火绒安全
HUORONG SECURITY

火绒终端安全管理系统 1.0

使用手册

2022/06/24

公　　司：北京火绒网络科技有限公司

地　　址：北京市朝阳区红军营南路 15 号瑞普大厦 D 座 4 层

网　　址：https://www.huorong.cn

电　　话：400-998-3555

版权声明

目录

一、概述

欢迎阅读《“火绒终端安全管理系统 1.0”使用手册》。为了能够更好的服务于用户，特别编写本手册，方便用户在第一次使用本产品时快速了解其中每个模块的功能，并掌握其操作方法及流程，解决用户在使用本产品时遇到的问题。

“火绒终端安全管理系统 1.0”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 1.0”产品优势及特点：

（一）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。

（二）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。

（三）成熟的终端，强悍轻巧干净。

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。

（四）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，将单位内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 1.0”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。

Tips:

- 如果您想了解“火绒终端安全管理系统 1.0”核心技术及理念策略，请参阅《“火绒终端安全管理系统 1.0”技术白皮书》。
- 如果您想了解“火绒终端安全管理系统 1.0”的安装需知和部署流程，请参阅《“火绒终端安全管理系统 1.0”安装部署手册》。

- 如果您想了解“火绒终端安全管理系统 1.0”产品的详细介绍，请参阅《“火绒终端安全管理系统 1.0”产品说明书》。

二、访问控制中心

2.1 访问方式

控制中心访问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：

- 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。

- 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输入地址+端口访问，在浏览器地址栏中输入：http(s)://[控制中心所在终端 IP 地址或者域名]，即可访问控制中心。

2.2 登录/登出

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，点击【登录】按钮验证通

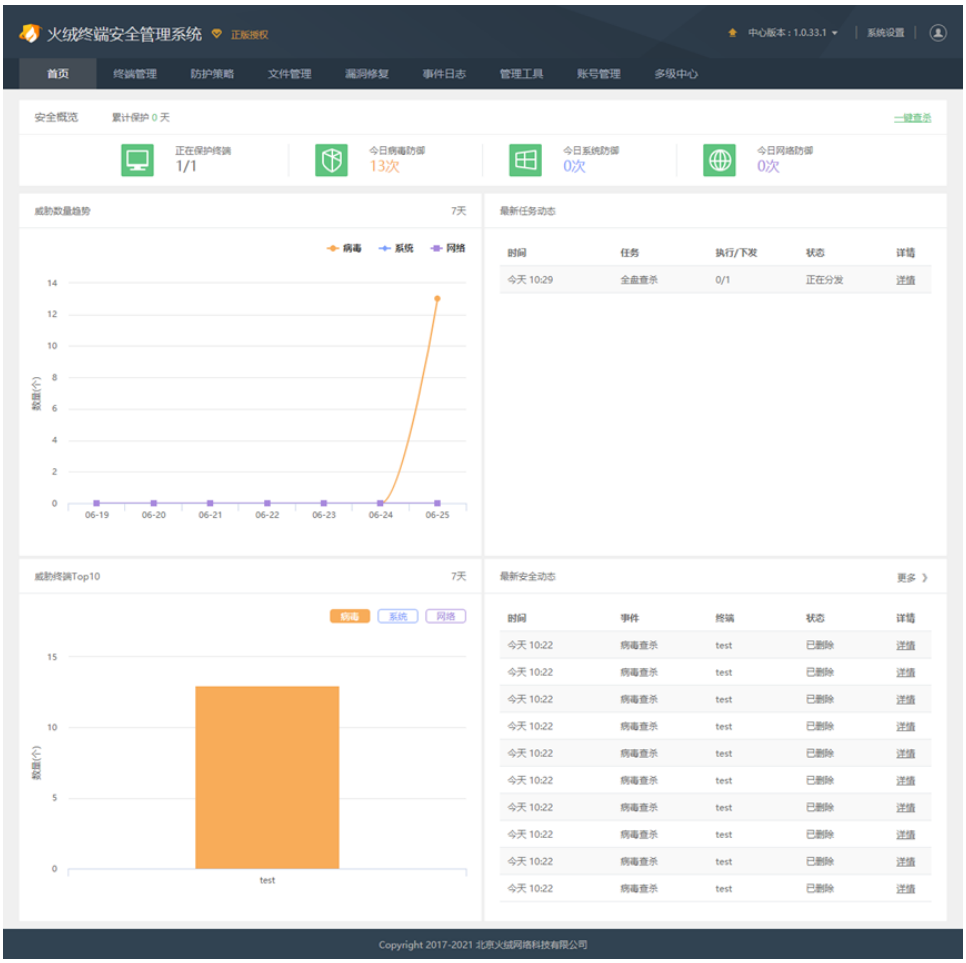
过后即可登录控制中心。

注：

- 密码输入错误 5 次后，将会在 15 分钟之内限制登录。
- 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。
- 超级管理员默认账号：admin 默认密码：admin
- 下次自动登录：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，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，用户可根据自身管理员账户属性，对应使用不同的解决方案。

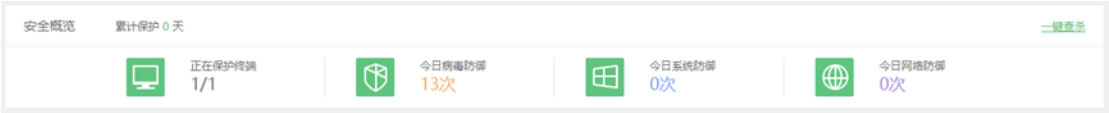
三、首页

通过【首页】界面可以更加直观的查看今日以及最近 7 天的终端总体安全概况



3.1 安全概览

安全概览包括了累计保护天数、一键查杀的快捷方式、正在保护的终端数目，同时包含了病毒、系统、网络防护的今日防御状态。



3.2 威胁数量趋势

威胁数量趋势折线图包含了病毒、系统、网络防护三大模块的近 7 天的防御情况。也可以点击查看具体某一模块的威胁数量趋势。

3.3 最新任务动态

最新任务动态模块包含了最新的任务收发情况。

时间	任务	执行/下发	状态	详情
今天 16:35	快速查杀	11/31	正在分发	详情
今天 15:07	升级任务	2/2	分发结束	详情
今天 15:06	升级任务	1/1	分发结束	详情
今天 13:56	通知任务	1/1	分发结束	详情
今天 13:55	通知任务	1/1	分发结束	详情
今天 13:11	升级任务	1/1	分发结束	详情
今天 10:31	通知任务	1/1	分发结束	详情
今天 10:30	通知任务	1/1	分发结束	详情
今天 10:29	通知任务	1/1	分发结束	详情
今天 10:26	通知任务	1/1	分发结束	详情

3.4 威胁终端 Top10

威胁终端 Top10 模块展示了控制中心下属终端受到威胁最多的前十名，可切换病毒、系统、网络防护的视角进行查看。

3.5 最新安全动态

最新安全动态模块包含了控制中心所有终端最新的安全防护的事件。

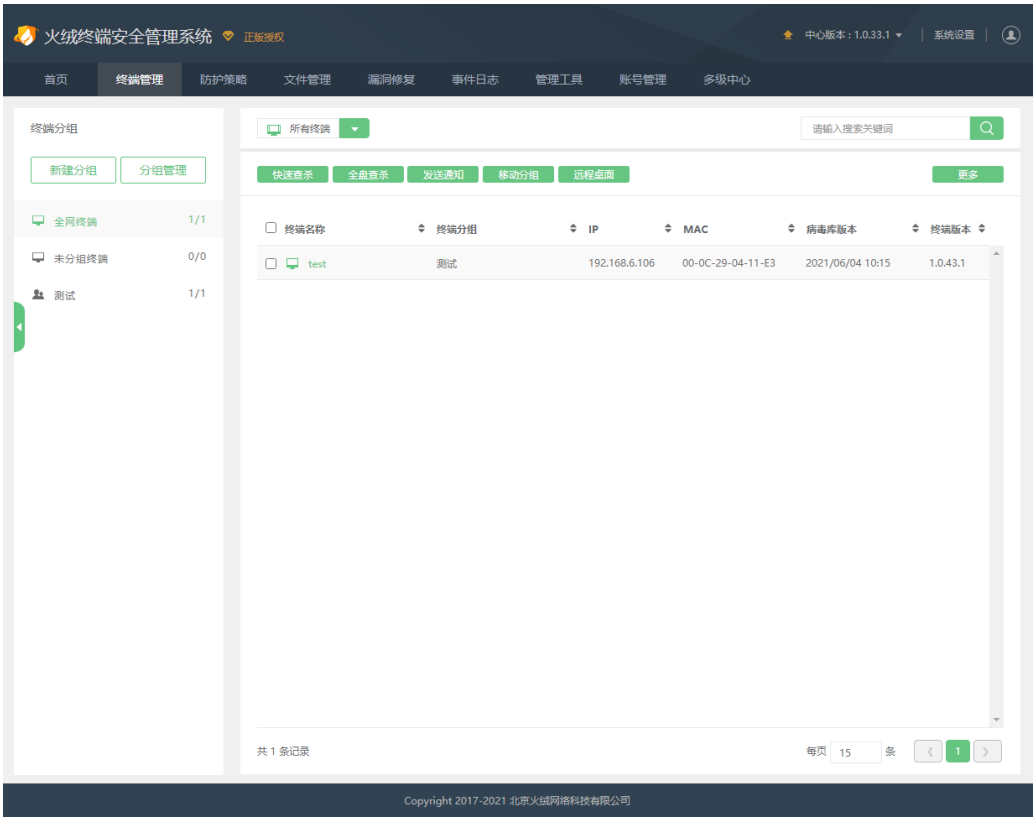
3.6 在线升级

火绒控制中心顶部包含了在线升级，中心最新版本，终端最新版本以及系统设置

当需要升级时，手动点击如图所示按钮进行更新检测。有新版本时即可进行升级

四、终端管理

通过终端部署的终端将会出现在终端管理模块（如下图即为刚刚部署的终端）



4.1 终端详情

通过点击终端名称可进入终端详情界面，支持管理员手动修改终端名称，修改后安全终端处对应显示修改后的终端名称；同时也统计了当前终端的网络信息、环境信息、终端版本及病毒库等其他信息，可供管理员查看。

4.2 快速查杀、全盘查杀

4.2.1 功能介绍

病毒查杀是安全杀毒软件的基础功能，您可以利用病毒查杀主动扫描在电脑中是否存在病毒、木马等威胁。

4.2.2 操作流程

第一步：控制中心选择需要进行病毒查杀的终端下发查杀任务。

第二步：可以通过修改查杀配置，管理终端对于查杀病毒的处理。

第三步：下发任务后，终端将在一定时间内接收任务进行查杀扫描任务、并且采取控制中心配置进行处理。

4.2.3 设置说明

- 当控制中心向终端下发查杀任务后，火绒客户端将会在后台自动进行扫描任务；当扫描完成发现病毒、木马时，根据部署的策略进行处理。
- 当您选择了需要查杀的目标，火绒将通过自主研发的反病毒引擎高效扫描目标文件，及时发现病毒、木马，并帮助您有效处理清除相关威胁。

4.3 发送消息

操作流程：

第一步：控制中心选择需要发送消息的终端进行消息的分发

第二步：输入消息的内容主体

第三步：确认下发消息通知

第四步：终端安全软件接收到消息后会进行弹窗提示

4.4 移动分组

4.4.1 功能介绍

用户可以将新加入的终端或者未分组终端移入到指定分组进行管理

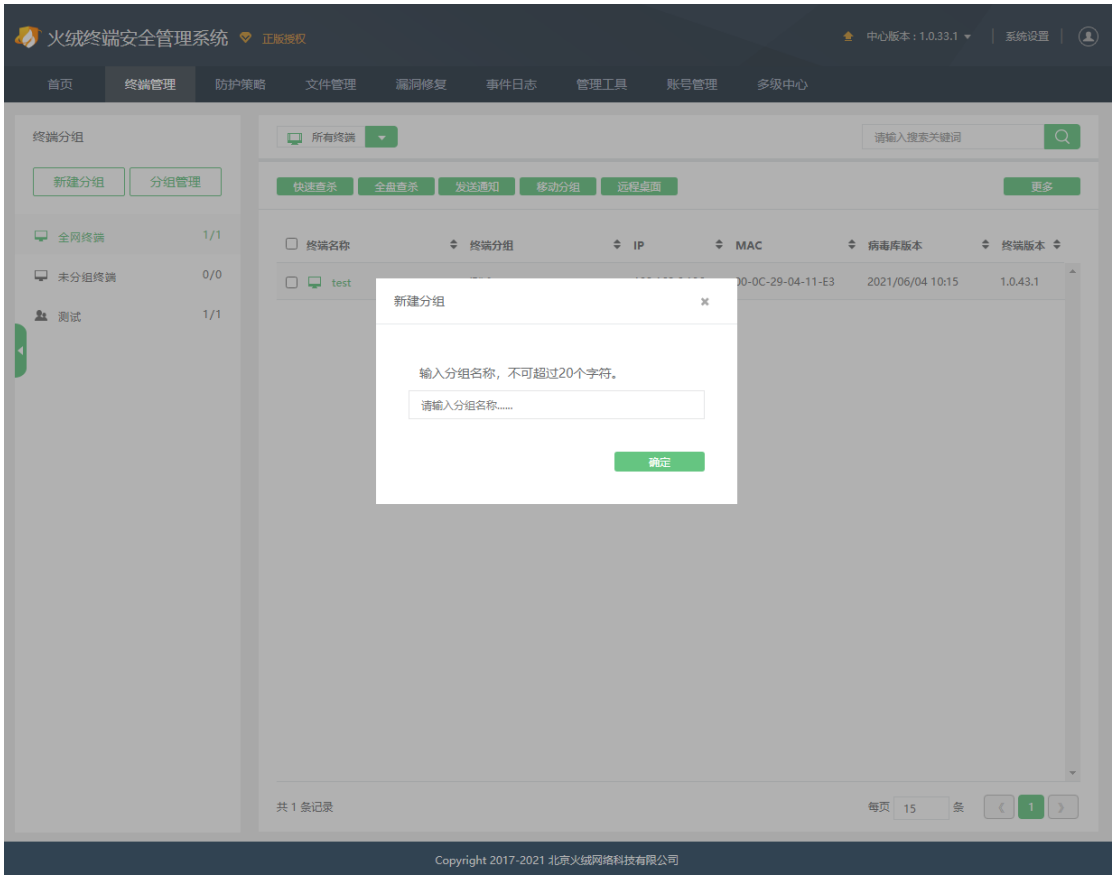
4.4.2 操作流程

第一步：点击打开终端管理

第二步：点击新建分组

第三步：输入分组名称新建

第四步：进行移动分组



4.5 远程桌面

4.5.1 功能介绍

管理员通过远程桌面控制客户端，帮助解决客户端使用过程中遇到的问题

4.5.2 操作流程

第一步：点击打开终端管理

第二步：点击远程桌面

第三步：选择远程类型、填写远程原因

第四步：点击确定，等待终端响应即可

4.5.3 设置说明

支持浏览器版本：Chrome 69 以上 ，Firefox 60 以上，Safari（推荐最新版），Opera 56 以上 ，Edge 17 以上，暂不支持 IE 浏览器

4.6 更多

- 终端升级：下发任务将控制中心所属终端升级软件版本以及病毒库
- 关机：下发任务将控制中心下属终端关机
- 重启：下发任务将控制中心下属终端重启
- 扫描漏洞：下发任务扫描终端漏洞，并将终端漏洞信息上报至中心
- 删除终端：将控制中心下属离线终端隔离出控制中心。
- 导出：将选择的终端的详情信息导出 excel

注：所有的任务将会在 30 秒左右被终端响应

五、防护策略

5.1 策略部署

5.1.1 功能介绍

策略的内容实质上与火绒安全软件的防护中心的各个功能相对应。用户可以在此为各个分组内的终端设置对应的防护策略，使终端具备自动处理事件的能力，提升系统安全性。

5.1.2 操作流程

第一步：点击打开防护策略

第二步：选择策略部署

第三步：建立一个新的策略

第四步：编辑刚刚新建的策略

第五步：选择分组并且部署防护策略

5.2 策略管理

5.2.1 终端说明（Windows 客户端防护中心）

5.2.1.1 病毒防御

文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控

- **文件实时监控**

当策略部署火绒文件实时监控开启时，默认情况下会在程序运行时，先实时扫描即将运行的程序是否安全，并拦截病毒程序执行，从而实时保护您电脑不受病毒侵害，同时不影响电脑日常使用。

当有威胁触发了【文件实时监控】时，根据部署的策略进行处理并提示。

- **恶意行为监控**

恶意行为监控是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，从而可以作为传统特征查杀的补充，极大提升电脑反病毒能力。

当有威胁触发了【恶意行为监控】时，根据部署的策略进行处理并提示。

- **U 盘防护**

为了避免病毒通过 U 盘进入电脑，在 U 盘接入电脑时，对 U 盘进行快速扫描，及时发现风险。同时移动存储设备也会自动纳入文件实时监控等其他监控功能保护范围，全方位保护您电脑的安全。

当有威胁触发了【U 盘防护】时，根据部署的策略进行处理并提示。

- **下载防护**

火绒将在您使用浏览器、下载工具、IM 进行文件下载时对文件进行病毒扫描，在病毒文件进入电脑的时候就将其查杀。

当有威胁触发了【下载保护】时，根据部署的策略进行处理并提示

- **邮件监控**

火绒将在您使用邮箱收、发邮件时，对邮件进行监控；

当有威胁触发了【邮件监控】时，根据部署的策略进行处理并提示。

5.2.1.2 系统防御

系统加固、软件安装拦截、浏览器保护

- **系统加固**

为了阻止不适合直接查杀的程序对您的电脑系统恶意篡改等行为，火绒提供了一套全方位的加固方案，保护您的电脑系统各个安全关键点。

当有威胁动作触犯【系统加固】时，火绒会弹窗提示，终端用户可以根据需要选择对这个动作的处理方式。

- **软件安装拦截**

在安装软件的时候，判断软件是否是推广软件，从而避免在不知情的情况下安装不需要的软件。

当发现有推广软件正在安装时，火绒会弹窗提示，您可以根据需要选择是否安装此软件。

- **浏览器保护**

由于恶意程序有可能通过篡改、锁定、劫持等各种侵犯您的权益的方式控制您的浏览器主页。这些侵权行为导致您的主页可能被不同软件反复篡改，影响您的体验。

火绒提供浏览器保护，可以锁定浏览器首页，防止您的浏览器设置被恶意篡改。（浏览器保护支持部分浏览器）

功能	说明
阻止	阻止本次安装行为
允许安装	允许本次安装行为
记住本次操作，下次自动处理	勾选后将记住这次的操作行为，下次再遇到此软件的安装，将会自动执行本次的选择，不再弹窗提示。

5.2.1.3 网络防御

黑客入侵防御、对外攻击检测、远程登录防护、恶意网站拦截

- 黑客入侵拦截

黑客入侵拦截将检测您通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免您的电脑遭到黑客入侵。

当有发现有黑客入侵时，火绒将阻止入侵，并通过托盘 tips 通知。

- **对外攻击检测**

黑客通过各种方式入侵了您的电脑后，可能利用您的电脑向其他终端目标发起对外攻击，从而达到破坏其他终端或致使其他终端网络瘫痪的目的。火绒提供对外攻击检测，防止您的电脑被黑客入侵后的对外对外攻击行为，避免您的利益受到损害。

当有发现有对外攻击时，火绒将记录攻击行为，并通过托盘 tips 通知。

- **远程登录防护**

黑客可以通过远程登录的方式访问电脑主机，一旦远程登录进入主机，用户可以操作主机允许的任何事情。当有发现 RDP 远程登录请求时，火绒将阻止登录行为。

- **恶意网址拦截**

恶意网站通过种植木马、病毒等恶意程序，发布虚假、欺骗信息，仿冒正规网站等手段，伪装诱导您等方式，使您的计算机感染病毒，造成您的损失。恶意网站拦截功能，可以在您访问网站时自动分辨即将访问的网站是否存在恶意风险。

当用户访问到有恶意风险的网站时，火绒将拦截网站并提示。

5.2.1.4 访问控制

- IP 协议控制

管理员可以通过添加 IP 地址、端口和协议类型等数据来创建规则，对入站和出站的网络协议数据进行控制，提前规避风险，增强终端使用安全。

- IP 黑名单

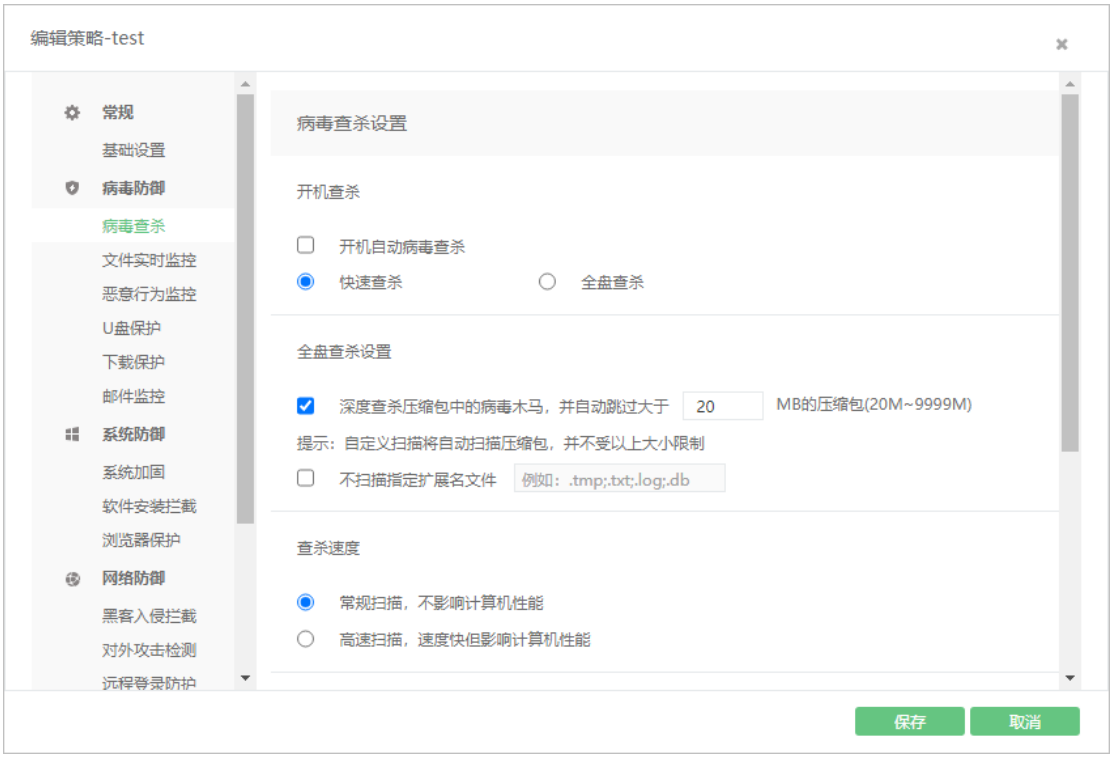
管理员可以将已知的恶意 IP 地址加入 IP 黑名单，添加入黑名单的 IP 将无法访问此电脑主机，保障主机不被恶意 IP 攻击。

- 设备控制

病毒通过 U 盘等外接设备传入，导致计算机感染病毒；机密文件、隐私信息等通过 U 盘等外接设备流出，导致信息泄露。设备控制功能，可以对终端进行统一的设备管控，保障隐私信息安全以及防止病毒从外传播。

当用户使用外接设备时，火绒将拦截设备并提示。

5.2.2 中心说明（防护策略）



5.2.2.1 病毒防御

- 病毒查杀

功能		说明
开机查杀	快速查杀	开机时自动对终端进行快速查杀
	全盘查杀	开机时自动对终端进行全盘查杀
全盘查杀设置	深度查杀	根据需要深度查杀压缩包中的病毒
	排除设置	病毒查杀时自动跳过指定扩展名的文件。 填写格式：.tmp;.txt;.log;.db 每个文件类型只需要填写.扩展名，多个文件类型之间用英文;来区分。
查杀速度		常规查杀将不影响计算机性能 快速查杀将占用计算机资源，快速
系统修复设置		扫描出威胁以及可修复项后选择是否修复
发现病毒时	弹窗提示	扫描出威胁后，询问您，让您来自主处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
清除病毒时	将病毒文件备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删

- **文件实时监控**


是否开启文件实时监控
开启
扫描时机
在文件执行时进行扫描,不影响性能（推荐）
在文件发生变化时进行扫描,将占用少量系统资源
在文件发生所有类型操作时进行扫描，将占用较多系统资源
排除设置
不扫描指定的程序的动作
发现病毒时
弹窗提示终端自主选择
自动处理
清除病毒时
将病毒文件备份至终端本地隔离区

功能		说明
扫描时机		根据您的需要和电脑配置情况选择实时监控生效时机 文件执行是指类似于 exe 等文件被双击打开 文件发生变化是指编辑等操作 文件所有类型操作是指移动等操作
排除设置		病毒实时监控的过程中，不扫描指定程序的文件操作。 填写事例：C:\Program Files\Test\>.exe;*\Test.exe 填写说明：需要填写要排除的程序路径，多条路径之间用英文;分割，*代表任意字符串，>代表该目录下所有指定类型的文件，但不包括子目录
发现病毒时	弹窗提示	扫描出威胁后，询问您，让您来自主处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
清除病毒时	将病毒文件备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删

- **恶意行为监控**

功能		说明
发现病毒时	弹窗提示	扫描出威胁后，询问您，让您来主动处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
清除病毒时	将病毒文件备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删
增强勒索病毒防护	开启勒索病毒诱捕	勾选后，将在系统中自动创建勒索病毒诱捕文件，一旦发现勒索病毒可快速处理。

- **U 盘保护**

功能		说明
U 盘介入电脑时	第一项	扫描 U 盘内是否存在被病毒修改的项目，如果存在，则提示您修复。
	第二项	扫描 U 盘根目录下是否存在威胁文件。
发现病毒时	弹窗提示	扫描出威胁以后，询问您，让您来主动处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
清除病毒时	将病毒文件备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删
压缩包扫描设置		根据需要深度查杀压缩包中的病毒

- **下载保护**

功能		说明
发现病毒时	弹窗提示	扫描出威胁后，询问您，让您来主动处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
清除病毒时	将病毒文件备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删
压缩包扫描设置		根据需要深度查杀压缩包中的病毒
排除设置		在文件下载的过程中，下载保护功能将不扫描填写的文件类型。填写格式：.tmp;.txt;.log;.db。每个文件类型只需要填写.扩展名，多个文件类型之间用英文;来区分。

- **邮件监控**

功能		说明
清除病毒时	将病毒文件备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删
邮件扫描	查杀病毒	自动跳过大于 20M 的邮件
邮件规则	端口、协议	需要支持 SMTP 或 POP3 的邮件软件方可

5.2.2.2 系统防御

- 系统加固

系统项目	说明
文件保护	保护基础文件不被篡改、破坏或恶意创建
注册表保护	防止特定注册表项目不被恶意篡改
危险动作拦截	监控针对系统的敏感性为，拦截高风险动作
执行防护	阻止特定命令行被恶意利用的行为
进程保护	保护系统重要进程，不会被攻击利用
病毒免疫	定义了一些通常只有病毒才会执行的恶意操作，从而免疫执行这些操作的病毒

- **软件安装拦截**

功能	说明
常规模式	根据用户需求弹窗提示是否安装软件
严格模式	自动阻止推广软件的一切安装行为

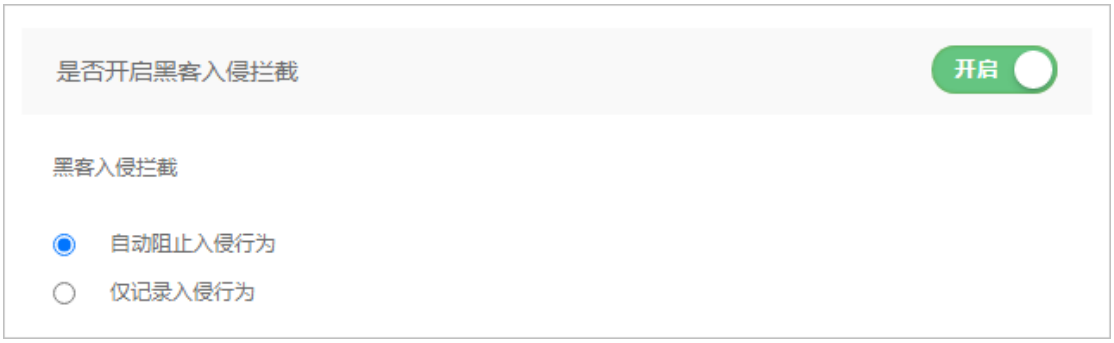
- **浏览器保护**

功能	说明
保护浏览器主页不被篡改	设置浏览器首页
自定义	根据需要锁定终端的浏览器主页

空白页	浏览器主页锁定为空白页

5.2.2.3 网络防御

- 黑客入侵拦截



功能	说明
自动阻止入侵行为	发现入侵行为自动阻止
仅记录入侵行为	发现入侵行为，只记录入侵行为，并不阻止

- 对外攻击检测

功能	说明
自动阻止行为	阻止对外攻击的行为，并且在日志中记录攻击行为。
仅记录攻击行为	不阻止对外攻击行为，只且在日志中记录攻击行为。

- 远程登录防护

功能	说明
添加 IP	添加需要放过的 IP 白名单，白名单外的 IP 将被自动阻止

	RDP 远程登录行为
删除所选	将选中的 IP 白名单删除

- **恶意网址拦截**

功能	说明
规 则 开 关	控制此条规则是否生效
恶意网址规则	木马、盗号 虚假、欺诈 钓鱼、假冒 流氓软件

5.2.2.4 访问控制

- IP 协议控制

功能	说明
添加规则	添加 IP 规则，通过 IP 地址、端口和协议类型等数据来创建规则，对入站和出站的网络协议数据进行控制
删除规则	删除所选规则

- IP 黑名单

功能	说明

添加规则	通过添加 IP 地址加入 IP 黑名单，添加入黑名单的 IP 将无法访问此电脑主机
删除规则	删除所选规则

- **设备控制**

功能	说明
功能开关 	控制此功能是否生效
设备开关	控制此设备是否禁用（开启即禁用）
设备类型	U 盘 便携设备 USB 无线网卡

	USB 有线网卡 打印机 光驱 蓝牙

5.3 信任区

5.3.1 功能介绍

添加需要信任的文件，信任的文件将不会被火绒反病毒引擎查杀。

5.3.2 操作流程

第一步：点击添加信任条目；

第二步：选择信任方式，选择信任文件路径时，需要用户输入信任文件的路径；选择信任文件校验和时，需要用户手动上传信任文件；

第三步：点击完成按钮，添加信任项目，终端将在 30 秒左右获取信任项目。

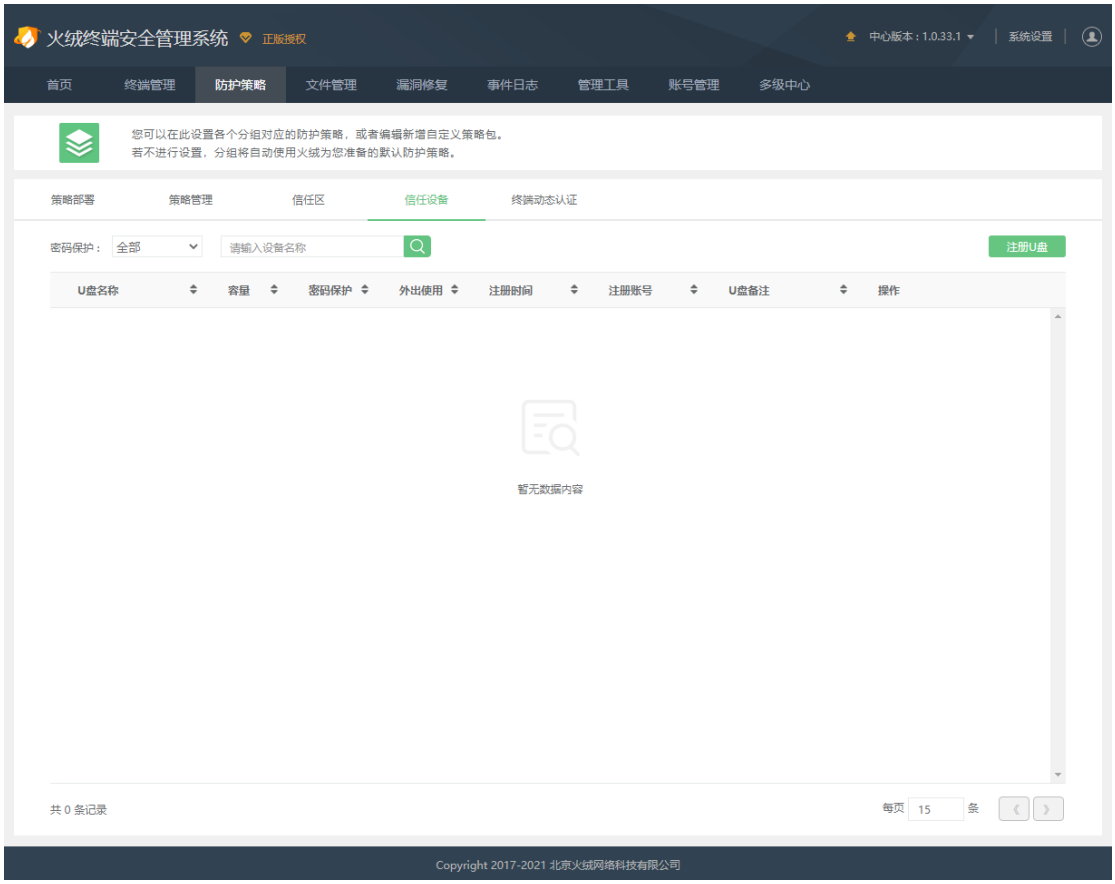
5.4 信任设备

5.4.1 功能介绍

通过信任设备注册的 U 盘将不被设备控制限制，可在终端上正常使用。

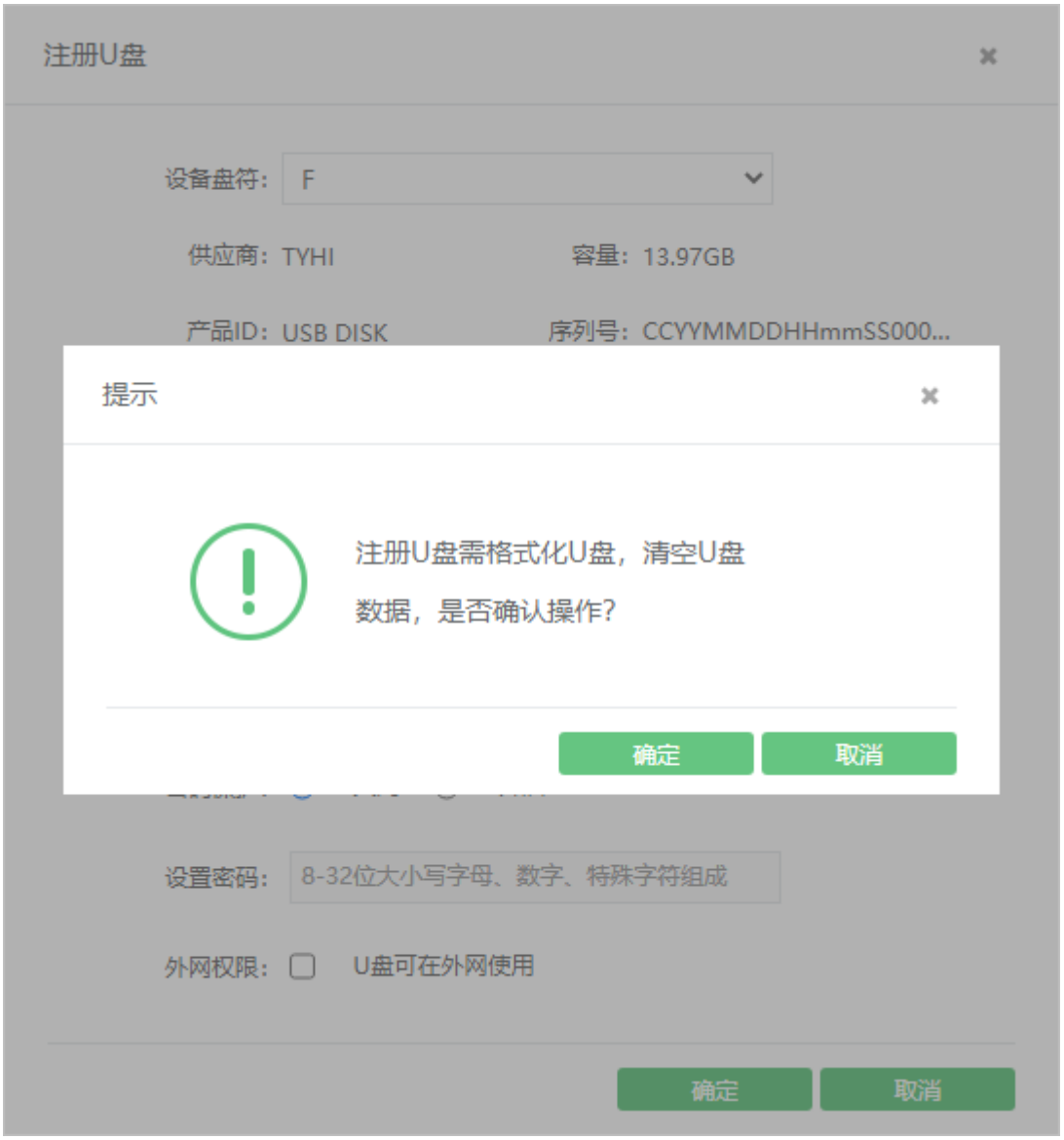
5.4.2 操作流程

第一步：将需要注册的 U 盘插入计算机后，点击注册 U 盘；

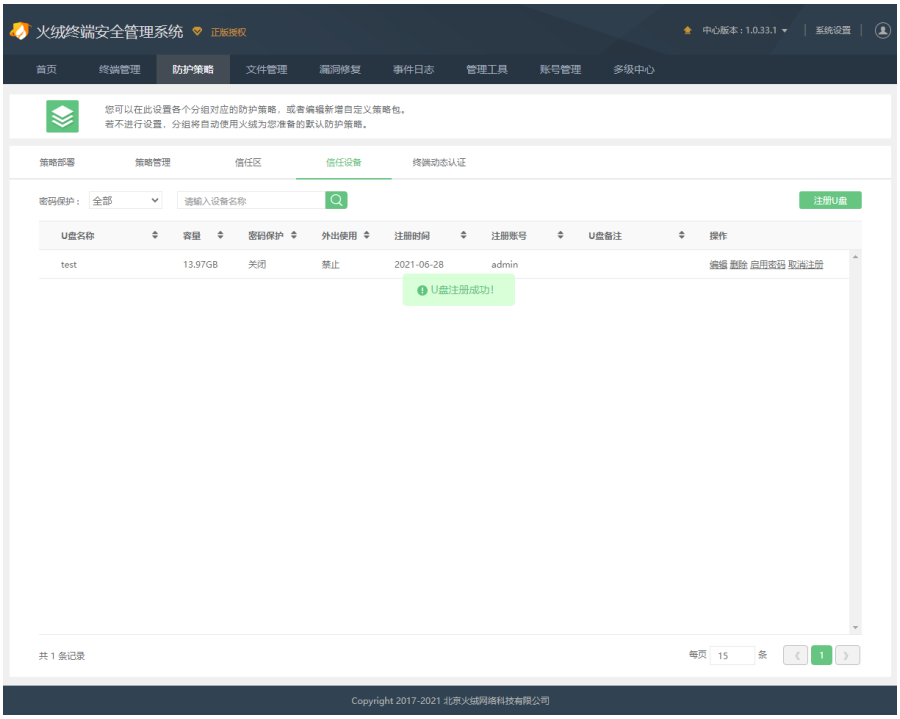


第二步：在弹出的注册 U 盘弹窗中，输入 U 盘名称后，根据需要设置密码保护以及外网权限后点击确定注册 U 盘。

在弹出的注册确认提示框中点击确定按钮；



第三步：等待注册完成后会弹出提示：注册成功。



5.5 终端动态认证

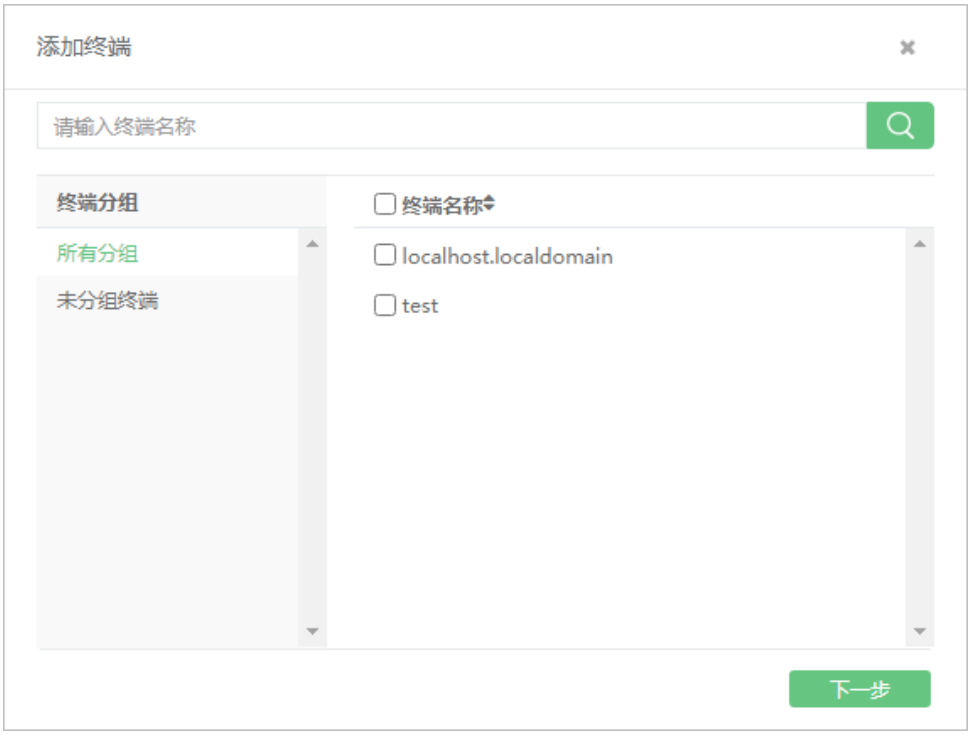
5.5.1 功能介绍

当受保护的终端进行登录操作时，需要再次输入火绒动态口令认证才可执行登录操作。

5.5.2 操作流程

第一步：在终端动态认证中点击添加按钮，弹出添加终端弹窗；

第二步：勾选需要开启终端动态认证的弹窗点击下一步进入选择终端动态认证的应用范围；



第三步：选择终端动态认证的应用范围，选择好应用范围后点击添加，将所选终端添加至终 端动态认证列表中。需等待 30 秒心跳同步至终端后终端动态认证才可启用。

六、文件管理

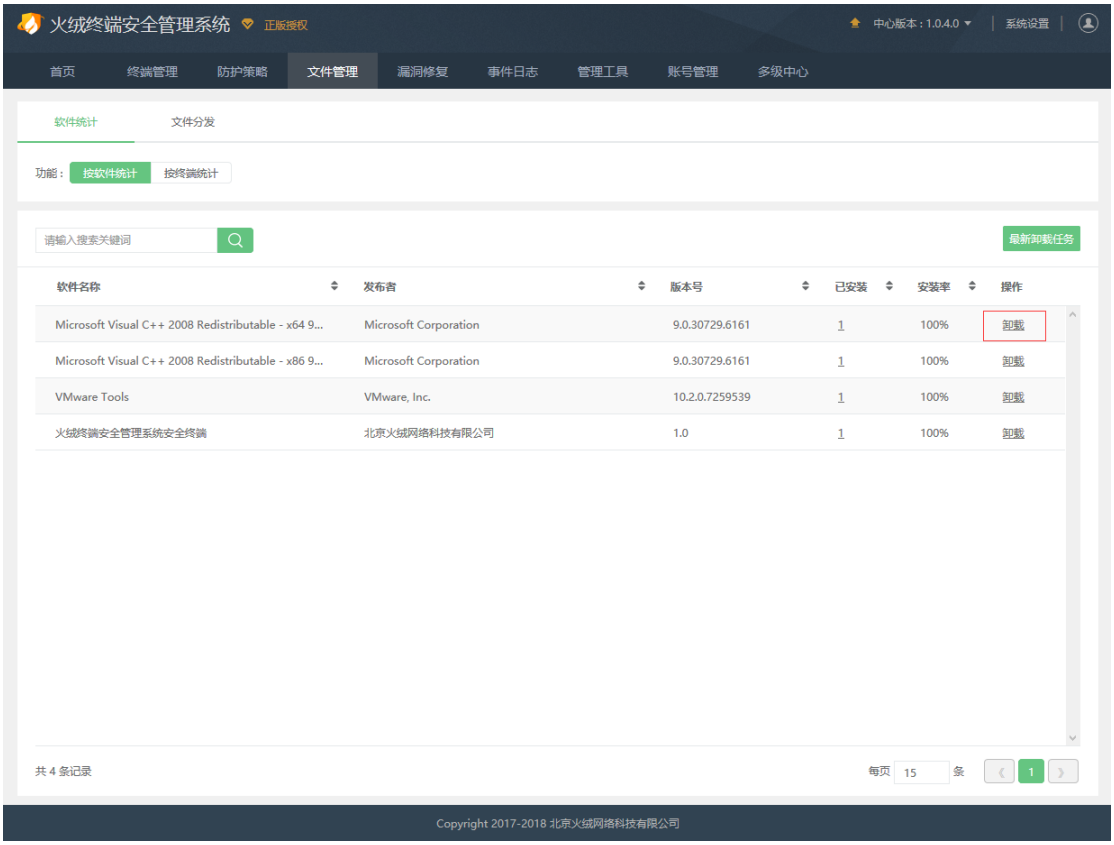
6.1 软件卸载

6.1.1 功能介绍

查看所有终端的软件安装情况，并可以要求终端卸载软件

6.1.2 操作流程

第一步：控制中心选择不符合公司安全规定的软件下发卸载任务



第二步：确认需要卸载软件的终端以及填写卸载通知详情

第三步：下发卸载通知后，终端将在 30 秒左右接收卸载任务并且选择执行

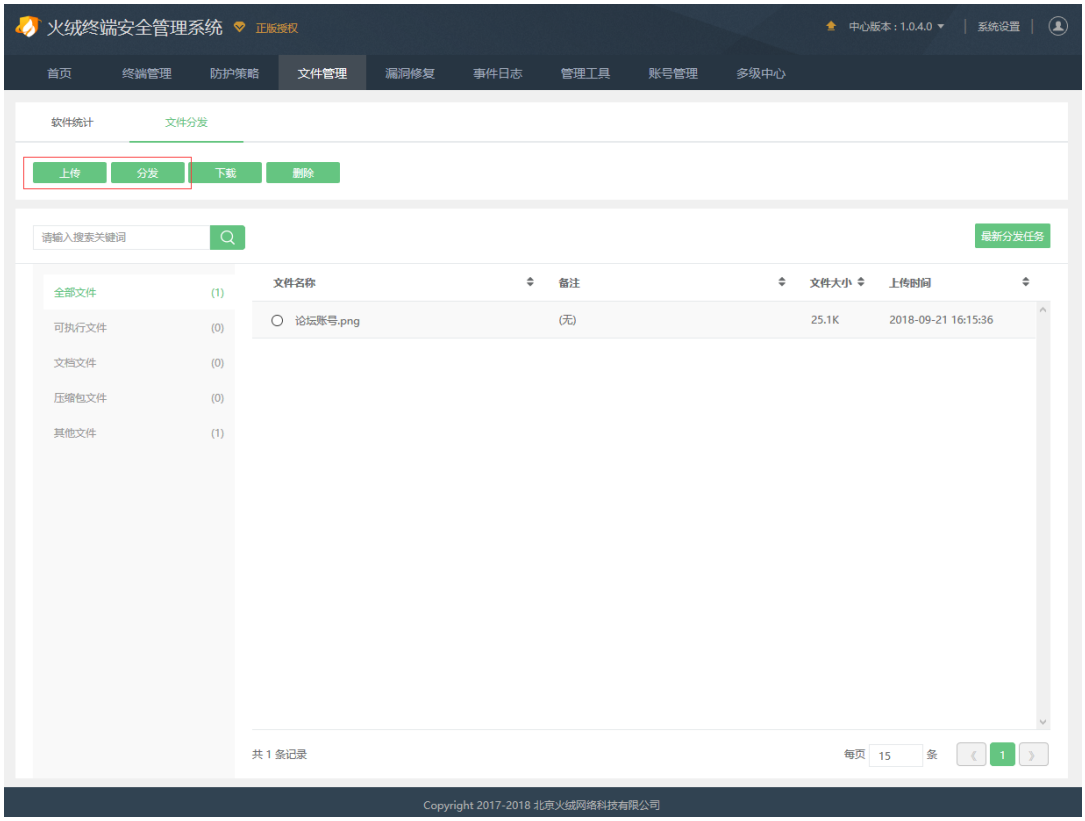
6.2 文件分发

6.2.1 功能介绍

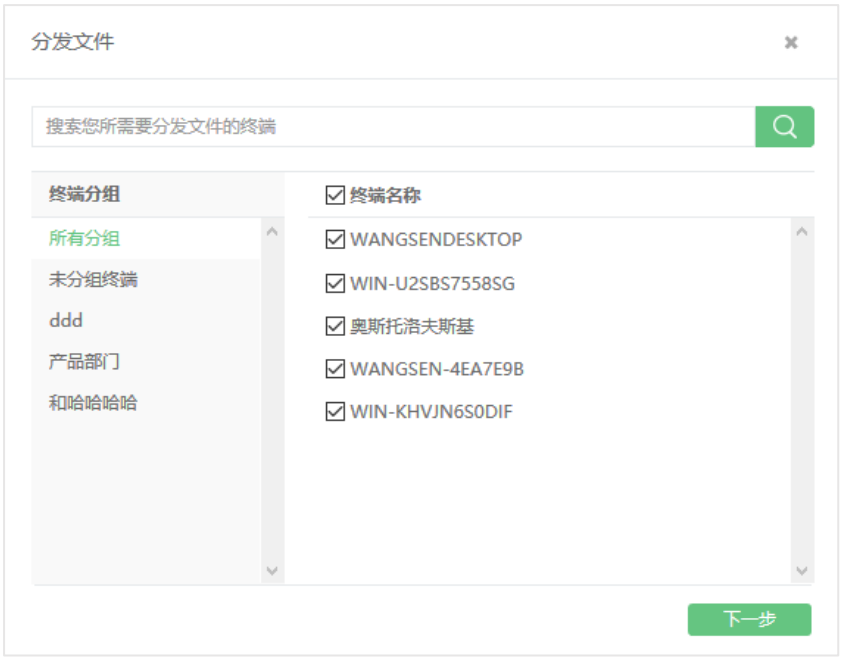
包含文件管理功能、文件分发功能；可以向指定终端推送安装某些软件或许下发某些文件。

6.2.2 操作流程

第一步：控制中心上传需要进行分发的文件或者直接选择待分发的文件

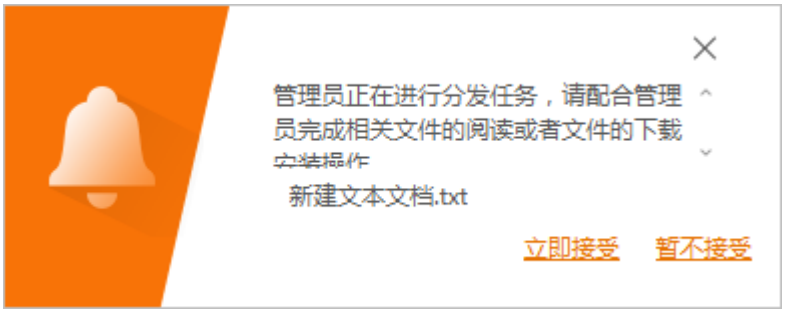


第二步：选择需要分发文件的终端以及分组



第三步：修改默认分发设置

第四步：下达文件分发的任务，终端将在一定时间内接收任务并且选择执行



七、漏洞修复

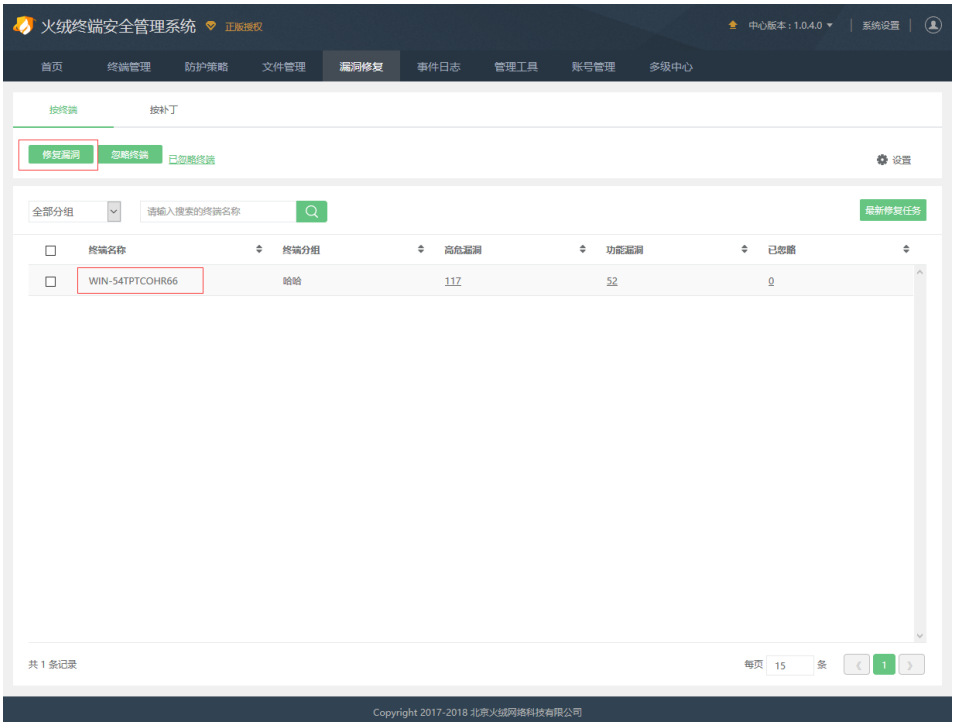
7.1 功能介绍

可以通过两种视角查看漏洞补丁，修复全网所有系统漏洞，也可以根据需要忽略

7.2 操作流程

第一步：选择终端扫描漏洞（由于控制中心默认策略时自动扫描漏洞，所以此步骤可以忽略）

第二步：选择相应的终端，修复漏洞



第三步：确定终端以及选择修复漏洞的类型（高危还是所有）

第四步：终端软件接收到任务后，就会自动修复相应的漏洞

7.3 设置说明

如果不想手动发布修复任务，可以在【设置】内勾选【自动修复高危漏洞】

默认是从微软官方下载补丁，也可以勾选【从中心下载补丁】，如果是从中心下载补丁，首次的修复任务将会失败，因为中心尚未存储系统补丁。

八、事件日志

8.1 功能介绍

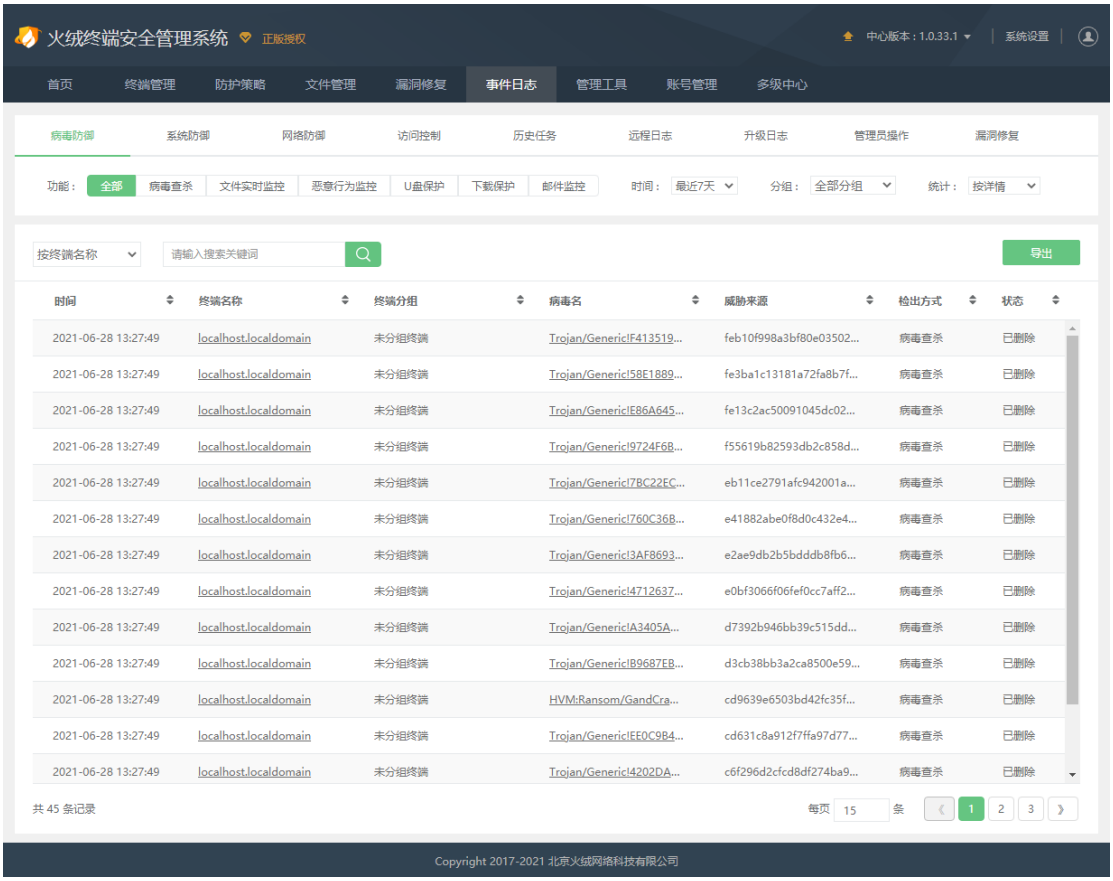
在这里可以查看所有事件包括病毒、系统、网络以及任务的发生和防护日志。您可以利用事件日志查看一段时间内电脑的安全情况，也可以根据日志来分析电脑遇到的问题。

8.2 操作流程

如何使用事件日志来查看终端以及中心做过的事情呢？

第一步：打开事件日志

第二步：根据需要选择要查看的日志内容



功能	说明
类别	根据实际情况选择要查看的内容的类别。例如：病毒防御
功能	根据选择的【类别】显示选择需要具体查看的功能。例如：病毒查杀
时间	提供了最近 7 天、最近 30 天、最近 90 天、最近 1 年、自定义时间的选择；例如：最近 7 天
分组	根据实际情况选择需查看的分组，例如：所有分组
按终端/按详情	根据实际情况选择按照终端显示还是按照详情显示
搜索	根据实际情况输入您想要搜索的关键词

日志详情	详细介绍当前选中日志的具体情况
每页显示条数	根据实际情况选择每页显示日志的具体数量
页数	根据实际情况选择您想要查看的具体页数的日志

8.3 设置说明

可以在【系统设置】中对【日志】进行设置

【设置】界面：在【控制中心相关设置】中，选择【中心日志配置】

功能	说明
日志保存	设置安全日志保存的时间 您可以根据需要设置保存安全日志的时间。
日志清理	你可以根据需要选择清理日志

九、管理工具

9.1 域部署工具

9.1.1 功能介绍

通过域部署工具可以在域环境内批量部署火绒终端安全软件，省去一台台安装的烦恼

9.1.2 操作流程

第一步：下载域部署工具

第二步：在域环境下打开域部署工具

第三步：填写控制中心地址以及端口

第四步：点击“安装脚本”

第五步：选择管理员用户

第六步：点击“启用脚本”

第七步：登录脚本部署完成

9.2 定时任务

9.2.1 功能介绍

提供快速查杀、全盘查杀、关机、重启等定时任务

9.2.2 操作流程

第一步：打开定时任务

第二步：选择您要进行的任务、下发的分组以及时间频率

第三步：添加即可

9.2.3 设置说明

快速查杀以及全盘查杀可以进行任务查杀的相关设置

9.3 日志清理工具

9.3.1 功能介绍

通过日志数据清理的清理，减轻控制中心的负担

9.3.2 操作流程

第一步：打开日志清理工具

第二步：选择您要进行清理的日志以及开始清理的时间

第三步：点击清理即可

9.4 离线升级工具

9.4.1 功能介绍

控制中心内部处于内网状态，无法连接外网升级版本以及病毒库，通过离线升级工具即可解决升级问题

9.4.2 操作流程

第一步：下载离线升级工具

第二步：在能够连接控制中心的机器上打开离线升级工具，输入控制中心地址以及管理员账号和密码，然后同步控制中心数据（同步控制台数据）

第三步：通过移动存储设备将离线升级工具以及同步的数据拷贝至能够连接外网的机器上，然后打开离线升级工具，进行升级数据的下载（下载离线数据）

第四步：通过移动存储设备将离线升级工具以及同步下载的数据拷贝至能够连接控制中心的机器上，然后打开离线升级工具，进行离线升级（更新数据到控制台）

9.4.3 设置说明

离线升级工具设置共分为两份：

一份用于同步和更新数据（内网），需要输入中心地址以及管理员账号密码

一份用于下载数据（外网），只需要能连接上火绒升级服务器即可

9.5 移动存储注册工具

9.5.1 功能介绍

用户需要注册信任 U 盘时，必须先下载安装移动存储注册工具才可以完成注册，若未安装将无法注册信任 U 盘

9.5.2 操作流程

注册信任设备之前，下载移动存储注册工具，双击安装即可。

9.6 火绒安全 U 盘

9.6.1 功能介绍

用户使用信任 U 盘时，如果将信任 U 盘中的启动程序误删，会导致用户无法访问注册后的 U 盘空间

9.6.2 操作流程

下载安全 U 盘程序，拷贝至需要使用的 U 盘中即可正常使用。

9.7 SHA-2 代码签名补丁修复工具

9.7.1 功能介绍

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。

9.7.2 操作流程

下载 SHA-2 代码签名补丁修复工具，双击运行即可。

十、账号管理

10.1 功能介绍

超级管理员通过管理其他管理员，并且给其他管理员分配操作模块的权限，使其协助管理控制中心以及终端

10.2 操作流程

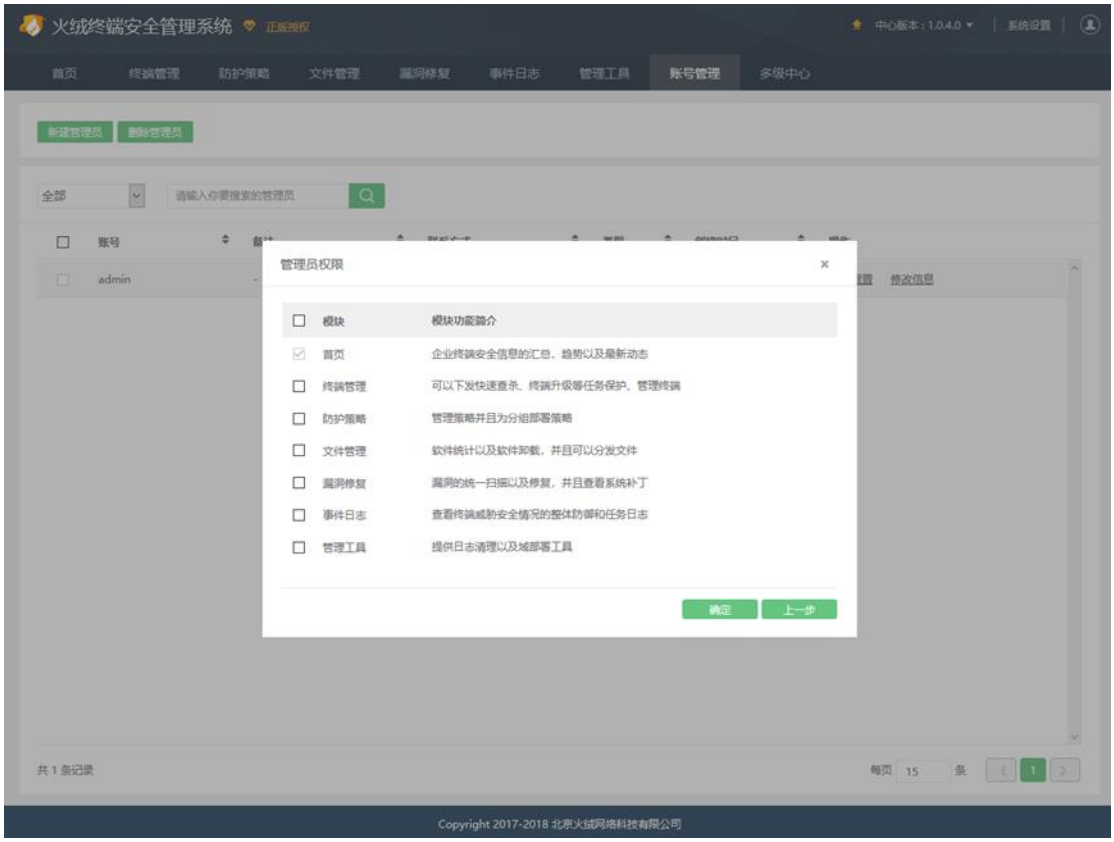
如何使用新建管理员并且分配权限来协助管理呢？

第一步：打开账号管理

第二步：选择新建管理员

第三步：输入管理员相应的信息

第四步：分配管理员权限



10.3 设置说明

功能	说明
管理员类型	超级管理员：系统自带，无法删除 普通管理员：根据需要分配模块权限 审计员：仅可查看事件日志以及首页

十一、多级中心

11.1 功能介绍

超级管理员通过多级中心，管理下级控制中心，缓解控制中心升级以及终端打补丁压力，并且给下级控制中心进行授权许可。

11.2 操作流程

- **如何部署多级中心（只需要将下级控制中心连接到上级即可）：**

第一步：在下级控制中心内，打开多级中心

第二步：多级中心的右上角，点击配置上级中心

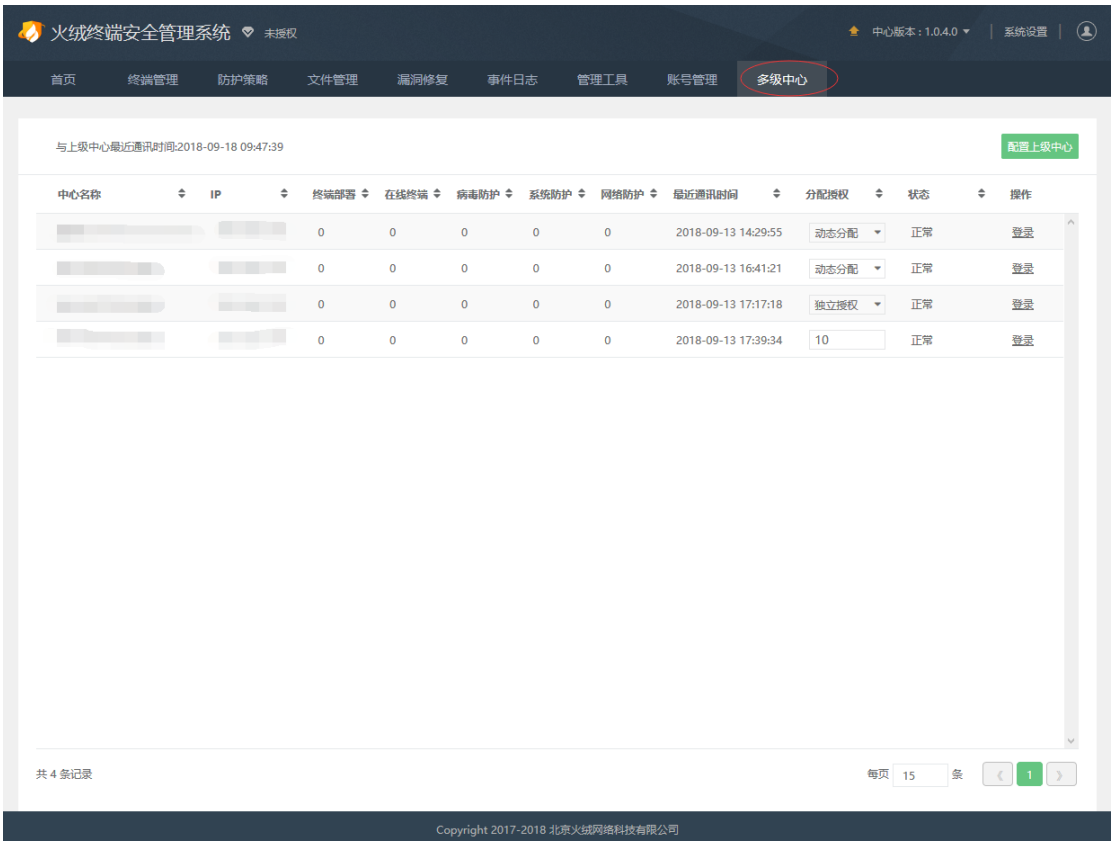
第三步：打开连接上级控制中心开关，输入地址以及秘钥

第四步：然后根据企业需要，选择相应的勾选项

第五步：点击确定，即可

- **如何使用多级中心进行分配授权：**

第一步：在上级控制中心内，打开多级中心



第二步：选择相应的下级控制中心，找到分配授权项，选择相应的授权方式即可

11.3 设置说明

功能	说明
允许上级中心直接管理，无需登录	勾选后，可以直接从上级控制中心登录到下级控制中心，不需要输入账号密码
允许从上级中心获取升级数据	勾选后，可以直接从上级控制中心获取升级数据
允许从上级中心获取补丁数据	该项是允许下级控制中心的客户端打补丁时可以通过上级控制中心获取，但是前提为需要在下级控制中心打开“从中心获取补丁”
授权方式	独立分配：上级控制中心对下级控制中心不进行授权，需要下级控制中心自己导入授权证书 动态分配：上级控制中心与下级控制中心共享授权 自定义授权：上级控制中心自定义控制下级控制中心授权台数