火绒安全
www.huorong.cn

火绒安全软件 5.0

产品使用手册

2019/12/18

公　　司：北京火绒网络科技有限公司

地　　址：北京市朝阳区红军营南路 15 号瑞普大厦 B 座 1202 室

网　　址：https://www.huorong.cn

电　　话：010-84905882

文档说明

衷心感谢您使用火绒安全软件。火绒安全软件是由火绒安全网络科技有限公司荣誉出品。本说明书主要介绍软件的功能与使用方式，帮助您了解火绒安全软件，更好的使用火绒的相关功能，保护您的计算机安全。

本说明书中的内容全部有效，但在今后的程序升级中，可能会对现有的功能进行调整或改变，我们将在相应的系统升级公告中进行说明，因此更改的内容将不会在此说明书中体现，敬请谅解。

本说明书中如有涉及第三方软件、图标等均不具有指向性，不代表针对其他软件。

目录

产品概述

火绒安全软件是针对互联网 PC 终端设计的安全软件，本软件与 Microsoft 合作，适用于 Windows XP、Windows VISTA、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows Server（2003 sp1 及以上）的消费者防病毒软件。

火绒安全软件主要针对杀、防、管、控这几方面进行功能设计，主要有病毒查杀、防护中心、访问控制、安全工具四部分功能。由拥有连续十五年以上网络安全经验的专业团队研发打造而成，特别针对国内安全趋势，自主研发拥有全套自主知识产权的反病毒底层核心技术。

火绒安全软件基于目前 PC 用户的真实应用环境和安全威胁而设计，除了拥有强大的自主知识产权的反病毒引擎等核心底层技术之外，更考虑到目前互联网环境下，用户所面临的各种威胁和困境，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，追求“强悍的性能、轻巧的体量”，让用户能够“安全、方便、自主地使用自己的电脑”。

基础功能说明

本部分将会为您介绍常用的软件功能，如病毒查杀、防护中心、访问控制、各类安全工具等。让您对火绒安全软件基础功能的使用有所了解。满足您日常生活中的网络安全防护需求。

软件安装

安装流程：

第一步：前往火绒官方网站下载软件安装包。官网地址：https://www.huorong.cn/

第二步：启动下载好的安装包。

第三步：点击极速安装等待安装完成即可（您也可以根据需要更改安装目录）。软件安装完成后将会自动打开运行。

程序主界面

火绒 5.0 新增支持三种语言设置：简体中文、繁体中文和英文，您可在语言设置中随时切换。

病毒查杀

火绒病毒查杀能主动扫描在电脑中已存在的病毒、木马威胁。当您选择了需要查杀的目标，火绒将通过自主研发的反病毒引擎高效扫描目标文件，及时发现病毒、木马，并帮助您有效处理清除相关威胁。

启动扫描

功能	说明
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，推荐您日常使用。
全盘查	针对计算机所有磁盘位置进行查杀，用时较长，推荐您定期使用或发现电脑中毒后进行全面排查。
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。推荐您在遇到无法确定部分文件安全时使用。

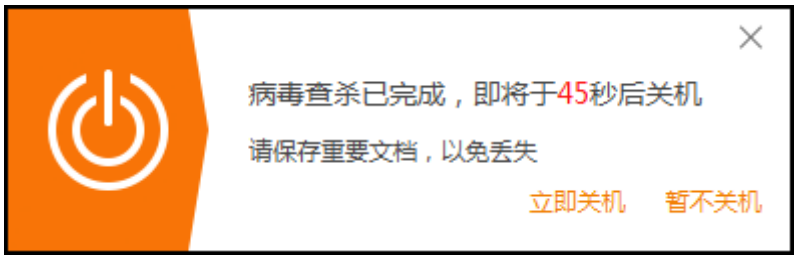
查杀速度

火绒为您提供了【常规】速度查杀和【高速】查杀（见下图）两种模式供您选择。

功能	说明
常规	占用较少的系统资源
高速	占用较多的系统资源，提高扫描速度。

查杀完成后自动关机

勾选即启用功能。勾选后火绒将自动处理病毒扫描完成后发现的威胁，在威胁处理完成时弹出关机提示（见下图），关机提示等待的时间为 45 秒，45 秒后将为您自动关闭电脑。您仍在此期间可点击“暂不关机”或“×”以取消自动关机。



发现威胁

当火绒在扫描中发现病毒时，会实时显示发现风险项的个数，您可通过【查看详情】(见下图）实时查看当前已发现的风险项。点击【退出详情】即可返回病毒扫描页面。

处理威胁

当扫描到威胁后，火绒安全软件提供病毒处理方式的选择。

【立即处理】：对所选择的风险项，进行隔离处理。（建议您操作此项）

【全部忽略】：对扫描出的风险项目不做处理。（下图）。

将威胁文件处理完毕后，提示扫描完成（下图），为您展示扫描概况，在上一步处理的威胁添加至【隔离区】。

隔离区

火绒会将扫描后清除的风险项文件，经过加密后备份至【隔离区】(见下图)，以便您有

特殊需要时，可以主动从隔离区中重新找回被清除的风险项文件。

功能	说明
删除	将选中的文件从隔离区删除，文件不可恢复。
恢复	将选中的文件恢复到其原始位置，同时从隔离区删除该文件。
提取	将选中的文件复制至指定目录。

隔离区可以在以下三个位置找到：

在首页的下拉菜单中找到隔离区（见下图）。

在处理风险项后的扫描报告页中可以找到隔离区（见下图）。

在鼠标右键单击火绒托盘图标后显示的快捷菜单中也可以找到隔离区（见下图）。

信任区

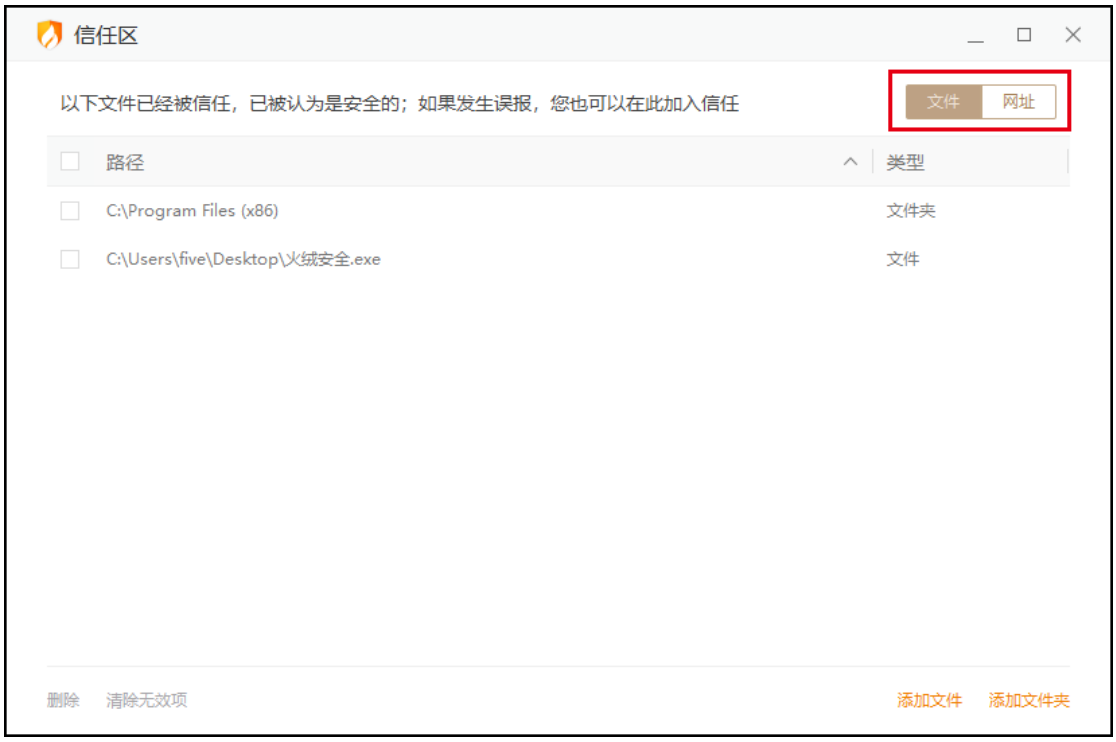
您可将确认安全的文件或网址添加到【信任区】(见下图)。信任区可以添加文件、文件夹与网址。受信任的项目将不会被认为包含风险，也不会被病毒查杀以及病毒防护的各项功能检测。您也可以在信任区中对已有的项目取消信任。

信任区可以在以下两个位置找到：

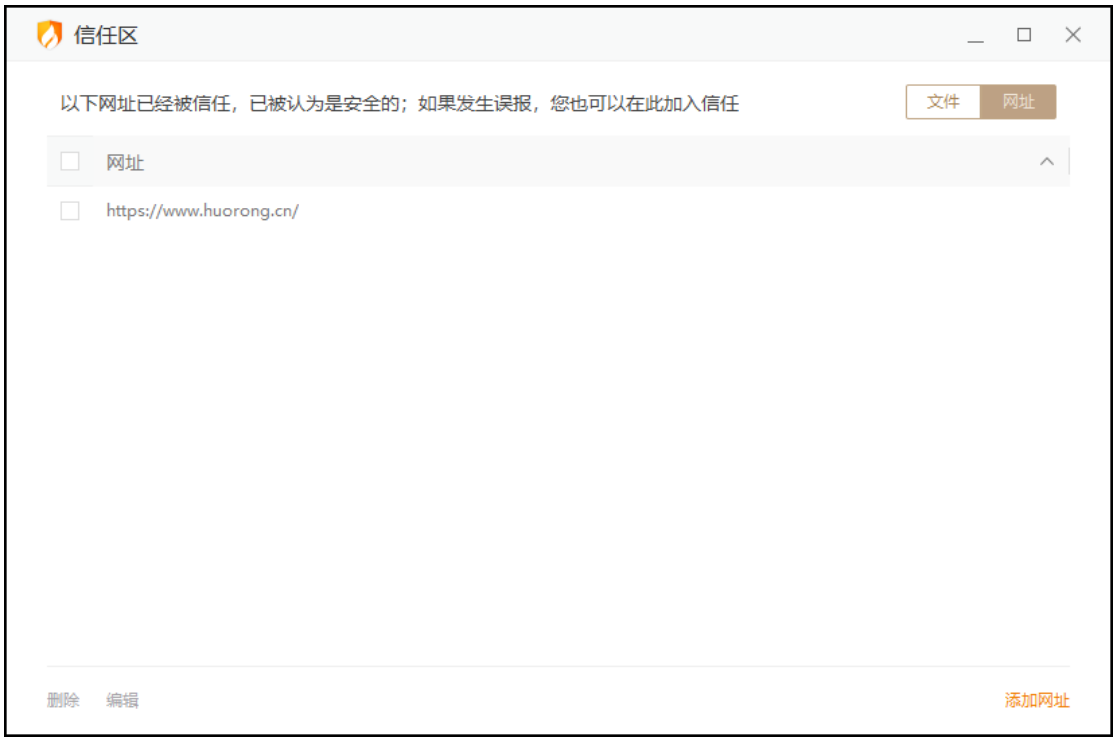
在首页的下拉菜单中可以找到信任区（见下图)。

在鼠标右键单击火绒托盘图标后显示的快捷菜单中可以找到信任区（见下图）。

点击文件/网址可切换显示信任的文件与网址。



功能	说明
删除路径	不再信任选中的文件/文件夹。
清除无效项	清除信任区中对应路径下已无该文件或文件夹的项目。
添加文件	将需要信任的文件添加至信任区。
添加文件夹	将需要信任的文件夹添加至信任区。



功能	说明
删除网址	不再信任选中的网址。
编辑网址	编辑选中网址链接。
添加网址	将需要信任的网址添加至信任区。

防护中心

火绒防护中心一共有四大安全模块，共包含 21 类安全防护内容。当发现威胁动作触发所设定的防护项目时，火绒将为您精准拦截威胁，帮助您计算机避免受到侵害。

病毒防护

病毒防护是针对电脑病毒设计的病毒实时防护系统。共包含文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、Web 扫描 6 项安全防护内容。

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，实时保护您的电脑不受病毒侵害。

当有威胁触发了【文件实时监控】时，火绒将自动清除病毒，并弹出提示弹窗（见下图）提示您。

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，极大提升电脑反病毒能力。

当有威胁触发了【恶意行为监控】时，火绒将弹出提示弹窗（见下图）提示您。您可根据需要选择相应处理方式。

3）U 盘保护

U 盘保护功能会在 U 盘接入电脑时对其根目录进行快速扫描，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。同时移动存储设备也会自动纳入文件实时监控等其他监控功能保护范围，全方位保护您电脑的安全。

当有威胁触发了【U 盘保护】时，火绒将自动清除病毒，并弹出提示弹窗（见下图）提示您。

4）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对文件进行病毒扫描，保护您的电脑安全。

当有威胁触发了【下载保护】时，火绒将自动清除病毒，并弹出提示弹窗（见下图）提示您。

5）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。

邮件监控目前仅支持邮件客户端收发的邮件，但不会对邮件客户端做出任何修改。

当有威胁触发了【邮件监控】时，火绒将自动处理威胁，并在处理完成后弹出提示弹窗（见下图）提示您。

接收病毒邮件：

发送病毒邮件：

6）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。

当有威胁触发了【Web 扫描】时，火绒将自动处理威胁，并在处理完成后弹出提示弹窗（见下图）提示您。

系统防护

系统防护模块用于防护电脑系统不被恶意程序侵害。系统防护共包含系统加固、应用加固、软件安装拦截、摄像头防护、浏览器保护、联网控制 6 项安全防护内容。

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。

当有威胁动作触犯【系统加固】时，火绒会弹窗（见下图）提示您，您可以根据需要选

择对这个动作的处理方式。

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。当有程序触发相应规则时，应用加固会弹窗（见下图）提示您，由您来决定是否允许该程序进行此项操作。

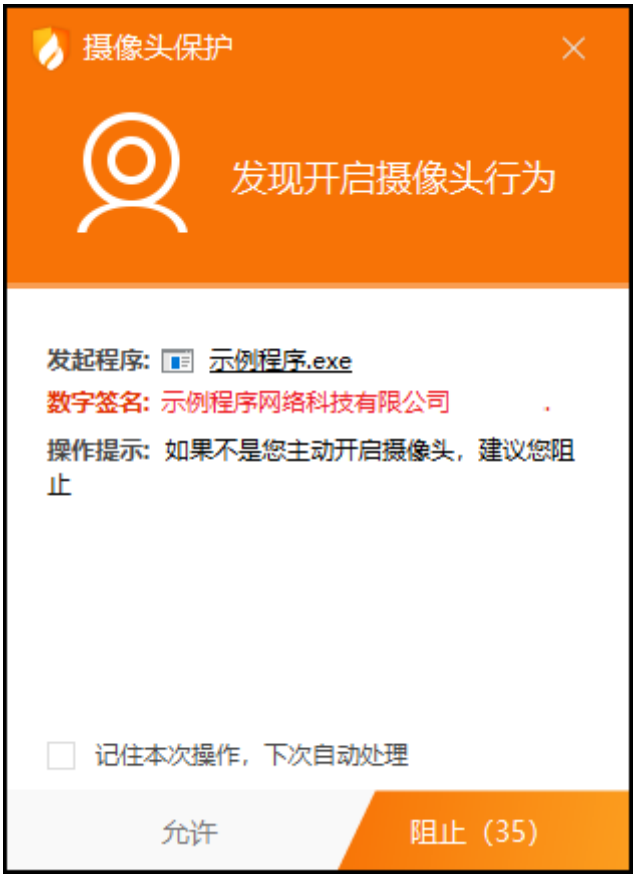
3）软件安装拦截

根据用户举报，对曾经出现过静默安装、被捆绑安装等行为的软件进行识别。此类软件在安装时软件安装拦截功能会在其安装时提示您（见下图）。

软件安装拦截能有效的减少您在不知情的情况下被安装不需要的软件。

4）摄像头保护

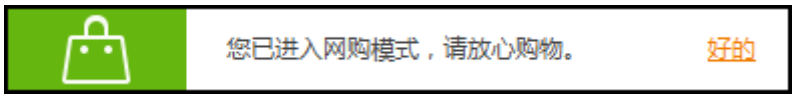
火绒摄像头防护会在有任意电脑软件要启用您的摄像头时弹窗（见下图）提示您，您可以根据需要选择是否允许程序启用摄像头。



5）浏览器保护

浏览器保护（见下图）能保护您的浏览器主页与搜索引擎不被随意篡改，此外在您访问电商网站与银行官网等网站时，自动进入网购保护模式，阻止支付页面被篡改等网购风险，为您的浏览器提供更全面的保护。

当您进入购物网站的时候，火绒会弹出保护提示。如您不需要，可取消勾选网购保护中的【当访问购物网站时弹窗提示】选项。



6) 联网控制

当您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（见下图），因此建议您根据需要决定是否开启此功能。

在弹出的联网控制弹窗中，您可以根据需要选择对这个动作的处理方式。

网络防护

网络防护主要保护计算机在使用过程中，对网络危险行为的防御。网络防护共包含网络入侵拦截、对外攻击拦截、僵尸网络防护、远程登录防护、We 服务保护、恶意网址拦截 6 项安全防护内容。

1）网络入侵拦截

当黑客通过远程系统漏洞攻击电脑时，网络入侵拦截能强力阻止攻击行为，保护受攻击的终端，有效降低系统面临的风险。

当发现有网络入侵行为时，火绒将自动阻止，并通过托盘消息通知您。

2）对外攻击拦截

对外攻击拦截功能与网络入侵拦截技术原理一致（都是通过识别漏洞攻击数据包），但是侧重于拦截本机对其它计算机的攻击行为。

当发现您的电脑有对外攻击行为时，火绒将自动阻止，并通过托盘消息通知您。

3）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。

当发现有僵尸网络行为时，火绒将自动阻止，并通过托盘消息通知您。

4）远程登录防护

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，用户可以操作主机允许的任何事情。

当有发现计算机受到密码破解攻击时，火绒将阻止攻击行为，并通过托盘消息通知您。

5) Web 服务保护

保护 Web 服务相关的软件，阻止针对这些软件的漏洞攻击行为。

当有发现计算机受到入侵时，火绒将记录攻击行为，并通过托盘消息通知您。

6) 恶意网址拦截

恶意网站拦截功能，可以在您访问网站时自动分辨即将访问的网站是否存在恶意风险，如果存在风险将拦截访问行为，并告知您，避免您的电脑受到侵害。

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（见下图）。

高级防护

高级防护中的详细内容您可在进阶说明-防护中心-高级防护中查看。

1） 自定义防护

自定义防护通过设置自定义防护规则能精准控制各项软件的执行，精准保护您不希望修改的文件、注册表等。有能力的用户可以通过自行编写防护规则，个性化的增强电脑防护能力。

当有威胁动作触犯【自定义防护】中的规则时，火绒会弹窗提示，您可以根据需要选择对这个动作的处理方式。

2） IP 黑名单

当您的电脑有不受欢迎的 IP 访问时，您可以添加这些 IP 加入 IP 黑名单中，以阻止这些 IP 的访问。

当发现有 IP 黑名单中地址的请求数据包时，火绒将直接丢弃，并通过托盘消息通知您。

3） IP 协议控制

有一定电脑基础的用户在访问网络的时候，当需要控制访问的具体动作，火绒提供了 IP 协议控制，具体是在 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。

当发现有触发 IP 协议控制规则的操作时，火绒根据用户设置的规则放过或阻止，并通过托盘消息通知用户。

访问控制

当有访客使用您的电脑时，您可以使用从上网时间、程序执行控制、网站内容控制、设备使用控制这些功能对访客的行为进行限制。

密码保护

在开启访问控制的各项功能后虽然已经可以限制电脑的使用，但是功能开关仍可被随意修改，同时火绒安全软件仍可被人为关闭或卸载。此时您可通过设置密码来解决。

在访问控制页面中点击【密码保护】，进入安全设置页面，设置密码保护。

1）设置密码

打开【安全设置】，在常规设置-基础设置中勾选【启用密码保护】（见下图），弹出密码设置页面。

在密码设置页（见下图）中，输入您需要设置的密码，勾选您希望密码保护的保护范围，

填写完毕后点击【保存】即可，密码保护将立即生效。

需要注意的是，如您忘记密码，火绒将无法为您找回之前的密码。请务必牢记您设置的密码。

当您在密码保护的范围中进行任意操作时，均会弹出输入密码的弹窗（见下图），要求您输入设置的密码才能进行相应操作。

2）修改密码和保护范围

当您在启用密码保护后，需要修改密码或修改密码保护范围时，您可在常规设置-基础

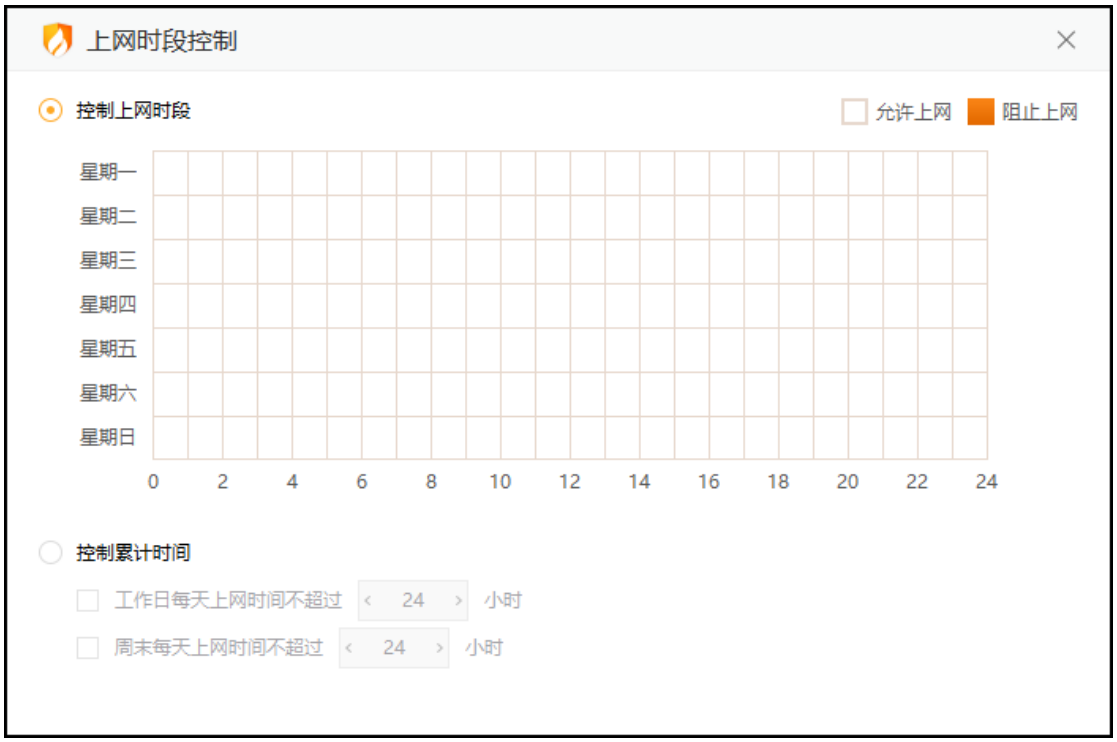
设置中点击【密码设置】（见下图）再次打开密码设置页。进行修改密码或修改保护范围。

3）关闭密码保护

您只需在常规设置-基础设置中取消勾选【启用密码保护】选项，即可关闭密码保护。

上网时段控制

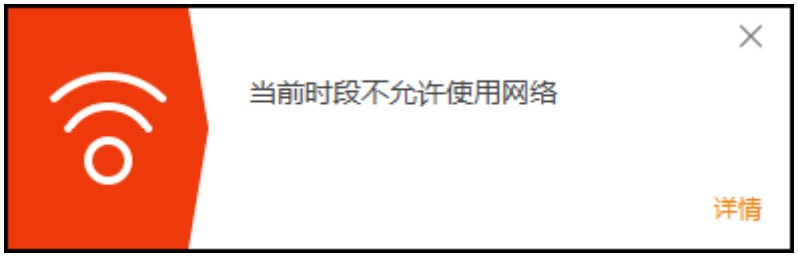
火绒上网时段控制可根据您设定的上网时间来对电脑联网功能进行控制。



当前提供两种限制方式：【控制上网时段】和【控制累计时间】

功能	说明
控制上网时段	以一星期（一周）为周期，将可上网时间段做作为限制，管控每天可上网的时间。
控制累计时间	将工作日（周一至周五）和周末（周六日）的累计上网时长作为限制，管控每天总上网时间。当发生流量变化时，就记为正在上网时间。

超出限定上网时间时，将弹出弹窗提示（见下图），并断网。您仍可点击【详情】或打开火绒安全软件解除上网时段控制。



网站内容控制

火绒网站内容控制可以限制计算机访问指定网址，达到屏蔽该网站的目的。限制访客访问不受您信任的网站。

功能	说明
编辑	编辑选中规则，内置 6 项基础规则无法选中、编辑。
删除	删除选中规则，内置 6 项基础规则无法选中、删除。
添加网站	添加需要屏蔽的网址，点击后打开添加拦截网址弹窗（见下图）。

除了火绒内置了 6 项常用的基础规则，您还可根据需要通过【添加网站】添加其他需要屏蔽的网址。

功能	说明
规则名	您可以自定义当前规则名称。
规则内容	填写要拦截的网址。 多网址通过换行区分，每一行为一个网址 网址支持通配符*?，比如 www.*.com：表示开头为 www.开始，以.com 结尾的所有网站都禁止访问
保存	保存此规则
取消	关闭弹窗

当电脑访问受限网站时，火绒将拦截网址，并在浏览器中显示拦截提示（见下图）。

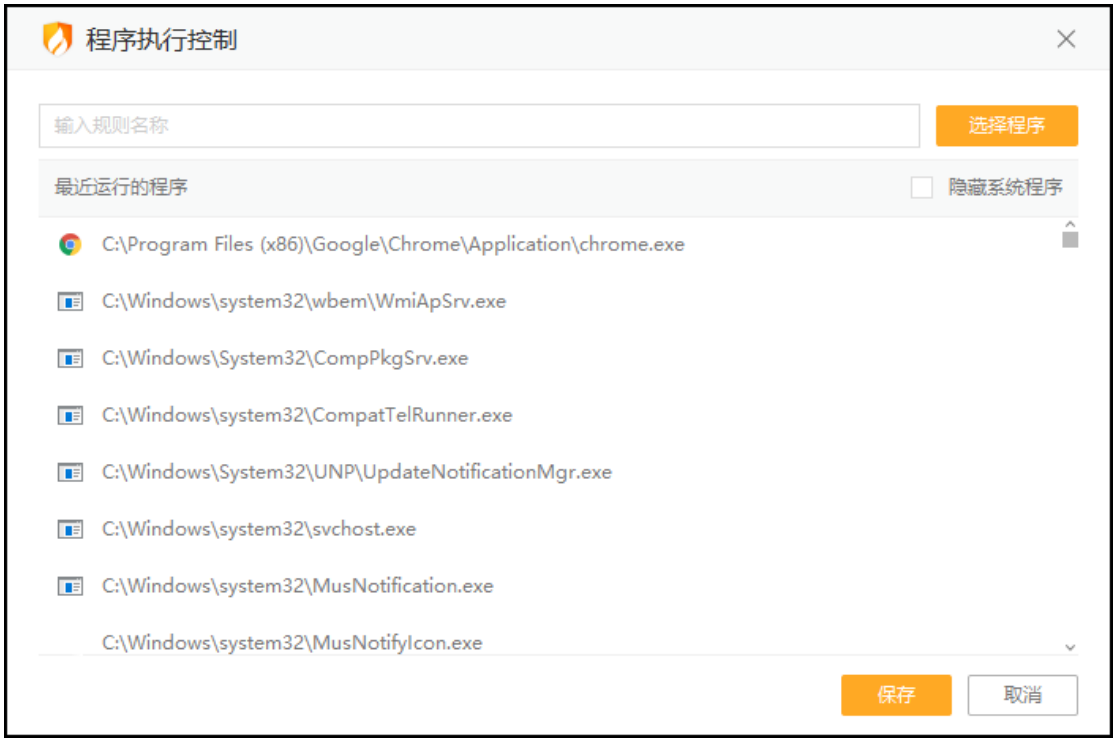
程序执行控制

在访客使用您电脑的过程中，若您希望限制访客使用您的部分软件；此时可开启程序执行控制，以限制某个或某类程序在电脑中的使用。

功能	说明

开关	绿色表示开启：程序执行控制将阻止该规则下的程序启动 灰色表示关闭：该规则内程序不受程序执行控制限制
删除程序	删除选中程序，内置 6 项规则无法选中、删除。
添加程序	添加需要屏蔽的程序，点击进入添加程序页面（见下图）

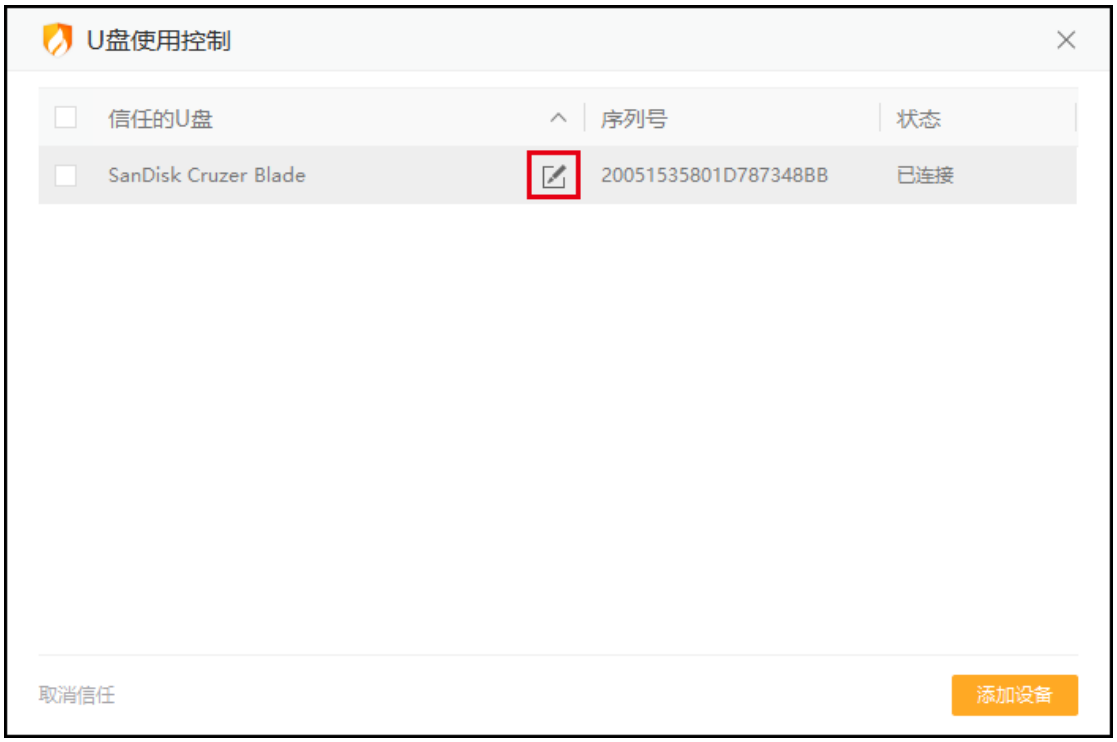
点击【选择程序】，选择您需要阻止运行的程序，点击保存即可。



当执行受限制程序时，火绒将弹窗提示您，并阻止程序执行。点击【详情】会打开火绒的程序执行控制页面，若您已设置密码，还会在页面上弹出输入密码提示弹窗。

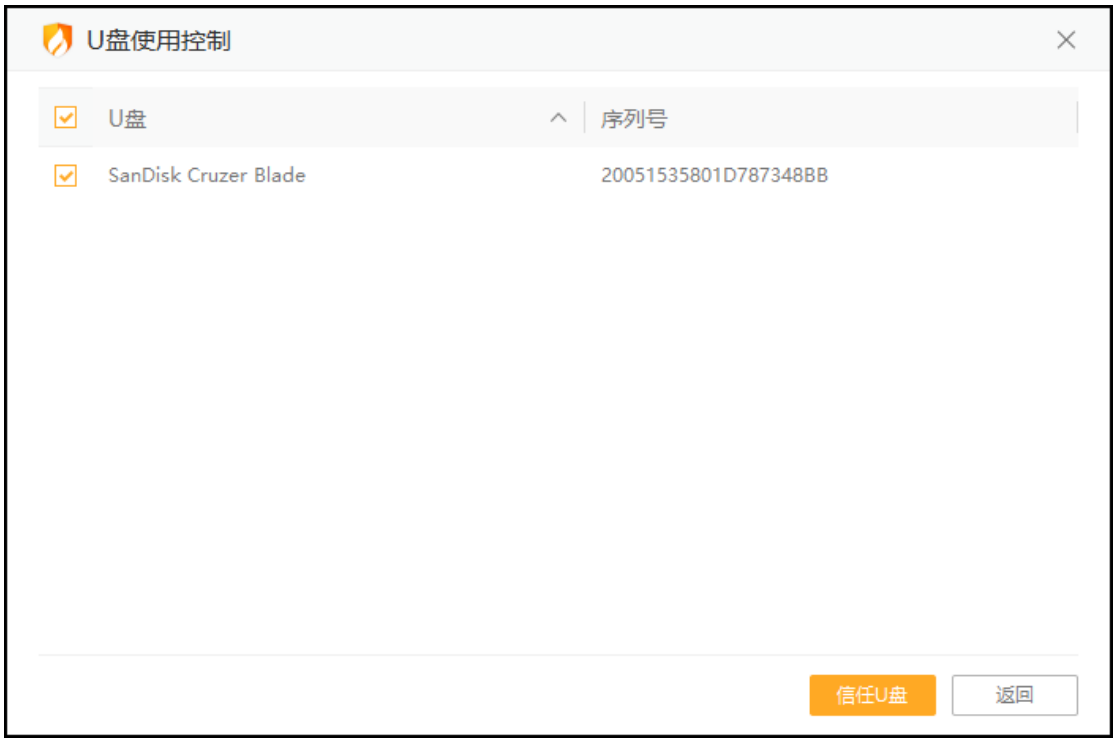
U 盘使用控制

火绒“U 盘使用控制”提供了阻挡不被信任的 U 盘接入电脑的功能。当开启 U 盘使用控制功能后，接入的 U 盘需添加信任，未信任的 U 盘将不能使用。



功能	说明
重命名	鼠标移入 U 盘名称显示，点击可对 U 盘进行重命名。
取消信任	取消选中的 U 盘。
添加设备	添加需要信任的 U 盘，点击进入添加设备页面（见下图）

选中需要信任的设备，点【添加信任】，U 盘即可正常连接使用。信任的设备在下一次连接电脑时无需再次确认，可直接连接。



功能	说明
添加信任	信任选中的 U 盘。
返回	返回上一页（U 盘使用控制首页）。

当接入的 U 盘不在信任列表内时，火绒将弹出阻止窗口（见下图）。点击【详情】会打开火绒的 U 盘使用控制页面，若您已设置密码，还会在页面上弹出输入密码提示弹窗。

安全工具

火绒除了在病毒防护与系统安全为您保驾护航，同时还提供了 15 种安全工具，帮助您更方便的使用以及管理您的电脑。此外火绒还专门为有一定电脑基础的用户提供了一项强大的系统管理工具——火绒剑。

您可在首页中的【安全工具】里，进入安全工具列表（见下图），点击对应的安全工具将立即打开运行。部分安全工具需要您下载后才能使用。

系统工具

1） 漏洞修复

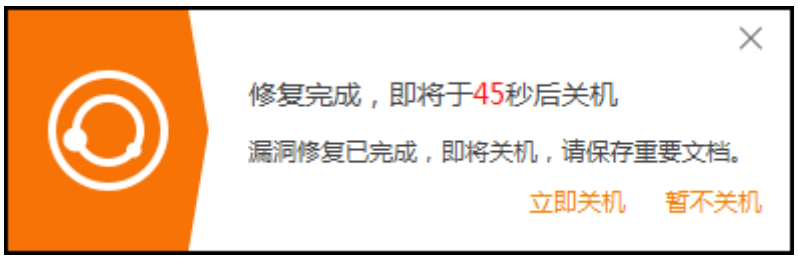
漏洞可能导致您的电脑被他人入侵利用。微软公司和其他软件公司会不定期地针对 Windows 操作系统以及在 Windows 操作系统上运行的其他应用发布相应的补丁程序，漏洞修复能第一时间获取补丁相关信息，及时修复已发现的漏洞。

打开漏洞修复进入漏洞修复首页（下图），点击开始扫描进行漏洞修复扫描。

扫描发现问题后火绒会默认勾选上高危漏洞补丁；功能漏洞补丁一般不容易导致电脑产生安全风险，因此不会自动为您勾选，建议有电脑经验的用户选择性修复。点击一键修复将开始下载安装已勾选的漏洞补丁。

功能	说明
一键修复	点击运行修复，将下载安装所有选中的漏洞补丁
暂不修复	放弃修复全部漏洞，进入修复完成页面
查看	查看该漏洞补丁的详细信息
忽略	忽略该漏洞补丁，并从列表中移出。忽略的漏洞补丁可在首页的【补丁管理】中查看（见下图）。
全选	将高危漏洞补丁与功能漏洞补丁全部选中
忽略选中项	将选中的漏洞补丁全部忽略，并加入至【补丁管理】中
导出漏洞信息	将选中的漏洞信息导出至电脑中，点击后选择需要存放的位置保存即可。
修复已完成时自动关机	勾选后，待漏洞补丁全部下载并安装完成后将弹出自动关机提示（见下图）。自动关机提示弹窗的等待时间为 45 秒。

补丁管理在漏洞修复首页右下角，在补丁管理中的项目我们将不予以扫描显示。您如需解除此状态，您可在补丁管理中选中需要解除忽略的项目并点击【取消忽略】。



有时漏洞较多或漏洞补丁较大时常常需要很长的下载时间与安装时间。您可在正在修复的页面中点击【后台修复】，将漏洞修复切换至后台并提示您（见下图）。在电脑右下角的托盘中您可再次找到漏洞修复。

2） 系统修复

系统修复能修复因为木马病毒篡改、软件的错误设置等原因导致的各类电脑系统异常、不稳定问题，以保证系统安全稳定地运行。

打开系统修复，进入系统修复主页，点击扫描按钮可开始扫描排查系统问题。

扫描完成发现问题后会显示扫描完成页（见下图），您可根据自己的需要勾选需要修复的项目，火绒默认只为您勾选推荐修复项。点击立即修复按钮进行系统修复。之后您等待修复完成即可。

功能	说明

立即修复	点击运行修复，将下载安装所有选中的漏洞补丁。
暂不修复	放弃修复全部漏洞，进入修复完成页面
查看	查看该漏洞补丁的详细信息
忽略	忽略该项，并从列表中移出。该项将在忽略的项目可在首页的【忽略区】中查看（见下图）。
全选	将推荐修复项与可选修复项全部选中
忽略选中项	将选中的项目全部忽略，并加入至【忽略区】中

忽略区在系统修复首页右下角，在忽略区中的项目我们将不予以扫描显示。您如需解除忽略状态，您可在忽略区中勾选该项并点击【取消忽略】。

3） 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。火绒弹窗拦截采用多种拦截形式，自主、有效的

拦截弹窗。

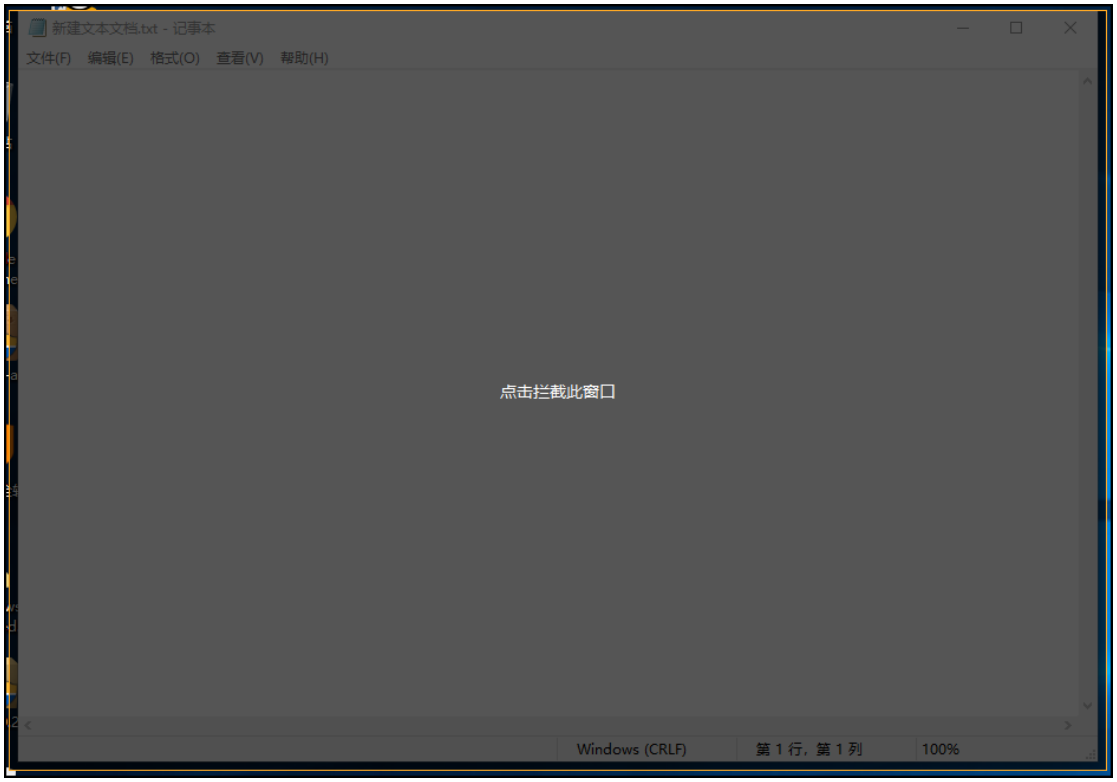
弹窗拦截开启后会自动扫描出您电脑软件中出现的广告弹窗，并开始自动拦截。您也可在首页中手动关闭某些您不想拦截的弹窗。

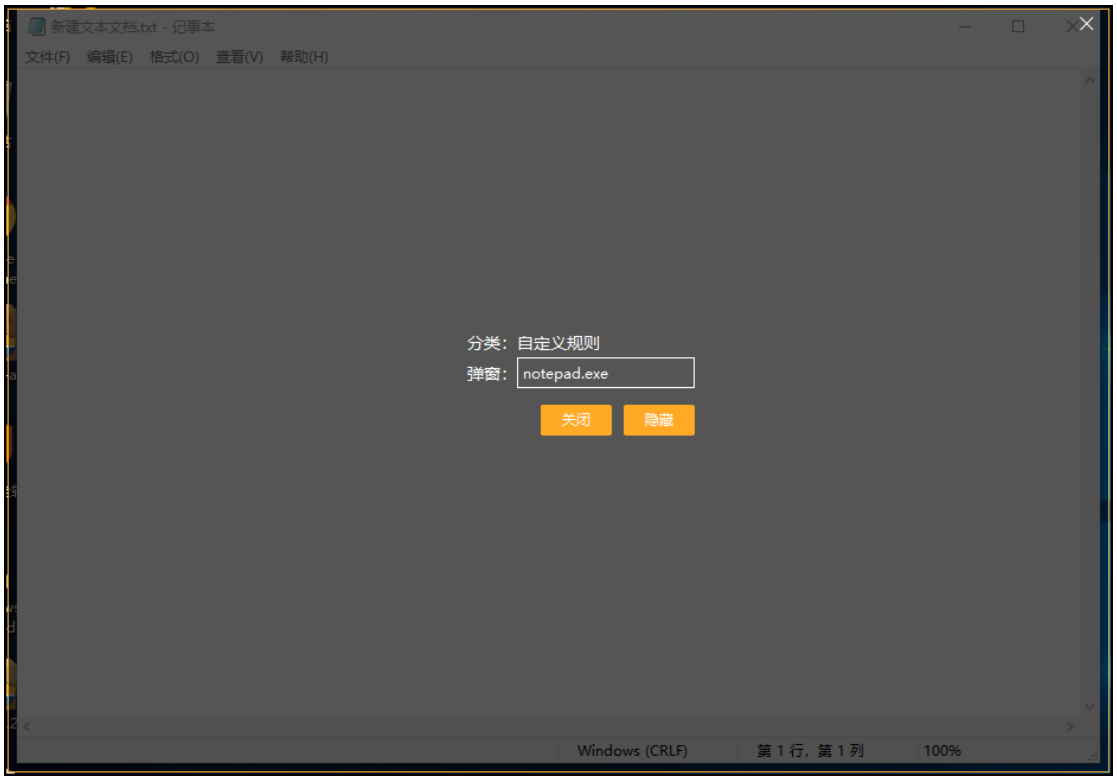
功能	说明
截图拦截	点击运行截图拦截
点击列表任意弹窗	打开该弹窗的拦截详情
清除无效规则	删除所有无效的规则 无效规则判定：对应路径下已无该程序
窗口记录/正在记录窗口	点击进入窗口记录页面 窗口记录开启时显示为【正在记录窗口】，窗口记录未开启时显示【窗口记录】

截图拦截

在您使用弹窗拦截的过程中，发现仍有部分窗口影响您电脑的使用时，您可点击弹窗拦

截首页中的【截图拦截】，手动定位选择需要屏蔽的窗口，点击关闭或隐藏（见下图），我们将为您自动生成一条关闭或隐藏此窗口的规则。您可在弹窗拦截首页的自定义规则中查看。





功能		说明
弹窗		自定义此弹窗名称
拦截方式	关闭	选择此项，当该弹窗再次弹出时火绒直接关闭弹窗
	隐藏	选择此项，当该弹窗再次弹出时火绒会将该弹窗移出屏幕的显示范围之外

拦截详情

当有弹窗被火绒拦截后，点击拦截次数可打开拦截详情。

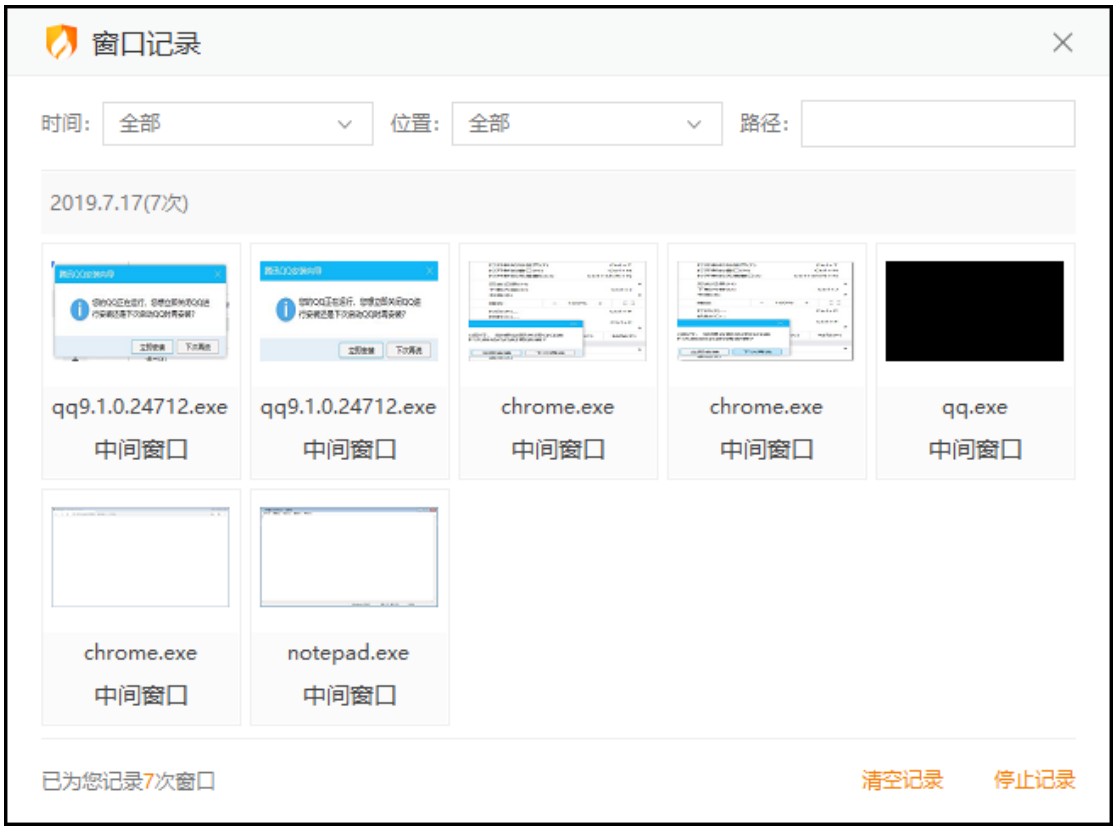
功能	说明
缩放	1、鼠标点击百分比旁的加减号，可放大缩小图片 2、鼠标移入图片滚动滚轮，可放大缩小图片 3、若图片小于拦截详情窗口，则不支持缩放
定位文件	打开弹窗程序所在文件夹

不再拦截/拦截弹窗	点击不再拦截将不拦截该弹窗，同时弹窗拦截首页中该弹窗开关关闭。按钮文字变为拦截弹窗 点击拦截弹窗将拦截该弹窗，同时弹窗拦截首页中该弹窗开关开启。按钮文字变为不再拦截

窗口记录/正在记录窗口

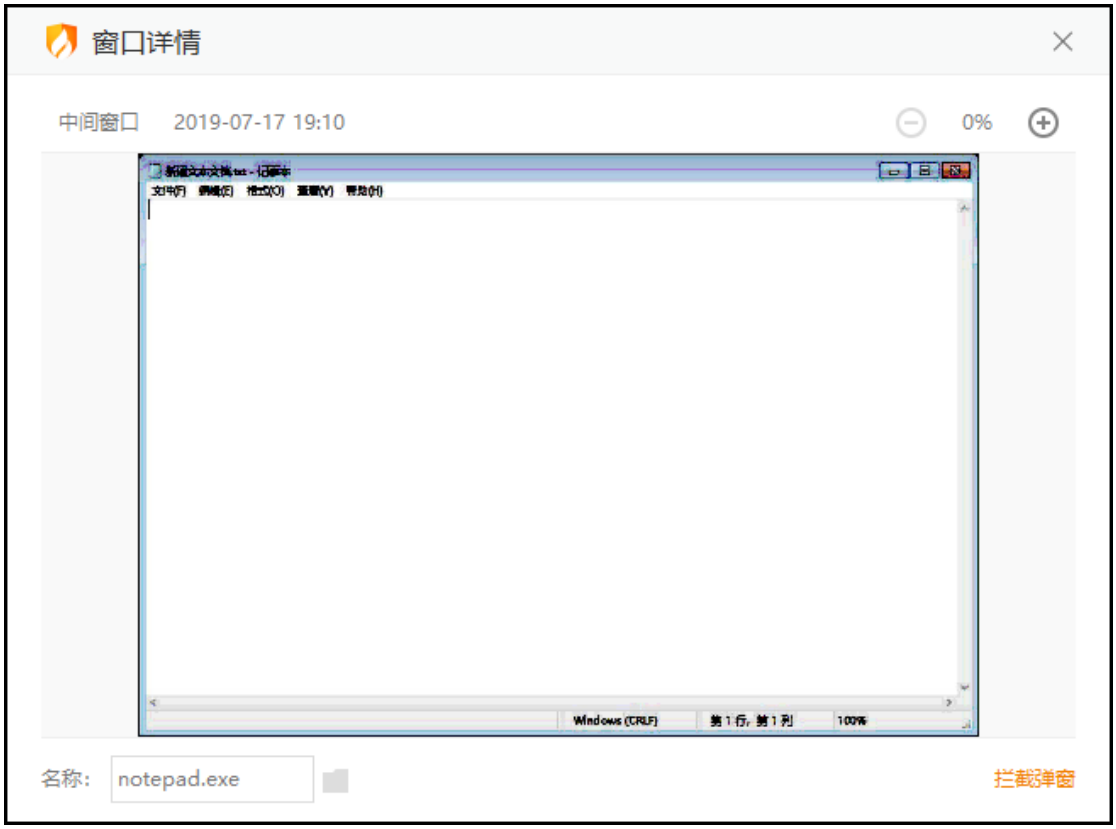
当有部分弹窗，弹窗拦截未检测显示，并且弹窗经常一闪而过，难以通过截图拦截捕捉到该弹窗时；您可开启窗口记录，在下次再出现该弹窗后，您可在窗口记录中找到该弹窗并开启拦截。

窗口记录默认为关闭状态，点击窗口记录右下角的【开启记录】（见下图）即可开启窗口记录功能。需要注意的是窗口记录会记录您所有软件弹出的窗口页面，包含正常的浏览器、办公软件、即时通讯软件等电脑软件弹出的所有窗口。



功能	说明

时间、位置、路径	提供给您的筛选项
清空记录	点击将清空当前所有的窗口记录
开启记录/停止记录	点击开启记录，火绒弹窗拦截将开启窗口记录功能，记录电脑中所有弹出的窗口 点击停止记录，火绒弹窗拦截将停止窗口记录功能



功能	说明
缩放	1、鼠标点击百分比旁的加减号，可放大缩小图片 2、鼠标移入图片滚动滚轮，可放大缩小图片 3、若图片小于拦截详情窗口，则不支持缩放
定位文件	打开窗口程序所在文件夹
拦截弹窗	点击将拦截该窗口，并在首页中自定义规则分组下创建对应规则。同时此条窗口记录将被删除。

托盘消息

鼠标移入弹窗拦截的托盘程序或为您显示最近拦截的弹窗（见下图）。

如您不想显示托盘消息，您可在弹窗拦截首页右上角的下拉菜单，打开软件设置，将提醒设置取消勾选（见下图）。

4） 垃圾清理

火绒为您提供了垃圾清理工具，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。

打开垃圾清理后，点击开始扫描即可开始扫描电脑垃圾。

扫描发现系统垃圾后，我们会为您智能选择勾选推荐清理的垃圾，您可根据需要勾选或取消勾选需要清理的垃圾。勾选完毕后点击一键清理等待垃圾清理自动完成即可。

如您不想每次手动扫描清理垃圾，火绒还为您提供了自动清理垃圾的功能。

您可点开软件设置，在设置中勾选【开机自动扫描】后再勾选【自动清理，无需弹窗提醒】（见下图），根据您的需要选择【清理大小】与【扫描周期】；火绒会根据您设置的扫描周期自动进行扫描清理的工作。

5） 启动项管理

您可以通过管理电脑开机启动项目，允许必要启动，禁止无用启动，使电脑达到最佳使

用状态。

您可在启动项管理首页中通过禁用或开启来控制软件的自启，管理您的启动项。

您还可点击首页中的【查看详情】功能（见上图红色框选），进入【一键优化】页面。点击一键优化自动为您禁止无需开机启动的项目。

所有优化的操作记录您均可在启动项管理首页右下角的【优化记录】中查看。

6） 文件粉碎

在您使用电脑过程中，有部分文件无法通过常规删除；或部分文件需要彻底删除，防止被技术手段恢复，这时就需要对文件进行彻底粉碎，火绒文件粉碎为您提供更安全的粉碎方式，保护您的个人隐私。

打开文件粉碎，您可通过拽托目标文件/文件夹或点击界面右下方的添加文件/添加目录来选择您需要粉碎的文件或文件夹。

添加完成后，会显示【开始粉碎】按钮（见下图），点击开始粉碎按钮时会弹出确认提示框进行二次确认，点击确定后将立即开始粉碎文件。

若您还需防止文件恢复，您可在开始粉碎前勾选【彻底粉碎】(见下图)，防止文件恢复，保护您的隐私安全。

7） 右键管理

火绒为您提供了针对右键菜单管理的小工具，方便您隐藏右键菜单中不需要的功能。

打开右键管理后，您可将不希望在右键菜单中显示的功能关闭，将需要显示的功能开启。右键管理一共可以管理包含：文件右键菜单、桌面右键菜单、IE 右键菜单三块区域。

网络工具

1） 断网修复

在电脑日常的使用过程中，有时会遇到电脑突然断网的情况。断网修复能为您检查出断网原因并进行自动修复出现的问题。为您恢复网络通畅。

打开断网修复运行全面检查（见下图）。

在发现问题后，点击立即修复，等待网络修复完成即可。如您有不想修复的项目，可在发现问题界面将鼠标移入该项并点击忽略（见下图）可忽略修复此项目。

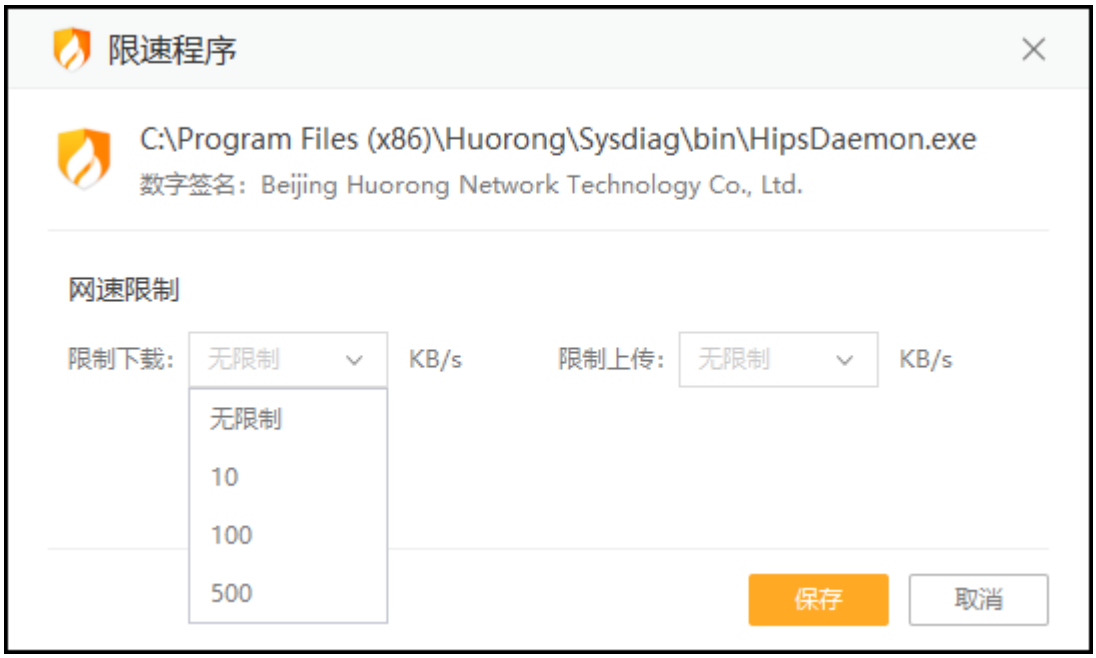
2） 流量监控

当很多程序都在利用网络下载上传数据时，会造成访问缓慢的情况，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，防止网络阻塞。

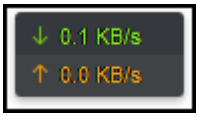
当需要限制某一程序网络传输速度时，打开流量监控，点开操作按钮，选择限制网速（见下图）打开限制网速窗口。

在限制网速窗口（下图）中，您可自行选择或手动输入限速的数值并点击保存。网速限制将立即生效。



如需查看流量使用历史，点击首页右上角的历史按钮（见下图），进入流量监控历史页面。在这里可以查看程序上传和下载的总量，同时依然可通过点击程序右侧的操作进行网速限制。

火绒还为您提供了便捷查看流量的方式，通过流量悬浮窗（见下图）可以查看当前流量使用状态，您可以通过以下两种方式开启流量悬浮窗。流量悬浮窗默认不显示：



方式一：通过鼠标右键点击火绒安全托盘图标，在弹出菜单中可以打开（下图）。

方式二：打开【安全设置】，在常规设置—基础配置中勾选【显示流量悬浮窗】(下图)。

3） 修改 HOSTS 文件

火绒为有一定计算机基础的用户提供了修改 HOSTS 文件的工具，当有些网站我们不想访问，或者有的网站访问不到，通过修改 hosts 文件就可以把域名指向的 IP 地址修改成我

们希望指向的 IP 地址，达到想要的效果。

点击修改 HOSTS 文件能一键打开 hosts 文件，方便快捷的修改 hosts 文件。

高级工具

1） 火绒剑

火绒剑是火绒为专业分析人员提供的分析工具，方便其分析软件动作，查找问题等专业行为。不在此文档中作详细介绍。

2） 专杀工具

专杀工具主要应对解决部分顽固木马病毒。这类顽固木马病毒运行后，不仅难以清除而且会阻止安全软件正常安装。因此需要专杀工具使用针对性的技术手段进行处理。

目前专杀工具需要单独下载，点击将前往火绒论坛，您可在论坛中下载程序后使用。

卸载安全工具

在安全工具的列表页，右键您想卸载的安全工具，在弹出的菜单中点击卸载工具，将会弹出确认卸载弹窗（见下图），点击确定即可卸载该安全工具。

托盘程序

火绒启动后会在电脑后台实时保护您的电脑，此过程中火绒程序进程将在托盘系统中继续运行，节省电脑资源。您可通过系统托盘区域，在需要火绒的时候方便快捷的找到火绒。

功能介绍

如何快速对在后台运行的火绒进行操作呢？

左键单击系统托盘图标，将显示火绒安全软件主界面。

右键单击系统托盘图标，将显示右键快捷菜单。

功能	说明
进入	进入火绒安全软件主界面
信任区	快速进入信任区
隔离区	快速进入隔离区
安全日志	点击打开安全日志，安全日志详细介绍请在进阶功能说明-安全日志中查看
检查更新	启动升级程序，检查软件版本情况。
流量悬浮窗	可快速开启或关闭流量悬浮窗，默认不开启
免打扰模式	默认不开启，开启后火绒将按推荐操作自动处理提示信息，不再弹出提示弹窗。 在您进入游戏和视频全屏时火绒会自动为您进入免打扰模式。
软件设置	快速打开软件设置页面
交流反馈	访问火绒官方论坛，您可在论坛中反馈您遇到的问题
退出火绒	关闭火绒安全，停止火绒对电脑的保护

托盘消息

火绒将各类非重要的消息为您统一收至托盘消息中。当您收到新的消息时，您只需鼠标移入系统托盘中火绒图标，即可显示火绒的托盘消息。

点击底部的【清除所有通知】可清空当前托盘消息。

您可在【安全设置】，常规设置-基础设置（见下图）中取消勾选【开启托盘消息】来关闭托盘消息。

软件卸载

火绒的卸载方法：

方法一：Windows7 通过“控制面板”—“卸载程序”中找到火绒，进行卸载。

Windows10 右键开始菜单选择“应用和功能”，找到火绒，进行卸载。

方法二：可以在火绒安装目录下找到卸载程序，将火绒安全卸载

进阶功能说明

火绒为有一定电脑知识背景的用户提供了可以手动自由控制杀毒软件以及电脑的方式，您可以通过调整火绒安全软件的设置，达到您自己想要实现的防护效果，更加精准地保护您的电脑。

病毒查杀

信任风险文件

在风险项中若含有您信任的文件，您不想文件被清除同时又不想被反复扫描出来，您可在点击该文件的【详情】，在弹出的【风险详情】中点击【信任文件】将该文件添加至信任区。

您仍可再次点击已信任文件的【详情】，再点击风险详情中的【取消信任】已继续查杀该风险文件。。

调整查杀设置

打开【安全设置】，点开选择常规设置-查杀设置，您可在查杀设置（见下图）中调整病毒查杀的相关配置，如扫描压缩包大小、排除扫描某些扩展名文件、修改病毒处理方式等。

功能		说明
全盘查杀设置	压缩包扫描	勾选后填写跳过扫描压缩包的大小。当压缩包大于您填写的数值时，扫描将自动跳过，以加快扫描速度。 若未勾选则在全盘查杀时将不扫描压缩包。

	不扫描/仅扫描指定扩展名文件	进行全盘查杀时，设置不扫描或仅扫描的文件类型。勾选此项后，根据您的需要选择不扫描或仅扫描，填写文件扩展名，填写格式：.tmp;.txt;.log;.db。 每个文件类型只需要填写.扩展名，多个文件类型之间用英文;来区分。
	扫描网络驱动器	勾选后，在运行全盘查杀时，火绒会同时扫描映射好的网络磁盘中的文件。
自定义查杀配置		无法取消勾选，自定义查杀时将深度查杀压缩包，无视大小限制
病毒处理方式	询问我	扫描出威胁后，显示发现的威胁文件，让您自主处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理威胁文件。
	清除病毒时备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，在出现误报误删的情况时，您可随时恢复误报误删的文件。
备份引导区		点击后选择保存位置，备份当前引导区。

防护中心

病毒防护

有一定电脑知识背景的用户可以通过对病毒防御模块的设置，来达到自己想要的防护效果。

1） 文件实时监控设置说明

通过设置可以调整【文件实时监控】所产生作用的形式，根据个人需要调整扫描时机、排除文件、处理病毒方式、清除病毒备份隔离区、查杀引擎等内容，防止已经隐藏在电脑上

的病毒对电脑造成伤害。

功能		说明
扫描时机		根据您的需要和电脑配置情况选择实时监控生效时机
病毒处理方式	询问我	扫描出威胁后，弹出提示弹窗，让您来自主处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
	清除病毒时备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删
排除		病毒实时监控的过程中，不扫描指定程序的文件操作。 填写示例：C:\Program Files\Test\>.exe;*\Test.exe 填写说明：需要填写要排除的程序路径， 多条路径之间用英文;分割

	?：匹配 1 个任意字符 *：匹配 0 到多个任意字符 >：匹配除 '\' 和 '/' 以外的 0 到多个任意字符

2） 恶意行为监控设置说明

通过设置可以调整【恶意行为监控】发现威胁动作时是否自动处理，处理病毒与清除病毒后备份隔离区等设置项目。

功能		说明
病毒处理方式	询问我	扫描出威胁后，询问您，让您来主动处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
	将病毒文件备份至隔离	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删

	区	
增强勒索病毒防护		火绒或生成若干常见文件格式的随机文件，病毒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。详细信息您可点击后方【了解详情】查看。

3） U 盘保护设置说明

通过设置可以管理【U 盘保护】的防护模式。调整自动扫描、病毒处理方式等内容，防止病毒通过 U 盘感染您的电脑。

功能		说明
可修复项目		勾选后将在自动扫描 U 盘的同时检测被病毒修改过的项目
压缩包扫描		勾选后填写跳过扫描压缩包的大小。当压缩包大于您填写的数值时，扫描将自动跳过，以加快扫描速度。
病毒处理方	询问我	扫描出威胁后，弹出提示弹窗，让您来自主处理威胁。

式	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
	清除病毒时备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删

U 盘修复功能

U 盘修复主要为您解决当清除部分 U 盘病毒后产生的两类遗留问题。一类是篡改 autorun 文件的病毒，在查杀后在可能会在 U 盘中遗留无效的 autorun.inf 文件；另一类是部分病毒会隐藏您正常文件，释放伪装文件，诱导您传播病毒，当火绒查杀了这类病毒后会清除病毒生成的伪装文件，但是会导致部分用户误以为杀毒软件把正常文件删除了。通过 U 盘修复可以删除无效的 autorun.inf 文件或检索 U 盘根目录中的隐藏文件与目录，引导您修复。

操作说明：

当 U 盘接入时发现可修复项目，弹窗提示

功能	说明
立即修复	修复选中的异常项目
暂不修复	关闭弹窗，不修复任何项目

您自行可以选择您需要修复的项目。

4） 下载保护设置说明

通过设置可以管理【下载保护】的生效方式，您可以根据自己的需要，对于下载的内容进行有针对性的查杀，防止病毒通过互联网下载文件感染您的电脑。

功能		说明
压缩包扫描		勾选后填写跳过扫描压缩包的大小。当压缩包大于您填写的数值时，扫描将自动跳过，以加快扫描速度。
病毒处理方式	询问我	扫描出威胁后，弹出提示弹窗，让您来自主处理威胁。
	自动处理	扫描出威胁后，火绒将根据推荐操作自动处理，不再询问您。
	清除病毒时备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删
排除		不扫描指定扩展名的文件操作 填写示例：.exe;.doc;.txt;.zip 填写说明：使用英文分号;区分多个扩展名

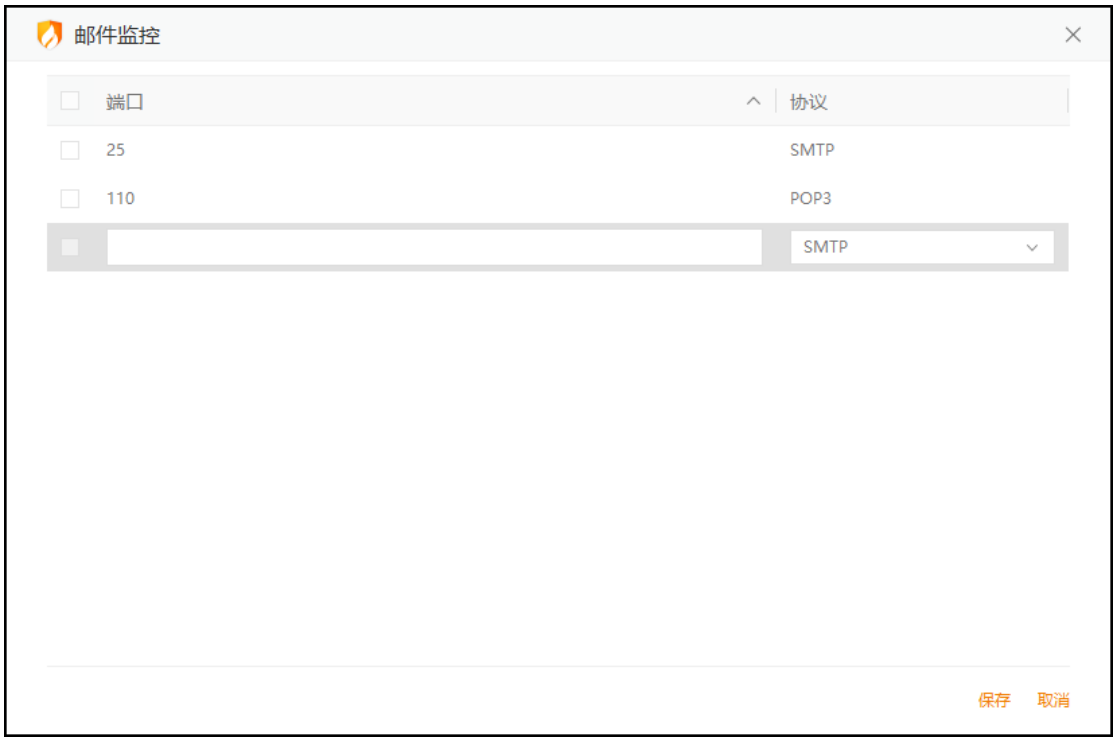
5） 邮件监控设置说明

通过设置可以管理【邮件监控】的生效方式，您可以根据自己的需要，对于发送、接受邮件进行有针对性的查杀，防止病毒通过邮件附件感染您的电脑。

功能		说明
保护范围		您可根据需要自由勾选邮件监控范围
邮件扫描		勾选后填写跳过扫描的邮件大小。当邮件大于您填写的数值时，邮件扫描将自动跳过，不予以扫描。
病毒处理方式	仅记录	发现病毒后火绒将不予以处理仅记录至安全日志中
	自动处理	发现病毒后，火绒将根据推荐操作自动处理，并记录至安全日志中
	备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找，防止误报误删
高级		设置邮件监控扫描的协议及端口，点击【配置规则】进入协议端口的配置页面（见下图）。

	默认存在两个规则：25 端口 SMTP 协议以及 110 端口 POP3 协议。

功能	说明
编辑	编辑勾选规则
删除	删除所有勾选规则
添加规则	添加新的需要扫描的协议和端口，点击后列表中新建一条规则（见下图）供您填写添加



功能	说明
保存	保存当前规则，添加至规则列表中
取消	退出添加规则状态，不保存当前规则

6） Web 扫描设置说明

通过设置可以管理【Web 扫描】的病毒处理方式，防止病毒通过您访问的网站感染您的电脑。

功能		说明
病毒处理方式	仅记录	发现病毒后火绒将不予以处理仅记录至安全日志中
	自动处理	发现病毒后，火绒将根据推荐操作自动处理，并记录至安全日志中
	备份至隔离区	勾选后，清除的病毒会被备份到隔离区，方便您进行查找

系统防护

有一定电脑知识背景的用户可以通过对系统防护模块的设置，配置相应规则，控制电脑中的程序对系统的修改与调整来达到对系统防护的效果。

1） 系统加固设置说明

通过设置可以管理【系统加固】的生效规则，火绒针对计算机系统，进行规则内置，您可以根据自己的需要，调整防护项目，防止电脑的各项系统设置被恶意程序篡改。

功能		说明
基础防护	文件防护	保护基础文件不被篡改、破坏或恶意创建
	注册表防护	防止特定注册表项目被恶意篡改
	执行防护	阻止特定命令行被恶意利用的行为
	启用内置过滤规则	监控针对系统的敏感性为，拦截高风险动作。保护系统重要进程，不会被攻击利用
自动防护	自动处理	点击进入自动处理页面，调整自动处理规则
智能防护	启用系统免疫	勾选后，火绒将自动阻止针对系统关键进程、特殊方式操作注册表、写物理内存等高危操作行为

基础防护：

您可在基础防护中针对文件防护、注册表防护、执行防护的防护项目进行修改调整。火绒为您默认配置了相应规则，您可根据需要自行调整，勾选您需要启动的防护项目，选择对应的生效方式即可。防护项目对应说明可参看后方的防护说明内容。

如您需恢复默认配置状态，您可点击页面左下角的【恢复默认】按钮。

自动防护：

部分程序为了达到持续篡改系统某些配置的目的，会反复执行相同操作，为了不反复弹窗提示拦截信息，打搅您的日常使用，所以提供了自动处理功能，您可以选择记住操作，减少相同弹窗提示。同时我们开放了自主添加自动处理项目的功能，方便您自由管控。

功能	说明
编辑	编辑选中规则
删除	删除所有选中规则
清除无效规则	删除所有无效的规则 无效规则判定：对应路径下已无该程序
添加规则	添加需自动处理的规则，点击后切换至添加规则页（见下图）供您填写添加

功能	说明
发起程序	选择控制操作的程序
保护对象	勾选需要自动阻止或自动允许的项目
保存	保存当前规则，添加至规则列表中
取消	切回自动处理规则列表，不保存当前规则

自动添加：

当危险行为触犯系统加固中生效方式为弹窗提示的规则时，会弹窗提示，如果您勾选【记住本次操作】（下图），就会将自动添加规则到【自动处理】列表中，下次遇到相同问题，则采取相同方式处理。

2） 应用加固设置说明

加固类型中勾选，代表该防护规则开启，后面的图标为您电脑中对应安装的应用程序。程序卸载后，对应图标消失。

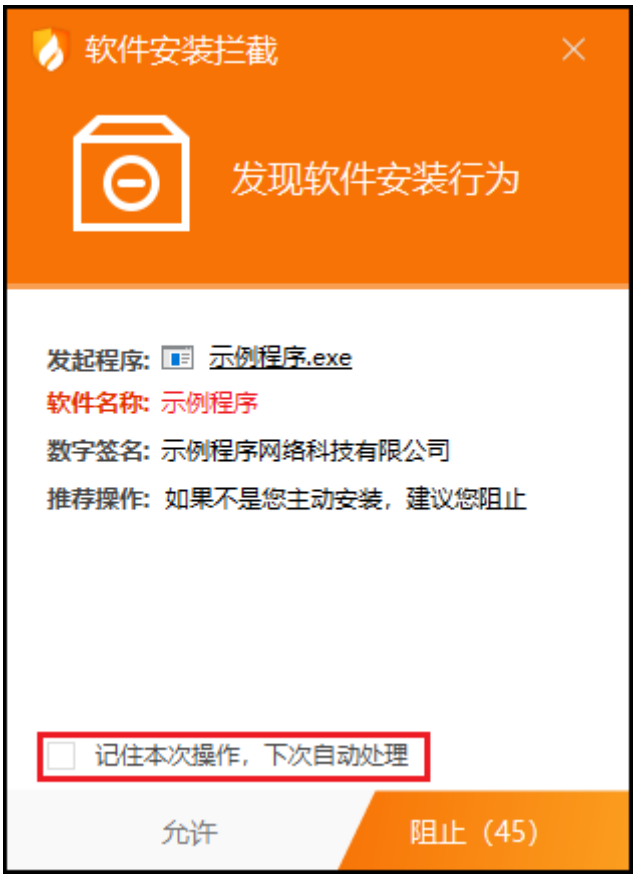
3） 软件安装拦截设置说明

您可在软件安装拦截设置中修改规则列表中程序的安装行为，此外还能自动阻止可识别软件的安装行为。

功能	说明

删除	删除所有选中规则
自动阻止列表外已识别软件的安装行为	勾选后，除列表内软件外，将自动阻止所有已识别软件的安装行为

在火绒发现推广软件的安装行为时会弹出提示弹窗，当您勾选【记住本次操作，下次自动处理】时，会自动添加一条对应规则至列表中。



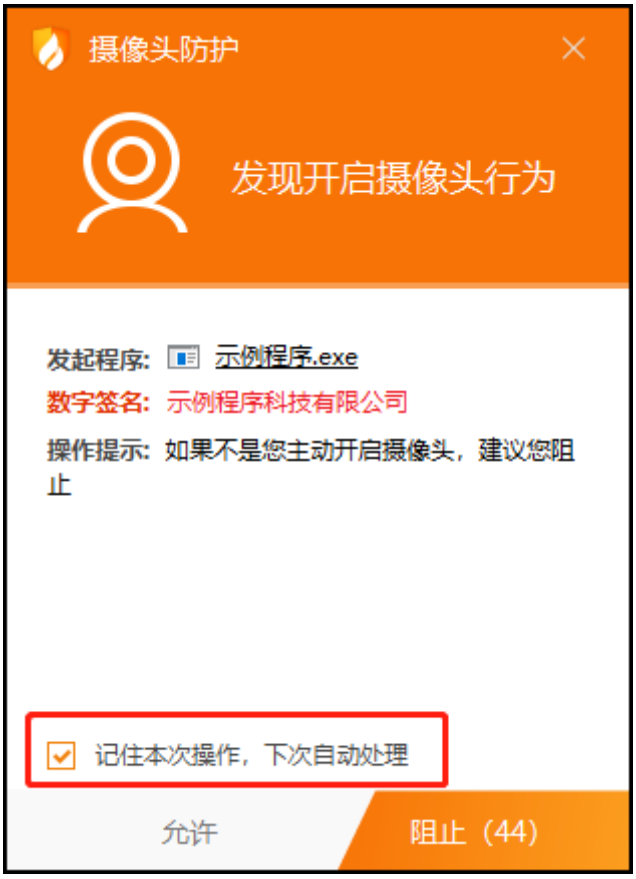
4） 摄像头防护设置说明

您可在摄像头防护设置中调整规则列表中程序的启动摄像头权限，同时还可自动阻止所有软件启用摄像头的行为。

功能	说明
删除	删除所有选中规则
清除无效规则	删除所有无效的规则 无效规则判定：对应路径下已无该程序
防护设置	点击打开摄像头防护设置
自动阻止列表外已识别软件的安装行为	勾选后，除列表内软件外，将自动阻止所有已识别软件访问摄像头的行为

功能	说明
自动放行带有数字签名的程序	勾选后，带有数字签名的程序启用摄像头时，将默认允许，不会弹窗提示
自动放行系统核心程序	勾选后，带有系统程序启用摄像头时，将默认允许，不会弹窗提示
保存	保存当前是设置
取消和“×”	关闭窗口，不保存设置

在火绒发现软件需要启动摄像头时会弹出提示弹窗，当您勾选【记住本次操作，下次自动处理】时，会自动添加一条对应规则至列表中。

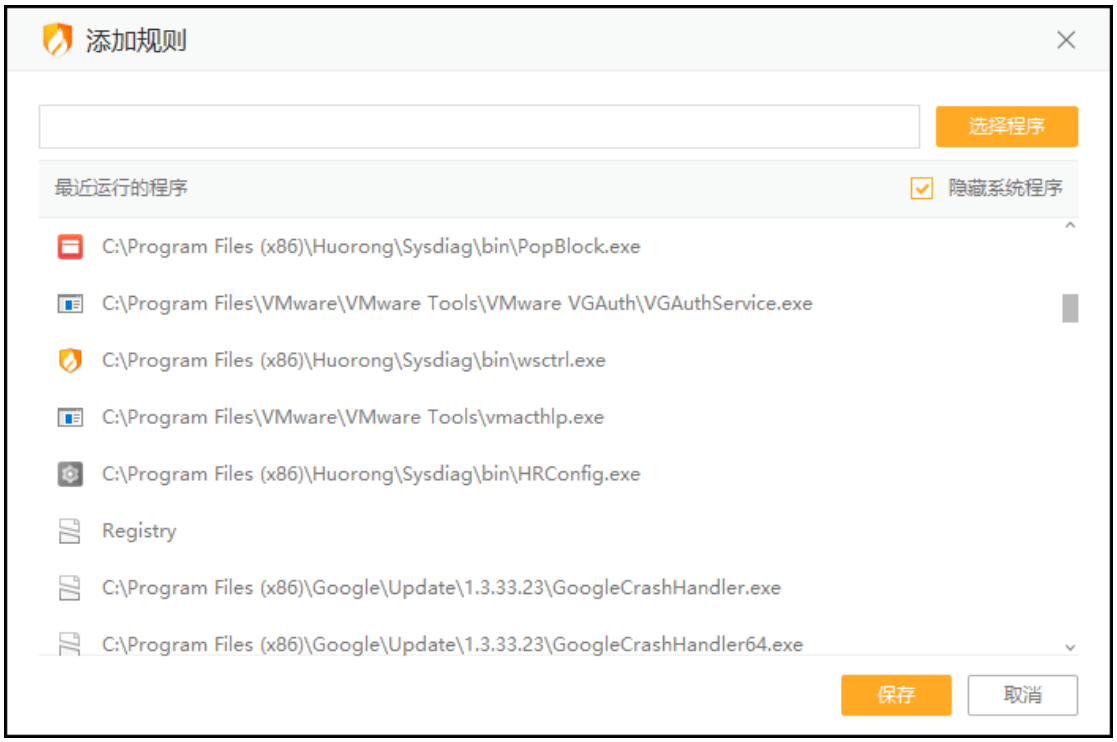


4） 联网控制设置说明

您可在联网控制设置中调整列表中程序的联网行为、添加新的程序联网规则、以及调整当前联网控制触发时机。

功能	说明
编辑	编辑选中的规则
删除	删除所有选中的规则
导入	点击后选择需要导入的规则，点击确定等待规则导入完成
导出	将导出所有选中的规则，点击后选择保存位置点击确定，等待导出完成
清除无效规则	删除所有无效的规则 无效规则判定：对应路径下已无该程序
联网设置	打开联网设置（见下图）
添加规则	点击打开添加程序窗口（见下图）

点击【添加规则】，弹出添加程序窗口（见下图）。此窗口支持拖拽添加程序，还支持使用通配符来批量添加需要限速的程序。



功能	说明
隐藏系统程序	默认勾选，在最近运行的程序列表中自动隐藏系统程序
保存	保存当前规则，添加至规则列表中
取消	退出添加规则状态，不保存当前规则

联网控制在开启后，除了用户手动设置阻止联网的程序外，均默认允许联网。如您希望调整此规则，您可点击【联网设置】， 根据需要选择适合您的模式：

功能	说明
允许联网	除了您阻止联网的程序以外，均默认允许其他程序联网。
阻止联网	除了您允许联网的程序以外，均默认阻止其他程序联网。
询问我	未在联网控制中设置的其他程序联网时，会增加弹窗提示。此项默认勾选。
自动放行带有数字签名的程序	选择阻止联网或询问我时启用，勾选后自动允许所有带有数字签名的程序联网。
自动放行系统核心程序	选择阻止联网或询问我时启用，勾选后自动允许系统核心程序联网。此项默认勾选。

当您在软件设置中选择询问我（默认选项）时，每当有联网控制以外的程序发送联网请求，联网控制会增加弹窗提示（见下图），您可根据需要选择对这个动作的处理方式。您也可勾选【记住本次操作】后点击允许/阻止，添加一条允许/阻止联网的规则到联网控制中。您仍可在联网控制中修改或删除此规则。

网络防护

1） 网络入侵拦截设置说明

您可在设置中调整当发生黑客入侵或其他网络入侵行为时火绒需进行的操作。

功能	说明
仅记录	发现入侵行为时，只在安全日志中记录入侵行为
自动处理	发现入侵行为时，在安全日志中记录并阻止入侵行为

2） 对外攻击拦截设置说明

您可在设置中调整当本机发生对外攻击行为时火绒需进行的操作。

功能	说明
仅记录	不阻止对外攻击行为，只在安全日志中记录攻击行为
自动处理	阻止对外攻击的行为，并且在安全日志中记录攻击行为

3） 僵尸网络防护设置说明

当您的计算机被非法远程控制时火绒需进行的操作。

功能	说明
仅记录	在安全日志中记录计算机被远程控制
自动处理	阻止远程控制，并记录至安全日志中

4） 远程登录设置说明

当您的计算机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时火绒需进行的操作。

功能	说明
仅记录	不阻止密码破解攻击，只在安全日志中记录攻击行为
自动处理	阻止密码破解攻击，并在安全日志中记录攻击行为

5） Web 服务保护设置说明

当黑客对安装了服务器软件的计算机发起攻击，入侵您计算机的服务器软件时火绒需进行的操作。

功能	说明
仅记录	不阻止对服务器软件的攻击，只在安全日志中记录攻击行为
自动处理	阻止对服务器软件的攻击，并在安全日志中记录攻击行为

6） 恶意网址拦截设置说明

调整需要拦截的网址类型，同时还能自定义添加需要拦截的网站。

功能	说明
编辑	编辑选中的规则
删除	删除所有选中的规则
导入	点击后选择需要导入的规则，点击确定等待规则导入完成
导出	将导出所有选中的规则，点击后选择保存位置点击确定，等待导出完成
添加规则	点击添加规则打开规则添加页面（见下图）

功能	说明
保存	保存当前规则，添加至规则列表中
取消	关闭添加规则窗口，不保存当前规则

高级防护

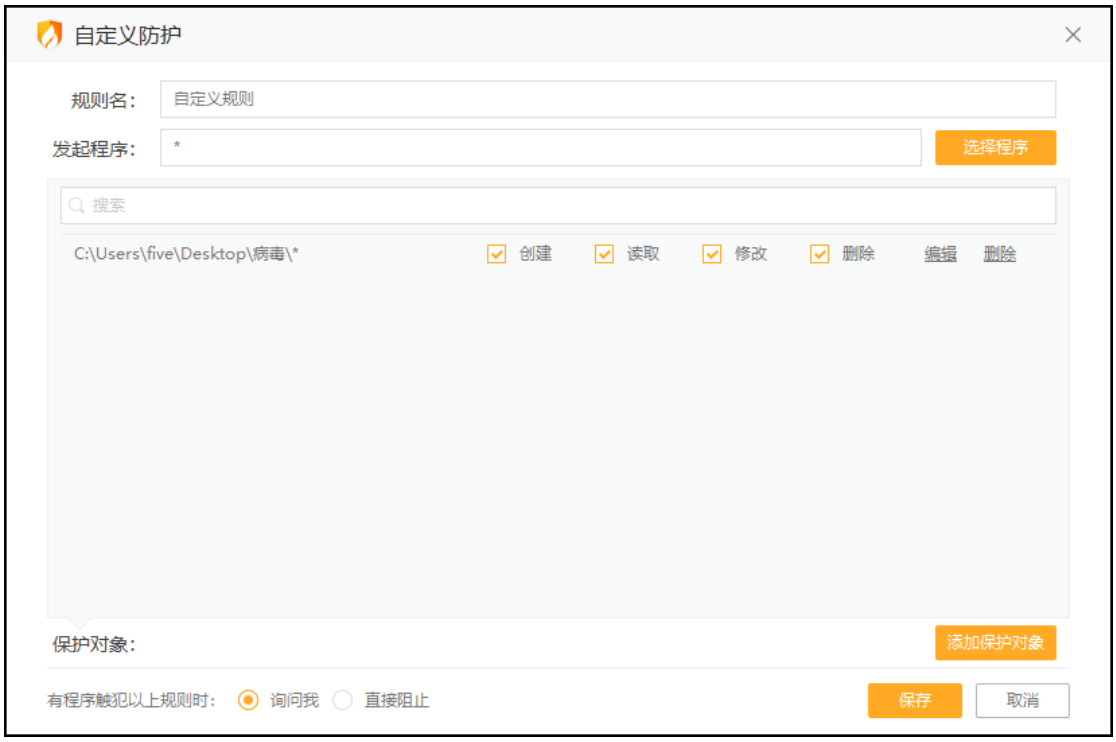
1） 自定义防护设置说明

您可在自定义防护设置中添加自定义防护规则，以及查看并管理所有您创建的自定义规则。自定义防护设置中包含自定义规则和自动处理两部分内容。您可点击顶部的标签，切换页面。

自定义防护-自定义规则：

点击【自定义规则】（见下图），进入自定义规则页面。

功能	说明
状态开关	开关橘色表示规则启用，开关灰色表示规则未启用
编辑	编辑选中的规则
删除	删除所有选中的规则
导入	点击后选择需要导入的规则，点击确定等待规则导入完成
导出	将导出所有选中的规则，点击后选择保存位置点击确定，等待导出完成
添加规则	点击添加规则进入自定义防护规则添加页面（见下图）



功能		说明
规则名		开关绿色表示规则启用，开关灰色表示规则未启用
发起程序		选择需要控制操作的程序，支持通配符
搜索		可针对保护对象内容进行搜索
保护对象	添加	添加阻止程序操作的对象，点击后显示添加保护对象页面（见下图）
	多项操作	点击可快速切换保护动作
	编辑	编辑选中规则
	删除	删除所有选中规则
记录日志		勾选后，每当有程序触发此规则时，火绒会自动记录至安全日志中
有程序触犯以上规则时	询问我	弹出提示弹窗，让您来自主处理威胁
	直接阻止	火绒将直接阻止程序操作，不再询问您

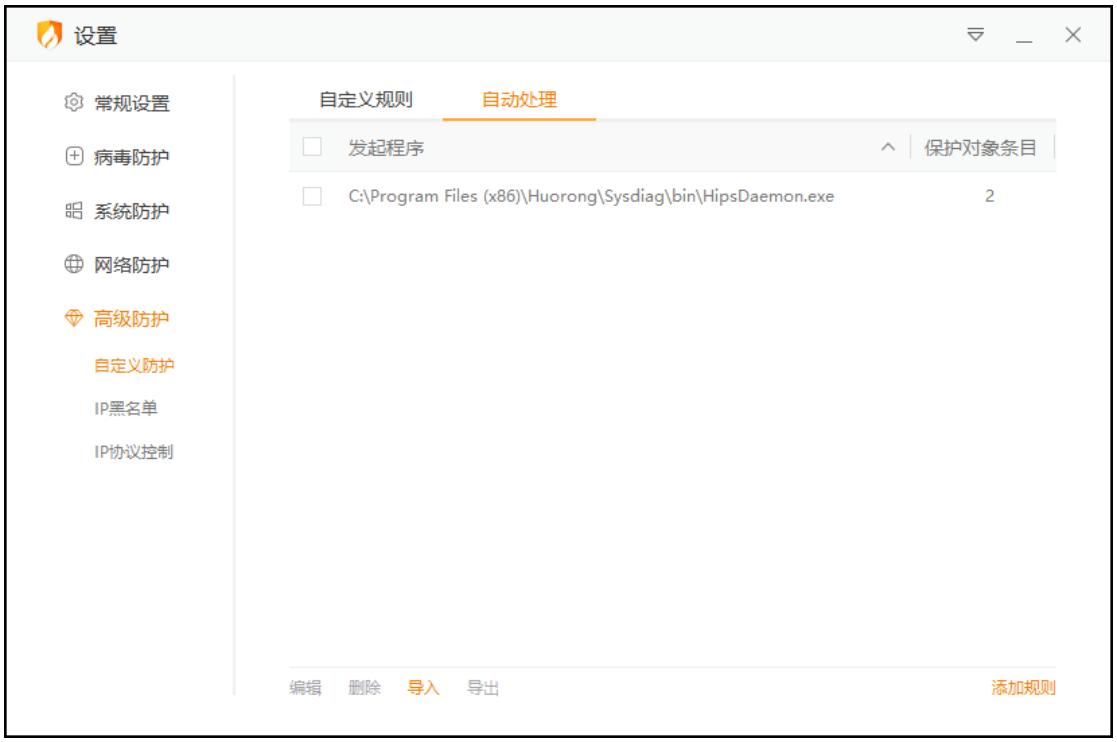
保存	保存当前规则，添加至自定义防护规则列表中
取消	点击关闭弹窗，不保存规则

添加规则-添加保护对象

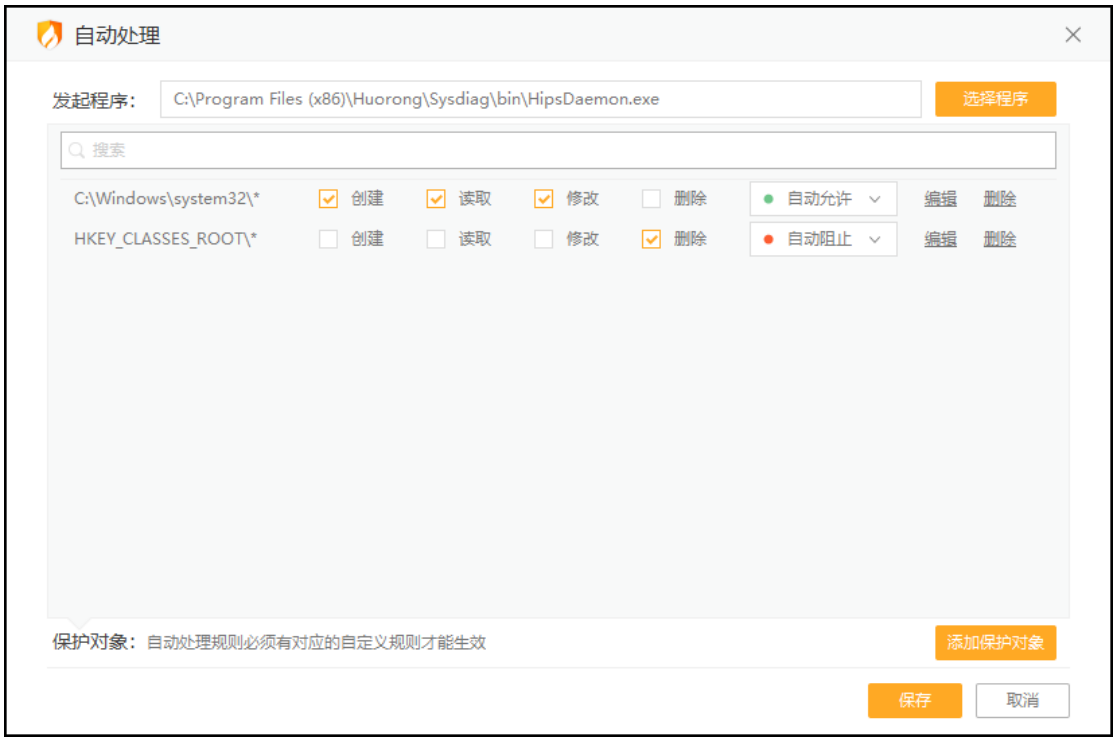
功能		说明
保护对象	文件规则	选择需要保护的文件，勾选需要阻止的操作，保护动作可选择创建、读取、写入、删除四项操作限制
	注册表规则	选择需要保护的注册表，勾选需要阻止的操作，保护动作可选择创建、读取、写入、删除四项操作限制
	执行规则	阻止程序运行其他程序，保护动作默认勾选执行且不可取消勾选
保存		保存此规则，添加至自定义防护规则列表中
取消		关闭添加保护对象页，不保存规则

自定义防护-自动处理：

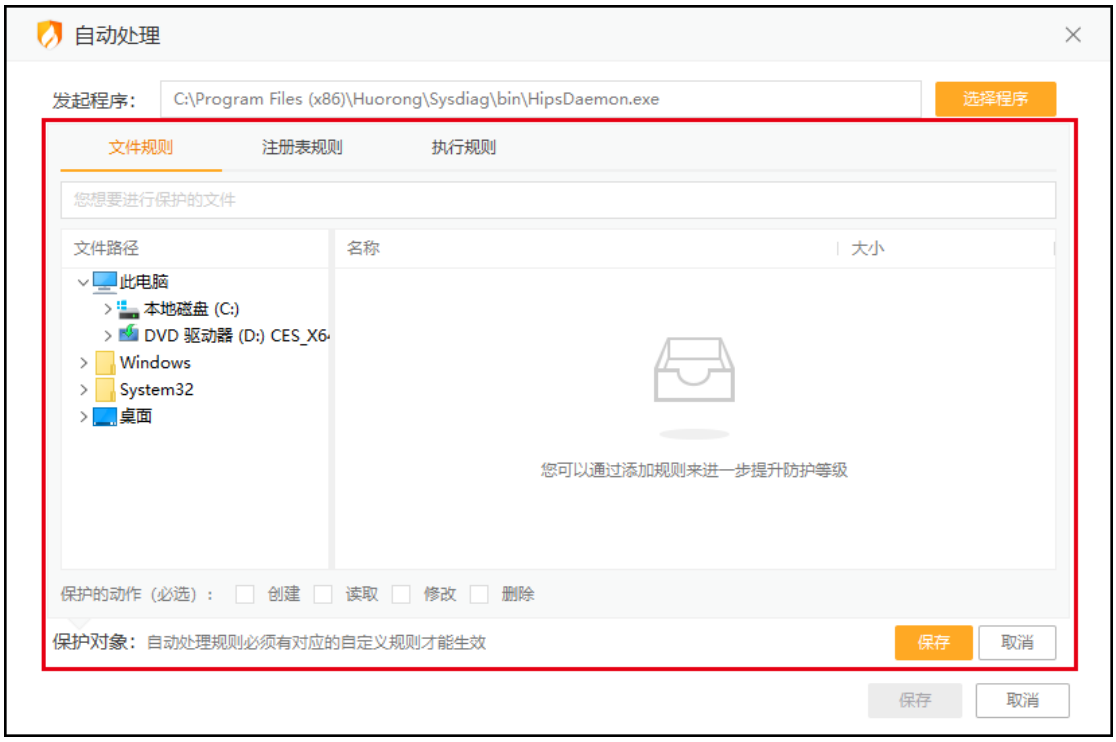
自动处理规则必须有对应的自定义规则才能生效，自动处理规则的优先级高于自定义规则。点击【自动处理】（见下图）进入自动处理规则页面。



功能	说明
编辑	编辑选中的规则
删除	删除所有选中的规则
导入	点击后选择需要导入的规则，点击确定等待规则导入完成
导出	将导出所有选中的规则，点击后选择保存位置点击确定，等待导出完成
添加规则	点击添加规则进入自动处理规则添加页面（见下图）



功能		说明
发起程序		选择需要阻止操作的程序，支持通配符
搜索		可针对保护对象内容进行搜索
保护对象	添加	添加阻止程序操作的对象，点击后显示添加保护对象页面（见下图）
	编辑	编辑选中规则
	删除	删除所有选中规则
记录日志		勾选后，每当有程序触发此规则时，火绒会自动记录至安全日志中
保存		保存当前规则，添加至自定义防护规则列表中
取消		点击关闭弹窗，不保存规则



功能		说明
保护对象	文件规则	选择需要保护的文件，勾选需要阻止的操作，可选择创建、读取、写入、删除四项操作限制
	注册表规则	选择需要保护的注册表，勾选需要阻止的操作，可选择创建、读取、写入、删除四项操作限制
	执行规则	阻止程序运行其他程序
保存		保存此规则
取消		关闭添加保护对象页，不保存规则

自动处理规则，除了可手动添加外，还可自动添加。当有程序触发自定义防护规则时，会弹出提示弹窗，当您勾选【记住本次操作，下次自动处理】选择允许/阻止后，将会自动添加一条对应规则至自动处理中。

2） IP 黑名单设置说明

您可在 IP 黑名单设置中管理黑名单中的所有 IP，同时还支持规则的导出与导入，方便您的操作。

功能	说明
编辑	编辑选中规则
删除	删除所有选中的规则
导入	点击后选择需要导入的规则，点击确定等待规则导入完成
导出	将导出所有勾选的规则，点击后选择保存位置点击确定，等待导出完成
添加规则	点击添加规则弹出 IP 黑名单添加弹窗（见下图）

功能	说明
远程 IP	填写您需要屏蔽的 IP 地址，多个 IP 请换行输入，IP 范围使用
备注	方便您辨识规则，可不填写
保存	保存当前规则，添加至 IP 黑名单规则列表中
取消	点击关闭弹窗，不保存规则

3） IP 协议控制设置说明

IP 协议控制是在 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。您可以根据自己的需要选择启用，同时您也可以自己编写 IP 协议规则。通过设置可以管理 IP 协议控制的相关规则。

功能	说明
状态开关	开关橘色表示规则启用，开关灰色表示规则未启用
编辑	编辑勾选规则
删除	删除所有勾选的规则
删除	删除所有勾选的规则
导入	点击后选择需要导入的规则，点击确定等待规则导入完成
导出	将导出所有勾选的规则，点击后选择保存位置点击确定，等待导出完成
添加规则	点击添加规则进入 IP 协议控制规则添加页面（见下图）

功能	说明
规则模板	为您提供了多个常用规则模板，选择后可快速设置添加规则页面
规则名称	您可以自定义此规则名称
应用程序	选择适用的应用程序，不填写默认为针对所有应用程序
操作	针对触发复合下列设置的条件行为，是放行还是阻止
方向	控制联网方向
协议	选择适用的网络协议
本地 IP	设置电脑本地的物理 IP
本地端口	设置电脑本地的物理端口

远程 IP	设置需要访问的远程 IP 地址
远程端口	设置需要访问的远程端口
优先级	选择该条规则优先级，当 IP 协议的规则冲突时优先执行优先级较高的规则。优先级 1 为最高级
保存	保存此规则
取消	关闭 IP 协议控制规则添加页面，返回至 IP 协议控制规则列表首页，不保存规则

按照上图中填写的规则进行保存，产生的规则含义是：

放行所有进出站采用 TCP 协议，并且通过本地全部 IP 和端口访问所有远程 IP 和端口的行为，规则优先级为 1。

管理设置

当您需要恢复设置的默认状态或是将规则设置导出并在另一台电脑上运行时，管理设置就能很好的满足您的需求。您可在安全设置的右上角找到【菜单按钮】（见下图）。

功能	说明
恢复默认设置	将回复您在火绒中修改的所有设置为默认状态，点击后弹出恢复默认设置提示弹窗（见下图）。点击确定恢复默认设置，点击取消和“×”关闭弹窗不恢复默认设置
导出设置	导出当前设置，点击后选择保存位置点击确定，等待导出完成即可
导入设置	点击后选择需要导入的规则，点击确定等待规则导入完成，即可导入设置

安全日志

安全日志是安全杀毒软件的一项基础功能，您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。

功能介绍

您可在首页的下来菜单中找到【安全日志】（见下图），打开安全日志。

在安全日志中，您可根据需要选择您要查看的内容。

功能	说明
时间	提供了【全部】、【今天】、【最近三天】、【最近七天】、【最近三十天】时间选择
类别	根据情况选择要查看的列表，共有全部、病毒防护、系统防护、网络防护、高级防护、其他等
功能	根据选择的【类别】显示需要具体查看的功能
概要	阐述当前日志的简单情况
查看详情	选中需要查看的日志，即可在下方显示该条日志详情
刷新	刷新当前日志列表
项目数	根据筛选条件，显示符合当前条件的日志总条数
清空本页日志	将符合筛选条件的日志全部清空
导出本页日志	将符合筛选条件的日志全部导出

安全日志设置说明

您可在设置中修改安全日志的保存天数。打开安全设置，在常规设置-基础设置找到【日志保存天数】(见下图)，选择对应天数即可。您也可选择自定义，手动填写安全日志需要保存的天数。

软件升级

升级方式

当前您可通过以自动升级或手动升级的方式来升级火绒至最新版本。

1) 自动升级

火绒默认使用自动升级，当火绒需要升级更新时，会自动与火绒服务器连接，进行升级，让软件时刻保持在最新状态，以保证病毒库和功能都是当前最完善的。当火绒升级完毕时会弹出弹窗提示您。

部分升级完成后需重启电脑，火绒推荐您在保存好文件后及时重启电脑，保证火绒各项功能与配置均处于最新状态，以最大程度保护好您的电脑。

2）手动升级

您也可通过手动升级，检查是否有可升级的内容。在下拉菜单中点击【检查升级】（见下图）、主界面中的升级按钮（见下图）以及右键火绒托盘程序，在右键快捷菜单中点击【检查升级】弹出在线升级弹窗，进行检查升级。

当有可升级的内容时，在线升级会显示：检查到最新版本（见下图），您可点击【立即升级】按钮来完成软件升级。

设置说明

在安全设置中，常规设置-软件升级可进入软件升级的设置页面。可对软件升级方式、升级提示、升级代理进行调整修改。

功能	说明
升级方式	您可根据需要选择升级方式，火绒推荐您保持自动升级
升级提示	勾选后自动更新完成时将不再弹出升级完成的提示弹窗
代理设置	勾选指定服务器代理后，填写地址、端口、账号、密码。将使用代理服务器来连接火绒升级服务器
网络测试	测试当前使用的连接方式能否连接上火绒服务器

总结

在《用户使用手册》中我们详细地为您介绍了火绒安全软件各项功能的使用方法，不管您是家庭用户还是专业技术人员，火绒都能为您提供合适的病毒防护模式，全方位保护您的计算机安全。如果您在火绒的使用中遇到任何问题或有任何意见与建议，您都可以通过前往

火绒官方论坛进行反馈：http://bbs.huorong.cn/

最后，再次感谢您选择火绒安全软件！