火绒终端安全管理系统
1.0 版

产品说明书

版权声明

北京火绒网络科技有限公司

地　　址：北京市朝阳区红军营南路 15 号瑞普大厦 B 座 1201 室

网　　址：http://www.huorong.cn

技术支持：010-84905882

目录

1.概述

欢迎阅读《“火绒终端安全管理系统 1.0”产品说明书》。为了能够更好的服务于用户，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控制中心的使用方法。

“火绒终端安全管理系统 1.0”是秉承“情报驱动安全”新理念，全面实施 EDR 运营体系的新一代企事业单位反病毒&终端安全软件。本产品能帮助用户完成终端安全软件的统一部署、全网管控，集强大的终端防护能力和丰富方便的全网管控功能于一体，性能卓越、轻巧干净，可以充分满足企事业单位用户在目前互联网威胁环境下的电脑终端防护需求。

“火绒终端安全管理系统 1.0”产品优势及特点：

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，强悍轻巧干净。火绒终端产品稳定成熟，运营和服务经验丰富，已拥有数百万用户。其独有的基于虚拟沙盒的新一代反病毒引擎及多层次主动防御系统，可确保对各种恶意软件的彻底查杀和严密防御。安装后占用资源少，日常内存占用不到 10M，平常使用中，几乎感觉不到火绒的存在。同时坚决恪守安全厂商的基本操守，没有任何捆绑、弹窗、侵占资源等行为，并强力狙杀各种流氓软件、商业软件的侵权行为。

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 1.0”的控制中心设计合理，拥有友好的界面、人性化的统计报表，安全管理信息和日志一目了然，能极大的提高安全管理效率。

Tips:

- 如果您想了解“火绒终端安全管理系统 1.0”核心技术及理念策略，请参阅《“火绒终端安全管理系统 1.0”技术白皮书》。
- 如果您是初次体验“火绒终端安全管理系统 1.0”，想要快速了解使用方法及操作流程，请参阅《“火绒终端安全管理系统 1.0”使用手册》。
- 如果您想了解“火绒终端安全管理系统 1.0”的安装需知和部署流程，请参阅《“火绒终端安全管理系统 1.0”安装部署手册》。

2.火绒安全控制中心

2.1.打开控制中心

安装结束后，将会在桌面创建一个快捷方式

双击即可打开控制中心网页

或者输入终端部署地址（IP 或者域名）也可进入

2.2.登录控制中心

a. 部署火绒安全终端

第一步：直接双击快捷方式打开网页

第二步：输入账号密码即可登录

b. 部署在火绒控制中心的终端

第一步：打开 IE 浏览器

第二步：地址栏输入地址：http：//[控制中心所在 IP 地址或者域名]：[端口号]

第三步：输入账号密码即可登录

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，将会登出

2.3. 退出控制中心

➢ 通过控制中心的右上角悬停头像上后出现的【退出登录】按钮退出

2.4. 修改登录密码

2.4.1. 忘记密码

1. 首先打开配置工具

开始菜单 -所有程序 -火绒终端安全管理系统-火绒终端安全管理系统配置工具

2.填写超级管理员密码并且确认，其他配置不修改即可

注：该配置工具只安装在装有火绒控制中心的终端上，无需密码即可打开

2.4.2. 未忘记密码

通过控制中心的右上角悬停头像上后出现的【修改密码】，输入原密码并且确认新密码，附带有密码强度的检测。

2.5. 修改中心部署地址

开始菜单 -所有程序 -火绒终端安全管理系统-火绒终端安全管理系统配置工具

修改终端部署地址以及端口。**已经安装客户端的终端需要重新下载，覆盖安装**

2.6. 中心授权

如图所示表明火绒终端安全管理系统未授权，点击未授权，展示授权信息页面，导入授权证书，即可更新到正式版。

授权快到期 15 天之后，会有弹窗提醒更新授权。

注：

正式版：正式授权到期后，版本以及病毒库不可升级

试用版：试用授权到期后，版本以及病毒库不可升级外，只可以连接 10 台终端

2.7. 更新升级

2.7.1. 手动升级

通过点击控制中心的右上角最左侧的升级按钮进行升级检测以及手动升级

2.7.2. 自动升级

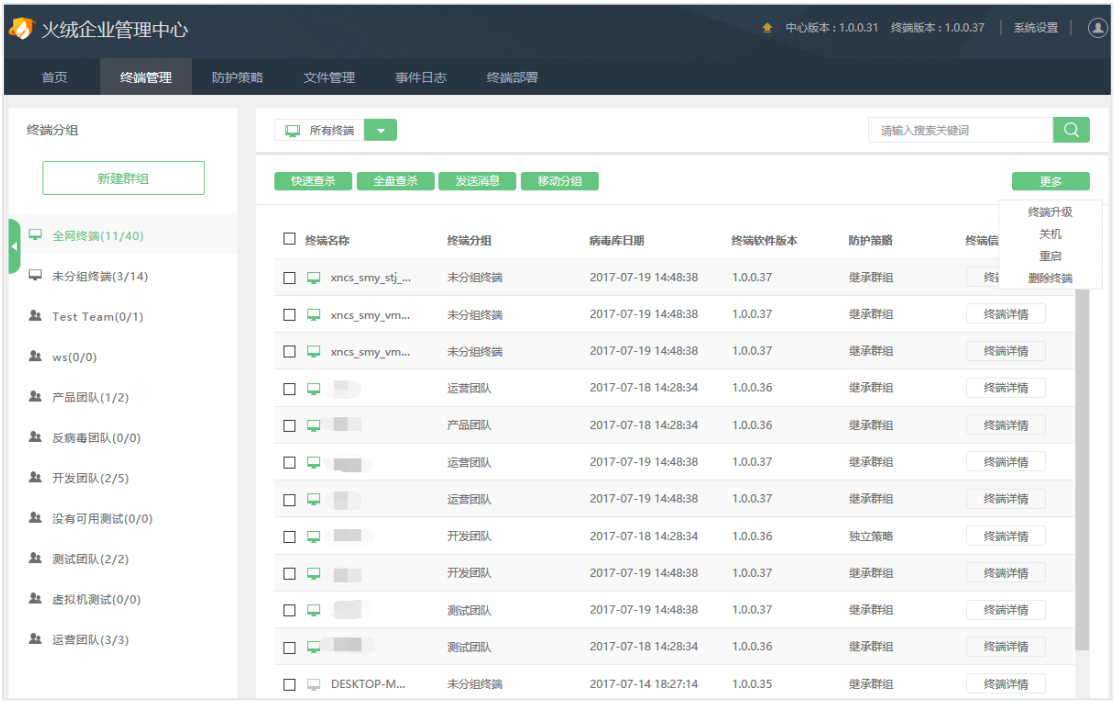
控制中心默认升级方式为自动升级，中心将会在每次进入时自动进行升级检测。

2.7.3. 离线升级包

考虑到单位内部控制中心服务器可能没有连接外网，所以无法进行在线升级。火绒为此准备了离线升级工具包，用于外网下载数据，内网离线升级版本。

2.8. 终端管理

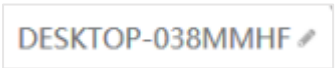
终端安装完火绒安全终端后，终端将会自动与中心通讯，并且终端的信息将会展示到中心的【终端管理】模块。管理员可以通过火绒控制中心对全网终端实施快速查杀、全盘查杀、发送消息、移动分组、终端升级、关机重启、删除终端等操作进行管理，安全防护。如图



2.8.1. 终端详情

点击任意终端的终端名称即可查看包括网络信息、环境信息以及其它信息等终端详情

2.8.2. 修改终端名称



终端名称默认为计算机名，可以点击编辑按钮进行修改，为空时自动恢复为修改

前名称

2.8.3. 新增分组

点击【新建分组】，输入分组名称即可

2.8.4. 分组管理

分组管理包括 IP 接入规则以及名称接入规则。可以根据相应的规则将接入的终端划分进入分组。

操作方法：点击【添加】，填写 IP 范围或者是终端名称（支持通配符），选择需要划分的分组，点击【确定】

2.8.5. 编辑/删除分组

鼠标移入分组名称所在位置后，编辑删除按钮显示后操作即可。

2.8.6. 快速查杀

快速地对病毒文件通常会感染电脑系统敏感位置进行查杀

操作方法：选择需要快速查杀的终端，点击【快速查杀】功能按钮即可

操作说明：可以点击设置按钮修改快速查杀配置，任务将在 10 秒内响应 

2.8.7. 全盘查杀

对计算机所有磁盘位置进行病毒扫描以及查杀

操作方法：选择需要全盘的终端，点击【全盘查杀】功能按钮即可

操作说明：可以点击设置按钮修改全盘查杀配置，任务将在 10 秒内响应 

2.8.8. 发送消息

选择终端，点击【发送消息】，填写消息内容，最后【确定】发送；终端将在 10 秒内响应

2.8.9. 移动分组

选择终端，点击【移动分组】，选择需要移动到的分组，最后【确定】即可；终端将在 10 秒内响应

2.8.10. 终端升级

选择终端，点击【终端升级】，确定需要升级的终端，最后【确定】即可；终端将在 10 秒内响应

2.8.11. 关机重启

选择终端，点击【关机】、【重启】，确定需要关机、重启的终端，最后【确定】即可；终端将在 10 秒内响应

2.8.12. 删除终端

选择终端，点击【删除终端】，确定需要删除的离线的终端，最后【确定】即可

2.8.13. 终端筛选

鼠标移入所有终端后，选择相应的状态即可筛选出终端

2.8.14. 导出

选择终端，点击【导出】，等待后台将需要的终端信息数据准备好，然后选择下载地址即可

2.9. 防护策略

为各个群组以及终端设置对应的防护策略，使终端具备自动处理事件的能力以及防护

2.9.1. 新建策略

点击【新建策略】，输入策略名称即可 

2.9.2. 编辑、删除策略

【新建策略】之后即可编辑策略，可以修改策略名称以及策略的防护方式等

2.9.3. 部署策略

在分组列表中选择具体的策略部署到分组中所有终端；终端将在 10 秒内响应策略

2.9.4. 信任文件

【添加信任条目】，输入需要信任的文件名称或者选择文件，点击【确定】；文件将在 10 秒内被终端信任

2.10. 文件管理

2.10.1. 软件卸载

选择需要卸载的软件，点击【卸载】；终端将在 10 秒内响应

2.10.2. 文件分发

点击【分发】，选择需要分发的文件以及想要分发到的终端，进行【文件分发】；终端将在 10 秒内响应

2.10.3. 文件上传

点击【上传】，选择需要上传的文件，输入文件名称以及版本号等信息，点击【确定】

2.10.4. 文件下载

点击【下载】，选择需要下载到本地的文件，点击【确定】

2.10.5. 文件删除

点击【删除】，选择需要从控制中心删除的文件，点击【确定】

2.11. 事件日志

事件日志包括病毒防护、系统防护、网络防护、历史任务、管理员操作等日志。还包括功能、时间、分组等筛选。可以非常方便的查看终端的安全防护情况

2.12. 管理工具

2.12.1. 离线升级工具

背景：如果您的控制中心处于局域网，无法连接外网的情况。可以采取使用离线升级工具进行升级。

操作方法：在连接有外网的机器上下载离线升级工具，通过移动设备等方式拷贝到控制中心的机器上，安装升级即可

2.12.2. 日志清理工具

背景：如果您需要清理数据库的旧日志，减少系统硬盘的占用，即可将日志进行清理

操作方法：点击日志清理，选择需要清理的日志，并且选择最近的 24 小时内清理，点击确认即可。

2.12.3. 定时任务

背景：如果你需要定期对全网的终端进行杀毒，可以采用定时任务

操作方法：点击定时任务，选择需要杀毒的终端分组以及对应的病毒处理设置，然后定义时间以及频率，下发定时任务即可

2.13.账号管理

超级管理员新增管理员后，通过给其他管理员分配操作模块的权限，使其协助管理控制中心以及终端

2.13.1.新建管理员

点击新建管理员，输入账号、选择账号类型、并且赋予管理员权限，即可成功创建管理员

2.13.2.删除管理员

选择需要删除的管理员，点击删除管理员按钮，即可将管理员删除。（超级管理员不可删除）

2.14.系统设置

2.14.1.终端相关设置

2.14.1.1.管理员设置

输入管理员的名称以及联系方式，方便终端出现问题时联系中心

2.14.1.2.密码保护

将安装终端进行密码保护，防止终端用户操作以及卸载安全终端软件

2.14.2.中心相关设置

2.14.2.1.中心日志设置

中心保存日志的期限，3 个月、6 个月、1 年

2.14.2.2.中心升级设置

在线升级方式包括自动升级以及手动升级

2.14.2.3.数据备份与恢复

将中心、终端数据进行备份，同时支持导入导出备份以及数据恢复

2.14.2.4.中心迁移

- 迁移中心至新的网络地址（本机迁移）：将所有的终端全部连接上新的控制中心
- 迁移中心至新的物理地址（迁移至另外一台机器）：将所有的终端全部连接上新的控制中心

3. 安全终端

火绒终端安全管理系统终端主要针对杀、防、管控这几方面进行功能设计，主要有病毒查杀、防护中心、扩展工具三部分功能。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。

3. 1. 首页

下图是终端首页，有病毒查杀、防护中心、扩展工具三部分功能。其中病毒查杀界面中，有已保护天数、快速查杀（全盘查杀、自定义查杀）、软件更新、版本号和病毒库信息、隔离区、信任区。

3.2. 病毒查杀

病毒查杀是自安全杀毒软件诞生之初就一直存在的基础功能，用户可以利用病毒查杀主动扫描在电脑中是否已经存在的病毒、木马威胁。选择了需要查杀的目标，火绒将通过自主研发的反病毒引擎高效扫描目标文件，及时发现病毒、木马，并帮助用户有效清除相关威胁。目前有快速查杀、全盘查杀、自定义查杀三种查杀方式。

3.2.1. 快速查杀

病毒文件通常会感染电脑系统敏感位置，【快速查杀】针对这些敏感位置进行快速的查杀，用时较少。

3.2.2. 全盘查杀

针对计算机所有磁盘位置，进行查杀，用时较长。

3.2.3. 自定义查杀

您可以指定磁盘中的任意位置进行病毒扫描，完全自主操作，有针对性地进行扫描查杀。

3.2.4. 信任区和隔离区

信任区相当于电脑文件的暂存库，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、下载保护功能扫描。信任区支持增加文件夹或者文件进行信任，同时支持取消信任。

隔离区相当于操作系统的回收站，火绒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。

用户可以通过以下方式（删除、恢复、提取）对隔离区、信任区的文件进行管理。

3.3. 防护中心

在这里可以快速的开启关闭相应的防护，火绒防护中心设置了多达 11 项安全防护内容，对于常规使用，只需要开启开关，当发现威胁动作触发所设定的防护项目时，火绒将精准拦截威胁，帮助您计算机避免受到侵害。

3.3.1. 病毒防御

此模块是针对防御电脑病毒而设计的实时防护系统。包括 5 项防护体系：文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控。

3.3.2. 系统防御

此模块功能主要防护计数机系统不被恶意程序侵害。包括 3 项防护体系：系统加固、软件安装拦截、浏览器保护。

3.3.3. 网络防御

此模块功能主要防护计数机在使用过程中，对网络危险行为的防御。包括 3 项防护体系：黑客入侵拦截、对外攻击拦截、恶意网站拦截。

3.4. 扩展工具

火绒为用户提供了方便操作管理电脑的工具。包括右键管理、垃圾清理、文件粉碎、弹窗拦截、启动项管理、网络流量。

3.4.1. 右键管理

火绒为用户提供了针对右键菜单管理的小工具，方便设置用户需要的右键菜单。

3.4.2. 垃圾清理

火绒为用户提供了垃圾清理工具，清理不必要的缓存文件，节省电脑使用空间。

3.4.3. 文件粉碎

用户使用电脑过程中，有部分不需要的文件，但是通过常规删除，无法删掉；或者有部分文件需要彻底删除，防止被技术手段恢复，这时需要对文件进行彻底粉碎，火绒文件粉碎提供稳定安全的粉碎方式。

3.4.4. 弹窗拦截

火绒弹窗拦截，采用多种拦截形式，自主、有效的拦截弹窗。

3.4.5. 启动项管理

用户可以通过管理启动项目，允许必要启动项，禁止不需要的启动项，使电脑达到最佳使用状态。

3.4.6. 网络流量

通过网络流量管理可以更好地控制上网的程序，查看使用网络情况，限制程序网速，防止网络阻塞。

3.5.客户端设置

终端策略的配置包括：常规、病毒查杀、病毒防御、系统防御、网络防御 5 个模块的设置。

常规

常规设置模块中主要为基础配置，包括：快捷操作和更新提示相关配置。

3.5.1.病毒查杀

病毒查杀设置模块中包括：常规查杀和修复白名单相关配置。

3.5.2. 病毒防御

病毒防御设置模块中包括：文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控相关配置。

3.5.3. 系统防御

系统防御设置模块中包括：系统加固、软件安装拦截、浏览器保护相关配置。

3.5.4. 网络防御

网络防御设置模块中包括：黑客入侵拦截、对外攻击检测、恶意网站拦截相关配置。

3.6. 客户端日志

安全日志是安全杀毒软件的一项基础功能，用户可以利用安全日志查看一段时间内电脑的安全情况，也可以根据日志来分析电脑遇到的问题。

3.7. 客户端更新

终端每次进行扫描的时候就会与病毒库的病毒样本进行对比，需要病毒库不断更新病毒样本，客户端默认是自动更新，用户也可手动更新。

3.8. 客户端联系管理员

终端用户在使用过程中，如遇到问题需联系管理员，可在首页菜单栏点击联系网管（如下图），来解决用户遇到的问题。

附录 A　参考信息

火绒安全主页	http://www.huorong.cn
火绒安全论坛主页	http://bbs.huorong.cn
病毒上报网址	http://bbs.huorong.cn/forum-44-1.html
火绒安全反馈网址	http://bbs.huorong.cn/forum-51-1.html
技术服务电话	010-84905882
传真	010-84905882

附录 B　技术支持以及售后

火绒终端安全管理系统是由火绒安全公司研发的一套功能强大的反病毒软件，如果你在使用的过程中遇到任何问题，可以先尝试到火绒安全论坛企业版模块中寻找答案，或者通过电话与我们的技术服务部门联系，如果你有任何意见或者建议，欢迎反馈！

服务方式：

登录 http://bbs.huorong.cn 论坛中根据问题的关键字进行搜索，查找相应问题的解决方法，或者到火绒安全的产品模块寻找常规安全问题的答案。

即时通讯方式反馈：

1.添加 QQ：1021205130，进行详细的问题沟通；

2.详细描述遇到的问题（截图）并提供操作系统版本、中心及客户端版本信息；

3.将会有相关工程师及时跟进反馈。

官方论坛方式反馈：

1.登陆火绒官方论坛：bbs.huorong.cn，点击发布新帖；

2.详细描述遇到的问题（截图）并提供操作系统版本、中心及客户端版本信息；

3.将会有相关工程师及时跟进反馈。

附录 C　关于火绒

火绒成立于 2011 年，长期专注于终端安全领域，潜心研发引擎等底层技术，秉承“情报驱动安全”理念，率先构建完成 EDR（终端、检测和响应）运营体系，逐渐开始领跑终端安全领域。火绒安全 2012 年发布的“火绒安全软件”是一款免费个人电脑安全软件，经过数年口碑相传，积累了以技术人员、专业人士、意见领袖为主的数百万用户。被认为是最纯粹的安全软件，以功能强悍、无流氓行为、占用资源少赢得了良好的口碑。“火绒终端安全管理系统 1.0”是火绒推出的第一款商业化产品，标志着火绒正式进军企业级市场。