火绒安全
HUORONG SECURITY

企业版

火绒终端安全管理系统 2.0

产品使用说明 >>>

2025/7/2

公　　司：北京火绒网络科技有限公司

地　　址：北京市朝阳区北苑路北京文化创意大厦 B 座 9 层

网　　址：https://www.huorong.cn

电　　话：400-998-3555

版权声明

目录 | CONTENTS

第一章 概述

欢迎阅读《“火绒终端安全管理系统 2.0”产品说明书》。为了能够更好地服务于用户，特别编写本手册。本文件分为“控制中心”、“安全终端”两部分，其中对各个模块的功能及操作步骤逐一进行了全面、详实的介绍。可帮助管理员了解并掌握终端及控制中心的使用方法。

“火绒终端安全管理系统 2.0”是秉承“情报驱动安全”新理念，全面实施 EDR 运营体系的新一代企事业单位反病毒&终端安全软件。本产品能帮助用户完成终端安全软件的统一部署、全网管控，集强大的终端防护能力和丰富方便的全网管控功能于一体，性能卓越、轻巧干净，可以充分满足企事业单位用户在目前互联网威胁环境下的电脑终端防护需求。

“火绒终端安全管理系统 2.0”产品优势及特点：

自主知识产权，适合国内用户。拥有自主知识产权和全部核心技术，可避免产品后门和敏感信息外泄等隐患。能够及时响应本地安全问题，迅速处理国产木马和流氓软件，同时具有沟通、处理时间短等优势。对国内安全问题的特殊性有深刻认知，除了反病毒、反黑客，更能有效防范商业软件侵权和国内病毒产业链。

全网威胁感知，EDR 运营体系。火绒安全秉承“情报驱动安全”理念，建立了 EDR 运营体系。EDR 运营体系以全网数百万“火绒安全软件”终端为探针，实时感知全网威胁信息。前端截获、预处理各种未知威胁后，交由后端进一步深度分析、处理，产出高价值威胁情报，以此升级产品和服务，真正做到实时感知、动态防御。

成熟的终端，强悍而轻巧。火绒终端产品稳定成熟，运营和服务经验丰富，已拥有数百万用户。其独有的基于虚拟沙盒的新一代反病毒引擎及多层次主动防御系统，可确保对各种恶意软件的彻底查杀和严密防御。安装后占用资源少，日常内存占用不到 10M，平常使用中，几乎感觉不到火绒的存在。同时坚决恪

守安全厂商的基本操守，没有任何捆绑、弹窗、侵占资源等行为，并强力狙杀各种流氓软件、商业软件的侵权行为。

高效的控制中心，可靠、易用。本产品拥有强大、高效的终端管理功能，统一部署、集中管理，将单位网络纳入严密的防控之中，确保安全无死角，每个终端的安全防御状况都能轻松掌握。基于对企事业单位用户的深刻理解，“火绒终端安全管理系统 2.0”的控制中心设计合理，拥有友好的界面、人性化的统计报表，安全管理信息和日志一目了然，能极大的提高安全管理效率。

第二章 火绒终端安全管理系统-控制中心

2.1 访问控制中心

火绒终端安全管理系统访问控制中心可通过以下两种方式：

1. 快捷方式访问：

火绒终端安全管理系统安装完成后，会自动创建名为“火绒终端安全控制中心”的桌面快捷方式，鼠标双击快捷方式即可通过系统默认浏览器访问控制中心。

2. 地址+端口访问：

火绒终端安全管理系统控制中心可通过浏览器地址+端口访问，在浏览器地址栏中输入：http(s)://[控制中心所在 IP 地址或者域名]:[中心管理端口]，即可访问控制中心。

2.2 控制中心登录与登出

2.2.1 控制中心登录

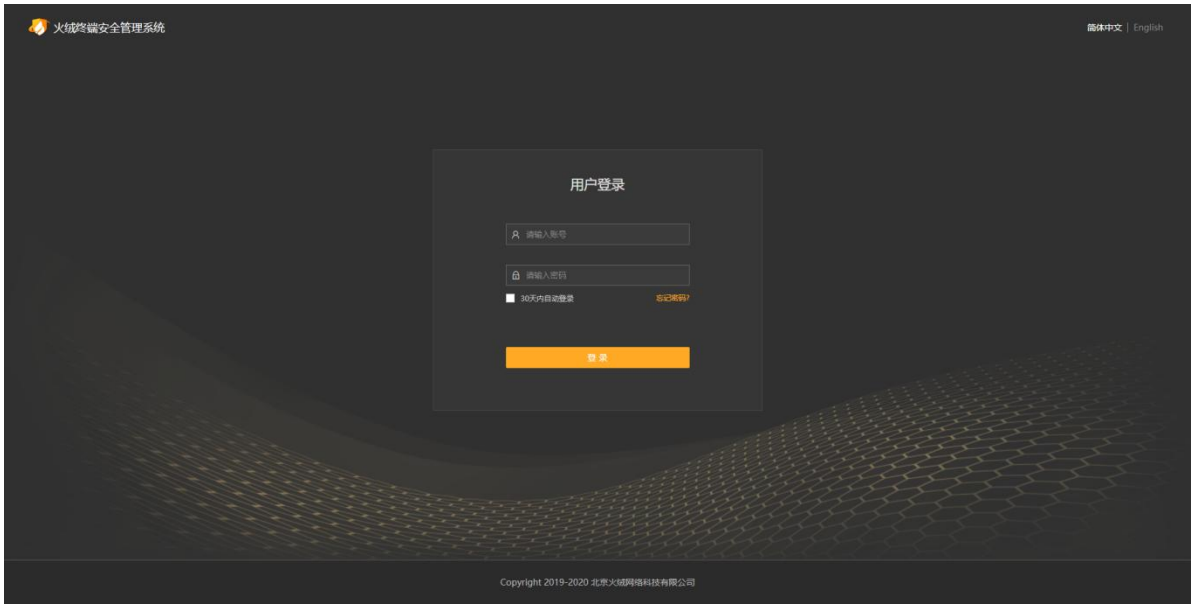
火绒终端安全管理系统登录需要正确输入管理员账号和密码，用户点击下方【登录】按钮即可登录控制中心。

注：

1. 密码输入错误 5 次后，将会在 15 分钟之内限制登录。
2. 登录之后如果 5 分钟之内没有进行任何数据操作，将会自动登出。
3. 超级管理员默认账号：admin 默认密码：admin

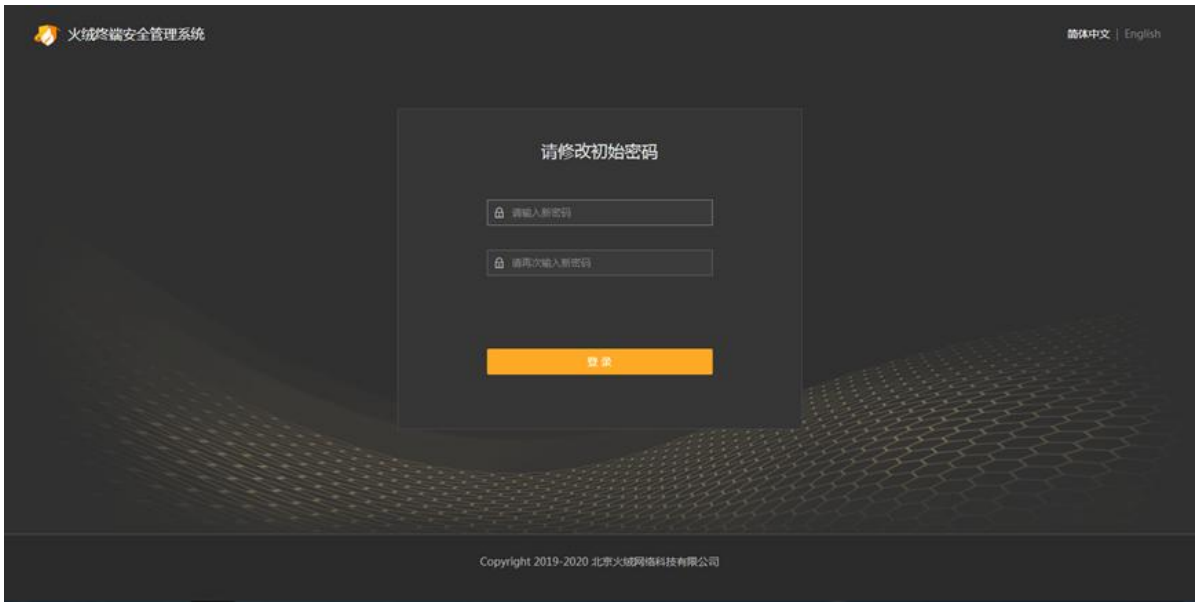
30 天内自动登录：用户登录控制中心时可选择勾选此项，勾选项选中代表用户登录成功后，30 个自然日内再次访问控制中心不需要登录验证，可自动登录控制中心；勾选项未选中，下次访问控制中心时需要重新输入管理员账号和密码进行登录验证。

忘记密码：用户点击忘记密码时，系统会弹出忘记密码解决办法提示框，用户可根据自身用户属性，对应寻找解决办法。



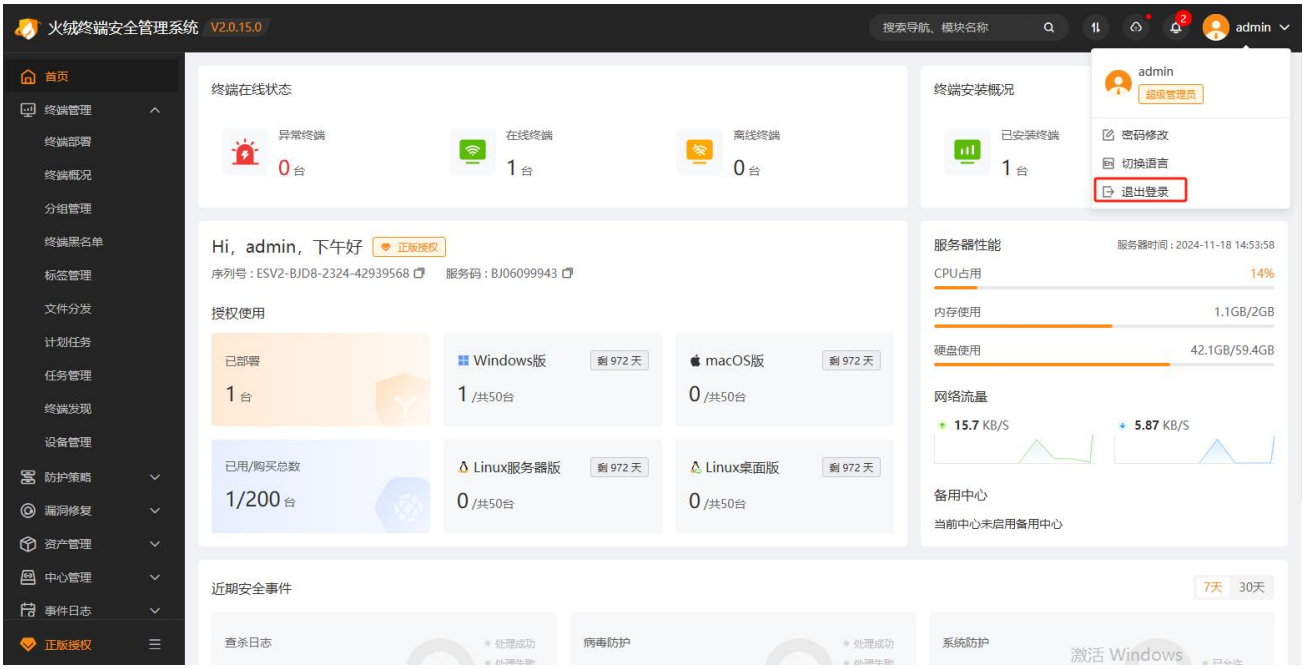
超级管理员首次登录时会强制用户修改弱口令密码，持续使用弱口令存在较大的安全风险，因此首次登录时强制修改的密码需要具备一定的复杂度规则，即密码必须由 8-32 位大小写字母、数字、特殊字符组

成，否则不允许登录控制中心，密码修改完成后会使用修改成功后的密码口令自动登录控制中心。



2.2.2 控制中心登出

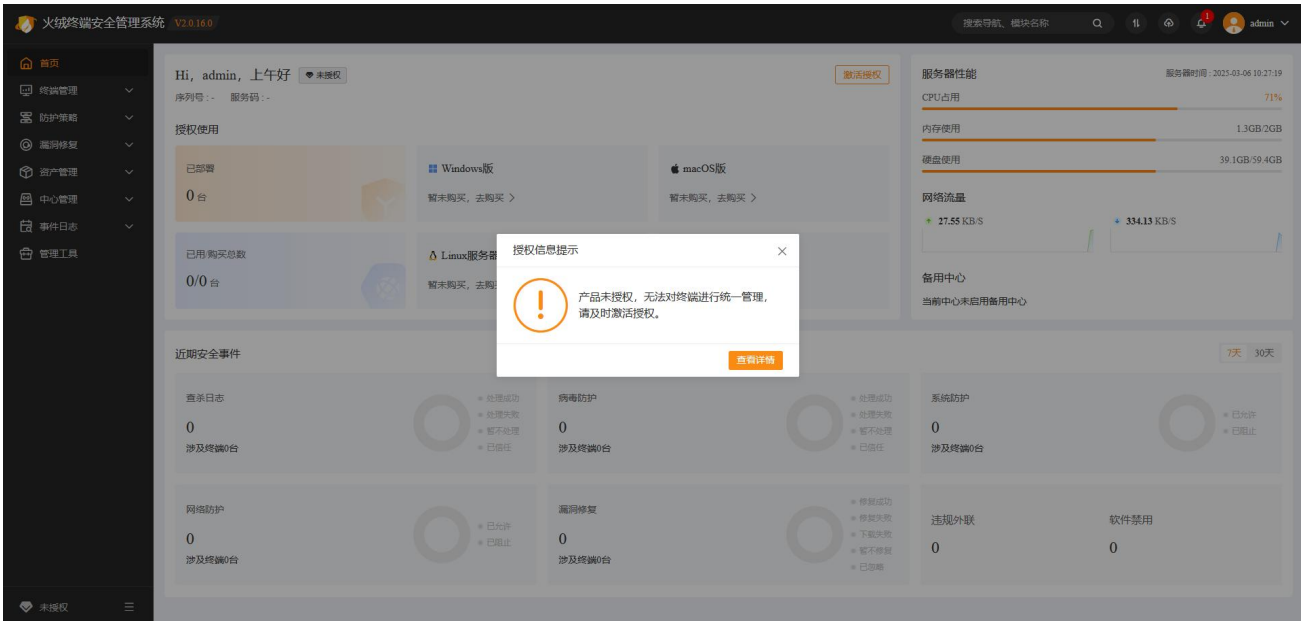
火绒终端安全管理系统控制中心登录成功后可手动登出，用户点击控制中心界面右上角管理员图标可出现下拉操作选项，鼠标单击【退出登录】按钮即可登出控制中心，返回管理员登录界面。



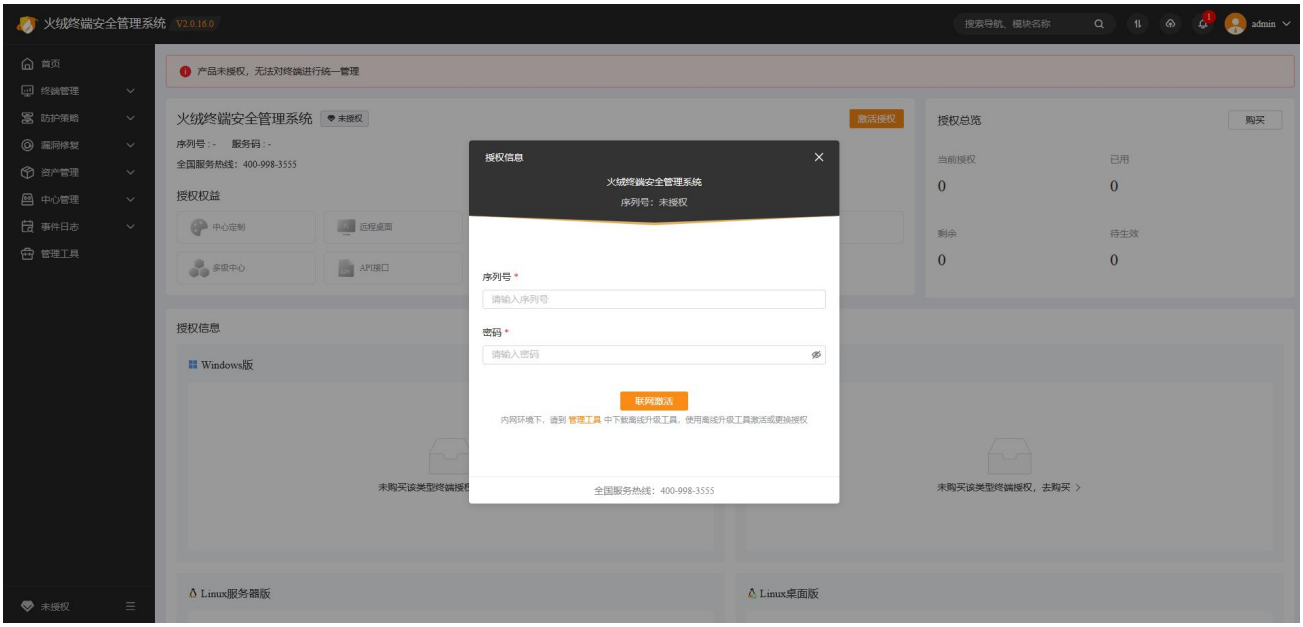
2.3 基础功能

2.3.1 授权管理

火绒终端安全管理系统部署完成后，首次访问控制中心，由于系统未授权，控制中心界面会自动弹出授权信息弹框，用户手动点击页面左下角授权状态图标及文字也可打开授权信息弹框；

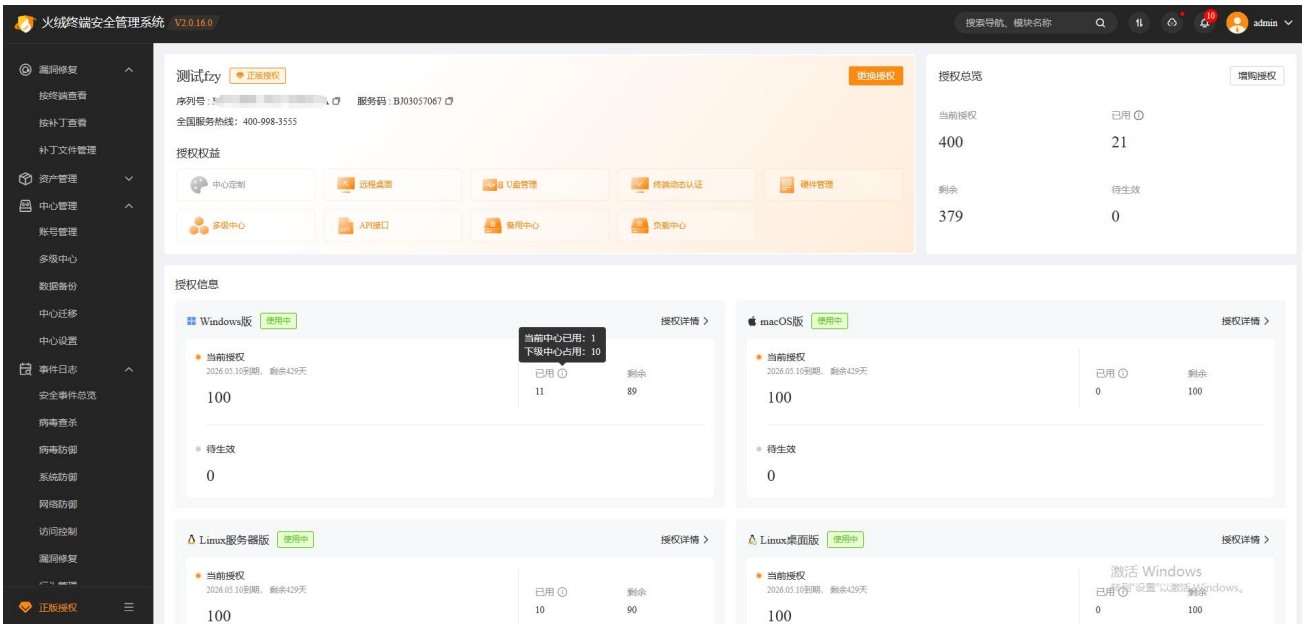


鼠标单击【查看详情】按钮时，进入授权详情界面。输入火绒提供的序列号及密码后，点击【联网激活】按钮系统自动进行联网验证，验证通过后即可成功激活授权。授权激活后鼠标单击【更换授权】按钮，输入火绒提供的新序列号及密码，可更换新的授权。

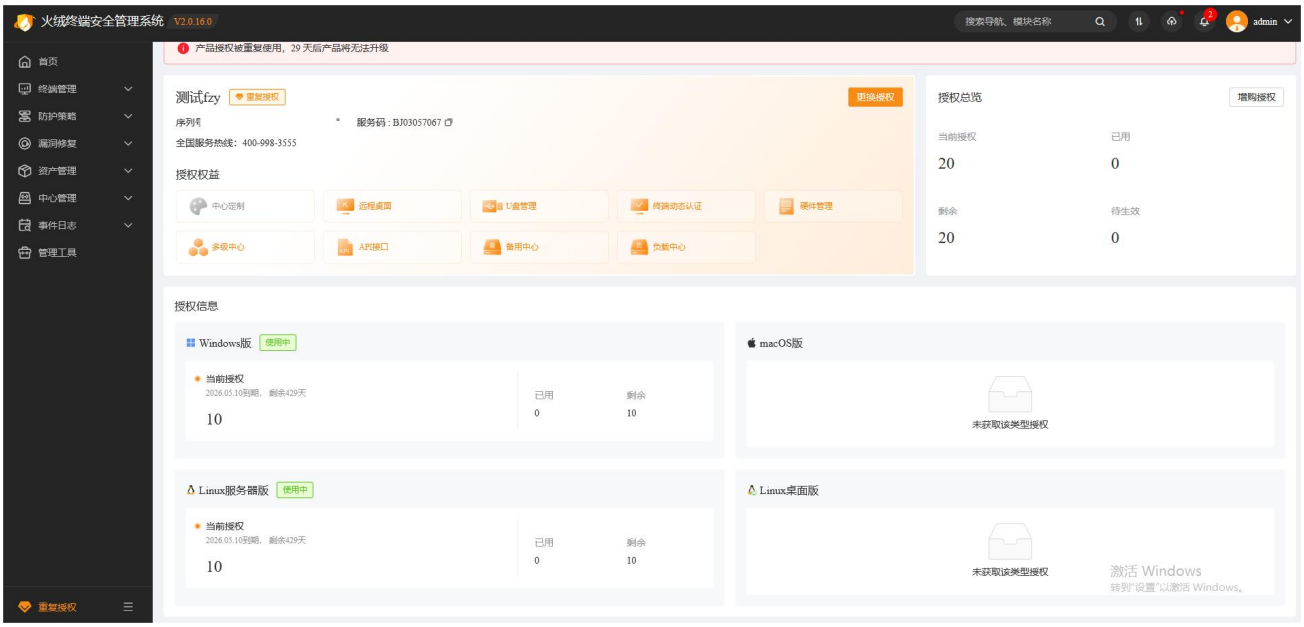


授权页可查看不同类型终端授权的使用状态和详细信息，如可查看 Windows 类型终端的当前授权购买点数，及当前购买的点数中已用和剩余的点数信息；如果您已续购，但还未到续购授权的开始日期时，可在【待生效】位置查看到续购的授权点数，更多的授权信息信息可点击【授权详情】查看。

存在下级中心时，鼠标悬浮【已用】，可查看到下级中心占用的点数信息。

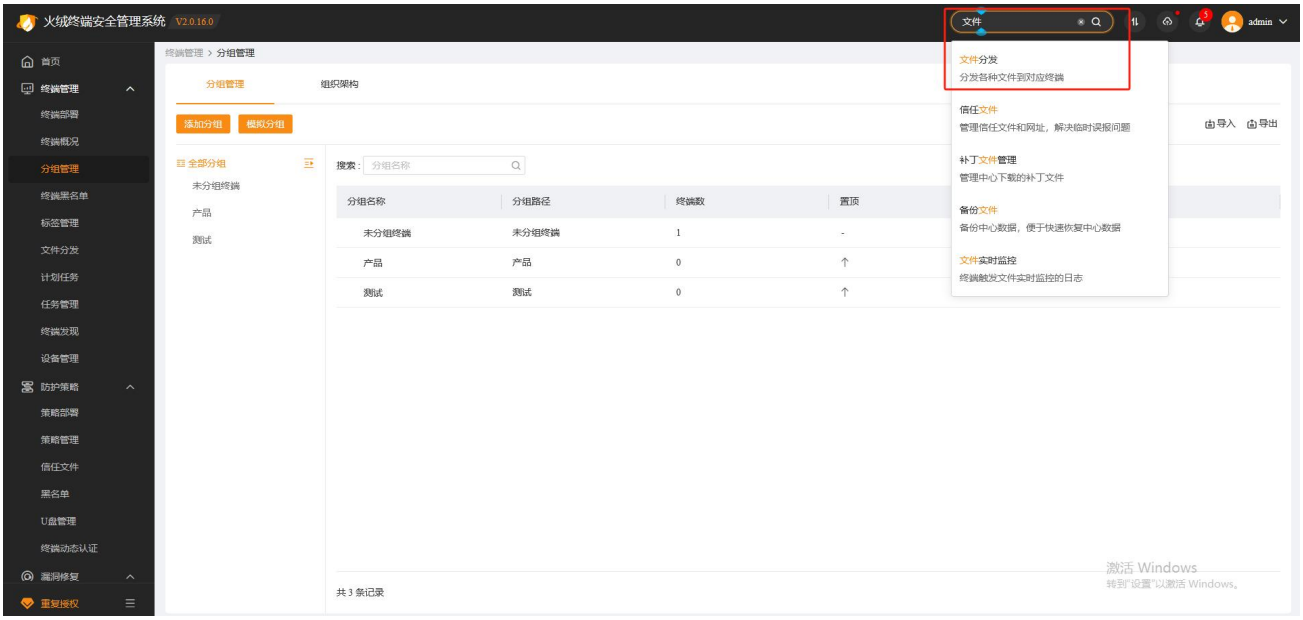


上级中心【自定义分配】或【动态分配】授权的下级中心的授权页，仅显示当前的授权信息，下级中心不会显示待生效的授权信息。



2.3.2 搜索

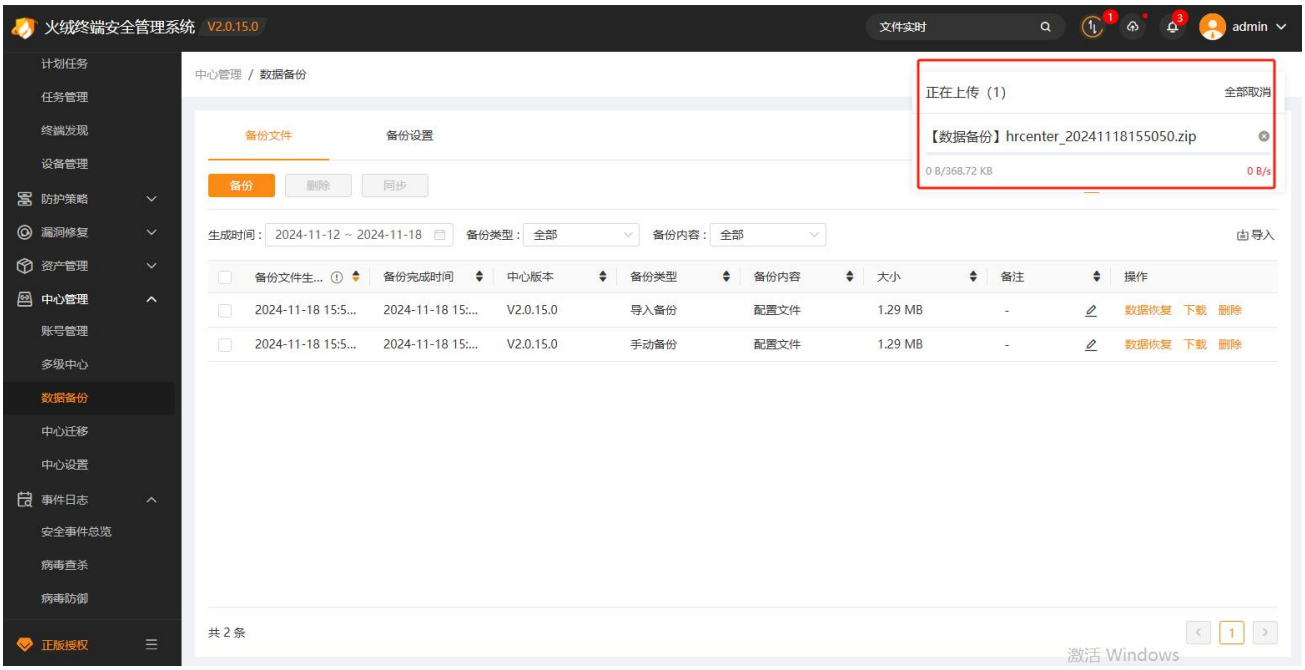
火绒终端安全管理系统控制中心提供了快速定位导航和模块的功能，帮助用户快速跳转到目标页面。



2.3.3 导入

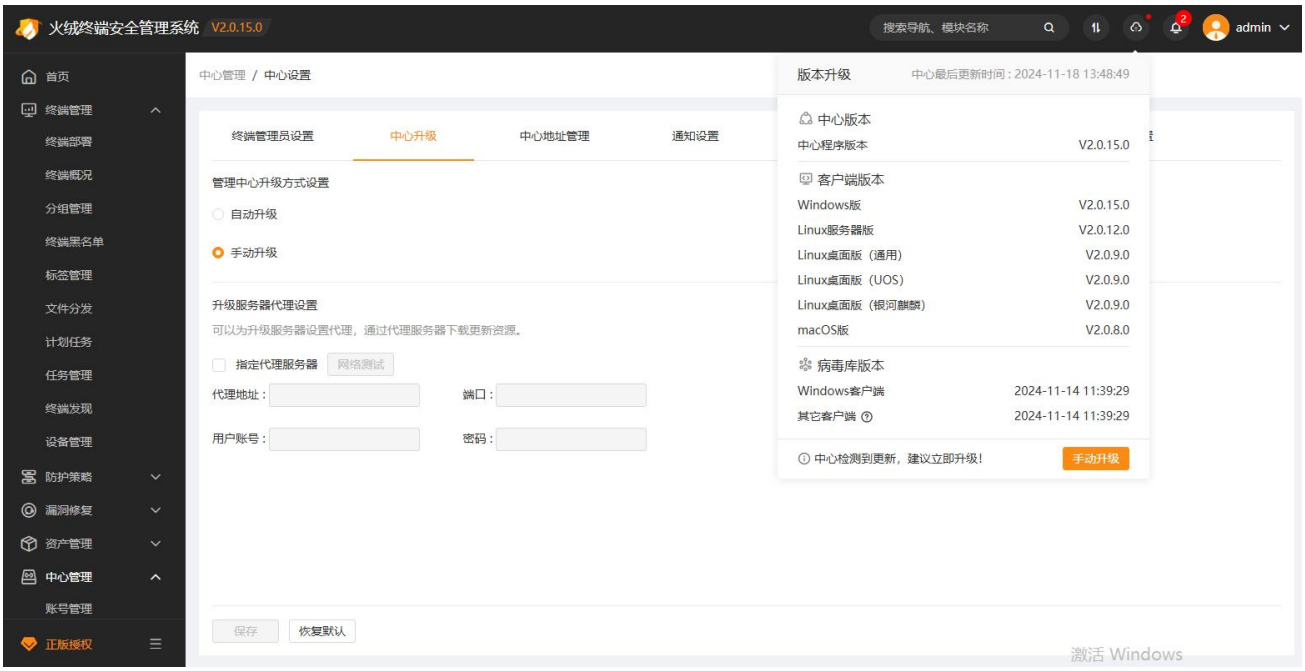
用户可在此处查看当前正在进行中的文件分发功能中的上传文件或数据备份功能中的导入数据备份的

进度。



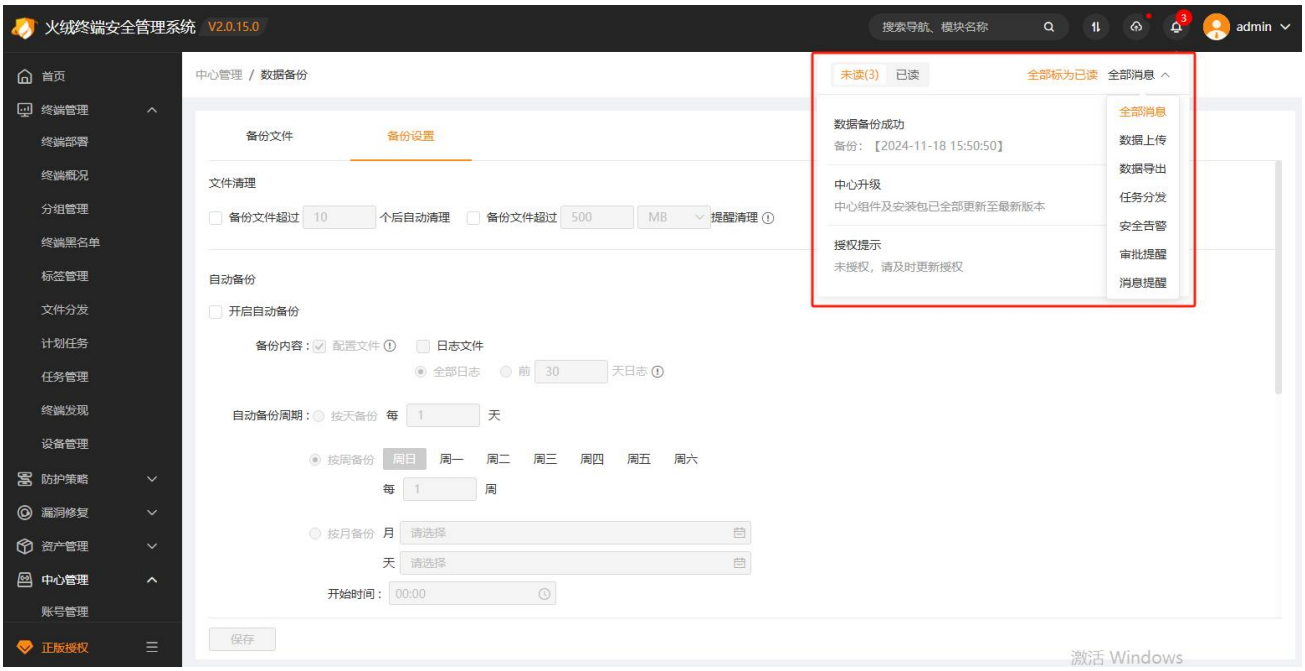
2.3.4 中心版本

火绒终端安全管理系统控制中心提供版本查看及更新服务，用户点击页面右上角【中心版本】按钮，系统自动弹出中心及终端版本信息和病毒库版本信息，用户点击【手动升级】可检查当前中心版本是否需要更新，发现新版本后出现更新提示，用户可自行对管理中心进行版本升级。



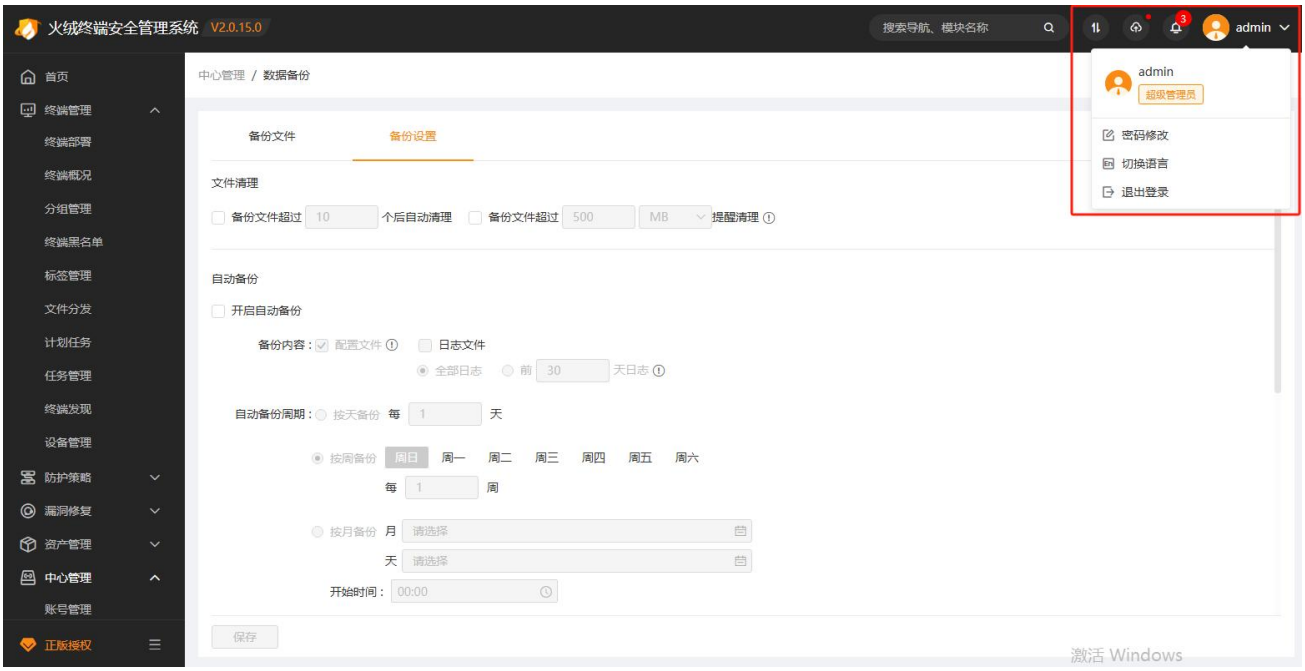
2.3.5 通知

火绒终端安全管理系统提供通知服务，用户数据上传、数据导出、任务分发、安全告警、审批通知、消息提醒都会自动产生一条通知消息，角标上显示未读消息数量。支持按照消息类型筛选查看对应类型的已读和未读的消息。点击【全部标为已读】，将当前类型下的全部未读消息变为已读。点击【清除所有通知】，清除当前类型下的全部已读的消息。



2.3.6 账户

火绒终端安全管理系统支持管理员对当前账户进行修改密码及退出登录操作，以及支持中文及英文切换。点击【修改密码】按钮，弹出修改密码弹框，输入新密码及原始密码后即可修改当前账户密码口令；点击【切换语言】，切换当前控制中心的显示语言。点击【退出登录】按钮，可注销当前用户在管理中心的登录，返回登录界面。



2.4 首页

火绒终端安全管理系统首页展示了终端的在线状态、终端安装概况、授权信息、服务器性能、近期安全事件（近 7 天及 30 天内各个防护模块事件数量及处理情况）。用户可以在首页直观的看到企业内的安全态势。终端在线状态、终端安装状态、近期安全事件模块，当前登录用户只能看到具有权限的分组的相关信息。授权信息模块和服务器性能模块显示当前控制中心的信息，与当前登录用户的分组权限无关。

点击【异常终端】【在线终端】【离线终端】，跳转到终端概况页且按照对应的类型进行筛选。

点击【已安装终端】，跳转到终端概况页，筛选全部终端。

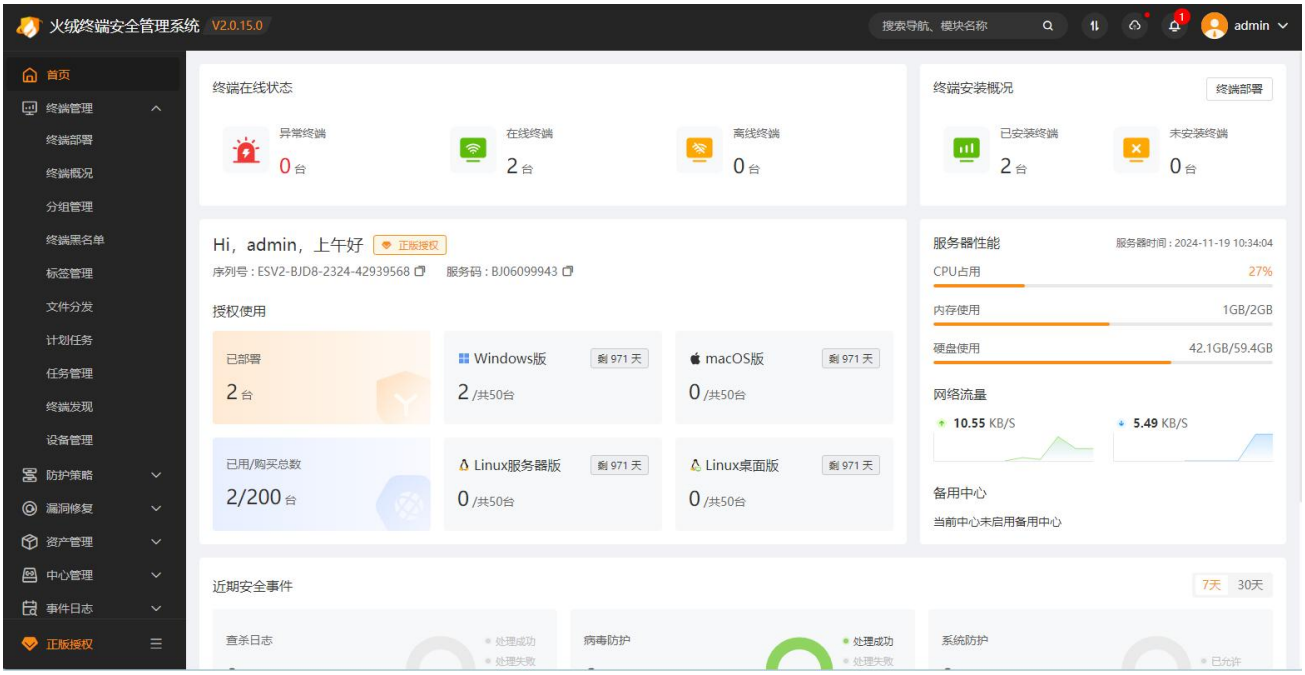
点击【未安装终端】，跳转到终端发现页-已发现终端页自动筛选未安装终端。

点击【终端部署】，跳转到终端部署页。

超级管理员点击授权信息中的【已部署】，跳转到终端概况页。点击【已用/购买总数】，跳转到授权页。

点击近期安全事件中的不同处理结果，跳转到安全日志总览页，并自动筛选对应的日志。点击【涉及

终端数】，跳转到安全日志总览页-统计页：按终端查看。



2.5 终端管理

2.5.1 终端部署

火绒终端安全管理系统提供便捷的终端部署功能，终端管理-终端部署页共提供了 3 种部署方式，用户根据自身情况选择合适的部署方式安装部署安全终端。

方式一：终端用户自助安装

管理员可通过邮件等方式，将链接分发给终端用户，终端用户通过浏览器访问链接后可依据自身系统环境下载不同类型终端，并按照链接中的描述安装终端。详细部署终端操作请参考《火绒终端安全管理系统 2.0-安装部署手册》。

方式二：下载安装包进行安装

如终端用户无法使用方式一自主安装，管理员可下载方式二中的安装包，拷贝至目标计算机上进行安装，安装步骤与方式一相同。

方式三：域部署工具部署

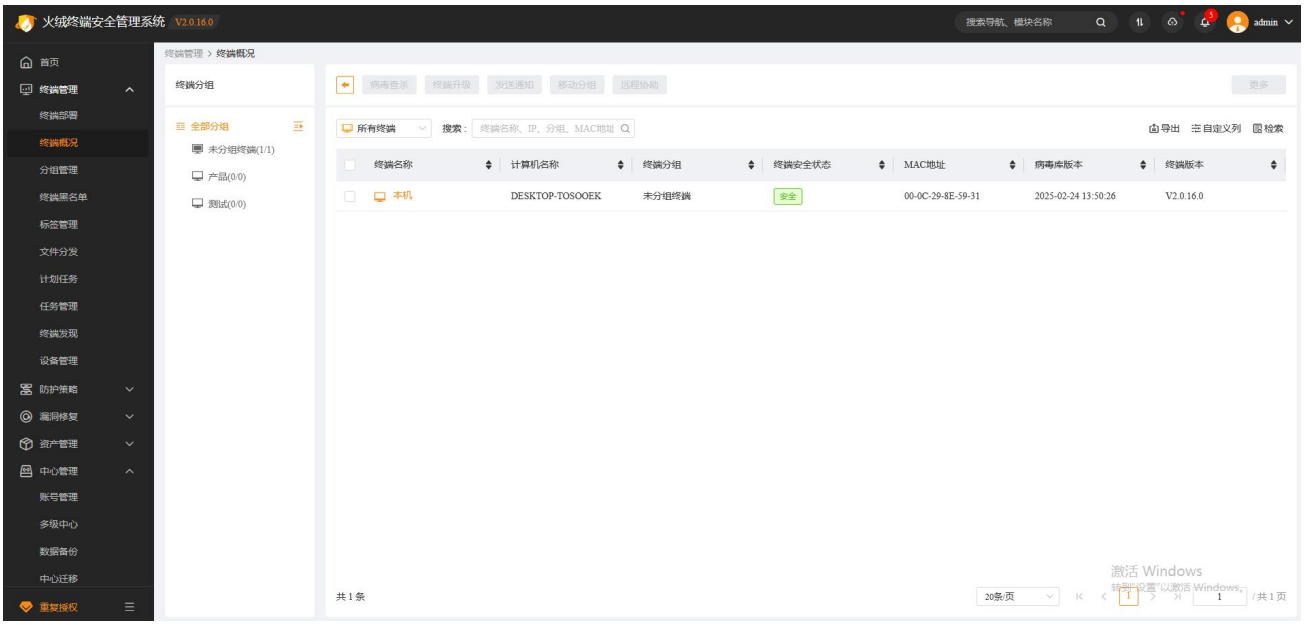
火绒安全终端提供域部署工具以供用户对域内用户进行统一安装部署，用户可通过终端部署页下载域部署工具，并且在域服务器上部署开机或者登录脚本，即可对域内用户完成自动安装部署（具体步骤可参考指引文档）。

2.5.2 终端概况

火绒终端安全管理系统为管理员提供了终端统一管理功能，管理员可通过管理中心统一管理及下发任务至指定终端。

当前支持的功能有：病毒查杀、终端升级、发送通知、移动分组、远程协助、同步防护策略、恢复隔

离文件、终端隔离、漏洞修复、文件分发、垃圾清理、计划任务、编辑标签、资产登记、关机、重启、删除终端、加入黑名单、卸载终端、筛选、导出、自定义列、模糊搜索、检索。



1. 病毒查杀

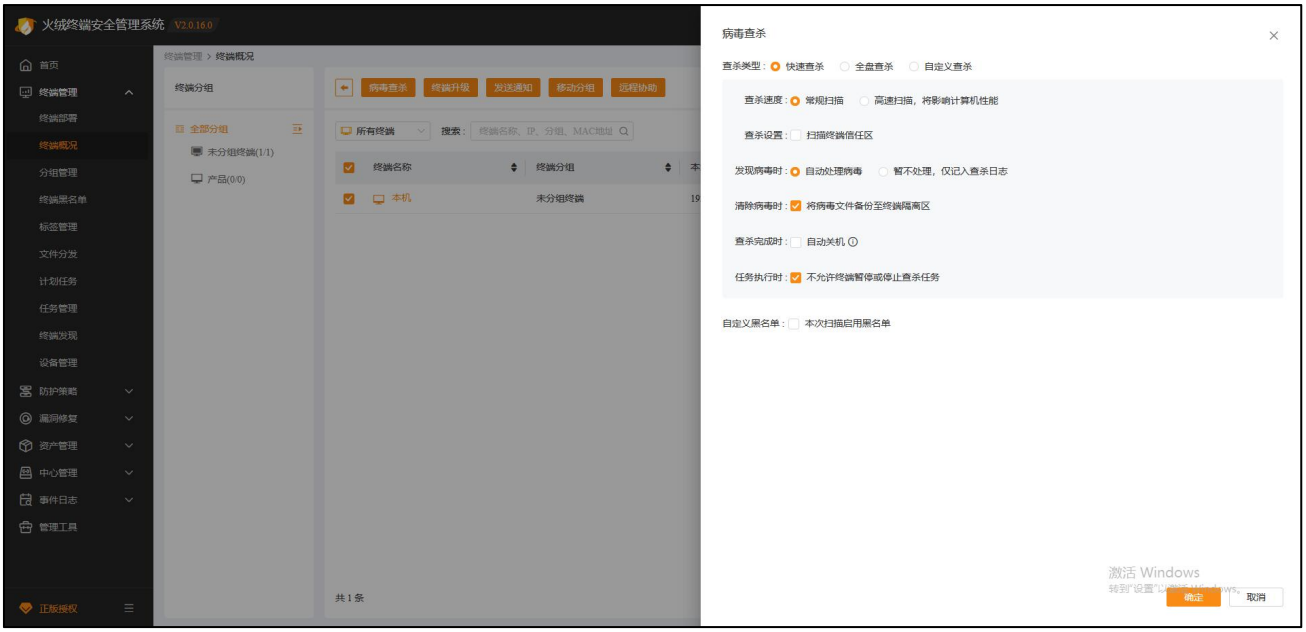
病毒查杀可分为三类，分别是快速查杀、全盘查杀、自定义查杀。

（1） 快速查杀：对病毒文件通常会感染电脑系统敏感位置进行病毒查杀，扫描范围没有包含磁盘所有存储空间，因此查杀速度较快。

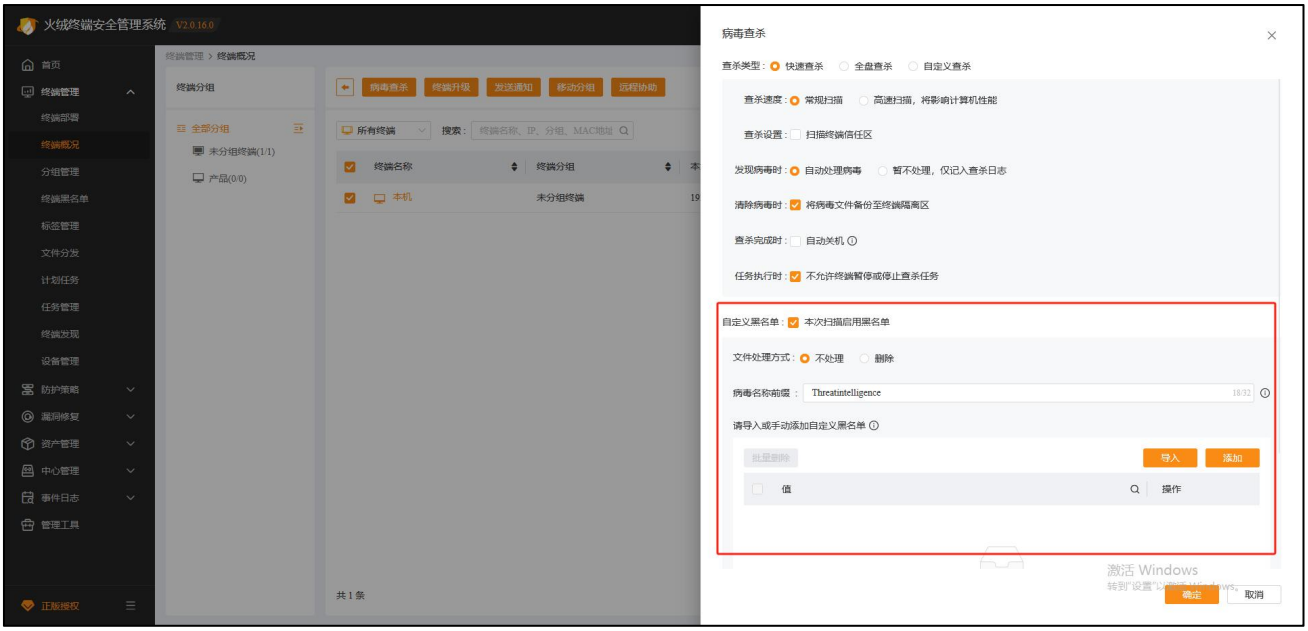
（2） 全盘查杀：对磁盘所有存储空间进行病毒查杀。

（3） 自定义查杀：可以自定义选择查杀位置进行病毒查杀。

用户选中需要下发病毒查杀任务的终端，点击【病毒查杀】按钮，设置完成查杀选项后，点击【确定】按钮即可对当前选中终端下发病毒查杀任务。



“自定义黑名单”默认不启用。当通过病毒查杀的自定义查杀功能，勾选【本次扫描启用黑名单】后，用户可在此页面向中心录入已知的文件 HASH 特征，如:MD5、SHA1、SHA256，并配置对命中自定义黑名单文件的处置方式。用户添加的自定义黑名单 HASH 特征，仅在当前扫描任务生效，病毒查杀任务下发后，中心将清空自定义黑名单数据。

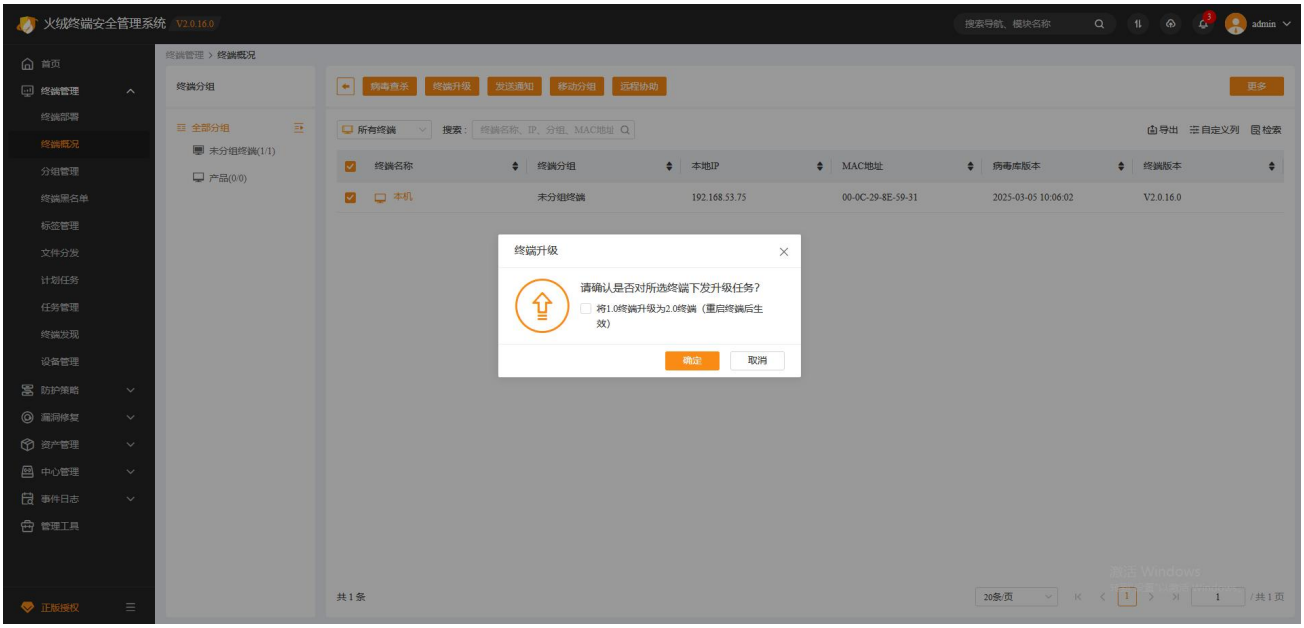


2. 终端升级

用户选中待升级终端，点击【终端升级】按钮，提示弹框出现后点击确定即可对当前所选终端下发升

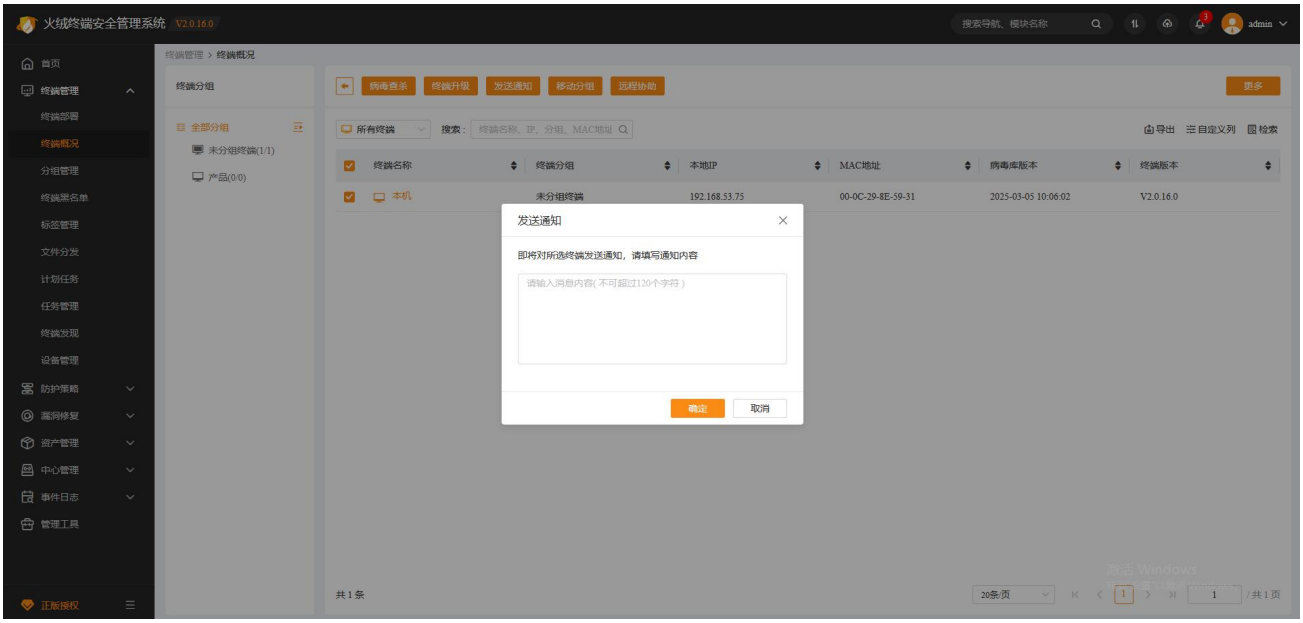
级任务。

将 1.0 版本终端升级为 2.0 版本终端：勾选后，可以将 1.0 版本终端跨版本升级至 2.0 版本，不勾选则只进行小版本升级（1.0 终端版本必须高于最小版本才可以跨版本升级至 2.0 版本，最小版本为：1.0.43.1）



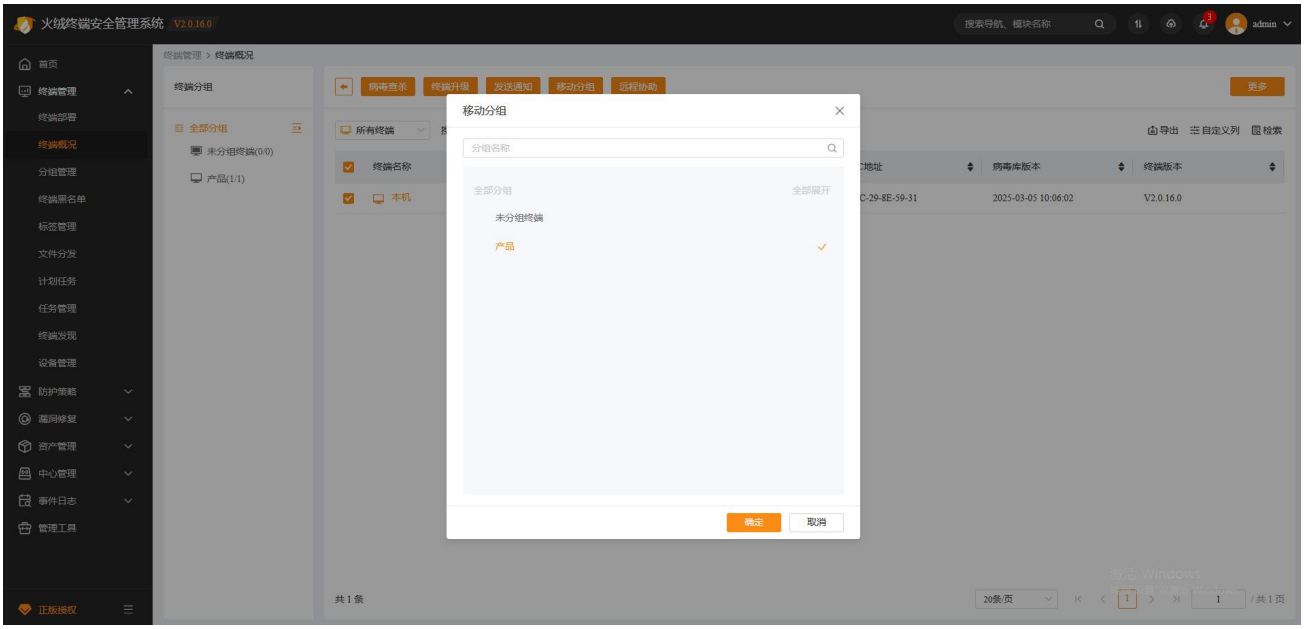
3. 发送通知

用户选中需要接收通知消息的终端，点击【发送通知】按钮，填写需要通知的内容之后，点击确定即可将通知消息发送至当前所选终端。



4. 移动分组

用户选中需要变更分组的终端，点击【移动分组】按钮，选择移动的目标分组，点击【确定】即可将当前选中终端移动至目标分组。



5. 远程协助

用户选中需要远程的终端，点击【远程协助】按钮，选择远程类型，确认后即可向当前选中终端发起远程任务。

远程桌面：弹窗通知终端用户，终端同意远程后，可查看和操作目标终端。

远程查看：弹窗通知终端用户，终端同意远程后，可查看目标终端。

远程 CMD：可设置是否弹窗通知终端用户，弹窗通知则需经过终端同意，不弹窗通知则无需经过终端同意，中心管理员可通过命令行的形式操作目标终端，目标终端无感知（后台执行命令行）。

注：远程协助支持浏览器版本如下：

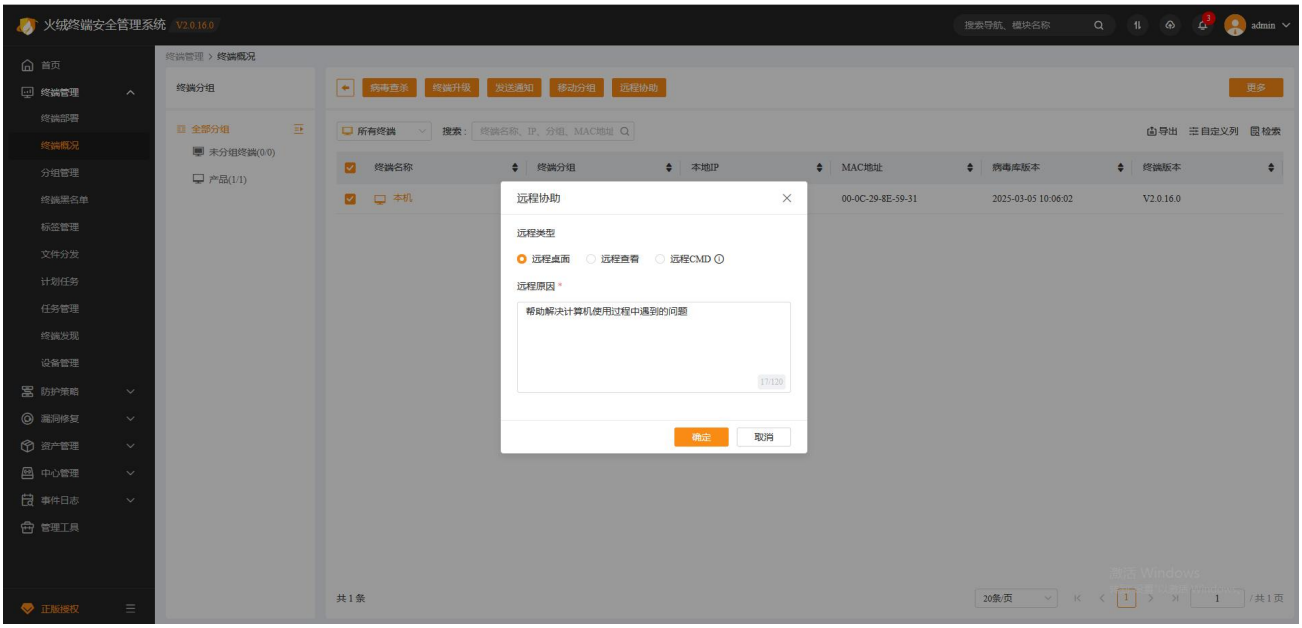
Google 浏览器版本大于等于 69

Firefox 浏览器版本大于等于 60

Safari 浏览器版本大于等于 10

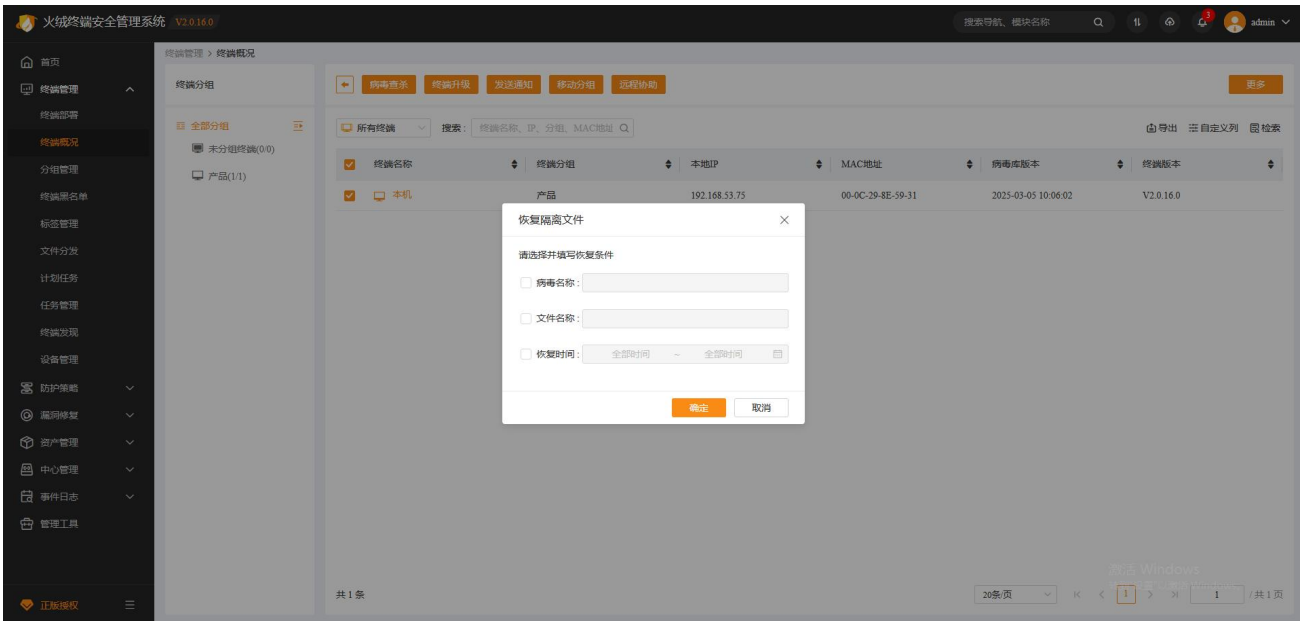
Opera 浏览器版本大于等于 56

Edge 浏览器版本大于等于 17



6. 恢复隔离文件

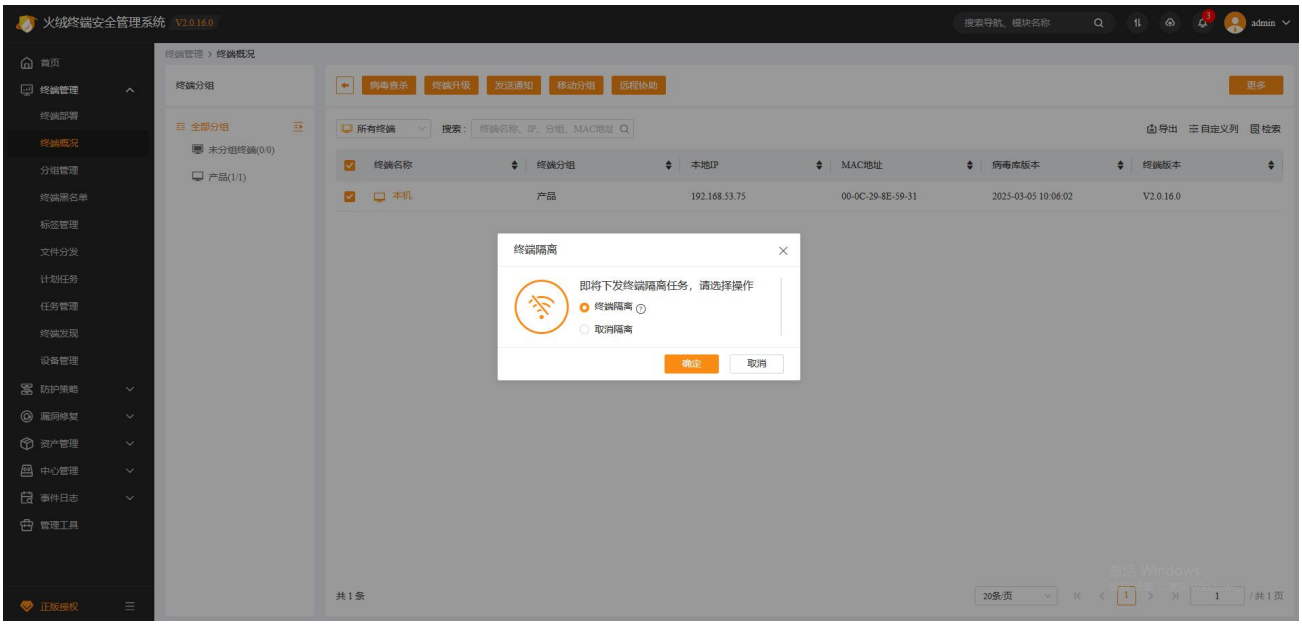
用户选中需要恢复文件的终端，点击【更多】-【恢复隔离文件】选项，填写恢复条件后点击确定即可向当前选中终端发起恢复隔离文件任务。



7. 终端隔离

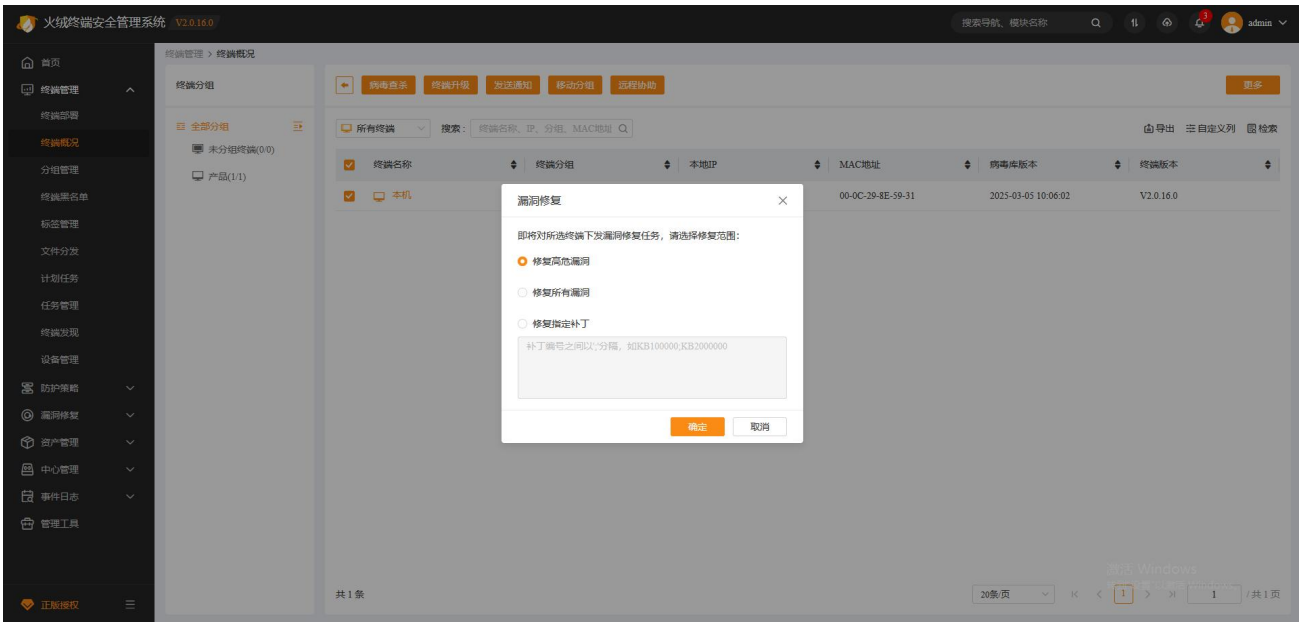
用户选中需要隔离的终端，点击【更多】-【终端隔离】选项，选择终端隔离或取消隔离，可以对终端网络连接进行管理。

终端隔离功能不会影响控制中心与终端的通讯，管理员仍可在中心查看、管控禁网终端。



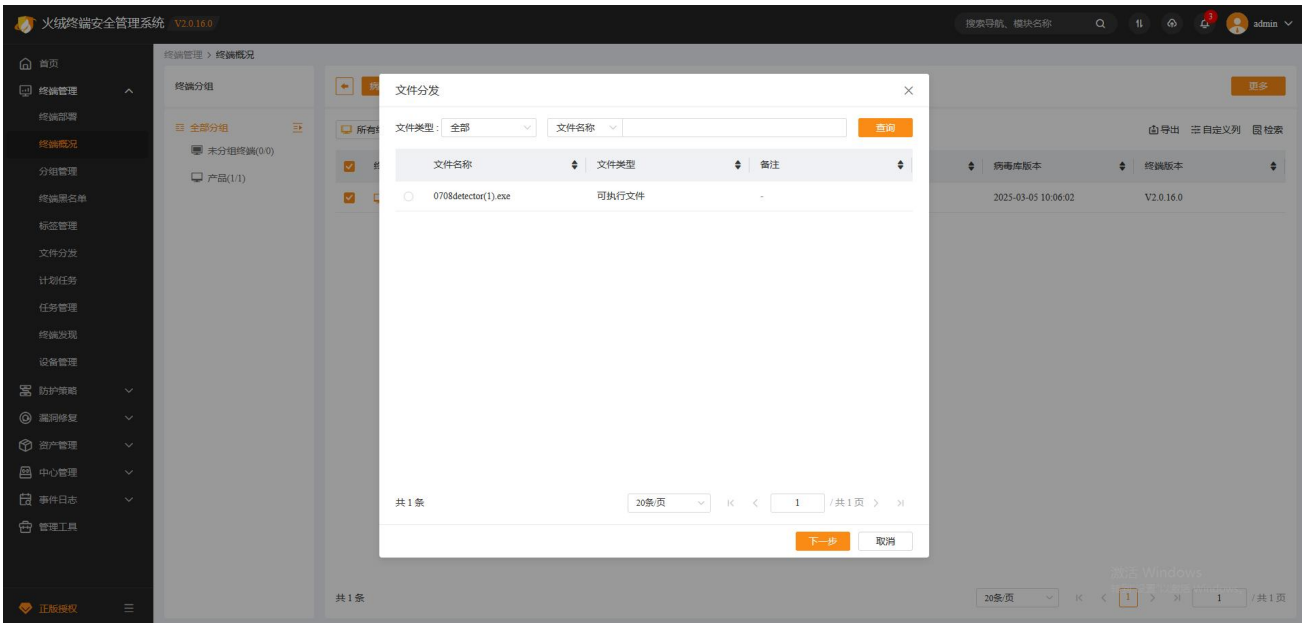
8. 漏洞修复

用户选中需要进行漏洞修复任务的终端，点击【更多】-【漏洞修复】选项，选择修复范围（修复高危漏洞、修复所有漏洞或修复指定补丁，选择【修复指定补丁】，可以输入想要修复的补丁编号，终端只修复这些特定的漏洞），点击【确定】按钮后即可对当前选中终端下发漏洞修复任务，终端收到漏洞修复任务后即可自行检测并修复系统漏洞。



9. 文件分发

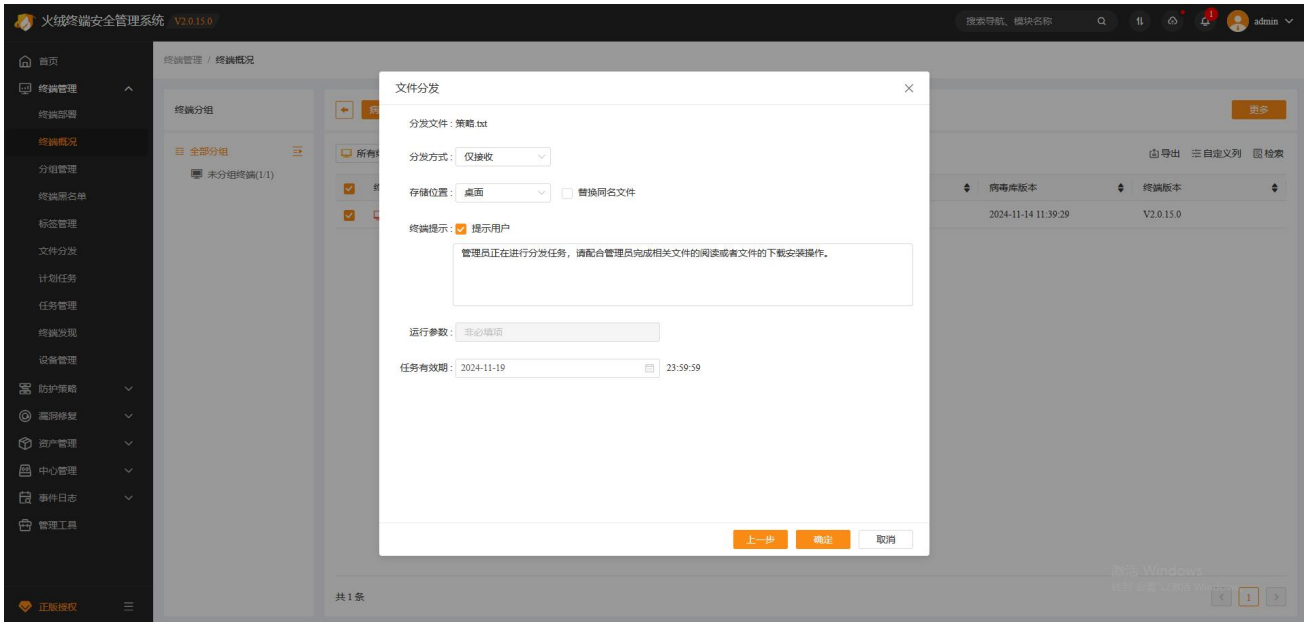
用户选中需要进行文件分发任务的终端，点击【更多】-【文件分发】选项，选择需要分发至终端的文件（此处待选择文件来源于【终端管理】-【文件分发】处上传的待分发文件列表）；



点击【下一步】进入分发设置界面，选择分发方式、存储位置、终端提示、运行参数及任务有效期后，点击【确定】即可将所选文件分发至指定终端。

（1） 分发方式：分发方式分为三种，分别是仅接收、接收并运行和以系统权限运行。选择仅接收

时，终端仅将文件接收并存储至所选位置，不会自动运行；选择接收并运行时，中心下发分发任务后，终端接收到文件会自动运行；选择以系统权限运行时，终端接收到文件后将以系统权限运行文件，无法显示程序界面；



(2) 存储位置：分发方式选择接收并运行或者仅接收时，可选存储位置为系统桌面、系统临时目录、自定义；选择【自定义】时，支持用户自定义存储路径，终端接收任务后发现不存在该自定义目录时，将自动创建该目录；分发方式选择以系统权限运行时，存储位置固定为系统盘根目录；

(3) 替换同名文件：勾选时，终端接收任务后，检测到已存在同名文件时，将自动替换同名文件；不勾选时，终端接收任务后，检测到已存在同名文件，将自动将分发的文件重命名为示例文件 (1)、示例文件（2）、以此类推；

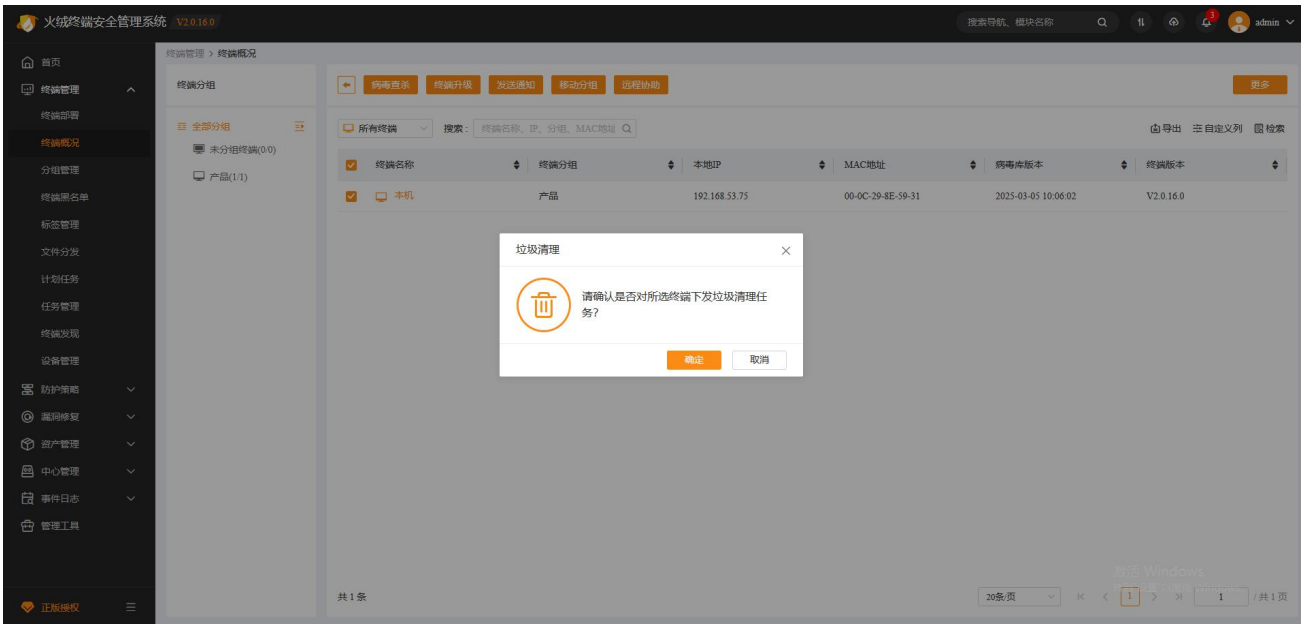
(4) 终端提示：勾选则下发分发任务后终端弹出提示框提示用户，不勾选则后台执行分发任务，不会弹框提示用户；

(5) 运行参数：用户可自定义输入运行参数，文件分发任务下发至终端后，可依照输入的运行参数运行当前分发文件；

（6） 任务有效期：用户可自行设定任务有效期，超过设定有效期限后，此条分发任务不再继续分发执行；

10. 垃圾清理：

用户选中需要进行垃圾清理任务的终端，点击【更多】-【垃圾清理】选项，中心下发任务后，终端接收到任务后会自动执行垃圾清理任务。



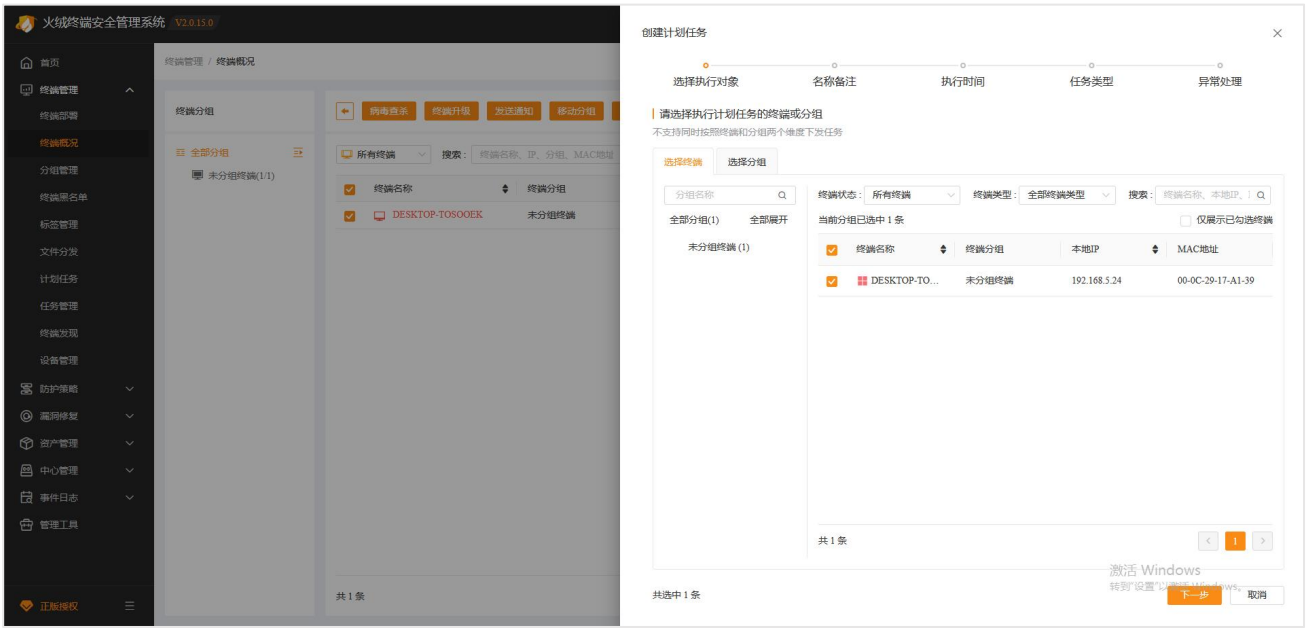
11. 计划任务

用户可对指定终端下发计划任务，创建计划任务时左侧按钮不可切换，需按引导先选择执行计划任务的对象，可以按终端添加或按分组添加，点击【下一步】，查看计划任务执行对象列表，确认执行计划任务的执行对象后，点击【下一步】，设置计划任务的名称和备注，可以修改计划任务的名称，设置该任务的备注信息，以便于后续管理，点击【上一步】可以查看执行计划任务的对象，点击【下一步】，选择执行该计划任务的时间，选择【单次任务】，则该计划任务只会根据执行时间，执行一次计划任务，选择【按天计划】、【按周计划】、【按月计划】、【开机执行】、【登录执行】等执行任务频率，将会根据任务频率，结合具体执行计划任务的时间，多次执行计划任务，设置好计划任务的【执行时间】后，点击【上

一步】，可以查看、修改计划任务的名称和备注信息，点击【下一步】可以设置计划任务的具体类型；下方为各设置项含义：

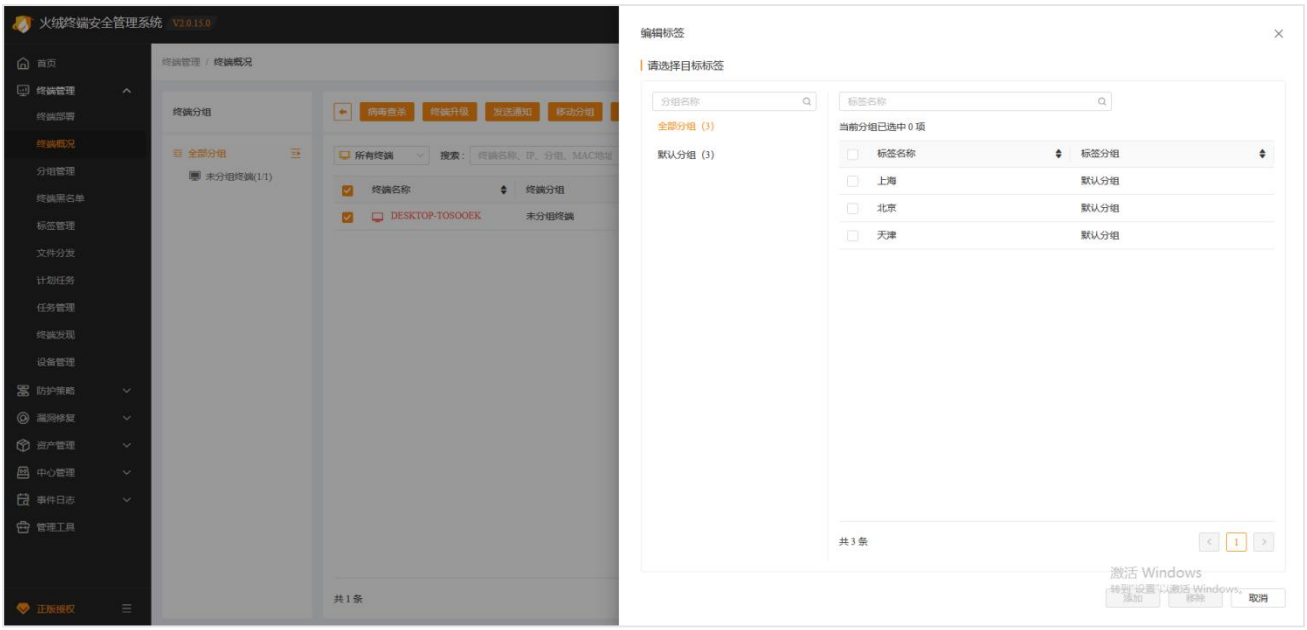
（1） 任务类型：可选设置计划、单次任务、开机执行和登录执行，选择设置计划时，任务将按照用户自定义的时间频率进行任务执行；选择单次任务，任务将按照用户设定的时间执行一次；选择开机执行，任务会在每次开机时自动执行；选择登录执行，任务会在每次用户登录时自动执行；

（2） 执行任务：企业版 2.0 目前支持的计划任务有九种，分别是：快速查杀、全盘查杀、自定义查杀、漏洞修复、终端升级、发送通知、垃圾清理、关机、重启；用户可根据自身需求自行选择计划任务进行设定并下发至终端。



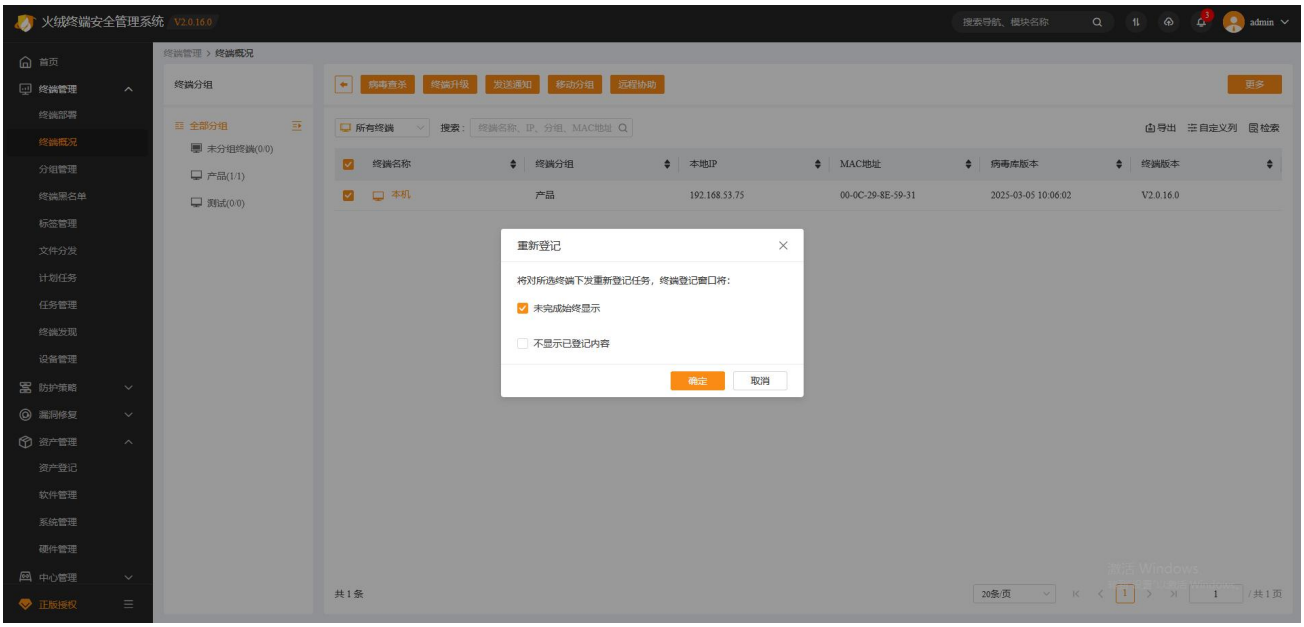
12. 编辑标签

用户可对指定终端标记不同标签（可同时标记多个），选择需要标记标签的终端，点击【更多】-【编辑标签】进入标签编辑界面，选择想要添加的标签，点击添加即可成功对当前终端添加标签，同理点击移除可移除当前选中的标签。



13. 资产登记

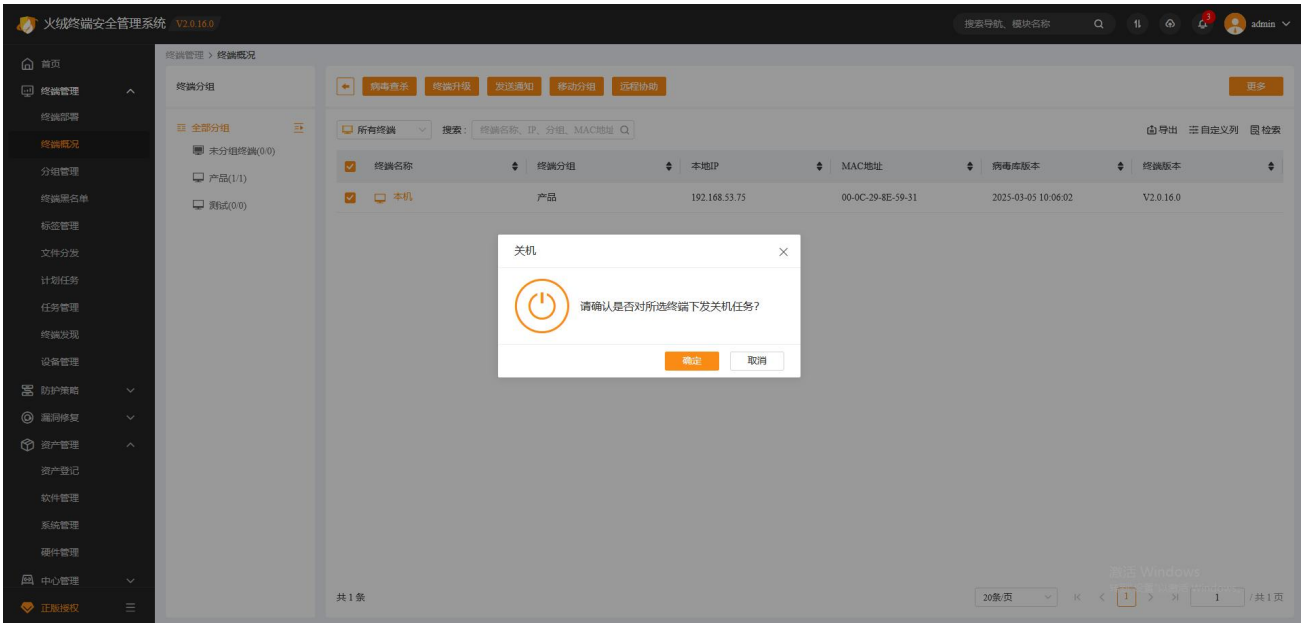
用户可通过下发资产登记任务对所选终端进行资产登记（资产登记内容来源于【资产管理】-【资产登记】-【登记信息管理】），资产登记完成后，可在【资产管理】-【资产登记】-【资产登记管理】查看登记信息。



14. 关机

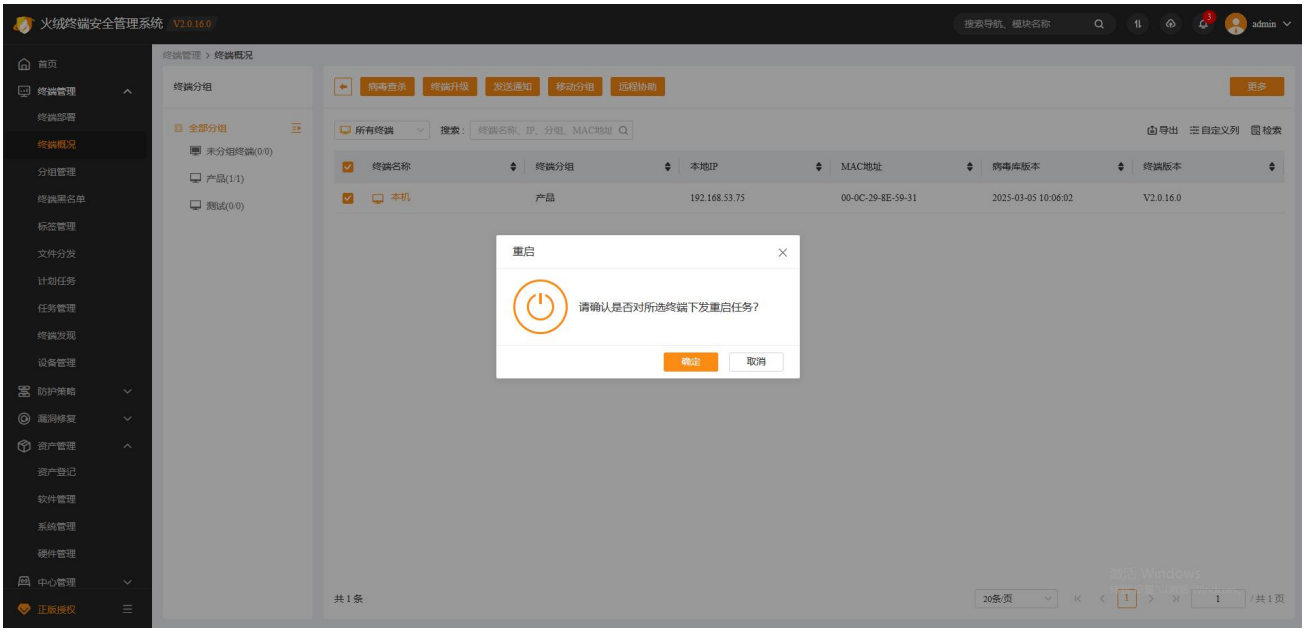
用户选中需要下发关机任务的终端，点击【更多】-【关机】选项，即可对当前选中终端下发关机任务，

终端收到关机任务后，会有一分钟倒计时关机提示，用户也可手动选择立即关机或暂不关机，倒计时结束后如果没有手动操作，终端则自动关机。



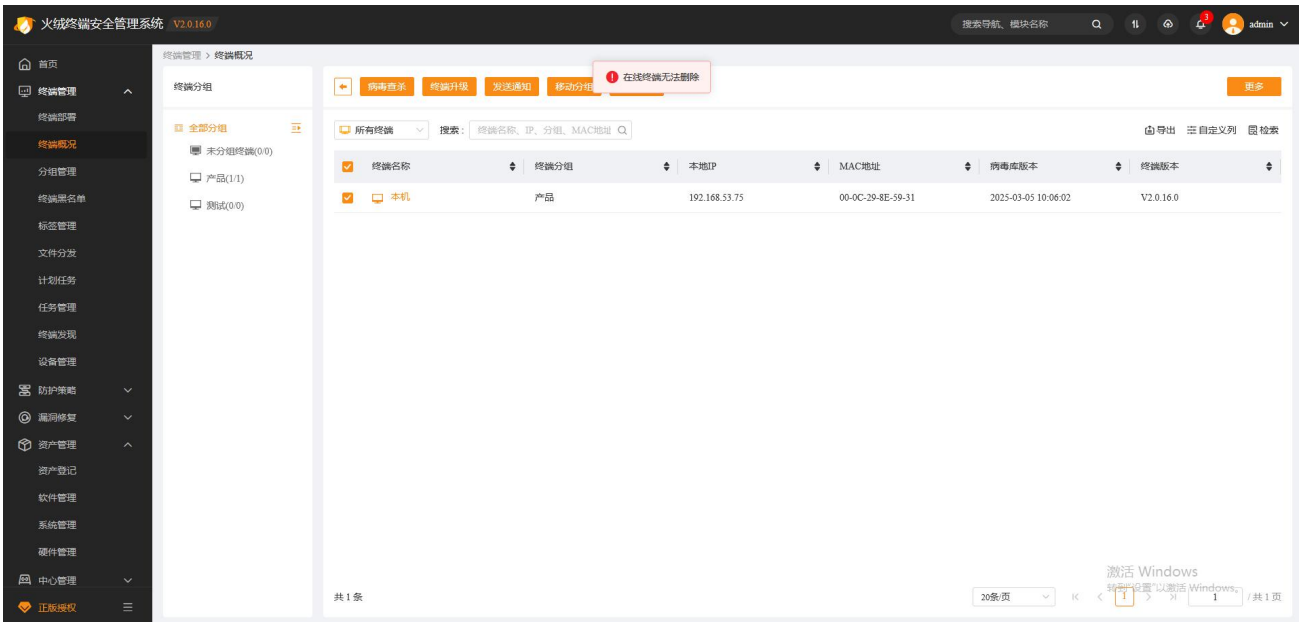
15. 重启

用户选中需要下发关机任务的终端，点击【更多】-【重启】选项，即可对当前选中终端下发重启任务，终端收到重启任务后，会有一分钟倒计时重启提示，用户也可手动选择立即重启或暂不重启，倒计时结束后如果没有手动操作，终端则自动重启。



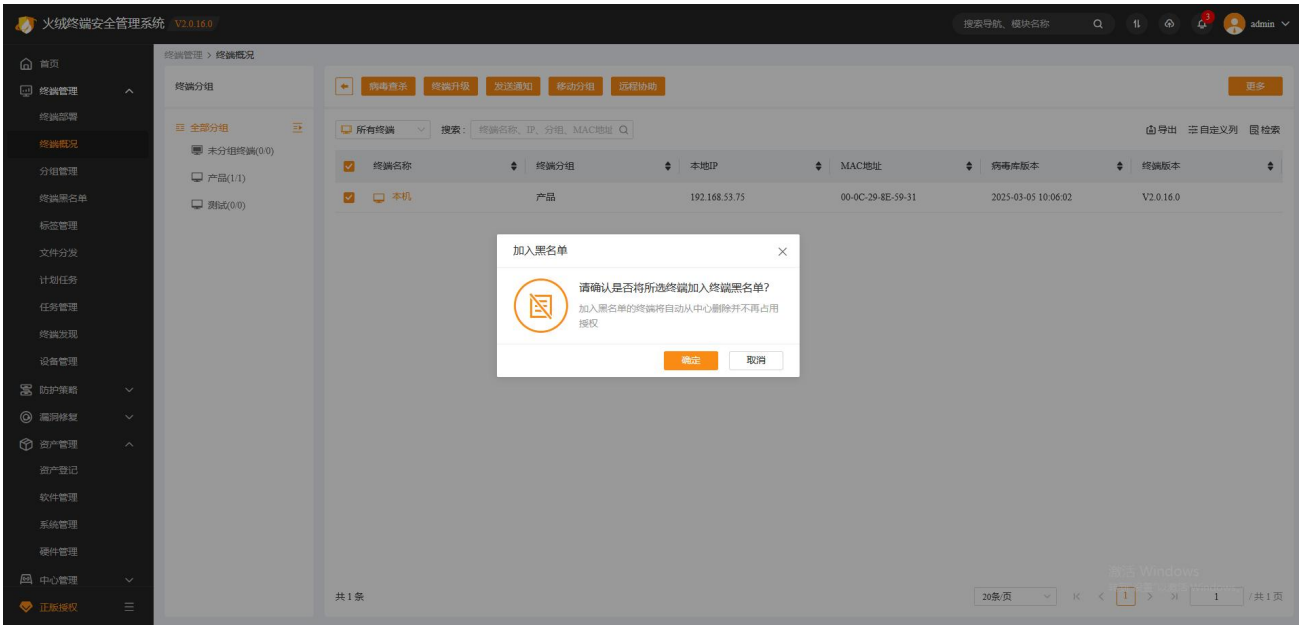
16. 删除终端

用户可通过删除终端来清理已经弃用或无需安全保护的终端，删除后，中心不再显示此终端信息。如果删除后想再次对删除的终端进行安全保护，只需要将受保护终端再次连接中心即可，在线的终端不能删除。



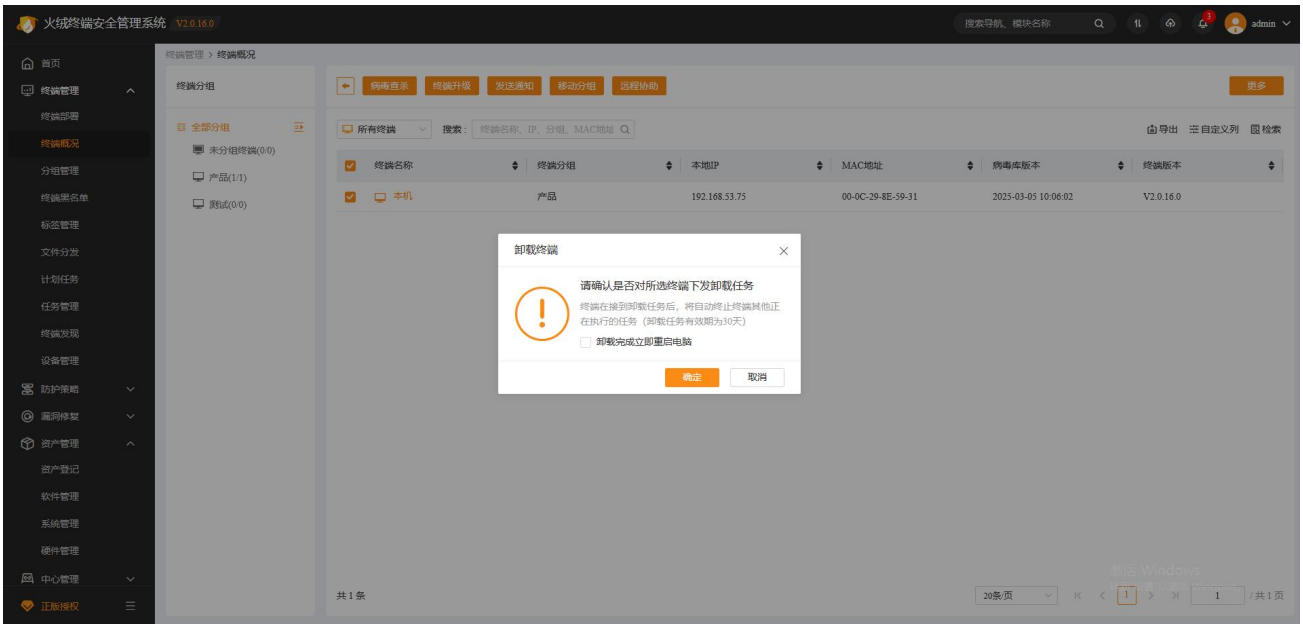
17. 加入黑名单

用户可通过加入黑名单，将所选终端加入黑名单列表，加入黑名单后，终端自动从中心删除并不再占用授权（加入黑名单的终端可在【终端管理】-【终端黑名单】查看及管理）。



18. 卸载终端

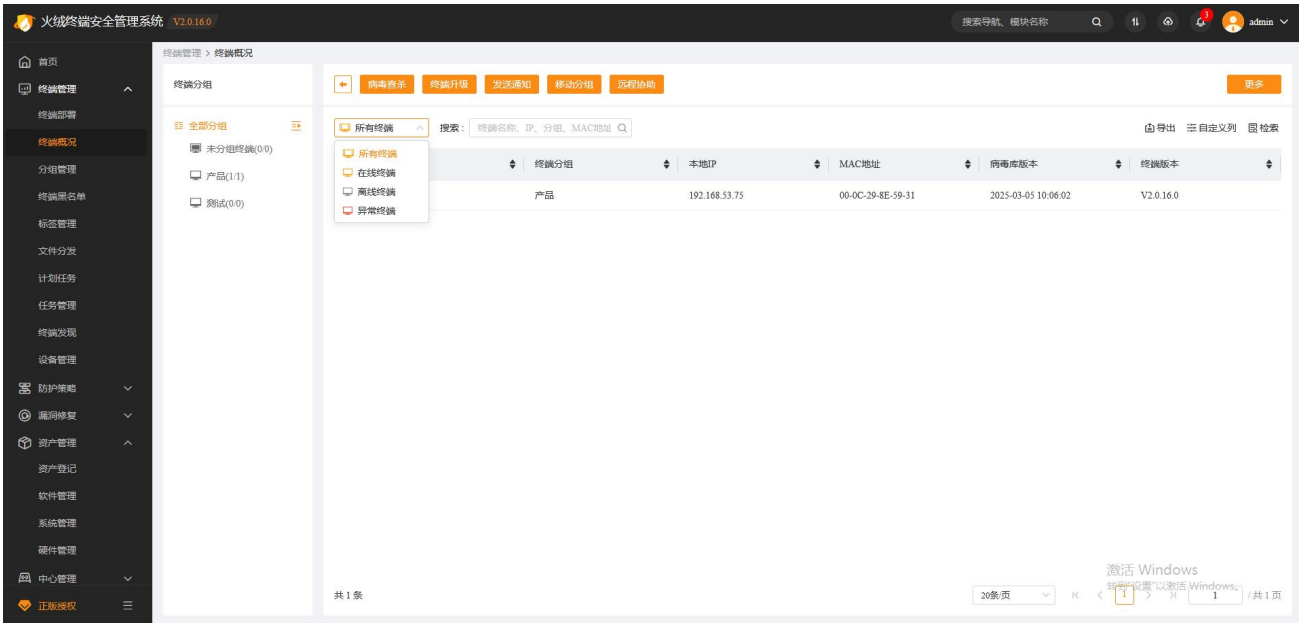
用户可通过卸载终端功能批量卸载终端；勾选【卸载完成立即重启电脑】时，卸载终端后将重启电脑。终端接收到卸载终端任务后，将停止当前正在执行的任务，直接开始静默卸载终端；卸载终端任务有效期为 30 天，超过 30 天后中心将结束分发卸载终端任务；



19. 筛选

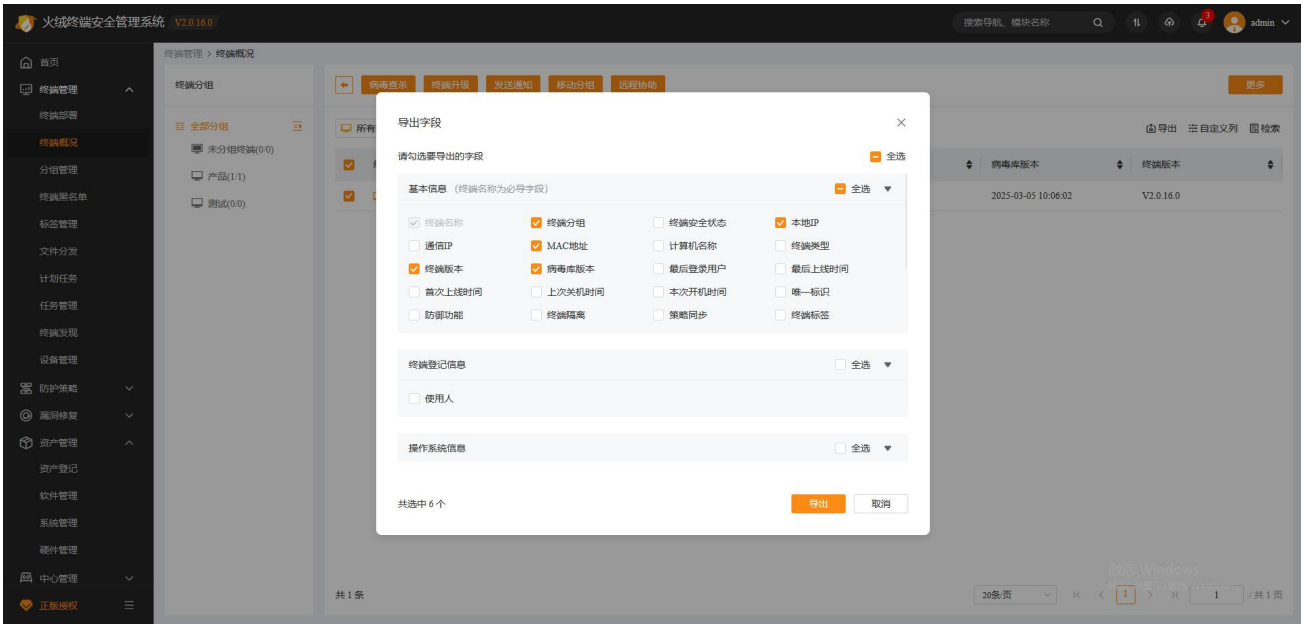
用户可通过筛选功能对当前终端进行分类筛选，可选项分别为所有终端、在线终端、离线终端、异常

终端（指终端服务异常时或有异常状态的终端），选择后可将列表中的终端筛选为指定类型终端进行显示，方便快速查找。



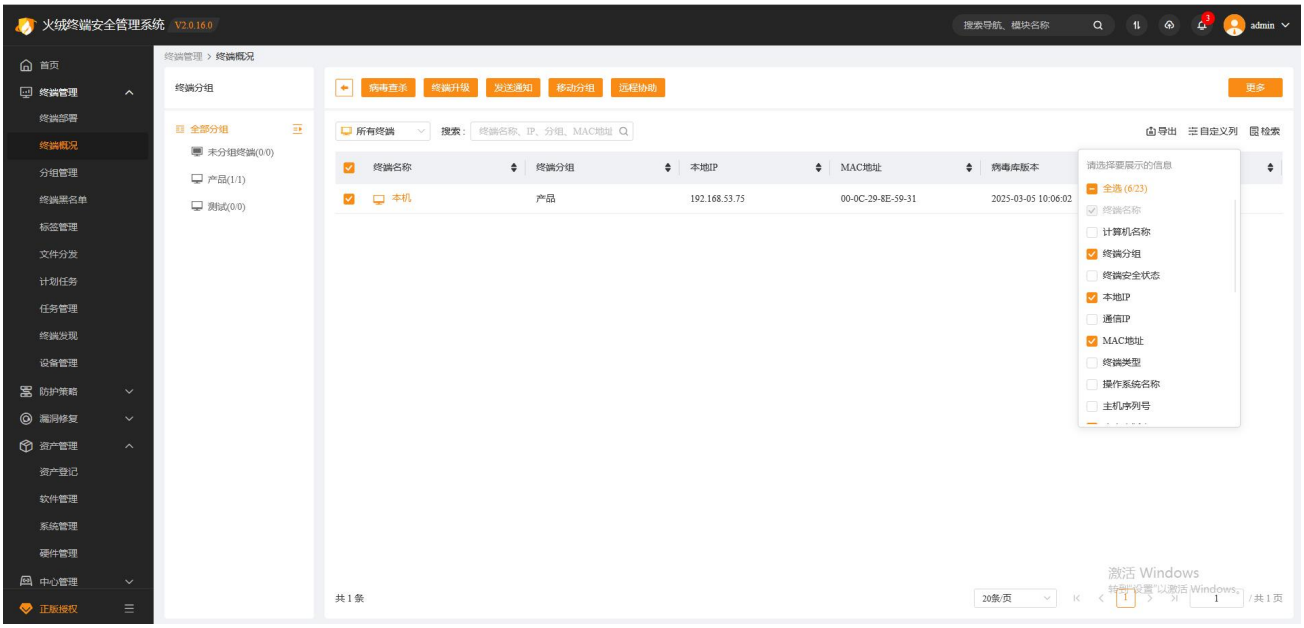
20. 导出

存在勾选的终端时，用户可自定义导出所有数据或导出选中的数据，并且用户可自定义要导出哪些字段，方便用户对终端信息进行分析处理，导出成功后，消息通知中显示下载信息。



21. 自定义列

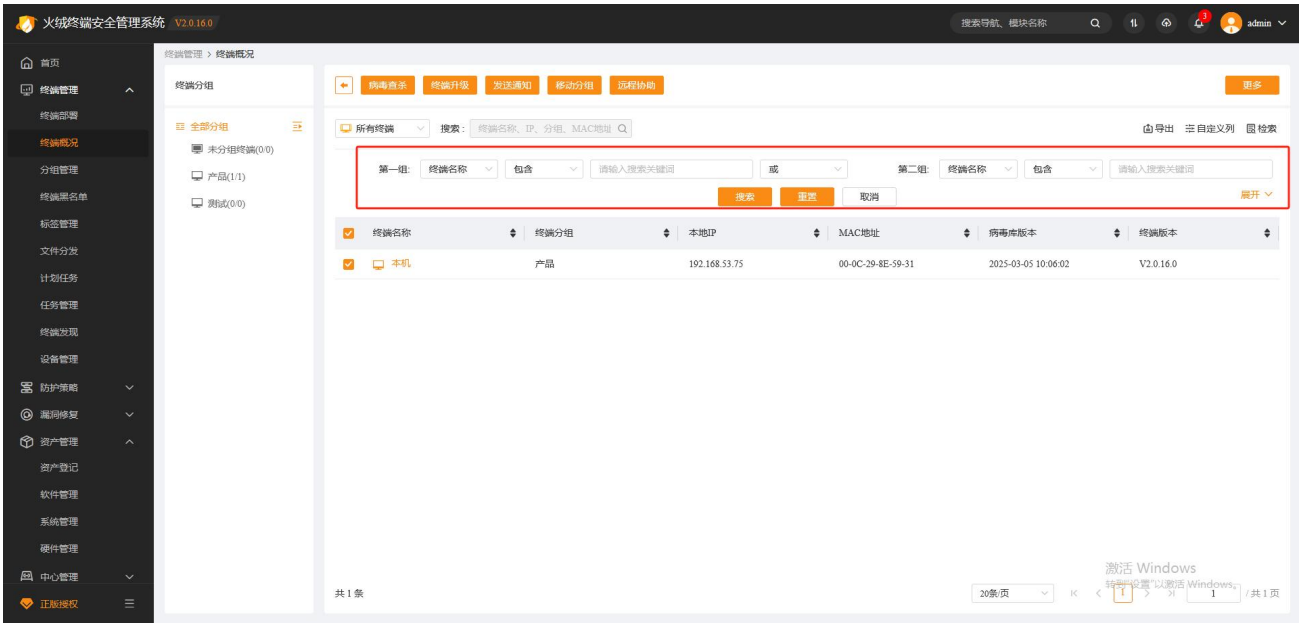
中心支持自定义列，用户可以根据自身需要，自定义列表显示信息，方便用户查看指定信息，减少无用信息显示。



22. 模糊搜索及检索

(1) 模糊搜索：用户可根据终端名称、终端分组、本地 IP、通信 IP 和 MAC 地址，进行快速搜索，能够满足基本的查找需求。

(2) 检索：支持对终端名称、计算机名称、终端分组、终端安全状态、本地 IP、通信 IP、MAC 地址、系统类型、操作系统版本、主机序列号、病毒库版本信息进行组合检索，精准定位目标终端，方便用户指定终端，满足精确搜索的需求。



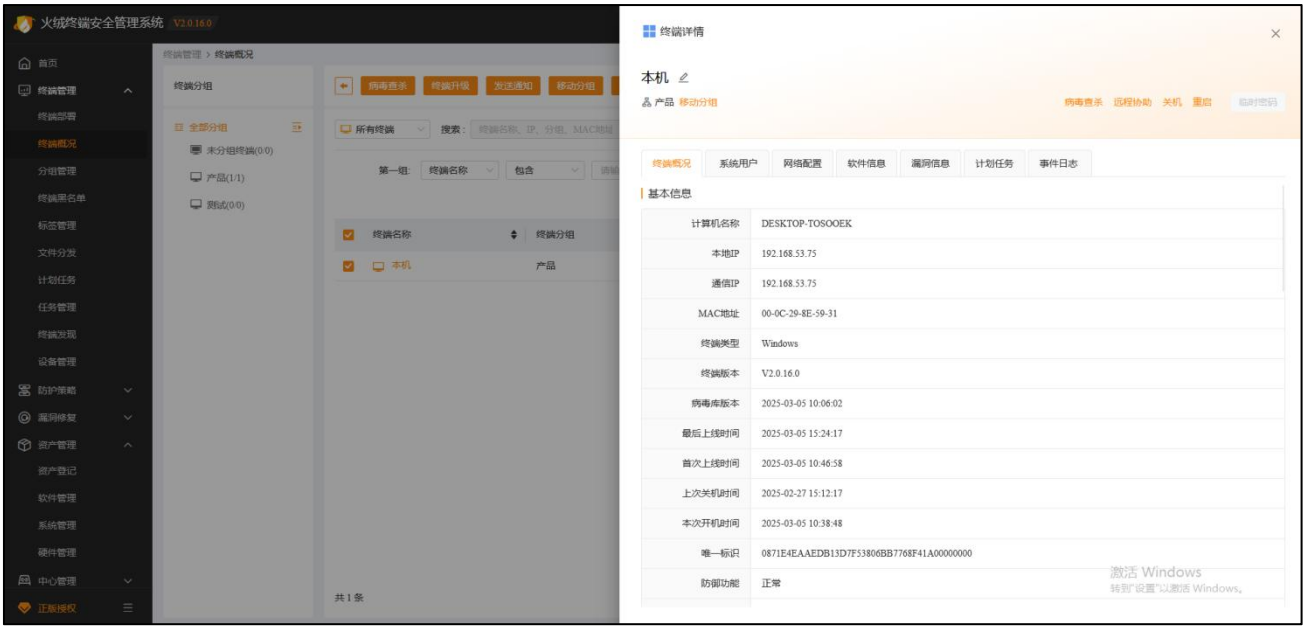
23. 终端详情

用户可通过点击终端名称查看终端详细信息，可查看包括终端概况、系统用户、网络配置、软件信息、漏洞信息、计划任务、事件日志七种类型的信息。

用户点击左上角终端名称，也可对当前用户终端信息名称自定义修改。

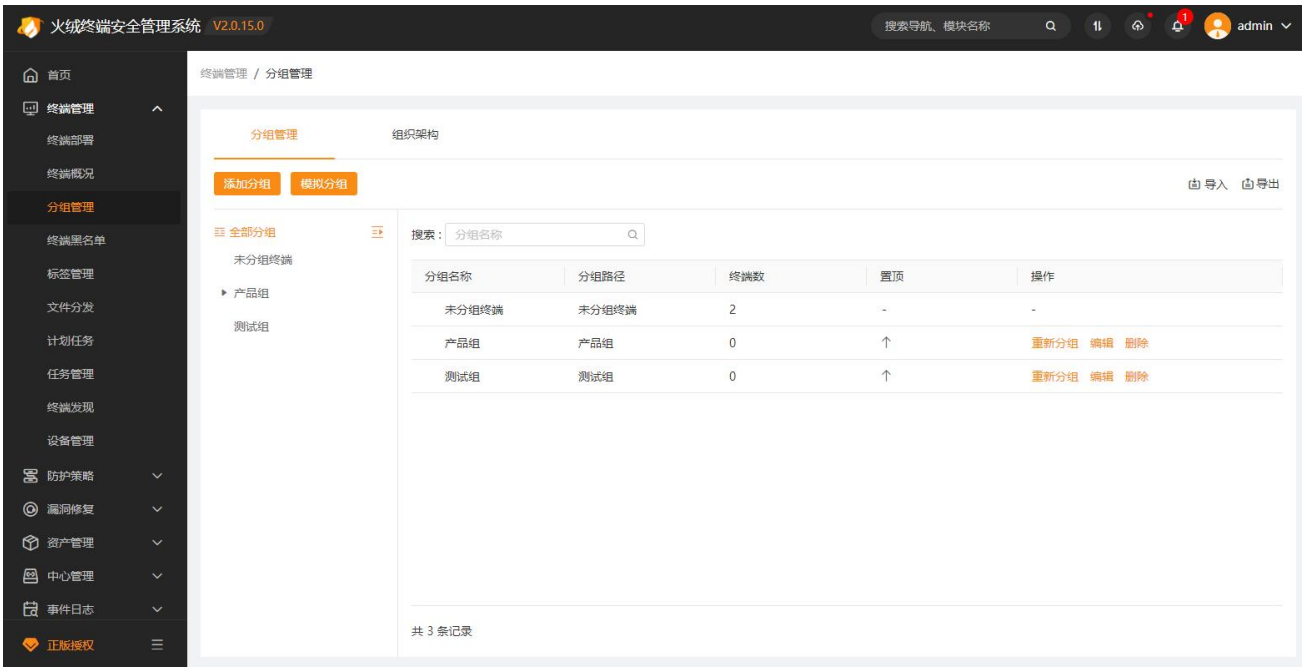
点击临时密码按钮，能够生成该终端对应的临时密码，可以设置临时密码的有效时间，在终端用户需要使用管理员密码时，生成临时密码发送给终端用户使用。

在终端详情页也支持【移动分组】和下发【病毒查杀】【远程协助】【关机】【重启】【漏洞修复】任务。



2.5.3 分组管理

用户点击【分组管理】按钮，切换至分组管理页面，页面顶部可以切换分组管理和组织架构。

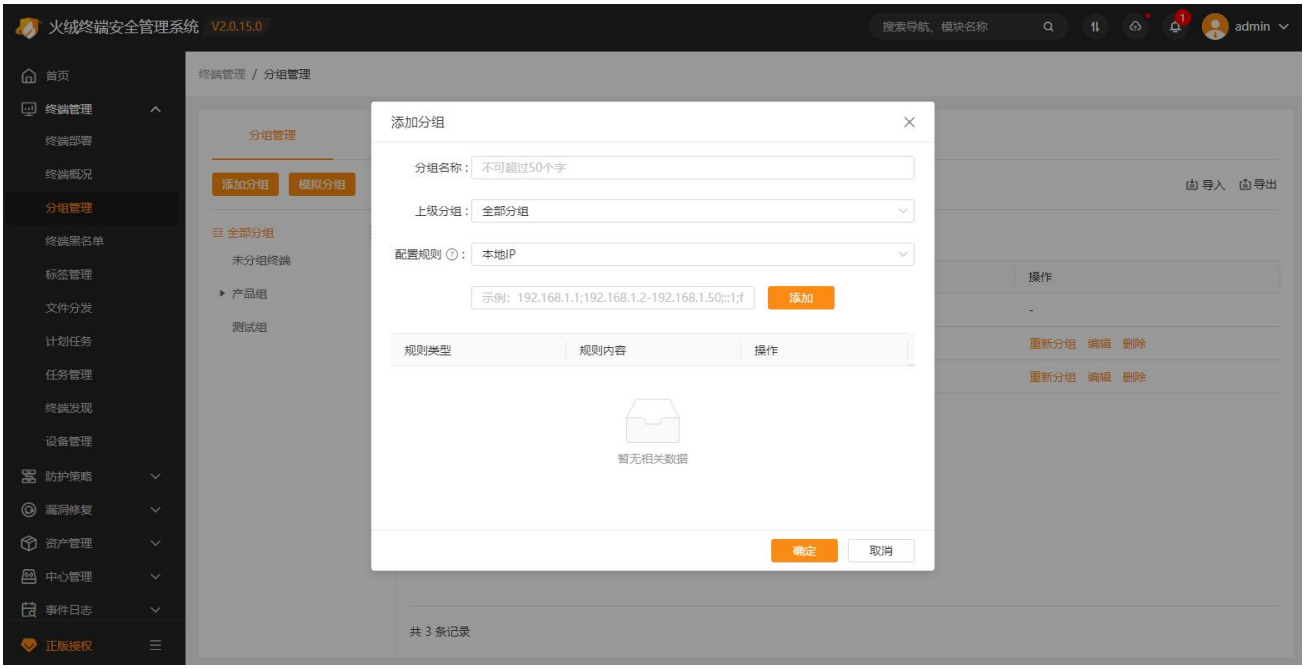


分组管理功能可以管理中心所有终端的分组或使用 LDAP 设置功能同步用户所在的组织架构，分组管理支持添加、编辑、删除分组、重新分组，导入、导出分组数据，模拟终端分组，调整分组的显示顺序和

规则匹配顺序。

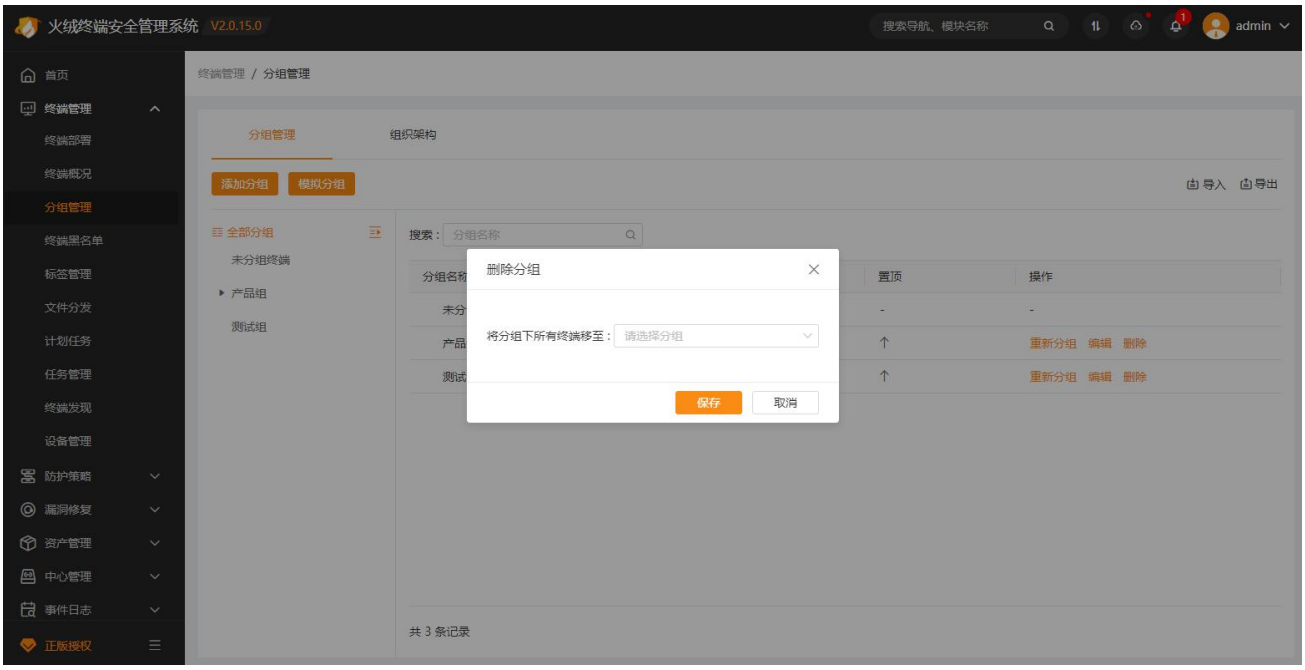
1. 分组管理

（1） 添加分组：点击【添加分组】按钮，显示添加分组弹窗，填写分组名称，选择上级分组后，点击确定即可添加新分组，添加新分组时可以填写当前分组的规则，符合当前分组规则的未分组终端和新终端将会自动移入当前分组。

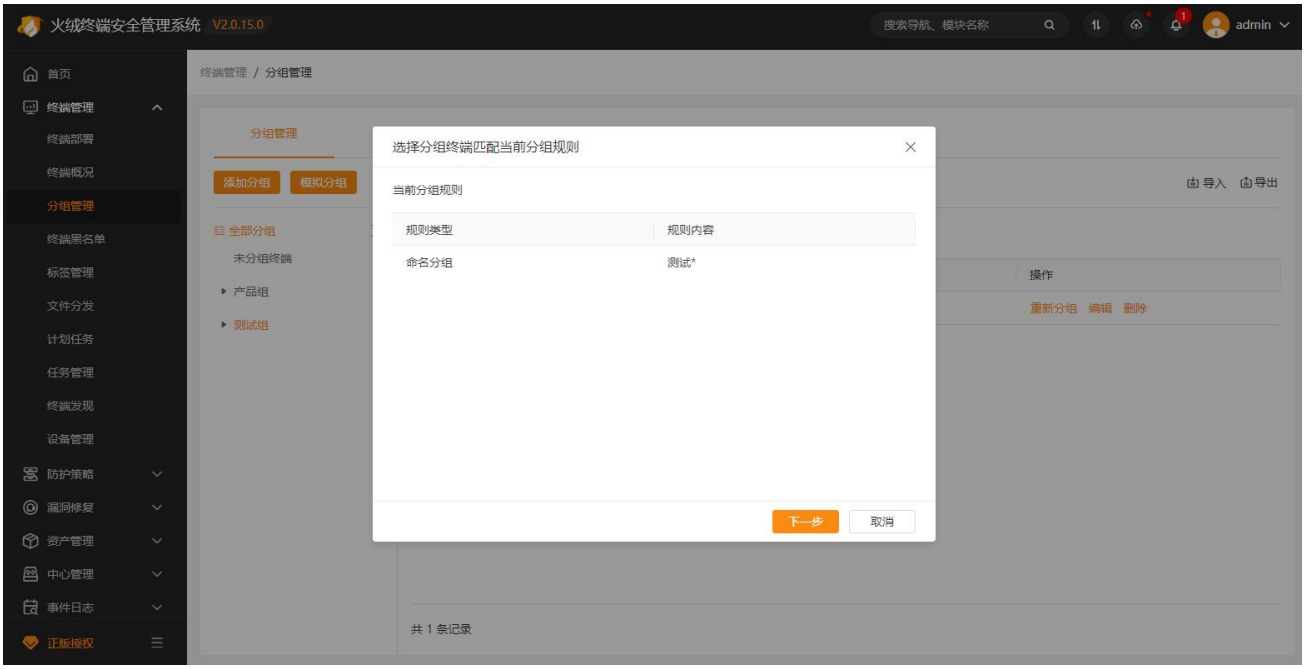


（2） 编辑分组：编辑分组时回显分组当前的信息，修改完成后，点击确定，即可保存对所选分组的修改。

（3） 删除分组：在分组所在行操作列，点击删除按钮，显示删除分组窗口，选择删除分组后，当前分组所辖终端需要移入的分组，点击确定按钮，删除所选分组。



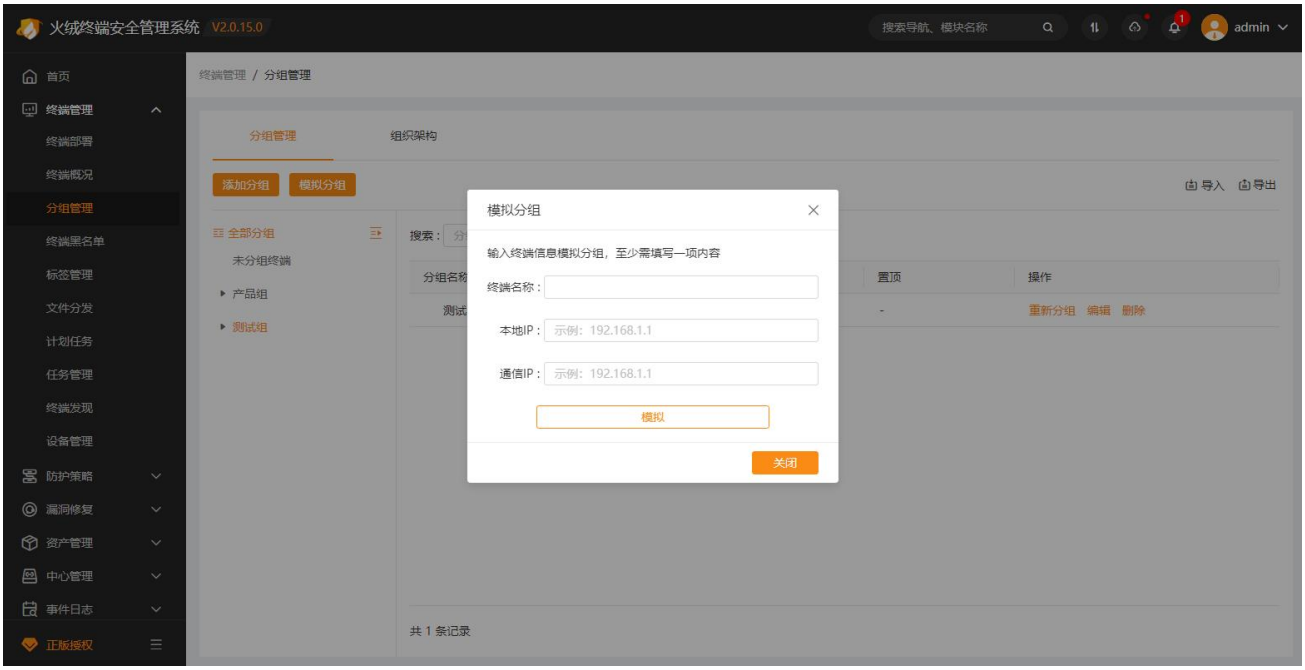
(4) 重新分组：点击当前分组所在行重新分组按钮，显示当前分组的分组规则，点击下一步，选择目标分组，确定后重新匹配当前分组规则，符合分组规则的终端，移入此分组中。



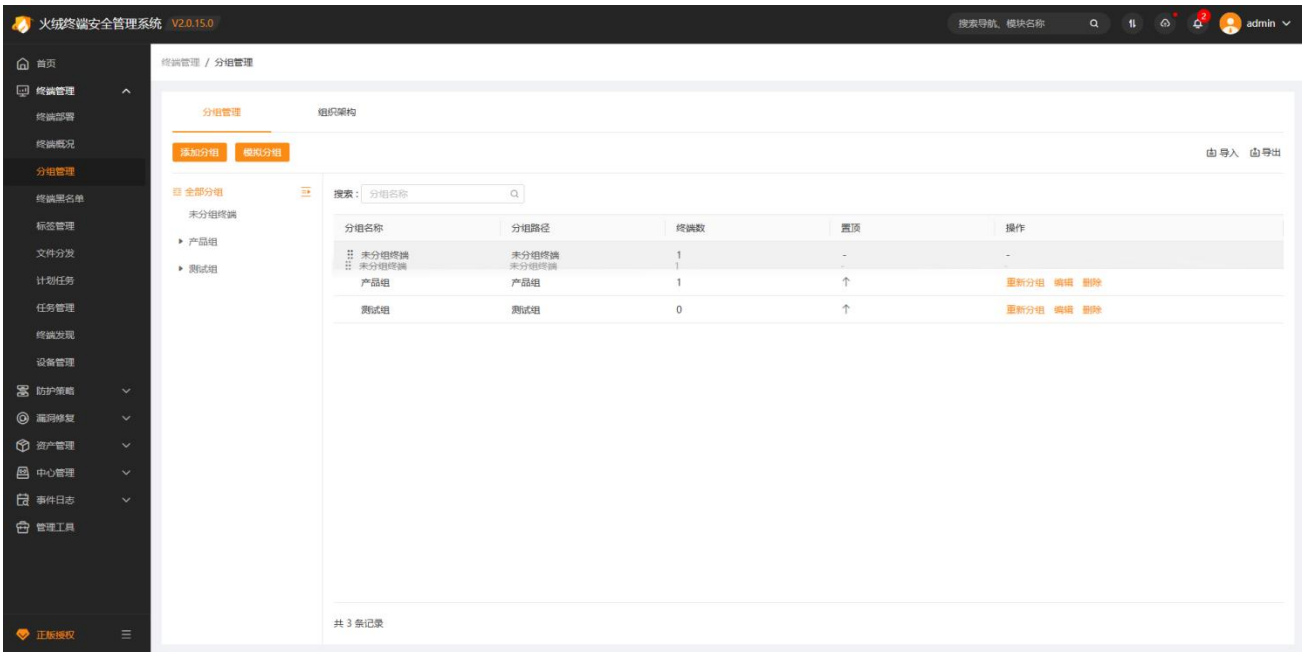
(5) 导入分组：火绒安全管理系统支持导入分组文件，根据导入的分组结构，调整中心分组，点击分组管理顶部导入按钮，显示导入分组窗口，可以下载导入分组的模板，填写后导入，文件导入成功后，点击确定按钮，更新当前中心的分组结构。

(6) 导出分组：点击分组管理页面顶部导出按钮，导出当前中心整体的分组结构，导出成功后，消息提醒中会有相关提示，下载后，可以查看中心的分组数据，包括分组名称和分组路径。

(7) 模拟分组：当管理员不知道新安装终端可能会移入哪个分组时，可以使用此功能预先试验，点击模拟分组，显示模拟分组窗口，根据提示填写信息，点击模拟，模拟该终端恰好匹配的分组，当有匹配的分组时，显示规则匹配的分组，当没有规则匹配，会提示没有恰好匹配的分组。



(8) 调整分组顺序：调整顺序的功能会同时改变分组的显示顺序和规则匹配顺序，鼠标移入分组名称左侧，显示移动分组的图标，此时，鼠标光标改变，按住鼠标拖动所在行即移动分组的顺序，鼠标松开后分组位置改变。如果想要目标分组显示在同级分组的顶部，点击指定图标，一键即可置顶。

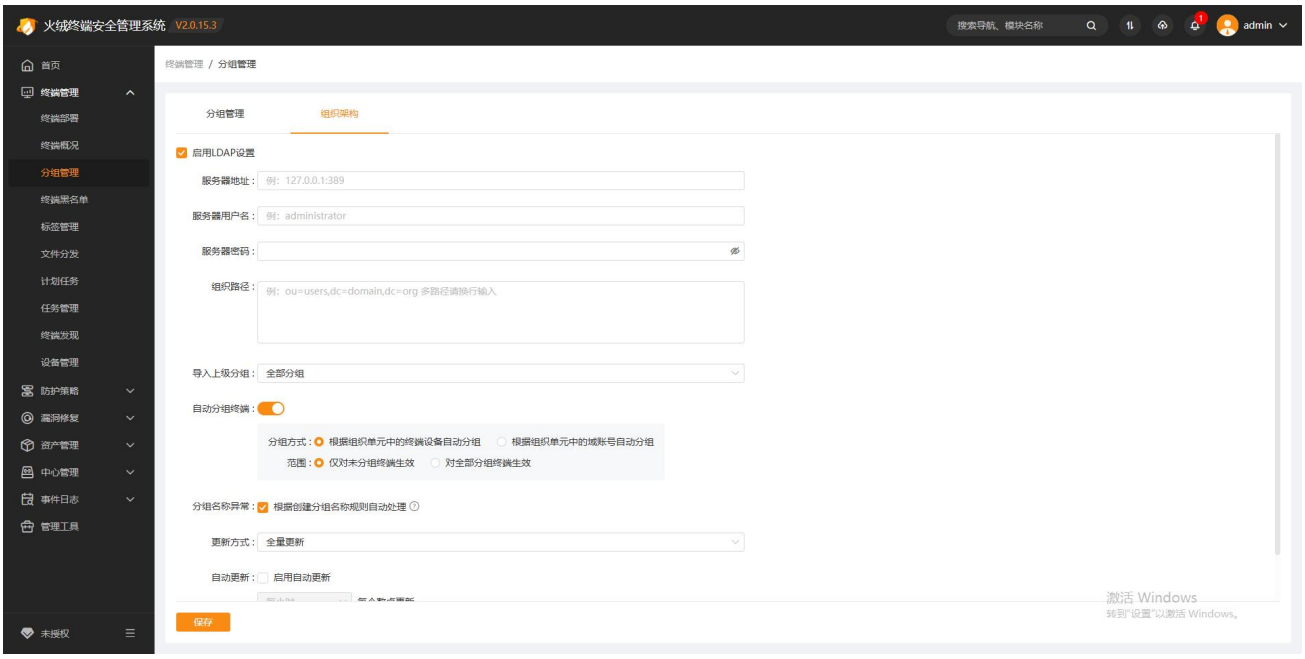


2. 组织架构

点击组织架构，分组管理切换至组织架构详情页，配置好数据源服务器及导入选项后，点击【立即更新】按钮即可开始同步源服务器组织架构数据。

未开启自动分组终端时，则仅更新组织架构；开启自动分组终端时，将根据设置将对应范围的终端按照设置的分组方式，重新自动分组。

更新方式：全量更新即 AD 域中增加和删除的组织单元会同步至控制中心；差量更新即 AD 域中增加的组织单元会同步至控制中心，AD 域中删除的组织单元不会同步至控制中心。

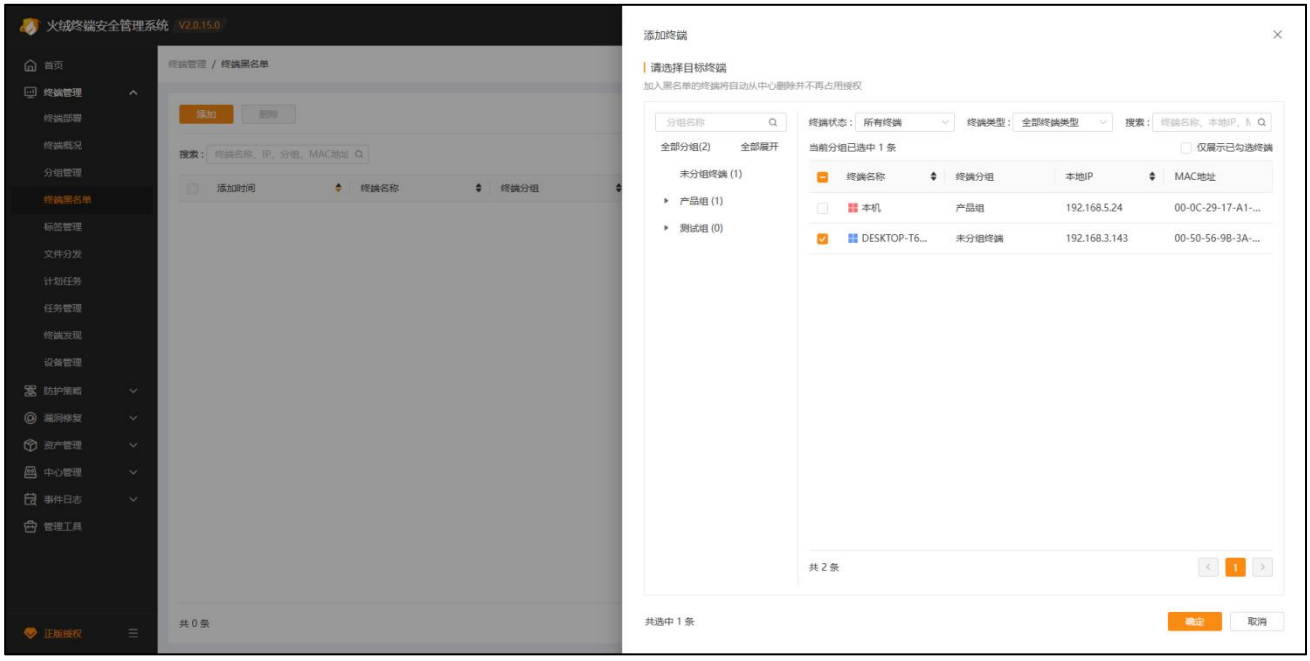


2.5.4 终端黑名单

1. 添加黑名单

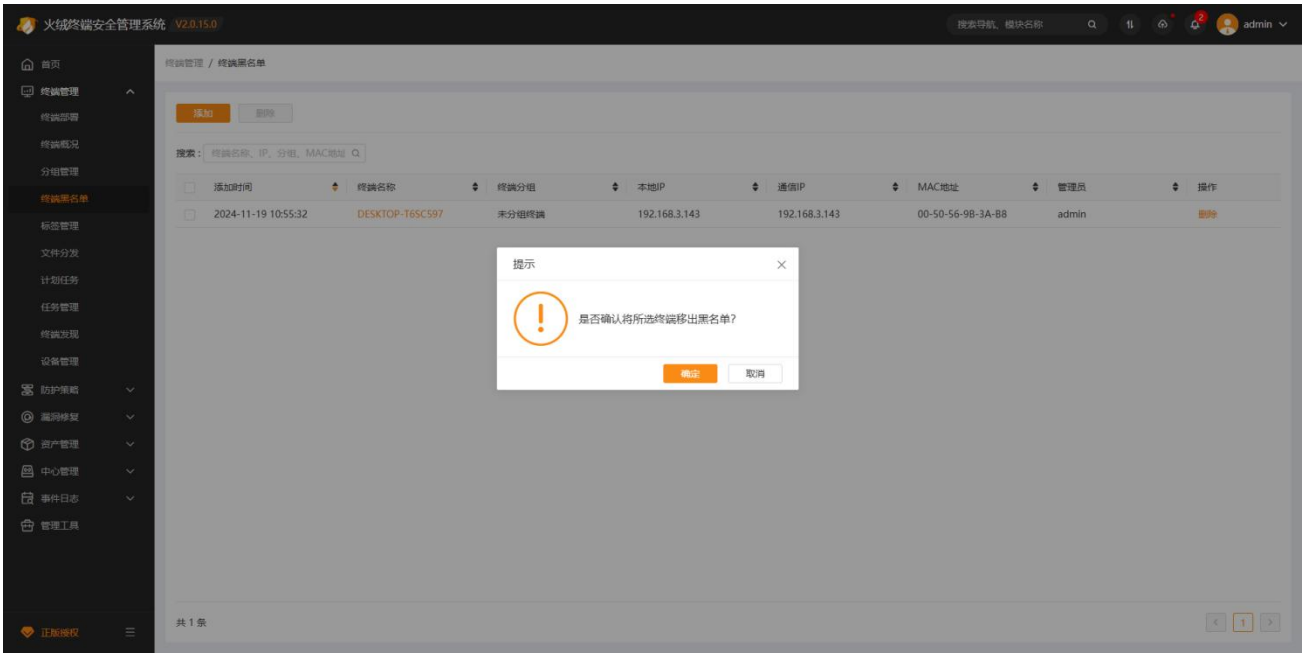
火绒终端安全管理系统支持添加终端黑名单功能，将终端添加至终端黑名单后，中心会将此终端拉黑并且不再占用授权。

用户选择目标终端，点击确定后即可将所选终端添加至黑名单中。



2. 删除黑名单

用户可在【终端管理】-【终端黑名单】界面中对已经加入黑名单的终端进行管理，点击黑名单终端右侧【删除】按钮，点击【确定】后可将黑名单终端恢复为正常终端。

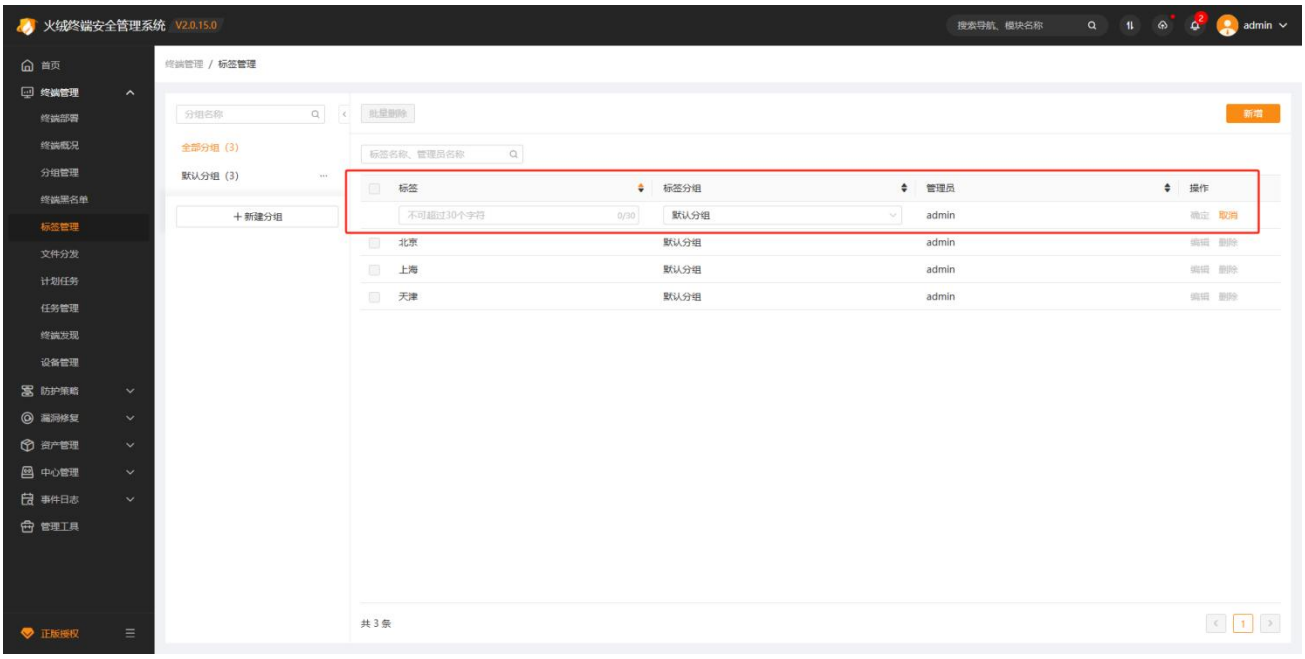


2.5.5 标签管理

火绒终端安全管理系统支持标签功能，用户可根据自身企业应用场景自定义标签，以此来作为条件对终端进行进一步区分，方便用户标识及管理企业内的终端。

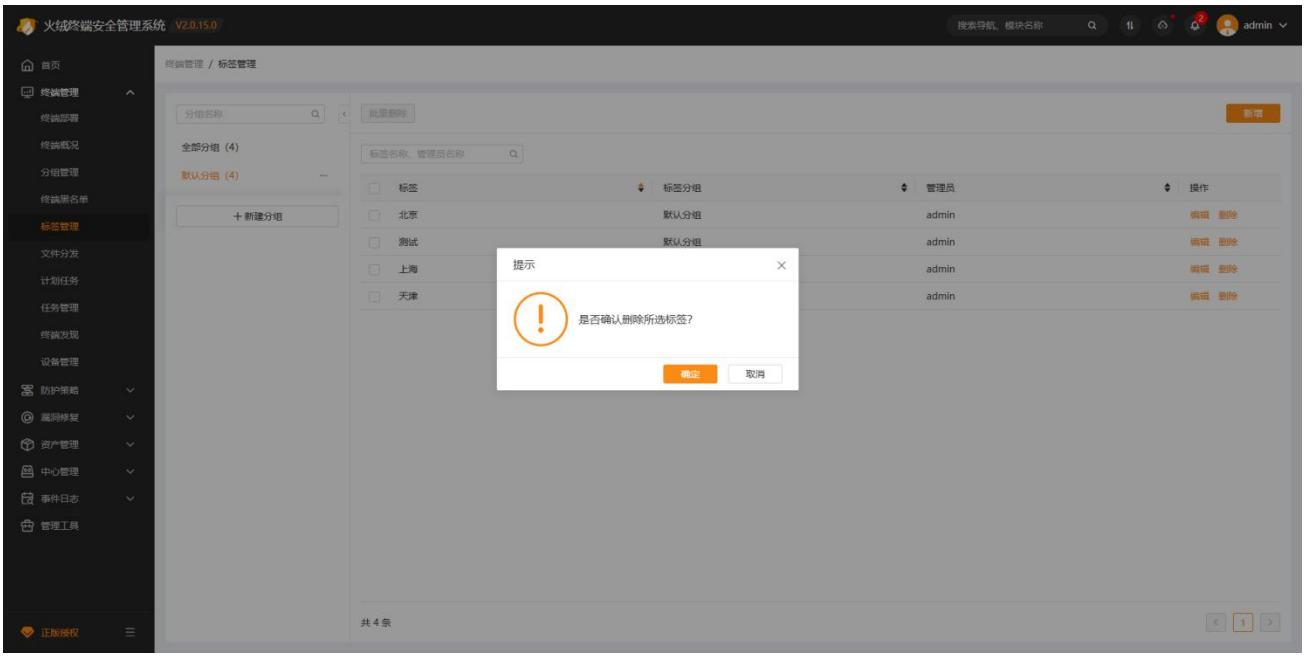
1. 新增标签

用户在【终端管理】-【标签管理】界面点击【新增】按钮，输入标签名称并选择标签分组，点击【确定】即可成功创建新标签。



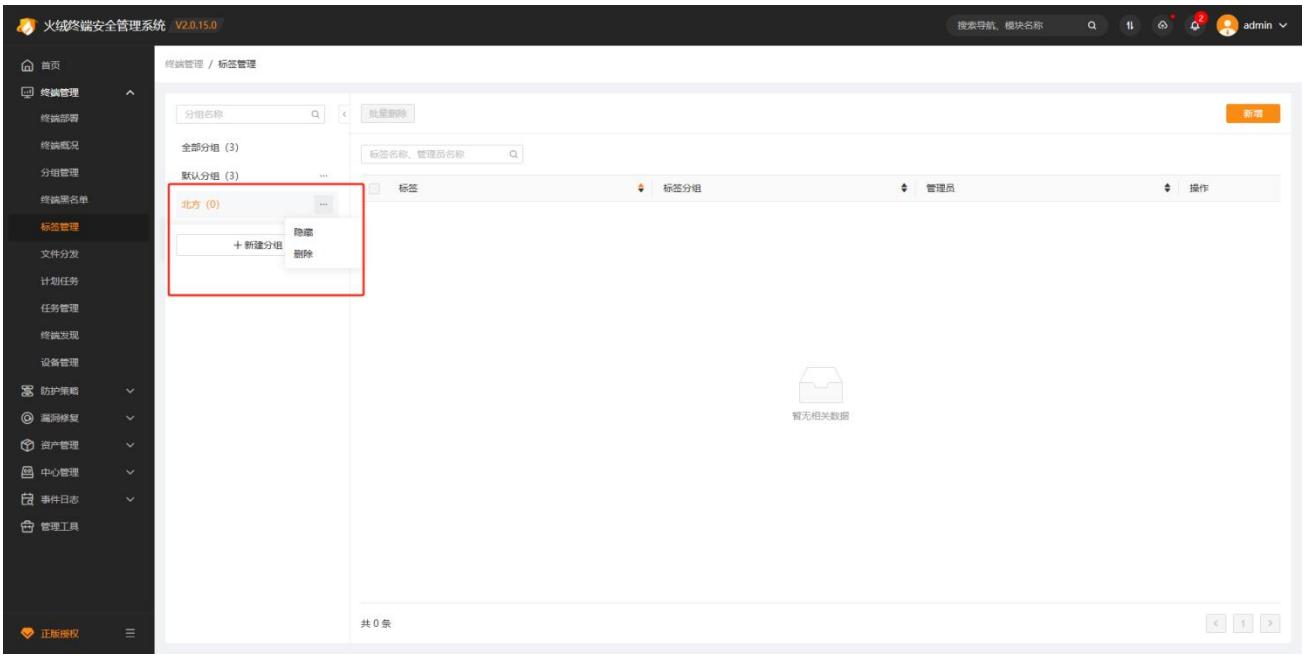
2. 删除标签

用户选中需要删除的标签，点击【删除】或【批量删除】按钮，点击【确定】后即可将当前选中标签删除，支持单个删除及批量删除。



3. 标签分组管理

用户可通过标签分组对同类型标签进行整理，方便查找及管理。用户可在【标签管理】界面左侧的分组列表中管理标签分组，支持新建、隐藏或删除标签分组。

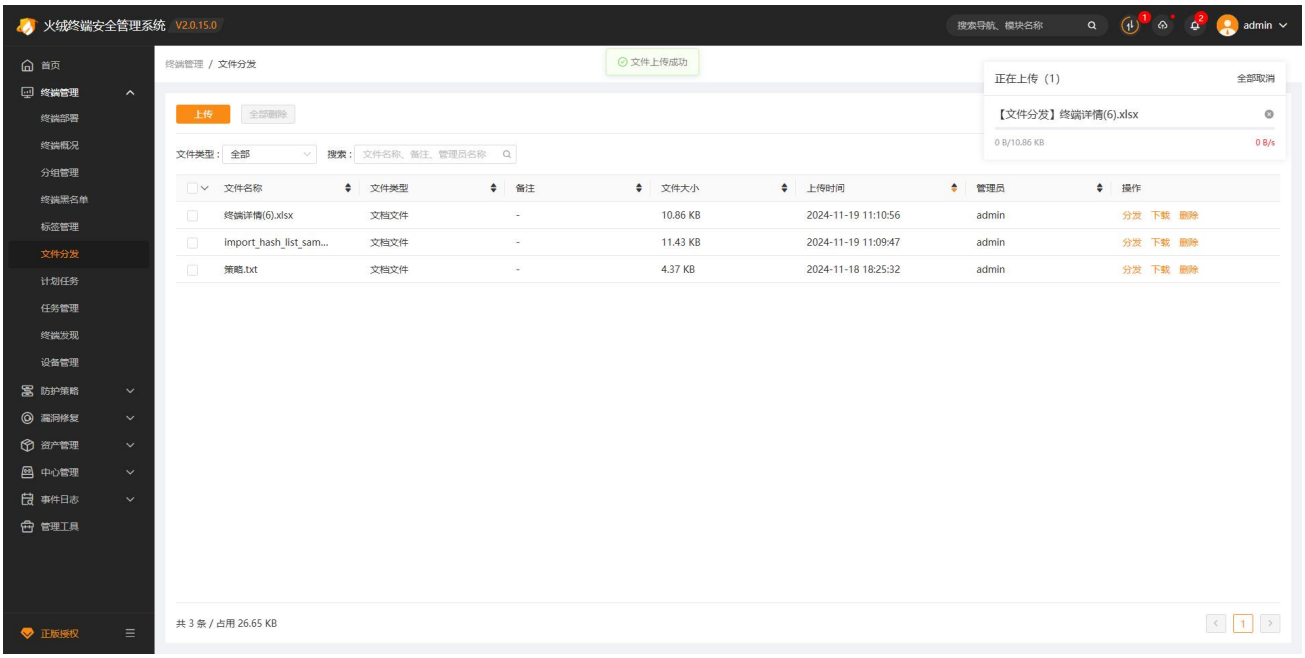


2.5.6 文件分发

火绒终端安全管理系统支持文件分发功能，通过文件分发用户可将文件下发至指定终端，方便用户对企业内终端及资产进行统一管理和维护。

1. 文件上传

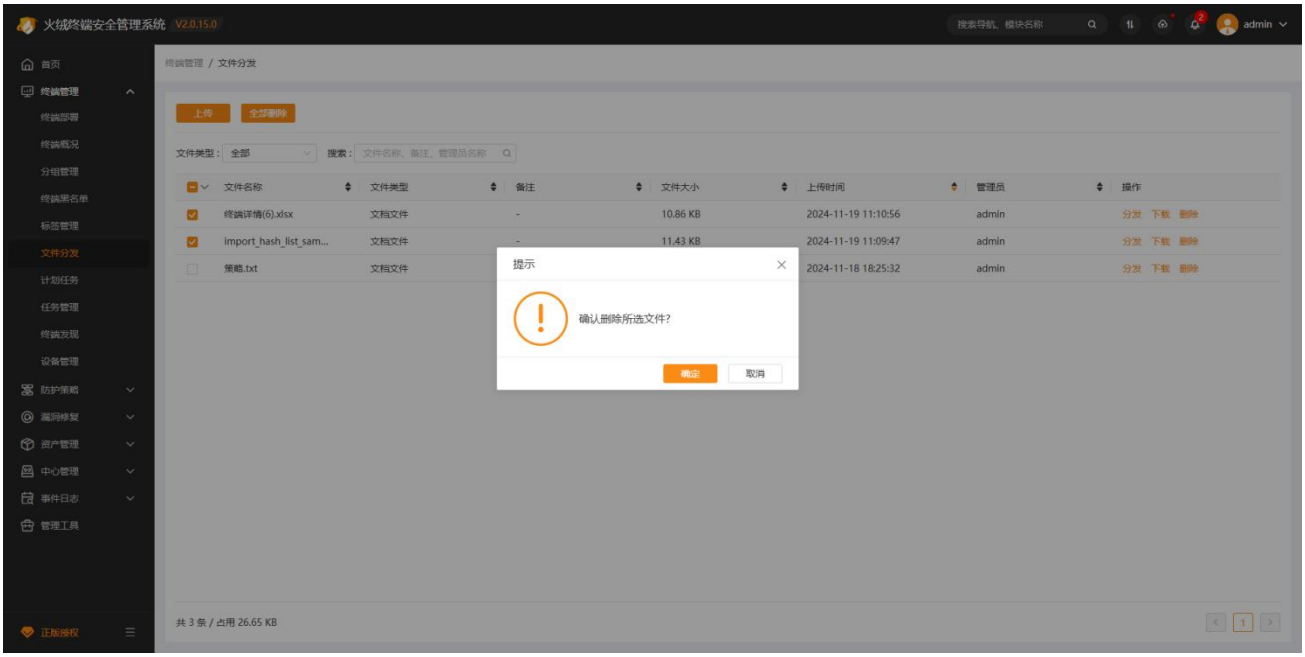
用户可在【终端管理】-【文件分发】界面点击【上传】将待分发文件上传至中心，单个文件大小不得超过 16GB，上传终端或失败时，可以再次选择文件继续上传、中心同一时间最多支持同时上传 3 个文件。



上传的任务进度在页面顶部导航栏查看。

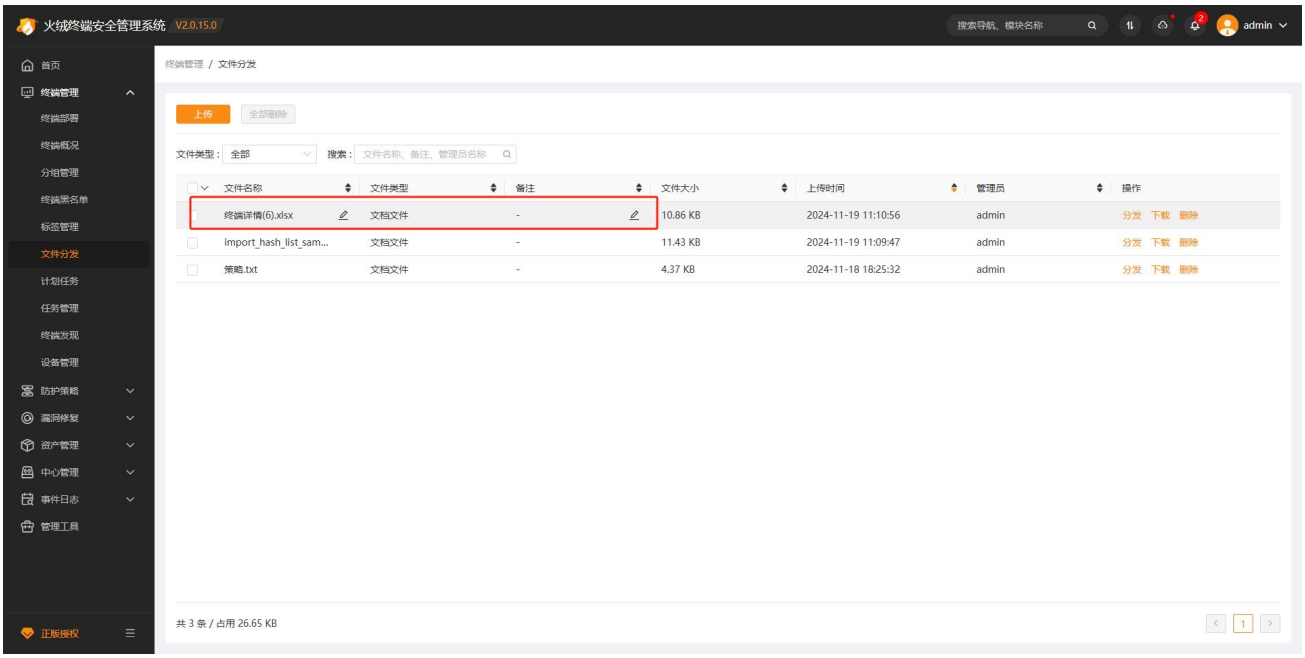
2. 文件删除

用户可在【终端管理】-【文件分发】界面选中需要删除的文件或点击右侧删除按钮，将上传至中心的文件删除，支持单条删除及批量删除。

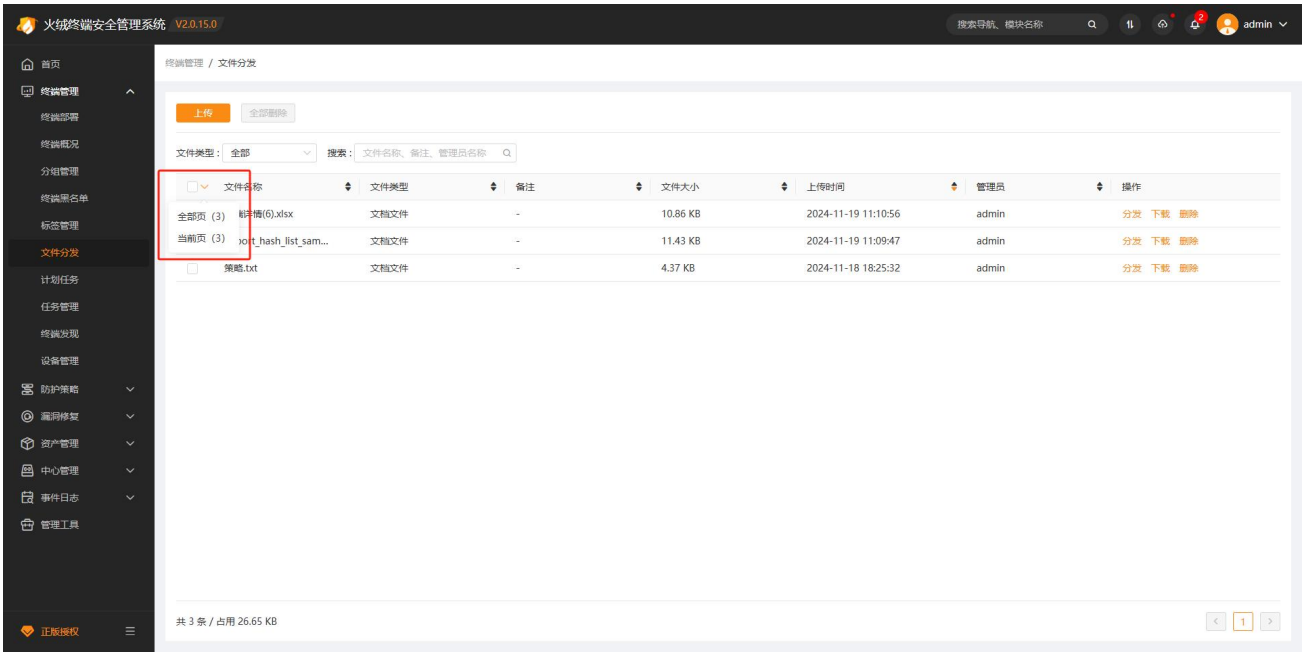


3. 编辑文件名称、备注

文件上传成功后，支持在列表中编辑文件名称和备注。



表头支持一键全选当前页所有文件，以及一键全选全部页的所有文件。



4. 文件分发

用户可在【终端管理】-【文件分发】界面点击右侧【分发】按钮，进入文件分发界面，选择目标终端后，点击下一步，设置分发方式、存储位置、终端提示、运行参数及任务有效期后，点击【确定】即可将所选文件分发至指定终端。

（1）分发方式：分发方式分为三种，分别是仅接收、接收并运行和以系统权限运行；选择仅接收时，

终端仅将文件接收并存储至所选位置，不会自动运行；选择接收并运行时，中心下发分发任务后，终端接收到文件会自动运行；选择以系统权限运行时，终端接收到文件后将在服务会话下运行文件，无法显示程序界面。

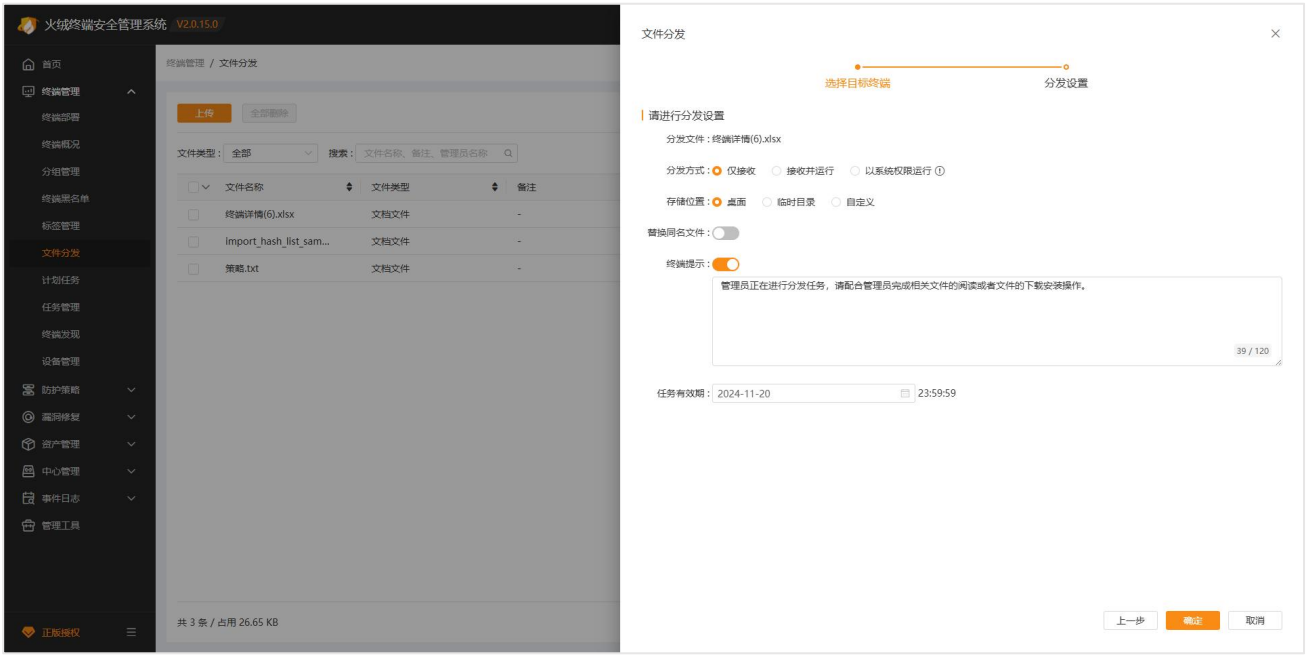
（2）存储位置：分发方式选择接收并运行或者仅接收时，可选存储位置为系统桌面、系统临时目录、自定义；选择【自定义】时，支持用户自定义存储路径，终端接收任务后发现不存在该自定义目录时，将自动创建该目录；分发方式选择以系统权限运行时，存储位置固定为系统盘根目录。

（3）替换同名文件：勾选时，终端接收任务后，检测到已存在同名文件时，将自动替换同名文件；不勾选时，终端接收任务后，检测到已存在同名文件，将自动将分发的文件重命名为示例文件（1）、示例文件（2）、以此类推。

（4）终端提示：勾选则下发分发任务后终端弹出提示框提示用户，不勾选则后台执行分发任务，不会弹框提示用户。

（5）运行参数：用户可自定义输入运行参数，文件分发任务下发至终端后，可依照输入的运行参数运行当前分发文件。

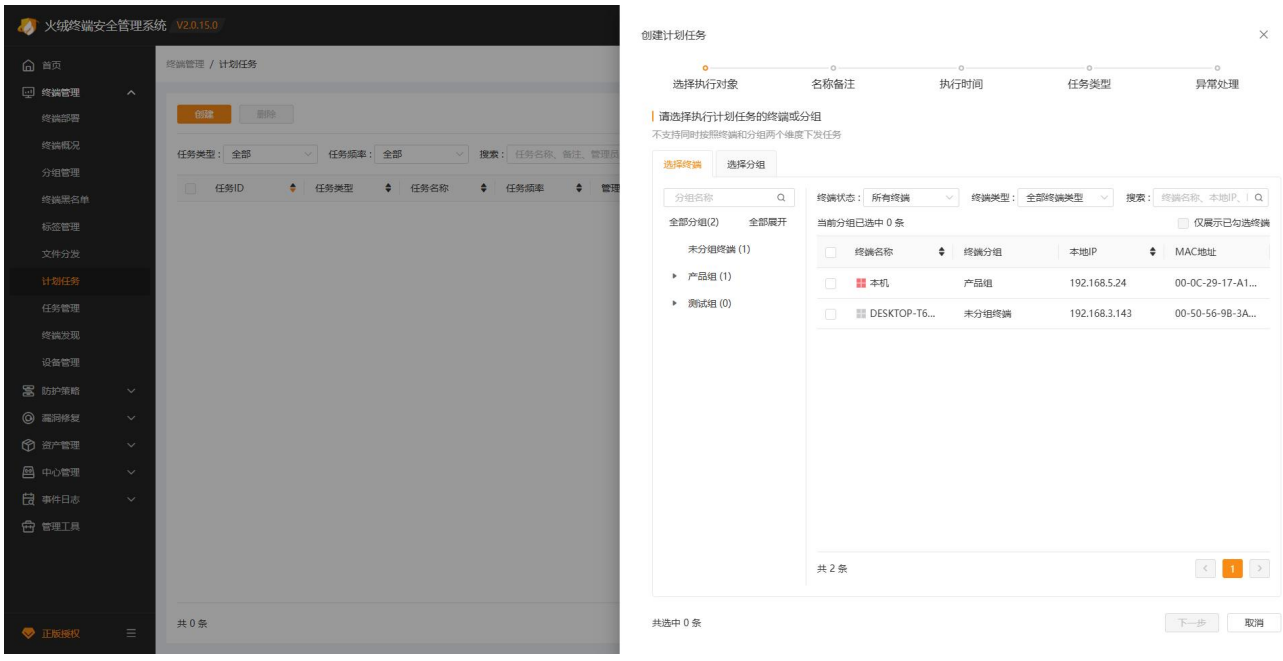
（6）任务有效期：用户可自行设定任务有效期，超过设定有效期限后，此条分发任务不再继续分发执行。



2.5.7 计划任务

火绒终端安全管理系统支持建立定时计划任务功能，可帮助用户定时执行任务，减少企业运维成本，降低管理员工作量，还可避免因长时间不进行安全扫描而带来的巨大的安全隐患。

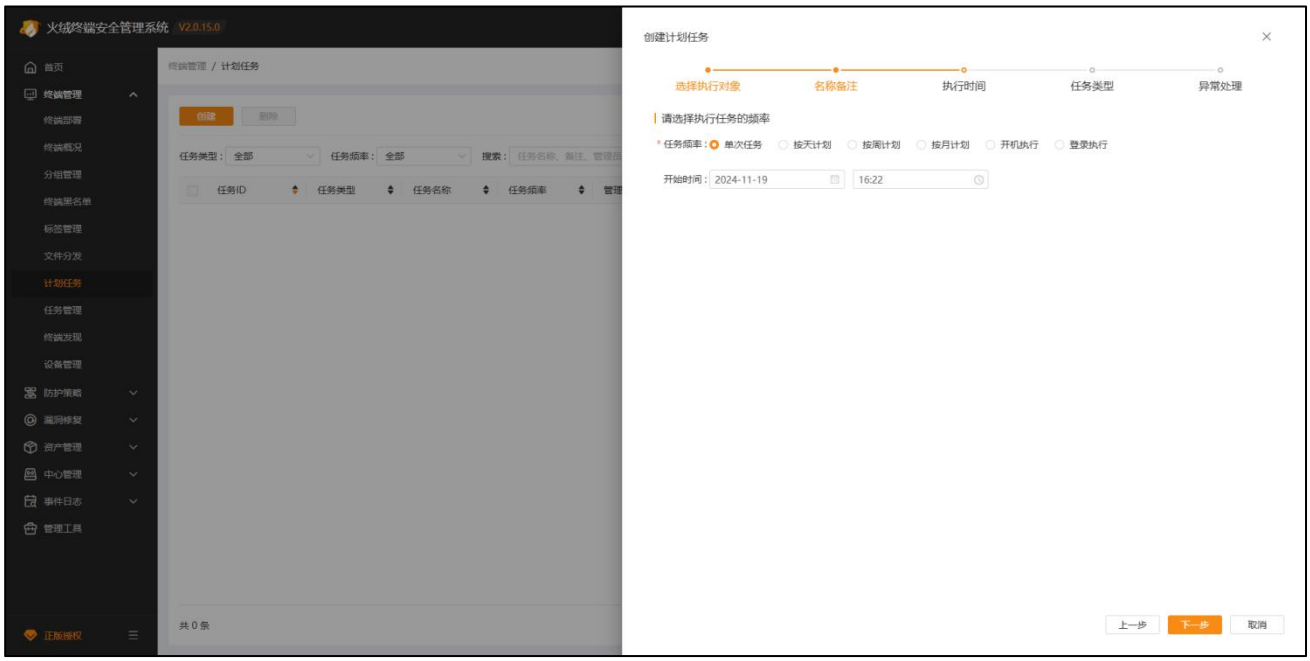
1. 创建计划任务



用户可在【终端管理】-【计划任务】界面点击【创建】按钮进入新建计划任务界面，步骤按钮不可切

换，需按引导先选择执行计划任务的对象，可以按终端添加或按分组添加，点击【下一步】，查看计划任务执行对象列表，确认执行计划任务的执行对象后，点击【下一步】，设置计划任务的名称和备注，可以修改计划任务的名称，设置该任务的备注信息，以便于后续管理，点击【上一步】可以查看执行计划任务的对象，点击【下一步】，选择执行该计划任务的时间，选择【单次任务】，则该计划任务只会根据执行时间，执行一次计划任务，选择【按天计划】、【按周计划】、【按月计划】、【开机执行】、【登录执行】等执行任务频率，将会根据任务频率，结合具体执行计划任务的时间，多次执行计划任务，设置好计划任务的【执行时间】后，点击【上一步】，可以查看、修改计划任务的名称和备注信息，点击【下一步】可以设置计划任务的具体类型；下方为各设置项含义：

（1） 任务频率：可选设置计划、单次任务、开机执行和登录执行，选择设置计划时，任务将按照用户自定义的时间频率进行任务执行；选择单次任务，任务将按照用户设定的时间执行一次；选择开机执行，任务会在每次开机时自动执行；选择登录执行，任务会在每次用户登录时自动执行。



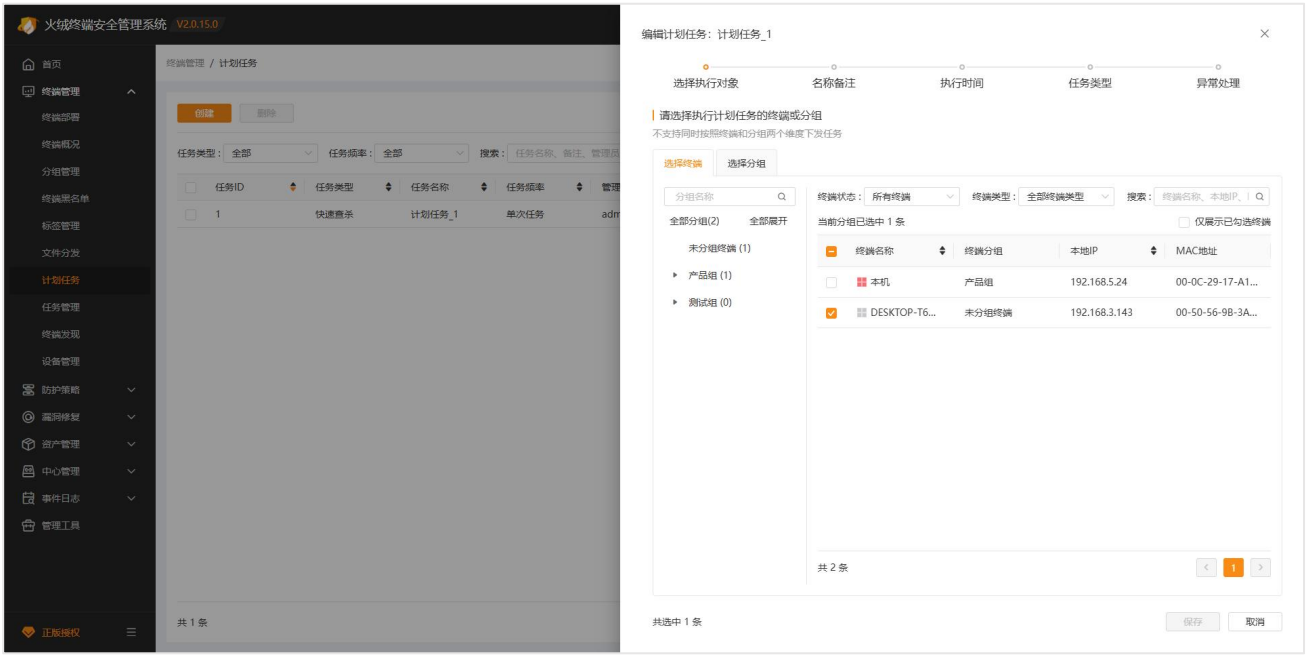
（2） 执行任务：企业版 2.0 目前支持的计划任务有九种，分别是：快速查杀、全盘查杀、自定义查杀、漏洞修复、终端升级、发送通知、垃圾清理、关机、重启；用户可根据自身需求自行选择

计划任务进行设定并下发至终端。

设置完计划任务的【任务类型】后，点击【上一步】，可以查看、更改执行计划任务的时间和频率，点击【下一步】，配置计划任务的【异常处理】设置，可以根据需求设置计划任务执行过程中出现异常情况的处理方案，此页面设置完成后，点击【上一步】，可以查看修改计划任务的【任务类型】，点击【完成】，中心将对计划任务选择的【执行对象】下发计划任务，终端将根据计划任务具体的执行时间、频率、任务类型和异常处理设置去执行计划任务。

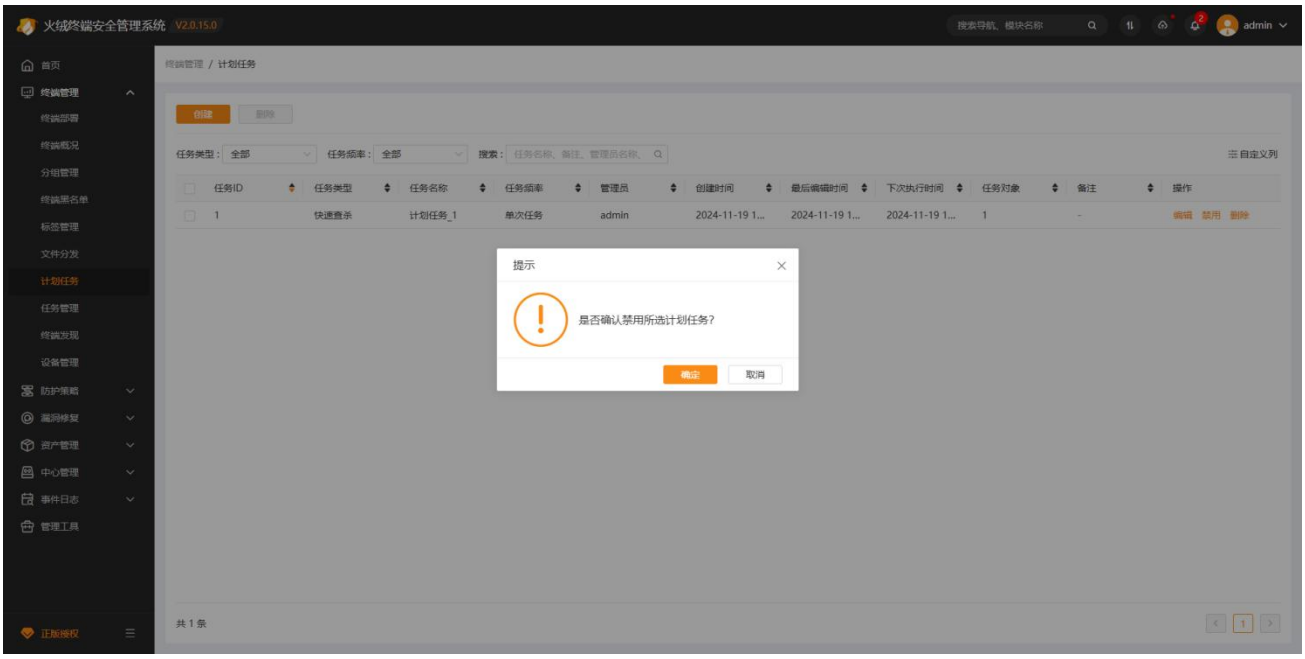
2. 编辑计划任务

用户可以对创建后的计划任务进行编辑，点击【编辑】后，可在弹窗标题栏中查看计划任务名称，在下方内容中，点击上方步骤按钮可以随意切换查看该计划任务的各项配置，在每个页面修改设置后，都可以点击【保存】按钮，保存对该计划任务的修改。



3. 禁止/启用计划任务

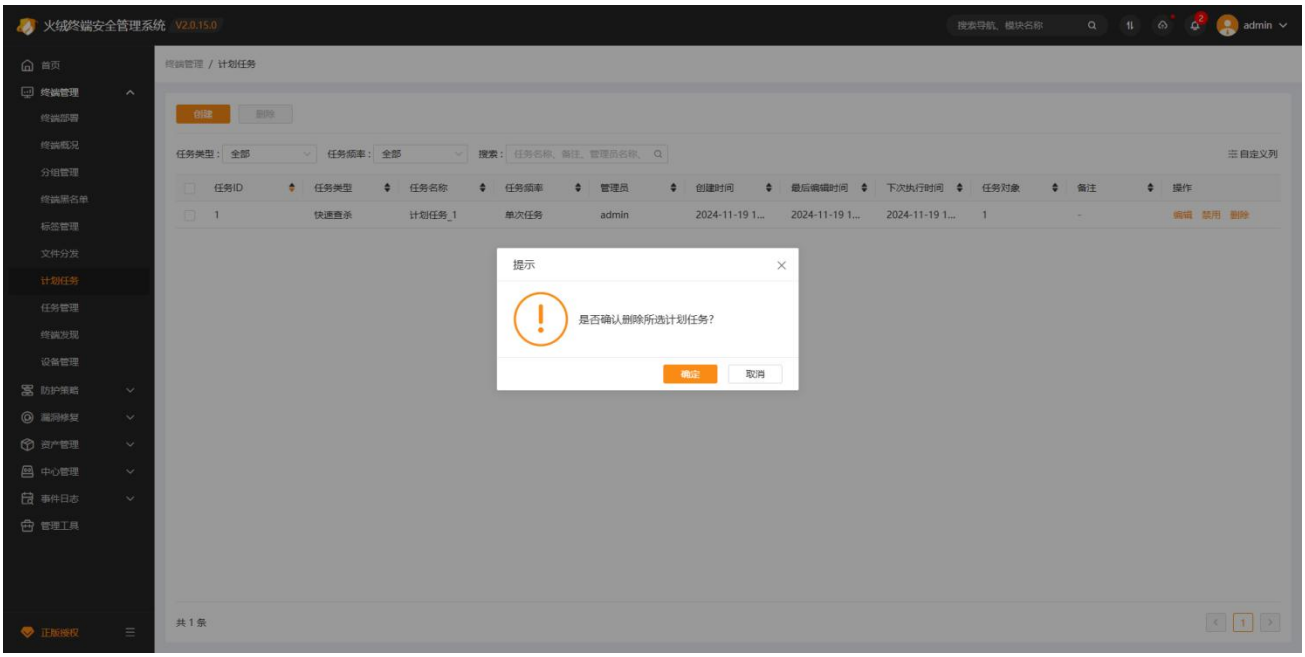
用户可以禁止执行在执行状态中的计划任务，点击【禁用】，会提示是否确认禁用所选计划任务，确认后将禁用该计划任务，禁用后，禁用按钮显示为启用，点击【启用】，将会启用被禁用的计划任务。



4. 删除计划任务

用户可通过选中需要删除的计划任务，点击上方导航栏中【删除】按钮，或直接点击右侧【删除】按

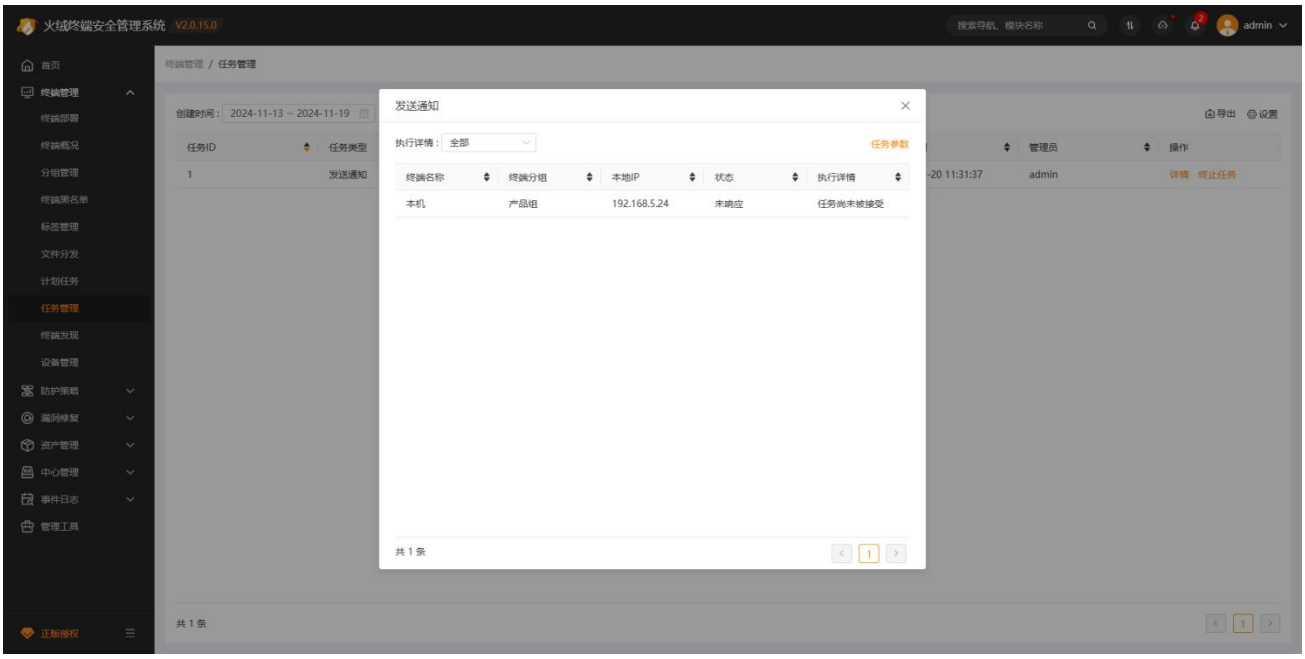
钮对已经创建的计划任务进行删除，支持单条删除及批量删除，计划任务删除后终端后续将不再执行此任务。



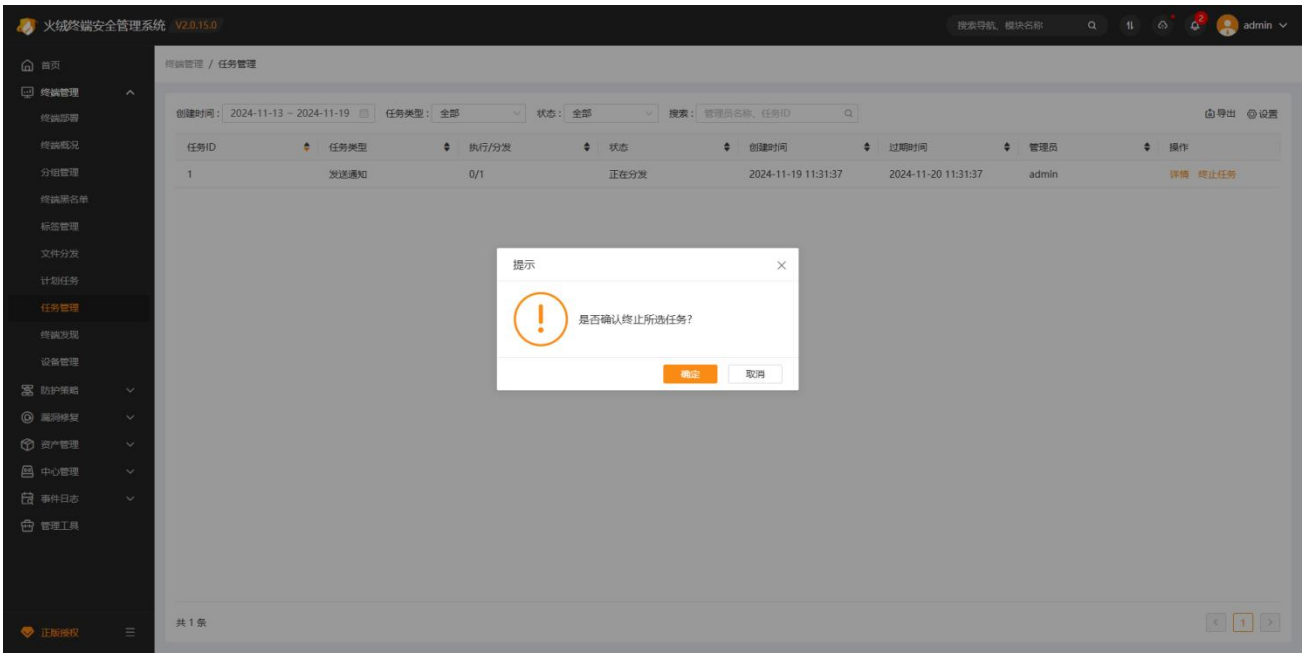
2.5.8 任务管理

火绒终端安全管理系统支持对当前中心所下发的所有任务进行留痕和管理，用户也通过任务管理查看已下发任务的状态和对待执行任务进行终止。

用户可在【终端管理】-【任务管理】界面查询任务，点击【详情】查看当前任务状态。



用户可在【终端管理】-【任务管理】界面查询任务，找到状态为正在分发的任务点击【终止任务】对当前任务进行终止执行。

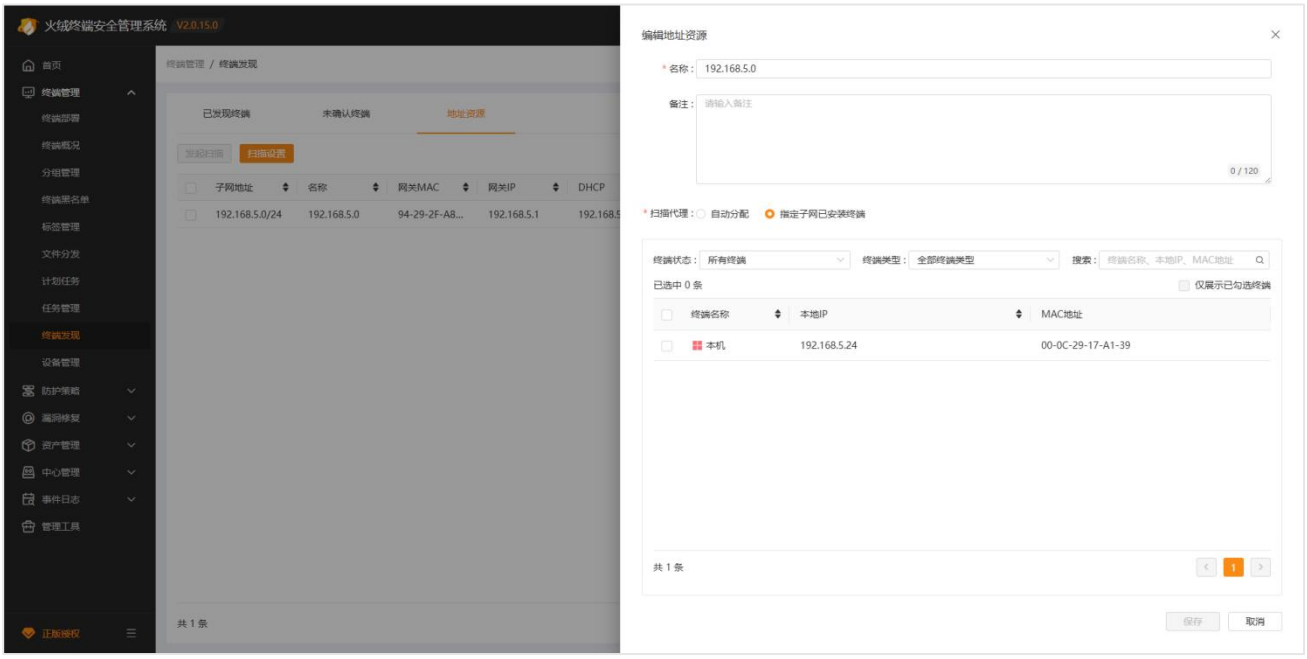


2.5.9 终端发现

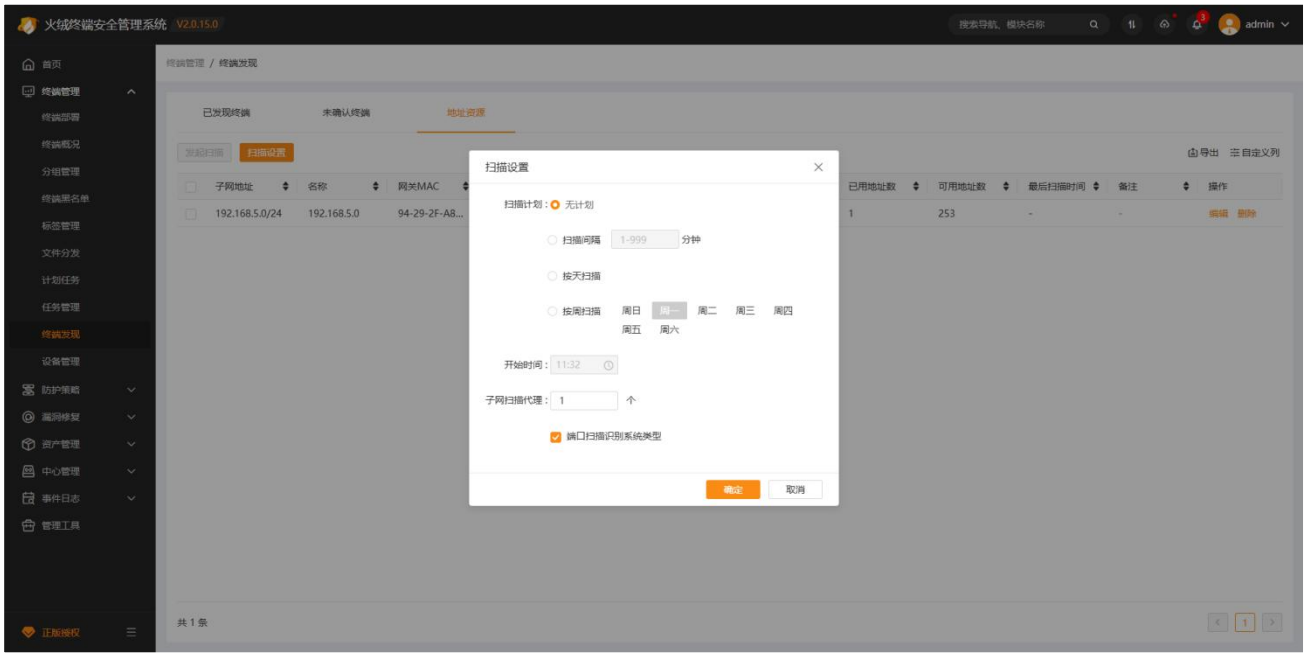
终端发现功能可以帮助管理员发现中心子网地址下，需要安装但没有安装火绒安全终端的计算机，以免出现漏管漏控的情况，此功能分为地址资源、未确认终端和已发现终端三个页面。

1. 地址资源

火绒安全管理系统中心和终端安装部署完成后，终端会上报所在子网的地址资源数据，可以查看当前地址资源信息，编辑子网的名称，给子网设置扫描时的代理终端。



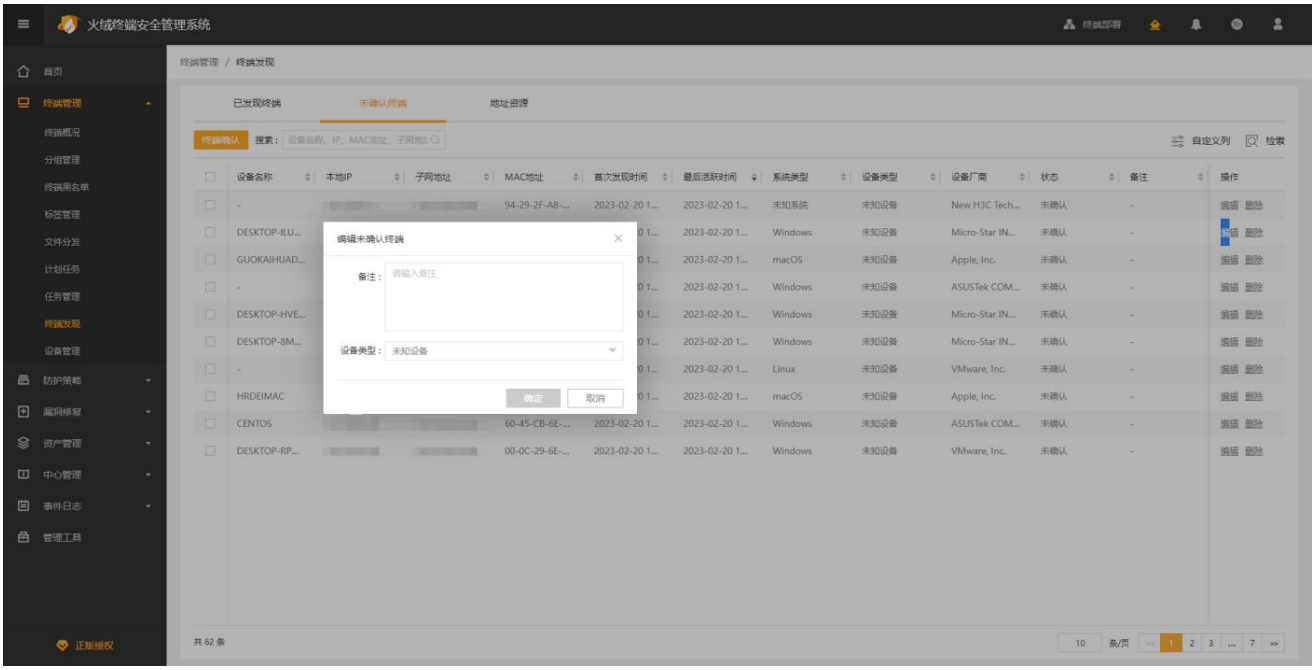
（1） 扫描设置：统一设置中心所有子网的扫描配置。点击扫描设置按钮，显示扫描设置窗口，可以设置终端发现扫描子网的频率、扫描计划开始的时间，子网扫描代理数量以及是否在端口扫描时，识别系统各类。



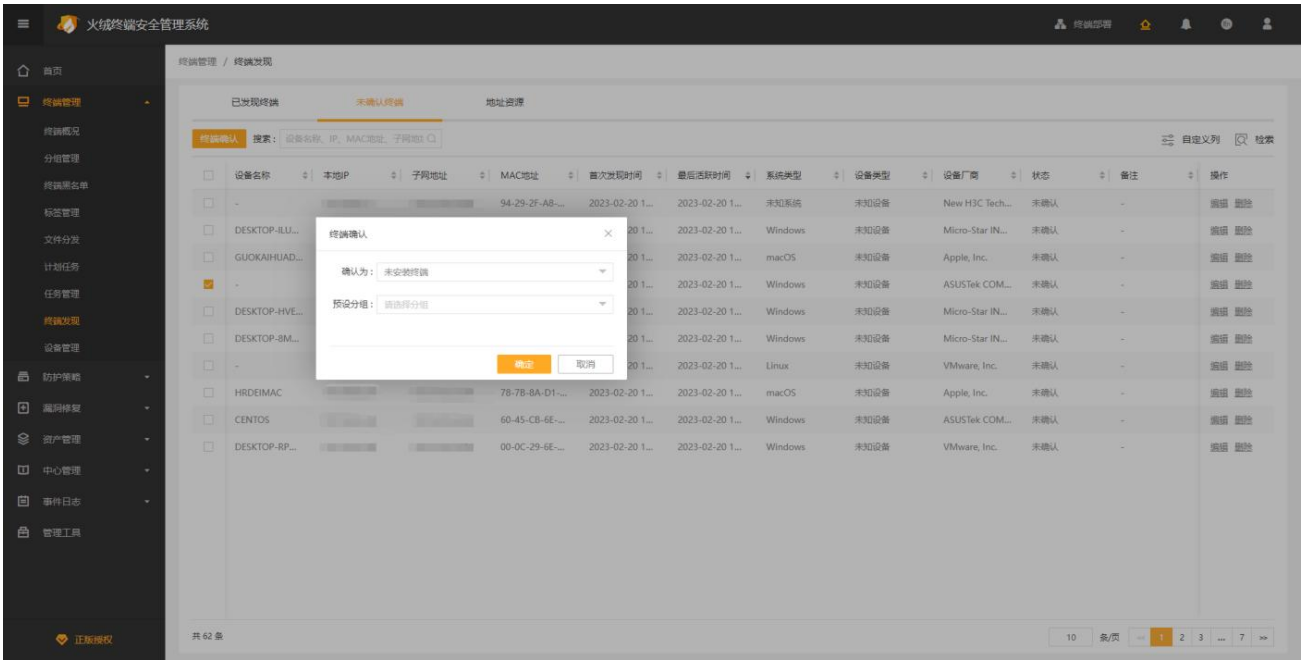
（2） 发起扫描：选择子网点击发起扫描按钮，会对所选子网的代理终端发布即时扫描任务。

2. 未确认终端

（1） 编辑设备：扫描发现的设备，会在未确认终端列表中显示，管理员可以根据列表显示的设备信息，编辑设备的备注和类型。

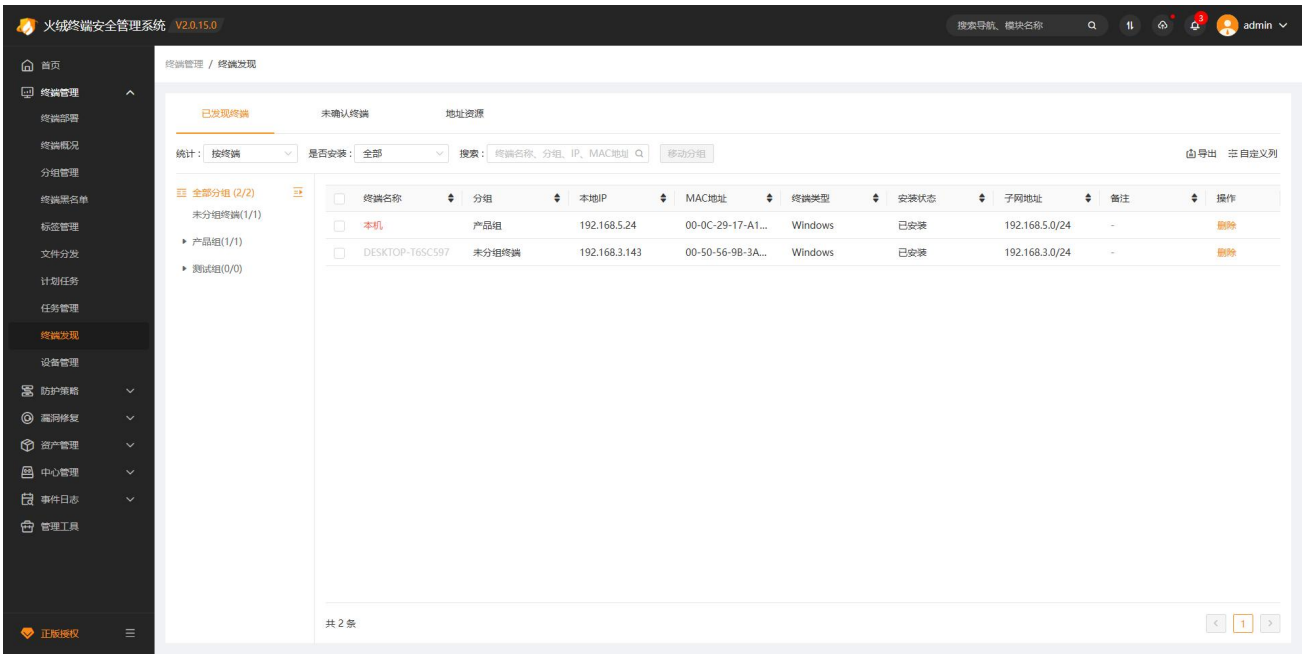


（2） 终端确认：再根据设备的类型信息确认目标设备是否为需要安装的终端，如果确认为需要安装但未安装的终端设备，可以为该终端预设分组，待安装上线后，移入对应的分组中。

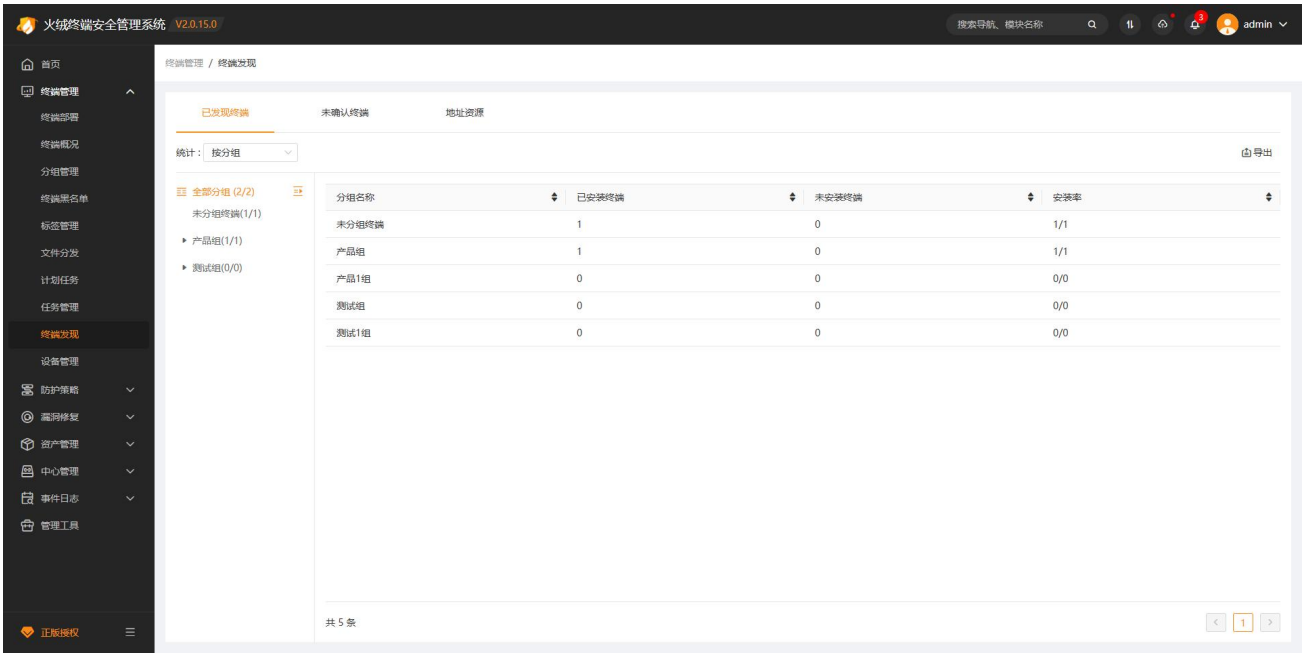


3. 已发现终端

已确认终端需要安装的终端设备，会按分组显示在已发现终端列表中，可以根据此列表的信息管理单位内部需要安装火绒安全终端的计算机设备。



可以导出已发现终端和数据，按终端查看时，导出的是所选分组已发现终端的详情数据，按分组查看时，导出的是各分组已发现终端的统计数据。



2.5.10 设备管理

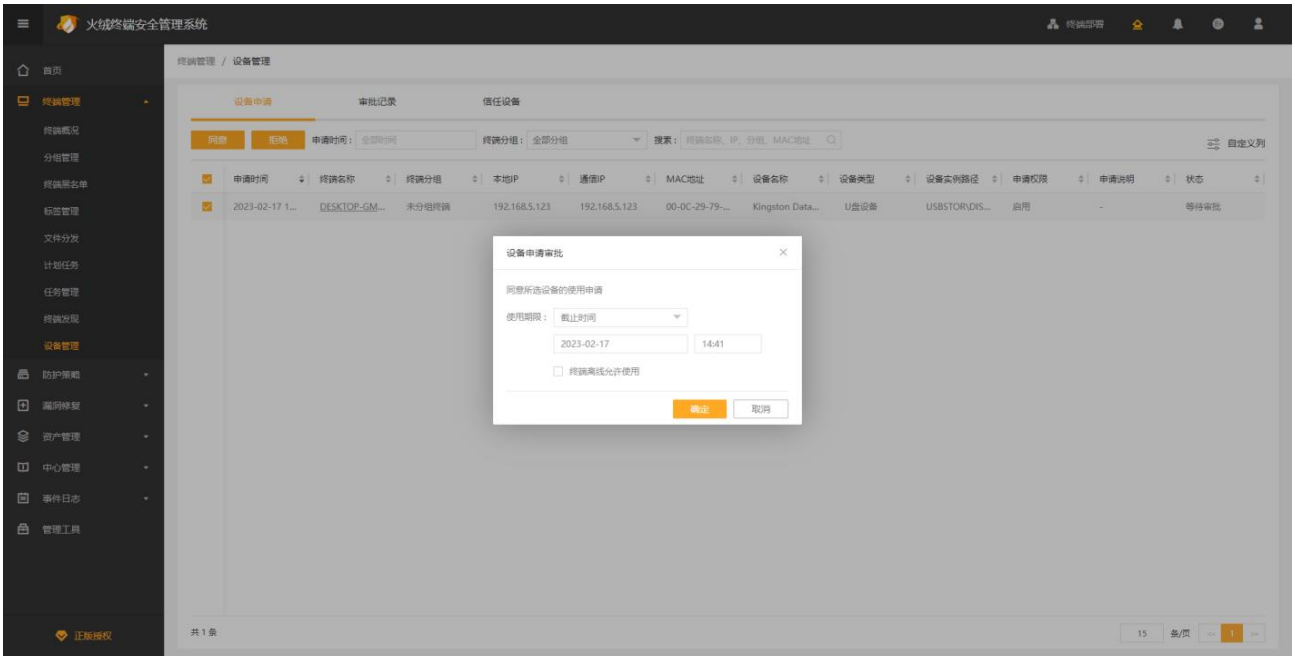
中心访问控制策略——设备控制开启后，对应部署该策略的终端用户使用设备会被限制，此时如果管理员不想改变整体防护策略，而终端用户又有需要使用某些设备，就只能通过添加白名单的方式来解决（中

心如果开启了密码保护，管理员还需要向终端用户发送密码），而终端通过白名单添加的设备使用时间和权限都不可控，会存在一定的风险。

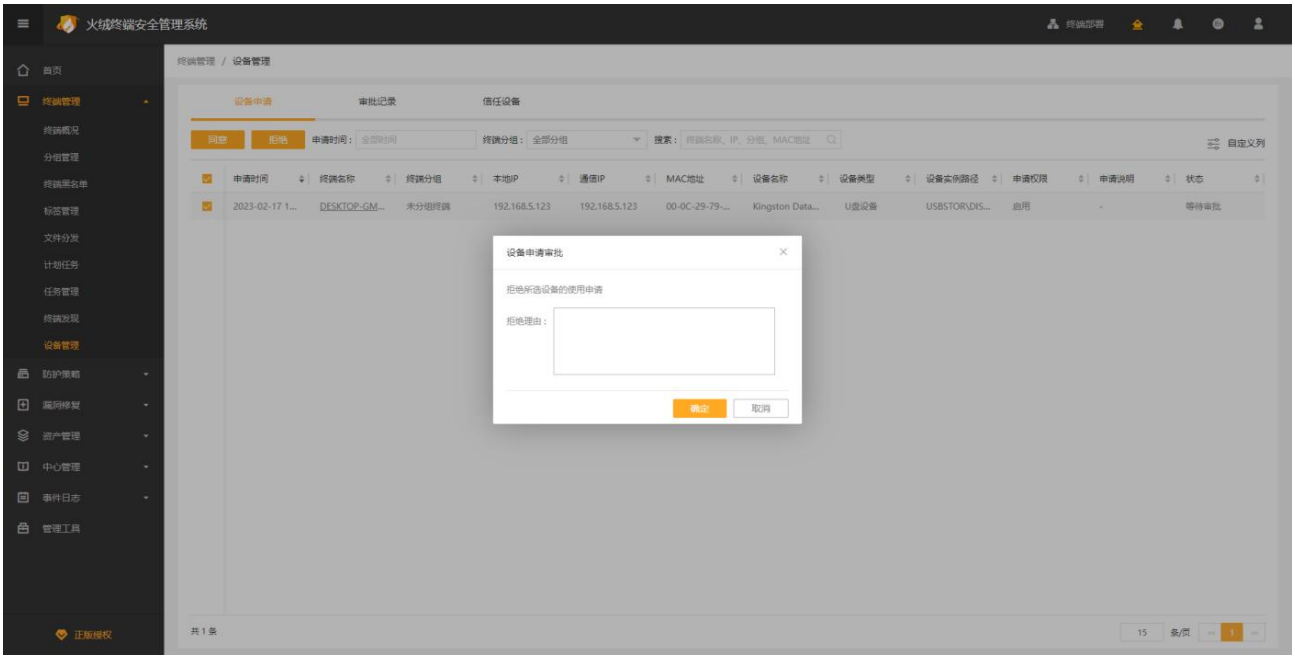
设备管理功能让需要使用禁用设备的终端用户主动向中心发起申请，中心管理员审批通过，该终端才能使用此设备，审批时管理员能够设置该设备的使用期限，审批通过的设备信息会显示在设备管理——信任设备的列表中，管理员随时能够删除此信任设备。

1. 设备申请

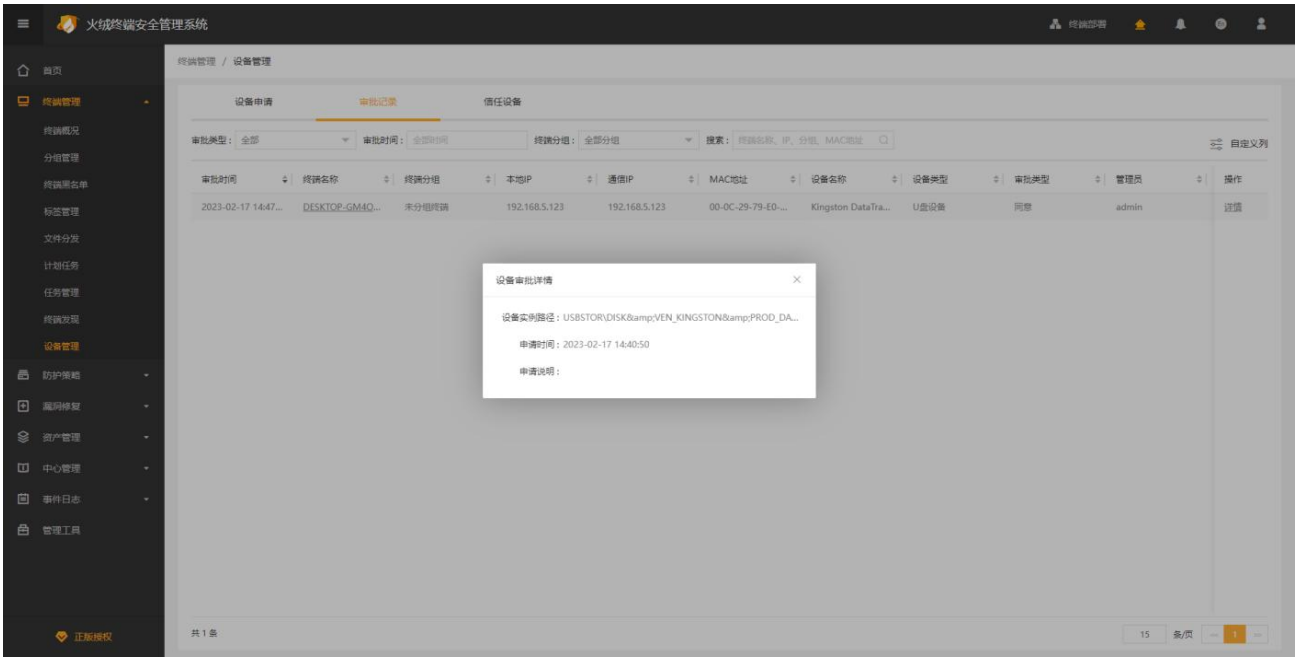
（1） 审批同意：终端提交的设备使用申请会显示在此列表中，管理员勾选设备后，点击【同意】或【拒绝】按钮，对审批进行统一处理，同意审批时可以设置该设备的使用时间，拒绝审批时可以填写申请理由，管理员审批过后，将会发送通知告知终端用户。



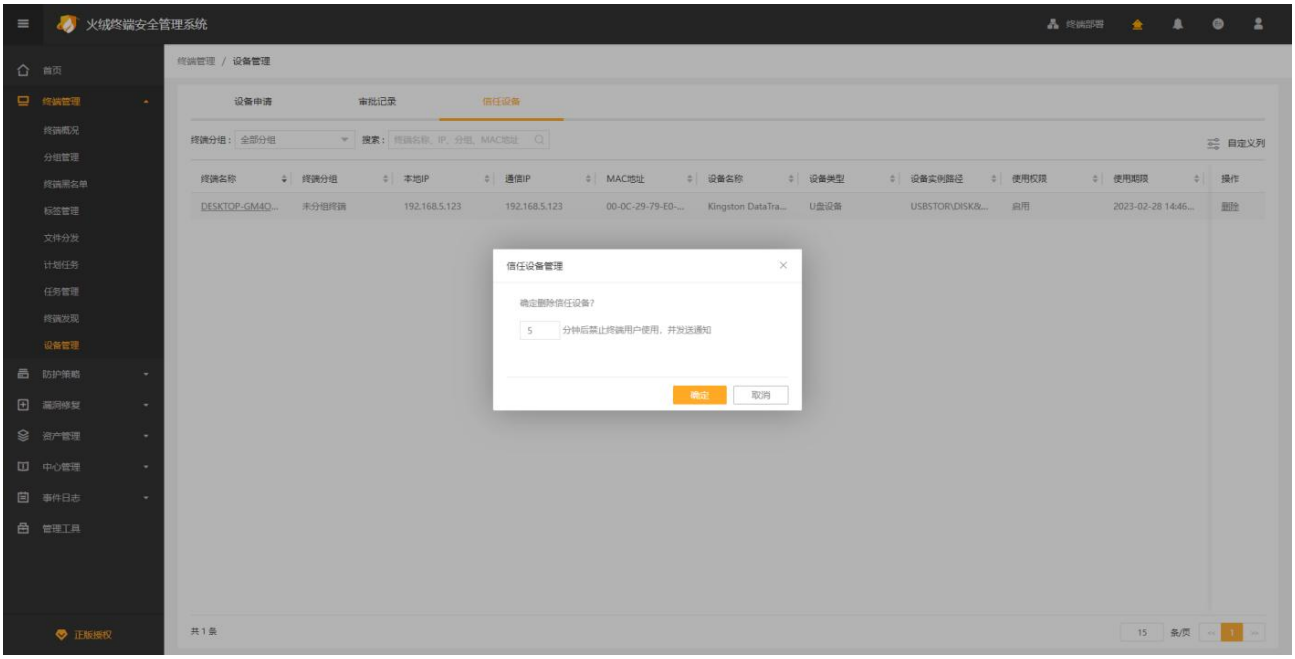
（2） 审批拒绝



（3） 审批记录：管理员审批过的设备申请记录，会保留在此列表中，可以根据审批类型、审批时间、终端基本信息进行筛选和模糊搜索，支持自定义列。点击操作列【详情】按钮，能够查看终端用户提交申请的详情信息。



2. 信任设备



审批通过的设备信息显示在此列表中，可以根据终端基本信息进行筛选和模糊搜索，支持自定义列。

管理员可以点击操作列【删除】按钮，删除信任设备，删除信任设备时会给终端用户发送禁用相关设备的通知，并为终端用户预留一定时间，避免因直接禁用设备造成数据丢失，删除信任设备后，终端将禁用该设备，可以再次申请使用。

2.6 防护策略

火绒终端安全管理系统为用户提供了安全策略部署功能，支持自定义安全策略配置，适配企业内复杂的安全防护场景，方便用户管理及防护企业终端环境。

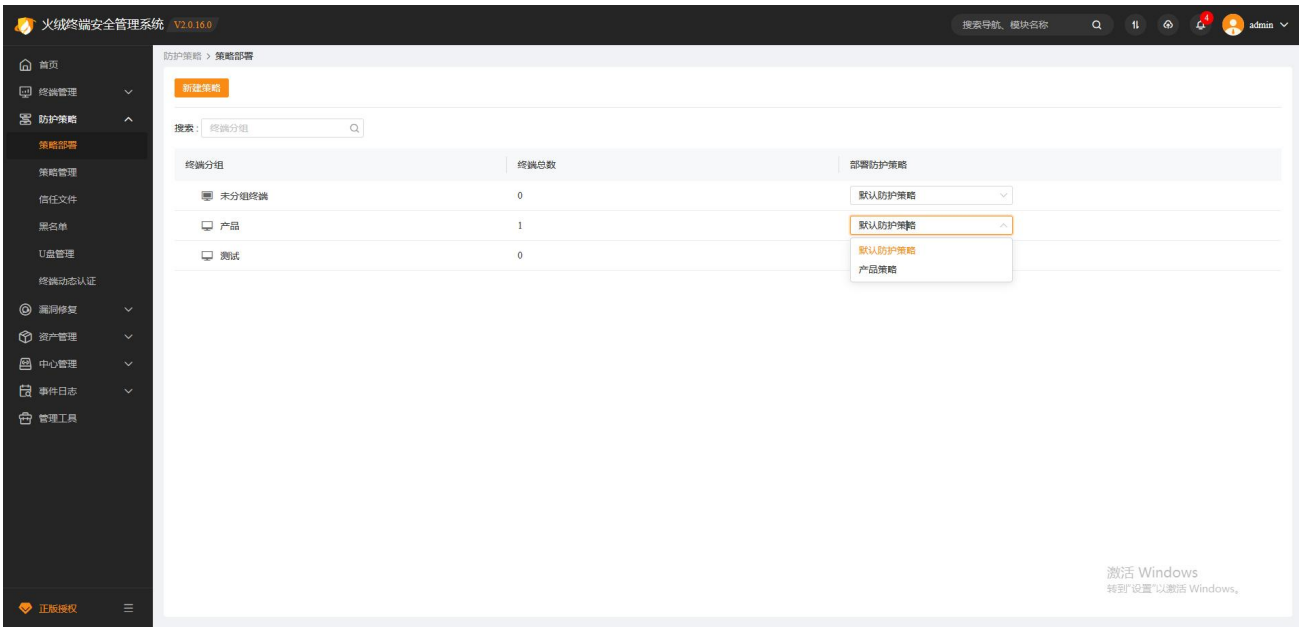
2.6.1 策略部署

用户可以在【防护策略】-【策略部署】界面查看及分配部署安全策略至不同的终端分组，也可在当前页面创建新策略。

1. 策略部署

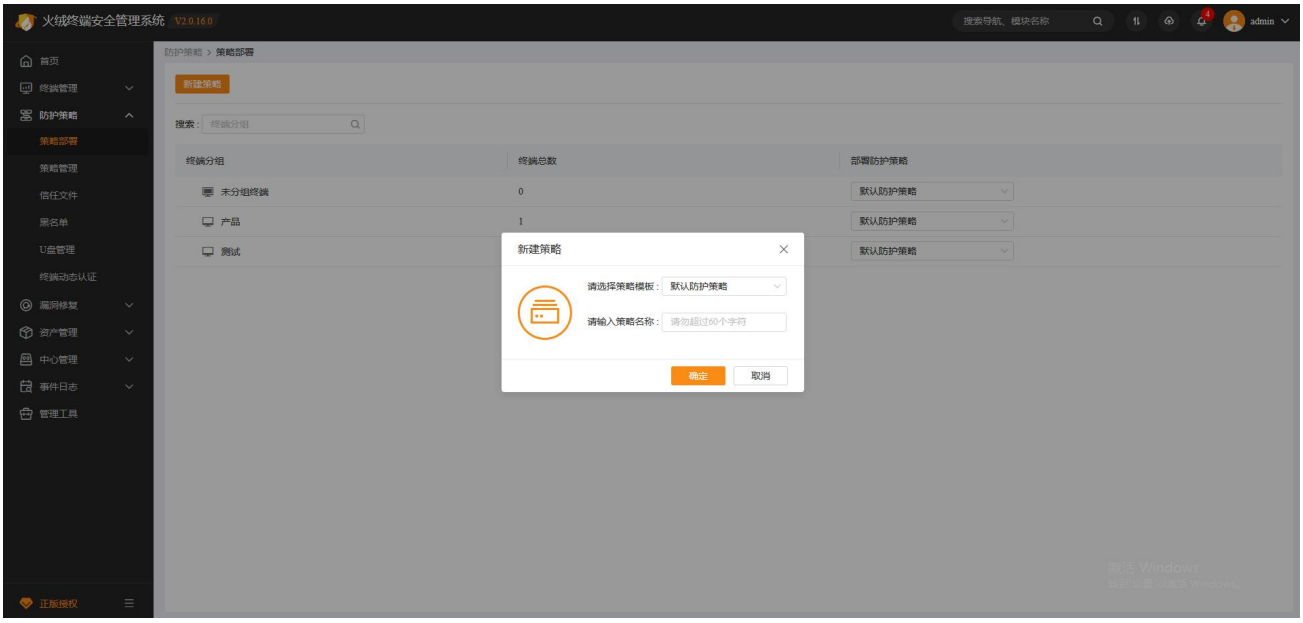
用户可在【防护策略】-【策略部署】界面进行策略部署，点击需要更改策略的终端分组右侧策略下拉

列表，选择需要分配的策略即可对当前终端分组分配指定策略。



2. 新建策略

用户可在【防护策略】-【策略部署】界面进行新建策略，新建策略时需要选择策略模板，以策略模板为基础创建新策略；输入策略名称（策略名称不可重复），点击确定后，即可成功创建安全策略，策略创建成功后可对当前策略进行编辑修改。

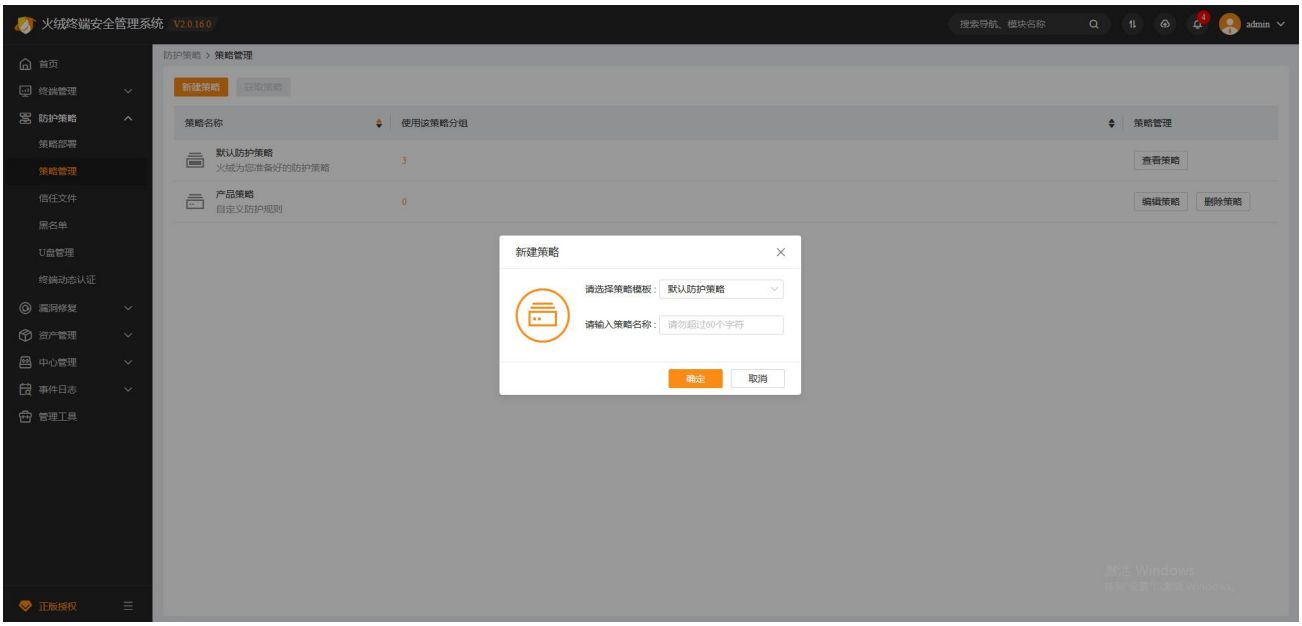


2.6.2 策略管理

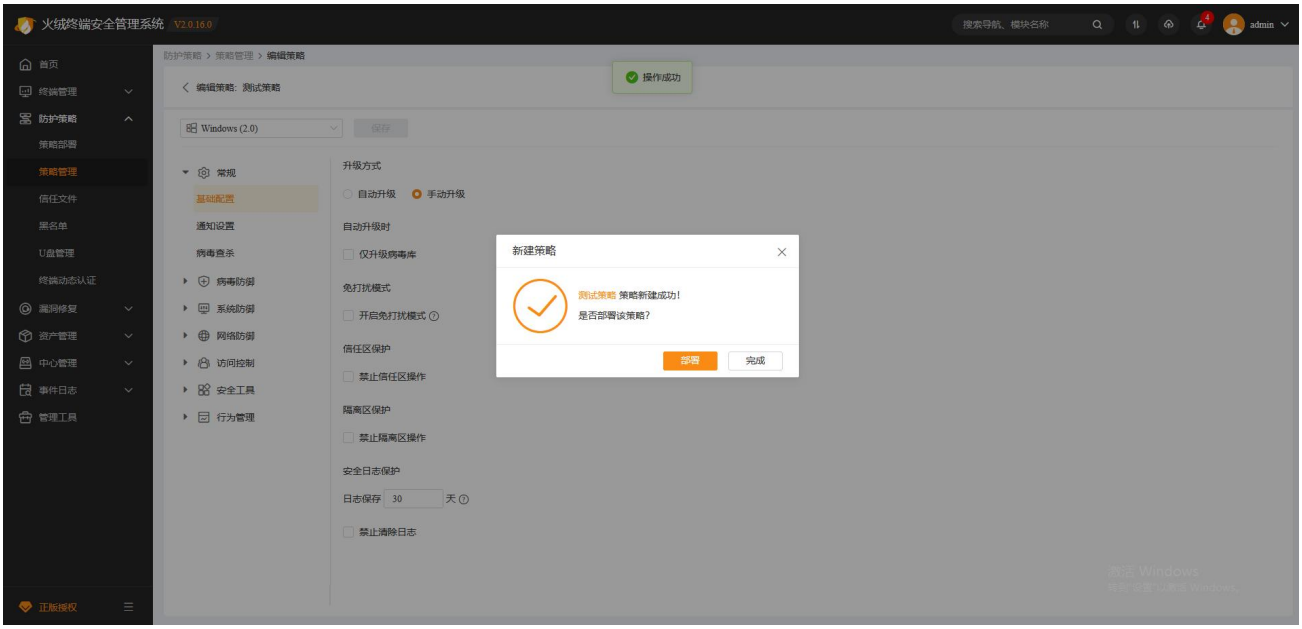
用户可以在【防护策略】-【策略管理】界面新增、查看、编辑及管理安全策略。

1. 新增策略

用户可通过点击【新建策略】按钮进行创建新策略，新建策略时需要选择策略模板，以策略模板为基础创建新策略；输入策略名称（策略名称不可重复），点击确定后，即可成功创建安全策略。



策略创建成功后进入策略编辑界面，编辑成功后，点击【保存】按钮保存策略，此时会询问是否部署策略，点击部署，去往策略部署页面，点击取消，留在策略编辑详情页。



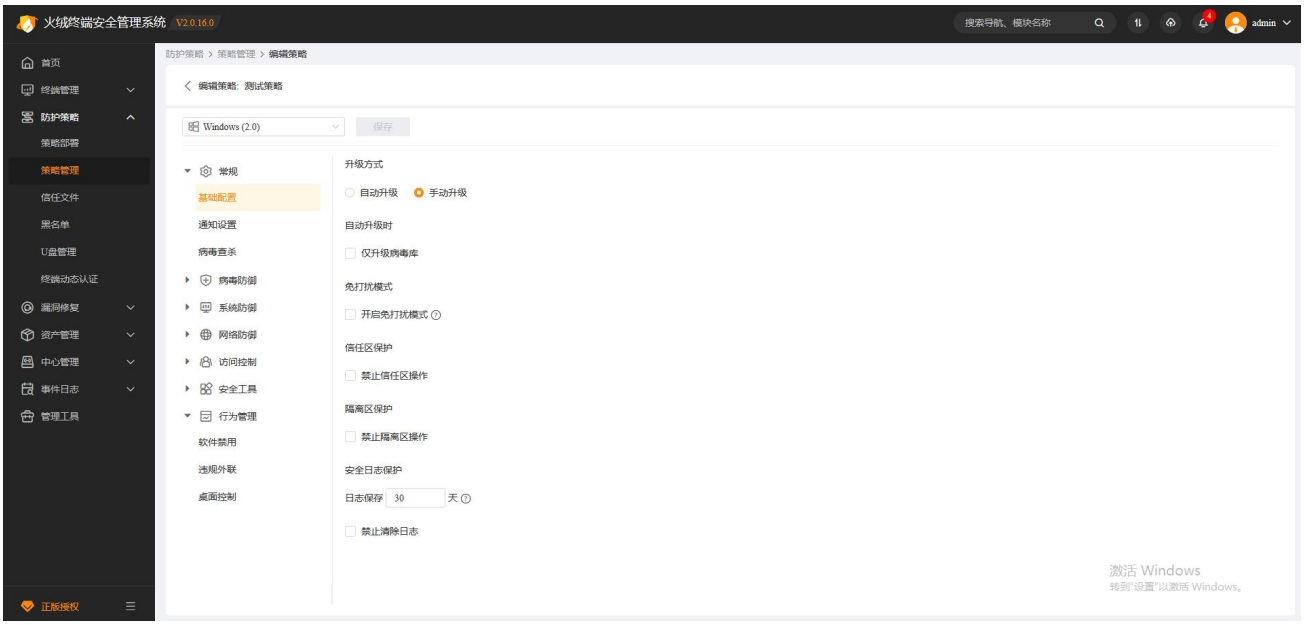
策略内容界面包含 7 块策略区，分别是常规、病毒防御、系统防御、网络防御、访问控制、安全工具、行为管理，对应了不同的终端防护功能，用户可根据自身企业安全建设需要自定义配置安全策略。策略详情如下：

（1） 常规

- 基础配置

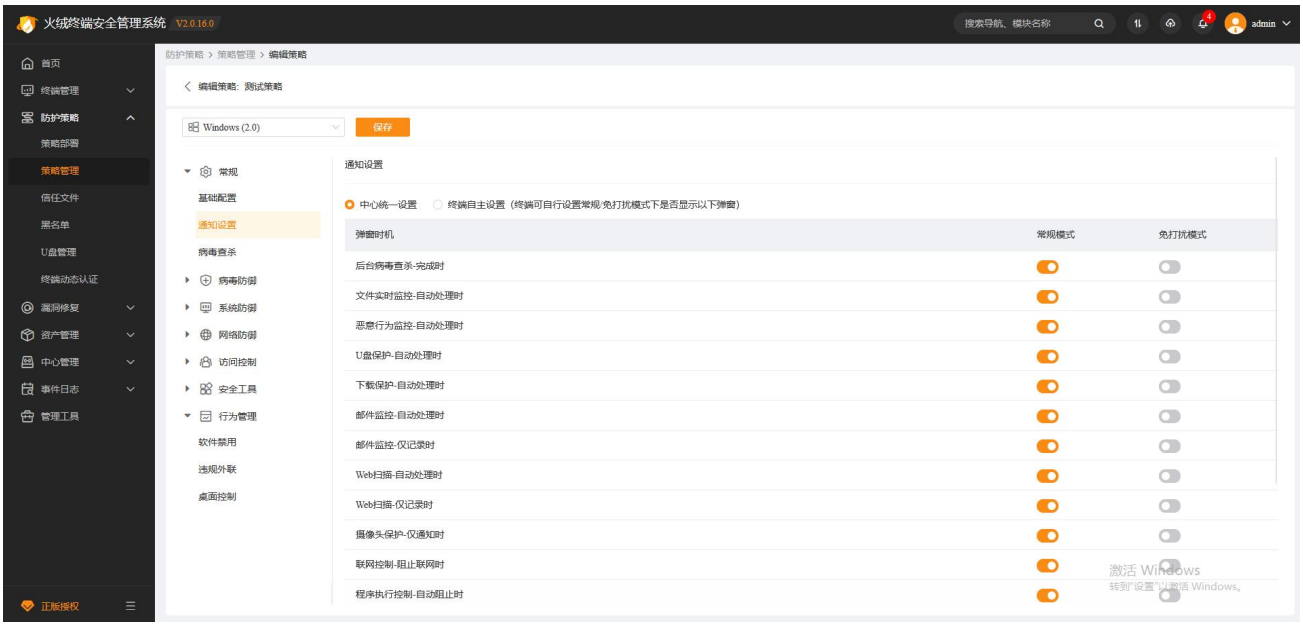
基础配置可帮助用户管理终端升级方式、自动升级选项、免打扰模式信任区保护及隔离区保护，还可以设置对应终端的日志保存时间（可以保存 1-180 天）和是否允许终端清除日志，用户可依据自身场景进行灵活配置。

注：免打扰模式开启后，火绒终端将不会显示火绒自身的部分提示弹窗（中心下发任务弹窗不会屏蔽），相关任务将按照火绒内置规则进行自动执行，不会屏蔽操作系统弹窗及其他相关软件弹窗。



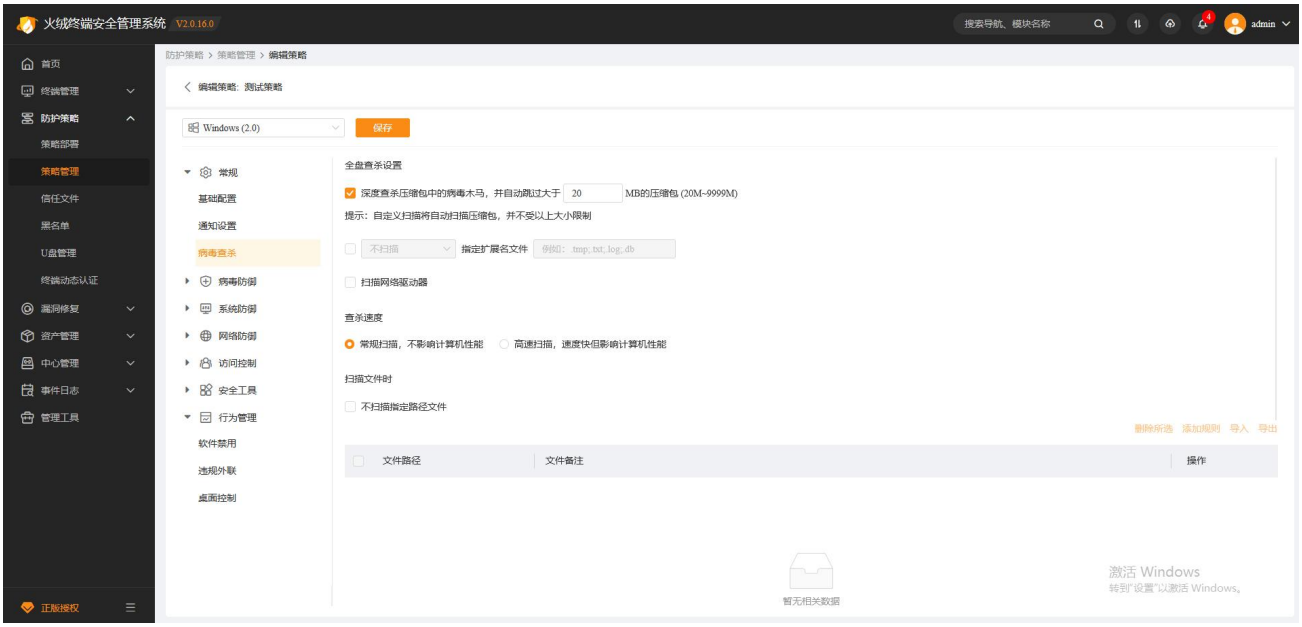
- 通知设置

通知设置功能可以帮助用户管理终端各个通知类弹窗在常规模式下和免打扰模式下是否显示；【常规模式】是指终端未开启免打扰模式的状态；【免打扰模式】是指终端开启免打扰模式的状态；选中【中心统一设置】时，终端将统一按照中心的设置显示通知类弹窗；选中【终端自主设置】时，终端可自行设置常规模式和免打扰模式下各个通知类弹窗是否显示。



- 病毒查杀

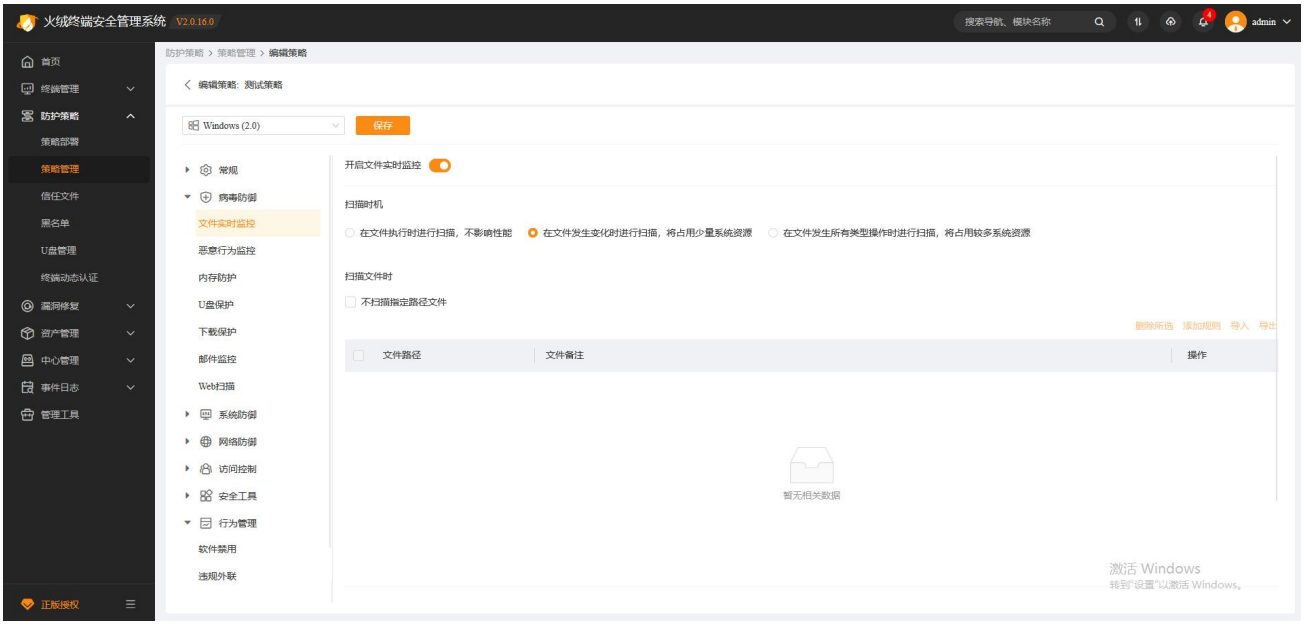
病毒查杀设置可针对病毒查杀功能进行细化配置，应用此策略的终端在进行病毒查杀任务时，会依照此设置进行病毒查杀和处理。



（2） 病毒防御

- 文件实时监控

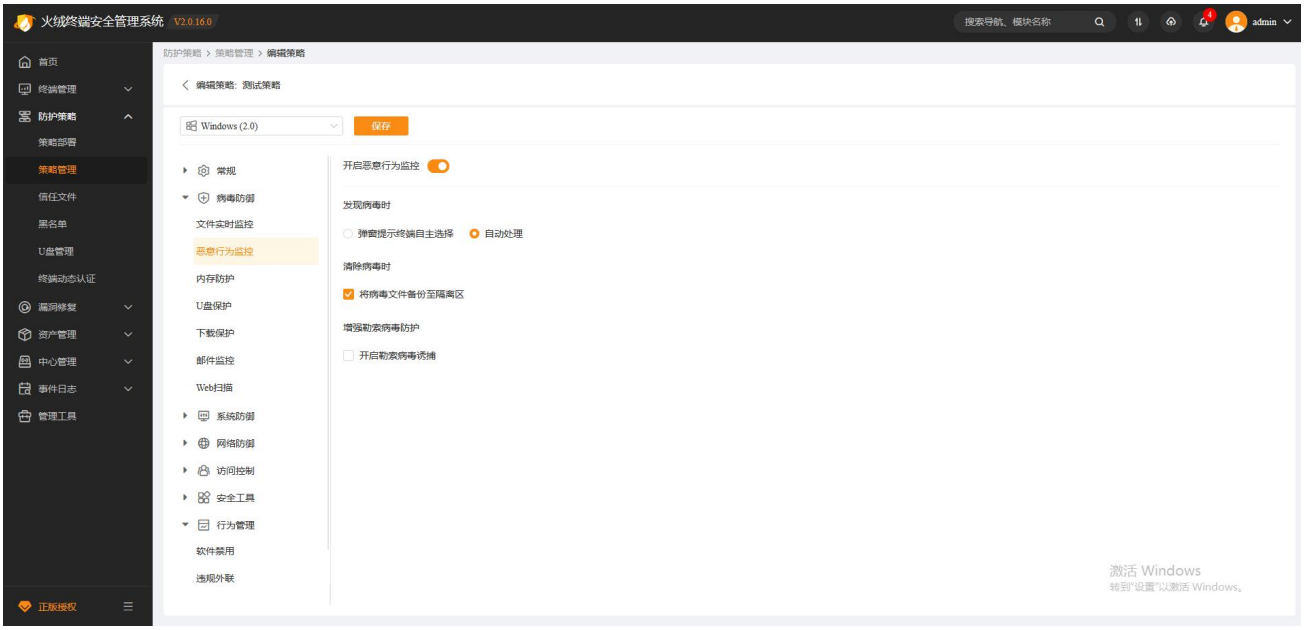
文件实时监控将在文件执行，修改或者打开时检测文件是否安全，即时拦截病毒程序。在不影响电脑正常使用的情况下，实时保护用户的终端不受病毒侵害。



- 恶意行为监控

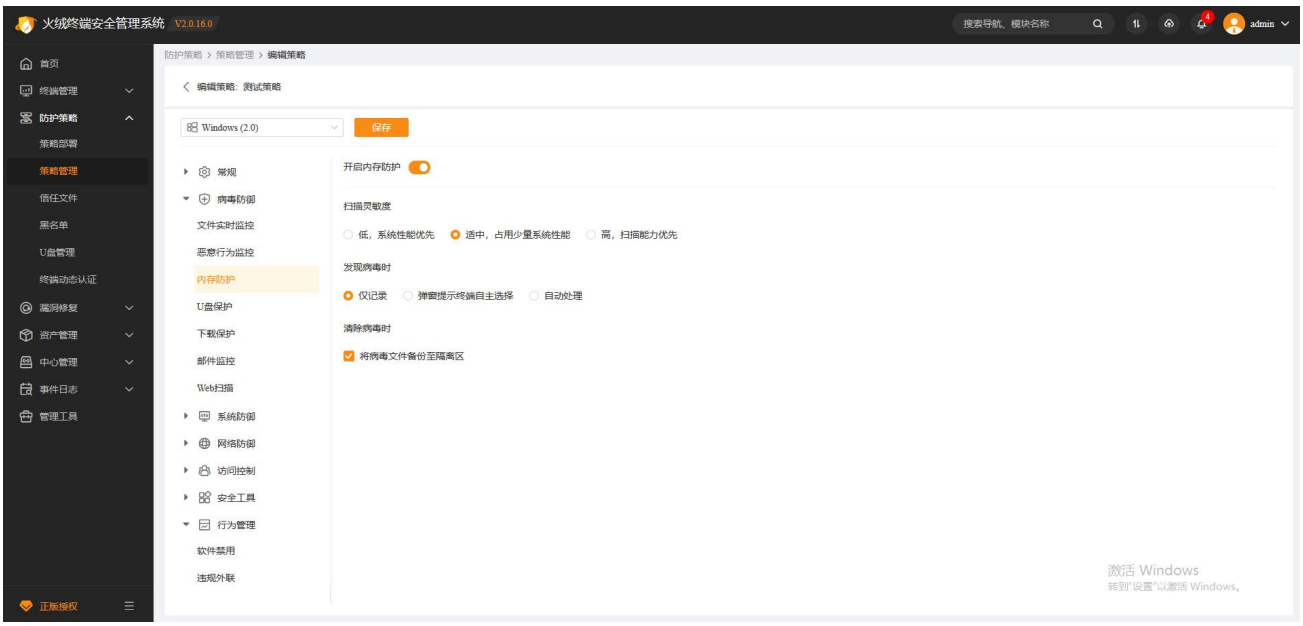
恶意行为监控通过监控程序运行过程中是否存在恶意操作来判断程序是否安全。

注：增强勒索病毒防护：开启该功能后，火绒安全软件会在系统盘符下创建两个具有隐藏属性的随机名文件目录，随机名文件目录里会有若干常见文件格式的随机文件，防护系统使用这些随机文件来诱捕勒索病毒，达到增强防护的目的。



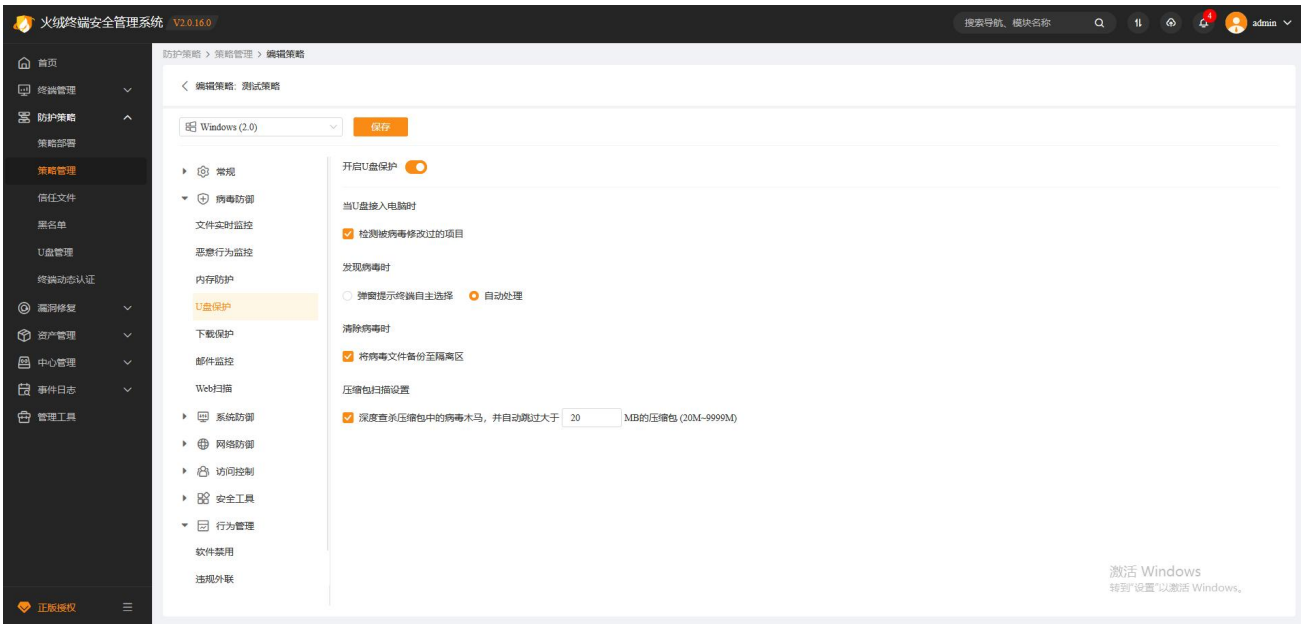
- 内存防护

内存防护功能主要针对无文件攻击类型的病毒，可及时发现内存中的恶意代码并阻止。



- U 盘保护

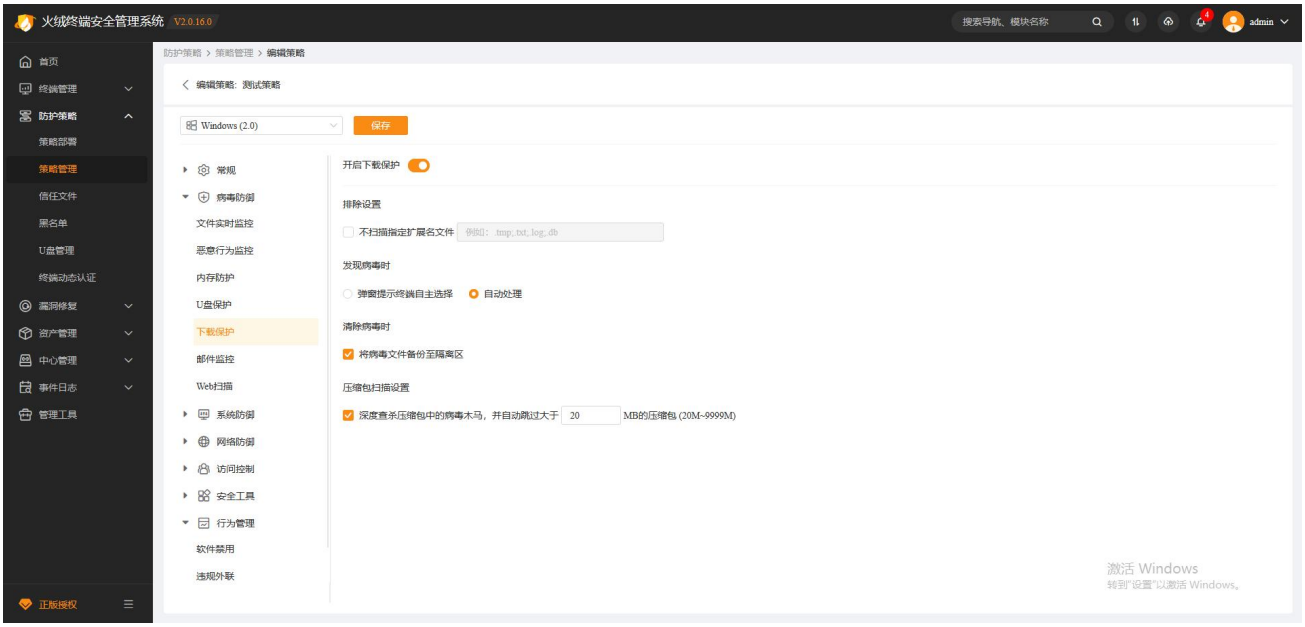
U 盘保护功能会在 U 盘接入电脑时对其进行快速扫描，及时发现并阻止安全风险，避免病毒通过 U 盘进入您的电脑。



- 下载保护

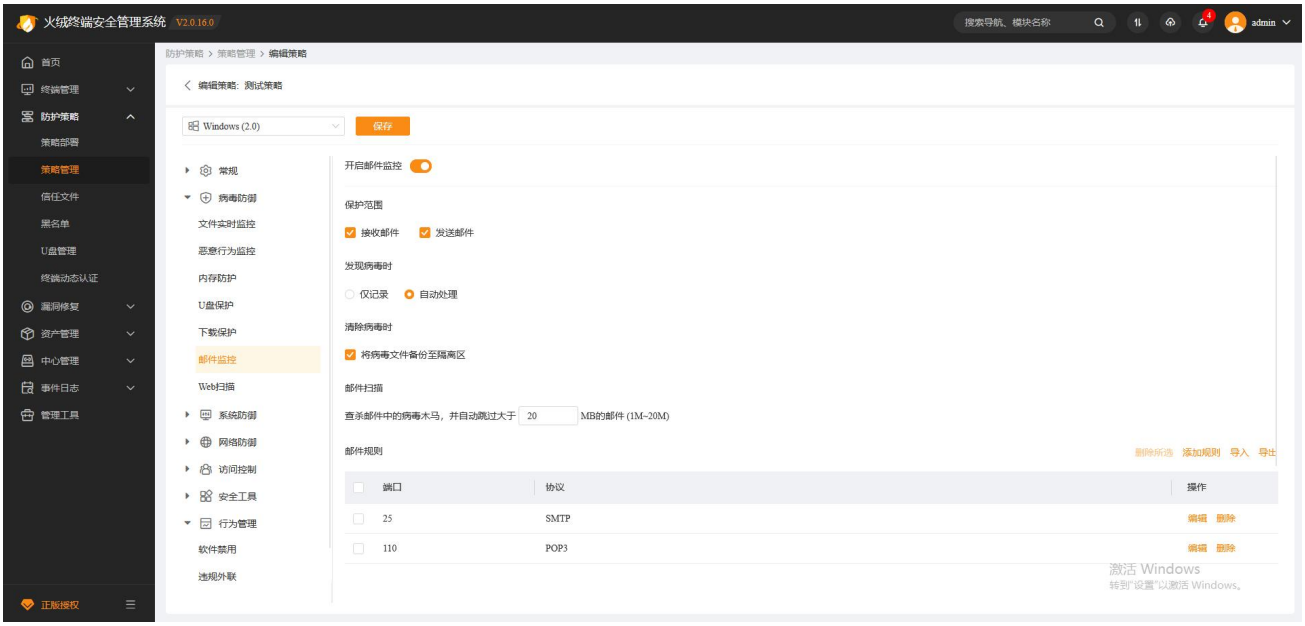
在您使用浏览器、下载软件、即时通讯软件进行文件下载时，下载保护会实时对所有从网络下载至终

端中的文件进行病毒扫描，保护您的终端安全。



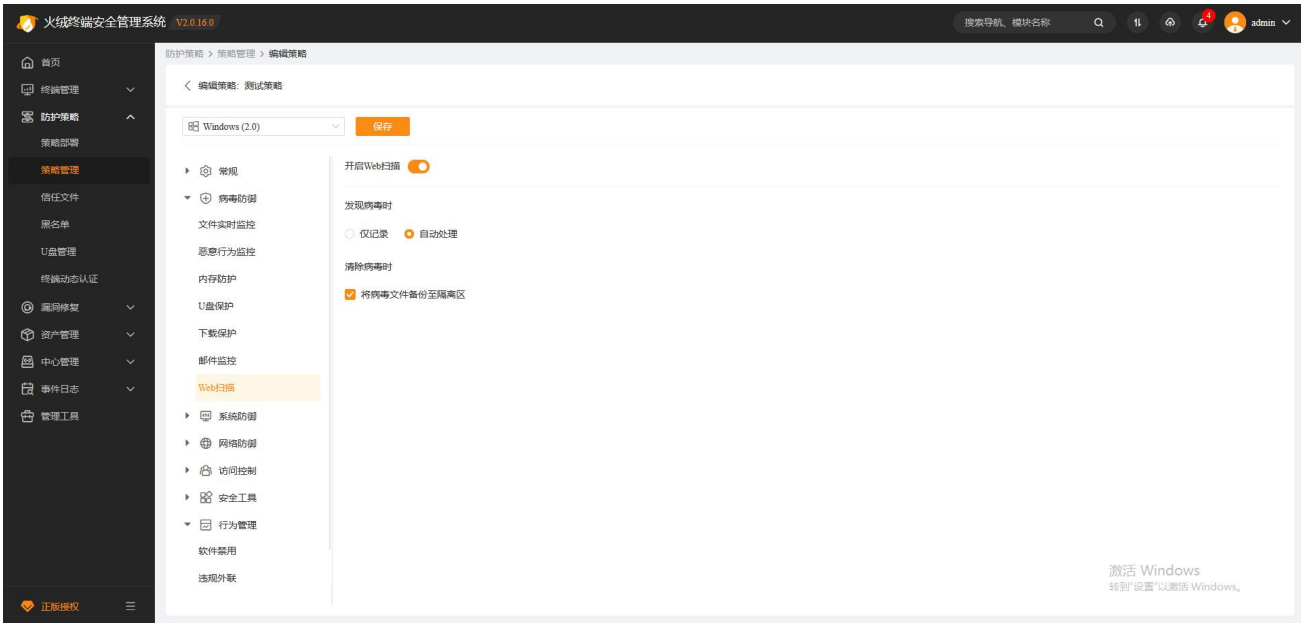
- 邮件监控

邮件监控会对所有接收的邮件进行扫描，当发现风险时，将会自动打包风险邮件至隔离区，并发送一封火绒已处理的回复邮件。对于发送的邮件，若发现邮件中包含病毒，火绒直接将终止您的邮件发送，并自动清除病毒邮件至隔离区，防止病毒传播。



- Web 扫描

当有应用程序与网站服务器进行通讯时，Web 扫描功能会检测网站服务器返回的数据，并及时阻止其中的恶意代码运行。

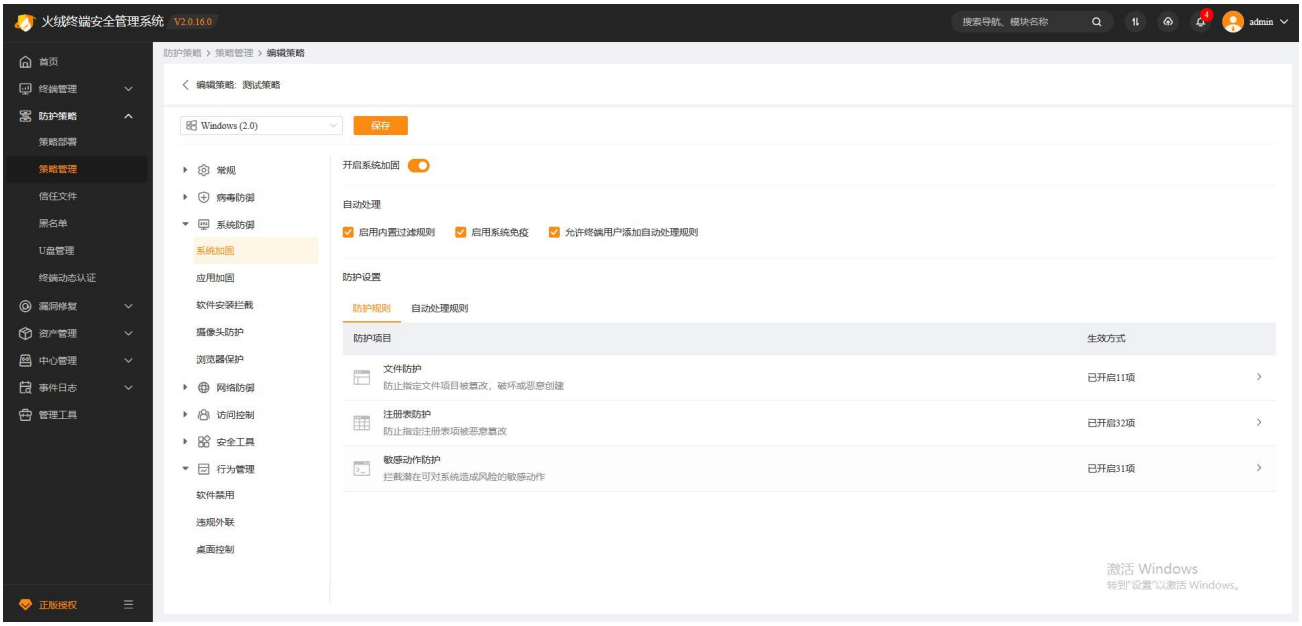


（3） 系统防御

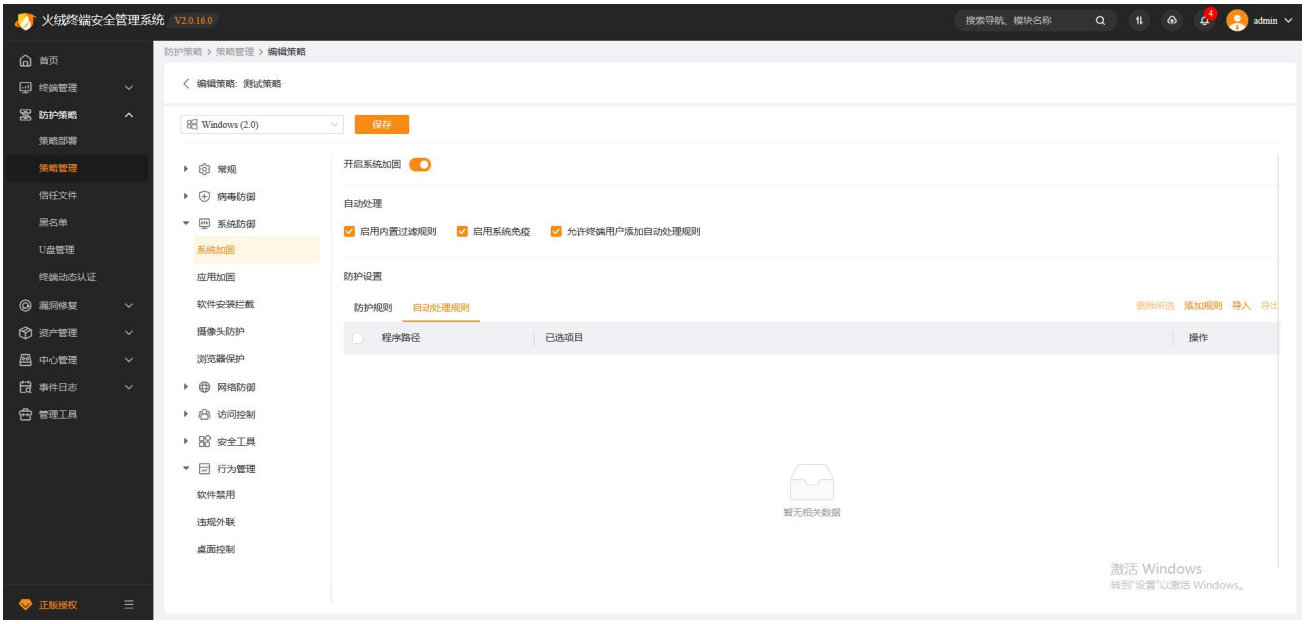
- 系统加固

系统加固功能根据火绒提供的安全加固策略，当程序对特定系统资源操作时提醒用户可能存在的安全风险。

系统加固策略分为防护规则和自动处理规则。防护规则为火绒安全管理系统自带的规则，管理员可以根据需求，自行选择是否开启；

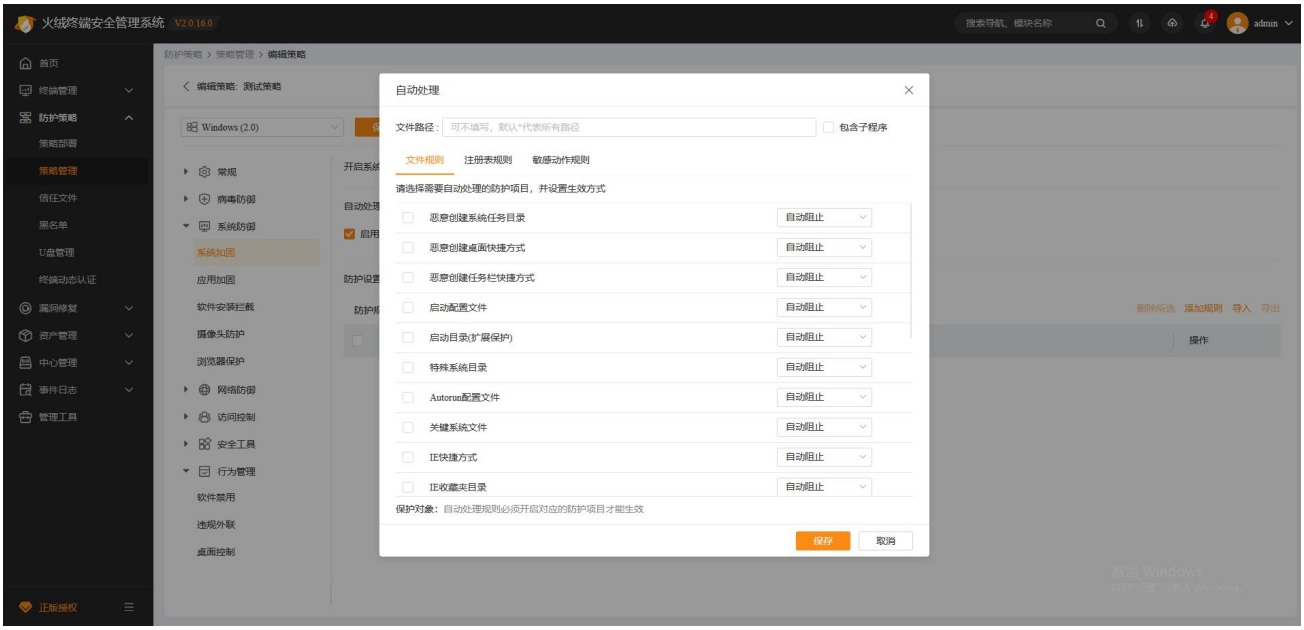


自动处理规则可以由中心管理员统一添加，使用该策略的终端都会添加这些处理规则。



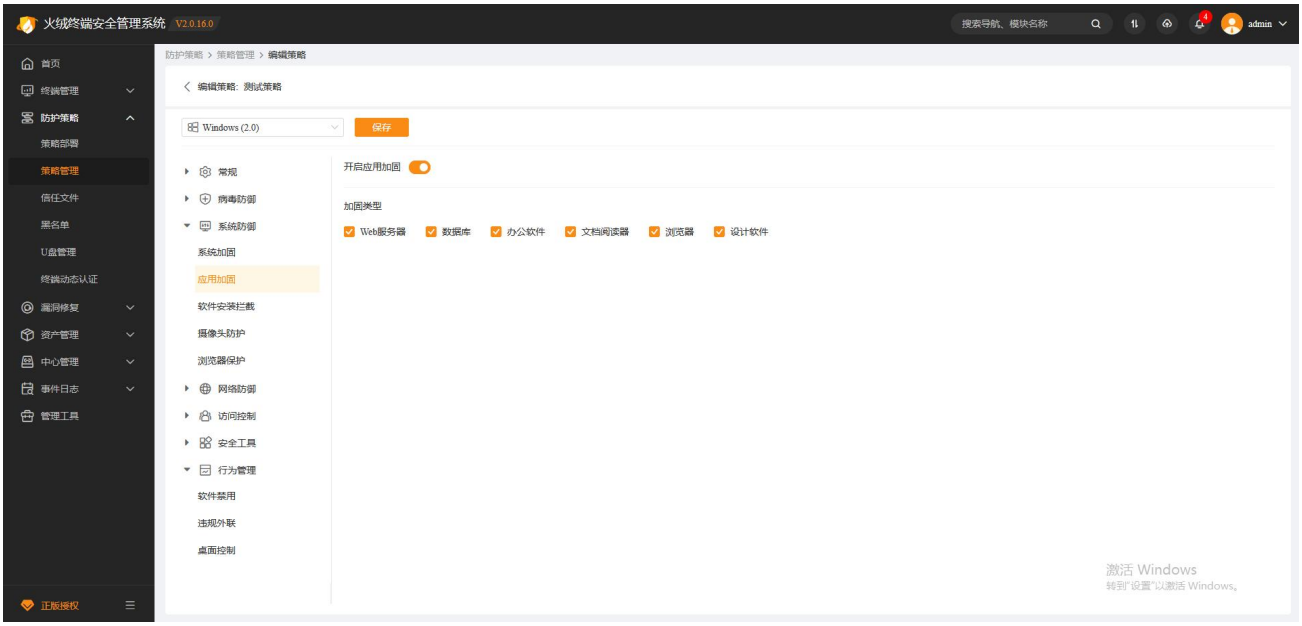
点击【添加规则】，显示添加自动处理规则窗口。自动处理规则需填写文件路径，勾选【包含子程序】配置后，表示添加程序的关联脚本程序一并会自动处理。

注：自动处理规则必须开启对应的防护项目才会生效，防护项目分为文件规则、注册表规则和敏感动作规则，点击标题按钮可切换。



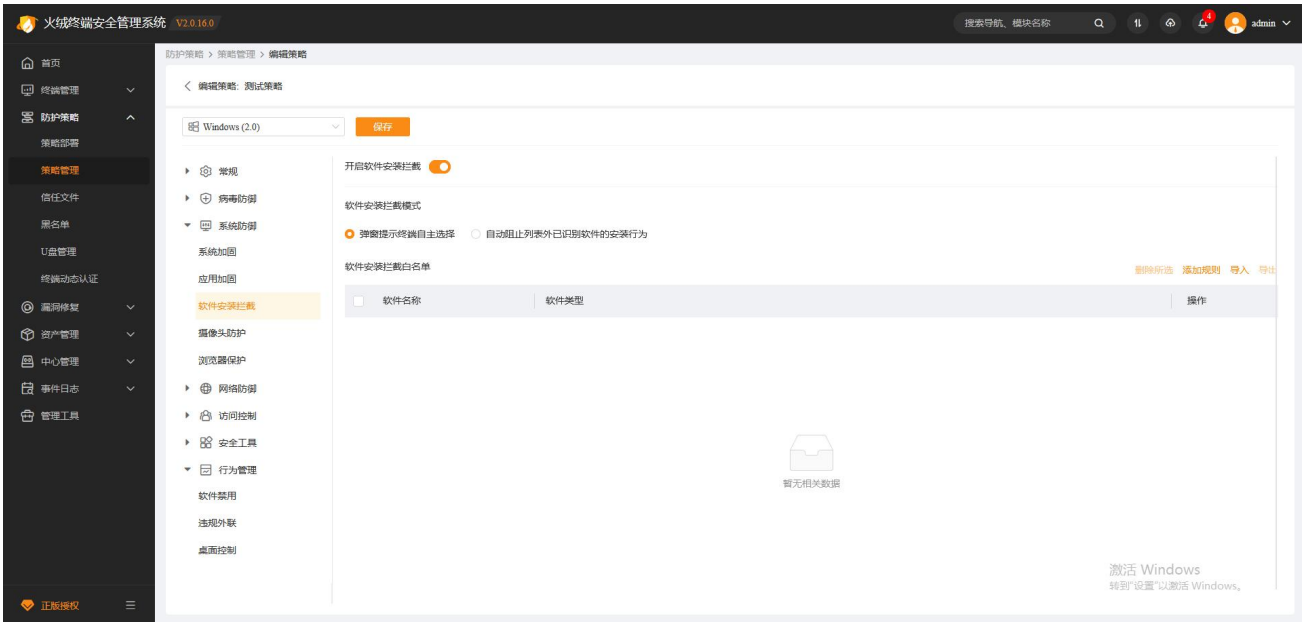
- 应用加固：

应用加固功能通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用。

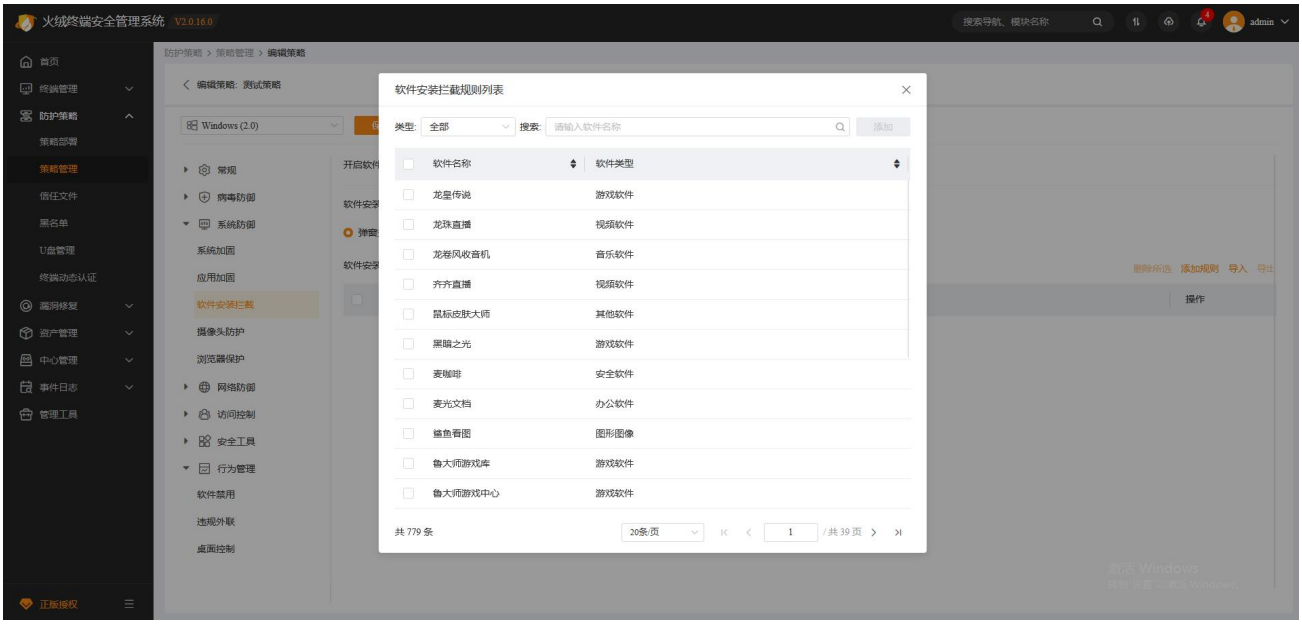


- 软件安装拦截

软件安装拦截功能会依据用户反馈搜集被恶意推广过的软件，并在其安装时提示终端用户，以阻止流氓软件恶意推广，静默安装软件的行为。软件安装拦截能有效的防止终端用户在不知情的情况下终端自动安装无关软件。

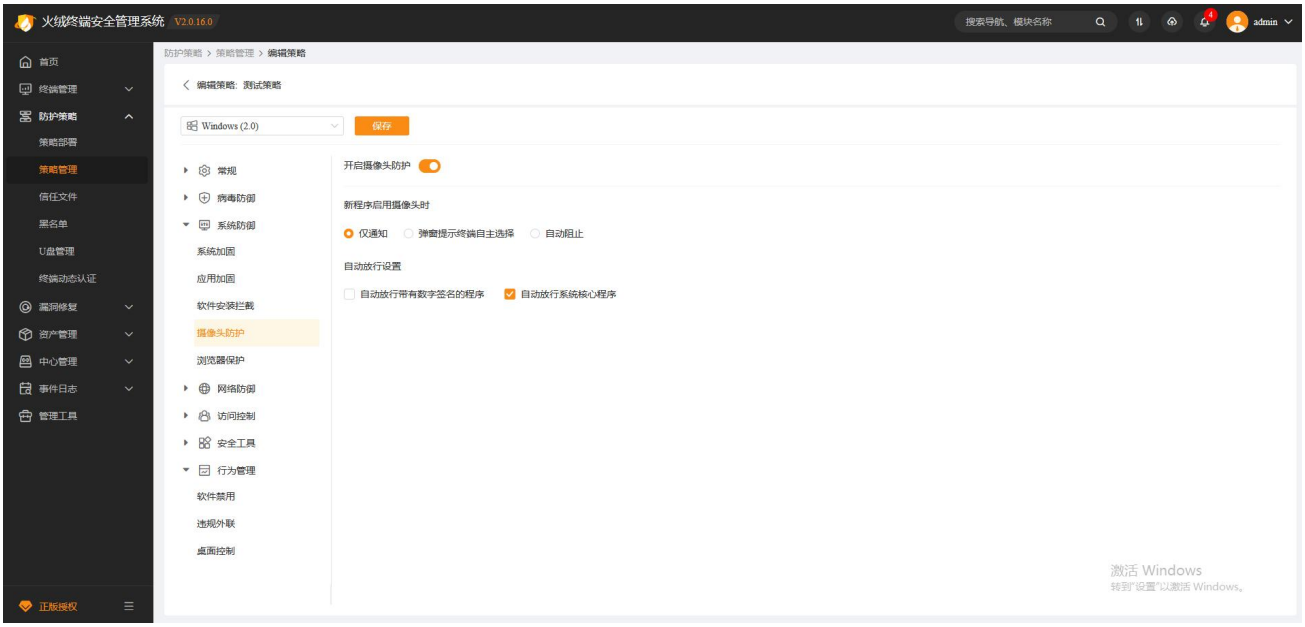


点击【添加规则】，显示添加软件窗口，在软件库中添加要拦截的软件，已添加的软件显示在列表中。



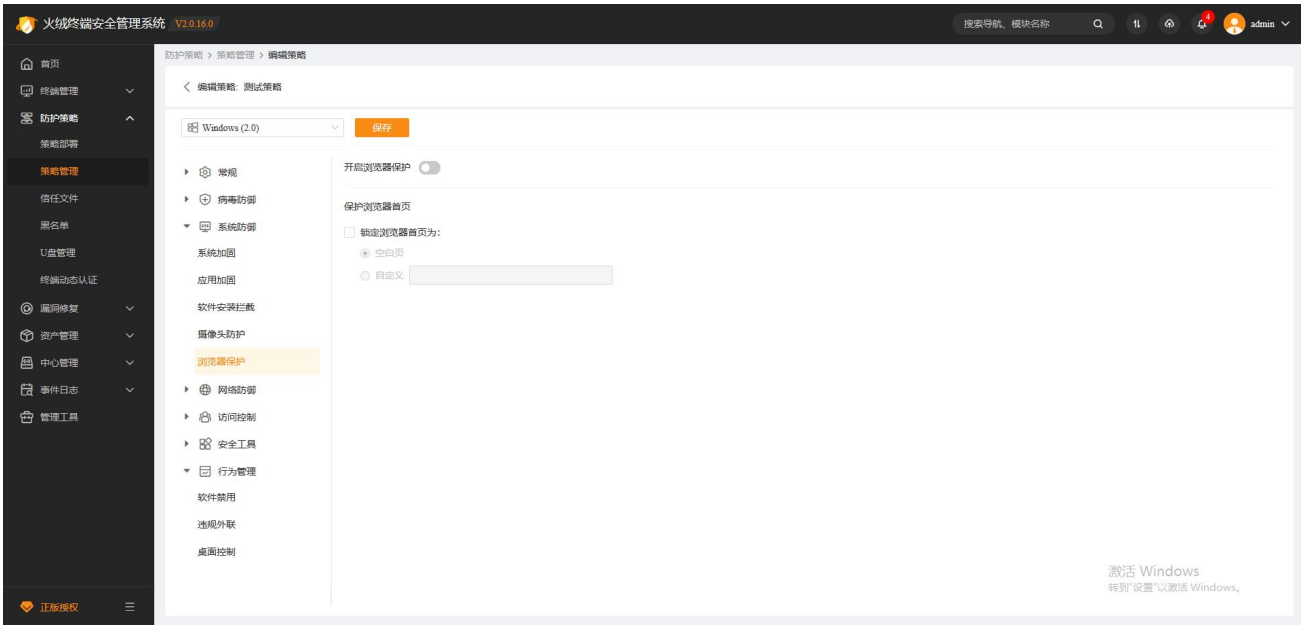
- 摄像头防护

火绒摄像头防护会在有任意终端软件要启用您的摄像头时弹窗提示您，您可以根据需要选择是否允许程序启用摄像头。



- 浏览器保护

浏览器保护能锁定您的浏览器主页不被任意程序篡改。



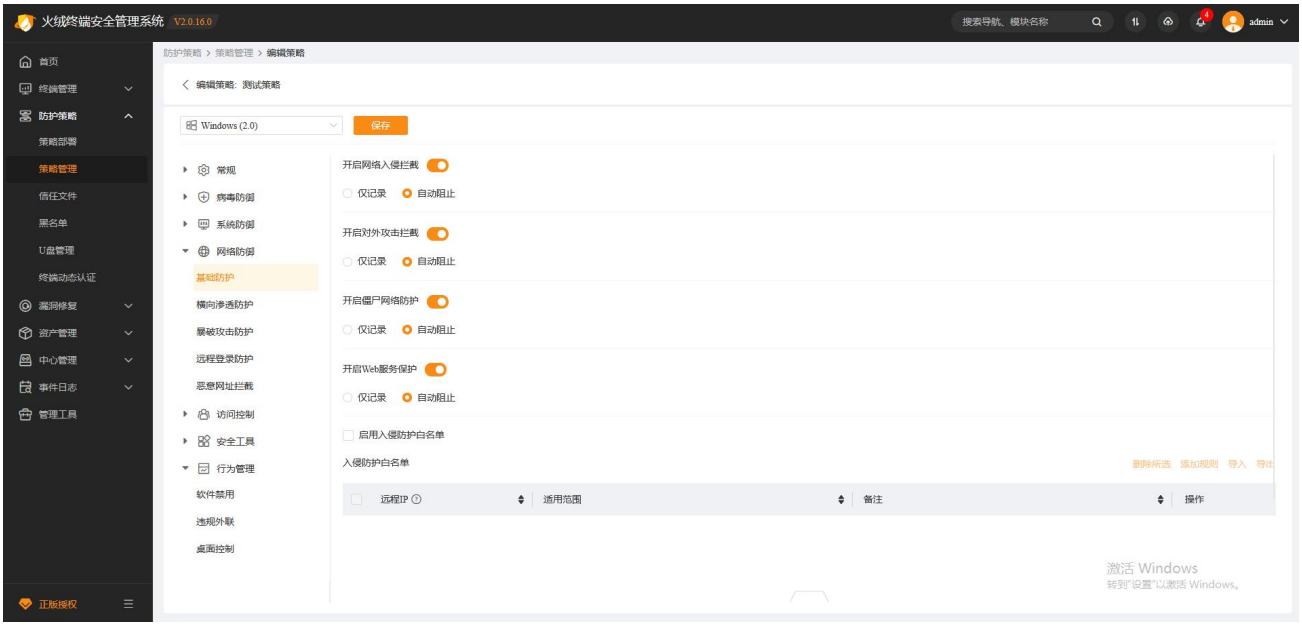
(4) 网络防御

网络防御策略分为基础防护策略和单项防护策略。

- 基础防护

基础防护策略分为网络入侵拦截、对外攻击拦截、僵尸网络防护和 Web 服务保护，以及入侵防护白名

单。



网络入侵拦截将检测网络传输的数据包中是否包含恶意攻击代码，通过中断这些数据包传输以避免您的电脑被黑客入侵。

对外攻击拦截将检测您电脑外联的数据包中是否包含恶意攻击代码，通过中断这些数据包传输以阻止用户的电脑被黑客利用。

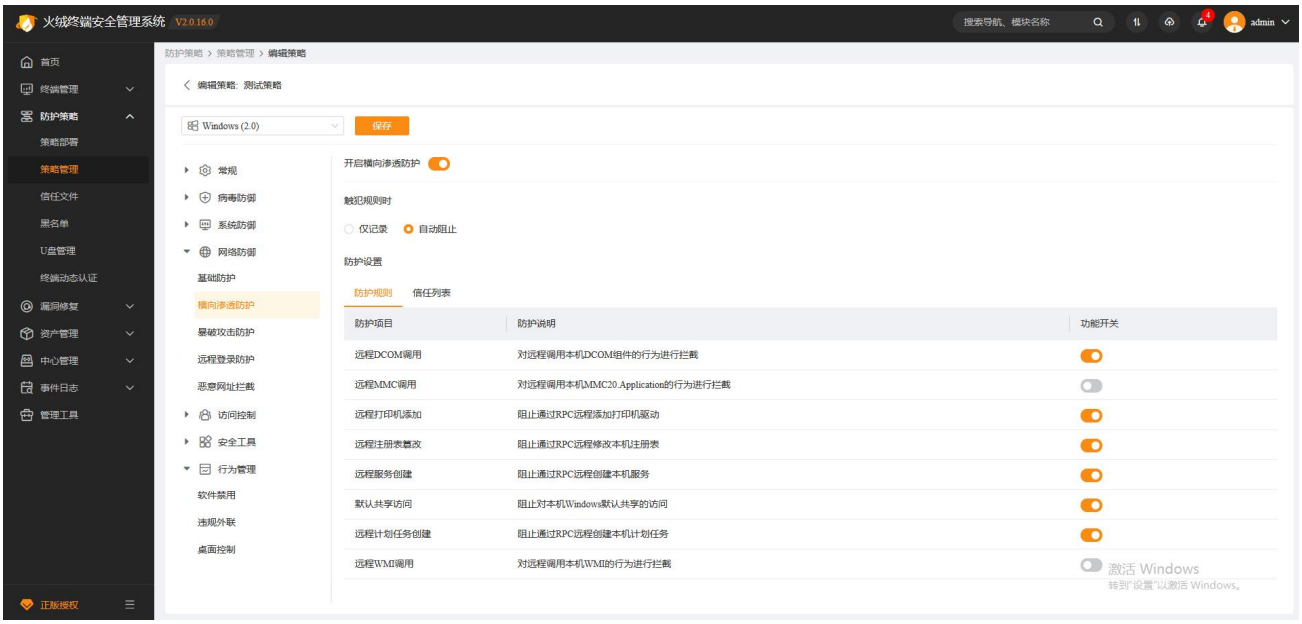
僵尸网络防护将检测网络传输的数据包中是否包含远程控制代码，通过中断这些数据包传输以避免您的电脑被黑客远程控制。

Web 服务保护，黑客可能会对安装了服务器软件的终端发起攻击，以入侵服务器，窃取隐私数据，甚至篡改支付信息等危险行为，对您造成一些不必要的损失。Web 入侵防护能全方位保护您计算机的服务器软件，主要从数据库、Web 服务器、Web 应用、Web 后门四个方面对安装有服务器软件的计算进行强力保护。

- 横向渗透防护

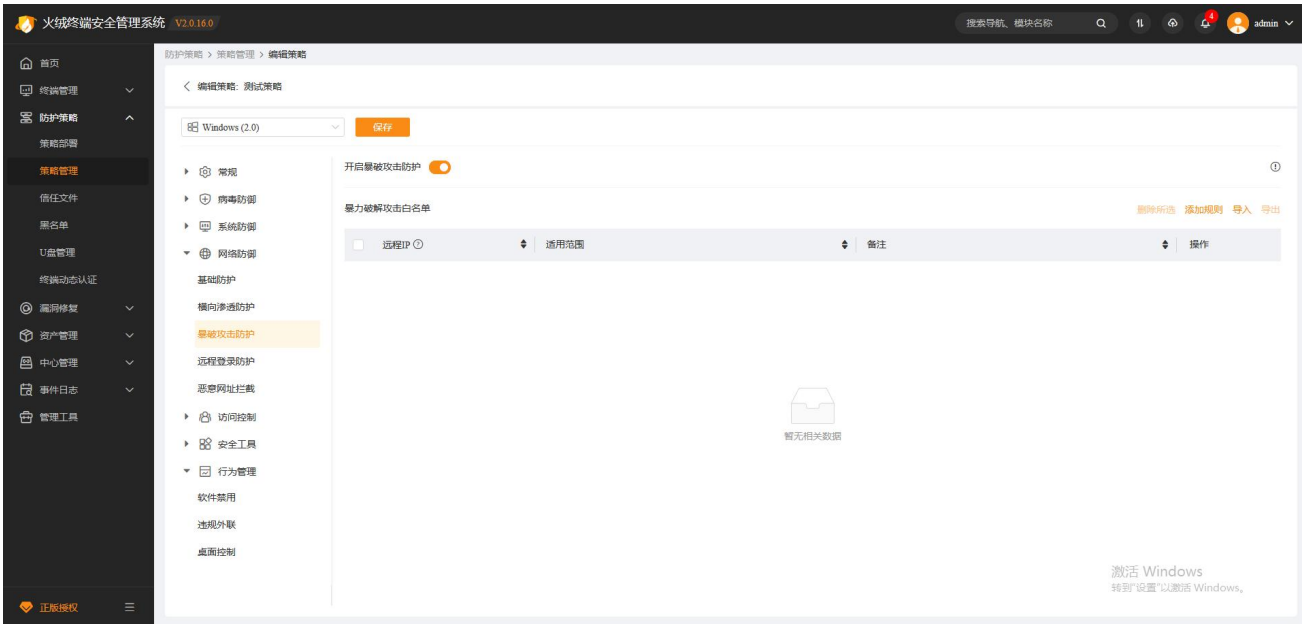
横向渗透防护可以对远程 DCOM 调用、远程 MMC 调用、远程打印机添加、远程注册表篡改、远程服

务创建、默认共享访问、远程计划任务创建、远程 WMI 调用这几种行为进行拦截，防止电脑中的病毒进行横向传播。



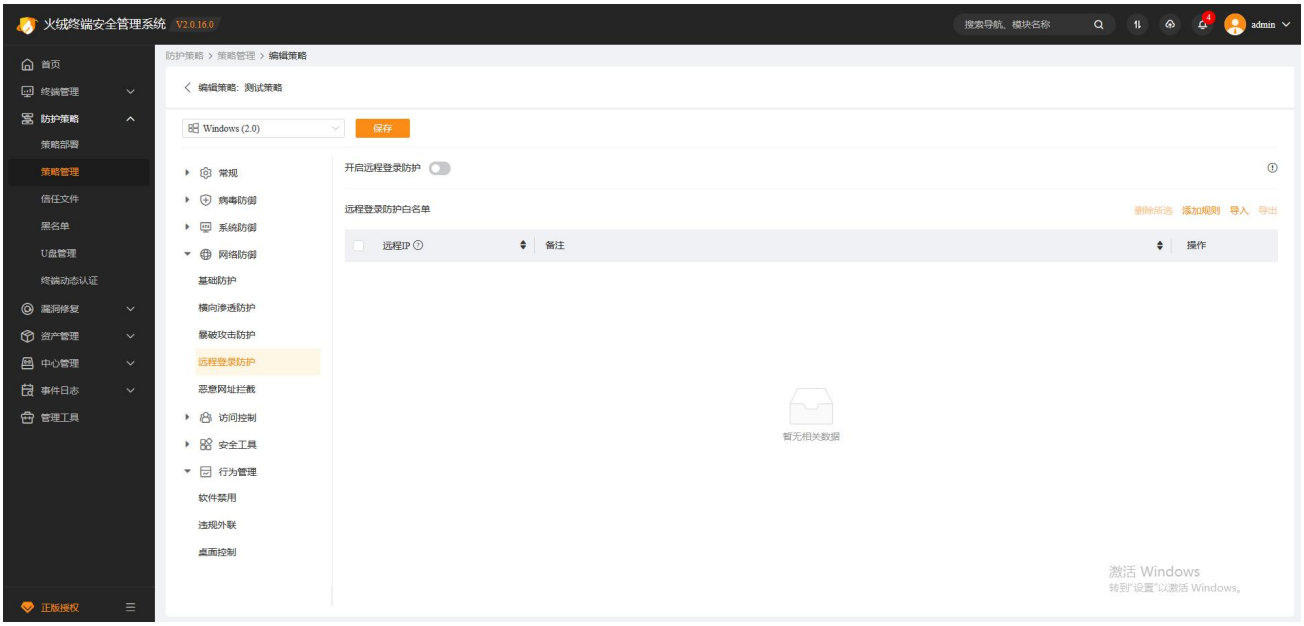
- 暴破攻击防护

不法分子常常通过暴力破解登录密码等密码破解攻击获取密码从而远程登录用户电脑，远程登录成功后，不法分子可以在权限允许范围内肆意操作主机。



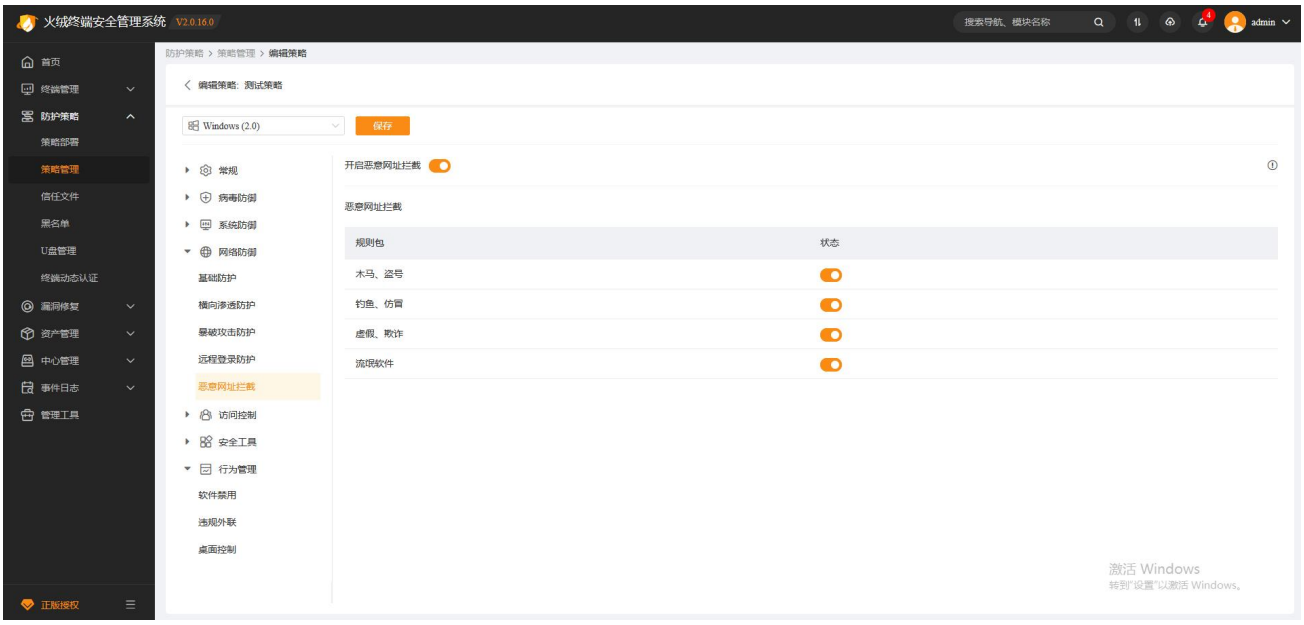
- 远程登录防护

开启后终端将自动阻止所有远程登录行为，如有需要可在设置中加白名单，以放过信任 IP 的远程登录。



- 恶意网址拦截

当您在浏览网页的时候，访问到有恶意风险的网站，火绒将拦截网站并弹出提示。

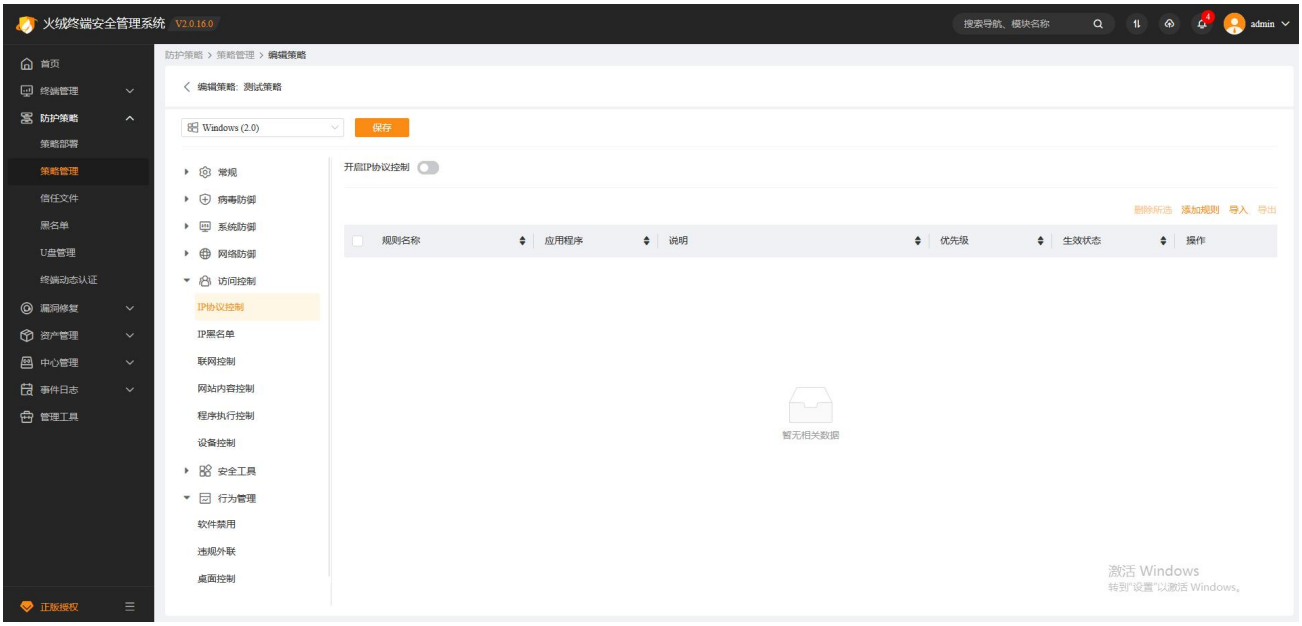


（5） 访问控制

- IP 协议控制

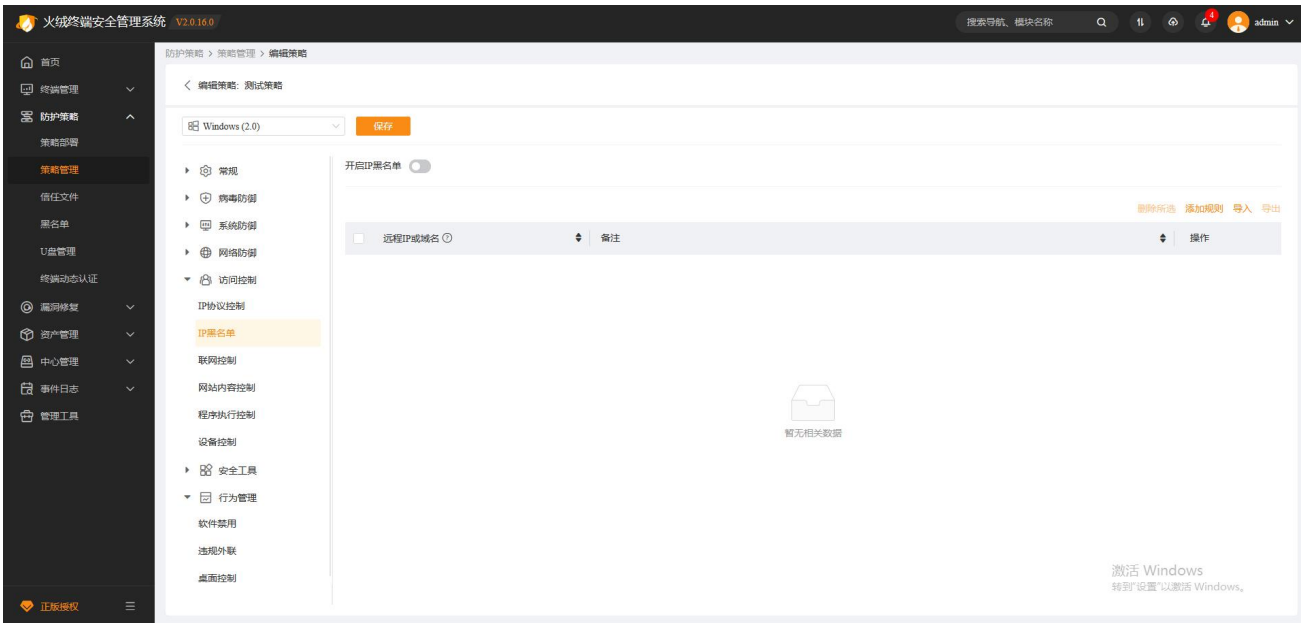
在 IP 协议层控制数据包进站、出站行为，并且针对这些行为做规则化的控制。需用户或管理员手动配

置对应规则，当发现有触发 IP 协议控制规则的操作时，火绒可根据用户设置的规则放过或阻止。



- IP 黑名单

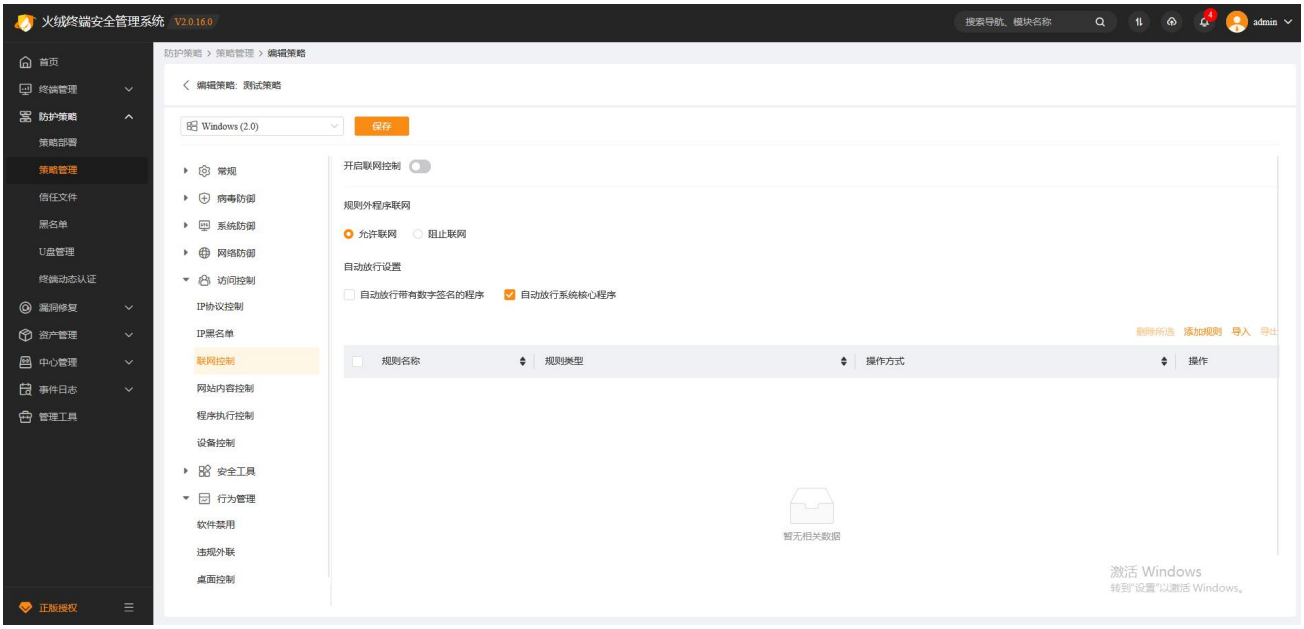
当终端有不受欢迎的 IP 访问时，用户可以添加这些 IP 加入 IP 黑名单中，以阻止这些 IP 的访问，IP 黑名单支持导入和导出，支持导入 excel、csv 格式文件。



- 联网控制

当用户需要阻止某程序联网，或者希望自行管控电脑中所有程序是否联网时，您可以通过联网控制功

能很好地管控电脑程序的联网行为。该功能默认不启用，开启后每当有任意程序进行联网时，联网控制都会弹出弹窗提示，建议您根据需要决定是否开启此功能。用户也可手动配置对应规则，自动放行或阻止对应程序的联网行为。

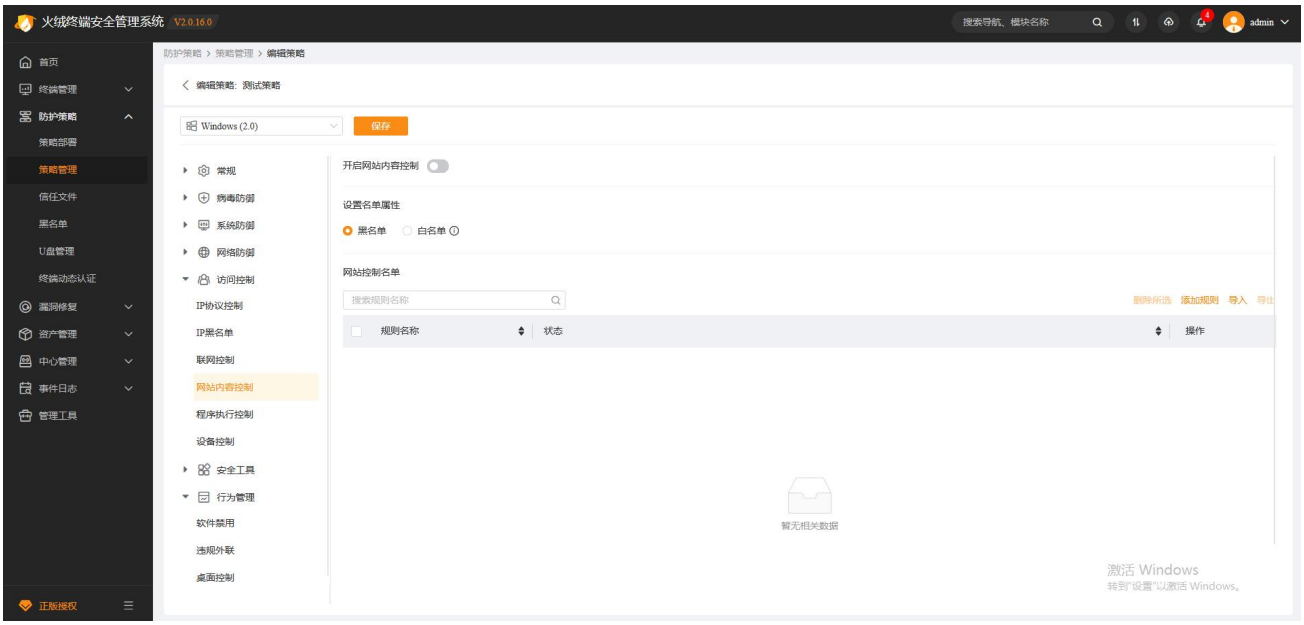


- 网站内容控制

管理员需要限制终端访问某些网站时，可添加网站进行访问内容限制（支持 HTTP 协议和 HTTPS 协议网址，支持通配符*）。

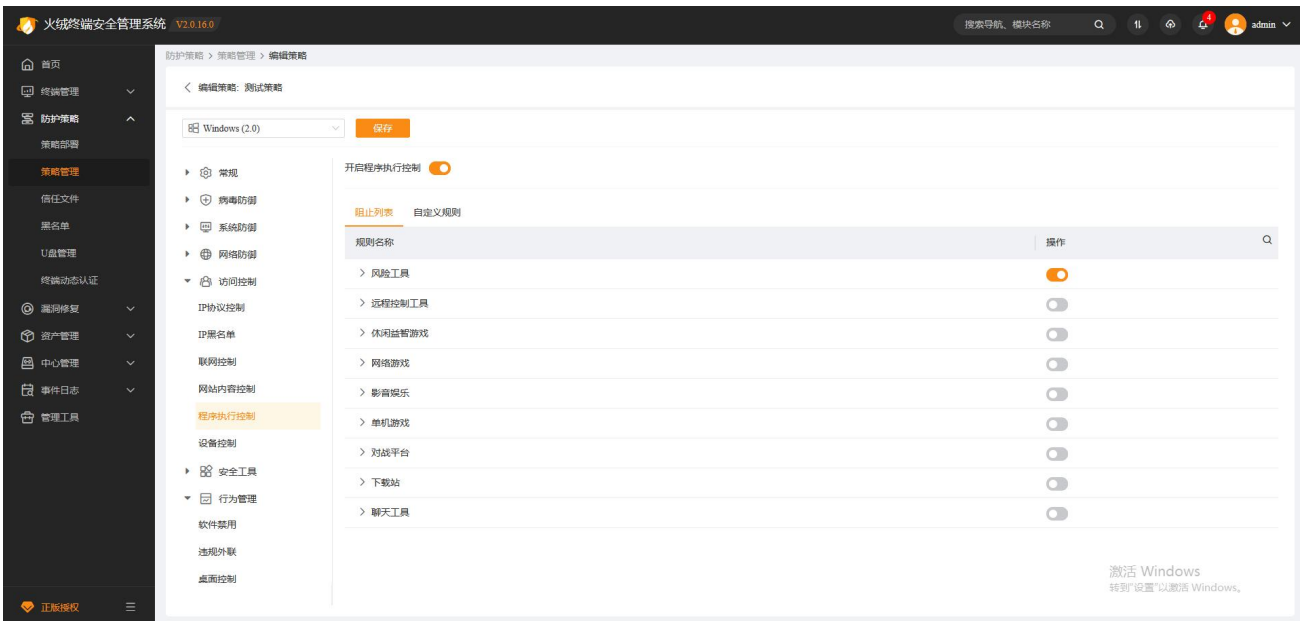
网站控制名单的属性分为黑名单和白名单，默认选择黑名单，此时终端用户将无法访问名单中网址，名单外的网址可以正常访问；当属性为白名单时，此时终端用户仅能访问名单中的网址，名单外的网址无法访问。

（注：以火绒为例，黑名单模式规则中设置了 https://www.huorong.cn 时，将仅拦截一级域名为“huorong.cn”子域名为“www”或无子域名的网址；规则中设置的 https://huorong.cn 时，将拦截一级域名为“huorong.cn”的所有网址）



- 程序执行控制

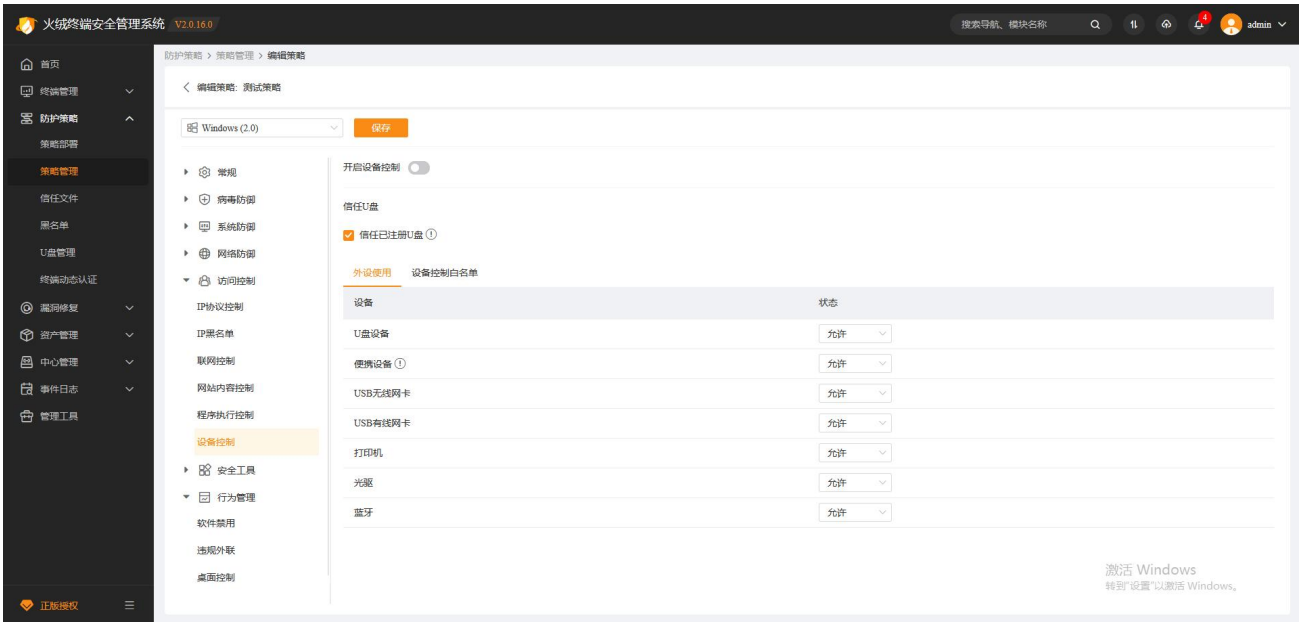
可根据用户需要设置对应规则以限制某个或某类程序在终端中执行和使用。



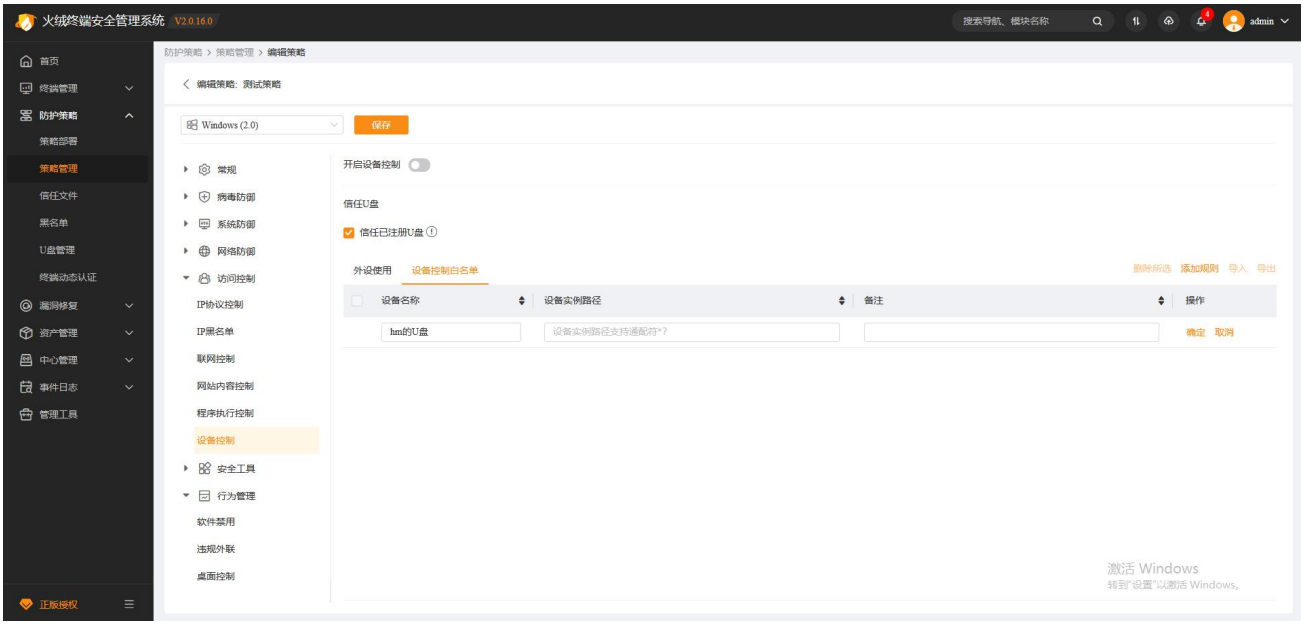
- 设备控制

控制设备是否可在计算机上的运行使用。当前支持的设备类型有：U 盘设备、便携设备、USB 无线网卡、USB 有线网卡、打印机、光驱、蓝牙。

设备控制支持添加设备控制白名单，对部分设备进行放过处理。

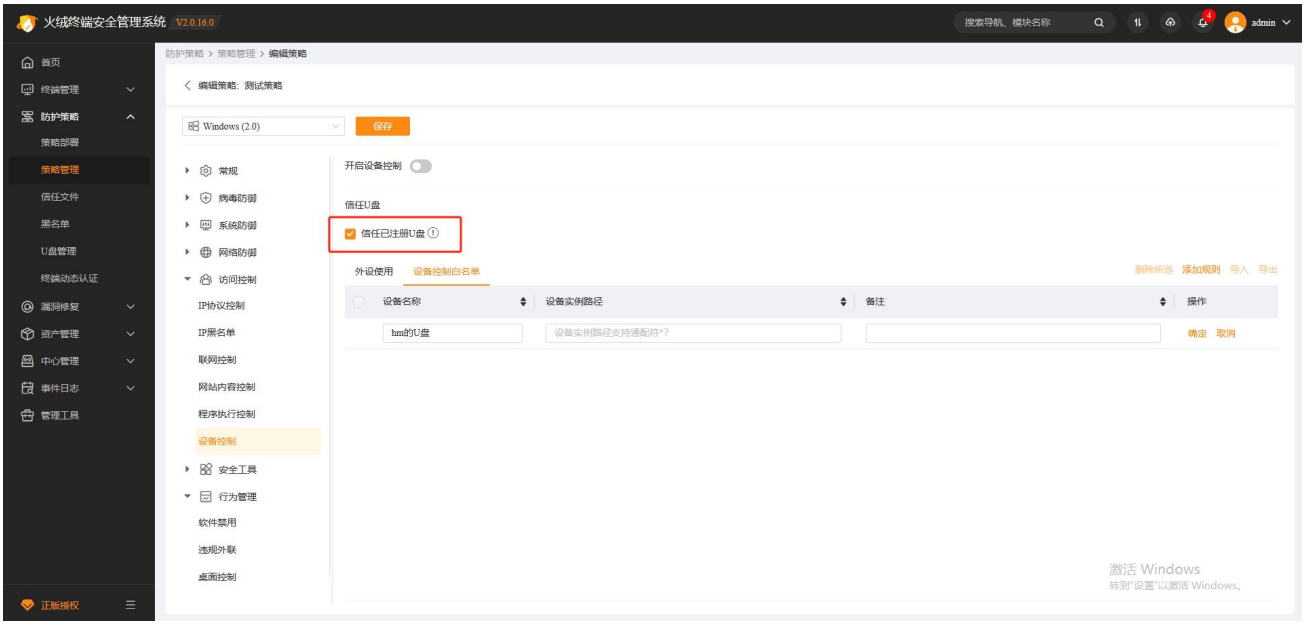


点击当前页面【设备控制白名单】按钮，显示设备控制白名单列表，点击右上角【添加规则】按钮，显示设备控制添加白名单规则窗口。



填写“设备名称”及“设备实例路径”，备注信息选填，点击【确定】按钮，添加信任设备至白名单列表，已经添加的设备，可以在列表删除，或多选后，点击列表顶部【删除所选】按钮，统一删除。

设备控制权限高于【策略防护-U 盘管理】，可用于控制使用对应策略的终端是否信任控制中心的注册 U 盘，【信任已注册 U 盘】配置项默认开启，已注册 U 盘列表可在【策略防护-U 盘管理】列表查看。



（6） 安全工具

除了病毒防护与系统安全为终端保驾护航，同时还提供了 9 种安全工具，帮助终端用户更方便的使用以及管理终端电脑。火绒针对安全工具为用户提供了三种操作方式：允许使用、禁止使用、禁止并隐藏。

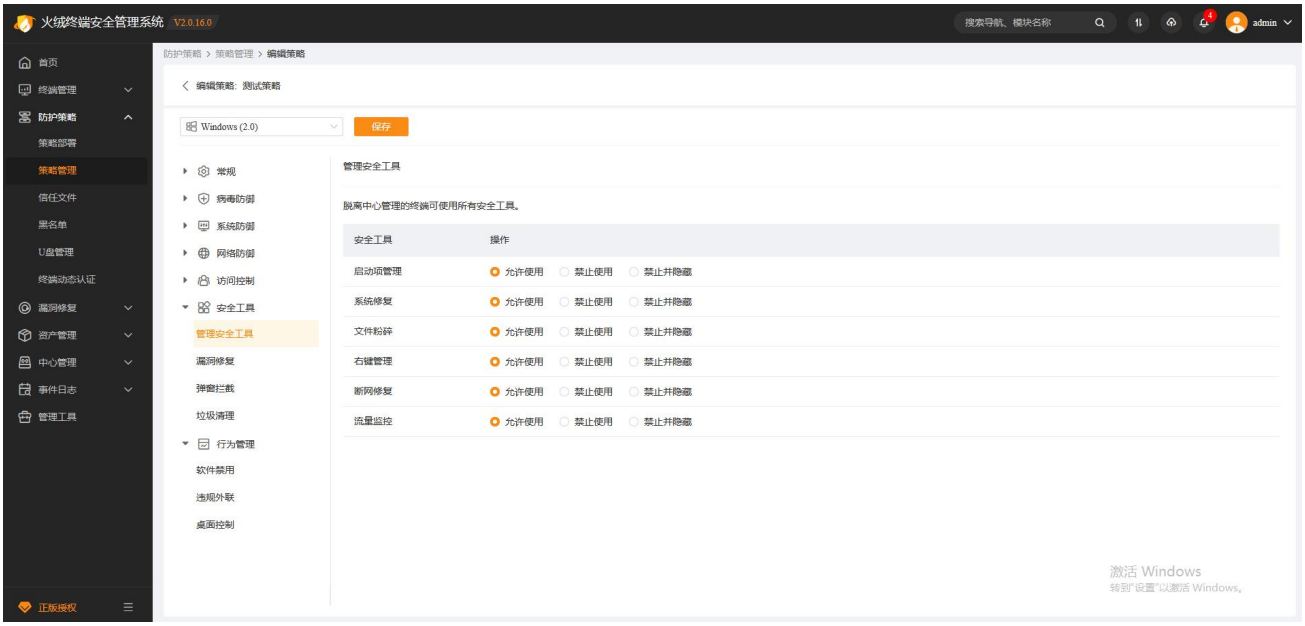
【允许使用】：终端用户可以在安全工具页看到该工具，并且可以正常使用。

【禁止使用】：终端用户可以在安全工具页看到该工具，但是无法使用。

【禁止并隐藏】：终端用户在安全工具页中看不到该工具并且无法使用。

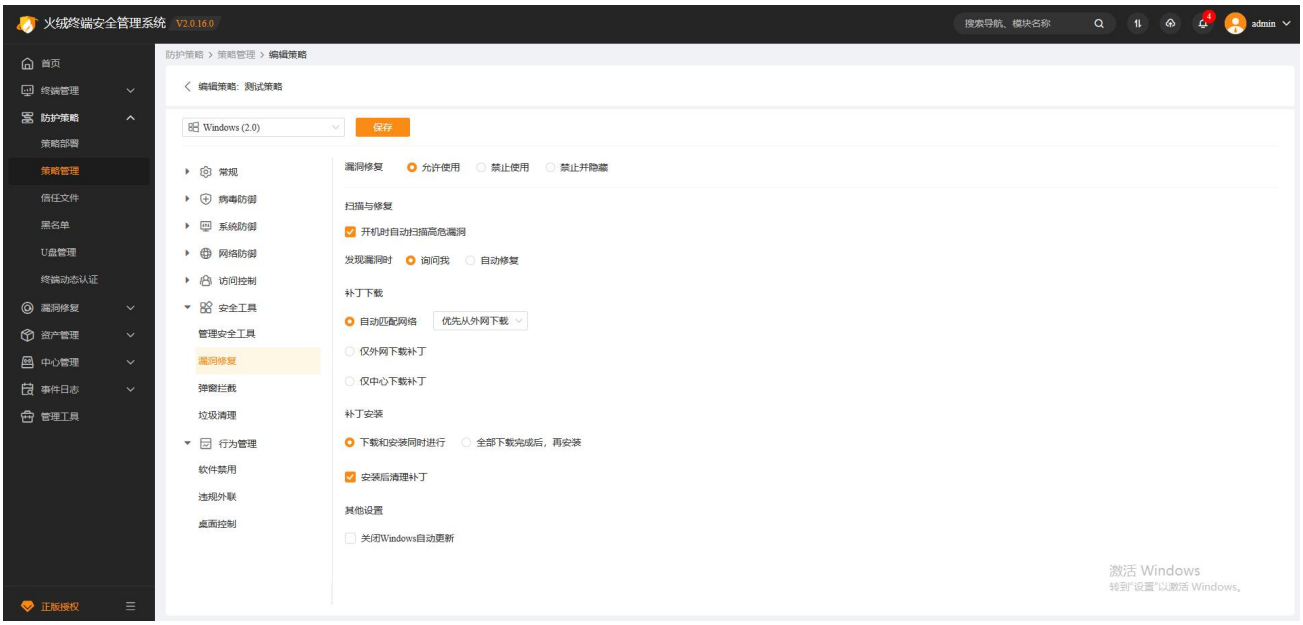
- 管理安全工具

管理安全工具页可对终端的【启动项管理】、【系统修复】、【文件粉碎】、【右键管理】、【断网修复】、【流量监控】6 个安全工具设置操作方式。



- 漏洞修复

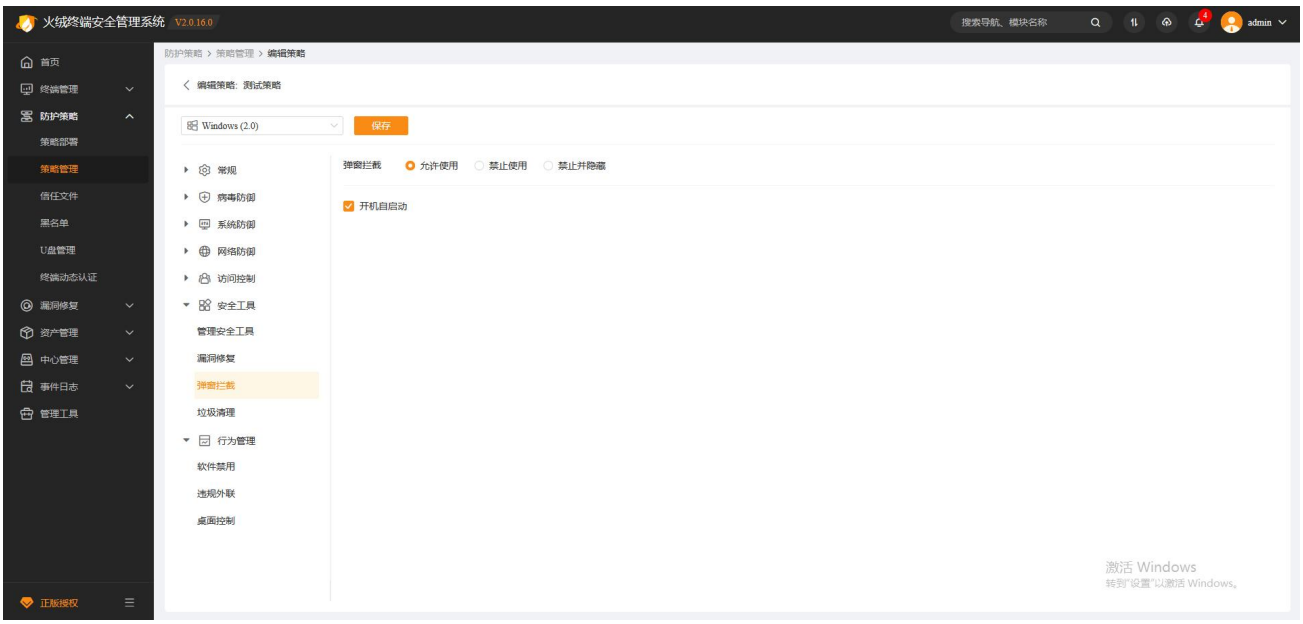
漏洞可能导致您的电脑被他人入侵利用，漏洞修复能第一时间获取补丁相关信息，及时修复已发现的漏洞。该页面可设置终端是否可以看到和使用该工具，还可以对漏洞修复进行详细设置。



- 弹窗拦截

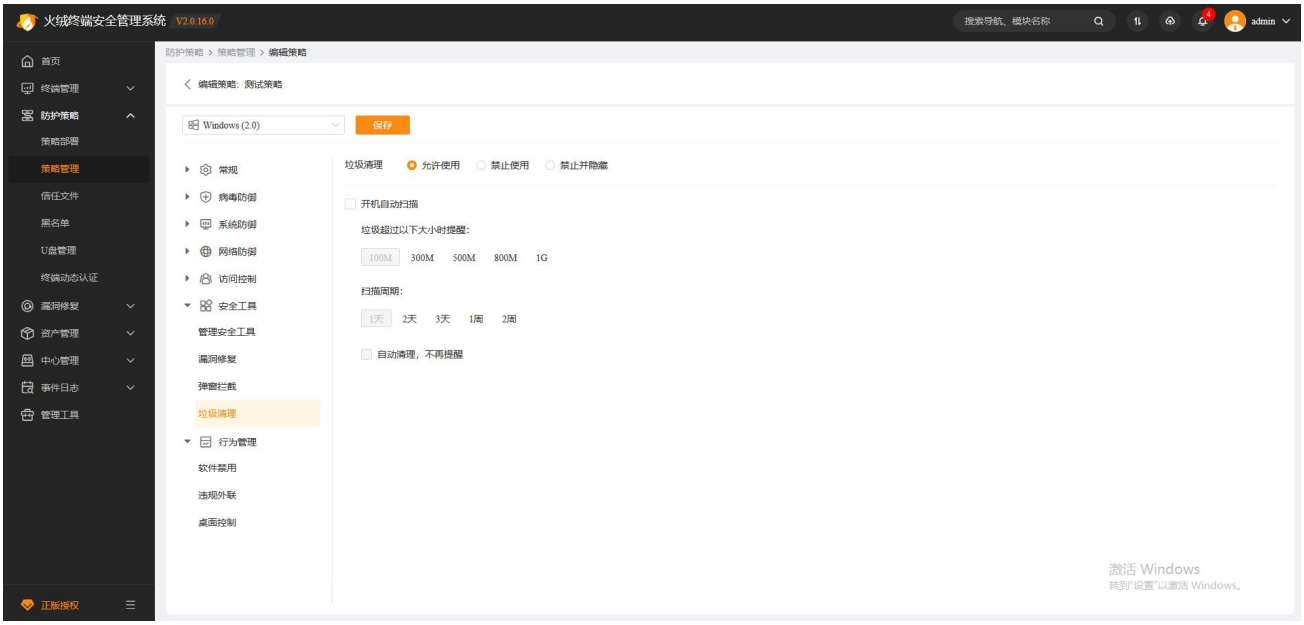
很多电脑软件在使用的过程中，会通过弹窗的形式，来推送资讯、广告甚至是一些其他软件，这些行为非常影响电脑的正常使用。弹窗拦截采用多种拦截形式，自主、有效的拦截弹窗。该页面可统一设置终

端弹窗拦截是否开机自启动以及终端是否可以看到和使用弹窗拦截功能。



- 垃圾清理

垃圾清理工具可以清理不必要的系统垃圾、缓存文件、无效注册表等，节省电脑使用空间。该页面可设置终端是否可以使用垃圾清理功能和开机自动扫描的详细规则。



（7） 行为管理

行为管理策略分为软件禁用和违规外联两部分，能够管理终端用户软件的使用，以及终端用户违规连

接外部网络的问题。

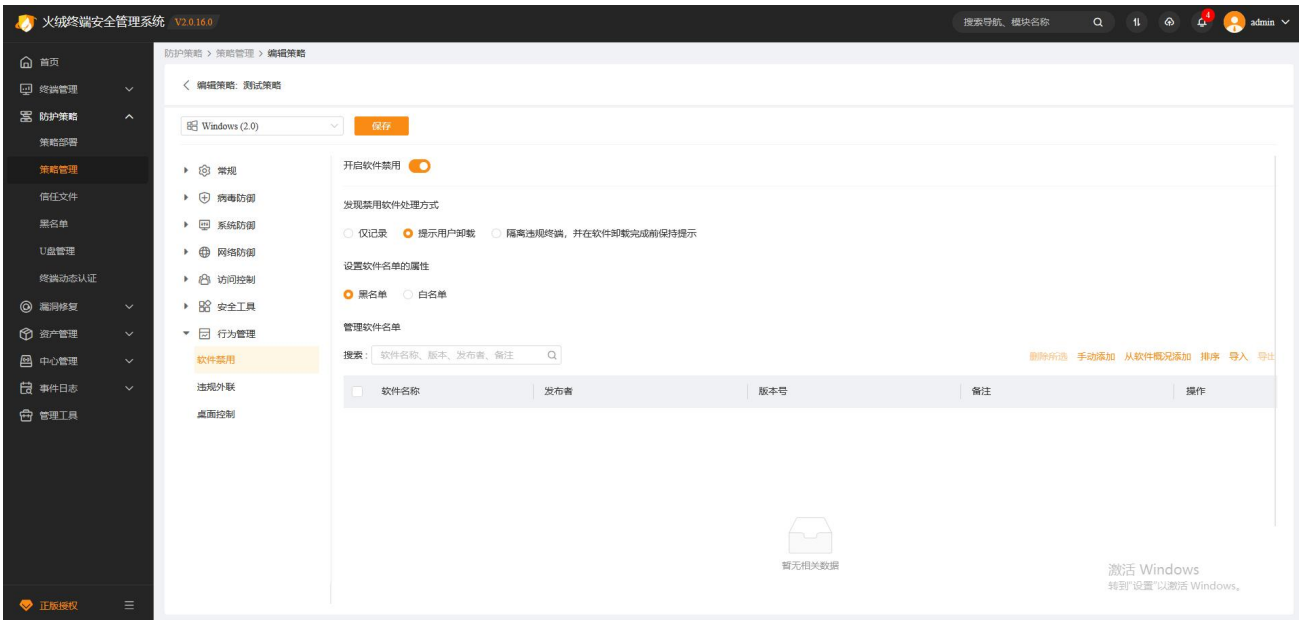
- 软件禁用

软件禁用策略可以选择软件名单的属性、添加软件名单以及设置发现终端使用禁用软件时的处理方式。

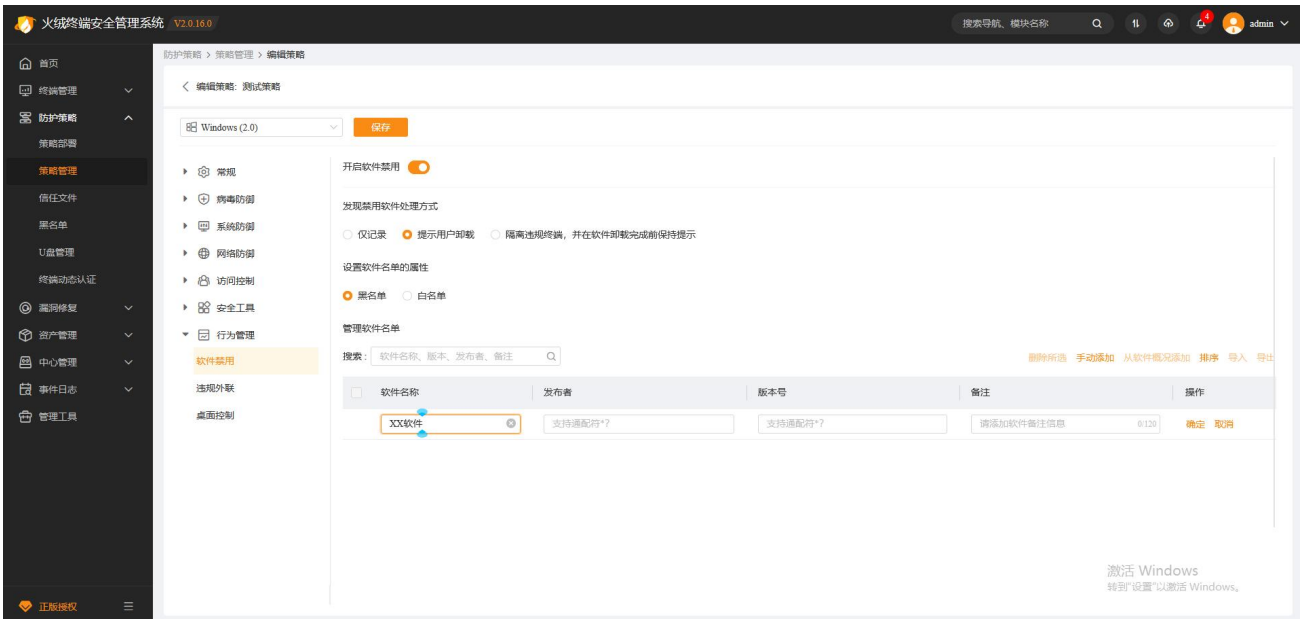
软件名单的属性分为黑名单和白名单，默认选择黑名单，此时，终端用户使用名单中添加的软件，会触发管理员设置的处理方式，名单外的软件可以正常使用；当设置软件白名单时，使用名单外的软件会触发管理员设置的处理方式，名单内的软件可以正常使用。

终端触发软件禁用有三种处理方式，管理员可以根据管控级别，设置不同的处理方式，1）仅记录，此种处理方式只会记录终端用户使用禁用软禁的行为，不会做出进一步处理；2）提示用户卸载，这种处理方式会以弹窗的形式，提醒终端用户卸载禁用软件；3）隔离违规终端并在软件卸载完成前保持提示，即对使用禁用软件的违规终端使用终端隔离功能，被隔离的终端除与中心通讯外，不能使用网络，弹窗提示终端用户软件卸载完成前无法使用网络。

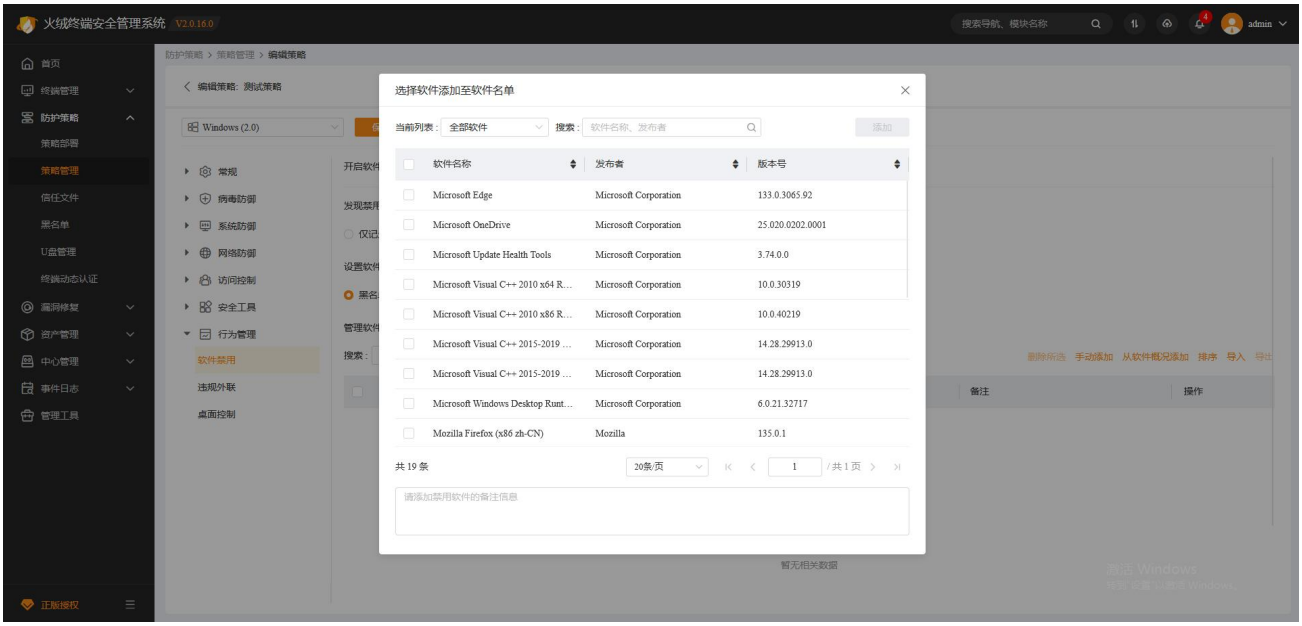
注：为避免误操作，当软件名单为空时，此策略不生效。



点击手动添加按钮，手动填写软件名称、发布者、版本号以及备注至软件名单。

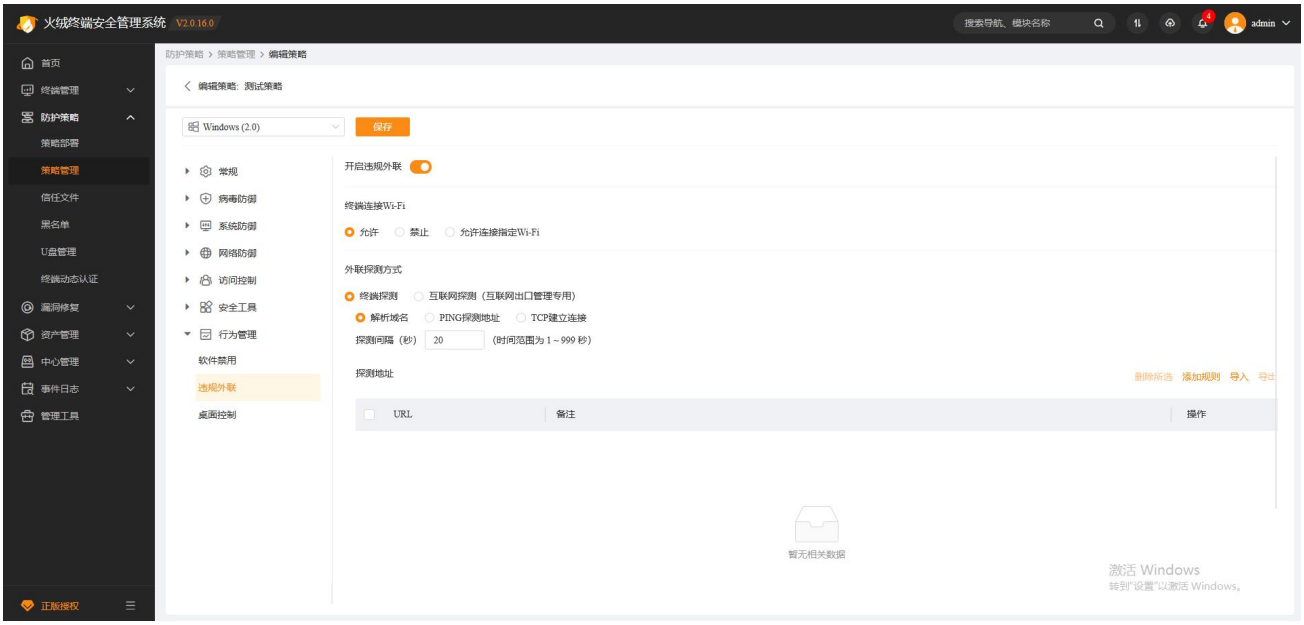


点击从软件概况中添加，可以在已有的列表中选择软件添加并设置备注。



- 违规外联

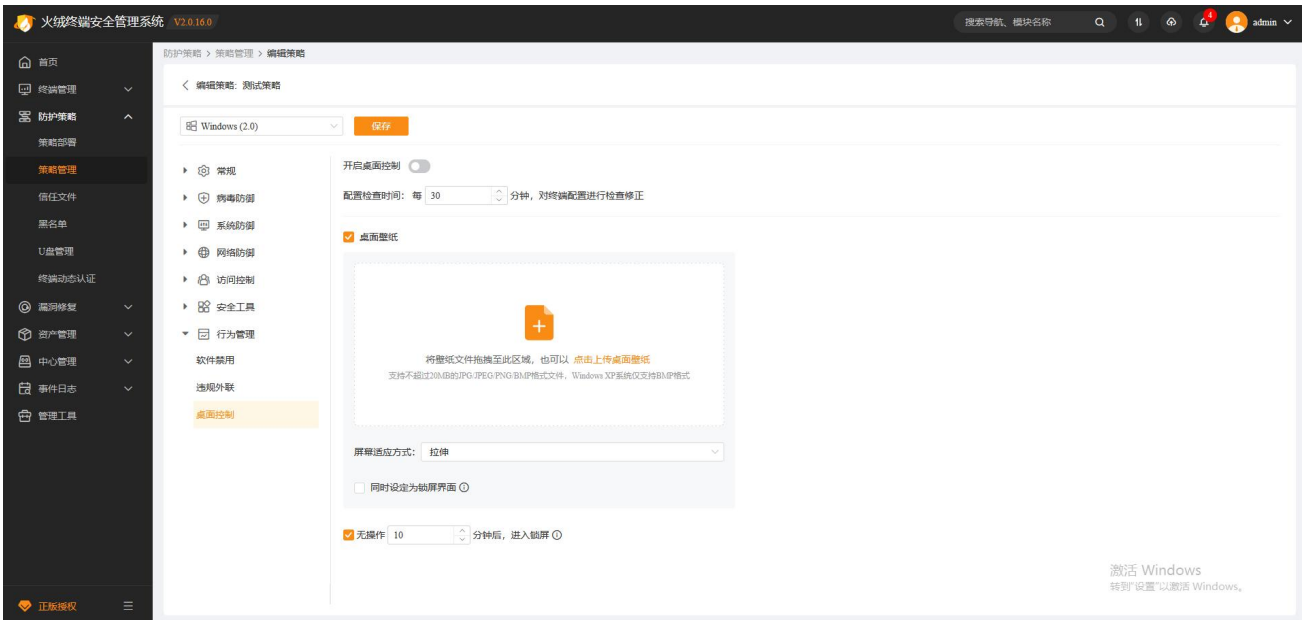
支持设置是否允许使用该策略的终端连接 Wi-Fi，或终端仅可连接指定的 Wi-Fi，管理员可自定义指定 Wi-Fi 信息。根据设置的外联探测方式探测终端用户是否有违规连接外部网络的行为，再根据处理违规外联的措施，处理终端用户的违规外联行为。



当处理方式为仅记录时，终端只记录违规外联的日志，不对违规行为做处理；当选择倒计时关机后，终端将在倒计时结束后强制关机；当选择断开网络时，将会对违规外联的终端用户进行断网处理。

- 桌面控制

支持统一设置桌面壁纸，锁屏壁纸，无操作自动锁屏时间（注：Linux 桌面版终端执行【无操作 N 分钟后，进入锁屏】策略时，若 Linux 终端不支持管理员填写的时间 A，则终端会自动在支持的数值中取一个最接近 A 且比 A 大的数值）。



2. 查看策略

系统内置默认防护策略，用户可依据企业内安全策略需要自行选用，内置策略默认不可修改，只允许查看策略内容。

用户点击策略右侧【查看策略】按钮即可查看当前策略内容。

3. 编辑策略

用户可对已创建的策略进行重新编辑修改，点击策略右侧【编辑策略】即可进入策略编辑界面。

4. 删除策略

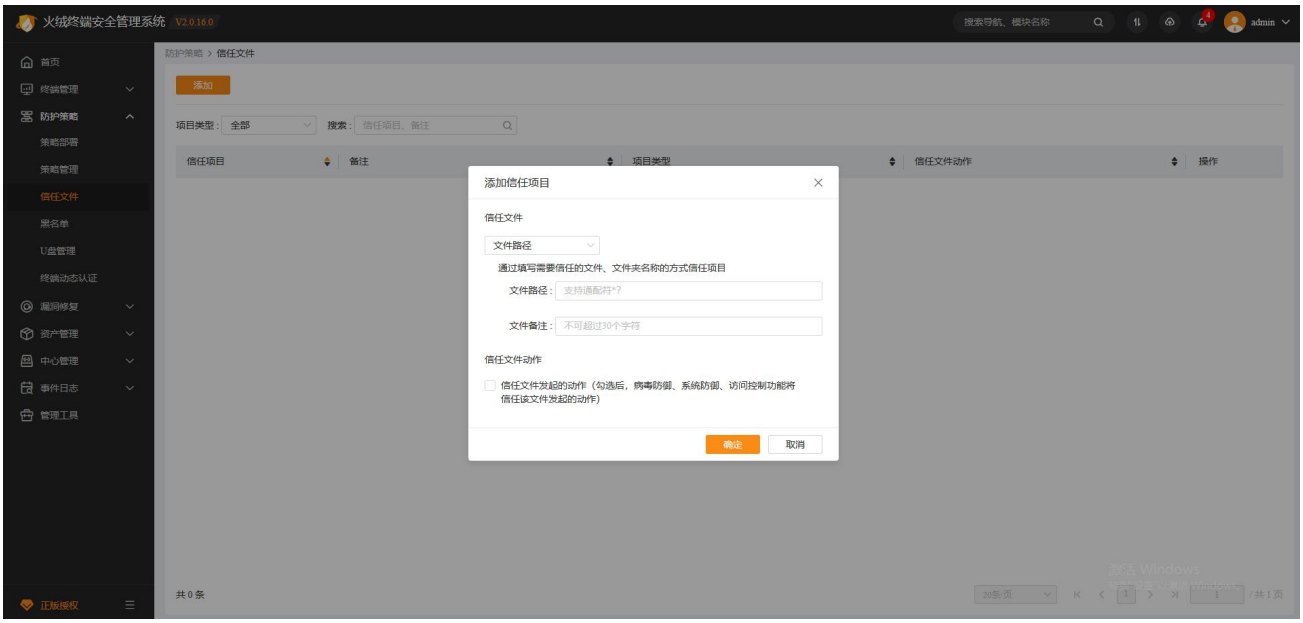
用户可删除已创建的安全策略，策略删除后，使用该策略的分组将自动切换为默认防护策略。

2.6.3 信任文件

火绒终端安全管理系统支持信任文件功能，用户可将指定文件作为可信任的文件，通过控制中心添加为信任文件，添加成功后，信任文件将不会被查杀；

用户点击【添加】按钮后，可进入信任文件添加界面，填写信任文件路径后点击【确定】即可成功添加信任文件，已添加的信任文件项目支持编辑与删除操作。当前支持通过三种方式添加信任项目：

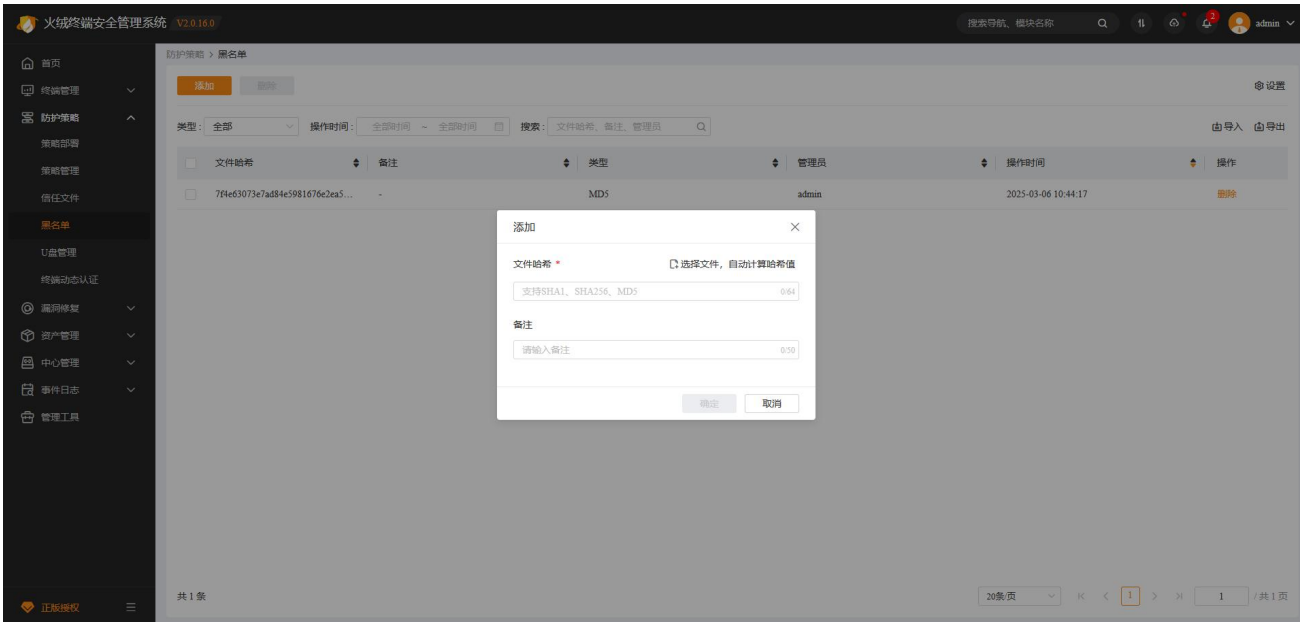
- 信任文件路径：输入文件路径信任文件，支持通配符（*和？），支持信任文件动作
- 信任文件 sha1：输入文件 sha1 来信任文件。在 IE8 以上的浏览器中支持选择本地文件自动算出对应 sha1，支持信任文件动作
- 信任网址：输入网址来信任该网址，不支持信任文件动作



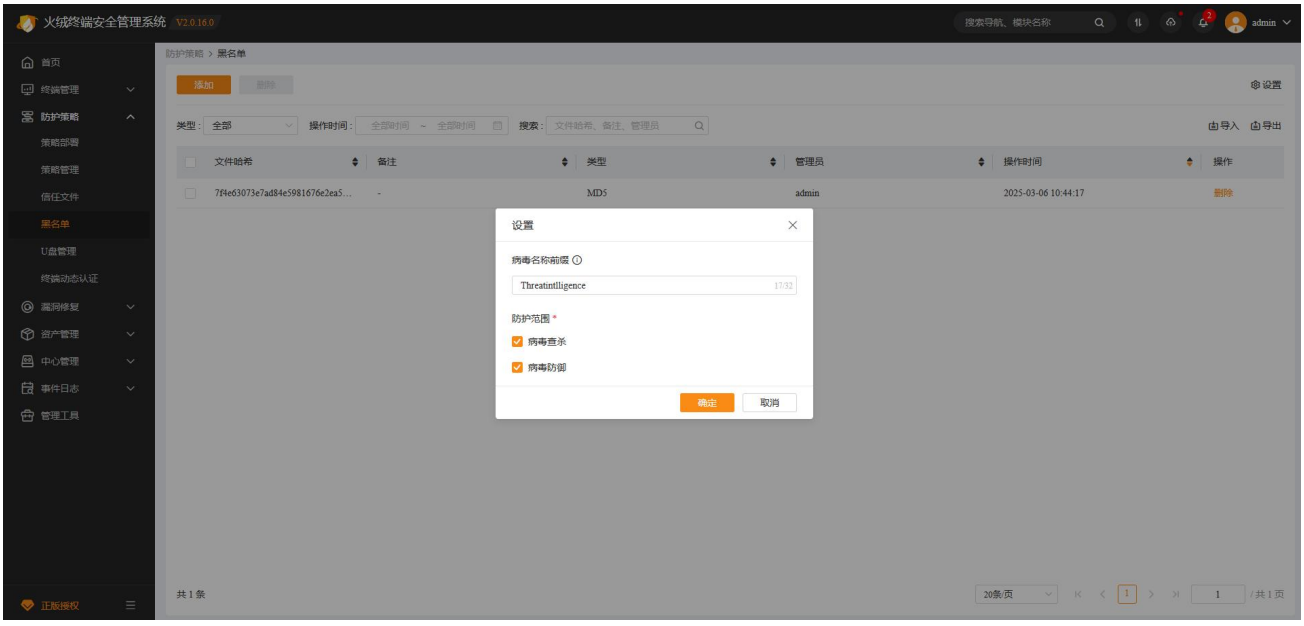
2.6.4 黑名单

火绒终端安全管理系统支持黑名单功能，用户可自定义将文件哈希添加至黑名单，添加成功后，终端检测到对应哈希值的文件将会被按照病毒处理；

用户点击【添加】按钮后，可进入黑名单添加界面，填写文件哈希（支持 SHA1、SHA256、MD5）后（还支持选择本地文件自动算出对应 SHA1），点击【确定】即可成功添加，已添加的黑名单支持删除操作。



支持设置终端检测到黑名单文件后日志中记录的病毒名称前缀，支持设置黑名单文件的涉及的防护范围，勾选后终端对应的防护功能会检测黑名单文件并按照病毒处理。

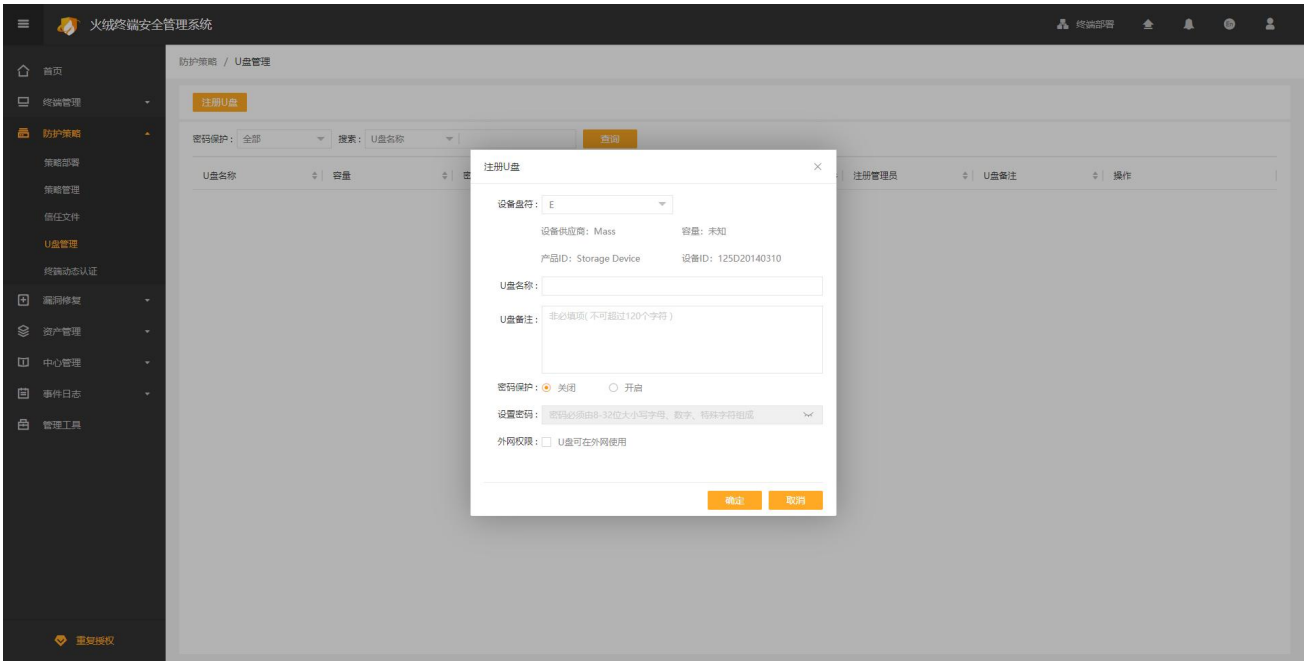


2.6.5 U 盘管理

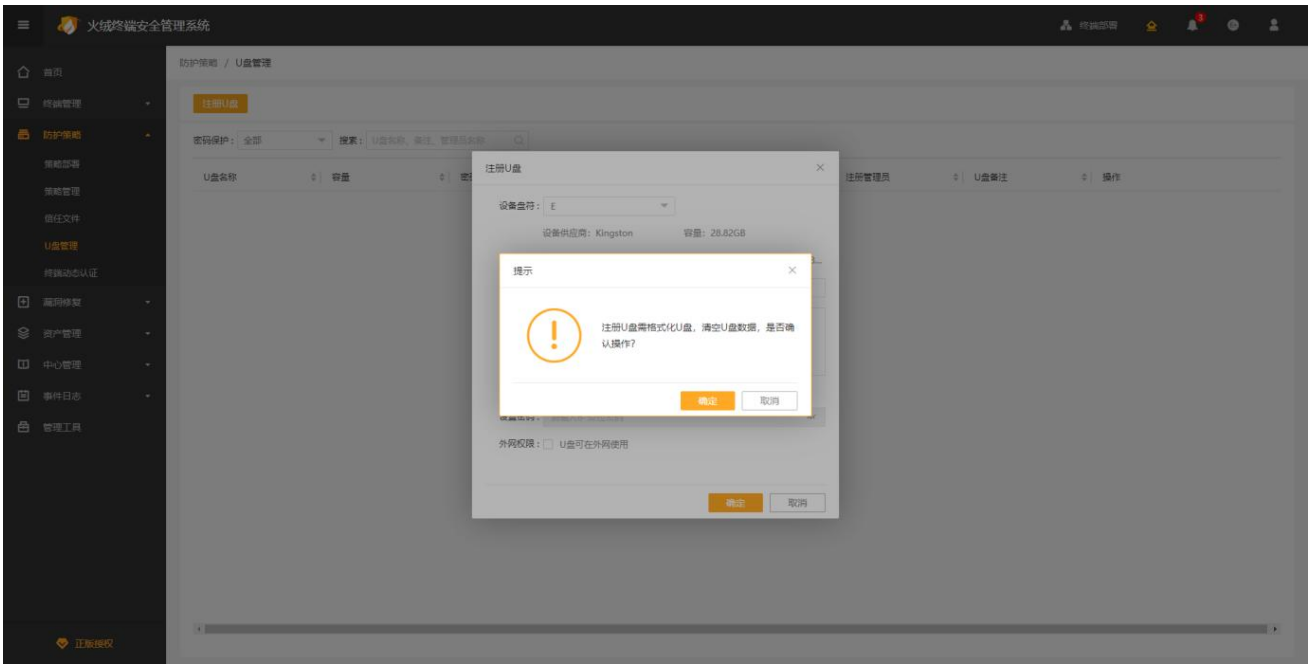
火绒终端安全管理系统支持 U 盘信任功能，用户可将 U 盘注册为信任 U 盘，防止未授权 U 盘访问企业内部环境，方便用户企业内部 U 盘使用情况进行管理。

用户可在【防护策略】-【U 盘管理】界面点击【注册 U 盘】按钮进行 U 盘信任注册（注册前必须下载安装移动存储注册工具），点击确定可对当前 U 盘进行注册。注册界面各选项含义：

- 设备盘符：点击可显示当前所有移动存储设备所在的盘符。选择后下方文字会显示所选移动存储设备的基本信息。
- U 盘名称：为 U 盘设备添加名称。
- U 盘备注：备注内容，可不填写。
- 密码保护：为 U 盘设备添加密码。默认为关闭，开启后下方设置密码输入框启用，为 U 盘设置密码。
- 外网权限：默认不勾选，不勾选时注册的 U 盘设备无法在未安装火绒终端或无法访问中心的计算机上运行。勾选后无此限制。



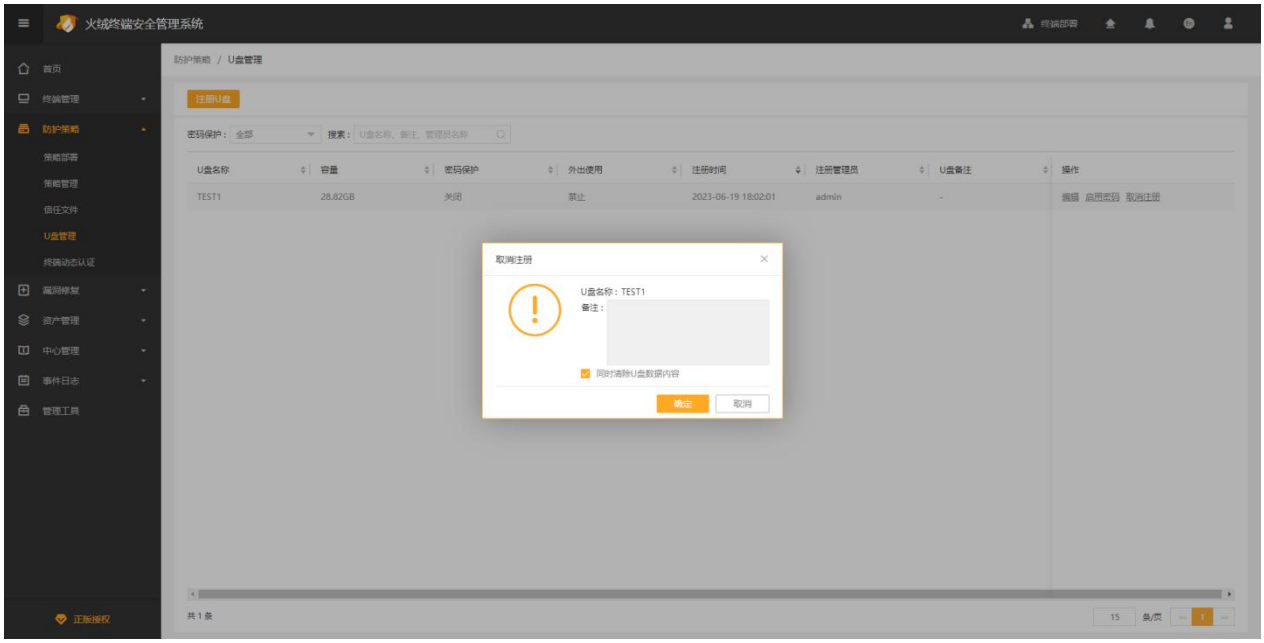
用户填写信息完毕后，点击【确定】弹出格式化提示框（注册 U 盘前必须将 U 盘格式化，请谨慎选择），再次点击【确定】即可开始注册信任 U 盘。



U 盘格式化及注册期间请勿拔出 U 盘。

U 盘注册完成后，中心【防护策略】-【U 盘管理】界面对应新增一条 U 盘注册记录，用户可对已注册 U 盘进行编辑、启用/修改密码、取消注册操作。

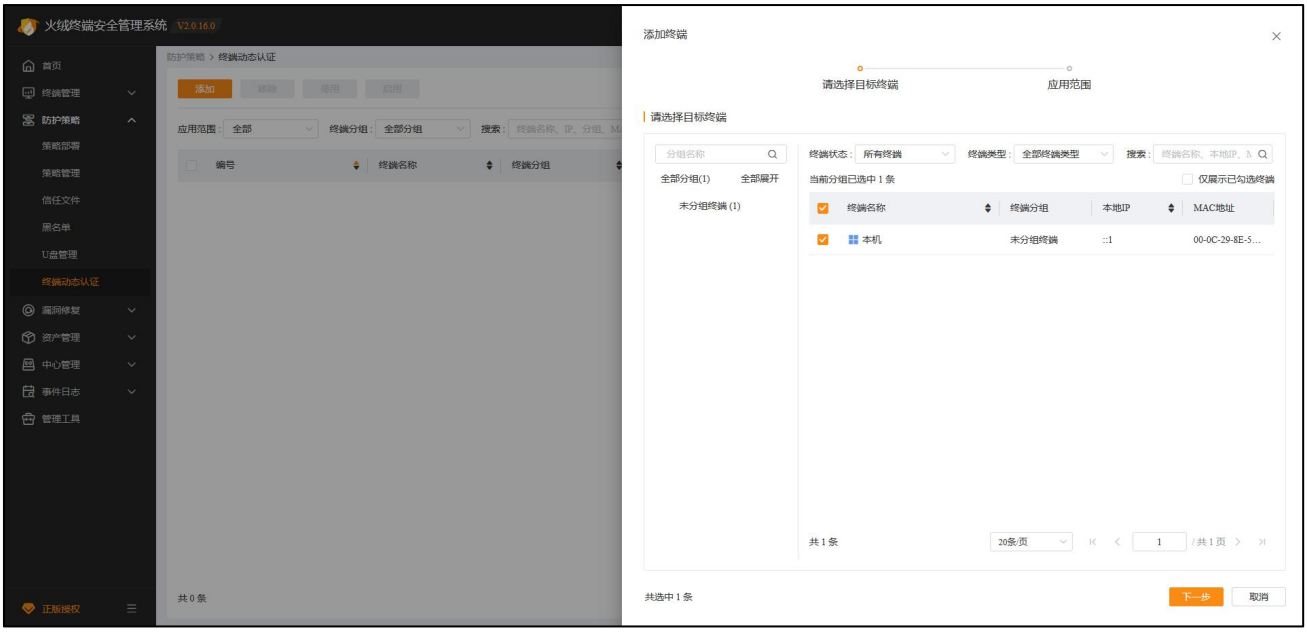
- 编辑：编辑已注册 U 盘名称及备注信息
- 启用/修改密码：未启用密码的 U 盘可进行密码启用，已启用密码的 U 盘可修改密码
- 取消注册：点击出现取消注册提示弹窗，取消注册窗口显示 U 盘名称、备注及清除 U 盘数据内容配置项，不管是否插入想要取消注册的已注册 U 盘，都可以取消注册该已注册 U 盘。



2.6.6 终端动态认证

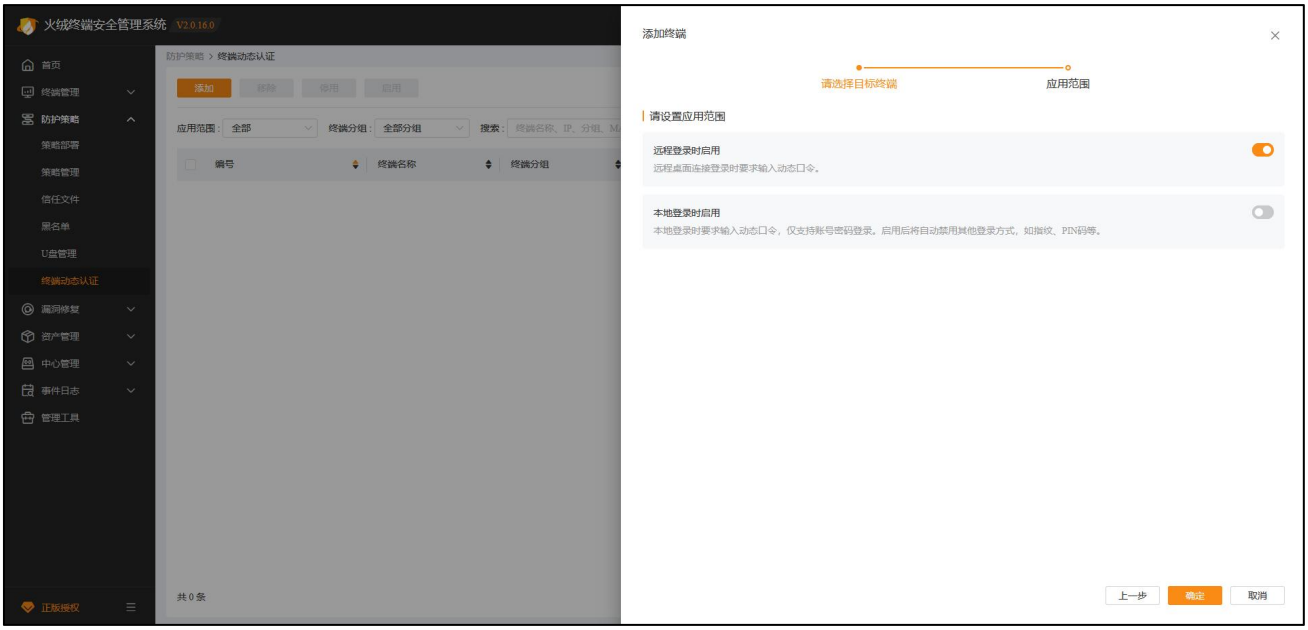
火绒终端安全管理系统支持终端动态认证功能，可分别针对远程登录和本地登录两种模式开启动态认证功能，动态认证功能开启后，终端进行对应模式登录时，需要正确输入火绒动态口令才可以登录成功，建议用户在需要频繁远程登录的终端或存放重要资料数据的终端开启此功能，增强终端安全性，避免非法用户通过非法手段登录终端造成不必要的损失。

用户可在【防护策略】-【终端动态认证】界面，点击【添加】按钮添加终端动态认证功能。



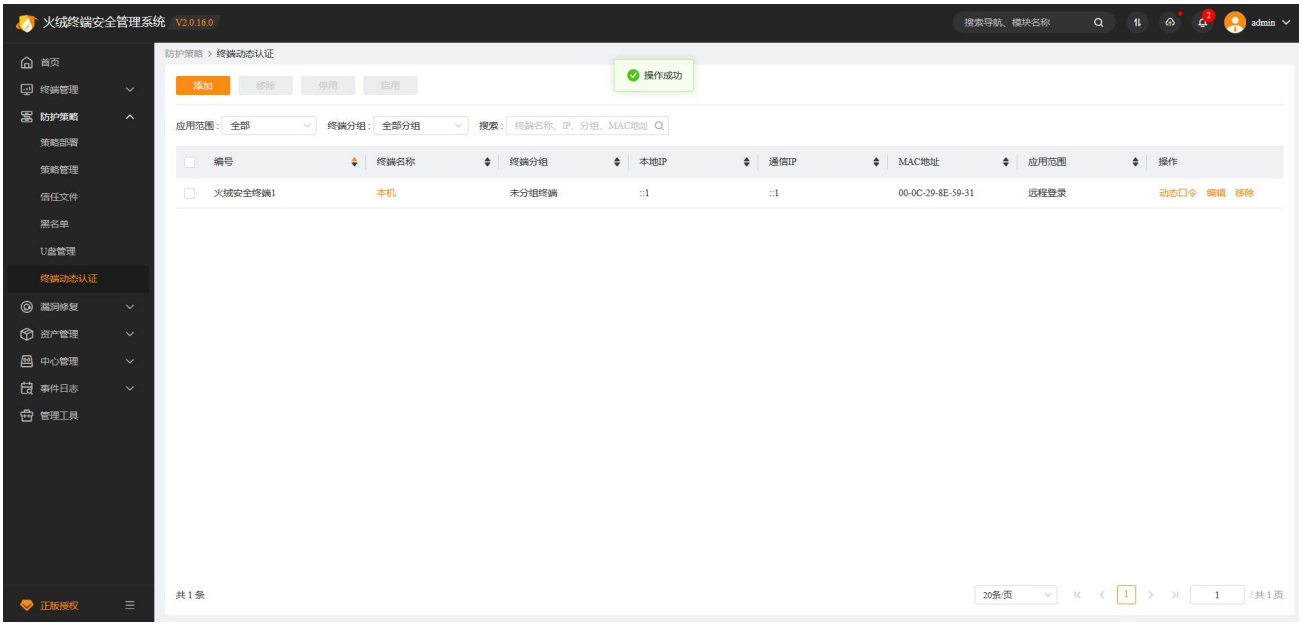
用户选择需要添加动态认证的终端后，点击【下一步】即可进入应用范围设置界面，应用范围设置目前支持远程登录及本地登录两种：

- 远程登录：开启后，远程桌面连接登录时要求输入动态口令
- 本地登录：开启后，本地登录时要求输入动态口令，仅支持账号密码登录。启用后将自动禁用其他登录方式，如指纹、PIN 码等

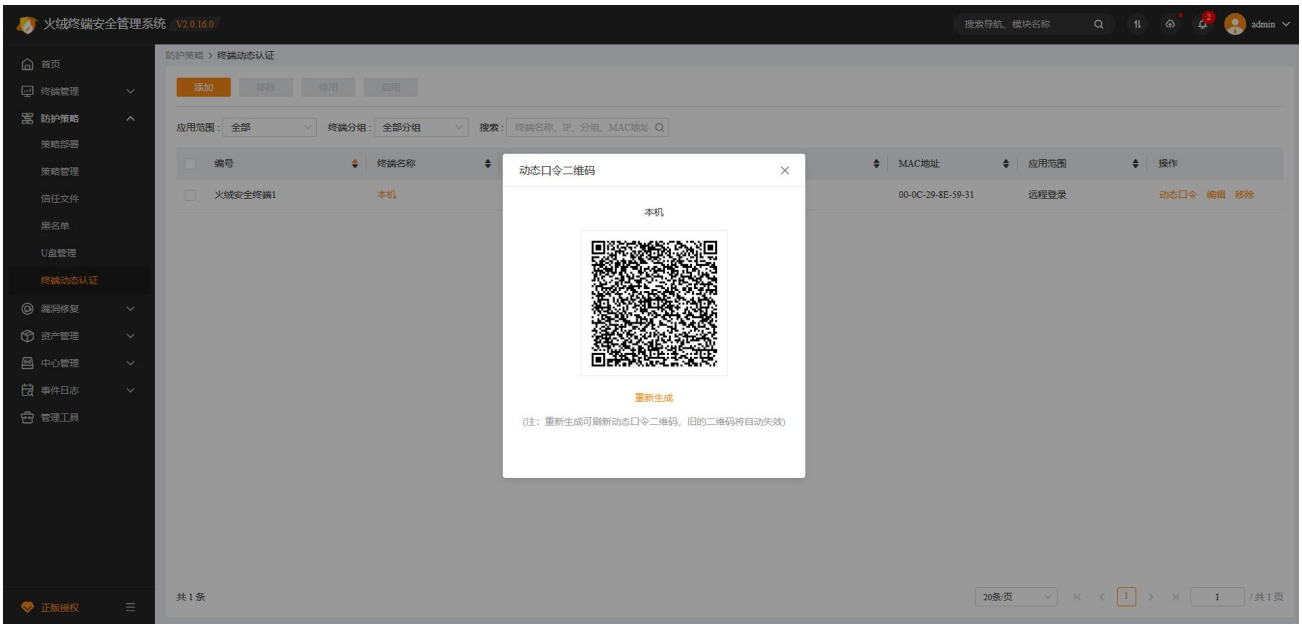


用户选中需要开启的应用范围后，点击【确定】即可成功开启终端动态认证功能，对于已开启此功能

的终端，用户可以进行动态认证口令查看及重新生成、编辑应用范围、停用、启用及移除操作。



点击终端操作列的动态口令按钮将弹出动态口令二维码，使用火绒安全动态口令微信小程序扫描二维码即可获取该终端的动态口令。



2.7 漏洞修复

火绒终端安全管理系统支持中心统一管理终端漏洞修复功能，用户可从中心查看连接当前中心的所有

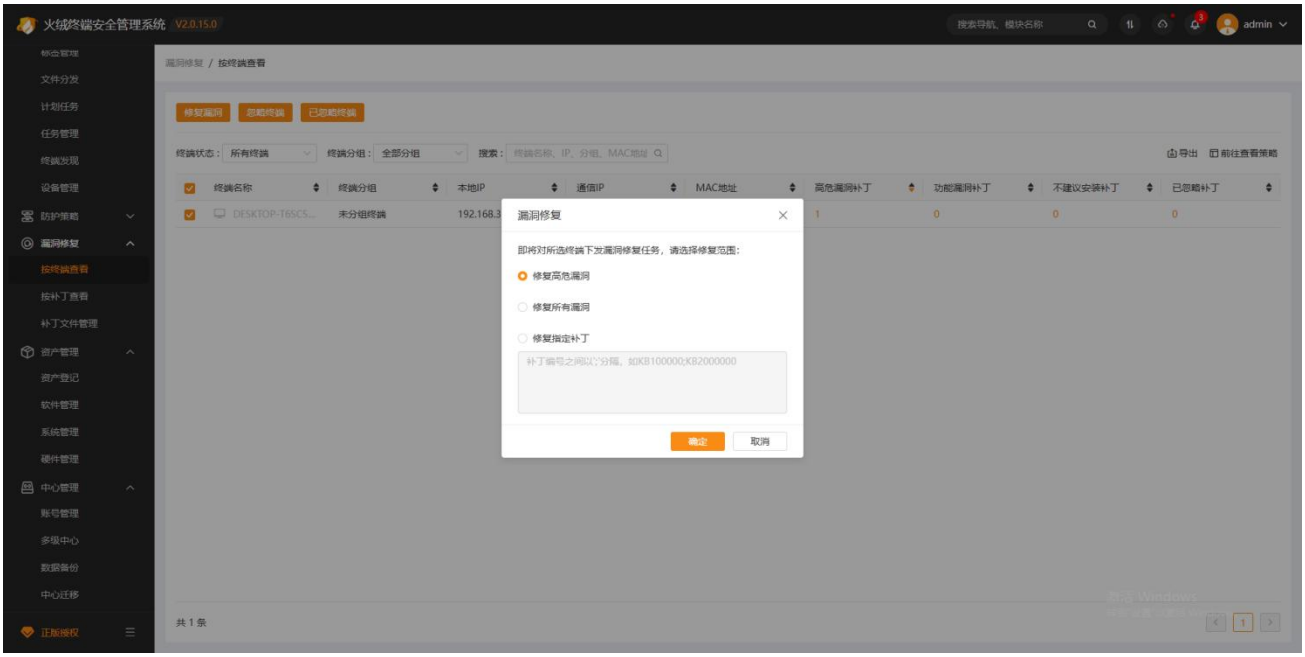
终端的漏洞信息，一键下发漏洞修复任务，方便用户统一管理与维护企业终端环境。

2.7.1 按终端查看

用户可通过【漏洞修复】-【按终端查看】界面，以终端为查看视角，查看各终端对应的不同类型补丁。

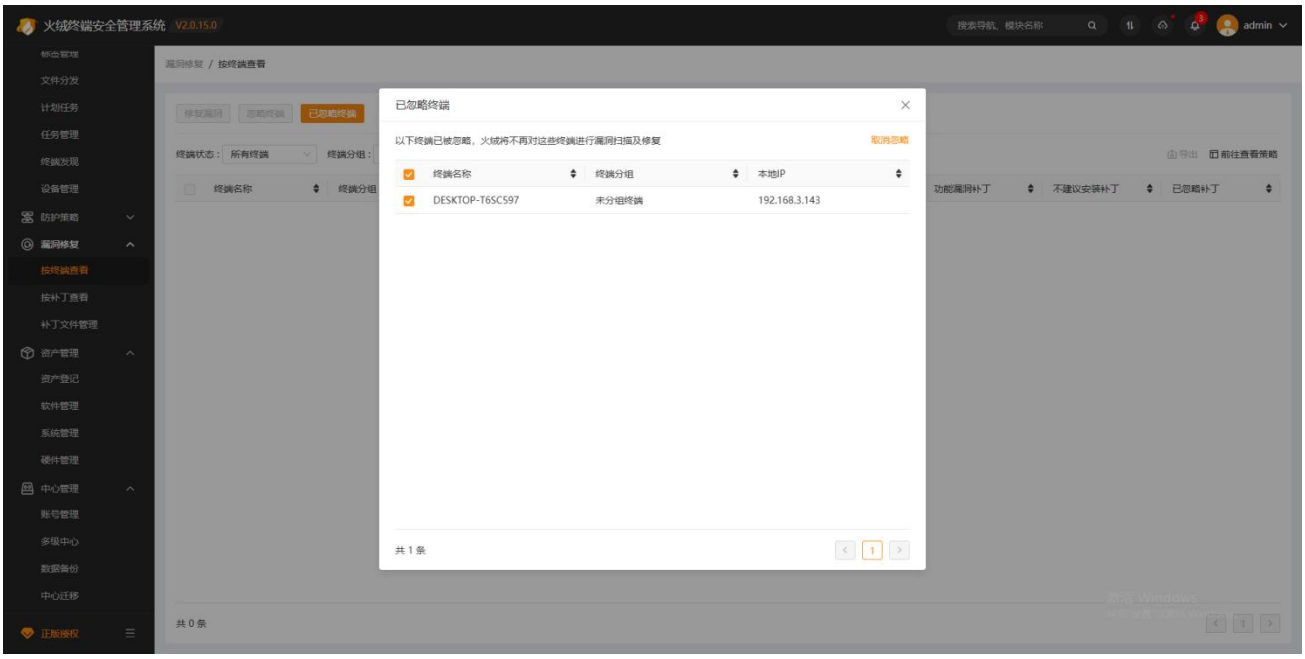
1. 修复漏洞

用户选中需要下发漏洞修复任务的终端后，点击【修复漏洞】按钮，选择修复范围后点击【确定】即可将漏洞修复任务下发至所选终端。



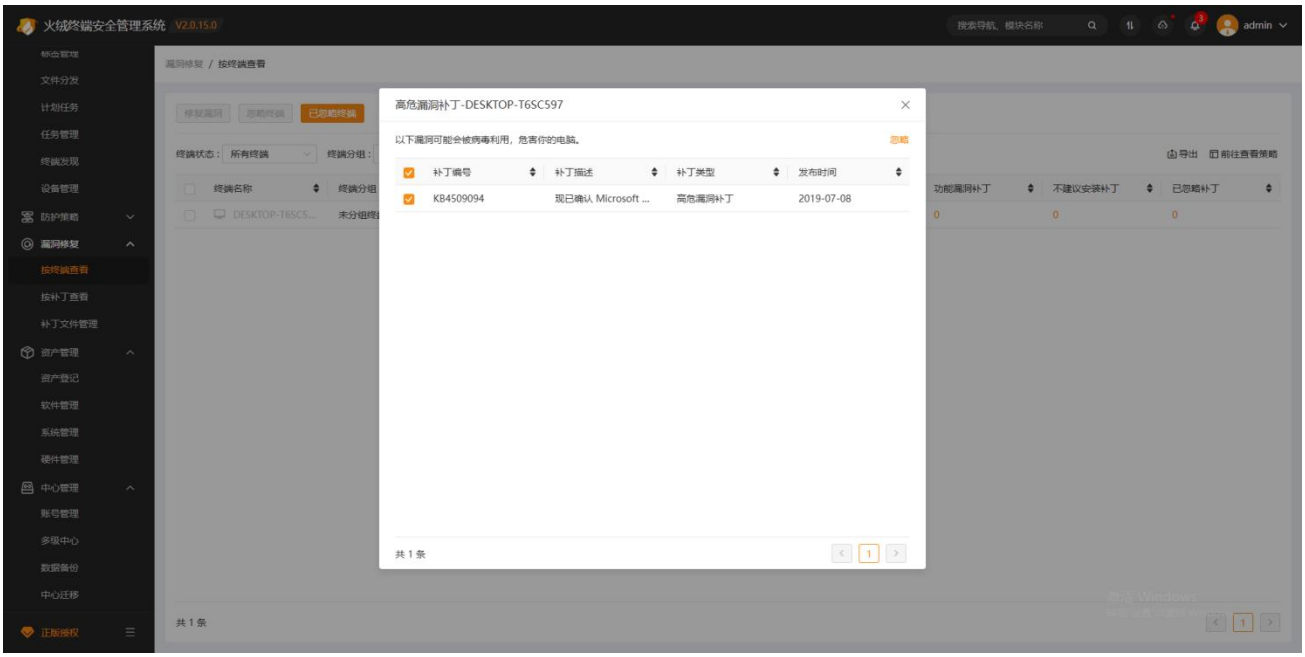
2. 忽略终端

用户可选择将部分终端忽略，终端忽略后将不会出现在漏洞修复的界面列表中，选中要忽略的终端，点击【忽略终端】即可将所选终端忽略漏洞修复。用户点击【已忽略终端】可查看当前中心已忽略的终端，选中已忽略终端后，点击【取消忽略】可以恢复终端状态，将已忽略终端重新添加至终端漏洞修复列表。



3. 忽略补丁

用户点击列表中补丁数量，可查看此类补丁详细信息，并且可以选中当前列表中的补丁，点击【忽略】即可忽略当前补丁，下发修复任务时自动忽略已忽略补丁；



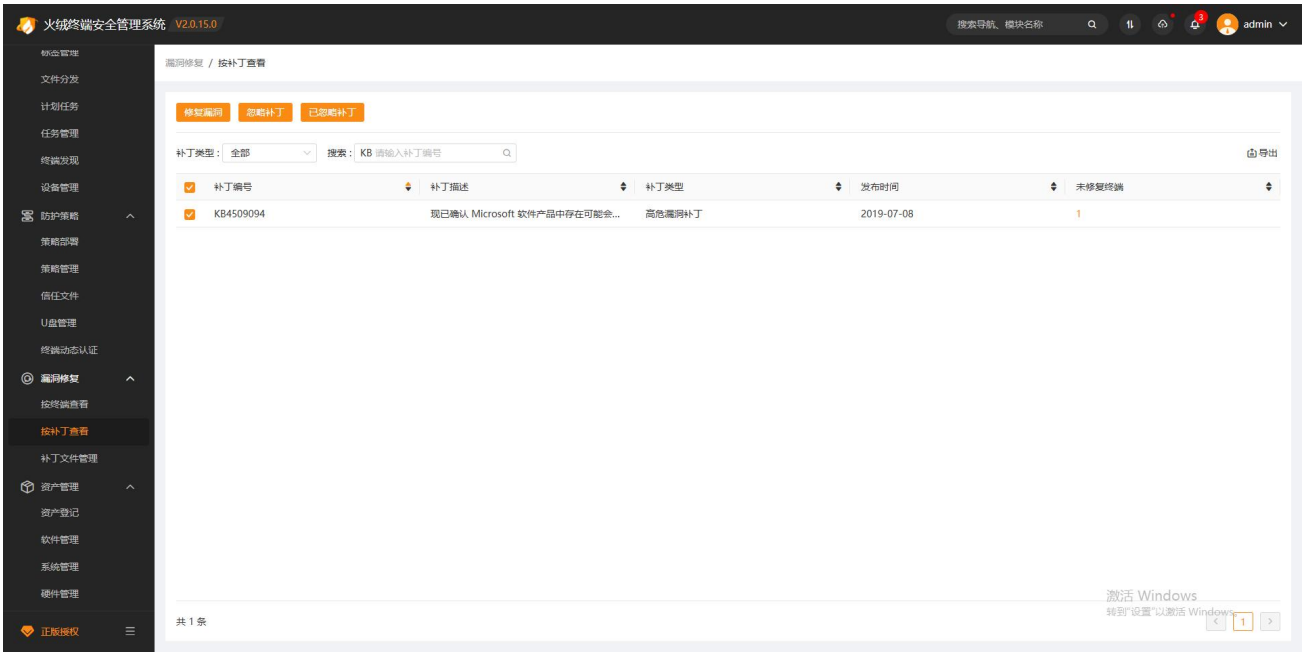
已忽略的补丁会显示在列表中“已忽略补丁”列表项中，点击已忽略补丁列表项可显示当前已忽略补丁，选中补丁后点击【取消忽略】可恢复当前补丁为待修复状态。

4. 前往查看策略

用户点击【前往查看策略】按钮，将跳转至防护策略-策略管理页面，用户可以自行选择策略，并编辑该策略下的漏洞修复功能的策略设置。

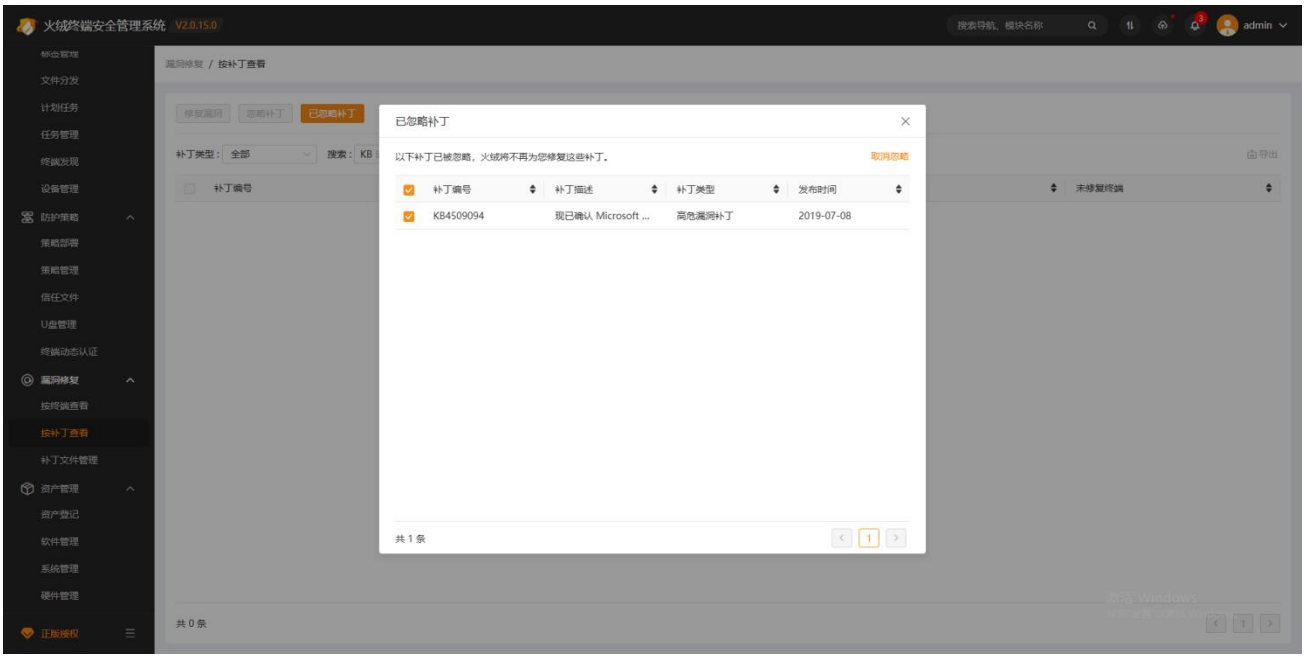
2.7.2 按补丁查看

用户可通过【漏洞修复】-【按补丁查看】界面，以补丁为查看视角，查看及管理所有终端检测到的待修复补丁文件。



用户可以使用【修复漏洞】功能，选择当前列表中的指定补丁，选择终端下发漏洞修复任务。

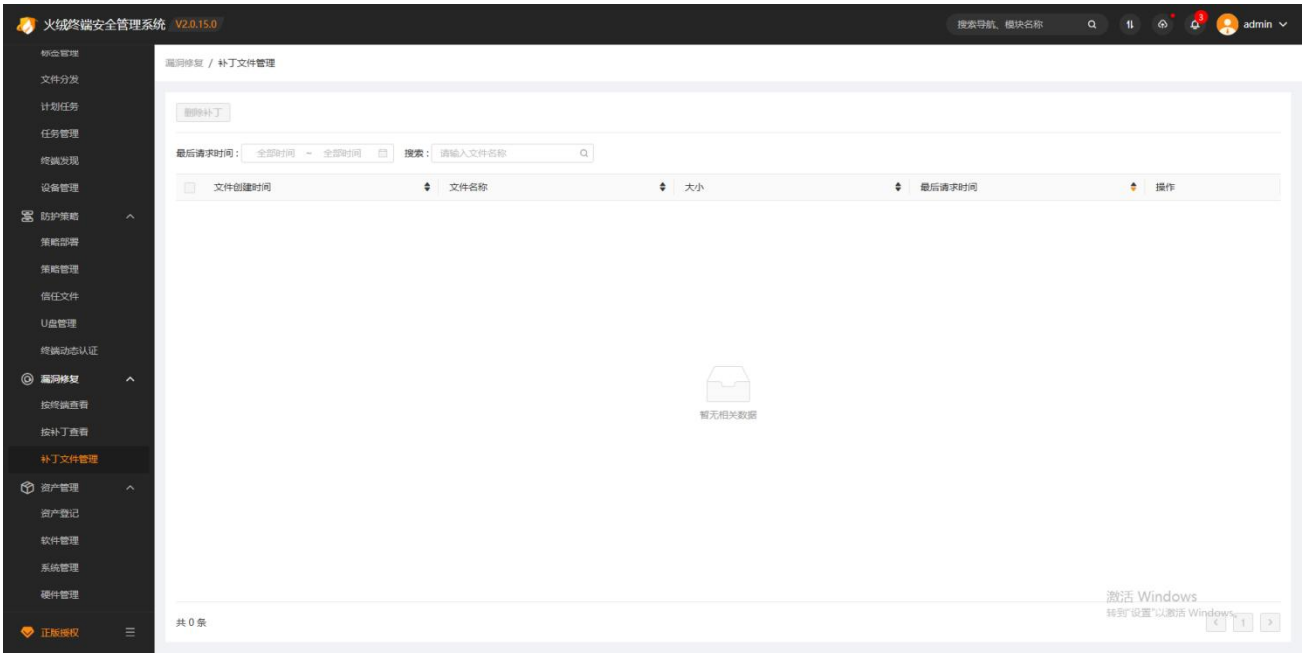
也可选择忽略部分补丁，忽略后的补丁终端将不再检测和修复。选择希望忽略掉的补丁，点击【忽略补丁】按钮即可将选中补丁忽略，已忽略的补丁可通过点击【已忽略补丁】按钮查看，选中补丁后点击【取消忽略】可恢复当前补丁为待修复状态。



2.7.3 补丁文件管理

用户可在【漏洞修复】-【补丁文件管理】界面查看当前已下载缓存在中心的所有补丁。并且提供最近一次该补丁被终端请求下载的时间“最后请求时间”，方便管理员删除长时间未使用的漏洞补丁。

用户可下载或删除漏洞补丁，支持批量删除。



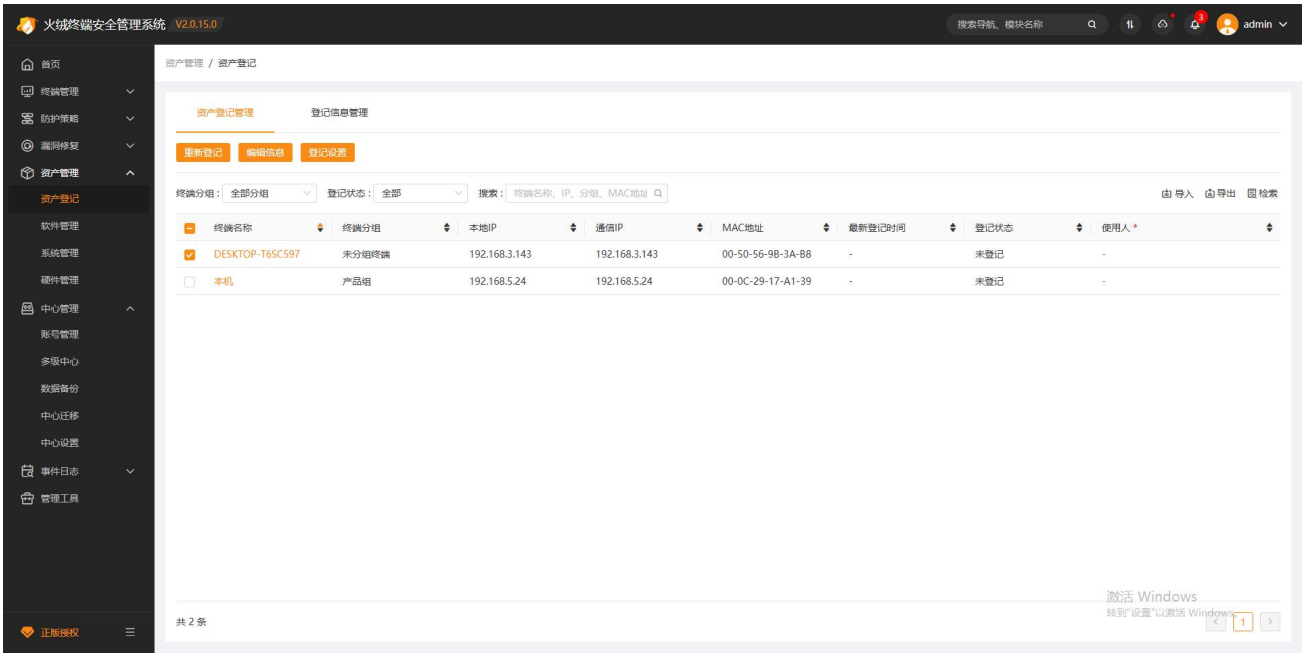
2.8 资产管理

火绒终端安全管理系统支持资产统一管理功能，用户可添加需要登记的信息，下发登记任务给终端。终端在接受资产登记任务后按登记信息填写并上报终端信息给中心。同时中心也会统计终端安装的软件、硬件及终端操作系统信息，方便管理员对终端资产的统计与管理。

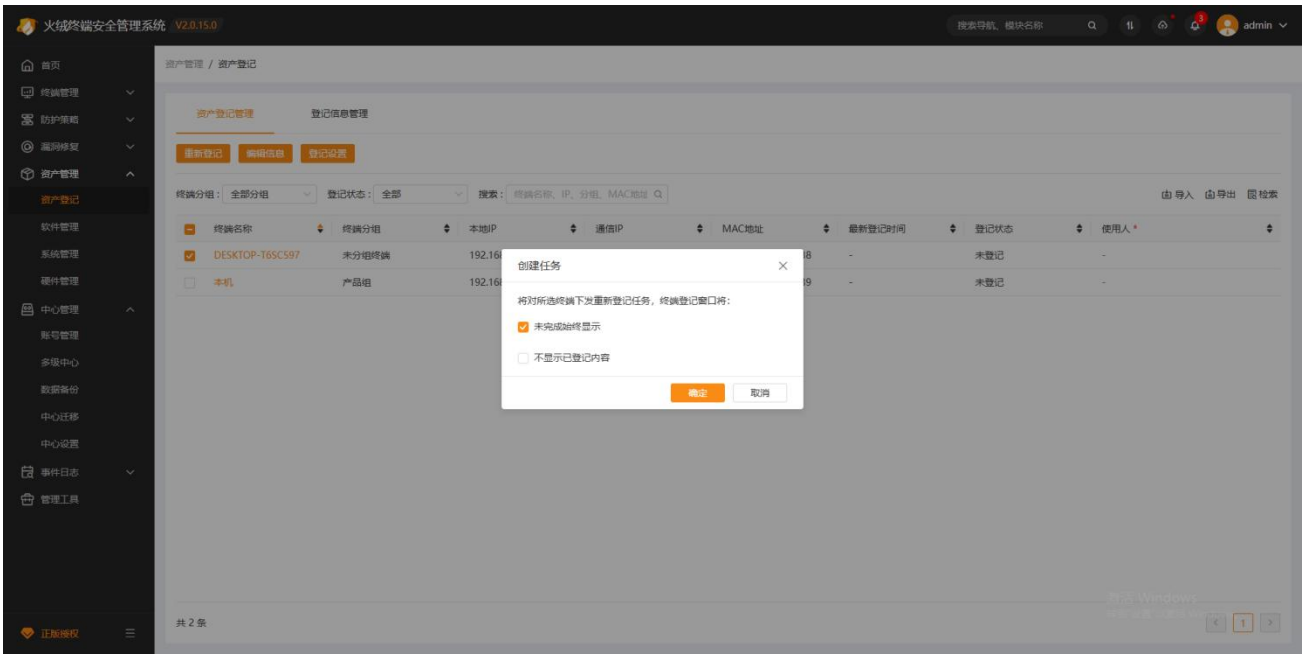
2.8.1 资产登记

1. 资产登记管理：

用户可在【资产管理】-【资产登记管理】界面进行资产登记任务的下发、终端资产的查看及编辑。

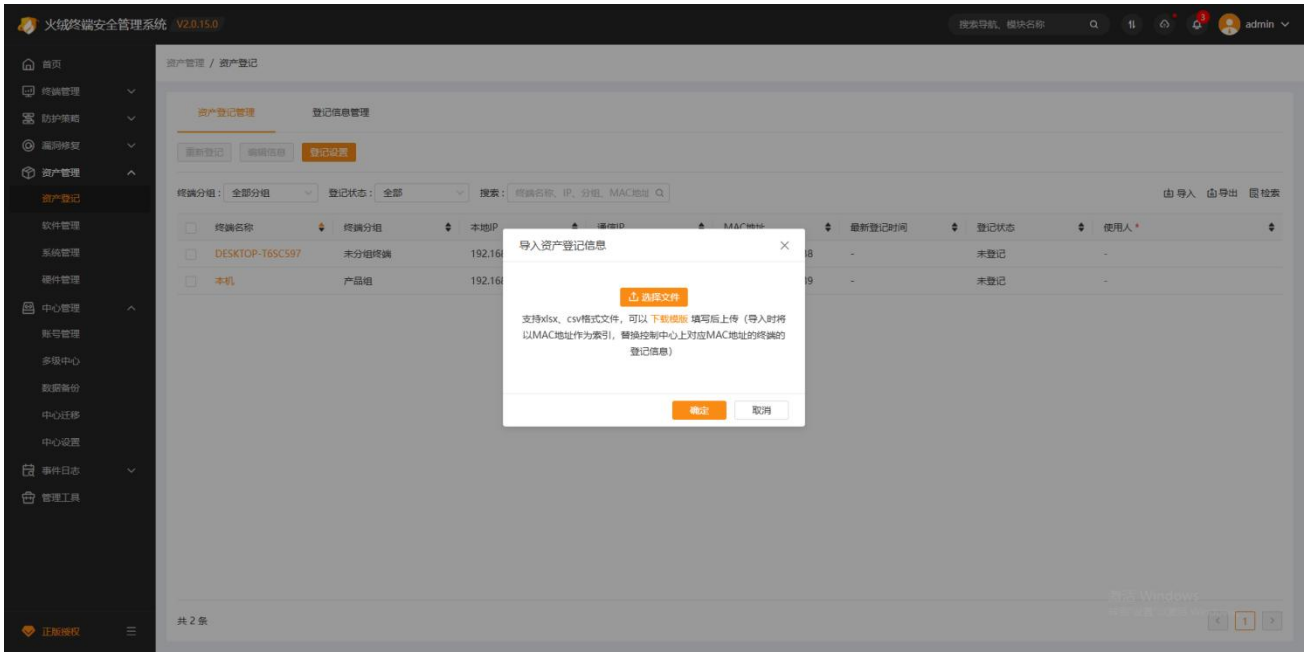


（1） 重新登记：用户选择需要重新下发资产登记任务的终端，点击【重新登记】按钮，用户可以根据需要设置终端登记是否进行强制登记、在终端页面是否可以查看已填写信息；点击【确定】中心将会对选中的终端重新下发资产登记任务。



(2) 编辑信息：用户选中待选终端，点击【编辑信息】按钮，可对终端当前登记的信息进行编辑修改。

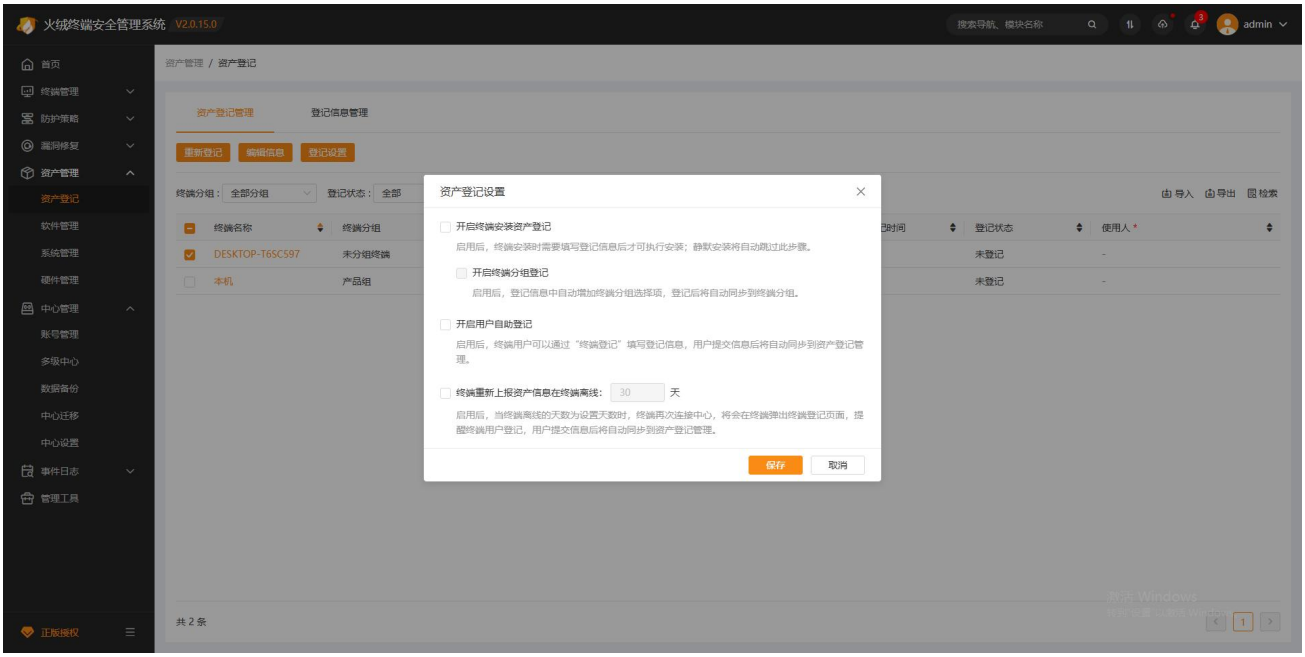
(3) 导入：支持导入登记信息，支持导入格式为 xlsx 或 csv。导入时将以 MAC 地址作为索引，替换控制中心上对应 MAC 地址的终端的登记信息字段的信息。在导入之前，请确保中心上的【登记信息管理】列表中已创建对应的登记信息字段，否则将导入失败。



(4) 导出：将当前登记的终端信息导出为 xlsx 格式数据表。

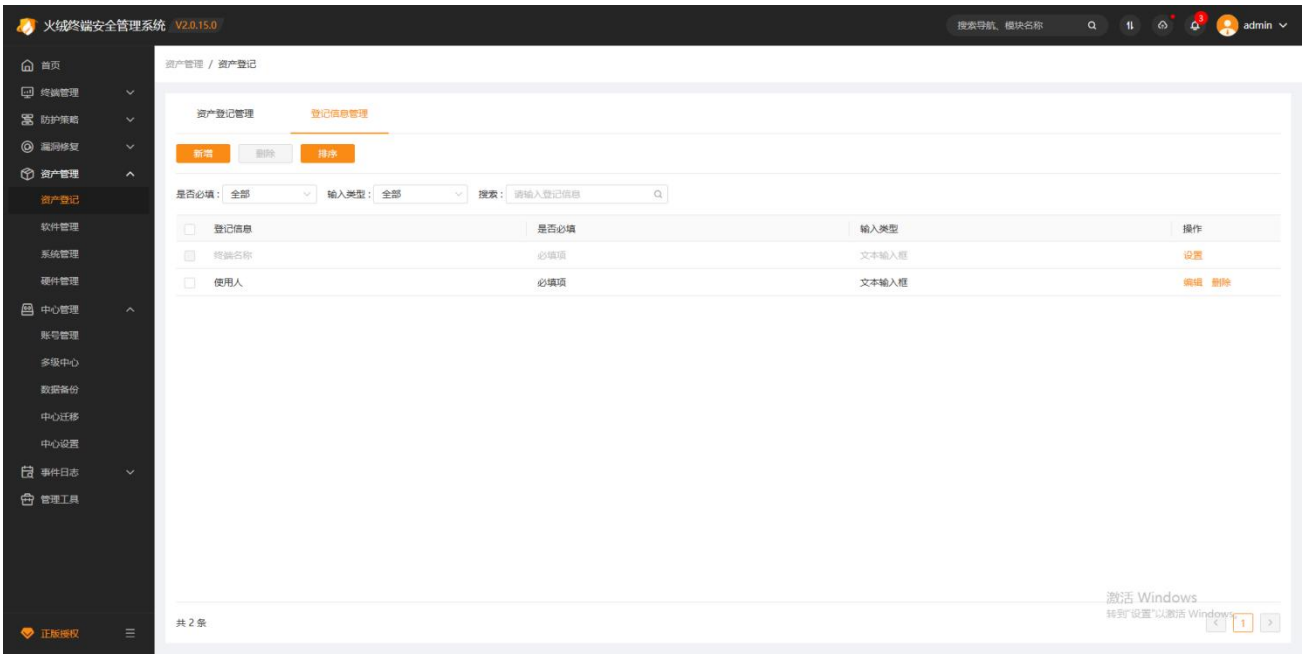
（5） 登记设置：

- 开启终端安装资产登记：开启后，终端需要在安装时进行资产登记，登记后信息将同步至控制中心。
- 开启终端分组登记：只有开启终端安装资产登记后才可以开启，开启后，终端登记信息中将有终端分组登记项，登记后信息将同步至控制中心。
- 终端重新上报资产信息在终端离线（30）天：启用后当终端离线天数为用户设置的天数时，将会在终端弹出终端登记页面，提醒终端用户进行重新登记，用户提交信息后将自动同步到资产登记管理中。
- 开启用户自助登记，配置开启后，终端用户可以在火绒安全终端主面板打开自助登记，根据中心设置的登记项，自助登记上报登记信息。

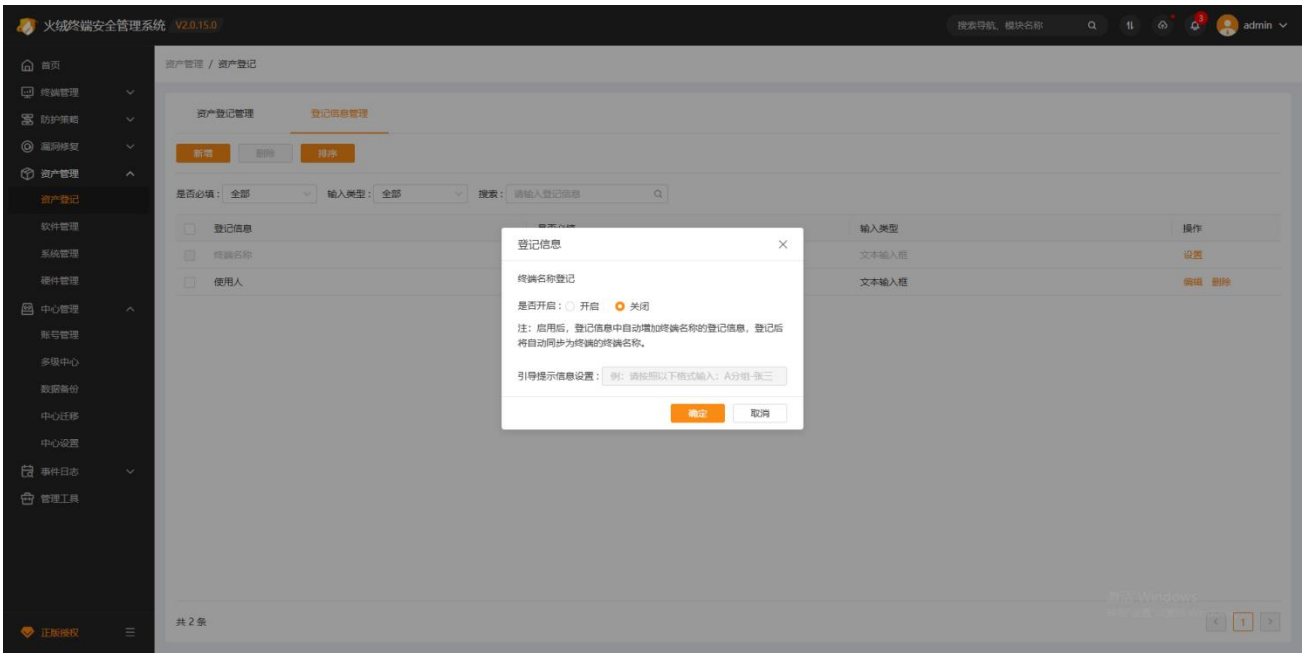


2. 登记信息管理：

用户可在【资产管理】-【登记信息管理】中查看及设置需要登记的信息，默认显示“终端名称”，用户可自定义登记信息项及信息必填项、输入类型，方便用户对登记信息进行统一管理。



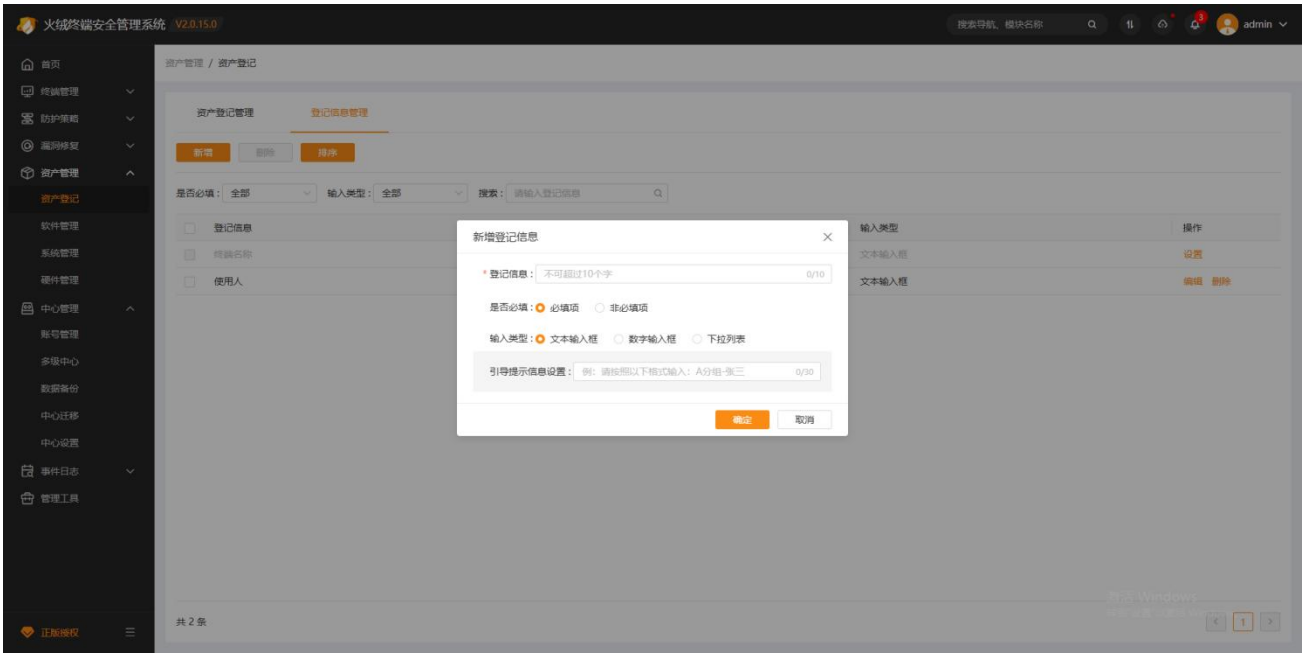
登记信息列默认显示“终端名称”，点击【设置】用户可以去开启终端名称登记并设置引导提示信息；登记后用户填写的终端名称信息将自动同步至中心并将当前终端的终端名称修改为登记上来的信息，此功能可配合分组规则一起使用，实现快速分组。



【排序】：若用户开启了终端名称或终端分组登记，将固定显示不可移动；用户点击【上移】登记项将会上移一格，点击【下移】登记项将会向下移动一格；鼠标左键长按可以拖动登记项进行排序；

- 登记信息：填写此登记信息项的名称。

- 是否必填：选择决定此登记信息项是否要求终端必填或选填。
- 输入类型：当前支持需要用户填写的文本输入框、数字输入框和提供选择项给用户选择的下拉列表三种类型。
- 列表项：当输入类型选择为下拉列表时列表项启用。用于添加下拉列表中的各选项。
- 列表：列表项中点击新增即可添加至列表中。列表汇中展示的是此下拉列表的所有选项。



2.8.2 软件管理

火绒终端安全管理系统支持统计终端软件安装情况，方便用户查看、管理终端已安装的软件，维护企业良好的软件使用环境。

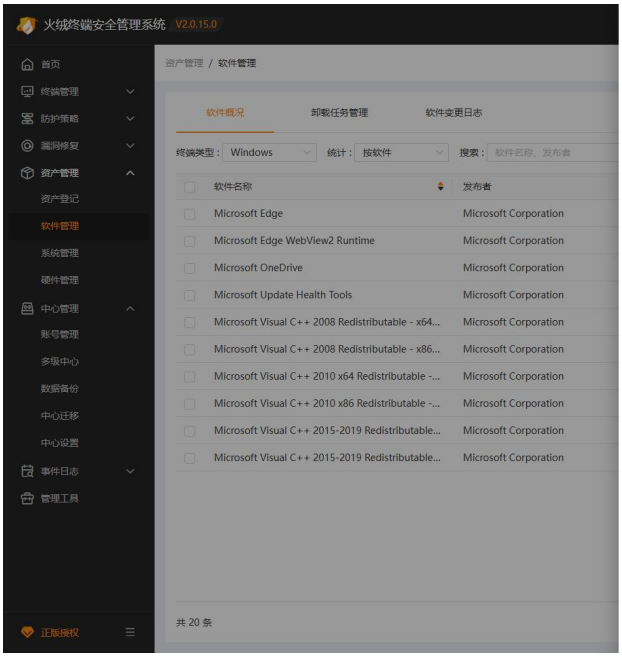
用户可在【资产管理】-【软件管理】界面进行终端软件安装情况的查看与管理，软件管理功能分为软件概况、卸载任务管理以及软件变更日志三个视图，对于不符合企业安全管理要求的软件，用户可下发软件卸载任务至指定终端。

软件安装情况统计分为三个维度，分别是按软件统计、按软件不同版本统计和按终端统计，以不同的统计视角进行分类展示，方便用户准确找到违规软件及安装违规软件的终端，并针对性下发卸载任务。

1. 按软件统计：

按软件视角为用户展示所有终端已安装的软件。不同版本的软件会视为同一软件。

用户可点击“已安装”列表栏下方终端数量查看安装当前软件的终端，如出现不符合企业安全管理要求的软件，用户可点击“操作”列表栏下方【卸载】按钮并选择需要卸载此软件的终端，点击【确定】对当前选中的终端下发卸载任务，可以选择多个软件对多个终端下发卸载任务，卸载软件时能够选择不同的卸载方式，设置不同的卸载配置。



2. 按软件不同版本统计：

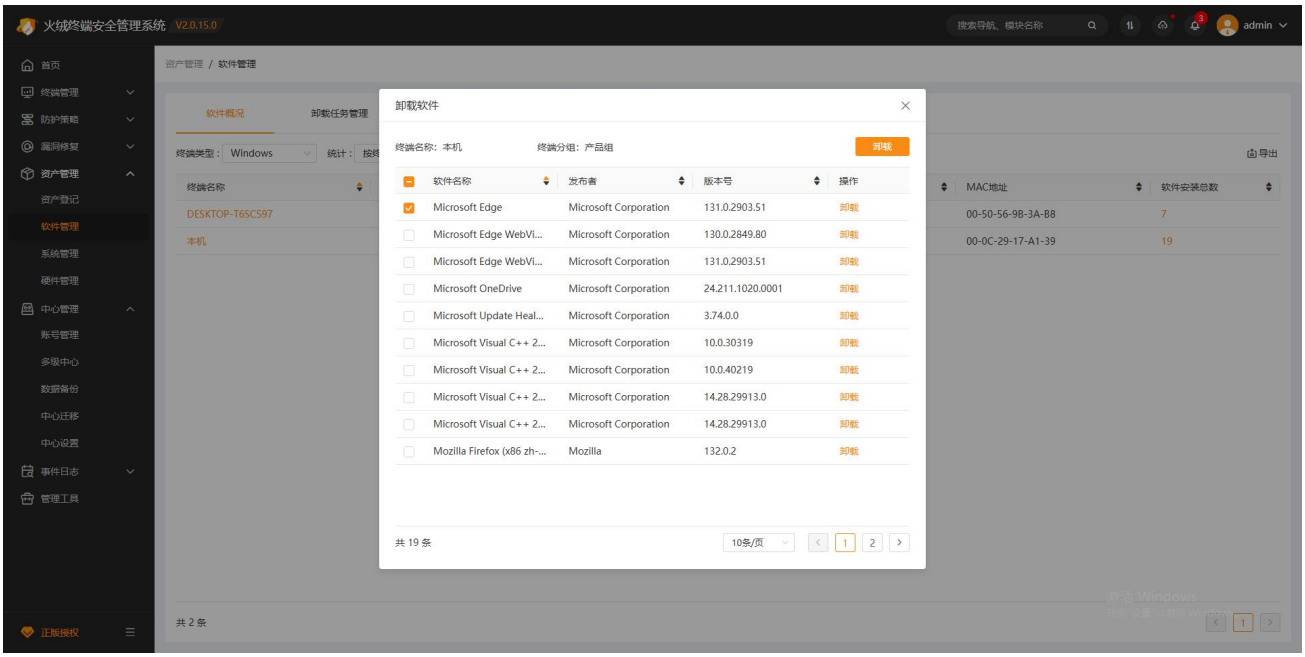
按软件不同版本统计与按软件统计，区别在于，按不同版本统计时，不同版本的软件会视为多个不同的软件，在导出数据时也会区分不同版本，便于管理员对不同版本软件的区分管理。

3. 按终端统计：

按终端视角为用户展示每个终端安装的软件。

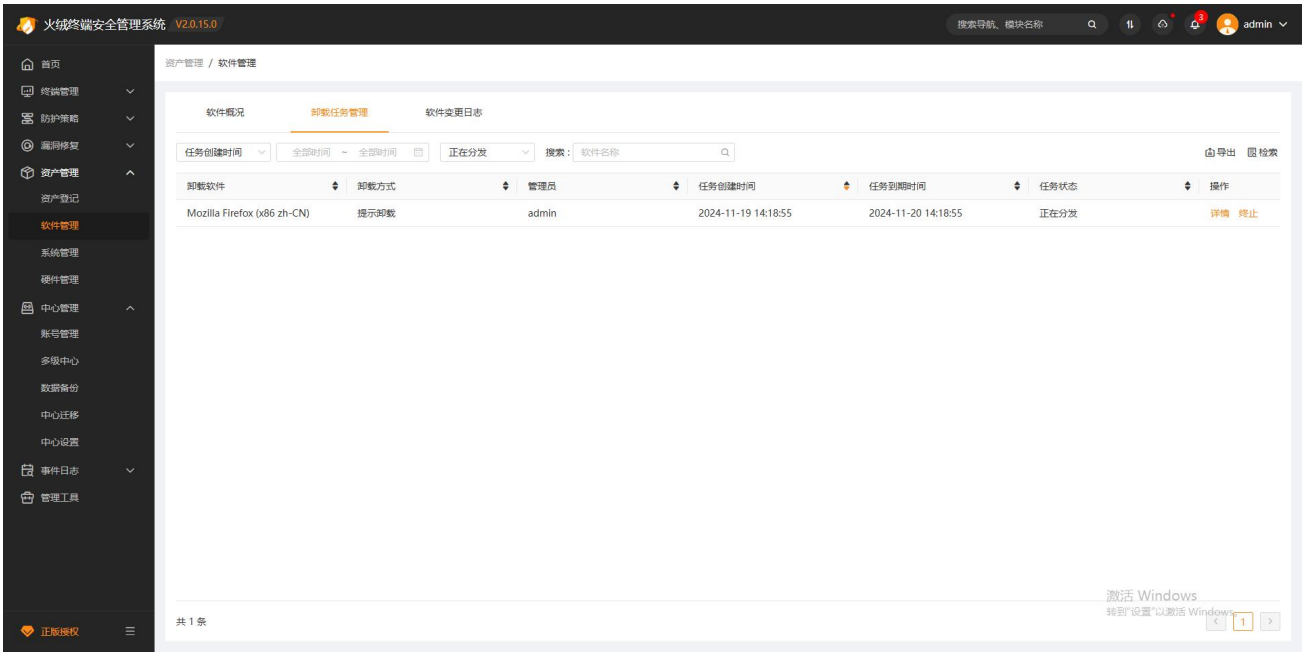
用户可点击“软件安装总数”列表栏下方软件安装数量查看当前终端的软件安装情况，点击“操作”列表栏中的【卸载】按钮即可对当前终端下发软件卸载任务，下发卸载任务时，可以选择多个软件进行卸

载。



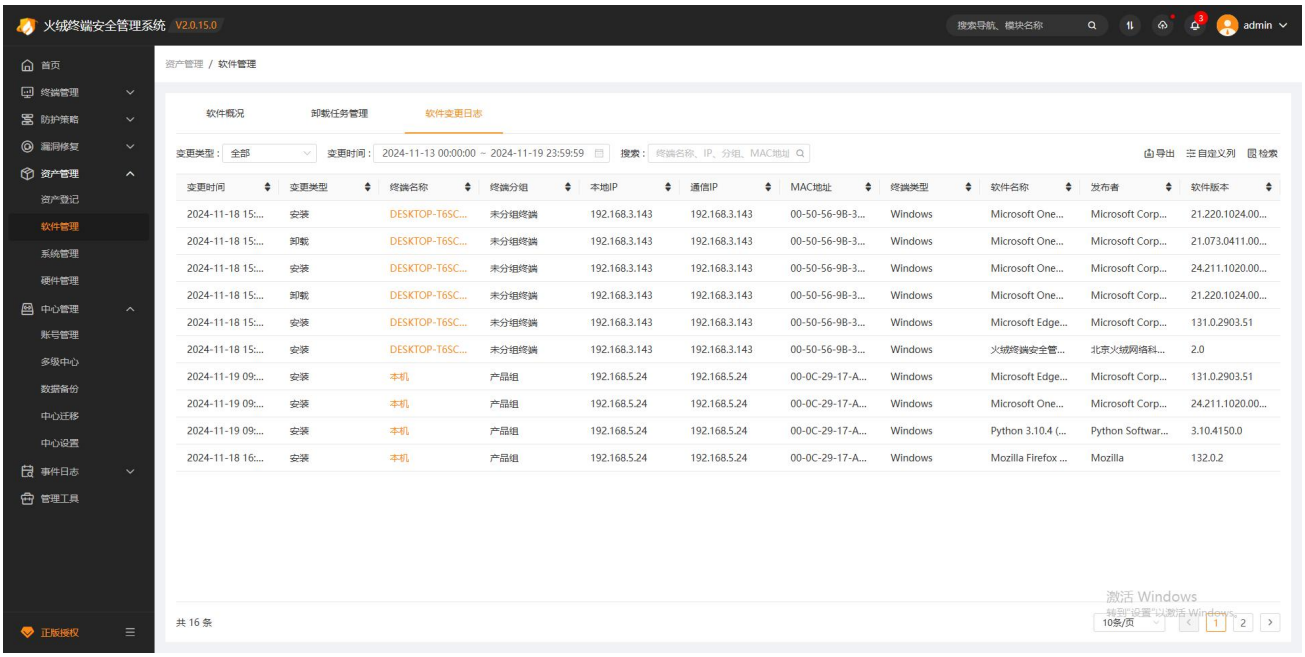
4. 卸载任务管理

卸载任务管理页面可以查看、管理下发的卸载任务，能够根据任务创建时间、到期时间筛选、查找卸载任务，可以导出卸载任务数据，查看卸载任务详情，终止卸载任务（任务处于有效期内且卸载任务并未完成）。



5. 软件变更日志

软件变更日志能够查看中心所有终端软件的变化情况，分为安装行为和卸载行为，能够根据终端软件变更类型及变更时间进行筛选和查找，支持导出终端软件变更的数据。

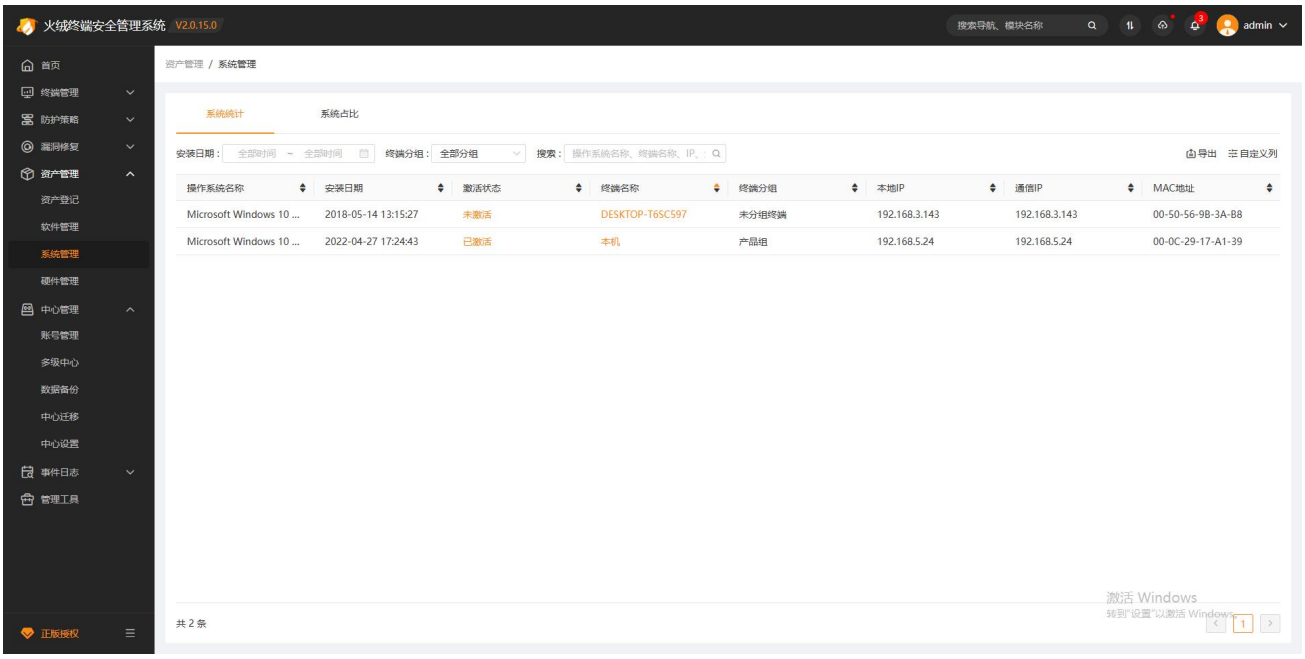


2.8.3 系统管理

火绒终端安全管理系统支持统计终端操作系统信息，方便用户查看和管理企业内终端系统环境。

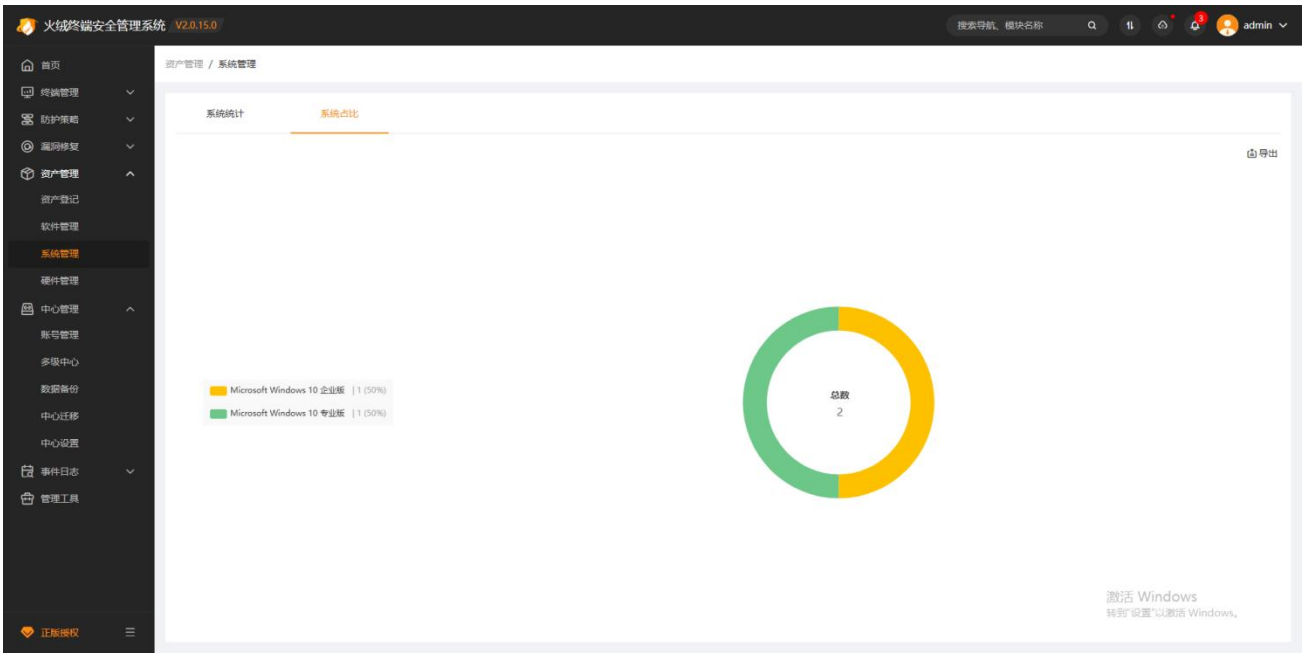
1. 系统统计：

用户可在【资产管理】-【系统管理】-【系统统计】界面查看当前所有终端的操作系统情况。



2. 系统占比：

用户可在【资产管理】-【系统管理】-【系统占比】界面查看当前所有终端的操作系统占比。

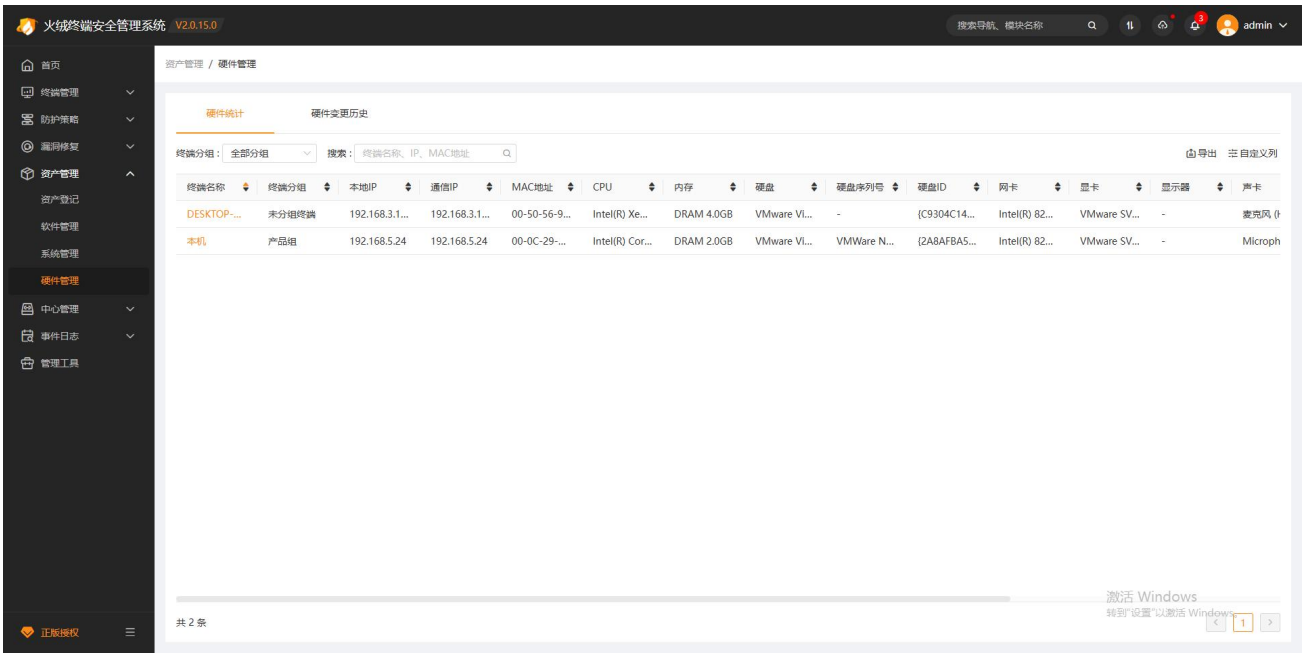


2.8.4 硬件管理

火绒终端安全管理系统支持统计终端硬件信息，方便用户对企业内终端硬件进行查看和管理。

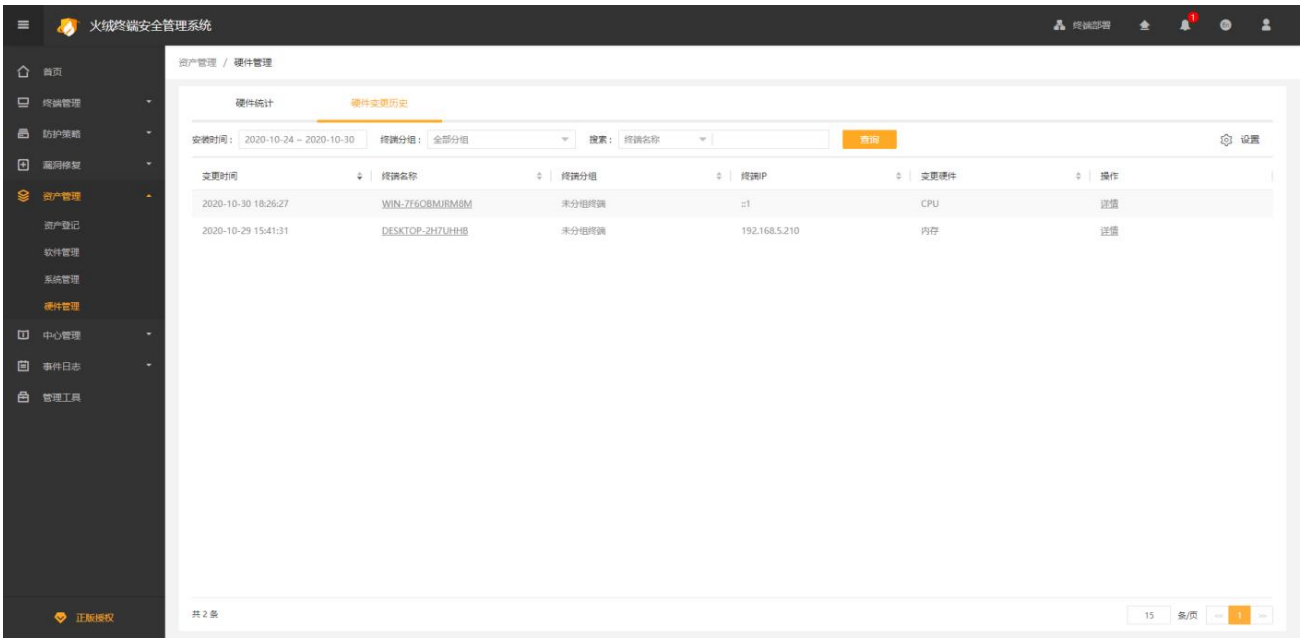
1. 硬件统计：

用户可在【资产管理】-【硬件管理】-【硬件统计】界面查看当前所有终端的硬件信息，支持导出为xlsx 格式表格。



2. 硬件变更历史：

用户可在【资产管理】-【硬件管理】-【硬件变更历史】界面查看当前所有终端的硬件变更记录，方便用户运维及管理企业内硬件变更情况。



点击硬件变更历史中的详情按钮弹出硬件变更详情。硬件变更详情中将会高亮显示变更的硬件信息。


硬件变更详情

终端名称：WIN-7F6OBMJRM8M　　终端分组：未分组终端

变更时间：2020-10-30 18:26:27　　变更硬件：CPU

硬件名称	变更前硬件信息	变更后硬件信息
cpu	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz
	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz
	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	-
	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	-
内存	DRAM 2.0GB	DRAM 2.0GB
硬盘	VMware, VMware Virtual S SCSI Disk Device 6...	VMware, VMware Virtual S SCSI Disk Device 6...
网卡	Intel(R) 82574L 千兆网络连接	Intel(R) 82574L 千兆网络连接
显卡	VMware SVGA 3D	VMware SVGA 3D
主板	Intel Corporation 440BX Desktop Reference Pl...	Intel Corporation 440BX Desktop Reference Pl...

2.9 中心管理

中心管理功能模块仅提供给超级管理员，不能将显示操作权限下发至下级管理员。中心管理模块中为超级管理员提供对中心所有管理员账号的管理，多级中心的配置，中心数据的备份与恢复，中心各项功能的设置调整等功能，方便用户对管理中心的管理及控制。

2.9.1 账号管理

用户可在【中心管理】-【账号管理】界面查看当前中心所有账号信息，并且提供新建账号以及编辑、删除、启用、停用已创建的账号功能。并且支持设置账号自动登出时间、登录时增加动态认证防护以及定期修改密码周期。

1. 新增

用户可点击【新增】按钮创建新的账号：

(1) 账号类型：有普通管理员与审计员两种类型。普通管理员可自定义设置分组权限和模块权限，审计员不可自定义设置分组权限和模块权限，默认具有全部分组权限和事件日志模块权限。

(2) 账号：账号名称，支持中英文，必填项。

(3) 密码：输入管理员密码，密码必须由 8-32 位大小写字母、数字、特殊字符组成，必填项。

(4) 生成强密码：点击在密码输入框中生成包含大小英文、数字与特殊字符组成的随机强密码。

(5) 确认密码：再次输入管理员密码，必填项。

(6) 下次登录：该配置为一次性配置，默认勾选。勾选后对应账号在下次登录时需修改密码，修改密码后才可登录成功进入首页，且后台自动取消该选项的勾选状态。

(7) 联系方式：管理员的联系方式，选填项。

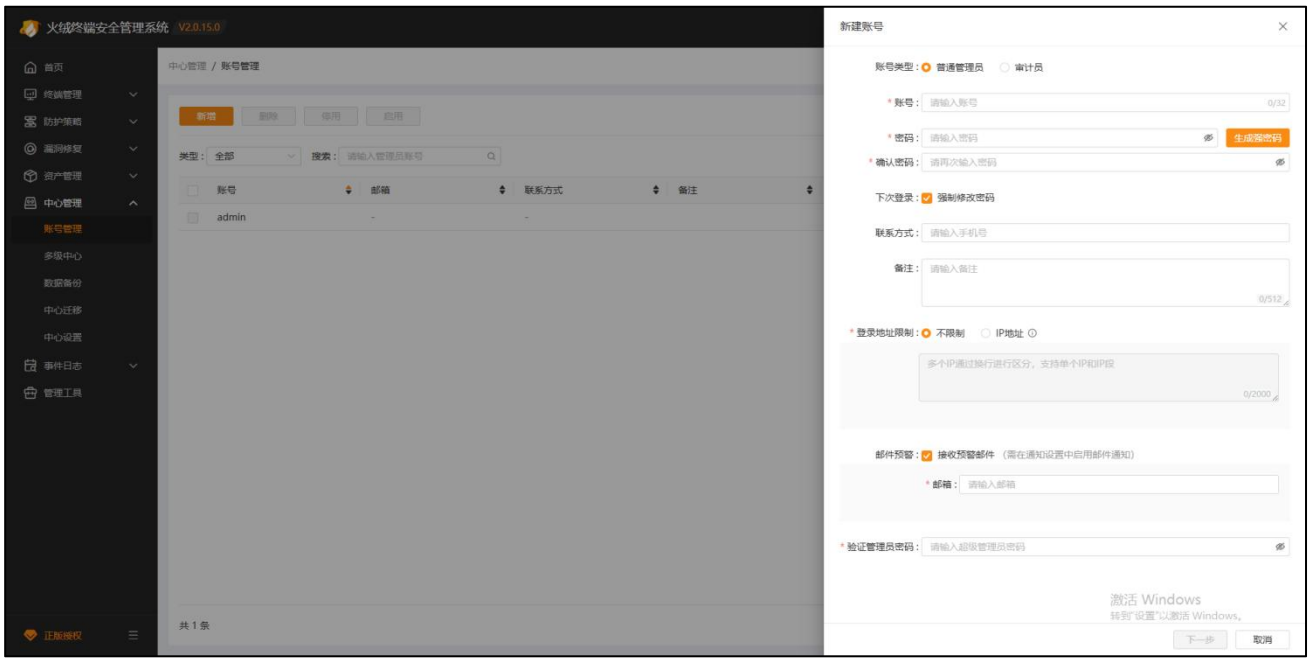
(8) 备注：管理员的信息，选填项。

(9) 登录地址限制：默认选中【不限制】，则该账号可在任意 IP 地址的电脑上登录控制中心。选中【IP 地址】时，需填写 IP 地址，配置后则该账号只能在设置的 IP 地址的电脑上登录控制中心。

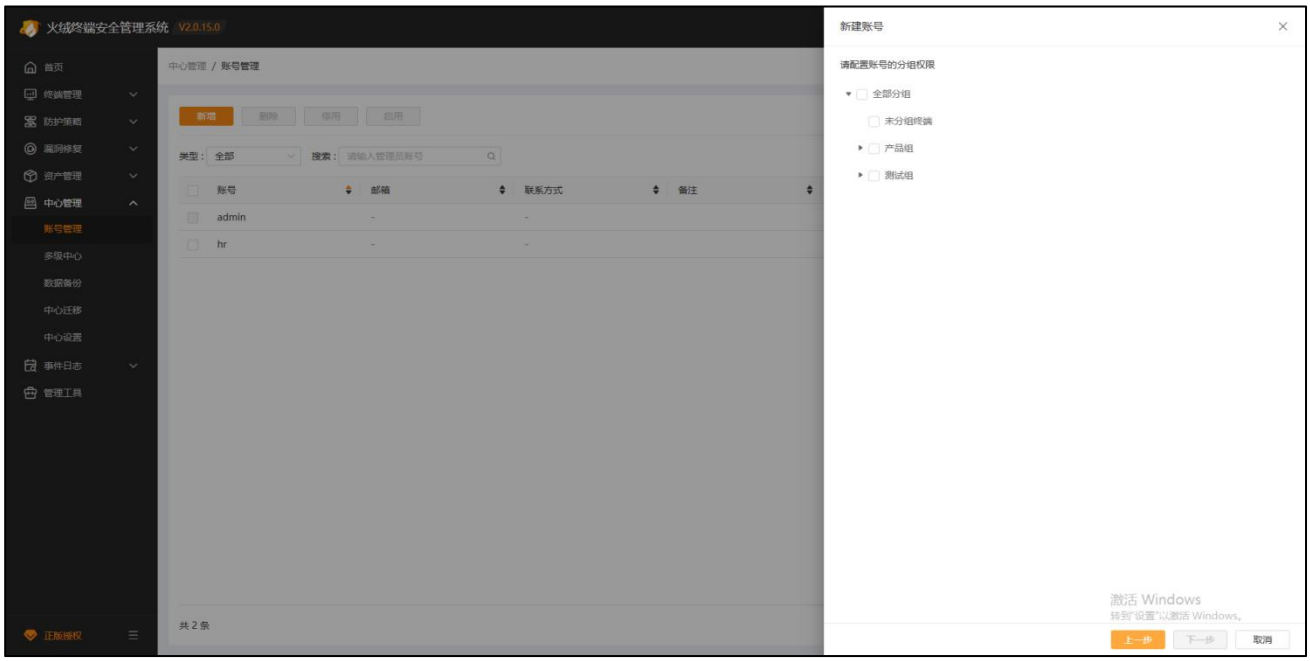
(10) 邮件预警：勾选后当该管理员所管理终端触发告警邮件时，将会发送告警邮件给此管理员。

(11) 邮箱：勾选邮件预警后，此项为必填项，填写接受告警邮件的邮箱地址；若未勾选邮件预警，则此项为选填项。

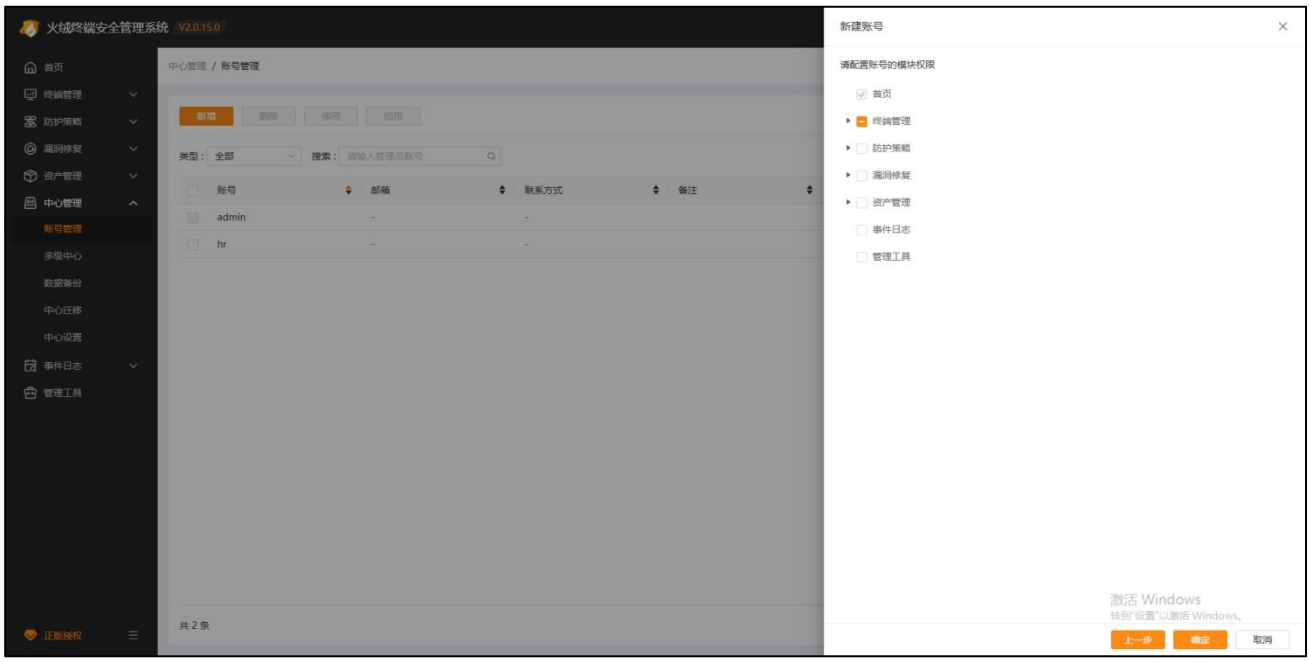
(12) 验证管理员密码：需输入超级管理员密码以验证操作安全性，必填项。



普通管理员类型的账号基本信息填写完成后，点击【下一步】进入分组权限设置，选择当前管理员可管理的分组范围（包括数据访问权限）；审计员类型的账号基本信息填写完成后，点击【确定】，则账号设置成功。

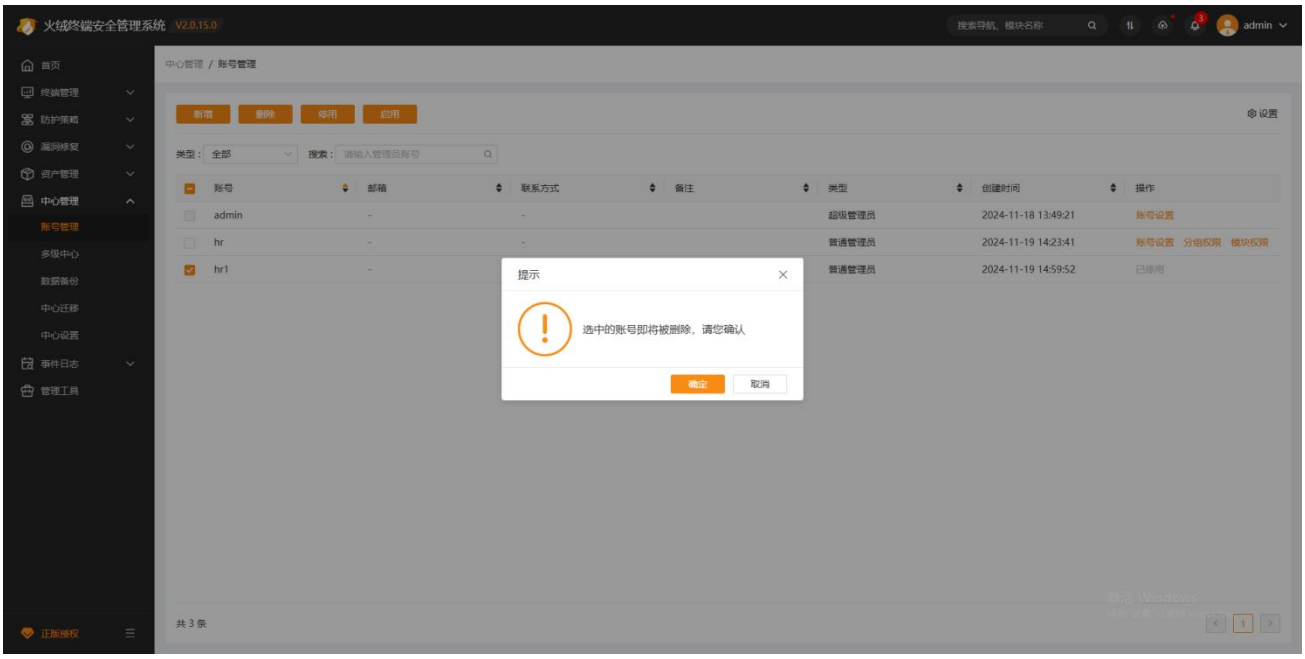


分组权限选择完成后点击【下一步】进入模块权限设置，选择当前管理员可管理的功能模块范围，细化管理员管理权限，点击确定即可成功创建普通管理员账号。



2. 删除

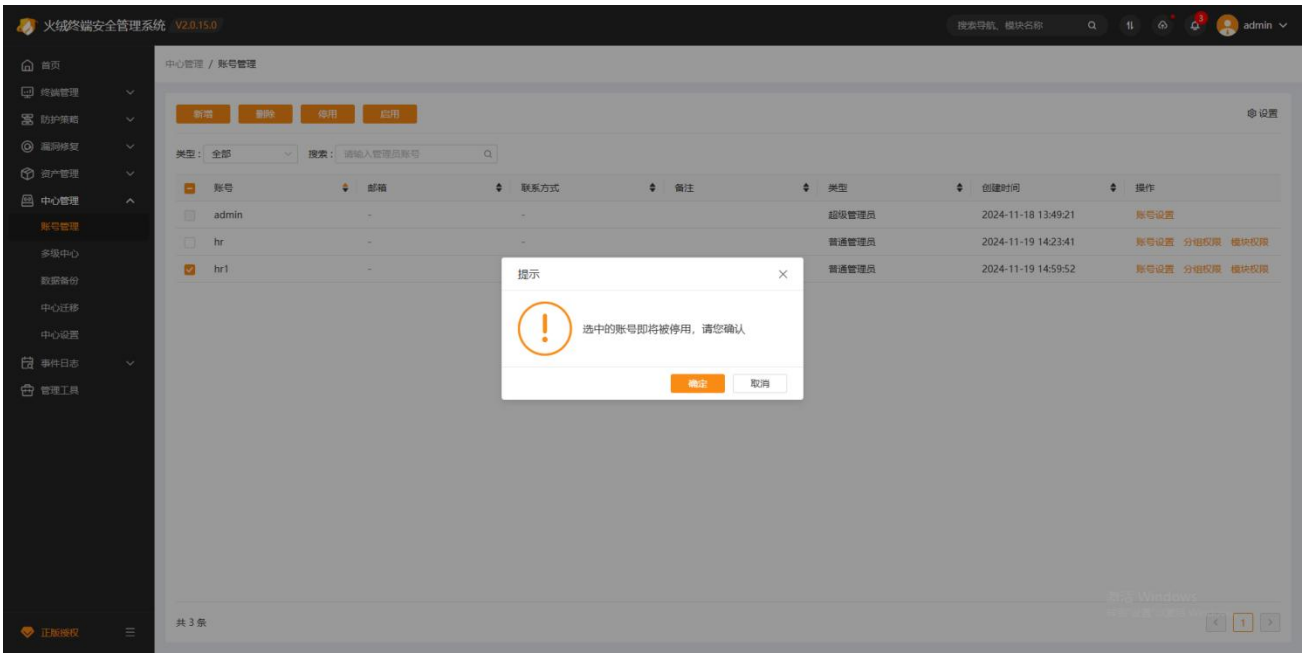
用户可选中已停用管理员账号（未停用的管理员账号不允许删除），点击【删除】按钮对已停用的账号进行删除操作。



3. 停用

用户可选中已启用的管理员账号，点击【停用】按钮，在弹出警告框中点击【确定】后即可对当前管

理员账号进行停用，停用的管理员账号不允许登录中心。

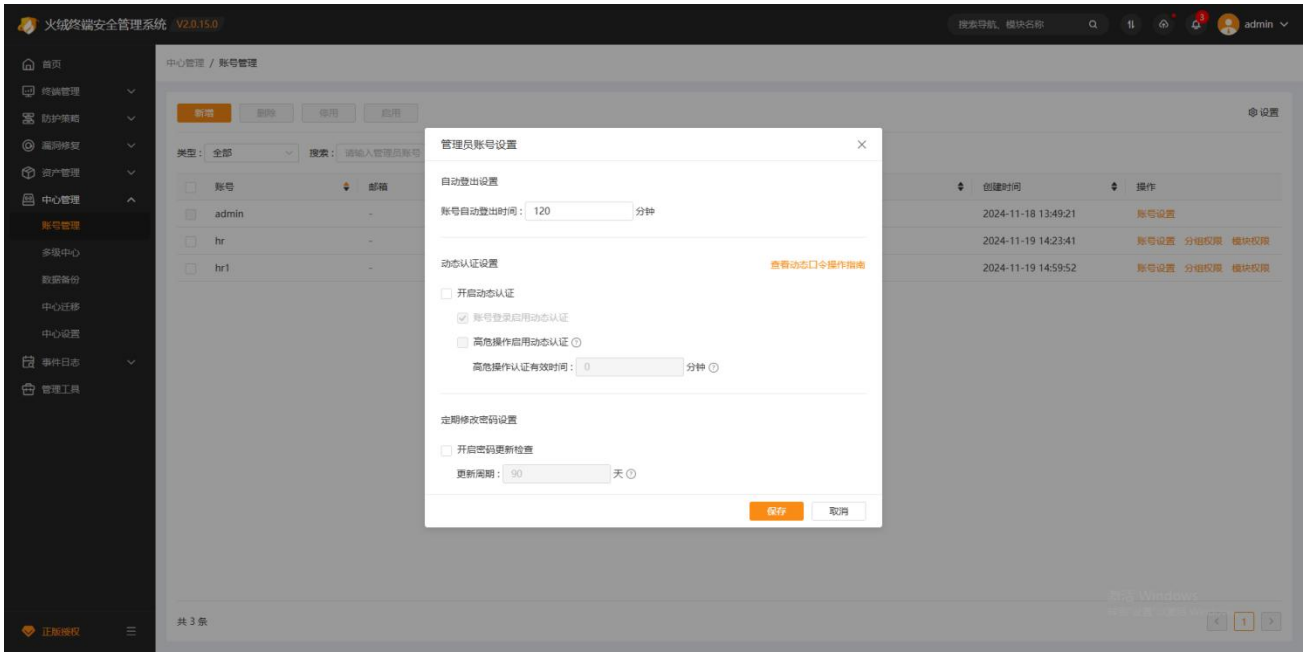


4. 启用

用户可选中已停用的管理员账号，点击【启用】按钮对当前管理员账号进行启用，启用后此管理员账号恢复正常使用状态。

5. 设置

用户可点击账号管理右侧的【设置】按钮弹出管理员账号设置。



（1） 自动登出设置：设置管理员中心无操作后自动登出的时间，默认为 5 分钟。输入范围 5~120 分钟。

（2） 动态认证设置：默认不开启，勾选开启动态认证后下方复选框与输入框启用。

- 账号登录启用动态认证：各类管理员登录时将需进行动态认证。此项默认勾选且无法取消勾选。
- 高危操作启用动态认证：勾选后执行远程桌面、添加信任文件、文件分发操作时需要再次进行动态认证，超级管理员不受高危操作的限制。
- 高危操作认证有效时间：在动态认证成功后的有效时间内，执行高危操作无需再次进行动态认证。设为 0 分钟时，则每次操作均需动态认证。默认设置为 0 分钟。输入范围 0~120 分钟。
- 查看动态口令操作指南：点击打开动态口令使用指南页面。

（3） 定期修改密码设置：设置管理员账户密码的检查更新周期，设置开启后，管理员密码一旦超过设定时间未修改，登录时将自动进入修改密码界面。

6. 其他

用户可对已启用的账号进行账号设置（包括密码重置、登录地址限制、修改邮箱、联系方式、备注等信息），以及对普通管理员账号重新设置分组权限和模块权限。

2.9.2 多级中心

火绒终端安全管理系统支持，多级中心支持管理员通过上级控制中心管理下级控制中心，可帮助管理员实现多级管理的需求，缓解单控制中心升级、打补丁压力，解决下属单位异地联动、多部门安全管理协同等管理难题。

注：上级中心与下级中心必须能够互相访问，否则无法配置多级中心。

1. 配置上级中心

用户可点击界面右侧【配置上级中心】按钮，弹出上级中心配置弹窗界面：

（1） 连接上级控制中心：用于控制是否连接上级中心，开启后下方输入框与勾选项才可启用。

（2） 上级控制中心地址：输入需要连接的上级控制中心地址。

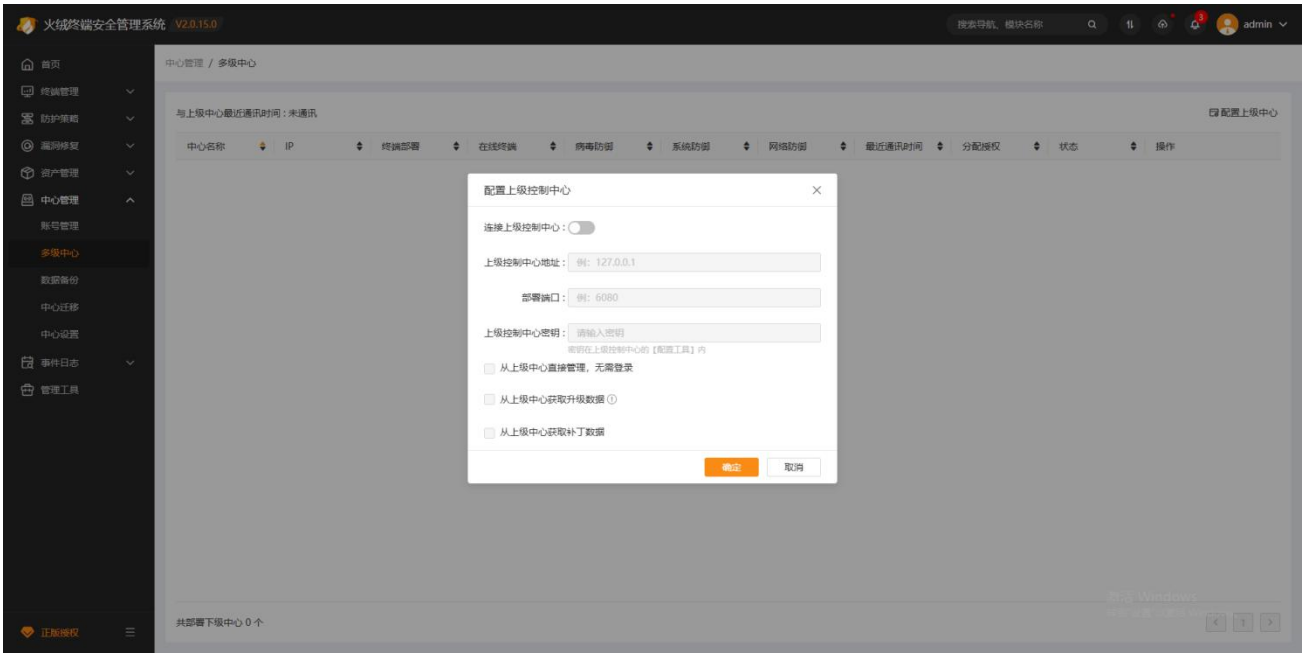
（3） 部署端口：填写当前终端部署端口（与配置工具中的终端部署端口一致即可）。

（4） 上级控制中心密钥：填写上级控制中心中配置工具里的中心密钥。

（5） 仅从上级中心直接管理，无需登录：勾选后，上级控制中心可直接访问下级控制中心。

（6） 仅从上级中心获取升级数据：勾选后，下级控制中心将从上级控制中心获取升级数据。

（7） 仅从上级中心获取补丁数据：勾选后，下级控制中心将从上级控制中心获取补丁数据。



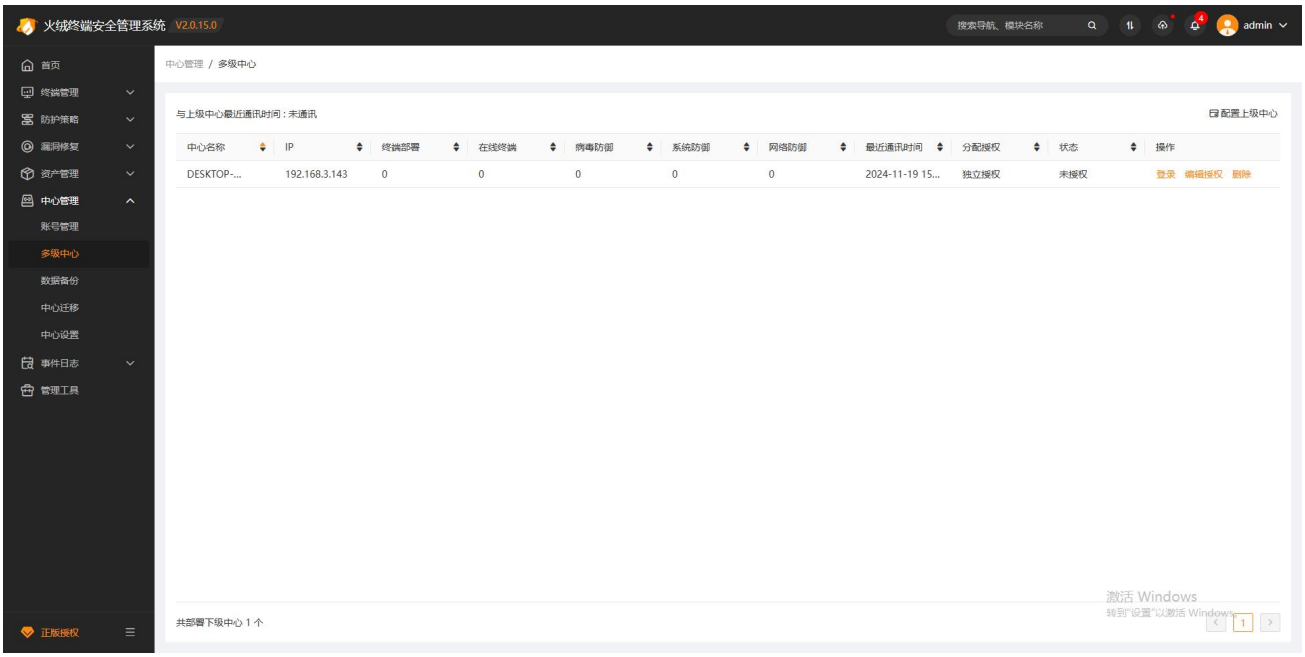
配置好上级控制中心后，点击确定按钮即可保存并连接上级控制中心。当成功连接后，上级控制中心的多级中心列表中就会显示出已连接的下级控制中心。

2. 登录

若下级控制中心在配置中已勾选“仅从上级中心直接管理、无需登录”选项，则上级中心管理员可直

接登入下级控制中心。

用户点击下级中心操作栏中的【登录】按钮，即可直接登录至下级中心。



3. 编辑授权

用户点击下级中心操作栏中的【编辑授权】按钮，可对当前中心进行授权分配管理当前授权方式分为三种：独立授权、动态分配、自定义分配。

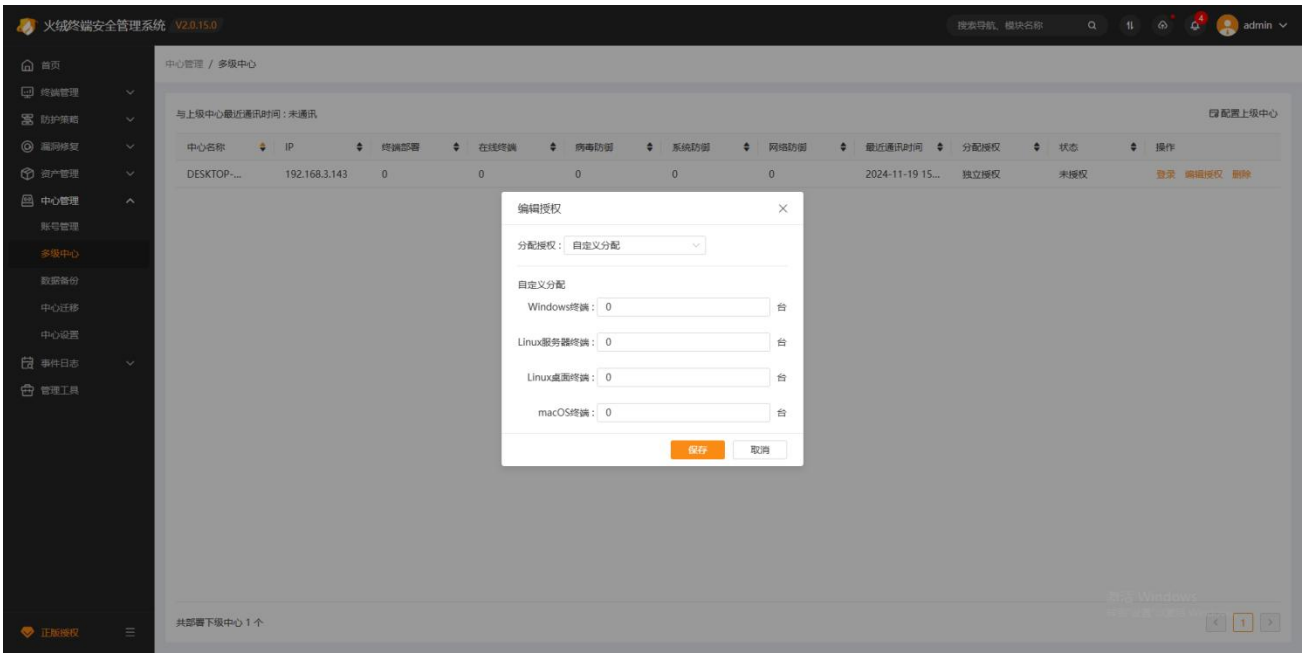
（1） 独立授权：下级控制中心连入后默认均为独立授权，独立授权时下级控制中心使用自己的授权，与上级控制中心的授权互无关联。

（2） 动态分配：下级控制中心根据自己需要向上级控制中心索取授权，使用上级控制中心的授权。但不可超过上级控制中心授权的总终端台数。

注：动态分配时，下级控制中心获得授权点数后将会持续占用，即使有终端下线，授权点数并不会因此减少。当上线的终端数超过授权点数后下级控制中心会继续向上级控制中心索取授权。因此动态分配是一个只能增加但不会减少的授权获取方式。

（3） 自定义分配：选择此项后，下方自定义分配输入框启用。手动输入需要分配给下级控制中心

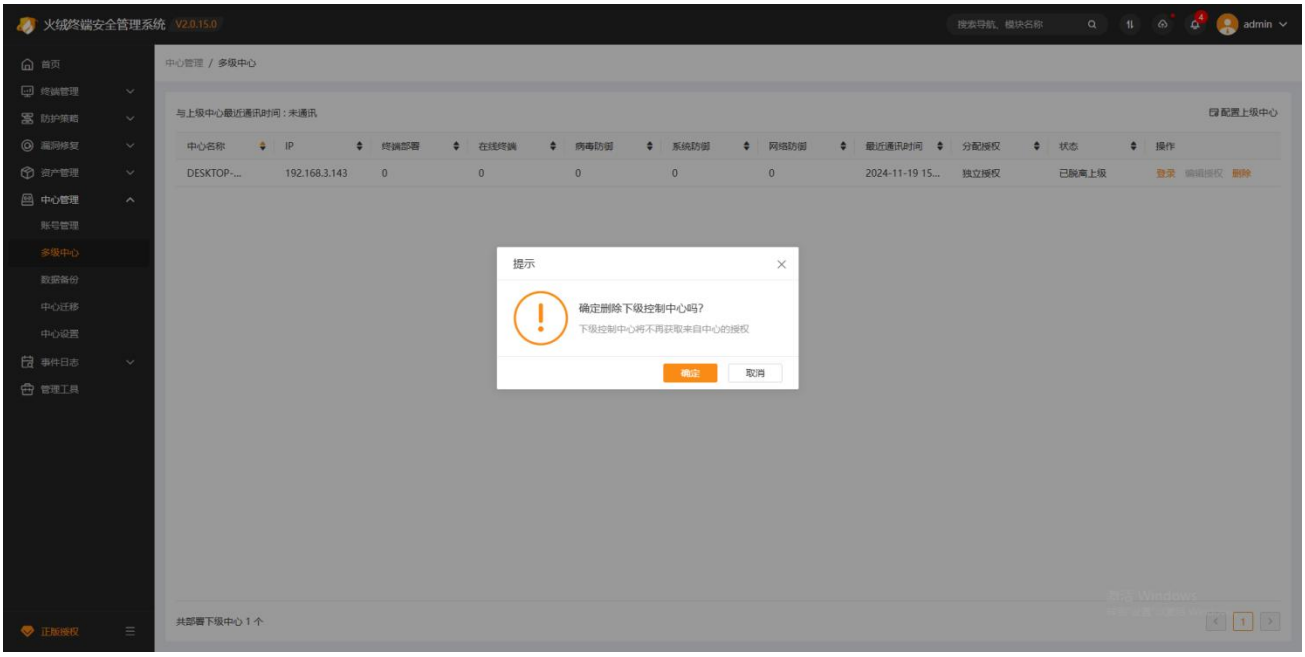
的授权台数。



4. 删除

用户可点击下级控制中心操作列的【删除】按钮弹出确认删除的提示弹窗。点击确定即可删除此下级控制中心。

注：删除的下级控制中心前，请先在下级控制中心的“配置上级控制中心”弹窗中关闭与上级控制中心的连接。

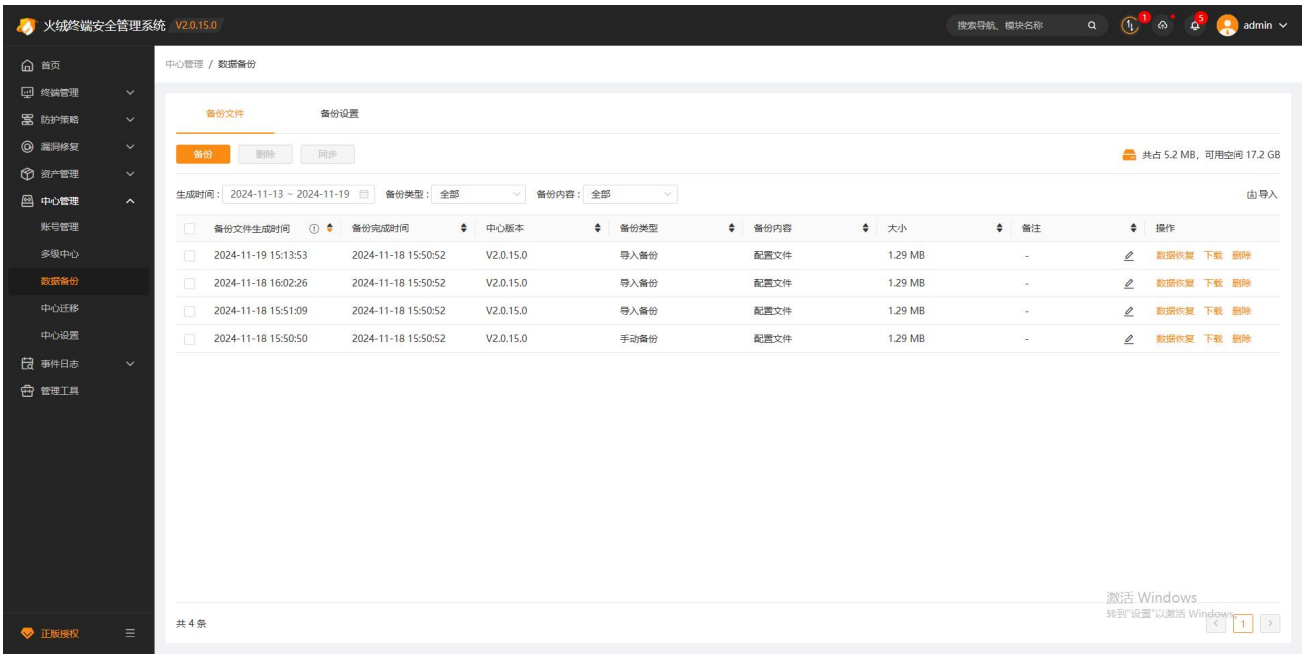


2.9.3 数据备份

火绒终端安全管理系统提供系统数据备份功能，可帮助用户因出现操作失误或系统故障导致中心数据丢失后找回历史数据，用户可以手动或设置系统自动备份，备份中心的配置数据及日志数据，还可以将备份数据同步至共享地址或 FTP 服务器。

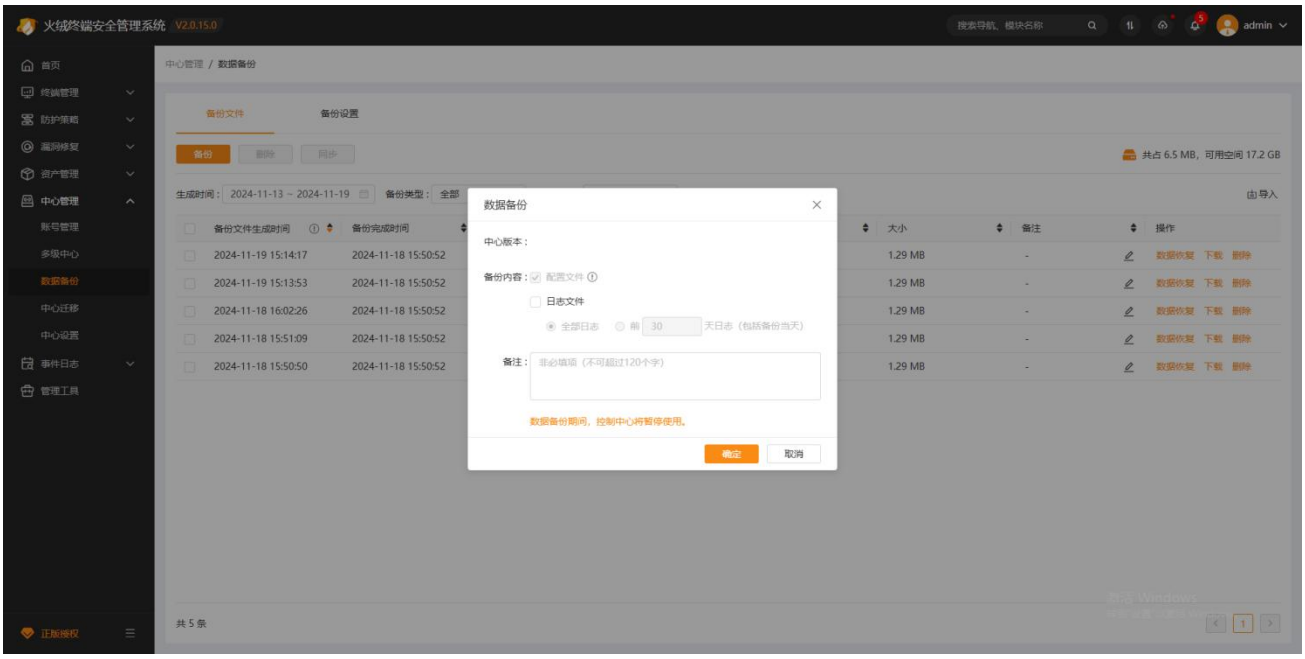
数据备份作为容灾的必要功能，方便用户管理及维护系统数据。

数据备份模块分为备份文件和备份设置两个页面，备份文件页面显示备份文件列表，提示当前备份文件所占空间及剩余可用空间，支持根据文件生成时间（指创建备份文件时间或备份文件导入的时间）、备份类型和备份内容筛选备份文件，支持导入备份文件。



1. 手动备份文件

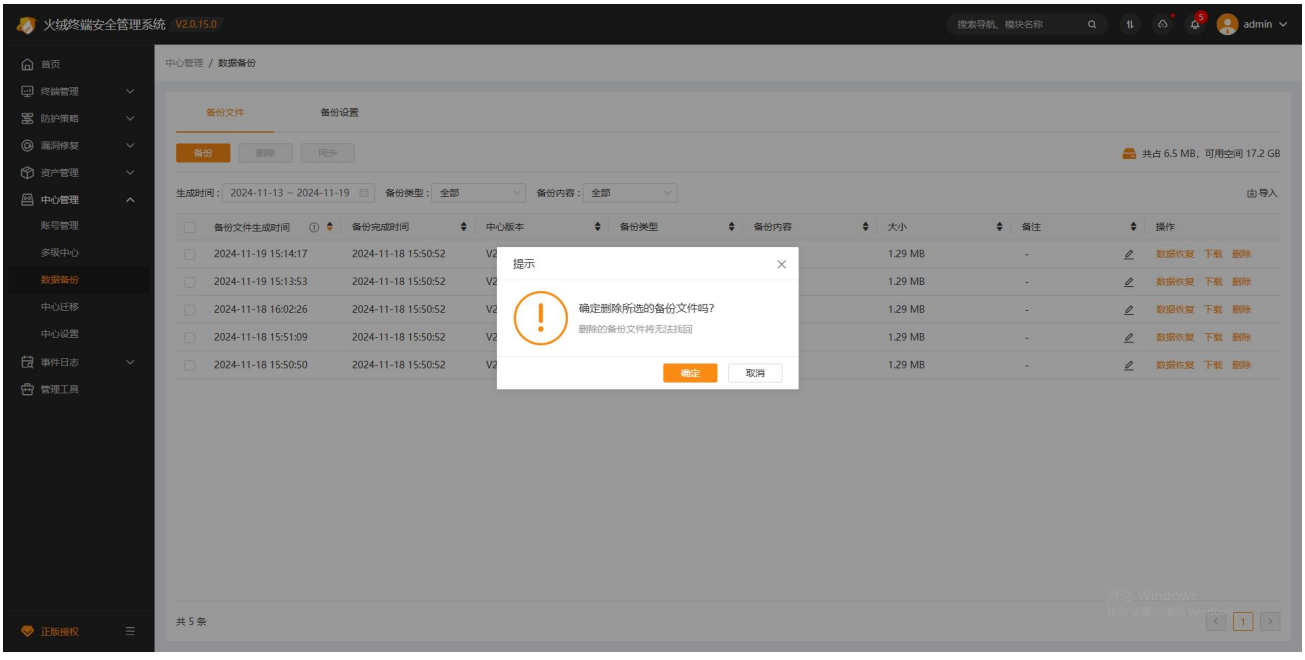
点击【备份】按钮，显示手动备份文件弹窗，窗口会显示当前中心的版本信息，配置文件是必须备份的内容，若不备份配置文件，日志文件无法正确显示，备份日志可以选择时间，默认备份前 30 天的日志，还可以填写备注，用于辅助记忆和识别备份文件，设置完成后，点击【确定】按钮，即开始备份，需要注意的是，数据备份期间，控制中心将暂停使用。



备份完成后，备份文件将显示在列表中，可以使用备份文件恢复中心数据，也可以删除和下载备份文件。

2. 删除备份文件

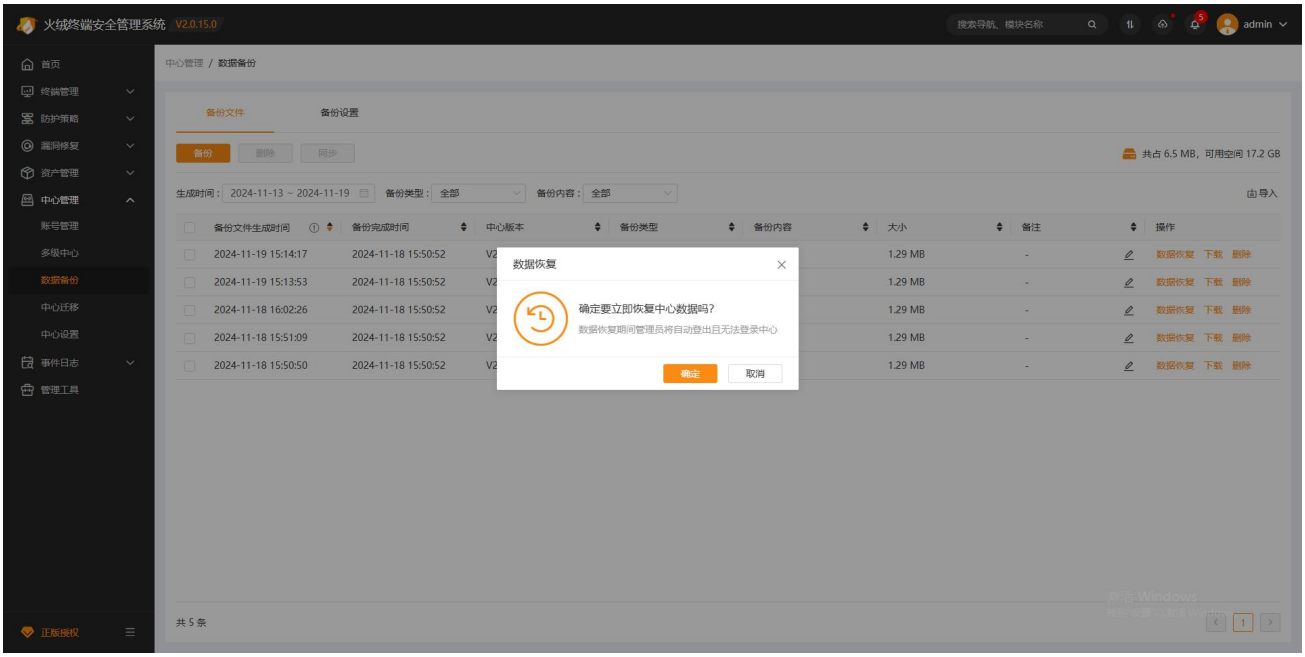
用户可以点击备份文件操作列【删除】按钮，删除备份文件，在确认窗口中，点击【确定】即删除备份文件；还可以选择多个文件后点击列表上方【删除】按钮，删除所选文件，在确认窗口中点击【确定】即删除所选备份文件。



3. 数据恢复

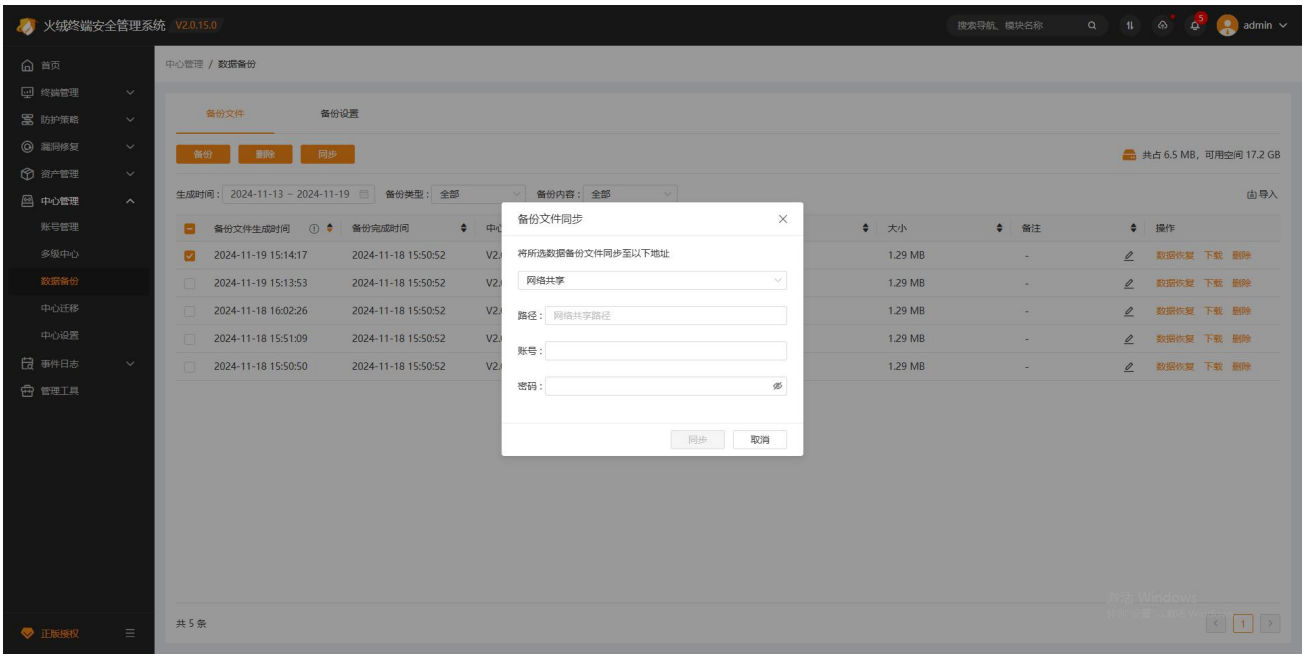
点击任意备份所在行操作列的【立即恢复】按钮，弹出立即恢复的确认弹窗，点击【确定】后将执行备份恢复。

当恢复备份的内容包含配置文件时（即备份内容类型为全部内容或配置文件），恢复备份时控制中心将需要短暂的暂停。因此会将所有管理员登出，当控制中心配置文件恢复完成后即可再次登入控制中心。



4. 手动同步备份文件

选择备份文件后，点击同步按钮，显示同步备份文件窗口，支持将备份文件同步至网络共享路径或 FTP 服务器，须填写网络共享路径、账号或服务器地址、账号，密码为选填，填写完成后点击【同步】按钮，将所选备份文件同步至目标地址。

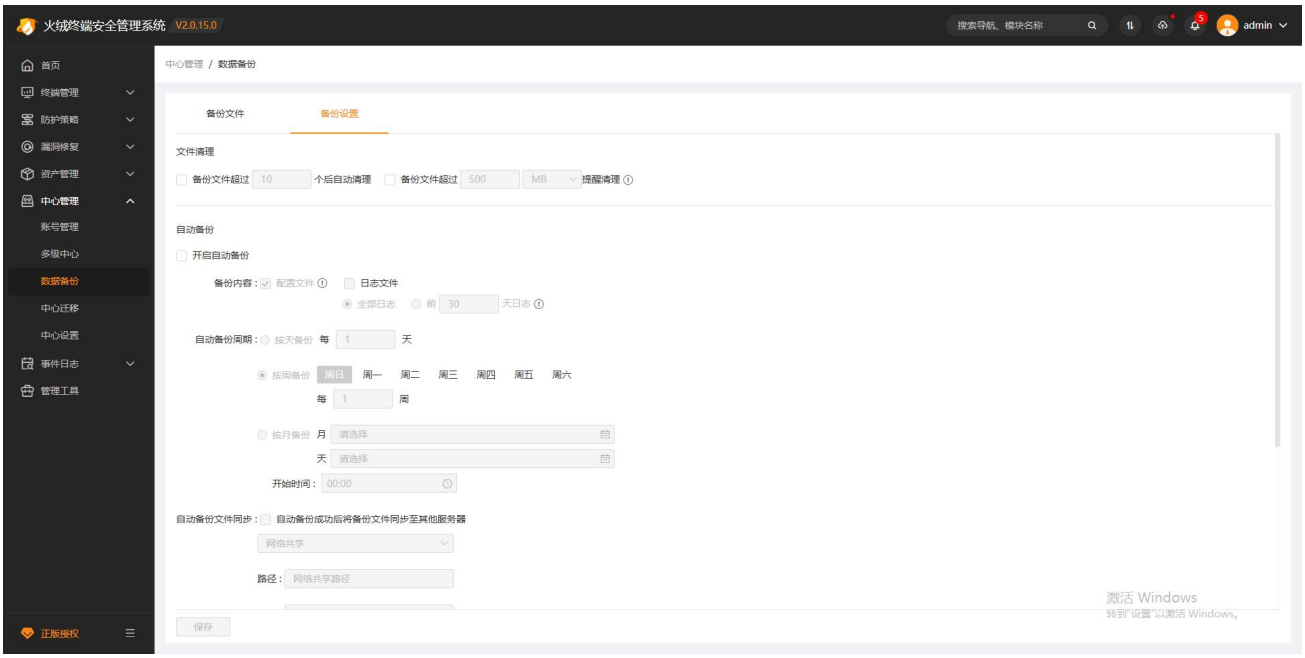


5. 备份设置

用户可以设置备份文件超过一定数量后自动清理，或备份文件占用空间超过一定大小后，在通知中心显示消息通知，提醒清理；

还可以设置自动进行控制中心的数据备份，自动备份时机可以设置每天、每周、每月，备份内容与手动备份一致，配置文件必选，日志文件可选；可以设置备份文件是否自动同步，同步设置与手动同步一致；

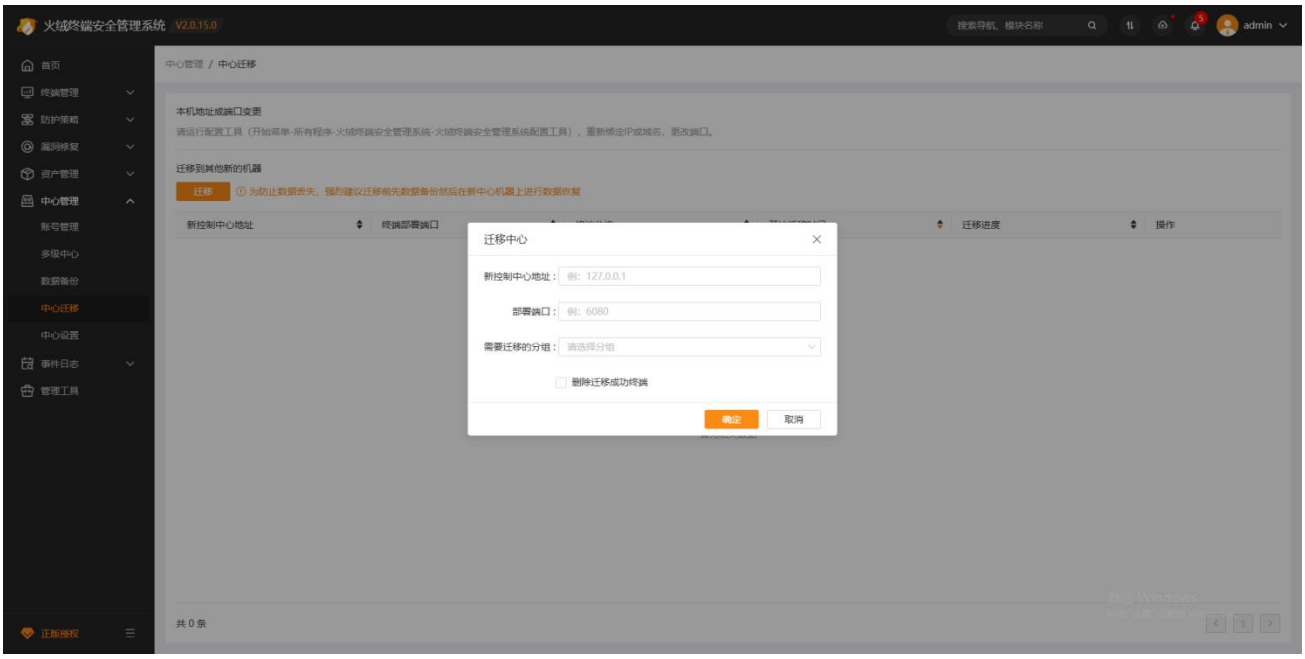
可以设置备份文件或同步数据出现异常情况时的处理方式，如自动备份时其他备份任务正在执行，可以选择等正在执行任务完毕后继续备份，还是取消本次自动备份并记录日志，以及自动备份失败或自动备份文件同步失败是否进行重新尝试。



2.9.4 中心迁移

火绒终端安全管理系统提供中心迁移功能，当中心进行更换域名或 IP 时，或需要将部分终端迁移至其他中心时可以使用中心迁移功能。中心迁移功能可以将当前控制中心中的部分或全部终端迁移至其他中心。

点击【迁移】按钮弹出迁移中心弹窗。填写迁移的新控制中心地址，并选择需要迁移的分组，同时可通过选中弹窗底部的删除迁移成功终端选项，删除已经迁移成功的终端。点击确定，即可创建迁移任务。迁移任务将在中心迁移列表中显示。



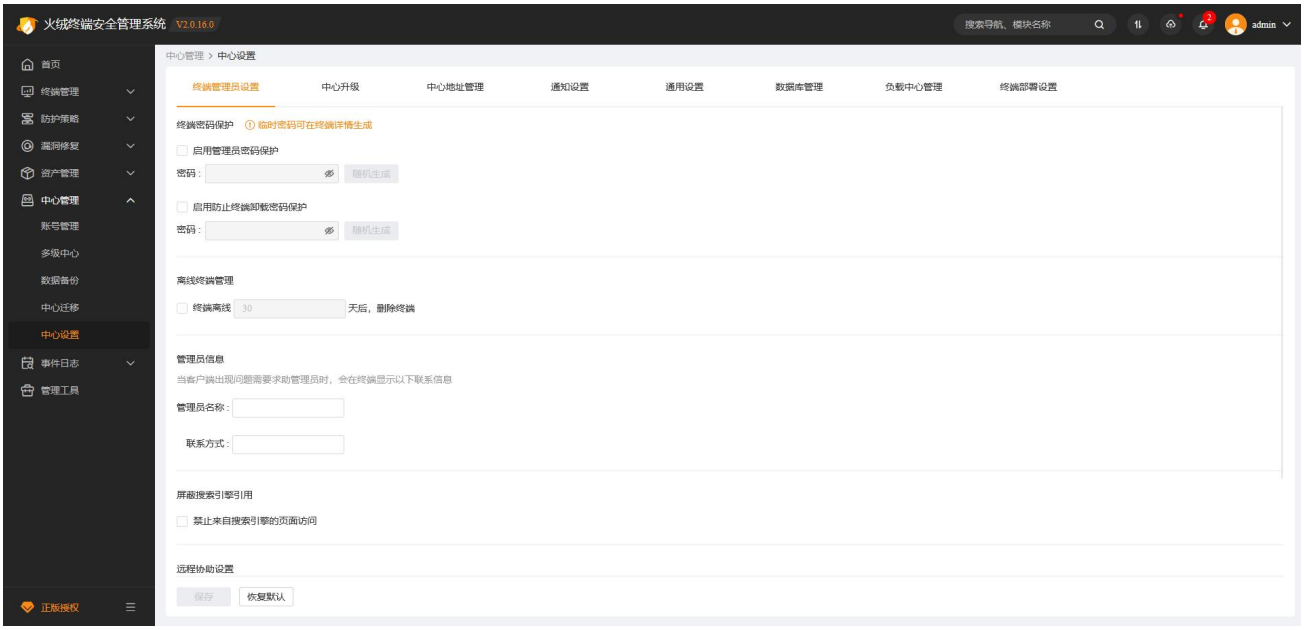
用户点击迁移任务后方的【查看详情】按钮，将弹出中心迁移详情弹窗。为管理员展示当前迁移任务中各终端的迁移状态。

用户点击未结束的迁移任务后方的【终止任务】按钮将弹出终止任务的确认提示弹窗。点击【确定】即可终止迁移任务，但仅对未完成迁移的终端有效。

2.9.5 中心设置

火绒终端安全管理系统提供如远程桌面应答时间、中心心跳间隔、是否配置升级代理、中心通知、告警邮件等各类中心功能设置的调整，方便用户对中心进行自定义配置与管理。

1. 终端管理员设置



(1) 终端密码保护

- 启用管理员密码保护，可以切换明文/密文显示，勾选后启用，当终端执行设置修改、功能开启或关闭、取消同步等操作时需要额外输入密码才可执行此类操作。
- 启用防止终端卸载密码保护，可以切换明文/密文显示，勾选后启用，若使用火绒卸载程序卸载终端时将需要额外输入密码才可执行卸载操作。
- 管理员密码保护及防止终端卸载密码保护，能够随机生成密码，也可以在终端概况——终端详情中生成临时密码，临时密码仅能对单一终端生效，通过限制临时密码适用范围及时效性，能够有效避免管理员密码泄露的风险。

(2) 离线终端管理：勾选后启用，当终端离线时间超过设置的天数时将自动删除此终端。支持设置的范围：7~180 天。

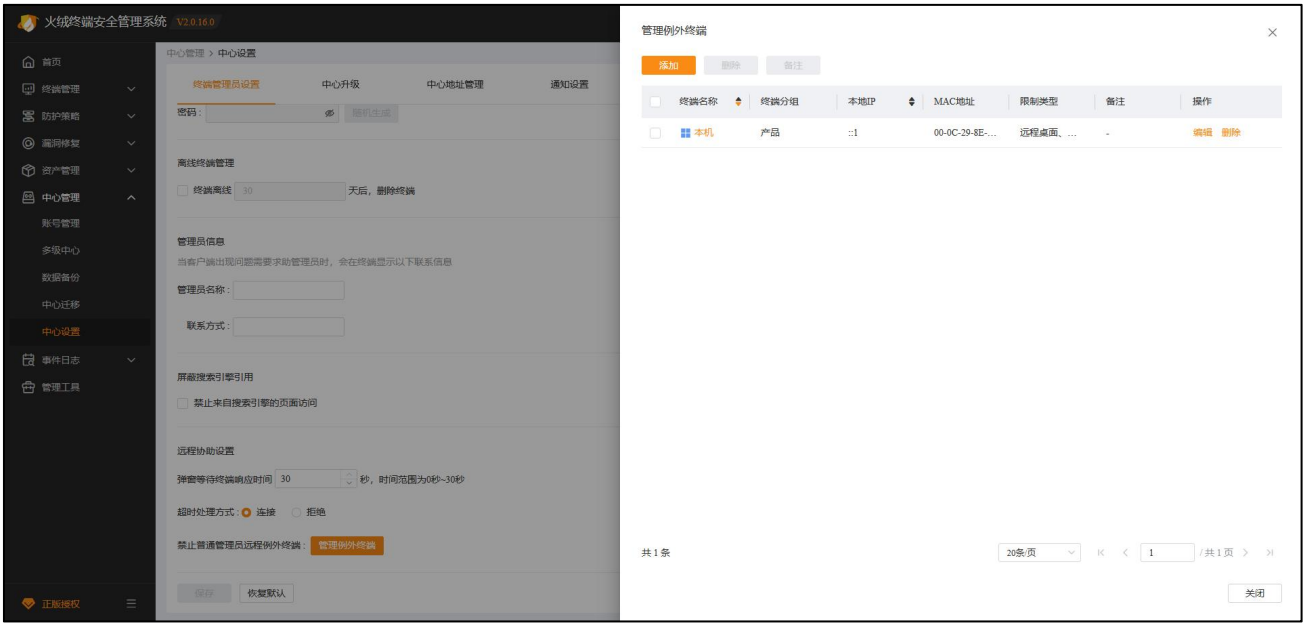
(3) 管理员信息：填写后将在终端“联系网管”功能中显示。

(4) 屏蔽搜索引擎引用：勾选后启用，当通过搜索引擎等其他方式搜索并访问中心的部署页面时，将被自动阻止显示。帮助缓解部署到外网的企业版中心通过搜索引擎结果直接跳转终端部署页面

的问题。

（5） 远程协助设置

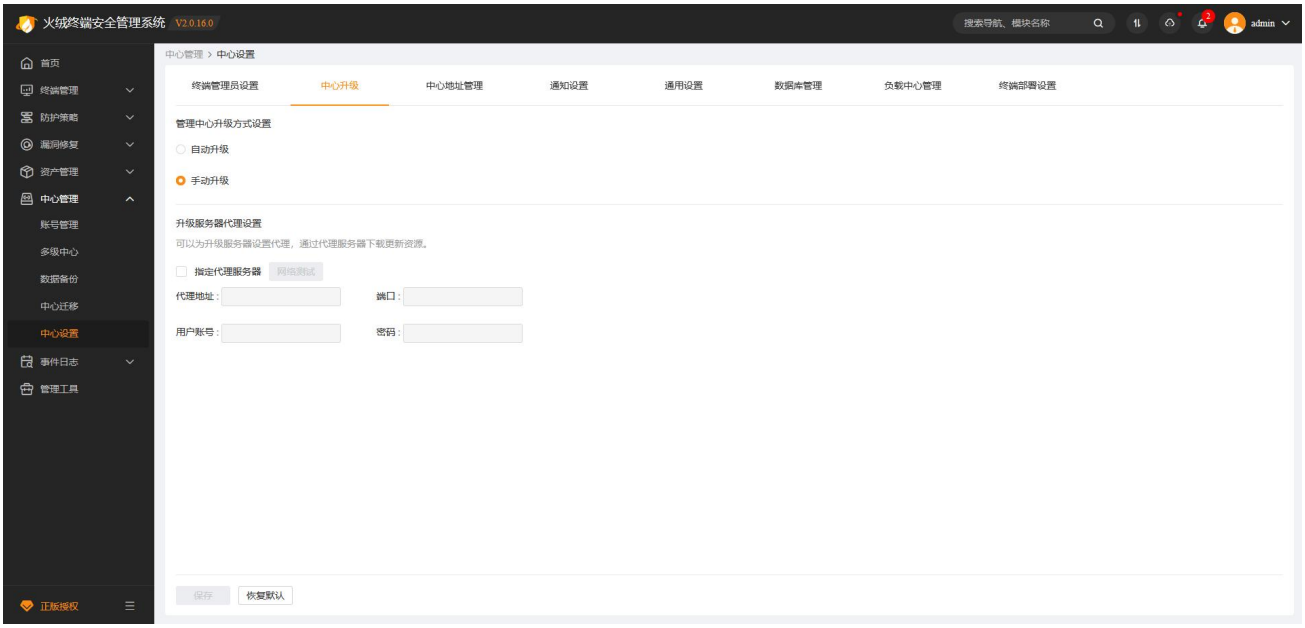
- 弹窗等待终端响应时间：默认 30 秒，最短可为 0 秒；终端接收到远程任务时，弹窗通知终端用户，终端用户需在响应时间内选择【允许】或【拒绝】。
- 超时处理方式：设置当终端用户在响应时间内未做选择，则弹窗关闭，默认【允许】或【拒绝】执行远程任务。
- 禁止普通管理员远程例外终端：支持设置例外终端，则普通管理员不可远程协助例外终端，超管不受此设置影响。



2. 中心升级

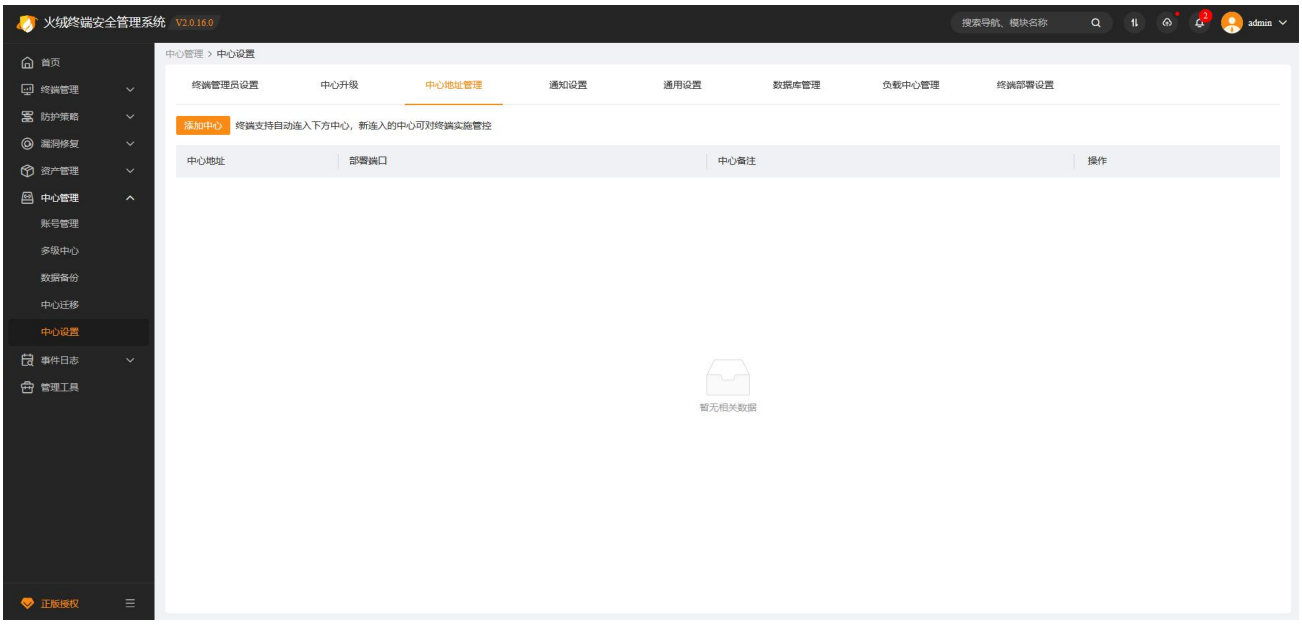
（1） 管理中心升级方式设置：选择中心升级方式，自动升级或手动升级。

（2） 升级服务器代理设置：可以为升级服务器设置代理，通过代理服务器下载中心升级数据。



3. 中心地址管理

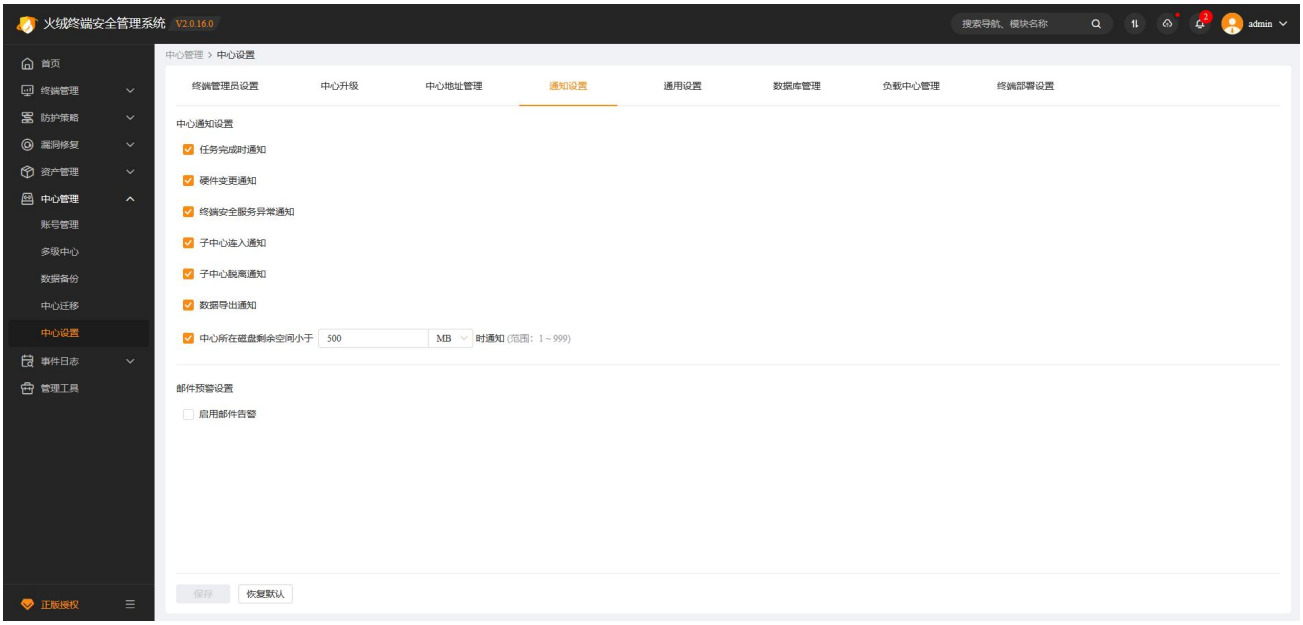
支持终端自动连入下方控制中心，当终端连入下列控制中心时，对应的控制中心即可对终端实施管控。用户点击【添加】按钮，输入中心地址及端口后即可成功添加中心，点击【保存】可保存当前配置。



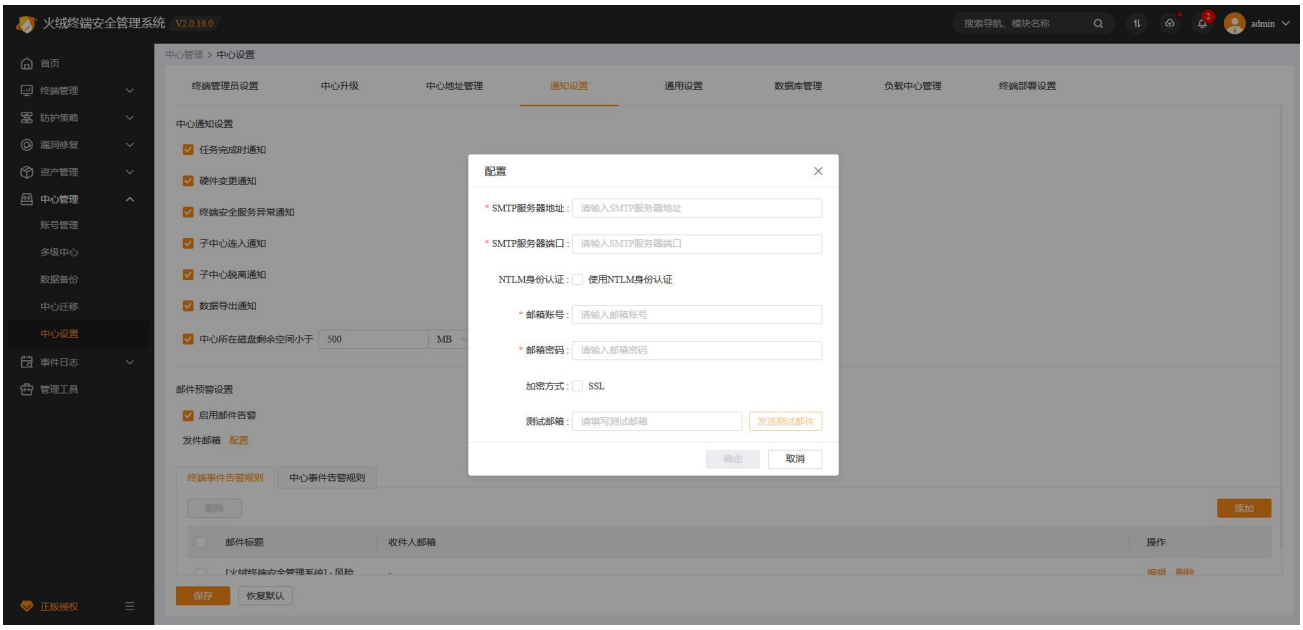
4. 通知设置

（1） 中心通知设置：设置控制中心的通知范围。勾选时表示控制中心右上角的消息通知中将显示此类型的通知，不勾选时表示不显示此通知。支持自定义控制中心所在磁盘剩余空间大小的告警

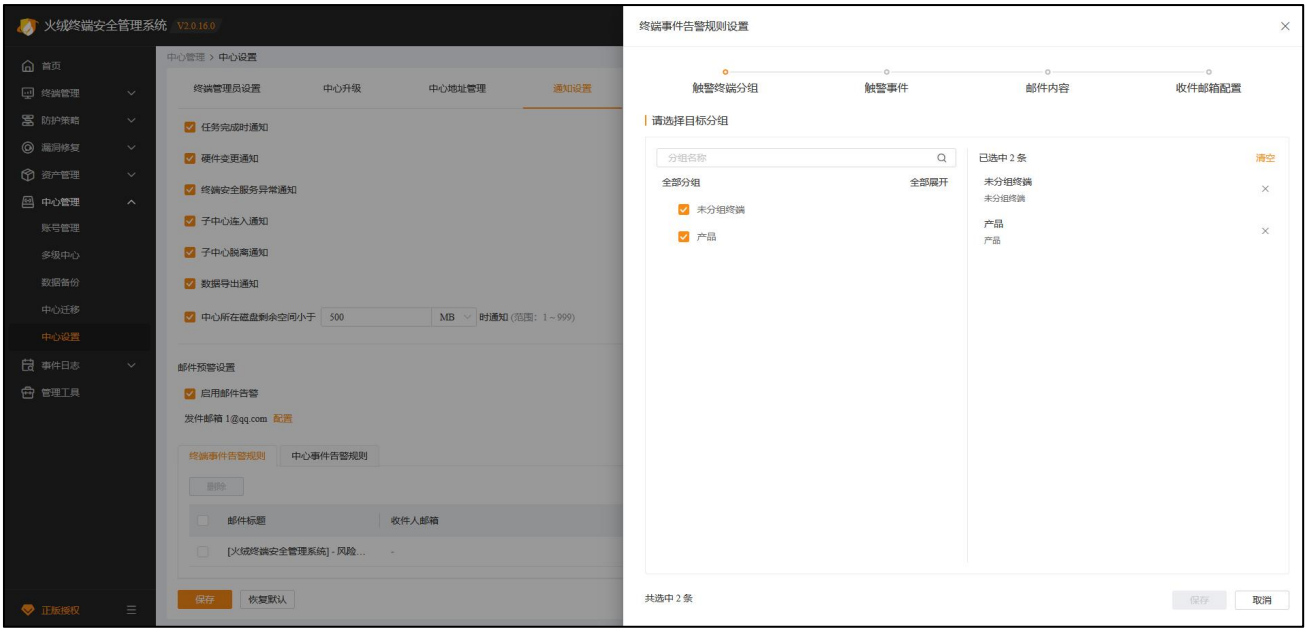
阈值，默认 500MB。



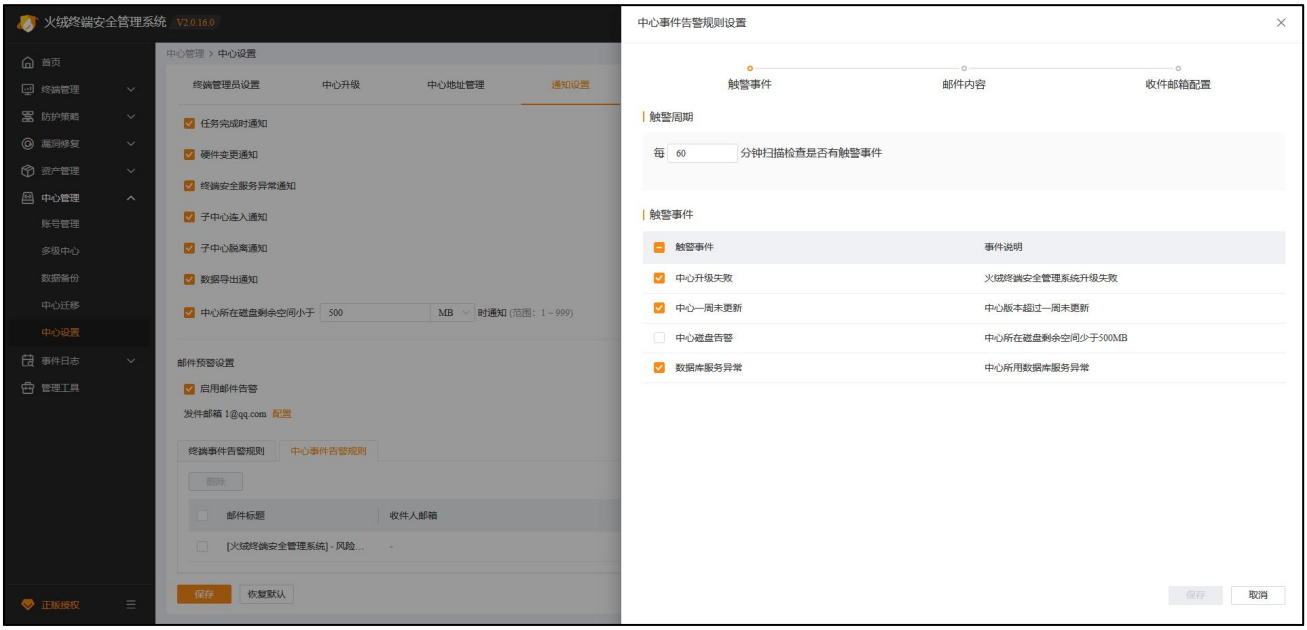
（2） 邮件预警设置：默认不勾选，勾选【启用邮件告警】需配置发件邮箱的信息。支持分别设置终端事件告警规则和中心事件告警规则，且对告警规则进行添加、编辑、删除操作。勾选时当触发用户设置的告警规则后将自动向对应的邮箱发送对应的告警邮件。



用户可自定义终端事件告警规则的触警终端分组、触警事件、邮件内容及收件邮件信息。



用户可自定义中心事件告警规则的触警事件、邮件内容及收件邮件信息。



5. 通用设置

（1） 通讯设置

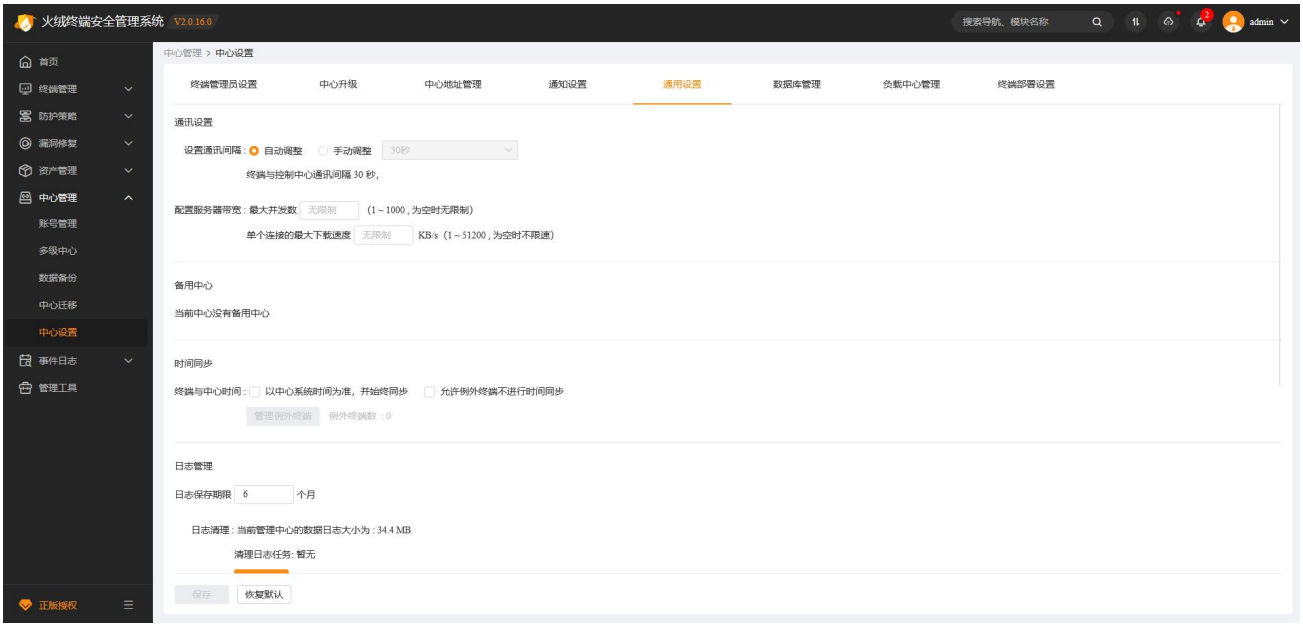
■ 设置通讯间隔：选择控制中心与终端的心跳时间，可选项有：15 秒、30 秒、1 分钟、5 分钟。

■ 配置服务器带宽：

✧ 最大并发数：设置“文件传输类”任务数量，包括(终端升级,文件分发,漏洞修复任务），输入

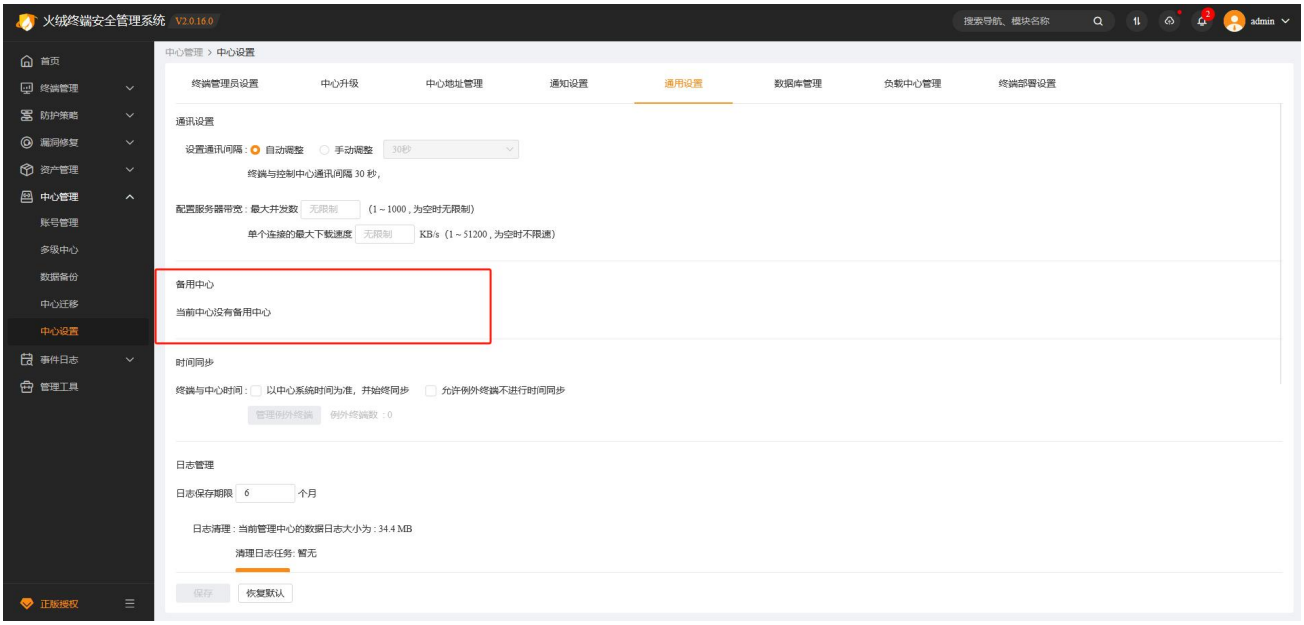
范围：1-1000，可为空，为空时表示无限制。

✧ 单个连接的最大下载速度：设置单个请求最大的下载速度。输入范围：1-51200KB/s，可为空，为空时表示无限制。



（2） 备用中心查看、审批

备用中心通过其本地安装的配置工具可以申请成为主中心的备用中心，备用中心提出申请后，主中心的通用设置中会显示待审批的备用中心信息，主中心审批通过后，主中心处显示备用中心的相关信息，并且开始同步数据。



（3） 时间同步

时间同步设置勾选后，中心所辖终端的时间将以中心的系统时间为准，并保持同步。可以添加例外终端。

（4） 日志管理

火绒终端安全管理系统提供中心日志的保存与清除。

- 日志保存期限：设置日志保存天数，超过日志保存时间的日志将自动删除。
- 日志清理：为管理员显示当前日志已占用大小，并提供日志清理功能，点击“清理日志”按钮弹出日志清理弹窗。管理员根据需要选择日志清理时间后点击保存即可。日志将在管理员设置的时间执行删除。

（5） Syslog 数据导出

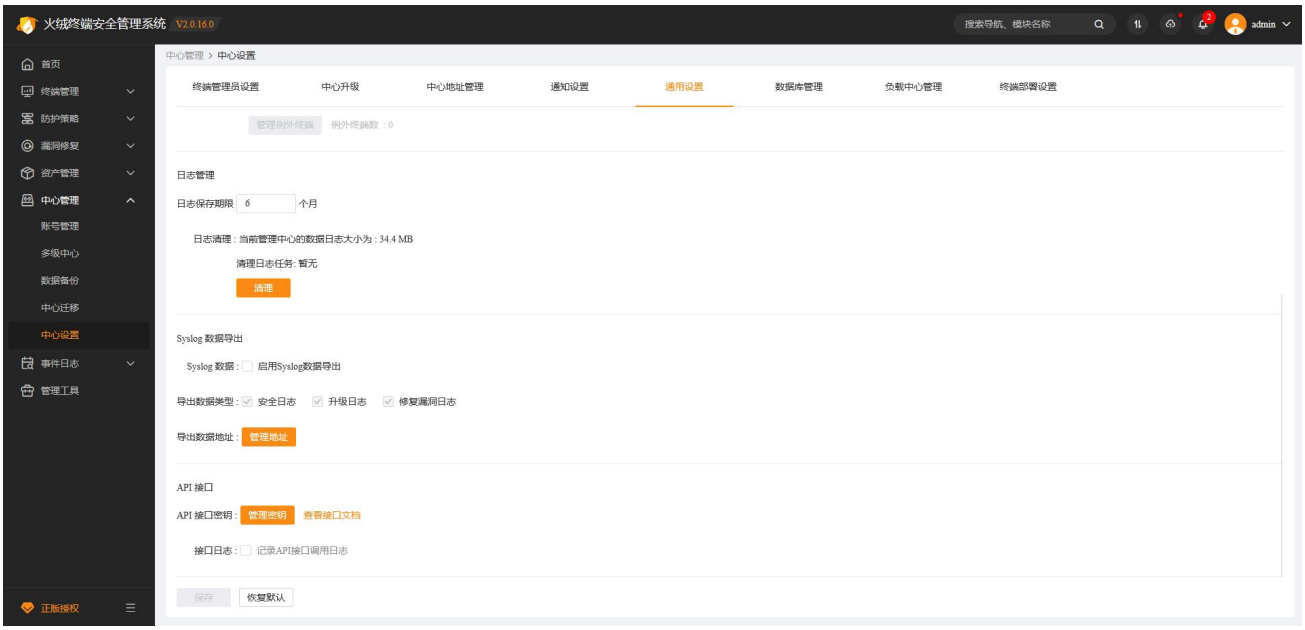
通过 Syslog 将中心日志传出给对应的接收端。填写接收端地址并启用后，每当有对应类型的日志产生控制中心都会将对应日志数据传输至接收端。

- Syslog 数据：勾选后启用 Syslog 数据导出。

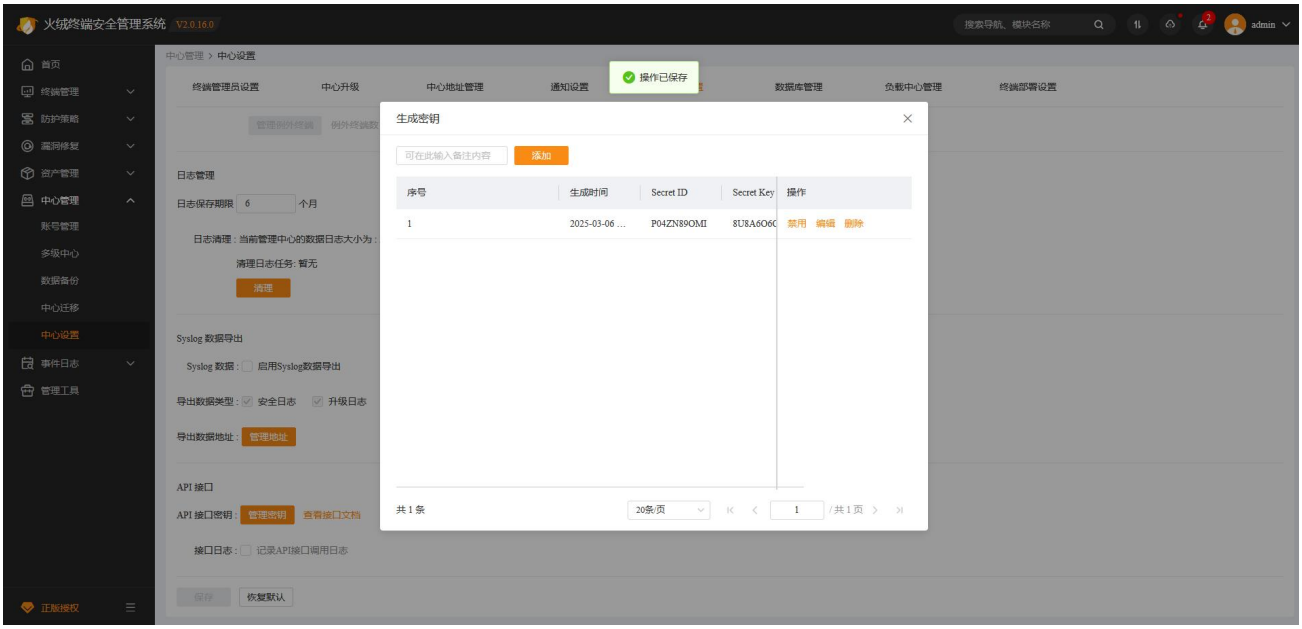
- 导出数据类型：选择需要导出的数据，当前支持安全日志、升级日志、修复漏洞日志。
- 导出数据地址：填写 Syslog 数据接收端的 IP 地址与端口。

（6） API 接口

支持通过调用火绒提供的 API 接口去隔离目标终端，并且可以记录调用 API 接口的日志，所记录的日志将显示在【系统管理日志-系统事件日志】中。



点击【管理秘钥】按钮，显示生成密钥窗口，点击添加可添加 API 接口，用户可根据添加的 API 接口 ID 及 Key 进行接口调用，添加完成的接口秘钥显示在列表中，支持对已添加的接口秘钥执行禁用、编辑和删除操作，调用接口日志的行为支持记录日志，可在【事件日志-系统管理日志-系统事件日志】列表查看。



6. 数据库管理

支持自定义数据存放位置，您可根据自身需要选择数据库。

默认数据库：即火绒提供的数据库。

外接数据库：目前支持选择 MySQL（5.6 及以上版本）或达梦数据（8.0 版本）。

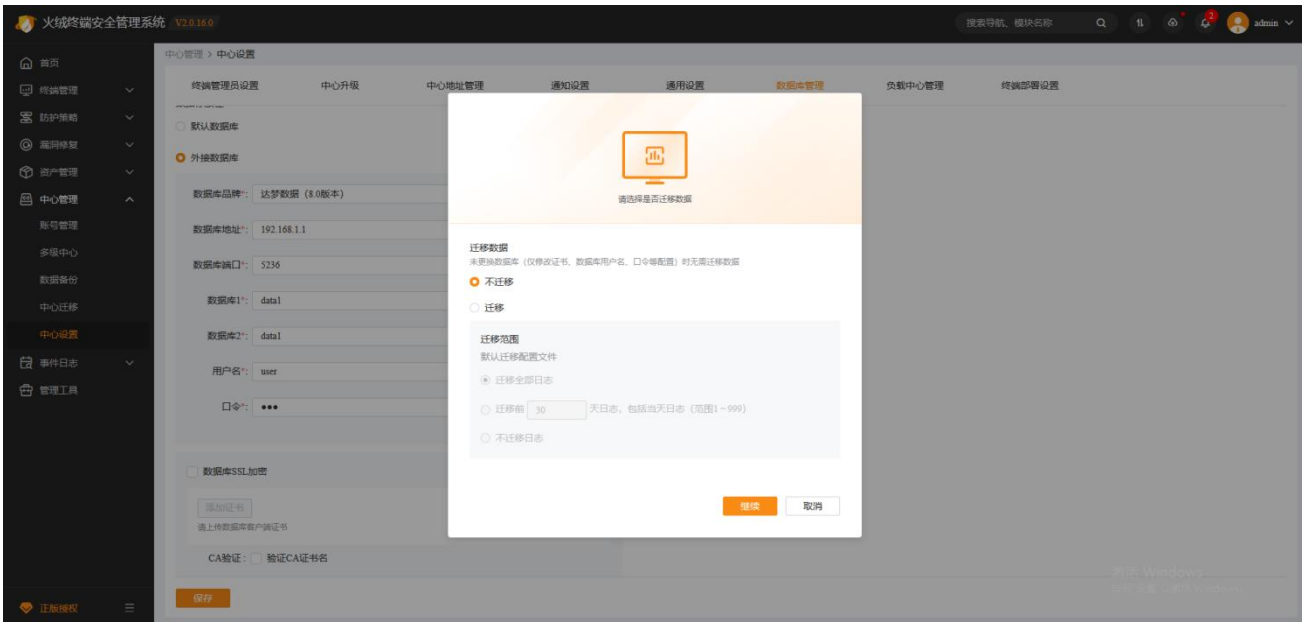
选择外接数据库后，需要填写数据库的相关信息，用以连接数据库。

注意事项：

建议达梦的数据库名使用数字、英文、下划线，不要使用其他特殊字符；

选择外接数据库时，为避免您的数据库宕机时，主、备用中心均无法使用，建议您在您连接的外接数据库中自行做好备份；

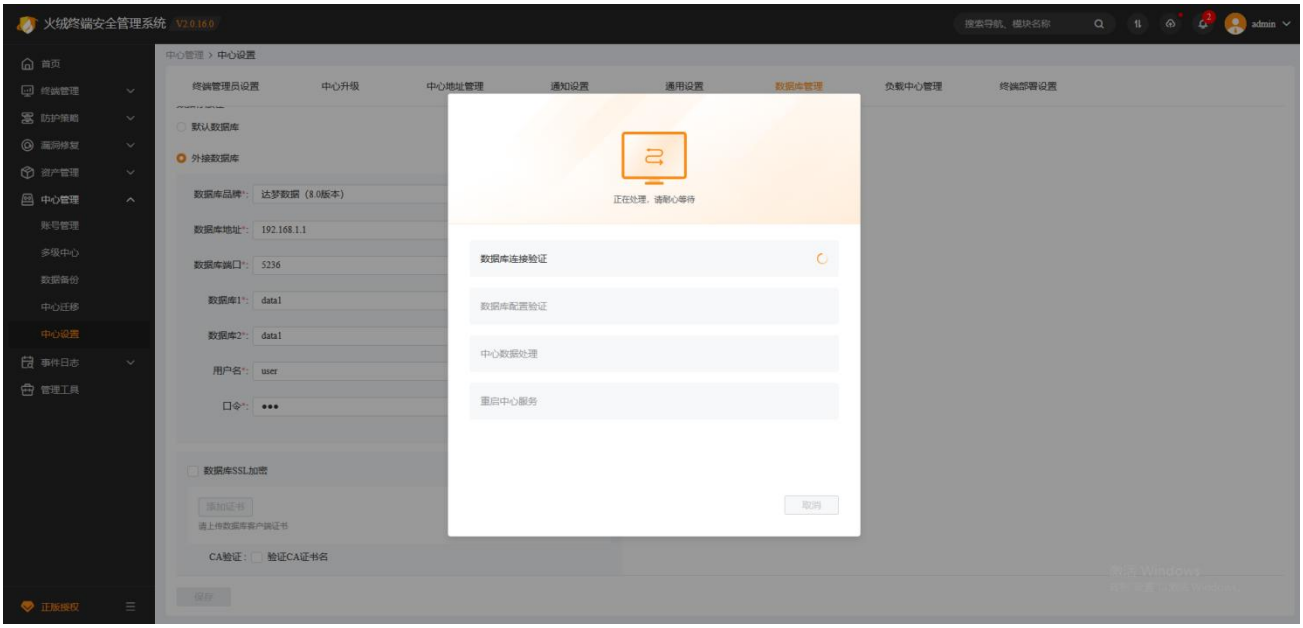
当您的外接数据库是【达梦】时，建议您将达梦部署在 Linux 系统环境下，若将达梦部署在 Windows 系统环境下，可能导致数据库性能低下



修改了数据库配置后保存时，需选择是否迁移数据，即是否要将原数据库中的数据迁移到新数据库中（注：建议您若变更了连接的数据库时选择【迁移】，若您未变更数据库，仅修改了数据库的配置信息时，选择【不迁移】）。

选择迁移数据时，需选择迁移的数据范围，配置文件默认迁移，您可自定义迁移的日志范围。

点击【继续】，将进行数据库连接验证和数据处理，需等待一段时间。

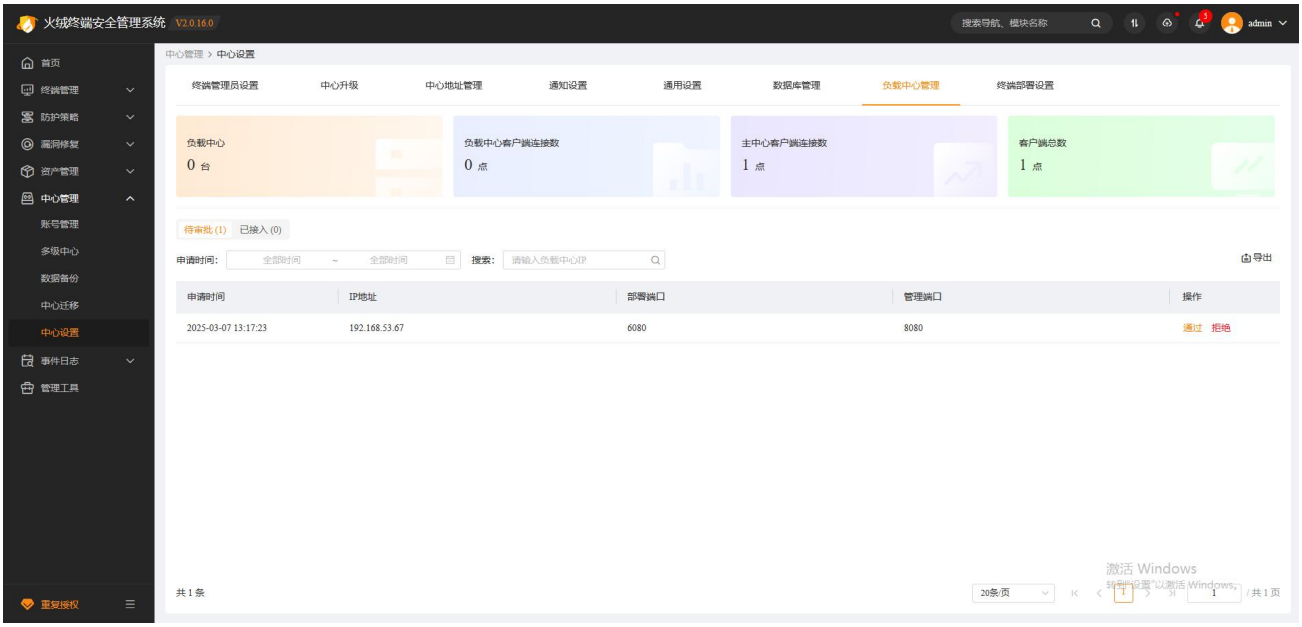


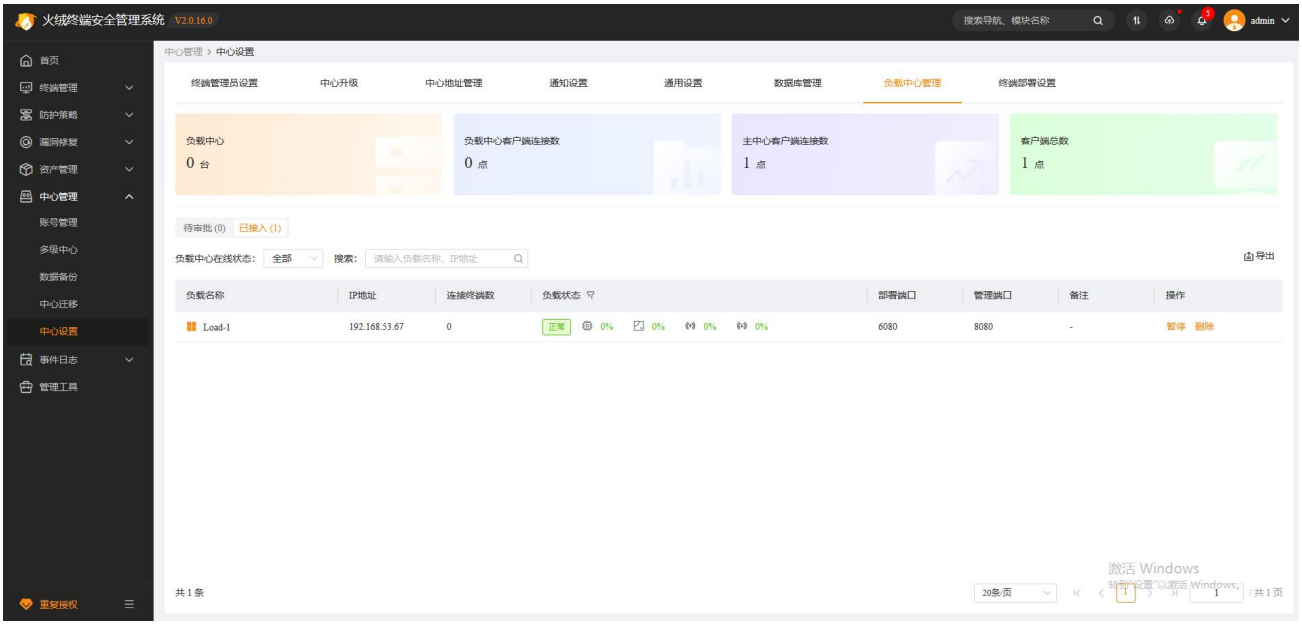
数据库连接验证和数据处理流程通过将自动重启中心服务，即数据库的修改保存成功。

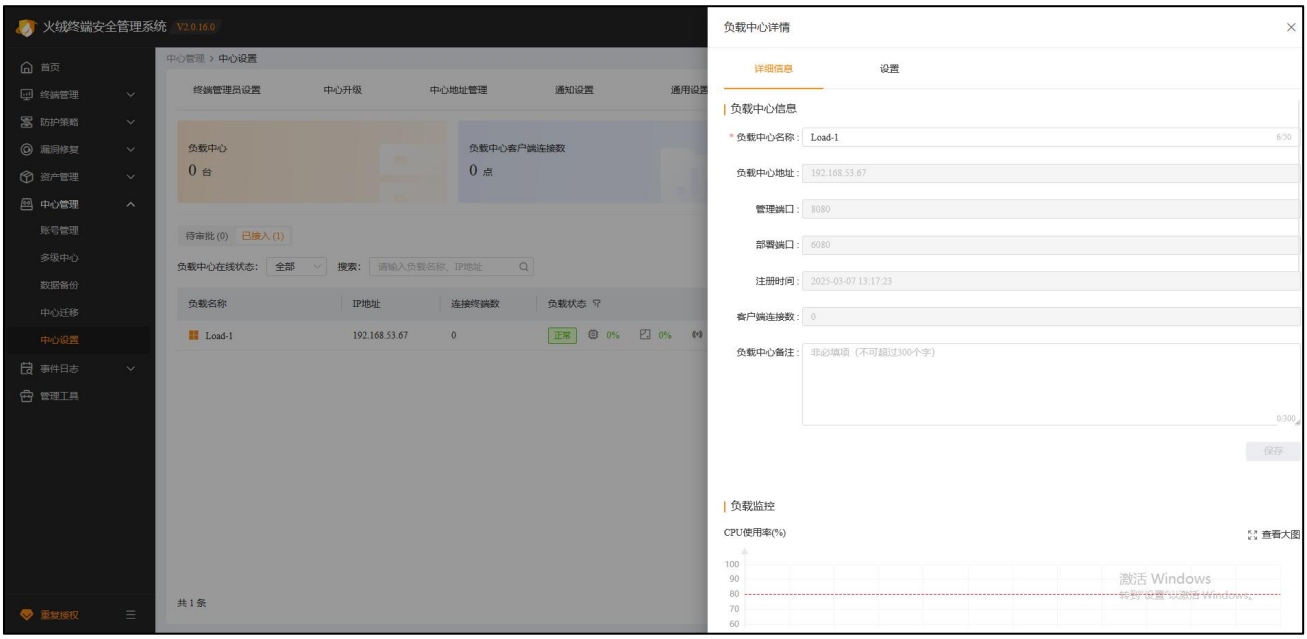
7. 负载中心管理

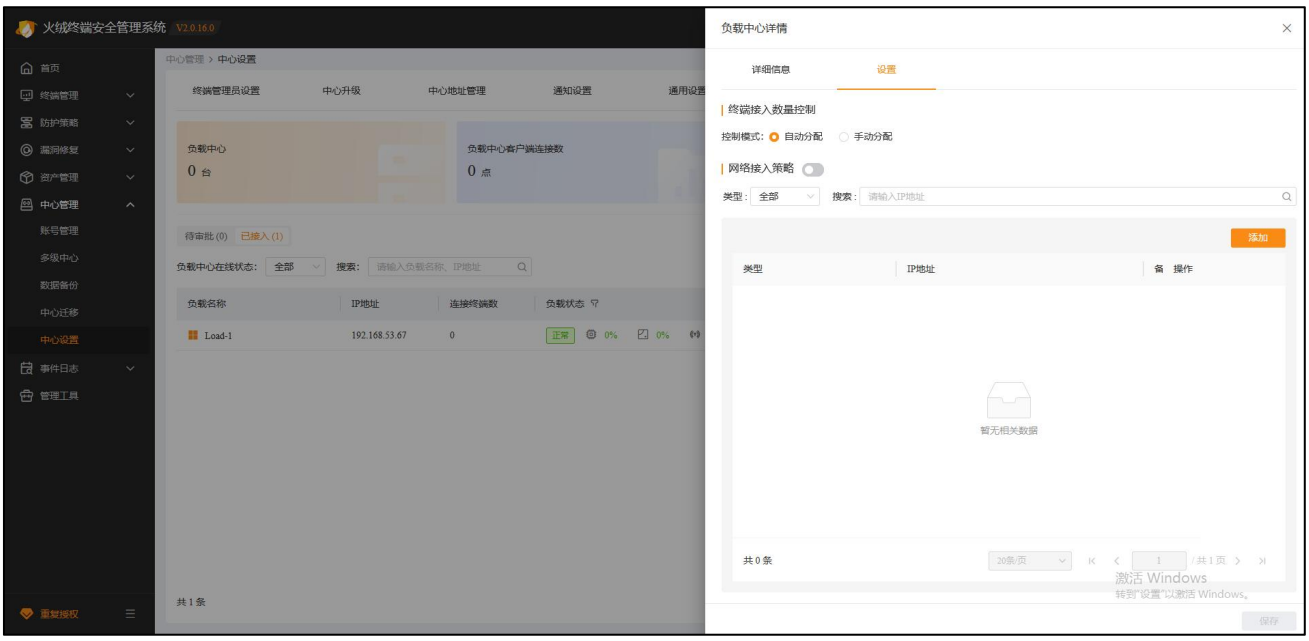
可以通过负载中心管理页面查看当前已经接入主中心的负载中心数量、接入负载中心客户端的数量、接入主中心客户端的数量、接入中心的客户端总数以及待审批和已接入的负载中心。

单击已接入的负载中心名称可以查看或管理负载中心。









8. 终端部署设置

（1） 部署页设置

部署页设置可以设置中心部署页面通知标题和通知内容，未做修改时，显示火绒预设的默认内容，允许根据使用需求进行编辑。

隐藏未授权类型下载链接，配置项勾选后，中心部署页会隐藏当前中心未授权系统类型的火绒安全终端下载链接，避免用户误下载未授权类型终端带来的沟通成本。

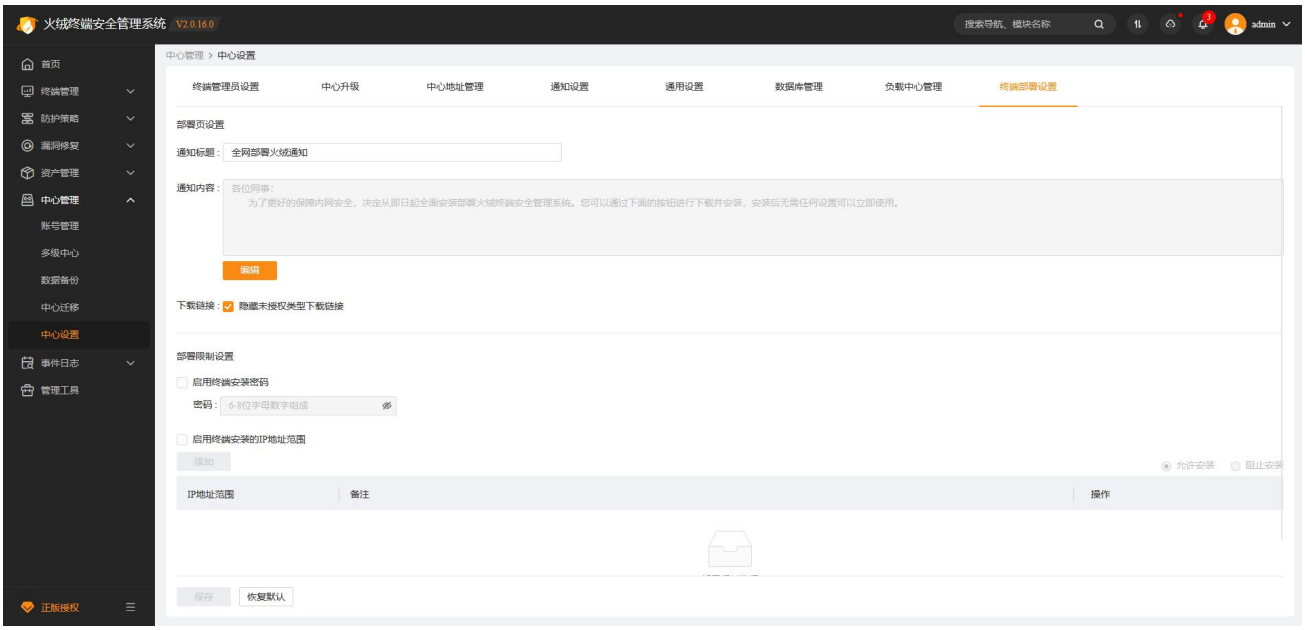
（2） 部署限制设置

部署限制设置分为终端安装密码限制和终端安装 IP 地址范围限制，这两种限制能够在一定程度上保护用户的利益，有效防止通过中心部署地址下载安装火绒安全终端，非法占用用户购买的点位。

启用终端安装密码后，管理员可以设置 6-8 位的终端安装密码，终端用户在安装过程中或终端上线时需验证中心设置的密码。

启用终端安装的 IP 地址范围，可以设置该中心允许安装或不允许安装的 IP 地址范围，用户在安装火绒安全终端或终端上线时需验证 IP 地址范围是否在中心允许安装的范围内，管理员设置的 IP 地址范围会显示在本页面底部的列表中，支持对已经添加的 IP 地址做编辑和删除操作。

如终端安装密码或 IP 地址范围验证失败，将无法安装或不能正常使用火绒安全终端。



9. 定制化

当前授权购买了【定制化】模块时，支持自定义控制中心和终端的名称和 LOGO。

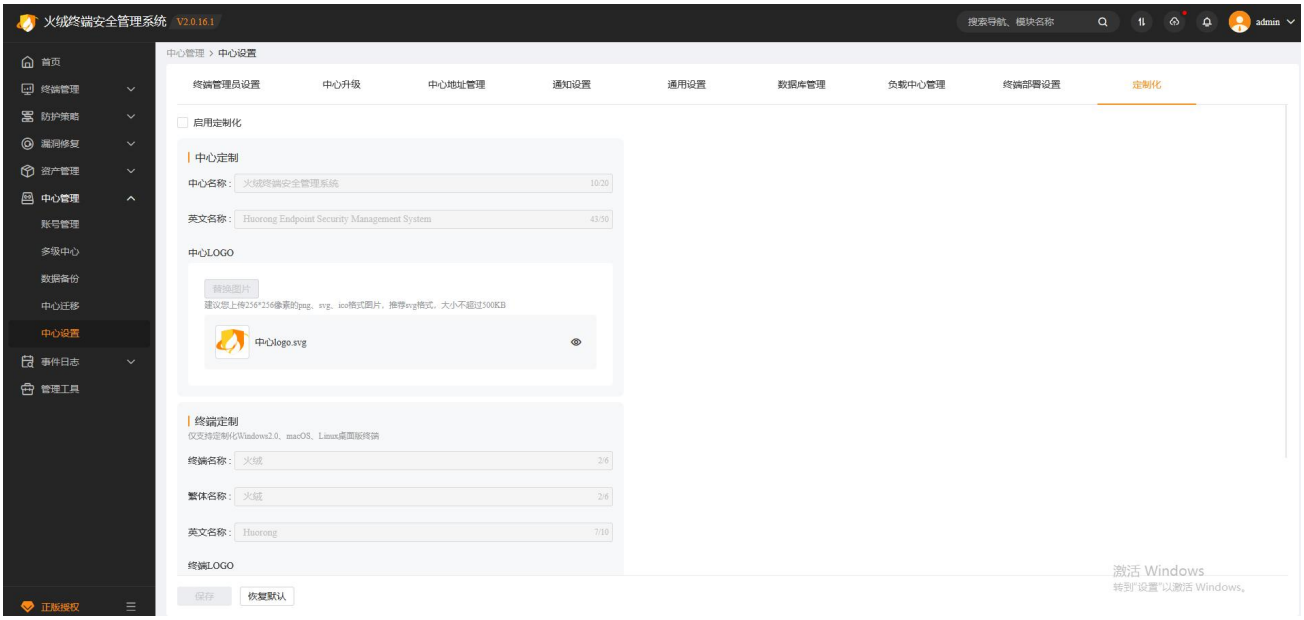
勾选后即中心和终端的部分页面会按照用户自定义的内容显示名称和 LOGO。取消勾选后即中心和终端切换回火绒的名称和 LOGO。

注：

上传 LOGO 时，为了避免 LOGO 模糊化，建议您上传 svg 格式。

建议不要上传改变过扩展名的图片，否则可能导致图片不可用。

通过【动态分配】【自定义分配】方式分配授权的下级中心，跟随上级中心授权是否具有定制化功能，但定制化的信息，需下级中心重新填写。



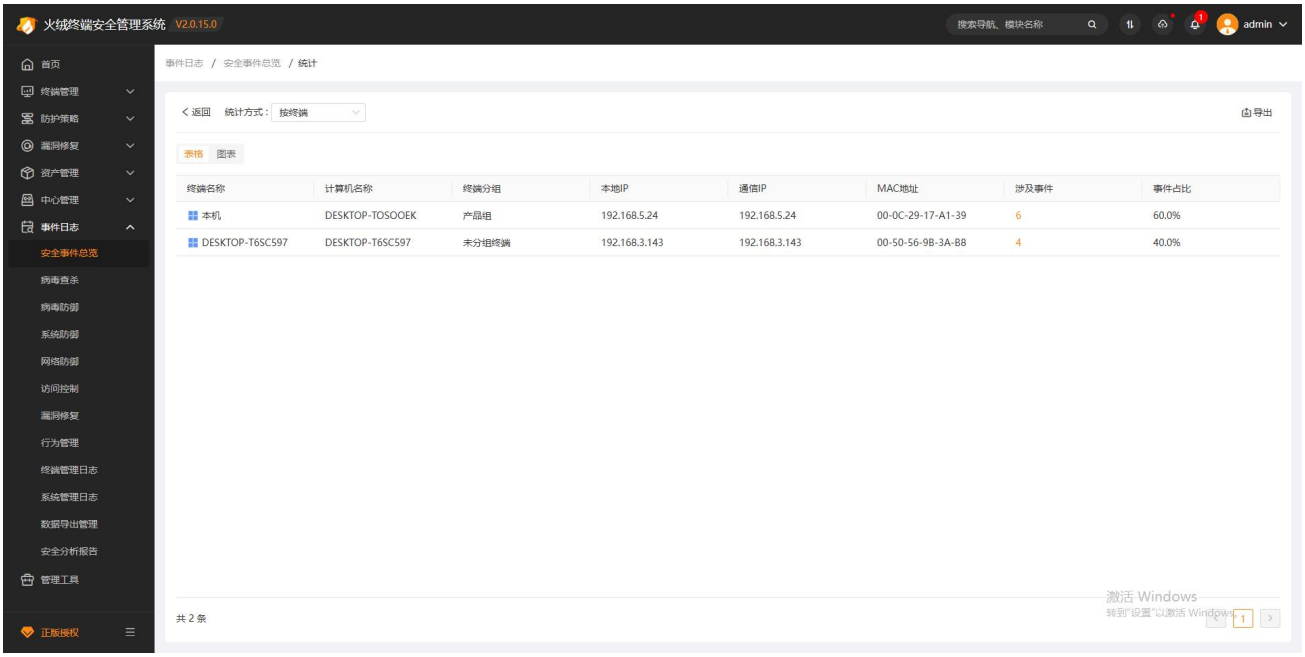
2.10 事件日志

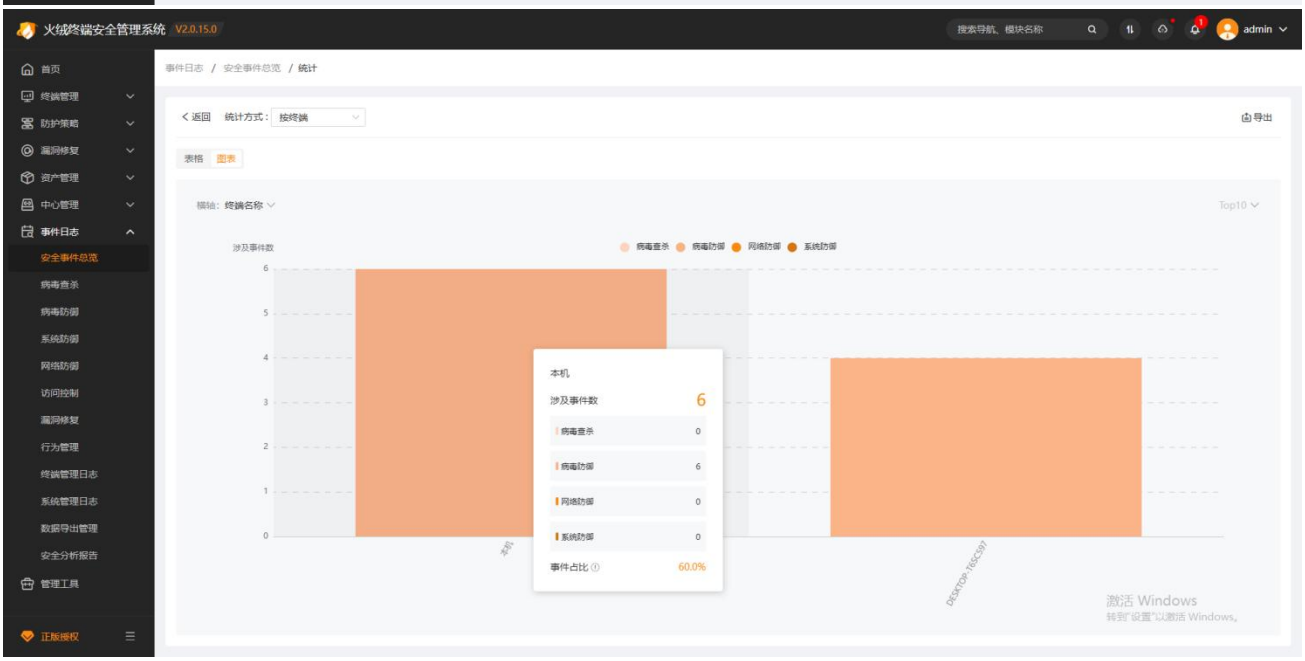
火绒终端安全管理系统提供全网安全事件日志及终端和系统管理日志记录，当 300 秒内出现相同事件时，中心将自动识别，并展示第一次记录日志的时间，以节省磁盘空间，更方便用户查看分析日志的，同时，还提供日志导出功能供用户线下分析汇报。

（1） 安全事件总览：病毒查杀（病毒日志）、病毒防御、系统防御、网络防御四项功能的日志综合列表。

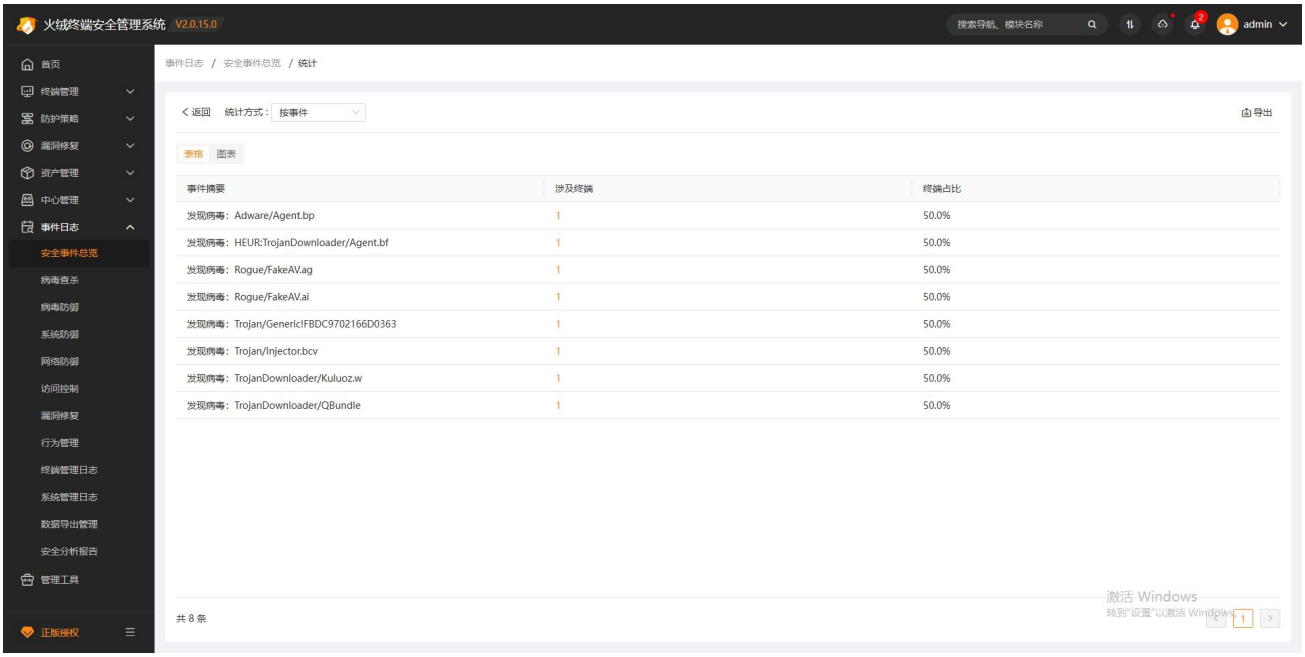
系统提供了多种筛选条件（事件类型筛选、终端时间筛选、关键词模糊搜索、分组筛选）和检索功能，帮助用户快速定位目标日志条目。点击【统计】，进入统计页，针对当前筛选出来的数据进行统计，支持 2 种统计方式：按终端、按事件。

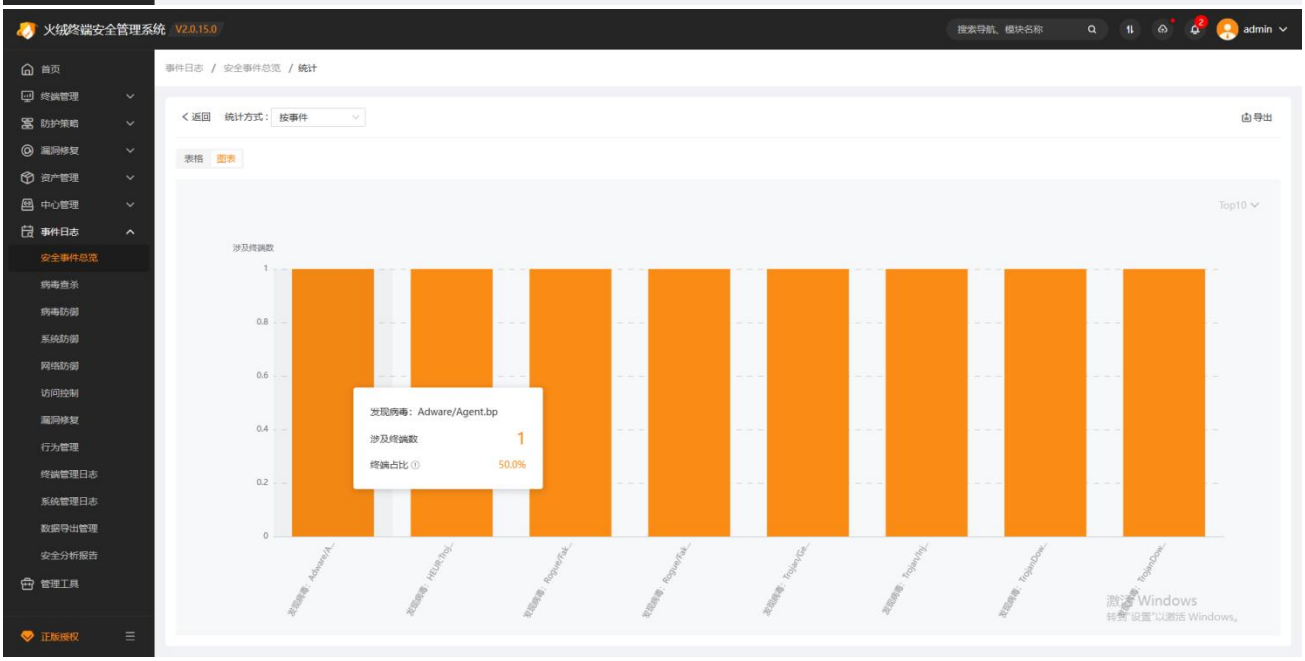
统计方式为按终端时，可通过表格或图表 2 种形式，查看每个终端涉及事件的数量以及占比，便于用户进行数据汇总。点击表格中的【涉及事件】，可查看涉及的事件详情，点击【导出】，同时导出表格和图表。





统计方式为按事件时，可通过表格或图表 2 种形式，查看每个事件涉及终端的数量以及占比，便于用户进行数据汇总。点击表格中的【涉及终端】，可查看涉及的终端的信息，点击【导出】，同时导出表格和图表。





(2) 病毒查杀日志：终端执行病毒查杀后生成的病毒日志和查杀日志。

(3) 病毒防御日志：终端触发病毒防御相关功能后生成的数据日志。

(4) 系统防御日志：终端触发系统防御相关功能后生成的数据日志。

（5） 网络防御日志：终端触发网络防御相关功能后生成的数据日志。

（6） 访问控制日志：终端触发访问控制相关功能后生成的数据日志。

（7） 漏洞修复日志：终端执行漏洞修复后生成的数据日志。

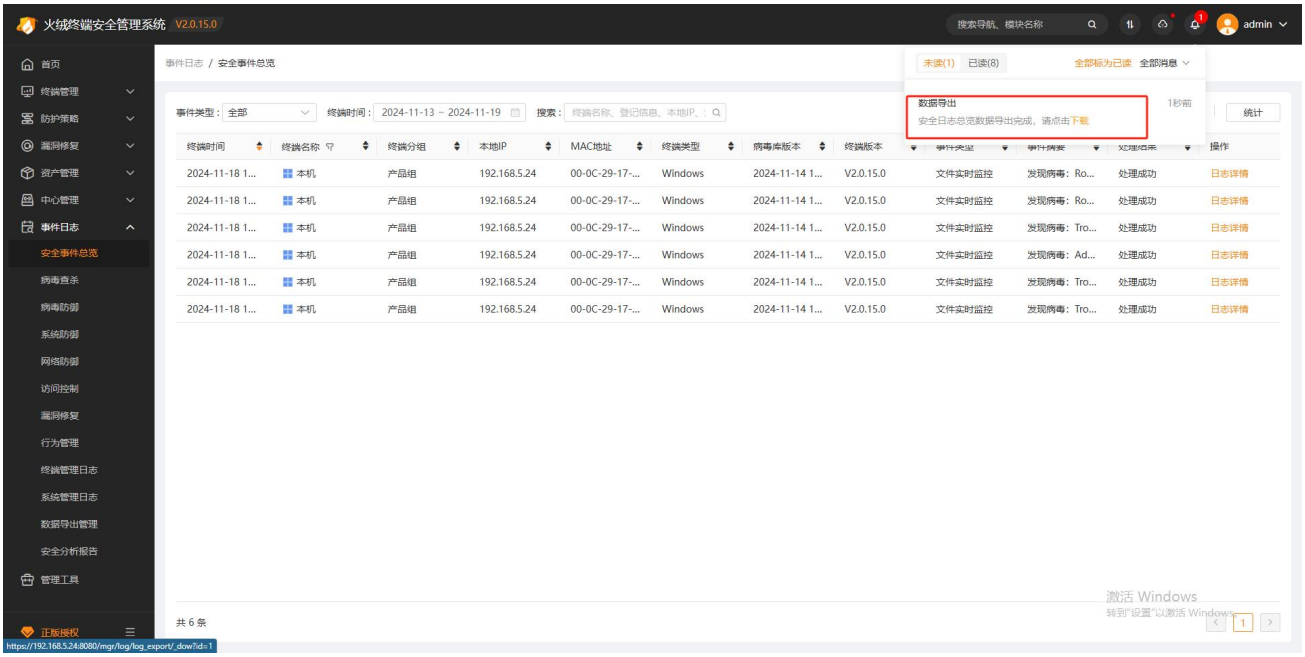
（8） 终端管理日志：显示终端升级日志与终端执行的操作日志和计划任务日志。

（9） 系统管理日志：显示中心升级日志与控制中心管理员的操作日志以及系统事件日志。

（10） 数据导出管理：显示中心内导出的数据文件，用户可在此界面对导出的数据文件进行状态查看及管理。

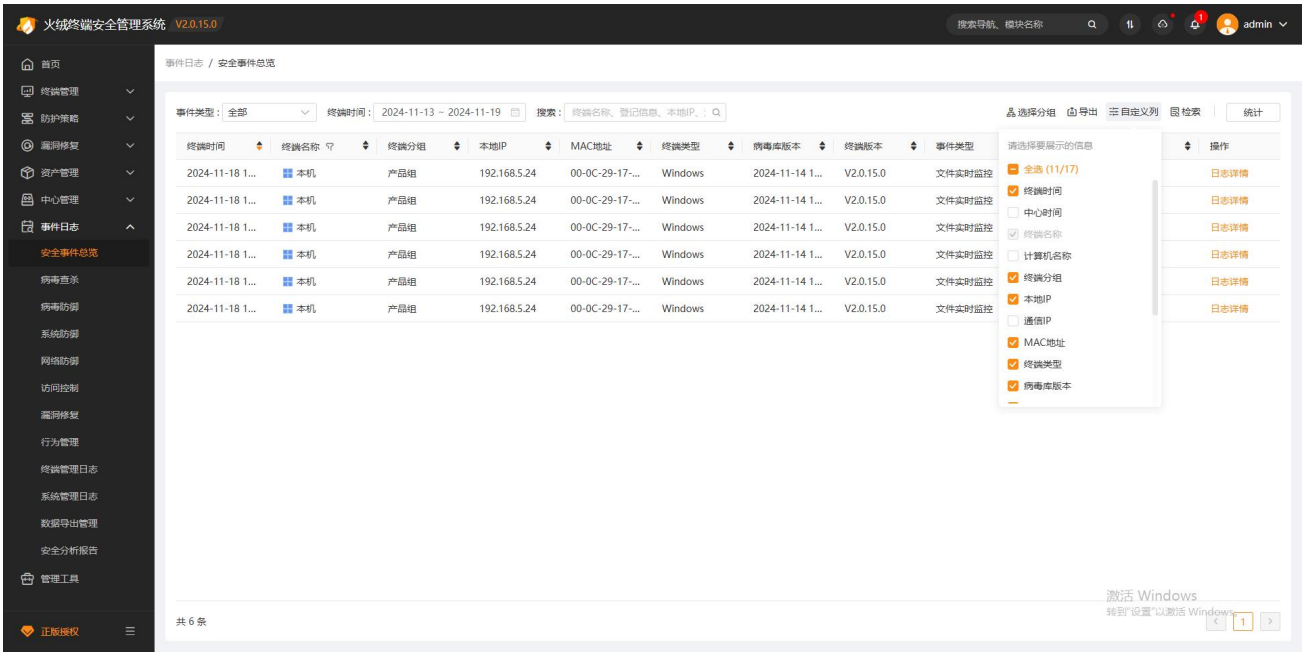
（11） 安全分析报告：可手动导出或订阅安全分析报告，将企业内的安全状态以直观、清晰的数据图表形式展示给用户。

所有事件日志均支持导出功能，用户可自定义导出哪些字段，导出后将在右上角消息通知处通知，点击下载，将导出数据下载在本地。

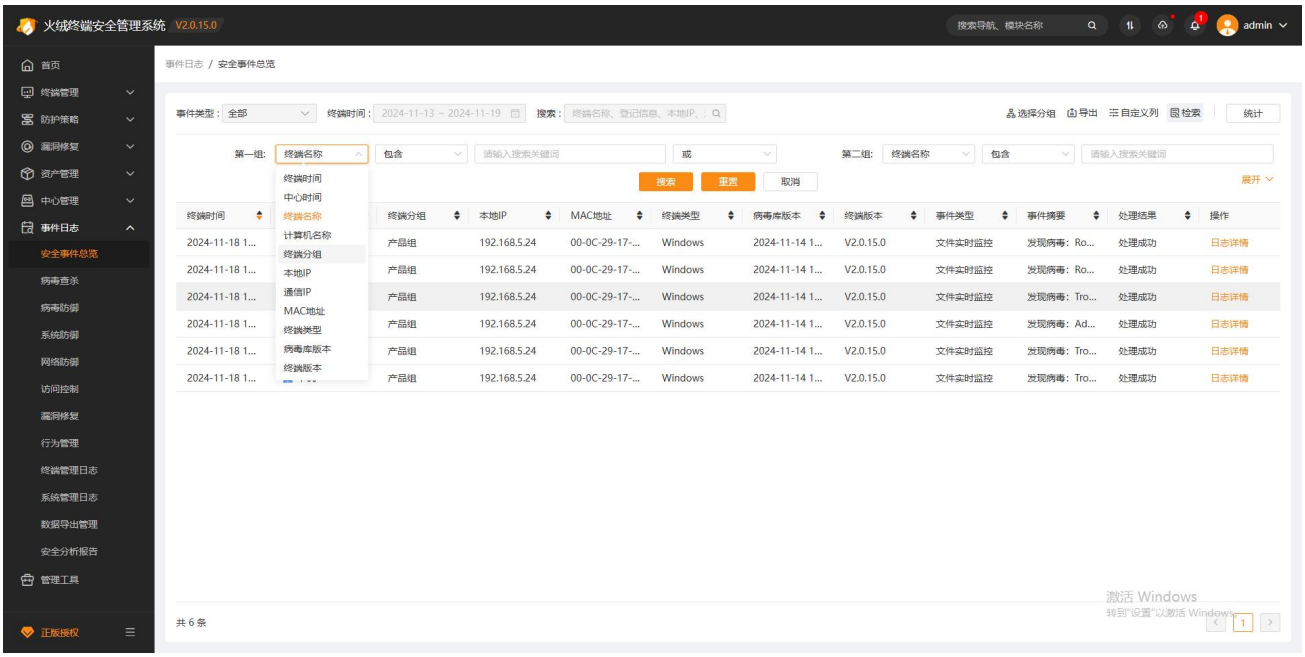


所有事件日志均支持自定义列功能，方便用户依据自身情况筛选重要日志数据列表显示，重点查看真

正关心的信息。



所有事件日志均支持多条件组合检索，方便用户定向查询日志，帮助用户快速精准查找指定安全日志条目。



2.11 管理工具

火绒终端安全管理系统提供辅助控制中心管理与操作的各类工具合集。

1. 域部署工具

避免在域环境中一台台部署火绒终端安全软件重复低效部署工作，用户可通过域部署工具对域用户统一安装部署火绒终端。

操作方法：

点击下载域部署工具；在域环境下打开域部署工具，首先导入脚本，然后选择域用户启用脚本即可。（详见使用说明）

2. 离线升级工具

如果您的控制中心无法连接火绒服务器，导致火绒终端安全管理系统无法升级更新，可以使用离线升级工具进行升级。

操作方法：

（1） 下载离线升级工具，在能够连接控制中心的计算机上同步控制中心数据；

（2） 通过移动设备等方式拷贝离线升级工具以及同步数据包 conf 文件夹，在连接有外网的机器上检查更新并下载离线升级数据；

（3） 通过移动设备等方式拷贝离线升级工具以及 conf 文件夹和下载数据包 upgrade 文件夹，到能够连接控制中心的机器上，更新中心即可。

3. 中心迁移工具

当需要针对单个终端执行中心迁移操作时可以使用中心迁移工具。将下载的中心迁移工具在需要迁移的终端上运行，填写迁移的中心地址点击迁移即可执行该终端的中心迁移。

4. 移动存储注册工具

当您需要添加信任设备时，请先下载并安装移动存储注册工具。移动存储注册工具是执行信任 U 盘设备时的必需软件，若未安装将无法注册设备。

5. 火绒安全 U 盘程序

火绒安全 U 盘程序是在 U 盘注册完成后自动再 U 盘生成的程序。当用户误操作删除注册 U 盘内的火绒安全 U 盘程序时，您可再次下载此程序，并将程序拷贝至注册 U 盘中，即可继续使用注册 U 盘。

6. 专杀工具

针对查杀内核级对抗类病毒，仅当火绒安全服务异常且修复失败时使用。不推荐管理员日常使用。

7. SHA-2 代码签名补丁修复工具

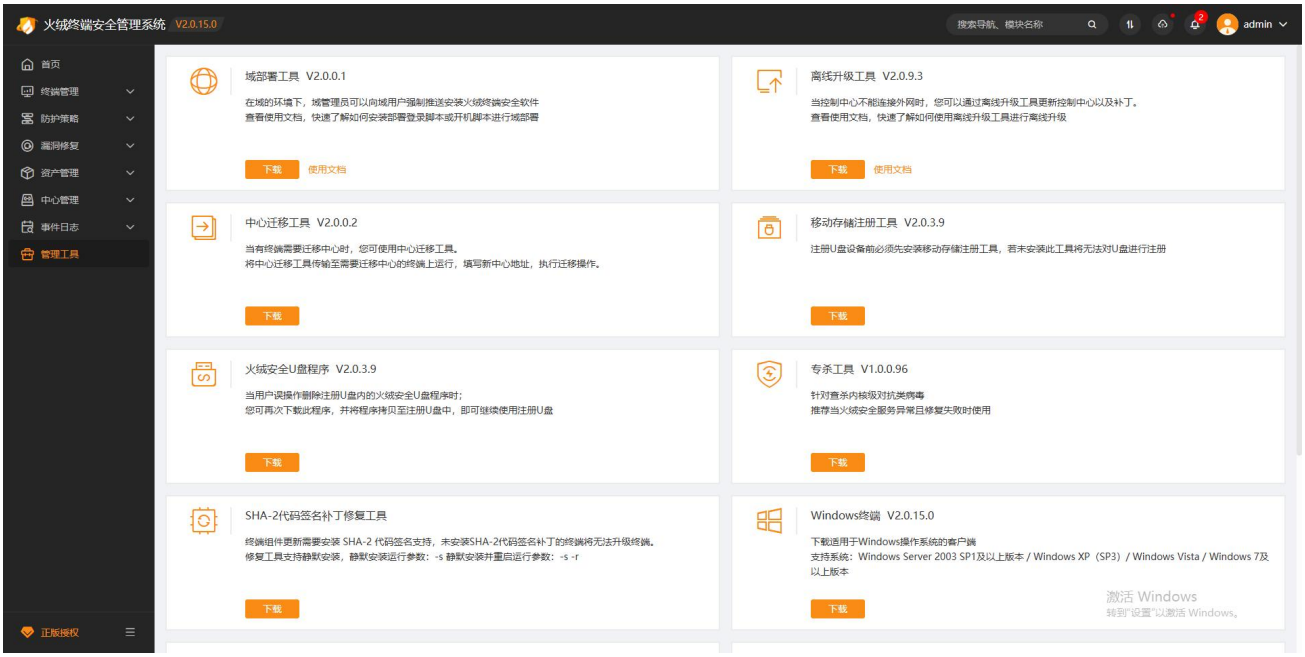
微软发布了 SHA-2 更新公告，将会把老版的哈希加密算法 SHA-1 升级为更新、更安全的 SHA-2。此工具可以针对环境自动做出检测，执行一键修复。

8. Windows 终端

下载适用于的 Windows 操作系统的客户端安装包。

9. Linux 终端

下载适用于 Linux 的操作系统的客户端安装包。



2.12 配置工具

用户可通过配置工具更改控制中心地址、HTTPS 设置、端口设置、文件存放位置、中心密钥及超级管理员密码，更改完成后，点击保存即可完成控制中心配置更改，不同安装类型的中心的配置工具内容存在不同。

1. 主中心配置工具

字段	说明

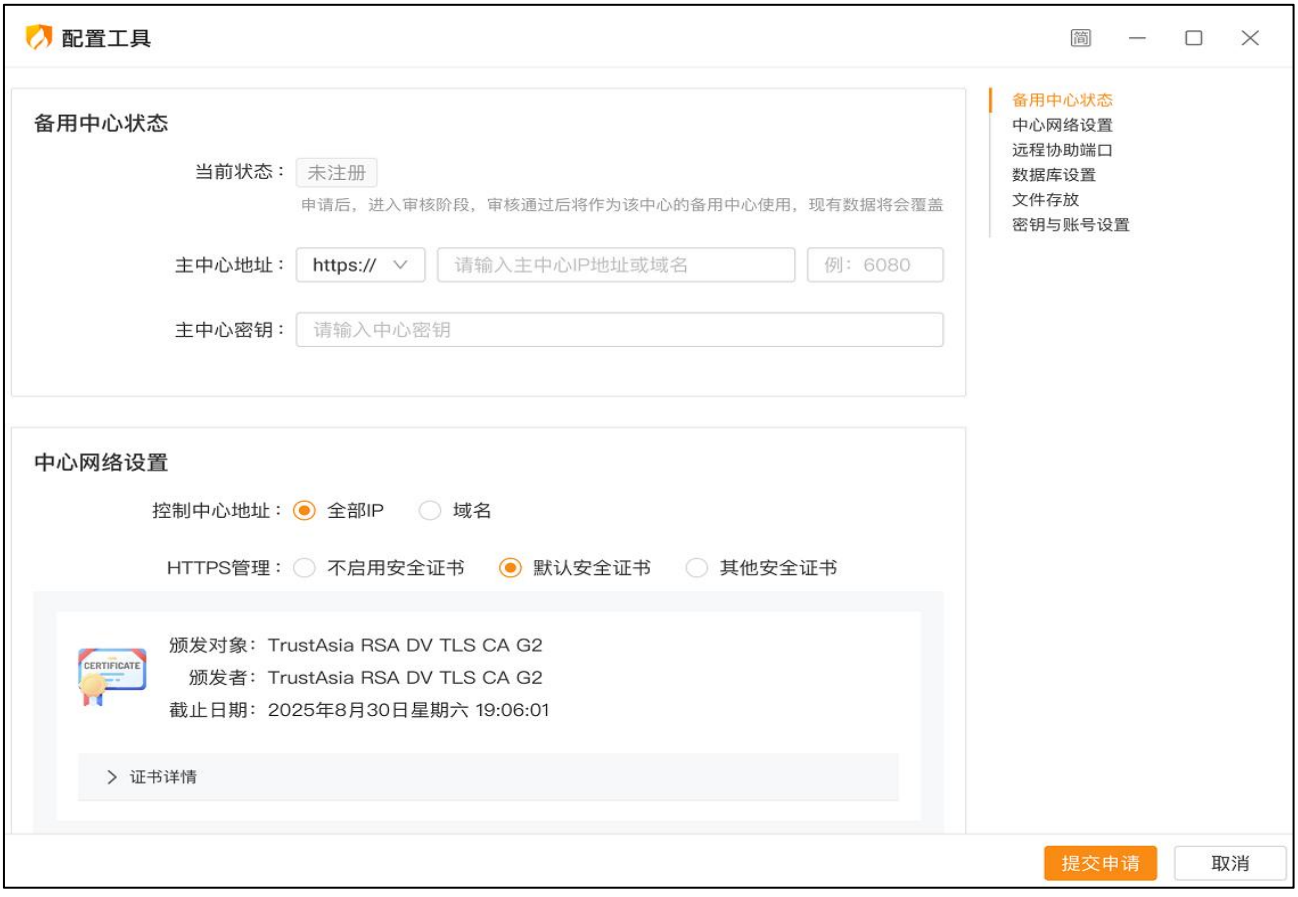
中心网络设置	**控制中心地址**	单选，默认选中【全部 IP】； 【全部 IP】通过动态获取 IP 进行终端部署； 多网卡中任一 IP 地址均可访问； 【域名】通过自定义域名进行终端部署，支持 HTTP 协议以及 HTTPS 协议；
	HTTPS 管理	设置是否使用 HTTPS 访问控制中心，单选； 不启用安全证书：使用 HTTP 访问控制中心； 默认安全证书（默认）：使用默认安全证书访问控制中心； 其他安全证书：使用自定义的安全证书访问控制中心；选择该选项时，需选择证书标准后再自定义上传对应的 Crt、Key 文件； 共 2 种证书标准： 国际标准（默认）：采用国际通用的算法进行加密的证书 国密标准：采用国密算法进行加密的证书
	中心管理端口	通过该端口访问控制中心，端口默认为 8080；
	终端部署端口	通过该端口访问终端部署页面，端口默认为 6080；
远程协助端口	**中心远程端口**	中心下发远程协助时中心使用的远程端口，端口默认 5901；
	终端远程桌面端口	远程桌面、远程查看时终端与中心连接使用的远程端口，端口默认 5500；

	终端远程 CMD 端口	远程 CMD 时终端与中心连接使用的远程端口，端口默认 5902;
数据库设置	**本地数据库端口**	中心本地数据库使用的端口，端口默认为 3306;
文件存放	**补丁存放目录**	漏洞修复补丁存放在中心的目录，可自定义存放目录;
	文件分发目录	文件分发上传的文件保存的目录，可自定义存放目录;
	中心备份目录	中心执行数据备份后备份文件的存放目录，可自定义存放目录;
	数据导出目录	中心导出的数据文件存放在中心的目录，可自定义存放目录;
密钥与账号设置	**超级管理员账号**	显示超级管理员的账号名称;
	超级管理员密码	可在此处强制修改超级管理员密码，修改密码时需要上传凭证，凭证来源于官网，可登录火绒官网(https://lic.buy.huorong.cn/html/dist/index.html#/login)生成并下载凭证;
	中心密钥	用于控制中心间通讯加密，可重新生成密钥;
修改终端部署地址或者端口后，已经部署的终端需要重新下载覆盖安装客户端;		

火绒官网生成并下载凭证位置


我的授权
我的订单
安装包工具
客服中心
Windows版控制中心安装包V2.0
安装火绒企业版后，使用默认账号:admin，密码:admin 登录控制中心输入序列号和密码激活授权，否则无法使用
产品安装部署手册
产品使用手册
安装包下载
Linux版控制中心安装包V2.0
请安装火绒企业版后，输入序列号和密码激活授权，否则无法使用
产品安装部署手册
产品使用手册
安装包下载
离线升级包
适用于内网环境进行升级
安装包下载
隔离网升级工具
适用于内网环境进行升级，仅支持中心2.0.10.0及以上版本下载
隔离网升级工具使用手册
安装包下载
超管凭证
修改控制中心超级管理员密码时，需要上传此凭证，此凭证具有有效期，下载后请尽快使用！(仅支持中心2.0.15.0及以上版本)
生成凭证

2. 备用中心配置工具


配置工具
备用中心状态
当前状态：
未注册
申请后，进入审核阶段，审核通过后将作为该中心的备用中心使用，现有数据将会覆盖
主中心地址：
https://
请输入主中心IP地址或域名
例：6080
主中心密钥：
请输入中心密钥
中心网络设置
控制中心地址：
全部IP
域名
HTTPS管理：
不启用安全证书
默认安全证书
其他安全证书
颁发对象：TrustAsia RSA DV TLS CA G2
颁发者：TrustAsia RSA DV TLS CA G2
截止日期：2025年8月30日星期六 19:06:01
证书详情
备用中心状态
中心网络设置
远程协助端口
数据库设置
文件存放
密钥与账号设置
提交申请
取消

字段		说明
备用中心状态	**当前状态**	显示当前备用中心的状态； 未注册：未申请成为任意主中心的备用中心或向主中心提交被拒绝时的状态； 审核中：主中心还未处理申请成为主中心的备用中心的申请时的状态； 已注册：申请成为主中心的备用中心的申请被主中心同意时的状态； 已注销：主中心删除了该备用中心时的状态；
	主中心地址	填写要连接的主中心的地址和端口；
	主中心密钥	填写要连接的主中心的密钥，可在主中心的配置工具中查看密钥；
其他字段信息参考主中心的配置工具		

3. 负载中心配置工具

字段		说明
负载中心状态	**当前状态**	显示当前负载中心的状态； 未注册：没有向主中心发起注册申请时的状态； 审核中：向主中心发起申请，等待主中心审核时，负载中心的状态； 拒绝注册：向主中心发起申请，但是被主中心审核拒绝时，负载中心的状态；

		已注册：向主中心发起申请，主中心审核通过时，负载中心的状态； 已注销：主中心删除了该负载中心时的状态；
	主中心地址	填写要连接的主中心的地址和端口；
	主中心密钥	填写要连接的主中心的密钥，可在主中心的配置工具中查看密钥；
负载中心配置	**数据缓存目录**	负载中心补丁文件，分发任务文件，升级文件的存储目录路径；
	管理端口	通过该端口访问负载中心的控制中心，端口默认为 8080；
	HTTPS 管理	设置是否使用 HTTPS 访问控制中心，单选； 不启用安全证书：使用 HTTP 访问控制中心； 默认安全证书（默认）：使用默认安全证书访问控制中心； 其他安全证书：自定义上传 Crt、Key 文件，使用自定义的安全证书访问控制中心；
	部署端口	通过该端口访问负载中心的终端部署页，默认 6080；

第三章 火绒终端安全管理系统-Windows终端

火绒终端安全管理系统安全终端作为安全防护功能执行终端，可以有效地帮助用户解决病毒、木马、流氓软件、恶意网站、黑客侵害等安全问题，为用户终端提供良好的运行环境。

3.1 首页

火绒安全终端首页为用户提供病毒查杀、版本更新、信任/隔离区功能快速访问入口以及当前终端版本、病毒库版本、当前连接中心（负载中心）信息。

3.1.1 病毒查杀

1. 全盘查杀

全盘查杀功能会针对计算机包括引导区、系统进程、启动项、服务与驱动、系统组件、系统关键位置和物理存储磁盘进行全方位查杀。全盘查杀功能查杀位置全面，覆盖面广，所以应用此查杀方式安全性将大大提升，但是用时较长。

用户单击【全盘查杀】即可对本地环境进行病毒全盘查杀。

（1） 停止：用户可手动停止病毒全盘查杀任务，点击【停止】按钮，弹出确认框中点击【确定】即可终止当前查杀任务，并将已扫描查杀的数据告知用户。

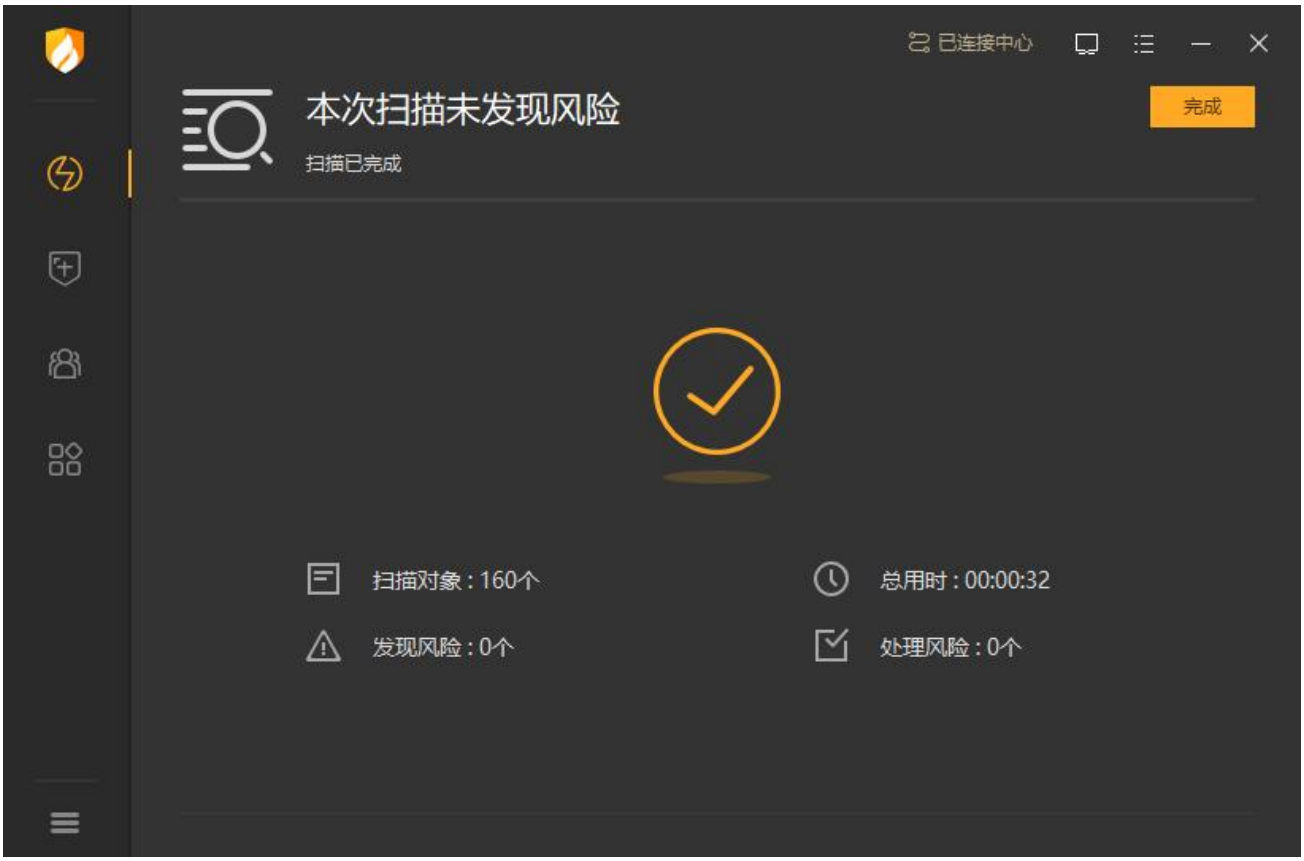
（2） 暂停：用户可暂停当前病毒查杀任务，点击【暂停】按钮，病毒查杀任务进入暂停状态，点击【继续】可继续当前查杀任务继续查杀，方便用户对当前任务进行管理。

（3） 常规：常规扫描模式下，病毒查杀任务会按照正常状态执行任务，不会特殊处理任务。

（4） 高速：高速扫描模式下，病毒查杀任务会提升优先级，增加系统资源调用以快速完成扫描任务。

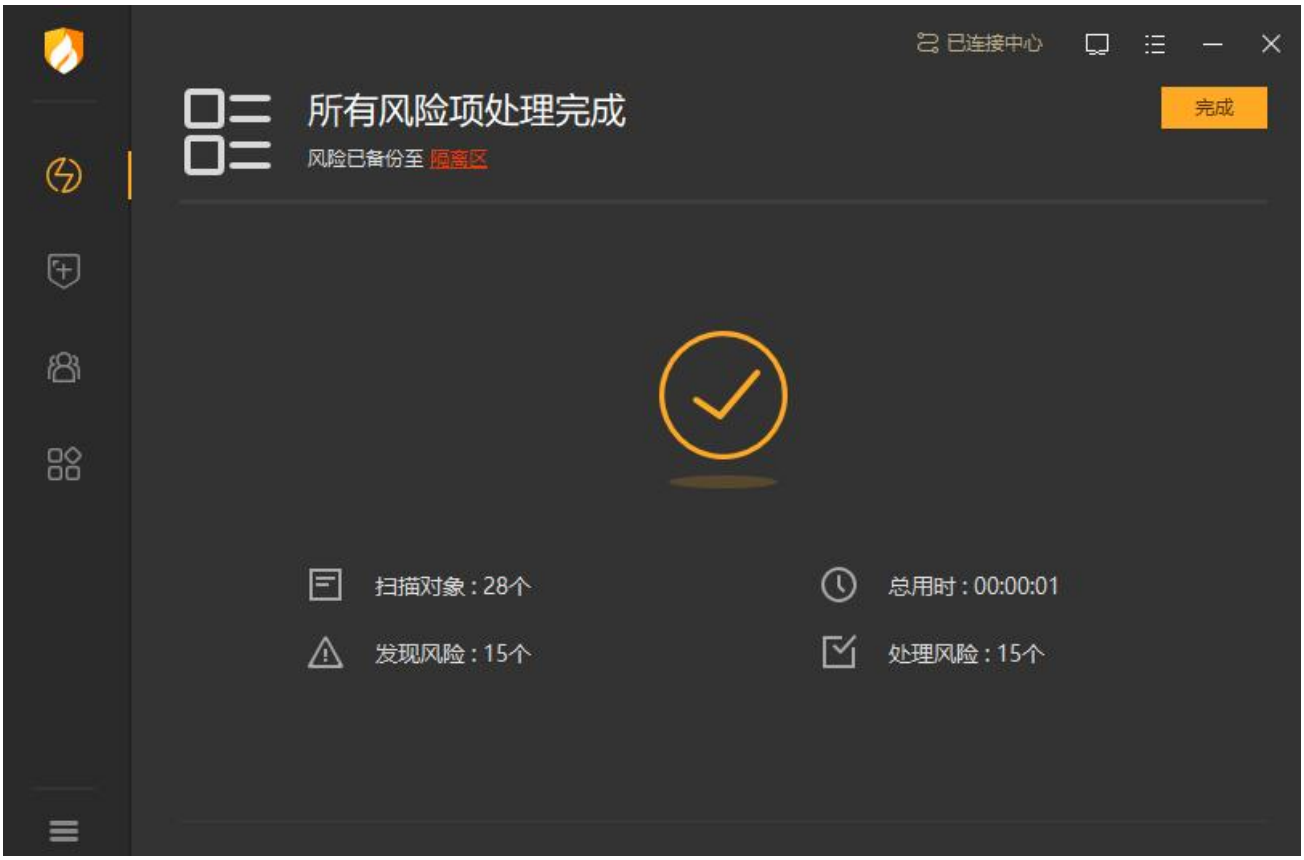
（5） 查杀完成后自动关机：勾选此项后，病毒查杀任务查杀完成之后，将自动关闭计算机。

病毒查杀任务执行完成后，如未发现任何风险项，将为用户展示当前扫描对象、任务耗时等扫描任务详情信息，用户单击【完成】按钮后会返回终端主界面。



病毒查杀任务执行完成后，如发现风险项目，则会将风险项目展示给用户，用户可自行选择清理或忽略风险项目。

点击【立即处理】后，终端将自动处理已勾选风险项，并为用户展示处理结果及扫描任务结果。



2. 快速查杀

快速查杀功能会针对计算机包括引导区、系统进程、启动项、服务与驱动、系统组件、系统关键位置这些敏感位置进行针对性查杀。快速查杀功能查杀位置相对全盘查杀较少，所以查杀速度较快。

用户单击【快速查杀】即可对本地环境进行病毒快速查杀。

快速查杀任务处理结果及展示与全盘查杀相同，详情请参见全盘查杀功能。

3. 自定义查杀

自定义查杀功能可自定义选择查杀位置，方便用户定点查杀指定存储目录，病毒查杀任务更加灵活。

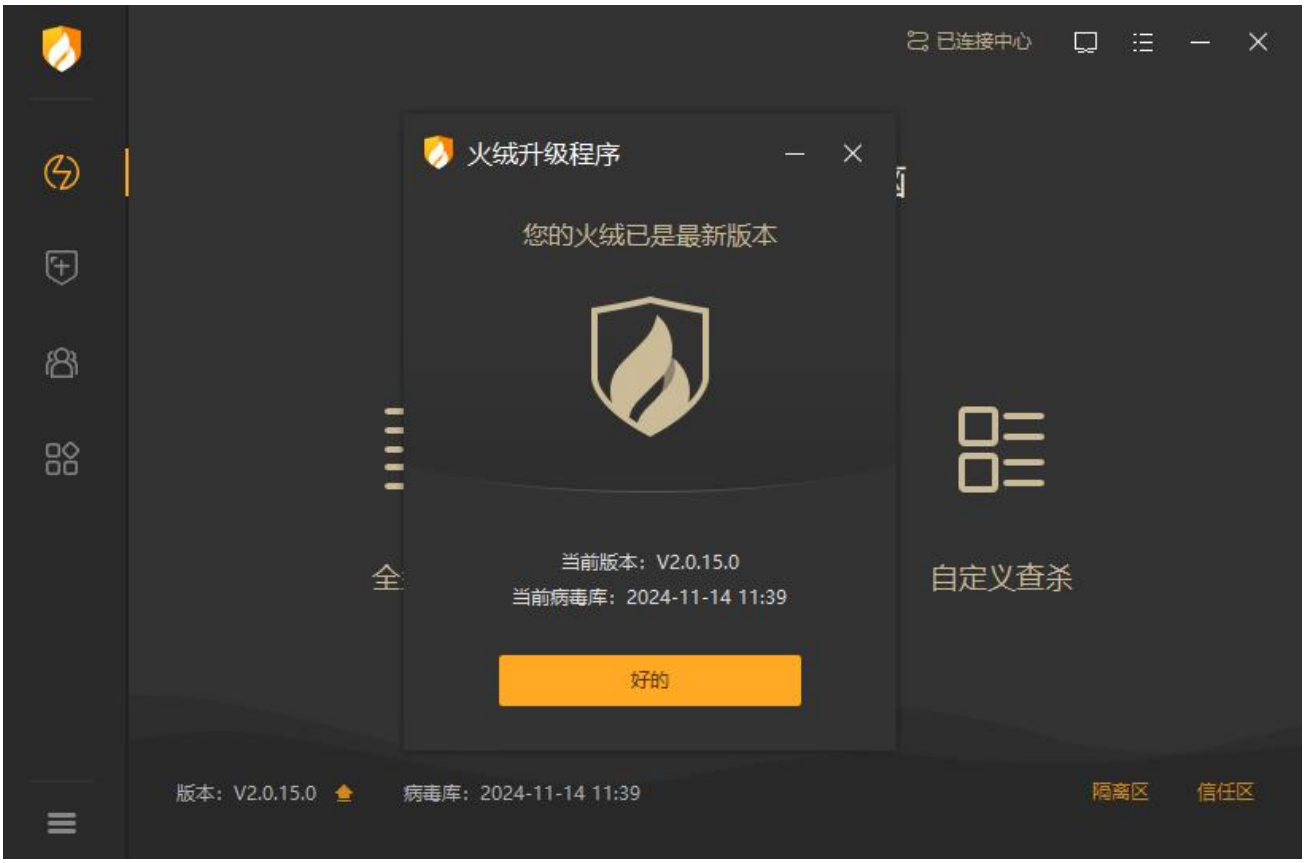
用户单击【自定义查杀】按钮，选择自定义查杀位置后单击【确定】即可对当前选择的查杀位置进行病毒查杀任务。

自定义查杀任务处理结果及展示与全盘查杀相同，详情请参见全盘查杀功能。

3.1.2 版本及更新

火绒安全终端首页提供了终端版本信息和病毒库版本信息展示，为方便用户手动检查终端版本，火绒安全终端也提供便捷版本更新检测入口。

用户点击版本信息后方升级按钮，终端会自动检测当前终端版本信息，如果检查到终端未更新至最新版本，会提示用户当前有新版本，用户可自行选择是否更新为当前检测到的最新版本。



3.1.3 信任/隔离区

火绒安全终端首页提供了信任/隔离区快捷访问入口，方便用户快速查看及管理当前已信任及已隔离的文件。

1. 隔离区

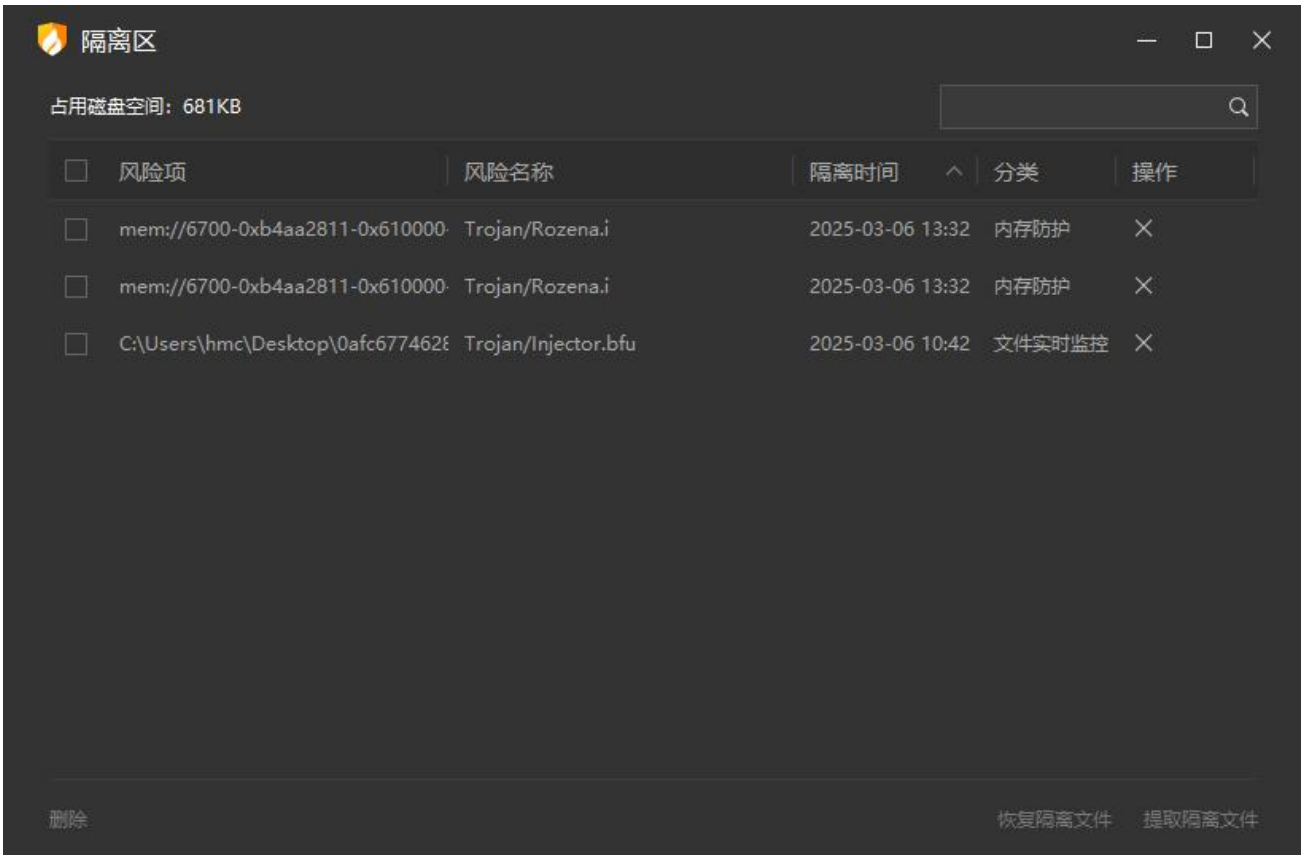
火绒安全终端会将扫描处理过的病毒威胁文件，经过加密后备份至隔离，以便您有特殊需要，可以主动从隔离区中重新找回被处理过的威胁文件。

用户单击火绒安全终端首页右下角【隔离区】弹出文件隔离区弹框，用户可查看当前隔离区隔离的所有风险文件。

（1） 删除：用户选中隔离区中的文件，单击左下角【删除】按钮，即可删除当前隔离区保存的风险文件样本。

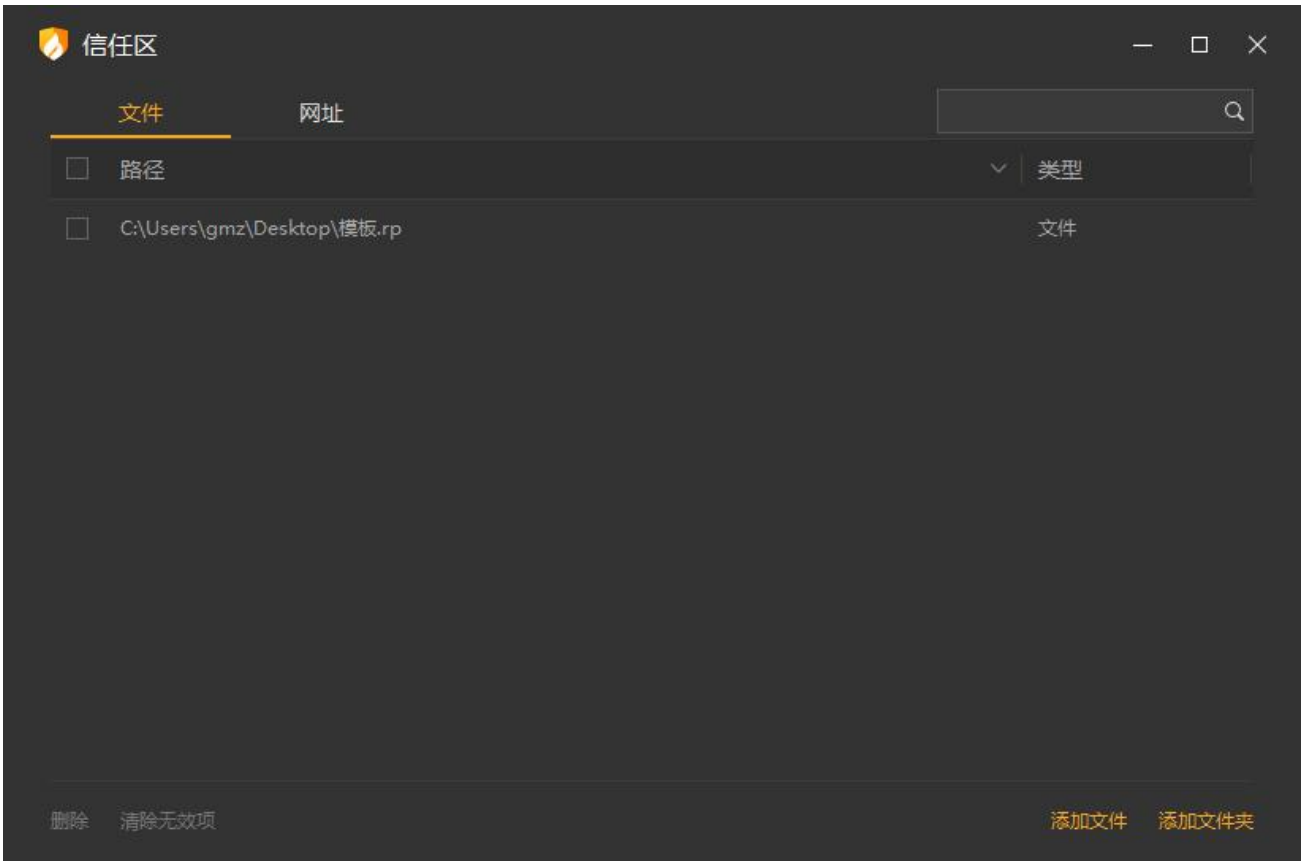
（2） 恢复：用户选中隔离区中的文件，单击右下角【恢复】按钮，即可恢复当前风险样本状态，不再隔离。

（3） 提取：用户选中隔离区中的文件，单击右下角【提取】按钮，即可提取当前风险样本至指定目录。



2. 信任区

火绒安全终端提供信任文件添加管理功能，用户确认安全的文件，不希望杀毒软件查杀的文件，可以添加信任，此列表中的文件或文件夹不会被病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、Web 扫描功能扫描。信任区支持增加文件、文件夹与网址进行信任，同时支持对已信任的文件取消信任。



3.2 防护中心

火绒安全终端支持提供查看、管理当前终端各项安全防护功能的启用情况。

用户可手动变更功能开启状态（管理员如果开启了管理员密码保护，改变功能防护状态前需要先输入管理员设定的保护密码）。

用户点击安全防护类型名称，可进入防护详情界面查看及编辑当前防护设置项（管理员如果开启了管理员密码保护，改变功能防护状态前需要先输入管理员设定的保护密码）。

3.2.1 病毒防御

1. 文件实时监控

文件实时监控将在文件执行，修改或者打开时检测文件是否安全，即时拦截病毒程序。在不影响电脑正常使用的情况下，实时保护用户的终端不受病毒侵害。

2. 恶意行为监控

恶意行为监控通过监控程序运行过程中是否存在恶意操作来判断程序是否安全。

注：增强勒索病毒防护：开启该功能后，火绒安全软件会在系统盘符下创建两个具有隐藏属性的随机名文件目录，随机名文件目录里会有若干常见文件格式的随机文件，防护系统使用这些随机文件来诱捕勒索病毒，达到增强防护的目的。

3. 内存防护

内存防护功能主要针对无文件攻击类型的病毒，可及时发现并阻止内存中的恶意代码。

4. U 盘保护

U 盘保护功能会在 U 盘接入电脑时对其进行快速扫描，及时发现并阻止安全风险，避免病毒通过 U 盘进入您的电脑。

5. 下载保护

在您使用浏览器、下载软件、即时通讯软件进行文件下载时，下载保护会实时对所有从网络下载至终端中的文件进行病毒扫描，保护您的终端安全。

6. 邮件监控

邮件监控会对所有接收的邮件进行扫描，当发现风险时，将会自动打包风险邮件至隔离区，并发送一封火绒已处理的回复邮件。对于发送的邮件，若发现邮件中包含病毒，火绒直接将终止您的邮件发送，并自动清除病毒邮件至隔离区，防止病毒传播。

7. Web 扫描

当有应用程序与网站服务器进行通讯时，Web 扫描功能会检测网站服务器返回的数据，并及时阻止其中的恶意代码运行。

3.2.2 系统防御

1. 系统加固

系统加固功能根据火绒提供的安全加固策略，当程序对特定系统资源操作时提醒用户可能存在的安全风险。

可以通过添加自动处理规则的方式，在某些程序触发系统加固规则时，自动进行处理，当中心开启允许终端添加自动处理规则，终端可以添加自定义处理规则，否则，统一使用中心管理员添加的自动处理规则。

2. 应用加固

应用加固功能通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用。

3. 软件安装拦截

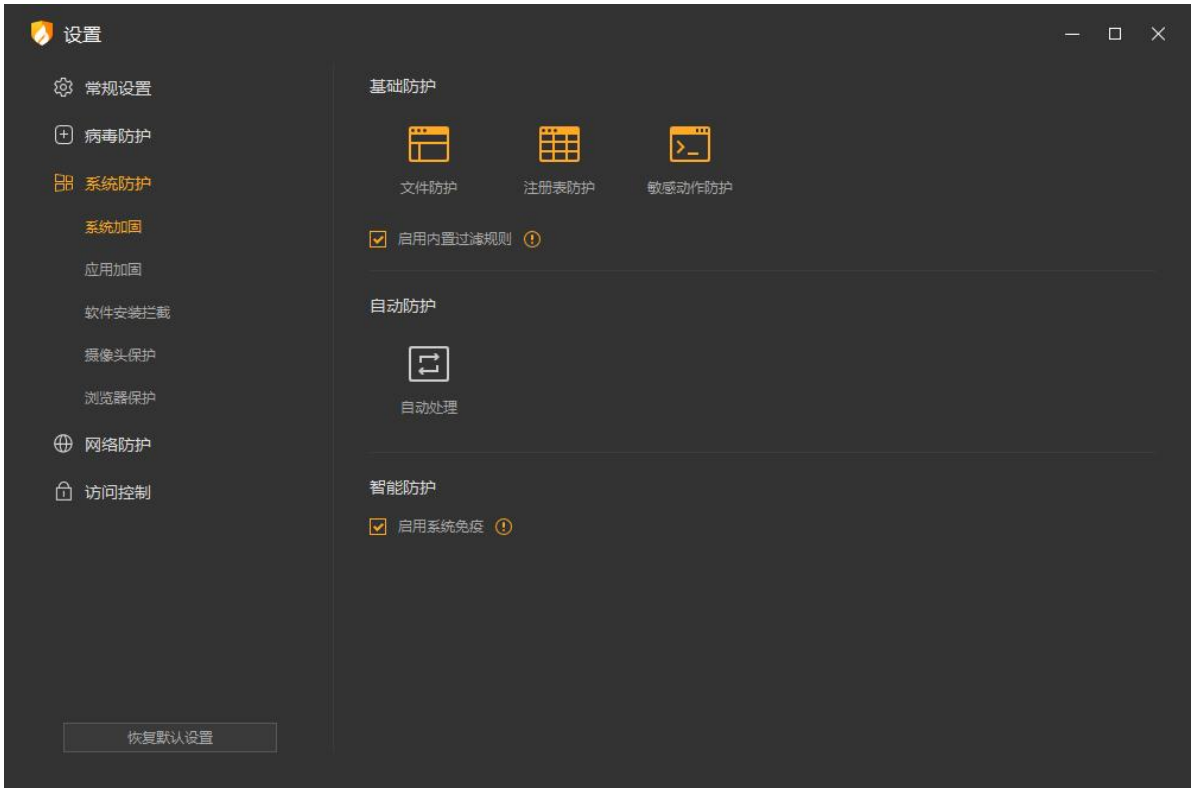
软件安装拦截功能会依据用户反馈搜集被恶意推广过的软件，并在其安装时提示您，以阻止流氓软件恶意推广，静默安装软件的行为。软件安装拦截能有效的阻止您在不知情的情况下终端自动安装无关软件。

4. 摄像头保护

火绒摄像头防护会在有任意终端软件要启用您的摄像头时弹窗提示您，您可以根据需要选择是否允许程序启用摄像头。

5. 浏览器保护

浏览器保护能锁定您的浏览器主页不被任意程序篡改。



3.2.3 网络防御

1. 网络入侵拦截

网络入侵拦截将检测网络传输的数据包中是否包含恶意攻击代码，通过中断这些数据包传输以避免您的电脑被黑客入侵。

2. 横向渗透防护

横向渗透防护可以对远程 DCOM 调用、远程 MMC 调用、远程打印机添加、远程注册表篡改、远程服务创建、默认共享访问、远程计划任务创建、远程 WMI 调用这几种行为进行拦截，防止电脑中的病毒进行横向传播。

3. 对外攻击检测

对外攻击拦截将检测您电脑外联的数据包中是否包含恶意攻击代码，通过中断这些数据包传输以阻止您的电脑被黑客利用。

4. 僵尸网络防护

僵尸网络防护将检测网络传输的数据包中是否包含远程控制代码，通过中断这些数据包传输以避免您的电脑被黑客远程控制。

5. Web 服务保护

黑客可能会对安装了服务器软件的终端发起攻击，以入侵服务器，窃取隐私数据，甚至篡改支付信息等危险行为，对您造成一些不必要的损失。Web 入侵防护能全方位保护您计算机的服务器软件，主要从数据库、Web 服务器、Web 应用、Web 后门四个方面对安装有服务器软件的计算进行强力保护。

6. 暴破攻击防护

不法分子常常通过暴力破解登录密码等其他密码破解攻击获取密码进行远程登录。一旦远程登录进入主机，用户可以在权限允许范围内肆意操作主机。

7. 远程登录防护

开启后终端将自动阻止所有远程登录行为，如有需要可在设置中加白名单，以放过信任 IP 的远程登录。

8. 恶意网址拦截

当您在浏览网页的时候，访问到有恶意风险的网站，火绒将拦截网站并弹出提示。

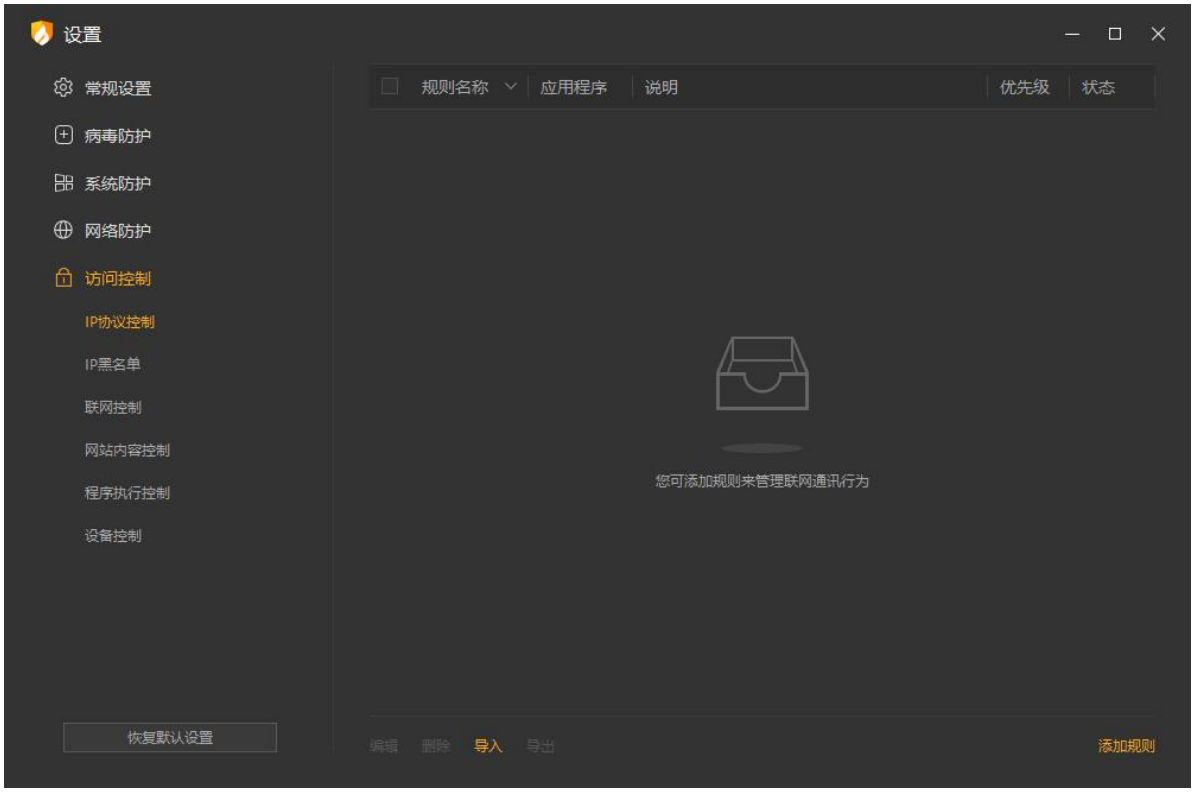
3.3 访问控制

火绒安全终端提供针对 IP 协议层访问控制、计算机应用程序执行与网络访问、设备控制等功能的查看与细节配置。

3.3.1 IP 协议控制

在 IP 协议层控制数据包进站、出站行为，并且针对这些行为做规则化的控制。需用户或管理员手动配置对应规则，当发现有触发 IP 协议控制规则的操作时，火绒可根据用户设置的规则放过或阻止。

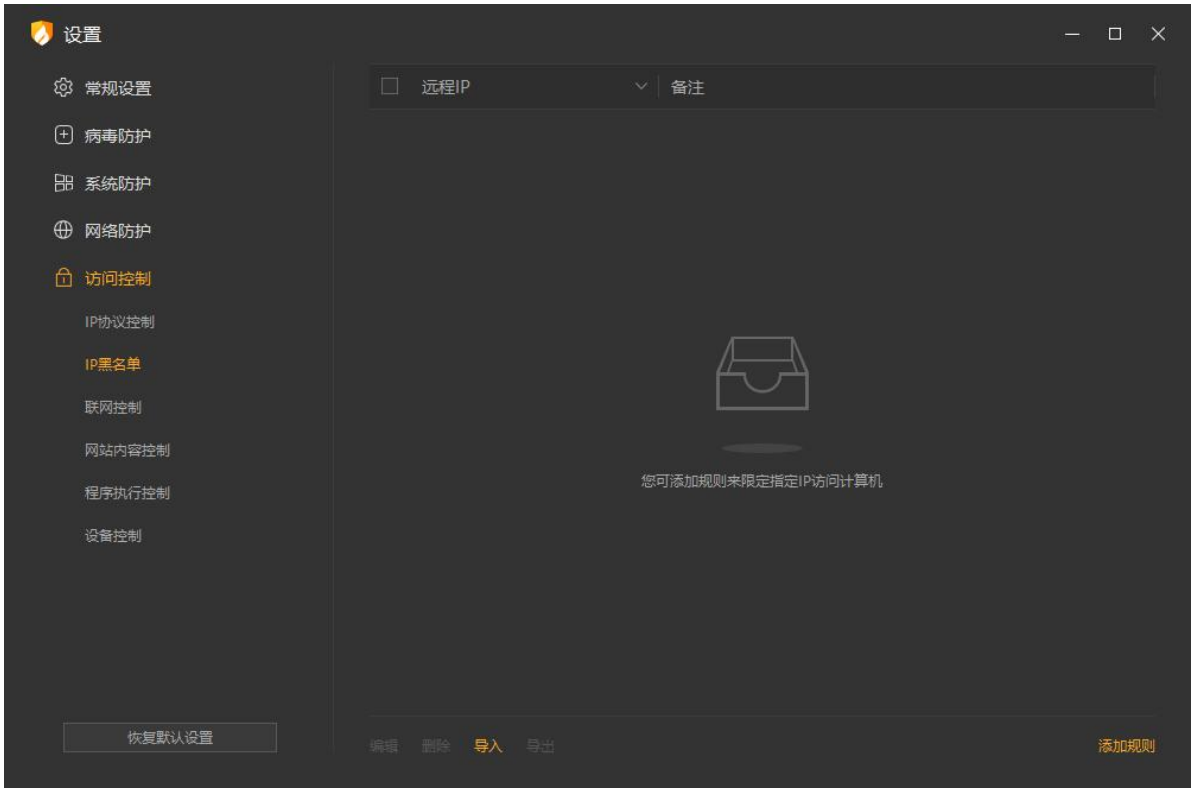
用户可导出当前配置或将历史配置导入后直接使用，点击【添加规则】可添加新规则，选中当前列表已有规则，可进行编辑或删除操作。



3.3.2 IP 黑名单

当终端有不受欢迎的 IP 访问时，用户可以添加这些 IP 加入 IP 黑名单中，以阻止这些 IP 的访问。

用户可导出当前配置或将历史配置导入后直接使用，点击【添加规则】可添加新规则，选中当前列表已有规则，可进行编辑或删除操作。



3.3.3 联网控制

当用户需要阻止某程序联网，或者希望自行管控电脑中所有程序是否联网时，您可以通过联网控制功能很好地管控电脑程序的联网行为。该功能默认不启用，开启后每当有任意程序进行联网时，联网控制都会弹出弹窗提示，建议您根据需要决定是否开启此功能。用户也可手动配置对应规则，自动放行或阻止对应程序的联网行为。

1. 规则外程序联网

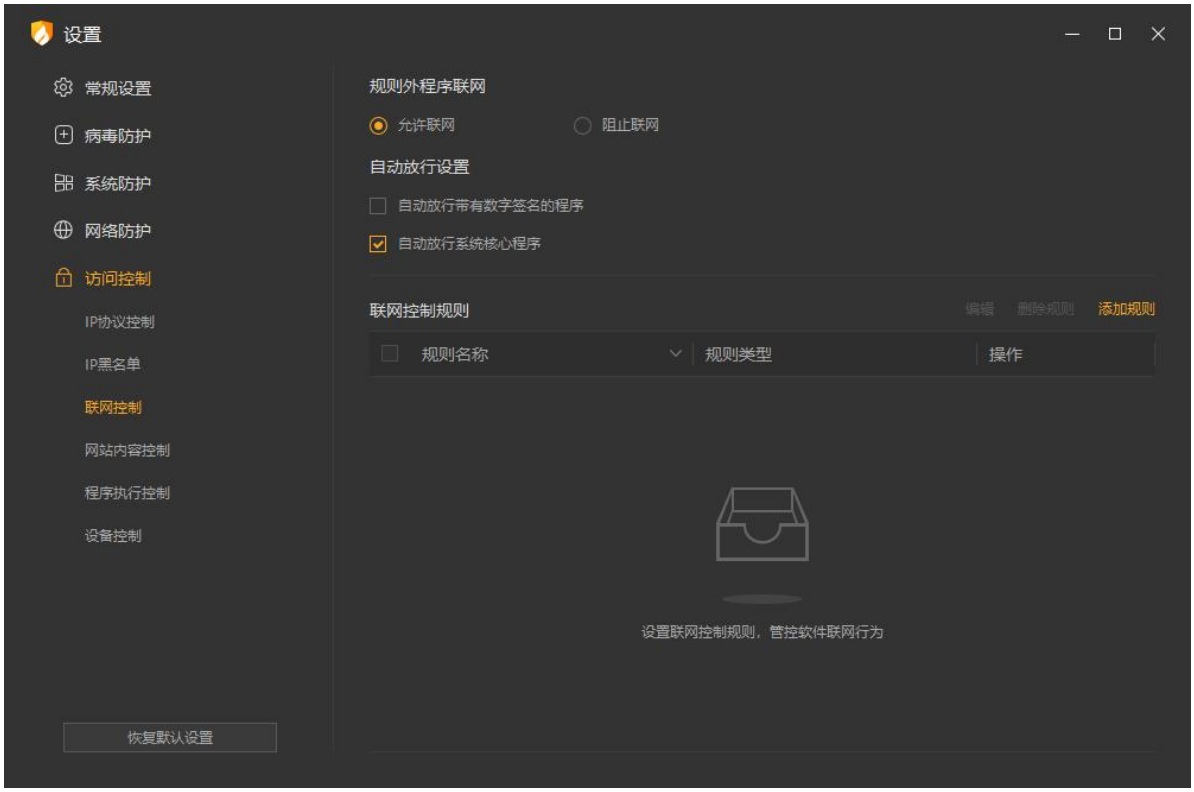
   用户可选择是否允许规则之外的程序的联网动作。

2. 自动放行设置

   用户可设置自动放行的范围。

3. 联网控制规则

   用户可手动添加规则，也可对已有规则进行编辑或删除。



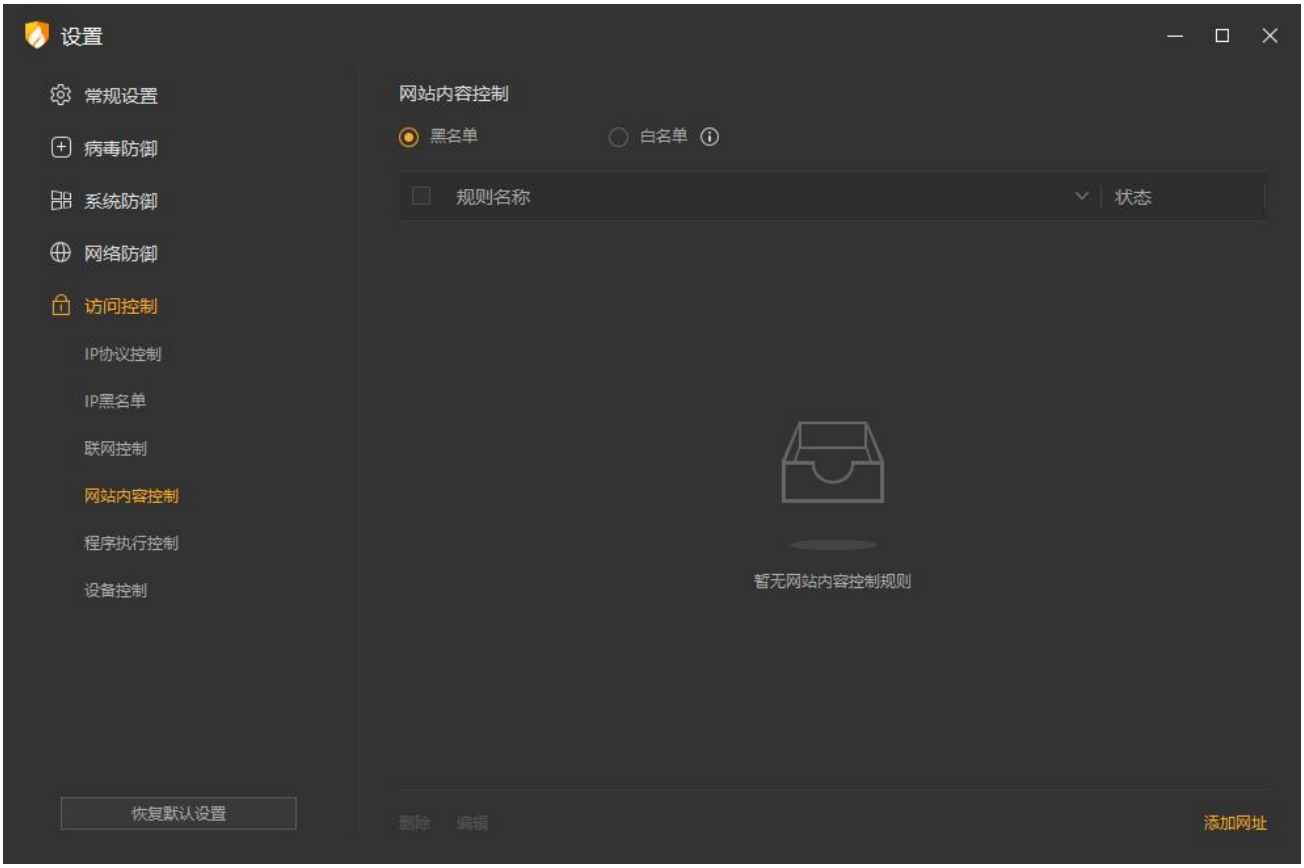
3.3.4 网站内容控制

用户需要限制终端访问某些网站时，可添加网站进行访问内容限制，支持限制 http/https 协议的网址。

用户点击【添加拦截网址】可添加规则，也可对已有规则进行编辑和删除。

网站控制名单的属性分为黑名单和白名单，默认选择黑名单，此时终端将无法访问名单中网址，名单外的网址可以正常访问；当属性为白名单时，此时终端用户仅能访问名单中的网址，名单外的网址无法访问；

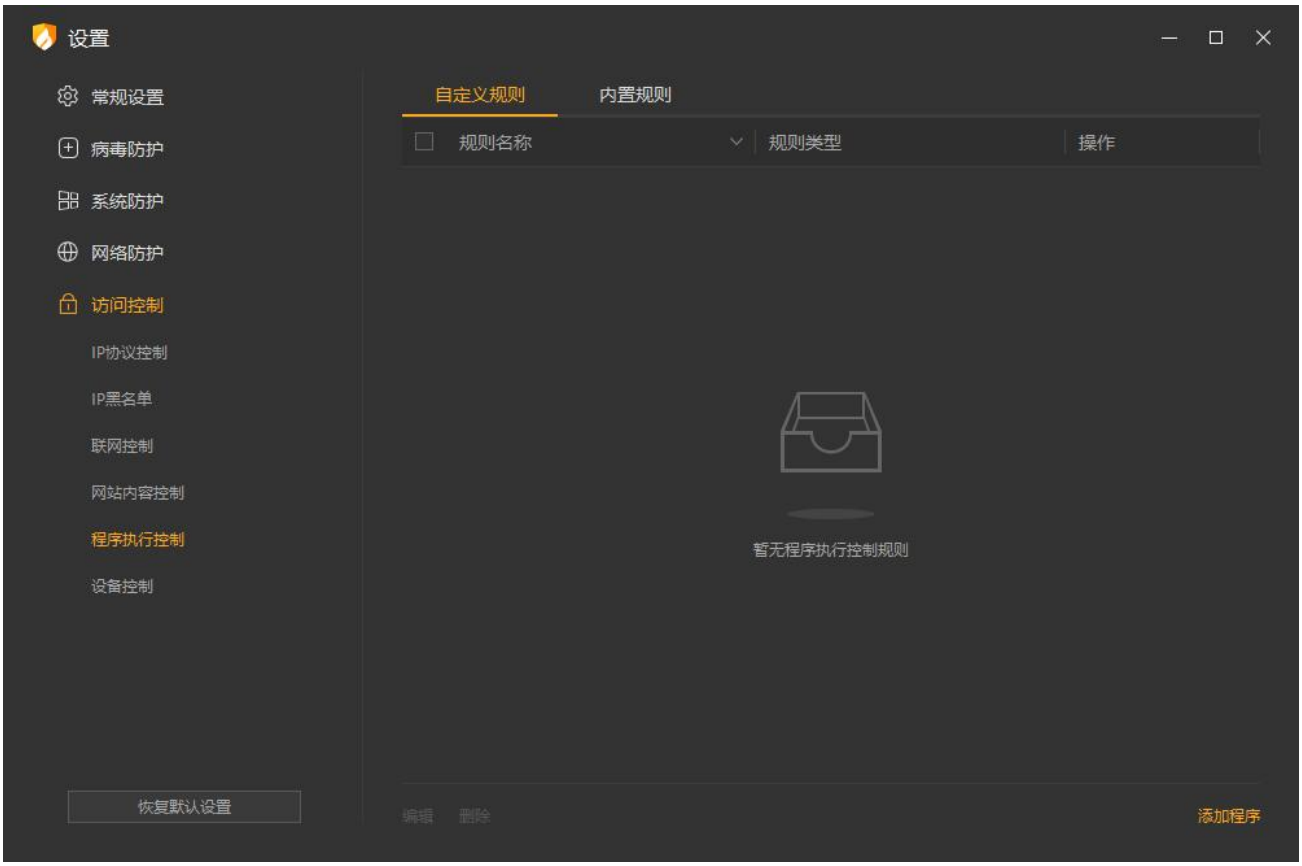
（注：以火绒为例，黑名单模式规则中设置了 https://www.huorong.cn 时，将仅拦截一级域名为“huorong.cn”子域名为“www”或无子域名的网址；规则中设置的 https://huorong.cn 时，将拦截一级域名为“huorong.cn”的所有网址）



3.3.5 程序执行控制

可根据用户需要设置对应规则以限制某个或某类程序在终端中执行和使用。

用户可点击【添加程序】可添加规则，也可对已有规则进行编辑和删除。



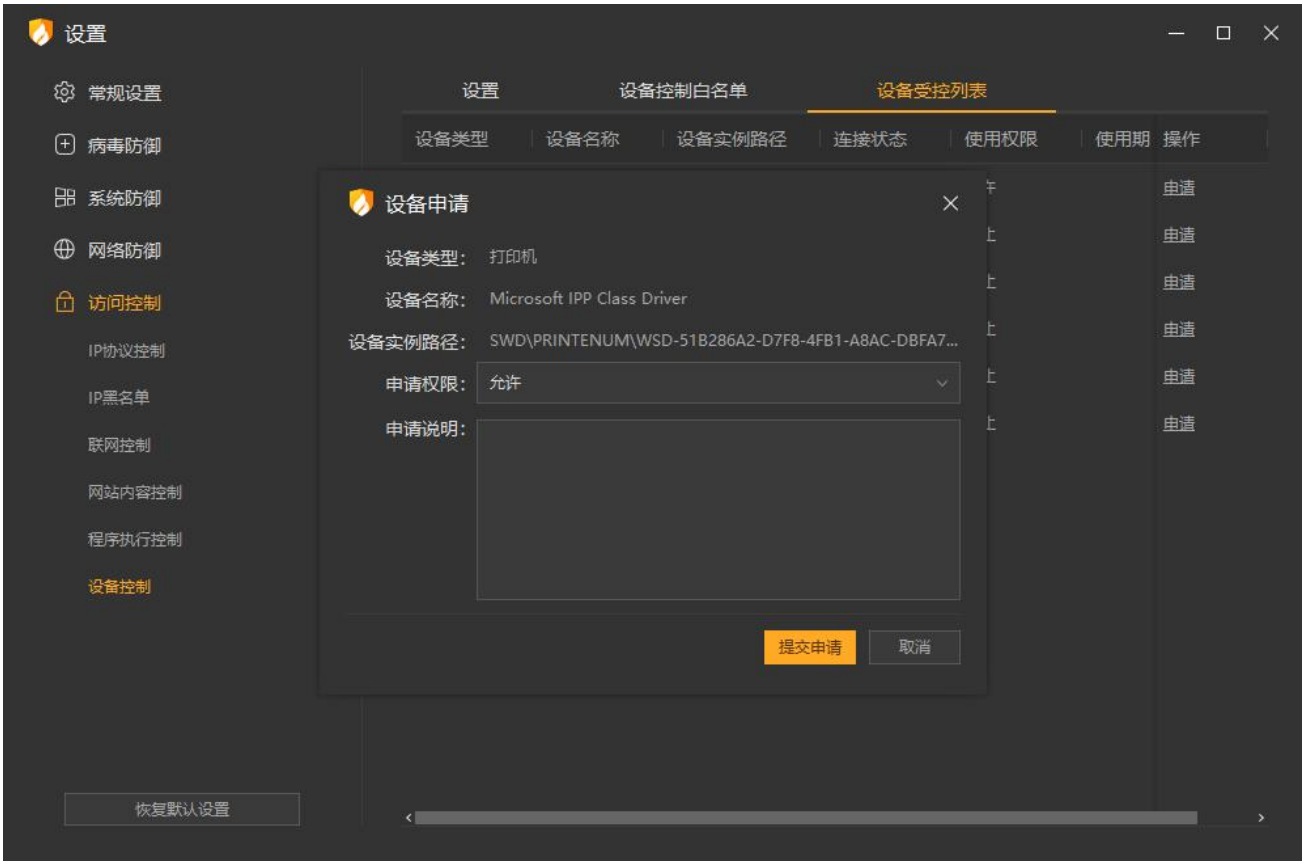
3.3.6 设备控制

控制设备是否可在计算机上运行使用。当前支持的设备类型有：U 盘设备、便携设备、USB 无线网卡、USB 有线网卡、打印机、光驱、蓝牙。

支持设置设备控制白名单，对某些设备进行放过处理。

用户可对现有支持的设备进行控制状态选择。

设备受控列表显示该终端被设备控制禁用的所有设备，终端用户可以自行申请使用设备，点击操作列【申请】按钮，填写申请说明后，向控制中心提交使用申请。



中心管理员审批通过后，设备使用权限会改变，终端用户可以使用该设备。

3.4 安全工具

火绒安全终端提供了 9 种安全工具，帮助终端用户更方便的使用以及管理终端电脑，用户可根据需要自行运行使用，为终端的环境安全保驾护航。

3.5 终端信息

火绒安全终端提供用户查看当前终端状态便捷入口，用户点击右上角【终端信息】图标，可查看当前终端的终端名称、IP、MAC 地址等计算机基础信息，以及火绒终端版本、病毒库版本、与中心连接状态、已连接的主中心地址和负载中心地址等信息。

3.6 更多功能

火绒安全终端提供了包括安全设置、安全日志、隔离区、信任区、语言设置、检查更新、联系网管、关于我们 8 种功能便捷访问入口，用户点击右上角【更多功能】按钮，可出现功能下拉菜单栏，点击可进入对应功能弹框界面。

3.6.1 安全设置

用户可点击【安全设置】打开设置，在设置中可对终端升级、弹窗显示、防御功能的细节规则调整进行自定义配置。

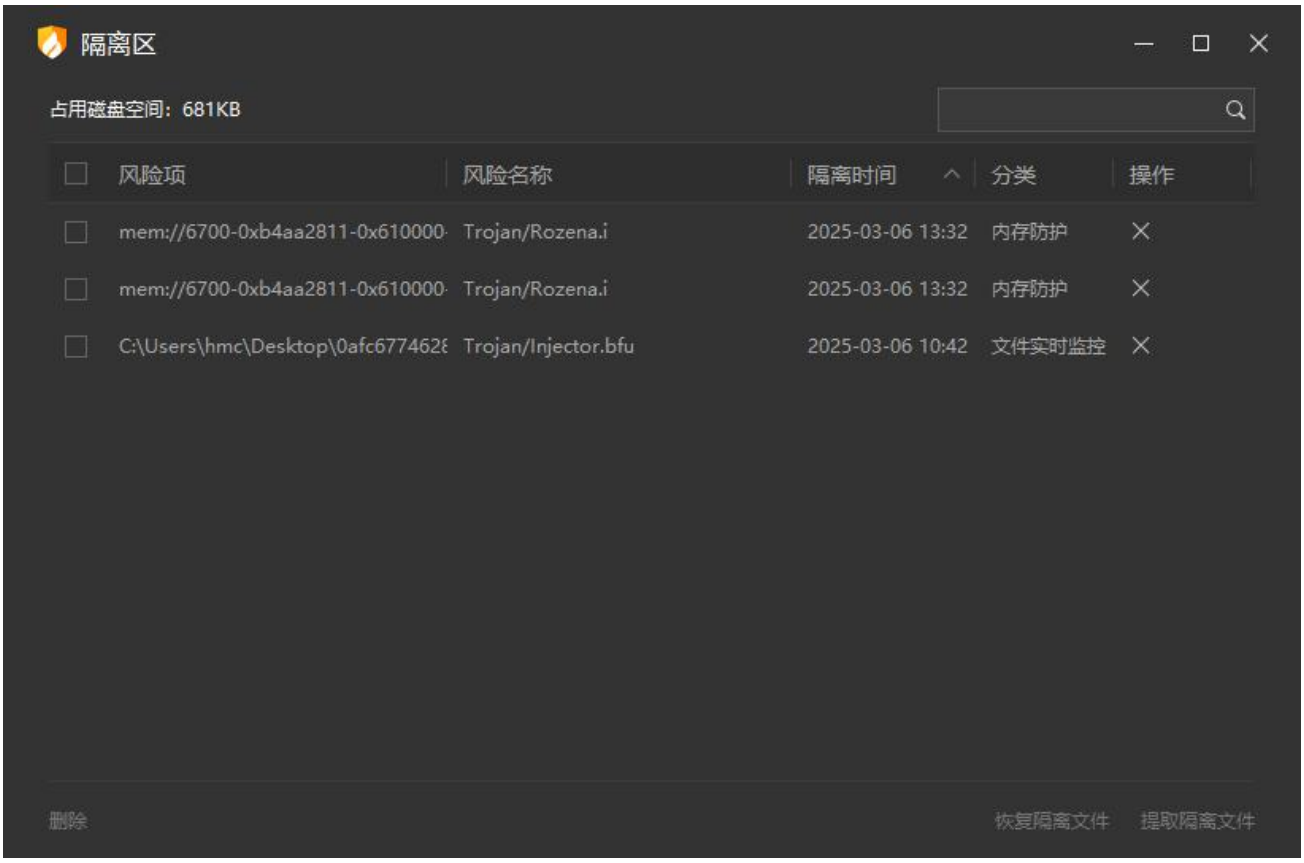
3.6.2 安全日志

用户可点击【安全日志】打开日志弹框，默认显示当天的日志信息，支持用户通过日期和模块筛选日志。可手动刷新日志信息，也可清除本页日志（中心策略为禁止清除日志时，终端用户不可清除日志）或将本页日志导出为独立文件。

3.6.3 隔离区

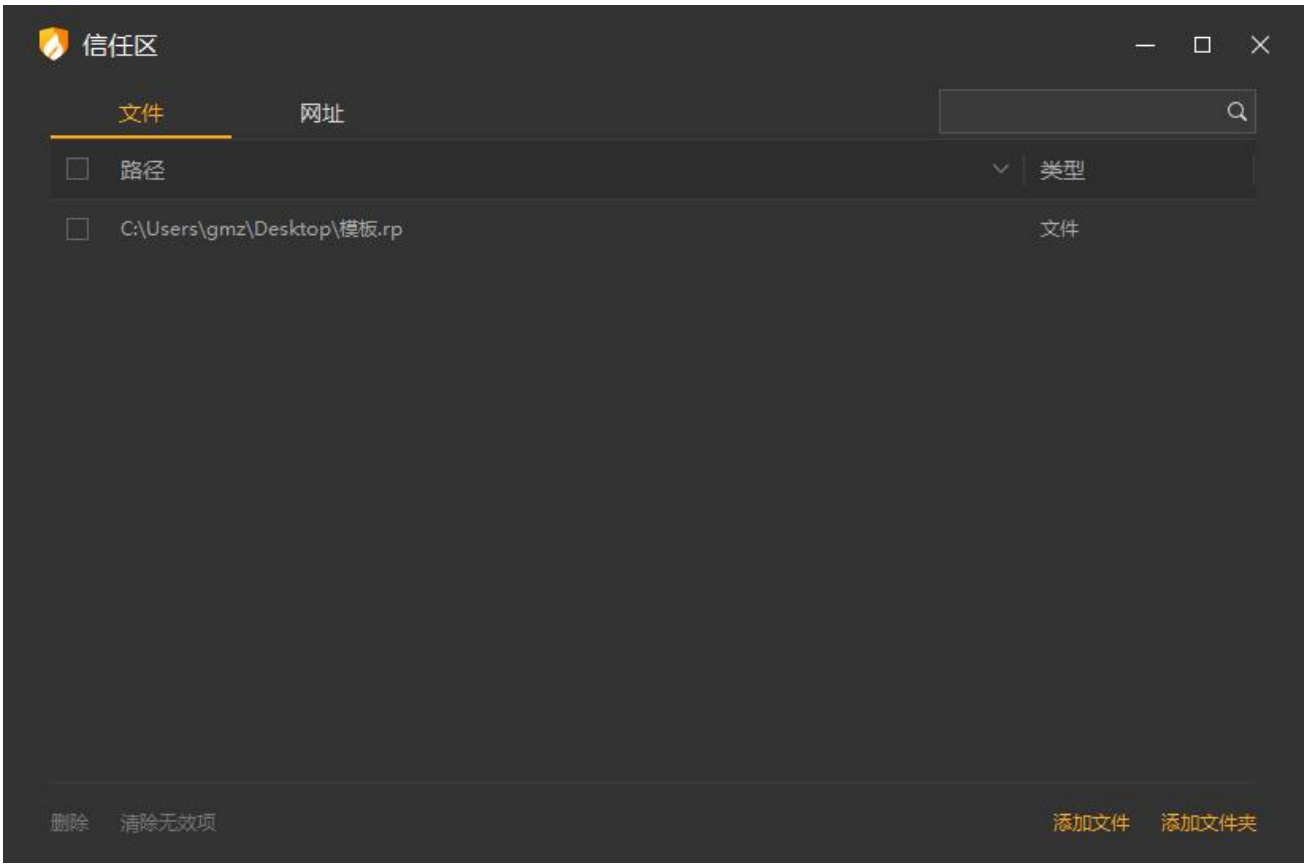
火绒安全终端会将扫描处理过的病毒威胁文件，经过加密后备份至隔离，以便您有特殊需要，可以主动从隔离区中重新找回被处理过的威胁文件。

用户可点击【隔离区】弹出文件隔离区弹框，用户可查看当前隔离区隔离的所有风险文件。



3.6.4 信任区

火绒安全终端提供信任文件添加管理功能，用户确认安全的文件，不希望杀毒软件查杀的文件，可以添加信任，此列表中的文件或文件夹（包含下级文件夹）不会被病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、Web 扫描功能扫描。信任区支持增加文件、文件夹与网址进行信任，同时支持对已信任的文件取消信任。

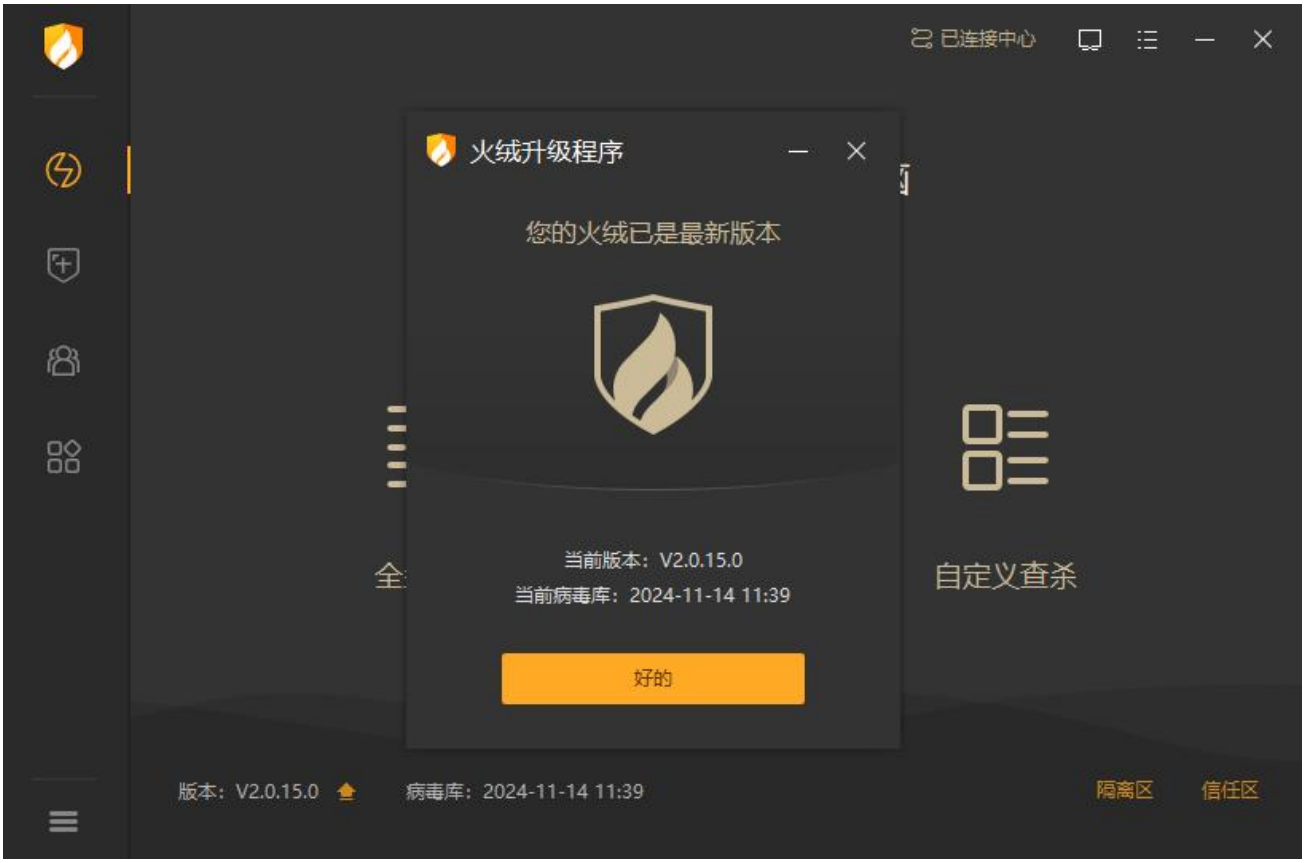


3.6.5 语言设置

火绒安全终端支持语言切换，可切换简体中文、繁体中文及英文。

3.6.6 检查更新

用户点击检查更新后，终端会自动检测当前终端版本信息，如果检查到终端未更新至最新版本，会提示用户当前有新版本，用户可自行选择是否更新为当前检测到的最新版本。

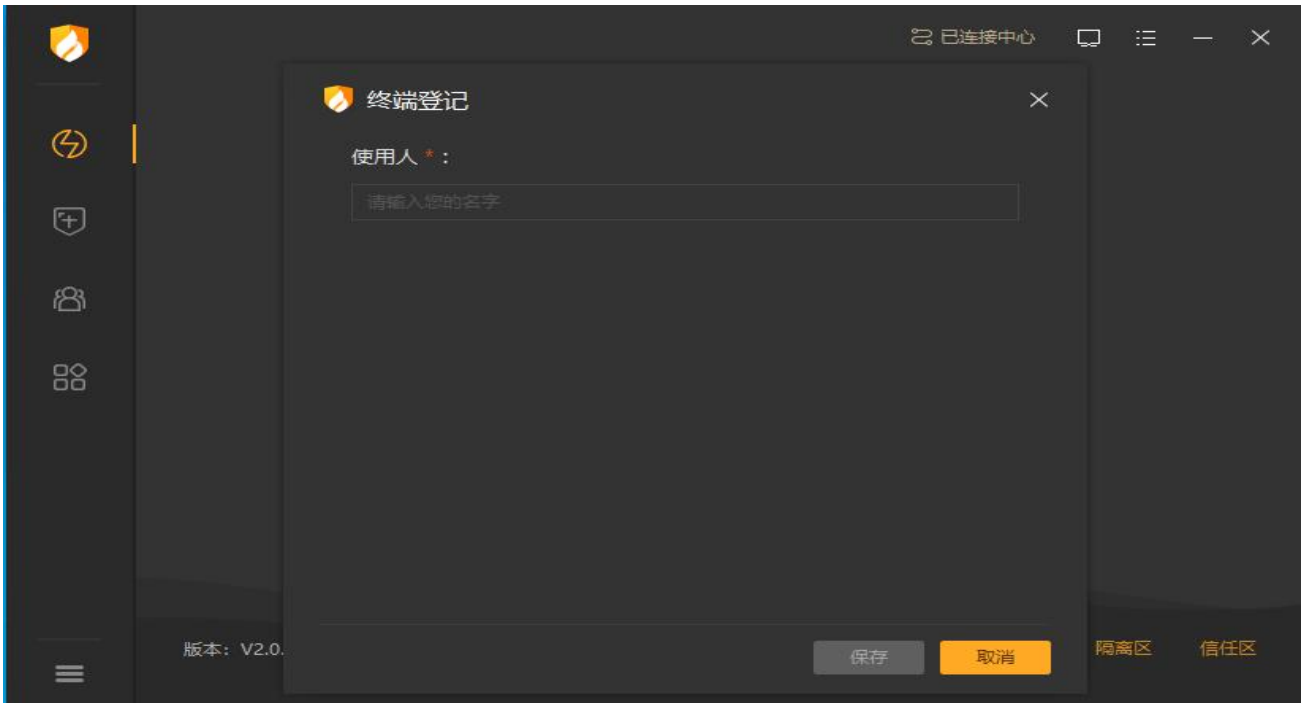


3.6.7 联系网管

火绒安全终端提供获取管理员联系方式功能，管理员在中心编辑完成管理员联系方式后，安全终端可点击【联系网管】查看管理员联系方式。

3.6.8 终端登记

火绒安全终端提供自助登记功能，管理员开启用户自助登记功能后，用户可以在终端设置中点击【终端登记】查看或填写登记信息。



3.6.9 关于我们

火绒安全终端提供关于火绒版权信息查看，用户可点击【关于我们】查看火绒的版权信息。

第四章 火绒终端安全管理系统-Linux 服务器版终端

用户可在 TUI 界面中查看火绒安全终端配置及状态信息，获取命令行操作帮助，修改配置项，本地进行扫描查杀，还可以对隔离区的文件进行恢复或删除操作，支持查看终端升级日志和扫描日志。

4.1 查看帮助信息

如需获取终端控制台帮助信息，需运行命令 hrconsole --help

示例如下：

```
root@ubuntu-s:/usr/local/huorong/bin# ./hrconsole --help
hrconsole --help

Huorong Endpoint Security Management System Client for Linux Server
Console
Copyright (c) Huorong Corporation. All rights reserved.

Usage: hrconsole [-h | --help]
                 <command> [<args>]

These are common hrconsole commands:

  stat            Endpoint status.

  scan            Create scan task.
    --full
      Runs a full scan checks all files on you PC for threats.
    --quick
      Runs a quick scan checks your PC for threat activity in its
      processes, critical files, and other susceptible areas.
    <path>
      Checks <path> files for threats.

  --help
    Show this message.
```

该内容显示了火绒安全终端的版权说明信息，以及如何查看终端状态和如何发起本地扫描任务。

想要在终端控制台查看火绒终端配置帮助信息，运行命令 hrconfig --help，即显示相关帮助信息。

示例如下：

```
root@ubuntu-s:/usr/local/huorong/bin# ./hrconfig --help
hrconfig
Huorong Endpoint Security Management System Client for Linux Server
Configuration Management Tools
Copyright (c) Huorong Corporation. All rights reserved.

Usage: hrconfig [Options...] <KeyName>=<Value>

Options:
    --all    Show all config.
    --set    Set config value.
    --get    Get config value.

KeyName:
  server.address=<URL>
    Server address.

  server.policy-sync=<true|false>
    Default value is true. If true, the endpoint automatically synchronizes policy.

  update.automatic=<true|false>
    Default value is true. If true, the endpoint is automatically upgraded.

  update.database-only=<true|false>
    Default value is false. If true, update only the malware definitions.

  scan.auto-clean=<true|false>
    Default value is false. If true, automatically clean malware when it is detected.

  scan.quarantine=<true|false>
    Default value is true. If true, quarantine malware before clean it.

  scan.unzip=<true|false>
    Default value is true. If true, the full scan detects the files in the compressed package.

  scan.unzip-limit=<size>
    Unzipped file limit for full-scan.The limit size in megabytes. Files that exceed the limit size will not be scanned.
      <size> default value is 20, maximum value is 9999 and minimum value is 20.

  scan.network-drive=<true|false>
    Default value is false. If true, network drives are scanned during a full scan.

  scan.exclude-file-extensions=<file extensions>
    Default value is empty. No scan specified file extensions.For example, input ".gz;jpg" to exclude ".gz" and ".jpg" files.

  filemon.enabled=<true|false>
    Default value is true. If false, realtime file monitoring will not be available for monitoring the specified file path.

  filemon.auto-clean=<true|false>
```

4.2 查看终端状态

查看当前终端运行状态，需使用命令 hrconsole stat，使用 ctrl+c 退出查看状态。

状态信息中显示火绒安全终端的版权说明，该终端连接的控制中心地址及连接状态，终端版本信息，终端名称、终端分组、终端的 IP 地址及 MAC 地址，以及终端防护策略是否同步等。

示例如下：

```
Huorong Endpoint Security Management System Client for Linux Server
Console
Copyright (c) Huorong Corporation. All rights reserved.

Server : https://192.168.6.236:6080/
Connection Status : Connect

Version : 2.0.11.0
Definition : 2024-07-17 02:05
Client Name : ubuntu-s
Group Name : 未分组终端
IP : 192.168.6.173
MAC : 00-1C-42-E8-9B-DA
Policy-Sync : Yes
```

4.3 发起本地扫描任务

支持本地发起扫描任务，命令为：

全盘查杀：hrconsole scan --full

快速查杀：hrconsole scan --quick

自定义查杀：hrconsole scan /usr/bin

扫描任务开始后，显示扫描过程，扫描结束后，显示扫描的结果，扫描过程中使用 ctrl+q，将会终止扫描，显示已扫描对象的扫描结果，使用 enter 键可以暂时中止或恢复扫描。

如下图所示，以快速查杀为例：

扫描任务显示终端的基本信息及扫描任务信息，实时显示扫描任务的进度。

```
Huorong Endpoint Security Management System Client for Linux Server
Console
Copyright (c) Huorong Corporation. All rights reserved.

Server : https://192.168.6.236:6080/
Connection Status : Connect

Version : 2.0.11.0
Definition : 2024-07-17 02:05
Client Name : ubuntu-s
Group Name : 未分组终端
IP : 192.168.6.173
MAC : 00-1C-42-E8-9B-DA
Policy-Sync : Yes

Scan Task ========================
Task Type : Full Scan
Task Creator : Local User
Scan Mode : Regular-Speed
  Press F2 change scan mode.
Start Time : 2024/07/22 00:27:28
Task Status : Scanning
Scan Path : /usr/lib/snapd/snap-repair
[=======================================>                                                                    ] 26.72%

Press Ctrl+q to end the task. Press Enter to pause or resume the task.
```

扫描完成后，显示扫描的结果，使用 ctrl+c 退出扫描任务的查看状态。

```
Huorong Endpoint Security Management System Client for Linux Server
Console
Copyright (c) Huorong Corporation. All rights reserved.

Server : https://192.168.6.236:6080/
Connection Status : Connect

Version : 2.0.11.0
Definition : 2024-07-17 02:05
Client Name : ubuntu-s
Group Name : 未分组终端
IP : 192.168.6.173
MAC : 00-1C-42-E8-9B-DA
Policy-Sync : Yes

Scan Task ========================
Task Type : Full Scan
Task Creator : Local User
Start Time : 2024/07/22 00:27:28
Task Status : Completed
Duration : 00:03:29
Object(s) : 35585
File(s) : 30376
Threat(s) : 0
Cleaned : 0
```

4.4 查看终端配置

如需查看当前终端所有配置项，命令为：hrconfig –all

示例如下：

```
root@ubuntu-s:/usr/local/huorong/bin# ./hrconfig --all
server.address="https://192.168.6.236:6080/"
server.policy-sync=true

update.automatic=true
update.database-only=false

scan.auto-clean=false
scan.quarantine=true
scan.unzip=true
scan.unzip-limit=20
scan.network-drive=false
scan.exclude-file-extensions=""

filemon.enabled=true
filemon.auto-clean=false
filemon.quarantine=true
filemon.scan-mode=w,x
filemon.skip-path=false

filemon.conf-skip-path:

log.retention-time=30
```

如需查看具体某个配置项信息，需要使用该配置项的命令。

以获取中心地址设置为例：

使用命令：hrconfig --get server.address

示例如下：

```
root@ubuntu-s:/usr/local/huorong/bin# ./hrconfig --get server.address
server.address="https://192.168.6.236:6080/"
```

获取其他设置，命令为：

获取策略同步设置：hrconfig --get server.policy-sync

获取自动升级设置：hrconfig --get update.automatic

获取仅更新病毒库设置：hrconfig --get update.database-only

获取发现病毒时自动清除设置：hrconfig --get scan.auto-clean

获取清除前隔离文件设置：hrconfig --get scan.quarantine

获取扫描压缩文件的设置：hrconfig --get scan.unzip

获取压缩文件大小限制设置：hrconfig --get scan.unzip-limit

获取扫描网络驱动器设置：hrconfig --get scan.network-drvie

获取不扫描扩展名文件设置：hrconfig --get scan.exclude-file-extensions

获取文件实时监控状态：hrconfig --get filemon.enabled

获取文件实时监控-发现病毒时设置：hrconfig --get filemon.auto-clean

获取文件实时监控-清除病毒时设置：hrconfig --get filemon.quarantine

获取文件实时监控-扫描时机设置：hrconfig --get filemon.scan-mode

获取文件实时监控-不扫描指定文件路径设置：hrconfig --get filemon.skip-path

获取文件实时监控-不扫描指定文件路径规则设置：hrconfig --get filemon.conf-skip-path

获取日志保留时间设置：hrconfig --get log.retention-time

4.5 修改配置项

如需修改某项配置，命令为 hrconfig --set update.automatic(配置名)=true/false

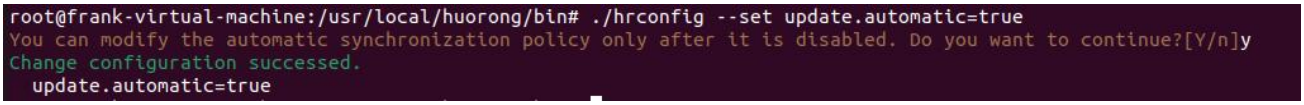
如修改某项配置需断开终端与中心的策略同步，则显示如下提示：

You can modify the automatic synchronization policy only after it is disabled. Do you want to continue?[y/n]

y，确认修改，并将同步策略配置修改为 false 状态。

n，取消修改配置。

以修改自动升级设置为例，使用命令 hrconfig --set update.automatic=true



4.5.1 修改中心地址

hrconfig --set server.address="https://192.168.2.200:6080"

// 修改成功

Change configuration successed.

server.address="https://192.168.2.200:6080"

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

输入无效的中心地址

hrconfig --set server.address="xxx"

// 输入中心地址无法连接

The entered server address cannot be connected.Do you want to continue?[Y/n]

// n 放弃修改配置

// Y 继续修改配置，server.address 设置为 false

Change configuration successed.

server.address="xxx"

4.5.2 修改策略同步设置

hrconfig --set server.policy-sync=false

// 修改成功

Change configuration successed.

server.policy-sync=false

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误；

Change configuration failed. Invalid value!

server.policy-sync=<true|false>

Default value is true. If true, the endpoint automatically synchronizes policy.

4.5.3 修改自动升级设置

hrconfig --set update.automatic=false

// 修改成功

Change configuration successed.

update.automatic=false

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误；输入值不为 "true" 或者 "false"。

Change configuration failed. Invalid value!

update.automatic=<true|false>

Default value is true. If true, the endpoint is automatically upgraded.

4.5.4 修改仅更新病毒库设置

hrconfig --set update.database-only=true

// 修改成功

Change configuration successed.

update.database-only=true

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误；输入值不为 "true" 或者 "false"。

Change configuration failed. Invalid value!

update.database-only=<true|false>

Default value is false. If true, update only the malware definitions.

4.5.5 修改发现病毒时自动清除设置

hrconfig --set scan.auto-clean=false

// 修改成功

Change configuration successed.

scan.auto-clean=false

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误

Change configuration failed. Invalid value!

scan.auto-clean=<true|false>

Default value is false. If true, automatically clean malware when it is detected.

4.5.6 修改清除前隔离文件设置

hrconfig --set scan.quarantine=false

// 修改成功

Change configuration successed.

scan.quarantine=false

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误

Change configuration failed. Invalid value!

scan.quarantine=<true|false>

Default value is true. If true, quarantine malware before clean it.

4.5.7 修改扫描压缩文件设置

hrconfig --set scan.unzip=false

// 修改成功

Change configuration successed.

scan.unzip=false

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误

Change configuration failed. Invalid value!

scan.unzip=<true|false>

Default value is true. If true, the full scan detects the files in the compressed package.

4.5.8 修改压缩文件大小限制设置

hrconfig --set scan.unzip-limit=100

// 修改成功

Change configuration successed.

scan.unzip-limit=100

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误

Change configuration failed. Invalid value!

scan.unzip-limit=<size>

Unzipped file limit for full-scan.The limit size in megabytes. Files that exceed the limit size will not be scanned.

<size> default value is 20, maximum value is 9999 and minimum value is 20.

4.5.9 修改扫描网络驱动器设置

hrconfig --set scan.network-drvie=true

// 修改成功

Change configuration successed.

scan.network-drvie=true

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误

Change configuration failed. Invalid value!

scan.network-drvie=<true|false>

Default value is false. If true, network drives are scanned during a full scan.

4.5.10 修改不扫描扩展名文件设置

hrconfig --set scan.exclude-file-extensions=".gz;.jpg"

// 修改成功

Change configuration successed.

scan.exclude-file-extensions=".gz;.jpg"

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

4.5.11 修改文件实时监控功能状态

hrconfig --set filemon.enabled=false

//修改成功

You can modify the automatic synchronization policy only after it is disabled. Do you want to continue?[Y/n]y

Change configuration successed.

filemon.enabled=false

//修改失败，配置文件访问错误

Change configuration failed.

//修改失败，配置值输入错误

Change configuration failed. Invalid value!

filemon.enabled=<true |false>

Default value is true. If false, realtime file monitoring will not be available for monitoring the specified file path.

4.5.12 修改文件实时监控-发现病毒时设置

hrconfig --set filemon.auto-clean=false

//修改成功

Filemon status is closed.

Change configuration successed.

filemon.auto-clean=false

//修改失败，配置文件访问错误

Change configuration failed.

//修改失败，配置值输入错误

Change configuration failed. Invalid value!

filemon.auto-clean=<true|false>

Default value is false. If true, automatically clean malware when it is detected.

4.5.13 修改文件实时监控-清除病毒时设置

hrconfig --set filemon.quarantine=false

//修改成功

Filemon status is closed.

Change configuration successed.

filemon.quarantine=false

//修改失败，配置文件访问错误

Change configuration failed.

//修改失败，配置值输入错误

Change configuration failed. Invalid value!

filemon.auto-clean=<true|false>

Default value is false. If true, automatically clean malware when it is detected.

4.5.14 修改文件实时监控-扫描时机设置

hrconfig --get filemon.scan-mode=r,w

//修改成功

Filemon status is closed.

Change configuration successed.

filemon.scan-mode=r,w

//修改失败，配置文件访问错误

Change configuration failed.

//修改失败，配置值输入错误

Change configuration failed. Invalid value!

filemon.scan-mode=<options>

Required value is "w". Multiple options separated by ",".

options:

w: Scan after file modification.

r: Scan on file read.

4.5.15 修改文件实时监控-不扫描指定文件路径设置

hrconfig --set filemon.skip-path=false

//修改成功

Filemon status is closed.

Change configuration successed.

filemon.skip-path=false

//修改失败，配置文件访问错误

Change configuration failed.

//修改失败，配置值错误

Change configuration failed. Invalid value!

filemon.skip-path=<true|false>

Default value is false. If true, filemon will skip the file path configured in filemon.conf-skip-path.

4.5.16 修改文件实时监控-不扫描指定路径规则设置

//添加不扫描指定路径

hrconfig --set filemon.conf-skip-path -a /home/ubuntu-s home

//删除不扫描指定路径

hrconfig --set filemon.conf-skip-path -d /home/ubuntu-s

//清空不扫描指定路径

hrconfig --set filemon.conf-skip-path -c

//修改成功

Filemon status is closed.

Change configuration successed.

/home/ubuntu-s home

1 row in set.

//修改失败，配置文件访问错误

Change configuration failed.

//修改失败，配置值输入错误

Change configuration failed. Invalid value!

filemon.conf-skip-path <options>

Configure directories to be skipped during file monitoring.

options:

-a <path> [note] Add the specified <path> to the skip path list. Wildcards (*,?) are supported.

-d <path> Remove the specified <path> from the skip path list.

-c Clear all skip path ruleset.

4.5.17 修改日志保留时间设置

hrconfig --set log.retention-time=30

// 修改成功

Change configuration successed.

log.retention-time=30

// 修改失败，配置文件访问错误

Change configuration failed. Access error!

// 修改失败，配置值输入错误

Change configuration failed. Invalid value!

log.retention-time=<days>

Number of days to retain logs.

<days> default value is 30. maximum value is 180 and minimum value is 1.

4.6 隔离区操作

Linux 终端支持隔离区，病毒查杀后可自动保存至隔离区中，用户可依据自身需要对隔离区文件进行恢复、删除、提取等操作。

1. 恢复隔离区文件

命令：

cd /usr/local/huorong/bin

./hrquarantine -r -i 5,10

释义：恢复隔离区中 ID 为 5 到 ID 为 10 的隔离文件,执行后可看到恢复成功和恢复失败的文件数量，再次查看隔离区文件列表会发现 ID 为 5-10 的文件已经被恢复。进入原文件目录查看，文件已被恢复至此目录中。

```
[root@localhost /]# cd /usr/local/huorong/bin
[root@localhost bin]# ./hrquarantine -r -i 5,10
success(6), ignored(0).
[root@localhost bin]# ./hrquarantine -l
Id:1    Path:/home/test/test3/02ac332f109b51acd815771021c9eca345d785ca          Name:Trojan/Generic!C360873A5B256514    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:2    Path:/home/test/test3/04c25d330d335e728835576776a03a3382cbb832          Name:Trojan/Generic!C360873A5B256514    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:3    Path:/home/test/test3/0a6be33293e16a86421b31a82c3f35513113089a          Name:Virus/Android.b    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:4    Path:/home/test/test3/1aa602e29b01978617e5c1ceb4a219269c28a0b2          Name:Virus/CTS.a        Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:11   Path:/home/test/test3/3a2aeed92524504e32ecb35892ceb26c14148319          Name:Trojan/Generic!C360873A5B256514    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:12   Path:/home/test/test3/3b637ab02e9aa5fe6780d1f221682721c134787b          Name:Virus/CTS.a        Time:2021-03-10 05:30:22        Reason:Anti-Virus
Id:13   Path:/home/test/test3/3ccb0bb49008831f618a15e89e529bad410b165a          Name:Virus/Floxif.gen   Time:2021-03-10 05:30:22        Reason:Anti-Virus
Id:14   Path:/home/test/test3/3d2a7568e2123284498bbb9d22fce3a456e75740          Name:Virus/CTS.a        Time:2021-03-10 05:30:22        Reason:Anti-Virus
Id:15   Path:/home/test/test3/3faccc73f57a0037bfe277e2b4462bb51f490cfb          Name:Virus/Viking.jj    Time:2021-03-10 05:30:23        Reason:Anti-Virus
Id:16   Path:/home/test/test3/5e5222b33c671abafc0618986293a8f934c5892a          Name:Virus/CTS.a        Time:2021-03-10 05:30:23        Reason:Anti-Virus
Id:17   Path:/home/test/test3/5ea82455770a459edef513ec8a95f5c1848b2962          Name:Virus/CTS.a        Time:2021-03-10 05:30:23        Reason:Anti-Virus
Id:18   Path:/home/test/test3/2fc7d96712607787099acd7e3d9dfe6dfc9ele92          Name:Virus/Viking.a!dll         Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:19   Path:/home/test/test3/6eb0ea37cf0321fdba482584b2e4e1ff330286ff          Name:Virus/CTS.a        Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:20   Path:/home/test/test4/0c3e0a545ba27aeadccfc18d2cffd46d64215764          Name:OMacro/Marker.s    Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:21   Path:/home/test/test4/0c7994b245ee476ebb0a3bbc7bb1922b4c23744f          Name:OMacro/ShellHide.a         Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:22   Path:/home/test/test4/0d5f98b56d4ba3b17a38b0d5430d6c9e918a5df0          Name:OMacro/Laroux.a    Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:23   Path:/home/test/test4/0e143bf006dd06fc7ecc03b1f5dbeb2f3a06638a          Name:OMacro/Downloader.ya       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:24   Path:/home/test/test4/1a1d20e844f5f6e82270827 8ccd33d30d00556d1          Name:OMacro/Downloader          Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:25   Path:/home/test/test4/1b934f1b9605561d113ee2a917719fc8d04dfd76          Name:OMacro/Agent.b     Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:26   Path:/home/test/test4/1ba0e2b196f83ba1a5a7a07c24214f5f998af770          Name:OMacro/Downloader.aiy      Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:27   Path:/home/test/test4/1bede09d10c13565da6aa242e6490e93b8f39bab          Name:OMacro/BlackIce    Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:28   Path:/home/test/test4/1bfb11d279496e34bef63696a0afb9fac8981739          Name:HEUR:OMacro/WinA.d         Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:29   Path:/home/test/test4/1c4b0f215e75a7ebaae85356849a4ff79849a996          Name:OMacro/Thus.a      Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:30   Path:/home/test/test4/1e14bb6fb1c1367a149c18cb3745bcdf9dc4009c          Name:OMacro/Downloader.ck       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:31   Path:/home/test/test4/1ef80cfcb14ef2231d5aaad5640dd80fef1f7d59          Name:OMacro/Nsi.b       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:32   Path:/home/test/test4/1f93f5ccd35b1f4bebfdc5318d24275a002ce3ff          Name:OMacro/Downloader.yb       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:33   Path:/home/test/test4/2dcc61336f03e9b21124a9645355dbf85f97a53c          Name:HEUR:OMacro/Obfuscated.c   Time:2021-03-10 05:30:26        Reason:Anti-Virus
```

原文件目录：

```
[root@localhost test]# cd /home/test/test3
[root@localhost test3]# ll
total 932
----------. 1 root root 441031 Mar 10 05:53 1ae0190134d9d5d8021e8adc6cc9a2907e3ce7ef
----------. 1 root root  37318 Mar 10 05:53 1aff1ede794458f2903492b1f9a348c1a1f1c1fc
----------. 1 root root 335360 Mar 10 05:53 1c8cf356d5b3e7dbec9c507856f2343f93f53bc4
----------. 1 root root  61406 Mar 10 05:53 1f2f0699c0a50a75443618721631aa4b3199aac9
----------. 1 root root  32801 Mar 10 05:53 1f86423ec785d7a583d2b2b8727d26453bc522db
----------. 1 root root  33249 Mar 10 05:53 2df6ddc7373747d76f25c8a2b0cc6e5e67cd4b63
[root@localhost test3]#
```

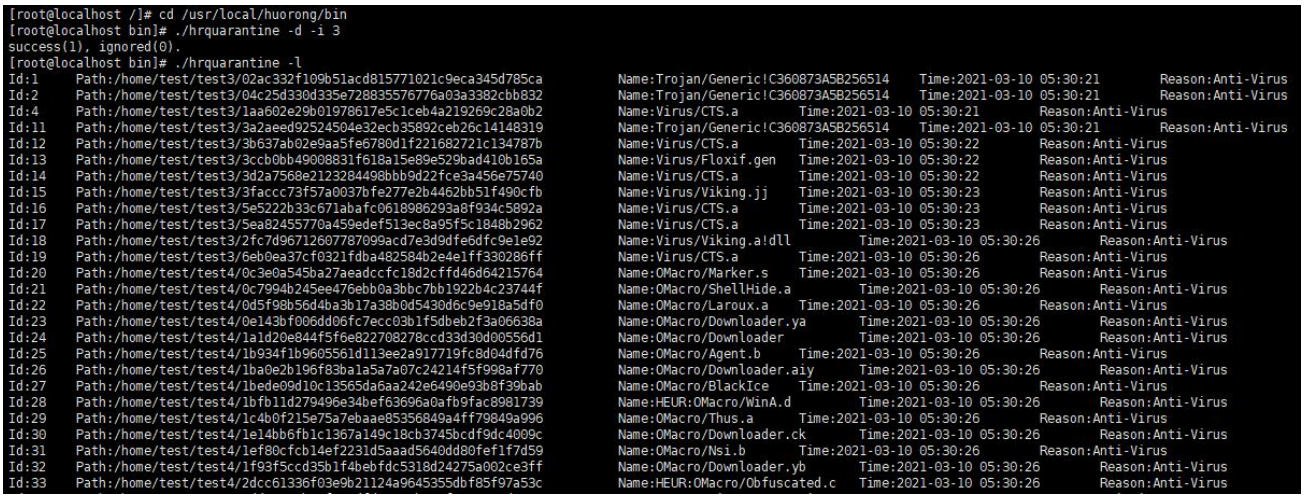
2. 删除隔离区文件

命令：

cd /usr/local/huorong/bin

./hrquarantine -d -i 3

释义：删除隔离区中 ID 为 3 的隔离文件，执行后可看到删除成功和删除失败的文件数量，再次查看隔离区文件列表会发现 ID 为 3 的文件已经被删除。



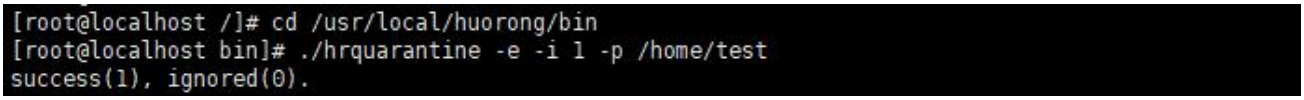
3. 提取隔离区文件

命令：

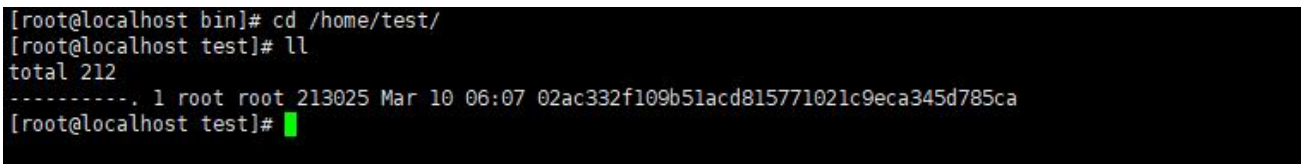
cd /usr/local/huorong/bin

./hrquarantine -e -i 1 -p /home/test

释义：提取隔离区中 ID 为 1 的隔离文件至 home 目录下的 test 目录中，执行后可看到删除成功和删除失败的文件数量，进入提取文件保存目录可看到提取成功后的文件。



查看提取文件保存目录：



4. 列出隔离区文件

命令：

cd /usr/local/huorong/bin

./hrquarantine -l

释义：列出隔离区内的隔离文件。

```
[root@localhost /]# cd /usr/local/huorong/bin
[root@localhost bin]# ./hrquarantine -l
Id:1    Path:/home/test/test3/02ac332f109b51acd815771021c9eca345d785ca        Name:Trojan/Generic!C360873A5B256514    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:2    Path:/home/test/test3/04c25d330d335e728835576776a03a3382cbb832        Name:Trojan/Generic!C360873A5B256514    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:3    Path:/home/test/test3/0a6be33293e16a86421b31a82c3f35513113089a        Name:Virus/Android.b    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:4    Path:/home/test/test3/1aa602e29b01978617e5c1ceb4a219269c28a0b2        Name:Virus/CTS.a        Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:5    Path:/home/test/test3/1ae0190134d9d5d8021e8adc6cc9a2907e3ce7ef        Name:Virus/Android.b    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:6    Path:/home/test/test3/1c8cf356d5b3e7dbec9c507856f2343f93f53bc4        Name:Virus/Jeefo        Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:7    Path:/home/test/test3/1aff1ede794458f2903492b1f9a348c1a1f1c1fc        Name:Virus/CTS.a        Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:8    Path:/home/test/test3/1f2f0699c0a50a75443618721631aa4b3199aac9        Name:Virus/CTS.a        Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:9    Path:/home/test/test3/1f86423ec785d7a583d2b2b8727d26453bc522db        Name:Trojan/Generic!C360873A5B256514    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:10   Path:/home/test/test3/2df6ddc7373747d76f25c8a2b0cc6e5e67cd4b63        Name:Virus/CTS.a        Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:11   Path:/home/test/test3/3a2aeed92524504e32ecb35892ceb26c14148319        Name:Trojan/Generic!C360873A5B256514    Time:2021-03-10 05:30:21        Reason:Anti-Virus
Id:12   Path:/home/test/test3/3b637ab02e9aa5fe6780d1f221682721c134787b        Name:Virus/CTS.a        Time:2021-03-10 05:30:22        Reason:Anti-Virus
Id:13   Path:/home/test/test3/3ccb0bb49008831f618a15e89e529bad410b165a        Name:Virus/Floxif.gen   Time:2021-03-10 05:30:22        Reason:Anti-Virus
Id:14   Path:/home/test/test3/3d2a7568e2123284498bbb9d22fce3a456e75740        Name:Virus/CTS.a        Time:2021-03-10 05:30:22        Reason:Anti-Virus
Id:15   Path:/home/test/test3/3faccc73f57a0037bfe277e2b4462bb51f490cfb        Name:Virus/Viking.jj    Time:2021-03-10 05:30:23        Reason:Anti-Virus
Id:16   Path:/home/test/test3/5e5222b33c671abafc0618986293a8f934c5892a        Name:Virus/CTS.a        Time:2021-03-10 05:30:23        Reason:Anti-Virus
Id:17   Path:/home/test/test3/5ea82455770a459edef513ec8a95f5c1848b2962        Name:Virus/CTS.a        Time:2021-03-10 05:30:23        Reason:Anti-Virus
Id:18   Path:/home/test/test3/2fc7d96712607787099acd7e3d9dfe6dfc9e1e92        Name:Virus/Viking.a!dll         Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:19   Path:/home/test/test3/6eb0ea37cf0321fdba482584b2e4e1ff330286ff        Name:Virus/CTS.a        Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:20   Path:/home/test/test4/0c3e0a545ba27aeadccfc18d2cffd46d64215764        Name:OMacro/Marker.s    Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:21   Path:/home/test/test4/0c7994b245ee476ebb0a3bbc7bb1922b4c23744f        Name:OMacro/ShellHide.a         Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:22   Path:/home/test/test4/0d5f98b56d4ba3b17a38b0d5430d6c9e918a5df0        Name:OMacro/Laroux.a    Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:23   Path:/home/test/test4/0e143bf006dd06fc7ecc03b1f5dbeb2f3a06638a        Name:OMacro/Downloader.ya       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:24   Path:/home/test/test4/1a1d20e844f5f6e822708278ccd33d30d00556d1        Name:OMacro/Downloader          Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:25   Path:/home/test/test4/1b934f1b9605561d113ee2a917719fc8d04dfd76        Name:OMacro/Agent.b     Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:26   Path:/home/test/test4/1ba0e2b196f83ba1a5a7a07c24214f5f998af770        Name:OMacro/Downloader.aiy      Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:27   Path:/home/test/test4/1bede09d10c13565da6aa242e6490e93b8f39bab        Name:OMacro/BlackIce    Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:28   Path:/home/test/test4/1bfb11d279496e34bef63696a0afb9fac8981739        Name:HEUR:OMacro/WinA.d         Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:29   Path:/home/test/test4/1c4b0f215e75a7ebaae85356849a4ff79849a996        Name:OMacro/Thus.a      Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:30   Path:/home/test/test4/1e14bb6fb1c1367a149c18cb3745bcdf9dc4009c        Name:OMacro/Downloader.ck       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:31   Path:/home/test/test4/1ef80cfcb14ef2231d5aaad5640dd80fef1f7d59        Name:OMacro/Nsi.b       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:32   Path:/home/test/test4/1f93f5ccd35b1f4bebfdc5318d24275a002ce3ff        Name:OMacro/Downloader.yb       Time:2021-03-10 05:30:26        Reason:Anti-Virus
Id:33   Path:/home/test/test4/2dcc61336f03e9b21124a9645355dbf85f97a53c        Name:HEUR:OMacro/Obfuscated.c   Time:2021-03-10 05:30:26        Reason:Anti-Virus
```

5. 查询隔离区文件占用大小

命令：

cd /usr/local/huorong/bin

./hrquarantine -s

释义：查询隔离区内的隔离文件当前占用空间大小。

```
[root@localhost /]# cd /usr/local/huorong/bin
[root@localhost bin]# ./hrquarantine -s
Quarantined items occupies 18MB of disk space
[root@localhost bin]#
```

6. 查看帮助

命令：

cd /usr/local/huorong/bin

./hrquarantine -h

释义：查看隔离区操作帮助说明。

```
[root@localhost /]# cd /usr/local/huorong/bin
[root@localhost bin]# ./hrquarantine -h
Usage:
        hrquarantine -h
        hrquarantine -l
        hrquarantine -s
        hrquarantine -d [-i [id|ranges]] [Options]
        hrquarantine -r [-i [id|ranges]] [Options]
        hrquarantine -e [-i [id|ranges]] -p DIRECTORY [Options]

id
        Specifies a decimal number that identifies a record.

ranges
        You can specify a id range by a pair of ids.

Commands:
        -h show this
        -l list item of  quarantine
        -s used space of quarantine
        -d remove file from quarantine
        -r restore file from quarantine
        -e extract file from quarantine

Options:
        -a all

Example:
        hrquarantine -d -a remove all file
        hrquarantine -d -i 1 remove file at the id 1.
        hrquarantine -r -i 5,10 restore file from id 5 to 10
[root@localhost bin]#
```

4.7 查看日志

支持使用命令查看终端的升级日志和查杀日志。

4.7.1 查看日志使用帮助

使用命令 hrlog --help 查看日志帮助命令行。

```
root@frank-virtual-machine:/usr/local/huorong/bin# ./hrlog --help
Huorong Endpoint Security Management System Client for Linux Server
Log viewer
Copyright (c) Huorong Corporation. All rights reserved.

Usage: hrlog [-h | --help]
             <command> [<args>]

These keys can be used to view log content:

  UpArrow ..... Backward one line.
  DownArrow or RETURN ..... Forward  one line.
  PageUp ..... Backward one window.
  PageDown ..... Forward  one window.
  Space ..... Forward  one window.
  ESC ..... Quit.

These are common hrlog commands:

  --function=<function1,function2>
    Show the logs of the specified function. Function can be scan, update.

  --since=<date>
  --after=<date>
    Show the logs more recent than a specific date. <date> format can be "YYYY-MM-DD" or "YYYY-MM-DD hh:mm:ss".
    For example, September 27, 2022 at 6 p.m. is represented as 2022-09-27 18:00:00.

  --until=<date>
  --before=<date>
    Show the logs older than a specific date. <date> format can be "YYYY-MM-DD" or "YYYY-MM-DD hh:mm:ss".
    For example, September 27, 2022 at 6 p.m. is represented as 2022-09-27 18:00:00.

  --format=<format>
    Pretty-print the contents of the logs, where <format> can be one of short,full.

  --show=<ID>
    Show the complete logs for the specified <ID>.

  --help
    Show this message.
```

4.7.2 查看不同格式日志

日志分为简短日志和详细日志。

查看简短日志命令为：hrlog --format=short

简短日志仅显示日志的 ID，日志的类型（升级日志 update/查杀日志 scan），日志时间，及日志概要：升级日志显示升级的结果和当前终端的版本号，查杀日志显示扫描结果是否发现病毒威胁。

```
ID:             1
Function:       Update
Date:           2023-06-26 15:25:29

  Auto Update Succeeded, version: V2.0.8.0

ID:             2
Function:       scan
Date:           2023-06-26 17:22:08

  0 risk(s) detected during Quick Scan

ID:             3
Function:       scan
Date:           2023-06-26 17:35:51

  0 risk(s) detected during Quick Scan

ID:             4
Function:       scan
Date:           2023-06-26 17:41:26

  0 risk(s) detected during Quick Scan

ID:             5
Function:       scan
Date:           2023-06-27 14:17:41

  0 risk(s) detected during Quick Scan

ID:             6
Function:       scan
Date:           2023-06-27 14:43:07

  0 risk(s) detected during Quick Scan

ID:             7
Function:       scan
Date:           2023-06-27 14:47:00

  0 risk(s) detected during Quick Scan

ID:             8
Function:       scan
Date:           2023-06-27 14:49:51

Press RETURN for more, or ESC to quit.
```

查看详细日志命令为：hrlog --format=full

详细日志显示日志 ID,日志类型（升级日志 update/查杀日志 scan），日志时间，不同日志类型显示详情不同：升级日志显示升级结果、升级方式（手动升级、自动升级）、当前终端版本号以及升级数据所在路径；查杀日志详情显示查杀类型（全盘查杀、快速查杀和自定义查杀），扫描开始时间和所用时间，扫描对象和扫描文件数，威胁数量及威胁处理数量。

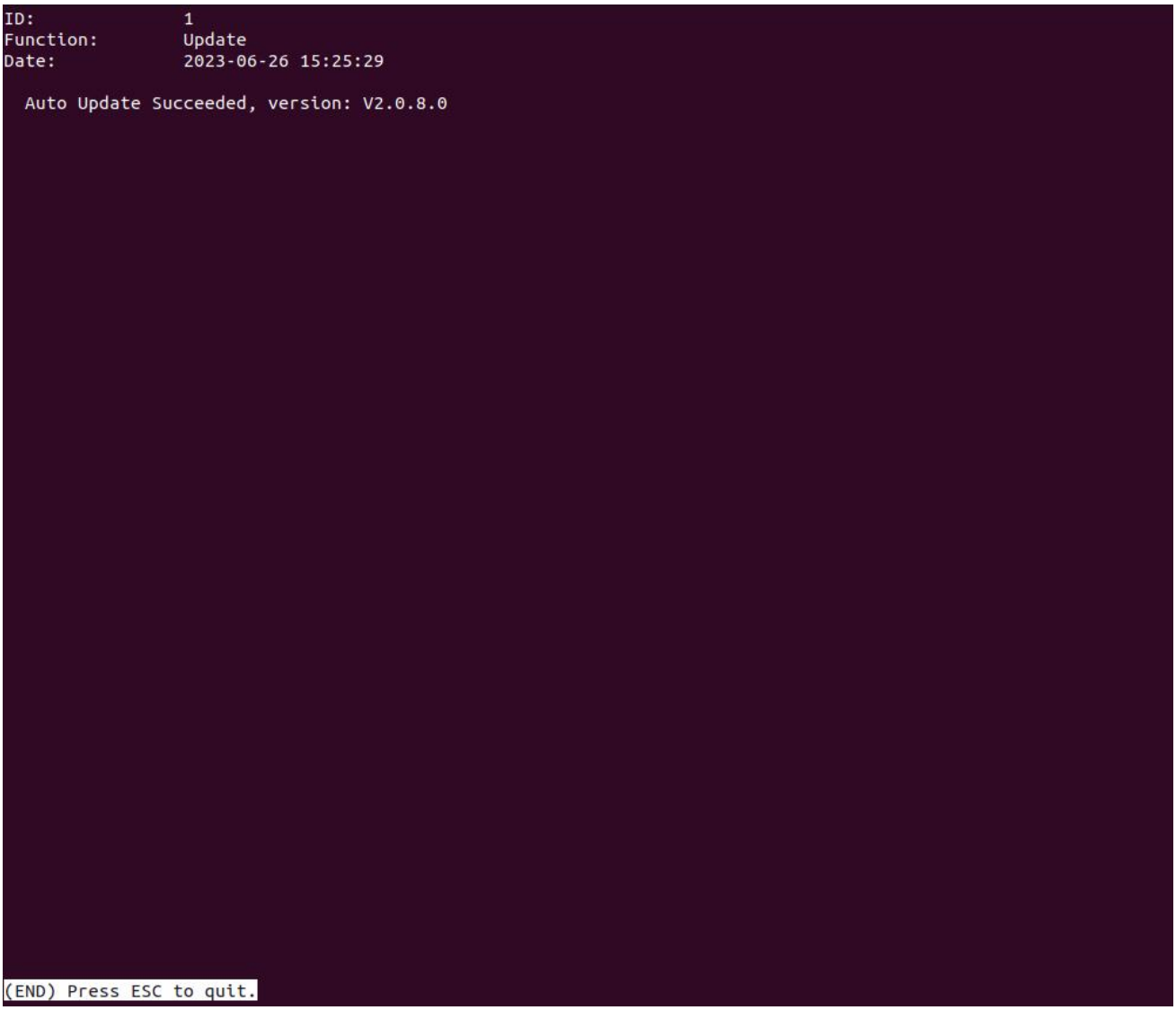
```
ID:             1
Function:       Update
Date:           2023-06-26 15:25:29

  Mode: Auto Update
  Result: Succeeded, version: V2.0.8.0
  Files downloaded:
    2023-06-26 15:25:28 /usr/local/huorong/share/xsse/libvxf.vdl
    2023-06-26 15:25:28 /usr/local/huorong/share/xsse/libvxf.dat
    2023-06-26 15:25:28 /usr/local/huorong/share/xsse/libvxf.tdl
    2023-06-26 15:25:28 /usr/local/huorong/share/virdb/hwl.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/prop.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/pset.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/troj.db

  Files updated:
    2023-06-26 15:25:29 /usr/local/huorong/share/xsse/libvxf.vdl
    2023-06-26 15:25:29 /usr/local/huorong/share/xsse/libvxf.dat
    2023-06-26 15:25:29 /usr/local/huorong/share/xsse/libvxf.tdl
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/hwl.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/prop.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/pset.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/troj.db


ID:             2
Function:       scan
Date:           2023-06-26 17:22:08

  Scan Type: Quick Scan
  Definition: 2023-06-08 18:10:20
  Started at: 2023-06-26 17:21:49
  Duration: 00:00:17
  Object(s): 2429
  File(s): 2403
  Threat(s): 0
  Cleaned: 0

ID:             3
Function:       scan
Date:           2023-06-26 17:35:51

  Scan Type: Quick Scan
  Definition: 2023-06-08 18:10:20
  Started at: 2023-06-26 17:35:29
  Duration: 00:00:21
Press RETURN for more, or ESC to quit.
```

4.7.3 查看不同功能日志

支持查看指定功能日志，命令为 hrlog --function=“功能名（scan，update）”

可以指定某个功能，如查杀日志，hrlog --function=scan，或升级日志 hrlog --function=update，也可以同时查询查杀日志和升级日志，功能之间以逗号“，”分隔，命令为 hrlog --function=scan,update

示例如下：



4.7.4 根据时间查看日志

支持查看指定时间范围的日志，时间格式为： * “年-月-日 时:分:秒”，如：“2022-8-18 20:22:00” * 也可以仅使用”年-月-日”，如：“2022-7-13”，等同于”2022-7-13 00:00:00”。

查看某天以来的日志，日志时间 >= date

hrlog --since=<date>

查看某天以后的日志，日志时间 > date

hrlog --after=<date>

查看直到某天的日志，日志时间 <= date

hrlog --until=<date>

查看某天以前的日志，日志时间 < date

hrlog --before=<date>

示例如下：

查看当前终端直到 2023 年 6 月 28 日的日志，命令为：hrlog --until=2023-6-28

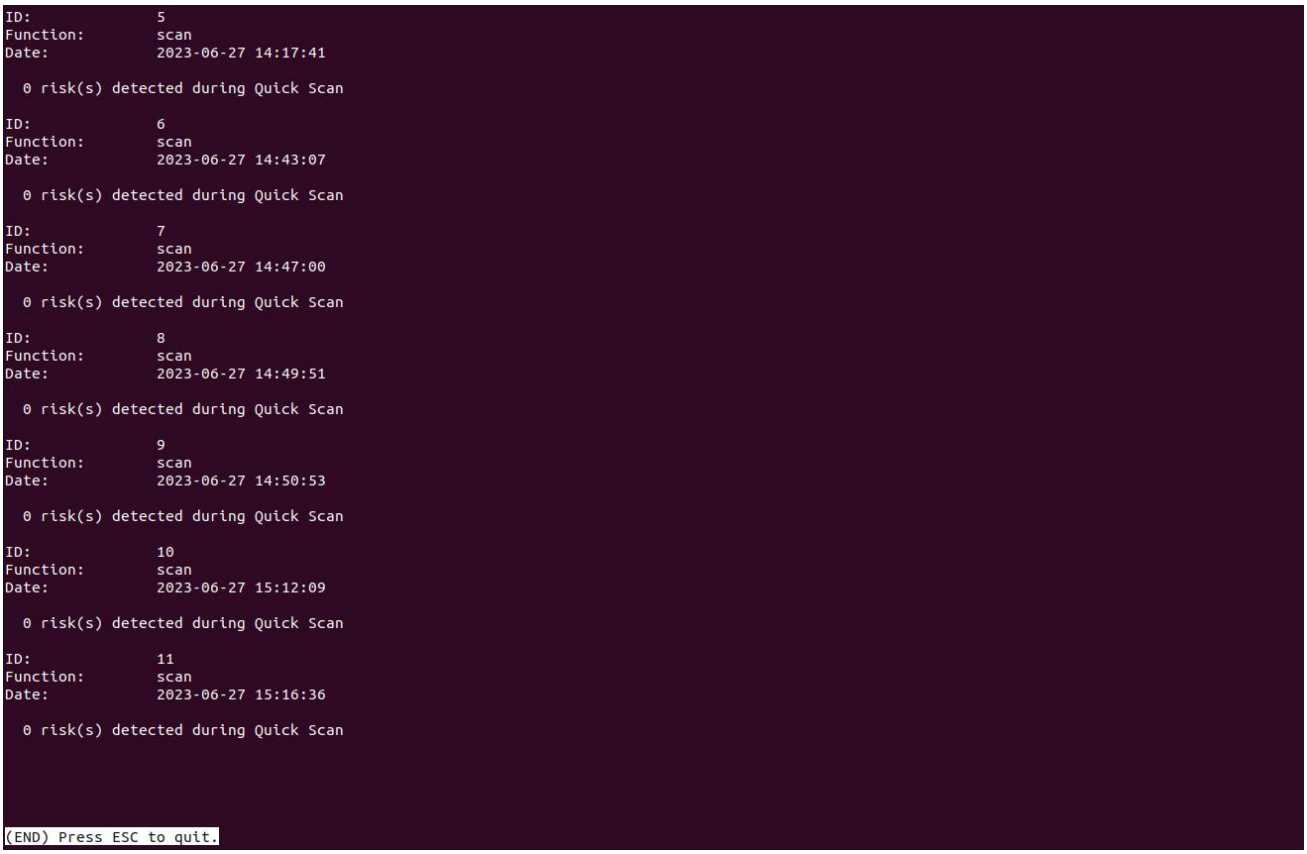
```
ID:             1
Function:       Update
Date:           2023-06-26 15:25:29

  Auto Update Succeeded, version: V2.0.8.0

ID:             2
Function:       scan
Date:           2023-06-26 17:22:08

  0 risk(s) detected during Quick Scan

ID:             3
Function:       scan
Date:           2023-06-26 17:35:51

  0 risk(s) detected during Quick Scan

ID:             4
Function:       scan
Date:           2023-06-26 17:41:26

  0 risk(s) detected during Quick Scan

ID:             5
Function:       scan
Date:           2023-06-27 14:17:41

  0 risk(s) detected during Quick Scan

ID:             6
Function:       scan
Date:           2023-06-27 14:43:07

  0 risk(s) detected during Quick Scan

ID:             7
Function:       scan
Date:           2023-06-27 14:47:00

  0 risk(s) detected during Quick Scan

ID:             8
Function:       scan
Date:           2023-06-27 14:49:51

Press RETURN for more, or ESC to quit.
```

4.7.5 多条件查询日志

支持输入多个查询条件，查询符合条件的日志数据。

如查询 2023 年 6 月 27 日后，2023 年 6 月 28 日前的查杀日志，命令为：

hrlog --function=scan --since=2023-6-27 --before=2023-6-28



4.7.6 查看指定 ID 完整日志

如查询日志显示的日志格式为简短日志，可以使用命令查看指定 ID 日志的详细（完整）日志。

例如，查询 ID 为 1 的完整日志，命令为 hrlog --show=1

```
ID:             1
Function:       Update
Date:           2023-06-26 15:25:29

  Mode: Auto Update
  Result: Succeeded, version: V2.0.8.0
  Files downloaded:
    2023-06-26 15:25:28 /usr/local/huorong/share/xsse/libvxf.vdl
    2023-06-26 15:25:28 /usr/local/huorong/share/xsse/libvxf.dat
    2023-06-26 15:25:28 /usr/local/huorong/share/xsse/libvxf.tdl
    2023-06-26 15:25:28 /usr/local/huorong/share/virdb/hwl.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/prop.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/pset.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/troj.db

  Files updated:
    2023-06-26 15:25:29 /usr/local/huorong/share/xsse/libvxf.vdl
    2023-06-26 15:25:29 /usr/local/huorong/share/xsse/libvxf.dat
    2023-06-26 15:25:29 /usr/local/huorong/share/xsse/libvxf.tdl
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/hwl.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/prop.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/pset.db
    2023-06-26 15:25:29 /usr/local/huorong/share/virdb/troj.db
```

第五章 火绒终端安全管理系统-Linux 桌面版终端

5.1 首页

火绒安全终端首页为用户提供病毒查杀、版本更新、文件实时监控、信任/隔离区功能快速访问入口以及当前终端版本和病毒库版本。

5.1.1 病毒查杀

1. 全盘查杀

全盘查杀功能会针对计算机包括系统设置、系统进程、启动项、服务项、常用软件、系统关键位置和物理存储磁盘进行全方位查杀。全盘查杀功能查杀位置全面，覆盖面广，所以应用此查杀方式安全性将大大提升，但是用时较长。

用户单击【全盘查杀】即可对本地环境进行病毒全盘查杀。

（1） 停止：用户可手动停止病毒全盘查杀任务，点击【停止】按钮，弹出确认框中点击【确定】即可终止当前查杀任务，并将已扫描查杀的数据告知用户。

（2） 暂停：用户可暂停当前病毒查杀任务，点击【暂停】按钮，病毒查杀任务进入暂停状态，点击【继续】可继续当前查杀任务继续查杀，方便用户对当前任务进行管理。

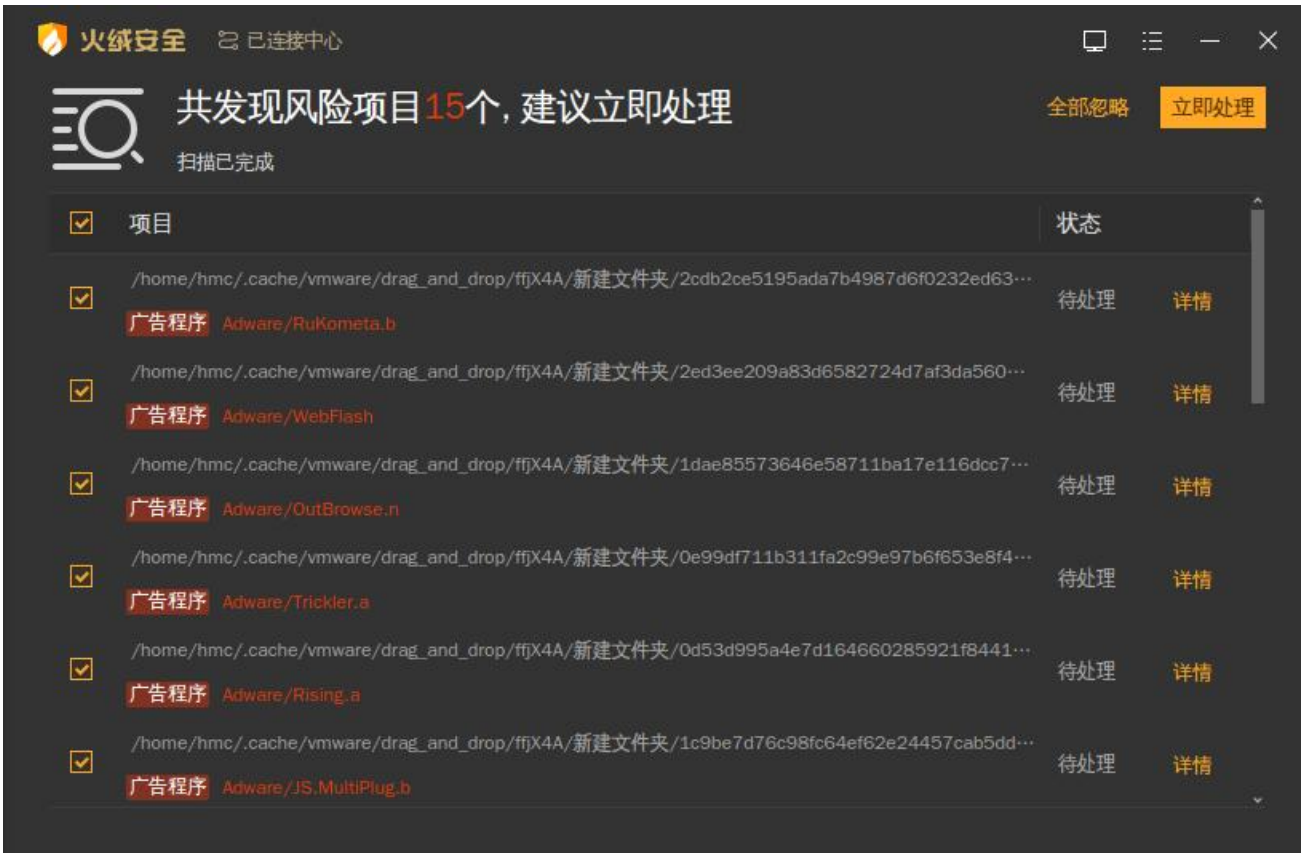
（3） 常规：常规扫描模式下，病毒查杀任务会按照正常状态执行任务，不会特殊处理任务。

（4） 高速：高速扫描模式下，病毒查杀任务会提升优先级，增加系统资源调用以快速完成扫描任务。

（5） 查杀完成后自动关机：勾选此项后，病毒查杀任务查杀完成之后，将自动关闭计算机。

病毒查杀任务执行完成后，如未发现任何风险项，将为用户展示当前扫描对象、任务耗时等扫描任务详情信息，用户单击【完成】按钮后会返回终端主界面。

病毒查杀任务执行完成后，如发现风险项目，则会将风险项目展示给用户，用户可自行选择清理或忽略风险项目。



点击【立即处理】后，终端将自动处理已勾选风险项，并为用户展示处理结果及扫描任务结果。

2. 快速查杀

快速查杀功能会针对计算机包括系统设置、系统进程、启动项、服务项、常用软件、关键位置这些敏感位置进行针对性查杀。快速查杀功能查杀位置相对全盘查杀较少，所以查杀速度较快。

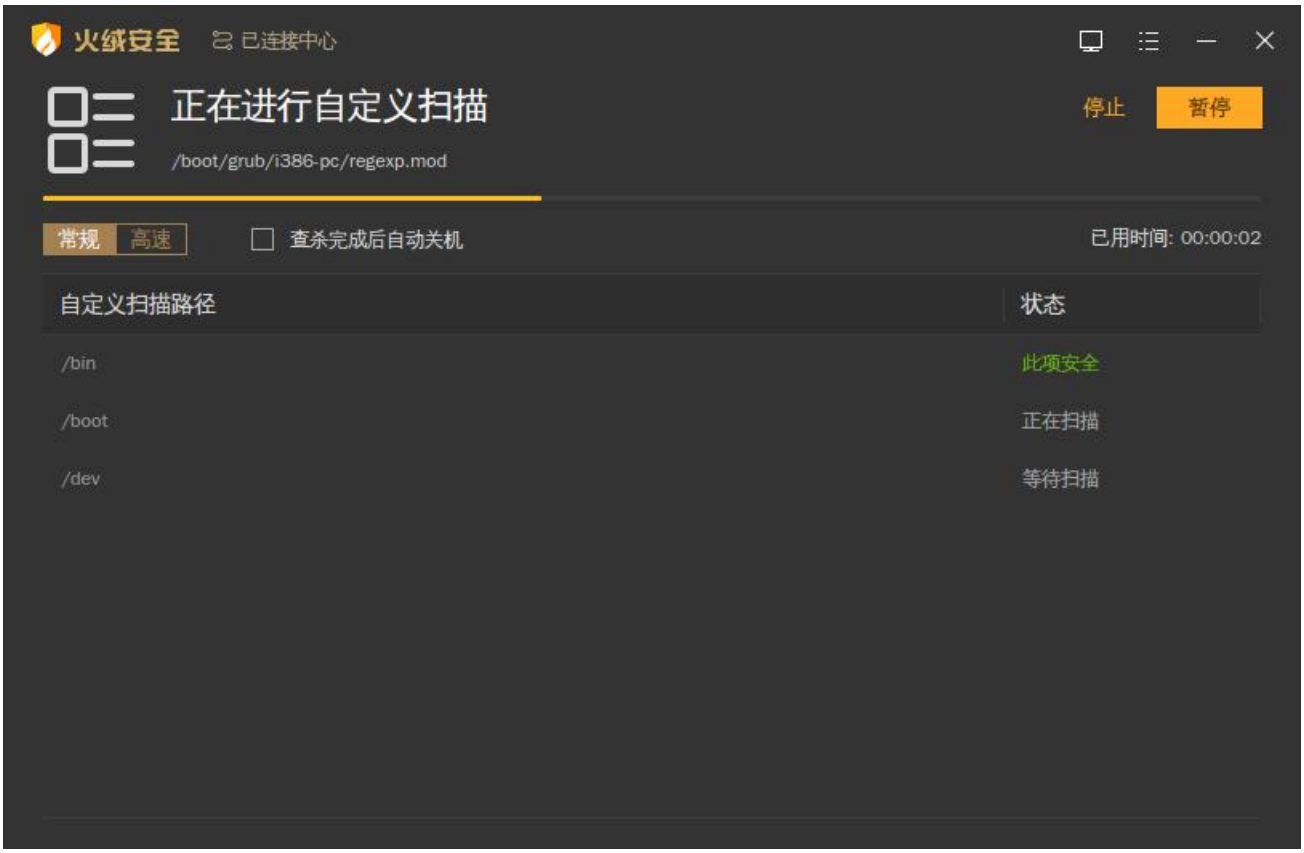
用户单击【快速查杀】即可对本地环境进行病毒快速查杀。

快速查杀任务处理结果及展示与全盘查杀相同，详情请参见全盘查杀功能。

3. 自定义查杀

自定义查杀功能可自定义选择查杀位置，方便用户定点查杀指定存储目录，病毒查杀任务更加灵活。

用户单击【自定义查杀】按钮，选择自定义查杀位置后单击【确定】即可对当前选择的查杀位置进行病毒查杀。



自定义查杀任务处理结果及展示与全盘查杀相同，详情请参见全盘查杀功能。

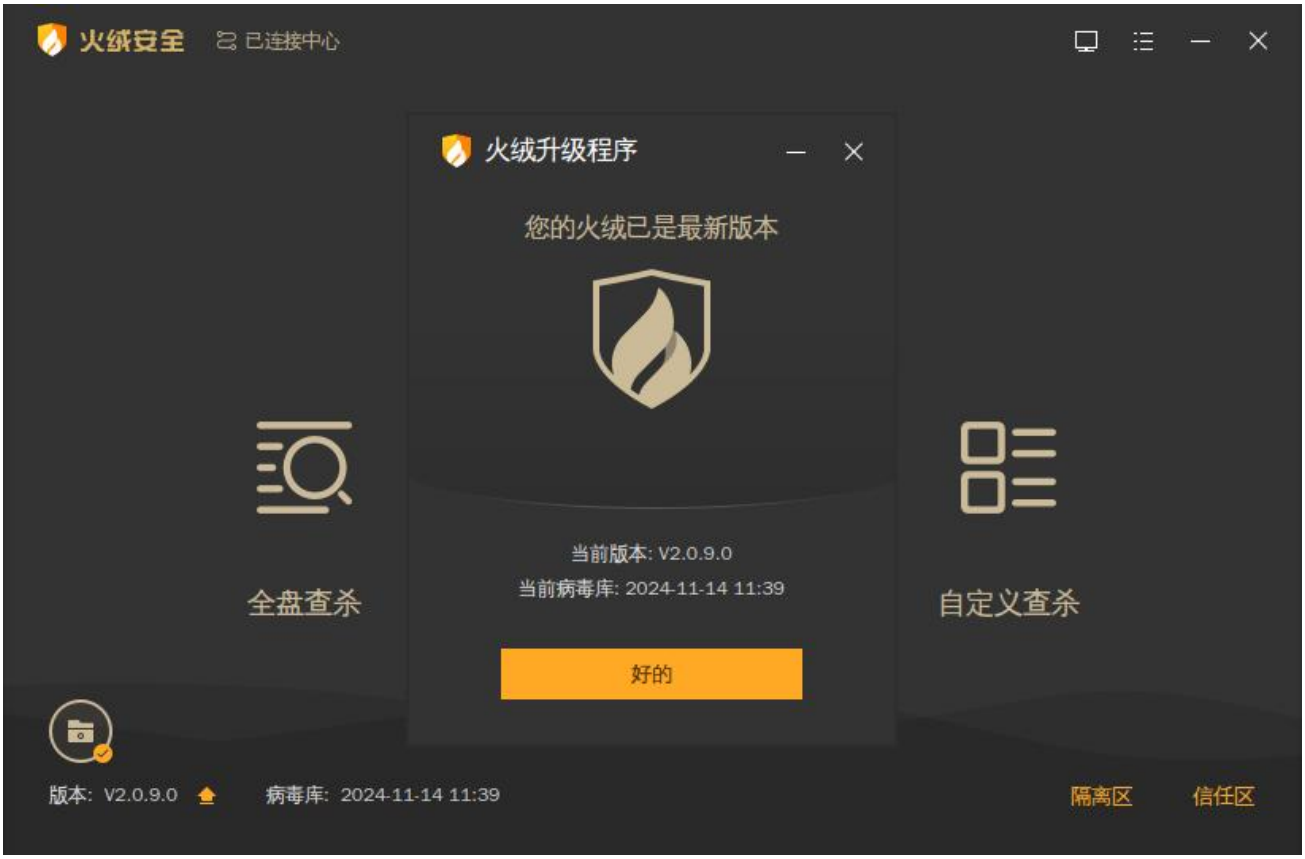
5.1.2 文件实时监控

在首页文件图标处可看到文件实时监控是否开启，点击进入安全设置对文件实时监控功能进行具体设置。可以选择在文件修改完成后，文件读取时或文件执行时检测文件是否安全，拦截病毒程序。在不影响电脑正常使用的情况下，实时保护用户的终端不受病毒侵害。

5.1.3 版本及更新

火绒安全终端首页提供了终端版本信息和病毒库版本信息展示，为方便用户手动检查终端版本，火绒安全终端也提供便捷版本更新检测入口。

用户点击版本信息后方升级按钮，终端会自动检测当前终端版本信息，如果检查到终端未更新至最新版本，会提示用户当前有新版本，用户可自行选择是否更新为当前检测到的最新版本。



5.1.4 信任/隔离区

火绒安全终端首页提供了信任/隔离区快捷访问入口，方便用户快速查看及管理当前已信任及已隔离的文件。

1. 隔离区

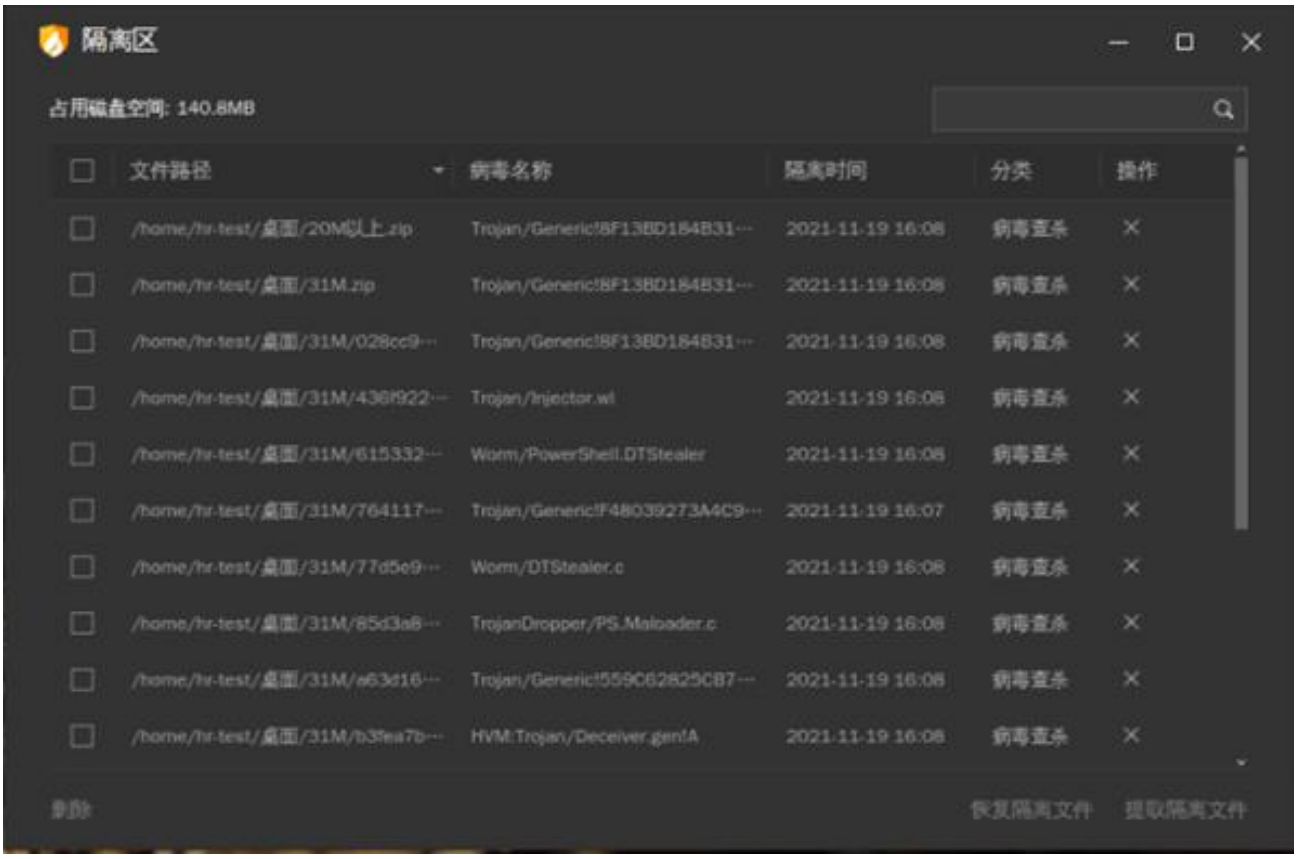
火绒安全终端会将扫描处理过的病毒威胁文件，经过加密后备份至隔离，以便您有特殊需要，可以主动从隔离区中重新找回被处理过的威胁文件。

用户单击火绒安全终端首页右下角【隔离区】弹出文件隔离区弹框，用户可查看当前隔离区隔离的所有风险文件。

（1） 删除：用户选中隔离区中的文件，单击左下角【删除】按钮，即可删除当前隔离区保存的风险文件样本。

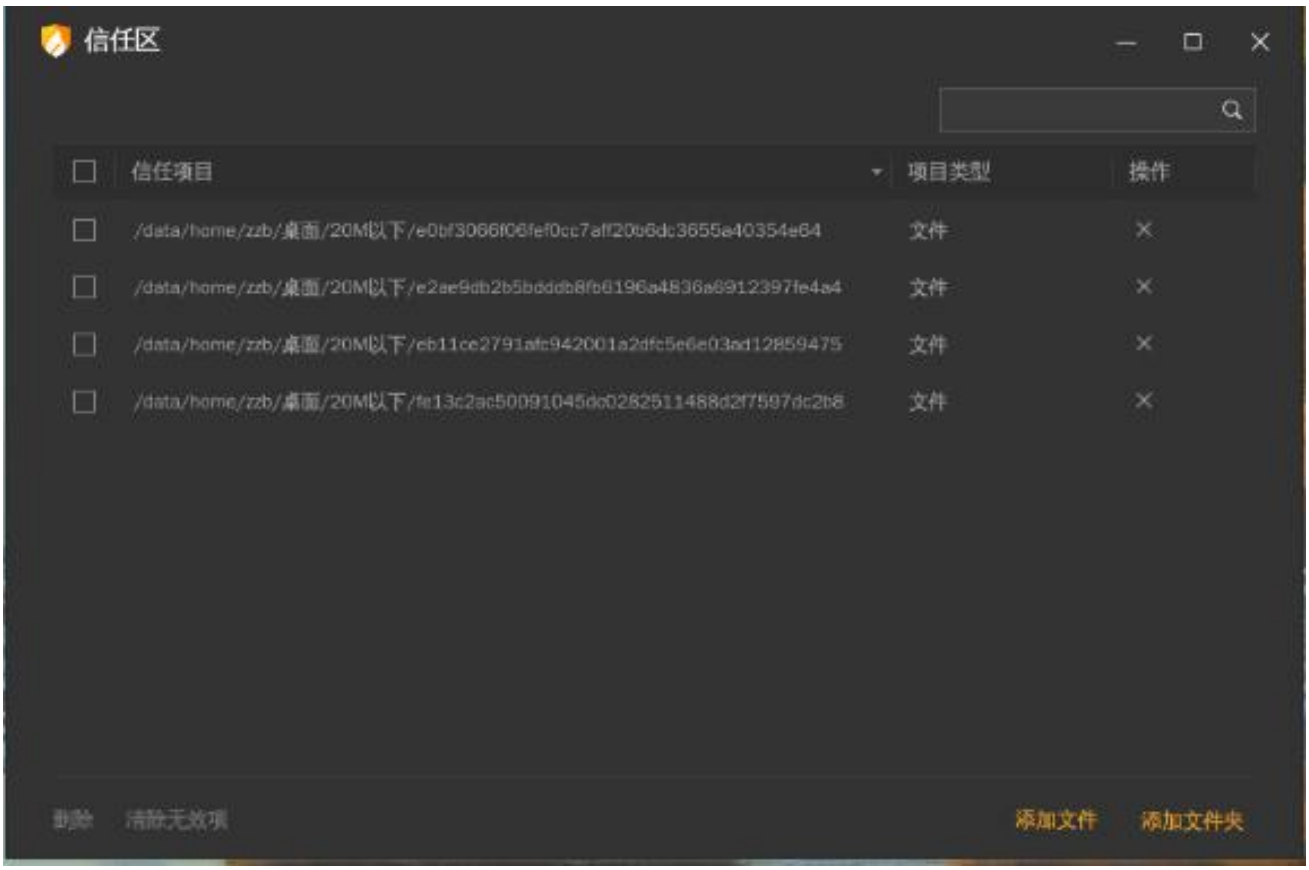
（2） 恢复：用户选中隔离区中的文件，单击右下角【恢复】按钮，即可恢复当前风险样本状态，不再隔离。

（3） 提取：用户选中隔离区中的文件，单击右下角【提取】按钮，即可提取当前风险样本至指定目录。



2. 信任区

火绒安全终端提供信任文件添加管理功能，用户确认安全的文件，不希望杀毒软件查杀的文件，可以添加信任，此列表中的文件或文件夹不会被病毒查杀、文件实时监控功能扫描。同时支持对已信任的文件取消信任。



5.2 终端信息

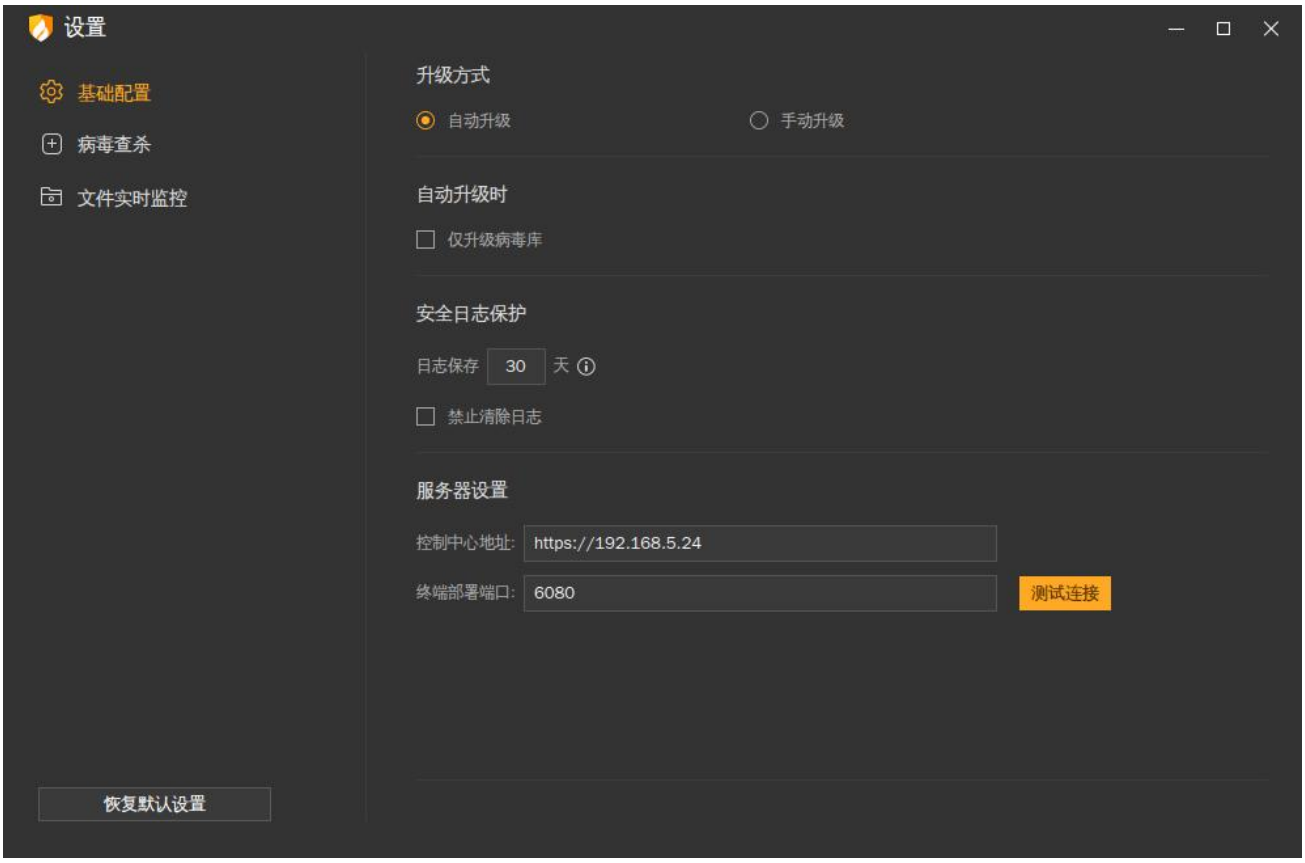
火绒安全终端提供用户查看当前终端状态便捷入口，用户点击右上角【终端信息】图标，可查看当前终端的终端名称、IP、MAC 地址等计算机基础信息，以及火绒终端版本、病毒库版本、与中心连接状态等信息。

5.3 更多功能

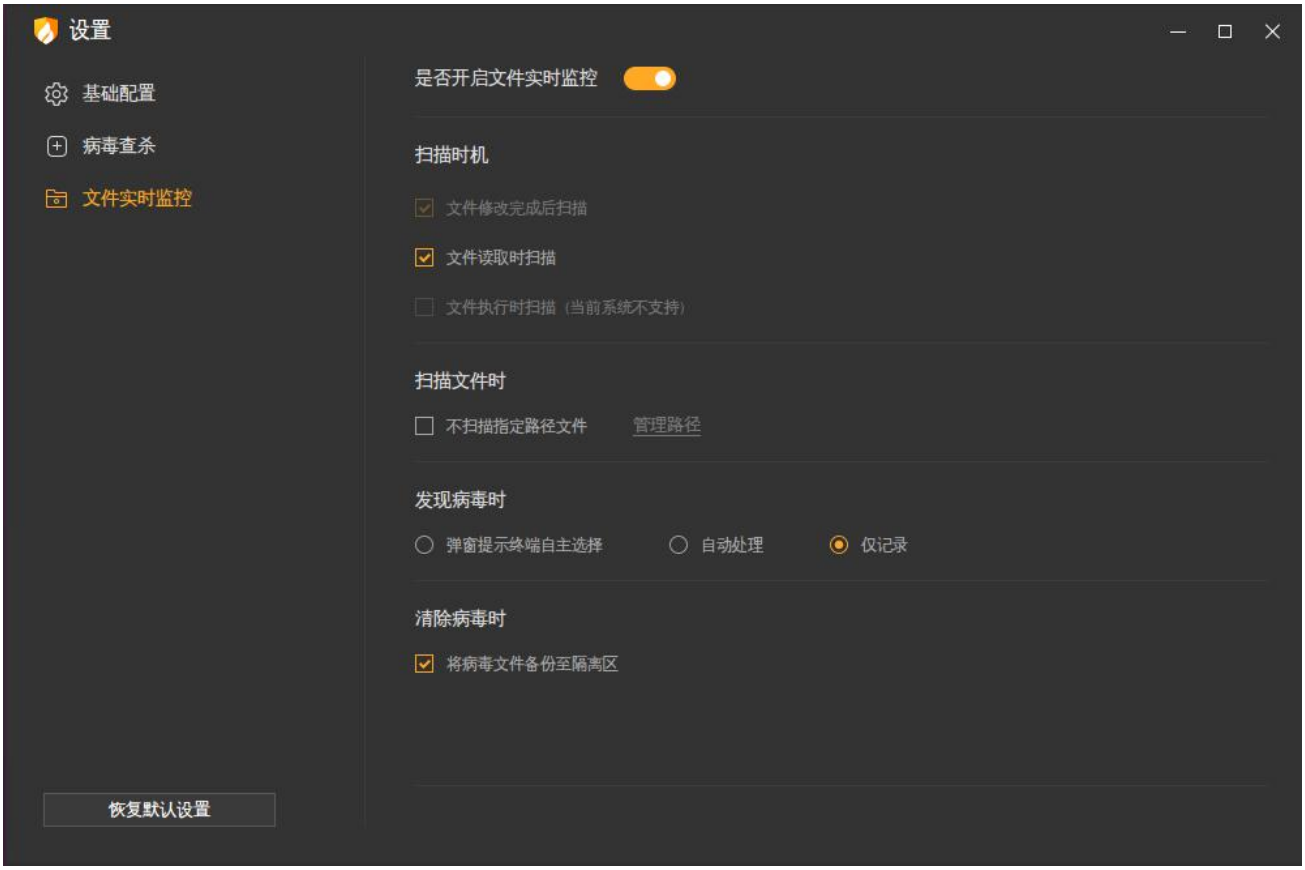
火绒安全终端提供了包括软件设置、安全日志、隔离区、信任区、语言设置、检查更新、联系网管、终端登记、关于火绒 9 个功能便捷访问入口，用户点击右上角【更多功能】按钮，可出现功能下拉菜单栏，点击可进入对应功能弹框界面。

5.3.1 安全设置

用户可点击【安全设置】打开设置，在设置中可对终端升级、弹窗显示、防御功能、文件实时监控的细节规则调整进行自定义配置。


设置
基础配置
病毒查杀
文件实时监控
升级方式
自动升级
手动升级
自动升级时
仅升级病毒库
安全日志保护
日志保存 30 天
禁止清除日志
服务器设置
控制中心地址: https://192.168.5.24
终端部署端口: 6080
测试连接
恢复默认设置


设置
基础配置
病毒查杀
文件实时监控
发现病毒时
询问我
自动处理
清除病毒时
将病毒文件备份至隔离区
全盘查杀设置
深度查杀压缩包中的病毒木马，并自动跳过大于 20 MB的压缩包(20M~9999M)
提示: 自定义扫描将自动扫描压缩包，并不受以上大小限制
不扫描
指定扩展名文件
扫描网络驱动器
恢复默认设置



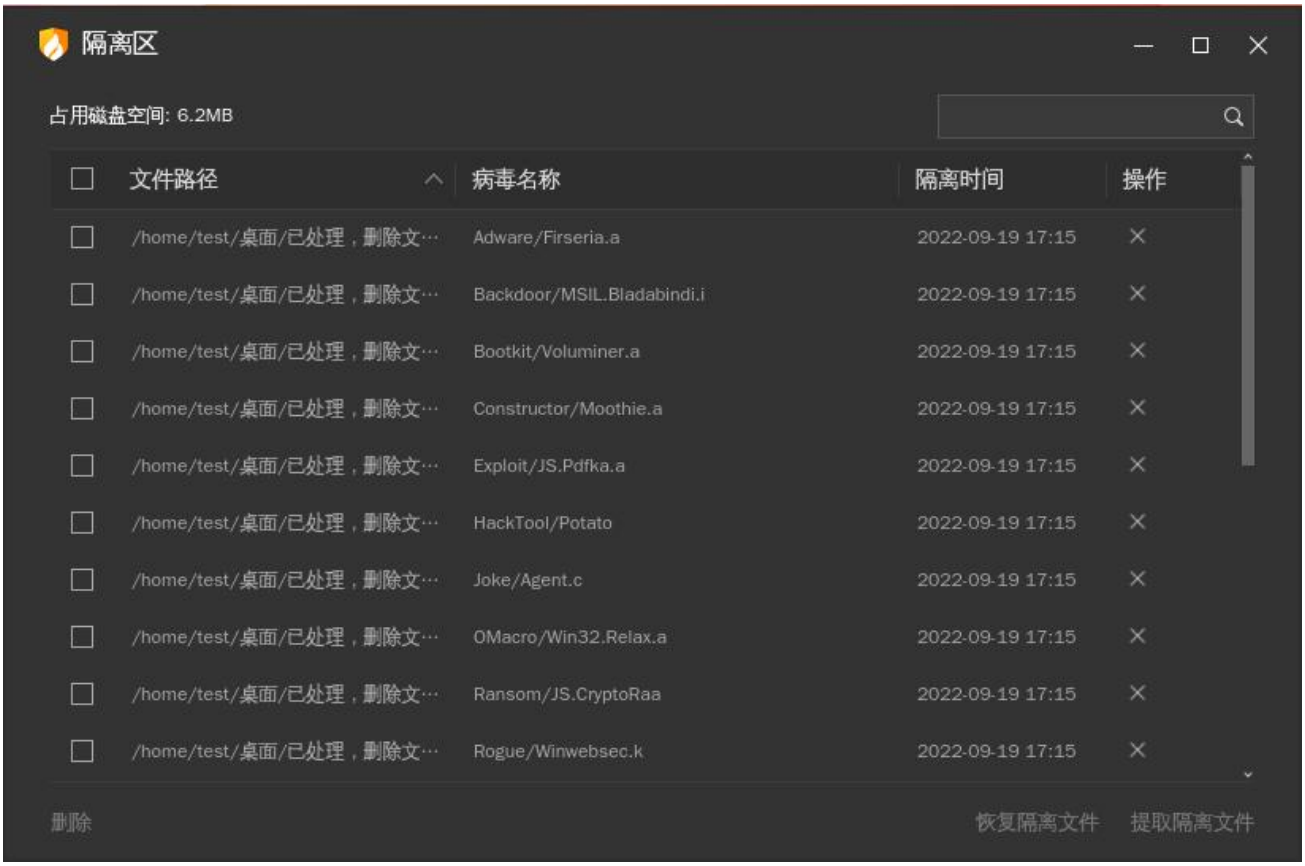
5.3.2 安全日志

用户可点击【安全日志】打开日志弹框，默认显示当天的日志信息，支持用户通过日期和模块筛选日志。可手动刷新日志信息，也可清除本页日志（中心策略为禁止清除日志时，终端用户不可清除日志）或将本页日志导出为独立文件。

5.3.3 隔离区

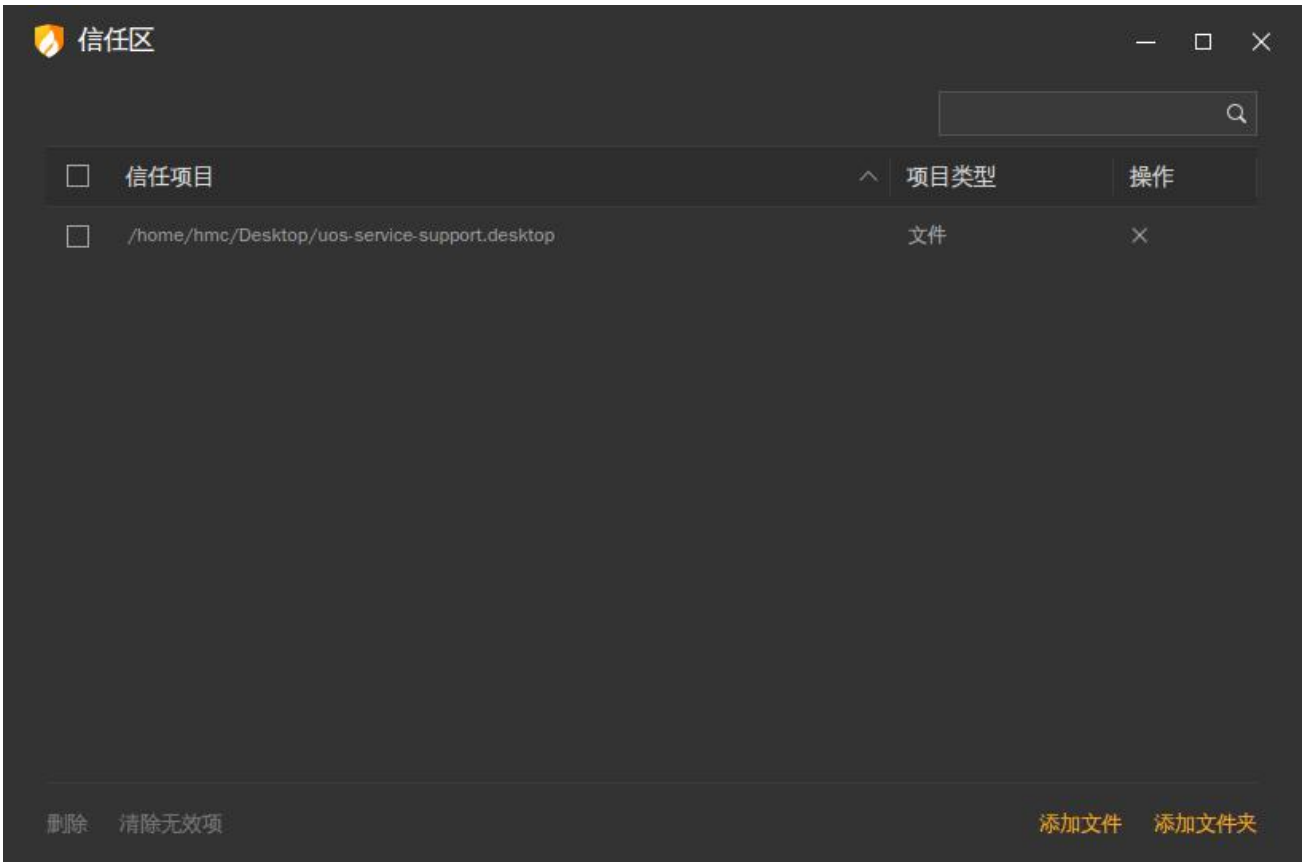
火绒安全终端会将扫描处理过的病毒威胁文件，经过加密后备份至隔离，以便您有特殊需要，可以主动从隔离区中重新找回被处理过的威胁文件。

用户可点击【隔离区】弹出文件隔离区弹框，用户可查看当前隔离区隔离的所有风险文件。



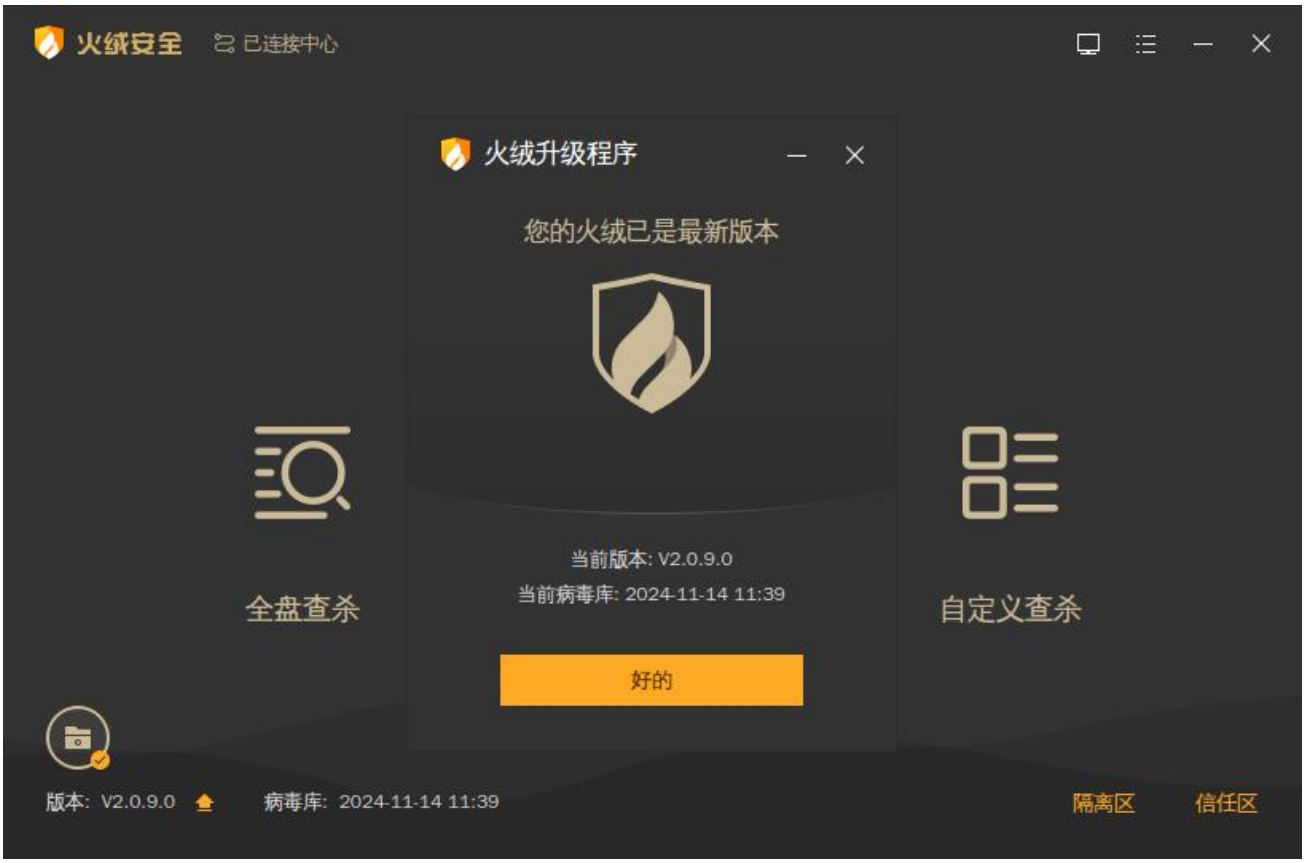
5.3.4 信任区

火绒安全终端提供信任文件添加管理功能，用户确认安全的文件，不希望杀毒软件查杀的文件，可以添加信任，此列表中的文件或文件夹不会被病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、Web 扫描功能扫描。信任区支持增加文件、文件夹与网址进行信任，同时支持对已信任的文件取消信任。



5.3.5 检查更新

火绒安全终端可手动检查终端版本，检查到新版本后可选择是否更新。



5.3.6 联系网管

火绒安全终端提供获取管理员联系方式功能，管理员在中心编辑完成管理员联系方式后，安全终端可点击【联系网管】查看管理员联系方式。

5.3.7 终端登记

火绒安全终端提供自助登记功能，管理员开启用户自助登记功能后，用户可以在终端设置中点击【终端登记】查看或填写登记信息。

5.3.8 关于我们

火绒安全终端提供关于火绒版权信息查看，用户可点击【关于我们】查看火绒的版权信息。


火绒安全
已连接中心
火绒正在保护您的电脑
关于火绒
火绒安全软件
北京火绒网络科技有限公司版权所有
Copyright©2012-2024 Huorong.All rights reserved.
查杀
版本: V2.0.9.0
病毒库: 2024-11-14 11:39
隔离区
信任区

第六章 火绒终端安全管理系统-macOS 终端

火绒终端安全管理系统安全终端作为安全防护功能执行终端，可以有效地帮助用户解决病毒、木马、流氓软件、恶意网站、黑客侵害等安全问题，为用户终端提供良好的运行环境。

6.1 首页

火绒安全终端首页为用户提供病毒查杀、版本更新、信任/隔离区功能、文件实时监控功能设置快速访问入口、查看网管信息以及当前终端版本、病毒库版本和当前连接中心（负载中心）的信息。

6.1.1 病毒查杀

在使用病毒查杀功能之前，需要在【隐私与安全性】中开启火绒安全终端的“完全磁盘访问权限”，否则无法使用病毒查杀功能。

1. 全盘查杀

全盘查杀功能会针对计算机包括系统进程、启动项、服务项、常用软件和物理存储磁盘进行全方位查杀。全盘查杀功能查杀位置全面，覆盖面广，所以应用此查杀方式安全性将大大提升，但是用时较长。

用户单击【全盘查杀】即可对本地环境进行病毒全盘查杀。

(1) 停止：用户可手动停止病毒全盘查杀任务，点击【停止】按钮，弹出确认框中点击【确定】即可终止当前查杀任务，并将已扫描查杀的数据告知用户。

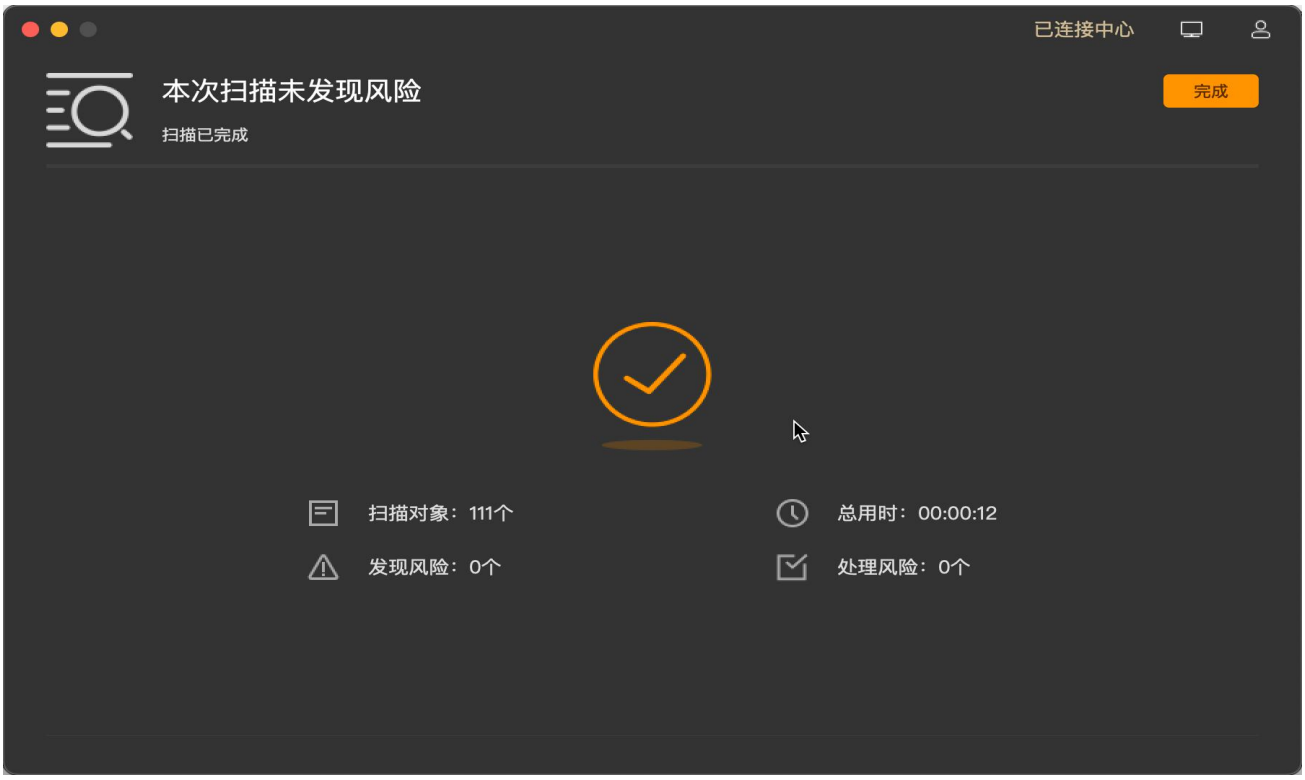
(2) 暂停：用户可暂停当前病毒查杀任务，点击【暂停】按钮，病毒查杀任务进入暂停状态，点击【继续】可继续当前查杀任务继续查杀，方便用户对当前任务进行管理。

(3) 常规：常规扫描模式下，病毒查杀任务会按照正常状态执行任务，不会特殊处理任务。

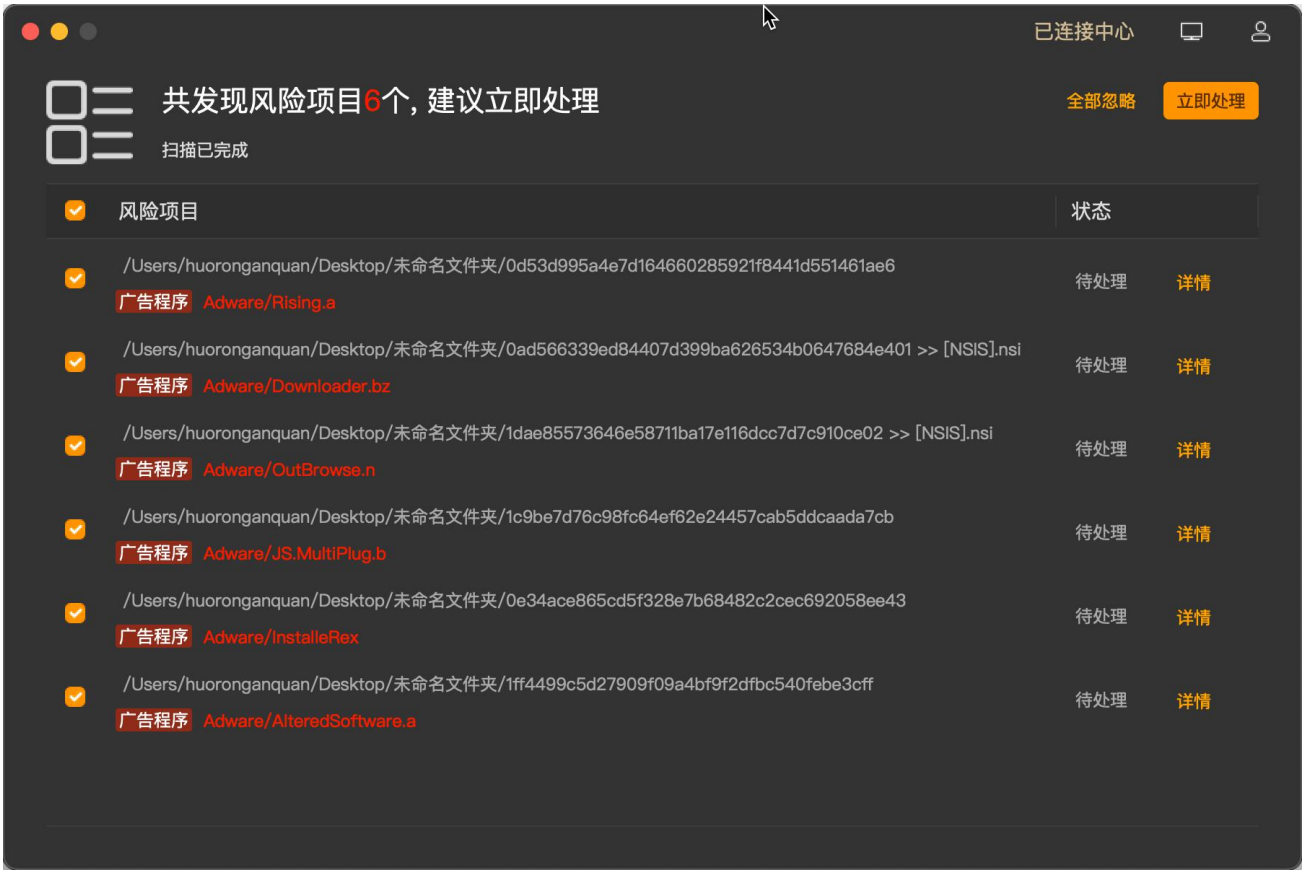
(4) 高速：高速扫描模式下，病毒查杀任务会提升优先级，增加系统资源调用以快速完成扫描任务。

(5) 查杀完成后自动关机：勾选此项后，病毒查杀任务查杀完成之后，将自动关闭计算机。

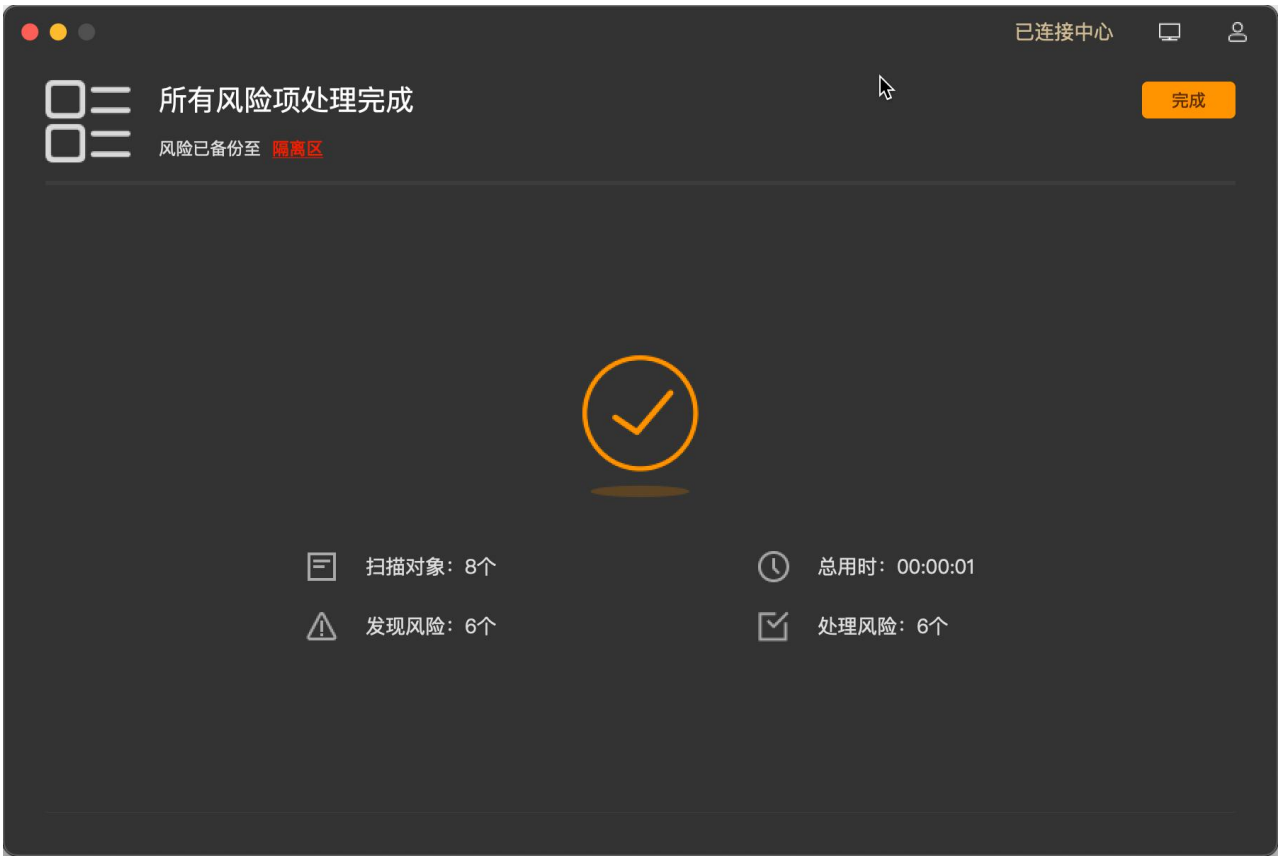
病毒查杀任务执行完成后，如未发现任何风险项，将为用户展示当前扫描对象、任务耗时等扫描任务详情信息，用户单击【完成】按钮后会返回终端主界面。



病毒查杀任务执行完成后，如发现风险项目，则会将风险项目展示给用户，用户可自行选择清理或忽略风险项目。



点击【立即处理】后，终端将自动处理已勾选风险项，并为用户展示处理结果及扫描任务结果。



2. 快速查杀

快速查杀功能会针对计算机包括系统进程、启动项、服务项、常用软件和系统关键位置这些敏感位置进行针对性查杀。快速查杀功能查杀位置相对全盘查杀较少，所以查杀速度较快。

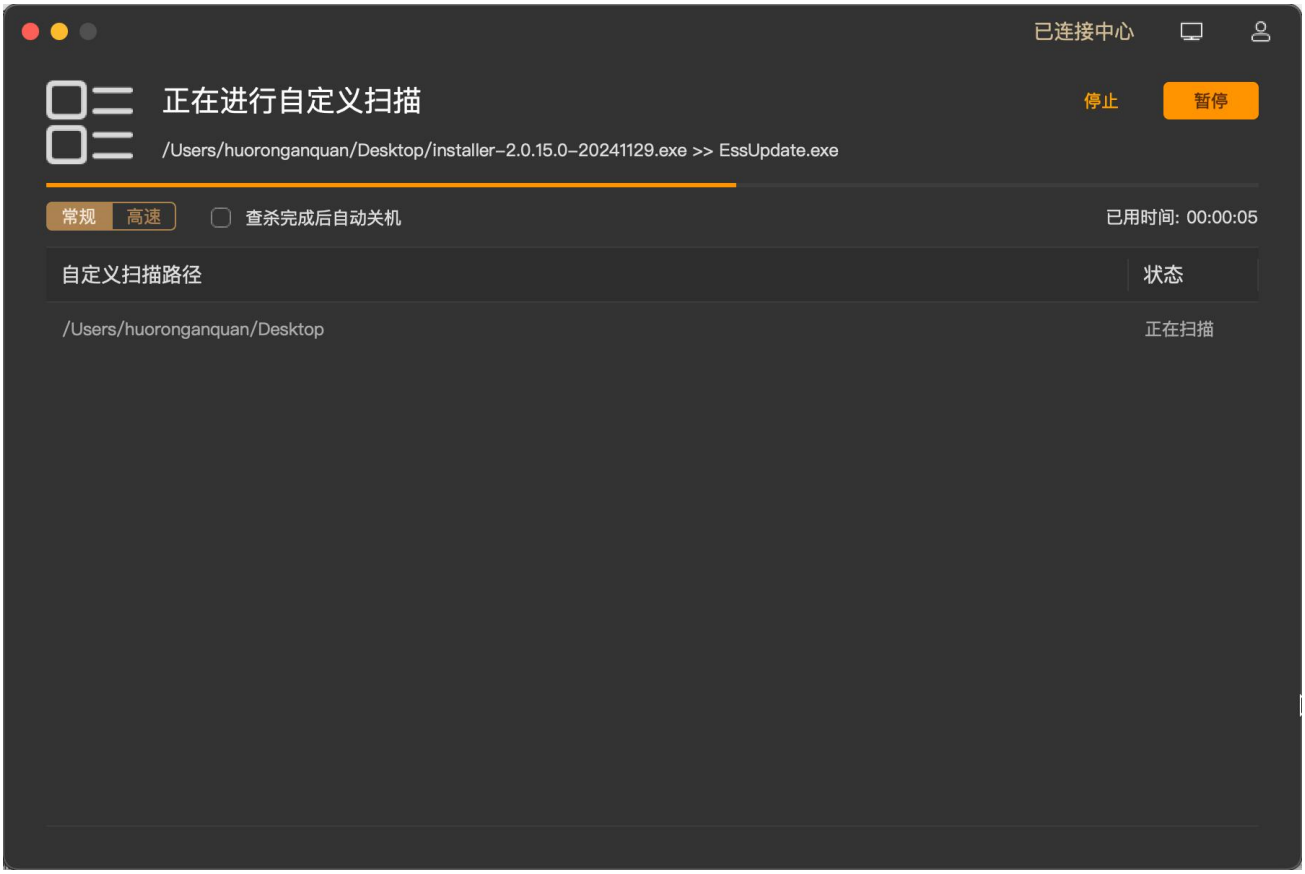
用户单击【快速查杀】即可对本地环境进行病毒快速查杀。

快速查杀任务处理结果及展示与全盘查杀相同，详情请参见全盘查杀功能。

3. 自定义查杀

自定义查杀功能可自定义选择查杀位置，方便用户定点查杀指定存储目录，病毒查杀任务更加灵活。

用户单击【自定义查杀】按钮，选择自定义查杀位置后单击【确定】即可对当前选择的查杀位置进行病毒查杀任务。



自定义查杀任务处理结果及展示与全盘查杀相同，详情请参见全盘查杀功能。

6.1.2 文件实时监控

在使用文件实时监控功能之前，需要在【隐私与安全性】中允许火绒安全终端安装“系统扩展”；否则无法使用文件实时监控功能。

在首页文件图标处可看到文件实时监控是否开启，点击进入安全设置对文件实时监控功能进行具体设置。可以选择在文件修改时，文件读取时或文件执行时检测文件是否安全，拦截病毒程序。在不影响电脑正常使用的情况下，实时保护用户的终端不受病毒侵害。

6.1.3 版本更新

火绒安全终端首页提供了终端版本信息和病毒库版本信息展示，为方便用户手动检查终端版本，火绒安全终端也提供便捷版本更新检测入口。

用户点击版本信息后方升级按钮，终端会自动检测当前终端版本信息，如果检查到终端未更新至最新版本，会提示用户当前有新版本，用户可自行选择是否更新为当前检测到的最新版本。

6.1.4 信任/隔离区

火绒安全终端首页提供了信任/隔离区快捷访问入口，方便用户快速查看及管理当前已信任及已隔离的文件。

1. 隔离区

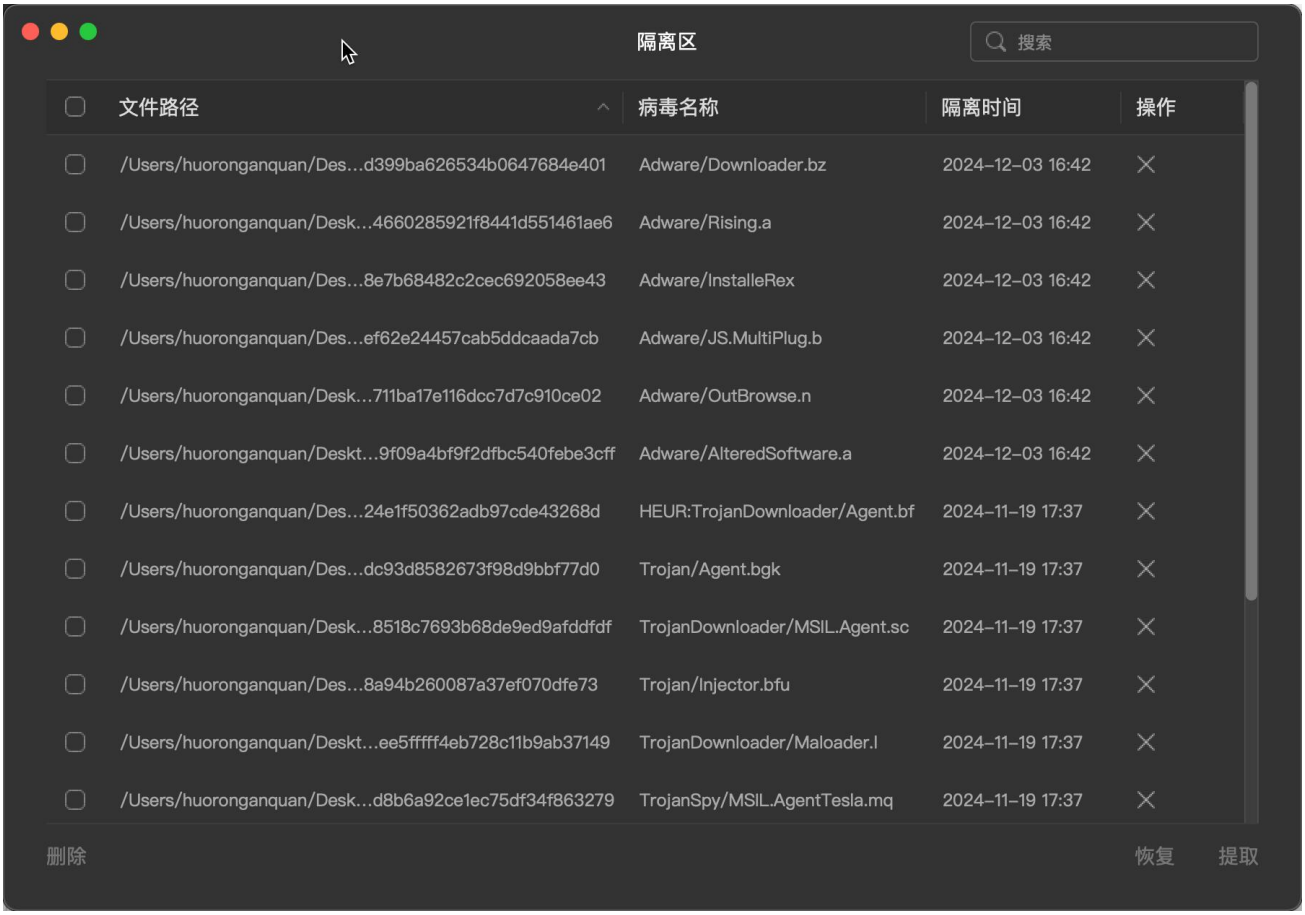
火绒安全终端会将扫描处理过的病毒威胁文件，经过加密后备份至隔离，以便您有特殊需要，可以主动从隔离区中重新找回被处理过的威胁文件。

用户单击火绒安全终端首页右下角【隔离区】弹出文件隔离区弹框，用户可查看当前隔离区隔离的所有风险文件。

（1） 删除：用户选中隔离区中的文件，单击左下角【删除】按钮，即可删除当前隔离区保存的风险文件样本。

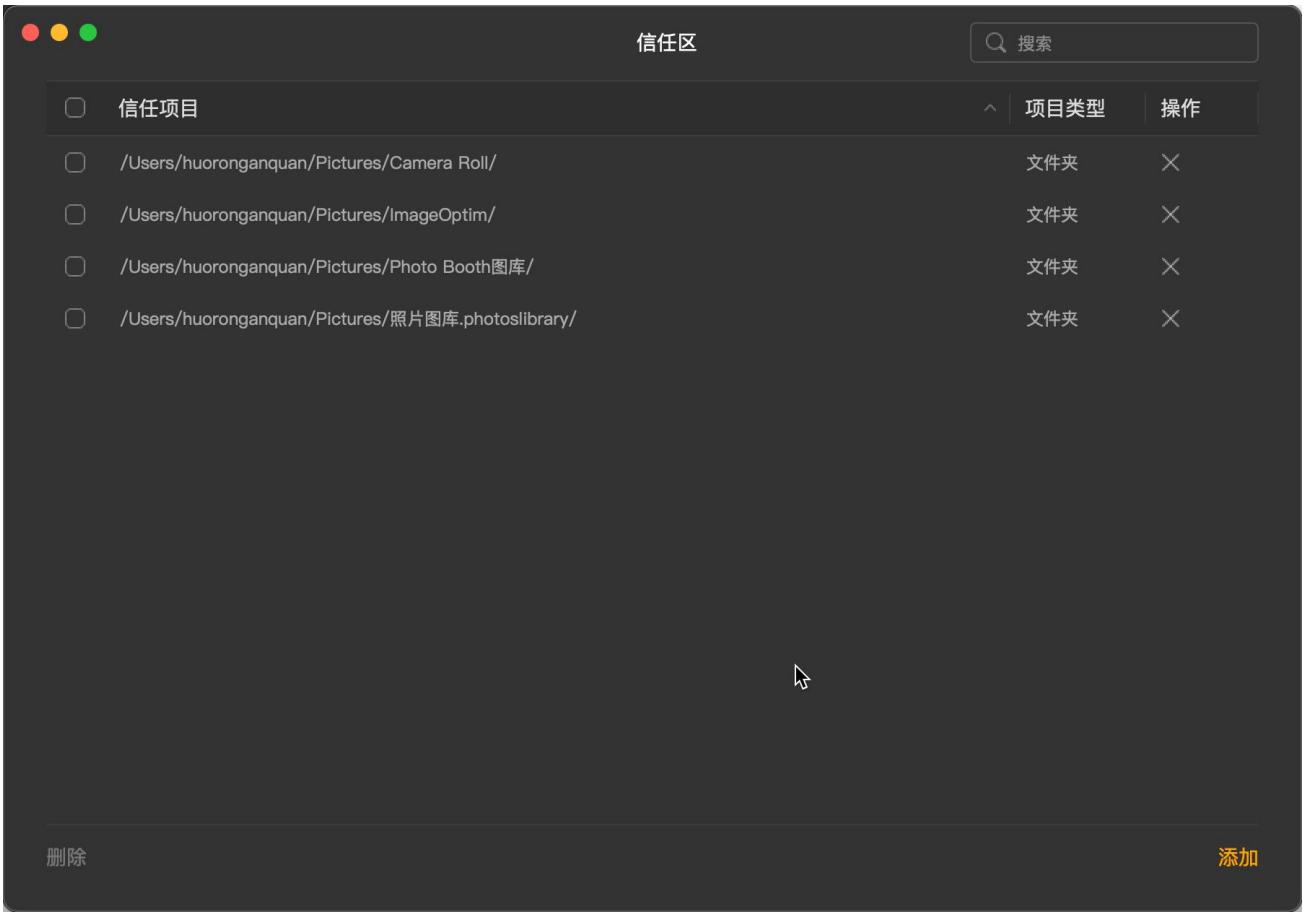
（2） 恢复：用户选中隔离区中的文件，单击右下角【恢复】按钮，即可恢复当前风险样本状态，不再隔离。

（3） 提取：用户选中隔离区中的文件，单击右下角【提取】按钮，即可提取当前风险样本至指定目录。



2. 信任区

火绒安全终端提供信任文件添加管理功能，用户确认安全的文件，不希望杀毒软件查杀的文件，可以添加信任，此列表中的文件或文件夹（下级文件夹）不会被病毒查杀、文件实时监控功能扫描。同时支持对已信任的文件取消信任。



6.1.5 联系网管

火绒安全终端提供获取管理员联系方式功能，管理员在中心编辑完成管理员联系方式后，安全终端可点击右上角小图标【联系网管】查看管理员联系方式。

6.2 终端信息

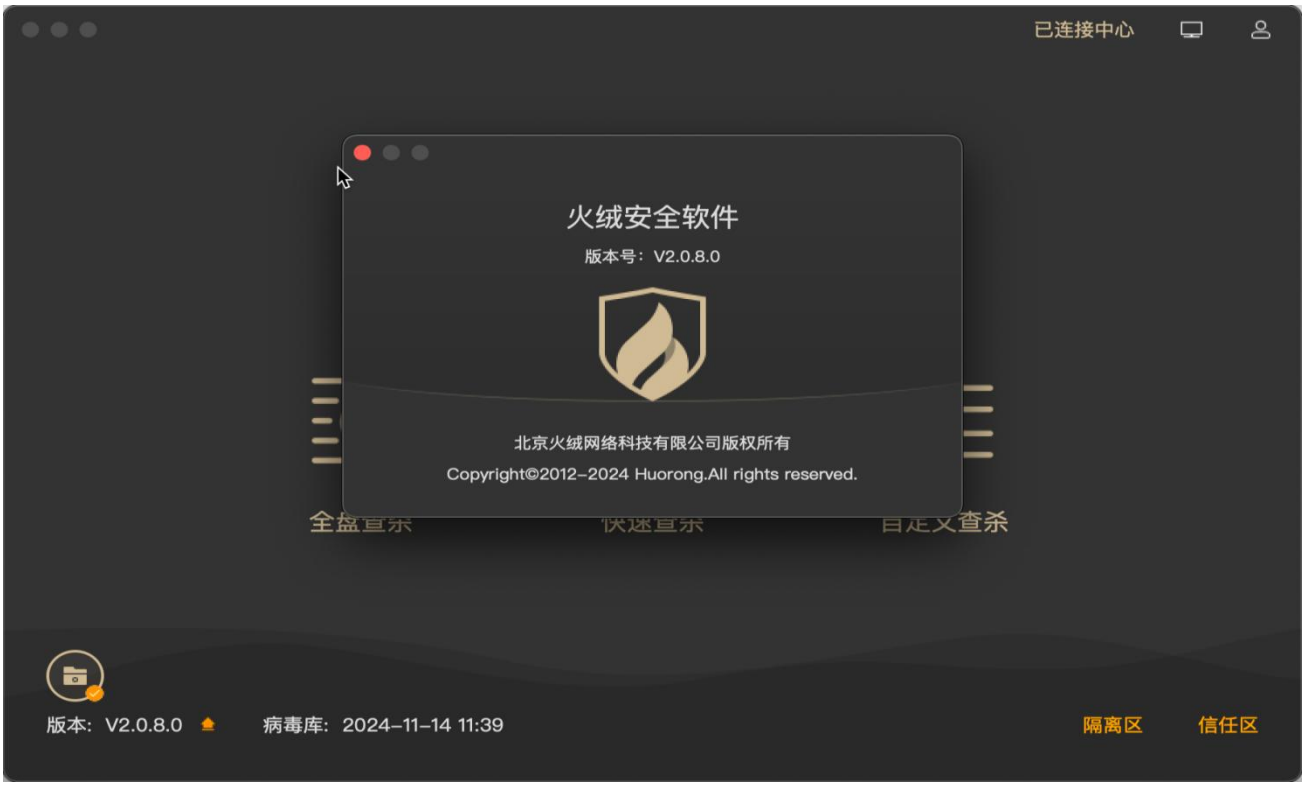
火绒安全终端提供用户查看当前终端状态便捷入口，用户点击右上角【终端信息】图标，可查看当前终端的终端名称、IP、MAC 地址等计算机基础信息，以及火绒终端版本、病毒库版本、与中心连接状态、当前连接的中心（负载中心）等信息。

6.3 更多功能

火绒安全终端提供了包括关于火绒安全终端、安全日志、检查更新、设置等功能便捷访问入口，用户点击顶部菜单栏左上角【火绒安全终端】按钮，可出现功能下拉菜单栏，点击可进入对应功能弹框界面。

6.3.1 关于我们

火绒安全终端提供关于火绒版权信息查看，用户可点击【关于我们】查看火绒的版权信息。



6.3.2 安全日志

用户可点击【安全日志】打开日志弹框，默认显示当天的日志信息，支持用户通过日期和模块筛选日志。可手动刷新日志信息，也可清除本页日志（中心策略为禁止清除日志时，终端用户不可清除日志）或将本页日志导出为独立文件。

6.3.3 终端登记

火绒安全终端提供自助登记功能，管理员开启用户自助登记功能后，用户可以在终端设置中点击【终端登记】查看或填写登记信息。

6.3.4 检查更新

火绒安全终端可手动检查终端版本，检查到新版本后可选择是否更新。

6.3.5 安全设置

用户可点击【安全设置】打开设置，在设置中可对基础设置、病毒查杀、文件实时监控功能的细节规则调整进行自定义配置。


设置
基础设置
病毒查杀
文件实时监控
升级方式:
自动升级
手动升级
自动升级时:
仅升级病毒库
安全日志保护:
日志保存
30
天
禁止清除日志
服务器设置:
控制中心地址:
http://192.168.3.41
终端部署端口:
6080
测试连接
恢复默认设置


设置
基础设置
病毒查杀
文件实时监控
发现病毒时:
询问我
自动处理
清除病毒时:
将病毒文件备份至隔离区
全盘查杀设置:
深度查杀压缩包中的病毒木马，并自动跳过大于
20
MB的压缩包
(20M~9999M)
提示: 自定义扫描将自动扫描压缩包，并不受以上大小限制
不扫描
指定扩展名文件
例如: .tmp; .txt; .log; .db
扫描网络驱动器
恢复默认设置


设置
基础设置
病毒查杀
文件实时监控
是否开启文件实时监控
扫描时机:
文件修改完成后扫描
文件读取时扫描
文件执行时扫描
扫描文件时:
不扫描指定路径文件
管理路径
发现病毒时:
弹窗提示终端自主选择
仅记录
自动处理
清除病毒时:
将病毒文件备份至隔离区
恢复默认设置