

企业版

火绒终端安全管理系统 2.0

产品使用说明 >>>>

2025/4/23





- 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

本文件所有内容版权受中国著作权法等有关知识产权法保护,为北京火绒网络科技有限公司(以下简

称"火绒安全")所有。

未经火绒安全允许,不得转载本文件内容,否则将视为侵权。转载或者引用本文内容请注明来源及原作者。

对于不遵守此声明或者其他违法使用本文件内容者,火绒安全依法保留追究其法律责任的权利。

另外,火绒安全保留修改本文件中描述产品的权利。如有修改,不另行通知。

目录 | CONTENTS

第一章 概述	
第二章 火绒终端安全管理系统-控制中心	12
2.1 访问控制中心	12
2.2 控制中心登录与登出	12
2.2.1 控制中心登录	13
2.2.2 控制中心登出	14
2.3 基础功能	15
2.3.1 授权管理	15
2.3.2 搜索	17
2.3.3 导入	17
2.3.4 中心版本	
2.3.5 通知	
2.3.6 账户	20
2.4 首页	21
2.5 终端管理	22
2.5.1 终端部署	22
2.5.2 终端概况	24
2.5.3 分组管理	42 3 / 261

2.5.4 终端黑名单	
2.5.5 标签管理	
2.5.6 文件分发	
2.5.7 计划任务	54
2.5.8 任务管理	
2.5.9 终端发现	
2.5.10 设备管理	63
2.6 防护策略	
2.6.1 策略部署	
2.6.2 策略管理	68
2.6.3 信任文件	93
2.6.4 黑名单	
2.6.5 U 盘管理	
2.6.6 终端动态认证	
2.7 漏洞修复	
2.7.1 按终端查看	
2.7.2 按补丁查看	
2.7.3 补丁文件管理	
2.8 资产管理	
2.8.1 资产登记	
2.8.2 软件管理	
	4 / 261

2.8.3 系统管理	
2.8.4 硬件管理	
2.9 中心管理	115
2.9.1 账号管理	
2.9.2 多级中心	
2.9.3 数据备份	
2.9.4 中心迁移	
2.9.5 中心设置	
2.10 事件日志	
2.11 管理工具	
2.12 配置工具	
第三章 火绒终端安全管理系统-WINDOWS 终端	
第三章 火绒终端安全管理系统-WINDOWS 终端	
第三章 火绒终端安全管理系统-WINDOWS 终端	157 157 157
 第三章 火绒终端安全管理系统-WINDOWS 终端	
 第三章 火绒终端安全管理系统-WINDOWS 终端	
 第三章 火绒终端安全管理系统-WINDOWS 终端	
 第三章 火绒终端安全管理系统-WINDOWS 终端 3.1 首页 3.1.1 病毒查杀 3.1.2 版本及更新 3.1.3 信任/隔离区 3.2 防护中心 3.2 防护中心 	
 第三章 火绒终端安全管理系统-WINDOWS 终端	

3.3 访问控制	174
3.3.1 IP 协议控制	
3.3.2 IP 黑名单	
3.3.3 联网控制	
3.3.4 网站内容控制	
3.3.5 程序执行控制	
3.3.6 设备控制	
3.4 安全工具	
3.5 终端信息	
3.6 更多功能	
3.6.1 安全设置	
3.6.2 安全日志	
3.6.3 隔离区	
3.6.4 信任区	
3.6.5 语言设置	
3.6.6 检查更新	
3.6.7 联系网管	
3.6.8 终端登记	
3.6.9 关于我们	
第四章 火绒终端安全管理系统-LINUX 服务器版终端	

4.1 查看帮助信息	
4.2 查看终端状态	
4.3 发起本地扫描任务	
4.4 查看终端配置	
4.5 修改配置项	197
4.5.1 修改中心地址	
4.5.2 修改策略同步设置	
4.5.3 修改自动升级设置	
4.5.4 修改仅更新病毒库设置	
4.5.5 修改发现病毒时自动清除设置	
4.5.6 修改清除前隔离文件设置	
4.5.7 修改扫描压缩文件设置	
4.5.8 修改压缩文件大小限制设置	
4.5.9 修改扫描网络驱动器设置	
4.5.10 修改不扫描扩展名文件设置	
4.5.11 修改文件实时监控功能状态	
4.5.12 修改文件实时监控-发现病毒时设置	
4.5.13 修改文件实时监控-清除病毒时设置	
4.5.14 修改文件实时监控-扫描时机设置	
4.5.15 修改文件实时监控-不扫描指定文件路径设置	
4.5.16 修改文件实时监控-不扫描指定路径规则设置	
	7 / 261

4.5.17 修改日志保留时间设置	
4.6 隔离区操作	
4.7 查看日志	
4.7.1 查看日志使用帮助	
4.7.2 查看不同格式日志	
4.7.3 查看不同功能日志	
4.7.4 根据时间查看日志	
4.7.5 多条件查询日志	
4.7.6 查看指定 ID 完整日志	
第五章 火绒终端安全管理系统-LINUX 桌面版终端	220
5.1 首页	
5.1.1 病毒查杀	
5.1.2 文件实时监控	
5.1.2 文件实时监控 5.1.3 版本及更新	
5.1.2 文件实时监控 5.1.3 版本及更新 5.1.4 信任/隔离区	
 5.1.2 文件实时监控 5.1.3 版本及更新 5.1.4 信任/隔离区 5.2 终端信息 	
 5.1.2 文件实时监控 5.1.3 版本及更新 5.1.4 信任/隔离区 5.2 终端信息 5.3 更多功能 	
 5.1.2 文件实时监控 5.1.3 版本及更新 5.1.4 信任/隔离区 5.2 终端信息 5.3 更多功能 5.3.1 安全设置 	
 5.1.2 文件实时监控 5.1.3 版本及更新 5.1.4 信任/隔离区 5.2 终端信息 5.3 更多功能 5.3.1 安全设置 5.3.2 安全日志 	
 5.1.2 文件实时监控 5.1.3 版本及更新 5.1.4 信任/隔离区 5.2 终端信息 5.3 更多功能 5.3 更多功能 5.3.1 安全设置 5.3.2 安全日志 5.3.3 隔离区 	227 227 228 230 230 231 232 234 235

5.3.4 信任区	236
5.3.5 检查更新	
5.3.6 联系网管	
5.3.7 终端登记	
5.3.8 关于我们	
第六章 火绒终端安全管理系统-MACOS 终端	241
6.1 首页	
6.1.1 病毒查杀	
6.1.2 文件实时监控	
6.1.3 版本更新	
6.1.4 信任/隔离区	
6.1.5 联系网管	
6.2 终端信息	254
6.3 更多功能	255
6.3.1 关于我们	
6.3.2 安全日志	
6.3.3 终端登记	
6.3.4 检查更新	
6.3.5 安全设置	

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 10/261 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。

🛷 火城终端安全管理系统		醫体中文 English
	用户登录	
	6 唐朝入西明 10万内国政治者 8128697	
	Copyright 2019-2020 北东火结网络科技有限公司	

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 13 / 261

🥔 火城终端安全管理系统		聞知中文 English
	请修改初始密码	
	Copyright 2019-2020 北东大战网络科技有限公司	

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。

🍠 火绒终端安全管理系统	を V2.0.15.0		搜索	导航、模块名称 Q	11 🔿 🦨 🤤 admin 🗸
 ○ 首页 □ 终端管理 へ 	终端在线状态			终端安装概况	admin 超级管理员
终端部署 终端既况 分组管理	戸総修勝 0 合	在线线端 1台	高线终端 0 台	已安装终端 日 会	 ② 密码修改 回 切换语言 ① 退出登录
终端黑名单 标签管理 文件分发	Hi, admin, 下午好 • 正時度 序列号: ESV2-BJD8-2324-42939568 ① 授权使用	】 服务码:BJ06099943 口		服务器性能 CPU占用 内存使用	服务器时间:2024-11-18 14:53:58 <mark>14%</mark> 1.1GB/2GB
计划任务 任务管理 终端发现	已部署 1 合	■ Windows版 剩 972 天 1 /共50台	● macOS版 創 972 天 0 /共50台	硬盘使用 网络流量 • 15.7 KB/S	42.1GB/59.4GB • 5.87 KB/S
 设备管理 26 防护策略 > (26 防护策略 > (27 流戸管理 > (27 流戸管理 > 	已用/胸买总数 1/200 台	▲ Linux服务器版	▲ Linux桌面版 到 972 天 0 /共50台	备用中心 当前中心未启用备用中心	
	近期安全事件				7天 30天
👳 正版授权 📃	查杀日志	 处理成功 病毒防护 A 1784生 Br 	● 处理成功 ● か理生物	系统防护	妨舌 Windows

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;

🛷 火绒终端安全管理系					Q 11 A 🖓 🧟 🌏 admin 🗸
 ▲ 首页 ● 炎嶺管理 ∨ S 防护策略 ∨ ○ 瀛淵終复 ∨ 	Hi, admin, 上午好 ● #嬰校 序列号:- 服务码:- 授权使用		2#85%	服务器性能 CPU占用 内存使用	腦時聽时间:2025-03-06 10:27-19 71% 1.3GB2GB
	已錄編 0 合	■ Windows版 督未购买, 去购买 >	 ≰ macOS版 福未购买, 去购买 > 	硬盘使用 网络流量 * 27.55 KB/S	39.1GB/59.4GB • 334.13 KB/S
	已用购买总数 0/0 合	△ Linux服务者 「 「 「 」 」 」 」 」 」 」 一 」 一 一 二 二 二 一 二 二 二 二 二 二 二 二 二 二 二 二 二	× 法对终端进行统一管理,	备用中心 当前中心未启用备用中心	
	近期安全事件		查看详晰		7天 30天
	查派日志 0 涉及终端0台	 - 经型成为 病毒防护 - 必要求表 - 包括年期 - 日日年 - 日日年 - 別及律論の合 	 · 他最成功 · 他最成功 · 他最成功 · 他最成功 · 他最低 · 他最低 · 已最低 · · ·	系統防护 0 涉及终端0台	
	网络防护 0 沙及终于0	 ・日治非 ・日治非 ・日治非 ・日治 ・日 ・日 ・日	 ● 供知道功 ● 使契尺式 ● 下製品式 ● 下製品式 ● 正初端 	违规外联 0	软件禁用 0
豪 未授权 三					

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。

// 火绒终端安	全管理系统	充 V2.0.16.0					搜索导航、模块名称	Q 11 @ 4	📍 🍳 admin 🗸
	~	产品未援权,无法对终端进行	行统一管理						
🖀 防护策略	~	火绒终端安全管理系统	♥ 未授权			激活授权	授权总览		购买
	~	序列号:- 服务码:-		送现信白	×			78	
	~	全国服务热线: 400-998-3555		火切修備	な全管理系统			0	
	~	授权权益		序列	計 未授权		0	0	
	~	中心定制	运程桌面				剩余	待生效	
		多级中心	API接口				0	0	
				序列号*					
		授权 信言		34492-0379-5					
		121210-0-		■ 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	<i>0</i> 5				
		III Windows版			-				
				联 内网环境下,请到 <mark>管理工具</mark> 中下数编线	<mark>网數第一</mark> 升级工具,使用電线升级工具激活或更接接权				
			未购买该类型终端授	全国服务热线	€: 400-998-3555		未购买该类型终端授权,去购买 >		
				4.8895470					
	=	△ Linux服务器版			▲ Linux桌面版				

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。

🧦 火绒终端安全管理系统	充 V2.0.16.0					搜索导航、模块名称	Q 11 63	📩 🖓 😜 admin 🗸
 運刷修复 へ 技能調査看 技补丁查看 补丁文件管理 	测试fzy • 正服授权 序列号: 5 全国服务热线: 400-998-3555 授权权益	、の 服务码:BJ03057067の			8194862	授权总览 当新授权 400	已用 ① 21	增购授权
⑦ 资产管理 ~	中心定制	远程桌面	<mark>≪</mark> ∎ U盘管理	终端动态认证	要件管理	剩余	待生效	
 四中心管理 へ 新号管理 	3 级中心	API接口	(1) 日本の	(二) の歌中心		379	0	
多级中心								
数据备份	授权信息							
中心迁移	■ Windows版 使用中		**********	授权详情 >	▲ macOS版 使用中			授权详情 >
中心设置 	 当前授权 2026.05.10到期, 剩余429天 100 		□前中心と用: 下级中心占用: 已用 ① 11	10 剩余 89	 当前授权 2026.05.10到明, 剩余429天 100 		已用 ① 0	剩余 100
病毒防御	● 待生效				• 待生效			
系统防御	0				0			
网络防御								
访问控制	△ Linux服务器版 使用中	1		授权详情 >	👃 Linux 桌面版 使用中			授权详情 >
	 当前授权 2026.05.10到期, 剩余429天 		己用①	剩余	 当前授权 2026.05.10到期,剩余429天 		激活 Wind 已用句 ^{"设置"以激}	OWS 如玉Windows。
< 正版授权 📃	100		10	90	100		0	100

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。

🍠 火绒終端安	安全管理系统	充 V2.0.16.0					搜索导航、模块名称	Q 11 🔿 🦨 🤗 admin 🗸
白首页		产品授权被重复使用, 29 天后	产品将无法升级					
	~	测试fzy 💌 重复接权				更换授权	授权总览	增购授权
富 防护策略	~	序列号	* 服务码:BJ03057067 C	7			strate infant	7.00
③ 漏洞修复	~	全国服务热线: 400-998-3555					□回按(X	Вля O
资产管理	~	授权权益					20	0
中心管理	~	中心定制	8 远程桌面	1000日 10日1日日	终端动态认证	要件管理	剩余	得生效
日本	~			() amount			20	0
🖻 管理工具		ee sate	API AFIRE	and and the	DOCHO			
		授权信息						
		II Windows版 使用中				▲ macOS版		
		 当前授权 2026.05.10到明, 剩余429天 10 		已用 0	剩余 10		未获取该类型授权	
		△ Linux服务器版 使用中				A Linux桌面版		
		 当前援权 2026.03.10预期, 剩余429天 10 		已用 0	剩余 10		未获取该类型授权	激活 Windows
	=							转到"设置"以激活 Windows。

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。

🧦 火绒终端安全管理系	统 V2.0.16.0					(x# N & 4 🤌 🤗	admin 🗸
습 普页	终端管理 > 分组管理					文件分发 (1)-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	-
经满管理 ^ 终端部署 终端都器 终端概況	分组管理 描述 一	组织架构				77因4年2月到7月回7日回2日。 備任文件 管理信任文件和网址,解决临时误报问题 自导入	自守出
分组管理	■全部分组 ····································	搜索 : 分组名称	Q			补丁文件管理 管理中心下载的补丁文件	
终端黑名单	产品	分组名称	分组路径	终端数	置顶	备份文件	
文件分发	测试	未分组终端	未分组终端	1	-	备份中心数据,使于快速恢复中心数据 	
计划任务		測试)*************************************	0	1	终端触发文件实时监控的日志	
任务管理 终端发现 设备管理							
S 防护策略 ^ 策略部署							
策略管理							
黑名单							
U盘管理							
		共3条记录				激活 Windows 转到"以蜀"以激活 Windows。	

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。

🧦 火绒终端安全	管理系统	卷 V2.0.15.0	文件实	时	٩	1	କ <u>ଚ</u>		admin 🗸
计划任务		中心管理 / 数据备份							
任务管理				正在上传	(1)			Ê	部取消
终端发现		备份文件 备份设置		【数据备份	hrcenter	202411	18155050.	zip	0
设备管理				0 B/368.72 K	в				0 B/s
宮 防护策略	~	备份 翻除 同步							_
◎ 漏洞修复	~	生成时间: 2024-11-12 ~ 2024-11-18 📄 备份类型: 全部 🗸 备份内容: 全部 🗸							自导入
资产管理 资产管理	~	● 备份文件生 ① ◆ 备份完成时间 ◆ 中心版本 ◆ 备份类型 ◆ 备份内容 ◆	大小	¢	备注	¢	操作		
🖾 中心管理	^	2024-11-18 15:5 2024-11-18 15: V2.0.15.0 导入备份 配置文件	1.29 M	В	-	0	数据恢复	下載删	除
账号管理		2024-11-18 15:5 2024-11-18 15: V2.0.15.0 手动备份 配置文件	1.29 M	В	2	0	数据恢复	下載删	 除
多级中心						_			
数据备份									
中心迁移									
中心设置									
日 事件日志	^								
安全事件总览									
病毒查杀									
病毒防御									
◇ 正版授权	≡	共2条				沙が壬 \	Vindows	< 1	

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。

🛷 火绒终端安全管理系	统 V2.0.15.0	搜索导航、模块名称 Q 11 6 🦨 😜 admin 🗸
向 首页	中心管理 / 中心设置	版本升级 中心最后更新时间:2024-11-18 13:48:49
 一 终端管理 へ 终端部署 终端和况 分田管理 	终端管理员设置 中心升极 中心地址管理 通知设置 管理中心升级方式设置 目动升级	△ 中心版本 中心程序版本 V2.0.15.0 図 客户端版本 Windows V2.0.15.0 Linux 405 円折 V2.0.12.0
终端黑名单 标签管理 立件公告	 手动升级 升级服务器代理设置 	Linux銀子編版 V2.0.12.0 Linux桌面版 (通用) V2.0.9.0 Linux桌面版 (UOS) V2.0.9.0 Linux桌面版 (伊可離離) V2.0.9.0
×1+77及 计划任务 任务管理	可以为升级服务器设置代理,通过代理服务器下载更新资源。 捕定代理服务器 网络测试	macOS版 V2.0.8.0 泰 病毒库版本 Macdaumまでは 2004 11 14 11-20-20
终端发现 设备管理	代理地址: 第二	
■ 防护策略 ∨		
★号管理 ◆ 正版授权 Ξ	保存 恢复默认	激活 Windows

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。

🛷 火绒终端安全管理系	3统 V2.0.15.0	搜索导航、模块名称 Q 11 🔊 🦨 💽 admin 🗸
合首页	中心管理 / 数据备份	未读(3) 已读 全部标为已读 全部消息 へ
梁端管理 へ 终端管理 へ 终端能容 终端能容 终端概况 分相管理 のかののため のかののため のかののため のかののため のかののため のかののため のかののため のかののため ののため のののため のののため ののののため ののののため ののののの のののの ののの のののの のののの のののの ののの のの のの ののの ののの ののの ののの ののの ののの のの の のの のの の のの のの	备份文件 备份设置 文件猜理 备份文件認过 10 个后自动清理 备份文件超过 500 MB ~ 提醒清理 ①	全部内息 数据省份成功 全部内息 皆分:[2024-11-18 15:50:50] 数据上传 步心升级 数据号出 中心升级 任务分发 中心组件及交谈包已全部更新至最新版本 安全舌管
^{交端黑名単} 标签管理 文件分发	目动备份	接段還示 审批提醒 未接权,请及时更新接权 消息提醒
计划任务 任务管理	备份内容: ☑ 配置文件 ① □ 日志文件 ● 全部日志 ○ 前 30 天日志 ①	
终端发现	自动备份周期: ② 按天警份 每 1 天	
乙 防护策略 >	● 技術資份 周日 周一周二 周三 周四 周五 周六 毎 1 周 周	
③ 漏洞修复 ~		
⑦ 资产管理 ~	 ○ 按月答份 月 南边峰 〒 〒 *浩浩塔 首 	
四 中心管理 へ 账号管理		
◆ 正版授权 🛛 🚍	9 77	激活 Windows

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。

🧦 火绒终端的	安全管理系统	统 V2.0.15.0 搜索导航、埋埃名称	Q 11 of 斗 🗛 admin	~
白前		中心管理 / 数据备份	admin 超级管理员	
终端管理 终端部署 终端概况 分组管理 分组管理	^	备份文件 备份设置 文件清理 备份文件超过 10 个后自动清理 备份文件超过 500 MB /提题清理 ①	② 密码修改 回 切换语言 ☞ 退出登录	
终端黑名单 标签管理		自动备份		
文件分发 计划任务		 开启自动备份 备份内容: ☑ 配置文件 ① □ 日志文件 ④ 全部日志 ○ 前 30 天日志 ① 		
终端发现设备管理		自动备份周期: ① 技天备份 每 1 天		
🖀 防护策略	~			
◎ 漏洞修复	~			
3 资产管理	~	 T (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		
四中心管理 账号管理	^	开始的间: 00:00 ①		
😔 正版授权	Ξ	保存	激活 Windows	

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。

<i> 秋</i> 秋 秋 終 端 安 全 管	理系统	V2.0.15.0				搜索	浙、模块名称 Q 1	u 👌 🖞 🤑 admin 🗸
局 首页 ☑ 终端管理	~	终端在线状态					终端安装概况	终端部署
终端部署 终端概况		 ・ ・ ・	 在线终端 2 台 		高线终端 〇 台		已安装终端 2 合	末安装修満 2 合
分组管理 终端黑名单		Hi, admin, 上午好 💌 🎟	渡权				服务器性能	服务器时间 : 2024-11-19 10:34:04
标签管理		序列号:ESV2-BJD8-2324-42939568	〕 服务码:BJ06099943 〕				CPU占用	27%
文件分发		授权使用					内存使用	1GB/2GB
计划任务		已部響	II Windows版	剩 971 天	é macOS版	剩 971 天	硬盘使用	42.1GB/59.4GB
终端发现		2台	2/共50台		0 /共50台		网络流量	
设备管理							• 10.55 KB/S	• 5.49 KB/S
富 防护策略	~	已用/购买总数 2/200 x	△ Linux服务器版	劇 971 天	A Linux桌面版	剩 971 天	各田中心	
③ 漏洞修复 · · · · · · · · · · · · · · · · · · ·	~	2/200音	0/共50台		0/共50台		当前中心未启用备用中心	
⑦ 资产管理	~							
□● 中心管理 ·	~	近期安全事件						7天 30天
	~							
😔 正版授权	≡	查杀日志 -	 处理成功 处理失败 	病毒防护		 处理成功 处理失敗 	系统防护	• E##

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。

🧦 火绒终端安全管理系	统 V2.0.15.0	搜索导航、模块名称 Q 📢 🔿 🗘 😜 admin 🗸
☐ 首页 ☑ 终端管理 ▲ 终端部署	终端部署 您需要部署火城安全终端来执行中心管理员制定的安全防护策略,请根据网络场景或需求使用以下不同方式部署	ey.tit
终端概况 分组管理	安全终端	
终端黑名单 标签管理	P 方式一:终端用户自助安装 以下链接为安装部署指导页地址,通过邮件或其他方式将链接分发给终端用户,终端用户通过浏览器进入部署指	目 导页面后,可以自助下载 实装 不同系统类型终端
文件分发 计划任务	https://192.168.5.24:6080 意能提表 https://localhost:6080	复制链接 https://[fe80:45ce:2bf3:e840:bd6e]:6080 复制链接
任务管理终端发现	方式二:下载安装包进行安装 如终端用户无法自助下载安装,管理员可以下载以下安装包,拷贝至目标计算机上进行安装	
设备管理	Windows安装包 V2.0.15.0 立即下載 ・ 下数送用于Windows還作系统的客户論 下数 下数 ・ ・ <td>macOS安装包 <u>V2.0.8.0</u> 范囲丁macOS操作系统的客户論</td>	macOS安装包 <u>V2.0.8.0</u> 范囲丁macOS操作系统的客户論
 高 防护策略 〇 漏洞修复 ~ 	メニキュを示: Windows Jerver 2005 SP12GULTERA-/ Windows XP(SPS)/ Windows Vista/ Windows /2GU 上版本	attori matus IVI I sociulizt®r
⑦ 资产管理 ~ 四 中心管理 ~	▲ Linux桌面版安装包 120.9.0 章番振日 立即下載 △ 下載适用于Linux桌面版设作系统的客户编 下動	Linux服务器实装包 V2.0.12.0 重書描引 立刻下数 認知于Linux服务器能缓作系统的案件请
□ 事件日志 ~ ✓ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	交持系統: 支持Ubuntu / SUSE / 统信UOS / 很可翻翻 / 中科紅旗 / 优翻翻 / 深度 / 龙芯 (Loongnix) 等发行 支持 版 (L	系統: 芝特CentOS / Ubuntu / SUSE / 统信UOS / 银河翻腳 / 中応翻腳 / 中科紅旗 / 优翻解 / 深度 / 龙芯 oongnix) 等没行版

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》。

秋/教 学校 大規模 端安全管理系统 日本 日本	简体中文	English
全网部署火绒通知		
各位同事: 为了更好的保障内网安全,决定从即日起全面安装部署火绒终端安全管理系统。您可以通过下面的按 钮进行下载并安装,安装后无需任何设置可以立即使用。		
📲 _ 下载 Windows 版		
获取 <u>更多经衡能署类型</u>		
Copyright 2019-2024 北京火城网络科技有限公司		

🛷 火绒终端安全管理系	充		简体中文 English
	Windows版 支持系统:Windows Server 2003 SP1及以上版本 / Windows XP(SP3)/ Windows Vista / Windows 7及以上版本 支持CPU: Intel / AMD	⊻ 下载	
Δ	Linux服务器版 支持系统:支持CentOS / Ubuntu / SUSE / 统信UOS / 銀河離鏡 / 中标離鏡 / 中科紅旗 / 优離鏡 / 深度 / 龙芯(Loongnix)等没行版 支持CPU:Intel / AMD / 飞腾 / 編鵬 / 兆芯 / 海光 / 龙芯		
	安装方式: 可以通过以下步载进行安装 1、点击下载安装脚本 2、将安装脚本持坝至线筒 3. 执行命令 chmod 0755 installer\(https_192.168.5.24_6080\).sh /installer\(https 192.168.5.24 6080\).sh	⊻ 下载	
	ッパーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー		
	Copyright 2019-2024 北京火城网络科技有限公司		

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。

		94								
🥖 火绒线	端安全管理系	统 V2.0.16.0					援索导	航、欄块名称 Q		🤗 admin 🗸
向 首页		终端管理 > 终端概况								
- 		终端分组	◆ 病毒查杀 终端升级	发送通知 移动分组						更多
- 终端部署										
终端概况			□ 所有终端 ∨ 搜索:	终端名称、IP、分组、MAC地	al Q				(金自主) 出得(面)	《列 昆检索
分组管理		■ 未方組残強(1/1)	终端名称	♦ 计算机名称	终端分组	参 终端安全状态	♦ MAC地址	病毒库版本	◆ 终端版本	\$
终端黑谷	単	□ 产品(0.0)	□ □ 本机	DESKTOP-TOSOOEK	未分组终端	安全	00-0C-29-8E-59-31	2025-02-24 13:50:26	V2.0.16.0	
标签管理		₩ 38135(0:0)								
文件分发										
计划任务										
任务管理										
终端发现										
设备管理										
罢 防护策略										
● 中心管理										
账号管理										
多级中心										
数据备份										
中心迁移								語	痰舌 Windows	
⇒ 重复授权			共1条				20	条页 ~ ド く	新設置"以激活 Windo 1 ショー 1	^{MS} 。 /共1页

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。

- 秋城終端安全管	管理系统 V2.0.16.0		病毒查杀 ×
局 首页	终端管理 > 终端概况		臺渋染型: O 侍津垂炎 ○ 左母垂炎 ○ 自定 V 善炎
□ 终端管理	终端分组	● 病毒查杀 终端升级 发送通知 移动分组 远程协助	
修業部署			直杀速度: ○ 鄉烟扫描 ○ 高速扫描, 将影响计算机性能
修建图记	■ 全部分組 王	□ 所有终端 ~ 搜索: 终端名称、IP、分组、MAC地址 Q	查杀设置: 扫描终端信任区
分组管理	■ 未分组终端(1/1)		发现病毒时: 🖸 自动处理病毒 🕥 督不处理。仅记入查杀日志
终端里名前	口 7年品(0/0)	🔽 🗆 本机 未分组终端 11	
标落管理			漏除病毒时: ☑ 将病毒文件备份至终端隔离区
文件分发			查杀完成时:自动关机 ()
1++++++			任务执行时: 💋 不允许终端暂停或停止直杀任务
他端台网			自定义黑名单: 〇本次扫描启用黑名单
310, 500, 2000			
R NUMBER			
	× III		
 (O) 漏河修复 (C) 漏河修复 	×		
资产管理	×		
一些 中心管理	×		
□ 每件日志	× III		
管 管理工具			
			潮注 Windowe
		#18	· · · · · · · · · · · · · · · · · · ·
🗇 正版授权	=	75 + ds	1002 -0013

"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。

🧦 火绒終端安	全管理系	统 V20160		病毒查杀	×
		终续管理 > 终端概况		童杀类型: 🗿 快速查杀 💿 全盘查杀 💿 自定义查杀	
		终端分组	◆ 病毒查杀 终端升级 发送通知 移动分组 远程协助	查杀速度: <mark>○</mark> 常规扫描 🛛 高速扫描,将影响计算机性税	
		亚 全部分组 · 王	➡ 所有终端 ∨ 搜索: 终端名称、P、分组、MAC地址 Q.	音光设置· □ 扫描终端信任区	
		■ 未分组终端(1/1)			
		🖵 产品(0/0)		发现病毒时: 🔿 自动处理病毒 🔷 暫不处理, 仅记入查杀日志	
			中机 未分组终端 19	清除病毒时: ✔ 将病毒文件备份至终端隔离区	
				查杀完成时: 目动关机 ①	
				任祭执行时 🛃 无价许终端暂值或值止香举任祭	
				自定义黑名单: 🛃 本次扫描扇用黑名单	
				文件处理方式: 🖸 不处理 💿 删除	
安 陈均策略					_
				Nymer 28664058 : Intreauntengence	J
				请导入或手动添加自定义黑名单 ①	
				批量到除 导入 添加	
🛱 事件日志				 值 Q 操作 	
				激活 Windows 转到 设置以通知 ws	
			共1条	· 取消	

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。

	戒终端安全管理	系统 V2.0.16.0						Q 11 🔿 🧬 🌅 admin 🗸
▲ 首页		终端管理 > 终端概况						
	管理へ	终端分组	 病毒查杀 终端升级 	发送通知 移动分组 远	壁协助			更多
终端		臣 全部分组 王	➡ 所有终端 ∨ 搜索:	8端名称、IP、分组、MAC地址 Q				自导出 注自定义列 圆检索
经销		■ 未分组终端(1/1)	and a standard to	A 197446340	A statem	A MACHERIN		A other
分组		□ 728品(0:0)	Science Pro-		♥ ***#BIT	♥ MACABAL	A Diamportition	▲ 2508400×4+
經黨			🗹 🖵 本机	未分组终端	192.168.53.75	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0
标签				发送通知	×			
文件				即将对所选终端发送通知,	请填写通知内容			
1131				请输入消息内容(不可超)	过120个字符)			
任务								
终端								
设备								
富 防护								
◎ 漏洞					确定 取消			
⑦ 资产								
國中心								
一 日 事件								
S IEK			共1条				20条/页 🗸 🛛	〈 1 〉 〉 1 /共1页

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。

- ()	火绒终端安全管	理系统 🔻									🤮 admin 🗸
		20 U	曾管理 > 终端概况								
	诺管理	~ [#]	寄端分组	◆ 病毒查杀 终	编升级 发送通知 移动分组 远稳	纷助	-				更多
(d)			1全部分组 豆	□ 所有终端 ∨	移动分组	×			۵	导出 走自定	义列 圆检索
·**			未分组终端(0.0)	2 终端名称	分组各称	Q	地址	病毒库版本	\$ 經道	城坂本	¢
ß			"20" / HH(+(+)	🗹 🖵 本机	全部分组	全部展开	C-29-8E-59-31	2025-03-05 10:06:02	V2.	0.16.0	
杤					本力 A11+23時 7年品	✓					
й т											
Œ											
约											
1938日1月1日日1月1日日1月1日日1月1日日1月1日日1月1日日1日1日1日1日		~									
© #		~									
¢÷		×									
en + Ed ≉		ž									
⊕ ≅						職定取消					
🤝 II		-		共1条				20条/页 🗸 🗸		> 1	/共1页

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

🛷 火绒终端安全	管理系统 V2.0.16.0				1	8索导航、模块名称	Q 11 Ø	🞝 🌔 admin 🗸
局 前页	终端管理 > 终端概况							
□ 终端管理	冬 端分组	◆ 病毒查杀 终端升级	发送通知 移动分组 远程协助					更多
终端部署	■ 全部分组 王	□ 所有终端 / 搜索: ◎	端名称、IP、分组、MAC地址 Q				● 合田 🗄	自定义列 圆检索
终端概况	■ 未分组终端(0.0)	1 1000-1220		• 1	MACHERIN	A 旅港市拓大	▲ 终端版本	
分组管理	□ 788品(1/1)	SC BELLION			MINCARAL	Non-Sheet Con-	▼ ×< muzt+	•
终端黑名单		🗹 🖵 本机	远程协助	×	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0	
标签管理			远程类型					
文件分发			○ 远程桌面 ○ 远程查看 ○ 远程CMD ①					
计划任务			远程原因*					
任务管理			帮助解决计算机使用过程中遇到的问题					
终端发现								
设备管理								
富 防护策略	~			17/120				
 (Q) 漏洞修复 	~							
191 资产管理	~		确定	取消				
♥ 中心愛理	~							
一 事件日志	~							
▼ 正版授权	=	共1条				20条/页 ~ K		1 /共1页

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。

🔊 火绒终端安全	管理系统	充 V2.0.16.0									e 🜔 🕹	admin 🗸
⋒ 前页		终端管理 > 终端概况	-									_
	~	终端分组	◆ 病毒查杀 终端升级 2	送通知 移动分组 远程协助	l.						Ŧ	E#
终端部署		靈 全部分组 亚	□ 所有终端 ∨ 搜索: 终端	名称、IP、分组、MAC地址 Q						自导出 田	自定义列(昆检索
终端就况 分组管理		■ 未分组终端(0.0)	1 终端名称	◆ 终端分组	◆ 本地IP	♦ MAC地址		病毒库版本	¢	终端版本		¢
终端黑名单		- na(<i>v</i> 1)	 二 本机 	产品	192.168.53.75	00-0C-29-83	-59-31	2025-03-05 10:06:02		V2.0.16.0		
标签管理				恢复隔离文件	×							
文件分发				请选择并填写恢复条件								
计划任务				病毒名称:								
任务管理				文件名称:								
终端发现					~ +594161 53							
设备管理												
	Č.				确定 取消							
	Č											
	~											
	~											
♥ 正版授权	≡		共1条					20条/页 ~ 10			1 /	共1页

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。

🧑 火绒终端3	安全管理系	统 V2.0.16.0					搜索导航、模块名称	Q 11 @ 🦊 🥞	admin 🗸
向 首页		终端管理 > 终端概况							
₩ 终端管理		终端分组	 前毒查杀 终端升级 	发送通知 移动分组 远	程协助				更多
终端部署		■ 全部分组 ■	師有终端 > 搜索:	终端名称、IP、分组、MAC地址 Q				自导出 辛自定义列	圓检索
分组管理		■ 未分组终端(0.0)	1 终端名称	◆ 终端分组	◆ 本地IP	◆ MAC地助止	前毒库版本	◆ 终端版本	¢
终端熈名单		un /~αα(1/1)		产品	192.168.53.75	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0	
标签管理				_					
文件分发				终端隔离	×				
计划任务				即将下发给	终端隔离任务,请选择操作				
任务管理					¶⊘				
终端发现					ξ.				
设备管理					确定 取消				
🖀 防护策略									
◎ 漏洞修复									
⑦ 资产管理									
🖾 中心管理									
🛱 事件日志									
🖶 管理工具									
♥ 正版授权			共1条				20条/页 ~ K		/共1页

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。

🧳 火绒终端3	安管理系	统 V2.0.16.0					搜索导航、模块名称	Q 11 @ 🚑 🌏 ads	min 🗸
局 首页		终病管理 > 终端概况	_						
□ 终端管理		终端分组	● 病毒查杀 终端升级 2	反送通知 移动分组 远程协助				De	
终端部署		■ 全部分组	□ 所有终端 ∨ 搜索: ◎	答称、IP、分组、MAC地址 Q				自导出 辛自定义列 國	检察
分组管理		■ 未分组终端(0/0)	2 终端名称	♦ 终端分组 ◆ 本地四		◆ MAC地址	病毒库版本	\$ 终端版本	\$
终端黑名单			🗹 🖵 本机	漏洞修复	×	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0	
标签管理									
文件分发				四村列州加加新聞「及雁川修复生好,附近年修复;	309;				
计划任务									
任务管理				○ 修复所有識詞					
终端发现				○ 修复指定补丁					
设备管理				补」第号之内以,为福, 別KB100000,KB20000	0				
富 防护策略									
◎ 漏洞修复					RD386				
(1) 約2000				MDAC.	40/5				
❷ 中心管理									
日 事件日志									
🔁 管理工具									
S IENGISIQ			共1条				20条/页 ~ K	< 1 > > 1 /#	1页

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);

🔊 火绒终端安全管	理系统 V2.0.16.0						搜索导航、模块名称	a 🕕 🔿 🚑 🤱	admin 🗸
▲ 首页	终端管理 > 终端概况								
─ 终端管理	终端分组		文件分发			×			更多
终端部署	四 全部分组	王 口 所有	文件类型: 全部 文件	名称 ~	ŧ	tio 👘		自导出 带自定义列	圆检索
分组管理	■ 未分组终端(0.0)		文件名称	◆ 文件类型	♦ 备注	٠	病毒库版本	◆ 终端版本	¢
终端黑名单		2	0708detector(1).exe	可执行文件			2025-03-05 10:06:02	V2.0.16.0	
标签管理									
文件分发						- 1			
计划任务						- 1			
任务管理						- 1			
终端发现						- 1			
						- 1			
						- 1			
⑦ 资产管理						- 1			
● 中心管理						- 1			
🛱 事件日志	/		共1条	20祭/页 ~	K < 1 /共1页 >	Я			
☆ 管理工具					T at B	1244			
						MT .			
		共1条					20条/页 🗸 🔀		/共1页
💎 正版授权		ו *							

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;

	而女王官理杀	37C V2.0.15.0			提案守机、標块名称	
白首页		终端管理 / 终端概况				
🚽 終端管理				文件分发 ×		
终端部署		终端分组	• 5	分发文件 : 策略 txt		更多
终端概况		□ 全部分组	🖵 所有約	分发方式: 仅接收 🗸		由导出 注自定义列 圆枪索
分组管理		■ 未分组终端(1/1)	17 4		▲ 病毒左折本	▲ 终端版本 ▲
终端原名4				存储位置: 桌面 > 首拨问名文件	2024.11.14 11:30:20	V20150
标签管理				终端退示: 🔽 提示用户		
文件分发				管理员正在进行分发任务,请配合管理员完成相关文件的阅读或者文件的下载安装操作。		
计划任务						
任务管理						
终端发现				运行参数: 非论境项		
设备管理				任务有效明: 2024-11-19 23:59:59		
富 防护策略						
 						
⑦ 资产管理						
🖾 中心管理						
日本 西洋日志						
🖻 管理工具				上一步 确定 取消		
TCP64287			共1条			

- (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。

🔊 火绒終端安	安管理系	统 V2.0.16.0					搜索导航、模块名称	Q 11 (A)	🚰 🤮 admin 🗸
▲ 前页		终端管理 > 终端概况							
		經備分組	● 病毒直杀 终端升级	发送通知 移动分组 远程	訪助				更多
终端部署		重全部分组 至	□ 所有终端 / 搜索: 約					自身出 淮	自定义列 圓检索
终端概况		■ 未分组终端(0.0)							
分组管理		🖵 产品(1/1)	12 終端名称	♥ 經備分组	◆ 本地IP	◆ MAC地町上	病毒库版本	经端版本	\$
终端黑名单			🗹 🖵 本机	产品	192.168.53.75	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0	
标签管理									
文件分发				垃圾清理	×				
计划任务					15° (m-66)				
任务管理					时期运输,下反垃圾清理性				
终端发现									
设备管理					确定取消				
富 防护策略									
◎ 漏洞修复									
资产管理 资产管理									
❷ 中心管理									
🛱 事件日志									
🖻 管理工具									
< 正版授权			共1条				20条/页 ~ 14		1 /共1页

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。

血斑 総議管理/総議規 登録管理/総議 化 登録管理/ 化 登録管理/	。 异常处理
使業部署 A 日本日本 日本日本 日本日本 日本	7117202
代約522 日金部分相 ■ 単新物業 ◇ 茂素: 営業合称: P. 分相、MAC地域 分相当量 ■ 未分相対策(11) 日本分相対策(11)	
● 「「「「「「」」」」 「「」」」 「「」」」 「「」」」 「「」」」 「「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」」 「」」 「」」」 「」」 「」」」 「」」 「」」」 「」」 「」」 「」」」 「」」 「」」」 「」」 「」」」 「」」」 「」」 」 「」」 」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 」 「」」 」 」 「」」 」 」 「」」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」	裕称、本地P、1Q
	(仅展示已勾选终端
文件分数 未分類経識(1) 🥑 終識各称 💠 終識分類 本地IP 💠 M	MAC地址
101任务 2011年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	00-0C-29-17-A1-39
任务管理	
 ⑦ 油产物理 	
■ 中心管理 ~	
※近 Windo	ows
(次)1 Window 共1条 共造中1条 特別役置(2)	下一步 取消

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。

秋/教堂端安全管理系统 12.0.15.0				编辑状态					
合首页		终端管理 / 终端概况		请选择目标标签					
		终端分组	· 病毒有杀 终端升级 发洗通知 称动分组	分组名称	分担名称 Q 荷法名称 Q				
10000				全部分組(3)	当前分组已选中 0 项				
经副期法		章 全部分组 王	□ 所有终端 ~ 搜索: 终端名称、D、分组、MAC地址	默认分组 (3)	标签名称	♦ 标签分组	\$		
分垍管理		團 未分组终端(1/1)	② 终端名称 ◆ 终端分组 ○ DESKTOP-TOSOOEK 未分譲终端		上海	默认分组			
终端黑名单					北京	默认分组			
标签管理					天津	默认分组			
文件分发									
计划任务									
任务管理									
终端发现									
设备管理									
器 防护策略									
③ 温洞修复									
合产管理									
國 中心管理									
日本 単作日志									
🖶 管理工具									
					共3 策				
						激活 Window	S		
			共1条			11 11 RC 44000 1	秋 取消		

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。

🛷 火绒终端安	全管理系	统 1/2.0.16.0					搜索导航、模块名称	Q 11 @ 🗳	🤗 admin 🗸
局 首页		终诺管理 > 终端概况							
□□ 终端管理		终端分组	● 病毒查杀 终端升级 :	发送通知 移动分组 远程协助	l.				更多
终端部署		□ 全部分组	□ 所有終端 ∨ 搜索: 終影					自导出 海自定义	②列 昆检索
终端概况		團 未分组终端(0.0)	1 终端名称	▲ 终端分组	≜ 本地理	≜ MACURUF	▲ 病毒库版本	▲ 终端版本	
分组管理		□ 产品(1/1)		-					
终端黑名单		🖵 測试(0.0)		/*m	192.108.55.75	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0	
标签管理				重新祭记	×				
文件分发					~				
计划任务				将对所选终端下发重新登记任务,	终端登记窗口将:				
任务管理				✓ 未完成始终显示					
终端发现				不显示已登记内容					
设留管理 					商会 取消				
IS 防护策略						- 10 C			
 (2) 満洞修复 (2) 満洞修复 									
资产管理									
资产登记									
软件管理									
<u>条统管理</u>									
硬件管理									
(194)中心管理			共1条				20条/页 🗸 🔀		/共1页
◆ 正版授权									

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

-	火绒終端安全	全管理系	统 V2.0.16.0						搜索导的	亢、模块名称	Q	11 💮	🧢 🧛 admin 🗸
୍			终端管理 > 终端概况										
Ţ	终端管理		终端分组	 病毒查杀 终端升级 	发送通知 移动分组 辽	超动助							更多
			 註 全部分组 ■ 未分组终端(0.0) 	所有终端 ど 提案:		2						自导出	畫自定义列 圆检索
				☑ 终端名称	♦ 终端分组	\$	本地IP	♦ MAC地址	\$ i	海南库版本	\$	终端版本	\$
			□ 羽伝式(0/0)	🗹 🖵 本机	产品		192.168.53.75	00-0C-29-8E-59-31	2	025-03-05 10:06:02		V2.0.16.0	
					-								
					关机			×					
					() 请确认是	否对所选终端	着下发关机任务?						
						_							
							<u>就定</u> 取消						
8													
© ~													
Ø	资产管理												
Ø													
-				共1条					209	V页 V K			1 /共1页

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。

🧦 火绒终端:	安全管理系	统 V2.0.16.0						Q 11 @ 🗳 🔮 ad	imin ~
合前页		终端管理 > 终端概况							
		經識分組	• 病毒查杀 终端升级	发送通知 移动分组 远	程协助			更	3
终端部署		□ 全部分组 至	□ 所有终端 ✓ 搜索: ◎					自导出 注自定义列 圆	检索
终端概况		■ 未分组终端(0.0)	aterials der file	A Constant (), (en	A selitor	A Tricilla	A standar of the star	A Artist Briter	
分组管理		🖵 产品(1/1)	Setting 0.704	₩ 58104773E	₩ ANUL	₩ACABAE	₩ #349/##224×	¥ seinnx≁	-
终端黑名单		型 现代代(0.0)	🗹 🖵 本机	产品	192.168.53.75	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0	
标签管理				_					
文件分发				重启	×				
计划任务									
任务管理				(())请确认是召	对所选终端下发重启任务?				
终端发现				\smile					
设备管理					職定取消				
富 防护策略									
 通用修复 									
③ 资产管理									
资产登记									
软件管理									
系统管理									
硬件管理									
◎ 中心管理									
			共1条				20条/页 🗸 🛛	< 1 > > 1 /#	41页
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。

🍠 火绒终端安全	管理系统 V2.0.16.0		搜索导航、模块名称	Q 11 @ 🛃 🧛 admin 🗸
	终端管理 > 终端概况			
	参端分组	★ 病毒直流 终端升级 发送送班 移动分组 ● 在线终端无法删除		更多
终端部署	□ 全部分组	□ 所有挖講 > 提案: 终端名称、 IP、 分祖、 MAC地址 Q		自导出 三自定义列 昆检索
分组管理	東京(10)	授辦名称 ◆ 终端分组 ◆ 本地 本地 ◆ ◆ ▲ ◆ ▲ ④ ▲	病毒库版本	◆ 终端版本 ◆
绞骗黑名单	東 測試(0.0)	2 🖵 本机 产品 192.168.53.75 00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.0.16.0
标签管理				
文件分发				
计划任务				
任务管理				
终病友境				
S 防护策略	.			
ー ② 漏洞修复	\sim			
资产管理	~			
资产登记				
软件管理				
系统管理				
硬件管理				激活 Windows
	=	共1条	20条/页 🗸 👘	< 1000 (1000)

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)。

🍠 火绒终端	安全管理系	统 V2.0.16.0							搜索导航	、模块名称	۹	11 🙃	8	admin 🗸
合首页		终端管理 > 终端概况												
□ 终端管理		终端分组	 病毒查杀 终端升级 	发送通知 移动分组 远	程协助									更多
终端部署		三 全部分组 正	所有终端 / 搜索:									由导出	※ 自定义列	昆检索
分组管理		□ 充品(1/1)	💟 終端名称	\$ 终端分组	¢	本地IP	¢	MAC地址	\$ 病	毒库版本	¢	终端版本		\$
终端黑名单		□ 测试(0.0)	🗹 📮 本机	产品		192.168.53.75		00-0C-29-8E-59-31	203	25-03-05 10:06:02		V2.0.16.0		
标签管理				_										
文件分发				加入黑名单		×								
计划任务				请确认是?	5将所选终望	劃加入终端黑名单?								
任务管理					的终端将自动	以中心删除并不再占用								
终端发现				1900	_									
设备管理						職定 取消								
🖀 防护策略														
◎ 漏洞修复														
资产管理														
资产登记														
软件管理														
系统管理														
硬件管理														
國 中心管理										F and an			/S Windows,	Laur
♥ 正版授权			共1余						20条/	д Y			1	

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;

🔊 火绒终端安全管理系	统 V2.0.16.0					搜索导航、模块名称	Q 11 A 🗳 🌅 admin 🗸
▲ 前页	終病管理 > 終 病概况						
	终端分组	● 病毒查杀 终端升级	发送通知 移动分组 远	呈协助			更多
终端部署	EI 全部分组 王	□ 所有终端 / 搜索: ◎	皆儒名称、IP、分组、MAC地址 Q				由导出 辛自定义列 國检索
Repart to	■ 未分组终端(0.0)	◎ 终端名称	◆ 终端分组	◆ 本地IP	◆ MAC地址	◆ 病毒库版本	◆ 终端版本 ◆
力坦管理	₩ 产品(1/1)		※日	102 168 53 75	00.0C 20.9E 50.31	2025 03 05 10-06-02	122.0.16.0
12/10/06/20	🖵 测试(0/0)		<i></i>	102.100.00.10	00002002000	2023 03 03 10:00:02	12.0.20.0
が広告注			卸载终端	Ŷ			
11/2/12/06			with adding with	^			
11/2/12/2			请确认是否	对所选终端下发卸载任务			
(1.7)官項 修進労羽			在执行的任务	各(卸载任务有效期为30天)			
设备管理				泣即重启电脑			
				職定取消			
→ 2-2							
软件管理							
系统管理							
硬件管理							
🖾 中心管理 🗸 🗸							
🗢 Elsisk 🚍		共1条				20条/页 🗸 🛛	〈 1 〉 > 1 /共1页

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。

🧦 火約	戒终端安全管理系	统 V2.0.16.0					搜索导航、模块名称 C		۰ 🖉	횑 admin 🗸
局 首页		终端管理 > 终端概况								
·····································	管理へ	终端分组	◆ 病毒查杀 终端升级 发送	到1 移动分组 远程协助						更多
终端	部署		□ 所有终端 ∧ 搜索: 终端名称	、IP、分组、MAC地址 Q				۵	导出 注自定义	列 昆检索
分组	管理	臺 未分組終調(00)	 □ 所有终端 □ 在线终端 	终端分组	◆ 本地IP	◆ MAC地址	病毒库版本	\$ 約	城灰本	¢
终端	黑名单	🖵 测陆(0.0)	□ 高线终端	产品	192.168.53.75	00-0C-29-8E-59-31	2025-03-05 10:06:02	V2.	0.16.0	
标签	管理		TT THE GRA							
文件:	分发									
1120	任劣 ⇔‴									
终端	发现									
设备	管理									
置 防护	策略 〜									
③ 漏洞	修复 〜									
⑦ 资产	管理へ									
资产	登记 =====									
501+1 系统	管理									
硬件	管理									
回 中心!	管理・							激活 Wi 转 到" 设置"	ndows 以激活 Window	/S
	授权 三		共1条				20號/页 🗸 🕅	CII S	> 1	/共1页

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。

🔊 火绒终端安全管理	系统 V2.0.16.0						搜索导航、模块名	🕸 Q 11 A 🔑 🌏 admin 🗸
▲ 首页	终端管理 > 终端概况							
回 終端管理 へ	终端分组	•	·直杀 终端升级 发	送通知 移动分组 远	程协助			更多
终端部署 终端概况	 重 全部分组 重 車 未分组终端(0.0) 	📮 所有	○ 所有 与出字段 × (b)口是思思出化口来??					由导出 法自定义列 圆检索
分组管理	□ 产品(1/1)		第4边要守山的子校 第十位帝 (1999年27年1)	100-L-201			◆ 病毒库版本	◆ 终端版本 ◆
终端黑名单	🖵 類試(0/0)		基本信息(珍丽当称为	(2)守子(2)		■ 主迹 ▼	2025-03-05	10:06:02 V2.0.16.0
标签管理			☑ 绥鏞名称	☑ 终端分组	终端安全状态	✓ 本地IP		
文件分发			通信IP	✓ MAC地址	计算机名称	终端类型		
计划任务			▲ 首次上线时间	上次关机时间	本次开机时间	· · · · · · · · · · · · · · · · · · ·		
任务管理			防御功能	终端隔离	策略同步	终端标签		
终端发现								
设备管理			终端登记信息			全选 ▼		
器防护策略 ~			使用人					
 								
⑦ 资产管理 ^			操作系统信息			全选 ▼		
30/~12/C								
秋(十國王 至14方開2開			共选中 6 个			号出 取消		
2010年1月1日 2010年1月1日 2010年1月1日							-	
同山心管理								
		共1条					20条/页	 K く 1 > N 1 /共1页

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。

2	火绒终端安	全管理系	统 <u>V2.0.16.0</u>							搜索	导航、模块名称	Q 11	ቀ 🕹	🤗 admin 🗸
ଜ	首页		终端管理 > 终端概况											
ģ	终端管理		终端分组	◆ 病毒查派 终端升线	发送通知 移动分组 远转	动助								更多
	终端部署		■ 全部分组 ■	所有终端 / 搜索:	终端名称、IP、分组、MAC地址 Q							€	阳 三自定义	列 圆检索
	分组管理			✓ 终端名称	◆ 终端分组	\$	本地IP	¢	MAC地址	\$	病毒库版本	请选择要展示的信	8	\$
	终端黑名单		- /-m(1/1)	🗹 🖵 本机	产品		192.168.53.75		00-0C-29-8E-59-31		2025-03-05 10:06:02	😑 全选 (6/23)		
	标签管理		- ABA(0.0)									✓ 終端名标 → 计算机名称		
												🔽 终端分组		
8	计划任务											终端安全状态		
ł	任务管理											✓ 本地IP		
	终端发现											MAC#Rh		
ŧ	设备管理											6 终端类型		
8	防护策略											操作系统名称		
0	漏洞修复											主机序列号		
Ø	资产管理													
	资产登记													
	软件管理													
a de la compañía de l	系统管理													
1	硬件管理													
Ø	中心管理											激活 Win	dows	
	正販授权			共1条						2	0策/页 🗸 🗟		>I Vindoi	/共1页

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。

<i> 秋</i> 秋 秋 終 端 安 全 管 理 系	统 V2.0.16.0			搜索导航、模块名称 Q 11 合 🗳 읒 admin 🗸
向 前页	终端管理>终端概况			
回 終備管理 へ	终端分组	◆ 病毒產杀 终端升级 发送通知 移动分组 远	呈协助	更多
终端部署	■ 全部分组 王	□ 所有终端 > 搜索: 终端名称、P、分组、MAC地址 Q		由导出 法自定义列 圆检察
分组管理	東分组终端(0.0)	第一组: 终端名称 🗸 包含 🗸 请输入	建紫关键词 或 ~ 第二组:	终端名称 · 包含 · 词输入搜索关键词
终端黑名单	□ 別試(00)		搜索 重置 取消	展开 マ
标签管理		 终端名称 终端分组 	◆ 本地IP ◆ MAC地址	 ◆ 病毒库版本 ◆ 终端版本 ◆
文件分发 计划任务		🗹 🖵 本机 产品	192.168.53.75 00-0C-29-8E-59-31	2025-03-05 10:06:02 V2.0.16.0
任务管理				
终端发现				
没备管理				
⑦ 资产管理 ^				
资产登记				
系统管理				
硬件管理				2014/2E 14 (See January
○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○		共1条		78/3石 Windows 20 余页 ∨ K く 時間 (20 第10 Windows) 1 /共1页

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。

🧦 火绒终端安全管	系统 V2.0.16.0		■ 终端详情		×
局 前页	终端管理;终端载况				
	經識分組	原毒查杀 终端开级 发达通知 移动分组	本机 🖉 & 产品 移动分组		病毒意杀 远程协助 关机 重磨 临时密码
经销售费	目 全部分组 三	□ 所有终端 ~ 搜索: 终端名称、 D、分组、 MAC地址			
终端配况	■ 未分组终端(0.0)		终端顺况 系统用/	P 网络配置 软件信息 漏洞信息 计划任务	事件日志
分组管理	□ 产品(1/1)	第一组:「我調告你」」「個書」」「「開始」	其木信息		
终偏居名单	₽ 現転(0.0)			DESETOR TOCODEV	
标壶管理		经编名称 \$ 终端分组	11 #1101%	DESKIOP-IOSOOEK	
又件分发		💟 🖵 本机 产品	本地IP	192.168.53.75	
17301195			通信IP	192.168.53.75	
住的管理			MACHBL	00-0C-29-8E-59-31	
四個次現			终端类型	Windows	
WHEN:			终端版本	V2.0.16.0	
			病毒库版本	2025-03-05 10:06:02	
			最后上线时间	2025-03-05 15:24:17	
0 30-83E			首次上线时间	2025-03-05 10:46:58	
			上次关机时间	2025-02-27 15:12:17	
5/17183/2 5/10/0018			本次开机时间	2025-03-05 10:38:48	
2010/11/02/201			96_4510	0\$71E4E4 A FINE13D7E5380ABB7768E41A0000000	
A normal of				verile-lenerop130/E3300000/70024120000000	激活 Windows
		共1条	BIRCUMPECA	正建	转到"设置"以激活 Windows。

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。

🎝 火绒終端安	全管理系	统 V2.0.15.0					搜索导航、模块名称	Q 11 @	🖞 🧛 admin 🗸
白首页		终端管理 / 分组管理							
₩ 終端管理	^								
终端部署		分组管理	ŝ	且织架构					
终端概况		添加分组 模拟分组							自导入 自导出
分组管理									
终端黑名单		■ 全部分组	■ 全部分组 まつ组络端		Q				
标签管理		未分组终端 ▶ 产品组 如1:49	分组名称	分组路径	终端数	置顶	操作		
文件分发			未分组终端	未分组终端	2	-	-		
计划任务		2310-3EL	MINE	产品组	产品组	0	\uparrow	重新分组编辑删除	
任务管理				测试组	测试组	0	\uparrow	重新分组编辑删除	
终端发现									
设备管理									
🖀 防护策略	~								
 圖洞修复 	~								
资产管理 资产管理	~								
🛛 中心管理	~								
日 事件日志	~								
✓ 正版授权	≡		́́́́́́						

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。

<i>[1]</i> 火绒终端安全管理系	统 V2.0.15.0		fi、模块名称 Q 1L の 🖓 🤤 admin 🗸
▲ 首页	终端管理 / 分组管理		
 □ 本 □ 株場管理 本 株場部等 な場面況 分知管理 外知管理 送場罷名单 标器管理 文件分发 计划任务 任务管理 代約定理 (○ 新洲所を見 ※ ※ ※ ※ 	分相管理 活加分组 雄成分组 三 全部分组 未分组终端 ・ 产品组 潮減組	添加分组 × 分组名称: 不可超过50个字 上级分组: 全部分组 · · · · · · · · · · · · · · · · · · ·	 由导入 (山导出) 銀作 - 重新分组 構織 翻除 重新分组 機構 翻除
四中心管理 ~		共 3 余记录	
💎 正版授权 🛛 🗏			

- (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。

🧦 火绒终端安全	管理系	统 V2.0.15.0					搜索导航、模块名称	Q 11 6	🖞 🤮 admin 🗸
☐ 首页 ☑ 终端管理 终端管理		终端管理 / 分组管理 分组管理	组织架构	9					
交通院兄 分组管理 终端型名单		添加分组 模拟分组 = 全部分组	⊒ 搜索	2: 分组名称	٩				自导入 自导出
~ 344.1 L +		未分组终端 > 产品组	分)组名称 删除分组 未分		×	置顶	操作	
计划任务 任务管理		测试组		产品 将分组下所有终端移至: 测试	请选择分组	~	↑ ↑	重新分组 编辑 删除 重新分组 编辑 删除	
终端发现 设备管理				-	保存	取消			
 富 防护策略 ③ 漏洞修复 									
⑦ 资产管理									
图 中心管理 甘 事件日志									
♥ 正版授权			共 3	条记录					

(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。

1	火绒终端安全	全管理系统	统 V2.0.15.0				莫块名称 Q 11 合 🦨 🤶 admin	
G			终端管理 / 分组管理					
Ţ	终端管理		分组管理			_		
	终端概况			选择分组终端匹配当前分组规则		×		
			添加分组 模拟分组	当前分组规则			自导入 自导的	H I
			■ 全部分组	规则类型	规则内容			
			未分组终端	命名分组	测试*		操作	
			▶ 产品组				重新分组编辑剧除	
	任务管理							
	終 病 友 圳 沿 条 管 理							
Se	防护策略							
0								
Ø	资产管理					▶────────────────────────────────────		
8	中心管理							
텺				#1 条记录				
	正版授权	Ξ		A TRUNK				

(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。

🎝 火绒终端安	全管理系	统 V2.0.15.0			搜索导航、模块名称	a 🕦 🚳 🦨 🧛 admin 🗸
▲ 首页 ☑ 终端管理		终端管理 / 分组管理				
终端部署 终端概况		分组管理 法加分组 模拟分组	组织架构			(山島)、山島田
分组管理		靈 全部分组		模拟分组 X		
终端黑名甲 标签管理		未分组终端	分组名利	输入终端信息模拟分组,至少需填写一项内容 终端名称:	置顶	操作
文件分发		▶ 产品3日 ▶ 须则武约日	测证	本地IP: 示例: 192.168.1.1		重新分组编辑删除
任务管理				通信IP: 示例: 192.168.1.1		
终端发现				機段		
圣 防护策略				关闭		
③ 漏洞修复						
资产管理						
回 中心管理						
日本 事件日志						
< 正版授权			共1条记载	Ŕ.		

(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。

<i>[]</i> 火绒终端安	全管理系	统 V2.0.15.0					搜索导航、模块名称 Q	1	ം 🧳 🧛 admin	· ~
☐ 首页 □ 终端管理		终端管理 / 分組管理								
- 终端部署 终端概况		分相管理	组织编档						由导入 由导	Ħ
分组管理 终端黑名单		藝 全部分组 主公份终端	■ 按索: 分组名称	٩						
标签管理 文件分发		 > 产品组 > 割試组 	分組名称 # 未分组终端 # 未分组终端	分組路径 未分组终端 未分组终端	终端数 1	置顶 -	操作			
计划任务			产品组	产品组 测试组	1	↑ ↑	更新分组 编辑 删除 更新分组 编辑 删除			
终端发现 设备管理										
 高 防护策略 ④ 漏洞修复 ④ 漏洞修复 										
🗢 TRINK			共 3 条记录							

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。

北京火绒网络科技有限公司

。 》	绒终端安全	管理系	统 V2.0.15.3			搜索导航、模块名称	Q	1। କ	4	🤗 admin 🗸
			终端管理 / 分组管理							
	ter and the state of the state	•								
<u>ب</u> هور بي										
络	治習習		分组管理	组织架构						
683	±#7:0									_
~~~	reneo d		✓ 启用LDAP设置							
分	1管理		服务器批計:	例: 127.0.0.1:389						
459	#黑名前									
			服务器用户名:	例: administrator						
标	S管理									
対	\$分发		服务器密码:		95					
भ	別任务		组织路径:	例: ou=users.dc=domain.dc=org 多路径请接行输入						
(£9	時管理									
199	需及现									
<b>设</b> (	a 管理									
			导入上级分组:	全部分组						
2 153	P策略		0-10/0/8/k							
o #3	剛修复		日本()力3日3%3時;							
<b>(2)</b> 283	2:96320			分组方式:○ 根据组织单元中的终端设备自动分组 🔷 根据组织单元中的域账号自动分组						
ΨΞ	III AL			大用・ヘ 収別主公司修繕生故 対今期公司修繕生故						
🖾 🖽	)管理									
	中市市									
LQ 94			分组名称异常:	✔ 根据创建分组名称规则自动处理 ⑦						
- <b>E</b>	<b>虹</b> 具									
			更新方式:	全量更新						
			目动更新:	后出目以更新			261			
				400 A. 044 400 A. 945-400 副244				古 Wind	IOWS	
_			保存				595 E	112001以		
♥ 未!	20X									

### 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。

》火绒终端安全管理	<b>系统</b> V2.0.15.0	~ 添加终端 ×
▲ 首页 ○ 终端管理 ▲	修动管理 / 终端果名单	· 通选择目标终端 加入服名单的终端将自动从中心删除并不再占用毁权
修講部署	15.00 BD9	分组合称 Q 终端状态:所有终端 V 终端类型:全部终端类型 V 搜索: 终端合称、本地P、M Q
终端既兄	接索: 终端名称、IP、分组、MAC地址 Q	全部分组(2) 全部展开 当前分组已进中1条 Q展示已勾选终端
分组管理		未分组终端 (1) 终端 (1) 终端 (1) 终端 (1) 终端 (1) (1) (2) 终端 (2) 
终端黑谷单		▶ 产品组(1) 音器 本机 产品组 192.168.5.24 00-0C-29-17-A1
标签管理		▶ 期试组 (0) 🔽 📑 DESKTOP-T6 未分组终端 192.168.3.143 00-50-56-98-3A
文件分发		
1101295		
终端发现		
设备管理		
宮 防护策略 🗸 🗸		
<ul> <li></li></ul>		
⑦ 资产管理 ~		
◎ 中心管理 ~		
□ ##日志 ~		
🕀 管理工具		
		共2条 (1)
C TERGISIO	共0条	共选中1条 歌消
- Interest		

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。

-87	火绒终端安全管理	鏡 <u>1/20150</u>	admin 🗸
6		终纵管理 / 核编展名单	
		820 800	
		現実:	
3		□ 漢加时间 ◆ 統執各称 ◆ 統執分組 ◆ 本地IP ◆ 通問P ◆ MAC地址 ◆ 管理员 ◆ 操作	
		□ 2024-11-19 10:55-32 DESKTOP-T6SC597 未分担修調 192.168.3.143 192.168.3.143 00-50-56-98-3A-88 admin ###	
ŝ		提示 X	
1			
3		局否确认均所选终端移出黑名单?	
i			
8			
Ŷ			
6			
	事件日志 ✓		
		共1条	

### 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。

<i>.</i>	火绒终端安全	全管理系统	V2.0.15.0							搜索导航、模块名称	Q 11	¢	2	흱 admin 🗸
@ ≝	顷		终端管理 / 标签管理											
¢ 100	· 满管理	^		0 4	01-124	80.0								52
51 51	(調節)等 (調概況		全部分组 (3)											
	相管理		默认分组 (3)		67323	5線、管理员名線	a	10000		961TE D			+# />-	
ŝ	(装黑名单		十新建分组			标金 不可超过30个字符	0/30	版法分组	• د	admin		•	和TF 微定	取消
	磁管理 2件分发					北京		默认分组		admin			编辑	019
	WE99					上海		默认分组		admin			编辑	剧除
đ	务管理					大庫		默认分组		admin			現田 !	Bible
11 12	1號发现 1各管理													
- 	护策略	~												
0 #	詞序复	~												
<b>∲</b> ≇	·广管理	ž												
⊟ Ŧ Ē:≢	*08年 •件日志	~												
순 1	理工具													
🗢 11	版接权	=			共3条								<	1 >

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

- 20	火绒终端安全	全管理系统									🧛 admin 🗸
G			终续管理 / 标签管理								
迎	<b>吃锅管理</b> 咚端部雪	Ŷ									新增
l.			全部分组 (4)	标签名称、管理员名称							
			默认分组 (4) …	标签		◆ 标签分组	¢ 12	理员	4	操作	
			十新建分组	- 北京		默认分组	ad	Imin		编辑	mile
				() 例试		默认分组	ad	Imin		编辑	####
				二 上海	提示	×	ad	Jmin		編編	####
				二 天津			ad	tmin		偏端	
					是否确认删	除所选标签?					
					100000	<b>商店</b> 取消					
88		~									
0		~									
•		ř									
T G		č									
ы ф		Ť									
<b></b>		1		共4家							

#### 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。

- 20	火绒終端安	全管理系统	¥2.0.15.0					搜索导航、模块名称	Q 11	ଚ	🦉 🤗 admin 🗸
6	首页		终端管理 / 标签管理								
Ţ	终端管理	^									
	终端部署		分组名称	Q (	批量删除						新增
	终端概况		全部分组 (3)		标签名称、管理员名称 Q						
	分组管理		默认分组 (3)			1		1 (1997)			
	终端黑名单		北方 (0)		一标签	♥ 标签分组	•	管理员		÷	操作
	标签管理			隐藏							
	文件分发		+ 新建分组	删除							
	计划任务										
	任务管理										
	终病发现										
	设备管理										
8	防护策略	~									
0	漏洞修复	~					智无相关数据				
Ø	资产管理	~									
8	中心管理	~									
贷	事件日志	~									
÷	管理工具										
					#0~						2 3 3
<b></b>	正版授权	=									

### 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。

🛷 火绒终端安全管理	<b>聚統</b> V2.0.15.0		搜索导航、提块合称 Q 🕕 ¹ み 🖧 📯 admin 🗸
▲ 普页	终端管理 / 文件分发	◎ 文件上传成功	正在上传(1) 全部取消
◎ 终端管理 へ 终端部署	<b>上榜</b> 全部期除		【文件分发】终端详情(6).xlsx ③
终端概况	文件关型: 全部 V 機索: 文件名称、备注、管理员名称 Q		0 8/10.86 KB 0 8/s
分组管理 终端黑名单	○ ∨ 文件名称 ◆ 文件类型 ◆ 备注	<ul> <li>◆ 文件大小</li> <li>◆ 上倚时间</li> </ul>	<ul> <li>● 管理员</li> <li>● 操作</li> </ul>
标签管理	终端详情(6).xlsx 文档文件 -	10.86 KB 2024-11-19 11:10:56	admin 分发下载 删除
文件分发	import_hash_list_sam 文档文件	11.43 KB 2024-11-19 11:09:47	admin 分发下载 删除
计划任务		4.37 NB 2024-11-16 16:25:32	admin 25.2 P#4 1000
任务管理			
终端发现			
安告官理 安 防治策略 、 、			
<ul> <li>副 #333 34 million</li> <li>● 贏洞修复</li> </ul>			
- ⑦ ^{治产管理} ~			
□ 中心管理 ~			
日 中午日志 V			
🔁 管理工具			
🗢 正版授权 🛛 🚍	共 3 条 / 占用 26.65 KB		

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。

-83	火绒終端安	全管理系																admin 🗸
G			终端管理 / :	文件分发														
ų	终端管理																	
			1248	12 COLUMN														
			文件类型:	全部 🗸	搜索:	文件喜称,备注,重												
			•	文件名称	¢	文件类型	¢	备注	\$	文件大小	¢	上传时间	٠	管理员	¢	操作		
			8	终端详情(6).xlsx		文档文件				10.86 KB		2024-11-19 11:10:56		admin		分发	下载 删除	
			23	import_hash_list_san	1	文档文件		2		11.43 KB		2024-11-19 11:09:47		admin		分发	下载删除	
				策略.txt		文档文件		提示			×	2024-11-18 18:25:32		admin		分发	下载删除	
								G	1									
								(	确认删除所选又	(件?								
										2010	1010							
3										THUE	409							
0																		
¢																		
Ē																		
÷																		
			共3条/1	占用 26.65 KB														
×																		

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。

#### 北京火绒网络科技有限公司

	火绒终端安全管	管理系统	V2.0.15.0	7									6	搜索导航、模块名称	٩	11	ക	e (	o admin 🗸
6	首页	1	8端管理 / :	文件分发												~	~		•
	65.200 CT																		
- -	2000 E-E		上传	全部删除															
	520mfRL/7C		文件类型:	全部 🗸	搜索:	文件名称、备注	、管理员名称	Q											
	分组管理			文件名称	¢	文件类型	\$	备注	+	文件大小	¢	上传时间	•	管理员	\$	操作			
	终端黑名单			终端详情(6).xlsx	L	文档文件		~	0	10.86 KB		2024-11-19 11:10:56		admin		分发	下载量	<b>顺余</b>	
_	标签管理			import hash list sam		文档文件				11.43 KB		2024-11-19 11:09:47		admin		分发	下载量	159	
	文件分发			· · · · · · · · · · · · · · · · · · ·		文档文件		:(2)		4.37 KB		2024-11-18 18:25:32		admin		分发	<b>T</b> 42 #	150	
	计划任务																		
	任务管理																		
	终端发现																		
	设备管理																		
8	防护策略	~																	
0	漏洞修复	~																	
Ø	资产管理	~																	
	中心管理	~																	
ta	事件日志	~																	
Ē	管理工具																		
	70464240	=	共3条/1	占用 26.65 KB															1 >
~																			

#### 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。

🛷 火绒终端安全管理系	5 <b>/6</b> V20.15.0	搜索导航、模块名称 Q 11 🔗 🖧 🌏 admin
合首页	终端管理 / 文件分发	
☑ 终端管理 ∧ 终端部署	<b>上份</b> 全部環境	
终端概况	文件类型:全部 ∨ 提表: 文件名称, 备注,管理员名称 Q.	
分组管理 终端里名单	○         文件名称         ◆         文件类型         ◆         备注         ◆         文件大小	◆         上传时间         ◆         管理员         ◆         操作
标签管理	全部页 (3) (時備(6).xlsx 文档文件 - 10.86 KB	2024-11-19 11:10:56 admin 分发 下载 翻除
文件分发	¹¹ 川山 (3) yot thash list_sam 文指文件 - 11.43 KB 須能.txt 文指文件 - 4.37 KB	2024-11-19 11:09:47 admin 分选下载 翻除 2024-11-18 18:25:32 admin 分选下载 翻除
计划任务 任务管理		
终端发现		
设备管理		
23 防护策略 ~ (の) 漏洞修复 ~		
⑦ 资产管理 ~		
■ 中心管理 ~		
🗢 正版授权 🛛 🚍	共 3 条 / 占用 26.65 KB	

#### 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。

🛷 火绒终端安全管理系	系统 V2.0.15.0	文件分发 X
	终端管理 / 文件分发	●
代謝部署     作演編第     作演編第     作演編第     作演編第     行道管理     作演編第     存述管理     文件分类     计划任务     计划任务	上传         会部務時           文件典型:         金部         陳素::         文件点段:         第第二、文件点段:         第第二、文件点段:         第三           ·         文件点段:         ◆         文件规型         ◆         編注           ·         文件点段:         ◆         文件规型         ◆         編注           ·         文件点段:         文相立作         -           ·         原稿计编句,xisx         文相立作         -           ·         原稿Lt         文相立作         -           ·         原稿Lt         文相立作         -	講进行分发设置           分发文件: 終端時間(6).xbx:           分发方式:● 欠倫收 ● 總校井道行 ● 以系統収限進行 ●           存储位置:● 点面 ● 臨時目录 ● 自主义           普遍同名文件: ●           建築規築: ●           電理风正在进行分发任务, 講配台管理局先成相关文件的间或或者文件的下载实装置作。
在另管理 作就发现 设备管理 / · · · · · · · · · · · · · · · · · ·		39/120 任時有效間: 2024-11-20 23:59:59
◆ 正版授权 三	共 3 条 / 占用 26.65 KB	上一步 電流 取用

# 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

🧳 火绒终端安全管理系	统 V2.0.15.0	创建计划任务		×
☐ 首页 ☑ 终端管理 ^	终端管理 / <b>计划任务</b>	◎ 选择执行对象	o         o         o         o           名称备注         执行时间         任务炎	2 异常处理
终端部署终端概况	前款         副時           任務実施:         全部          (任務実施:         (任務会話、衛王、堂道西	请选择执行计划任务的终端或 不支持同时按照终端和分组两个维度 选择终端 选择分组	分组 實下发任务	
分相管理 终端黑名单 标签管理	□ 任務10 ◆ 任務英型 ◆ 任務名称 ◆ 任務標準 ◆ 電理	分组名称 Q. 全部分组(2) 全部展开	终端状态: 所有终端 ∨ 终端关型: 全部终端关型 当前分组已选中 0 条	✓ 搜索: 终端谷称、本地IP、   Q ○ 仅展示已勾选终端
文件分发		未分组终端 (1) 产品组 (1)	终端名称     ◆     终端分组     本地P       ■     本机     产品组     192.16	◆ MAC地址 58.5.24 00-0C-29-17-A1
任务管理终端发现		▶ 測试组(0)	□ III DESKTOP-T6 未分组终端 192.16	58.3.143 00-50-56-98-3A
设备管理 富 防护策略  ~				
<ul> <li></li></ul>				
			共 2 条	< 1 >
	共0条	共选中 0 条		下一步取消

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。

8	火绒终端安	全管理系	V2.0.15.0	创建计划任务					×
			修調管理 / 计 <b>划任务</b>	•		•	o	o	
	终端管理			选择执行对象	名称备注	执行时间	任务类型	异常处理	
				请选择执行任务的频率					
			任务类型:全部 > 任务频率:全部 > 搜索:任务信称、备注、管理信	●任务频率:○ 单次任务	○ 按天计划 ○ 按周计划	○ 按月计划 ○ 开机执行	○ 登录执行		
				开始时间: 2024-11-19	16:22				
			□ 任勞口 ● 任躬类型 ● 任务名称 ● 任躬旗奉 ● 置垣						
			共0条				上一步	<b>►</b> →∌ I	<b>以消</b>

(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 55 / 261 计划任务进行设定并下发至终端。

秋绒终端安全管理     秋	<b>乐统 V2.0.15.0</b>	创建计划任务	×
	修調管理 / <b>计和任务</b>	· · · · · · · · · · · · · · · · · · ·	
<ul> <li>読録管理 へ</li> <li>性調節環</li> <li>性調節環</li> <li>性調節環</li> <li>性調節環</li> <li>性調節環</li> <li>性調節環</li> <li>大件分支</li> <li>计初任务</li> <li>任务管理</li> <li>(行务管理</li> </ul>			
2016万50 设备管理 器 防护策略 ~		任务执行时:22 不允许终端暂停或停止宣杀任务	
<ul> <li>◎ 温洞修复 ~</li> <li>⑦ 资产管理 ~</li> <li>◎ 中心管理 ~</li> </ul>			
☐ 事件日志 ∨ ☐ 管理工具			
🗢 iekskyk =	共0条	L-#	-步 取消

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。

🛷 火绒终端安全管理系	46 V20.150	编辑计划任务:计划任务_1	×
☐ 首页 ☑ 终端管理 ▲	终调管理 / 计划任务	● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	EQU
终端部署 终端概况 分组管理	(13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)     (13)	请选择执行计划任务的终端或分组 不支持同时按照终端和分组两个独实下发任务 选择转换 选择分组	
终端黑名单		分组名称         Q.         经購状去:新有控調         经購読型:全部修講樂型         搜索:將請名称:本地           全部分组(2)         全部原用         当前分组已进中1条         (风展示元)	P、I Q 勾选终端
文件分发		未分類終講 (1)   を 終端分組 本地IP   体 MAC地址	
计划任务		▶ 产品组 (1)	r-A1
任务管理		▶ 測试組 (0) 図 Ⅲ DESKTOP-T6 未分组终端 192.168.3.143 00-50-56-94	3-3A
终端发现			
设备管理			
器防护策略 ∨			
		共2条 <	3
S ILIGIBIQ =	共1条	共选中1条	取消

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。

-87	火绒终端安全	管理系	统 V2.0.15.0							搜	素导航、模块名称	Q 11	ം 🧟 (	🔋 admin 🗸
G			终病管理 / 计划任务											
	华 <b>装管理</b> 终端部署		<b>812</b> 809											
			任务类型:全部	▽ 任务频率: :	255 🗸	<b>搜索:</b> 任务名称,								志自定义列
			任务ID ◆	任务类型	• 任务名称	◆ 任务颁率	◆ 管理员	◆ 创建时间 ◆	最后编辑时间 \$	下次执行时间 🗘	任务对象 🗘	备注	<b>◆ 操作</b>	
			1	快速查杀	计划任务_1	单次任务	admin	2024-11-19 1	2024-11-19 1	2024-11-19 1	1		编辑 禁用	BIR:
4						根示			×					
3						DE'T			^					
							是否确认删除所	选计划任务?						
	终端发现					$\mathbf{\cdot}$	27.5							
-								<b>确定</b> 取消	1					
0														
Ø														
8														
ta -														
±														
			共1条											

### 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。

🤊 火绒終端	安全管理系	统 V2.0.15.0								技术导航	、模块名称	a 11 of 🖧 (	admin 🗸
白首页		修調管理 / 任务管理											
□ 终端管理		创建时间: 2024-1	1-13 - 2024-11-19 📋	发送通知					×			۵.	出◎设置
终端概况		任务ID	♦ 任务类型	执行详情: 全部					E务参数		◆ 管理员	◆ 操作	
分组管理		1	发送通知	终端名称	♦ 终端分组	本地IP	♦ 状态	执行详情	٠	-20 11:31:37	admin	洋情 终止9	务
终端黑名单				本机	产品组	192.168.5.24	未响应	任务尚未被接	Ψ.				
标签管理													
文件分发													
计划任务													
任务管理													
终端发现													
设备管理													
富 防护策略													
<ul> <li>④ 通知修支</li> <li>④ 通知修支</li> </ul>													
				共1条				< 1	3				
IERGRERZ		共1条											

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。

- 20	火绒终端安全	管理系	统 V2.0.15.0									🧬 💽 admin 🗸
G			修調管理 / 任务管理									
Ţ	终 <b>端管理</b> 终端部署		创建时间: 2024-11	1-13 - 2024-11-19 📋 任务类	型: 全部 🗸 秋3	5: 全部 · 搜	素: 管理员名称、任务ID					自导出 ◎设置
1			任务ID	♦ 任务类型	◆ 执行/分发	♦ 状态		¢	过期时间	◆ 管理员	\$ 摄们	
			1	发送通知	0/1	正在分发	2024-11-19	9 11:31:37	2024-11-20 11:31:37	admin	144	¥ 终止任务
					提示		×					
						是否确认终止所选任	봄?					
					·							
							<b>航空</b> 取消					
8	防护策略											
Ø												
8												
ŧ												
⊕												
			共1条									

# 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。

秋/	<b>以2.0.15.0</b>	编辑地址资源	×
白首页	核纳管理 / <b>终跳觉现</b>	* 名称: 192.168.5.0	
一 传納管理 ^ 修讷部署 修讷部署 修讷既兒		<b>编注:</b> 游输入输注	
分组管理终端黑名单	22565381 子和地址 ◆ 名称 ◆ 與关MAC ◆ 限关IP ◆ DHCP	0/120	ŧ
标签管理 文件分发	192.1885.0/24 192.1085.0 94-29-27-A8 192.1085.1 192.1883	* 12時17月 ○ 日初700 ● 南田子利1554年86時 「夜論状态: 所有疫調 >	
计划任务 任务管理		已油中 0 余     仅展示已勾造终端       0 终端名称     ◆       本地P     ◆       MAC地址	i I
修建发现 设备管理		□ ■ 本玑 192.168.5.24 00-0C-29-17-A1-39	
a Moltimat     の 高別修复      マ     の 高別修复      マ     の 高別修复      マ			
<ul> <li>● 中心管理 </li> <li>□ 中心管理 </li> <li>□ 中心管理 </li> </ul>			
		#14	
● 正版錄収 三	共1条	(RF) 10H	

(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。

🧦 火绒终端安全管理系	渡朱守航、福庆名称 Q 11 6 6	🤮 admin 🗸
@ 普页	终病管理 / 终端发现	
□ 终端管理 へ 終端部票	已没现吃病 未确认吃病 地址资源	
终端既况		出 辛自走义列
分组管理	扫描设置         ×           □ 子卵地址         各称         ● 局关MAC         ◆           □ 日地址数         ◆ 最后扫描时间         ◆ 徽注         ◆	操作
珍儀黒石車 标签管理	□ 192.168.5.0/24 192.168.5.0 94-29-2F-A8 1月開计划: O 无计划 1 253 -	1999 - 1999
文件分发	○ 扫描间隔 1-999 分钟	
计划任务		
终端发现		
设备管理	Heedel : 11.32	
<ul> <li>器 防护策略 ~</li> <li>④ 漏洞修复 ~</li> </ul>	子與扫描代題: 1 个	
⑦ 资产管理 ∨	♥ 編□日面(印刷系统)地型	
	<b>809</b>	
🗢 tensisia 🚍	共1章	

(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。

■ 🧦 火绒终端安全管	的理系统	A raiser 🚖 A O 1
合 首页	终端管理 / 终端发现	
	已发现终端 未确认终端 地址资源	
终請概况	(会議報表) 建業: 記録名称、Pr、MACB2L、子同地LC	三、自定义列 📿 检索
分相管理	□ 设备名称 ◇ 本地P ◇ 子和地址 ◇ MAC地址 ◇ 首次进取时间 ◇ 最后活跃时间 ◇ 系统典型 ◇ 设备开商 ◇ 《	秋志 4 备注 4 操作
《如用名中 标答管理	- 94-29-2F-A8 2023-02-20 1 2023-02-20 1 未知能能 未知能能 New H3C Tech 3	末時以 - 居田 勤勉
文件分发	DESKTOP-ILU…     g编集未确认终端     X    D 1… 2023-02-20 1… Windows 未知识後 Micro-Star IN… 5	来确认 - 希望 服怨
计划任务	GUOKAIHUAD     GUOKAIHUAD     GUE: 副始入音注	未确认 - 論語 删除
任务管理	01 2023-02-201 Windows 未知识新 ASUSTek COM 5	未确认 · 道道 删除
片研究现	DESKTOP-HVE 01. 2023-02-20 1 Windows #B028 Micro-Star IN 5	天体以 - 製田 単法 中決1 - 第二 単位
设备管理		
台 防护策略 ・	HRDEIMAC     現法 取用 01 2023-02-201 macOS 未知识者 Apple, Inc. ま	未确认 - 编祖 删除
<ul> <li>建同條复</li> </ul>	CENTOS 60-45-CB-6E 2023-02-20 1 2023-02-20 1 Windows #3062# ASUSTek COM #	朱微认 - 集積 删除
\$ 街产管理 ・	DESKTOP-RP 00-0C-29-6E 2023-02-20 1 Vindows #3002# VMvare, Inc. 5	未确认 - 適個 勤勉
□ 中心管理 •		
<b>首</b> 事件日志 •		
♥ 正版授权	并经查	10 象/页 = 1 2 3 7 >>

(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 发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。

=	🧦 火绒终端安全	全管理系统	统										<b>a</b> 1943	# <u>0</u> 4	
		终端	管理 /	终端发现											
				已发现终端	示确认	爬曲	地址资源								
			终端降		K, IP, MACIBI	、子問取 Q								<u>.</u>	建定义列 📿 检索
				设备名称 💠	本地IP	⇒│ 子网地址	MAC地址	: 首次发现时间 ;	● 最后活跃时间 😜	系统类型	+ 设备类型	: 设备厂商 :	状态	: 备注	0 操作
							94-29-2F-A8	2023-02-20 1	2023-02-20 1	未知系统	未知设备	New H3C Tech	未确认		SE 22
				DESKTOP-ILU	终端确认			× ²⁰ 1	2023-02-20 1	Windows	未知设备	Micro-Star IN	末确认		编辑 删除
				GUOKAIHUAD	确认为:	未安教终端		20 1	2023-02-20 1	macOS	未知设备	Apple, Inc.	朱确认		编辑 删除
					预设分组:			20 1	2023-02-20 1	Windows	未知设备	ASUSTek COM	未确认		编辑 删除
				DESKTOP-HVE				20 1	2023-02-20 1	Windows	未知识者	Micro-Star IN	未能日		255 B14
							構成	取消 20 1	2023-02-20 1	Linux	未知设备	VMware, Inc.	未确认		1018 HR2
6				HRDEIMAC	-	-	78-78-8A-D1	2023-02-20 1	2023-02-20 1	macOS	未知设备	Apple, Inc.	末确认		编辑 删除
				CENTOS			60-45-CB-6E	2023-02-20 1	2023-02-20 1	Windows	未知设备	ASUSTek COM	朱羲认		1845 B22
				DESKTOP-RP	-	1.000	00-0C-29-6E	2023-02-20 1	2023-02-20 1	Windows	未知设备	VMware, Inc.	未确认		编辑 删除
Ē															
		Ħ	€ 62 鱼										10 5	隆/页 ··· 1 2	3 7 >>

#### 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。

																							1.000 D
-	火绒终端安	<del>:</del> 全管理系统 	V2.0.15.0													搜测	2号航	模块名称	٩		କ	4 <mark>3</mark>	🤗 admin 🗸
6	首页		终端管理 / 终端发现																				
۽ <u>ت</u>	《端管理	^	已发现终端		未确认	终端	inti	日初海															
8			统计: 按终端		是否安装:	全部		<b>搜索</b> : 终端名称	、分组、	IP、MAC地址 Q	移	动分组										自导出	二 造 自定义列
2 \$	7祖宮埋 冬端黒名单		至 全部分组 (2/2)	<u>=</u>		终端名称	¢	分组	\$	本地IP	¢	MAC地址	¢	终端类型	•	安装状态	\$	子网地址	•	备注		¢	操作
8	家签管理		未分组终端(1/1)			本机		产品组		192.168.5.24		00-0C-29-17-A	1	Windows		已安装		192.168.5.0/24		-			Billion:
2	文件分发		▶ 产品组(1/1)			DESKTOP-		未分组终端		192.168.3.143		00-50-56-9B-3	A	Windows		已安装		192.168.3.0/24		-			删除
	十划任务		▶ 测试组(0/0)																				
f	王务管理																						
	冬端发现																						
ù	设备管理																						
	方护策略	~																					
0	副洞修复	~																					
Ô i	部产管理	~																					
@ •	中心管理	~																					
녆	#件日志	~																					
<u> 문</u> 1	朝王具																						
🤝 I	E版授权	=			共2 \$	Ŕ																	(1)

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。

🛷 火绒终端安全管理系	系统 V2.0.15.0			搜索导航、模块名和	၈ 오 비 ၈ 🖓 🗛 admin ~
▲ 普页	终端管理 / 终端发现				
ジェンジェンジェンジェンジェンジョン (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995) (1995)	已发现终端	未确认终端 地址资源			
终端概况 分组管理	统计: 按分组 🗸				自导出
终端黑名单	Ⅲ 全部分组 (2/2)	分组名称	已安装终端	未安装终端 ♦	安装车 🗘
标签管理	未分组终端(1/1)	未分组终端	1	0	1/1
文件分发	▶ 产品组(1/1)	产品组	1	0	1/1
计划任务	<ul> <li>Malatar(0)(0)</li> </ul>	产晶1组	0	0	0/0
任务管理		测试组	0	0	0/0
终端发现		测试1组	0	0	0/0
设备管理					
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>					
<ul> <li></li></ul>					
资产管理      ✓					
🖾 中心管理 🛛 🗸					
日、事件日志 ~					
🗢 正版授权 🛛 🚍		共5条			

### 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

= 🛷 火绒终的	安全管理系	3统 🛔 终端27号 🚖 🌲	0 1
合 首页	终期	(1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	
		· · · · · · · · · · · · · · · · · · ·	
终请规况		<b>阿奈 新治</b> 申請封詞: 全部別列 構識分類: 全部分組 ▼ 推案: 作識名称, IP, 分性, MACB社 C	三。 自定义列
好出言理			
标签管理		1921-02-17 1 <u>DESKTOP-GM</u> 未分组密编 192168.5.123 192.168.5.123 00-0C-29-79 Kingston Data U盘设备 US85TOR:DIS 血用 - 等待	审批
文件分发			
计划任务		设备申请审批 ×	
任务管理		拒绝所造动推的使用申请	
终端发现		相处理由:	
设备管理			
<b>西</b> 防护策略	·		
● 贏同修复	·	<b>942</b> 3739	
◎ 资产管理	· •		
中心管理			
■ 事件日志			
💝 正版授权	4	其1章 15 委/页	-

(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。

=	🥭 火蛾	冬端安全管	管理系统	A CHATE	۵ ک	• 1
			终端管理 / <b>设备管理</b>			
			· 设备中海			
			<b>車批測型: 全部 ▼ 車批封用: 全部10月                                    </b>			📑 自定义列
			审批时间 ◆ 终于在称 ÷ 终于分组 ÷ 本地P ÷ 通常P ÷ MACR社 ◆ 设备在称 ÷ 设备更型 ÷	⇒ 审批类型 ◆	管理员 ;	操作
			2023-02-17 1447 <u>DESKTOP-GM4Q</u> 未分担相請 192.168.5.123 192.168.5.123 00-0C-29-79-E0 Kingston DataTra U盘设备	同意	admin	谨慎
			设备审批序情 ×			
			设备实外期径:USBSTOR\DISK8ampVEN KINGSTON8ampPROD DA			
			申请时间:2023-02-1714-0050			
6			中语说明:			
Ð						
8						
۵						
曲						
			<b>共1</b> 章		15 条/页	- 1 -

2. 信任设备

≡ 🛷 火绒终端安	2-全管理系统 ▲ ◎ ▲ ◎ ▲
合 首页	約納世後 / 设备管理
	· 迎發申請 审批记录 使任何表
终调概况	推測分组: 全部分组 ▼ 接索: 终端名称: P. 分组, MACB社 Q 菜 自定义列
が坦言理	「 「現著名称 +
标签管理	DESKTOP-GMAQ         非分错终端         192.168.5.123         192.168.5.123         00-0C-29-79-E0         Kingston DataTra         U盘设备         USBSTOR.DISK8         展用         2023-02-28 1446         服性
文件分发	
计划任务	個任後醫體機 ×
任务管理	确定删除供任设备?
终端发现	5 分钟后篇过终跳用户使用,并没送渡知
	<b>80</b> 2
<ul> <li>Interview and</li> <li>Interview and</li> </ul>	
S IEKENSKI	共1章 15 氢度 - 1

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。

🍠 火绒终端安全	管理系统	V2.0.16.0		搜索导航、模块各称	Q 11 II 🔿 📌 📯 admin 🗸
合首页	105	が塗結 > <b>策略部署</b>			
😡 终端管理	~	新建築略			
宮 防护策略	^	援索:终端分组 Q			
策略部署	_	终端分组	终端总数	部響防护策略	
策略管理		■ 未分组终端	0	獣込防护策略	
1日注义1年			1	歌込防护策略	
₩□中			0	默认防护策略	
终端动态认证		· · · · · ·		产品策略	
<ul> <li>圖洞修复</li> </ul>	~				
⑦ 资产管理	~				
<b>四</b> 中心管理	~				
<b>己</b> 事件日志	~				
🖻 管理工具					
					激活 Windows 转到"设置"以激活 Windows。
⇒ 正版授权	Ξ				

#### 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。

🄊 火绒终端安全管理到	<b>聚统</b> <u>V2.0.16.0</u>		授索导航、楔块名称 Q, 11 🛛 🖉 🤹 admin 🗸
▲ 首页	防护策略 > <b>策略部署</b>		
□ 終講管理 ∨	新版的编辑		
宮 防护策略 へ	搜索: 终端分组 Q		
策略部署			
策略管理	彩號分組	· 培訓思数	當一個的方式的影響
信任文件	■ 未分组终端	0	默认防护策略
黑名单	♀ 产品	1	默认防护策略
U盘管理	u Nit	新建策略 ×	默认防护策略 🗸
终端动态认证		→ 请选择策略模板: 默认防护策略	
<ul> <li>&gt; 編詞修复</li> <li>&gt; </li> </ul>			
资 资产管理 ~		新新文革明为秋: 新公照月90小子小	
❷ 中心管理 ~			
🔁 管理工具			
STEREIGHZ =			

# 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。

// 火绒終端安	全管理系							🗳 🤮 admin 🗸
白首页		防护策略 > 策略管理						
😡 终端管理	~	新建筑路						
置 防护策略	^	策略名称	•	使用该策略分组		¢	策略管理	
策略部署		二 默认防护策略					音看策略	
策略管理		▶ 火绒为您准备好的防护策略						
信任文件		一 产品策略 自定义防护规则					编辑策略	删除策略
黑名单								
U盘管理					新建末略 ×			
					資法経策賠償板: 駅以防护策略 ∨			
	Č				·····································			
	~							
日 事件日志	~				<b>稍定</b> 取消			
合管理工具								
♥ 正版授权	≡							

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。

🛷 火绒终端安全管理	系统 V2.0.16.0					搜索导航、模块名称	Q 11	e 🕹 (	🤱 admin 🗸
局 首页 □ 终端管理 >	防护策略>策略管理>编辑策略			❷ 操作成功					
国防护策略 へ 策略部署	8 Windows (2.0)								
住民管理 低任文件 単名章 総論効応以征 ④ 課務修复 ~ ⑦ 読子管理 ~ 日 中心管理 ~ 行 幸好日志 ~ 合 管理工具	<ul> <li>② 東規</li> <li>三級政策</li> <li>通知総置</li> <li>成準監察</li> <li>③ 病毒防損</li> <li>● 原稿防損</li> </ul>	升級方式 前級方式 前助升级 ● 手助升级 回动升级射 (欠升级病毒体 免打扰模式 一 开启免打扰模式 ② 借任区保护 責止信任区操作 既屬区保护 莫止居属区操作 安全日志保护 日志保存 30 天 ③	新建策略 () 一) 一) 一) 一) 一) 一) 一) 一) 一) 一	領感新御成功! 成現和? 二字语	× Ruš				
♥ IIMINK =		○ 禁止満除日志							

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。

🧦 火绒终端安全管理	系统 V2.0.16.0	搜索导航、模块	·名称 Q	1	֎ 😵	🤗 admin 🗸
▲ 首页	防护策略 > 策略管理 > 編編策略					
回終端管理 イ	く 編編策略: 測试策略					
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	🗄 Windows (2.0)					
策略管理	▼ 1② 業規	升级方式				
信任文件	基础配置	○ 自动升级 ● 手动升级				
黑各单	通知设置	自动升级时				
U盘管理	病毒查杀	(2升级病毒库				
终端动态认证	▶ ⊕ 病毒防御	免打扰模式				
<ul> <li>(2) 漏洞修复</li> <li>(2) 漏洞修复</li> </ul>	▶  系统防御	开启免打扰模式 🕥				
⑦ 资产管理 ~	● 网络防御	信任区保护				
□ 中心管理 ∨	▶ 18 访问控制	禁止倍任区操作				
	<ul> <li>B2 安全工具</li> </ul>	mar //Rth				
	▼ 図 行为管理	mileicons/ 年上回本区場所				
	软件禁用	Distribution of the second s				
	违规外联	安全日志保护				
	桌面控制	日志保存 30 天①				
		蒙止消除日志				
			72	败舌 Wir	idows	
🗢 正版授权 🛛 🚍				erre willing h	AZUE WING	

● 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。

🌔 火绒终端安	全管理系统	¥ V2.0.16.0		搜索导航、模块名称 Q	11. I admin 🗸
白首页		防护策略 > 策略管理 > 编辑策略			
₩ 终端管理	~	く 編編策略: 測试策略			
S 防护策略 策略部署	^	8 Windows (2.0)	✓ @tr		
策略管理		▼ ② 常规	通知设置		
信任文件		基础配置	中心统一设置 《 终端自主设置 (终端可自行设置常规/免打扰模式下是否显示以下弹窗)		
黑名单		通知设置	3年逾四寸471	举规模式	免打扰模式
U盘管理		病毒查杀	后台病毒查杀·完成时	•	0
终端动态认证		<ul> <li>一 病毒防御</li> </ul>	文件实时监控-自动处理时		
<ul> <li>         · 漏洞修复         ·         ·         ·</li></ul>	~	● 一系統防御	恶意行为监控。自动处理时		0
资产管理	~	<ul> <li>● 网络防御</li> </ul>			
□● 中心管理	~	<ul> <li>IBI 访问控制</li> </ul>		-	0
日 事件日志	~	▶ BS 安全工具	下现保护一旦式以优性的		
		▼ □ 行为管理	邮件监控。自动处理时		
		软件禁用	邮件监控-仅记录时		
		违规外联	Web扫描-自动处理时		
		桌面控制	Web归描-仅记录时		
			摄像头保护-仅通知时		
			联网控制-阻止联网时	•	數活 Windows
◇ 正版授权	Ξ		程序执行控制,自动阻止时	<b>()</b>	詩到"设置"以邀活 Windows。

● 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。

🍠 火绒终端安全管理系	<b>彩统</b> V20160	搜索导航、模块名称 Q 11 🗇 🖧 🌻 admin 🗸
▲ 首页 ● 终端管理 ✓	防护推动 > 操制管理 > <b>编编译略</b> 《 编辑课题 · 编编课题	
<ul> <li>院防沖衛</li> <li>策略部構</li> <li>策略部構</li> <li>定任文件</li> <li>定任文件</li> <li>定任文件</li> <li>定任文件</li> <li>空機動効素以近</li> <li>(企)</li> <li>(行)</li>     &lt;</ul>	<ul> <li>(2.0) ● 667</li> <li>② 常規</li> <li>全盘音乐设置</li> <li>③ 常規</li> <li>学 尿度音乐证欄包中的肉肉木马,并自动测过大于 20 MB8的压缩包 (20M-9999M)</li> <li>地元: 自追义归属符自动归風压缩包,并不受以上大小限制</li> <li>内病音乐</li> <li>● 741億 ● 6450 備</li> <li>● 11屆网络瓶动器</li> <li>● 第級訪問</li> <li>● 11屆四條約(前前出),這麼快個影响計算机性能</li> <li>○ 前用出稿,這麼快個影响計算机性能</li> </ul>	
	<ul> <li>次 安全具員</li> <li>不 扫描描述 描述 2 (件)</li> <li>※ 付 第 用 造船外線</li> <li>並用 定制</li> <li>文件 描述</li> <li>文件 描述</li> </ul>	副時所造 第2000 今人 号出 操作 游活 Windows 時所の感感 Windows
→ 正版授权 📃	暫无相关数据	

- (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。

🧦 火绒終端安	全管理系	统 V2.0.16.0			(	搜索导航、模块名称	۹ (	I A	🛃 🤗 ad	Imin 🗸
白首页		防护策略>策略管理>编编策略								
₩ 终端管理		〈 編編策略: 測试策略								
🖀 防护策略		88 Windows (2.0)	──保存							
策略部署										
策略管理		▶ ② 常規	开启文件实时监控 🌕							
信任文件		▼ → 病毒防御	扫描时机							
黑名单		文件实时监控	<ul> <li>在文件执行时进行扫描,不影响性能</li> </ul>	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				
U盘管理		恶意行为监控								
终端动态认证		内存防护	扫描文件时							
◎ 漏洞修复		U盘保护	不扫描指定路径文件							
金产管理		下载保护						除所选	漆加规则 导入 !	
🛛 中心管理		邮件监控	文件路径	文件备注					操作	
🛱 事件日志		Web扫描								
		▶  系統防御								
		▶ ⊕ 网络防御								
		· IBI 访问控制								
		<ul> <li>B 安全工具</li> </ul>			暂无相关数据					
		▼ 団 行为管理								
		软件禁用								
		违规外联					激活	Windo 習慣"以激詞	WS § Windows,	
⇒ 正版授权										

● 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

🧦 火绒终端安全	全管理系	統 V2.0.16.0	接索导航 模块名称	Q 11	🔿 🤌 🤗 admin 🗸
<b>合</b> 首页		防护策略>策略管理>编攝策略			
─ 终端管理		〈 編編策略: 測试策略			
22 防护策略 策略部署		🖶 Windows (2.0)	✓ 0000		
策略管理		▶ ③ 常规	开启恶意行为监控 💽		
信任文件		▼ → 病毒防御	发现病毒时		
黑名单		文件实时监控	● 補數還示终端自主选择 ● 自动处理		
U盘管理		恶意行为监控	3#55.emmtra4		
终端动态认证		内存防护			
◎ 漏洞修复		U盘保护			
🖗 资产管理		下载保护	增强初步病毒防护		
🙆 中心管理		邮件监控	开启敬赏病毒诱捕		
🛱 事件日志		Web扫描			
🖶 管理工具		▶  系统防御			
		▶ ⊕ 网络防御			
		▶ (8)访问控制			
		<ul> <li>B2 安全工具</li> </ul>			
		▼   行为管理			
		软件禁用			
		违规外联		激活 \ 转到"设	VINdows 置"以激活 Windows。
☞ 正版授权					

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。

🍠 火绒終端安	全管理系	统 V2.0.16.0	<b>搜索导航、模块</b> 名称	Q 11 🔿 🗳 🐥 admin 🗸
白首页		防护策略 > 策略管理 > 編編策略		
🚽 終端管理		〈 编辑策略: 测试策略		
S 防护策略 策略部署		8E Windows (2.0)	<ul> <li>✓ \$27</li> </ul>	
策略管理		▶ ③ 端规	开局内存防护 🌔	
信任文件		▼ ⊕ 病毒防御	扫描灵敏度	
黑谷单		文件实时监控	○ 低,系统性能优先    ○ 适中,占用少量系统性能    ○ 高,扫描能力优先	
U盘管理		恶意行为监控	分词晚趣时	
终端动态认证		内存防护		
◎ 漏洞修复		U盘保护		
⑦ 资产管理		下载保护	满种病毒时	
🖾 中心管理		邮件监控	☑ 将傍晦文件备份至隔离区	
<b>甘</b> 事件日志		Web扫描		
		▶ 團 系统防御		
		▶ ⊕ 网络防御		
		· (3) 访问控制		
		<ul> <li>B 安全工具</li> </ul>		
		▼ 🖂 行为管理		
		软件禁用		MANT MAL
		违规外联		闭心石 WINDOWS 转到"设置"以激活 Windows。
😔 正版授权				

● 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。

🧦 火绒终端安全管理	系统 V2.0.16.0	提供导致、模块名称	۹	11 🔿	🧔 🧛 admin 🗸
<b>向</b> 首页	防护策略 > 策略管理 > 编辑策略				
🥶 终端管理 🗸 🗸	〈 编辑策略: 测试策略				
S 防护策略 へ 策略部署	🖶 Windows (2.0)				
策略管理	③ 常規	开启心盘保护 💽			
信任文件	▼ ⊕ 病毒防御	当U盘接入电脑时			
黑名单	文件实时监控	✓ 检测核病毒核改计的项目			
U盘管理	恶意行为监控				
终端动态认证	内存防护	发现两番时			
<ul> <li>③ 漏洞修复 ~</li> </ul>	U盘保护	○ 弹簧提示终端目主选择   ○ 目动处理			
	下载保护	清除病毒时			
<b>四</b> 中心管理 ~	邮件监控	❷ 将病毒文件备份至隔离区			
	Web扫描	压缩包扫描设置			
合 管理工具	▶  系统防御	☑ 深度查泳压缩包中的病毒木马,并自动跳过大于 20 MB的压缩包(20M-9999M)			
	▶ ⊕ 网络防御				
	▶ 哈 访问控制				
	▶ 路 安全工具				
	▼ □ 行为管理				
	软件禁用				
	违规外联		湯女汗 (赤豆)	Window	VS
				94.000, 97.000,00	

● 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。

》 火绒终端安全管理	系统 V2.0.16.0	投资导航、模块名称	Q 11. AP 📌 🌏 adma	in 🗸
▲ 首页 回 终端管理 >	防护策略 > 策略管理 > 编辑策略 < 编辑策略: 观试策略			
	88 Windows (2.0)	<		
第編管理 倍任文件 展名単 以自管理 作員动志い证 ⑥ 扁同除数 ~ ⑦ 音介管理 ~ 〇 音介管理 ~ 〇 音介管理 ~	<ul> <li>② 米規</li> <li>③ 桃梅的朗</li> <li>文件抜き料道投</li> <li>思察行力道投</li> <li>内存防护</li> <li>以虚保护</li> <li>下配保护</li> <li>邮件监控</li> <li>Web扫描</li> <li>● 网络防弱</li> <li>● 网络防弱</li> <li>● 防防防制</li> <li>● 防防防弱</li> </ul>	井田 平板線9 ●		
🗢 正版授权 🛛 🚍	软件禁用 违规外联		激活 Windows ^{转到"设置"} 以激活 Windows。	

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。

🛷 火绒终端安全管理系	统 V2.0.16.0	(	搜索导航、模块名称	Q 11 (	ə 🦺 🧛 admin 🗸
▲ 首页 ■ 终端管理 >	防护策略 > 策略管理 > 編編策略				
<b>宮防护策略へ</b> 策略部署	🗄 Windows (2.0)	<ul> <li>✓</li> <li>Ø#</li> </ul>			
兼編管理       偏任文件       黒名母       U血管理       修論功応以正       ③ 顧明修友       ⑦ 近行管理       中心管理       一〇 寄作日志       〇 警道工具	<ul> <li>③ 常規</li> <li>④ 病毒防御 文件(未)利益臣&lt;</li> <li>思想行为益臣</li> <li>内容防护</li> <li>以截保护</li> <li>下数保护</li> <li>邮件监控</li> <li>Web引順</li> <li>● 原 系統防御</li> </ul>	<ul> <li> 开启邮件监控 <ul> <li>保护范置</li> <li>建改邮件 2 没送邮件</li> </ul> </li> <li>2 接收邮件 2 没送邮件</li> <li>2 按照师母け</li> <li>② 仪记录 ● 自动处理</li> <li>清除师母け</li> <li>③ 将病毒文件备份至隔离区</li> <li>邮件目調</li> <li>重水邮件中的病毒水马,并自动爬过大于 20 MB的邮件 (1M-20M)</li> </ul>			
	<ul> <li>● 网络助卵</li> <li>● 切伯拉制</li> <li>● 欲 安全工具</li> <li>○ 行力管理</li> <li>(六) 行力管理</li> <li>(秋件規用</li> <li>(池泉外駅)</li> </ul>	BPF+7809       BPC       25       NITP       110       POP3		謝除所述 激活 Wind 转到"设置"(1)	液カの規則 発生 線構 酸除 酸酸 酸酸 酸酸 酸酸 酸酸 酸酸 酸酸 酸酸 酸酸
				read well the	

● 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。

🍠 火绒终端安全管	管理系统 V2.0.16.0	检索	导航、模块名称 C	11 4	> 🔮	🤗 admin 🗸
▲ 首页 ● 终端管理	防护策略 > 策略管理 > <b>編編策略</b>					
S 防护策略 策略部署	▲ 88 Windows (2.0)	✓ 貸存				
第略管理 信任文件 尿名単 U皇管理 終続功志认证 ② 贏術修复	<ul> <li>③ 密規</li> <li>④ 病毒防御</li> <li>文件支討监控</li> <li>思察行为监控</li> <li>内存防护</li> <li>U盘保护</li> <li>工業内内</li> </ul>	开館Web43版				
	✓ PacketP* ● 即件监控 ✓ Web扫描					
	<ul> <li>● 系統防御</li> <li>● 网络防御</li> <li>○ 访问控制</li> <li>&gt; ⑥ 安全工具</li> <li>○ 行力管理</li> <li>次件祭用</li> </ul>					
◆ 正版授权	<b>违规外联</b>			激活 Wind 转到"设置"以	lows 數活 Windo	WS.

- (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;

🧦 火绒终端安全	管理系统	V2.0.16.0	搜	索导航、模块名称	Q	1	ନ 🕹	🤗 admin 🗸
▲ 首页 ◎ 终端管理	~	防护策略 > 策略管理 > 編編策略						
S 防护策略 策略部署	^	😫 Windows (2.0)	<ul> <li>✓ G#</li> </ul>					
策略管理 信任文件		<ul> <li>              ô) 常规      </li> <li>             f) 病毒防御         </li> </ul>	开加系统加固 💽					
黑谷单		<ul> <li>▼ □ 系统防御</li> </ul>	自动处理					
6 四日日日 修備动态认证		应用如固	1051-162 <u>m</u>					
<ul> <li>(2) 編詞條复</li> <li>(3) 资产管理</li> </ul>	~	软件 <del>安装巨</del> 截 摄像头防护	8219-96(19) 自动处理规则 1019-96(11)		生效方式			
● 中心管理 □ 中心管理 □ 中心管理	~	<ul><li>浏览器保护</li><li>● 网络防御</li></ul>	文件版的 防止指定文件项目被算改,被环动想思创建		已开启11	项		>
		<ul> <li>/8)访问控制</li> <li>&gt; 88 安全工具</li> </ul>	注册表现理》 防止指定注册表示意义		已开启32	项		>
		<ul> <li>         行为管理         软件禁用     </li> </ul>	ROSE-2017年10月24 EULISING在可对当场地运动内容的标志小作		已开启31	项		>
		违规外联 桌面控制						
- ▼ 正版授权	=				游灯 转到	舌 Win 『设置"D	dows 激活 Wind	óws,

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。

🧦 火绒終端安全	管理系	充 V2.0.16.0	(	搜索导航、模块名称	Q 11 A 🦨 🧛 admin 🗸
▲ 首页		防护策略 > 策略管理 > 编辑策略			
♀ 终端管理	~	〈 编辑策略: 测试策略			
S 防护策略 策略部署	^	88 Windows (2.0)	्		
策略管理		▶ ② 常規	开启系统加固 🔼		
信任文件		▶ → 病毒防御	自动处理		
黑名单		▼ 型 系统防御	🗹 启用内置过滤规则 🛛 🔽 启用系统免疫 🛛 🔽 允许终端用户添加自动处理规则		
U盘管理		系統加固			
终端动态认证		应用加固	防护设置		
④ 漏洞修复	~	软件安装拦截	防护规则 自动处理规则		删除新选 添加规则 导入导出
⑦ 资产管理	~	摄像头防护	程序路径		操作
中心管理	~	浏览器保护			
<b>日</b> 事件日志	~	▶ ⊕ 网络防御			
		> 🕒 访问控制			
		<ul> <li>B 安全工具</li> </ul>			
		▼ □ 行为管理			
		软件禁用			
		违规外联	暂无相关数据		
		真面控制			
					激活 Windows
✓ 正版授权	≡				4479 次国 NAME MILLIOM2®

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。

🍠 火绒終端安	全管理系	统 V2.0.16.0			15	紫导航、機块名称 Q 11 命 🗳 <page-header> admin 🗸</page-header>
▲ 首页		防护策略>策略管理>编辑策略	ŝ			
🚽 终端管理		〈 编辑策略: 测试策略		自动处理	×	
<b>富防护策略</b> 策略部署		🔀 Windows (2.0)	~	<b>文件路径</b> : 可不填写, 默认"代表所有路径	0 包含子程序	
策略管理		▶ ◎ 常规	开启系统	文件规则 注册表规则 敏感动作规则		
信任文件		<ul> <li>         ·   ·   ·   ·   病毒防御     </li> </ul>	自动处理	请选择需要自动处理的防护项目,并设置生效方式		
黑谷单		▼ 및 系統防御	□ 扁用	恶意创建系统任务目录	自动阻止 ~	
U盘管理		系统加固		恶意创建桌面快捷方式	目动阻止 >	
终端动态认证		应用加固	防护设置	恶意创建任务栏快捷方式	自动阻止 >	
③ 漏洞修复		软件安装拦截	防护规	启动配置文件	自动阻止 ~	删除新选 添加规则 导入 导出
资产管理		摄像头防护		启动目录(扩展保护)	自动阻止 🗸	操作
<b>四</b> 中心管理		浏览器保护		特殊系统目录	自动阻止	
🔂 事件日志		▶ ⊕ 网络防御		Autorun配置文件	自动阻止	
🔁 管理工具		<ul> <li>/8) 访问控制</li> </ul>		关键系统文件	自动阻止	
		▶ BS 安全工具		IE快捷方式	自动阻止	
		▼ □ 行为管理		IE收藏夹目录	自动阻止	
		软件票用		保护对象: 自动处理规则必须开启对应的防护项目才能生效	· · · · · ·	
		述规外联			保存取消	
		桌面控制				
◆ 正版授权						

● 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。

🎝 火绒终端安全管理	97 V20160	搜索导航、模块名称	Q 11 🔿 🧬 🧛 admin 🗸
▲ 首页	防护策略》策略管理》編纂策略		
・ 終端管理 く	〈 编辑策略: 测试策略		
<b>宮防护策略 へ</b> 策略部署	6号 Windows (2.0). (2.6)		
策略管理	・ ③ 増現 开启应用加固 💽		
信任文件	▶ ④ 病毒防御 加固类型		
黑名单	一 四 系統防御     「 Web服务器    「 数据库    「		
U盘管理	系統加固		
终端动态认证	应用加固		
② 漏洞修复 ~	软件安装拦截		
⑦ 资产管理 ~	摄像头防护		
🙆 中心管理 🛛 🗸	道法醫院的		
	• ④ 网络8500		
由 管理工具	> 图 访问控制		
	<ul> <li>B8 安全工具</li> </ul>		
	▼ 図 行为管理		
	软件舔用		
	违规分联		
	直面控制		
			激沽 Windows 转到"设置"以激活 Windows。
⇒ 正版授权 =			

● 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。

🛷 火绒终端安	安管理系	统 12.0.16.0			搜索导航、模块名称	Q 11 🔿 🚑 🌏 admin 🗸
白茴		防护策略 > 策略管理 > 编辑策略				
😡 终端管理		〈 编辑策略: 测试策略				
器防护策略 策略部署		😤 Windows (2.0)	✓ 保存			
策略管理		▶ ② 常规	开启软件安装拦截 🌕			
信任文件		▶ ⊕ 病毒防御	软件安装拦截模式			
黑名单		▼ 型 系统防御	○ 弹窗提示终端目主选择 ○ 自动阻止列表外已识别软件的安	装行为		
U盘管理		系統加固	软件安装拦截白名单			制除标准 法加援制 导入 导生
终端动态认证		应用加固				40 Au
◎ 漏洞修复		软件安装拦截	软件各称 软件类型			J梁17F
资 资产管理		攝像头防护				
🖾 中心管理		浏览器保护				
13 事件日志		<ul> <li>● 网络防御</li> </ul>				
		▶ 🕒 访问控制				
		▶ BS 安全工具				
		▼   行为管理		新王相关数据		
		软件禁用		PERMIT		
		违规外联				
		桌面控制				
◇ 正版授权						

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。

🧦 火绒终端安全管	理系统 12.0.16.0						Q 11 🔿 🗳 🤑 admin 🗸
白首页	防护策略>策略管理> 鏡欄策略						
2 终端管理	< 编辑策略: 测试策略		软件安装拦截规则列表			×	
S 防护策略 策略部署	▲ Windows (2.0)		<u> 类型:</u> 全部 🗸	<b>搜索:</b> 请输入软件名称	Q	18.b0	
策略管理	• ⑥ 常规	开启软件	软件名称	♦ 软件类型		۰	
信任文件	▶ ⊕ 病毒防御	软件安察	龙皇传说	游戏软件			
黑谷单	▼ 型 系统防御	0 弹窗	龙珠直播	視頻軟件			
U盘管理	系统加固	软件安察	龙卷风收音机	音乐软件			
终端动态认证	应用加固	1 International	齐齐直播	视频软件			
<ul> <li>高洞修复</li> </ul>	◇ 軟件安装拦截	and the second se	鼠标皮肤大师	其他软件			23621 F-
⑦ 资产管理	◇ 摄像头防护		黑暗之光	游戏软件			
			麦咖啡	安全软件			
			麦光文档	办公软件			
E BALM	<ul> <li>▶ № 安全TE</li> </ul>		鲨鱼看图	图形图像			
	▼ 団 行为管理		鲁大师游戏库	游戏软件			
	软件藻用		鲁大师游戏中心	游戏软件			
	违规外联		共 779 条	20条/页	× K く 1 /共39	р页 >	
	桌面控制					_	
● 正版授权	=						

● 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。

🧷 火绒终端安	全管理系	统 1/2.0.16.0		夏索导航、模块名称	Q 11	ଚ 🛵	🤗 admin 🗸
☐ 首页 ☑ 终端管理		防护策略 > 策略管理 > <b>编辑策略</b> 〈 编辑策略: 演试策略					
器防护策略 策略部署		E Windows (2.0)	× <u>99</u>				
<ul> <li>第8時期</li> <li>高丘文件</li> <li>黒名単</li> <li>以盆管理</li> <li>終端动志以正</li> <li>(金) 識別除发</li> <li>(金) 違か管理</li> <li>(金) 御作日志</li> <li>(金) 管理工具</li> </ul>		<ul> <li>③ 常規</li> <li>④ 病毒防闭</li> <li>圖 系統防闭</li> <li>風 系統防闭</li> <li>成用加固</li> <li>软件交換拦截</li> <li><b>國金先防护</b></li> <li>週間關保护</li> <li>● 网络防闭</li> <li>合。访问控制</li> <li>路 安全工具</li> <li>マ 行为管理</li> <li>软件前用</li> <li>边规外联</li> </ul>	开启攝像共動評 ●       新程末風用攝像共動       ● (双通知 ● } } / 滑動燈示容論目主选择 ● 自动阻止       目助故行设置       ● 自动放行形有数字签名的程序:       ● 自动放行形有数字签名的程序:   ● 目动放行形有数字签名的程序:				
❤ 正版接权		桌面控制			激活 Win ^{转到"设置"以}	dows 激活 Windo	ws,

● 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。

🧦 火绒终端安	全管理系	充 V2.0.16.0	搜索导航、模块各			🔮 🧛 admin 🗸
合首页		防护策略>策略管理>编编策略				
₩ 终端管理	~	く 編編策略: 測试策略				
S 防护策略 策略部署	^	H Windows (2.0)	✓ 066			
策略管理		▶ ② 業規	开启浏览器保护			
信任文件		<ul> <li>(1) 病毒防御</li> </ul>	保护浏览器首页			
黑名单		▼ Ⅲ 系统防御				
U盘管理		系統加固	● 空白页			
终端动态认证		应用加固	◎ 自定义			
③ 漏洞修复	~	软件安装拦截				
⑦ 资产管理	~	摄像头防护				
<b>四</b> 中心管理	~	浏览器保护				
🛱 事件日志	~	<ul> <li>● 网络防御</li> </ul>				
🔁 管理工具		<ul> <li>/8) 访问控制</li> </ul>				
		▶ 88 安全工具				
		▼ 図 行为管理				
		软件禁用				
		违规外联				
		桌面控制				
				激	活 Windows	
➡ 正版授权	≡					

(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。

🧦 火绒终端安全管理系	<b>钱务</b> V20160 搜索	导航、模块名称 Q	11 🔿 🦨 🧛 admin 🗸
☐ 首页 ☑ 终端管理 ∨	訪护策略,外期管理,9 <b>編成策略</b> < 編成策略: 劉武策略		
<ul> <li>         防护体験         不前応認識         新航管理         備任文件         居名单         以監管理         终端のおい征         </li> </ul>	限 Windows (2.0)     保存       第 第規     开届网络入爆世戦 ●       • 第 等時時期     · 仅记录 ● 自动相止       • ● 時期時期     · 仅记录 ● 自动相止       • 東田訪りな法世戦 ●     · (口记录 ● 自动相止		
<ul> <li>○ 薬得修复 &gt;</li> <li>⑦ 遊产管理 &gt;</li> <li>四 中心管理 &gt;</li> <li>一 中心管理 &gt;</li> <li>一 南中日市 &gt;</li> <li>一 管理工具</li> </ul>	<ul> <li>株向後遊坊</li> <li>开启電戸向館坊</li> <li>(C2表 ● 自动組止</li> <li>近程登式坊か</li> <li>近2章 気坊か</li> <li>万記、松服务望か ●</li> <li>(C2表 ● 自动組止</li> <li>(C2 = 1)</li> <li>(C2 = 1)</li></ul>		副時所語 編成開始 令入 守住
	\$\krt \$\rt \$\rt \$\rt \$\rt \$\rt \$\rt \$\krt \$\rt \$\krt \$\rt \$\rt \$\rt \$\rt \$\krt \$\krt \$\krt \$\krt \$\rt \$\krt \$	98 新	◆ 操作 然活 Windows 例"设置"以激活 Windows。

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。

火绒终端安全管理	系统 V20160			搜索导航、模块名称	Q 11 @ 🦨 🤗 admin 🗸
▲ 首页	防护策略 > 策略管理 > 编辑策略				
回 终端管理 く	〈 编辑策略: 测试策略				
図防护策略 へ 策略部署	🛱 Windows (2.0)	▽ 保存			
策略管理	▶ ◎ 常规	开启横向渗透防护 🌔			
信任文件	▶ ⊕ 病毒防御	触犯规则时			
黑名单	▶ 型 系统防御	○ 仅记录  ○ 自动阻止			
U盘管理	▼ ● 网络防御	防护设置			
终端动态认证	基础防护	防护规则 信任列表			
<ul> <li>         ·</li></ul>	横向渗透防护	Relation	PetrovkoR		14.00TT <del>**</del>
⑦ 资产管理 ~	暴破攻击防护		6-920-12CM		VIBC/TX
四中心管理 く	远程登录防护	远程DCOM调用	对远程调用本机DCOM组件的行为进行拦截		
	恶意网址拦截	远程MMC调用	对远程调用本机MMC20.Application的行为进行拦截		•
	▶ 1名 访问控制	远程打印机添加	阻止通过RPC远程添加打印机驱动		
	▶ 昭 安全工具	远程注册表篡改	阻止通过RPC远程修改本机注册表		
	▼ 図 行为管理	远程服务创建	阻止通过RPC远程创建本机服务		
	软件禁用	默认共享访问	阻止对本机Windows默认共享的访问		
	违规外联	远程计划任务创建	阻止通过RPC远程创建本机计划任务		
	桌曲控制	远程WMI调用	对远程调用本机WMI的行为进行拦截		● 激活 Windows
					转到"设置"以激活 Windows。

● 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。

🎝 火绒终端 <del>安</del> 全管理	系统 <u>V2.0.160</u>			提索导致	t、模块名称 Q 11 @ 🗳 😜 admin 🗸
▲ 首页	防护策略 > 策略管理 > 编辑策略				
♀ 终端管理 ~	く 編編策略: 測試策略				
富防护策略 <b>^</b> 策略部署	88 Windows (2.0)	~ 保存			
策略管理	▶ ◎ 常規	开启暴破攻击防护 🌔			0
信任文件	▶ ⊕ 病毒防御	暴力破解攻击白名单			· 國際新造 添加规则 导入 导出
黑名单	▶  系統防御		▲ 活田芥園	▲ @注	▲ JE//=
U盘管理	▼ ⊕ 网络防御	ZMEIP ()	▲ 18/13/468	• BL/I	▼ 1780 P
终端动态认证	基础防护				
圖洞修复 ~	橫向渗透防护				
资 资产管理 ~	暴破攻击防护				
❷ 中心管理 ∨	远程登录防护				
	恶意网址拦截				
管理工具	▶ 181 访问控制				
	<ul> <li>BS 安全工具</li> </ul>			智尤相关数据	
	▼ □ 行为管理				
	软件禁用				
	违规外联				
	桌面控制				NUMBER AND A
					激活 Windows 转到"设置"以激活 Windows。
🗢 正版授权 📃					

● 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。

🍠 火绒終端安全	管理系统	¥ V2.0.16.0			搜索导航、模块名称 Q	11 🔿 🗳 🧛 admin 🗸
▲ 単页		防护策略 > 策略管理 > 编辑策略				
₩ 終端管理	~	〈 编辑策略: 测试策略				
IS 防护策略 策略部	^	8 Windows (2.0)	✓ <b>侯存</b>			
策略管理		▶ ② 常规	开启远程登录防护			0
信任文件		<ul> <li>→ 病毒防御</li> </ul>	远程登录防护白谷单			删除所选 添加规则 导入导出
黑名单		▶ 型 系统防御				A +117/0-
U盘管理		▼ ⊕ 网络防御				₩ DRTF
终端动态认证		基础防护				
◎ 漏洞修复	~	橫向渗透防护				
资产管理	~	蒙破攻击防护				
❷ 中心管理	~	远程登录防护				
<b>一日</b> 事件日志	~	恶意网址拦截				
		▶ 🔠 访问控制				
		<ul> <li>B 安全工具</li> </ul>		暂无相关数据		
		▼ □ 行为管理				
		软件禁用				
		违规外联				
		桌面控制				
					調	敷沽 Windows 倒"设置"以激活 Windows。
→ 正版授权	≡					

● 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。

🧦 火绒终端安	全管理系	统 1/2.0.16.0			搜索导航、模块名称	Q 11	ଚ 🦺	🤗 admin 🗸
白菌		防护策略 > 策略管理 > 编辑策略						
😡 终端管理		〈 編編策略: 測试策略						
宮 防护策略 策略部署		8 Windows (2.0)	<ul> <li>保存</li> </ul>					
策略管理		▶ ③ 举规	开启恶意网址拦截 🛑					0
信任文件		<ul> <li>(十)病毒防御</li> </ul>	恶癖颐山兰藏					
黑名单		▶  系统防御						
U盘管理		▼ ⊕ 网络防御	规则包	状态				
终端动态认证		基础防护	木马、盗号					
〇 漏洞修复		横向渗透防护	钓鱼、仿冒					
😚 资产管理		暴破攻击防护	虚假、欺诈					
❷ 中心管理		远程登录防护	流氓软件					
日本 事件日志		恶意网址拦截						
🔁 管理工具		▶ 18 访问控制						
		<ul> <li>B2 安全工具</li> </ul>						
		▼ □ 行为管理						
		软件禁用						
		违规外联						
		桌面控制						
						激活 ₩	/indows どに激活 Windo	
✓ 正版授权								

- (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。

🧦 火绒终端安全管理	系统 V2.0.16.0					搜索导航、	模块名称 Q	11 🔿 🛃	🤗 admin 🗸
合前页	防护策略 > 策略管理 > 编辑策略								
፼ 终端管理 ~	〈 编辑策略: 测试策略								
S 防护策略 へ ^{策略部署}	H Windows (2.0)	< ── 保存							
策略管理	▶ ⑥ 常規	开启IP协议控制							
信任文件	<ul> <li>         ·</li></ul>							删除所选 添加规则	19 导入 导出
黑名单	▶ 型 系统防御	规则名称	▲ 应用程序	▲ 漫明		▲ 优先级	▲ 牛顿状态	▲ 接作	
U盘管理	▶ ⊕ 网络防御		•	•			· Lonros	• 1 •	
终端动态认证	▼ 181 访问控制								
<ul> <li>         通訊修复 ~     </li> </ul>	IP协议控制								
⑦ 资产管理 ~	IP黑名单								
■ 中心管理 ~	联网控制								
	网站内容控制								
🔂 管理工具	程序执行控制				報无相关数据				
	设备控制								
	▶ BS 安全工具								
	▼ □ 行为管理								
	软件禁用								
	违规外联						滑灯	5 Windows	
	泉面控制						转到	"设置"以激活 Wind	lows
😔 正版授权 🗧									

● 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。

🧦 火绒终端安全管理	系统 V2.0.16.0				搜索导航、模块名称	Q 11 @ 🗳 <table-cell> admin ~</table-cell>
▲ 首页	防护策略 > 策略管理 > 编辑策略					
♀ 终端管理 ~	〈 编辑策略: 测试策略					
宮防护策略 へ	88 Windows (2.0)	◇ 保存				
策略管理	▶ ② 常规	开启IP黑名单				
信任文件	<ul> <li>→ 病毒防御</li> </ul>					
黑名单	<ul> <li>              手統防御      </li> </ul>					
U盘管理	<ul> <li>● 网络防御</li> </ul>	远程IP或域名②	♥ 备注			◆ 操作
终端动态认证	▼ 18 访问控制					
<ul> <li></li></ul>	IP协议控制					
⑦ 资产管理 ~	IP黑名单					
🛛 中心管理 🛛 🗸	联网控制					
	网站内容控制					
⊕ 管理工具	程序执行控制					
	设备控制			智无相关数据		
	▶ BS 安全工具					
	▼ □ 行为管理					
	软件禁用					
	违规外联					
	桌面控制					激活 Windows 转到"设置"以激活 Windows。
🗢 正版授权 🛛 🚍						

● 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。

🧦 火绒终端安全	管理系统	花 V2.0.16.0				搜索导航、模块名称	Q 11 A 🦨 🤶 admin 🗸
白首页		防护策略 > 策略管理 > 编辑策略					
🝚 终端管理	~	〈 编辑策略: 测试策略					
<b>国 防护策略</b> 策略部署	^	🗄 Windows (2.0)	~ 保存				
策略管理		▶ ② 端规	开启联网控制 🔘				
信任文件		▶ 🕀 病毒防御	规则外程序联网				
黑名单		▶ 型 系统防御	○ 允许联网 ○ 阻止联网				
U盘管理		▶ ⊕ 网络防御	自动放行设置				
终端动态认证		<ul> <li>哈 访问控制</li> </ul>	自动放行带有数字签名的程序	✓ 自动放行系统核心程度			
◎ 漏洞修复	~	IP协议控制					
资产管理	~	IP黑名单					· 影除所选 深加规则 导入 导出
🖾 中心管理	~	联网控制	规则名称	◆ 规则操型	\$	操作方式	◆ 操作
<b>甘</b> 事件日志	~	网站内容控制					
		程序执行控制					
		设备控制					
		<ul> <li>BS 安全工具</li> </ul>					
		▼ 🖂 行为管理					
		软件禁用			暂无相关数据		
		违规外联					No. 27 Aug. 1
		桌面控制					游灯石 WINDOWS 转到"设置"以激活 Windows。
✓ 正版授权	=						

● 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 M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)

🧦 火绒终端安全	全管理系	统 V2.0.16.0	我太守	流、模块名称 Q	11 🔿	🖨 🧛 admin 🗸
白首页		防护策略 > 策略管理 > 编辑策略				_
🖳 终端管理		〈 编辑策略: 测试策略				
器防护策略 策略部署		H Windows (2.0)	v <u>au</u>			
策略管理		▶ ③ 常规	开启网站内窗控制 💽			
信任文件		→ 病毒防御	设置名单属性			
黑名单		▶ 型 系统防御	<ul> <li>○ 黑谷单 ○ 白谷单 ○</li> </ul>			
U盘管理		▶ ⊕ 网络防御				
终端动态认证		▼ 1合 访问控制	网络拉利名里			
③ 漏洞修复		IP协议控制	BEDRAUU SIA		制料析法 流力	网络则 导入 导出
资产管理		IP黑名单	- 規则名称		♦ 操	作
🚇 中心管理		联网控制				
12 事件日志		网站内容控制				
		程序执行控制				
		设备控制				
		<ul> <li>B 安全工具</li> </ul>				
		▼ 🖂 行为管理				
		软件禁用	<b>鞘无相关数据</b>			
		违规外联				
		桌面控制			敷活 Windows ^{後到"设置"} 以激活 v	s Vindows。
◇ 正版授权						

● 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。

🌔 火绒終端安全管理系	统 120160	搜索导航、模块名称Q	11 🔿 📌 🤤 admin 🗸
白首页	助が接着 > 無線構成		
○ 终端管理 ∨ S 防护*策略 ∧ 策略部署 策略管理	<ul> <li>Seetama: 2055.004</li> <li>20 第規</li> <li>用指程序执行控制 </li> </ul>		
信任文件 黒名単 以島管理 検護功応以近 ② 運得修复 ~ ③ 運得修复 ~	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	援作 〇 〇 〇	٩
● 中心管理 ~ □ 神件日志 ~ □ 管理工具	联份控制         > 网络游戏           网站内音控制         > 影高级乐           起床从行控制         > 单划游戏           设备控制         > 声划游戏           设备控制         > 对战平台           > 日行力管理         > 下载站           放件契用         > WR工具           支加分明         > WR工具		激活 Windows
→ 正版授权 🚍			转到"设置"以激活 Windows。

● 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。

🍠 火绒终端安	全管理系统	充 V2.0.16.0			搜索导航、模块名称	۹	11 🔿	J .	admin 🗸
▲ 首页		防护策略 > 策略管理 > 编辑策略							
😡 终端管理	~	〈 编辑策略: 测试策略							
S 防护策略 策略部署	^	🕾 Windows (2.0)	<ul> <li>Q存</li> </ul>						
策略管理		▶ ② 举规	开启设备控制 🔵						
信任文件		<ul> <li>一 病毒防御</li> </ul>	信任U盘						
黑名单		▶ 型 系统防御	☑ 信任已注册U盘 ①						
U盘管理		▶ ⊕ 网络防御							
终端动态认证		▼ 18 访问控制	外疫使用 设备控制日沿单						
③ 漏洞修复	~	IP协议控制	设备	状态					
资产管理     资产管理	~	IP黑名单	U盘设备	允许 🗸					
🙆 中心管理	~	联网控制	便携设备①	允许 ~					
🛱 事件日志	~	网站内容控制	USB无线网卡	允许 🗸					
🔁 管理工具		程序执行控制	USB有线网卡	允许					
		设备控制	打印机	允许					
		<ul> <li>BS 安全工具</li> </ul>	光驱	允许					
		▼ 図 行为管理	蓝牙	允许   ∨					
		软件禁用							
		违规外联				油炉田	Window	MS	
		桌面控制				病知"	设置"以激混	f Windows,	
😔 正版授权	Ξ								

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。

🍠 火绒终端安全管理	系统 V2.0.16.0				搜索导航、模块名称 Q	11 🔿 🗳 📯 admin 🗸
合首页	防护策略>策略管理>编辑策略					
፼ 终端管理 ✓	〈 编辑策略: 测试策略					
宮防护策略 へ ^{策略部署}	🖶 Windows (2.0)	~ <b>6.17</b>				
策略管理	▶ ③ 常规	开启设备控制				
信任文件	▶ (十)病毒防御	信任U盘				
黑名单	▶ 型 系统防御	☑ 信任已注册U盘 ①				
U盘管理	▶ ⊕ 网络防御					
终端动态认证	▼ (8) 访问控制	外國使用一個會控制日石車	_			
③ 漏洞修复 ~	IP协议控制	设备名称		♦ 备注		◆ 操作
资产管理 ~	IP黑名单	hm的U盘	设备实例路径支持通配符*?			确定 取消
回中心管理 く	联网控制					
は事件日志 ~	网站内容控制					
🔁 管理工具	程序执行控制					
	设备控制					
	▶ 路安全工具					
	▼ □ 行为管理					
	软件禁用					
	违规外联					
	桌面控制					激活 Windows 转到"设置"以激活 Windows。
❤ 正版授权 ☰						

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。

🛷 火绒终端安全	管理系统	€ V2.0.16.0					搜索导航、模块名称	Q	1	⊕ ⁴ / ₄	🤗 admin 🗸
▲ 首页		防护策略 > 策略管理 > 编辑策略									
🚽 終端管理	~	〈 编編策略: 测试策略									
<b>富防护策略</b> 策略部署	^	88 Windows (2.0)	保存								
策略管理		▶ ② 常规	开启设备控制								
信任文件		▶ ⊕ 病毒防御	信任U盘								
黑名单		▶ 團 系统防御	🔽 信任已注册U盘 🛈								
U盘管理		▶ ⊕ 网络防御							INCO ST	all State	N 91 94
终端动态认证		▼ 1台 访问控制	外腹股州 设备控制日名单								ৰ মান্য কৰা
◎ 漏洞修复	~	IP协议控制	设备名称	+	设备实例路径	♦ 备注				✿ 操作	
资产管理     资产管理	~	IP黑名单	hm的U盘		设备实例路径支持通配符*?					确定	取消
🖾 中心管理	~	联网控制									
日 事件日志	$\sim$	网站内容控制									
🖨 管理工具		程序执行控制									
		设备控制									
		<ul> <li></li></ul>									
		▼ □ 行为管理									
		软件禁用									
		违规外联									
		桌面控制						湯	if Wir	ndows 江歌师 Wind	
♥ 正版授权	=								es etall r		

(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。

》 火绒终端安全	全管理系统	¥ V2.0.16.0						搜索导航、模块名	称 Q	11	କ 🛃	odmin 🗸
<b>向</b> 首页		防护策略 > 策略管理 > 编辑策略										
₩ 终端管理	~	〈 編編策略: 測试策略										
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	^	🔀 Windows (2.0)	< ── 保存									
策略管理		▶ ② 举规	管理安全工具									
信任文件		▶ 🕀 病毒防御	脱离中心管理的终端可使	使用所有安全工具。								
黑名单 U&管理		<ul> <li>● 系统防御</li> <li>● 网络防御</li> </ul>	安全工具	操作								
终端动态认证		▶ (A) 访问控制	启动项管理	○ 允许使用	) 禁止使用	○ 禁止并隐藏						
<ul> <li>高河修复</li> </ul>	~	▼ 88 安全工具	系统修复	○ 允许使用	○ 禁止使用	○ 禁止并隐藏						
资产管理	~	管理安全工具	文件粉碎	○ 允许便用	○ 禁止使用	○ 禁止并隐藏						
🕮 中心管理	~	漏洞修复	右键管理	○ 允许使用	○ 禁止使用	○ 禁止并隐藏						
🛱 事件日志	~	弹窗拦截	断网修复	○ 允许使用	○ 禁止使用	○ 禁止并隐藏						
🖻 管理工具		垃圾清理	流量监控	○ 允许使用	○ 禁止使用	○ 禁止并隐藏						
		▼ □ 行为管理										
		软件禁用										
		违规外联										
		桌面控制										
										飲活 Wi ^{変到"设置"}	ndows 以激活 Wind	
⇒ 正版授权	≡											

● 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。

🍠 火绒终端安全管理	系统 V2.0.16.0	<b>搜索导航、模块告</b> 标	Q 11	@ 🦺	🤗 admin 🗸
▲ 首页 □ ◎ 終端管理 ~	防护策略 > 策略管理 > 編編策略 < 編編策略: 測試策略				
国防护策略 へ 策略部署	82 Windows (2.0)				
第8管理 低任文件 黒名単 じ盘管理 作装功おい征 ④ 薬明修复 ~ ① 造产管理 ~ 日 中心管理 ~ 亡 管理工具	<ul> <li>② 常規</li> <li>③ 内局防弱</li> <li>○ 内局防弱</li> <li>○ 内局防弱</li> <li>④ 防局控制</li> <li>② 防局控制</li> <li>※ 安全工具</li> <li>管理安全工具</li> <li>建築支工具</li> <li>建築支工具</li> <li>建築支工具</li> <li>2 (万力管理 軟件執用</li> </ul>	▲明学奖 ● 九行使用 ● 泉止使用 ● 泉止使用 ● 泉上井釉鉱       13瓶号学复       ● 开印台目动扫描高色遮明       发现黑铜时 ● 询问我 ● 自动修复       や丁下载       ● 自动征配网络 ● 优先从外网下载 ~       ● 自动征配网络 ● 优先从外网下载 ~       ● ① 代本小丁載       ● ① 不载印度法同时进行 ● 全部下载完成后,再安装       ● 下载印度法同时进行 ● 全部下载完成后,再安装			
▼ IINGHRQ Ξ	造現外戰	其他设置 关闭Wadows自动更新	激活 W 转到"设置	indows 『以激活 Windo	ows,

● 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。

🍠 火绒終端安	全管理系	统 V2.0.16.0	證素导統、總共在称 Q	11 🔿 🛃	🤗 admin 🗸
白首页		防护策略>策略管理>编辑策略			
😡 终端管理		〈 編編策略: 測试策略			
S 防护策略 策略部署		Hindows (2.0)	✓ 847		
策略管理		▶ ② 筆規	弹鐵拦截 📀 允许使用 💿 禁止使用 💿 禁止并隐藏		
		<ul> <li>一 病毒防御</li> </ul>	✓ 开机自局边		
黑名单		▶  系统防御			
U盘管理		▶ ⊕ 网络防御			
终端动态认证		哈 访问控制			
◎ 漏洞修复		▼ 路 安全工具			
资产管理		管理安全工具			
❷ 中心管理		漏洞修复			
日 事件日志		弹窗拦截			
		垃圾清理			
		▼ □ 行为管理			
		软件禁用			
		违规外联			
		桌面控制			
			[20] 1995	舌 Windows 『设置"以激活 Wind	
✓ 正版授权					

● 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。

🎝 火绒终端安全管理系	統 v20160 世表号航	模块名称 Q 11 🛛 🖨 🤤 admin 🗸
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	(秋) 1000         (秋日秋年)         (秋日	鐵块容称 Q 11 @ 🔑 Q admin ∨
	<ul> <li>□ 行為管理</li> <li>         ☆件 振用         通販控制     </li> </ul>	激活 Windows 转时记者"以激声 Windows,
🔷 正版授权 📃		

(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。

🍠 火绒终端安全管理	系统 1/2.0.16.0				搜索导航、模块名称	Q 11 🔿 🛃 <page-header> admin 🗸</page-header>
▲ 前页 ○ 総構管理 → ※ 防护策略 へ 策略部層 策略部層 病階管理 信任文件 黑名单 U型管理	<ul> <li>         防护策略 &gt; 策略管理 &gt; 鐵編筆略                                                                                                                                     &lt;</li></ul>	<ul> <li></li></ul>	吸线锅,并在软件卸载完成前保持提示			
<ul> <li>終講动応认证</li> <li>③ 漏房修复 ~</li> <li>⑦ 资产管理 ~</li> <li>四 中心管理 ~</li> </ul>	<ul> <li>              らの時期      </li> <li>             会会主工具         </li> <li>             伝行為管理         </li> <li>             な件為用         </li> </ul>	设置软件名单的属性 <ul> <li>用名单</li> <li>自名单</li> <li>雷弦件名单</li> <li>撒簧: 软件名称, 版本, 发布者, 备注</li> </ul>	Q		Billenna fi	动添加 从软件都完成加 排序 导入 导生
	注地化外联 点面积2时	软件名称	发布者	版本号 新元用大数据	留注	<b>操作</b> 渺活 Windows
- ▽ 正版授权 - 三						转到"设置"以激活 Windows。

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。

🌔 火绒终端安	全管理系统	充 V2.0.16.0				搜索导航、模块名称 C	າ ແ 🤉 🦨 (	odmin 🗸
<ul> <li>         ・         ・         ・</li></ul>	~	防护策略 > 策略管理 > <b>编辑策略</b> < 編編策略: <b>測试策略</b>						
S 防护策略 策略部署	^	8 Windows (2.0)	✓ 保存					
第時管理 信任文件 黒名単 し創管理 终端の応认征 ⑥ 瀧同修复 ⑦ 治产管理	~ ~	<ul> <li>⑤ 常規</li> <li>⑤ 常規(5)</li> <li>○ 原場(5)</li> <li>● 阿爾(5)</li> <li>● 阿爾(5)</li> <li>● 伊爾(5)</li> <li>● (5)</li> <li>○ (5)<th>开启软件装用</th><th>1出现发展,并在软件和联先成前/保持提示</th><th></th><th></th><th></th><th></th></li></ul>	开启软件装用	1出现发展,并在软件和联先成前/保持提示				
四) 中心管理 日本	~	*X(中 <del>族</del> )用 违规外联	软件名称	发布者	版本号	备注	操作	
		点面(23)		1 支持運動符*?	支16/高起行*?	调动品口软件器注信器	etta 新聞	jij
◇ 正版接权	Ξ						報到"设置"以激活 Windov	//S ₀

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。

🐠 火绒終端安	安管理系	统 V2.0.16.0		搜索导航、模块名称 Q 11 @ 🧬 🥥 admin 🗸
▲ 首页		防护策略 > 策略管理 > 編編策略		
🚽 终端管理		〈 编辑策略: 测试策略	选择软件添加至软件名单 ×	
<b>运防护策略</b> 策略部署		🗄 Windows (2.0)	当前列表: 全部软件 ✓ 提案: 软件名称, 没布者 Q 系加	
策略管理		▶ ◎ 常規 开启\$	软件名称         ◆         发布者         ◆         版本号         ◆	
信任文件		▶ ⊕ 病毒防御 发现票	Microsoft Edge Microsoft Corporation 133.0.3065.92	
黑名单		▶  系統防御 ○ 仅	Microsoft OneDrive Microsoft Corporation 25.020.0202.0001	
U盘管理		▶ ⊕ 网络防御 设置部	Microsoft Update Health Tools Microsoft Corporation 3.74.0.0	
终端动态认证		▶ ④ 访问控制	Microsoft Visual C++ 2010 x64 R Microsoft Corporation 10.0.30319	
<ul> <li>圖洞修复</li> </ul>		▶ B8 安全工具	Microsoft Visual C++ 2010 x86 R Microsoft Corporation 10.0.40219	
资产管理		▼ 図 行为管理 目240 19/10	Microsoft Visual C++ 2015-2019 Microsoft Corporation 14.28.29913.0	
· 中心管理		软件禁用 按承 -	Microsoft Visual C++ 2015-2019 Microsoft Corporation 14.28.29913.0	的原始症 于动脉和 从软件和力脉和 操行 每人 守卫
		造现外联 []]	Microsoft Windows Desktop Runt Microsoft Corporation 6.0.21.32717	备注 操作
四、居建工堂		W(B)LT#J	Mozilla Firefox (x86 zh-CN) Mozilla 135.0.1	
			<b>共19条</b> 20象页 ◇ K 〈 Ⅰ /共1页 〉 >>	
			谢溪加縣用软件的餐注信息	
			智无相关数据	
◆ 正版授权				

● 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。

🎝 火绒终端安	全管理系	统 V2.0.16.0			搜索导航、模块名称	۹	11	ه 🐣	🤑 admin 🗸
合首页		防护策略 > 策略管理 > <b>编辑策略</b>							
<ul> <li>○ 终端管理</li> <li>○ 防护策略</li> <li>策略部署</li> <li>策略部署</li> <li>第時管理</li> <li>信任文件</li> <li>黑合单</li> <li>じ盘管理</li> <li>终端动志认证</li> <li>○ 運動修算</li> </ul>		<ul> <li>( 線磁発電: 透明式発電</li> <li>( ) Windows (2.0)</li> <li>( ) 常規</li> <li>( ) 病毒防闭</li> <li>( ) 病毒防闭</li> <li>( ) 所毒防闭</li> <li>( ) 所高防闭</li> <li>( ) ( ) ( ) () () () () () () () () () (</li></ul>	安存           开启出现外联 ●           環境進齢WiFi           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・           ・						
<ul> <li>         · · · · · · · · · · · · · · ·</li></ul>		<ul> <li>□ 行为管理</li> <li>軟件禁用</li> <li>透泉外敷</li> </ul>					删除所述	告 添加规则	<del></del>
		威国拉制	URL %KE	11元用大数据		激氾	Win	操作 dows 激话 Wind	
✓ 正版授权						(18:21)	(오페 니)		

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)。

🧦 火绒终端安全管理	系统 V2.0.16.0		搜索导航、模块名称	Q 11 A 🦨 🧛 admin 🗸
▲ 首页	防护策略 > 策略管理 > 编辑策略			
	〈 編編策略: 測试策略			
器防护策略 へ 策略部署	🔠 Windows (2.0)			
策略管理	▶ ◎ 常规	开启桌面控制 💽		
信任文件	▶ ⊕ 病毒防御	<b>配置检查时间:</b> 每 30 🗘 分钟, 对终端配置进行检查修正		
黑名单	▶  系统防御	● 概面錄作		
U盘管理	▶ ● 网络防御	- montane-v		
终端动态认证	▶ (2) 访问控制			
<ul> <li>〇 漏洞修复 ~</li> </ul>	<ul> <li>BS 安全工具</li> </ul>			
资产管理      ✓	▼ □ 行为管理	<b>•</b>		
四中心管理 ~	软件禁用	将盤挺文件指摘至此区域、也可以点击上传点面整纸		
日本の日本	违规外联	2514-12015 VANDREN ON FOLLY AND IN TERPOLITY AND AN ADDRENG STATION REPO		
	桌面控制			
		屏幕适应方式: 拉伸 🗸		
		□ 同时设设为税属界面 ◎		
		2 无操作 10		
				激活 Windows 转到"设置"以激活 Windows。
下版授权 =				

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

》 火绒终端安全	管理系统 V2016.0			搜索导航、模块名称	Q 11 A 🗳 🌏 admin 🗸
▲ 首页 ○ 终端管理	防护策略 > <b>信任文件</b>				
22 防护策略 策略部署	▲ 项目类型: 全部	✓ 搜索: 信任项目、备注	Q		
策略管理	信任项目	♦ 笛注	★ 项目类型 添加信任项目 ×	會任文件动作	◆ 操作
黑名单			信任文件		
U盘管理 终端动态认证			文件描述 通过填写需要信任的文件、文件夹名称的方式信任项目		
	× .		文件指注: 文仲國配行"/ 文件备注: 不可超过30个字符		
● □○ □ □ □ ■ 中心管理	×.		信任文件动作		
<ul> <li>日 単件日志</li> <li>日 単件日志</li> <li>日 管理工具</li> </ul>	. <b>∞</b> :		信任文件发起的动作(初退后,病毒防御、系統防御、访问控制功能将 信任该文件发起的动作)		
			職定取消		
ITIE HEART	±0条				

## 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。

🔊 火绒终端安全	管理系	统 \\2.0.16.0			搜索导航、模块名称 Q	11 🔿 🗘 🌏 admin 🗸
▲ 首页		防护策略 > 黑名单				
□ 终端管理		添加				命设置
S 防护策略		<b>类型: 全部 / 操作时间:</b> 全部时间 ~ 全部时间	四 <b>搜索</b> : 文件哈希、备注、管理			由导入 由导出
策略管理		文件驗希 💠 畜注	◆ 类型	◆ 管理员	◆ 操作时间	◆ 操作
信任文件		7£4e63073e7ad84e5981676e2ea5	MD5	admin	2025-03-06 10:44:17	删除
黑名单			添加	×		
U盘管理			文件哈希*	□选择文件,自动计算阶希值		
终端动态认证			支持SHA1、SHA256、MD5	0/64		
◎ 漏洞修复			祭注			
资产管理			请输入备注	0.50		
中心管理						
				确定 取消		
田 管理工具						
☞ 正版授权		共1条			20条/页 ~ K <	1 〉 〉 1 /共1页

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。

减 火绒终端安全管理系	<b>5统</b> V2.0.16.0				oʻ 🗳 혽 admin 🗸
▲ 首页	防护策略 > 黑名单				
♀ 終端管理 ~	<b>浙山</b> 副标案				命设置
器防护策略 ^ 策略部署	<b>类型:全部 &gt; 操作时间:</b> 全部时间 ~ 全部时间	回 <b>搜索</b> : 文件驗希、备注、管理员 Q			自导入 自导出
策略管理	○ 文件始希 ◆ 备注	◆ 类型	◆ 管理员	◆ 操作时间	◆ 操作
信任文件	7f4e63073e7ad84e5981676e2ea5	MD5	admin	2025-03-06 10:44:17	删除
黑名单		设置	×		
U盘管理		病毒名称前缀 ①			
终端动态认证		Threatintlligence	17/32		
<ul> <li>         ·          ·          ·</li></ul>		防护范围*			
资产管理      ✓		✓ 病毒查杀			
□ 中心管理 ~		✓ 病毒防御			
		确定	取消		
合管理工具					
	共1条			20条/页 🗸 🤘 🕹 🕹	>> 1 /共1页

## 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。
   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。

≡ 🧦 火統終端安全管理系统	👗 终端部署 🚖 🌲 🌀 💄
合 首页         助护策略 / U監管理	
□ 终端散现 •	
局 防护策略 * 密码硬件: 全部 ▼ 提案: U监会称 ▼	
	÷ ↓ 操作
策然管理 但在学品	
10日本19 	
)作品ID:Storage Device 设备ID:125D20140310 终端的お从证	
U盘含称:	
U金審任: #20頃頃(木可認近120个学校) ・ () ・ () ・ () ・ () ・ () ・ () ・ () ・	
□ 中心管理 ・	
(首) ●件日志 ● ※ ● 発行 ○ 光台	
97MAUX: UE945/WER	

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。

=	閷 火鐵路	胺全律	會理系統	A sease	≙	 0	2
<ul> <li>□</li> </ul>			5599(第第)/ U <b>監管理</b> 11991(第1)				
				0   <b>1941</b>			

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。

= 🧦 火!	终端安全管	▲ 些調整 ▲ 生態	ra <b>≜ I</b>		2
☆ 首页					
中 約約管理		性態以當			
<b>各</b> 防护策略		<b>密切保护: 全部 マ 接表:</b> U進本称、単注、変現所本称 Q			
領暗部著			操作		
角帽管理		TEST1 28.826B 关闭 算止 2023-06-19 18:02:01 admin -	编辑 启用武码 取消日	EE.	
16/678					
终端动态认证		取响注册 ×			
田 漏洞修复		() 山倉倉(): 15571			
-					
10 中心開閉					
		图 同时清除し盘数据内容			
		<b>6</b> (2) R0(9)			
E BALLER					
					•
		其1金	15 🚆	Ø - 1	20

## 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。

🔊 火绒终端安全管理系	<u> </u>	添加终端			×
▲ 前页	防护策略 > 终端动态认证		0	0	
	<b>凑加</b> 移输 修用 瓜用		请选择目标终端	应用范围	
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	広用范頼・金幣 ∨ 終爆分組・金幣分組 ∨ 接受・終送会後 D 分組 M	请选择目标终端			
策略部署	an and a final second and a second and a second and a second and a second and	分组名称 Q	终端状态:所有终端 > 约	冬端类型:全部终端类型 > 搜索:	經銷名称、本地IP、 N Q
	● 編号 ◆ 终端名称 ◆ 终端分组 ◆	全部分组(1) 全部展开	当前分组已选中1条		仅展示已勾选终端
		未分组终端 (1)	✓ 终端各称	♦ 终端分组 本地IP	♦ MAC地地
黑名单			🗹 🚦 本机	未分组终端 ::1	00-0C-29-8E-5
终端动态认证					
			W. 5		
			共1张	20號/页 ~ 1< <	1 /共1页 > >>
	#0.6	井洪山 1 冬			下一步。即游
📚 正版授权 📃	火り家	FRANT 1 St			ACH

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

閷 火绒終端安	全管理系	统 1/20160	添加终端	×
合首页		防护策略 > 终端动态认证	••	
		<b>法加</b> 移称 停用 扁用	请选择目标终端 应用范围	
罟 防护策略		应用范围:全部 / 终端分组:全部分组 / 搜索:终端谷积、卫、分组、	请设置应用范围	
策略部署			远程登录时启用	
策略管理			▼ 远楼盘面连接登录时要求输入动态□ 令。	
信任文件			本地登录时启用	
開谷甲			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,如撤议、PDV码等。	
终端动态认证				
<ul> <li>通詞修复</li> </ul>				
资产管理				
图 中心管理				
日 事件日志				
♥ 正版授权		共0象	上一步 朝途 取	び消

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

99 / 261

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。

<i> []</i> 火绒終端安	全管理系统	充 V2.0.16.0										搜索导	钪、模	块名称	۹	11	⊛	4 <mark>2</mark> (	🤁 admin 🗸
<b>⋒</b> 省页		防护策略 > 终端动态认证				6		6											
	~	添加 移除				-	✓ 操作成功												
S 防护策略 策略部署	^	应用范围: 全部	∨ 终端分组: 全部	/组 ∨ 搜索	: 终端名称、IP、分	湘. MAC	地址Q												
策略管理		编号	🔷 终端名	称 🔶	终端分组	\$	本地IP		¢   3	通信IP	•	MAC地址	\$	应用范围		\$	操作		
信任文件		火绒安全终端1	本机		未分组终端		::1			::1		00-0C-29-8E-59-31		远程登录			动态口令	编辑	1514
黑名单																			
U盘管理																			
终端动态认证																			
③ 漏洞修复	~																		
资 资产管理	~																		
中心管理	~																		
🛱 事件日志	~																		
🔁 管理工具																			
🗢 正版授权	≡	共1条										20	条/页	~	< < [	1 >	н	1	/共1页

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。

🛷 火绒终端安全管理系	系统 V2.0.16.0				Q 11 🔿 🦨 🧛 admin 🗸
▲ 普页	防护策略 > 终端动态认证				
■ 終端管理 ∨	<b>添加</b> 移除 停用 启用				
<b>宮防护策略 へ</b> ^{策略部署}	应用范围: 全部 💛 终端分组: 全部分组	接索: 终端名称、IP、分組、MAC地址 Q			
策略管理	▲ 約	◆ 动态口令二维码	× ♦ MAC#	創止 ◆ 应用范围	◆ 操作
信任文件	火城安全终端1 本机		00-0C-3	29-8E-59-31 远程登录	动态口令编辑移除
黑名单		42-81.			
U盘管理					
终端动态认证					
<ul> <li>(2) 漏洞修复</li> <li>(2) 漏洞修复</li> </ul>					
⑦ 资产管理 >					
		Elektron State 200675			
		重新生成			
田 管理工具		(注: 重新生成可刷新动态口令二维码, 旧的二维码将自动失	530)		
	共1条			20条/页 🗸 🔣	〈 1 〉 》 1 /共1页

# 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。

- 20	火绒终端安全	管理系	55 V20.15.0					ർ" 👌 🧛	admin 🗸
			运用地址 / <b>防收换数</b> 算						
			99220 SRITE CODIES						
à			「経緯状态: 所有修調 ✓ 授満分祖: 全部分祖 ✓ 提索: 総論包称, IP、分祖, MAC地址 Q					自导出 日前往意	酒策略
			📴 缩碱名称 🗢 缩碱分组 🗢 本地IP 🔶 通信IP 💠	MAC地址 \$	高危漏洞补丁	功能漏洞补丁 🗘	不建议安装补丁	已忽略补丁	¢
8			☑ □ DESKTOP-TESCS 未分组修論 192.168.3 温洞修复	×	4				
0	贏洞修复		即将对所选终端下发漏洞修复任务,请近	6择修复范围:					
1			○ 修复高危漏洞						
1			○ 修复所有漏洞						
~			○ 修复指定补丁						
Φ	677官理 675817		种丁编号之间以为分辐。如KB100000	KB2000000					
2			· · · · · · · · · · · · · · · · · · ·	取得					
0									
ġ									
8									
-	正版接权		共1条					× 1	

#### 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。

-83	火绒终端安	全管理系	统 V2.0.15.0								按索导航、模块	KS称 Q	າເ ຄໍ 🖧 (	🧕 admin 🗸
			贏詞修复 / 按终講查看											
			Common common		已忽略终端					×				
			[存复篇][]] 即略终调	Elänäisyä				* <b>=</b>		With Carlo and				
			终端状态:所有终端	⊻ 终端分组:	A PROBLEM	848, XMM749A125	22030021340095350007	P92.		-			@74 <b>0</b>	航往查看策略
			2 终端名称	◆ 經濟分組	2 終端	名称 (TOD T65C507	◆ 终端分组 主公的终端	÷	本地IP	\$	功能漏洞补丁	本建议安装补丁		٥
56					UESI	(101-1030357	ACC HERITAGE		192.100.5.145					
0	漏洞修复													
~														
Φ	治产登记													
8														
					共1条					< 1 >				
			共0条											

#### 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;

🧦 火绒终端安全	管理系	统 V2.0.15.0		接卖母航,提块名称 Q. 11 6 🧔 admin 🗸
NORT		贏洞條复 / 按终端查看		
文件分发				
计划任务		修复黨用 加险终期 已初始终期	高危漏洞补丁-DESKTOP-T6SC597 ×	
任务管理			以下灑洞可能会被病毒利用,危害你的电脑。	
终跌发现		段調功心: 所有段調 · 段請方祖:	✓ 补丁编号 ◆ 补丁描述 ◆ 补丁描述 ◆ 发布时间 ◆	(1) 行出 □ 用約至豐有來助
设备管理		● 终端名称 \$ 终端分射	KB4509094 現已确认 Microsoft 高危漏洞补丁 2019-07-08	功能漏同补丁 🗘 不建议安装补丁 🗘 已忽略补丁 🗘
富 防护策略		□ □ DESKTOP-T6SCS 未分包的	Disconfision     P9995662500566645666     P9995662500566645566     P9995662500566645566     P9995662500566645566     P9995662500566645566     P9995662500566445566     P9995662500566     P9995662500566     P9995662500566     P99956625005     P99956625005     P9995662500     P999566250     P9995662500     P999566250     P999566250     P999566250     P999566250     P999566250     P999566250     P9995662     P9995662     P9995662     P999566     P999566     P999566     P999566     P999566     P999566     P999566     P999566     P99956     P99956     P99956     P99956     P9995     P99956     P99956     P999     P99956     P999     P999     P999     P999     P999     P99956     P999     P99     P999     P99     P99     P99     P99     P99	0 0 0
◎ 漏洞修复				
按總辦查看				
按补丁直看				
补丁文件管理				
资产管理     资产管理				
资产登记				
软件管理				
系统管理				
硬件管理				
图 中心管理				
账号管理				
多级中心			+14	
数据备份			大「家 」 【 】 /	
中心迁移				
IERERER	Ξ	共1条		

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。

🎝 火绒终端安全管理系	统 V20.150	擦索导航、標块名称 Q 11 の 👶 😜 admin 🗸
氨亞管理	※同修复 / 按补丁查看	
文件分发		
计划任务	修复漏洞 忽略补丁 已忽略补丁	
任务管理	补丁类型: 全部 ∨ 搜索: KB 歯給入补丁端号 Q	自要出
终端发现		
		▼ 次(htr)日) ▼ 木修复珍調 ▼
高防护策略へ	KK45U9094 现已编队, MICTOSOTT \$X(中/=前十件学生可能完示 向因编词种)	2019-07-08
38,853,03489		
信任文件		
U盘管理		
终端动态认证		
② 漏洞修复 ^		
按终端直看		
按补丁查看		
补丁文件管理		
⑦ 资产管理 ^		
资产登记		
软件管理		
系統管理		
硬件管理		激活 Windows
🗢 正版授权 🛛 🗮	共1条	T

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。

	火绒終端安全	全管理系统	充 V2.0.15.0									搜索导航、模块名称	Q 11	୍ଦ୍ର 👌	🧿 admin 🗸
			温洞修复 / 按补丁查看												
			修复雇用 忽略补丁 已忽略补丁	已忽日	8补丁						×				
			补丁类型: 全部 ∨ 搜索: KB	以下判	丁已被忽略,火绒将	所再为您	修复这些补丁。			1	取消忽略				
			11 非丁编号		补丁编号	٥	补丁描述 ♦	补丁类型	\$ 23	術时间	•	\$	未修复终端		•
18		~			KB4509094		现已确认 Microsoft	高危漏洞补丁	20	019-07-08					
											_				
0	福河修复	~													
¢		^													
											100				
				共19	t.					<u> </u>					
		Ξ	共0余												

## 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。

🛷 火绒终端安全管理	系统 V2.0.15.0			搜索导航、模块名称	० १। 🔿 👶 🤤 admin ~
标壶管理 文件分发	温洞修复 / 补丁文件管理				
计划任务	000++-T				
终续发现	最后请求时间: 全部时间 - 全部时间	目 <b>搜索</b> : 请输入文件名称	۹		
设备管理	文件创建时间	文件名称	◆ 大小	最后请求时间	◆ 操作
器防护策略 ^					
策略部署					
策略管理					
信任文件					
U虚管理					
位终端声音					
按补丁查看			智无相关数据		
补丁文件管理					
资 资产管理 へ					
治产登记					
软件管理					
系统管理					
硬件管理					激活 Windows
	共0条				转到"设置"以激活 Windows。1

# 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。

k 🔇	(绒终端安全	管理系	统 V2.0.1										搜究	8导航、模块名称					<mark>(</mark> ) a	idmin 🗸
<u>ا ا</u>			资产管理	1 / 资产登记																
	常管理	~																		
富防	户策略	~	ž	资产登记管理	登记信	言息管理														
o #	同修复	~	重新	f登记 编辑信息	登记设	置														
(Ý) 86	∽管理	^			_															
资	*登记		终端分	分组: 全部分组	~ 3	紀状态: 全部	<b>搜索</b> : 终端名称、	IP, 🛠	附组、MAC地址 Q								(±	导入值	导出	圓检索
软	4管理			终端名称	۰.	终端分组	\$ 本地IP	¢	通信IP	\$ MAC地址	¢	最新登记时间	¢	登记状态	¢	使用人*				\$
л.	充管理			DESKTOP-T6SC597		未分组终端	192.168.3.143		192.168.3.143	00-50-56-9B-3A-B8	3	-		未登记						
硬	牛管理			本机		产品组	192.168.5.24		192.168.5.24	00-0C-29-17-A1-39	9			未登记						
圖 中	)管理	^																		
账	号管理																			
\$ ⁵	及中心																			
数	居备份																			
<b>P</b> (	心迁移																			
<b>P</b>	心设置																			
はず		~																		
±	聖工具																			
																激化于	Wind	ows		
			共 2 条	R.												·63.10 转到"设	置"以清	的话 Wind	ows 1	
🧇 IB	版授权	Ξ																		<b>,</b> (1997)

(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。

<i>.</i>	火绒终端安	全管理系	统 V2.0.1	15.0												按索	导航,模块名称	٩	11	ം 👌	adm	nin 🗸
			资产管理	1 / 资产登记		_											_					
富防			-	的产登记管理	登记	信息管理																
© #	69999 英 萨管理				512																	
			56.947	99日: 王部759日 终端名称	•	2004/00: 王副 终端分组	¢	·····································	Lagendaria, in.	建信IP		¢	MAC地址	÷	最新登记时间	¢	登记状态	¢	使用人*	田守人日	19900 0813	\$
				DESKTOP-T6SC59		未分组终端		192.16	创建任务				×	18			未登记					
						/ 009		132.10	将对所选终端	下发重新登记( 8月元	任务,终端	登记會口	将:				ALLO					
									□ 不显示已	登记内容												
												确定	取消									
# #																						
			共24	R																		

(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。

🧦 火绒终端	安全管理系	统 V2.0.15.0							搜索导航,模块名称	Q 11	ം 🐉	🥘 admin 🗸
白首页		资产管理 / 资产登记										
😡 终端管理												
富 防护策略		海产登记管理	登记信息管理									
③ 漏洞修复		重新登记 编辑信母	發记设置									
⑦ 资产管理												
Site 19		终端分组: 全部分组	◇ 登记状态: 全部	✓ 搜索: 资档:							自导入 值	身出 昆检索
软件管理		终端名称	♦ 终端分组	◆ 本地IP	≜ ≔raiD	▲ M∆CHbHi-	¢ #	新登记时间	✿ 登记状态	\$ 使用人 •		•
系統管理		DESKTOP-T6SC597	未分组终端	192.16	资产登记信息	×	- 81		未登记			
硬件管理		二 本机	产品组	192.16	_	_	19 -		未登记			
圖 中心管理				+1								
账号管理				LUN IN	IAC地址作为索引, 曹操控制中心	》上对应MAC地址的终端的						
多级中心					登记信息)							
数据备份												
中心迁移						<b>确定</b> 取消						
中心设置												
<b>甘</b> 事件日志												
🤝 正版接段		共2条										

(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。
  - 冬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。

- 20	火绒终端安全	管理系									e a	dmin 🗸
			资产管理 / 资产登记 资产登记管理	登记信息管理								
Ø	资产管理 资产登记		终端分组:全部分组	<ul> <li>✓C023</li> <li>✓ 登记状态: 全部</li> </ul>	资产登记设置	<				自导入	□ 号出	圓检索
			■ 控験名称 型 DESKTOP-T6SC59 ○ 本利	・         終端分祖           7         未分單跨碼           产品相	<ul> <li>一 开始转换交换的型記</li> <li>品用后,传统会探问需要将写望记信最后;可执行会深;静软交深符自动测过此步像。</li> <li>□ 开启线势均量記</li> <li>点用后,包记信息中自动增加终端分组选择话,登记后将自动同步到终线分组。</li> <li>□ 方面用户自动营记</li> <li>品用后,终端用户可以通过"转换银记"填写登记信息,用户线交信息后将自动同步到的小数记管</li> <li>二 转换重新上段资产信息在线转转线: 30 天</li> <li>点用后,当终端表线的无数为点型无数时,低端再以压接中心,将会在终端喷出该缺登记页面,提 能够满用户登记,用户线交信局后将自动同步到的产型记管语。</li> </ul>	E E	9(ii)	\$ 登记状态 未登记 未登记	\$ 使用人* - -			\$
Ē	管理工具		共2条									

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。

<i>[]</i> 火绒約	《端安全管理系	<b>5统 V2.0.15.0</b>					搜索导航、模块名称	a (1)	ം 👌	🤗 admin 🗸
白首页		资产管理 / 资产登记								
终端管理     长端管理     朱端管理     朱端管理     朱端管理     朱端管理     朱端管理     朱端管理     朱端管理     朱端管理     朱统管理     朱统计和     朱统理		资产登记管理	登记信息管理							
④ 編詞#3 (1) 資产費	ι ~ 1 ^	新着一副除	排序							
arei		是否必填: 全部	◇ 输入类型: 全部	送款: 请输入登记信息	Q					
软件管理	Ę	登记信息		是否必填		输入类型			操作	
系统管理	E	() 终端名称		必填頂		文本输入框			设置	
硬件管理	Ē	使用人		必填项		文本输入框			编组	图除
<b>四</b> 中心管理	۰ I									
账号管理	E									
多级中心										
数据备位										
中心迁移										
中心设置										
日 事件日志										
								激活 Wir	ndows	
		共2条						1973) U.H. (		

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。

- <b>(</b> )	、绒终端安全管	理系统 V20.15.0		接索导航、模块名称 Q 11 命 🖧 🌅 admin イ
@ #		资产管理 / 资产登记		
111 111 111 111 1111 1111 11111 1111111		资产型记管理 型记语息管理		
© # ന #	洞修复 、	Bit		
		是否必須: 全部 🗸 輸入無型: 全部 🗸 援索:		
53			第二人共型 登记信息 ×	操作
		<ul> <li>         使用人         </li> </ul>	终端名称登记 文本输入框	》(唐 ) 编辑 删除
@ +	心管理 /		是否开启: 开启 O 关闭 注: 启用后, 登记信息中目动增加终端名称约登记信息, 登记后	
70 15			将自动同步为终端的终端名称。	
B			引导提示信息设置:例:请按照以下预试输入:A分如-张二	
ф ф			1039	
₩ 5				
⊕ e				
🧇 II	版接段	共2条		

【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。

- <b>(</b> )	V 绒终端安全管理	系统 V2.0.15.0			👌 🌏 admin 🗸
6 #		资产管理 / <b>资产登记</b>			
當防		资产登记管理 登记信息管理			
0 #		新書目除 非序			
9 s 8		是否必填: 全部 🛛 输入类型: 全部			
\$7		· 登记信息	新播登记信息	输入类型	操作
系		●	*登记信息: 不可超过10个字 (	文本输入框 /10 文本输入框	设置 编辑 删除
9 +			是否必填: 📀 必填頂 📄 非必填頂		
94 5			输入类型: 🔿 文本输入權 🔷 数字输入權 🔷 下拉列表		
Ð			引导提示信息设置: 例: 請按照以下指式输入: A分相-张三 0/3		
#					
+- +:					
÷					
II 🧇		共2条			

# 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。

-	火绒终端安全	管理系		卸载软件	×
			资产管理 / 软件管理	o○ 选择目标线端 卸载配置	
8			软件概况 卸载任务管理 软件变更日志	请选择目标终端	
0			终端笑型: Windows > 统计: 按软件 > 搜索: 软件名称、发布者	分组合称         Q         终端状态:         所有终端         >         终端关型:         全部终端关型         搜索:         终端关	B称、本地IP、N Q
Ø	资产管理		<ul> <li>□ 軟件各称</li></ul>	全部分组(2) 全部展开 当前分组已选中 2 条	仅展示已勾选终端
			Microsoft Edge Microsoft Corporation	未分組経講(1) ✓ 终端名称 ◆ 终端分组 本地P ◆ MJ	AC地址
			Microsoft Edge WebView2 Runtime Microsoft Corporation	产品组(1)     ビ      載本机     产品组     192.168.5.24     00	-0C-29-17-A1
			Microsoft OneDrive Microsoft Corporation	・ 調试组(0) 図 III DESKTOP-T6 未分组修満 192.168.3.143 000	-50-56-9B-3A
<i>.</i> @.,			Microsoft Update Health Tools Microsoft Corporation		
			Microsoft Visual C++ 2008 Redistributable - x64 Microsoft Corporation		
;			Microsoft Visual C++ 2008 Redistributable - x86 Microsoft Corporation		
			Microsoft Visual C++ 2010 x64 Redistributable Microsoft Corporation		
			Microsoft Visual C++ 2010 x86 Redistributable Microsoft Corporation		
			Microsoft Visual C++ 2015-2019 Redistributable Microsoft Corporation		
	事件日志		Microsoft Visual C++ 2015-2019 Redistributable Microsoft Corporation		
÷	管理工具				
				共2条	< 1 >
				激活 Windo	WS
			共 20 条	共造中 2 条 30 ED 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16 20 16	5—步 取消

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。

🧦 火绒终的	端安全管理系	统 V2.0.15.0								ł	现索导航、模块名称	a 11	ം 🕹 🧲	admin 🗸
白首页		资产管理 / 软件管理												
🝚 终端管理				卸载软件					>	<				
富 防护策略		软件微光	卸载任务管理											
◎ 漏洞修复		终端类型: Windows	◇ 统计: 按线	终端名称:本机	總備	常分组: 产品组			卸載					自导出
⑦ 资产管理		终端名称		- 软件名称	\$	发布者	◆ 版本号	¢	操作	\$	MAC地址	¢	软件安装总数	\$
资产登记		DESKTOP-T6SC597		Microsoft	dge	Microsoft Corporation	131.0.2903.9	1	卸载		00-50-56-9B-3A-B8			
软件管理		本机		Microsoft	dge WebVi	Microsoft Corporation	130.0.2849.8	0	卸载		00-0C-29-17-A1-39		19	
系统管理				Microsoft	dge WebVi	Microsoft Corporation	131.0.2903.9	1	卸载					
硬件管理				Microsoft	DneDrive	Microsoft Corporation	24.211.1020	0001	印载					
🖾 中心管理				Microsoft	Jpdate Heal	Microsoft Corporation	3.74.0.0		卸载					
账号管理				Microsoft	/isual C++ 2	Microsoft Corporation	10.0.30319		卸载					
多级中心				Microsoft	/isual C++ 2	Microsoft Corporation	10.0.40219		卸載					
数据备份				Microsoft	/isual C++ 2	Microsoft Corporation	14.28.29913	0	卸载					
中心迁移				Microsoft	/isual C++ 2	Microsoft Corporation	14.28.29913	0	卸载					
中心设置				Mozilla Fir	efox (x86 zh	Mozilla	132.0.2		卸载					
日 事件日志														
				# 19 &			10\$/7	5 v (s						
										· .				
👳 正版授权		共2条												

#### 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)。

لا 🏷	<b>火绒终端安全管理</b>	L系统 V2.0.15.0					搜索导航、模块名称 (	11 6° 🗳  admin 🗸
<b>6</b> ≅		资产管理 / 软件管理						
	著管理  く	Market BOD	or Data J-C for any TD					
富昉	护策略 ~	4人1十亿0元	104801E361838	秋件受更日志				
© #	洞修复 ~	任务创建时间	全部时间 ~ 全部时间	正在分发 > 投索: 软件名称	Q			自导出 圆检索
() a		卸载软件	♦ 卸载方式	◆ 管理员	任务创建时间	任务到期时间	任务状态	◆ 操作
50 E	「立し	Mozilla Firefox (x86 a	zh-CN) 提示卸载	admin	2024-11-19 14:18:55	2024-11-20 14:	18:55 正在分发	详情 终止
系	統管理							
硬	件管理							
<b>@</b> #	心管理へ							
账	号管理							
Ş	级中心							
数	据备份							
ф	心迁移							
н т								
# ۲. و	140 V							
	#1 <del>%</del>							
								激活 Windows 转到"设置"以激活 Windows
II 🤝	版授权 📃	共1余						

# 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

🧦 火绒络	《端安全管理》	系统 V2.0.15.0							(	搜索导航、模块名称	Q 11 @	👌 🧛 admin 🗸
合颜		资产管理 / 软件管理										
🖳 终端管理												
🖀 防护策略		软件概况	卸载任务管理	软件变更日志								
② 漏洞修复		态 <b>田</b> 举型 · 全部	~ 空田时间,	2024-11-13.00:00:00	~ 2024-11-19 2	2-50-50 m 18-18 (18-18	名称 IP 会组 MACt	ntti 0			の見出	当自由之利 同始素
③ 资产管理	• •	XXXE. IP	3636431431	2024 11 13 00:00:00	2024 11 10 2.	5.55.55 E 18.4. See					040	LE BALLON EL 19204
资产登记		変更时间 ♦	変更类型 ♦	终端名称	终端分组	◆ 本地IP ◆	通信IP 💠	MAC地址	终端类型	<ul> <li>软件名称</li> </ul>	发布者	软件版本 🔶
软件管理		2024-11-18 15:	安装	DESKTOP-T6SC	未分组终端	192.168.3.143	192.168.3.143	00-50-56-9B-3	Windows	Microsoft One	Microsoft Corp	21.220.1024.00
系统管理		2024-11-18 15:	卸载	DESKTOP-T6SC	未分组终端	192.168.3.143	192.168.3.143	00-50-56-9B-3	Windows	Microsoft One	Microsoft Corp	21.073.0411.00
硬件管理		2024-11-18 15:	安装	DESKTOP-T6SC	未分组终端	192.168.3.143	192.168.3.143	00-50-56-9B-3	Windows	Microsoft One	Microsoft Corp	24.211.1020.00
🖾 中心管理		2024-11-18 15:	卸載	DESKTOP-T6SC	未分组终端	192.168.3.143	192.168.3.143	00-50-56-9B-3	Windows	Microsoft One	Microsoft Corp	21.220.1024.00
		2024-11-18 15:	安装	DESKTOP-T6SC	未分组终端	192.168.3.143	192.168.3.143	00-50-56-9B-3	Windows	Microsoft Edge	Microsoft Corp	131.0.2903.51
多级中心		2024-11-18 15:	安装	DESKTOP-T6SC	未分组终端	192.168.3.143	192.168.3.143	00-50-56-9B-3	Windows	火绒终端安全管	北京火城网络科	2.0
数据备份		2024-11-19 09:	安装	本机	产品组	192.168.5.24	192.168.5.24	00-0C-29-17-A	Windows	Microsoft Edge	Microsoft Corp	131.0.2903.51
中心迁移		2024-11-19 09:	安装	本机	产品组	192.168.5.24	192.168.5.24	00-0C-29-17-A	Windows	Microsoft One	Microsoft Corp	24.211.1020.00
中心设置		2024-11-19 09:	安装	本机	产品组	192.168.5.24	192.168.5.24	00-0C-29-17-A	Windows	Python 3.10.4 (	Python Softwar	3.10.4150.0
🛱 事件日志		2024-11-18 16:	安装	本机	产品组	192.168.5.24	192.168.5.24	00-0C-29-17-A	Windows	Mozilla Firefox	Mozilla	132.0.2
с, «піс	1											
											激活 Windo	WS
😔 正版授权		共 16 条									10条/页	Windows,

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。

#### 北京火绒网络科技有限公司

<b>.</b>	火绒终端安全	全管理系	统 V2.0.15.0					(	搜索导航、模块名称 C	a. 11. 🔊 🗳 읒 admin ~
6	鈵		资产管理 / 系统管理							
	《端管理									
<b>2</b> 1	防护策略		系统统计	系統占比						
© #	制修复		安装日期: 全部时间 ~ 全	部时间 間 修繕分组:	全部分组 > 複数	<b>索:</b> 操作系统名称、终端名称、	2			南导出 连自定义列
(†) 1	的产管理									
ž	<del>这一型</del> 记		操作系统名称  ●	安装日期	● 激活状态	<ul> <li>终端名标</li> </ul>	♥ 终端分组	◆ 本地IP	♥ 通信IP	MACHELE
\$	次件管理		Microsoft Windows 10	2018-05-14 13:15:27	未御店	DESKTOP-16SC597	未分组终端	192.168.3.143	192.168.3.143	00-50-56-98-3A-88
3	6统管理		MICrosoft Windows TU	2022-04-27 17:24:43	日初店	~彻	P*669E	192.108.5.24	192.108.5.24	00-00-29-17-A1-39
a	更件管理									
<b>8</b> 4	中心管理									
Ŗ	长号管理									
\$	≶级中心									
ž	<b>火据省份</b>									
4	中心迁移									
4	中心设置									
वि व	时日志									
÷	會理工具									
										激活 Windows
🤝 I	E版授权		共2条							報到"设置"以激活 Windows 1

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。

🕖 火绒終端	安全管理系	统 V2.0.15.0	搬売時紙、橋块谷称 Q. 11. 崎 💐 💭 admin	~
<b>向</b> 首页		迎产管理 / 系统管理		
😡 终端管理				
富 防护策略		系统统计系统合比		
◎ 漏洞修复			自导出	
③ 资产管理				
资产登记				
软件管理				
系統管理				
硬件管理				
國 中心管理				
账号管理				
多级中心				
数据备份		Microsoft Windows 10 企业版   1 (50%)	8W	
中心迁移		Microsoft Windows 10 专业版   1 (50%)	2	
中心设置				
日 事件日志				
管理工具				
			激活 Windows exercise 2000年2000年2000年2000年2000年2000年2000年200	
❤ 正版授权			4920 BCEL OADIS YHINOTS,	

# 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。

<i>🌔</i> 火绒终端	安全管理系	统 V2.0.15.0									搜索导	航、模块名称	٩	I @	• 🕹	🤗 admin 🗸
▲ 首页		资产管理 / 硬件管理	1													
🝚 终端管理																
富 防护策略		硬件统计	硬作	牛变更历史												
◎ 漏洞修复		终端分组: 全部分	组 ~	<b>搜索</b> : 终端名称、IP	、MAC地址	Q									自导出	臣 自定义列
资产管理		终端名称 🗘	终端分组	◆ 本地IP ◆	通信IP ♦	MAC地址 🖨	CPU 🗘	内存 🗘	硬盘	硬盘序列号 🔷	硬盘ID 💠	网卡 🗘	显卡	¢ 5	示器	◆ 声卡
资产登记		DESKTOP	未分组终端	192.168.3.1	192.168.3.1	00-50-56-9	Intel(R) Xe	DRAM 4.0GB	VMware Vi	-	{C9304C14	Intel(R) 82	VMware SV	I		麦克风(
软件管理		本机	产品组	192.168.5.24	192.168.5.24	00-0C-29	Intel(R) Cor	DRAM 2.0GB	VMware Vi	VMWare N	{2A8AFBA5	Intel(R) 82	VMware SV	I		Microph
赤地管理																
四 中心管理																
🖨 管理工具																
													激泪	5 Winc	lows	
⇒ 正版授权		共2条											转到"	设置"以	敞活 Wind	« 1

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

=	1	火绒终端安全	管理系统								▲ 终端部署	±	<b>Å</b> 0	1
습			资产管理 / 硬件管理											
	终端管理	•	硬件统计	硬件变更历	诀									
6	防护策略	•	安装时间: 2020-10-24 - 202	0-10-30 終調	<b>1分组</b> : 全部分组	÷	搜索: 终请名称	*	賣資				ŵ	设置
Ð	藏洞修复	*	変更时间	4 / 約3	高称	0 修辞	粉粗	☆ │ 終新IP	0   3	定更硬件	◎   操作			
8	资产管理	<u>.</u>	2020-10-30 18:26:27	Will	N-7F6OBMJRM8M	未分	相终端	=1	(	:PU	谨慎			
	51£*16		2020-10-29 15:41:31	DE	SKTOP-2H7UHHB	未分	相终确	192.168.5.210	3	对存	谨慎			
	软件管理													
	新物田坦													
	中心管理	•												
Ē	事件日志	-												
ē	管理工具													
	🗢 II	版授权	共2条									15	条/页 ~~	1 14

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。

件变更详情		
冬端名称: W を更时间: 2(	/IN-7F6OBMJRM8M 终端分 020-10-30 18:26:27 变更硬	组:未分组终端 进件: CPU
硬件名称	变更前硬件信息	变更后硬件信息
	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
cpu	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
図卡	Intel(R) 82574L 千兆网络连接	Intel(R) 82574L 千兆网络连接
副卡	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。

- 20	火绒终端安全管	管理系	5 <b>44</b> V2.0.15.0	新建账号	×
â			中心管理 / 账号管理	账号类型: O 普通管理员 O 审计员	
			817 E50 528	* 账号: 這能入账号	
@ ()				* 密码: 请输入监钥 Ø	生成强密码
Ø				*确认密码: 请再次输入密码	ø
9	中心管理		admin	下次登录: 💋 强制修改密码	
				联系方式: 请输入手机号	
				<b>御注:</b> 请输入做注	
9					0/512 2
į				* 登录地址限制: 🔾 不限制 💿 IP地址 💿	
tit A				多个PP通过操行进行区分,支持单个IP和IP段	
8	管理工具				0/2000
				影件符容:	
				*邮箱: 请输入邮箱	
				*验证管理员密码: 请输入超级管理员密码	ø
			#1%	激活 Windows 特到"设置"以激活 Windo	WS,
				下一步	取消

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。

- 20	火绒终端安全	管理系			新建账号	×
â			中心管理 / 账号管理		请配置账号的分组权限	
ų					▼ □ 全部分组	
8					□ 未分组终端	
0			<b>关型:全部 水路索: 清</b> 输入管闭品联系		▶ ○ 产品组	
Ø					▶ □ 測试组	
8	中心管理			♥ 紙魚万式 ♥ 輸注	•	
			hr			
ja S						
贷						
⊕						
						MARTINE IN T
						湖沽 WINDOWS 转到"设置"以激活 Windows,
			共2款			上一步 下一步 取消

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。

<i>。</i> 秋纸终端安全管理系	V20.15.0	新建账号	×
▲ 首页 □ 终端管理 ~	中心管理/账号管理	请配置账号的概块权限 ◎ 首页	
富防护策略 >	800 B00 B00 B00 B00 B00 B00 B00 B00 B00	▶ 📮 终端管理	
◎ 漏洞修复 ~	关型: 全部 /	▶ □ 訪茄/預期	
⑦ 资产管理 ∨	○ 账号 ◆ 邮箱 ◆ 联系方式 ◆ 备注 ◆	▶ □ 瀧洞修复	
	🗇 admin	<ul> <li>         · 」</li></ul>	
多级中心		- - - - - - - - - -	
数据备份			
中心迁移			
中心设置			
管理工具			
		激活 Windows	
🗢 iekska 🚍	共2条	area see Loans windows, 上一步	

## 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。

- 43	火绒终端安全	管理系	统 V2.0.1															4	🕽 admin 🗸
G			中心管理	/ 账号管理															
Q			1																
56			31	201	停用	虚用													命设置
0			类型:	全部	~ 搜索:														
Ø				-											Autom UT		489.154		
Ø	中心管理			Jee		■ 2040	-	联系力式	•	· 简注		Ŧ	天卫	•	FORENLIN	÷	11:21		
			10	admin									超极管理员		2024-11-18 13:49:21		原管设置		
				hr									普通管理员		2024-11-19 14:23:41		账号设置		機块权限
				hr1				提示			×		普通管理员		2024-11-19 14:59:52				
								()											
									选中的账号即将	被删除,请您确	角认								
臣								$\cup$											
÷										織定	取消								
			共3旁	R															
			1																

## 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。

🧦 火绒终端	安全管理系	<b>系统 <u>V2.0.15.</u>0</b>	0)						搜索	导航,模块名称	a (1	I 6	<b>8</b> (	👂 admin 🗸
白甸		中心管理 /	账号管理											
😡 终端管理		1												
富 防护策略		- 1723	· · · · · · · · · · · · · · · · · · ·	B ASH										申设置
<ul> <li></li></ul>		类型: 3	全部 🗸 投業											
② 资产管理			<b>K</b> 2	a etas	REAT	A (6)1		261 <b>7</b> 7		0(200+(6)		182.012		
四 中心管理		-	admin	• #0*194	-	T MILL		約約管理局		2024-11-18 13:49:21		NEIOE		
账号管理			br					普通管理用		2024-11-19 14:23:41		BUESIDER		10 10 10 10
多级中心		2	hrl		un=			普通管理局		2024-11-19 14:59:52		NCOW.		101010
数据备份					短示		~							
中心迁移						milita Auto Ada anna - Salta Auto Ada Si I								
中心设置					送中的账号	14符被停用,请恐備认								
<b>甘</b> 事件日志														
🗗 管理工具						inter A								
S IERGRADZ		共3条												

### 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。

- 20	火绒终端安全	全管理系					🔲 🕕 💣 🥵	admin 🗸
G			中心管理 / 账号管理					
<u> </u>								@ (0 #
88								\$ KE
0			关型:全部 / 搜索: 请输入管理员联带	官理员账号设直	×			
8	地で管理		₩-5 <b>\$</b> \$\$¥\$	自动登出设置		\$ 创建时间	● 提作	
	KCOBE		admin -	账号自动登出时间: 120 分钟		2024-11-18 13:49:21	账号设置	
8	多级中心		🗇 hr -			2024-11-19 14:23:41	账号设置 分组权限 4	制建设限
			🗆 hrt -	动态认证设置	查看动态口令操作指南 ————————————————————————————————————	2024-11-19 14:59:52	账号设置 分组权限 长	戰快权限
				开启动态认证				
ġ				◎ 席で豆果治用助点以近 ○				
贷				高能操作认证有效时间: 0 分钟 ⑦				
÷	管理工具							
				定期修改密码设置				
				开启密码更新检查				
				更新周期: 90 天 ⑦				
					取用			
<b></b>	正版授权	=	共3条					

- (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。

-	火绒终端安全	论管理系	34 V2.0.15.0 提索导航、模块各称	a ा। 💣 🛃 🌏 admin 🗸
G			中心管理 / 多級中心	
94 194			与上级中心最近最近时间:未通讯	同配置上级中心
0			中心名称 • 19 • 终端回题 • 在这时地 • 病毒的组 • 系统的组 • 网络的组 • 最近通用时间 • 分配接权 • 状态	\$ 操作F
() ()	資产管理 中心管理		配置上級控制中心	
			· 油線上報控制中心: ①	
			上版控制中心地址: 创: 127.0.0.1	
			部署通口: 例: 6080	
			上級控制中心書明:「請給入密明	
問			●#FIGLENRE#FIGE([BasLak])*/	
Ð			□ 从上版中心获取升级数据①	
			□ 从上版中心获取补丁数据	
-			大部分目的 中国 小田	

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。

🍠 火绒终端	安全管理系	统 V2.0.15.0								搜索导航、模块名称	α	11 କ	🖌 🔮 🧛 admin 🗸
		中心管理 / 多级中心	ŝ										
型 Signed 2 防护策略		与上级中心最近通行	刊时间:未通讯										日配置上级中心
③ 漏洞修复		中心名称	<b>♦</b> IP	\$终端部署	在线终端	◆ 病毒防御	◆ 系统防御	◆ 网络防御	♦ 最近通讯时间 ♦	分配授权 🗘	状态	◆ 操作	
🖗 资产管理		DESKTOP	192.168.3.143	0	0	0	0	0	2024-11-19 15	独立授权	未授权	23	。 编辑授权 删除
四中心管理													
账号管理													
多级中心													
数据备份													
中心迂步													
日 事件日志													
												改活 Wind 回"设置"以達	OWS 然舌 Windows
😔 正版接权		共部署下级中心 1 ·	<b>^</b>										< 1 >

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。

-	火绒终端安	全管理系	统 V2.0.15.0										搜索导航、模	快名称	٩	11	6	e 🗧	) admin 🗸
			中心管理 / 多级中心																
			与上级中心最近通讯时	饷:未通讯														(3 R)	<u>累上</u> 级中心
			中心名称	IP	\$ 终端部署	◆ 在线	SM \$	病毒防御	\$ 系统防	e 🗘	网络防御	截近通讯时问 🗘	分配接权	٠	状态	٥	操作		
			DESKTOP	192.168.3.143	0	0		0	0		0	2024-11-19 15	独立接权		未授权		登录	编辑授权	HRP
	中心管理						编辑授权				×								
							公配运行。	白宗议公配											
							STREET,	LINEXCOME:											
							目定义分配	-											
							window	SEE (MG : U			E .								
							Linux服务器	終端: 0			台								
	#N+CAD BARTE						Linux處面	診察論: 0			台								
							macOS	S終講: 0			台								
									<u>6</u> 24	1	取消								
			共部署下级中心 1 个																

# 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。

<i>《</i> 》 火绒终端:	安全管理系	统 V2.0.15.0								搜索导航、模块名	(新 Q	11 6	· 🦉 🍕	🕽 admin 🗸
		中心管理 / 多级中心												
		-												
富 防护策略		与上级中心最近通讯时	间:未通讯										C7 6	置上级中心
		中心各称 🗘	IP \$	终端部署	在线终期 \$	病毒防御 🗘	系统防御	网络防御 🗘	最近通讯时间 🗘	分配接权	• 状态	¢ 15	ſF	
		DESKTOP	192.168.3.143	0	0	0	0	0	2024-11-19 15	独立接权	已脱离上级	2	录 喻组接权	删除
◎ 中心管理														
					提示			×						
						确定删除下级控制	制中心吗?							
					$\cdot$	下级控制中心将不	再获取来自中心的授权							
							ance in the	274						
		社営業工程中心する												
		米設備で坂中心「个												



# 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。

🧦 火绒终端	安全管理系统	统 V2.0.15.0						搜索导航、模块名称	۹ (	ղ <mark>1</mark> օ՝ գ ⁵	🤗 admin 🗸
白首页		中心管理 / 数据备份									
🚽 终端管理	~										
富 防护策略	~	备份文件 备份1	<u>2</u>								
③ 漏洞修复	~	备份 删除 同步							3	💼 共占 5.2 MB, 同	J用空间 17.2 GB
资产管理     资产管理	~										
◎ 中心管理	^	生成时间: 2024-11-13 ~ 2024-11-1	19 📄 备份类型: 全部	── 备份内容: 全部	5 🗸						自导入
账号管理		□ 备份文件生成时间 ① 🗘	备份完成时间	中心版本	备份类型	备份内容	◆ 大小	◆ 备注		◆ 操作	
多级中心		2024-11-19 15:13:53	2024-11-18 15:50:52	V2.0.15.0	导入备份	配置文件	1.29 MB	u=		● 数据恢复下	载删除
数据备份		2024-11-18 16:02:26	2024-11-18 15:50:52	V2.0.15.0	导入备份	配置文件	1.29 MB			数据恢复 T	載 删除
中心迁移		2024-11-18 15:51:09	2024-11-18 15:50:52	V2.0.15.0	导入备份	配置文件	1.29 MB	-		▲ 数据恢复 T	載 删除
中心设置		2024-11-18 15:50:50	2024-11-18 15:50:52	V2.0.15.0	手动备份	配置文件	1.29 MB	-		● 数据恢复 下	戰 删除
日 事件日志	~										
🖻 管理工具											
									湯y) 转至	古 WINdoWs 『设置 [®] 以激活 Wine	lows
😔 正版授权	≡	共 4 派									

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。

- 20	火绒终端安全	全管理系	统 <u>V2.0.15.0</u>				搜索导航、模块名称	α 11	ି 👌	admin	~
	火債務構会: 首页 能動管理 助学課題 第一中登録 の中心 の の の の の の の を して の の の の の の の の の の の の の の の の の の	全管理系	第一〇世世 / 数据集分         第一〇世世 / 数据集分         第一〇世世 / 数据集分         第一〇世世 / 数据集分         第一〇世世 / 11-13         第日〇世世 / 11-19         第日〇世 / 11-19         第日〇世 / 11-19         第日〇世 / 11-19         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         1111         11111         11111         11111         11111         11111         11111         111111         111111111         1111111111111 </th <th><ul> <li>●新砂类型:金部</li> <li>●数据等位</li> <li>中心版本</li> <li>+11-18 15:50:52</li> <li>+11-18 15:50:52</li> <li>+11-18 15:50:52</li> <li>+11-18 15:50:52</li> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul></th> <th><ul> <li>2 配置文件 ①</li> <li>日志文件</li> <li>全型日志 ○ 単 30 天日志 (包括協会加大)</li> <li>目の環境 (不可超出120个字)</li> <li>記録報句類時, 控句中心特質得像現,</li> <li>配合</li> </ul></th> <th>×</th> <th>(株大名称) (株大名称) ★ 新社 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○&lt;</th> <th>Q 11</th> <th>C C C C C C C C C C C C C C C C C C C</th> <th><ul> <li>admin</li> <li>可用空间 17.2 G</li> <li>(山 寺)</li> <li>(山 寺)</li></ul></th> <th>iB i i i i i i i i i i i i i i i i i i</th>	<ul> <li>●新砂类型:金部</li> <li>●数据等位</li> <li>中心版本</li> <li>+11-18 15:50:52</li> <li>+11-18 15:50:52</li> <li>+11-18 15:50:52</li> <li>+11-18 15:50:52</li> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	<ul> <li>2 配置文件 ①</li> <li>日志文件</li> <li>全型日志 ○ 単 30 天日志 (包括協会加大)</li> <li>目の環境 (不可超出120个字)</li> <li>記録報句類時, 控句中心特質得像現,</li> <li>配合</li> </ul>	×	(株大名称) (株大名称) ★ 新社 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○<	Q 11	C C C C C C C C C C C C C C C C C C C	<ul> <li>admin</li> <li>可用空间 17.2 G</li> <li>(山 寺)</li> <li>(山 寺)</li></ul>	iB i i i i i i i i i i i i i i i i i i
			共5条								

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。

🧦 火绒终端;	安全管理系	统 V2.0.15.0						搜索导航、模块名称	Q 11	୍ଦ୍ର 🖧	🤮 admin 🗸
白首页		中心管理 / 数据备份									
😡 终端管理											
〓 防护策略		备份文件 备份计	9 <u>m</u>								
◎ 漏洞修复		<b>备份</b> 副除 同步							<b>#</b>	長占 6.5 MB, 司	「用空间 17.2 GB
🕜 资产管理											
🖾 中心管理		生成时间: 2024-11-13 ~ 2024-11-1	9 🖹 备份类型: 全部	「「「「」」「「」」「「」」「」」「「」」「」」「」」「」」「」」「」」「」」	3容: 全部 🗸						由导入
账号管理		备份文件生成时间 ① 🗘	备份完成时间	◆ 中心版本	♦ 备份类型	备份内容	◆ 大小	<b>\$</b> 备注	\$	操作	
多级中心		2024-11-19 15:14:17	2024-11-18 15:50:52	V2 提示		×	1.29 MB		2	数据恢复 下	截 删除
数据备份		2024-11-19 15:13:53	2024-11-18 15:50:52	V2			1.29 MB		2	数据恢复 下	载 删除
中心迁移		2024-11-18 16:02:26	2024-11-18 15:50:52	V2	确定删除所选的备份文件吗?		1.29 MB		<u>e</u>	数据恢复 下	载 删除
中心设置		2024-11-18 15:51:09	2024-11-18 15:50:52	vz 💽	删除的备份文件将无法找回		1.29 MB		<u>e</u>	数据恢复 下	载 删除
日 事件日志		2024-11-18 15:50:50	2024-11-18 15:50:52	V2	确定	取消	1.29 MB		2	数据恢复 下	载 删除
🗄 管理工具											
		++ [ 7									
🗇 正版授权		共う京									

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。

-	火绒终端安全	管理系	统 V2.0.15.0									admin 🕚	
G			中心管理 / 数据备份										
9			备份文件 备份	125									
0												790m/2017.0.00	
Ø										*	는데 0.5 MID, 다	/H19200 17.2 00	
8	中心管理		生成时间: 2024-11-13 ~ 2024-11-	19 🖹 备份类型: 全部	✓ 备份内?	容: 全部 🗸			and a second			自导入	
			备份文件生成时间 ① 🗘	备份完成时间 2024-11-18 15:50:52	中心版本 V2	♦ 备份类型	◆ 备份内容	大小 1.29 MB	◆ 借注	\$	操作数据恢复门	载 删除	
			2024-11-19 15:13:53	2024-11-18 15:50:52	数据恢复 V2		×	1.29 MB			数据恢复	载删除	
			2024-11-18 16:02:26	2024-11-18 15:50:52	V2 (5)	确定要立即恢复中心数	据吗?	1.29 MB		2	数据恢复	載 删除	
1			2024-11-18 15:51:09	2024-11-18 15:50:52	V2	\$000X2000052200704		1.29 MB		2	数据恢复	·戰 删除	
Ē			2024-11-18 15:50:50	2024-11-16 15:50:52	VZ		<b>設備</b> 取消	1.29 MB		<u> </u>	<u> </u>	19X 2010	
-			共5条										

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。

🛷 火绒终端安全管理系统	휹 V2.0.15.0	搜索导航、模块名称	० १। 🔿 🞝 🌏 admin 🗸
<ul> <li>○ 首页</li> <li>○ 终端管理</li> <li>&gt; </li> <li>S 防护策略</li> <li>&gt; </li> <li>○ 漏洞般复</li> <li>&gt; </li> </ul>	中心管理 / 數請論份		🚔 共占 6.5 MB,可用空间 17.2 G8
① 近产管理     、       〇 近小管理     へ       単心管理     へ       単心目表     ・       中心記器     ・       一     一       ●     単中日志       ○     管理工具	生成期间: 202411-13 - 202411-19 ● 备份提案: 全部 ● 备份方件同步 × ● 命約文件同步 × ● 命約文件同步 × ● の方件同步 × ● の方中 ● の方 ● の方 ● の方中 ● の方 ● のう ● のう ● のう ● のう ● のう ● のう ● のう ● のう ● のう ● の方 ● のう ● の方 ● のう ● の方 ● のう ● の方 ● のう ● のう ● のう ● のう ● のう ● のう ● のう ● のう	<ul> <li>第注</li> <li>-</li> <li>-</li> <li>-</li> <li>-</li> <li>-</li> </ul>	日本     日本
S IEKISK E	—————————————————————————————————————		

#### 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。

🧦 火蛾	冬端安全管理系	<b>按杰导航 模块名称</b>	०. १। 🔿 🖧 😜 admin 🗸
白前		中心證理 / 数据备份	
🛄 终端管理	e ~		
富 防护策	ii v	备份文件 备份设置	
③ 漏洞修約	ę v	文件滿理	
😚 资产管理	e ~		
图 中心管理	e ~		
账号管理	æ	自动衡份	
多级中国		开度自动差份	
数据备付		餐的内容: ② 和王文件 ① □ 日志文件	
中心迁和	its	<ul> <li>金銀田志</li> <li>前</li> <li>30</li> <li>天田志</li> <li>0</li> </ul>	
中心设计	Æ	自动备份周期: ① 标子备份 每 1 天	
日 事件日詞	5 V		
 ⇔ ⊛⊞⊺1	8	◎ 該局面份 周日 周一 周三 周四 周五 周六	
		44 1 周	
		② 捡月餐份 月 滴洗样 問	
		天前時季	
		774ae101: 00:00 🕓	
		自动条份文件回步: 自动备份成功后将备份文件回步至其他服务器	
		周海共等	
		<b>路径:</b> 网络共享路径	潮汗 Windows
			转到"设置"以激活 Windows。
😔 正版接机		0677	

# 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。

												-
- 400	火绒终端安全	管理系	统 V2.0.15.0								ଳ <b>ି</b> ଜିଂ (	🤮 admin 🗸
@ #			中心管理 / 中心迁移									
Q #			-									
富 17			本机地址或编口变更			In Marine Marine 1						
0 1			南语们配置上码(并闻积率-Arfel	出序		·丹),重新明定H100现名,更	in and in a second s					
Ø 8			迁移到其他新的机器									
@ 4	中心管理		<b>王恭</b> ④ 为防止数据丢失	,强烈建议迁移前先数据备份然后在	新中心机器上进行数据	副恢复						
用			新控制中心地址	◆ 终端部署端口	迁移中心	Admittati di Ami		×	◆ 迁移进度	¢	操作	
8					20010							
Ę					新控制中心地址:	例: 127.0.0.1		_				
9					部署端口:	94: 6080						
9					需要迁移的分组:	请选择分组		~				
tig a						副除汗死市市这种						
윤 🗉						00010-F17_65-100-4/199(94)		_				
							कोइट प्राय	消				
_												
<b>•</b> 1			共0条									
V 11			2									

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

🔊 火绒终端的	安全管理系	统 <u>V2.0.16.0</u>						(	搜索导航、模块名称	٩	11 🔿	🧟 🧛 admin 🗸
白首页		中心管理 > 中心设置										
💷 终端管理	~	终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
富 防护策略	~	终端密码保护 ① 临时密码	阿在终端详情生成									
◎ 漏洞修复	~	启用管理员密码保护										
资产管理     资产管理	~	密码:	<b>%</b> 随机生成									
◎ 中心管理	^	自用防止终端卸载密码()	2P									
账号管理		密码:	<b>Ø</b> 随机生成									
多级中心												
数据备份		离线终端管理										
中心迁移	_	終端高线 30	天后, 删除约	F3論								
中心设置												
□ 事件日志	~	管理页信息 当客户端出现问题需要求助	曹理员时,会在终端显示以	「下联系信息								
🖻 管理工具		管理员名称:										
		That we also also										
		联系力式:										
		屏蔽搜索引擎引用										
		禁止来自搜索引擎的页面	前访问									
		远程协助设置										
⇒ 正版授权	≡	保存恢复默认										

- (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
  - 建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,

🍠 火绒终端安全管理系		管理例外终端	×
	中心管理》中心设置	<b>溪加</b> 副除 畜注	
	终端管理员设置 中心升级 中心地址管理 通知设置	终端名称 ◆ 终端分组 本地IP ◆ MAC地址 限制类型 备注 操作	
🖀 防护策略 🛛 🗸	<b>卷码:</b>		
		▲ 本初, P*63 ::1 00-0C-29-8E 近程集团、 編編 前	ř.
	商线终端管理		
◎ 中心管理 へ	一 终端离线 30 天后, 删除终端		
	当時戶端口观问起需要求即管理只时,完在珍嬌显示以下既影問思		
	管理员名称:		
	联系方式:		
	屏蔽機索引擊引用		
	□ 禁止来自搜索引擎的页面访问		
	HT SPALABNIC 200		
	34-mir/di/25/20404/07/03/04 20		
	超时处理方式: O 连接 O 拒绝		
	禁止普通管理员远程例外终端:管理例外终端	<b>共1条</b> 20象页 ~ K 〈 1 /共1页	> >1
💎 iensista 😑	依提繁认		关闭

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。

》大绒终端:	安全管理系	系统 V2.0.16.0						(	搜索导航、模块名称	۹	11 6	e 🕹 (	🤗 admin 🗸
白前		中心管理 > 中心设置											
- 终端管理		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置				
富 防护策略		管理中心升级方式设置											
③ 漏洞修复		○ 自动升级											
🕜 资产管理		○ 手动升级											
❷ 中心管理													
账号管理		升级服务器代理设置 可以为升级服务器设置代理	通过代油能容器上和田	52010									
多级中心		指定代理服务器 网络	VERSE I GREEKESS WIT THATSES	V12+CM0Va									
数据备份		代理地址:	端口										
中心迁移		HONE.	598.272										
		/ U/ XA 5 .	1219										
- Parte													
		保存恢复默认											
◇ 正版授权	Ξ												

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。

🧦 火绒终端	安全管理系	统 <u>V2.0.16.0</u>							搜索导航、模块名称	Q	11 6	» 🖧	🤗 admin 🗸
白首页		中心管理 > 中心设置											
😡 终端管理		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置				
富 防护策略		添加中心 终端支持自动	连入下方中心,新连入的中	中心可对终端实施管控									
③ 漏洞修复		中心地址	部響端口			中心备	ŧ			操作			
⑦ 资产管理						1.0000							
多级中心													
数据备份													
中心迁移													
中心设置													
日 事件日志													
							9						
						首无相关致	<b>白</b>						
😔 正版授权													

- 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。

🍠 火绒終端	安全管理系	统 V2.0.16.0						(	搜索导航、模块名称	Q	11 6 4	🤰 🤗 admin 🗸
白首页		中心管理 > 中心设置										_
□ 终端管理		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
🖀 防护策略		中心通知设置										
◎ 漏洞修复		✓ 任务完成时通知										
资产管理		☑ 硬件变更通知										
四中心管理		✓ 终端安全服务异常通知										
账号管理		✓ 子中心连入通知										
多级中心		✓ 子中心腔意通知										
政治审切		■ 数据导出通知										
中心设置			-									
日 事件日志		☑ 中心所在磁盘剩余空间/	N-F 500		4: 1~999)							
		邮件预警设置										
		启用邮件告答										
🗢 正版授权		保存使复数认										

(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。

🛷 火绒終端安全管理系	统 V20.16.0		搜索导航、模块名称 Q 11 🚳 🦨 💽 admin 🗸
	中心管理 > <b>中心设置</b>		
	终端管理员设置 中心升级 中心地址	言理 通知设置 通用设置 数据库管理 负数中位	)管理 终端部署设置
富防护策略 🗸	中心通知设置		
	🗹 任务完成时通知		
	📴 硬件变更通知		
◎ 中心管理 へ	☑ 终端安全服务异常通知	* SMTP服务器地址: 请输入SMTP服务器地址	
	🗹 子中心连入通知	* SMTP服务器端口: 请输入SMTP服务器端口	
	☑ 子中心脱离通知		
	S 数据导出通知	NTENCE O MARE - C ROUNTENCE O MAR	
		* 邮稿联号: 请输入邮销账号	
	ALCHREEKERSHARENARD, 200 MID	* 創稿密码: 请输入邮箱密码	
	邮件预警设置	加密方式: 🗌 SSL	
	☑ 启用邮件告答	<b>浅试邮箱</b> : 请填写测试邮箱 发送测试邮件	
	发件邮箱 配置		
	终端事件告警规则中心事件告警规则	URITE AKIN	
	<b>新</b> 你会		添加
	邮件标题 收件人邮箱		<b>提作</b>
	「火蟒線端办全等理系統1. 风险		
	保存恢复默认		

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。

》 火绒終端安全管理系		中心事件告警规则设置	×
▲ 普页	中心管理 > 中心设置	0	0 0
♀ 终端管理 ~	终端管理员设置 中心升级 中心地址管理 通知设置	<u> </u>	IF件内容 收件邮箱配置
🖀 防护策略 🗸 🗸	2 任务完成时通知	触警周期	
<ul> <li>         通過修复 ~     </li> </ul>	☑ 硬件变更通知	每 60 分钟扫描检查是否有触警事件	
⑦ 资产管理 ~	☑ 终端安全服务异常通知		
	☑ 子中心连入通知	触警事件	
麻ら管理	2 子中心脱离通知	■ 触醫事件	哪件说明
数据备份		─ 中心升级失败	火绒终端安全管理系统升级失败
中心迁移	10.155年2時毎期4条分開小工 500 302 マロト第20 (空間・1、000)	✓ 中心→周末更新	中心版本超过一周未更新
中心设置		中心磁盘告警	中心所在磁盘剩余空间少于500MB
	邮件预警设置	✓ 数据库服务异常	中心所用数据库服务异業
⊕ 管理工具	☑ 启用邮件告答		
	发件邮稿 1@qq.com 配置		
	终就事件告醫規則 中心事件告醫規則		
	89%		
	1 邮件标题 收件人邮箱		
	[火城终端安全管理系统] - 风险		
	保存		保存 取消

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

🍠 火绒终端安	全管理系統	充 V2.0.16.0							搜索导航、模块名称		୍ଚ୍ଚ୍ଚ୍ଚ୍ଚ୍ଚ୍ଚ୍	admi 🤗	n 🗸
白黄		中心管理 > 中心设置											
₩ 终端管理	~	终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置				
🖀 防护策略	~	通讯设置											
◎ 漏洞修复	~	设置通讯问隔: 🔵 自动调整	● 手动调整 30	6 v									
🕅 资产管理	~	终端与控制中	4心通讯间隔 30 秒,										
	^	配置服务器带宽:最大并发数	无限制 (1~100	0,为空时无限制)									
多级中心		单个连接的最	大下载速度无限制	KB/s (1~51200,为空日	时不暇速)								
数据备份		备用中心											
中心迁移		当前中心没有备用中心											
中心设置													
日 事件日志	~	时间同步											
		终端与中心时间:  以中心系	统时间为准,并始终同 谱  例外终端数:0	步 🗌 允许例外终端不进	行时间同步								
		日志管理											
		日志保存期限 6 个	下月										
		日志清理:当前管理中心的	]数据日志大小为:34.4 )	ИB									
		清理日志任务: 著	<b>9</b> 无										
♥ 正版授权		保存恢复默认											

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。

#### 北京火绒网络科技有限公司

🍠 火绒终端安	全管理系	统 V20160						(	搜索导航、模块名称	٩	പര്മ	2 🜔 admin 🗸
▲ 首页		中心管理 > <b>中心设置</b>										
😡 终端管理		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
置 防护策略		通讯设置										
③ 漏洞修复		设置通讯问隔: 🔵 自动调整	隆 〇 手动调整 3	· (1)								
资产管理		终端与控制中	中心通讯间隔 30 秒,									
❷ 中心管理		配置服务器带宽:最大并发数	无限制 (1~10	00,为空时无限制)								
账号管理		单个连接的	最大下载速度一无限制	KB/s (1~51200,为空时	才不限速)							
多级中心												
中心汗용		备用中心										
中心设置		当前中心没有备用中心										
🛱 事件日志		时间同步										
		终端与中心时间: 2 以中心到	系統时间为准, 并始终同 例外终端数 :0	步 6并例外终端不进	厅时间同步							
		日志管理										
		日志保存期限 6	个月									
		日志清理:当前管理中心的	的数据日志大小为:34.4	MB								
		清理日志任务:	智无									
⇒ 正版授权		保存使复新认										

#### (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。

🧦 火绒终端安:	全管理系	统 V2.0.16.0						(	搜索导航、模块名称	Q II	ଚ୍ଚ 🕹	🤗 admin 🗸
<b>合</b> 首页		中心管理 > 中心设置										
₩ 终端管理		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
🖀 防护策略		管理例外组	E調 例外經過数:0									
③ 漏洞修复												
资产管理		日志管理										
◎ 中心管理		日志保存期限 6	个月									
账号管理		日志清理:当前管理中心	的数据日志大小为:34.4 M	В								
多级中心		清理日志任务:	暂无									
数据备份		清理										
中心迁移												
		Syslog 数据导出										
		Syslog 数据 : 启用Syslo	g数据导出									
		导出数据类型: ☑ 安全日志	🗹 升级日志 🗹 條	复漏洞日志								
		导出数据地址:管理地址										
		API 接口										
		API 接口密钥: 管理密钥	查看接口文档									
		接口日志: 🗌 记录API接	口调用日志									
♥ 正版授权		保存使复数认										

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。

🧦 火绒终端多	安全管理系	统 V2.0.16.0						搜索导航、模块名称	Q 11	୍	🚑 🧛 admin 🗸
		中心管理 > 中心设置									
		终端管理员设置中心升级	中心地址管理	通知设置	操作已保存	数据库管理	负载中心管理	终端部署设置			
🖀 防护策略			生成密钥				×				
			可在此输入备注内容	添加							
		日志管理	+5	4. 1994/27	0	+== 10	- 8				
◎ 中心管理		日志保存期限 6 个月	19-15	于政府引问	Secret ID Secret Key	IRTF					
		日志清理:当前管理中心的数据日志大学	1	2025-03-06	P04ZN89OMI 8U8A6O6	禁用编辑删除					
		清理日志任务: 暂无									
		清理									
		Syslog 数据导出									
		Syslog 数据: 🦳 启用Syslog数据导出									
🔁 管理工具		导出数据类型: 🗹 安全日志 🛛 升级日	<i></i>								
		导出数据地址: 管理地址									
		API 接口									
		API接口密钥:管理密钥 查看接口文林	共1条	2	0条/页	1 /共1页	» э				
		接口日志: 🗌 记录API接口调用日志									
		<b>保存</b> 恢复默认									

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

- 100 火绒终端	安全管理系	统 12.0.16.0							搜索导航、模块名称	Q	11 💮	🕻 🤔 🌏 admin 🗸
白前		中心管理 > 中心设置										_
		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
富 防护策略		○ 默认数据库			11.1							
⑥ 贏同條复		0 外接数据库				565						
⑦ 资产管理		Water of Distance	24 35 W/177 / 2 08C-4-1									
□ 中心管理		SX(STIN=COMF :	16.080(4)		40	號得是否迁移数据						
账号管理 条级由心		数据库地址":	192 168 1 1	迁移数据								
数据备份		数据库满口气	5236	未更换数据库 (	(仅停改证书、数据库用户名	<ol> <li>口令等配置)时无需迁移数据</li> </ol>						
中心迁移		数据库1*:	data1	○ 迁移								
PORE		数据库2*:	datal	迁移范围								
<b>日</b> 事件日志		用户名*:	user	<ul> <li>         新认迁移西         <ul> <li>             近形全             </li> </ul> </li> </ul>	記置文件 部日志							
		□�*:	•••	○ 迁移前	30 天日志,	包括当天日志 (范围1~999)						
				() 不迁移	日志							
		数据库SSL加	峦									
		深加证书。					<b>建</b> 体 取消					
		演上传数层库有户	"满证书			_						
		CA验证:	验证CA证书名									
♥ 正版授权		保存										

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。

🌔 火绒終端	安全管理系	统 12.0.16.0						搜索	<b>浔航、模块名称</b>		ଚ 🕹 🤇	🤌 admin 🗸
白首页		中心管理 > 中心设置										
🚽 终端管理		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
🖀 防护策略												
◎ 漏洞修复		负载中心		负载中心客户	端连接数		主中心客户端连接数		春户端总数			
🕜 资产管理		0 台		0 点			1 点		1 点			
四中心管理												
账号管理		待审批(1) 已接入(0)										
多级中心		申请时间: 全部时间	~ 全部时间	目 授索: 请	输入负载中心IP	Q						自守田
数据备份		申请时间	IP地址			部臀端口		管理端口			操作	
中心迁移		2025-03-07 13:17:23	192.168.53.67			6080		8080			通过 拒绝	
舟 管理工具												
										State VALUE	dours	
1.00		共1条						2	0条/页 🗸 🗸	成はWIN 新刊役置では く、「「「」」、	はOWS 以激活 Window	57/共1页
🔷 重复授权												

全管理系统	¥ V2.0.16.0							搜索导航、模块名称			🤗 admin 🗸
	中心管理 > 中心设置										
~	终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
~											
~	负载中心		负载中心客户端 0	站车接数		主中心春户端连接数		香户端总	数		
~	0 台		U Æ			1 点		1 点			
^											
	待审批(0) 已接入(1)										
	负载中心在线状态: 全部	── 搜索: 请输入负!	载名称、IP地址 Q								自导出
	负载名称	IP地址	连接终端数	负载状态 7			部署端口	管理端口	备注	操作	
	Eoad-1	192.168.53.67	0	<b>IR</b> 0%	C. 0% (**) 0%	<b>6-9</b> 0%	6080	8080	-	暂停 删除	
~											
									激活 V	Vindows	
≡	共1条							20条/页 ~	K <		/共1页
	全管理系3 ・ ・ ・ ・ ・ ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	全管理系統 V22188 中心管理 3 中心設置 9 中心設置 9 中心設置 9 中心管理 3 中心設置 9 中心学 9 中心 9 中心 9 中心 9 中心 9 中心 9 中心 9 中心 9 中心	全管理系统 v20.16 中心理系 中心理系 中心理系 中心理系 中心理系 中心理系 中心理系 中心理系	全管理系统     Y20160       中心程度・中心设置     中心开展       中心研展     中心研展       気数中心     ①       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ①     白       ②     う       ②     う       ②     う       ②     う       ②     白       ③     白       ③     白       ③     白       ③     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白       ○     白 </th <th>全省理念社     V2.0160       中心記述     中心記述       中心記述     中心記述       「意思中心」     泉歌中心一声户描述       「意思中心」     泉歌中心一声户描述       「意思中心在然状态:     全部 / 第       「「読む中心在然状态:     全部 / 第       「「読む中心在然状态:     全部 / 第       「「読む中心在然状态:     192166.33.67       ●     ●       ●     ●       ●     ●       ●     ●       ●     ●</th> <th>全省理究純     Y20160       中心思想、中心深遠     中心汗液       中心汗液     中心治道       「気気中心     気気中心       「気気中心     気気中心       ()     点       ()     <t< th=""><th>全省理351 12210         中の活動・中の消息         中の消息       中の消息         の点       1点         日本市地(の) 日時入(1)         完成中の中の経営技術:       全部で、「新知人の気気の病、戸地社」の         大概名称       戸地社         支援市の       0.5         1       122.108.53.67         0       正常(1)         1       122.108.53.67         1       122.108.53.67         1       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67</th><th>全会性認知: v2.116/         中心思想: 中心功思       中心功思 中心功思       通知设置       通用设置       取読成電管: 金銀中心管:         「意思中心       ①       ①       第回公司       第回公司       第回公司         「意思中心       ①       ①       ①       第回公司       第回公司       第回公司         「日本市山       ①       ①       ①       第回公司       第回公司<th>全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全</th><th></th><th></th></th></t<></th>	全省理念社     V2.0160       中心記述     中心記述       中心記述     中心記述       「意思中心」     泉歌中心一声户描述       「意思中心」     泉歌中心一声户描述       「意思中心在然状态:     全部 / 第       「「読む中心在然状态:     全部 / 第       「「読む中心在然状态:     全部 / 第       「「読む中心在然状态:     192166.33.67       ●     ●       ●     ●       ●     ●       ●     ●       ●     ●	全省理究純     Y20160       中心思想、中心深遠     中心汗液       中心汗液     中心治道       「気気中心     気気中心       「気気中心     気気中心       ()     点       () <t< th=""><th>全省理351 12210         中の活動・中の消息         中の消息       中の消息         の点       1点         日本市地(の) 日時入(1)         完成中の中の経営技術:       全部で、「新知人の気気の病、戸地社」の         大概名称       戸地社         支援市の       0.5         1       122.108.53.67         0       正常(1)         1       122.108.53.67         1       122.108.53.67         1       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67</th><th>全会性認知: v2.116/         中心思想: 中心功思       中心功思 中心功思       通知设置       通用设置       取読成電管: 金銀中心管:         「意思中心       ①       ①       第回公司       第回公司       第回公司         「意思中心       ①       ①       ①       第回公司       第回公司       第回公司         「日本市山       ①       ①       ①       第回公司       第回公司<th>全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全</th><th></th><th></th></th></t<>	全省理351 12210         中の活動・中の消息         中の消息       中の消息         の点       1点         日本市地(の) 日時入(1)         完成中の中の経営技術:       全部で、「新知人の気気の病、戸地社」の         大概名称       戸地社         支援市の       0.5         1       122.108.53.67         0       正常(1)         1       122.108.53.67         1       122.108.53.67         1       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67         日本       122.108.53.67	全会性認知: v2.116/         中心思想: 中心功思       中心功思 中心功思       通知设置       通用设置       取読成電管: 金銀中心管:         「意思中心       ①       ①       第回公司       第回公司       第回公司         「意思中心       ①       ①       ①       第回公司       第回公司       第回公司         「日本市山       ①       ①       ①       第回公司       第回公司 <th>全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全</th> <th></th> <th></th>	全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全 全		

#### 北京火绒网络科技有限公司

🍠 火绒终端安全管理系	统 V2.0.16.0				负载中心详情		×
▲ 首页	中心管理 > 中心设置				详细信息	设置	
回 终端管理 く	终端管理员设置	中心升级 中	心地址管理	通知设置	通用设置		
🖀 防护策略 🛛 🗸					英载中心信息		
<ul> <li></li></ul>	负载中心		负载中心客	沪端连接数	* 负载中心名称:	Load-1	6/30
资产管理      ✓	0 台		0 点		负载中心地址:	192.168.53.67	
◎ 中心管理 へ					管理送口:	8080	
账号管理	待审批(0) 已接入(1)				部署端口:	6080	
多级中心	负载中心在线状态: 全部	· 搜索: 请输入负载名			100407		
数据备份	负载名称	IP地址	连接终端数	负载状态 9	(王田市)[中]		
中心迁移	I.oad-1	192 168 53 67	0	<b>FR (3</b> 0% <b>P</b> .	客户端连接数:		
					负载中心备注	非必填项 (不可超过300个字)	
							0/300
					●负载监控		
					CPU使用率(%)		23 查看大图
					100		
					90 80		激活 Windows
	共1条				70		
火绒终端安全管理系	统 V2.0.16.0				负载中心详情		×
》 火绒终端安全管理系 前 前页	统 V20160 中心管理 > 中心设置	_	_	_	负载中心详情 详细信息	设置	×
<ul> <li>         火城終端安全管理系     <li></li></li></ul>	<ul> <li>休 V20160</li> <li>中心管理 &gt; 中心设置</li> <li>终端管理员设置</li> </ul>	中心升级 中	心地址管理	通知设置	负载中心详情 详细信息 通用设置	0 <u>m</u>	×
<ul> <li></li></ul>	ゲ、V20160 中心管理 > 中心设置 終端管理员设置	中心升级 中	心地址管理	透知设置	负载中心详情           通用设置           / 终端接入数量/           / 终端接入数量/           / 約欄成: 0	2 2 2 1 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1	×
火焼約端安全管理系           血         善市           型         約端管理         ~           器         防炉販売         ~           ⑥         薬同除気         ~	<ul> <li>ゲ、V2.0160</li> <li>中心管理 &gt; 中心设置</li> <li>疾病管理员设置</li> <li>魚都中心</li> <li>魚 4</li> </ul>	Ф <u>О</u> #& Ф		透知设置		22篇 22期 12分配 ○ 手动分配	×
・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・    ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・   ・	统 (V20160) 中の管理→ 中の设置 終端管理员设置 负載中心 0 会	Ф <del>0Л</del> & Ф	心地址管理 负赖中心客 0 点	通知设置	负载中心详情 详细信息 建筑接入数量 控制模式: ● 目: 网络按入策略 案职 全部	23月 23月 か分配 ○ 手动分配 ● ●	×
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	统 (V20160) 中心管理 > 中心设置 終編管理员设置 负載中心 0 会	Ф¢#& Ф	心地址管理 负载中心音 0 点	递加设置 产弹流法统数	负载中心详情 详细信息 终端按入数量 拉制模式: ④ 即 网络按入策略 来型: 全部	22週 23週 か分配 ○手幼分配 ○ ② 検索: ③約約入12180法	x Q
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	统 (V20160) 中心部語 > 中心设置 終端管理员设置 の載中心 ① 会 荷布批(の) 己族人(1)	<b>₽©∄\$</b> #	心地址管理 负载中心客 0 点	道加限重	负载中心详情 译细信息 终端按入数量 控制模式: ① 自 网络按入策略 关型: 全部	22週 23月 か分配 ○ 手动分配 ○ ○ 数次: 第960人12980法	Q (\$to
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	<ul> <li>休 V20160</li> <li>中の部語 &gt; 中の设置</li> <li>総納管理员设置</li> <li>の最中心</li> <li>① 合</li> <li>の春批(の) 已線入(1)</li> <li>免萄中心在該状态: 全部</li> </ul>	中心升级 中 中心升级 中 学 養業: 時後入気気が	<ul> <li>         ・2時は管理         ・2        ・2        ・2        ・2</li></ul>	選加股票 建加股票 产质注册数	负载中心详情 運用設置 自然議会入数量 控制模式: ① 自定 风绪接入策略 哭啦: 全部 果型	22冊 22期 か分配 ○ 手动分配 ○ 「 「 按索: 「時級入1P地址:	ス () (美元) (美元)
・	<ul> <li>ペンシン 180</li> <li>ペンシン 180</li> <li>ペンシン クシン 200</li> <li>ペンシン 200</li> <li>ペン</li></ul>	中心升级 中 (1) 中心升级 中 (1) 東京: (1) 日本(1) 11 1001 1001 1001 1001 1001 1001 100	心地址管理 ① 成数中心者 ② 点 R、IPP8社 连接行编载	通知股票 通知股票 中操主法数 Q 负数状态: 平	负载中心详情 详细信息 体强接入数量 控制模式: ① 自由 风绪接入策略 笑犯: 全部 类型	22 23 か3記 ○ 手助分配 ○ 該索: (新助入19地址: 19地址	ス () (新聞) (新聞作)
大焼乾端安全管理系           血         前页           印         然協管理           ②         脳防学策略           ③         二           ④         二           ⑦         二           ●         中心管理           ●         単心管理           ※現年も         実現市会           支援市会         中心管理           中心正形         中心空間	<ul> <li>ペンシン 160</li> <li>中心部団 &gt; 中心協選</li> <li>検病管理员设置</li> <li>魚歌中心</li> <li>① 台</li> <li>(約 南北(の) 已統入(1)</li> <li>免歌中心在該状态: 全部</li> <li>① 魚都和心在該状态: 全部</li> <li>① 魚都和心在該状态: 全部</li> </ul>	中心升级 中 学 建素: 函输入系统部 IP地址 192.168.53.67	<ul> <li>         ・の助送管理         <ul> <li></li></ul></li></ul>	選加保置 (中純主要数 Q (2) (2) (2) (2) (2) (2) (2) (2)	①数 中心详備 運用設置 単相信息 1 体獄後入数量 注相信息 2 体獄後入数量 注射模式: ① 目: 2 例络接入策略 笑犯: 全部 楽型 205 例	22 22 か分配 ○ 手助分配 ○ 接索: 済始入口地址 12P総址	ス () () 名 操作
・             ・		中心升级 中 学 建築: 国和人名法名 192.166.53.67	<ul> <li>○地址管理</li> <li>① 点</li> <li>① 点</li> <li>○ 点</li> <li>○ 点</li> </ul>	第10段置 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)<	①数初中心详備 详細信息       通用設置       通用設置       (修筑後入数量)       20時間第二       (1)       (2)       (2)       (2)       (2)       (2)       (2)       (2)       (2)	22 22 か分配 ○ 手助分配 ● 接索: 第第ADP地址 12P地址	ス () () 名 操作
・             ・		中心升级 中 学 建築: 国地入名型名 19216853.67	<ul> <li>○地址管理</li> <li>① 点</li> <li>○ 点</li> <li>○ 点</li> <li>○ 点</li> <li>○ 点</li> <li>○ 点</li> <li>○ 点</li> </ul>	選加股票 (中純正接数 (2) (2) (2) (2) (2) (2) (2) (3) (3) (3) (4) (4) (5) (4) (5) (5) (5) (5) (5) (5) (5) (5	①数初中心详備 详細信息       通用設置       (修筑後入数量)       20時間       (約約後入策略)       光型:       (本部)       ※型:	22 22 か分配 (手助分配) で 接索: 第第人口地址 17P総址	ス () (名) (名) (名) (名) (名) (名) (名) (名) (名)
・             ・		中心升级 中 建業: 評給人名奥尔 印地址 1921685367	<ul> <li>○応比管理</li> <li>① 点</li> <li>① 点</li> <li>○ 点</li> <li>○ 点</li> </ul>	第10段目 (中純主味教)	①数     ①数     注烟信息       連用設計     注烟信息       注烟信息     注烟信息       注約     注烟信息       注約     注約       注約     注約       20%     43	2期 か記 ● 手助分配 ● 様素: 第48AD98年 1989年	× () () () () () () () () () ()
・             ・	<ul> <li>ペンロ160</li> <li>中心協調 &gt; 中心協調</li> <li>総議審理員设置</li> <li>原載中心</li> <li>① 台</li> <li>① 台</li> <li>(())</li> <li>① 台</li> <li>○ 台</li></ul>	中心升级 中 建筑: 1980人名思名 1921685367	<ul> <li>○応比管理</li> <li>① 点</li> <li>① 点</li> <li>○ 点</li> <li>○ 点</li> <li>○ 点</li> </ul>	第10段目 (中純主味教) (二) (元) (元) (元) (元) (元) (元) (元) (元) (元) (元	①数ボ中心详備           運用設計           (谷誠法入政量)           26頃後入取着           26頃後入取着           26頃後入取着           2705	2期 か記 ● 手助分配 ● 様素: 単始入12地址 12地址 12地址	ス () () () () () () () () () () () () ()
火焼炸端安全管理系           血         前页           二         前页           二         前页           二         防炉販売         ~           二         防炉販売         ~           ご         防炉販売         ~           ご         加炉販売         ~            中心管理         ^            中心管理         ^            中心管形         ~            中心管         ~            中心目歩         ~            中心管         ~           管 管理工具	<ul> <li>ペンシン 150</li> <li>中心協調 &gt; 中心協調</li> <li>年の協調 &gt; 中心協調</li> <li>(株装飾管道県設置</li> <li>① 会</li> <li>① 会</li> <li>① 合</li> <li>○ 合</li> <l< th=""><th>中心升级 中 学 建家: 約約入合组合料 192.148.53.67</th><th><ul> <li>○地址管理</li> <li>① 点</li> <li>① 点</li> <li>R. IPP8社</li> <li>通知対映数</li> <li>0</li> </ul></th><th>2002日 学院主体教 Q 会報状态 マ 三王 © 0% ご</th><th>①55 \$P</th><th>22 23 分配 ○ 手助分配 ○ 接京: 清助入口地址 □ P地址 □ 日地址</th><th>۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲</th></l<></ul>	中心升级 中 学 建家: 約約入合组合料 192.148.53.67	<ul> <li>○地址管理</li> <li>① 点</li> <li>① 点</li> <li>R. IPP8社</li> <li>通知対映数</li> <li>0</li> </ul>	2002日 学院主体教 Q 会報状态 マ 三王 © 0% ご	①55 \$P	22 23 分配 ○ 手助分配 ○ 接京: 清助入口地址 □ P地址 □ 日地址	۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲ ۲
火焼炸端安全管理系           血         前页           印         然端節週         ~           富         防炉策略         ~           6         瀧房除夏         ~           6         瀧房除夏         ~           6         龍月除夏         ~           6         中心管理         ~           6         中心管理         ~           7         から管理         ~           10         中心管理         ~           11         中心管         ~           12         新日日志         ~           13         新日日志         ~	<ul> <li>ペロ160</li> <li>中心協調 &gt; 中心協調</li> <li>(株装飾物画の設置</li> <li>(集装飾物画の)</li> <li>(株装飾物画の)</li> <li>(株装合称)</li> <li>(株式会社)</li> </ul>	中心升级 中 学 雅家: 所知入公司公司 即地址 192.168.53.67	○地址管理 の成本 の点 の点 を、IPP地址 も無料で編数 の	通知設置	①数初中心详情 详细信息       通用设置       修確接入数量       20%       10       20%	23月 23月 か分配 ● 手动分配 ● 接索: 前沿入19地址 19地址 ■ 19地址	د بی م بی پی
(a)       前页         (c)          (c)       <	<ul> <li>ペロ160</li> <li>中心協調 &gt; 中心協調</li> <li>(株装備管理局設置</li> <li>魚敷中心</li> <li>① 会</li> <li>(特定批(の) 日総入(1)</li> <li>① 会</li> <li>○ 会</li>     &lt;</ul>	中心升级 中 一	○地址管理 の成本 の点 の点 を、IPP地址 も無料で編数 の	通知設置	①数初中心详情       運用設置       送朝儀式:       1 修識接入数量       送朝儀式:       1 网络接入策略       光聖:       全部	23月 23月 か分配 ● 手动分配 ● 接索: 前級入17地址 ■ 17階址 ■ 第元相知	د چ بید م
火焼炸端安全管理系           血         苗氏           印         統備管理         ~           第         防炉原配         ~           第         防炉原配         ~           第         防炉原配         ~           第         防炉原配         ~           第         中心管理         ~           中心管理         ~            中心管理         ~            中心管理         ~            中心管理         ~            市口         第中日志         ~           合         管理工具	<ul> <li>ペンシン 150</li> <li>中心部語 &gt; 中心设置</li> <li>総議管理員设置</li> <li>魚戦中心</li> <li>① 会</li> <li>() 合数中心在线状态: 全部</li> <li>① 気気名称</li> <li>() Load-1</li> </ul>	中心升級 中	○地址管理 ① 気報中心者 ② 点	通知設置	①、 10 ① ① ② ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ③ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦	23月 23月 かえ ● 手助分配 ● 使変: 消除入P2地址 ■ P地址 ■ 1P地址	م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي           م         ي
・	<ul> <li>ペンシン160</li> <li>中心証言 &gt; 中心设置</li> <li>総議管理员设置</li> <li>免戦中心</li> <li>日 会</li> <li>① 会</li> <li>(○ 会</li> <li(○ li="" 会<=""> <li>(○ 会</li> <li>(○ 会</li> <li>(○ 会&lt;</li></li(○></ul>	中心升級 中	○地址管理 ① 気報中心者 ② 点 (1) 小型 (1) ) (1) 小 (1) ) (1)	通知设置	①気気中心洋清       運用設置       通用設置       26気法人気量       26気法人気量       26気法人気量       27日       27日	22 23 23 23 23 23 23 23 23 23 23 23 23 2	ス           第二           第二

#### 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。

🧦 火绒终端3	安全管理系统	充 V2.0.16.0						(	搜索导航、模块名称	۹	1 6 4	admin 🗸
白首页		中心管理 > 中心设置										
🚽 终端管理	~	终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置			
富 防护策略	~	部署页设置										
③ 漏洞修复	~	通知标题: 全网部署火绒通知	0									
资产管理     资产管理	~											
◎ 中心管理	^	为了更好的保	障内网安全,决定从	17日起全面安装部署火绒终端的	R全管理系统。您可以通过	下面的按钮进行下载并安徽	束,安装后无需任何设置可以	以立即使用。				
账号管理												
多级中心		海道										
数据备份												
中心迁移	_	下载链接: 🔽 隐藏未授权类型	1下载链接									
中心设置												
日本 事件日志	~	自用修繕安装密码										
🖶 管理工具		密码: 6-8位字母数字组成	R ø									
		启用修缮安装的IP排赴范围	1									
											<ul> <li>允许安</li> </ul>	業 🔘 阻止安装
		IP地址范围	备注							操作		
						<u> </u>						
♥ 正版授权	Ξ	保存恢复默认										

## 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。

🧦 火绒终端	安全管理系	统 V2.0.16.1						(	搜索导航、模块名称	ຊ 14 ຄໍ ໑	admin 🗸
合黄		中心管理 > 中心设置									
- 终端管理		终端管理员设置	中心升级	中心地址管理	通知设置	通用设置	数据库管理	负载中心管理	终端部署设置	定制化	
富 防护策略		启用定制化									
③ 漏洞修复		and a standard of									
⑦ 资产管理		中心定制									
🖾 中心管理		4-0-dex. X300									
账号管理		英文名称: Huor	ong Endpoint Security Managemer	nt System							
多级中心		中心LOGO									
数据备份											
中心迁移		建议想上传256*1	56像寨的png、svg、ico格式图片,推	矇wg格式,大小不超过500KB							
中心设置		🔊 е	Dogo.svg		۲						
🛱 事件日志											
🔂 管理工具											
		终端定制 仅支持定制化Window	s2.0、macOS、Linux桌面服终销								
		终端名称: 火绒			2/6						
		繁体名称: 火統			2/6						
		英文名称: Huor	ong								
		终端LOGO								激活 Windows	
√ 正版授权		保存恢复	赋认							转到"设置"以激活 Win	idows,

# 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。

🧦 火绒终端安全管理系	统 V2.0.15.0					搜索	予航、模块名称	ର୍ ୩ ଚା 🖓 😔 admin
▲ 首页	事件日志 / 安全事件总览 / 錄	充计						
♀ 终端管理 ~								
S 防护策略 >	く 返回 焼け方式: 按修護	<b>∺</b> ∨						自导出
<ul> <li>圖洞修复 </li> </ul>								
- ⑦ 资产管理 ~	大格 図表							
・ 一回 中心管理 ・ く	终端名称	计算机名称	终端分组	本地IP	通信IP	MAC地址	涉及事件	事件占比
ー 日 事件日志 へ	1 本机	DESKTOP-TOSOOEK	产品组	192.168.5.24	192.168.5.24	00-0C-29-17-A1-39	6	60.0%
安全事件总览	DESKTOP-T6SC597	DESKTOP-T6SC597	未分组终端	192.168.3.143	192.168.3.143	00-50-56-9B-3A-B8	4	40.0%
病毒查杀								
病毒防御								
系统防御								
网络防御								
14:01:0								
2月6日								
11万言理								
愛講習理日本								
系统管理日志								
数据导出管理								
安全分析报告								
🔂 管理工具								激汗 Windows
💎 正版授权 🛛 🚍	共2条							時X1日 Windows 转到"设置"以激活 Windows。1 >
🧦 火绒终端安全管理系	统 V2.0.15.0					搜索	爭航、模块名称	으. 11. 하 🖧 🤤 admin
火绒终端安全管理系 〇 首页	统 V2.0.15.0 事件日志 / 安全事件总览 / 編	充计				授太早	子航、模块名称	o. 11 🔊 🕹 📀 admin
<ul> <li>         火銀終端安全管理系     <li></li></li></ul>	统 V2.0.15.0 事件日志 / 安全事件总选 / 统	充计				·浓雪	<b>导航、模块名称</b>	o, 11 of 🧔 😜 admin
火绒終端安全管理系 前 首页 梁 终端管理 ~ 第 防护策略 ~	统 V2.0.15.0 事件日志 / 安全事件总范 / 錄 《返回 统计方式: 按终疑	£i <del>f</del> . ≋ ∼				證券	學航、櫻块名称	Q. 11. 6 4 2 3 admin 企 9日
<ul> <li>◇ 火焼終端安全管理系</li> <li>○ 首页</li> <li>□ 年減管理 ~</li> <li>図 防扩策局 ~</li> <li>○ 漏卵修复 ~</li> </ul>	统 V2.0.15.0 事件日志 / 安全事件总览 / 統 < 返回 统计方式: 按续数	é. * ∨				授業	對此、櫻块名称	Q 11 6 4 9 2 admin
◇ 火城終端安全管理系 ○ 首页 □ 当页 □ 生装管理 ◇ 2 防护策略 ◇ ○ 薬用時度 ◇ ① 次が管理 ◇	统 V2.0.15.0 事件目志 / 安全事件急宽 / 紙 《返回 统计方式: 按终望 类指 重要	eif * ~				<b>按索</b> 4	對敵、機块名称	Q 11 6 4 9 2 admin
<ul> <li>◇ 火焼炸器女全管理系</li> <li>○ 首页</li> <li>□ 年減管理</li> <li>◇</li> <li>窓 防炉焼配</li> <li>○ 運卵修复</li> <li>◇</li> <li>◇</li> <li>◇</li> <li>◇</li> <li>◇</li> <li>◇</li> <li>◇</li> <li>○</li> <li>○</li></ul>	依 V2.0.15.0 事件目志 / 安全事件急気 / 紙 く返回 続け方式: 接続器 要括 重要 照時: 供換容数 >	€i† * ─ ─ ─				<b>按</b> 然4	旁航、欄块名称	Q 11 6 2 2 admin 会导出
大阪啓蒙女全管理系     山 前页     単気管理     マ     ち該管理     マ     ち該管理     マ     ち防労策略     マ     の     面の特友     マ     の     面の特友     マ     の     の     の     市で管理     マ     日     市で管理     マ     市で管理     マ     市で管理     マ     市で     れ     ち     市で     れ     ち     市で     れ     ち     市で     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     れ     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち     ち	统 V2.0.15.0 事件日志 / 安全事件总范 / 紙 《返回 统计方式: 按跨 要搭 室業 / 紙給: 按鍋名称 >	8H * ~				P\$254	Pàt, 優快名称	a 11 6 P の admin 企 号出 Top10 ~
<ul> <li>◇ 火娘终端女全皆理系</li> <li>○ 前页</li> <li>◇ 均衡策略</li> <li>◇ 第時時限</li> <li>◇ 第時時限</li> <li>◇ 第時時</li> <li>◇ 第時日志</li> <li>◇</li> <li>◇ 会事件印</li> </ul>	统 V2.0.15.0 部件日志 / 安全部件总范 / 統 《 返回 统计方式: 按統對 梁格 圖號 / / / / / / / / / / / / / / / / / / /	€i+ * ─ ✓		6 5625	<ul> <li>লক্ষাচেল          <ul> <li>শেষাচেল              <ul> <li>শেষাচেল              <ul> <li>শেষাচেল                       <ul></ul></li></ul></li></ul></li></ul></li></ul>	接续	9新、 银环名称	Q 11 6 2 (2) admin 企 导出 Top10 ~
<li>         ・         ・         ・</li>	<ul> <li>休 (22,0,15.0)</li> <li>御仲日志 / 安全専件急気 / 値</li> <li>く 返回 続け方式: 抜焼器</li> <li>※格 監察</li> <li>振输: 統論名称 &gt;</li> <li>沙及専件数</li> <li>6</li> </ul>	€i+ *		. Ree*	<ul> <li>লক্ষাচেল          <ul> <li>শেষাচেল              <ul> <li>শেষাচেল              <ul> <li>শেষাচেল                       <ul></ul></li></ul></li></ul></li></ul></li></ul>	1624 26	9新、银环名称	Q 11 6 2 (2) admin 会界出 Top10 〜
火鉄株器会全管理系           論 単次           学 総論管理           学 部件印表           小部音楽           病毒音楽           病毒音楽	<ul> <li>休 (V2.0.15.0)</li> <li>御仲日志 / 安全専件急気 / 値</li> <li>く 返回 続け方式: 按続望 表格 回来</li> <li>細胞: 按論名称 &gt;</li> <li>沙及専件故</li> <li>5</li> </ul>	€i+ * ✓		• ster	<ul> <li>লক্ষাচেরা          <ul> <li>শেকাচেরা             </li></ul> </li> </ul>	1624 16	9新、银环名称	<ul> <li>Q 11 6 2 (2) admin</li> <li>企 导出</li> <li>Top10 ~</li> </ul>
・             ・	第 √2.0.150 第件日志 / 安全事件总法 / 第 《返回 統计方式: 接渡資源 ※据 室際 振祉: 鉄道名称 ~ 第25時間 6 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	€i+ *		• R42X	<ul> <li>লক্ষাচের্জ          <ul> <li>শ্বিকাচের্জ              <ul> <li>শ্বিকাচের্জ              <ul> <li>শ্বিকাচের্জ                       <ul></ul></li></ul></li></ul></li></ul></li></ul>	按点	9新、 银环名称	Q 11 6 2 (2) admin 会界出 Top10 ~
シン状体や描文全管理系         品       首页         二       単成管理       ・         二       第時常用       ・         ②       温剛修复       ・         ③       温剛修复       ・         ③       温剛修复       ・         ④       温剛修复       ・         ④       当時年間       ・         ●       中心管理       ・         ●       事件日志       ・         ●       赤寺香音系       赤寺奇防朝         系統防衛       三       5.0556	第 √2.0150 第件日志 / 安全事件总法 / ダ く返回 統计方式: 接続算 要指 室業 個級: 鉄鋼倉祭 ~ 第23時4数 6 5  4	8H * V		• R42*	<ul> <li>matos</li> <li>Relation</li> <li>Relation</li> </ul>	按点 指	9新、 但 环 名 称	Q 11 6 2
火焼終端安全営理系           品         自災           型         炭焼管理         ~           図         筋炉策略         ~           図         海外管理         ~           図         海外管理         ~           図         市の管理         ~           (2)         海外管理         ~           (3)         中心管理         ~           (4)         事件日志         ~           (5)         第時書並         ~           5.統訪初朝             5.統訪朝             1         公会事件の意味            1         (450)            1         (450)	第 (220150) 単作日志 / 安全事件包支 / ダ く 延回 統计方式: 接続調 要指 回来 福祉: 貸換名称 ~ 沙及事件数 6 5 4	8:+ * V		<ul> <li>病毒差米</li> <li>木利</li> </ul>	<ul> <li>লক্ষাচেল</li> <li>শিংগাচেল</li> <li>মাধা</li> </ul>	按点 强	9新、 银环名称	<ul> <li>a min</li> <li>a dmin</li> <li>a dmin</li> <li>a dmin</li> </ul>
・             ・	<ul> <li>休 (V2.0150)</li> <li>御仲日志 / 安全事件急流 / ダ</li> <li>《 返回 統计方式: 除残損</li> <li>※ 振振 重要</li> <li>「 (城船: 按論合称 &gt;</li></ul>			<ul> <li>病毒重求</li> <li>本机</li> <li>沙及事件致</li> </ul>	<ul> <li>সমাচল • শগাচল • মাধ্য</li> <li>বি</li> </ul>	17.25 17.25	<b>9新、银环名称</b>	<ul> <li>a min</li> <li>a dmin</li> <li>a dmin</li> </ul>
・             ・	<ul> <li>休 (220150)</li> <li>単件日志 / 安全事件总正 / 第</li> <li>&lt; 返回 統計方式: 按規算</li> <li>※指 重要</li> <li></li>     &lt;</ul>			本机 ))及事件致 )) 病毒素系	• 19441595 • 19441595 • 1944	17.25 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15 17.15	<b>9新、银环名称</b>	<ul> <li>a dmin</li> <li>a dmin</li> </ul>
・             ・	<ul> <li>休 (220150)</li> <li>御侍日志 / 安全事件急気 / ダ</li> <li>《 延回 桃田方式: 加速調</li> <li>※ 振笛 重算</li> <li>「 「 「 」」</li> <li>「 」」</li> <li>「 」」</li> <li>「 」」</li> <li>「 」」</li> <li>「 」」</li> <li>」</li> <li>…</li> <li>」</li> <li>…</li> <li>」</li> <li>…</li> <li></li></ul>			本机. 沙及事件数 「病毒素系 」 病毒素系	• пяльтя • Рантой • жилл 6 0 6	17.23 17.2 17.2 17.2 17.2 17.2 17.2 17.2 17.2	<b>9新、银环名称</b>	Q 1
	<ul> <li>休 (V20150)</li> <li>事件日志 / 安全事件总正 / 第</li> <li>《 返回 桃田方式: 接続調整</li> <li>※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※</li></ul>			<ul> <li>病毒量水</li> <li>水町、</li> <li>沙及事件数</li> <li>1 病毒豊原</li> <li>1 病毒世俗</li> </ul>	• яналом • яналом • кноло 6 0 6	按款 12	<b>}新、缆块名称</b>	Q 1 O O O O O O O O O O O O O O O O O O
<ul> <li>         ・         ・         ・</li></ul>	<ul> <li>休 (220150)</li> <li>事件日志 / 安全事件总页 / 修</li> <li>《 返回 執計方式: 接続算</li> <li>※ 推 重重</li> <li>( 返回 執計方式: 接続算</li> <li>( 返回 執計方式: 接続算</li> <li>( 返回 執計方式: 長端名称 &gt; 1)</li> <li>( 返回 和計)</li> <li>( 返回 和計)<!--</th--><th></th><th></th><th><ul> <li>病毒素が</li> <li>水机</li> <li>沙及事件数</li> <li>病毒批測</li> <li>病毒批測</li> <li>同毒批測</li> <li>同時批測</li> </ul></th><th>• янися • янися • жис 6 0 6 0</th><th>授款</th><th><b>7新、缆块名称</b></th><th>Q       1       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A</th></li></ul>			<ul> <li>病毒素が</li> <li>水机</li> <li>沙及事件数</li> <li>病毒批測</li> <li>病毒批測</li> <li>同毒批測</li> <li>同時批測</li> </ul>	• янися • янися • жис 6 0 6 0	授款	<b>7新、缆块名称</b>	Q       1       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A
<ul> <li></li></ul>	<ul> <li>休 (223150)</li> <li>事件日志 / 安全事件总页 / 修</li> <li>《 返回 執计方式: 接供調</li> <li>※ 推 重重</li> <li>( 返回 執计方式: 接供調</li> <li>( 返回 執计方式: 接供調</li> <li>( 返回 執计方式: 長代調</li> <li>( 返回 執计方式: 長代調</li> <li>( 返回 和)</li> <li>( 返回 和)<th></th><th></th><th>本-II、 沙及事件教   病毒改得   内助防衛   天助防衛</th><th>Realow     Realow     Realow     A</th><th>12</th><th><b>瑞、</b> 煤块名称</th><th>Q       1       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A</th></li></ul>			本-II、 沙及事件教   病毒改得   内助防衛   天助防衛	Realow     Realow     Realow     A	12	<b>瑞、</b> 煤块名称	Q       1       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A
<ul> <li></li></ul>	<ul> <li>休 V2.0150</li> <li>事件日志 / 安全事件总法 / 修</li> <li>《 返回 執计方式: 接供對</li> <li>※ 接信 重用</li> <li>( 減給: 控制名称 &gt;</li> <li>3</li> <li>4</li> <li>3</li> <li>4</li> <li>1</li> <li>0</li> </ul>		ŝ	本机 沙及事件数 「病毒意乐 」所助功师 「解助功师 」系助功师 事件占比①	Realow     Realow	173 173	<b>瑞.</b> 煤灰名称	Q       1       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A       A
	<ul> <li>外日志 / 安全等待急気 / ダ</li> <li>冬田田 供付方式: 使残望</li> <li>※ 近日 供付方式: 使残望</li> <li>※ 近日 供付方式: 使残望</li> <li>※ 近日 (11)</li> <li>※ 近日 (11)</li></ul>		ŝ	本町、 沙及事件数 第時電奈 1 府総防衛 1 死約防衛 第件台比(2)	Greaters     Presters	75 15	第1、 信 た 名称	Q 1 A A A A A A A A A A A A A A A A A A

144 / 261
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。

🧦 火绒终端安全管	大铖终端安全管理系统 V20.15.0     度素导航、標块名称 Q II の 4										e 🤗 admin 🗸		
白首页		御件日志 / 安全事件总范  * 流(1) 日近(3) 全部病功已還 全部病息 ✓											
₩ 终端管理	~	<b>本作米刑</b> · <del>众</del> 或	(Kates+ia) ·	2024-11-12 - 2024	11.10 B tom-	1000000 2017/m	m chimip 0			数据导出		1秒前	(4)+
S 防护策略	č	(KmeHill)	10144/0127 CD 🛔	10211115 E021	stehiD .	MACIMINE .	102 44 60 11 1 1 14 1	· (中国)	统计学	安全日志总览数据导出家	宅成,请点击下载		18/h
	~	2024-11-18 1	■ 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	发现病毒: Ro	处理成功	日志详情
🖾 中心管理	~	2024-11-18 1	📕 本机	产晶组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	发现病毒: Ro	处理成功	日志详情
🗟 事件日志	^	2024-11-18 1	# 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	发现病毒: Tro	处理成功	日志详情
安全事件总览		2024-11-18 1	# 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	发现病毒: Ad	处理成功	日志详情
病毒查杀		2024-11-18 1	🔛 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	发现病毒: Tro	处理成功	日志详情
病毒防御		2024-11-18 1	# 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	发现病毒: Tro	处理成功	日志详情
系统防御													
网络防御													
访问控制													
漏洞修复													
行为管理													
终端管理日志													
系统管理日志													
数据导出管理													
安全分析报告													
四管理工具												激活 Windows	
♥ 正版授权	=	共6条										转到"设置"以激活 W	indows, 1

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。

🧦 火绒终端安全	》 火焼終端安全管理系统 V2.0.15.0 後未导航、 様決 5.6 Q 11 6 Q ¹ (2) admin ~												
白首页		事件日志 / 安全事件总员	5										
🚽 终端管理	~												
富 防护策略	~	事件类型: 全部	∨ 终端时间:	2024-11-13 ~ 202	4-11-19 📄 搜索	: 终端名称、登记信	息、本地IP、:Q				品选择分组 由导出 辛自定义	例 昆检索	统计
② 漏洞修复	~	终端时间 🔶	终端名称 🖓 🔶	终端分组 🗘	本地IP 🝦	MAC地址	终端类型	◆ 病毒库版本 ◆	终端版本	事件类型	请选择要展示的信息	◆ 操作	
资产管理	~	2024-11-18 1	🔛 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	😑 全选 (11/17)	日志	详情
❷ 中心管理	~	2024-11-18 1	# 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	✓ 終端时间	日志	详情
日 事件日志	^	2024-11-18 1	₩ 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	☑ 终端名称	日志	详情
安全事件总览		2024-11-18 1	# 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	□ 计算机名称	日志	详情
病毒查杀		2024-11-18 1	🔛 本机	产品组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	፼ 终端分组	日志	详情
病毒防御		2024-11-18 1	🔛 本机	产晶组	192.168.5.24	00-0C-29-17	Windows	2024-11-14 1	V2.0.15.0	文件实时监控	✓ 本地P 通信IP	日志	详情
系統防御											MAC地址		
网络防御											☑ 终端类型		
访问控制											─ 病毒库版本 一		
漏洞修复													
行为管理													
终端管理日志													
系统管理日志													
数据导出管理													
安全分析报告													
☐ 管理工具											潮的天 V	lindows	
🔶 正版授权	=	共6条									转到"设计	『以激活 Window	1

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。

🥖 火瓴	酸端安全	管理系	统 V2.0.15.0											搜索导航	吭、模坊	快名称	٩	11 6	<b>,</b> 4	🧛 admin 🗸
合颜			事件日志 / 安全事件总数	E																
型 San 25 防护	宮埋 策略		事件类型: 全部	> 终端时间:	2024-11-13	- 2024-	11-19 🗎 搜索	终端名称、登记信	割、本地IP、;	Q					몷	选择分组(	日中山	^臣 自定义列	昆检索	统计
() 漏洞	修复		第一组:	终端名称	包含		请输入搜索关键词		蔵			第二组:	终端名称	R ~	包含		调制	入搜索关键词		
	管理			终端时间 由心时间					搜索	重置	取消									展开 ~
	11年		終端时间 🕴	终端名称	终端分组	٠	本地IP 🔶	MAC地址 \$	终端类型	٠	病毒库版本	终端版本	\$	事件类型	\$	事件摘要	\$	处理结果	\$	操作
安全	事件总览		2024-11-18 1	计算机名称 终端分组	产品组		192.168.5.24	00-0C-29-17	Windows		2024-11-14 1	V2.0.15.0	)	文件实时监控	2	发现病毒:	Ro	处理成功		日志详情
病毒	直杀		2024-11-18 1	本地IP	产晶组		192.168.5.24	00-0C-29-17	Windows		2024-11-14 1	V2.0.15.0	)	文件实时监控	ž	发现病毒:	Ro	处理成功		日志详情
病毒	访御		2024-11-18 1	通信IP MAC地址	产品组		192.168.5.24	00-0C-29-17	Windows		2024-11-14 1	V2.0.15.0	)	文件实时监控	2	发现病毒:	Tro	处理成功		日志详情
系统	防御		2024-11-18 1	终端类型	产品组		192.168.5.24	00-0C-29-17	Windows		2024-11-14 1	V2.0.15.0	)	文件实时监控	2	发现病毒:	Ad	处理成功		日志详情
网络	防御		2024-11-18 1	终端版本	产品组		192.168.5.24	00-0C-29-17	Windows		2024-11-14 1	V2.0.15.0	)	文件实时监督	2	发现病毒:	Tro	处理成功		日志详情
访问	控制														-					
漏洞	修复																			
(S)(1)(1)	^{時7年} 管理日志																			
系统	管理日志																			
数据	导出管理																			
安全的	分析报告																			
⊕ ≌理	IĦ																	obhorn Antina	dours	
◆ 正版	度权		共6条															成in VVIN 转到"设置"以	波GWS 激活 Wii	dows 1
and the second s																				

# 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 -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。

🧦 火绒终端安全管理系	统 V2.0.15.0			推索导航、模块名称 Q 11 🔗 🧔 admin 🗸					
<ul> <li>○ 首页</li> <li>□ 均減管理</li> <li>○ 案前時策略</li> <li>○ 案前時策略</li> <li>○ 案前時度</li> <li>○ 第一管理</li> <li>○</li> </ul>		域部署工具 V2.0.0.1 在地站环境下,域管理员可以向域用户强制推送全块火线转换会全软件 查看使用文档,快速了解如何实装部署登录脚本或开机脚本进行或部署 下點 使用文档	<b>L</b> ↑	高統升极工具 V2.0.9.3 当控制中心不能超越外网时,您可以通过直线升极工具更新控制中心以及补丁。 查看使用文档,快速了解动问使用角线升极工具进行高线升极 下框 使用文档					
	→	中心迁移工具 V2.0.2 当有终端需要迁移中心时,您可使用中心迁移工具。 将中心迁移工具传输至需要迁移中心的终端上进行,填写新中心地址,执行迁移操作。 下载	ð	移动存储注册工具 V2.0.3.9 注册U盘设备前必须先安装修动存储注册工具,若未安装此工具将无法对U盘进行注册 下载					
	Ø	火城安全山盤提売 V2.0.3.9 当用中保護所制除注册U島内的火城安全U島環保時; 忽可再次下載此環序, 并将程序拷贝至注册U島中, 即可继续使用注册U盒 下覧	3	专承工具 V10.0.96 科对查杀内病吸对抗类病毒 推得当火烧全量游异常显修复失败时使用 下账					
	0	SHA-2代码签名补丁修复工具 终端值件重整需要要。SHA-2件码签查支持,未安聚SHA-2件码签查补丁的终端两元法升级终端。 修复工具支持静就变得,静就实施运行参数:静就实施升重应运行参数:3r 下程		Windows检辑 V2.0.15.0 下电话用于Windows場件SKR的电户确 支持系统: Windows Server 2003 SP133&上版本 / Windows XP (SP3) / Windows Vista / Windows 7及 以上版本 下电 激活 Windows 转到"以量" 以激活 Windows,					
🗢 正版授权 📃	1								

# 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

🧭 配置工具			EN	— (			
中心网络设置 控制中心地址: <ul> <li>全部IP</li> <li>域名</li> </ul> HTTPS管理: 不启用安全证书	3 ● 默认安全证书	个中小 运行 数数 文付 他安全证书 密封	<mark>ン网络设置</mark> 呈协助端口 国库设置 牛存放 月与账号设置				
> 证书详情							
中心管理端口: 8080 终端部署端口: 6080							
☑ 通讯加密兼容低版本加	密算法						
远程协助端口 中心远程端口: 5901							
1 若需要切换中心模式, 请卸载中心后重新安装			保存		取消		
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#/log			
		<u>in</u> )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		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

#### 北京火绒网络科技有限公司

	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 序列号和密码激活接权,否则无法使用 合 产品安装部署手册 ① 产品使用手册	admin 登录控制中心输入 ① 安装包下载	۵	Linux版控制中心安装包V2.( 请安装火绒企业版后,输入序列 合产品安装部署手册 ① 产	) 号和密码激活接权,否则无法使用 ■ 品使用手册
	<b>高线升级包</b> 适用于内网环境进行升级 ① 安装包下载		Ţ	隔离网升级工具 适用于内网环境进行升级,仅支 「隔离网升级工具使用手册	持中心2.0.10.0及以上版本下载
ß	超管凭证 修改控制中心超级管理员密码时,需要上传此凭 下载后请尽快使用!(仅支持中心2.0.15.0及以上	证,此凭证具有有效期, 版本)			

## 2. 备用中心配置工具

💋 配置工具	简 — 🗆 🗙							
<b>备用中心状态</b> 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	<ul> <li>备用中心状态</li> <li>中心网络设置</li> <li>远程协助端口</li> <li>数据库设置</li> <li>文件存放</li> <li>密钥与账号设置</li> </ul>							
<b>主中心地址: https:// ~</b> 请输入主中心IP地址或域名 例: 6080								
<b>主中心密钥:</b> 请输入中心密钥								
中心网络设置 控制中心地址: <ul> <li>全部P</li> <li>域名</li> </ul>								
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								
	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	中心的配置工具	

### 3. 负载中心配置工具

💋 配置工具	₿ — □ ×
负载中心状态	
当前状态: 审核中	
Main center address: https:// > 请输入主中心IP地址或域名 化	
主中心密钥: HGJKNEKDSKFHedfhguhkds	
负载中心配置	
数据缓存目录: C:\Program Files (x86)\Huorong\ESCenter.crt	选择
HTTPS管理: 🦳 不启用安全证书 💦 默认安全证书 💿 其他安全证书	
	更换证书
> 证书详情	
中心管理端口: 8080	
① 若需要切换中心模式,请卸载中心后重新安装	关闭

	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。

<b>(</b> )	王 王 disk://\.\Physic	全盘扫描 alDrive0	2 已连接	中心 ロ II ー X 停止 <mark>暫停</mark>
Ŧ	常规 高速 □ 启用の	PU加速 🗌 查杀完成后自	动关机	已用时间: 00:00:01
කී	Ш	<b>P</b>	ල	
	引导区安全	系统进程 正在扫描…	<b>启动项</b> 等待扫描	
	ŵ	 ப	Ø	<b>本地磁盘</b> 等待扫描
	服务与驱动等待扫描	<b>系统组件</b> 等待扫描	<b>系统关键位置</b> 等待扫描	
≡				

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。

0			28 已连接中心	口 ::: 一 X 完成
(5)				
Ŧ				
Ý		-		
සී		$(\lambda)$		
00		$\bigcirc$		
ŏŏ				
		~		
	三 扫描对象:160个	Ű	总用时:00:00:32	
	\land 发现风险:0个	L L	处理风险:0个	
=				

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。

0	2 已连接中心		≡ - ×
G	□二 共发现风险项目15个,建议立即处理 ^会 □二 _{∃描已完成}	認略	立即处理
	☑ 风险项目	状态	
Ŧ	C:\Users\hmc\Desktop\\04e17a0595f35663b2c08e8d4cdf028e266f8b49 >> mjs.exe 蠕虫病毒 Worm/Qunsender.v	待处理	~ 详情
තී	C:\Users\hmc\Desk\0ad566339ed84407d399ba626534b0647684e401 >> [NSIS].nsi 广告程序 Adware/Downloader.bz	待处理	<mark>详情</mark>
	C:\Users\hmc\Desktop\新建文件夹\0d53d995a4e7d164660285921f8441d551461ae6 正告程序 Adware/Rising.a	待处理	详情
	C:\Users\hmc\Deskt\0d860049b42bc497817c2657a104debeed427754 >> [NSIS].nsi 广告程序 Adware/Widgi.c	待处理	详情
	C:\Users\hmc\Desktop\新建文件夹\0e34ace865cd5f328e7b68482c2cec692058ee43 广告程序 Adware/InstalleRex	待处理	详情
	<ul> <li>C:\Users\hmc\Desktop\新建文件夹\0e99df711b311fa2c99e97b6f653e8f491bfd512</li> <li>广告程序 Adware/Trickler.a</li> </ul>	待处理	详情
=			

## 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。

0			28 已连接中心	Q	≝ -	- ×
6)					75	
Ŧ						
කී		$\bigcirc$				
	三 扫描対象:28个	٩	总用时:00:00:01			
	⚠️ 发现风险:15个	Ľ	处理风险:15个			
=						

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。

<b>&gt;</b>	「」 正在进行快速把 C:\Windows\System32\dr	]描 ivers\HIDCLASS.SYS	2:33 日连接中心 □ □ □ × ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
Ŧ	常规 高速 同 启用GPU加速	🗌 查杀完成后自动关机	已用时间: 00:00:02
ക്	[L]	<b></b>	ල
88	引导区 _{安全}	系统进程 正在扫描…	启动项等待扫描
	ଚ	53	Q
	<b>米</b> 米 服务与驱动 等待扫描	系统组件 等待扫描	系统关键位置等待扫描
=			

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。

0	2 已连接中/	۵ D	≣	- ×
6)	火绒正在保护您的电脑			
Ŧ	<ul> <li></li></ul>			
කී	> □			
	>□ 桌面			
	确定 取消	查杀		
=	版本: V2.0.15.0 🚖 病毒库: 2024-11-14 11:39	R	漓区	信任区

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。

Ĩ	🤈 隔	离区					— c	ı ×	
	占用礷	盘空间: 681KB						Q	
		风险项	风险名称	隔离时间		分类	操作		
		mem://6700-0xb4aa2811-0x610000	Trojan/Rozena.i	2025-03-06 1	3:32	内存防护	×		
		mem://6700-0xb4aa2811-0x610000	Trojan/Rozena.i	2025-03-06 1	3:32	内存防护	×		
		C:\Users\hmc\Desktop\0afc6774628	Trojan/Injector.bfu	2025-03-06 1	0:42	文件实时监控	×		
						恢复隔离文件		8文件	

#### 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。

🥖 信	任区				- 🗆 X
	文件	网址			٩
	路径			~ ● 类型	
	C:\Users\gmz\Des	ctop∖模板.rp		文件	
	清除无效项			添加文件	添加文件夹

# 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。

0	防护中心		ຊ ເ	已连接中心 📮 🗄 — 🗙
2	查看、管理各项安全防护功能			
(5)	$\bigtriangledown$		稆	æ
Ŧ	病毒防御	>	系统防御	网络防御
ස	文件实时监控	-	针对计算机系统潜在弱点保	在网络层面拦截漏洞攻击、
₽Q	恶意行为监控	-	护,间时空制应用但手行 为,防止被恶意软件利用。	<u>崇</u> 奋入 <b>反</b> 等甘坝女王威励。
00	内存防护	- 8-		
	U盘保护 下载保护			
	邮件监控	_		
	Web扫描	-	4项 防护已开启	7项 防护已开启

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)。

0	防护中心	28日進	接中心 📮 🗄 — 🗙
	查看、管理各项安全防护功能		
9			4
FI I			9
♥ 1	6月二、日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	>	く 各防御 入 うれの うれの しんしょう しょうしょう
ස	^{文件实时}	<b>将新开中心策略同步</b>	]络层面拦截漏洞攻击、
	恶意行为 ( ) 新开中心策略	品步后终端将使用独立策略,如需恢复同	F八位等百以女王威彻。
äč	内存防护	這中重新升启策略同步。	
	U盘保护		-2
	下载保护	确定取消	
	邮件监控		
	Web扫描 C		
		4项 防护口升后	7. 奶护己开启
=			
田户占書		要面杳看及编辑当前防护设置	雪顶 (管理品如里开启了管

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。

💛 设置		- ¤ ×
段 常规设置	基础防护	
(+) 病毒防护		
品 系统防护	文件防护 注册表防护 敏感动作防护	
系统加固	☑ 启用内置过滤规则 ①	
应用加固		
软件安装拦截	自动防护	
摄像头保护	E	
浏览器保护		
⊕ 网络防护		
<b>①</b> 访问控制	智能防护	
	☑ 启用系统免疫 ①	
恢复默认设置		

## 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。

173 / 261



# 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。

🧔 设置			– 🗆 X
② 常规设置	□ 远程IP	~ 备注	
+ 病毒防护			
品 系统防护			
⊕ 网络防护			
☐ 访问控制			
IP协议控制			
IP黑名单		Æ	
联网控制			
网站内容控制		後すまれる副中国ニモニルングングの	
程序执行控制		芯·时冷加热则未被定相定IP功问开异仇	
设备控制			
恢复默认设置	编辑 删除 <b>导</b> 入 导出		添加规则

## 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。

🦪 设置			– = ×
② 常规设置	规则外程序联网		
: 病毒防护	◎ 允许联网	○ 阻止联网	
品 系统防护			
⊕ 网络防护	<ul> <li>日初成订审有数子並在</li> <li>目动放行系统核心程序</li> </ul>	ידי	
<b>①</b> 访问控制			
IP协议控制	联网控制规则		编辑 图绘规则 添加规则
IP黑名单	规则名称	> 规则类型	操作
联网控制			
网站内容控制			
程序执行控制			
设备控制			
		设置联网控制规则,管控软件联网行为	
恢复默认设置			

# 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)

🦪 设置				-		×
◎ 常规设置	网站内容控制					
① 病毒防御	◎ 黑名单					
品 系统防御	- 规则名称			< │ 状态		
⊕ 网络防御						
白 访问控制						
IP协议控制						
IP黑名单						
联网控制		Æ				
网站内容控制						
程序执行控制						
设备控制		暂无网站内	り容控制规则			
体复彩计设备						
秋发新从设置					添加网	斑

# 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。

🤣 设置			- = ×
② 常规设置	自定义规则	内置规则	
(土) 病毒防护	□ 规则名称	──────────────────────────────────────	操作
品 系统防护			
⊕ 网络防护			
<b>台</b> 访问控制			
IP协议控制			
IP黑名单			
联网控制			
网站内容控制			
程序执行控制		暂无程序执行控制规则	
设备控制			
恢复默认设置			添加程序

# 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。

🥠 设置				- • ×
◎ 常规设置	设置	设备控制白名单	设备受控列表	
(土)病毒防御	设备			状态
品 系统防御	U盘设备			• 禁止 ∨
④ 网络防御	便携设备 🛈			• 禁止 ~
<b>白</b> 访问控制	USB无线网卡			● 禁止 ∨
IP协议控制	USB有线网卡			● 禁止   ∨
IP黑名单	打印机			• 禁止 · ·
联网控制	元巡			• <u>兼止</u> · ·
网站内容控制	mA			
程序执行控制				
设备控制				
恢复默认设置				

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。
#### 北京火绒网络科技有限公司

<ul> <li>3</li> <li>3</li> <li>4</li> <li>4</li></ul>									- <u></u> -	×
礅	常规设置	设计	置	设备控	制白名单	设备受控	列表			
Ð	病毒防御	设备类型		设备名称	设备实例路径	连接状态	使用权限	使用期	操作	
88	系统防御	打印机		Microsoft IPP	SWD\PRINTENU	未连接	允许		申遭	
$\oplus$	网络防御	打印机			SWD\PRINTENU	已连接	禁止		申遺	
₫	访问控制	打印机		OneNote for	SWD\PRINTENU	已连接	禁止		<u> 申</u> 遺	
	IP协议控制	打印机		Microsoft XP	SWD\PRINTENU	已连接	禁止		申遣	
	IP黑名单	打印机		Microsoft Pri	SWD\PRINTENU	已连接	禁止		申遣	
	联网控制	光驱		NECVMWar V	SCSI\CDROM&V	已连接	禁止		申遣	
	网站内容控制									
	程序执行控制									
	设备控制									
	恢复默认设置									
	Address of Const	<								2
🕖 ផ្ល										×
ŝ	常规设置	设	置	设备招	制白名单	设备受控	列表			
Ð	病毒防御	设备类型		设备名称	- 设备实例路径	连接状态	使用权限	使用期	操作	
	系统防御	设备由清				>	Ŧ		申遣	
⊕	网络防御	の日子市	±तमाश्ची						申遺	
A	访问控制	设备名称:	Micros	oft IPP Class Driv	/er				申這	
	IP协议控制 设备	实例路径:	SWD\P	RINTENUM\WSE	)-51B286A2-D7F8-4	FB1-A8AC-DBFA7.			申遺	
	IP黑名单	申请权限:	允许						申遭	
	联网控制	申请说明:							申這	
	网站内容控制									
	程序执行控制									
	设备控制									
					根交目	1 取消				
					2.00					
8										
	恢复默认设置	<							-	

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。

0	安全工具		SR B连接中心 □ Ξ - X
	包含漏洞修复、系统修复等各项扩展	ĨĄ	
(4)	$\bigcirc$	×	
Ŧ	漏洞修复	系统修复	弹窗拦截
සී	6	舟	÷
88	启动项管理	垃圾清理	文件粉碎
	Ð	( <del>+</del> )	
	右键管理	断网修复	
_			
=			

# 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。

0		8 E	3连接中心 📮 🗄	- ×
9	🤣 终端信息		×	
Ŧ		本机 防护策略: 已同步 取消同步 终端隔离: 否 终端隔离		
සී		服务码: BJ06099943 ▶版本信息		
		版本: V2.0.15.0 病毒库: 2024-11-14 11:39		
		▶ 网络信息 IP地址: 172.20.1.92		
	28 已连接中心 主中心地址: 172.20.1.92:6080	MAC地址: 00-0C-29-17-A1-39		
			关闭	
=	版本: V2.0.15.0 🚖 病毒库: 2024-11-14	11:39	隋离区	信任区

# 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。

🤣 设置		- ¤ ×
<ul> <li>         · 常规设置         · 基础设置         · 通知设置         ·         ·         ·</li></ul>	快捷操作 ✓ 把"病毒扫描"加入右键菜单 □ 显示流量暴浮窗	Î
<ul> <li>查杀设置</li> <li>① 病毒防御</li> <li>□ 系統防御</li> <li>① 网络防御</li> </ul>	升级方式         ● 自动升级       ● 手动升级         自动升级时         □ 仅更新病毒库	
☐ 访问控制	扫描设置 自用GPU加速 ① 免打扰模式	
恢复默认设置	配色方案 〇 売  ③ 暗 信仟区保护	

## 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。

#### 北京火绒网络科技有限公司



#### 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。

🥖 信	任区				an a	- 🗆	×
	文件	网址					۹
	路径				类型		
	C:\Users\gmz\Des	ktop\模板.rp			文件		
	清除无效项				添加文件	添加文件	挟

## 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。

0				28 已连接中心 🛛 🖸		≡ —	×			
					2	◎ 安全设 	置			
(G)			左伊拉你的中脑			<ol> <li>安全日</li> <li>ラーテーク</li> </ol>	志			
(F)			3保护 20 大		Ľ		- 			
$\sim$					5	サ 店首交			) 181/AHPX	
ß					¢	う 检查更 。	新	麼	」 繁體中文 -	
	_					5 联系网	皆	EN	) English	
nô		$\overline{\mathbf{O}}$			[	3 终端登	5			
ŏŏ	=	<u></u>	L'J		(	〕 关于我	(1)			
	全	盘查杀	快速查杀	自定义查杀						
									-	
	版本: V2.0.15.0 🖕	病毒库: 2024-11-14 11:39			隔离区	信任				
=										

188 / 261

## 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。

0		
G	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	× 」
÷		
සී		
	hr hr	
	联系方式: 13142438/84 全型	自定义查杀
=	版本: V2.0.15.0 🚖 病毒库: 2024-11-14 11:39	隔离区 信任区

## 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。

<ul> <li>No.</li> </ul>		28 已连接中心	Q	≔	- >	×
	🤣 终端登记	×				
9	使用人*:					
Ŧ						
ස						
	版本: V2.0.	保存 取消	隔离		信任区	

190 / 261

## 3.6.9 关于我们

0		
G	火绒正在保护您的电	朋友
Ŧ	🏷 关于火绒	×
	火绒安全软件	
සී		
		Ē
	北京火绒网络科技有限公司版权所有 Conversiont © 2012-2024 Huserong All visibit record	uad 杏 ^文
	Copyright @ 2012 2024 Hidolong. An rights reser	veu. 旦水
	版本: V2.0.15.0 📤 病毒库: 2024-11-14 11:39	隔离区 信任区

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:

```
Iroot@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.
                  Create scan task.
  scan
     -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 config value. --get KevName: 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;</pre> 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-E8-98-DA Policy-Sync : Yes

] 26.72%

#### 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.

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

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

# 4.4 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

## 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@lo [root@lo success) [root@lo	calhost /]# cd /usr/local/huorong/bin calhost bin]# ./hrquarantine -r -i 5,10 6), ignored(0). calhost 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/laa602e29b01978617e5c1ceb4a219269c28a0b2	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/lba0e2b196f83ba1a5a7a07c24214f5f998af770	Name:OMacro/Downloader.aiy Time:2021-03-10 05:30:26 Reason:Anti-Virus
Id:27	Path:/home/test/test4/lbede09d10c13565da6aa242e6490e93b8f39bab	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/lel4bb6fblcl367al49cl8cb3745bcdf9dc4009c	Name:OMacro/Downloader.ck Time:2021-03-10 05:30:26 Reason:Anti-Virus
Id:31	Path:/home/test/test4/lef80cfcb14ef2231d5aaad5640dd80fef1f7d59	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 lae0190134d9d5d8021e8adc6cc9a2907e3ce7ef						
1 root root 37318 Mar 10 05:53 lafflede794458f2903492b1f9a348clalflclfc						
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。

[roota]	calhost /l# cd /usr/local/huorong/bin			
Trootal	calhost binl# ./hrouarantine -d -i 3			
success	1), ignored(0).			
[root@lo	calhost binl# ./hrouarantine -l			
Id:1	Path:/home/test/test3/02ac332f109b51acd815771021c9eca345d785ca	Name:Trojan/Generic!C360873A5B25651	Time:2021-03-10	05:30:21 Reason:Anti-Virus
Id:2	Path:/home/test/test3/04c25d330d335e728835576776a03a3382cbb832	Name:Trojan/Generic!C360873A5B25651	1 Time:2021-03-10	05:30:21 Reason:Anti-Virus
Id:4	Path:/home/test/test3/laa602e29b01978617e5c1ceb4a219269c28a0b2	Name:Virus/CTS.a Time:2021-0	3-10 05:30:21	Reason:Anti-Virus
Id:11	Path:/home/test/test3/3a2aeed92524504e32ecb35892ceb26c14148319	Name:Trojan/Generic!C360873A5B25651	Time:2021-03-10	05:30:21 Reason:Anti-Virus
Id:12	Path:/home/test/test3/3b637ab02e9aa5fe6780d1f221682721c134787b	Name:Virus/CTS.a Time:2021-0	3-10 05:30:22	Reason:Anti-Virus
Id:13	Path:/home/test/test3/3ccb0bb49008831f618a15e89e529bad410b165a	Name:Virus/Floxif.gen Time:2021-0	3-10 05:30:22	Reason:Anti-Virus
Id:14	Path:/home/test/test3/3d2a7568e2123284498bbb9d22fce3a456e75740	Name:Virus/CTS.a Time:2021-0	3-10 05:30:22	Reason:Anti-Virus
Id:15	Path:/home/test/test3/3faccc73f57a0037bfe277e2b4462bb51f490cfb	Name:Virus/Viking.jj Time:2021-0	3-10 05:30:23	Reason:Anti-Virus
Id:16	Path:/home/test/test3/5e5222b33c671abafc0618986293a8f934c5892a	Name:Virus/CTS.a Time:2021-0	3-10 05:30:23	Reason:Anti-Virus
Id:17	Path:/home/test/test3/5ea82455770a459edef513ec8a95f5c1848b2962	Name:Virus/CTS.a Time:2021-0	3-10 05:30:23	Reason:Anti-Virus
Id:18	Path:/home/test/test3/2fc7d96712607787099acd7e3d9dfe6dfc9e1e92	Name:Virus/Viking.a!dll Time	:2021-03-10 05:30:2	6 Reason: Anti-Virus
Id:19	Path:/home/test/test3/6eb0ea37cf0321fdba482584b2e4e1ff330286ff	Name:Virus/CTS.a Time:2021-0	3-10 05:30:26	Reason:Anti-Virus
Id:20	Path:/home/test/test4/0c3e0a545ba27aeadccfc18d2cffd46d64215764	Name:OMacro/Marker.s Time:2021-0	3-10 05:30:26	Reason:Anti-Virus
Id:21	Path:/home/test/test4/0c7994b245ee476ebb0a3bbc7bb1922b4c23744f	Name:OMacro/ShellHide.a Time	e:2021-03-10 05:30:2	6 Reason:Anti-Virus
Id:22	Path:/home/test/test4/0d5f98b56d4ba3b17a38b0d5430d6c9e918a5df0	Name:OMacro/Laroux.a Time:2021-0	3-10 05:30:26	Reason:Anti-Virus
Id:23	Path:/home/test/test4/0e143bf006dd06fc7ecc03b1f5dbeb2f3a06638a	Name:OMacro/Downloader.ya Time	e:2021-03-10 05:30:2	6 Reason:Anti-Virus
Id:24	Path:/home/test/test4/lald20e844f5f6e822708278ccd33d30d00556d1	Name:OMacro/Downloader Time	e:2021-03-10 05:30:2	6 Reason:Anti-Virus
Id:25	Path:/home/test/test4/1b934f1b9605561d113ee2a917719fc8d04dfd76	Name:OMacro/Agent.b Time:2021-0	3-10 05:30:26	Reason:Anti-Virus
Id:26	Path:/home/test/test4/1ba0e2b196f83ba1a5a7a07c24214f5f998af770	Name:OMacro/Downloader.aiy Time	e:2021-03-10 05:30:2	6 Reason:Anti-Virus
Id:27	Path:/home/test/test4/lbede09d10c13565da6aa242e6490e93b8f39bab	Name:OMacro/BlackIce Time:2021-0	3-10 05:30:26	Reason:Anti-Virus
Id:28	Path:/home/test/test4/1bfb11d279496e34bef63696a0afb9fac8981739	Name:HEUR:OMacro/WinA.d Time	e:2021-03-10 05:30:2	6 Reason: Anti-Virus
Id:29	Path:/home/test/test4/1c4b0f215e75a7ebaae85356849a4ff79849a996	Name:OMacro/Thus.a Time:2021-0	3-10 05:30:26	Reason:Anti-Virus
Id:30	Path:/home/test/test4/le14bb6fb1c1367a149c18cb3745bcdf9dc4009c	Name:OMacro/Downloader.ck Time	e:2021-03-10 05:30:2	6 Reason: Anti-Virus
Id:31	Path:/home/test/test4/lef80cfcb14ef2231d5aaad5640dd80fef1f7d59	Name:OMacro/Nsi.b Time:2021-0	3-10 05:30:26	Reason:Anti-Virus
Id:32	Path:/home/test/test4/lf93f5ccd35blf4bebfdc5318d24275a002ce3ff	Name:OMacro/Downloader.yb Time	e:2021-03-10 05:30:2	6 Reason:Anti-Virus
Id:33	Path:/home/test/test4/2dcc61336f03e9b21124a9645355dbf85f97a53c	Name:HEUR:OMacro/Obfuscated.c Time	e:2021-03-10 05:30:2	6 Reason:Anti-Virus

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。

```
[root@localhost /]# cd /usr/local/huorong/bin
[root@localhost bin]# ./hrquarantine -e -i 1 -p /home/test
success(1), ignored(0).
```

查看提取文件保存目录:

```
[root@localhost bin]# cd /home/test/
[root@localhost test]# ll
total 212
------. 1 root root 213025 Mar 10 06:07 02ac332f109b51acd815771021c9eca345d785ca
[root@localhost test]#
```

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@lo	ocalhost /]# cd /usr/local/huorong/bin					
[root@lo	ocalhost bin]# ./hrquarantine -l					
Id:1	Path:/home/test/test3/02ac332f109b51acd815771021c9eca345d785ca	Name:Trojan/Generic!C36	0873A5B256514	Time:2021-03-10	05:30:21	Reason:Anti-Virus
Id:2	Path:/home/test/test3/04c25d330d335e728835576776a03a3382cbb832	Name:Trojan/Generic!C36	0873A5B256514	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-Vir	us
Id:4	Path:/home/test/test3/laa602e29b01978617e5c1ceb4a219269c28a0b2	Name:Virus/CTS.a	Time:2021-03-10	05:30:21	Reason: Anti-Vir	us
Id:5	Path:/home/test/test3/lae0190134d9d5d8021e8adc6cc9a2907e3ce7ef	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/lafflede794458f2903492blf9a348clalflclfc	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-Vir	us
Id:9	Path:/home/test/test3/1f86423ec785d7a583d2b2b8727d26453bc522db	Name:Trojan/Generic!C36	0873A5B256514	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-Vir	us
Id:11	Path:/home/test/test3/3a2aeed92524504e32ecb35892ceb26c14148319	Name:Trojan/Generic!C36	0873A5B256514	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-Vir	us
Id:13	Path:/home/test/test3/3ccb0bb49008831f618a15e89e529bad410b165a	Name:Virus/Floxif.gen	Time:2021-03-10	05:30:22	Reason: Anti-Vir	us
Id:14	Path:/home/test/test3/3d2a7568e2123284498bbb9d22fce3a456e75740	Name:Virus/CTS.a	Time:2021-03-10	05:30:22	Reason: Anti-Vir	us
Id:15	Path:/home/test/test3/3faccc73f57a0037bfe277e2b4462bb51f490cfb	Name:Virus/Viking.jj	Time:2021-03-10	05:30:23	Reason: Anti-Vir	us
Id:16	Path:/home/test/test3/5e5222b33c671abafc0618986293a8f934c5892a	Name:Virus/CTS.a	Time:2021-03-10	05:30:23	Reason: Anti-Vir	us
Id:17	Path:/home/test/test3/5ea82455770a459edef513ec8a95f5c1848b2962	Name:Virus/CTS.a	Time:2021-03-10	05:30:23	Reason: Anti-Vir	us
Id:18	Path:/home/test/test3/2fc7d96712607787099acd7e3d9dfe6dfc9e1e92	Name:Virus/Viking.a!dll	Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:19	Path:/home/test/test3/6eb0ea37cf0321fdba482584b2e4e1ff330286ff	Name:Virus/CTS.a	Time:2021-03-10	05:30:26	Reason: Anti-Vir	us
Id:20	Path:/home/test/test4/0c3e0a545ba27aeadccfc18d2cffd46d64215764	Name:OMacro/Marker.s	Time:2021-03-10	05:30:26	Reason: Anti-Vir	us
Id:21	Path:/home/test/test4/0c7994b245ee476ebb0a3bbc7bb1922b4c23744f	Name:OMacro/ShellHide.a	Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:22	Path:/home/test/test4/0d5f98b56d4ba3b17a38b0d5430d6c9e918a5df0	Name:OMacro/Laroux.a	Time:2021-03-10	05:30:26	Reason: Anti-Vir	us
Id:23	Path:/home/test/test4/0e143bf006dd06fc7ecc03b1f5dbeb2f3a06638a	Name:OMacro/Downloader.	ya Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:24	Path:/home/test/test4/lald20e844f5f6e822708278ccd33d30d00556d1	Name:OMacro/Downloader	Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:25	Path:/home/test/test4/1b934f1b9605561d113ee2a917719fc8d04dfd76	Name:OMacro/Agent.b	Time:2021-03-10	05:30:26	Reason: Anti-Vir	us
Id:26	Path:/home/test/test4/lba0e2b196f83ba1a5a7a07c24214f5f998af770	Name:OMacro/Downloader.	aiy Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:27	Path:/home/test/test4/lbede09d10c13565da6aa242e6490e93b8f39bab	Name:OMacro/BlackIce	Time:2021-03-10	05:30:26	Reason:Anti-Vir	us
Id:28	Path:/home/test/test4/1bfb11d279496e34bef63696a0afb9fac8981739	Name:HEUR:OMacro/WinA.d	Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:29	Path:/home/test/test4/1c4b0f215e75a7ebaae85356849a4ff79849a996	Name:OMacro/Thus.a	Time:2021-03-10	05:30:26	Reason: Anti-Vir	us
Id:30	Path:/home/test/test4/lel4bb6fblcl367al49cl8cb3745bcdf9dc4009c	Name:OMacro/Downloader.	ck Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:31	Path:/home/test/test4/lef80cfcb14ef2231d5aaad5640dd80fef1f7d59	Name:OMacro/Nsi.b	Time:2021-03-10	05:30:26	Reason:Anti-Vir	us
Id:32	Path:/home/test/test4/lf93f5ccd35blf4bebfdc5318d24275a002ce3ff	Name:OMacro/Downloader.	yb Time:202	21-03-10 05:30:20	6 Reason:	Anti-Virus
Id:33	Path:/home/test/test4/2dcc61336f03e9b21124a9645355dbf85f97a53c	Name:HEUR:OMacro/Obfusc	ated.c Time:202	21-03-10 05:30:20	6 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
       hrguarantine -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:
       hrguarantine -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.
  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 Undate	Succeeded version: V2.0.8.0
have opened i	
ID:	2
Function:	Scan
Date:	2023-06-26 17:22:08
0 risk(s) de	tected during Quick Scan
ID:	3
Function:	Scan
Date:	2023-06-26 17:35:51
0 risk(s) de	tected during Quick Scan
TD:	4
Function:	Scan
Date:	2023-06-26 17:41:26
0 risk(s) de	tected during Quick Scan
ID:	5
Function:	scan
Date:	2023-06-27 14:17:41
0 risk(s) de	tected during Quick Scan
ID:	6
Function:	scan
Date:	2023-06-27 14:43:07
0 risk(s) de	tected during Quick Scan
ID:	7
Function:	scan
Date:	2023-06-27 14:47:00
0 risk(s) de	tected during Quick Scan
ID:	8
Function:	scan
Date:	2023-06-27 14:49:51
Press RETURN fo	or 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:				
Function:	Update			
Date:	2023-06-26 15:25:29			
Mode: Auto Upo	late			
Result: Succee	ded, version: V2.0.8.0			
Files download	led:			
2023-06-26 1	.5:25:28 /usr/local/huorong/share/xsse/libvxf.vdl			
2023-06-26 1	.5:25:28 /usr/local/huorong/share/xsse/libvxf.dat			
2023-06-26 1	.5:25:28 /usr/local/huorong/share/xsse/libvxf.tdl			
2023-06-26 1	.5:25:28 /usr/local/huorong/share/virdb/hwl.db			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/virdb/prop.db			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/virdb/pset.db			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/virdb/troj.db			
Files updated:				
2023-06-26 1	.5:25:29 /usr/local/huorong/share/xsse/libvxf.vdl			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/xsse/libvxf.dat			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/xsse/libvxf.tdl			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/virdb/hwl.db			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/virdb/prop.db			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/virdb/pset.db			
2023-06-26 1	.5:25:29 /usr/local/huorong/share/virdb/troj.db			
32.xc				
ID:	2			
Function:	scan			
Date:	2023-06-26 17:22:08			
Scan Type: Qui	Scan Type: Quick Scan			
Derth (100) 2023-00-08 18:10120				
Started at: 20	1/23-00-20 1/:21:49			
Duration: 00:0				
Ubject(s): 242	9			
File(s): 2403				
Inreat(s): 0				
Cleaned: 0				
TD •	3			
Function:	S C D C			
Date:	3-011 2003-06-26 17-35-51			
vace.	2023-00-20-11-33-31			
Scan Type: Oui	ck Scan			
Definition: 26	23-06-08 18:10:20			
Started at: 26	23-06-26 17:35:29			
Duration: 00:0				
Press RETURN for	more or FSC to quit.			
TED REFORM TO				

## 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 Upda	te Succeeded, version: V2.0.8.0		
TD:	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 RETUR	N for more, or ESC to quit.		
and the second second second second			

#### 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

10.	±	
Function:	Update	
Date:	2023-06	-26 15:25:29
Mode: Auto U	odate	
Result: Succ	eeded. ver	sion: V2.0.8.0
Files downlo	aded:	
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 update	d:	
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
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。

🦪 火绒安全 💈	28 已连接中心		₽ Ξ	- ×
	火绒 E	E在保护您的电脑 E保护 231 天		
	<u>=0</u>	[ <del>1</del> ]		
	全盘查杀	快速查杀	自定义查杀	
版本: V2.0.9.0 👌	病毒库: 2024-11-14 11:39		隔离区	信任区

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。

<ul> <li>火鐵豆全 28 已连接中心</li> <li>正在进行全盘扫描 /etc/hostapd/ifupdown.sh</li> </ul>		□ ≔ - × 停止 <mark>暂停</mark>
常规 高速 🗌 查杀完成后自动关机		己用时间: 00:00:03
<b>『</b> <b>系统设置</b> 正在扫描…	<b>系统进程</b> 等待扫描…	<b>に</b> 启动项 等待扫描…
<b>能务项</b> 等待扫描	定 常用软件 等待扫描…	<b>全部磁盘文件</b> 等待扫描

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。

		<u> </u>	≡ — ×
<u>=C</u>	大发现风险项目15个,建议立即处理	全部忽略	立即处理
	项目	状态	Î
	/home/hmc/.cache/vmware/drag_and_drop/ffjX4A/新建文件夹/2cdb2ce5195ada7b4987d6f0232ed63… 广告程序 Adware/RuKometa.b	待处理	详情
	/home/hmc/.cache/vmware/drag_and_drop/ffjX4A/新建文件夹/2ed3ee209a83d6582724d7af3da560… 广告程序 Adware/WebFlash	待处理	详情
	/home/hmc/.cache/vmware/drag_and_drop/ffjX4A/新建文件夹/1dae85573646e58711ba17e116dcc7… 广告程序 Adware/OutBrowse.n	待处理	详情
	/home/hmc/.cache/vmware/drag_and_drop/ffjX4A/新建文件夹/0e99df711b311fa2c99e97b6f653e8f4… 广告程序 Adware/Trickler.a	待处理	详情
	/home/hmc/.cache/vmware/drag_and_drop/ffjX4A/新建文件夹/0d53d995a4e7d164660285921f8441… 广告程序 Adware/Rising.a	待处理	详情
	/home/hmc/.cache/vmware/drag_and_drop/ffjX4A/新建文件夹/1c9be7d76c98fc64ef62e24457cab5dd… 广告程序 Adware/JS.MultiPlug.b	待处理	详情

#### 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。

汉 火绒豆	<b>全</b> 22 已连接中心				Q	∷≘	<u></u>	×
<u>=0</u>	所有风险功	顶处理完成 ◎					完成	
	E	扫描对象:5478个	0	总用时:00:00:48				
	${\mathbb A}$	发现风险:15个	≌	处理风险:15个				

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。

🔊 火绒安全 😂	2 已连接中心		□ = - ×
	火结	<b>绒正在保护您的电脑</b> 已保护 231 天	
	<u>=0</u>	[4]	
	全盘查杀	快速查杀	自定义查杀
<b>版本: V2.0.9.0</b>	病毒库: 2024-11-14 11:39		隔离区 信任区

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。

🤣 火绒安全 🙁 已连接中心	<b>□</b> = - ×
火绒正在保护您的电脑	
○ 请选择扫描路径 ×	
> [] 🚞 dev > [] 🚔 etc	
→ □ = nome → □ = lib → □ = lib32	Ξ
> [] = lib64 . [] = libc22 *	( <b>*</b> X
全 3 □ 显示隐藏项	、鱼尔
版本: V2.0.9.0 🖕 病毒库: 2024-11-14 11:39	隔离区信任区
汐 <b>火绒安全</b> 🛛 8 已连接中心	<b>□</b> := - ×
日二 正在进行自定义扫描	停止 暂停
/boot/grub/i386-pc/regexp.mod	
	已用时间: 00:00:02
	<b>秋念</b>
/boot	正在扫描
/dev	等待扫描

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。

👩 隔1	新区				- 1	3	×
占用職員	皇空间: 140.8MB					٩	
	文件器径 +	病毒名称	隔离时间	分类	操作		İ.
	/home/tir-test/桌面/20M以上 zip	Trojan/Generic/8F138D184831…	2021-11-19 16:08	病毒查杀			
	/home/hr-test/皇面/31M.zip	Trojan/Generic18F138D184831	2021-11-19 16:08	病毒素质			
	/home/hr-test/桌面/31M/028cc9…	Trojan/Generic18F138D184831····	2021/11/19 16:08	病现意外			
	/home/hr-test/桌面/31M/430/922	Trojan/Injector.wl	2021-11-19 16:08	病毒查杀			
	/home/hr-test/皇王/31M/615332	Worm/PowerShell.DTStealer	2021-11-19 16:05	病毒重杀			
	/home/hr-test/桌面/31M/764117…	Trojan/Generic/F48039273A4C9···	2021-11-19 16:07	病毒查杀			
	/home/hr-test/皇面/31M/77d5e9…	Worm/DTStealer.c	2021-11-19 16:08	病毒查杀	×		
	/home/hr-test/皇世/31M/85d3a8…	TrojanDropper/PS.Maloader.c	2021-11-19 16:08	的母童杀			
	/home/hr-test/桌面/31M/a63d16	Trojan/Generic1559C62825C87	2021-11-19 16:08	病毒查杀			
	/home/hr-test/桌面/31M/b3fea7b	HVM:Trojan/Deceiver.gen1A	2021-11-19 16:08	病毒素杀			
				恢复隔离文件		04.Xł	

#### 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。

0	信	1区		8	- 0	×
						a
i.		信任項目	项目类型		操作	
6		/data/home/zzb/桌面/20M以下/e0bf3066f06fef0cc7aff20b6dc3655a40354e64	文件			
		/data/home/zzb/桌面/20M以下/e2ae9db2b5bdddb8fb6196a4836a6912397fe4a4	文件		×	
1		/data/home/zzb/桌面/20M以下/eb11ce2791afc942001a2dfc5e6e03ad12859475	文件			
8		/data/home/zzb/卓面/20M以下/fk13c2ac50091045do0282511488d2f7597dc2b8	文件		×	
8						
Ę.						
l.						
э	90:	清除无效项		添加文件	添加文件	夾

# 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。

🍠 火绒安全 😂 已连接中心		□ :: - ×
🦪 终端信息		×
	<ul> <li>hmc-PC</li> <li>防护策略: こ同步 取消同步</li> <li>服务码: BJ06099943</li> <li>● 版本信息</li> <li>版本: V2.0.9.0</li> <li>病毒库: 2024-11-14 11:39</li> <li>● 网络信息</li> <li>IP地址: 172.20.1.95</li> <li>MAC地址: 00-0C-29-BB-6C-CC</li> <li>● 连接信息</li> <li>主中心地址: 172.20.1.92</li> </ul>	
		关闭
版本: V2.0.9.0 🚖 病毒库: 2024-11-14 11:39		隔离区  信任区

# 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				×
⑥ 基础配置	升级方式			
<ul> <li>(+) 病毒查杀</li> </ul>	◎ 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 ①			
	□ 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				×
改置     资 基础配置	发现病毒时			×
<ul> <li>         ・ジ          ・ 送          ・ 送          ・ 送</li></ul>	<b>发现病毒时</b> <ul> <li>         • 询问我         •         •         •</li></ul>	〇 自动处理		×
<ul> <li></li></ul>	<b>发现病毒时</b> <ul> <li>询问我</li> <li>清除病毒时</li> </ul>	〇 自动处理		×
<ul> <li>&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt;</li></ul>	<b>发现病毒时</b> <ul> <li>         ・ 询问我         </li> <li>              前除病毒时      </li> <li>             将病毒文件备份至隔离区         </li> </ul>	〇 自动处理		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>◆ 病毒查杀</li> <li>⑦ 文件实时监控</li> </ul>	<ul> <li>发现病毒时</li> <li>● 询问我</li> <li>清除病毒时</li> <li>✓ 将病毒文件备份至隔离区</li> </ul>	〇 自动处理		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>● 病毒查杀</li> <li>⑦ 文件实时监控</li> </ul>	<ul> <li>发现病毒时</li> <li>④ 询问我</li> <li>清除病毒时</li> <li>水病毒文件备份至隔离区</li> <li>全盘查杀设置</li> <li>· 深度查杀压缩包中的病毒木马,并自动</li> </ul>	○ 自动处理 跳过大于 20 MB的压缩包(20M~9999M)		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>① 病毒查杀</li> <li>③ 文件实时监控</li> </ul>	<ul> <li>发现病毒时</li> <li> ● 询问我 </li> <li>清除病毒时 ✓ 将病毒文件备份至隔离区 </li> <li>全盘查杀设置 ✓ 深度查杀压缩包中的病毒木马,并自动器 提示:自定义扫描将自动扫描压缩包,并不要</li></ul>	○ 自动处理 跳过大于 20 MB的压缩包(20M~9999M) 段以上大小限制		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>① 病毒查杀</li> <li>③ 文件实时监控</li> </ul>	<ul> <li>次現病毒时</li> <li>● 询问我</li> <li>清除病毒时</li> <li>✓ 将病毒文件备份至隔离区</li> <li>全盘查杀设置</li> <li>✓ 深度查杀压缩包中的病毒木马,并自磷超提示:自定义扫描将自动扫描压缩包,并不受</li> <li>□ 不扫描 → 指定扩展名文件</li> </ul>	<ul> <li>自动处理</li> <li>跳过大于 20 MB的压缩包(20M~9999M)</li> <li>战以上大小限制</li> </ul>		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>◆ 病毒查杀</li> <li>→ 文件实时监控</li> </ul>	通回我                  適回我                 清除病毒时                 水病毒文件备份至隔离区                 全盘查杀设置                 梁度查杀压缩包中的病毒木马,并自动提提示:自定义扫描将自动扫描压缩包,并不受                 不扫描                 不扫描                 日満岡蜂驱动器	<ul> <li>自动处理</li> <li>跳过大于 20 MB的压缩包(20M~9999M)</li> <li>战以上大小限制</li> </ul>		×
<ul> <li>◇ 送础配置</li> <li>◆ 病毒查杀</li> <li>· 方本</li> <li>· 文件实时监控</li> </ul>	<ul> <li>发现病毒时</li> <li>● 询问我</li> <li>清除病毒时</li> <li>✓ 将病毒文件备份至隔离区</li> <li>全盘查杀设置</li> <li>✓ 深度查杀压缩包中的病毒木马,并自动强度示:自定义扫描将自动扫描压缩包,并不受□ 不扫描 ∨ 指定扩展名文件</li> <li>□ 打描网络驱动器</li> </ul>	<ul> <li>自动处理</li> <li>跳过大于 20 MB的压缩包(20M~9999M)</li> <li>默让上大小限制</li> </ul>		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>● 病毒查杀</li> <li>&gt; 文件实时监控</li> </ul>	通回我                  通回我                 清除病毒时                 米病毒文件备份至隔离区                 全盘查杀设置                 梁度查杀压缩包中的病毒木马、并自动提提示:自定义扫描将自动扫描压缩包、并不受                 不扫描             《             指定扩展名文件                 日相网络驱动器	<ul> <li>自动处理</li> <li>跳过大于 20 MB的压缩包(20M~9999M)</li> <li>战以上大小限制</li> </ul>		×
<ul> <li>◇</li></ul>		<ul> <li>自动处理</li> <li>跳过大于 20 MB的压缩包(20M~9999M)</li> <li>毁以上大小限制</li> </ul>		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>● 病毒查杀</li> <li>&gt; 文件实时监控</li> </ul>	发现病毒时         ④ 询问我         清除病毒可         ③ 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、并自动加速器:         世示白莲、少扫描将自动扫描压缩包、并不受         一 不扫描 ~ 指定扩展名文件         一 扫描网络驱动器	<ul> <li>自动处理</li> <li>跳过大于 20 MB的压缩包(20M~9999M)</li> <li>致以上大小限制</li> </ul>		×
<ul> <li>◇ 设置</li> <li>◇ 基础配置</li> <li>● 病毒查杀</li> <li>⑦ 文件实时监控</li> </ul>	<ul> <li>发现病毒时</li> <li>● 询问我</li> <li>清除病毒可</li> <li>▼ 将病毒文件备份至隔离区</li> <li>全盘查杀设置</li> <li>マ 深度查杀压缩包中的病毒木马,并自动症 提示:自定义扫描将自动扫描压缩包,并不受</li> <li>□ 不扫描 ∨ 指定扩展名文件</li> <li>□ 扫描网络驱动器</li> </ul>	<ul> <li>自动处理</li> <li>跳过大于 20 MB的压缩包(20M~9999M)</li> <li>段以上大小限制</li> </ul>		×

🦪 设置		– 🗆 🗙
诊 基础配置	是否开启文件实时监控	
(+) 病毒查杀	扫描时机	
定 文件实时监控	<ul> <li>✓ 文件修改完成后扫描</li> <li>✓ 文件读取时扫描</li> <li>□ 文件执行时扫描 (当前系统不支持)</li> </ul>	
	<b>扫描文件时</b> □ 不扫描指定路径文件 管理路径	
	<b>发现病毒时</b> ○ 弹窗提示终端自主选择   ○ 自动处理   ● 仅记录	
	<b>清除病毒时</b> ✔ 将病毒文件备份至隔离区	
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。

2	> 安全日志		- 🗆 X
	时间: 2024/11/19 — 2024/11/19 日 全部 🗸 全部	~ 概要	
d	刷新 项目数: 0	清除本页日志	导出本页日志

#### 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。

👩 隔詞	海区				– 🗆 X
占用磁盘	監空间: 6.2MB				Q
	文件路径		病毒名称	隔离时间	操作
	/home/test/桌面/已处理	删除文…	Adware/Firseria.a	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	Backdoor/MSIL.Bladabindi.i	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	Bootkit/Voluminer.a	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	Constructor/Moothie.a	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	Exploit/JS.Pdfka.a	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	HackTool/Potato	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	Joke/Agent.c	2022-09-19 17:15	
	/home/test/桌面/已处理	,删除文…	OMacro/Win32.Relax.a	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	Ransom/JS.CryptoRaa	2022-09-19 17:15	×
	/home/test/桌面/已处理	,删除文…	Rogue/Winwebsec.k	2022-09-19 17:15	×
				恢复隔离文件	提取隔离文件

### 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。

🤣 信任区		- 🗆 X
		٩
□ 信任项目	∧ 项目类型	操作
/home/hmc/Desktop/uos-service-support.desktop	文件	×
剰除 清除无效项	添加	文件 添加文件夹

## 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。

🔗 火ダ安全 😪 己连接中心			₽ ≞	- ×
	🤣 网管信息	×		
Ē	hr 联系方式:13512451421			
全盘查;	杀		自定义查杀	
版本: V2.0.9.0 ▲ 病毒库:	2024-11-14 11:39		隔离区	信任区

#### 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。



# 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。

•	打开您的"	<b>完</b> 名 系统偏好设置",进行: 安全	全磁盘访问权降 身份验证并在"完全程 含端以及相关组件。	<mark>艮</mark> ^{磁盘访问权限"列表[,]}	中选择火绒
			安全性与隐私	Q提業	
			刮 文件保险箱 防火墙 <mark>隐私</mark>		
		<ul> <li>補助功能</li> <li>輸入监视</li> </ul>	允许以下App访问诸如"邮件 器、"家庭"、时间机器备份, 部分管理设置等数据。	"、"信息"、Safari 浏览 以及此 Mac 上所有用户的	
		完全磁盘访问权限	2 火城安全终端		
		文件和文件夹	Cn.huorong.Hips		
		<b>读</b> 自动化			
		₩ 开发者工具			
		15改进			
	(	按钮以进行更改。			
			前往"安全性与隐私"		

#### 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。

•••		已连接中心 🖵 呂
この 正在进行全盘扫描		停止 暂停
/System/Library/ExtensionKit/Ext	ensions/AccessibilitySetsion.appex/Contents/Mac	oOS/AccessibilitySettingsExtension
常规 高速 🗌 查杀完成后自动关机		已用时间: 00:00:01
<b>系统进程</b> 扫描中	↓ 启动项	
<b>そう</b> 服务项	常用软件	全部磁盘

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。

						已连接中心	Ţ	8
ĒQ	本次扫描未发现 _{扫描已完成}	!风险					完成	
			_					
			$\langle \rangle$					
				\$				
	E	扫描对象: 111个		0	总用时:00:00:12			
		发现风险:0个		$\mathbb{M}$	处理风险:0个			

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。

•••		₿.	已连接中心	₽	8
			全部忽略	立即处理	
2	风险项目		状态		
2	/Users/huoronganquan/Desktop/未命名文件夹/0d53d995a4e7d16466028 <b>广告程序</b> Adware/Rising.a	85921f8441d551461ae6	待处理	详情	
	/Users/huoronganquan/Desktop/未命名文件夹/0ad566339ed84407d399 <b>广告程序</b> Adware/Downloader.bz	ba626534b0647684e401 >> [NSIS].n:	si 待处理	详情	
•	/Users/huoronganquan/Desktop/未命名文件夹/1dae85573646e58711ba17 <b>广告程序</b> Adware/OutBrowse.n	7e116dcc7d7c910ce02 >> [NSIS].nsi	待处理	详情	
	/Users/huoronganquan/Desktop/未命名文件夹/1c9be7d76c98fc64ef62eź <b>广告程序</b> Adware/JS.MultiPlug.b	24457cab5ddcaada7cb	待处理	详情	
•	/Users/huoronganquan/Desktop/未命名文件夹/0e34ace865cd5f328e7b6 <b>广告程序</b> Adware/InstalleRex	8482c2cec692058ee43	待处理	详情	
•	/Users/huoronganquan/Desktop/未命名文件夹/1ff4499c5d27909f09a4bf 广告程序 Adware/AlteredSoftware.a	9f2dfbc540febe3cff	待处理	详情	

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。

●●● 「「」」 「」」 「」」 「」」 「」」 「」」 「」」	已连接中心 🖵 呂 🔓
	$\geq$
三   扫描対象: 8个	① 总用时: 00:00:01
⚠️ 发现风险:6个	▶ 处理风险:6个

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。

•••		この こ
「 して して して して して して した 进行快速 扫描 (usr/libexec/searchpartyuseragent		停止暂停
常规 高速 🗋 查杀完成后自动关机		已用时间: 00:00:01
系统进程 扫描中 服条项 服条项	高动项	关键位置文件

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。

<b>又</b> 火绒安全终端需要安装"系统	<b>系统扩展程序安装</b> 扩展",请打开"设置"–"安全性与隐私"进行配置。
<ul> <li>① ② 沒來</li> <li>② :衍与聚焦</li> <li>② :衍与聚焦</li> <li>② 》 Sin与聚焦</li> <li>② 》 Sin与聚焦</li> <li>③ 》 题示器</li> <li>③ 還示器</li> <li>③ 還承紙</li> <li>③ 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一</li></ul>	<ul> <li>         Apple」         <ul> <li>Apple」</li></ul></li></ul>
	前往"安全性与隐私"

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。

•••		₿.	隔离区	Q, 搜索	
		文件路径 个	病毒名称	隔离时间	操作
		/Users/huoronganquan/Desd399ba626534b0647684e401	Adware/Downloader.bz	2024–12–03 16:42	×
		/Users/huoronganquan/Desk4660285921f8441d551461ae6	Adware/Rising.a	2024–12–03 16:42	×
		/Users/huoronganquan/Des8e7b68482c2cec692058ee43	Adware/InstalleRex	2024–12–03 16:42	×
		/Users/huoronganquan/Desef62e24457cab5ddcaada7cb	Adware/JS.MultiPlug.b	2024–12–03 16:42	×
		/Users/huoronganquan/Desk711ba17e116dcc7d7c910ce02	Adware/OutBrowse.n	2024–12–03 16:42	×
		/Users/huoronganquan/Deskt9f09a4bf9f2dfbc540febe3cff	Adware/AlteredSoftware.a	2024–12–03 16:42	×
		/Users/huoronganquan/Des24e1f50362adb97cde43268d	HEUR:TrojanDownloader/Agent.bf	2024–11–19 17:37	×
		/Users/huoronganquan/Desdc93d8582673f98d9bbf77d0	Trojan/Agent.bgk	2024–11–19 17:37	×
		/Users/huoronganquan/Desk8518c7693b68de9ed9afddfdf	TrojanDownloader/MSIL.Agent.sc	2024–11–19 17:37	×
		/Users/huoronganquan/Des8a94b260087a37ef070dfe73	Trojan/Injector.bfu	2024–11–19 17:37	×
		/Users/huoronganquan/Desktee5fffff4eb728c11b9ab37149	TrojanDownloader/Maloader.l	2024–11–19 17:37	×
		/Users/huoronganquan/Deskd8b6a92ce1ec75df34f863279	TrojanSpy/MSIL.AgentTesla.mq	2024–11–19 17:37	×
					恢复 提取

#### 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)不会被病毒查杀功能扫描。信任区支持增加文件、文件夹进行信任,同时支持对已信任的文件取消信任。
#### 北京火绒网络科技有限公司

•	••		信任区			Q 搜索		
		信任项目				项目类型	操作	
		/Users/huoronganquan/Pictures/Camera Roll/				文件夹	×	
		/Users/huoronganquan/Pictures/ImageOptim/				文件夹	×	
		/Users/huoronganquan/Pictures/Photo Booth图库/				文件夹	×	
		/Users/huoronganquan/Pictures/照片图库.photoslibrary/				文件夹	×	
				N				
				45				
							添加	

### 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。



255 / 261

## 6.3.1 关于我们

				已连接中心	Ţ	8
	ľ	火绒安全软件				
		版本号:V2.0.8.0				
	<b>—</b>	北京火绒网络科技有限公司版权所有	=			
	Copyri	ght©2012–2024 Huorong.All rights reserved.				
	全世间世	1411111111111111	日正又杳杀			
	王丽回八	八座三八				
版本: V2.0.8.0 🖕 病	病毒库: 2024-11-14 11:39	)		隔离区	信任	X

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。

#### 北京火绒网络科技有限公司

•	• •				安全日志				
	时间	2024/12/03 —	- 2024/12/03 📋	类别 全部		功能	全部 🗸		
	时间		类别		功能		概要		
	2024–12	2–03 16:44:16	病毒防御		病毒查杀		自定义扫描,发现0个风险项	页目	
	2024–12	2–03 16:43:37	病毒防御		病毒查杀		自定义扫描,发现0个风险项	页目	
	2024–12	2–03 16:43:19	病毒防御		病毒查杀		自定义扫描,发现0个风险项	瓦目	
	2024–12	2–03 16:43:13	病毒防御		病毒查杀		自定义扫描,发现0个风险项	瓦目	
	2024–12	2–03 16:42:51	病毒防御		病毒查杀		快速扫描,发现0个风险项目	3	
		2_03 16:42:23	病畫防御		病畫杏杀		白完ツ扫描 労和6个风险の	<b>T</b> E	
	病毒阵时间的人物。 有一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次	间: 2024–11–14 11: ]: 2024–12–03 16:4 f: 00:00:29 k: 770 ∹ 30 注: 0  险: 0	39 13						
Ú	刷新						清除本页	[日志 导出本页	印志

### 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
	☆      ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆
升级方式:	<ul><li>○ 自动升级</li><li>○ 手动升级</li></ul>
自动升级时:	○ 仅升级病毒库
安全日志保护:	日志保存 30 天 ①
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

	· · · · · · · · · · · · · · · · · · ·					
	☆      ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆					
发现病毒时:	<ul> <li>询问我</li> <li>自动处理</li> </ul>					
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 (20M~9999M)						
	□ 不扫描 ✓ 指定扩展名文件 例如: .tmp; .bd; .log; .db					
	○ 扫描网络驱动器					
	恢复默认设置					

•	•			设置			
		⊆ 基础ì	〕 <b>殳置</b>	(分) 病毒查杀	□ 文件实时监控		
是	書开启文件实	6时监控 🦲					
ŧ	]描时机:	<ul> <li>文件修改完成后</li> <li>文件读取时扫描</li> <li>文件执行时扫描</li> </ul>	扫描				
Ē	]描文件时:	○ 不扫描指定路径	文件	管理路径			
发	<b>〔现病毒时</b> :	○ 弹窗提示终端自 ○ 仅记录 ○ 自动处理	主选择				
清	<b>请除病毒</b> 时:	✓ 将病毒文件备份	至隔离区	ζ		恢复默认设置	