

360 企业安全云 产品操作手册

2022.3

【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。

版本信息

文档名称	更改内容	文档版本	密级	创建日期
360 安全卫士团队版使用手册	官网大幅度改版	V3.0	公开	2020/11/03
360 安全卫士团队版使用手册	官网大幅度改版	V4.0	公开	2020/12/18
360 安全卫士团队版帮助手册	部分样式更新	V4.1	公开	2021/02/02
360 安全卫士团队版帮助说明	新增部分功能	V4.2	公开	2021/03/17
360 安全卫士团队版使用手册	新增部分功能及问题修复	V4.3	公开	2021/05/10
360 安全卫士团队版产品操作手册	新增部分功能及问题修复	V4.5	公开	2021/07/09
360 安全卫士团队版产品操作手册	新增部分功能及问题修复	V4.6	公开	2021/10/20
360 安全卫士团队版产品操作手册	新增部分功能及问题修复	V4.7	公开	2021/12/31
360 企业安全云产品操作手册	全面升级改版	V5.0	公开	2022/03

目录

1、安装部署指南	7
1.1 客户端配置环境要求	7
1.2 企业注册	7
1.3 客户端部署	9
1.3.1 windows 系统提供五种部署方式	9
1.3.2 Linux 系统部署	20
1.3.3 macOS 系统部署	22
1.4 退出企业	26
2、管理后台功能简介	27
2.1 总览	27
2.2 终端	27
2.2.1 终端部署	27
2.2.2 终端管理	28
2.2.3 终端状态	31
2.2.3.1 运行状态	31
2.2.3.2 安全状态	32
2.2.3.3 版本状态	33
2.2.4 终端定制	33
2.2.5 外设管理	35
2.2.6 设备安全	37
2.2.6.1 安全体检	37

2.2.6.2 木马查杀.....	37
2.2.6.3 杀毒管理.....	37
2.2.6.4 漏洞修复.....	38
2.2.6.5 系统修复.....	38
2.6.6 分组策略（部分专业安全管理运维服务）	39
2.3 资产	57
2.3.1 资产管理	57
2.4 软件	57
2.4.1 软件管理	57
2.4.2 软件分发	59
2.4.3 文件分发（专业安全管理运维服务）	60
2.4.4 软件优化	60
2.4.4.1 弹窗过滤（专业安全管理运维服务）	60
2.4.4.2 启动项优化	61
2.5 上网	62
2.5.1 上网限制	62
2.6 数据	63
2.6.1 屏幕水印（专业安全管理运维服务）	63
2.6.2 安全设置（专业安全管理运维服务）	64
2.7 防勒索	64
2.7.1 勒索防护（专业安全管理运维服务）	64
2.7.2 安全基线（专业安全管理运维服务）	65

2.8 服务	66
2.9 页眉功能导航.....	67
2.9.1 关键字搜索.....	67
2.9.2 设置	67
2.9.2.1 团队管理.....	67
2.9.2.2 全局设置.....	68
2.9.2.3 身份认证.....	70
2.9.3 站内信	70
2.9.3.1 站内消息.....	70
2.9.3.2 历史推送.....	71
2.9.4 工单系统.....	71
2.9.4.1 提交工单.....	71
2.9.4.2 历史工单.....	72
2.9.5 账号设置	73
2.9.5.1 积分中心.....	73
2.9.5.2 切换团队.....	73
2.9.5.3 账号中心.....	74
2.9.5.4 退出登录.....	75
3、客户端主要功能简介.....	76
3.1 首页体检.....	76
3.2 木马查杀.....	77
3.3 系统安全.....	78

3.4 网络安全.....	79
3.5 数据安全.....	80
3.6 优化加速.....	81
3.7 安全大脑.....	81
3.8 软件管家.....	82
4、客户端退出、卸载.....	84
4.1 退出	84
4.2 卸载	85

1、安装部署指南

1.1 客户端配置环境要求

类型	操作系统	CPU	内存	硬盘	备注
Windows 终端	Windows XP	双核 2.0GHZ	1G	>20G	最低配置
	Windows Vista				
	Windows 7				
	Windows 8				
	Windows 10				
	Windows 11				

1.2 企业注册

通过官方网址 <https://ent.online.360.cn/> 管理员可以为企业注册账号，注册非常简单，只需要填写注册手机号、验证码和设置密码即可。

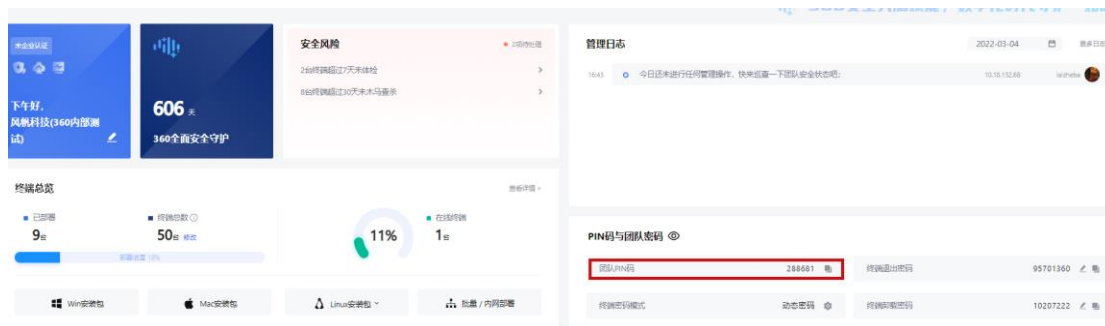


注册成功, 补充填写企业的真实信息后, 就可以进入管理后台了。



登录管理后台会有企业专属的 PIN 码, 这是客户端 (员工) 将本地的 360 安全卫士连接到

企业组网的识别编码，每个企业都有唯一的 PIN 码。



1.3 客户端部署

1.3.1 windows 系统提供五种部署方式

方式一，未安装个人版 360 安全卫士，管理员登录管理后台后直接下载企业专属安装包分发给企业成员进行安装；即可自动加入企业组织完成部署。



方式二，已安装个人版 360 安全卫士的成员，可与 360 企业安全云客户端无缝转换，只需要通过安全卫士界面右上角设置菜单中的“加入团队”选项，输入正确的 PIN 码即可自动升级为 360 企业安全云客户端并加入相应企业组织。



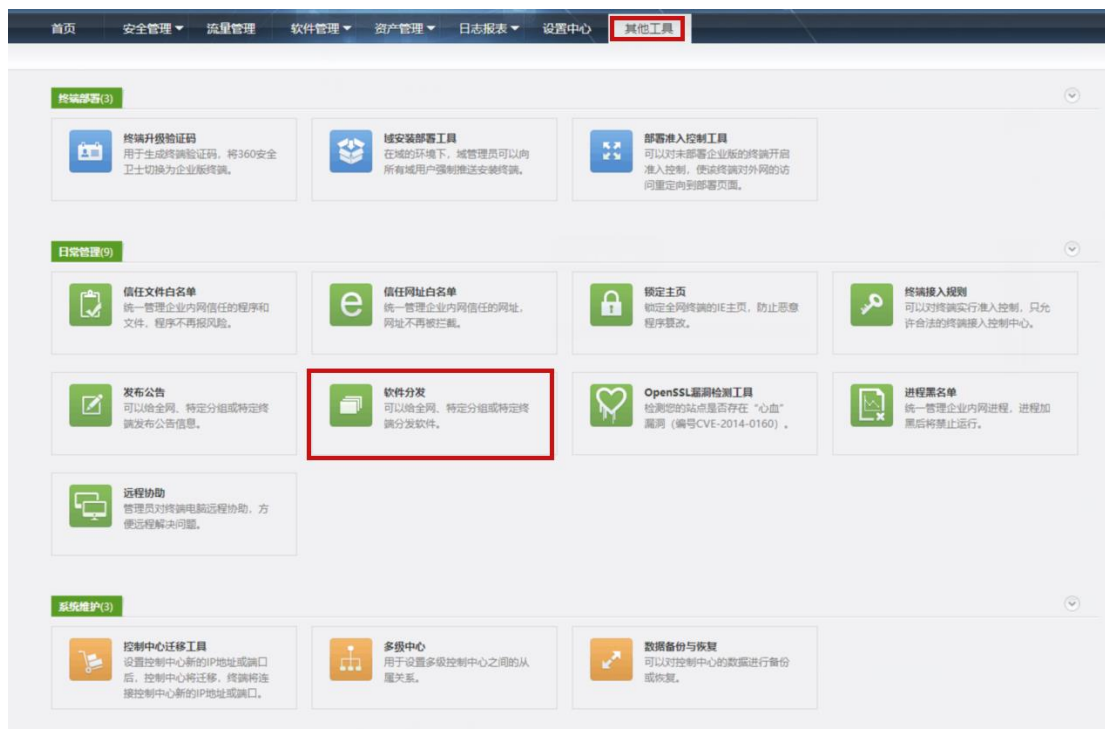
加入企业组织后，可在客户端输入或修改终端登记信息，用于标识设备的归属人。



方式三：已部署 360 网管版的终端，可通过网管版控制中心推送 360 企业安全云的新版安装包，请先从管理后台 --> 【终端】--> 【终端部署】--> 【外网场景部署】下载需要的安装包，如下图：



然后打开 360 网管版控制中心--> 【其他工具】--> 【软件分发】浏览上传下载的 360 企业安全云安装包，选择弹窗告知接收，接收后运行，完成批量版本切换。



请先选择要上传的软件或文件

[查看发布记录](#)

浏览

上传

(建议不要超过200M, 最大不超过 1G)

360[000510].exe (11.8MB) [删除](#)
上传成功。

终端提醒方式：☐ 弹窗询问接收 ☒ 弹窗告知接收（终端无法拒绝）

终端执行方式：☐ 只接收 ☒ 接收后运行

软件存放位置：

360根目录

软件运行参数：

/S

（可不输入）

软件备注：

安全卫士团队版更新

（还可输入22个字符，可不输入）

有效期至：

2020-08-08

（超过有效期，终端将不再执行分发指令）

方式四：代理终端部署，对于有防火墙或代理出口方式控制互联网访问的企业，360 企业安全云提供了简单便捷的部署方法：

首先确保内网终端和联网终端可以连接，联网终端可以按需连接互联网，然后在管理后台的

【终端】→【终端部署】→【内网场景部署】页面，下方【内网代理安装包定制】输入代理 IP 和端口，点击【生成安装包】按钮

终端安全

终端部署

终端管理

终端状态

终端定制

外设管理

设备安全

分组策略

外网场景部署

内网场景部署

从360网管版迁移

准入规则

针对内网设备，可以参考以下部署方式（暂不支持私有化部署）

将卫士域名加白放行

如果您的网络出口支持针对特定域名加白放行，可以将卫士域名添加到您的网络出口白名单中。之后按照外网场景部署即可。
请确保放行这些域名/IP的 80 和 443 端口，否则可能影响使用

复制域名

查看域名/IP列表

使用代理方式联网

在本页「内网代理安装包定制」中设置代理服务端的IP和端口，并获取安装包。

查看指引

完全隔离网环境部署

360企业安全云 是 SAAS 化的线上服务，并不支持完全隔离的网络环境
如果您的企业需要纯隔离网环境的安全防护系统，可以了解我们的另一款产品 360终端安全管理系统

如果您的团队通过代理服务端联网，可以在此处进行代理服务器设置。

需要满足以下条件：
1. 代理服务端能够访问网络；
2. 保持安装包原文件名，将其安装在代理机与每个内网终端上。

内网代理安装包定制

代理服务端地址 IP地址 192.168.28.131 端口号 80

生成安装包

即可下载代理专用安装包。

准入规则

去配置

规则名称	自动分组	备注信息	授权期限	操作
无授权码终端	未分组	使用团队版客户端的登记信息	不限时间	启用

代理部署

启用代理部署

代理机IP-端口: 192.168.28.131 : 80

支持的安装包

Windows

linux

macOS

该安装包既用于代理服务端，也用于代理终端的安装，注意：该 IP 是联网机器的本机 IP，如果内网终端访问该机器 IP 是经过映射的，部署内网终端时需要更改一下安装包文件名对应的 IP 和端口，例如：服务端安装包文件名是 T1nGtrFf[192.168.28.131-80].exe，其内网映射 IP 是 192.168.86.144，那客户端安装包就改成 T1nGtrFf [192.168.86.144-80]Update.exe 后再执行安装。

代理服务端安装后只提供 360 安全卫士功能相关的域名和 IP 代理，如病毒库升级、补丁包

下载等，不可用户其他网站访问。（注意：请勿修改此安装包的文件名，以免安装部署失败）

目前 360 企业安全云暂不支持第三方代理软件，如果代理出口 IP 有变化，请下载新安装包覆盖安装，或者手动修改代理地址。

客户端代理设置入口：鼠标右键点击电脑任务栏 360 安全卫士图标，选择【升级-360 下载管理】页面右上角的设置即可打开设置。



如果代理服务端测试未成功，请检查网络防火墙设置，确保放行下列域名和 IP 的 80、443

端口：请访问管理后台→终端→终端部署→内网场景部署→复制域名。



方式五：域控方式部署

➤ 管理员通过管理后台获取域控安装包



- 将安装包放入共享目录下，并记录当前路径（格式一般为`\\IP 地址\目录名`）（请务必测试目标机器确实可以直接访问此共享文件夹）
- 创建脚本，新建一个文本文件，修改文件名及后缀名为 `start.bat`（文件名可自定义，后缀名必须为 `.bat`），`start.bat` 内的文本内容分两种情况：

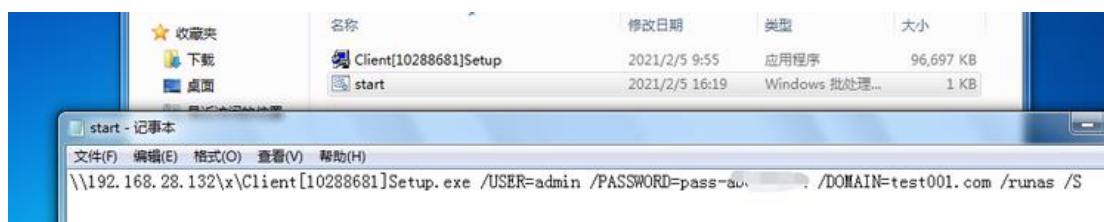
(1) 目标机器有管理员权限，直接/S 参数运行 exe 即可，示例：

`\\192.168.28.132\x\Setup[T0HLWK].exe /S`

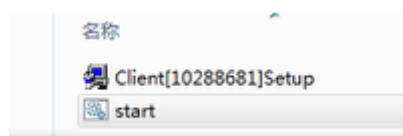
(2) 目标机器无管理员权限，需要在域控服务器里创建管理器权限的账户，并以命令行方式将账号密码传入安装包（部署完毕后可以删除此临时提权用的账号），

示 例 :\\192.168.28.132\\x\\Setup[T0HLWK].exe /USER=admin
/PASSWORD=pass-** /DOMAIN=test001.com /runas /S

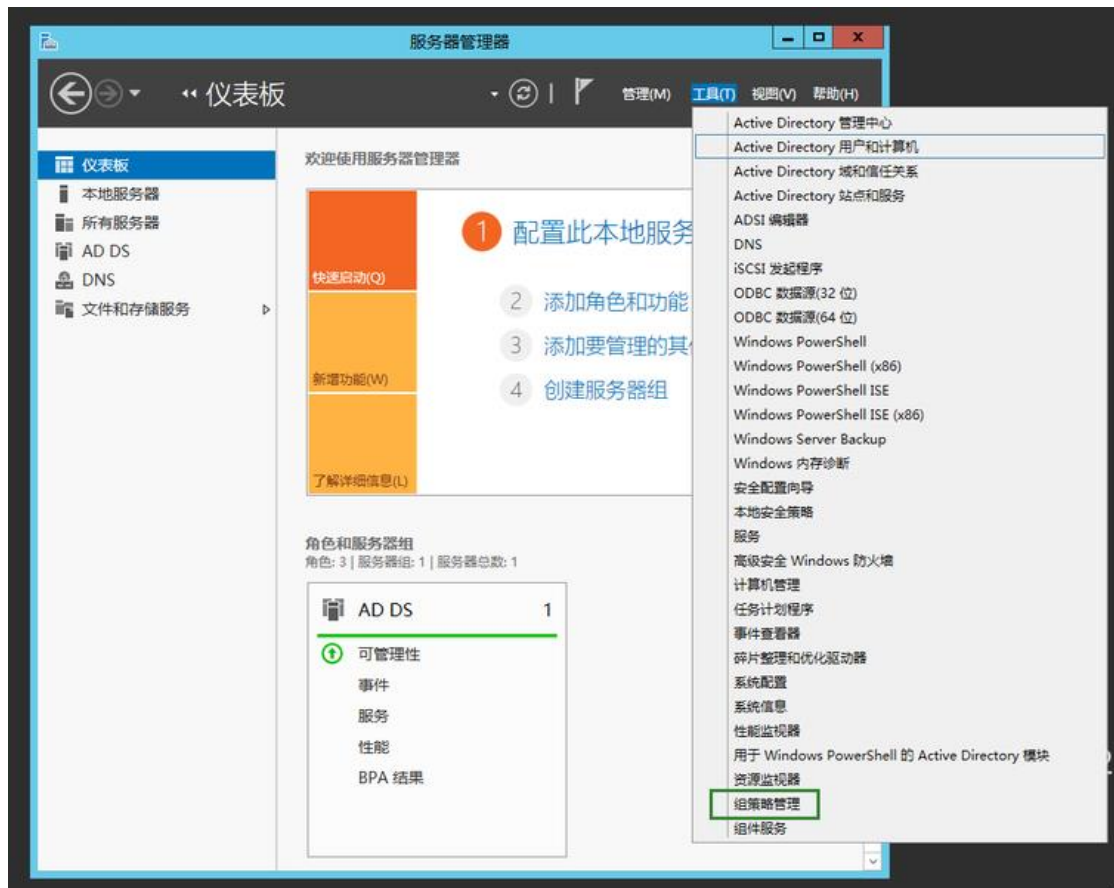
【说明：admin 请使用您创建的账号替换，pass-**请使用您设置的密码替换，
test001.com 替换为您的域】



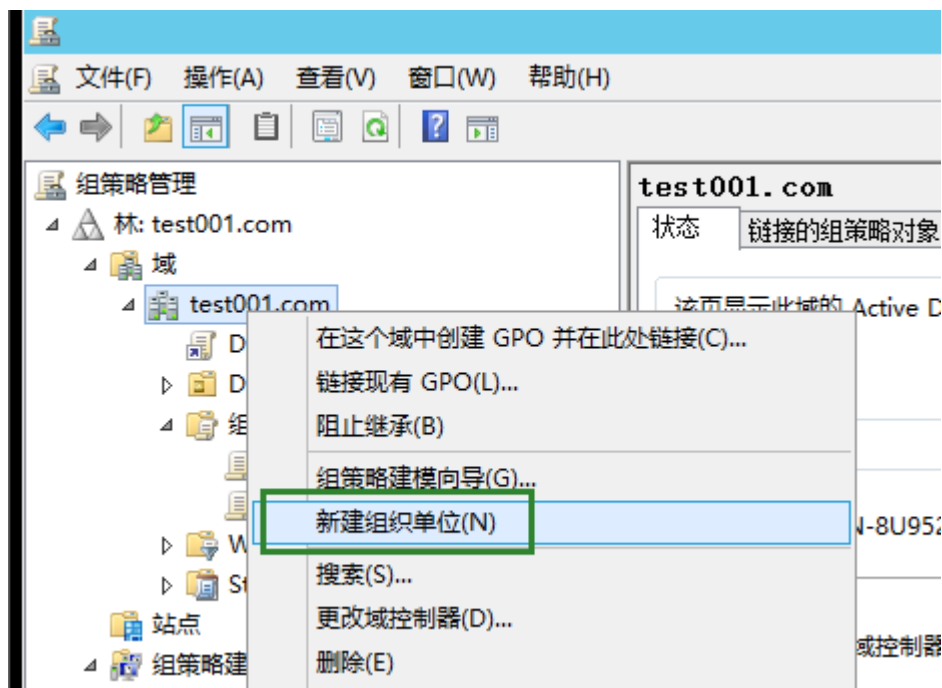
- 将脚本与安装包放到同一个共享目录下



- 进行域控下发：进入组策略管理页面

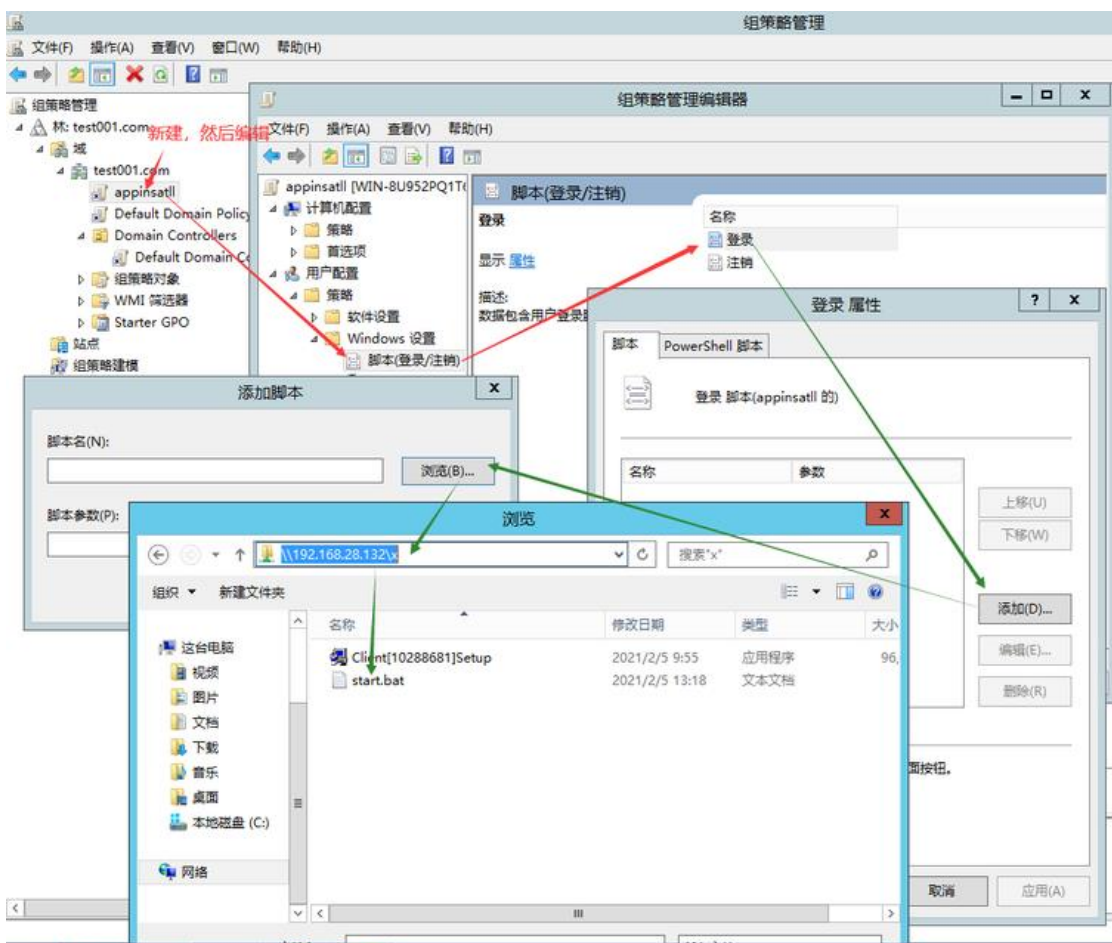
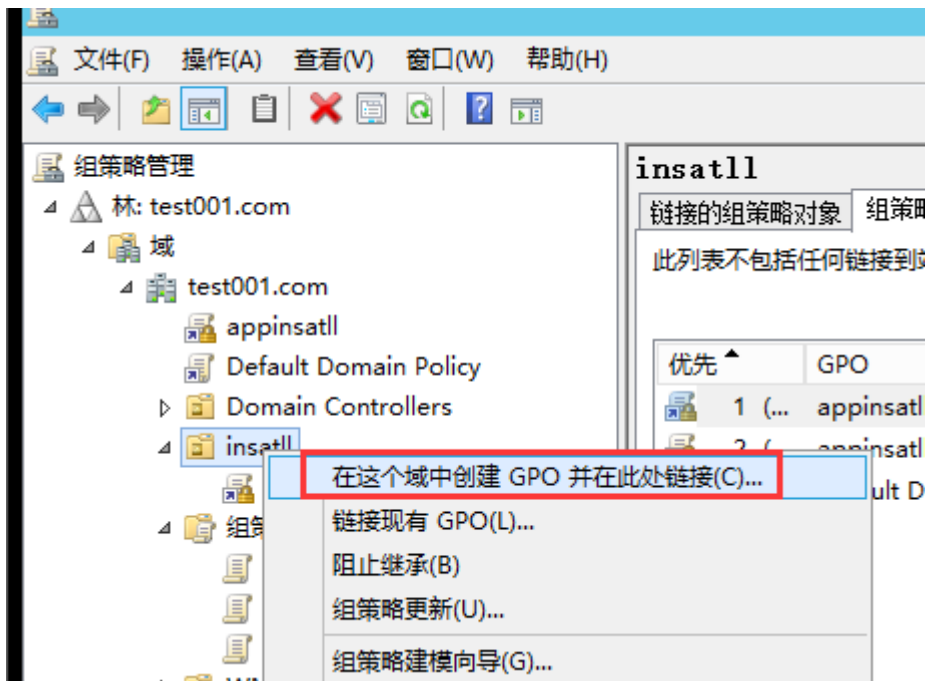


- 然后使用已有组织单元或者新建组织单元 (请注意查看里面涉及的机器是否是目标机器)



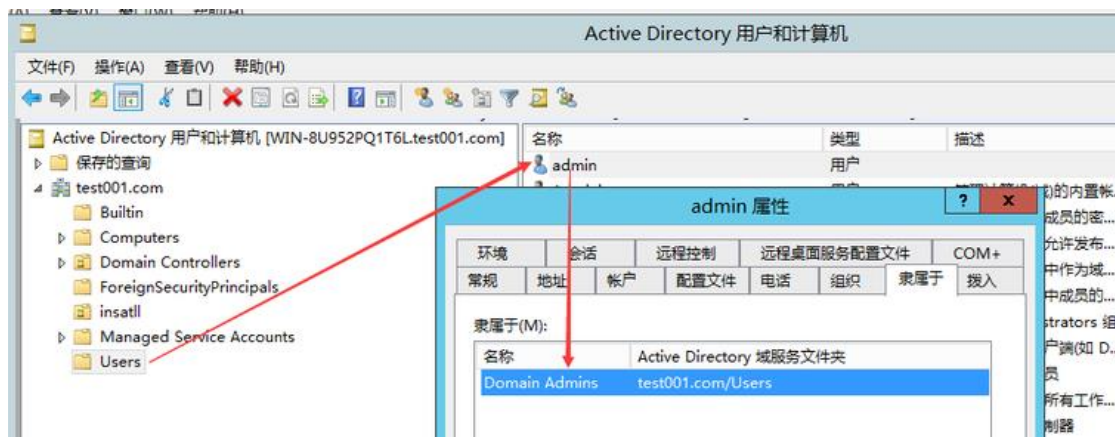
- 创建 GPO 并连接, 然后编辑, 如下图示, 选择用户配置→策略→Windows 设置→脚本→登录, 将编辑好的在共享目录里的 start.bat 文件选入, (只能选入网络路径, 切记

不要选本地的!)

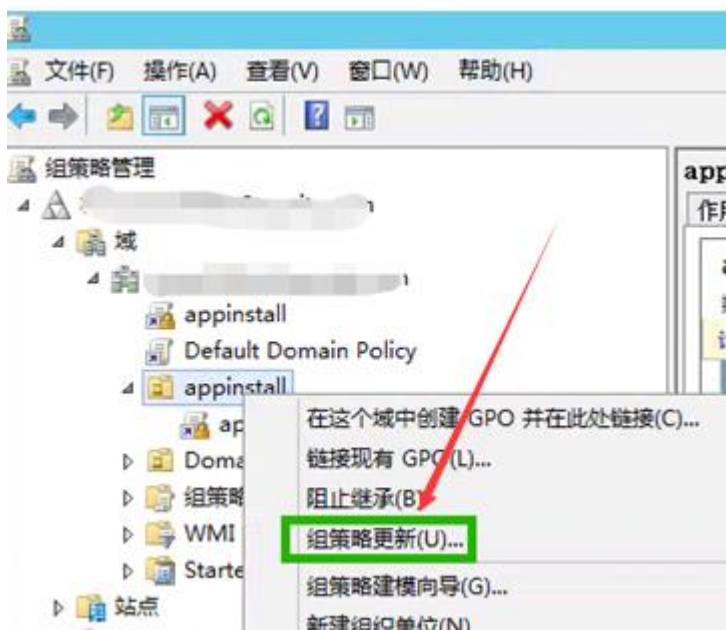


- 若是目标机器没有管理员权限的情况, 请确保存在管理员权限的域账户 (且在 start.bat

里编辑的此账号密码是无误的)



- 执行组策略更新，也可以通过 cmd 下执行 `gpupdate /force` 来操作。



- 目标机器重启后，会执行静默安装，安装完成后会自动加入企业组织并启动主界面，需要企业成员填写登记信息，用于识别设备的归属人。



1.3.2 Linux 系统部署

目前支持 Ubuntu18、Ubuntu16、Centos7、Centos6、Deepin 20。

请先在控制台下载最新的 linux 部署安装包。



下载完成后，执行./Team{10590864}.run 即可安装。(./后是您文件名的全称) 请勿修改安装包名称。

➤ 安装完成后即可在管理后台查看终端信息并对终端下发管理策略。



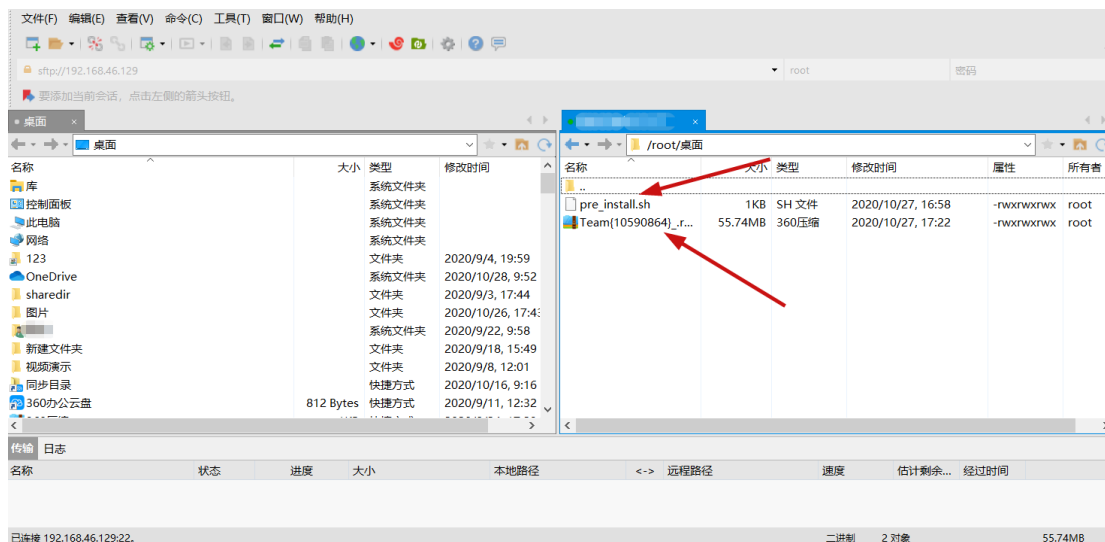
温馨提示:

FTP 上传文件举例:

- 1、以 xFTP 为列, 下载并安装 xFTP, 选择【文件】-【新建】
- 2、根据终端具体情况, 填入正确 IP、端口及登录用户名和密码



- 3、将 Team{数字 PIN 码}.EL7.x86_64.rpm 安装包文件上传到 Linux 终端上, 此处以放在桌面举例:



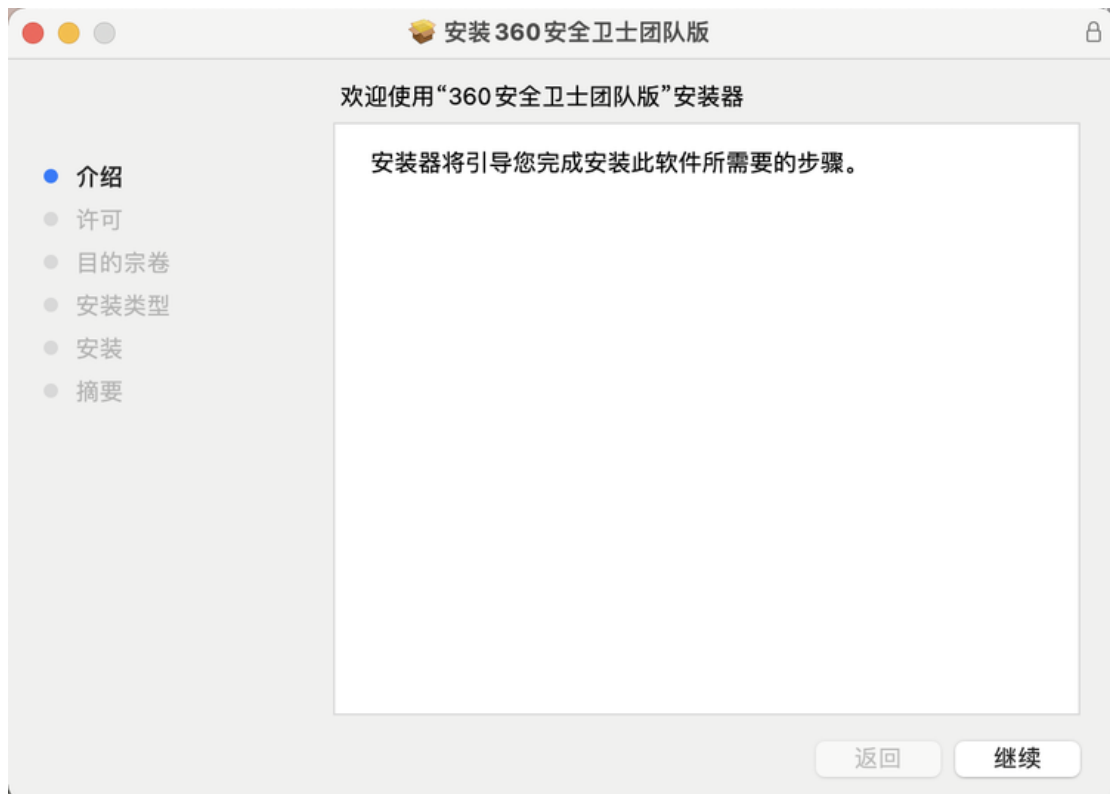
1.3.3 macOS 系统部署

➤ 360 企业安全云在 macOS 系统上的部署：

请先在管控后台下载适配 macOS 系统的安装包，



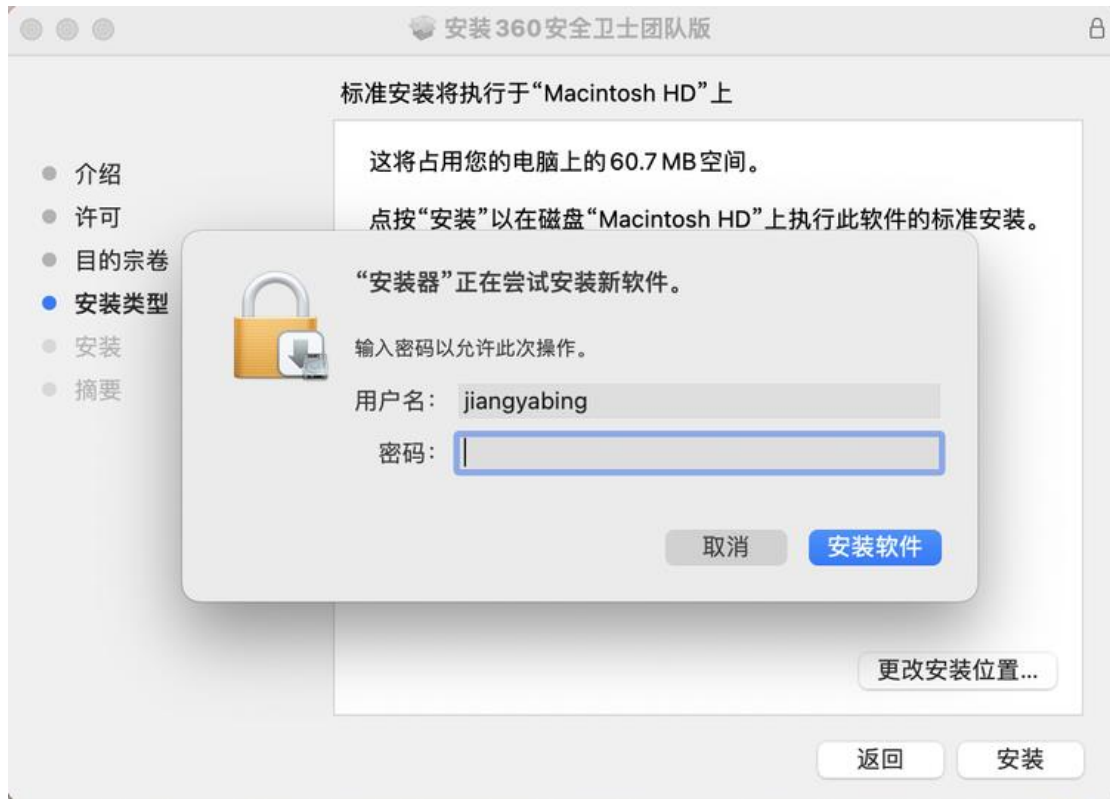
将下载下来的 pkg 安装包放到可读写的文件夹内，切勿修改文件名。然后双击 pkg 文件，根据安装向导点击“继续”。



点击“安装”“继续”按钮



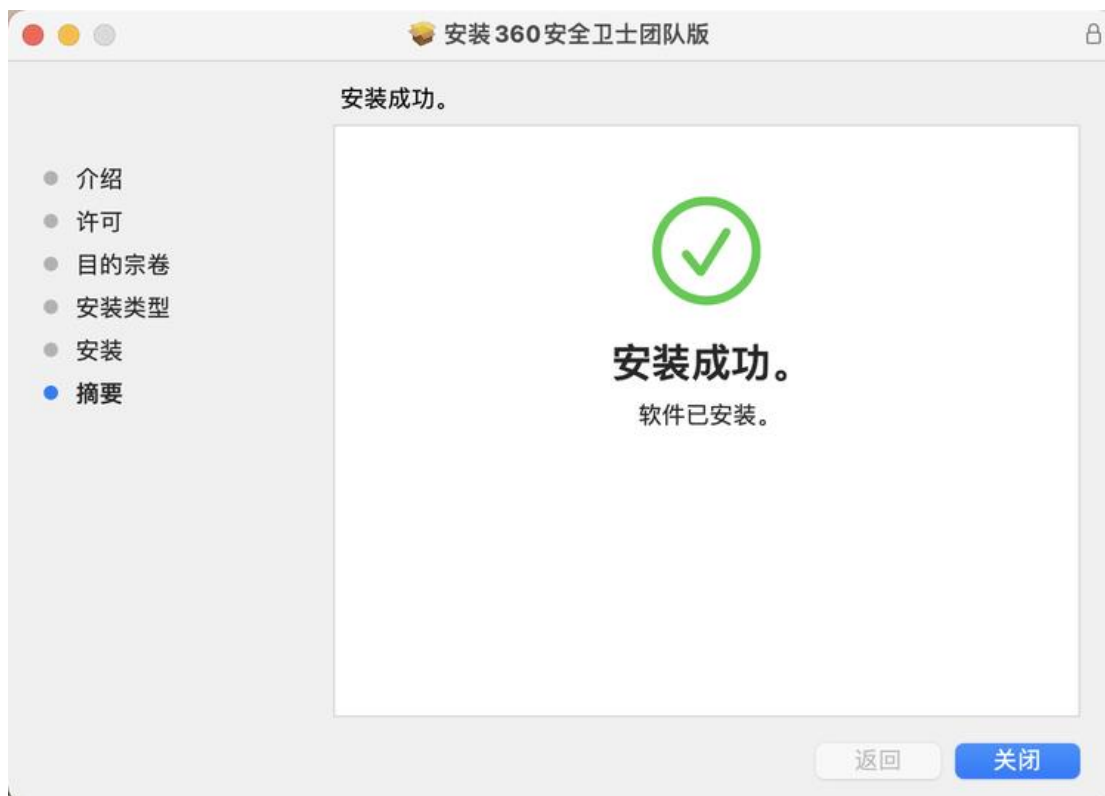
点击“安装”，弹出用户密码框，输入密码，点击“安装软件”按钮



安装过程中，会出现系统弹出的文件夹访问的确认框，请点击“好”



剩余安装过程，请耐心等待



如果提示安装失败，请重启系统，重新执行安装过程。

安装完成后即可启动界面



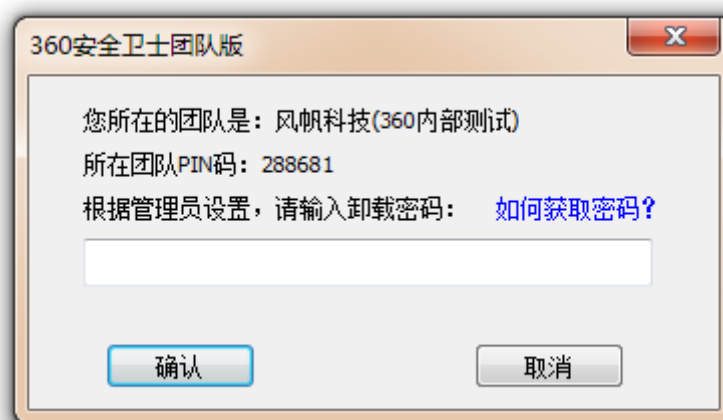
➤ 即可在控制台【设备管理】-【终端管理】中查看终端信息，并对终端下发管理策略



1.4 退出企业

退出企业组织的方式有两种：

方式一，卸载客户端，会提示用户输入卸载密码，用户填写正确的卸载密码后会退出企业



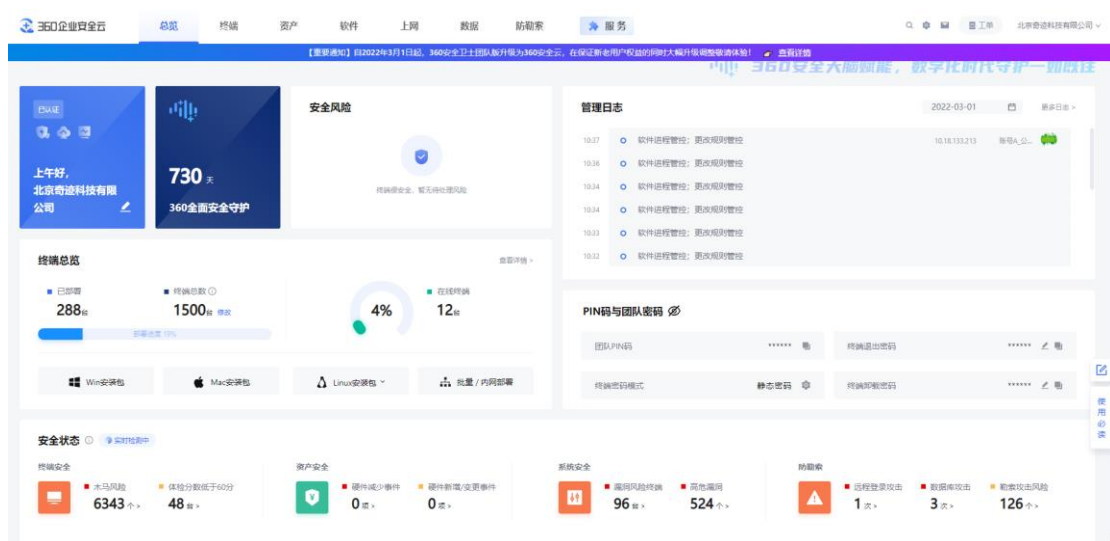
方式二，联系管理员，在管理后台【终端】-【终端管理】中进行删除，（需要注意的是，这种方式删除终端之后，该终端的数据将不能恢复，请谨慎操作）。



2、管理后台功能简介

2.1 总览

首页总览直观展示了企业全网终端的状态，包括：终端数量和状态统计、风险处理情况、安全状态、管理日志、PIN 码与团队密码、系统安全、防勒索信息等，便于管理员全面了解当前终端的整体情况。



2.2 终端

2.2.1 终端部署

用户可根据各自企业内部网络情况选择不同部署方式，包括外网场景部署，内网场景部署，从 360 网管版迁移部署，亦可设置准入规则，此页面给予用户明确的部署方案。

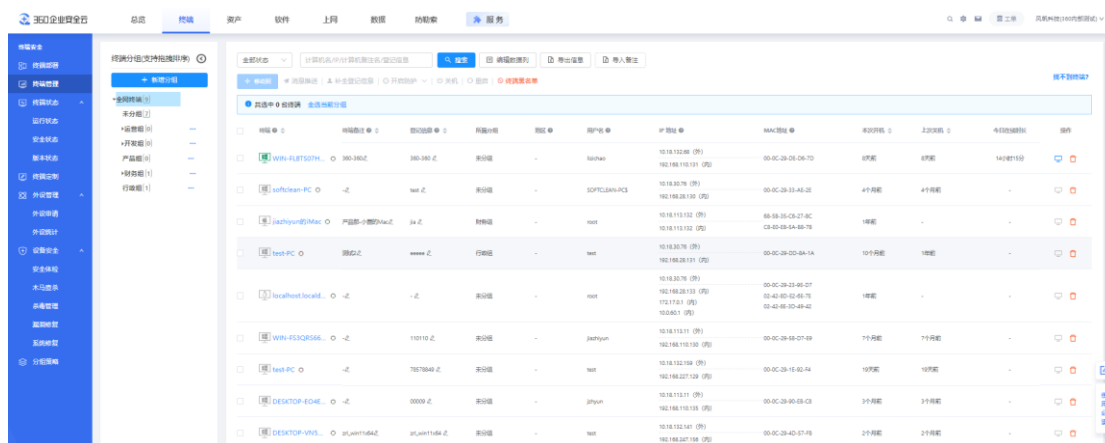


准入规则设置（专业安全管理运维服务），可以下载相应规则的安装包，获取授权码，分发给终端用户安装部署即可，可有效避免非团队终端误加入团队。



2.2.2 终端管理

展示了企业内所有终端的基本情况，包括计算机基本信息：在线状态、计算机名、终端策略、备注名、登记信息、所属分组、IP、用户名、操作系统、开关机时间等，管理员可根据计算机名、IP、备注名等信息进行搜索，也可自定义列表展示信息，并且可以进行消息推送和一键关机重启的操作。

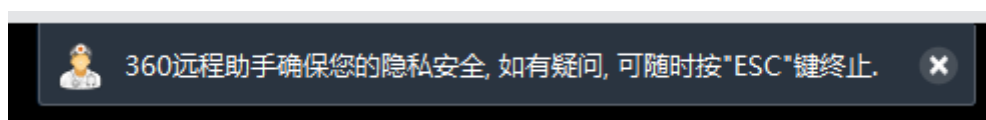
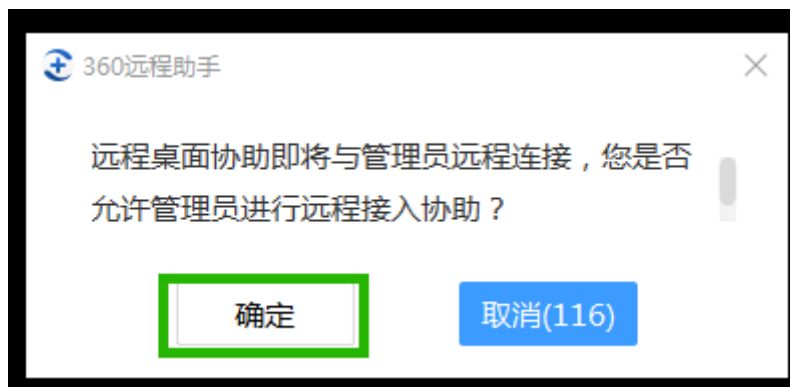


如果管理员想对某个终端进行远程协助，也可以在终端管理里操作

点击远程桌面-开始



等终端弹出 360 远程助手的提示框，点击确定



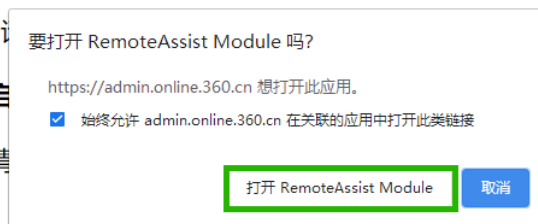
控制台会提示启动 360 远程助手，点击开启远程即可

终端状态: 终端已就绪, 可随时远程 结束

如果您看到系统对话框, 请点击“**启动应用**”, 启动360远程助手

如果点击了“**取消应用启动**”, 请 [点击此处](#) 重启360远程助手

如果浏览器未提示任何信息, 请检查网络状态, 或 [下载并运行360远程助手](#)



终端状态: 终端已就绪, 可随时远程 结束

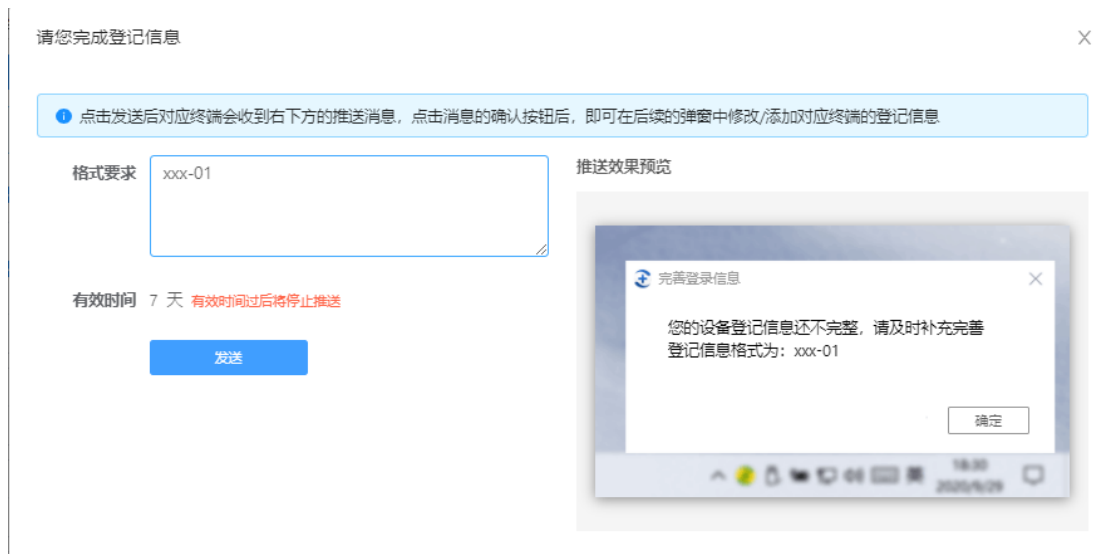
如果您看到系统对话框, 请点击“**启动应用**”, 启动360远程助手

如果点击了“**取消应用启动**”, 请 [点击此处](#) 重启360远程助手

如果浏览器未提示任何信息, 请检查网络状态, 或 [下载并运行360远程助手](#)

在此页面也可以给终端发送补全登记信息的通知, 以便管理员统计与管理。

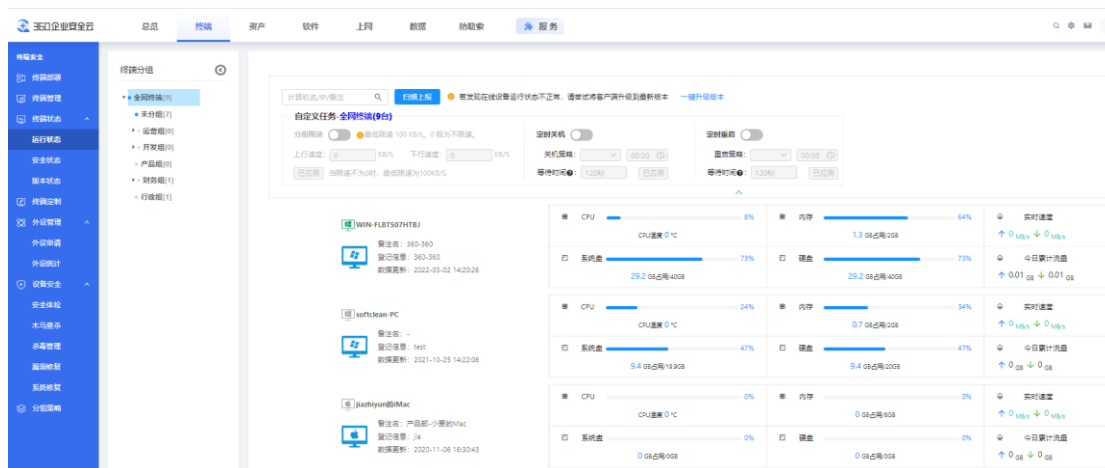




2.2.3 终端状态

2.2.3.1 运行状态

可以查看每台终端的运行状态，CPU（占用百分比和温度），内存（占用百分比和具体数据），系统盘（占用百分比和具体数据），硬盘（占用百分比和具体数据），实时速度，今日累计流量（包括上传下载）。



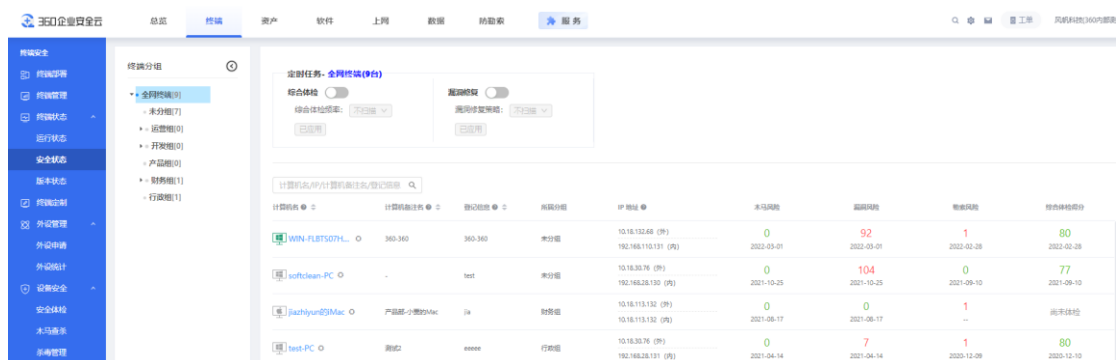
当然也可以对分组进行限速设置，还有分组定时关机和定时重启设置



2.2.3.2 安全状态

主要展示各终端的木马风险，漏洞风险和勒索风险，以及综合体检得分，帮助管理员快速发现风险，并修复存在的各种风险。

展示内容有计算机名，备注名，登记信息，所属分组，IP 地址，木马风险，漏洞风险，勒索风险，综合体检得分



同时可对分组进行定时体检和定时漏洞修复的设置



2.2.3.3 版本状态

可通过终端分组的维度，查看 360 企业安全云的版本，病毒库版本等，管理员可对分组或全局终端一键升级 360 企业安全云的版本，一键升级病毒库，亦可以对单台终端进行升级，如果您觉得此页面显示版本号未更新，可以点击【扫描上报】更新控制台的数据。



2.2.4 终端定制

➤ 安全卫士主界面

默认样式：

客户端默认界面，展示默认 logo



定制样式：

可在客户端主界面展示您企业组织的品牌 logo，企业信息卡片上可以显示管理员的联系方式及常用网址快捷入口，需要注意的是企业 logo 请按规定格式上传。



➤ 桌面壁纸（专业安全管理运维服务）

管理员可不限桌面壁纸，终端用户可全权自行设置桌面壁纸样式；也可设置终端统一桌面壁纸。目前桌面壁纸功能只支持 windows 系统，每日上传壁纸次数为 3 次，壁纸库数

量不得大于 10 张（包括审核+未审核）；壁纸文件格式为 JPG、PNG，且大小不能超过 20M。

安全卫士主界面 桌面壁纸

目前壁纸只支持windows系统。需要团队组件版本大于1720，且卫士客户端版本大于13 [一键升级版本](#)
每日上传壁纸次数为3次，壁纸库数量不得大于10张（包括审核+未审核）；壁纸文件格式为JPG、PNG，且大小不能超过20M；
即日起壁纸上传升级为先审核后审核模式。上传后可立即点击应用，如壁纸因违规被驳回后，已应用的壁纸依旧生效，但不能再次应用，如超过30日管理员未下架违规壁纸，平台将自动进行删除

桌面壁纸模式

☐ 不限制桌面壁纸
终端用户可全权自行设置壁纸样式

☒ 使用自定义桌面壁纸
可上传自定义图片，并分发至终端作为桌面壁纸

自适应终端屏幕尺寸方式：

请选择桌面壁纸今日剩余上传次数：3次： 为避免壁纸应用后出现拉伸/黑边的情况，请根据电脑屏幕尺寸选择合适比例的壁纸~

2.2.5 外设管理

在【外设申请】中，可以处理终端上提交使用 U 盘和网卡的申请。可以放行或者拒绝。设置成功后还可以再进行更改。

具体的外设限制策略，见【分组策略】中的【外设禁用】和【网卡禁用】

360 企业安全云 总览 策略 资产 软件 上网 数据 防勒索 服务

申请状态 ☒ 待处理 ☐ 已同意 ☐ 已拒绝 关键字 搜索

☐	状态	设备名称	设备名称	外设备注	设备型号	设备类型	申请人	申请时间
☐	待处理	309325f5ec135a7872d4db336d282	00e94a82101	- 无	Realtek Semiconductor Corp.—RTL8188...	网卡设备	lylei-5524138	2022-02-25 18:23:28
☐	待处理	3d8951ae5ac5b473d50e3e147646ae	68221945886081	- 无	Silicon Motion, Inc. - Taiwan (Formerly Fei...	U盘设备	lylei-5524138	2022-02-25 15:34:38
☐	待处理	2089487b48293a786d895c96e7ae57	685948f586086	- 无	Silicon Motion, Inc. - Taiwan (Formerly Fei...	U盘设备	SC-2021132291821	2022-02-24 19:37:10
☐	待处理	11f18f8642d8b237a7e11a3885a8bc7b	4c53200020204106130	- 无	SanDisk Corp.	U盘设备	zx-win764new-PC	2022-02-15 18:31:18
☐	待处理	5395742b63d9506476b5ee6144bc3	#####e950306a2	- 无	Toshiba Corp.—Kingston DataTraveler 102...	U盘设备	DCJHW12	2022-01-29 10:25:43
☐	待处理	4b3309b74432c7f1b6596416291d298	78347695cd680000	- 无	Samsung Electronics Co., Ltd.—Galaxy seri...	U盘设备	DESKTOP-E58GCH6	2021-09-28 17:56:08
☐	待处理	afda026a01143c5eae725d9c0c33188	68388cd704b60000	- 无	Ours Technology, Inc.	-	DESKTOP-LSPB00-win10	2021-09-13 14:58:42
☐	待处理	99a77c5a23ba26314963f949533181b	2004301483189a40a362	ddid 无	SanDisk Corp.—Cruzer Glide	U盘设备	DESKTOP-LSPB00-win10	2021-09-13 14:58:42

审批记录中可查看处理外设申请的记录，支持申请人、审批人、设备名、设备码、拒绝原因搜索。

360企业安全云									
总览		终端	资产	软件	上网	数据	防勒索	服务	
关键字 支持申请人、申请人、目的地原因、设备名、设备id 清除									
数据只展示4月21日后的数据									
状态	设备名称	设备名称	厂商型号	申请人	申请时间	申请人	审批时间	审批理由	
已同意	dc3ff174c4e6tub68a13630e12c838ff6	6x18dweed58d0d1	Silicon Motion, Inc. - Taiwan ...	DESKTOP-85BGCH6	2022-02-25 16:55:23	陈号A_公用电脑	2022-02-25 16:59:32	-	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	DESKTOP-85BGCH6	2022-02-25 15:12:58	陈号A_公用电脑	2022-02-25 16:59:24	-	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	DESKTOP-85BGCH6	2022-02-25 15:12:58	陈号A_公用电脑	2022-02-25 16:59:20	1	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	lyjlei-5524138	2022-02-25 18:23:28	陈号A_公用电脑	2022-02-25 16:42:40	-	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	lyjlei-5524138	2022-02-25 18:23:28	陈号A_公用电脑	2022-02-25 16:42:15	-	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	DESKTOP-85BGCH6	2022-02-25 15:12:58	陈号A_公用电脑	2022-02-25 15:14:19	-	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	DESKTOP-85BGCH6	2022-02-25 15:12:58	陈号A_公用电脑	2022-02-25 15:14:16	下	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	DESKTOP-85BGCH6	2022-02-25 15:12:58	陈号A_公用电脑	2022-02-25 15:13:09	-	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	DESKTOP-85BGCH6	2022-02-25 15:12:58	陈号A_公用电脑	2022-02-25 15:13:05	下	
已同意	3093f29c5ec130b9f72dedab336d82	00e04c9d2101	Realtek Semiconductor Corp...	lyjlei-5524138	2022-02-25 18:23:28	陈号A_公用电脑	2022-02-25 14:58:35	1	

外设管控是一个很常用的功能，【外设统计】中可按终端和设备两个维度统计，亦可查看使用外设记录。

网络安全

终端管理

终端状态

终端控制

外设管理

外设申请

外设统计

设备安全

分电策略

终端审批

按终端统计

按设备统计

关键词

计算机/PC/计算服务器/服务器

状态

选择器

搜索

计算机名	计算机名称	默认组	所属分组	IP 地址	累计使用流量
DESKTOP-DLFRER	无享	Lion118	未分组	10.162.7.2 (内) 172.26.63.134 (内)	5
WIN-8C7H12EUL	-	123456	无_恶意	10.19.1.152 (内) 10.19.1.152 (内)	0
SCD100L4G5	-	11	未分组	10.16.134.35 (内) 10.16.134.35 (内)	1
WIN-45OHMARO...	xxxx	-	QAQ	10.19.1.150 (内) 192.168.237.129 (内)	0
jyt-4-PC	-	jyt	未分组	10.19.1.196 (内) 192.168.149.139 (内)	12
SC-202112291821	-	gordon	qgf	10.16.133.213 (内) 192.168.81.134 (内)	5
wy-9f3cf323c5b	-	www	未分组	10.19.5.5 (内) 192.168.81.138 (内)	3
DC2HWY2	-	gordon	qgf	10.16.133.213 (内) 10.16.133.213 (内)	5
CCM682	-	-	未分组	10.19.100.18 (内) 10.19.100.18 (内)	0
6CH62732PP	-	-	无_恶意	10.19.1.26 (内) 10.19.1.26 (内)	0

网络安全

终端管理

终端状态

终端控制

外设管理

外设申请

外设统计

设备安全

分电策略

终端审批

按终端统计

按设备统计

关键词

设备名称/外设类型/设备型号

搜索

设备名	设备名称	设备备注	设备型号	设备类型	设备空间	可用空间	使用过流量峰值
62075c66c44b870ac3e36e4423ba07c	5879c738480b1	-Z-	Realtek Semiconductor Corp.—RTL8188GU 802.11n W...	无线设备	-	-	1
718c5ee99330c6f9e699445a6b7c	79104c5d80b1	-Z-	Realtek Semiconductor Corp.—RTL8188GU 802.11n W...	无线设备	-	-	1
208946720a27913736305c5f9703bae7	68248f56b0b6	-Z-	Silicon Motion, Inc. - Taiwan (Formerly Feiya Techno...	无线设备	1483 G	3.62 G	1
04124c59f7b761627ba1728d5dc2e33e	5879c738480b3	-Z-	Silicon Motion, Inc. - Taiwan (Formerly Feiya Techno...	无线设备	1483 G	3.62 G	1
431946627ae3a777abdb4970703bae	681b8ee680b2	-Z-	Silicon Motion, Inc. - Taiwan (Formerly Feiya Techno...	无线设备	1483 G	3.62 G	2
dc3f174c4ebd46d8f1833ea133338f	681b8ee680b1	-Z-	Silicon Motion, Inc. - Taiwan (Formerly Feiya Techno...	无线设备	1483 G	3.62 G	2
a517a3a3a8c3329027b486438f36b6	682219488a0b2	-Z-	Realtek Semiconductor Corp.—RTL8188GU 802.11n W...	无线设备	-	-	1
a66b917820e4a4e432556c11023ee4	681b8ee680b1	-Z-	Realtek Semiconductor Corp.—RTL8188GU 802.11n W...	无线设备	-	-	2
2e1023c15ae3f580d7189942baf6a	6810346f180b2	-Z-	Silicon Motion, Inc. - Taiwan (Formerly Feiya Techno...	无线设备	1483 G	3.62 G	1
aca89ca01119190f7833f9a63af	6810346f180b1	-Z-	Silicon Motion, Inc. - Taiwan (Formerly Feiya Techno...	无线设备	1483 G	3.62 G	2

2.2.6 设备安全

2.2.6.1 安全体检

在安全体检页面中，可以查看全网终端的在线离线状态、IP 地址、MAC 地址以及体检状态等，可以对特别的终端进行修复，或者对多个终端进行一键扫描和一键修复。



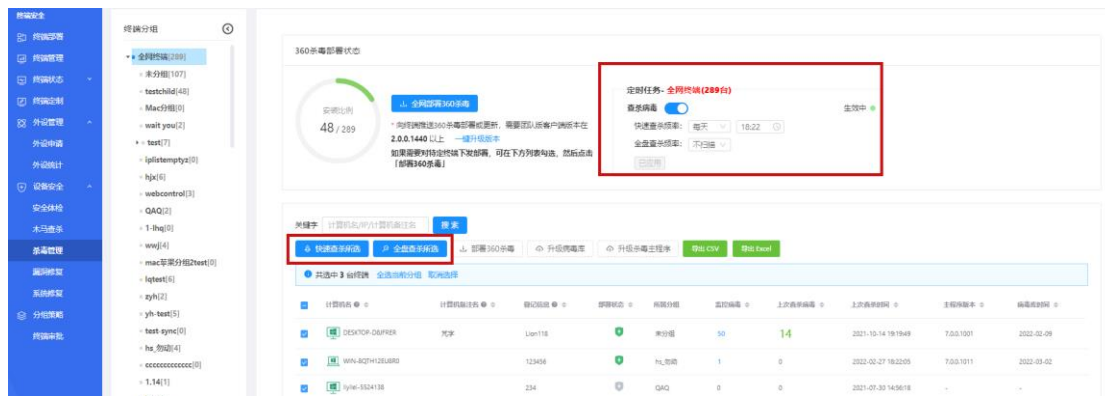
2.2.6.2 木马查杀

支持选择终端进行【快速查杀】和【全盘查杀】，并展示查杀进度、查杀时间等。



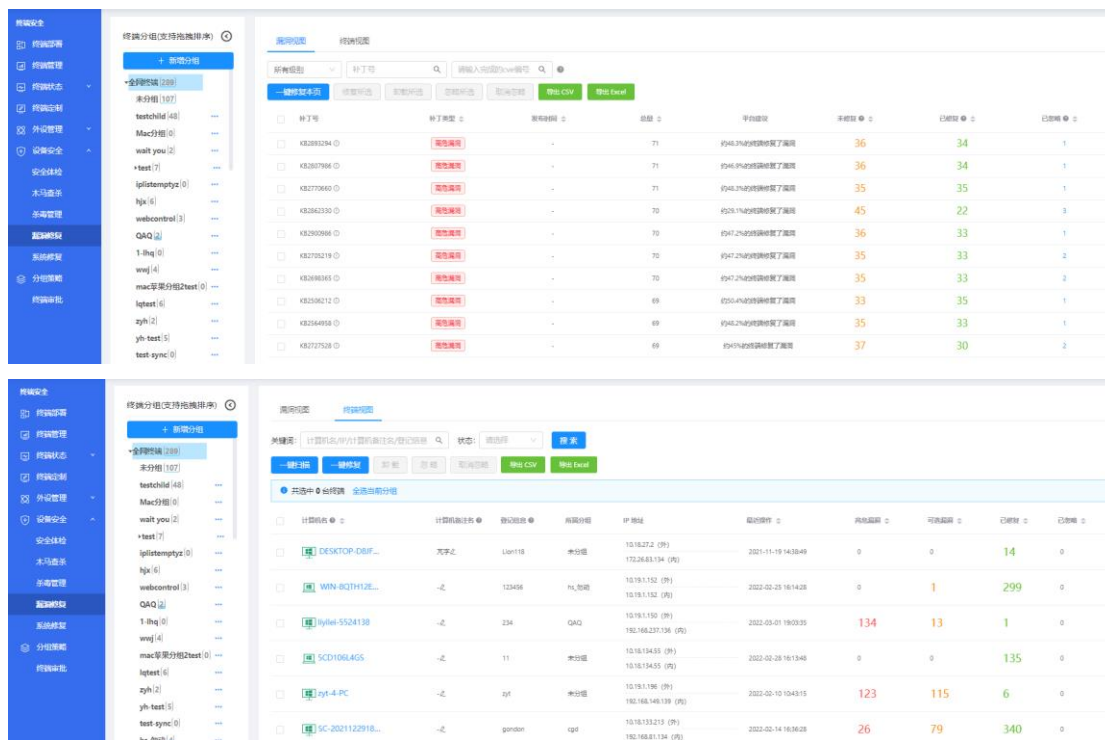
2.2.6.3 杀毒管理

360 企业安全云可以轻松的批量部署 360 杀毒，该功能是为了满足对 360 杀毒有需求的用户提供的。在该页面中，可以进行【快速扫描】、【全盘扫描】。也可以一键全网部署 360 杀毒，并升级病毒库。同时，在此也可进行分组定时杀毒设置。



2.2.6.4 漏洞修复

可以从漏洞统计和终端统计的不同维度展现目前整个企业内终端的漏洞情况, 管理员可以针对不同程度的漏洞和特定的终端下发扫描、修复、卸载、忽略、取消忽略的命令。



2.2.6.5 系统修复

可以从项目统计和终端统计的维度展现修复项的数量。

按项目统计页面可以查看修复项的名称、描述、类别、操作建议及未修复和已修复数量,



可对**全网终端**和**分组终端**进行基本设置、防护设置、消息推送、浏览器设置、文件白名单设置、漏洞管理、软件管家、外设禁用、USB 网卡禁用、预警设置、上网限制、安全基线、勒索防护等策略设置。

提示：面向分组设置不同的安全策略，设置过的分组和策略，会标记为 **XXX**，设置过的子分组**不继承**上级分组的策略。



➤ 基本设置：

● 客户端设置

卸载密码：设置防止终端卸载客户端的密码

退出密码：设置防止终端退出客户端的密码

可设置密码策略为动态密码或者静态密码



➤ 防护设置：

防护设置功能，可以批量设置是否允许用户修改客户端安全防护中心和设置中心的设置，暂时仅支持 windows 终端。



可以对终端客户端的设置中心和安全防护中心进行统一设置之后进行策略下发，以避免多台客户端进行重复设置。



➤ 消息设置：

用于创建全局或者分组下发给终端的定时和周期性通知，管理员可根据通知需求进行内容编辑和时间设置，有效期过后，终端将不再接受消息。

Windows Linux macOS

当前分组：全网终端

基本设置 防护设置 消息设置 浏览器设置 文件白名单 漏洞管理 软件管家 外设禁用

向终端推送定时和周期性的消息。有效期过后，终端将不再接收消息。

消息设置

消息设置开启 ☒

* 消息标题

会议通知

* 消息内容

即日起每天上午九点开晨会，全体员工参与。|

推送URL ?

URL地址，例如: https://www.360.cn

* 有效期至

🕒 2022-04-28 10:00:00

发布时间

☒ 开机显示

☐ 周期显示

每周一 ▼

🕒 08:00

应用

➤ **浏览器设置 (专业安全管理运维服务):**

可设置全局或者分组终端的默认浏览器和浏览器主页。

Windows

Linux

macOS

当前分组：全网终端

[基本设置](#) [防护设置](#) [消息设置](#) [浏览器设置](#) [文件白名单](#) [漏洞管理](#) [软件管家](#) [外设禁用](#) [USB网卡禁用](#)

锁定主页或默认浏览器

1. 「主页锁定」功能将锁定所有浏览器的主页为选定的项（可输入自定义网址），不允许修改；
2. 设置「浏览器锁定」后，其他浏览器仍可以正常运行，但打开外部链接（如QQ聊天中的链接）时将在默认浏览器中打开。

浏览器和主页设置

浏览器主页锁定（可下拉选择，或点击文本框直接输入自定义主页）

360搜索

[查看示例](#)

默认浏览器锁定

360极速浏览器



应用

➤ 文件白名单：

对木马查杀任务的自定义设置，可以添加目录白名单、文件白名单、MD5 白名单，添加信任之后，木马查杀任务将不再扫描这些位置和文件。

Windows Linux macOS

当前分组：全网终端

[基本设置](#) [防护设置](#) [消息设置](#) [浏览器设置](#) [文件白名单](#) [漏洞管理](#) [软件管家](#) [外设禁用](#) [USB网卡禁用](#) [预警设置](#) [上网限制](#) [安全基线](#) [勒索防护](#)

文件或目录加入白后，查杀引擎在扫描时会将其跳过。请确保添加的是可信的文件/目录。软件报错提交。 [点击进入>>](#)

自定义设置

目录白名单
① (目录信任模式)

C:\Users\softclean\Desktop 自删除
C:\Windows\System32 自删除

输入目录 添加

文件白名单
① (文件信任模式)

未添加

文件绝对路径 添加

MD5白名单
① (输入32位长度的数字或字母)

d884da1b668951109c36f0822b44c26f 自删除

输入32位长度的数字或字母 添加

如何查询文件MD5?

应用

➤ 漏洞管理：

管理员对终端下发漏洞修复策略的设置，包括修复漏洞时间、漏洞类型、漏洞级别、修复完是否重启等设置。



➤ 软件管家：

这里可以设置是否屏蔽软件管家入口，是否禁用软件管家的下载功能，可以防止终端通过软件管家下载不必要的软件。

WindowsLinuxmacOS

当前分组：全网终端

基本设置

防护设置

消息设置

浏览器设置

文件白名单

漏洞管理

软件管家

外设禁用

❗

屏蔽软件管家入口：屏蔽软件管家入口后，客户端会隐藏软件管家的卫士入口和桌面图标，同时限制手动打开软件管家。
开启捆绑软件拦截：捆绑软件是当你安装一款软件时，同时会静默给你偷偷安装的软件。捆绑软件拦截开启后，自
禁用软件管家下载功能：客户端会屏蔽软件管家下载入口、隐藏宝库升级等界面，只留卸载和净化；在卫士中依然

软件管家策略

屏蔽软件管家入口

开启捆绑软件拦截

禁用软件管家下载功能

允许操作软件升级

2.0.0.1630后的客户端支持

2.0.0.1710后的客户端支持

查看版本详情

软件管家放行模式

该功能已迁移至「管控->软件管理->终端视图」页面。

查看详情

➤ 外设禁用（专业安全管理运维服务）：

管理员可设置全局终端或分组终端的外设读写模式，并可添加外设的信任列表。

当前分组：全网终端

基本设置

防护设置

消息设置

浏览器设置

文件白名单

漏洞管理

软件管家

外设禁用

USB网卡禁用

预警设置

上网限制

安全基线

勒索防护

❗

外设读写模式

1. 使用「禁用模式」时，请确保您的策略不会影响团队业务的正常开展。通常情况下，不建议使用此模式。
2. 出于系统安全和稳定性考虑，策略下发成功后再重新插拔外设后方可生效。

外设读写模式设置

读写模式

只读模式

禁用模式

终端正常使用所有外设，可读可写

终端只可读取外设内容，不可写入

只允许「信任列表」中的外设接入终端

禁用模式下将禁用团队可识别的所有带U盘/读卡器以外的设备，不仅仅包含U盘。若与您的预期不符，欢迎提交工单讨论沟通

应用

外设信任列表

展示字段优先展示U盘/网卡的用户备注。若无备注展示外设的厂商型号，若识别不到厂商型号，则展示外设名称

1项

本组未信任外设

设备名称/外设备注/设备码

设备名称	设备码	状态	外设备注	设备型号
☐	f9c8d283c5a665b56b9ee82dc0fa1f5b	未信任	京东小宠物	Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.)

应用

2项

已信任外设（禁用模式下生效）

设备名称	外设备注
☐	68103465e180&1
☐	4c530000100314111244

➤ USB 网卡禁用（专业安全管理运维服务）：

管理员可设置全局终端或分组终端的网卡启用/禁用模式，并可添加网卡的信任列表。



➤ 预警设置：

可以设置全局终端和分组终端的预警时间和预警类型。预警时间可以设置预警频率和预警时间段；预警类型可以选择哪些关注的项目进行预警提示，设置预警阈值并邮件告警。



➤ 上网限制（专业安全管理运维服务）：

上网限制分为无限制、黑名单和白名单三种模式，默认为无限制模式。

黑名单模式即不允许终端访问黑名单中的域名网站；可设置上网时段限制。

上网限制

- 限制模式 ☐ 无限制
- ☒ 黑名单模式 (不允许终端访问黑名单中的域名网站)
- ☐ 白名单模式 (只允许终端访问白名单中域名相关的网站)

黑名单设置 通过分类添加

☐ 分类列表 0/33

☐ 企业

☐ 体育

☐ 健康

☐ 儿童

☐ 军事

☐ 动漫

☐ 其他

☐ 分类黑名单 0/0

无数据

自定义添加

域名黑名单

① 黑名单应用后，终端将无法访问名单内的域名（最多只能添加100个）

添加

白名单设置 信任名单

域名白名单

① 此名单中的域名可以将黑名单中的部分域名额外加白

添加

上网时段限制 可通过点击下方节点选择黑/白名单策略生效的时间段，未选中区间内可自由上网，不受限制

上网时段限制: ☐

限制策略生效日期: ☐ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六 ☐ 周日

限制策略生效时间段:

00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00

12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 24:00

应用

白名单模式即只允许访问白名单中域名相关的网站，可设置上网时段限制

上网限制

限制模式 ☐ 无限制☐ 黑名单模式 (不允许终端访问黑名单中的域名网站)☒ 白名单模式 (只允许终端访问白名单中域名相关的网站)

白名单设置 | 自定义添加

域名白名单

① 在白名单模式下, 只有白名单内的域名才可以访问 (最多只能添加100个)

输入需要加入白名单的域名

添加

上网时段限制 | 可通过点击下方节点选择黑/白名单策略生效的时间段, 未选中区间内可自由上网, 不受限制

上网时段限制: ☐限制策略生效日期: ☐ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六 ☐ 周日

限制策略生效时间段:

00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00

12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 24:00

应用

➤ 安全基线 (专业安全管理运维服务):

检查有助于用户一键获知全网主机安全基线配置详情, 找出不符合安全管理规范的终端, 节省大量人工检查时间, 并能持续进行监控。此功能设置后, 可以在【防勒索】-【安全基线】页面中查看对应的防护效果。

Windows Linux macOS

当前分组: 全网终端

基本设置 防护设置 消息设置 浏览器设置 文件白名单 漏洞管理 软件管家 外设禁用 USB网卡禁用 预警设置 上网限制 安全基线 勒索防护

向终端推送定时和周期性的消息, 有效期过后, 终端将不再接收消息。

安全基线防护

☐ 选择所有防护项 0 / 36

查找防护项

☐ 关闭空密码远程登陆

☐ 关闭远程协助服务

☐ 关闭Telnet远程链接服务

☐ 关闭远程桌面服务

☐ 修复系统账号弱密码

☐ 关闭远程注册表服务

☐ 关闭高风险系统账号

☐ 关闭隐藏盘符共享

☐ 关闭admins管理员共享

☐ 检测mysql数据库弱密码

☐ 检测sqlserver数据库弱密码

☐ 关闭共享目录写入权限

☐ 开启账户锁定策略

应用

➤ 勒索防护 (专业安全管理运维服务):

对于终端的勒索防护设置可以选择允许远程桌面连接的时间段。



Linux 系统：

目前 Linux 系统支持的分组策略有基本设置、消息设置、文件白名单和预警设置，并且在持续更新中，策略下发与 windows 系统一致。

➤ 基本设置：



➤ 消息设置：

全网终端[1]

未分组[1]

运营组[0]

开发组[0]

产品组[0]

财务组[0]

行政组[0]

WindowsLinuxmacOS

当前分组：全网终端

基本设置消息设置文件白名单预警设置

向终端推送定时和周期性的消息。有效期过后，终端将不再接收消息。

消息设置

消息设置开启

消息标题

消息内容

推送URL

URL地址，例如：https://www.360.cn

有效期至

选择时间

发布时间

开机显示

周期显示

每周一

08:00

应用

文件白名单：

全网终端[1]

未分组[1]

运营组[0]

开发组[0]

产品组[0]

财务组[0]

行政组[0]

WindowsLinuxmacOS

当前分组：全网终端

基本设置消息设置文件白名单预警设置

文件或目录加入白后，病毒引擎在扫描时会将其放过。请确保添加的是可信的文件/目录。

自定义设置

目录白名单

文件白名单

MDS白名单

应用

预警设置：

全网终端[1]

未分组[1]

运营组[0]

开发组[0]

产品组[0]

财务组[0]

行政组[0]

WindowsLinuxmacOS

当前分组：全网终端

基本设置消息设置文件白名单预警设置

预警时间

预警频率 两次预警间隔不小于 30 分钟

时间段 上午 9 点到 12 点 下午 14 点到 18 点

预警类型

邮件告警	预警类型	预警阈值
☒	病毒木马预警	病毒风险项超过1天未处理
☐	版本更新预警	病毒库、木马库超过1周末更新
☐	高危漏洞预警	高危漏洞超过1周末修复
☐	系统盘占用预警	系统盘占用超过90%
☐	磁盘总体占用预警	磁盘总体占用超过90%
☒	CPU占用预警	CPU占用超过90%，并持续10分钟以上
☒	内存占用预警	内存占用超过90%，并持续10分钟以上
☒	CPU温度预警	CPU温度超过70℃，并持续10分钟以上
☒	硬盘温度预警	硬盘温度超过70℃，并持续10分钟以上
☒	上传网速预警	上传网速超过70MB/s，并持续10分钟以上
☒	下载网速预警	下载网速超过70MB/s，并持续10分钟以上

邮件方式预警请点击我设置邮箱

macOS 系统：

目前 macOS 系统支持的分组策略有基本设置、消息设置、文件白名单、外设禁用和预警设置，并且在持续更新中，策略下发与 windows 系统一致。

➤ 基本设置：

Windows

Linux

macOS

当前分组：全网终端

• 基本设置 • 消息设置 • 文件白名单 • 外设禁用  • 预警设置

① 设置「卸载密码」和「退出密码」可以防止终端用户随意卸载/退出客户端。

客户端设置

① 当前应用策略为动态密码，此处并未生效 [【查看动态密码】](#) [【修改密码策略】](#)

卸载密码



应用

退出密码

应用

➤ 消息设置

Windows

Linux

macOS

当前分组：全网终端

[基本设置](#) [消息设置](#) [文件白名单](#) [外设禁用](#) [预警设置](#)

向终端推送定时和周期性的消息。有效期过后，终端将不再接收消息。

消息设置

消息设置开启 ☒

* 消息标题 会议通知

* 消息内容 即日起每天上午九点开晨会，全员参加。

推送URL  URL地址，例如：https://www.360.cn

* 有效期至 2022-04-30 20:00:00

发布时间 ☒ 开机显示☐ 周期显示

每周一

08:00

应用

文件白名单

Windows

Linux

macOS

当前分组：全网终端

[基本设置](#) [消息设置](#) [文件白名单](#) [外设禁用](#) [预警设置](#)

文件或目录添加后，查杀引擎在扫描时会将其跳过。请确保添加的是可信的文件/目录。软件误报提交，[点击进入>>](#)

自定义设置

目录白名单

① (目录信任模式)

未添加

输入目录

添加

文件白名单

① (文件信任模式)

未添加

文件绝对路径

添加

MD5白名单

① (输入32位长度的数字或字母)

未添加

输入32位长度的数字或字母

[如何查询文件MD5?](#)

添加

应用

外设禁用 (专业安全管理运维服务):

🍏 全网终端[1]

未分组[0]

运营组[0]

开发组[0]

产品组[0]

财务组[1]

行政组[0]

WindowsLinuxmacOS

当前分组：全网终端

基本设置消息设置文件白名单外设禁用 **外设读写** 预警设置

⚠️ macOS网卡禁用
macOS不支持网卡的禁用管控

⚠️ 外设读写模式
1. 使用「禁用模式」时，请确保您的策略不会影响团队业务的正常开展。通常情况下，不建议使用此模式。
2. 出于系统安全和稳定性考虑，策略下发成功后需重新插拔外设后方可生效。

外设读写模式设置

读写模式 终端正常使用所有外设，可读可写

禁用模式 只允许「信任列表」中的外设接入终端

应用

外设信任列表 展示字段优先展示U盘/网卡的用户备注，若无备注展示外设的厂商型号，若识别不到厂商型号，则展示外设名称

本组未信任外设 0/7

请输入搜索内容

☐ 京东小狗狗

☐ Initio Corporation—INIC-3619PN SATA B...

☐ VMware, Inc.

☐ SanDisk Corp.—Ultra

☐ [鼠标]Logitech, Inc.—M105 Optical Mouse

☐ Parallel Dice Co., Ltd

☐ Parallel Dice Co., Ltd

应用

已信任外设 (禁用模式下生效) 0/0

请输入搜索内容

无数据

➤ 预警设置：

Windows

Linux

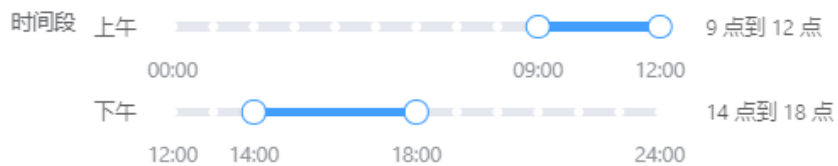
macOS

当前分组：全网终端

[基本设置](#) [消息设置](#) [文件白名单](#) [外设禁用](#) [预警设置](#)

预警时间

预警频率 两次预警间隔不小于 30 分钟



预警类型

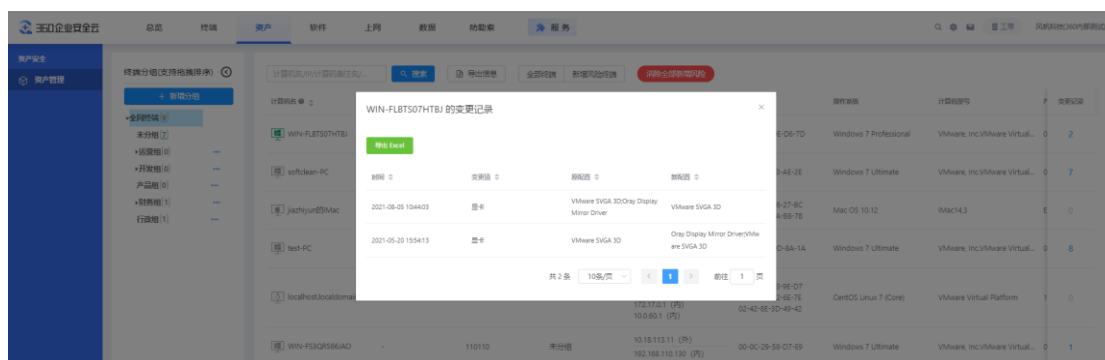
邮件告警	预警类型	预警阈值
☒	病毒木马预警	病毒风险项超过1天未处理 🔗
☐	版本更新预警	病毒库、木马库超过1周末更新 🔗
☐	高危漏洞预警	高危漏洞超过1周末修复 🔗
☐	系统盘占用预警	系统盘占用超过90% 🔗
☐	磁盘总体占用预警	磁盘总体占用超过90% 🔗
☒	CPU占用预警	CPU占用超过90%，并持续10分钟以上 🔗
☒	内存占用预警	内存占用超过90%，并持续10分钟以上 🔗
☒	CPU温度预警	CPU温度超过70°C，并持续10分钟以上 🔗
☒	硬盘温度预警	硬盘温度超过70°C，并持续10分钟以上 🔗
☒	上传网速预警	上传网速超过70MB/s，并持续10分钟以上 🔗
☒	下载网速预警	下载网速超过70MB/s，并持续10分钟以上 🔗

[邮件方式预警请先点击我设置邮箱](#)

2.3 资产

2.3.1 资产管理

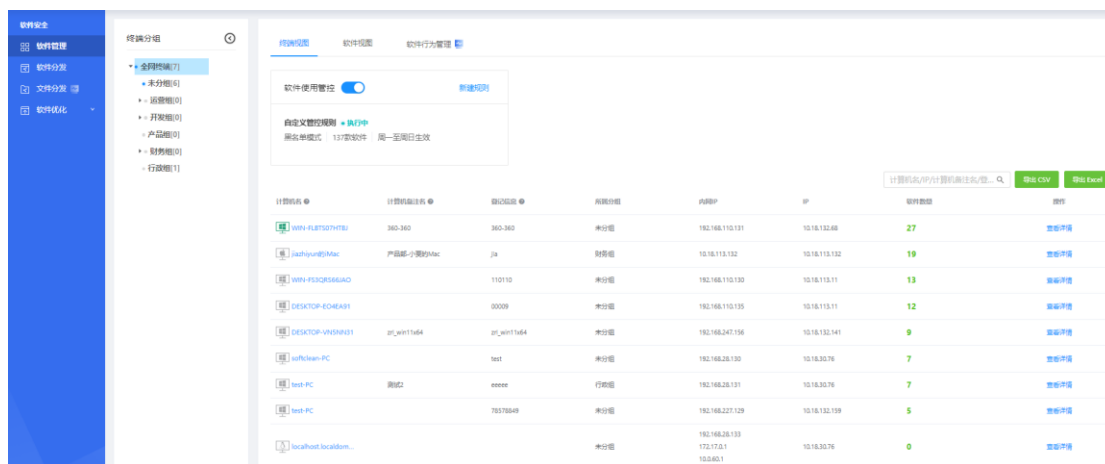
方便管理员针对终端的系统（操作系统版本，产品 ID）、硬件信息（计算机型号，CPU、内存容量，内存信息，硬盘，主板，显卡，网卡，声卡，显示器，SN 码等）、变更记录进行查看，导出分析。

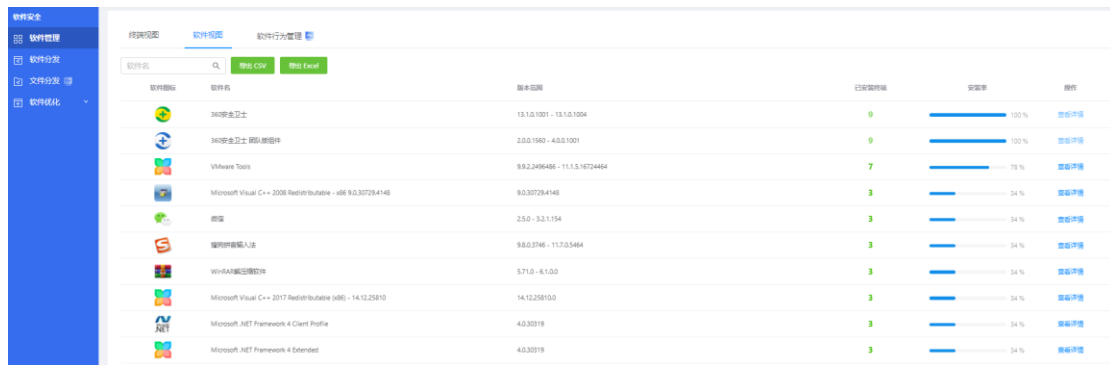


2.4 软件

2.4.1 软件管理

软件管理可以对终端已安装的软件情况进行查看以及相应的操作：卸载、数据导出、软件升级。具体的操作请点击该终端对应“查看详情”。



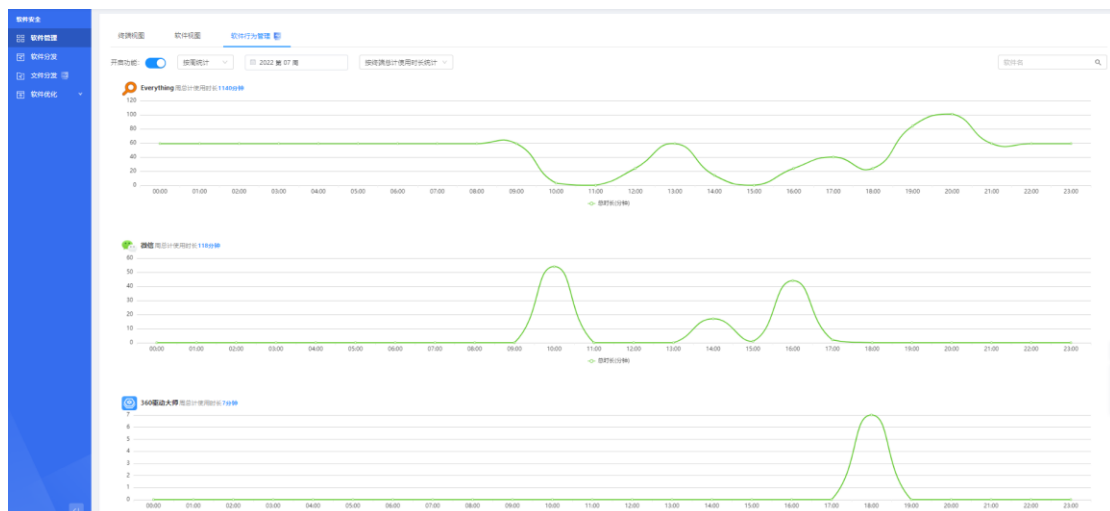
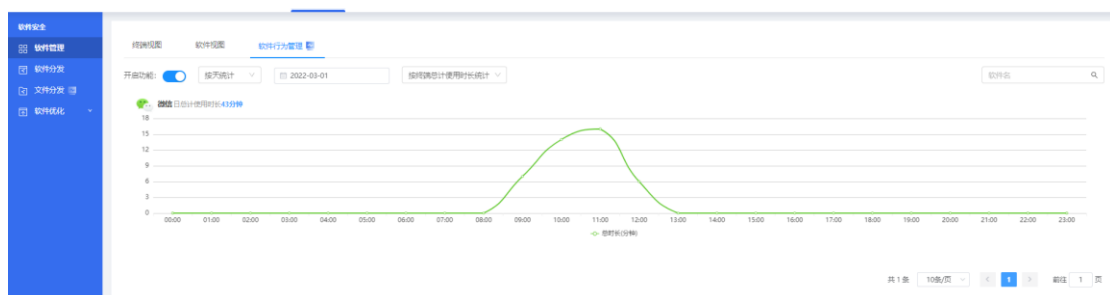


软件图标	软件名称	版本范围	已安装终端	安装率	操作
	360安全卫士	13.1.0.1001 - 13.1.0.1004	9	100 %	查看详情
	360安全卫士 网络版组件	2.0.0.1960 - 4.0.0.1001	9	100 %	查看详情
	VMware Tools	9.9.2.2495486 - 11.1.5.16724464	7	75 %	查看详情
	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4146	9.0.30729.4146	3	34 %	查看详情
	迅雷	2.5.0 - 3.2.1.154	3	34 %	查看详情
	迅雷网络版输入法	9.8.0.3746 - 11.7.0.5464	3	34 %	查看详情
	WinRAR解压软件	5.71.0 - 6.1.0.0	3	34 %	查看详情
	Microsoft Visual C++ 2017 Redistributable (x86) - 14.12.25810	14.12.25810.0	3	34 %	查看详情
	Microsoft .NET Framework 4 Client Profile	4.0.30319	3	34 %	查看详情
	Microsoft .NET Framework 4 Extended	4.0.30319	3	34 %	查看详情

➤ 软件行为管理（专业安全管理运维服务）

软件行为管理，可以按天，周针对终端进行软件使用总时长，软件使用平均时长统计。

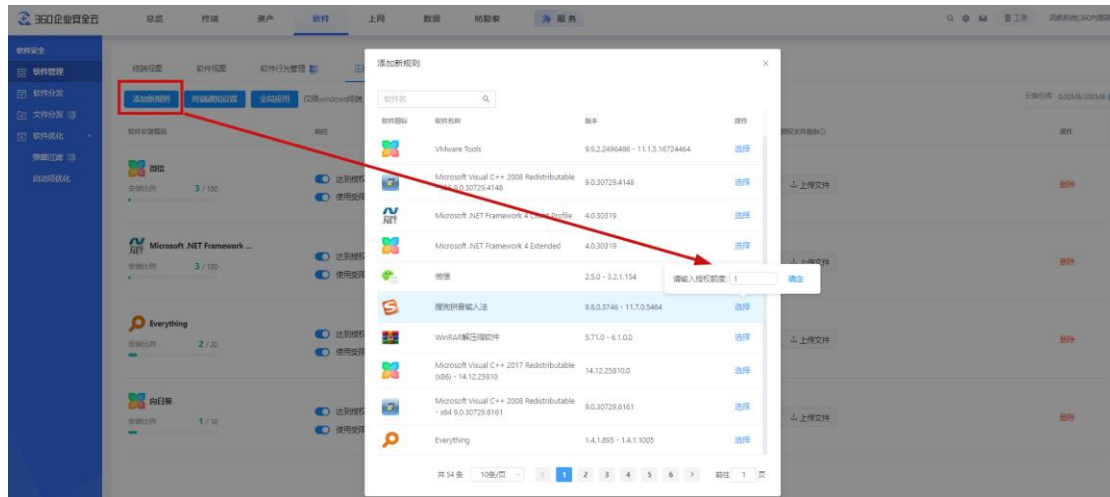
也可以统计软件使用的终端数和时间段。



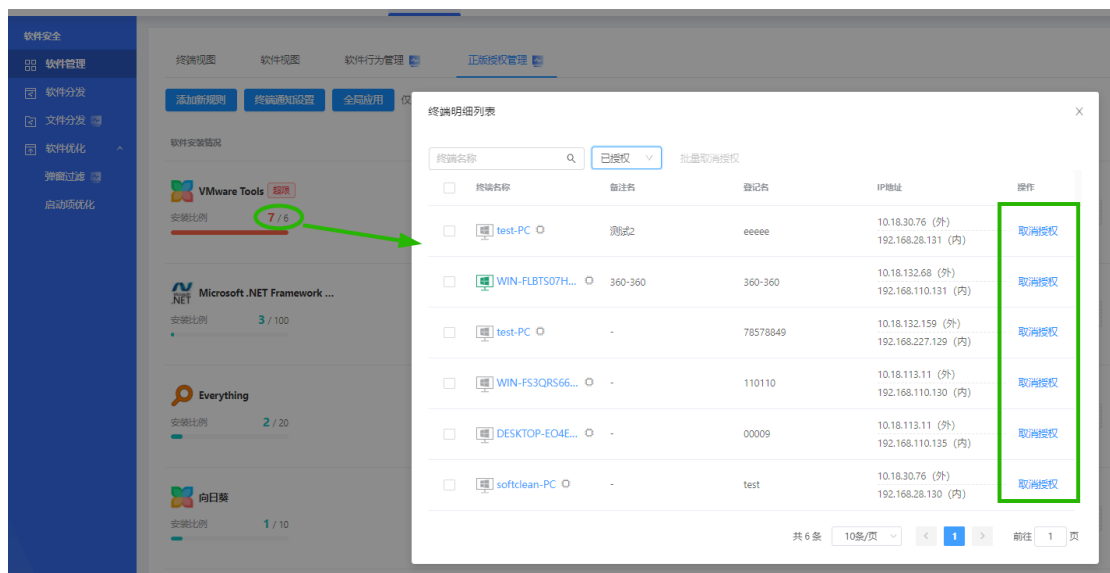
➤ 正版授权管理（专业安全管理运维服务）

此功能可以设置在终端上运行的软件，达到软件授权的数量后，剩余的终端将不能使用此

软件，有效的提高正版软件的使用率。软件使用受限时，会提醒终端用户。

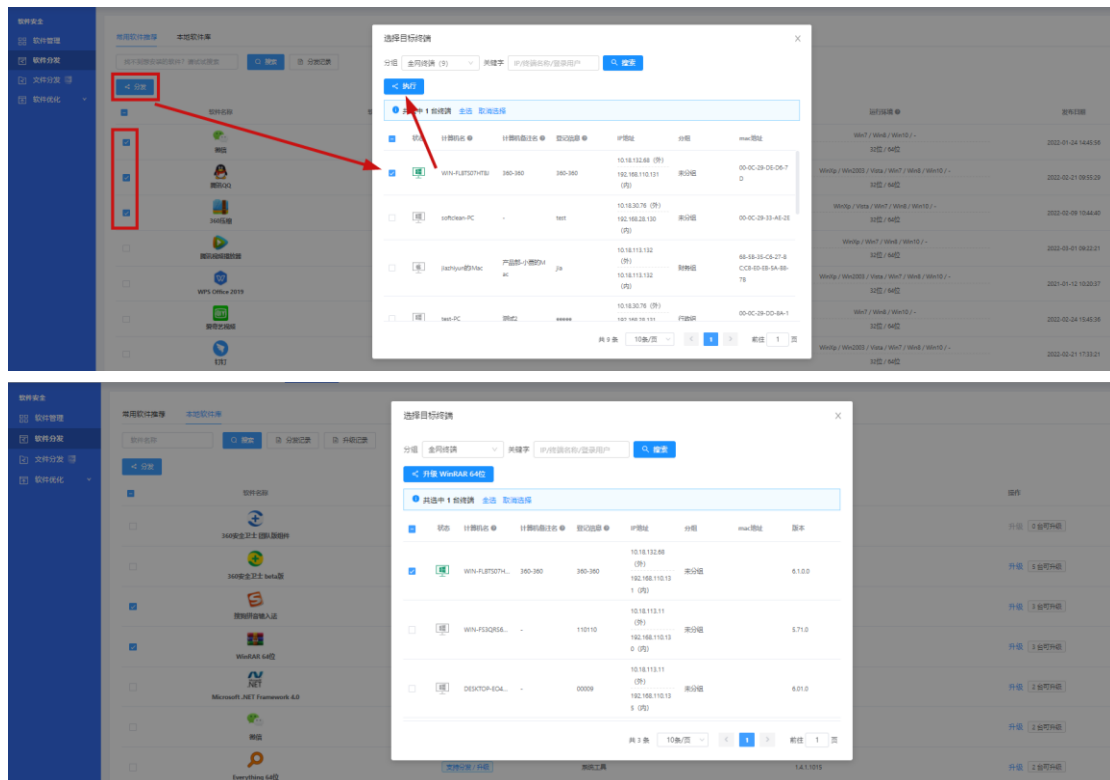


点击安装比例的数字，可以查看终端明细，进行授权和取消授权的操作。



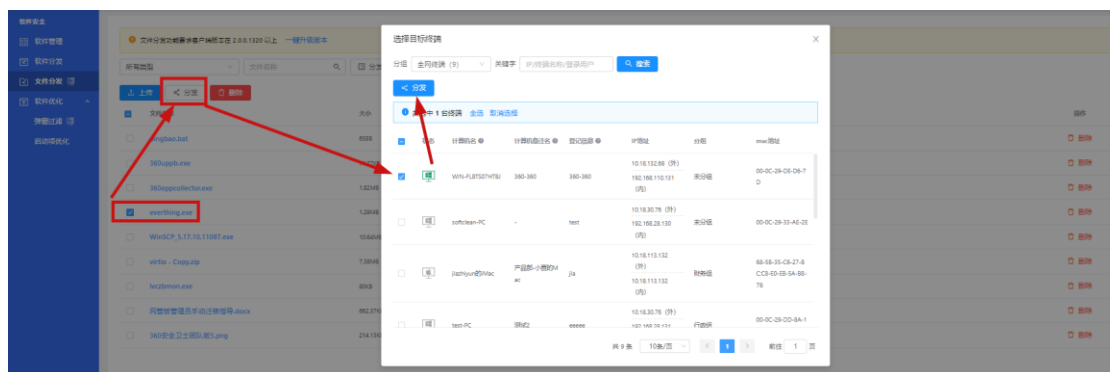
2.4.2 软件分发

软件分发顾名思义是对软件的一种分发策略。在【常用软件推荐】中，提供了部分用户常用的软件，可以直接进行分发。【本地软件库】中的软件识别是来自全网终端上安装的软件。可以对版本较低的终端进行升级。



2.4.3 文件分发（专业安全管理运维服务）

文件分发是可以分发文件、或者一些软件安装包。操作流程是先将文件上传到云服务器，然后通过云服务器进行分发，如果是安装包可以设置在终端执行。

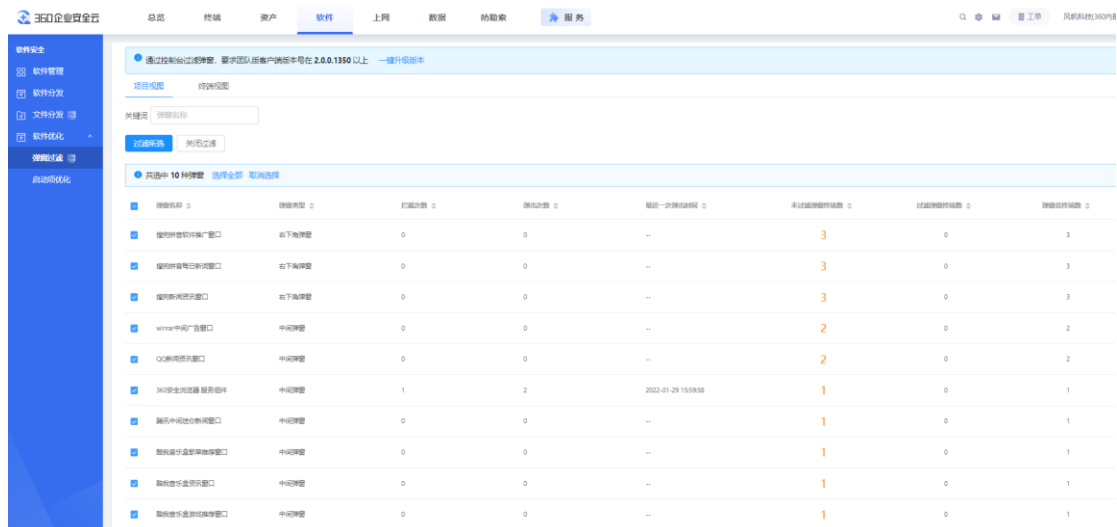


2.4.4 软件优化

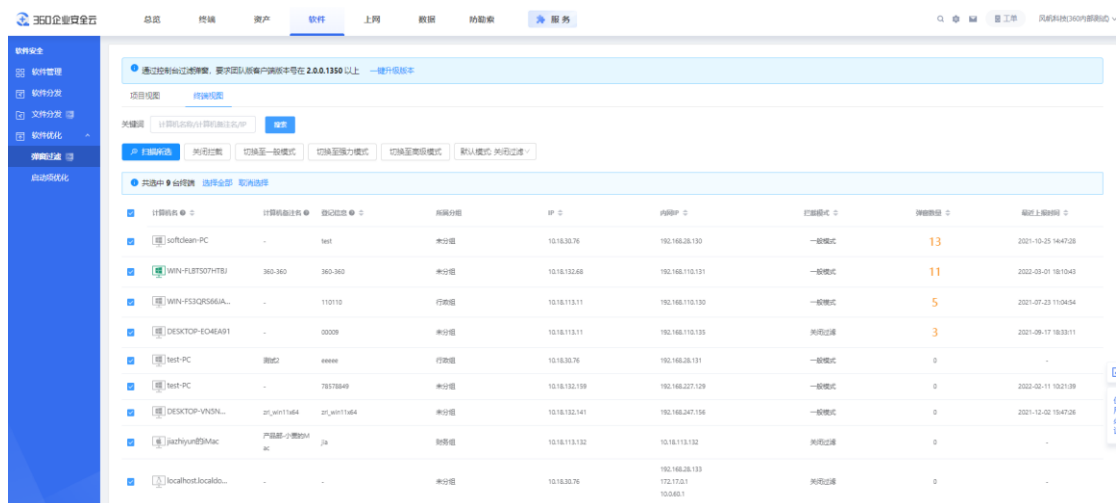
2.4.4.1 弹窗过滤（专业安全管理运维服务）

项目视图，显示目前全网终端所有弹窗的信息，可选择对某个项目开启或者关闭过滤策

略。



终端视图，可以设置全网终端的弹窗拦截策略，拦截模式分为一般模式、强力模式和高级模式，可根据不同终端实行不同拦截模式。



2.4.4.2 启动项优化

从启动项目维度具体可以查看启动项的名称、描述、类型、优化建议等，点击对应数字均可查看每个项目未优化终端和已优化终端，管理员可以按需下发优化、恢复和信任项目的指令。

名称	描述	应用名称	启动类型	运行操作	优化建议	未优化项数	已优化项数
微软Office的相片任务	用于支持微软Office的相片任务。	office相片任务.exe	计划任务	建议保留存在的项目	需94%用户优化此项目	1	0
Windows搜索索引任务	当知入新设备并计划任务后，开始索引设备数据和系统设置。	indexer.exe	计划任务	允许禁止	需93%用户优化此项目	1	0
Media Center搜索索引任务	用于媒体中心搜索索引任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需92%用户优化此项目	1	0
Media Center开放式的电视节目的播放任务	用于媒体中心开放式的电视节目的播放任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需92%用户优化此项目	4	0
Media Center开放式的电视节目的播放任务	用于媒体中心开放式的电视节目的播放任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需92%用户优化此项目	1	0
Media Center开放式的电视节目的播放任务	用于媒体中心开放式的电视节目的播放任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需92%用户优化此项目	1	0
Media Center搜索索引任务	用于媒体中心搜索索引任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需91%用户优化此项目	4	0
Media CenterPlayReady安装任务	用于媒体中心PlayReady安装任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需91%用户优化此项目	4	0
Media Center搜索索引任务	用于媒体中心搜索索引任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需91%用户优化此项目	4	0
Media Center开放式的电视节目的播放任务	用于媒体中心开放式的电视节目的播放任务，不需要启动。	mediacenter.exe	计划任务	允许禁止	需91%用户优化此项目	4	0

从终端统计维度展现各个终端活跃启动项、可优化启动项、已优化启动的数量。点击数字可以查看具体启动项目。如需即时更新，可点击【扫描上报】按钮。

名称	描述	应用名称	IP地址	未优化项数	可优化	已优化
WIN-FLTSOYHTB	360-360	360-360	未设置	0	0	2
softcan-PC	未设置	未设置	10.18.102.68 (内) 192.168.1.10.131 (内)	54	54	0
jackylin@Mac	产品部-少量部Mac	ja	10.18.113.132 (内) 10.18.113.132 (内)	0	0	0
net-PC	测试	emee	10.18.102.76 (内) 192.168.28.131 (内)	80	80	0
localhost.localdomain	未设置	未设置	10.18.102.76 (内) 192.168.28.131 (内) 172.17.0.1 (内) 192.168.1.1 (内)	0	0	0

管理员也可添加和移除全局信任项目。

名称	文件路径	启动类型
Windows Firewall (Windows防火墙服务)	C:\Windows\system32\mpssvc.dll	服务

2.5 上网

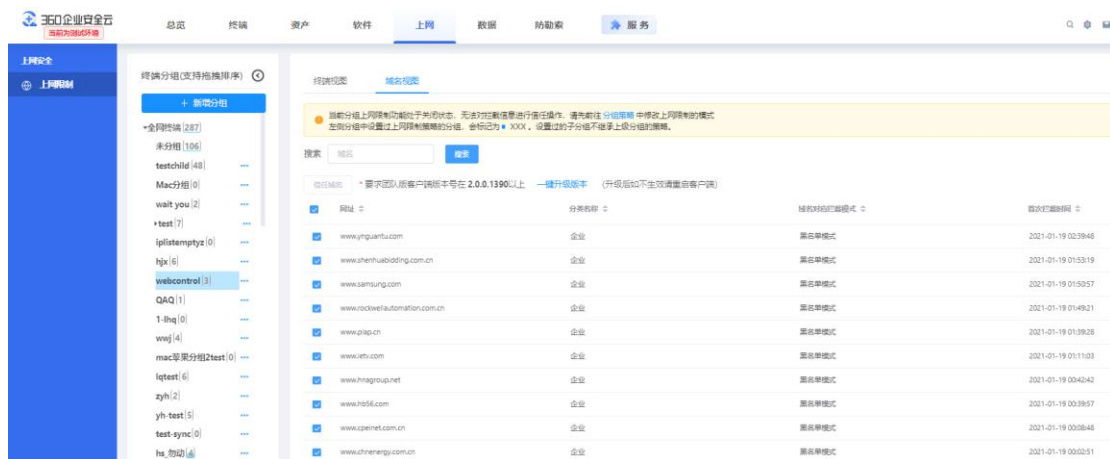
2.5.1 上网限制

上网限制功能主要有黑名单和白名单两种策略，在此页面中，可以查看到具体终端受到域

名拦截的次数。



也可按域名展示，查看已设置域名的规则和具体域名是什么。



2.6 数据

2.6.1 屏幕水印（专业安全管理运维服务）

开启屏幕水印，将在终端屏幕顶层覆盖自定义信息，可以追溯截图来源，实现版权保护。



2.6.2 安全设置（专业安全管理运维服务）

开启屏幕锁屏，所选分组终端将在无人使用时定时自动锁屏，可节省电费、延迟设备使用寿命，保护企业电脑隐私安全，防止他人偷偷获取或修改企业重要数据。

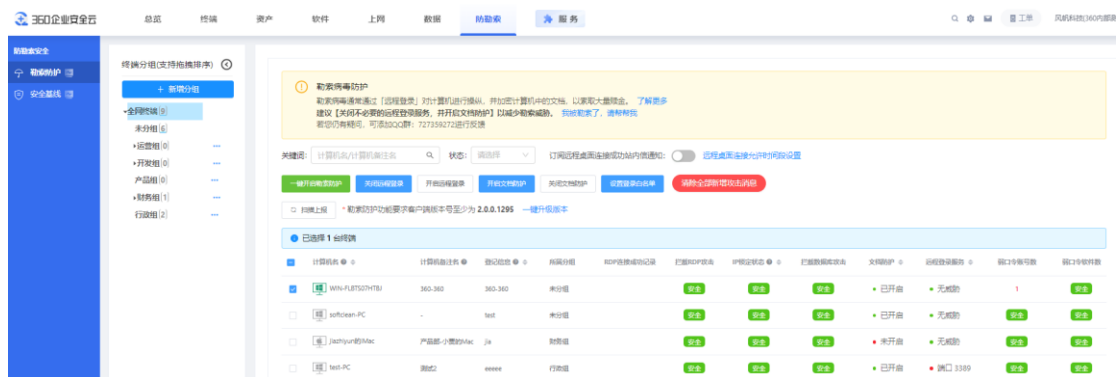


2.7 防勒索

2.7.1 勒索防护（专业安全管理运维服务）

管理员可查看电脑的防护状态：文档防护状态，远程登录服务端口的状态，拦截 RDP 攻击

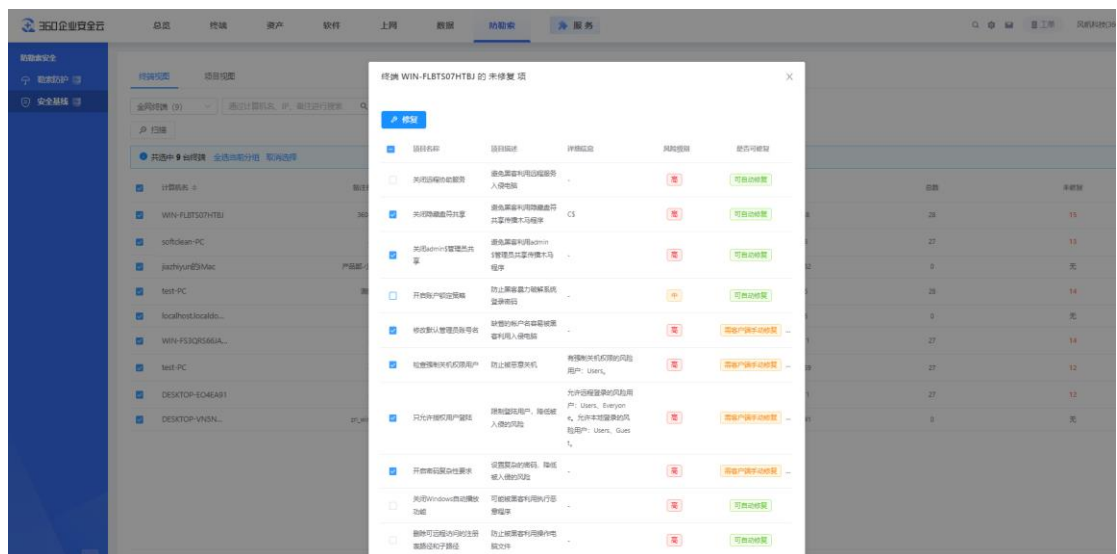
次数，IP 锁定状态，拦截数据库攻击次数，弱口令账号数，弱口令账号软件等。情动一键批量开启或关闭远程登录，文档防护功能，以避免勒索病毒加密电脑中的重要文档。也可在【终端】-【分组策略】-【勒索防护】对允许远程桌面连接的时间进行设置。



2.7.2 安全基线（专业安全管理运维服务）

安全基线检查有助于用户一键获知全网终端安全基线配置详情，找出不符合安全管理规范的主机，节省大量人工检查时间，并能持续进行监控。

此功能需要在【终端】-【分组策略】-【安全基线】中进行功能开启和配置。



2.8 服务

服务模块将展示您已订阅的服务和服务市场，您可以在此页面看到订阅详情和服务内容。

已订阅服务

 **【助力产业数字化】全面安全守护服务** 长期有效

获赠特权 ?

使用中

剩余时长 长期有效

服务版本 -

终端数量 不限制

长期有效

 **【助力产业数字化】通用云存储服务** 长期有效

 **专业安全管理运维服务** 剩余285天

为助力产业数字化，【全面安全守护服务】和【通用云存储服务】可永久免费使用，不限制终端数量，【专业安全管理运维服务】可选择购买。

点击相应服务即可查看具体服务内容。

服务市场



数字化团队



【助力产业数字化】全面安全防护服务

#QIHU0001

0使用门檻的终端安全防护与管理服务，安全大脑接入，为数字化建设保驾护航

¥ 0 / 终端 / 年 原价¥60

已订阅



【助力产业数字化】通用云存储服务

#QIHU0002

1GB云存储空间，应用于数字卫士中各功能的数据存储

¥ 0 / 终端 / 年 原价¥19

已订阅

通用安全团队



专业安全管理运维服务

#QIHU0101

专业而易用的深度管理与安全策略配置，覆盖更多企业级场景化需求

¥ 60 / 终端 / 年 原价¥199

已订阅

2.9 页眉功能导航

2.9.1 关键字搜索

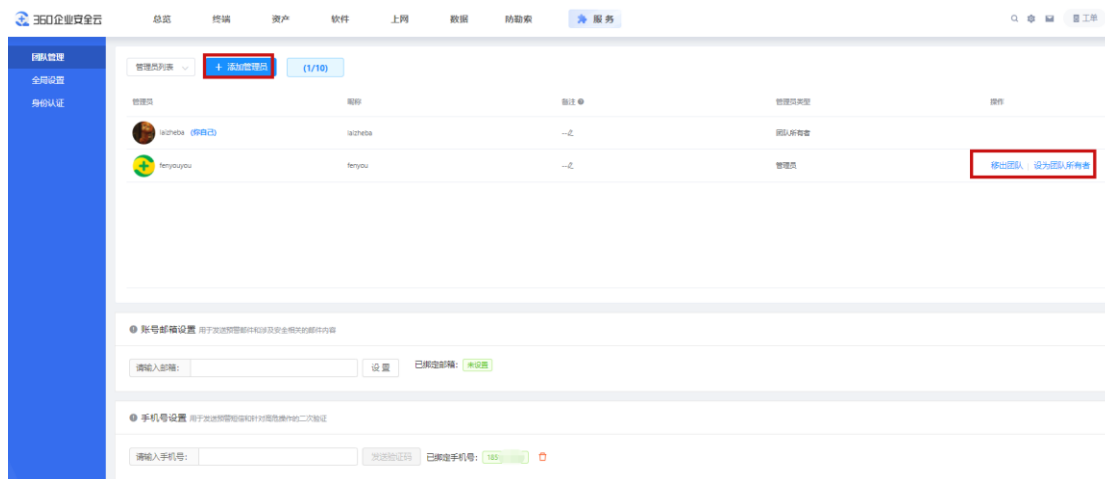
根据您需要的具体功能，可以查询跳转到对应的功能页面，比如搜索：“木马查杀”、“体检”、“软件分发”、“弹窗过滤”等关键字进行页面跳转。



2.9.2 设置

2.9.2.1 团队管理

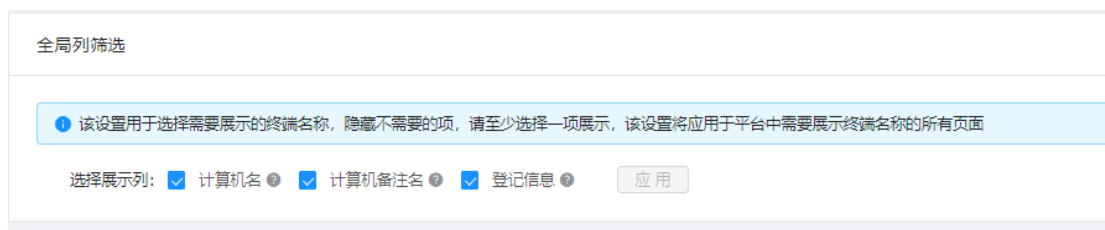
支持添加管理员，转移权限，设置新的账号所有者，绑定和设置用于接收预警邮件及安全相关邮件内容的邮箱和手机号码。



2.9.2.2 全局设置

➤ 全局列筛选

该设置用于选择需要展示的终端名称，隐藏不需要的项，请至少选择一项展示，该设置将应用于平台中需要展示终端名称的所有页面



➤ 通知推送设置

平台为您提供全方位的终端信息同步，方便您第一时间掌握终端现状以实现及时的安全管控需要，通知均可关闭，可按照需要设置

2.9.2.3 身份认证

购买付费服务、开具产品授权声明需要进行身份认证，个人、企业认证后均可获得产品授权声明，未进行企业认证时购买的订单，不能开具增值税专用发票。

购买付费服务、开具产品授权声明需要进行身份认证

个人、企业认证后均可获得产品授权声明。未进行企业认证时购买的订单，仅能开具个人抬头发票。



2.9.3 站内信

2.9.3.1 站内消息

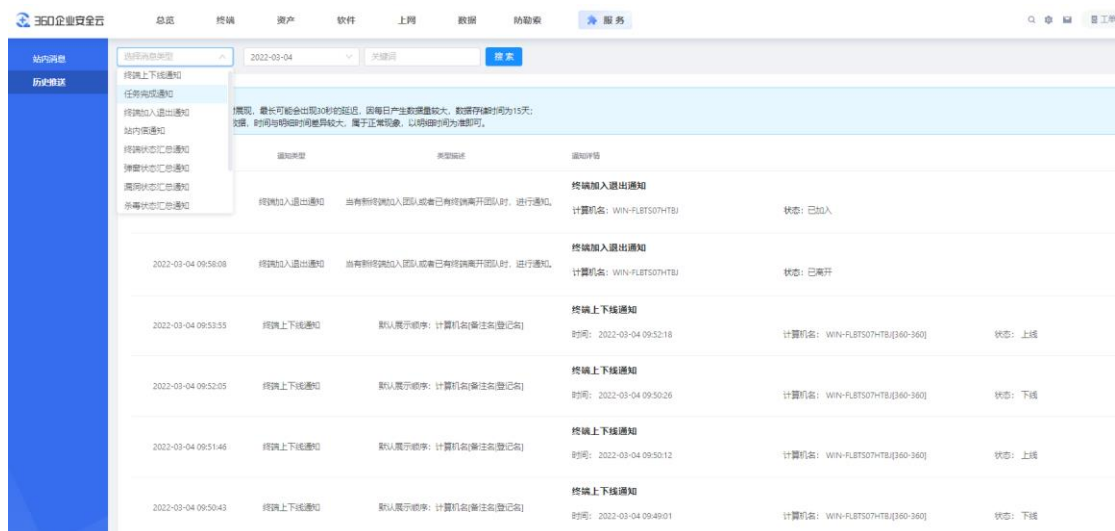
360 企业安全云的公告、通知、预警信息、壁纸和 logo 审核结果等都会通过站内消息发送给管理员，记录在此。



2.9.3.2 历史推送

管理员可查看终端上下线通知，任务完成通知，终端加入退出等通知，

需注意的是：历史推送数据非实时展现，最长可能会出现 30 秒的延迟，因每日产生数据量较大，数据存储时间为 15 天。

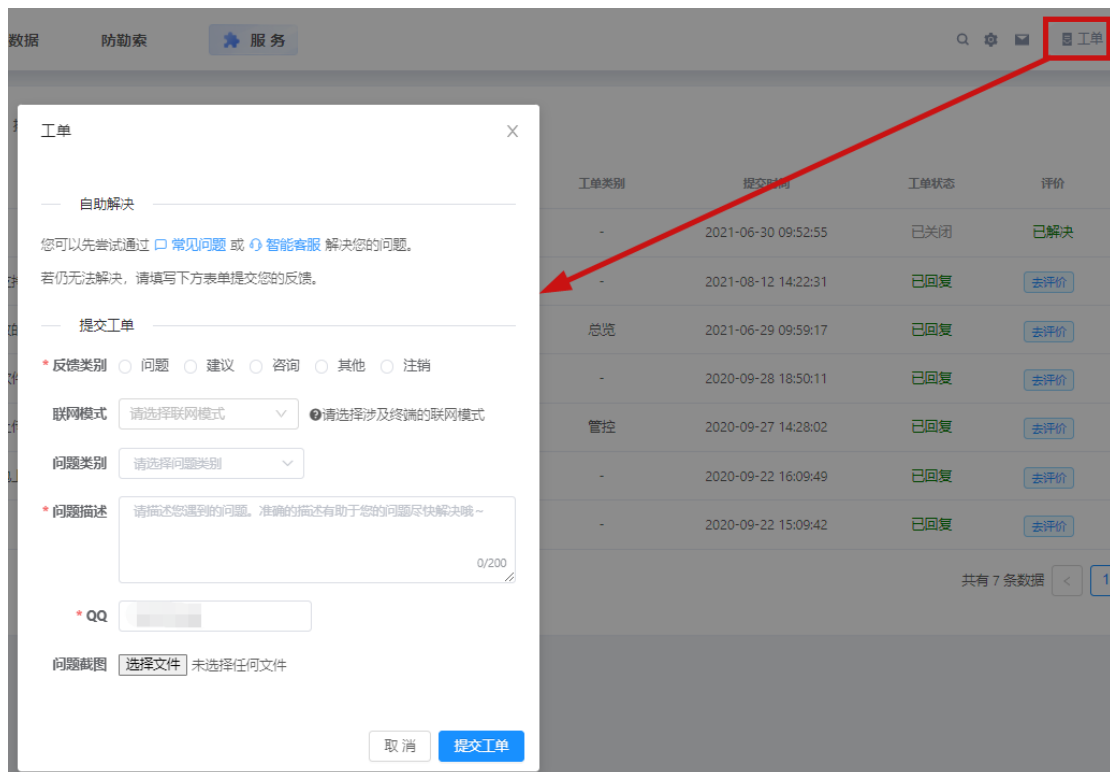


2.9.4 工单系统

2.9.4.1 提交工单

如果您在安装和使用 360 企业安全云的过程中有什么问题或者建议，欢迎通过【提交工单】

反馈给我们，点击“提交工单”即可选择相应的问题分类，客服人员收到您的反馈会第一时间回复或与您取得联系核实问题。

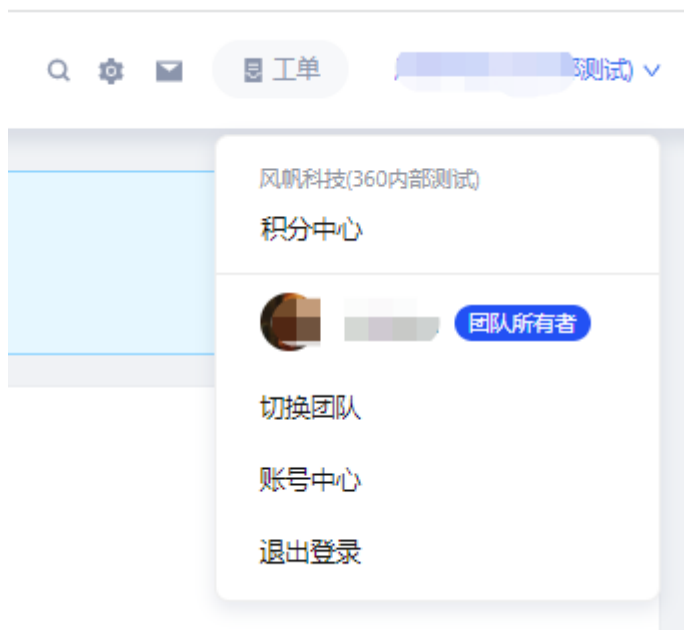


2.9.4.2 历史工单

工单列表展示的是您曾经提交过的工单，可以在次查看客服人员给您的回复或者继续追问。

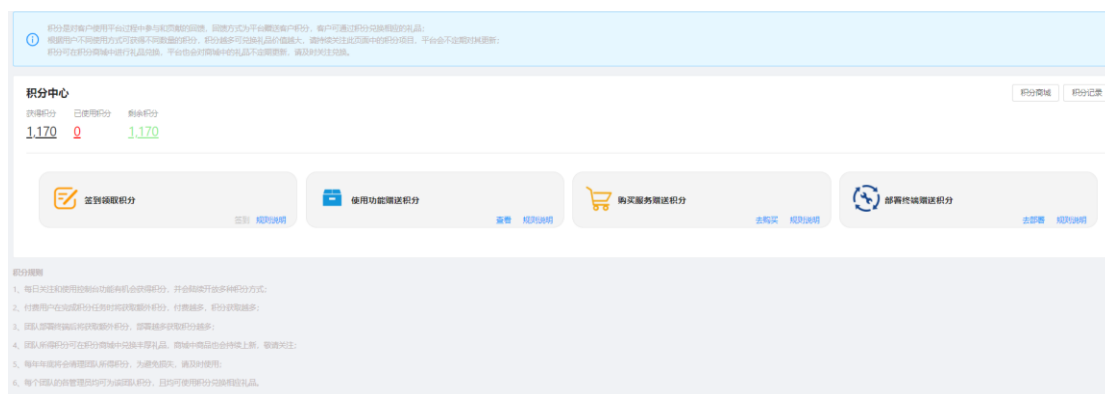


2.9.5 账号设置



2.9.5.1 积分中心

积分是对用户使用平台过程中参与和贡献的回馈，回馈方式为平台赠送用户积分，根据用户不同使用方式可获得不同数量的积分，积分越多可兑换礼品的金额越大。请用户关注此页面上的积分项目，平台会不定期对积分进行兑换。



2.9.5.2 切换团队

同一个账号下可以创建多个企业团队，比如既有收费版本，又有免费版本的企业；一个集团下面多个子公司的企业，更方便管理。

切换团队

X



2.9.5.3 账号中心

可以对账号的绑定手机号码、邮箱、登录密码进行修改。

[首页](#)[帐号安全](#)[帐号信息](#)[修改昵称](#)[签到](#)**最近一次登录:**

2022年03月04日 09:45 局域网

常用操作

**登录密码**定期修改密码，能提高帐号安全 [修改等级](#)**登录邮箱**

j****@m

[验证](#)**绑定手机:**

185****

[修改](#)**帐号卫士:**

未绑定

[绑定](#)

2.9.5.4 退出登录

退出登录即可回到 360 企业安全云管理后台的登录页面。



3、客户端主要功能简介

3.1 首页体检

体检为电脑进行从病毒木马、高危漏洞、系统异常、电脑垃圾、电脑速度等方面的安全性快速检测，解读安全性能，指引快速修复，帮助用户保持电脑健康。

打开 360 企业安全云，会直接展现体检主界面，点击“立即体检”开始体检。



扫描完成, 会展现电脑健康得分与电脑当前存在的问题, 并提供解决方案, 点击“一键修复”即可。



3.2 木马查杀

全球领先的云查杀技术, 加上立体的主动防御系统和人工智能查杀引擎, 第一时间拦截查杀

最新木马。

查杀方式分为快速查杀，全盘查杀和按位置查杀，用户可以自由选择查杀类型。



3.3 系统安全

修补电脑漏洞，修复系统故障，及时更新补丁和驱动，确保电脑安全。修复方式分为全面修复和单项修复，用户可按需选择。



扫描完成，会将可修复项分类展现，点击“一键修复”即可修复完成。



3.4 网络安全

保护网络安全，杜绝网络隐患，解决网络信号差。



3.5 数据安全

保障数据安全，解决文档被勒索、篡改的问题。



3.6 优化加速

清理电脑垃圾，全面优化电脑性能，轻装运行。



3.7 安全大脑

直观感受 360 安全大脑单日实时数据概览，也可将本地风险文件上传进行分析



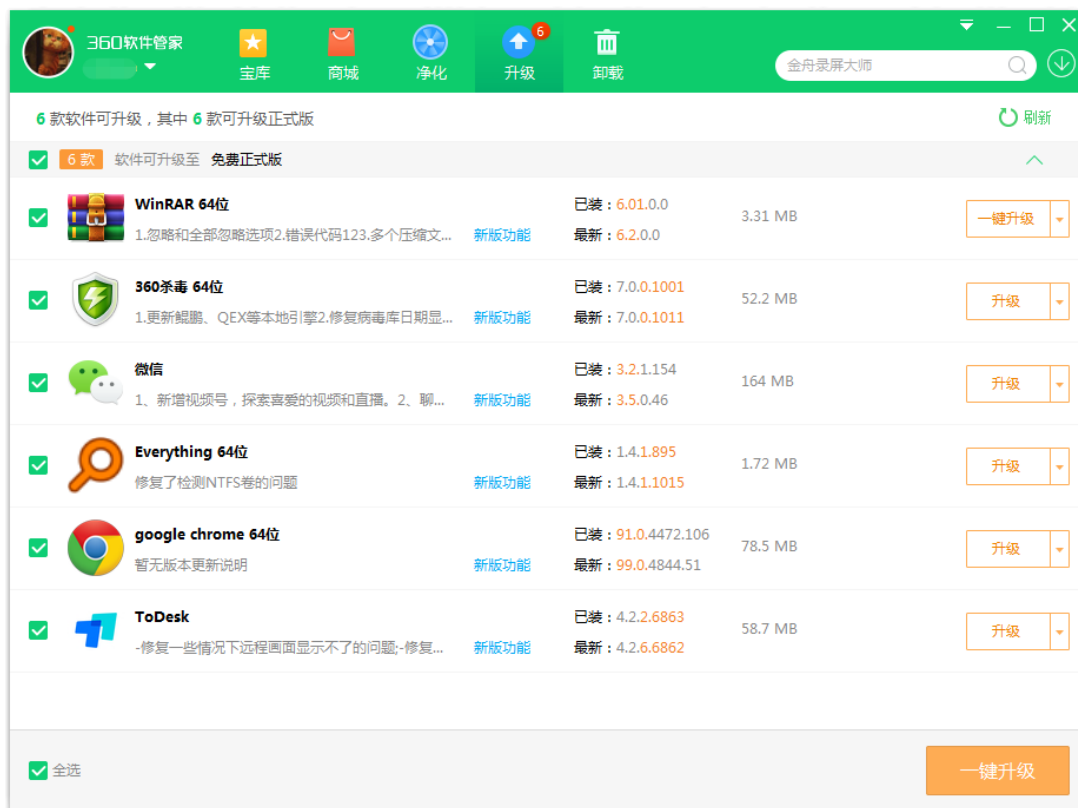
3.8 软件管家

软件管家为用户提供海量的正版软件的高速安全下载服务。

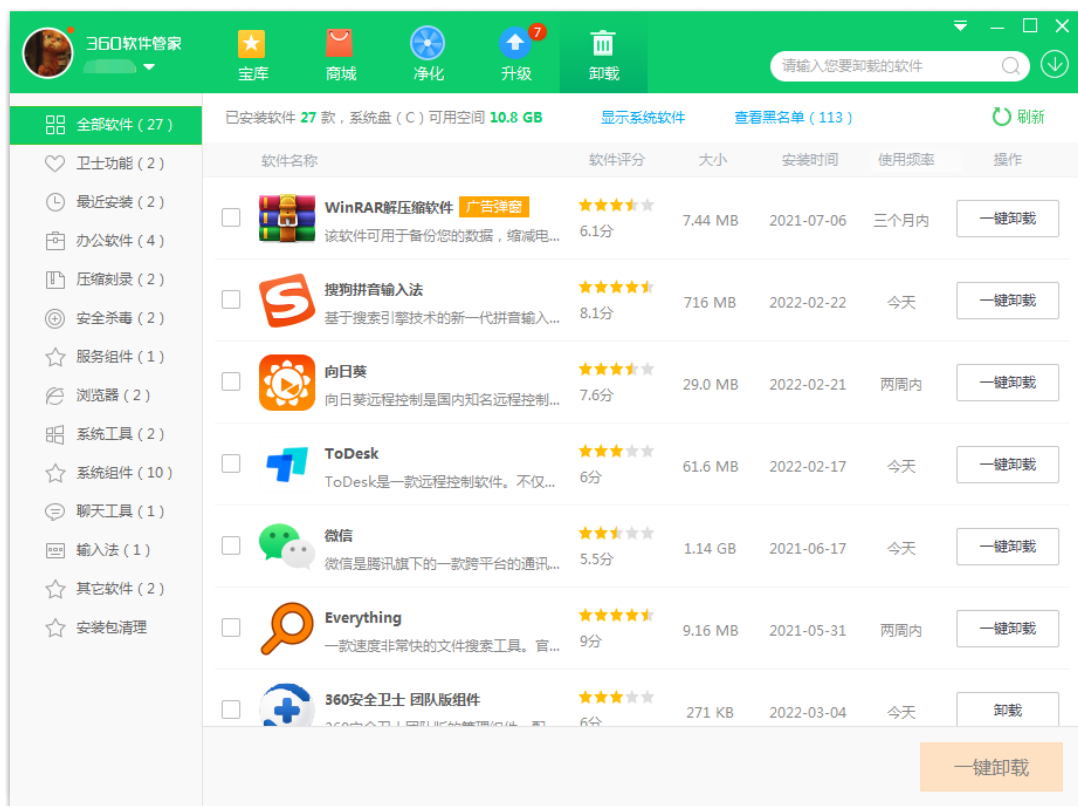
用户可以通过左侧分类导航或者搜索功能快速定位到所需软件，点击“一键安装”即可。



点击软件管家主界面上的“升级”界面，可为用户提供可升级软件的详细更新信息，用户可点击“一键升级”对软件进行升级。



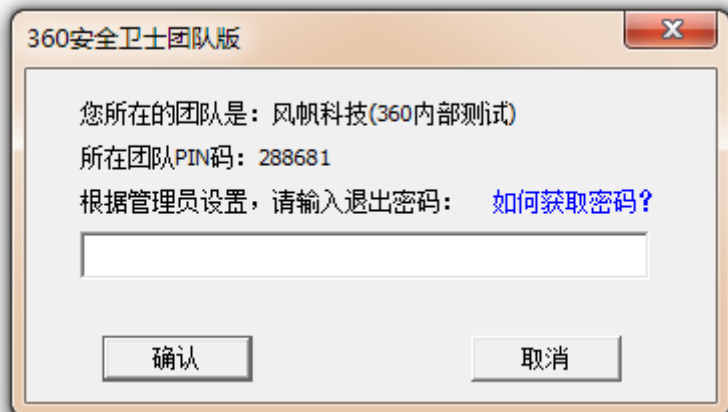
点击软件管家主界面上的“卸载”界面,用户可以通过左侧分类导航或者搜索功能快速定位到需要卸载的软件,点击“一键卸载”即可卸载。



4、客户端退出、卸载

4.1 退出

已加入企业组织的终端,如果想在本地退出,需要输入退出密码,密码需要联系管理员获取。

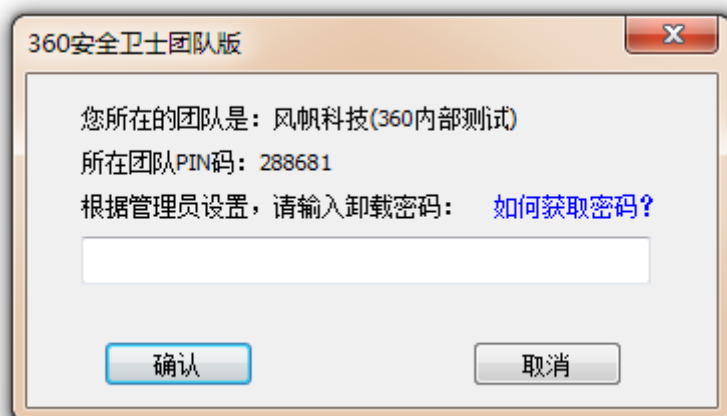


输入正确的退出密码后，可进入正常退出的流程。



4.2 卸载

已加入企业组织的终端，如果想在本地卸载，需要输入卸载密码，密码需要联系管理员获取。



输入正确的卸载密码后，可进入正常的卸载流程。

