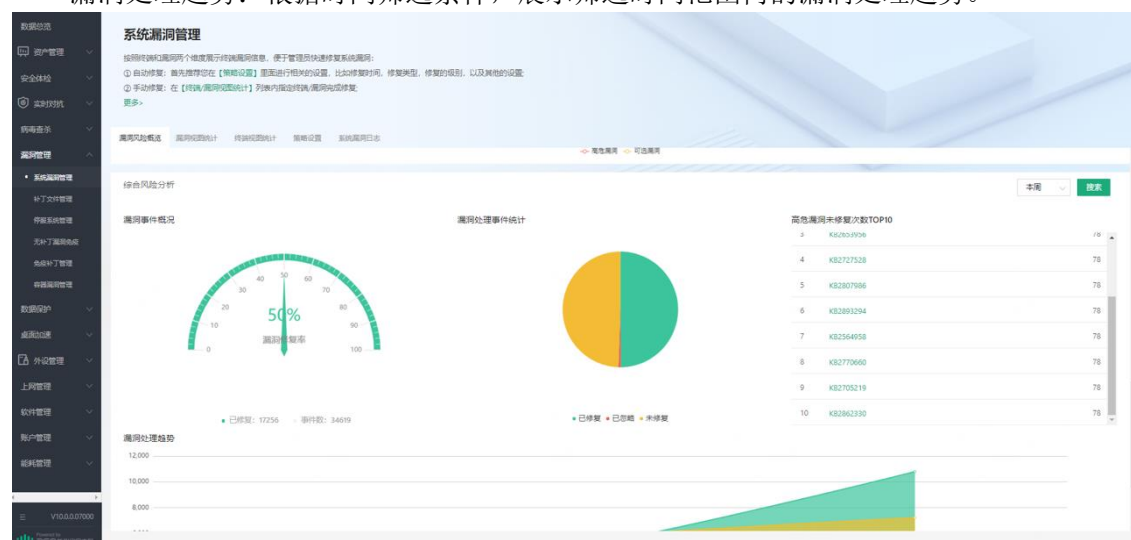
##### A. 当前风险概览

- 漏洞分类总览：统计当前状态下，全网终端检出的漏洞总数，其中类型为操作系统的漏洞个数及占比，类型为第三方软件的漏洞个数及占比。
- 未修复原因占比：统计当前状态下，全网终端检出的未修复漏洞原因占比统计。
- 分组漏洞修复率 TOP10：统计当前状态下，各个分组检查出的未修复、已修复、已忽略、漏洞总数、以及未漏洞修复率的 TOP10。
- 高危未修复漏洞终端 TOP10：统计当前状态下，高危未修复漏洞终端 TOP10。
- 未修复漏洞趋势：统计近 30 天内，每天高危未修复漏洞和可选未修复漏洞的数量趋势。



## B. 综合风险分析



- **漏洞事件概况：**根据时间筛选条件，展示筛选时间范围内的漏洞事件概况。
- **漏洞处理事件统计：**根据时间筛选条件，展示筛选时间范围内的漏洞处理事件统计。
- **高危漏洞未修复次数 TOP10：**统计所选时间范围内，全网终端漏洞检出次数中，漏洞被检出为高危漏洞，且未修复的次数 TOP10。
- **漏洞处理趋势：**根据时间筛选条件，展示筛选时间范围内的漏洞处理趋势。



## 7.2.2.漏洞视图统计

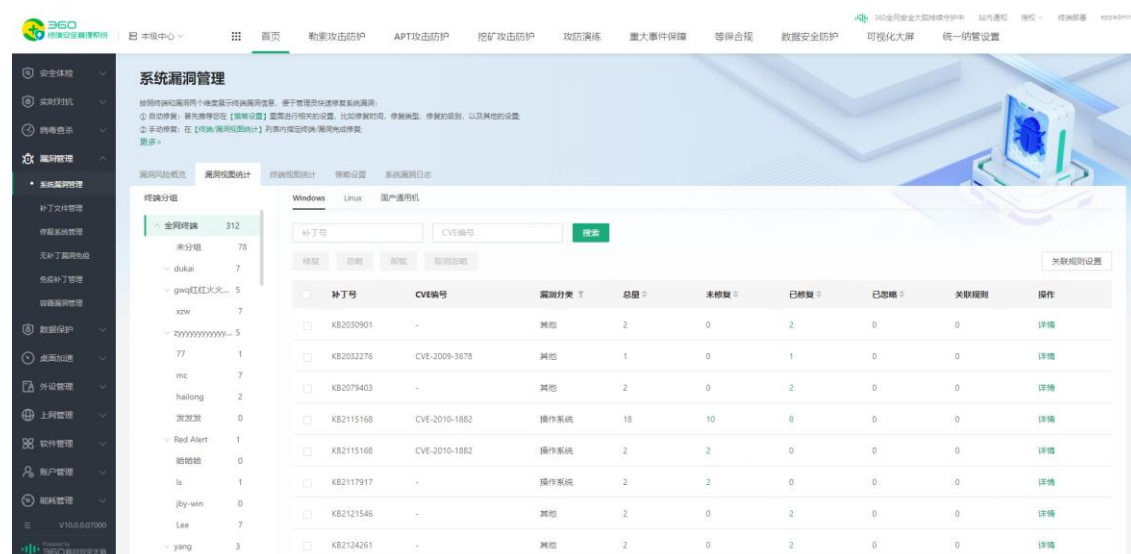
点击左侧功能导航：漏洞管理——系统漏洞管理——漏洞视图统计

### A. Windows

- 检索：在“补丁号”搜索框输入需要检索的补丁号，点击“搜索”按钮，完成检索操作。
- 修复：勾选需要进行修复的补丁，必须在补丁列表中有“未修复”终端数时“修复”按钮才会变绿，点击修复按钮，实现对“未修复”终端的修复操作。
- 忽略：勾选需要进行忽略的补丁，必须在补丁列表中有“未修复”终端数时“忽略”按钮才会变绿，点击忽略按钮，实现对“未修复”终端的忽略操作。
- 卸载：勾选需要进行卸载的补丁，必须在补丁列表中有“已修复”终端数时“卸载”按钮才会变绿，点击卸载按钮，实现对“已修复”终端的卸载操作。
- 取消忽略：勾选需要进行取消忽略的补丁，必须在补丁列表中有“已忽略”终端数时“取消忽略”按钮才会变绿，点击取消忽略按钮，实现对“已忽略”终端的取消忽略操作。
- 关联规则设置：点击“关联规则设置”按钮后在弹窗进行勾选，点击“确定”按钮即可与 IPS 规则进行关联。当未修复漏洞存在规则，自动更新关联规则到未修复漏洞的终端。
- 终端数：未修复、已修复、已忽略、关联规则所统计的终端数可以点击，查看相对应的终端列表以及被关联的规则。
- 补丁列表：可以在补丁列表的表头点击  和  筛选按钮，完成对“漏洞分类”和“总量”的筛选工作；点击操作栏的“详情”按钮，可以查看补丁的详情：补丁名称、补丁级别、修复建议和发布时间。


补丁详情

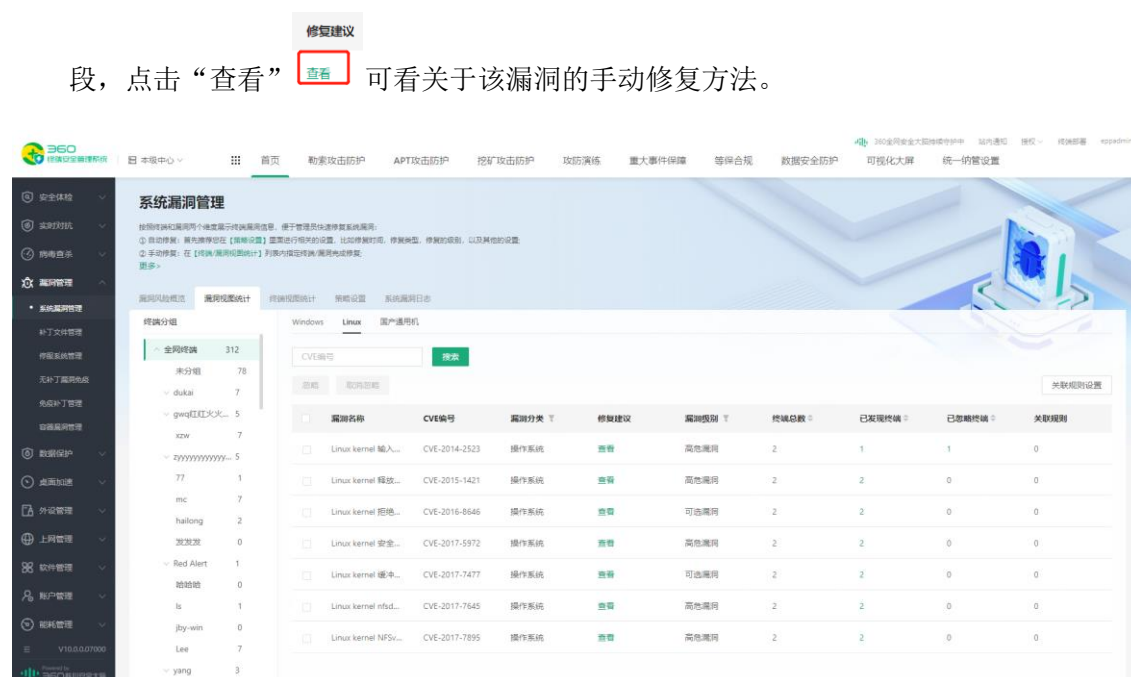
补丁名称	漏洞级别 ▼	修复建议	发布时间 ▼
Windows Server 2008 R2 x64 Edition 安全更新	高危漏洞	建议修复	2012-07-11
Windows Server 2003 安全更新程序 (KB2698365)	高危漏洞	建议修复	2012-07-11
Windows XP 安全更新 (KB2698365)	高危漏洞	建议修复	2023-03-15
用于Windows的更新程序	-	-	2023-03-23
Windows XP 安全更新程序 (KB2698365)	高危漏洞	建议修复	2012-07-11
Windows 7 安全更新程序 (KB2698365)	高危漏洞	建议修复	2014-08-13



Windows 漏洞视图统计

## B. Linux

- Linux 操作逻辑同 Windows，Linux 操作系统无“修复”和“卸载”按钮。
- Linux 只有漏洞列表，检索条件需要按 CVE 编号进行，在漏洞列表中新增“修复建议”字段，点击“查看” 可看关于该漏洞的手动修复方法。



Linux 漏洞视图统计

## C. 国产通用机

- 国产通用机操作逻辑同 Windows，国产通用机操作系统无“修复”按钮。
- 国产通用机检索条件包括：品牌、漏洞级别、公告编号、CVE 编号以及公告摘要。
- 国产通用机漏洞列表不支持“关联规则设置”。

- 补丁列表新增：公告编号（相当于 Windows 补丁号）、CVE 编号、品牌、平台类型（桌面机、服务器）、公告摘要、漏洞级别、修复建议。

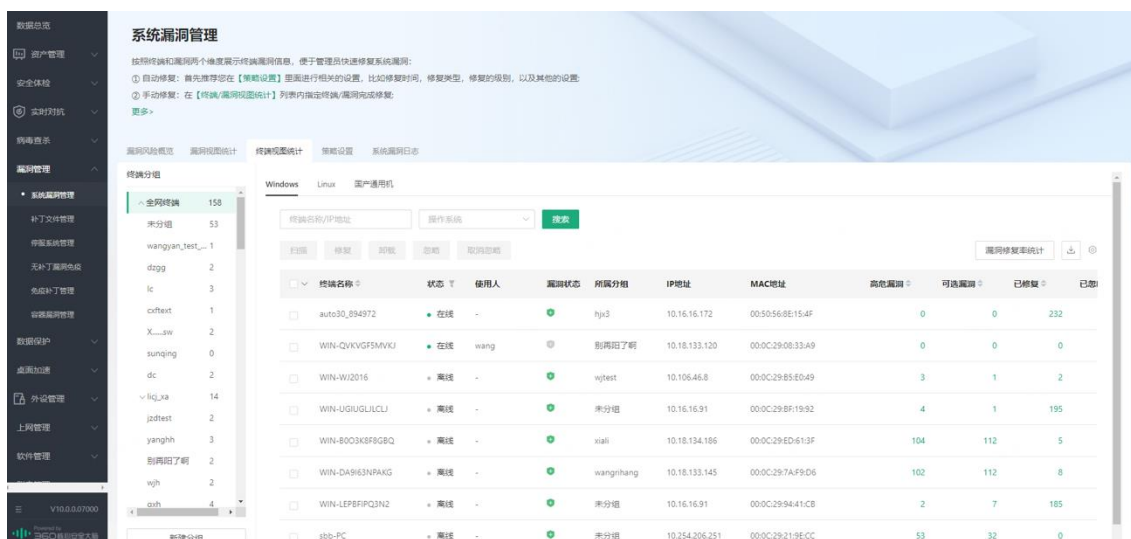


## 7.2.3. 终端视图统计

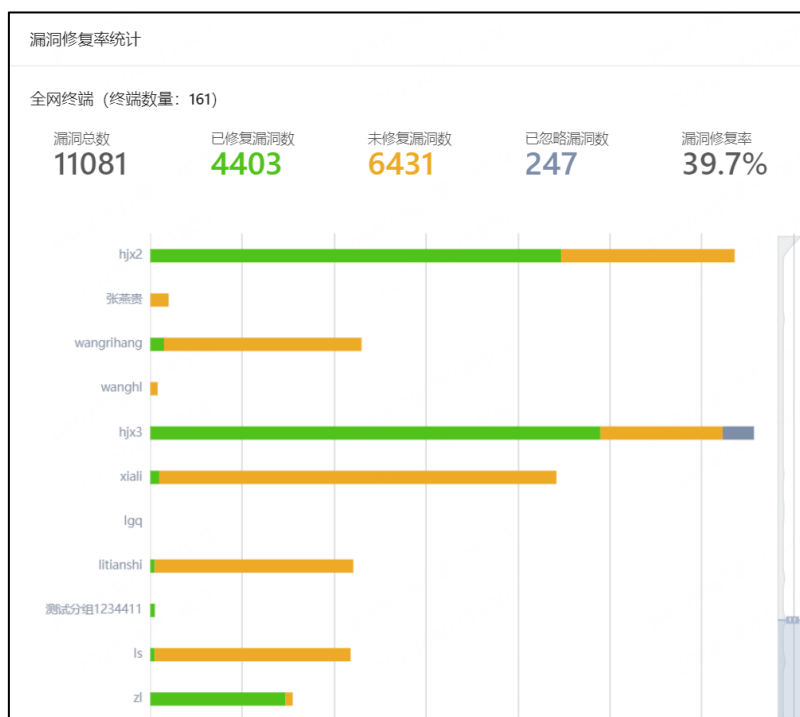
点击左侧功能导航：漏洞管理——系统漏洞管理——终端视图统计

### A. Windows

- 在检索框输入关注的终端名称、IP 地址、操作系统类型，点击“搜索”按钮可以在终端列表搜索相关终端。
- 以终端维度对漏洞进行扫描、修复、卸载、忽略、取消忽略等操作，点击列表高亮数字超链接，显示漏洞修复详情。



- 点击【漏洞修复率统计】可查看漏洞修复率统计



## B. Linux

- 在检索框输入关注的终端名称、IP 地址、操作系统类型，点击“搜索”按钮可以在终端列表搜索相关终端。
- 以终端名称维度对漏洞进行扫描、忽略和取消忽略操作，点击列表高亮数字超链接，显示漏洞修复详情。

系统漏洞管理

按照终端和漏洞两个维度展示终端漏洞信息，便于管理员快速修复系统漏洞。

① 自动修复：首先推荐您在【策略设置】页面进行相关的设置，比如修复时间、修复类型、修复的级别、以及其他设置。

② 手动修复：在【终端/漏洞统计】列表内指定终端/漏洞地址修复。

更多>

漏洞风险概览 漏洞修复统计 终端修复统计 策略设置 系统漏洞日志

终端分组

全网终端 158

未分组 53

wangyan\_test\_... 1

dtzg 2

lc 3

corfeix 1

X...sw 2

sunqing 0

dc 2

liqja 14

jdtest 2

yangyh 3

Windows Linux 国产通用机

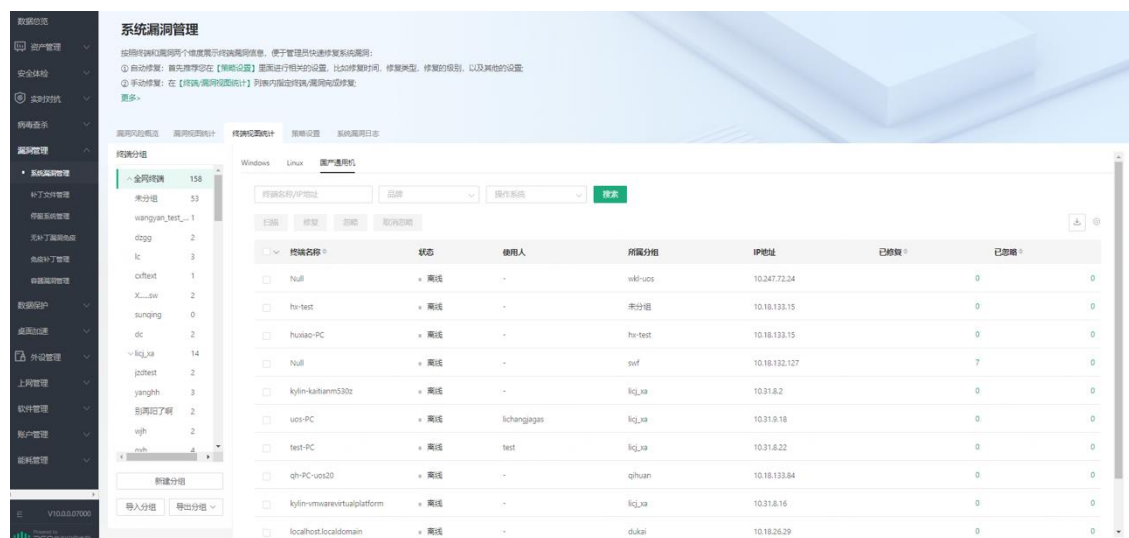
终端名称/IP地址 操作系统 搜索

扫描 忽略 取消忽略

终端名称	状态	使用人	漏洞状态	所属分组	IP地址	MAC地址	高危漏洞	可选漏洞	已忽略
localhost.localdomain	在线	-	0	未分组	10.18.132.21	00:0C:29:E5:74:67 52:54:00:D5:18:69	0	0	0
localhost.localdomain	离线	-	0	wanghl	10.39.85.19	00:0C:29:87:59:3E	5	3	0
self-virtual-machine	离线	-	0	未分组	10.18.132.127	00:0C:29:E2:80:D2	0	0	0
localhost.localdomain	离线	-	0	未分组	10.18.190.194	00:0C:29:6C:67:8E 52:54:00:9C:7D:33	0	0	0

## C. 国产通用机



- 在检索框输入关注的终端名称、IP 地址、品牌、操作系统类型，点击“搜索”按钮可以在终端列表搜索相关终端。
- 以终端维度对漏洞进行扫描、修复、忽略、取消忽略等操作，点击列表高亮数字超链接，显示漏洞修复详情。



## 7.2.4.策略设置

点击左侧功能导航：漏洞管理——系统漏洞管理——策略设置

### A. Windows

- 模块化设置：勾选  漏洞修复 ，点击“应用”按钮，选择需要下发策略终端，将会安装模块相关组件。

- 漏洞管理：管理员对全网终端下发漏洞修复策略，终端补丁库升级后，终端会自动进行漏洞扫描修复。

- 定期自动修复漏洞：可以添加多个自动修复时间，选择周期为每天，每周，每月以及时间点数，可添加多个。

☒ 开启定期自动修复

每天

19:59

- 漏洞类型：可选择操作系统类型、Microsoft Office 和第三方软件类型。

漏洞类型

☒ 操作系统类（包含操作系统、IE、.NET Framework、内嵌在IE中的Adobe Flash Player）

☒ Windows XP ☐ Windows Vista ☐ Windows 7 ☐ Windows 8 ☐ Windows 8.1 ☐ Windows 10  
☐ Service Pack（操作系统补丁）

☒ Microsoft Office

☒ Office 2003 ☒ Office 2007 ☒ Office 2010 ☒ Office 2013 ☒ Office 2016 ☒ Service Pack（Office补丁）☒ 其他

☒ 第三方软件

☒ Adobe

- 漏洞级别：选择高危和可选的高危两类。

漏洞级别

☐ 高危 ☐ 可选的高危

- 补丁安装完成后是否重启提示：可选提醒时机或者是否重启。



补丁安装完成提示重启/自动重启（使补丁及时生效） ☐ 锁定子分组

- ☒ 提醒一次
- ☐ 间隔提醒 - 30 + 分钟
- ☐ 自动重启
- ☐ 规定时间段重启 20:00 - 3:00

➤ 补丁下载安装顺序：选择边下载边安装模式或者下载完统一安装模式。

补丁下载安装顺序

- ☒ 补丁下载、安装同时进行（节省修复时间）
- ☐ 补丁下载完成后，再逐个安装（大幅度减少下载时占用的 CPU）

➤ 终端漏洞修复限制：限制客户端是否可以忽略补丁。

终端漏洞修复限制

☐ 禁止在终端忽略补丁

➤ 其他设置：包括升级补丁库后自动扫描、关闭 Windows Update、开启蓝屏修复以及打补丁影响用户时提醒功能。

其他设置

- ☒ 升级补丁库后自动扫描
- ☒ 关闭 Windows Update
- ☒ 开启蓝屏修复功能
- ☐ 打补丁影响到编辑 Office 文档时，提醒用户及时保存文档，避免丢失

➤ 补丁库高级设置：开启补丁排除列表，在列表内的补丁将被排除不进行修复；开启补丁包含列表，只修复在列表内的补丁；补丁排除列表和补丁包含列表均支持手动添加补丁号，手动添加内容支持删除。

补丁库高级设置 ☐ 锁定子分组

☐ 关闭补丁限制列表

☒ 开启补丁排除列表 ^

☐ 补丁列表 (0/1988) + -

请输入搜索内容

☐ KBtest - 高危漏洞 手动添加

☐ KB2030902 - 高危漏洞 手动添加

☐ KB11111111 - 高危漏洞 手动添加

☐ KB2032276

☐ KB2079403

☐ KB2115168 - 高危漏洞

< >

☐ 被排除补丁 (0/2)

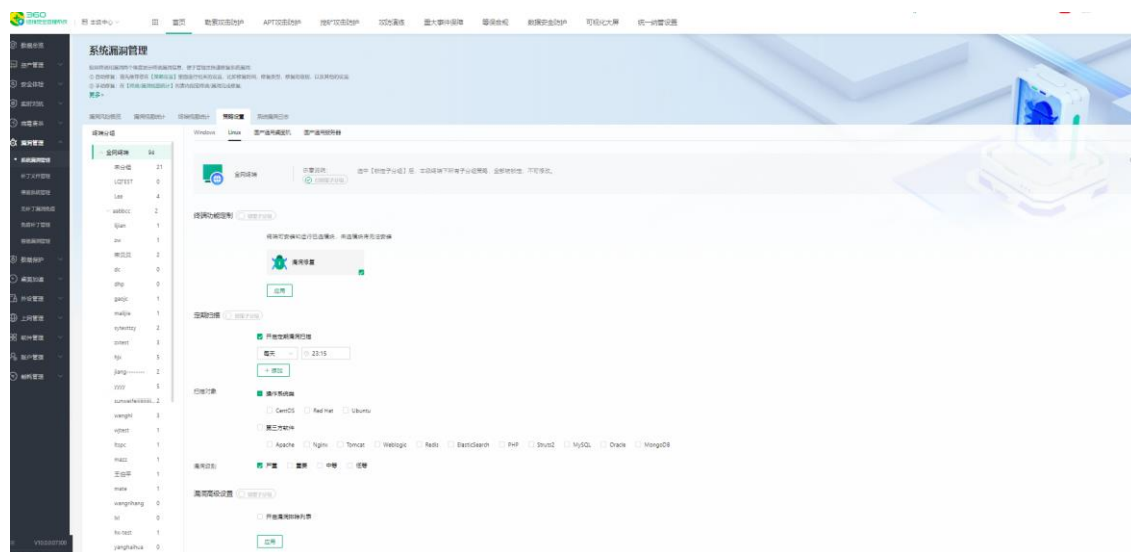
请输入搜索内容

☐ KB123456845555! @ - 可选漏洞 手动添加

☐ KB2030901

☐ 开启补丁包含列表 v





## B. Linux

- 漏洞管理：管理员对全网终端下发漏洞修复策略，终端会自动进行漏洞扫描。
  - 定期自动修复漏洞：可以添加多个自动修复时间，选择周期为每天，每周，每月以及时间点数，可添加多个。

☒ 开启定期自动修复

每天

- 漏洞类型：可选择操作系统类型和第三方软件类型。

扫描对象 ☒ 操作系统类

☐ CentOS ☐ Red Hat ☐ Ubuntu

☐ 第三方软件

☐ Apache ☐ Nginx ☐ Tomcat ☐ Weblogic ☐ Redis ☐ Elasticsearch ☐ PHP ☐ Struts2 ☐ MySQL ☐ Oracle ☐ MongoDB

- 漏洞级别：可选扫描的漏洞级别是严重、重要、中等、低等。

漏洞级别 ☒ 严重 ☐ 重要 ☐ 中等 ☐ 低等

- 漏洞高级设置：开启补丁排除列表，在列表内的补丁将被排除不进行扫描；

漏洞高级设置 ☐ 锁定子分组

☒ 开启漏洞排除列表

☐ 漏洞列表 (0/577)

☐ LDY-2021-00003727 - 严重

☐ LDY-2021-00003745 - 中等

☐ LDY-2021-00004830 - 重要

☐ LDY-2021-00005216 - 重要

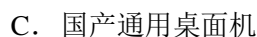
☐ LDY-2021-00005304 - 中等

☐ LDY-2021-00006205

应用

☐ 被排除漏洞 (0/0)

无数据



- 定期自动修复漏洞：可以添加多个自动修复时间，选择周期为每天，每周，每月以及时间点数，可添加多个。

每天 19:59

- 漏洞类型
- ✔ 操作系统类
  - ✔ 银河麒麟桌面操作系统

- 漏洞级别 ☒ 严重 ☒ 重要 ☒ 中等 ☒ 低等 ☐ 不受影响

- 补丁安装完成提示重启/自动重启 (使补丁及时生效) ☐ 锁定子分组

- ☒ 提醒一次
- ☐ 间隔提醒  分钟
- ☐ 自动重启
- ☐ 规定时间段重启  -

- 补丁下载安装顺序：选择边下载边安装模式或者下载完统一安装模式。

#### 补丁下载安装顺序

- ☒ 补丁下载、安装同时进行（节省修复时间）
- ☐ 补丁下载完成后，再逐个安装（大幅度减少下载时占用的 CPU）

➤ 终端漏洞修复限制：限制客户端是否可以忽略补丁。

#### 终端漏洞修复限制

- ☐ 禁止在终端忽略补丁

➤ 其他设置：包括升级补丁库后自动扫描、以及开启智能忽略功能。

#### 其他设置

- ☒ 升级补丁库后自动扫描
- ☒ 开启智能忽略(补丁安装失败三次终端自动忽略不进行安装)

➤ 补丁安装方式：可选 dpkg 补丁安装方式以及 apt 补丁安装方式，按用户现场环境决定。

#### 补丁安装方式

- ☒ dpkg补丁安装方式(依照管控中心同步的漏洞库信息进行补丁安装，无网络限制)
- ☐ apt补丁安装方式(交由系统自带包管理工具进行补丁文件下载，完成修复，更智能，需要终端能够直接连接互联网)

➤ 补丁库高级设置：开启补丁排除列表，在列表内的补丁将被排除不进行修复；开启补丁包含列表，只修复在列表内的补丁；补丁排除列表和补丁包含列表均支持手动添加补丁号，手动添加内容支持删除。

补丁库高级设置 ☐ 锁定子分组

☐ 关闭补丁限制列表

☒ 开启补丁排除列表 ^

☐ 补丁列表 (0/2693) + -

Q 请输入搜索内容

- ☐ KYSA-202101-00371 - 严重 手动添加
- ☐ KYSA-123123 - 严重 手动添加
- ☐ UTSA-123 - 严重 手动添加
- ☐ NFSCSN-2100-0002 - 不受影响 手动添加
- ☐ UTSA-2100-0003 - 严重 手动添加
- ☐ KYSA-201604-1001 - 低等

☐ 被排除补丁 (0/2)

Q 请输入搜索内容

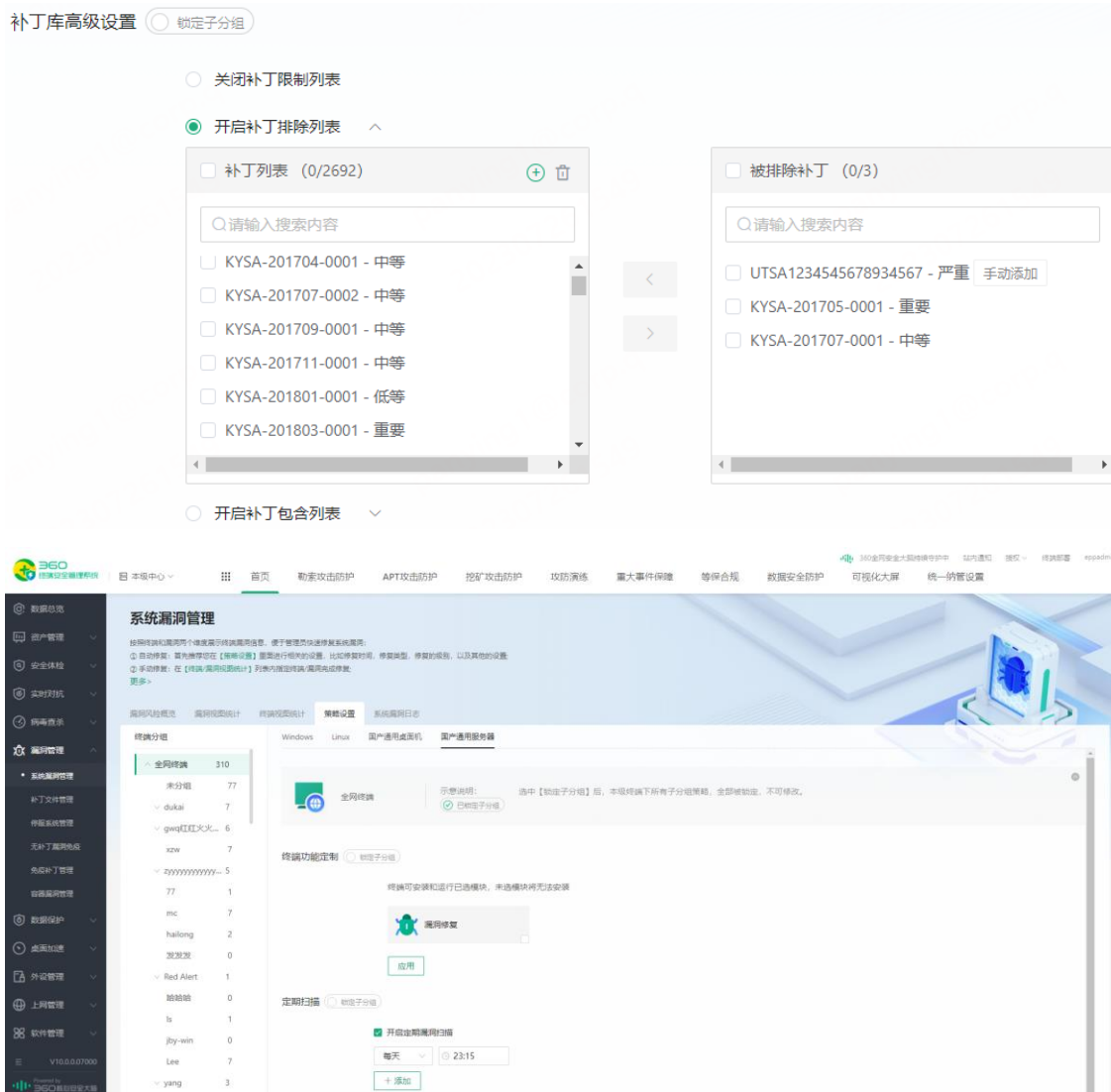
- ☐ KYSA-201704-001 - 中等 手动添加
- ☐ KYSA-201605-0001 - 中等

☐ 开启补丁包含列表 v



## D. 国产通用服务器

- 模块化设置：勾选  漏洞修复 , 点击“应用”按钮, 选择需要下发策略终端, 将会安装模块相关组件。
- 漏洞管理：管理员对全网终端下发漏洞修复策略, 终端补丁库升级后, 终端会自动进行漏洞扫描修复。
  - 定期自动修复漏洞：可以添加多个自动修复时间, 选择周期为每天, 每周, 每月以及时间点数, 可添加多个。
  - 漏洞类型：可选择操作系统类型。
  - 漏洞级别：选择严重、重要、中等、低等和不受影响五类级别。
  - 补丁库高级设置：开启补丁排除列表, 在列表内的补丁将被排除不进行修复；开启补丁包含列表, 只修复在列表内的补丁；补丁排除列表和补丁包含列表均支持手动添加补丁号, 手动添加内容支持删除。



## 7.2.5. 系统漏洞日志

点击左侧功能导航：漏洞管理——系统漏洞管理——系统漏洞日志

### A. 按终端查看

以终端维度查看 Windows/Linux/国产通用机系统漏洞日志信息，点击“检出量”列的高亮绿色统计数字，可以查看该终端检出的漏洞详情。

默认查看一周日志，支持终端名称/IP 地址模糊搜索，管理员可以自定义时间段查看漏洞扫描日志。可导出报表。



## B. 按漏洞查看

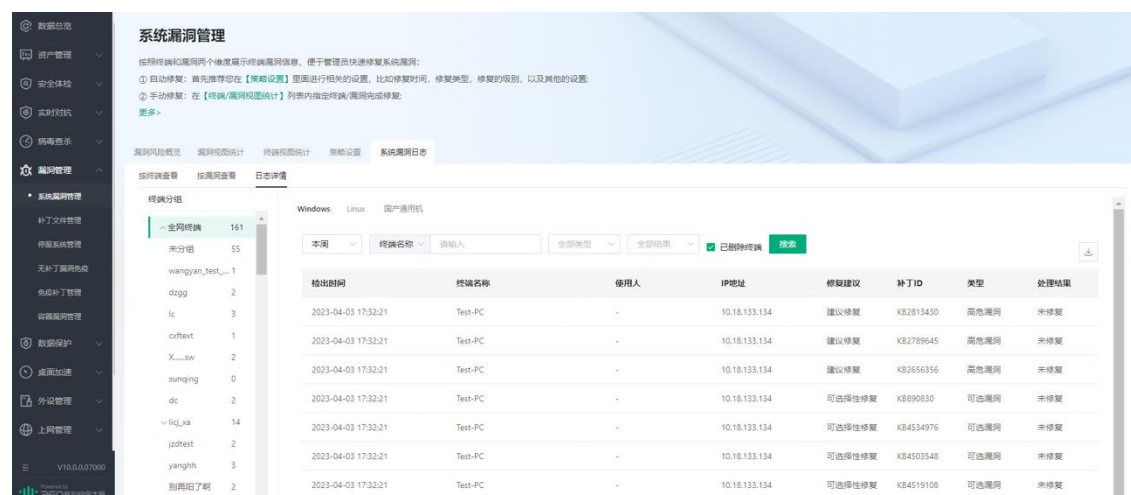
以漏洞维度查看 Windows/Linux/国产通用机系统漏洞日志信息，点击“检出量”列的高亮绿色统计数字，可以查看该补丁/漏洞名/公告编号检出的终端详情。

默认查看一周日志，管理员可以自定义时间段查看漏洞扫描日志。可导出报表。



## C. 日志详情

通过检索条件可以查找 Windows/Linux/国产通用机的检出日志详情，查看修复建议以及处理结果。可导出报表。



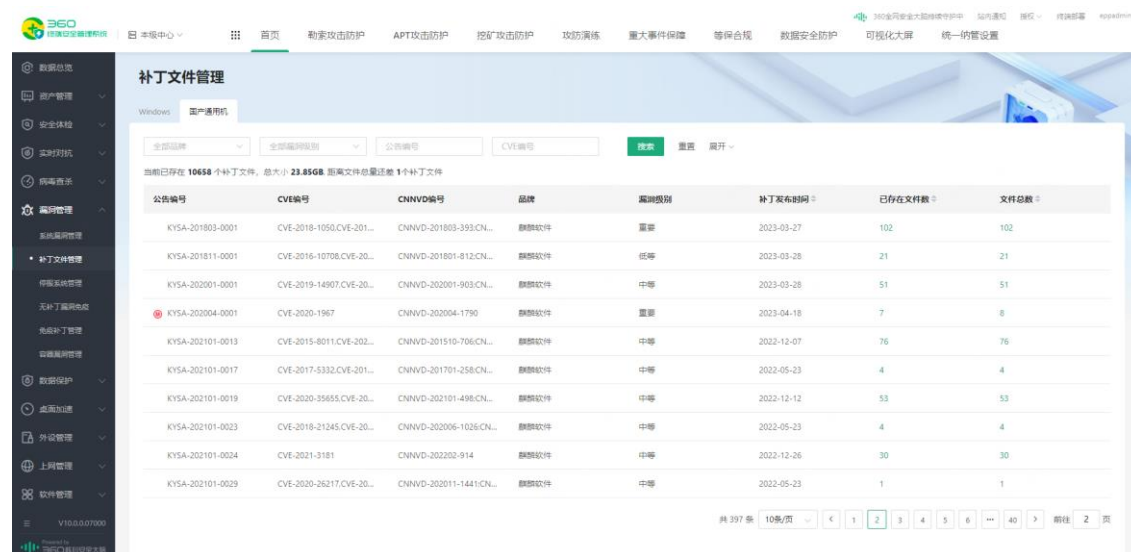
## 7.3. 补丁文件管理

点击左侧功能导航：漏洞管理——补丁文件管理

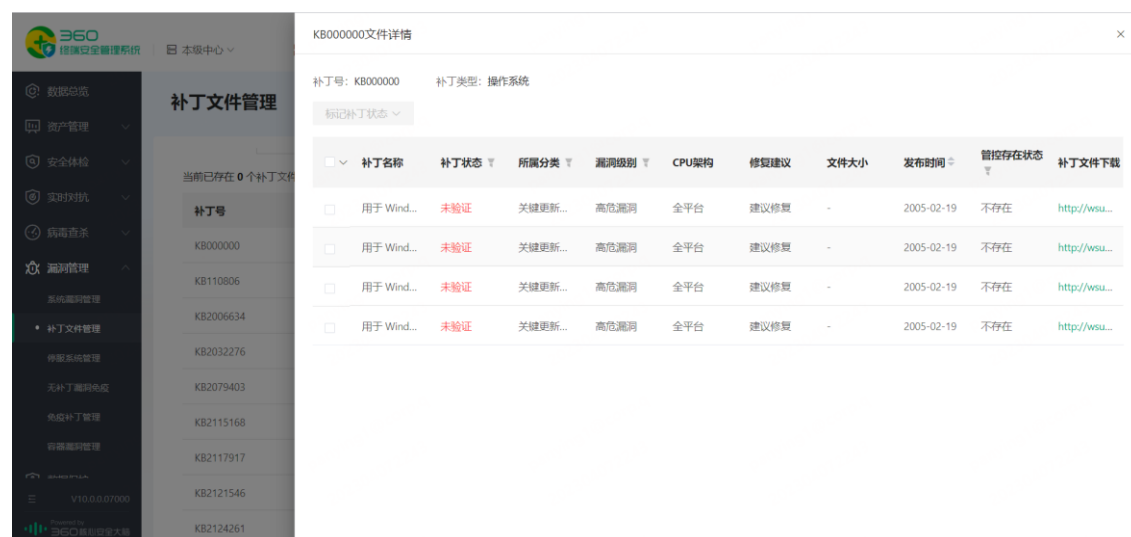
补丁文件管理功能可以显示 Windows/国产通用机显示补丁文件的补丁号/公告编号、类型、是否存在和文件总数，国产通用机还包括：CVE、CNNVD、品牌以及补丁发布时间等参数，管理员可以根据相关参数对关注的补丁文件进行搜索。







Windows 和国产通用机的补丁文件列表中点击文件总数数字链接，可查看补丁详细信息。管理员可在此处编辑补丁验证状态，未验证的补丁可选择不安装。

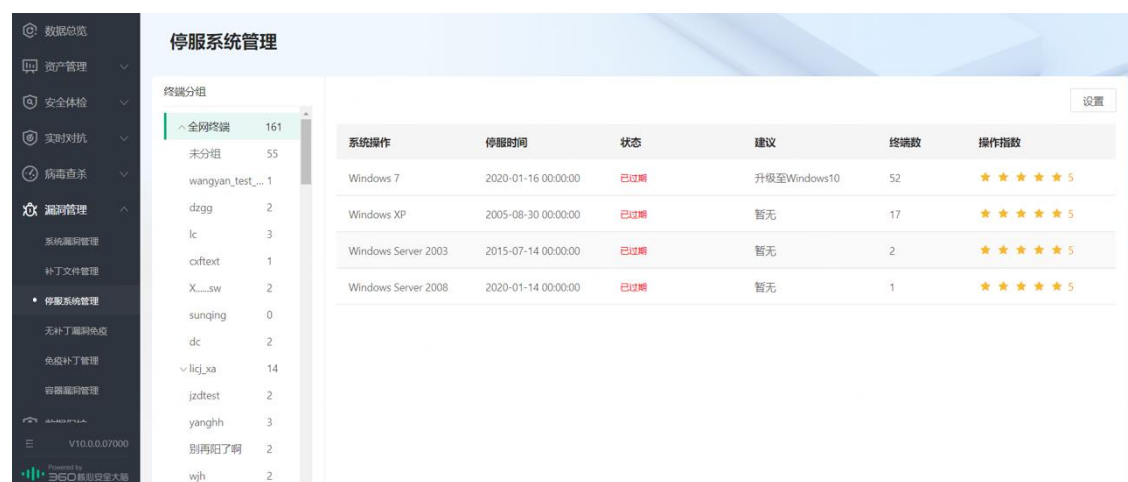


## 7.4. 停用系统管理

点击左侧功能导航：漏洞管理——停用系统管理

根据设置时间显示即将停服的 Windows 系统信息，点击终端数可以查看该类系统的终端名称、IP 地址、所属分组等详细信息：



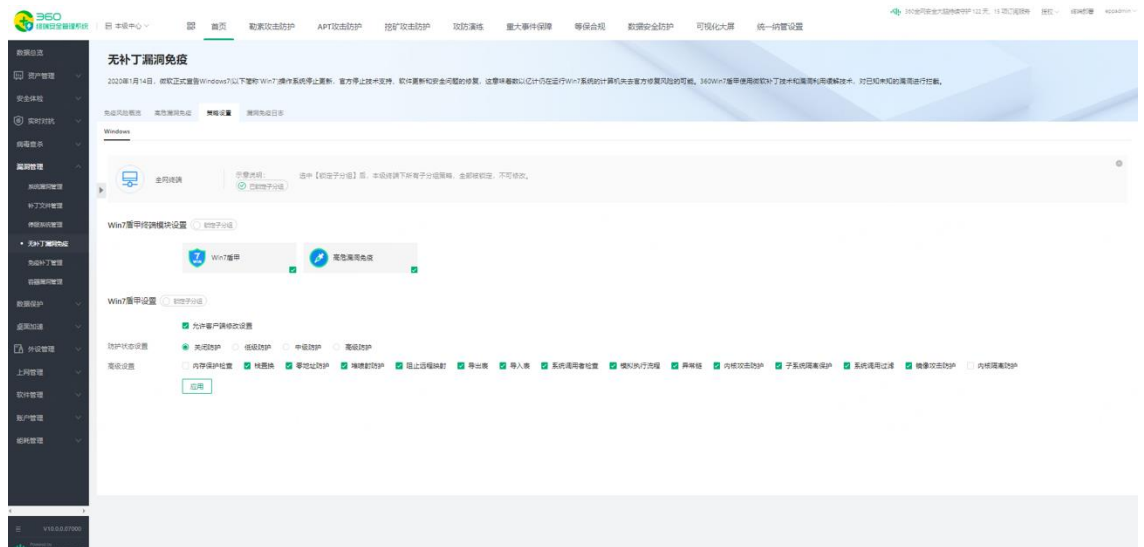


## 7.5. 无补丁漏洞免疫

策略包含了管控中心对终端 win7 盾甲防护状态的开关设置。包括防护状态设置、高级设置。

步骤一：设置 win7 盾甲策略

- 1、登录控制台，在左侧导航栏，选择漏洞管理>无补丁漏洞免疫>策略设置
- 2、在策略面板设置防护开关配置。



## 步骤二：按照漏洞维度查看终端免疫情况

### 1、登录控制台，在左侧导航栏，选择漏洞管理>无补丁漏洞免疫>高危漏洞免疫>按漏洞

## 项目统计

漏洞编号	防护对象	免疫补丁号	漏洞描述	终端总数	开启免疫终端	关闭免疫终端	无免疫终端	CPU架构
CVE-2019-2565	高危	2020117	漏洞编号CVE-2019-2565, 浏览器漏洞...	51	12	1	38	x86
CVE-2018-8174	高危	2020118	漏洞编号CVE-2018-8174, 浏览器漏洞...	71	40	0	31	x86
CVE-2019-2565	高危	2020118	漏洞编号CVE-2019-2565, 浏览器漏洞...	28	2	0	24	x64
CVE-2018-8174	高危	2020120	漏洞编号CVE-2018-8174, 浏览器漏洞...	42	26	0	16	x64
CVE-2019-0802	高危	2020121	漏洞编号CVE-2019-0802, Microsoft...	67	0	0	67	x86
CVE-2018-0798	高危	2020123	漏洞编号CVE-2018-0798, Microsoft...	67	0	0	67	x86
CVE-2018-0189	高危	2020124	漏洞编号CVE-2018-0189, 浏览器漏洞...	51	3	0	48	x86
CVE-2018-0189-62	高危	2020125	漏洞编号CVE-2018-0189, 浏览器漏洞...	51	39	0	12	x86
CVE-2012-0155	高危	2020126	漏洞编号CVE-2012-0155, 浏览器漏洞...	51	1	0	50	x86
CVE-2014-1776	高危	2020127	漏洞编号CVE-2014-1776, 浏览器漏洞...	52	25	0	27	x86

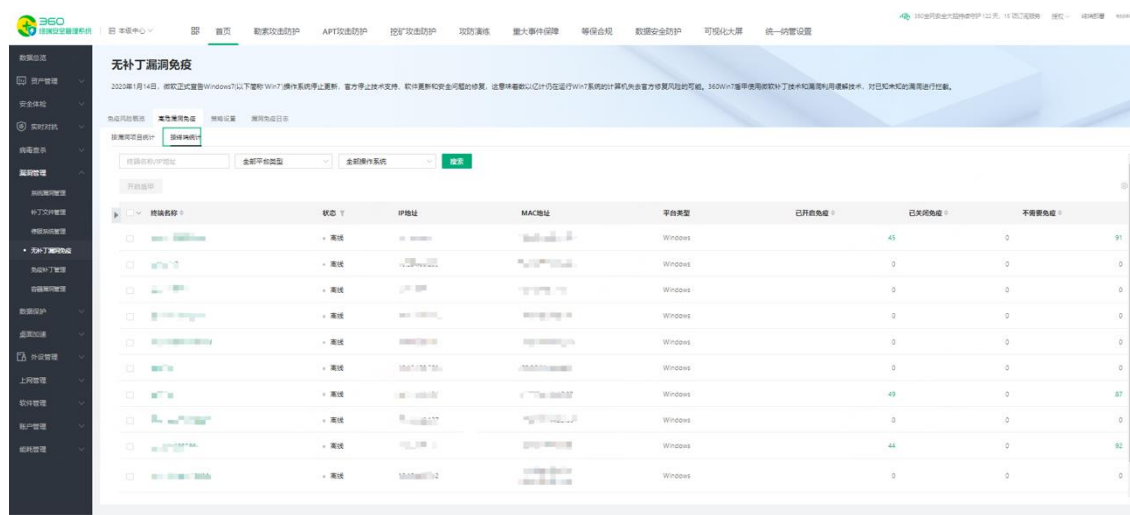
针对未开启免疫的终端，可下发【开启免疫】指令；

针对已开启免疫的终端，可下发【关闭免疫】指令。

## 步骤三：按照终端维度查看免疫情况

### 1、登录控制台，在左侧导航栏，选择漏洞管理>无补丁漏洞免疫>高危漏洞免疫>按终端

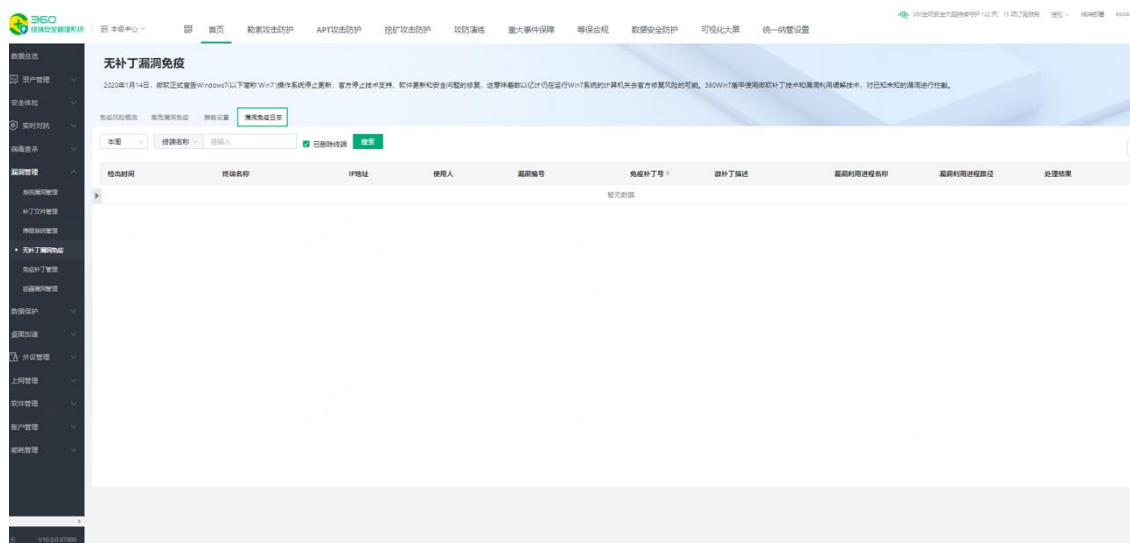
## 统计



针对未开启免疫的终端，可下发【开启盾甲】指令。

步骤四：查看终端免疫防疫日志

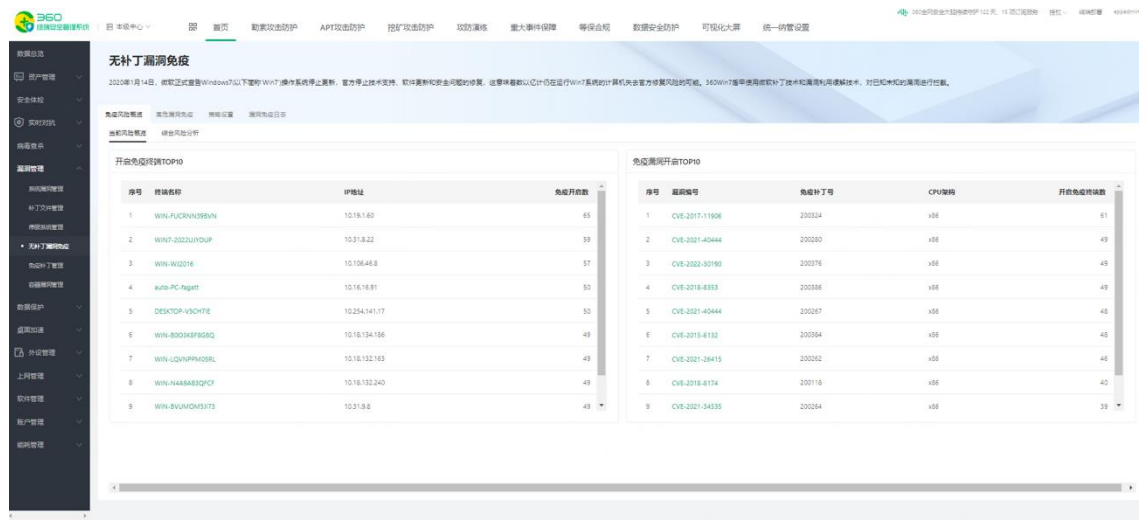
1、登录控制台，在左侧导航栏，选择漏洞管理>无补丁漏洞免疫>高危漏洞免疫>漏洞免疫日志



包含：检出时间、终端名称、IP 地址、使用人、漏洞编号、免疫补丁号、微补丁描述、漏洞利用进程名、漏洞利用进程路径、处理结果。

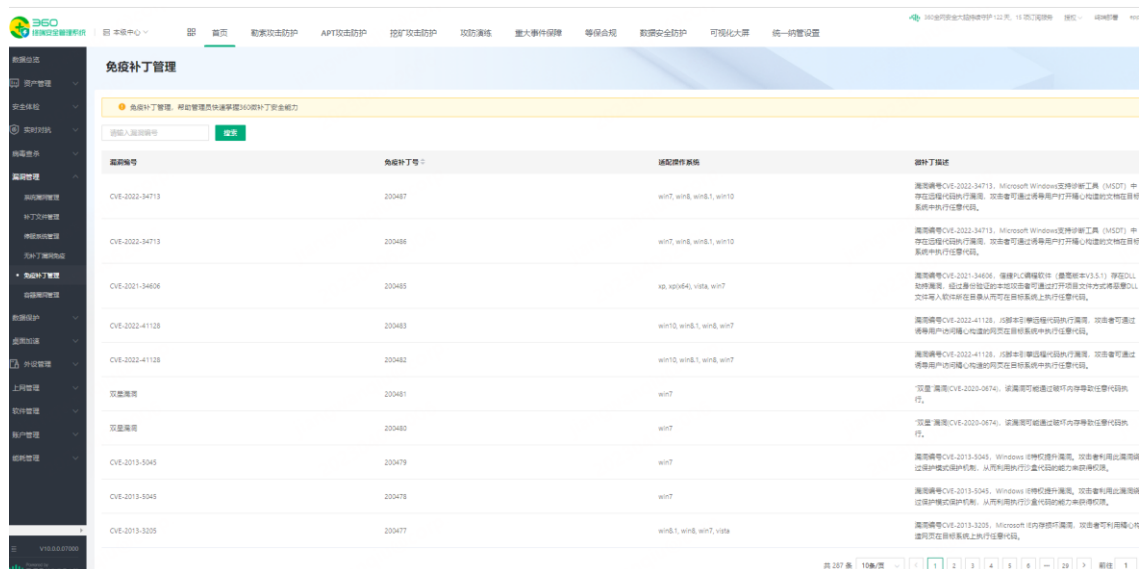
步骤五：查看免疫风险概览

1、登录控制台，在左侧导航栏，选择漏洞管理>无补丁漏洞免疫>高危漏洞免疫>免疫风险概览 >当前风险概览&综合分析



## 步骤六：免疫补丁库可视化管理

### 1、登录控制台，在左侧导航栏，选择漏洞管理> 免疫补丁管理



页面可查看当前免疫补丁库补详情，包含：漏洞编号、免疫补丁号、适配操作系统、微补丁描述。

## 8. 数据保护

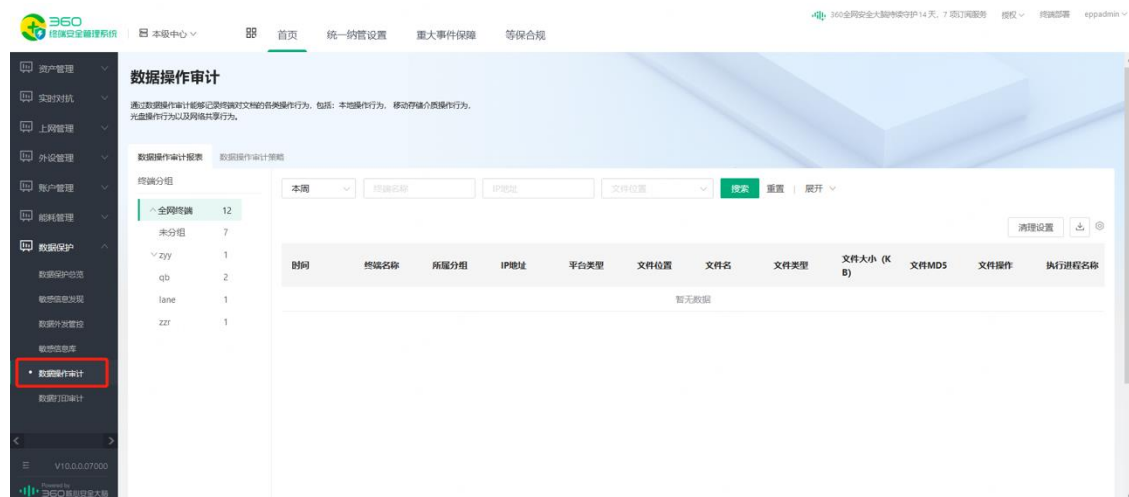
### 8.1. 数据操作审计

记录终端用户操作本地硬盘中的文件、移动存储设备中的文件、光盘中的文件、以及网络共享中的文件操作行为。

\*该功能支持对 Windows 终端的管理。

#### 8.1.1. 功能入口

首页→数据保护→数据操作审计



#### 8.1.2. Windows 终端策略配置

##### 1. 开启管理策略

策略默认是关闭状态，开启策略请选择**启用策略**：



##### 2. 设置审计文件位置

设置要审计的文件的存储位置，包括：本地文件审计、移动存储审计、光盘审计、网

络共享审计。

### 3. 设置审计文件范围

设置要审计的文件范围，包括：所有文件、指定文件。针对本地文件，可支持审计系统盘符文件。

审计指定文件：如果审计范围选择了指定文件，需要配置具体的审计条件，包括文件的存储路径、文件的类型。

- 指定审计文件路径(仅限本地文件)：本地指定文件审计，可添加本地文件路径列表，支持系统环境变量。
- 指定审计文件类型：审计移动存储、光盘、网络共享的指定文件，可添加文件扩展列表，输入扩展名。

### 4. 设置审计操作

设置要审计的文件操作类型，包括：读取、修改、删除、重命名、创建、复制、移动、恢复。

## 5. 设置例外进程

例外列表内的进程触发的文件操作，均不会被审计，可配置进程名。

### 例外进程设置

#### 例外进程 ②

请输入要例外的进程

添加

## 6. 设置文件备份

对有创建、复制、移动操作的文件，支持备份对应的文件。可设置备份文件大小的上限值，默认值为 5M，如果不填写或填写为 0，则不限制备份文件的大小。

### 文件备份设置

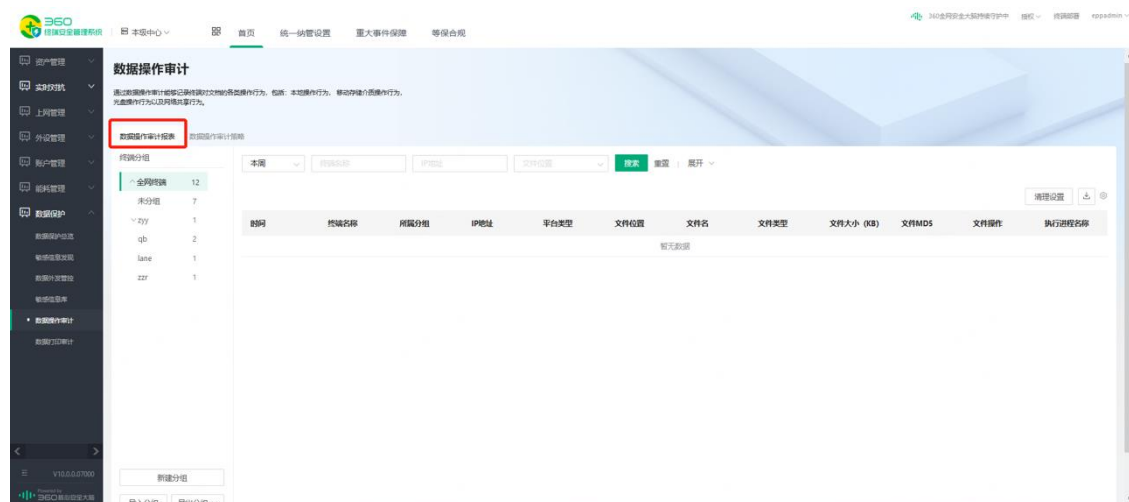
☒ 备份审计文件：仅备份创建、复制、移动操作的文件，限制备份

5

MB 以内的文件 ②

## 8.1.3. 日志记录

当终端用户发生符合策略配置的文件操作行为时，系统将自动记录日志。



## 8.1.4. 注意说明

审计所有文件，可能产生较大的审计日志，易造成系统卡顿，请谨慎选择。

## 8.2. 数据打印审计

记录终端打印文件的行为，同时也可禁止计算机打印文件，保证重要文件无法通过打印方式流失。

\*该功能支持对 Windows 终端和国产通用桌面机终端的管理。

## 8.2.1. 功能入口

首页→数据保护→数据操作审计



## 8.2.2. Windows 终端策略配置

### 1. 策略入口

首页→数据保护→数据操作审计→数据打印审计策略→Windows



### 2. 开启管理策略

策略默认是关闭状态，开启策略请选择启用策略：



## 数据打印审计策略 ? 锁定子分组

☒ 启用策略 ☐ 禁用策略

### 3. 设置审计打印行为

设置打印审计的范围，包括：

- a) 监控记录终端所有打印操作：对终端的所有打印行为进行审计；
- b) 仅监控记录终端指定文件类型的打印操作：对终端上的指定文件类型的打印操作进行审计，可添加文件扩展名。

打印审计

☐ 监控记录终端所有打印操作 ☒ 仅监控记录终端指定文件类型的打印操作

请输入扩展名，如php

添加

### 4. 设置阻止打印行为

打印控制：默认不开启，即终端可正常打印。开启“阻止终端打印操作”，则阻止终端的打印行为，并提示终端用户。

若现场有需要例外能够打印的软件或打印机，可添加例外进程、例外打印机，来允许其发生打印操作。

打印控制

☒ 阻止终端打印操作

例外进程

请输入要例外的进程

添加

例外打印机

请输入要例外的打印机

添加

## 8.2.3. 国产通用桌面机终端策略配置

### 1. 策略入口

首页 → 数据保护 → 数据操作审计 → 数据打印审计策略 → 国产通用桌面机



## 2. 开启管理策略

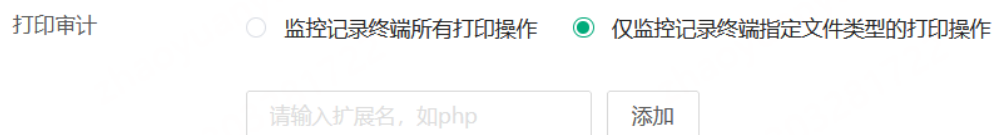
策略默认是关闭状态，开启策略请选择**启用策略**：



## 3. 设置审计打印行为

设置打印审计的范围，包括：

- a) 监控记录终端所有打印操作：对终端的所有打印行为进行审计；
- b) 仅监控记录终端指定文件类型的打印操作：对终端上的指定文件类型的打印操作进行审计，可添加文件扩展名。



## 8.2.4. 日志记录

当终端用户发生符合策略配置的文件打印行为时，系统将自动记录日志。

360

终端安全管理系统

本级中心

首页

勒索攻击防护

APT攻击防护

挖矿攻击防护

攻防演练

重大事件保障

等保合规

数据安全防护

可视化大屏

360全网安全大脑持续守护中

授权

终端部署

eggadmin

漏洞管理

数据保护

数据保护总览

数字水印

敏感信息发现

数据外发管控

敏感信息库

数据操作审计

数据打印审计

屏摄监控

文档智能备份

数据安全工具

V10.0.0.07000

Powered by 360 基础安全大脑

### 数据打印审计

通过文档打印审计能够记录终端的各类打印操作，不限于本地打印和网络打印，并且可以限制终端的打印行为。

**数据打印审计概览**

终端分组

本周

终端名称

IP地址

是否阻止打印

搜索

重置

展开

时间	终端名称	所属分组	IP地址	平台类型	打印进程名	文件名称	文件MD5	文件路径	是否阻止打印	打印结果
<a href="#">前往数据</a>										

终端分组

^ 全网终端 153

未分组 51

wangyan\_test\_... 1

dzgg 2

lc 3

cxftext 1

X...sw 2

sunqing 0

dc 2

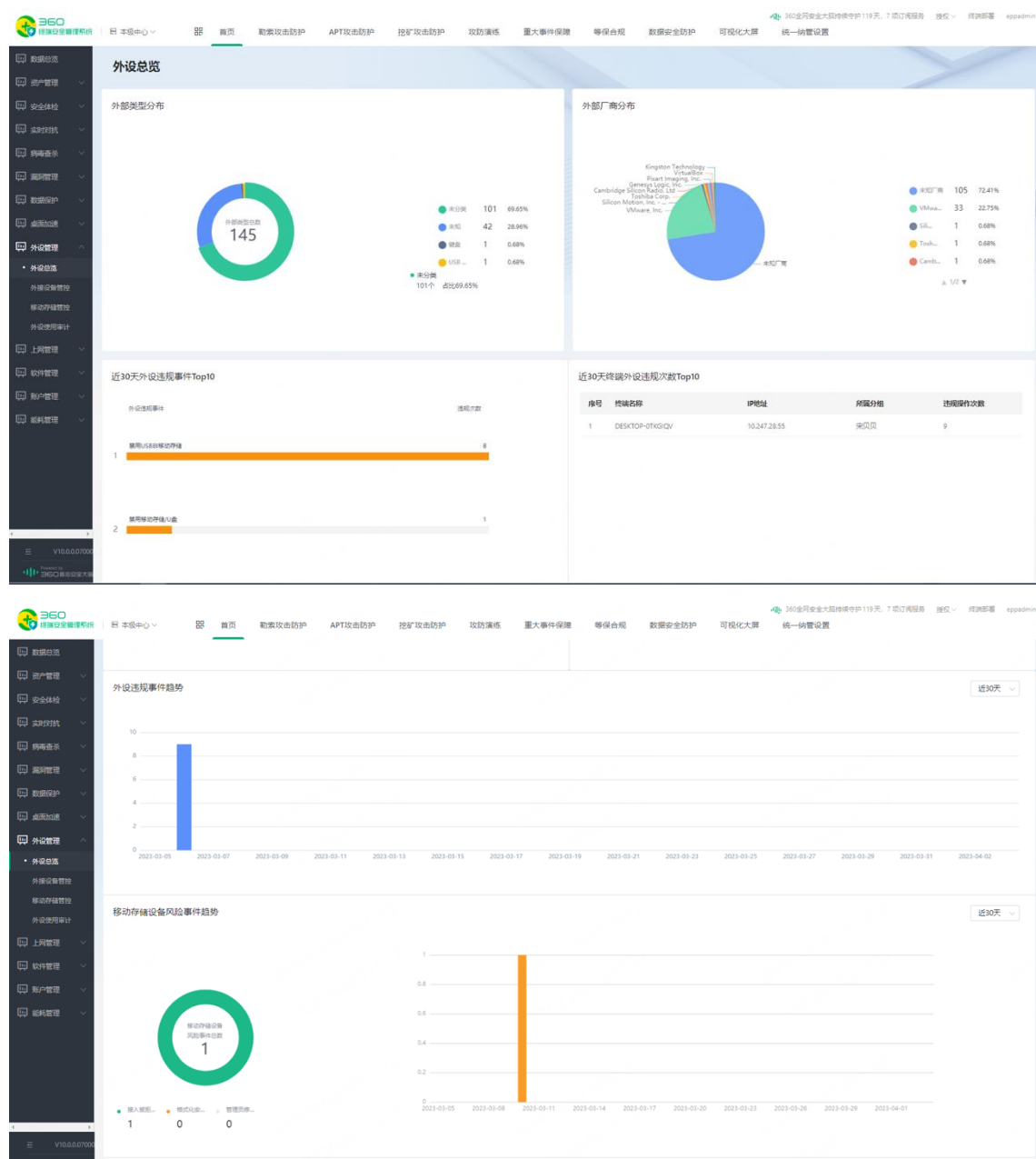
liqj\_xa 14

jzdfest 2

## 9. 外设管理

### 9.1. 外设总览

入口：外观管理>外设总览，用于展示全网的外接设备与移动存储设备的分布情况，例如：  
外设类型分布、外部厂商分布、近 30 天外设违规事件 TOP10、近 30 天终端外设归为次数 TOP10、外设违规事件趋势、移动存储设备风险事件趋势、近 30 天终端移动存储设备风险 TOP10，如下图：



序号	终端名称	IP地址	所属分组	风险操作次数
1	qushlong-PC	10.18.190.27	未分组	1

## 9.2. 外接设备管控

### 9.2.1. 外设库

1. 按外接设备类型视角，查看当前外接设备列表。如下图：

设备编号	设备名称	设备类型	分类形式	厂商	产品	设备实例路径	类型	VID	PID	状态	白名单方式	设备来源	类GUID	备注
167662770809118...	Generic USB Hub	未分类	未处理	VMware, Inc.	Virtual USB Hub	USB\VID_080F&PID...	USB	080F	0002	-	-	终端上报	{B6FC9E6D...	-
1676341945554708...	Generic USB Hub	USB H...	手动	VMware, Inc.	Virtual USB Hub	USB\VID_080F&PID...	USB	080F	0002	-	-	终端上报	{B6FC9E6D...	-
167591136393919...	USB 集线器	-	未处理	VMware, Inc.	Virtual USB Hub	USB\VID_080F&PID...	USB	080F	0002	-	-	终端上报	{B6FC9E6D...	-
1675911363979645...	USB 集线器	-	未处理	VMware, Inc.	Virtual USB Hub	USB\VID_080F&PID...	USB	080F	0002	-	-	终端上报	{B6FC9E6D...	-

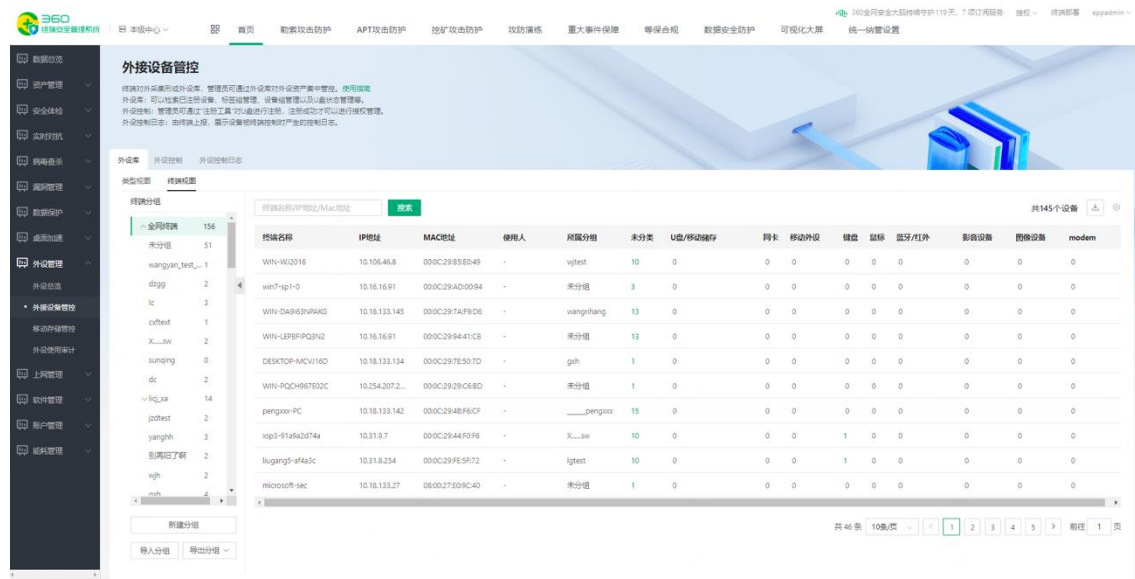
支持通过设备名称/设备编号/厂商/产品、设备来源、白名单方式、分类形式、类型分类检索外接设备列表信息；

支持新增、删除类型分类；

支持新增、修改类型、删除、导出外接设备信息；

支持设备设置上报方式；

2. 按终端视角，查看终端上外接设备信息。如下图



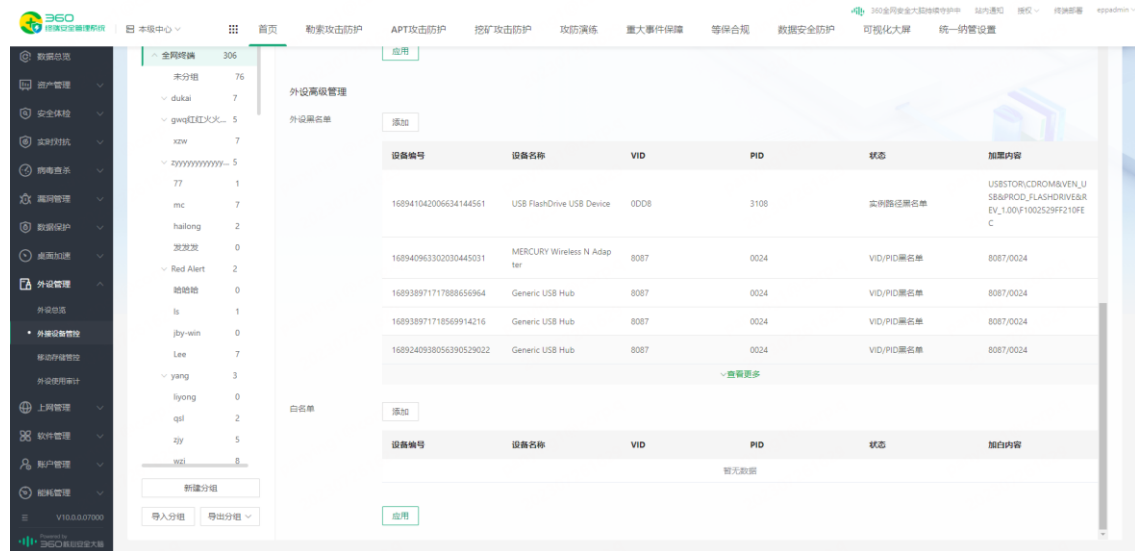
支持通过终端名称/IP 地址/Mac 地址、分组，检索终端信息；

支持导出终端列表信息；

## 9.2.2.外设控制

管理员通过分组形式，给终端下发外设控制策略，详细页面如下：





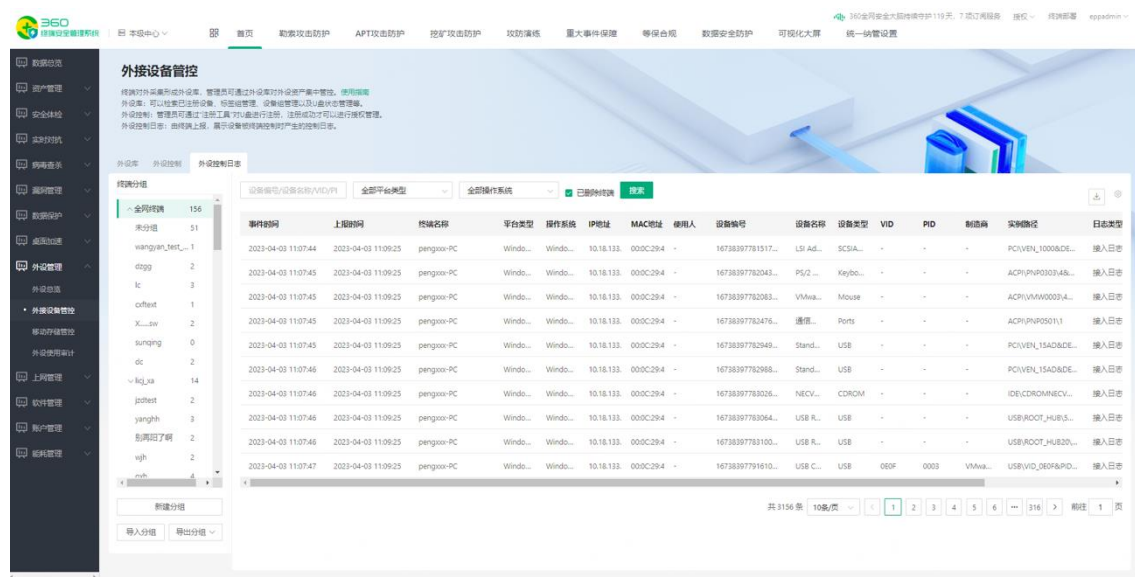
支持控制类型接口控制、光驱控制（内置光驱、USB 光驱）、设备控制；

支持添加外接设备黑白名单；

支持 windows 终端、国产通用桌面机终端；

## 9.2.3.外设控制日志

查看外设控制过程中，终端用户使用外设所产生的行为日志，如下图：



支持通过设备编号/设备名称/VID/PID、平台类型、操作系统类型、分组进行日志检索；

支持导出日志列表；

## 9.3. 移动存储管控

### 9.3.1. 设备列表

管理员用于管理已注册的移动存储设备。如下图：



支持通过设备名称/设备编号/责任人、分组、设备类型、设备状态、标签组、设备组，检索移动存储设备信息；

支持新增、删除标签组；

支持新增、删除设备组；

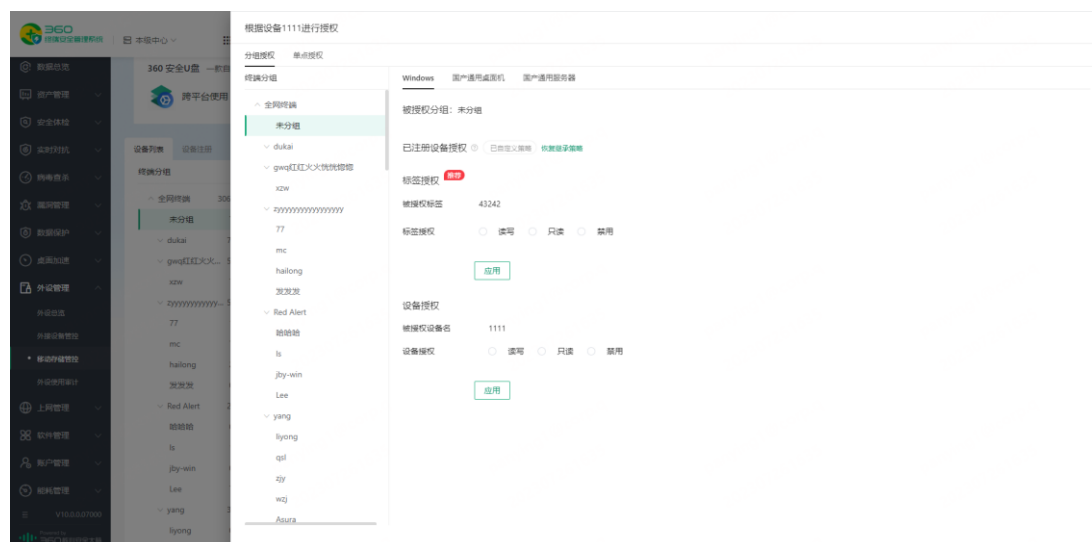
支持查看设备硬件信息；

支持挂失、停用、启用设备；

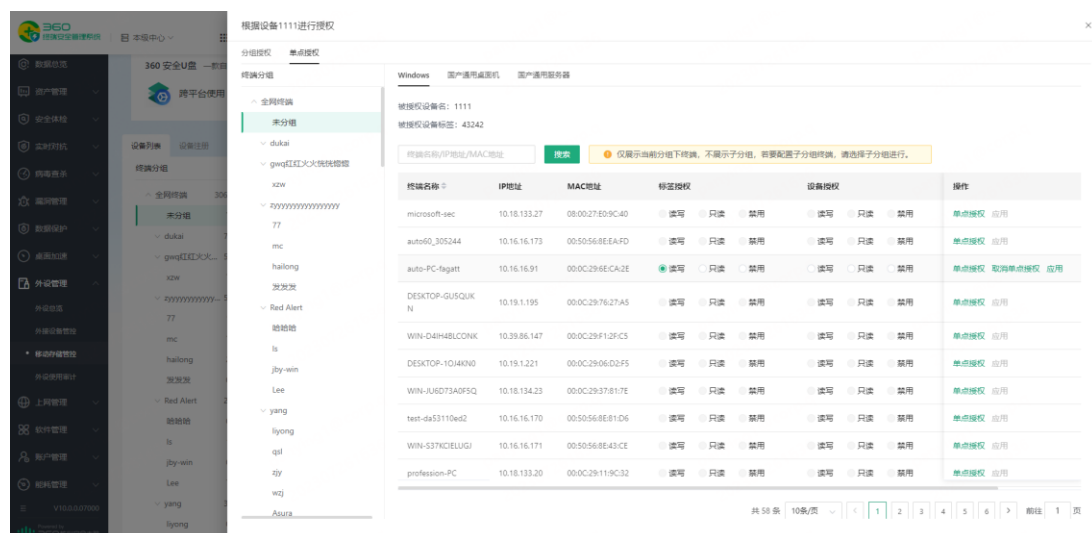
支持导出设备列表信息；

支持基于设备进行授权控制；





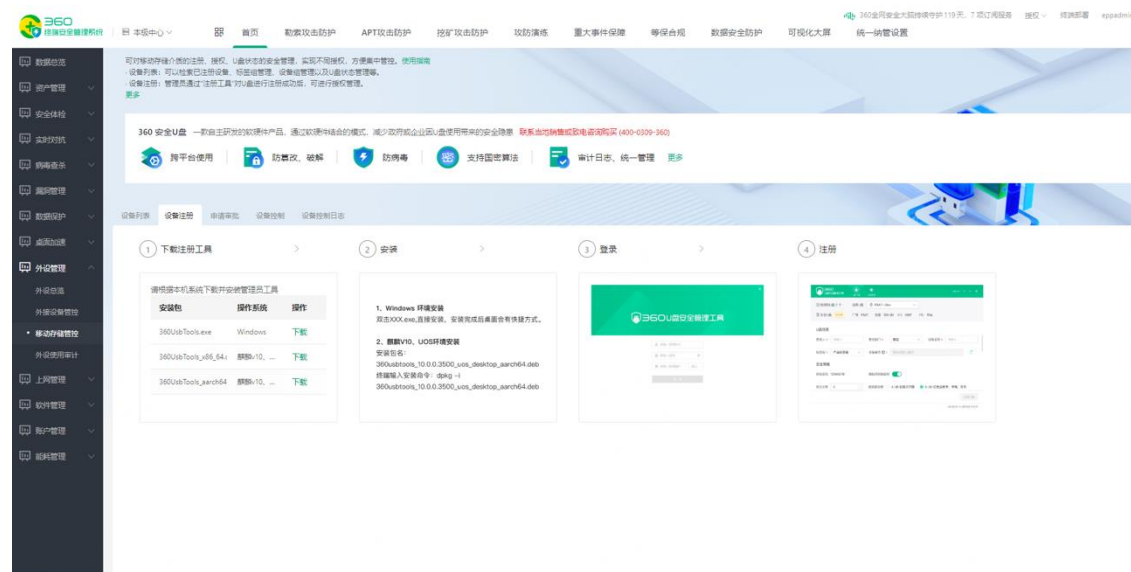
对设备进行分组授权



对设备进行单点授权

## 9.3.2. 设备注册

管理员可通过当前功能，引导管理员进行设备注册。如下图：

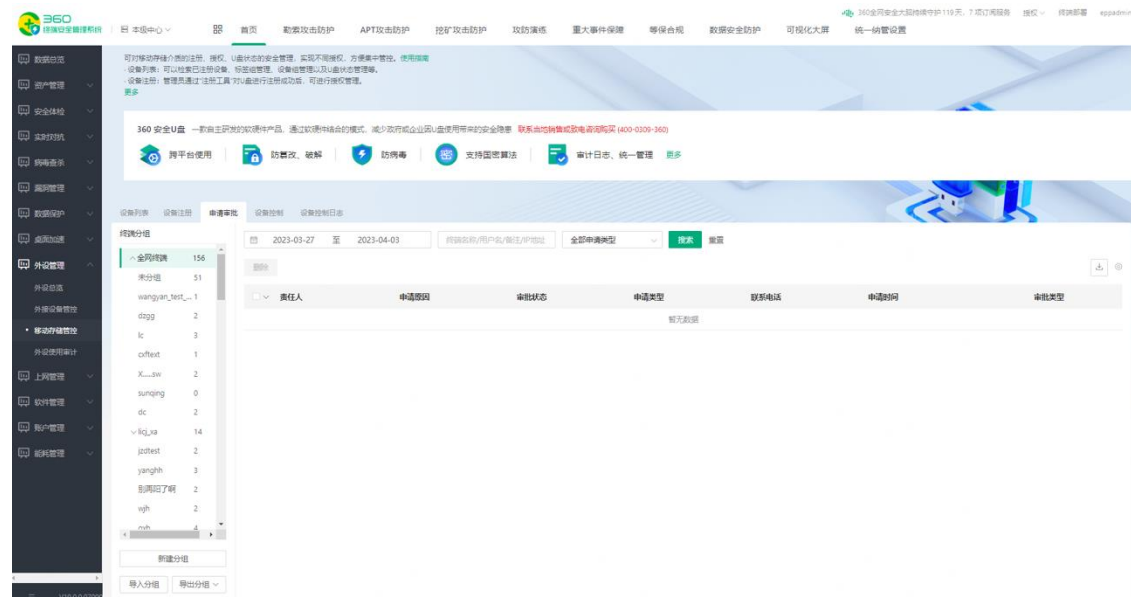


支持根据系统类型需要，下载管理员工具：

工具适配：windows 端、麒麟 V10/UOS+x86、麒麟 V10/UOS+aarch；

### 9.3.3. 设备审批

管理员可通过当前功能，对终端用户的注册申请、注销申请进行审批。如下图：



支持通过时间段、终端名称/用户名/备注/IP 地址、申请类型、分组，对终端用户申请记录进行检索；

支持删除、审批终端申请记录；

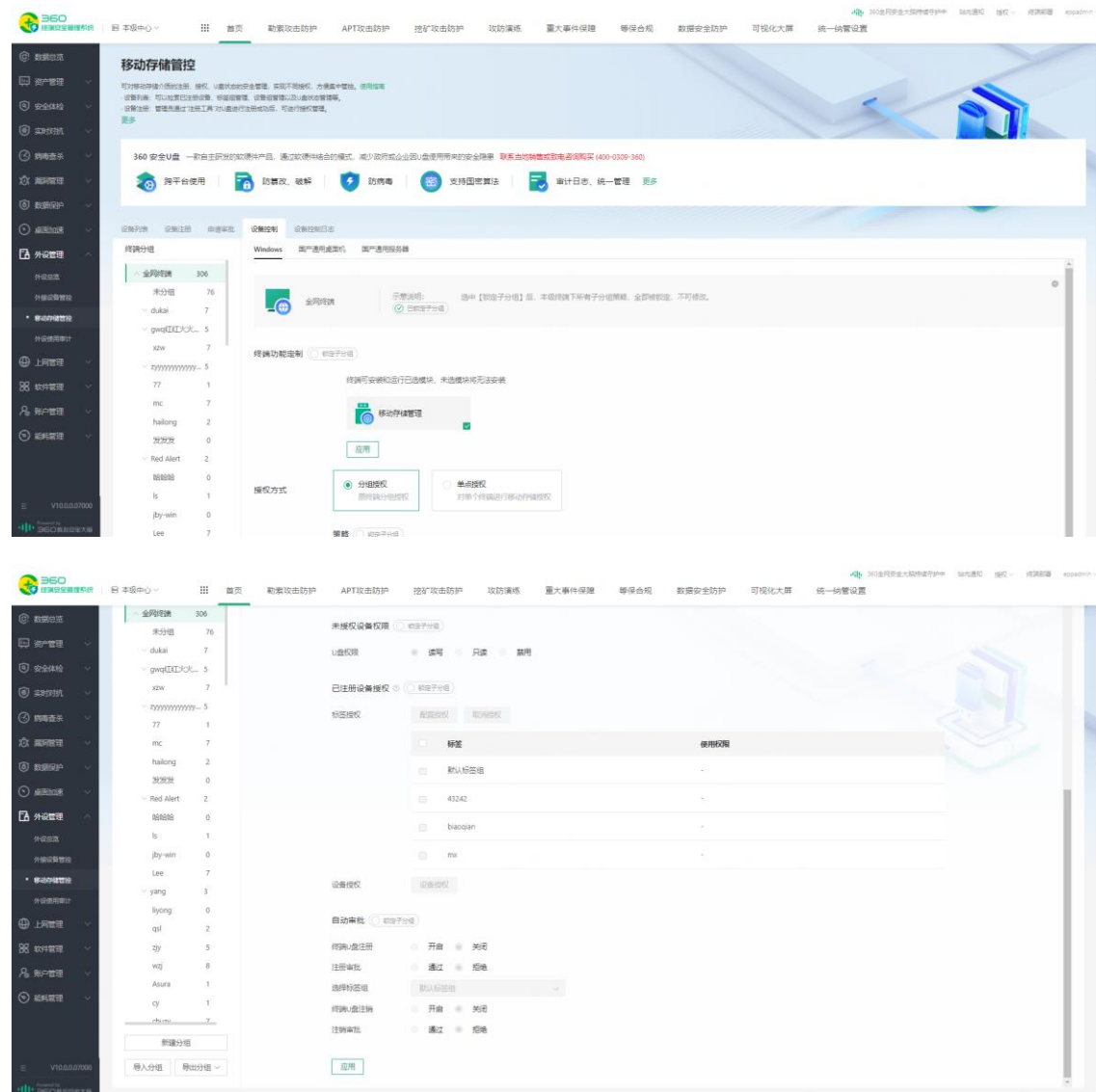
支持导出终端审计记录列表；

说明：目前终端申请仅支持普通 U 盘在 windows 终端下进行申请；

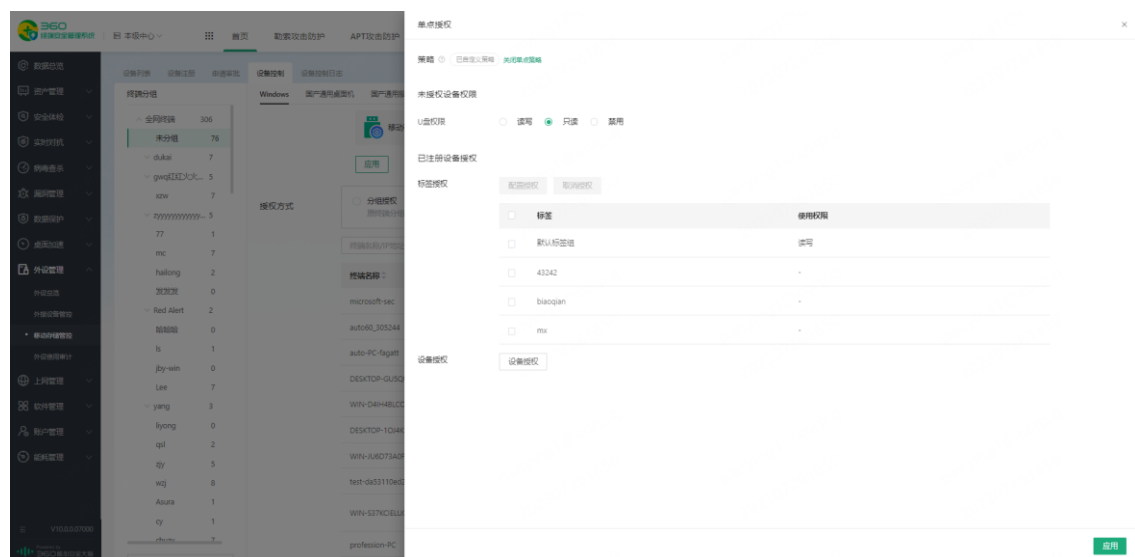
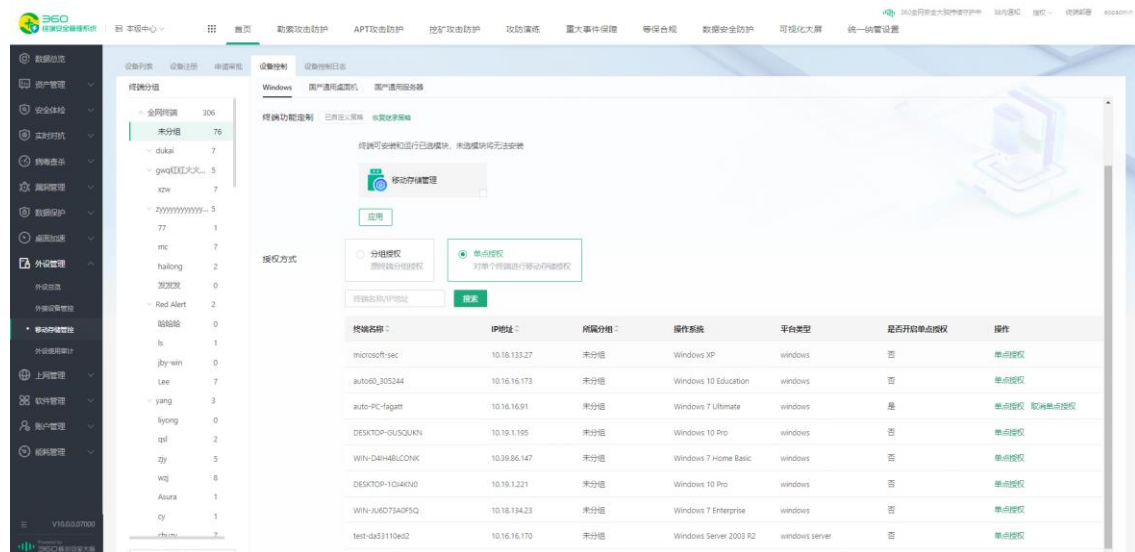
## 9.3.4. 设备控制

管理员通过分组方式，下发移动存储策略到终端，对插入终端的移动存储设备进行控制。

如下图：



分组授权控制



单点授权界面

支持分组授权和单点授权方式；

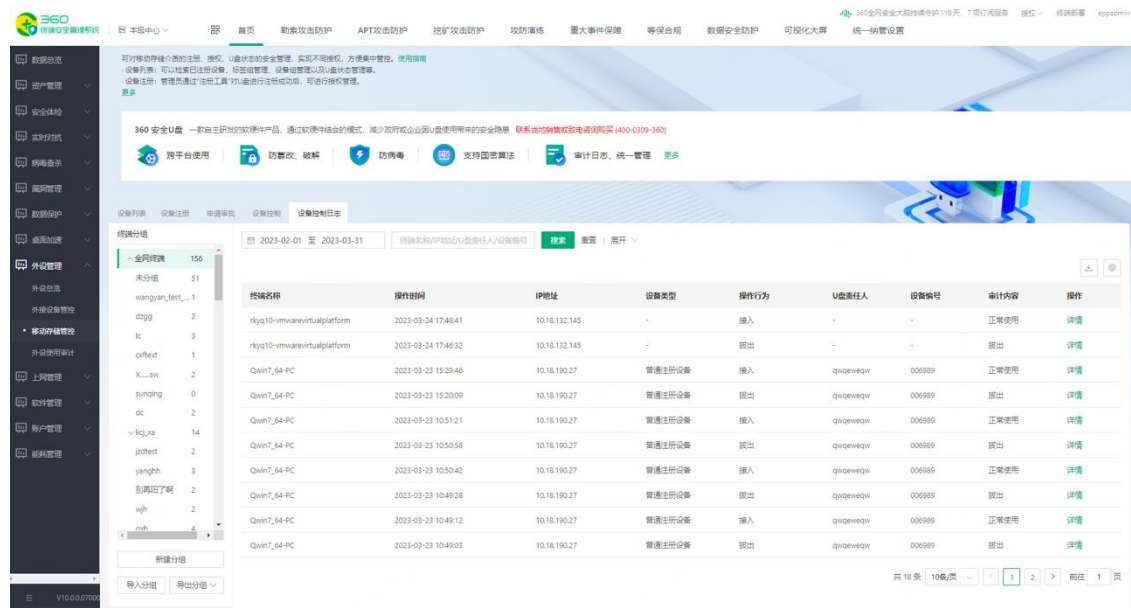
支持未授权设备授权、标签授权、设备授权；

支持自动审批，仅支持普通 U 盘在 windows 终端上；

说明：适配 windows、国产通用桌面机、国产通用服务器；

## 9.3.5. 设备控制日志

管理员查看移动存储设备控制日志。如下图：



支持通过分组、上报时间段、终端名称/IP 地址/U 盘责任人/设备编号、设备类型、U 盘责任部门、平台类型、操作行为类型，进行日志检索；

支持导出日志列表；

支持查看日志详情；

## 9.4. 外设使用审计

记录终端用户使用 USB、蓝牙等外接设备的行为，包括插入、拔出的外接设备的信息。

\*该功能支持对 Windows 终端和国产通用桌面机终端的管理。

### 9.4.1. 功能入口

首页 → 外设管理 → 外设使用审计



## 9.4.2. Windows 终端策略配置

### 1. 策略入口

首页→外设管理→外设使用审计→审计策略→Windows



### 2. 开启管理策略

策略默认是关闭状态，开启策略请选择**启用策略**：



### 3. 设置审计范围

可审计的网络连接范围包括：所有外设的插拔行为、满足特定条件的外设插拔行为。

- 监控记录终端所有外设插拔行为：对终端的所有外设插拔行为进行审计。
- 仅监控记录终端指定的外设插拔操作：对终端接入的特定名称、VID/PID 的设备进行审计。

审计内容

☐ 监控记录终端所有外设插拔行为
 ☒ 仅监控记录终端指定的外设插拔操作

☒ 只审计以下外设的插拔行为
 ☐ 以下外设的插拔行为，不审计（其他均审计）

设备名称列表

设备VID/PID

VID  PID

#### 4. 设置例外鼠标、键盘

对于日常办公常用的鼠标、键盘，可设置例外，不做审计。

☒ 键盘、鼠标类型的插拔行为不做审计

### 9.4.3. 国产通用通用桌面机策略配置

#### 1. 策略入口

首页→外设管理→外设使用审计→审计策略→国产通用桌面机



#### 2. 开启管理策略

策略默认是关闭状态，开启策略请选择启用策略：

外设使用审计 ☐ 锁定子分组

☒ 启用策略 ☐ 禁用策略



### 3. 设置审计范围

可审计的网络连接范围包括：所有外设的插拔行为、满足特定条件的外设插拔行为。

- 监控记录终端所有外设插拔行为：对终端的所有外设插拔行为进行审计。
- 仅监控记录终端指定的外设插拔操作：对终端接入的指定 VID/PID 的设备进行审计。

审计内容

☐ 监控记录终端所有外设插拔行为
 ☒ 仅监控记录终端指定的外设插拔操作

☒ 只审计以下外设的插拔行为
 ☐ 以下外设的插拔行为，不审计（其他均审计）

设备VID/PID

VID 
 PID

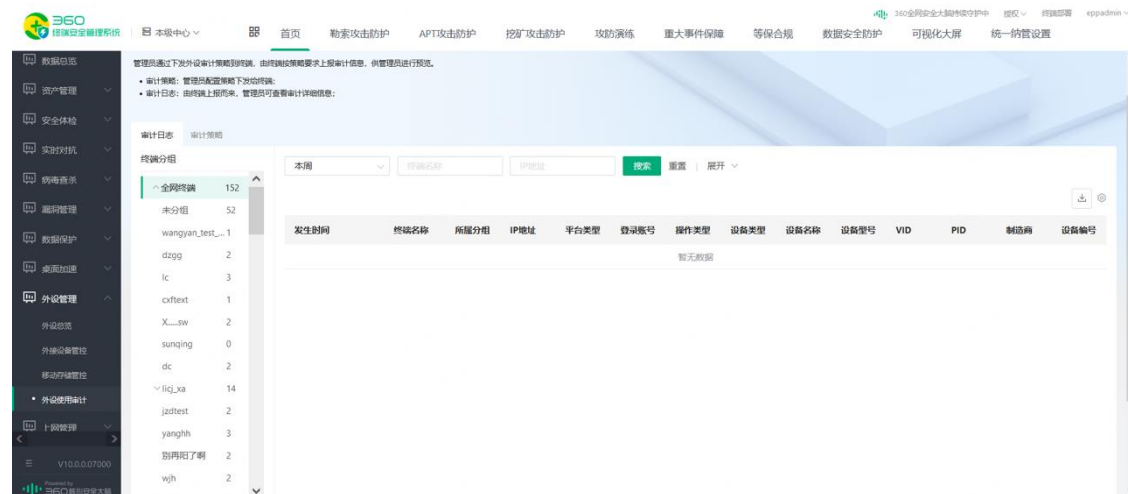
### 4. 设置例外鼠标、键盘

对于日常办公常用的鼠标、键盘，可设置例外，不做审计。

☒ 键盘、鼠标类型的插拔行为不做审计

## 9.4.4. 日志记录

当终端用户发生符合策略配置的外设使用行为时，系统将自动记录日志。



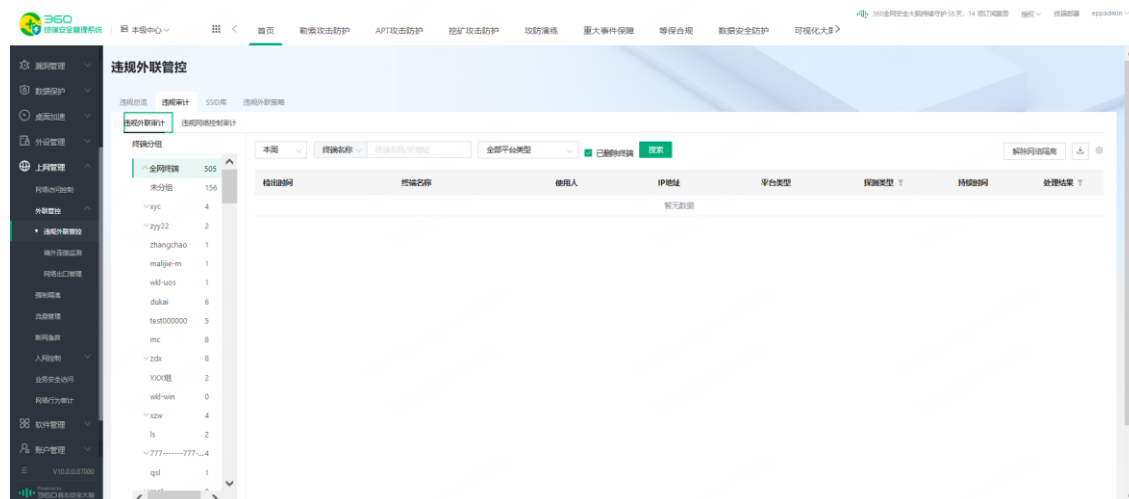




## 10.1.1.2. 违规审计

### 12.3.1.2.1 违规外联审计

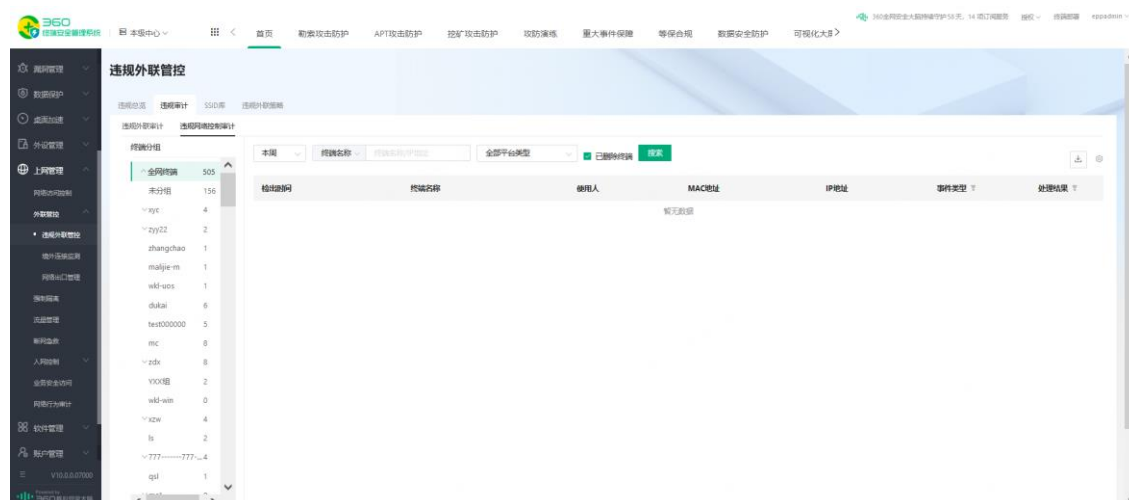
管理员通过此功能，用于查看违规外联审计日志。如下图：



- 支持按分组、时间段、终端名称/IP 地址、平台类型，进行检索；
- 产生违规外联且被断网的终端，支持解除网络隔离；
- 支持导出列表信息；

### 12.3.1.2.2 违规网络控制审计

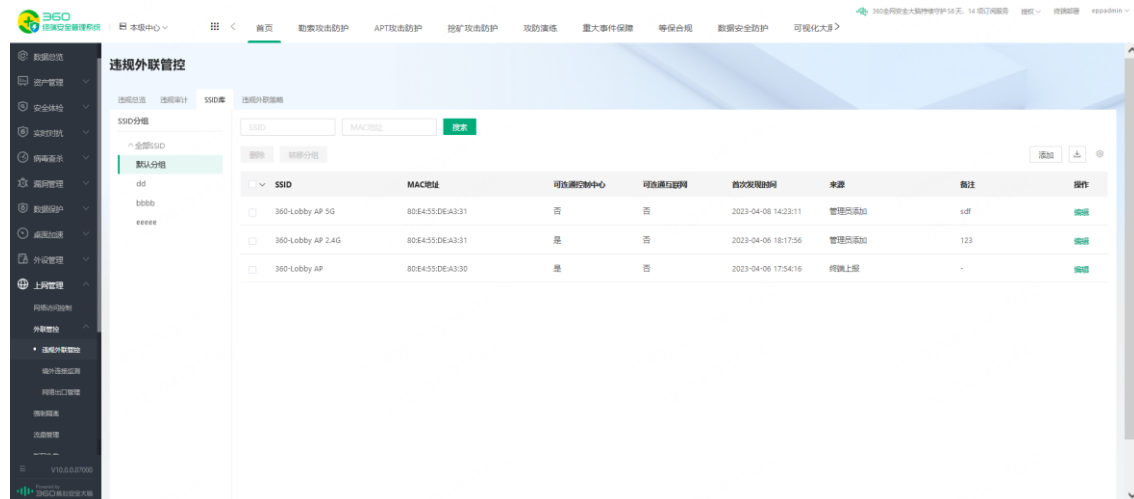
管理员通过此功能，用于查看违规网络控制审计日志。如下图：



- 支持按分组、时间段、终端名称/IP 地址、平台类型，进行检索；
- 支持导出列表信息；

### 10.1.1.3. SSID 库

管理员通过此功能，管理 SSID 信息。如下图：

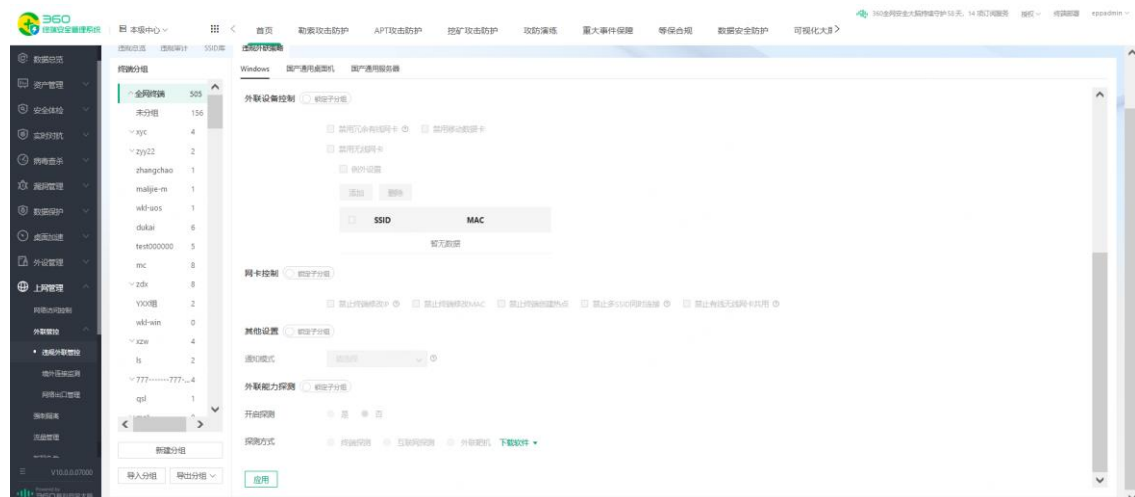


- 支持新增、编辑、删除 SSID 分组信息；
- 支持按 SSID 分组、SSID 名称、MAC 地址，进行检索；
- 支持添加、编辑、删除 SSID 信息；
- 支持转移 SSID 到 SSID 分组；
- 支持导出列表信息；

### 10.1.1.4. 违规外联策略

管理员通过此功能，下发违规外联策略到终端，终端根据策略进行外联设备控制、网卡控制、其他设置、外联能力探测。如下图：





- 支持通过分组下发违规外联策略到终端；
- 支持外设设备控制，包含：禁用冗余有线网卡、禁用移动数据卡、禁用无线网卡、以及 SSID 例外；
- 支持网卡控制，包含：禁止终端修改 IP、禁止终端修改 MAC、禁止终端创建热点、禁止多 SSID 同时连接、禁止有线无线网卡共用；
- 支持其他设置-通知模式设置，包含：直接拦截、拦截时提示终端用户；
- 支持外联能力探测，包含：终端探测、互联网探测、外联靶机；

<1> 终端探测：支持设置探测间隔、探测地址、终端违规处理（不处理、仅告警、断开网络（重启后恢复）、关机（重启后恢复）、断开网络+终端锁屏（重启后恢复）、终端锁屏（重启后恢复）、终端提示）、锁屏密码、外联防护（开机防护、网络变化防护）；

<2> 互联网探测：支持设置探测间隔、出口白名单、终端违规处理（不处理、仅告警、断开网络（重启后恢复）、关机（重启后恢复）、断开网络+终端锁屏（重启后恢复）、终端锁屏（重启后恢复）、终端提示）、锁屏密码、外联防护（开机防护、网络变化防护）；

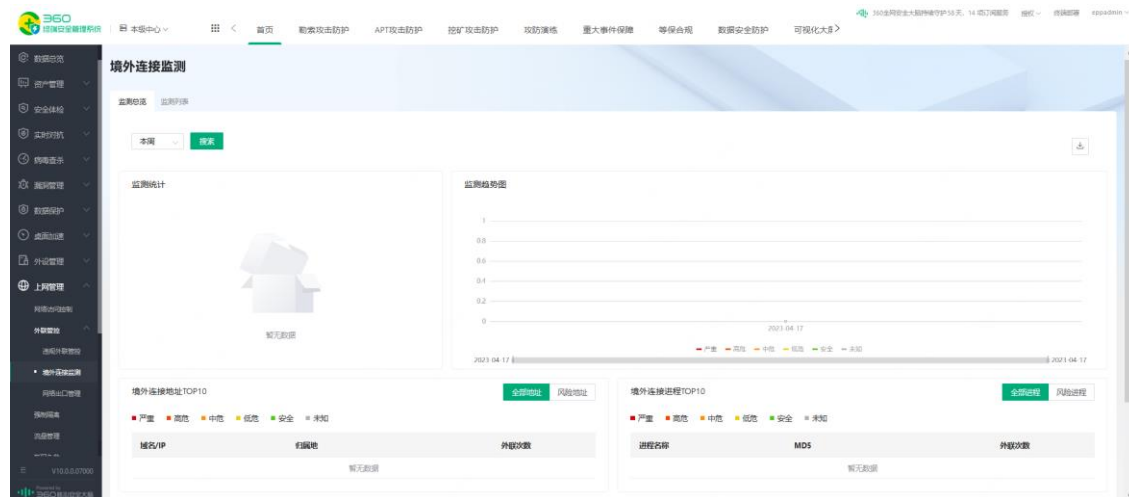
<3> 互联网探测：支持设置探测间隔、外联靶机地址、出口白名单、终端违规处理（不处理、仅告警、断开网络（重启后恢复）、关机（重启后恢复）、断开网络+终端锁屏（重启后恢复）、终端锁屏（重启后恢复）、终端提示）、锁屏密码、外联防护（开机防护、网络变化防护）；

- 支持终端类型：windows、国产通用桌面机、国产通用服务器；

## 10.1.2. 境外连接监测

### 10.1.2.1. 监测总览

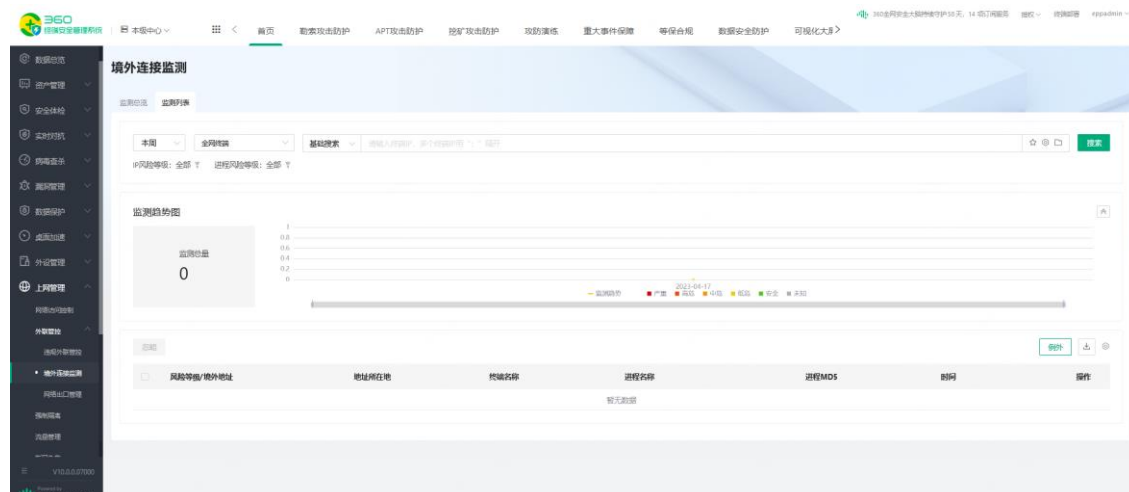
管理员通过此功能，可查看全网境外连接分布情况，包含监测统计数量、监测趋势图、境外连接地址 TOP10、境外连接进程 TOP10、境外连接终端 TOP10。如下图：



- 支持通过时间段来查看监测总览数据；

### 10.1.2.2. 监测列表

管理员通过此功能，可查看境外连接的详细监测数据。如下图：

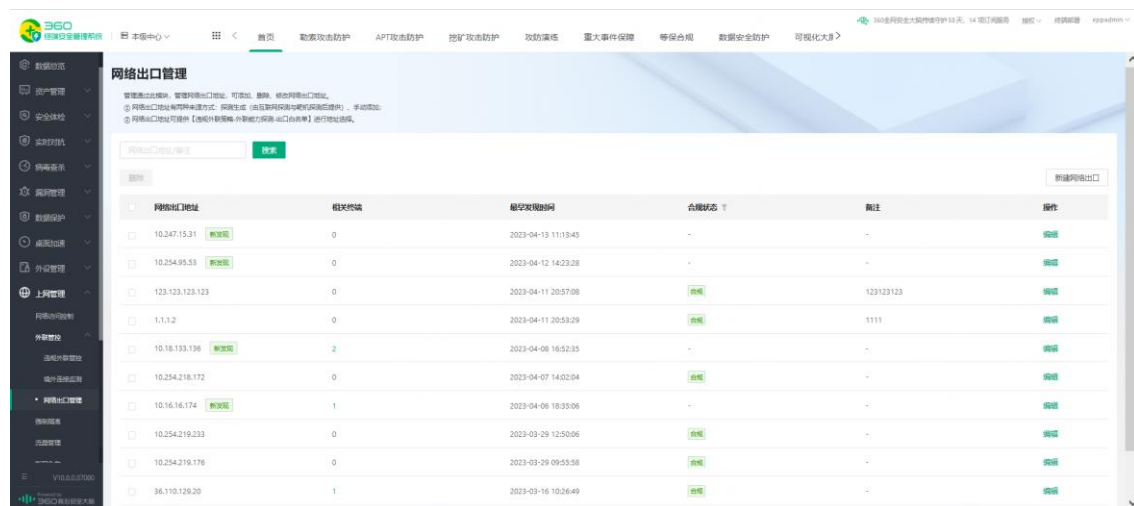


- 支持通过时间段、终端分组、基础搜索、高级搜索，进行检索；
- 基础搜索与高级搜索：支持收藏、查看收藏、检索使用指南；
- 支持忽略、例外监测地址；

- 支持导出监测地址列表；

## 10.1.3.网络出口管理

管理员通过此功能，可对网络出口进行管理。如下图：

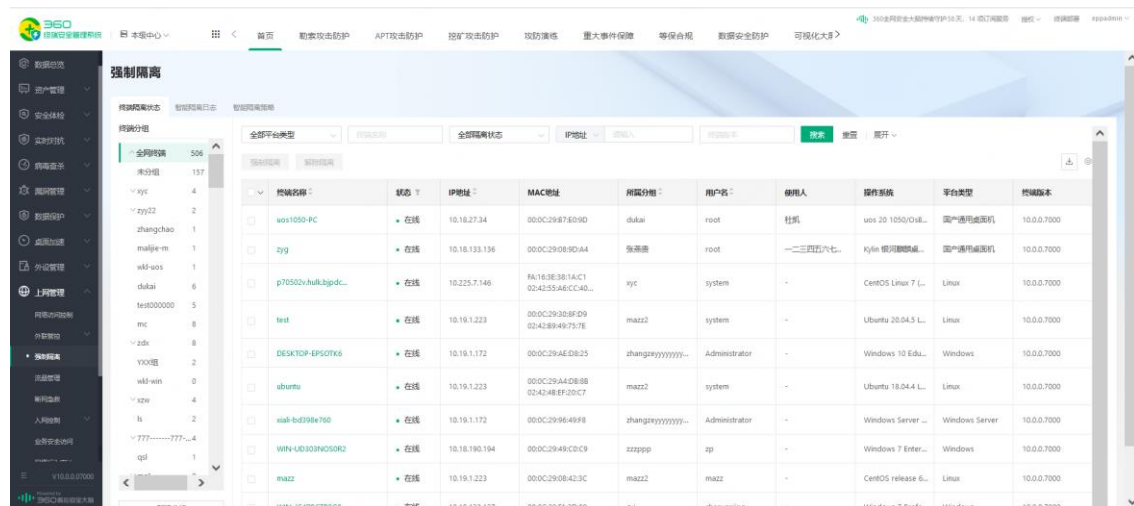


- 支持通过网络出口地址/备注、合规状态，进行检索网络出口信息；
- 支持新增、编辑、删除网络出口信息；
- 支持标记网络出口是否合规；

## 10.2. 强制隔离

### 10.2.1.终端隔离状态

点击左侧功能导航：首页>上网管理>强制隔离>终端隔离状态，进入终端隔离状态页面。



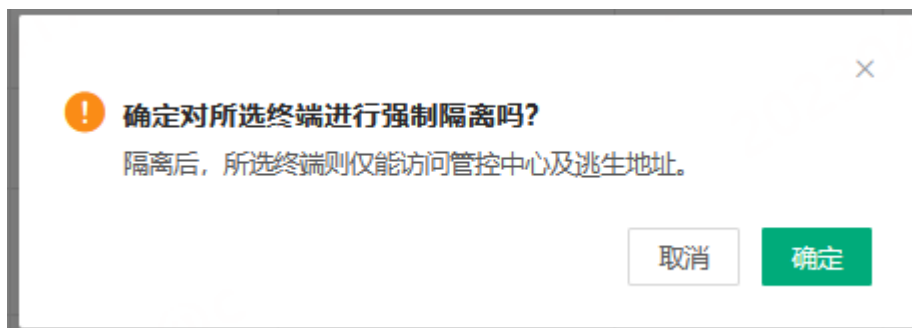
1、筛选：支持根据平台类型、终端名称、隔离状态、IP/IP 段、终端版本、操作系统、Mac 地址、用户名、内网 IP/IP 段、使用人、归属部门，对终端列表进行筛选查看。

## 2、强制隔离

1) 可手动在列表中勾选需要隔离的终端，勾选后点击“强制隔离”操作按钮。

强制隔离 解除隔离 已选 1 条										
<input checked="" type="checkbox"/>	终端名称	状态	IP地址	MAC地址	所属分组	用户名	使用人	操作系统	平台类型	终端版本
<input checked="" type="checkbox"/>	uos1050-PC	在线	10.18.27.34	FA:16:3E:38:1A:C1 02:42:55:A6:CC:40	dukai	root	杜凯	uos 20 1050/Os8...	国产通用桌面机	10.0.0.7000
<input type="checkbox"/>	zyg	在线	10.18.133.136	02:42:38:C0:3D:0E	张燕贵	root	一二三四五六七	Kylin 银河麒麟桌...	国产通用桌面机	10.0.0.7000
<input type="checkbox"/>	p70502v.hulkbjpdc...	在线	10.225.7.146	FA:16:3E:38:1A:C1 02:42:55:A6:CC:40...	xye	system	-	CentOS Linux 7 (...)	Linux	10.0.0.7000

2) 页面弹出二次确认窗口，确认是否对所选终端下发隔离操作。点击“确认”后，则对所选终端下发隔离指令；点击“取消”则返回列表。



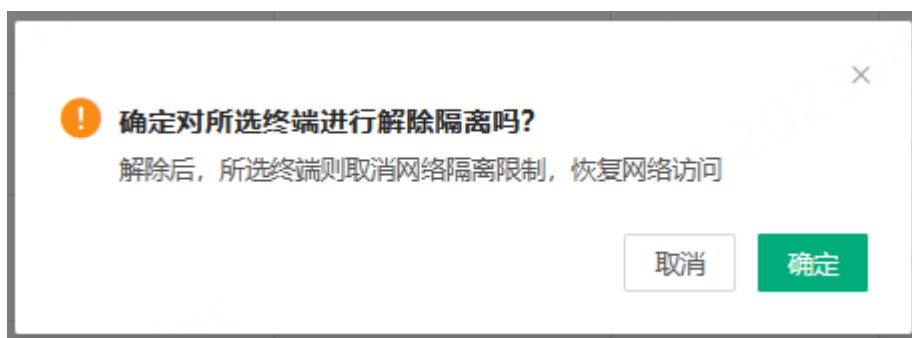
3) 终端被隔离后，隔离状态则变为已隔离状态。

## 3、解除隔离

1) 可手动在列表中勾选需要解除隔离的终端，勾选后点击“解除隔离”操作按钮。

强制隔离 解除隔离 已选 1 条										
<input checked="" type="checkbox"/>	终端名称	状态	IP地址	MAC地址	所属分组	用户名	使用人	操作系统	平台类型	终端版本
<input checked="" type="checkbox"/>	uos1050-PC	在线	10.18.27.34	00:0C:29:87:E0:9D	dukai	root	杜凯	uos 20 1050/Os8...	国产通用桌面机	10.0.0.7000
<input type="checkbox"/>	zyg	在线	10.18.133.136	00:0C:29:08:9D:A4	张燕贵	root	一二三四五六七	Kylin 银河麒麟桌...	国产通用桌面机	10.0.0.7000
<input type="checkbox"/>	p70502v.hulkbjpdc...	在线	10.225.7.146	FA:16:3E:38:1A:C1 02:42:55:A6:CC:40...	xye	system	-	CentOS Linux 7 (...)	Linux	10.0.0.7000

2) 页面弹出二次确认窗口，确认是否对所选终端下发隔离操作。点击“确认”后，则对所选终端下发隔离指令；点击“取消”则返回列表。



3) 终端被解除隔离后，隔离状态则变为未隔离状态。

4、导出列表：点击“导出”按钮，支持导出终端隔离状态列表。

强制隔离

解除隔离

已选 1 条

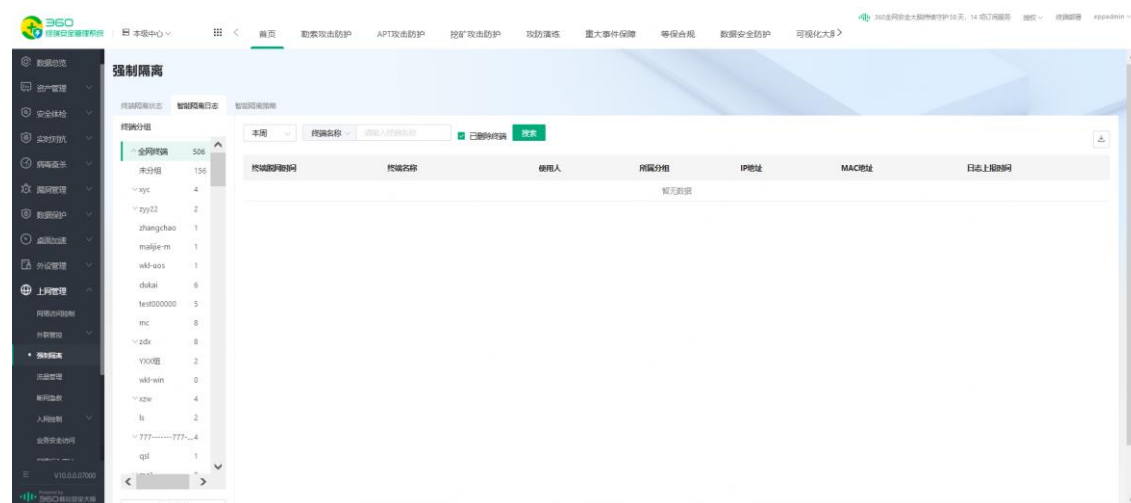
📄

🔍

<input checked="" type="checkbox"/> 终端名称	状态	IP地址	MAC地址	所属分组	用户名	使用人	操作系统	平台类型	终端版本
<input checked="" type="checkbox"/> uos1050-PC	<div>● 在线</div>	10.18.27.34	00:0C:29:87:E0:9D	dukai	root	杜凯	uos 20 1050/Os8...	国产通用桌面机	10.0.0.7000
<input type="checkbox"/> zyg	<div>● 在线</div>	10.18.133.136	00:0C:29:08:9D:A4	张燕贵	root	一二三四五六七...	Kylin 银河麒麟桌...	国产通用桌面机	10.0.0.7000
<input type="checkbox"/> p70502vhulkbjpd...	<div>● 在线</div>	10.225.7.146	FA:16:3E:3B:1A:C1 02:42:55:A6:CC:4D...	xyz	system	-	CentOS Linux 7 (...	Linux	10.0.0.7000

## 10.2.2.智能隔离日志

点击左侧功能导航：首页>上网管理>强制隔离>智能隔离日志，进入智能隔离日志页面。



1、筛选：支持根据时间、终端名称、IP 地址筛选查看智能隔离日志



2、导出：支持点击“导出”按钮，将智能隔离日志导出为 xls 文件。

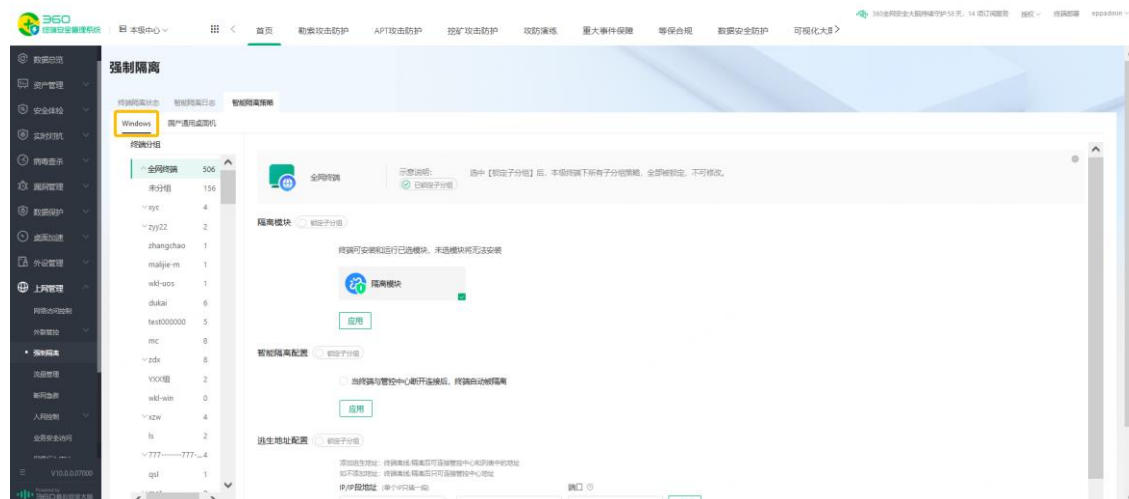


## 10.2.3.智能隔离策略

### 10.2.3.1. Windows 平台策略

点击左侧功能导航：首页>上网管理>强制隔离>智能隔离策略>windows，进入智能隔离策略页面。





## 1、隔离模块

隔离模块 ☐ 锁定子分组

终端可安装和运行已选模块，未选模块将无法安装



应用

隔离模块：勾选/取消该模块，终端则会动态安装/卸载该模块。

## 2、智能隔离配置

智能隔离配置 ☐ 锁定子分组

☐ 当终端与管控中心断开连接后，终端自动被隔离

应用

当终端与管控中心断开连接后，终端自动被隔离：勾选该项策略后，如果终端与管控中心断开连接，则终端自动被隔离；当终端恢复与管控中心连接后，则终端自动恢复到未隔离状态。隔离后的终端，则仅允许访问管控中心地址及逃生地址。

## 3、逃生地址配置

#### 逃生地址配置 ☐ 锁定子分组

添加逃生地址：终端离线/隔离后可连接管控中心和列表中的地址  
如不添加地址：终端离线/隔离后只可连接管控中心地址

IP/IP段地址 (单个IP只填一段)

端口 <sup>?</sup>

IP地址	端口	操作
暂无数据		

可在此处配置逃生地址；当终端状态为隔离状态时，也可以正常访问该列表中配置的地址。

### 10.2.3.2. 国产通用桌面机平台策略

点击左侧功能导航：首页>上网管理>强制隔离>智能隔离策略>windows，进入智能隔离策略页面。

#### 1、智能隔离配置

##### 智能隔离配置

☐ 锁定子分组

☐ 当终端与管控中心断开连接后，终端自动被隔离

应用

当终端与管控中心断开连接后，终端自动被隔离：勾选该项策略后，如果终端与管控中心断开连接，则终端自动被隔离；当终端恢复与管控中心连接后，则终端自动恢复到未隔离状态。隔离后的终端，则仅允许访问管控中心地址及逃生地址。

#### 2、逃生地址配置

##### 逃生地址配置 ☐ 锁定子分组

添加逃生地址：终端离线/隔离后可连接管控中心和列表中的地址  
如不添加地址：终端离线/隔离后只可连接管控中心地址

IP/IP段地址 (单个IP只填一段)

端口 <sup>?</sup>

IP地址	端口	操作
暂无数据		

可在此处配置逃生地址；当终端状态为隔离状态时，也可以正常访问该列表中配置的地

址。

## 10.3. 典型场景

### 1. 网络连接审计

- 场景描述：员工在日常工作中，出于工作或娱乐的需要，都或多或少的涉及到与网络的连接。如果用户访问了不安全的网站，可能给企业网络引入病毒、或窃取重要数据等安全风险。为了后续对终端网络访问行为的审计、以及违规溯源，需要能够还原事件。
- 解决方案：开启“网络连接审计”功能，设定要审计的网络连接范围。当终端用户发生符合策略要求的访问行为时，系统将自动记录连接日志，定位到终端信息、访问的目标 IP 及端口信息等。

### 2. 外联管控

出于安全保密需要，特定的政企单位或者机要部门需要在隔离网环境办公，切断跟外部互联网的联系。为了更有效、更及时侦测内部终端是否存在非法连接外网或指定网络的行为，360 终端安全管理系统提供了外联探测功能。通过域名解析、PING 地址探测、TCP 链接检测的方式，去发现终端的非法外联行为，并可对违规终端执行断网处置。对于互联网用户则支持互联网出口地址检测，及时发现通过非法出口联网的行为。支持对可信无线 SSID 做白名单管理。

### 3. 强制隔离

当用户在进行攻防演练和重保场景时，终端设备如果出现沦陷的情况，可立即采取对该终端网络进行强制隔离操作，限制该终端的网络访问，防止终端风险扩散。当终端解除风险后，可再通过解除隔离操作，对终端进行隔离解除，恢复终端网络。

### 4. 入网控制场景 1（防止非法终端访问核心业务服务器，守护 EPP 客户端，保障入网终端安全可信）

- 场景描述：未知终端或不安全的终端对关键业务服务器的访问，可能会给内网核心业务服务器造成极大的安全风险，也可能造成内部重要业务系统信息被非法访问。
- 解决方案：可启用应用准入功能，同时开启入网安全检查，为安装 epp 客户端或安全检查未通过的终端，无法访问业务服务器。

### 5. 入网控制场景 2（网络边界端口级接入防护）

- 场景描述：企业内部网络建设相对规范，对于网络接入有较为严格的管理需求，希望

能在链路层对网络接入进行控制。

- 解决方案：可启用 802.1X 准入功能，对接入终端和用户进行认证，未经认证的终端和用户将无法接入网络。

#### 6. 入网控制场景 3（强制入网绑定）

- 场景描述：希望对终端接入的 ip、mac、用户名、交换机端口等条件中的一个或多个进行绑定。
- 解决方案：可启用 802.1X 准入的入网绑定规则条件，不符合绑定条件的认证请求将无法接入网络。

#### 7. 入网控制场景 4（身份认证对接）

- 场景描述：希望在准入认证过程中对接入用户身份进行认证，且认证源为企业已有认证源
- 解决方案：通过配置身份认证策略规则，可实现与 ad、ldap、钉钉、短信等认证源的对接认证。

#### 8. 入网控制场景 5（访客入网）

- 场景描述：存在访客入网的需求，且希望对访客入网进行认证。
- 解决方案：启用应用准入无客户端认证，开启申请入网。

#### 9. 入网控制场景 6（从链路层控制接入网络后的网络访问权限）

- 场景描述：在准入认证通过后，能在链路层对终端可访问网络的权限进行控制，避免终端越权访问网络资源。
- 解决方案：启用 802.1X 准入或 portal 准入，并配置“访问范围控制”策略。

#### 10. 网站访问管理场景

- 场景描述：员工使用办公电脑工作期间，为了提高工作效率，禁止员工访问诸如视频、游戏等娱乐网站。同时，为了防止员工向贴吧等网站发送包含工作信息的内容，也阻止其访问此类网站。
- 解决方案：启用网络访问行为监控策略，在终端访问以上网站时，实施拦截，阻止访问。

## 11. 软件管理

### 11.1. 基本概念

#### 11.1.1. 软件管家

软件管家提供软件自助管理功能，通过软件管家，终端用户可以便捷安装并更新与业务有关的应用软件，管理员则可以通过软件管家构建一套由单位自运营的合规软件平台。

提供本地软件库以及互联网软件库，可以根据需要选择使用、内置几千款精选软件满足通用办公需求，用户自主使用，终端用户可自行下载、安装或更新办公应用。

#### 11.1.2. 应用软件

应用软件（Application）是和系统软件相对应的，分为应用软件包和用户程序。

软件管家中的软件主要是指应用软件，是为满足用户不同领域、不同问题的应用需求而提供的那部分软件，运行于 WINDOWS 操作系统中，可以拓宽计算机系统的应用领域，放大硬件的功能。

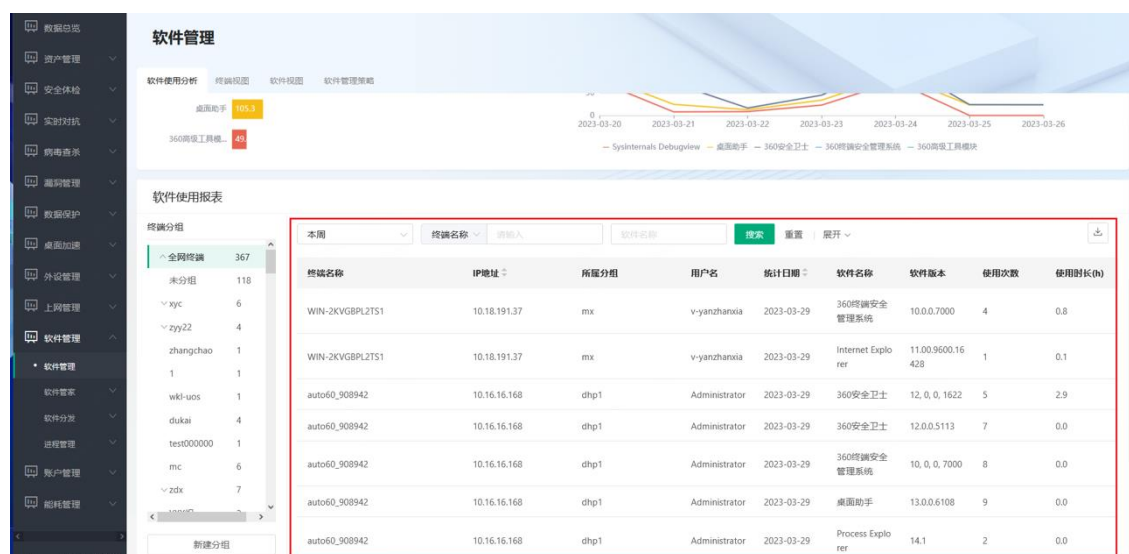
### 11.2. 软件管理

#### 11.2.1. 软件使用分析

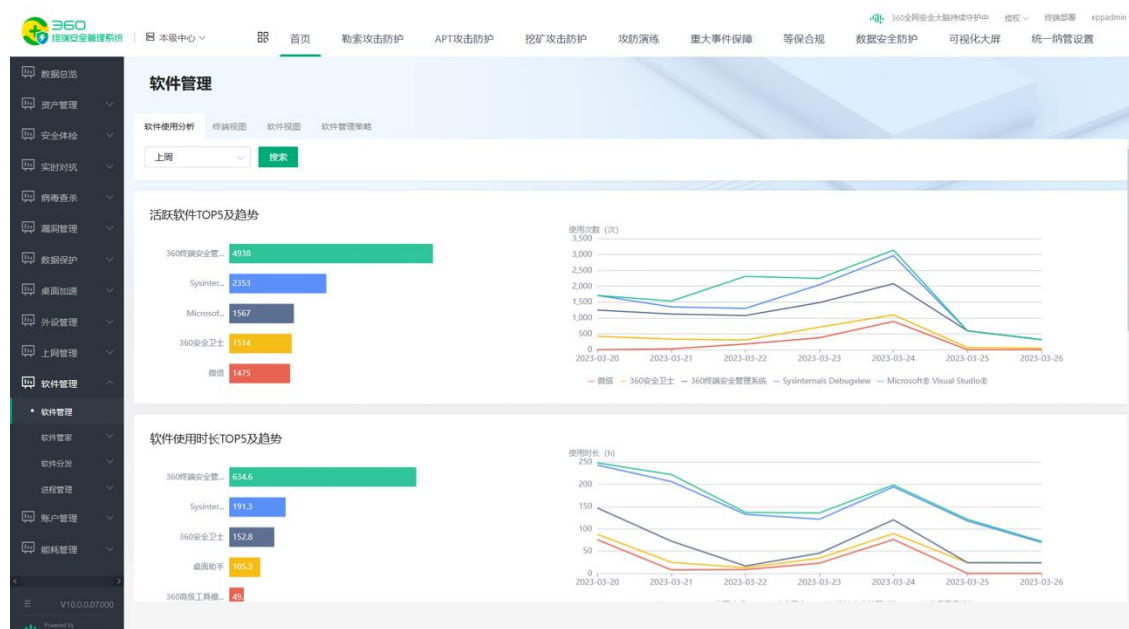
- (1) 软件使用分析：软件使用信息采集和分析，针对终端每天使用应用程序的时长和次数进行统计。
- (2) 软件使用报表：对软件使用情况进行记录，包括统计日期、软件名称、软件版本、使用次数、使用时长。
- (3) 软件活跃度统计：统计周期范围内，全网终端软件使用次数 top5 的软件，绘制每天的使用趋势。
- (4) 软件使用时长统计：统计周期范围内，全网终端软件使用时长 top5 的软件，绘制每天的使用趋势。

点击左侧导航：**软件管理** > **软件管理** > **软件使用分析**，进入页面查看。

- 使用日志



## ● 趋势分析

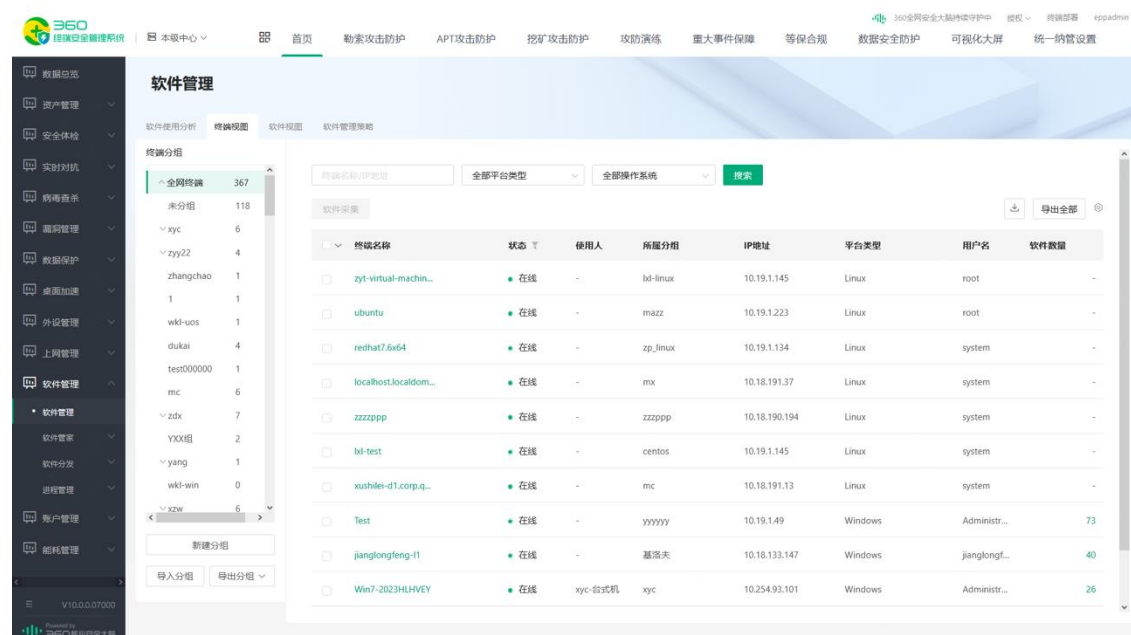


## 11.2.2.终端视图

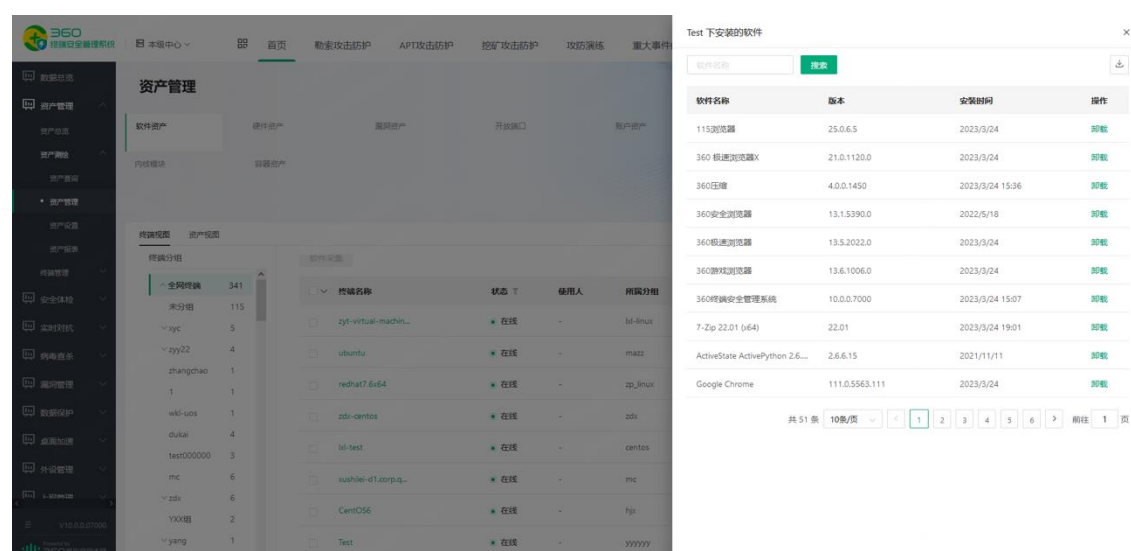
以终端为维度，查看终端已安装的软件列表，支持平台类型、操作系统匹配模糊搜索；支持点击高亮数字查看终端信息；支持对终端已安装的软件卸载。

点击左侧导航：**软件管理** > **软件管理** > **终端视图**，进入页面查看。

### 1) 终端视图



## 2) 终端软件列表



说明：国产通用桌面机、国产通用服务器、linux 系统不支持卸载软件。

## 11.2.3.软件视图

以软件名为维度，查看终端已安装的软件列表，可以点击高亮数字查看终端信息。支持对终端已安装的软件卸载。



点击左侧导航：软件管理>软件管理>软件视图，进入页面查看。

### 3) 资产视图

**软件管理**

软件使用分析 终端视图 软件视图 软件管理策略

终端分组

- 全网终端 367
  - 未分组 118
  - xyx 6
  - zyy22 4
  - zhangchao 1
  - 1 1
  - wkl-uos 1
  - dukai 4
  - test000000 1
  - mc 6
  - zdx 7
  - YXX组 2
  - yang 1
  - wkl-win 0
  - xzw 6

新建分组 导入分组 导出分组

Windows&Winserver终端: 367台 | “软件信息”模块开启统计 已开启: 186台 | 未开启: 181台

软件名	版本范围	已安装终端
Apache Tomcat 7.0 Tomcat7 (remove only)	7.0.75	1
Java 7 Update 80 (64-bit)	7.0.800	1
Java SE Development Kit 7 Update 80 (64-bit)	1.7.0.800	1
Java(TM) SE Development Kit 11.0.16 (64-bit)	11.0.16.0	1
Microsoft Office 2003 Web Components	11.0.6558.0	1
Microsoft SQL Server 2005 (64 位)	-	1
Microsoft SQL Server 2005 简体中文	8.05.1054	1
Microsoft SQL Server 2008 R2 安装程序(简体中文)	10.52.4000.0	1
Microsoft SQL Server Native Client	9.00.1399.06	1
Microsoft SQL Server VSS 编辑器	9.00.1399.06	1

### 4) 终端列表

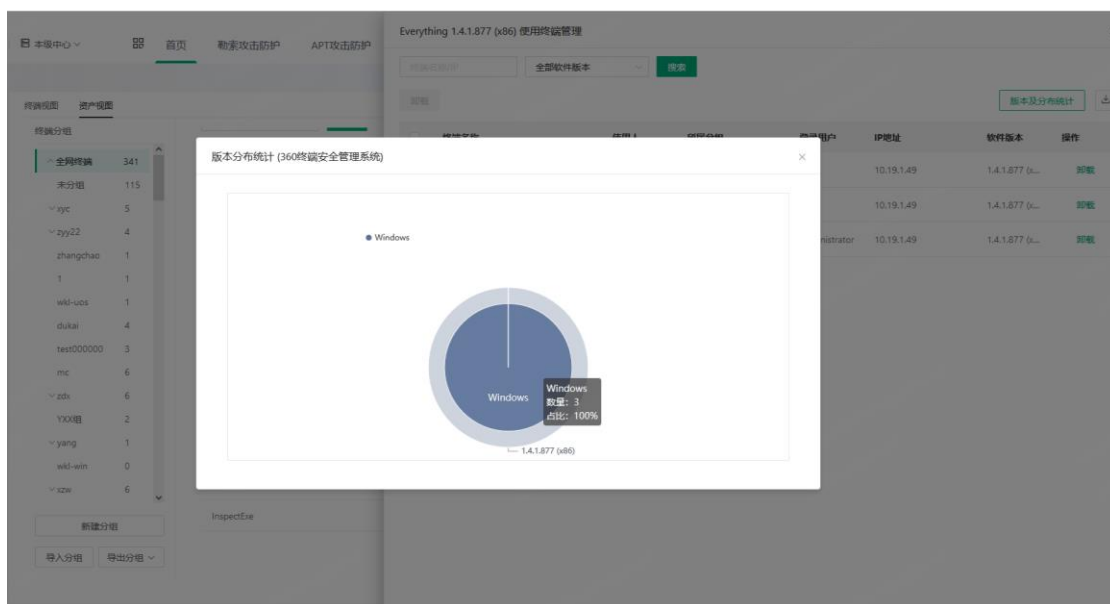
**Everything 1.4.1.877 (x86) 使用终端管理**

终端名称 使用人 所属分组 登录用户 IP地址 软件版本 操作

DESKTOP-J914859	-	YXXXXY	Test	10.19.1.49	1.4.1.877 (x86)	卸载
DESKTOP-J914859	-	YXXXXY	Test	10.19.1.49	1.4.1.877 (x86)	卸载
lylle-5524138	-	未分组	Administrator	10.19.1.49	1.4.1.877 (x86)	卸载

### 5) 版本分布





说明：国产通用桌面机、国产通用服务器、linux 系统不支持卸载软件。

## 11.2.4.软件安装监控日志

支持查看软件安装监控日志。



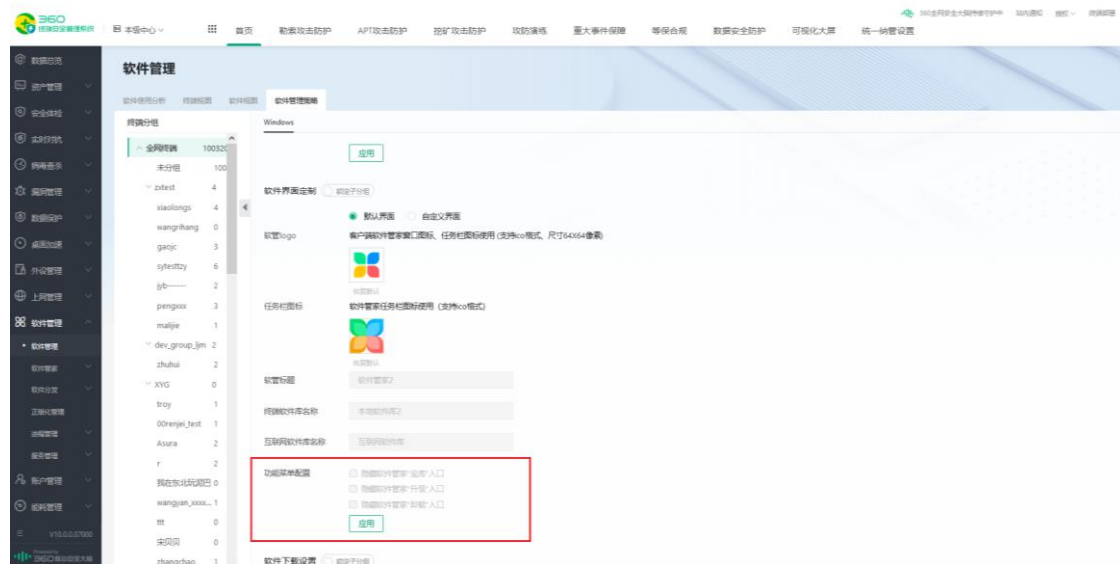
## 11.2.5.软件管理策略

支持按分组策略对终端软件管家的相关能力进行配置，具体包括：

(1) 软件管家客户端：软件管家功能模块化，管理员可在此为分组终端设置是否显示软件管家客户端。

(2) 终端软件库：管理员可为终端分组设置客户端所显示的软件库，支持终端同时显示本地软件库和互联网软件库

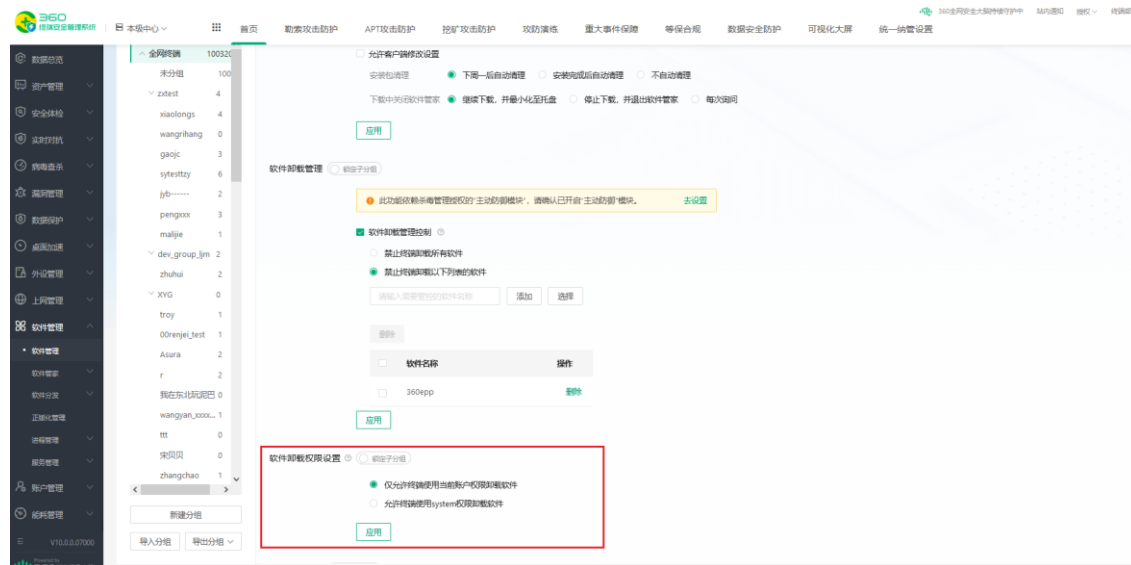
(3) 软管界面定制：支持对软管 logo、软管标题、软件库名称进行定制展示。支持对“宝库”、“升级”、“卸载”三个菜单项的隐藏状态进行配置。当勾选并下发后，软件管家客户端不显示相应的菜单项。



(4) 客户端设置项-可管可控：支持对客户端软件下载设置项进行配置，可限制终端用户进行修改。管理员可统一配置客户端软件下载保存路径，并能锁定保存路径。

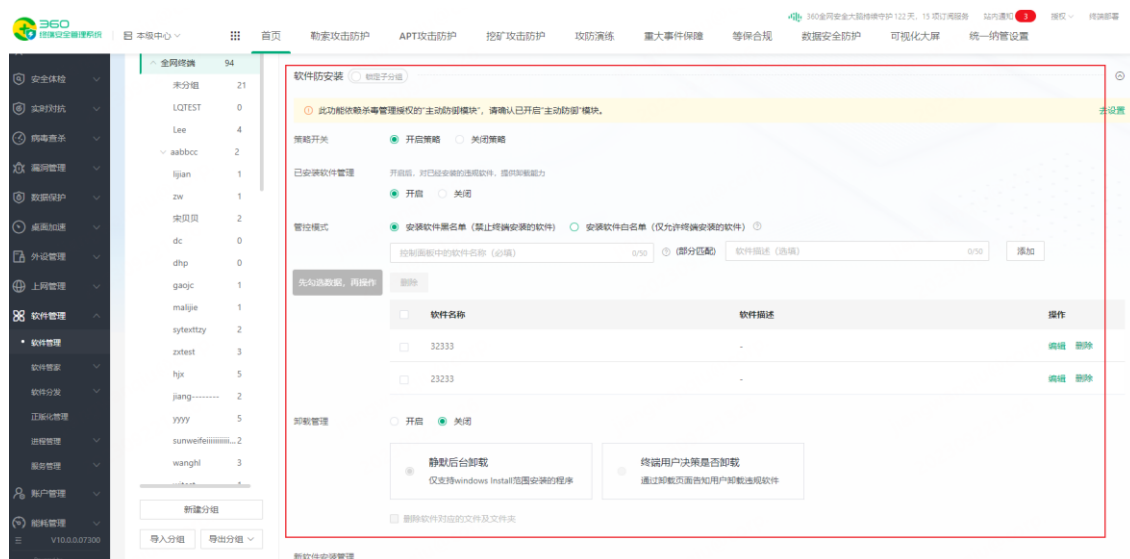
(5) 软件卸载管理：支持配置软件卸载相关策略，可以对软件在终端的卸载行为进行控制，达到终端用户无法卸载某些软件的效果。

(6) 软管卸载权限配置：提供“仅允许终端使用当前账户权限卸载软件”和“允许终端使用 system 权限卸载软件”两种模式，提供管理员按需进行配置软管客户端的卸载权限。

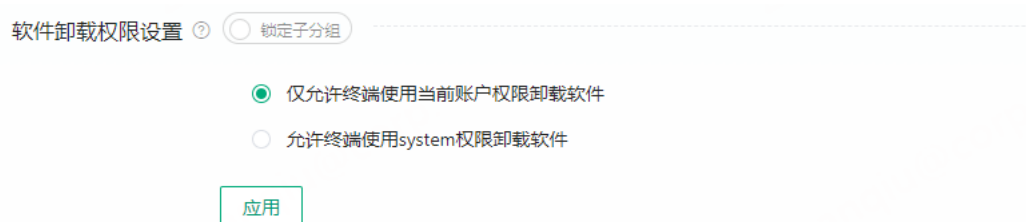


(7) 软件使用分析上报：支持配置软件数据统计相关策略，管理终端软件使用信息日志上报频率等功能。

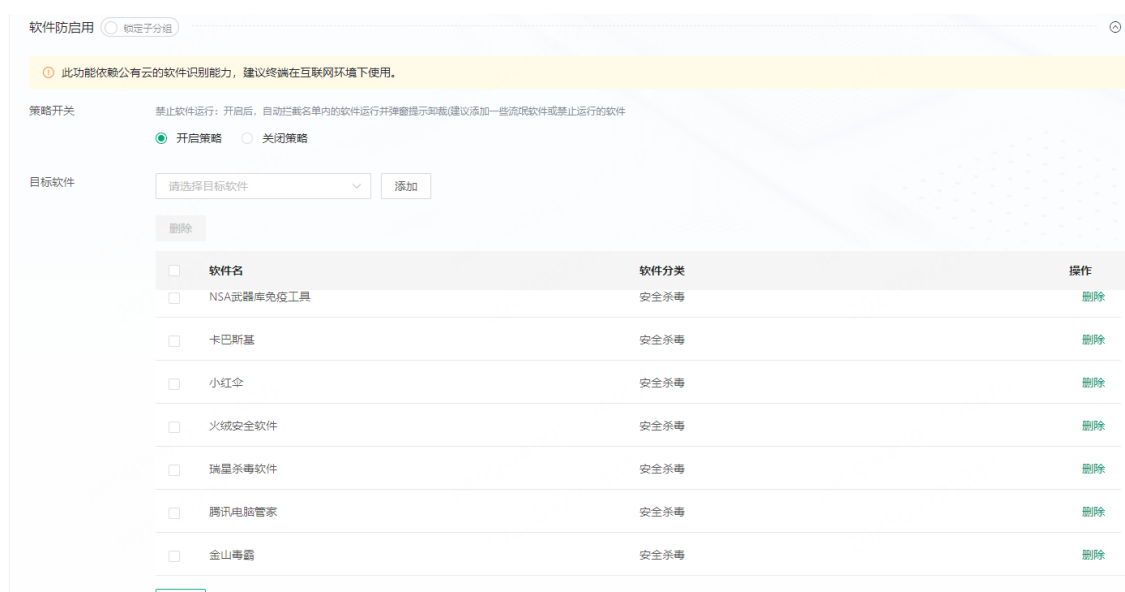
(8) 软件防安装：针对终端已经安装的软件进行管理，防止终端安装违规软件。支持以黑白名单的形式，设定违规范围。终端通过比对已安装软件的名称进行检查。



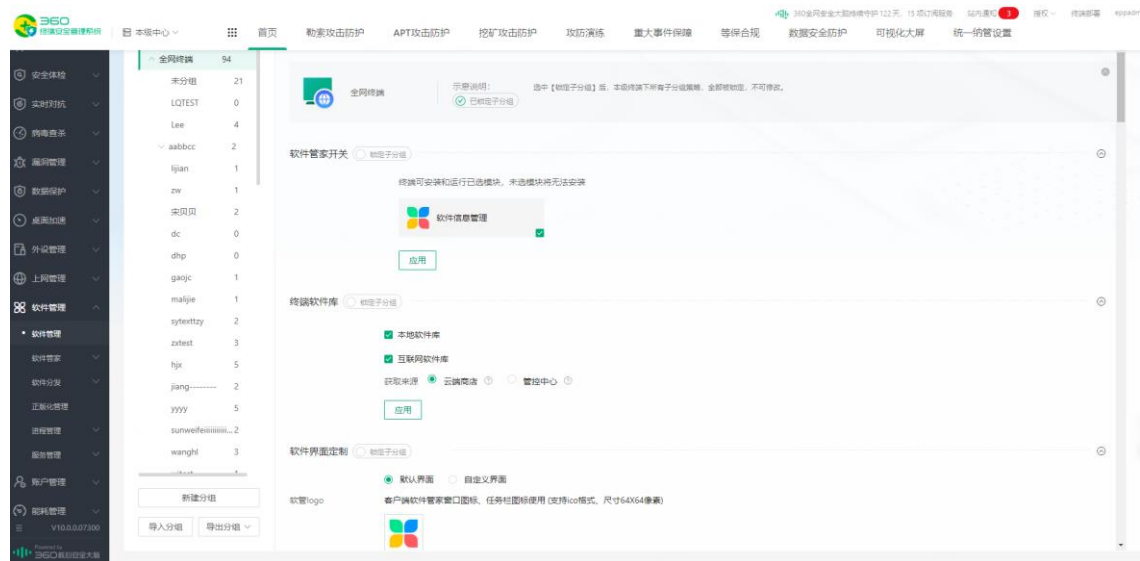
(9) 支持“仅允许终端使用当前账户权限卸载软件”和“允许终端使用 system 权限卸载软件”两种模式，管理员可按需配置分组终端软管客户端的卸载权限。

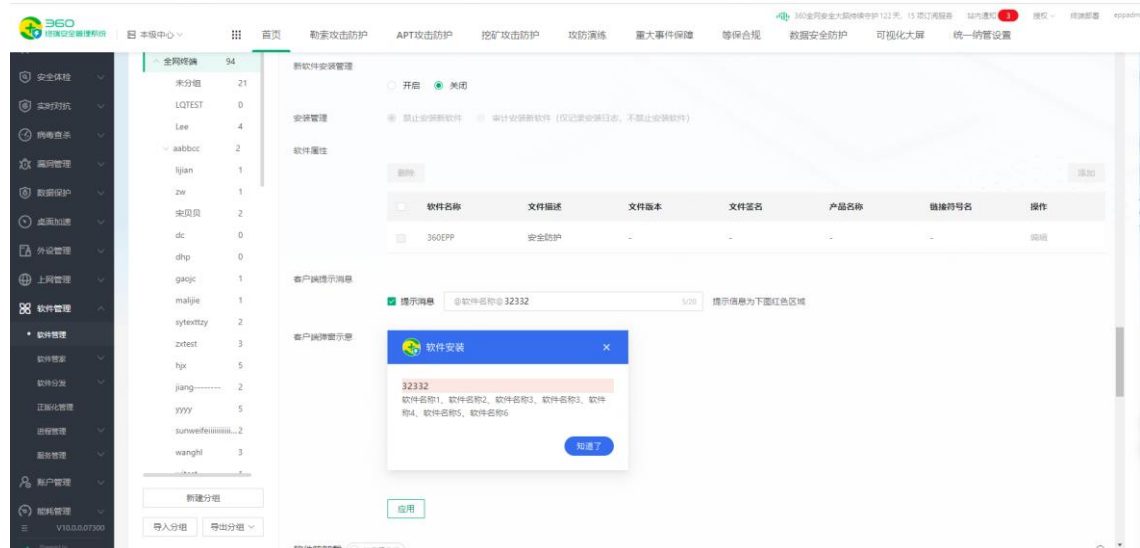


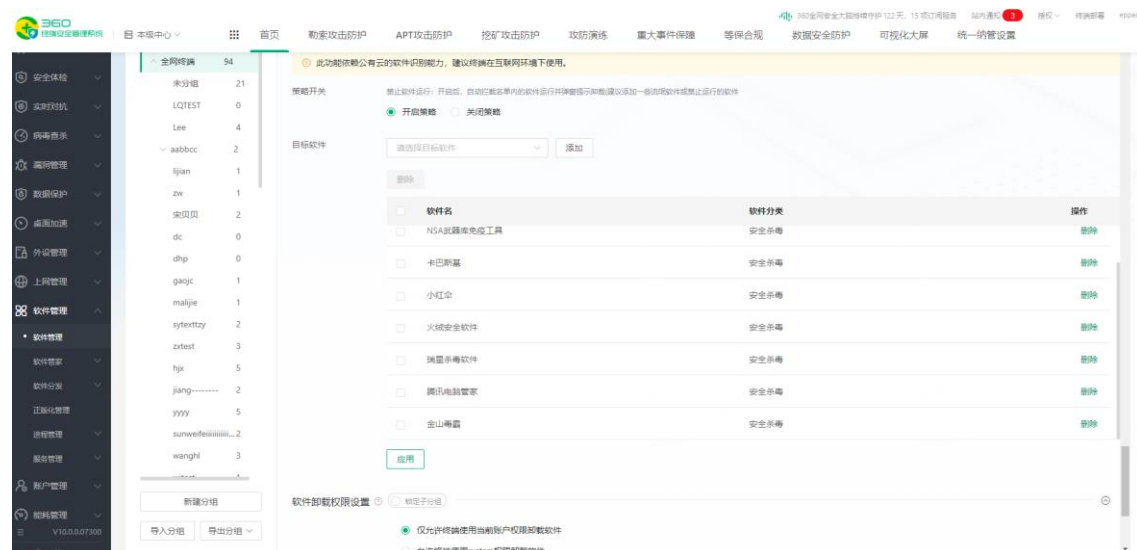
(10) 支持管理员将一些流氓软件或管理上需要禁止运行的软件加入黑名单中。开启策略后，系统会对名单内目标软件的运行进行拦截并提醒终端用户进行卸载。



点击左侧导航：软件管理>软件管理>软件管理策略(Windows/国产桌面机/国产服务器)，  
进入页面查看、配置。







## 11.3. 软件管家

### 11.3.1. 软件市场

#### 13.3.1.1 互联网软件库

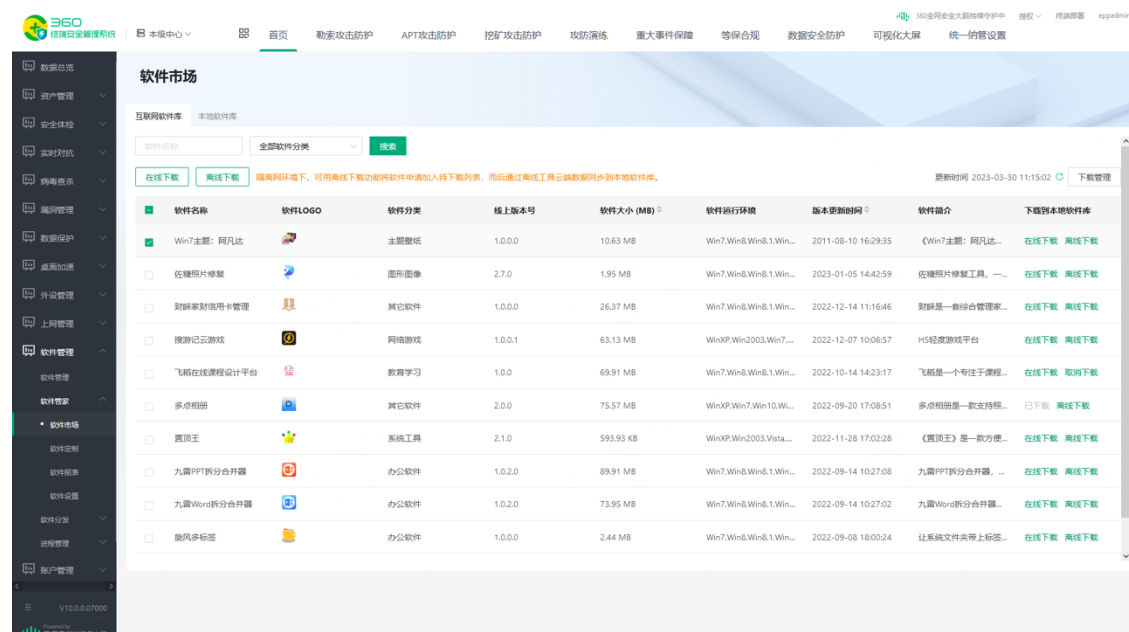
互联网软件库展示云端商店的软件列表，分类覆盖广泛，软件资源丰富。

- (1) 展示互联网软件库列表，包括软件名称、软件分类、版本德国，支持列表刷新；
- (2) 在线下载：可单个/批量下载互联网软件到本地软件库。
- (3) 离线下载：隔离网环境下，可用离线下载功能单个/批量将软件申请加入离线待下载

列表，而后通过离线工具下载云端数据并同步到本地软件库。

(4) 下载管理：在线下载的软件任务，可在下载管理列表中管理；

点击左侧导航：软件管理>软件管家>软件市场>互联网软件库 tab，进入页面查看、管理。



### 13.3.1.2 本地软件库

管理员可通过管控平台对本地软件库进行维护，包括：

(1) 支持创建本地软件列表，对软件进行创建、上架、管理和下架等；

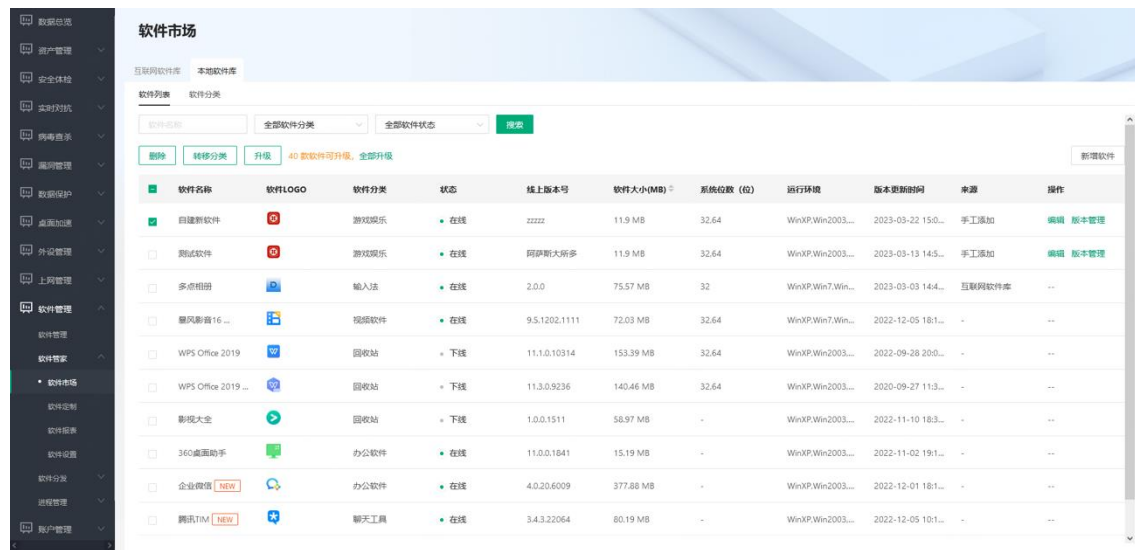
(2) 软件分类管理：支持创建软件分类和分类排序管理；

(3) 检查更新：针对有升级标记的软件，管理员可通过点击“升级”按钮连接云端商店下载更新新版软件，升级完成后去除新版标记。支持统计可升级软件个数，支持批量全部升级更新。

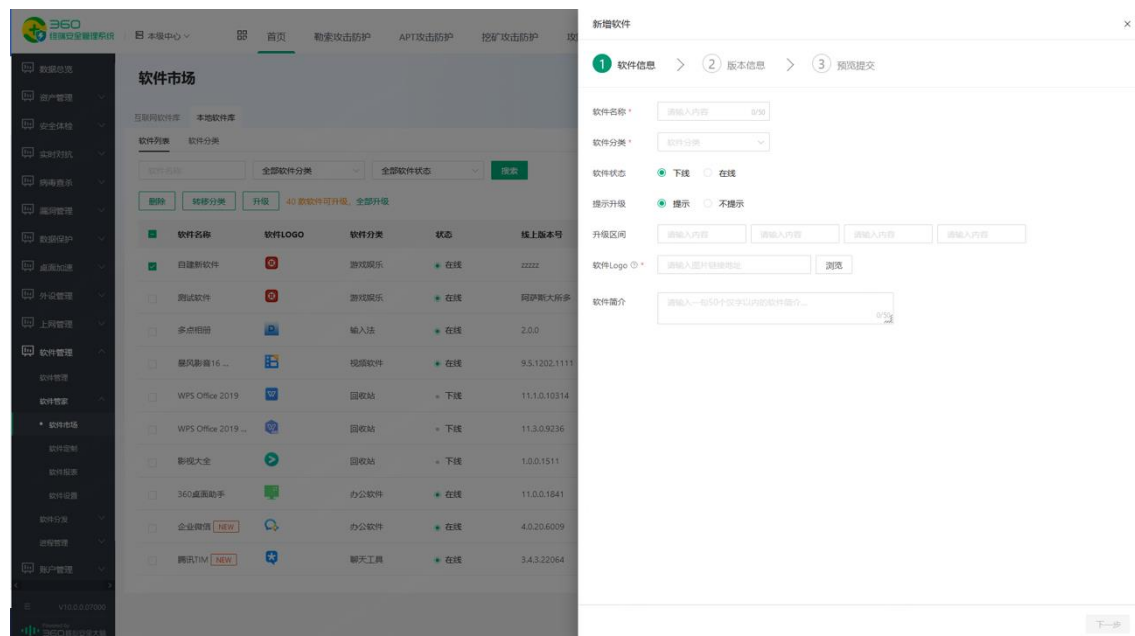
点击左侧导航：软件管理>软件管家>软件市场>互联网软件库 tab，进入页面查看、管理。

#### 6) 软件列表



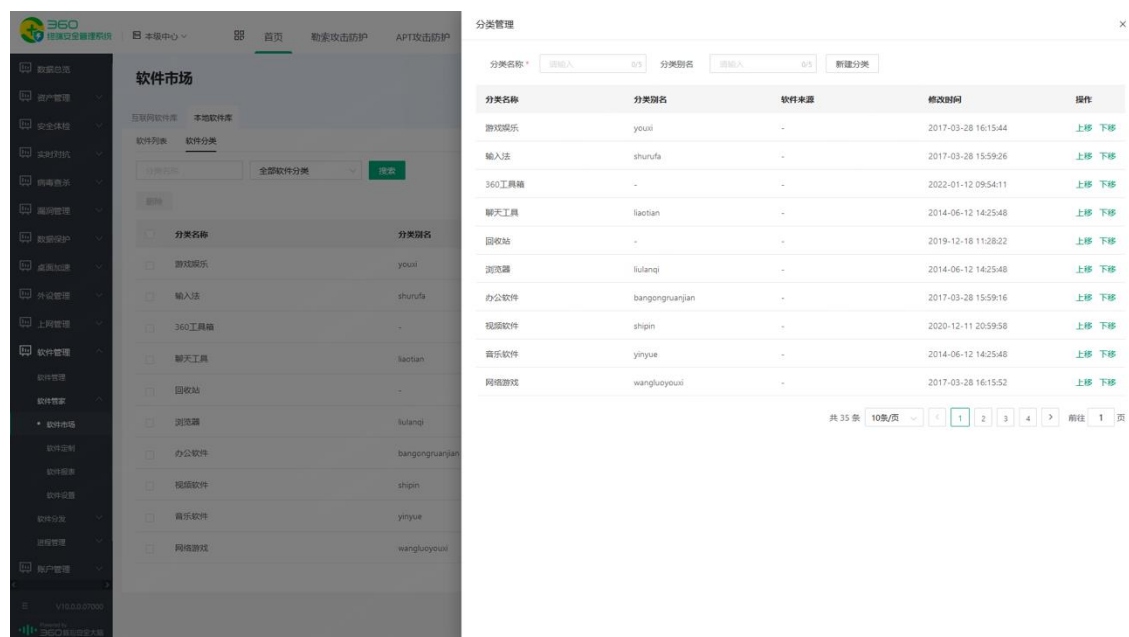


## 7) 软件上架



## 8) 分类管理





## 11.3.2. 软件定制

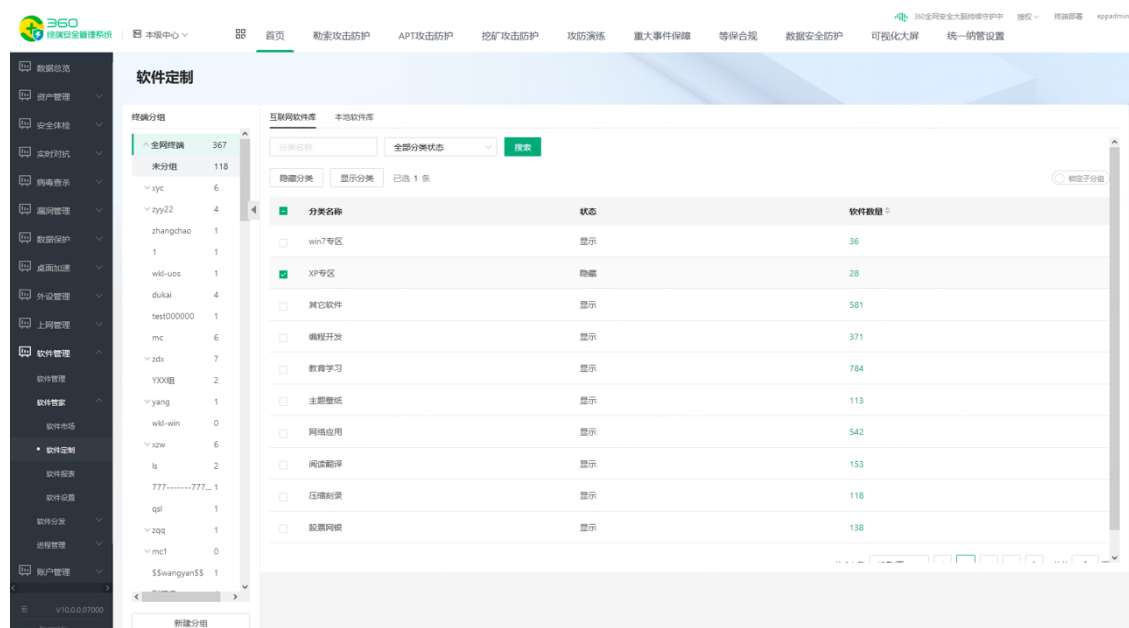
支持不同分组展示不同的软件列表，对终端软件展示权限进行定制，包括：

(1) 按分类定制：支持本地软件库、互联网软件库按软件分类进行隐藏/显示，保存后，所辖分组的终端相应软件分类在客户端隐藏/显示

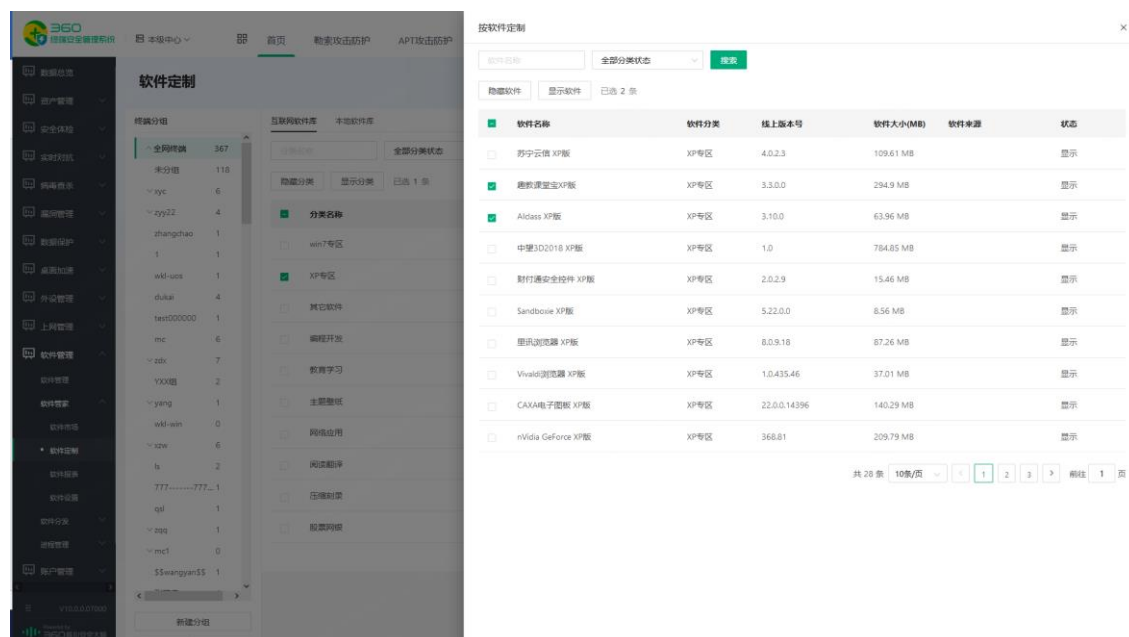
(2) 按软件定制：支持本地软件库、互联网软件库按软件进行隐藏/显示，保存后，所辖分组的终端相应软件在客户端隐藏/显示

点击左侧导航：软件管理>软件管家>软件定制，进入页面查看、管理。

### 9) 按分类定制



## 10) 按软件定制



## 11.3.3. 软件设置

- (1) 互联网软件库数据获取：互联网软件库列表可配置从上级中心或云端商店进行获取。
  - (2) 本地软件库数据获取：支持从上级同步本地软件库列表和相关安装文件。如果开启，则本地软件库数据既可来源于本级管控也可来源于上级管控，或两者共存。
  - (3) 软件存储统计：对所有软件占用存储空间和失效软件占用存储空间进行统计，每次刷新页面时候获取最新数据进行展示。
  - (4) 清理失效软件：支持直接删除失效软件的安装包文件，同时更新软件存储统计值。
- 点击左侧导航：软件管理>软件管家>软件设置，进入页面查看、管理。



## 11.3.4. 软管报表

支持对内网软件操作行为进行统计，如支持软件软件卸载、软件下载、软件安装、软件升级趋势统计。支持对安装软件 TOP5、软件卸载 TOP5、软件下载排行等进行统计。

(1) 软管操作日志：针对软件管家的操作行为进行记录，具体行为包括下载、安装、升级、卸载。

(2) 软管操作事件统计：统计周期范围内软管操作日志各操作类型的日志条数，绘制分类占比和操作趋势。

(3) 软件安装 top5 统计周期范围内安装次数最多的软件，取 top 展示，帮助管理员发现安装使用最多的是哪些软件。

(4) 软件卸载 top5 统计周期范围内卸载次数最多的软件，取 top 展示，帮助管理员发现卸载最多的是哪些软件。

(5) 下载次数最多的软件排行 统计周期范围内下载次数最多的软件，取 top 展示，帮助管理员发现下载最多的是哪些软件。

(6) 下载次数最多的软件分类排行 统计周期范围内下载次数最多的软件分类，取 top 展示，帮助管理员发现下载最多的是哪些软件分类。

(7) 软管下载量分布统计 统计周期范围内本地软件库和互联网软件库的下载量，比较其下载分布和趋势。

点击左侧导航：软件管理>软件管家>软管报表，进入页面查看、管理。

### 11) 软管操作日志

软管报表

统计范围：软件操作日志

终端分组：全部终端 367

未分组 118

zyx 6

zyy22 4

zhangchao 1

1 1

wkl-uos 1

dukai 4

test000000 1

mrc 6

zdx 7

VXXX组 2

yang 1

wkl-win 0

XZY 6

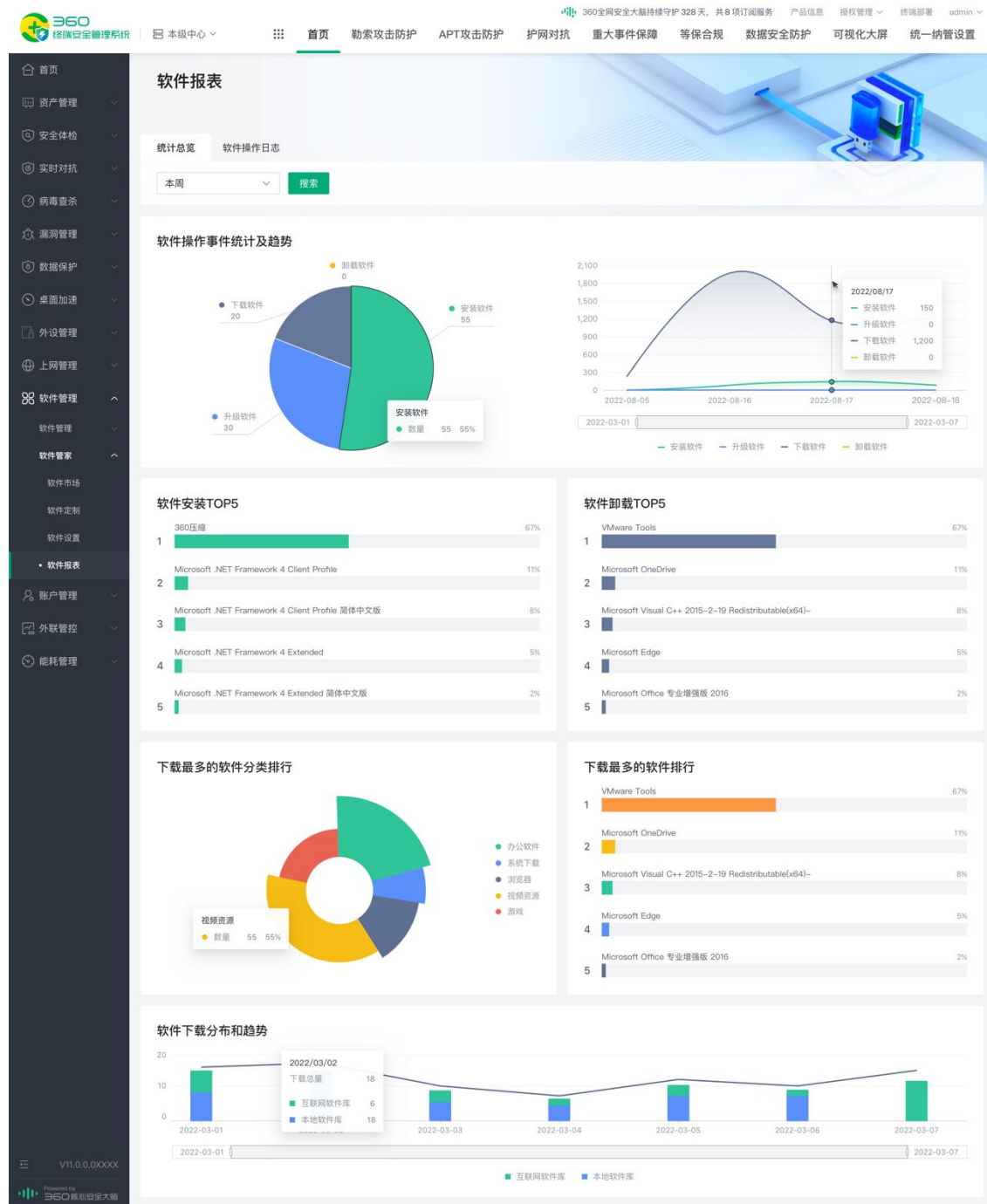
新建分组

导入分组 导出分组

操作时间	终端名称	IP地址	所属分组	操作类型	软件名称	软件分类	软件版本	软件大小(MB)	下载源
2023-03-28 19:06:42	Test	10.19.1.49	yyyyyy	下载	美图相机	图形图...	-	4.74 MB	互联网
2023-03-28 19:06:28	Test	10.19.1.49	yyyyyy	下载	美图秀秀批处理	图形图...	-	146.2 MB	互联网
2023-03-28 19:06:27	Test	10.19.1.49	yyyyyy	下载	光影魔术手	图形图...	-	11.01 MB	互联网
2023-03-28 19:06:18	Test	10.19.1.49	yyyyyy	下载	Adobe Photoshop	图形图...	-	2.05 MB	互联网
2023-03-28 19:06:02	Test	10.19.1.49	yyyyyy	下载	CAD迷你看图	图形图...	-	47.66 MB	互联网
2023-03-28 19:05:43	Test	10.19.1.49	yyyyyy	下载	糖果游戏浏览器	浏览器	-	8.03 MB	互联网
2023-03-28 19:05:43	Test	10.19.1.49	yyyyyy	下载	YandexBrowser	浏览器	-	141.44 MB	互联网
2023-03-28 19:05:42	Test	10.19.1.49	yyyyyy	下载	115电脑版	浏览器	-	109.91 MB	互联网
2023-03-28 19:05:40	Test	10.19.1.49	yyyyyy	下载	小K3浏览器	浏览器	-	82.89 MB	互联网
2023-03-28 19:05:39	Test	10.19.1.49	yyyyyy	下载	You123浏览器	浏览器	-	57.88 MB	互联网

共 25 条 10条/页 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

### 12) 软管报表



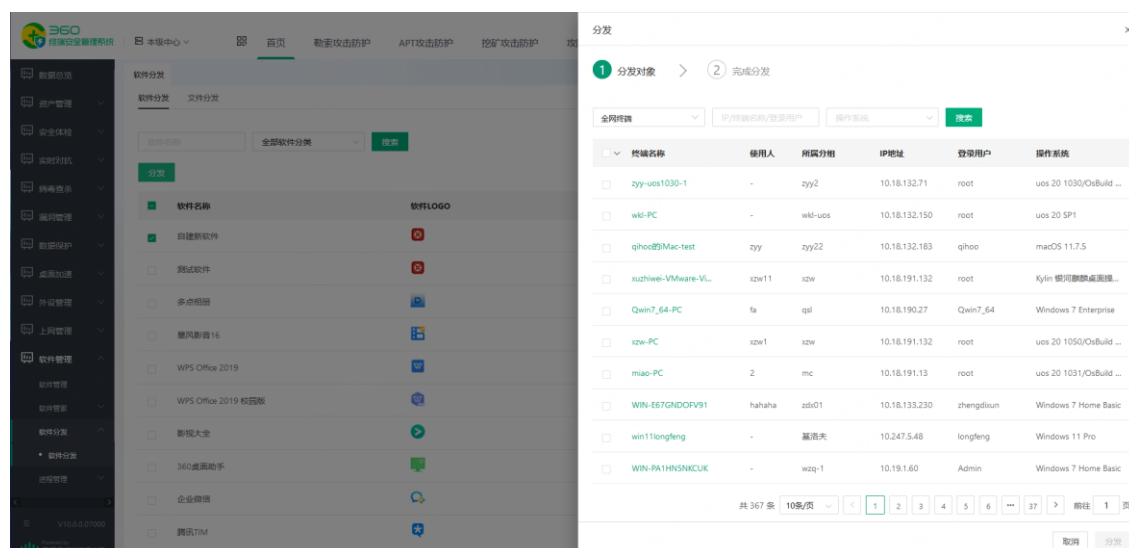
## 11.4. 分发管理

### 11.4.1. 软件分发

管理员可给客户端分发本地软件库的软件。支持按软件名称、软件分类模糊搜索，支持分发和分发管理。

点击左侧导航：**软件管理** > **软件分发** > **软件分发**，进入页面查看、管理。

#### 13) 软件分发



## 14) 分发管理



## 11.4.2.文件分发

(1) 管理员可向客户端分发文件。支持文件上传管理、文件分发等；

(2) 分发参数：可设置分发文件的存放位置、失败重发、运行权限、分发条件，可配置软件运行参数。

### ● 运行权限设置

管理员在分发设置时，可配置运行时是否提权。提供当前登录用户权限和 **system** 权限两种运行权限设置项，默认为当前登录用户权限。---此配置项仅针对 **win/winservice** 平台生效，国产桌面机和国产服务器平台还是同旧逻辑一致，默认使用 **root** 权限安装，不支持指定当前用户权限安装。

### ● 分发条件设置

管理员可配置分发条件规则，在分发时根据配置的逻辑规则判断终端是否可被分发。客户端收到文件分发指令后，判断是否满足分发条件（如有）。对于满足分发条件的终端，根据

执行方式配置，进行文件下载（接收）；不满足分发条件的终端，不执行文件分发指令，同时上报信息至分发管理“不支持终端”中。分发条件具体包括：

A. 终端已安装了软件名 XXX 的软件：检查该终端软件资产列表中，是否命中管理员所填的“软件名称”，若命中，则满足此条件；

B. 终端 XXX 进程正在运行：检查该终端正在运行的进程列表中，是否命中管理员所填的“进程名称”，若命中，则满足此条件；

C. 终端 IP 在 XXX 范围内：检查该终端的内网 IP 地址，是否在管理员所填的“IP 段”内，若在段内，则满足此条件；

D. 文件/注册表检查：管理员可根据实际所需，配置文件路径、大小、版本号或注册表项、值等检测内容，对终端文件/注册表进行检查，以此来判断是否满足条件。

（3）文件签名：对要分发的文件进行签名，避免被恶意利用。

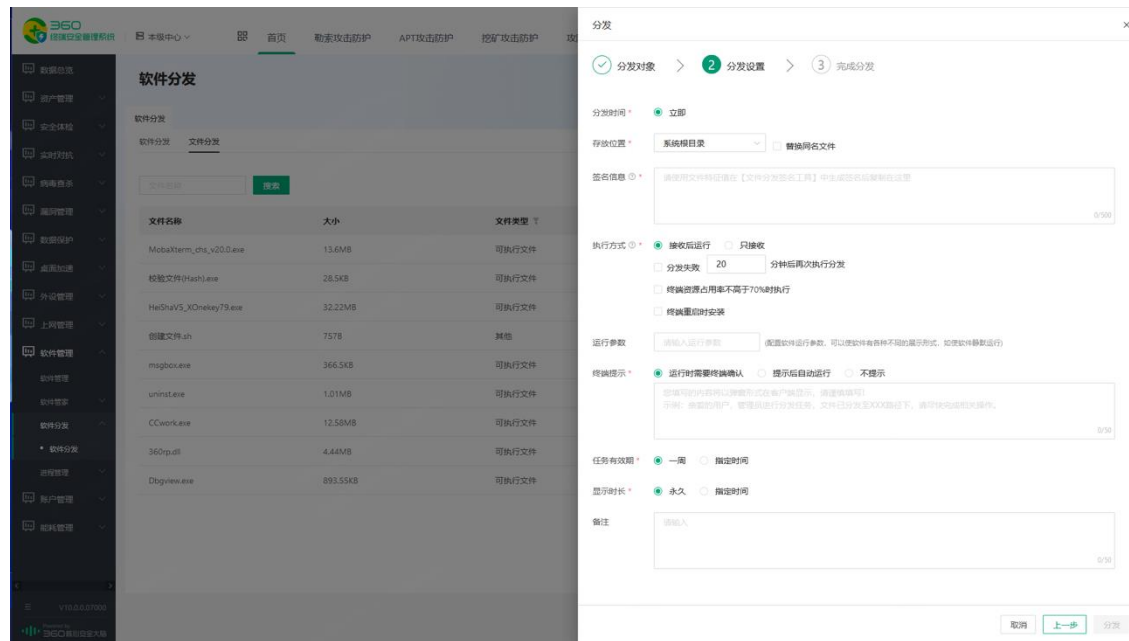
（4）分发管理：管理已分发的任务，查看相关进度

点击左侧导航：软件管理>软件分发>文件分发，进入页面查看、管理。

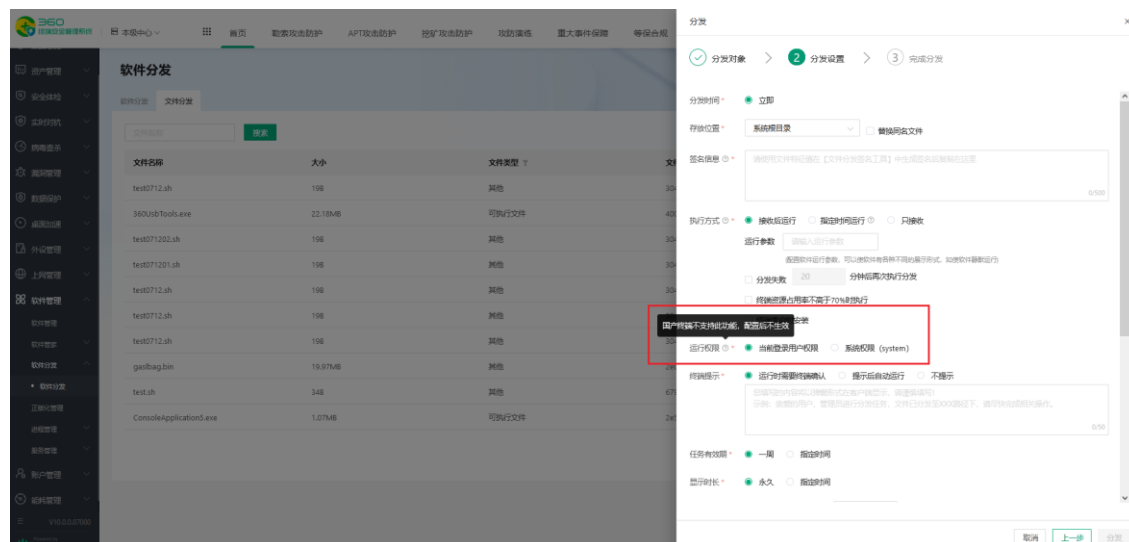
## ● 文件管理

文件名称	大小	文件类型	文件特征值	创建日期	操作
MobaXterm_cli_v20.0.exe	13.6MB	可执行文件	626fd2e6cc7e6caa1db048886f11b08...	2023-03-22 10:54:49	分发 删除
校验文件(hash).exe	28.5KB	可执行文件	e572fa067f5e48773c9f76acafa42536c...	2023-03-22 10:54:24	分发 删除
HeShuVS_XOnekey79.exe	32.22MB	可执行文件	4edea9d2a5336ad1633974d666b78b2...	2023-03-22 10:02:01	分发 删除
创建文件.sh	757B	脚本	8d7a59dc0a4e85b5884a174a798a8b...	2023-03-21 15:44:11	分发 删除
msgbox.exe	366.5KB	可执行文件	818614cc9a846a301b65699c5051e67c...	2023-03-20 17:12:00	分发 删除
uninst.exe	1.01MB	可执行文件	5c8c00310464d4fe41a4ac97334f1ab7...	2023-03-09 10:23:16	分发 删除
CCwork.exe	12.58MB	可执行文件	17c52cc37860a8b0c490ad0f1b064c4...	2023-03-09 10:23:03	分发 删除
360p.dll	4.44MB	可执行文件	3940b6321077349dc1750bd80a35d5...	2023-02-28 10:45:40	分发 删除
Dbgview.exe	893.55KB	可执行文件	c3a06eba04e67cc244bfc97689316d0c...	2023-02-23 10:27:51	分发 删除

## ● 文件分发

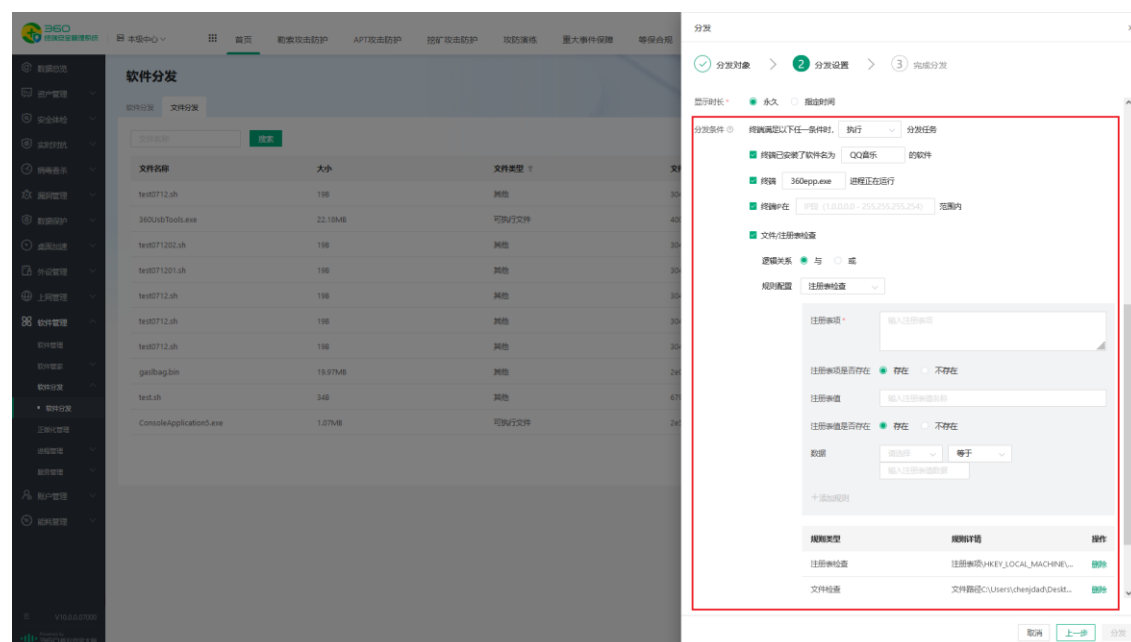


## ● 运行权限配置

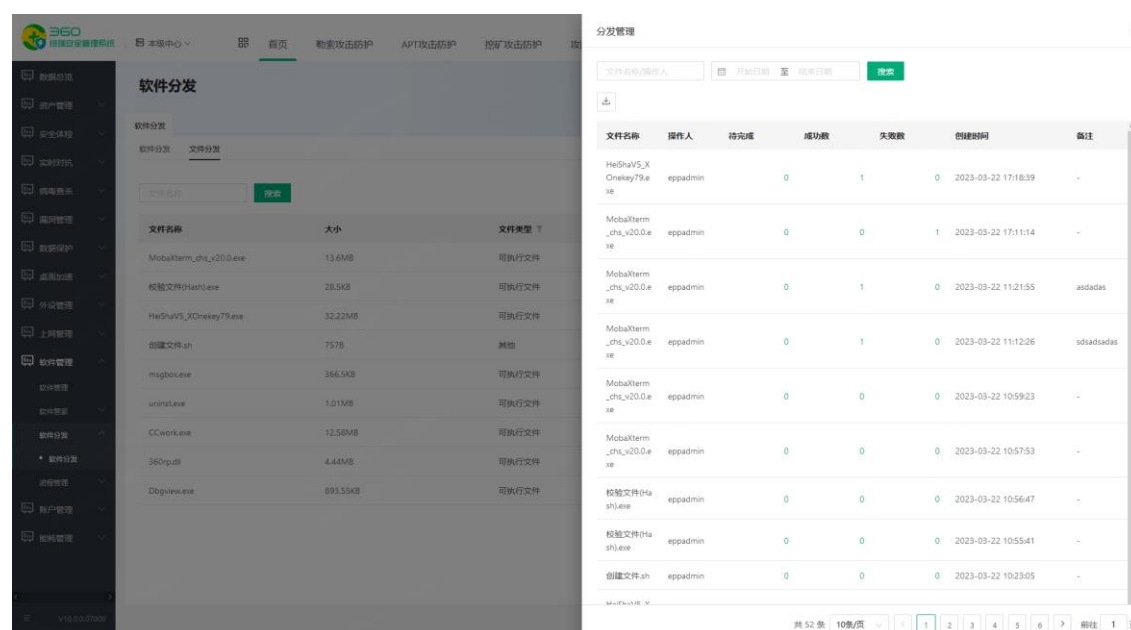


## ● 分发条件判断





## ● 分发管理



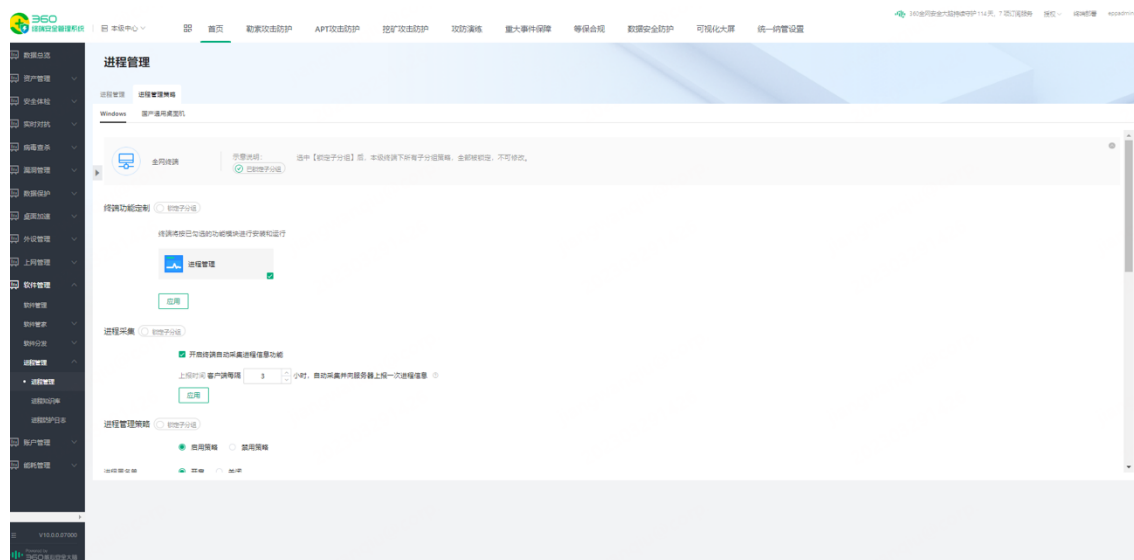
## 11.5. 进程管理

管控中心可配置终端进程管理策略。包括进程黑名单、进程红名单。

步骤一：设置进程策略

- 1、登录控制台，在左侧导航栏，选择软件管理>进程管理>进程管理策略；
- 2、在策略管理面板，按需求配置进程管理策略





其中：

### 3、Windows 策略：

- 1) 进程采集时间配置：配置自动采集时间，终端自动采集并向服务器上报告一次进程信息。
- 2) 进程黑名单：包含监控模式、防护模式。



若选择监控模式：当终端发现违规进程启动时，将记录一条监控日志，上报至管控中心；  
若选择防护模式：当终端发现违规进程启动时，将主动拦截并记录一条拦截日志，上报至管控中心。

黑名单匹配规则设置：若勾选配置后，终端将按照所选进程中对应的属性信息，进行黑名单监控/拦截。

黑名单匹配规则 ☒ 启动路径 ☒ MD5 ☐ SHA1 ☐ 产品名称 ☐ 公司名称 ☐ 进程名称

黑名单匹配条件设置：满足以上所选任意条件、满足以上所选全部条件

匹配条件 ☐ 满足以上所选任意条件 ☒ 满足以上所选全部条件

若此处配置为“满足以上所选任意条件”，则终端匹配进程时，将按照黑名单匹配规则设置的内容，命中一个规则，即执行监控/拦截动作；

若此处配置为“满足以上所选的全部条件”，则终端匹配进程时，将按照黑名单匹配规则设置的内容，命中全部所选规则，即执行监控/拦截动作。

- 3) 进程红名单：包括必须启动进程、进程保护。



当配置为进程保护，则当终端发现进程被恶意结束，将进行阻止。

当配置为必须启动进程，则当终端发现进程未运行时，将按照进程启动路径，自动完成进程的启动；

启动验证 ☐ 启动进程前验证MD5 <sup>①</sup>

为提升终端安全，必须启动的进程可配置是否要校验 MD5，若验证失败，将不启动进程。

同时，可配置进程保护匹配规则和条件：

进程保护匹配规则 <sup>①</sup> ☐ 启动路径 ☒ MD5 ☐ SHA1 ☐ 产品名称 ☐ 公司名称 ☐ 进程名称

匹配条件 ☐ 满足以上所选的任意条件 ☒ 满足以上所选的全部条件 <sup>②</sup>

若配置为“满足以上所选的任意条件”，则当终端发现与进程保护列表内任意一个规则属性相同的进程，则将执行进程保护，阻止该进程被结束。

若配置为“满足以上所选的全部条件”，则当终端发现与进程保护列表内全部规则属性相同的进程，则将执行进程保护，阻止该进程被结束。

支持配置进程保护时，终端的提示信息：



2) 进程灰名单：可记录重要进程启动和关闭的状态变化。



4、Linux/国产服务器策略：

1) 进程采集时间配置：配置自动采集时间，终端自动采集并向服务器上报告一次进程信息。

## 2) 进程黑名单：包含监控模式、防护模式。

若选择监控模式：当终端发现违规进程启动时，将记录一条监控日志，上报至管控中心；

若选择防护模式：当终端发现违规进程启动时，将主动拦截并记录一条拦截日志，上报至管控中心。

同时，支持选择黑名单进程，并根据所选进程的启动路径进程黑名单匹配。

## 2、国产桌面机

1) 进程采集时间配置：配置自动采集时间，终端自动采集并向服务器上报告一次进程信息。

2) 进程黑名单：包含监控模式、防护模式。

若选择监控模式：当终端发现违规进程启动时，将记录一条监控日志，上报至管控中心；

若选择防护模式：当终端发现违规进程启动时，将主动拦截并记录一条拦截日志，上报至管控中心。

支持配置触发黑名单规则时，终端的提示信息：

3) 进程红名单：包括必须启动进程、进程保护。

当配置为进程保护，则当终端发现进程被恶意结束，将进行阻止。

支持配置进程保护时，终端的提示信息：

4) 进程灰名单：可记录重要进程启动和关闭的状态变化。

## 进程灰名单

进程灰名单

☒ 开启 ☐ 关闭

灰名单列表

<input type="checkbox"/>	进程名称	MD5	启动路径
<input type="checkbox"/>	assetd	FFD8F2FEEDB00F9...	/opt/nesys/bfmap...

## 步骤二：进程防护日志查看

登录控制台，在左侧导航栏，选择软件管理>进程管理>进程防护日志

进程防护日志

上月 进程名称 已删除 生成

结束时间	进程名称	IP地址	进程路径	控制方式	事件类型	结果	详情
2023-02-22 17:56:56	explorer.exe	192.168.1.102	C:\Users\Administrator\Desktop\explorer.exe	禁止启动	控制进程	成功	C:\Windows\explorer.exe尝试启动...
2023-02-22 17:56:41	explorer.exe	192.168.1.102	C:\Users\Administrator\Desktop\explorer.exe	禁止启动	控制进程	成功	C:\Windows\explorer.exe尝试启动...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Program Files (x86)\360\SafeRiskControl\...	禁止启动	控制进程	成功	C:\Program Files (x86)\360\SafeRisk...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Program Files (x86)\360\SafeRiskControl\...	禁止启动	控制进程	成功	C:\Program Files (x86)\360\SafeRisk...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Windows\System32\cmd.exe	禁止启动	控制进程	成功	C:\Windows\System32\cmd.exe...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Windows\System32\cmd.exe	禁止启动	控制进程	成功	C:\Windows\System32\cmd.exe...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Windows\System32\cmd.exe	禁止启动	控制进程	成功	C:\Windows\System32\cmd.exe...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Windows\System32\cmd.exe	禁止启动	控制进程	成功	C:\Windows\System32\cmd.exe...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Windows\System32\cmd.exe	禁止启动	控制进程	成功	C:\Windows\System32\cmd.exe...
2023-02-22 17:48:21	System Idle Process	192.168.1.102	C:\Windows\System32\cmd.exe	禁止启动	控制进程	成功	C:\Windows\System32\cmd.exe...

共 34 条 10条/页 1 2 3 4 5 6 7 8 9 10 页

## 步骤三：终端进程管理查看

登录控制台，在左侧导航栏，选择软件管理>进程管理>终端进程管理

终端进程管理

进程名称 进程管理 生成

进程名称 (仅支持Windows/Linux平台) (已安装终端管理客户端) (仅支持Linux平台) (已安装终端管理客户端)

进程名称	状态	使用人	所属分组	IP地址	用户名
explorer.exe	运行	-	explorer	192.168.1.102	root
System Idle Process	运行	-	System Idle Process	192.168.1.102	Test
System Idle Process	运行	root	explorer	192.168.1.102	root
System Idle Process	运行	root	explorer	192.168.1.102	root
System Idle Process	运行	-	wanghang	192.168.1.102	wanghang
System Idle Process	运行	root	System Idle Process	192.168.1.102	root
System Idle Process	运行	chenxi	chenxi	192.168.1.102	root
System Idle Process	运行	-	System Idle Process	192.168.1.102	Administrator
System Idle Process	运行	-	System Idle Process	192.168.1.102	system
System Idle Process	运行	-	System Idle Process	192.168.1.102	system