火绒安全
HUORONG SECURITY

火绒安全软件 6.0

用户操作手册

2026/08/31

公　　司：北京火绒网络科技有限公司

地　　址：北京市朝阳区北苑路北京文化创意大厦 B 座 9 层

网　　址：https://www.huorong.cn

电　　话：400-998-3555

版权声明

目录

◆ 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（sp3 及以上）、Windows VISTA、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows 11、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、访问控制以及各类安全设置等。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

● 获取安装包

您可以访问火绒官网获取最新安装包：https://www.huorong.cn/

● 运行安装包

您需要勾选阅读并接受许可协议&隐私政策，若您不同意，则无法使用本软件。

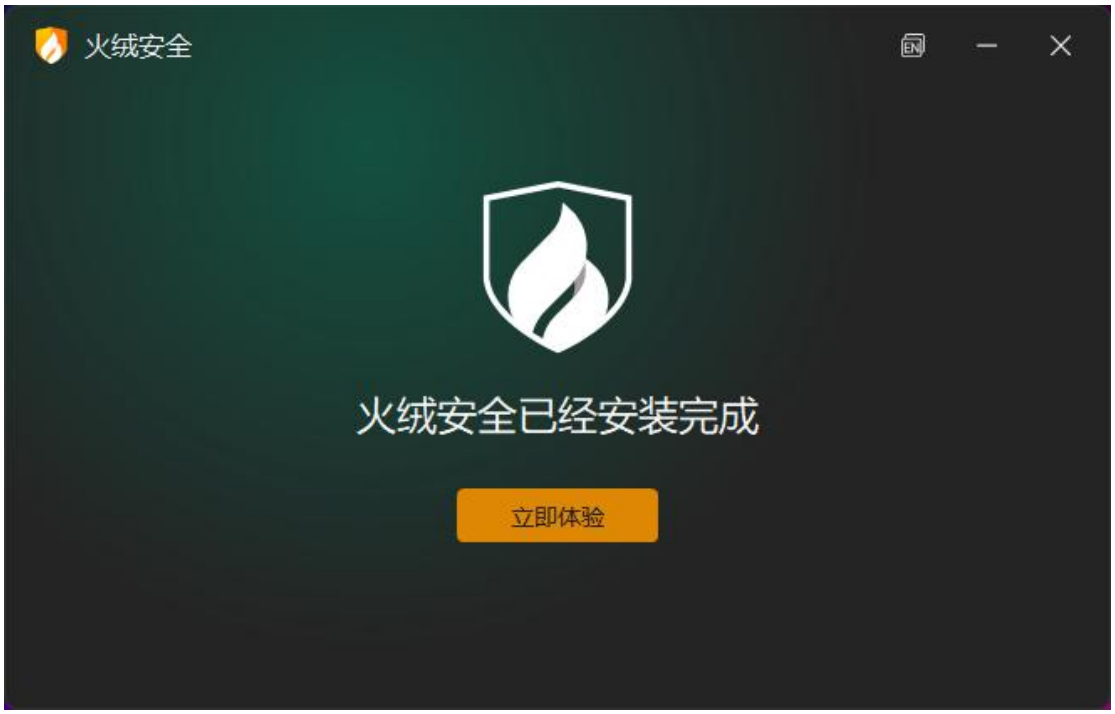
安装方式：

- 极速安装：火绒默认为极速安装，您可点击“极速安装”按钮直接进行安装，安装完成后即可使用。
- 自定义安装：当您需要将火绒安装在指定磁盘位置时可以选择此方式，您可以点击“安装目录”。

注：在展开的安装目录选择信息中，点击右侧浏览可选择您要安装的位置。

- 安装完成
  - 静待安装：耐心等待安装完成。

- 立即使用：安装完成后，点击“立即体验”即可启动火绒安全防护。



- 重启服务：因隐私设备保护等服务项需要您重启设备后才能生效，您可以根据自身需要随时选择重启。

➢ 程序主界面

功能		说明
左侧导航栏		点击左侧导航栏，可进入对应的功能模块：主页、病毒查杀、防护中心、访问控制、安全工具、火绒应用商店、安全设置。
右上角主菜单	**安全日志**	打开安全日志页
	隔离区	打开隔离区
	信任区	打开信任区
	检查更新	开始检查更新
	语言设置	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。
	问题反馈	打开火绒安全官方论坛

	病毒上报	打开火绒安全官方论坛查看病毒样本上报途径说明
	关于我们	查看火绒安全软件的许可协议，隐私政策。
快捷入口	**检查更新**	开始检查更新
	安全日志	打开安全日志页
	信任区	打开信任区
	隔离区	打开隔离区
主页建议		根据用户使用习惯和您当前计算机状态，在主页位置主动向您推送火绒的使用建议或功能推荐；多条建议时支持切换；支持对单条建议直接打开和关闭该条建议（见下图）。

➢ 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

您可通过主页（见下图）按钮处，选择查杀方式，火绒支持【快速查杀】、【全盘查杀】、【自定义查杀】3 种查杀方式，您选择合适的查杀方式后，可一键开启查杀。

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。

全盘查杀	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。 在您选择查杀位置时，提供易感染区域选择项，针对计算机易感染位置提供自定义扫描入口。

● 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。

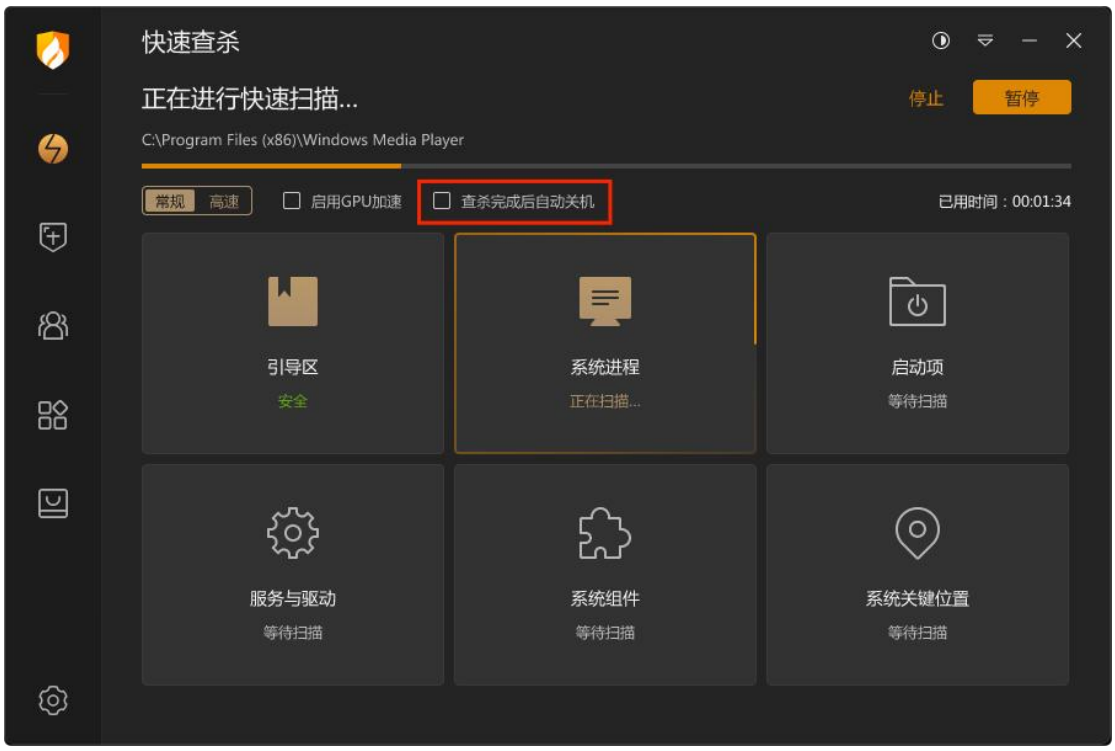
功能	说明
常规	占用较少的系统资源。
高速	占用较多的系统资源，提高扫描速度。

● 启用 GPU 加速

勾选即启用，启用后反病毒引擎会在此次扫描的适当时机使用 GPU 进行计算，进而提升扫描效率（仅 DirectX 11 及以上版本支持）。

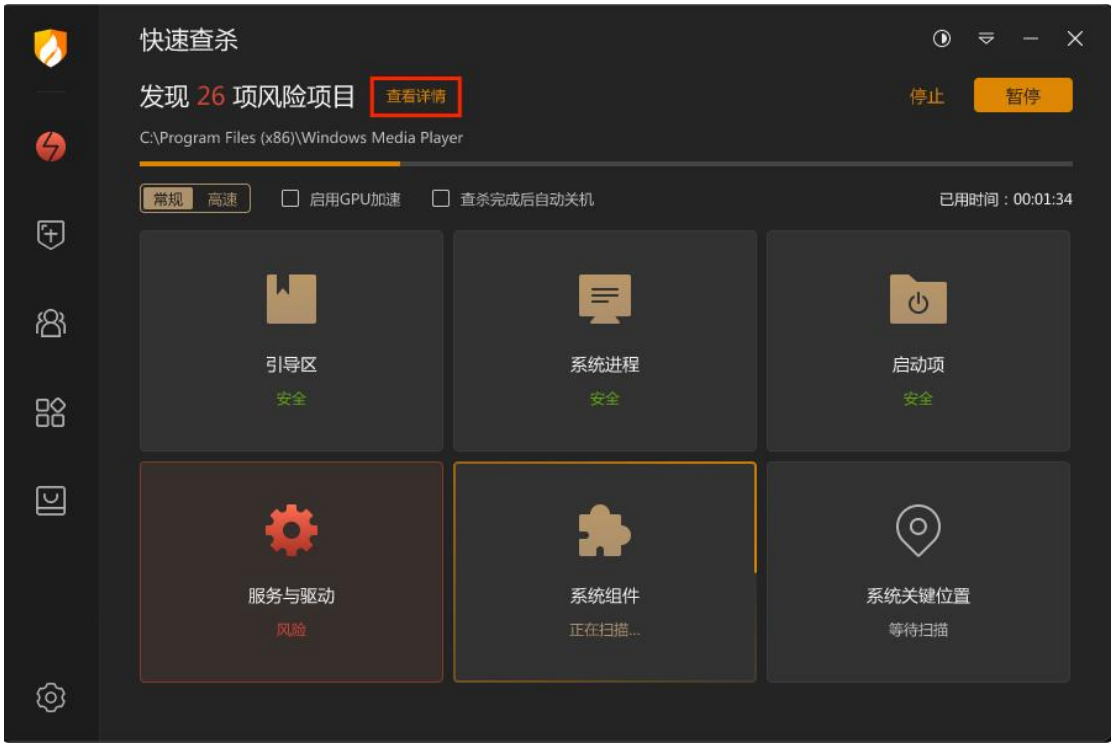
● 查杀完成后自动关机

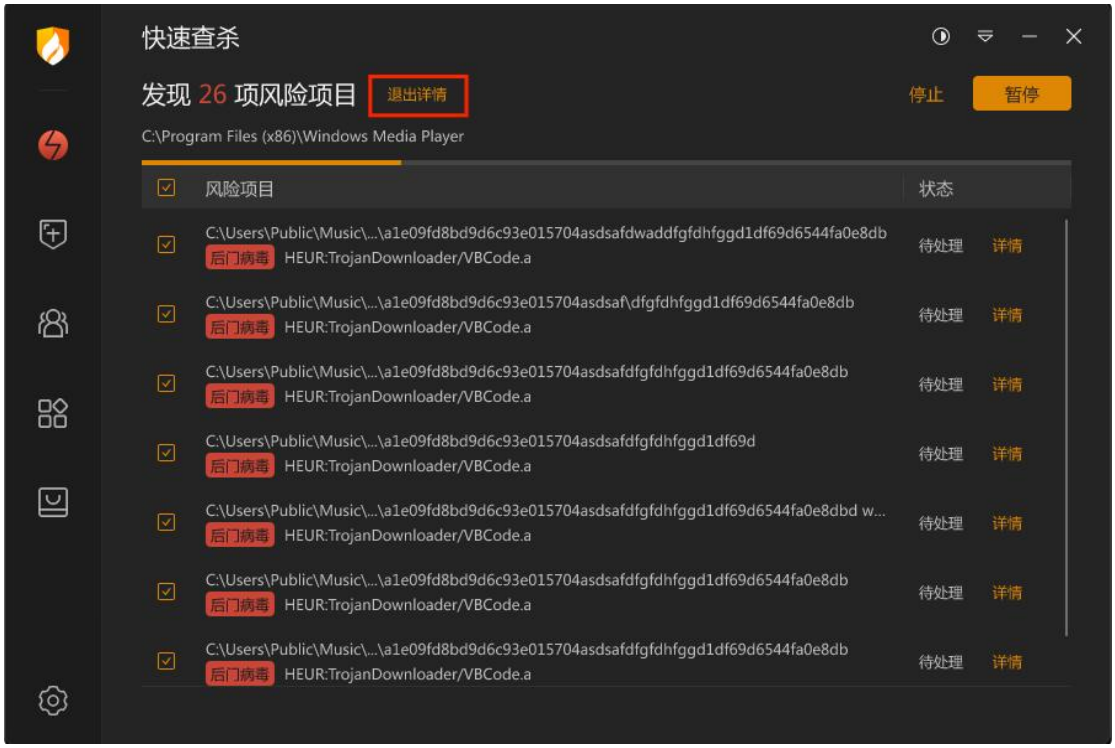
勾选即启用功能。勾选后火绒将在扫描完成时弹出关机提示（见下图），关机提示等待的时间为 25 秒，25 秒后将为您自动关闭电脑。在此期间您可点击“暂不关机”或“×”以取消自动关机。



● 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。



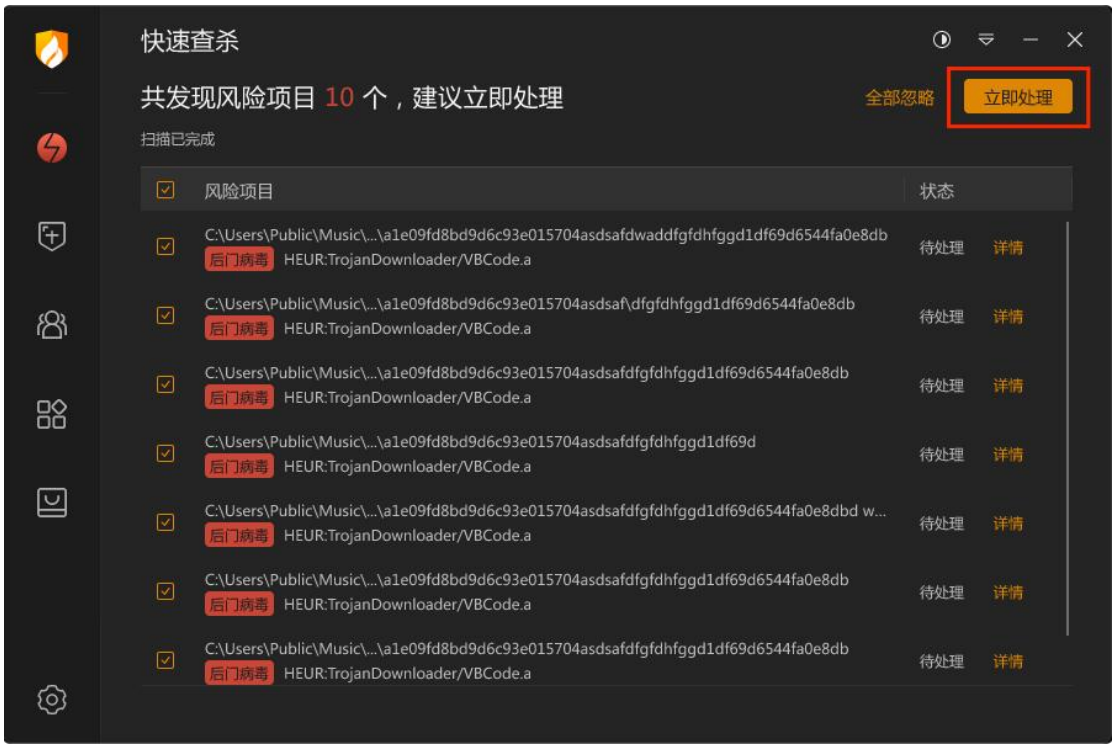


● 处理威胁

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（见下图）。



将威胁文件处理完毕后，提示扫描完成（见下图），为您展示扫描概况，将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。

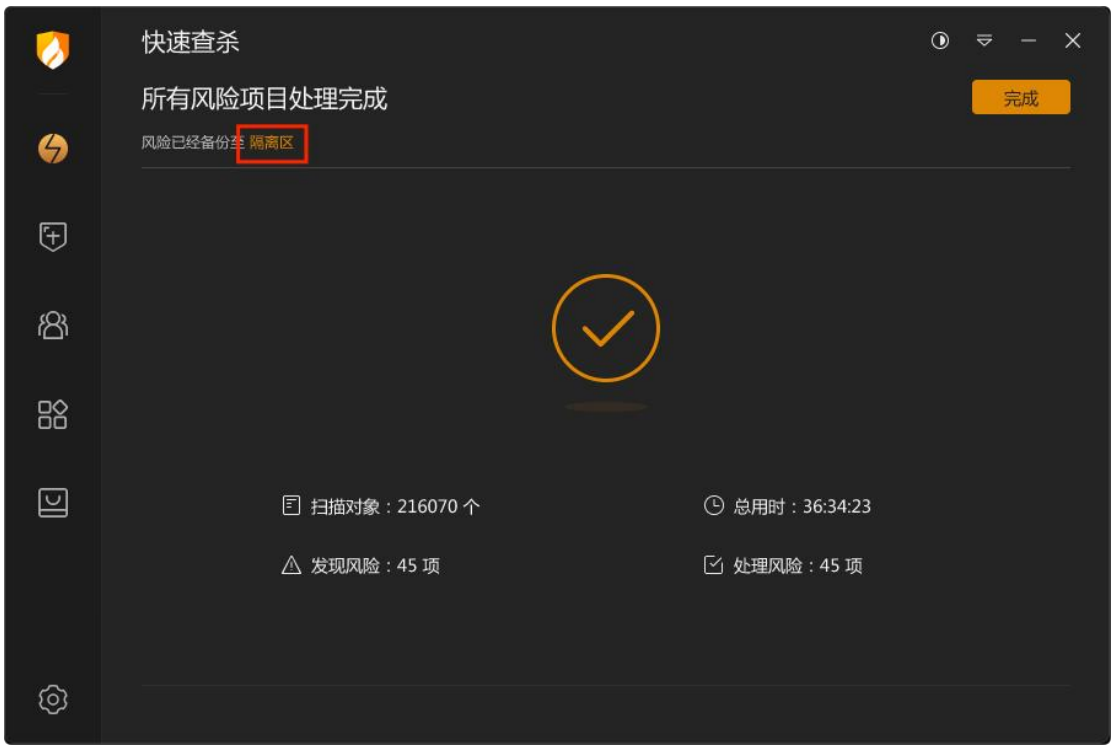
功能	说明
删除所选	将选中的文件从隔离区删除，文件不可恢复。
恢复所选	将选中的文件恢复到其原始位置，同时从隔离区删除该文件。
提取所选	将选中的文件复制至指定目录。

隔离区可以在以下四个位置进入：

➡ 1：在首页的下拉菜单中找到隔离区（见下图）。

➡ 2：点击主页快捷入口的隔离区按钮，进入隔离区（见下图）。

➡ 3：在处理风险项后的扫描报告页中可以找到隔离区（见下图）。



➡ 4：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）。

隔离区设置

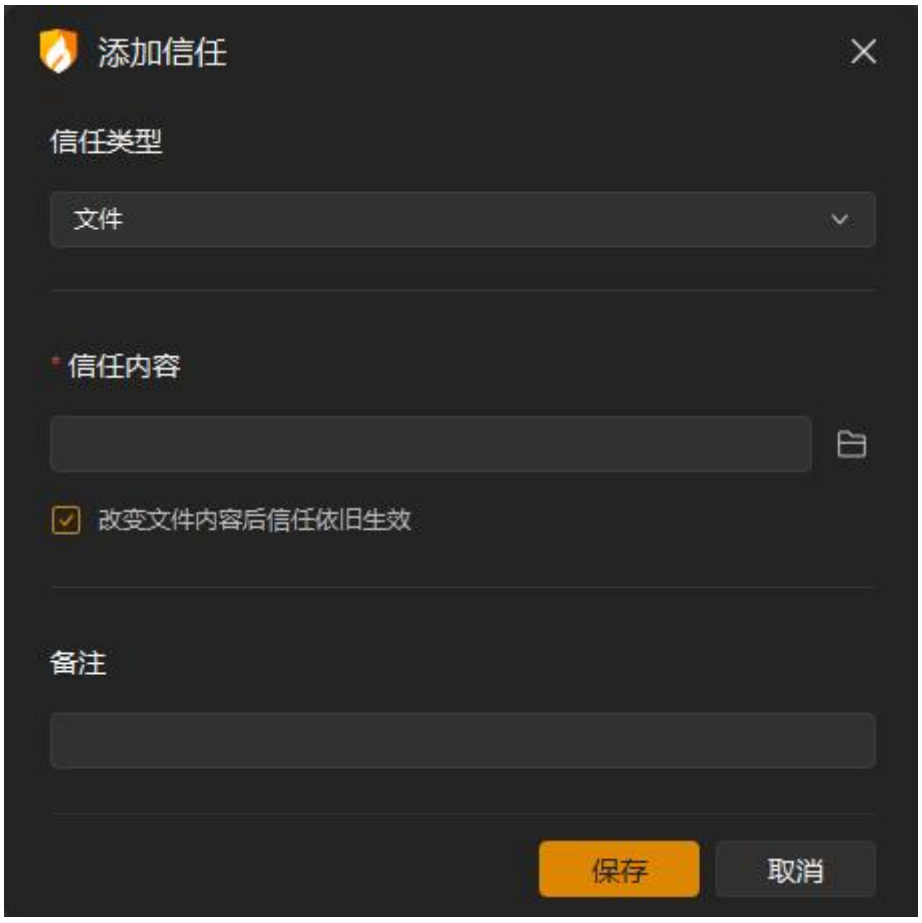
您可在【安全设置】-【常规设置】-【日志和隔离】中限制隔离区存储大小，勾选后，超过存储限制或磁盘已满时自动移除最早的隔离项。

● 信任区

您可将确认安全的文件/文件夹或网址添加到【信任区】（见下图）。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--选中数据【删除所选】。

功能	说明
删除所选	不再信任选中的信任项
清除无效项	点击【搜索】右侧开关，选择【清除无效项】，可清除信任区中对应路径下已无该文件或文件夹的项目。
编辑	重新编辑所选信任项的信息
添加信任	将需要信任的文件夹/文件/网址添加至信任区

添加信任：



功能	说明
信任类型	文件/文件夹/网址。
信任内容	选择要信任的文件/文件夹路径或填写网址地址。
改变文件内容后信任依旧生效	选择信任类型为文件类型时，可勾选此项，勾选后，您配置的信任文件将记录为文件指纹类型，改变文件内容后信任依旧生效。
备注	方便您辨别信任项，可不填写。

信任区可以在以下三个位置进入：

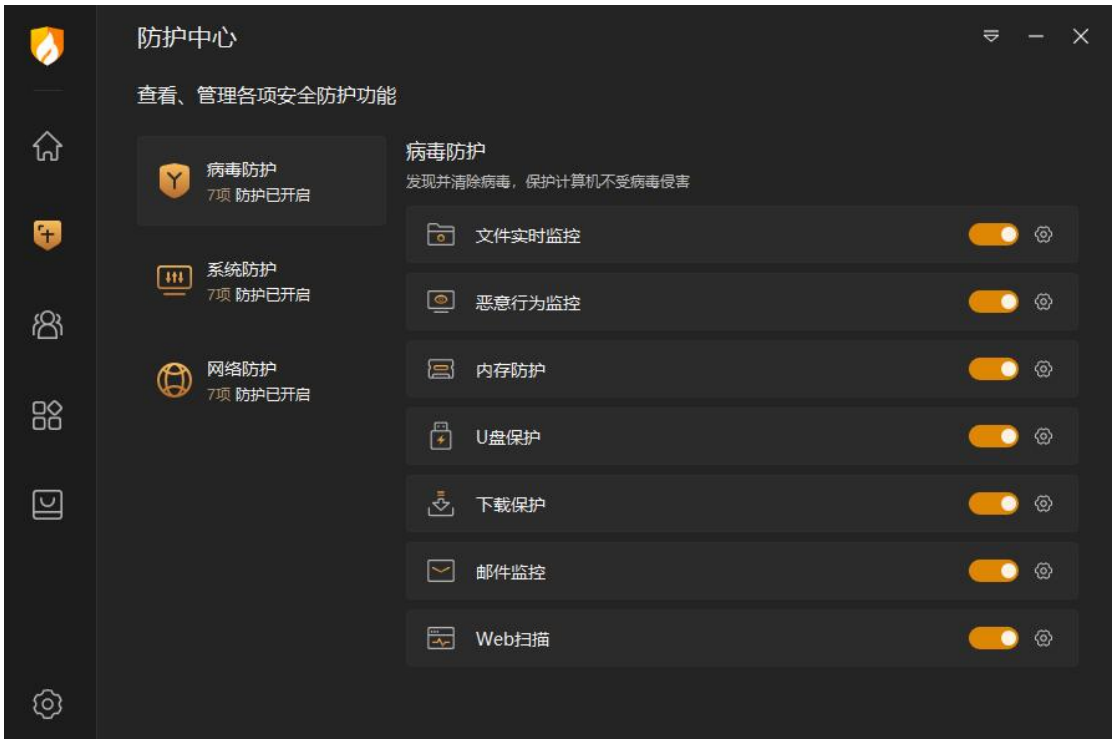
- 1：在首页的下拉菜单中可以找到信任区（见下图）。

➡ 2：点击主页快捷入口的信任区按钮，进入信任区（见下图）。

➡ 3：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）。

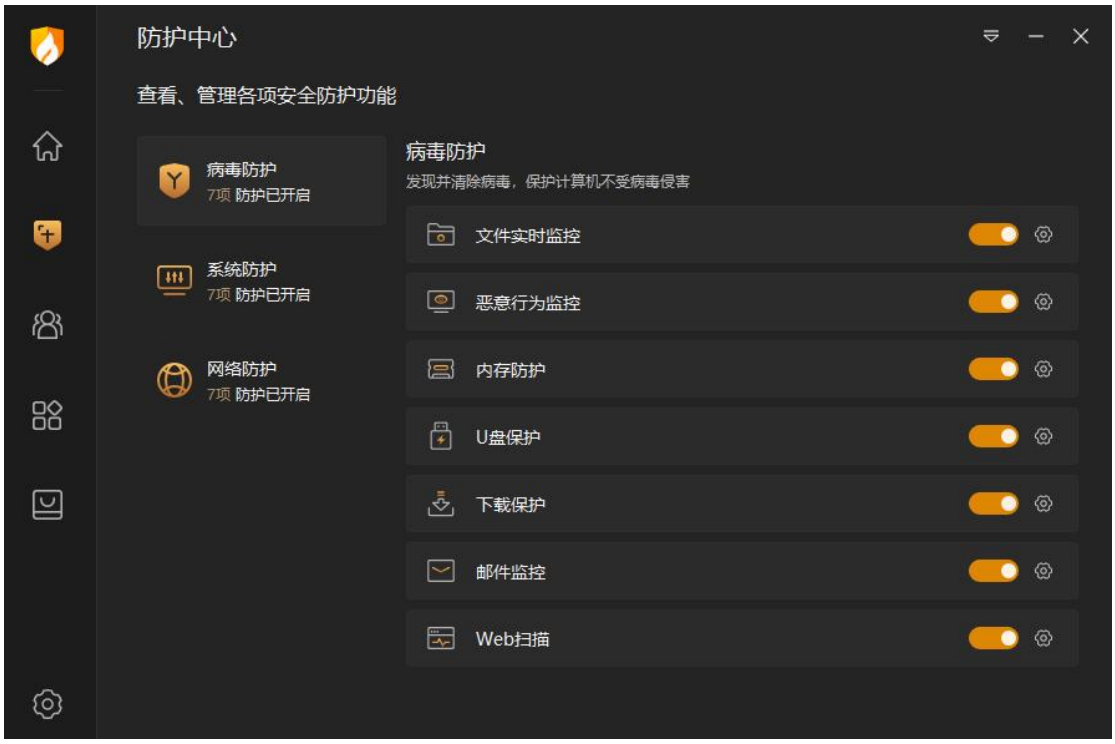
➢ 防护中心

火绒防护中心一共有三大安全模块，共包含 22 类安全防护内容。当发现威胁动作触发设定的防护项目时，火绒将为您精准拦截威胁，避免计算机受到侵害。



● 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、内存防护、U 盘保护、下载保护、邮件监控、Web 扫描 7 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：内存防护**

内存防护功能是针对混淆类恶意代码攻击和无文件攻击的场景进行深度防护，及时发现并阻止安全风险；当有威胁触发了【内存防护】时，火绒将自动清除病毒，并弹出提示弹窗（见下图）提示您。

➡ **4：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。

➡ **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。

➡ **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。

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：

➡ **7：Web 扫描**

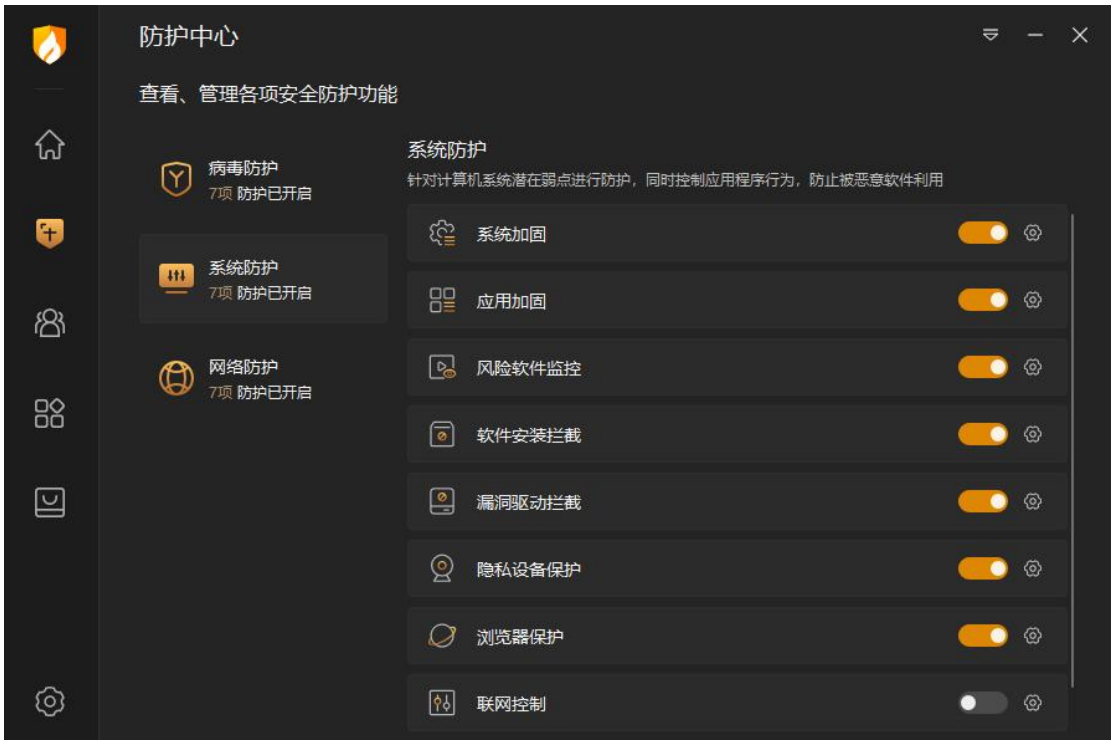
当有应用程序与网站服务器进行通讯时，Web 扫描功能会对使用 SSL 加密的数据进行病毒扫描检测，并及时阻止其中的恶意代码运行。

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、风险软件监控、软件安装拦截、漏洞驱动拦截、隐私设备保护、浏览器保护、联网控制、自定义防护 9 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：风险软件监控

此功能可设置监控不同类型的风险软件，默认仅监控潜在不受欢迎软件；当潜在不受欢迎软件运行时，将会弹窗询问用户如何处理，弹出以下弹窗（如下图）。

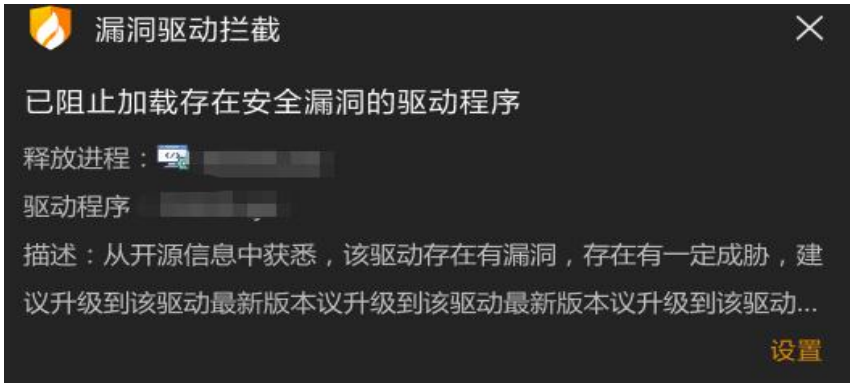
➡ **4：软件安装拦截**

火绒会根据用户举报，将出现未经允许安装到用户计算机行为的软件，加入到安装拦截列表中，在其他用户安装相同软件时进行弹窗提示（如下图）。

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。

➡ **5：漏洞驱动拦截**

火绒漏洞驱动拦截功能可有效管控具有风险的驱动的加载行为。默认选择“自动阻止”，当加载存在安全漏洞的驱动时将自动阻止且弹窗（见下图）提示您。



➡ **6：隐私设备保护**

火绒隐私设备保护默认选择“仅通知”，当有电脑软件要启用您的摄像头或麦克风时弹窗（见下图）提示您，您可以根据需要在隐私设备保护的保护设置中设置是否允许电脑软件启用摄像头或麦克风。

7：浏览器保护

浏览器保护（见下图）能保护您的浏览器首页不被随意篡改，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。

8：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。

9：自定义防护

自定义防护通过设置自定义防护规则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。

● 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、横向渗透防护、对外攻击拦截、僵尸网络防护、暴破攻击防护、Web 服务保护、恶意网址拦截 7 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：横向渗透防护

主要防护内网（局域网）中的其他已经中毒电脑对本机的渗透，阻断病毒木马的传播和扩散。

当发现有横向渗透行为时，火绒将阻止渗透行为，并通过托盘信息通知您。

3：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。

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。

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。

➡ **5：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。

➡ **6：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。

➡ **7：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（支持识别 https 协议网址），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，部分网址支持在浏览器中显示拦截提示（见下图 1），不支持在浏览器中显示拦截提示的将在电脑右下角弹窗通知（见下图 2）。

注：自定义的恶意网址规则通知弹窗中不支持提交误报申诉。

图 1

图 2

➢ 访问控制

当有访客使用您的电脑时，您可以使用上网时段控制、程序执行控制、网站内容控制、USB 设备控制、IP 协议控制、IP 黑名单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。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。

● 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。

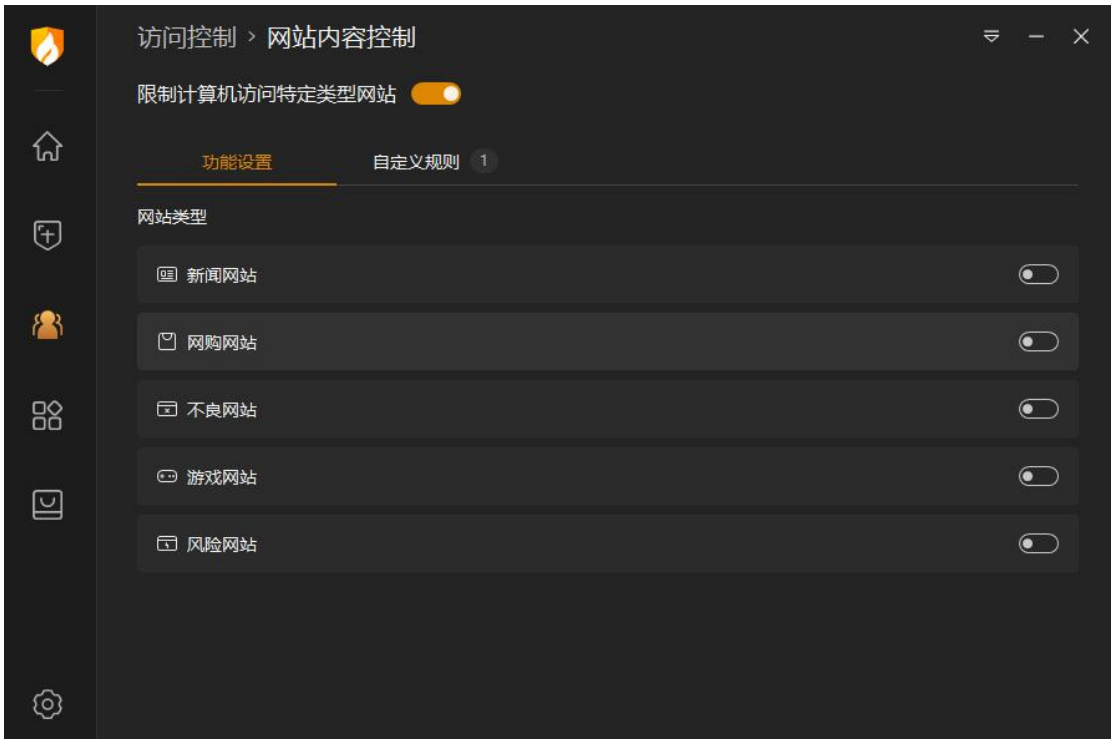
当前提供两种限制方式：【控制上网时段】和【控制累计时间】。

功能	说明
控制上网时段	以一星期（一周）为周期，将可上网时间段作为限制，管控每天可上网的时间。 点击【添加时段】，可快速将限制时间批量添加至目标限制日期下。 鼠标悬浮网格中的某行，单击，可针对该行对应的日期添加限制时间。
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。
功能开关	开启，即上网时段控制功能生效。 关闭，即上网时段控制功能未生效。

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

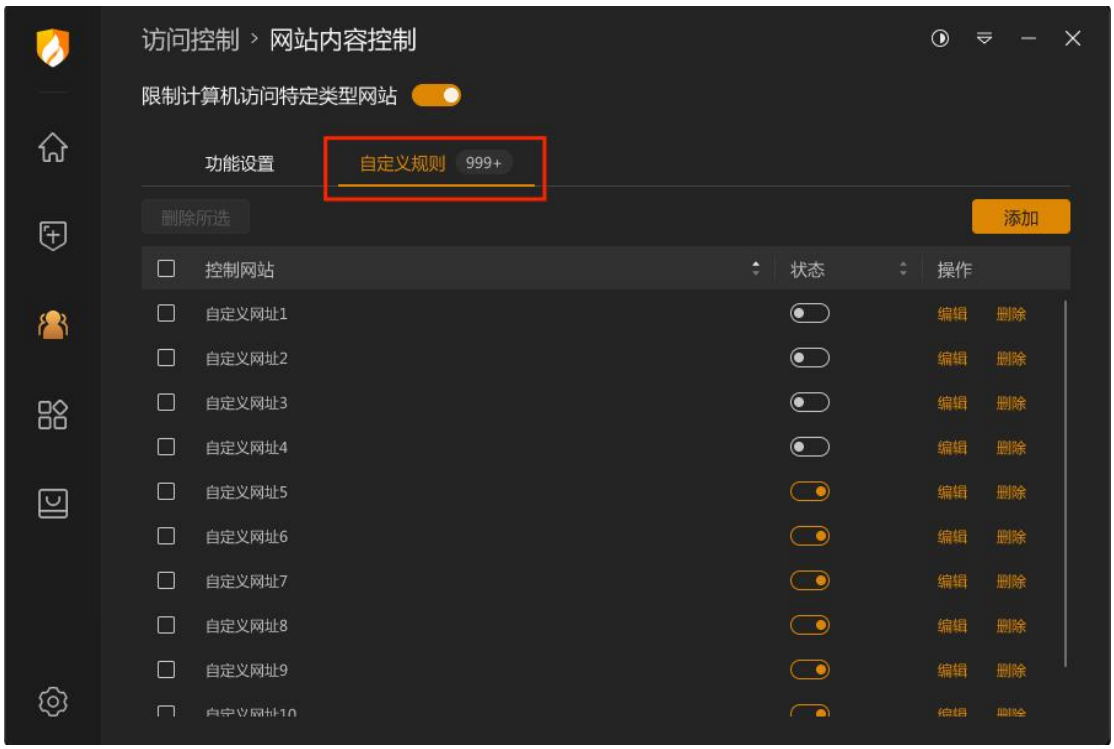
● 网站内容控制

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
功能开关	开启，即网站内容控制功能生效。 关闭，即网站内容控制功能未生效。
网站类型开关	功能开关开启后： 开启，即所选网站类型网站内容控制功能生效。 关闭，即所选网站类型网站内容控制功能未生效。
自定义规则	您可自定义添加需要屏蔽的网址，点击后打开添加拦截网址弹窗。

除了火绒内置了 5 项常用的基础规则，您还可根据需要通过【自定义规则】添加其他需要屏蔽的网址。



功能	说明
添加	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）。
编辑	编辑选中规则
删除所选	删除所有选中的规则
功能开关	您添加的自定义规则，必须在网站内容控制开启时才生效， 您可通过每条规则后的状态开关，自定义调整规则是否生效。

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，支持识别 https 协议网址。 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，部分网址支持在浏览器中显示拦截提示（见下图 1），不支持在浏览器中显示拦截提示的将在电脑右下角弹窗通知（见下图 2）。

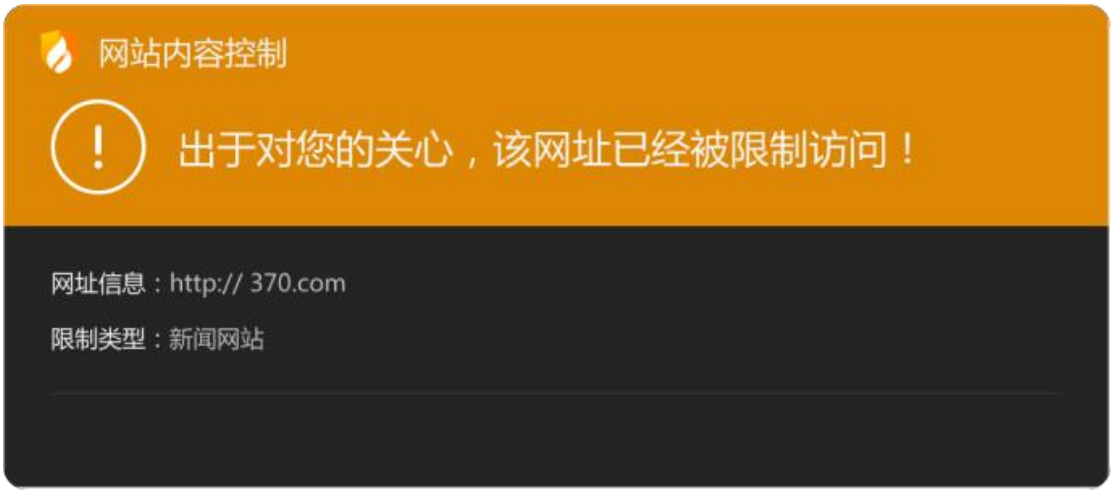


图 1

图 2

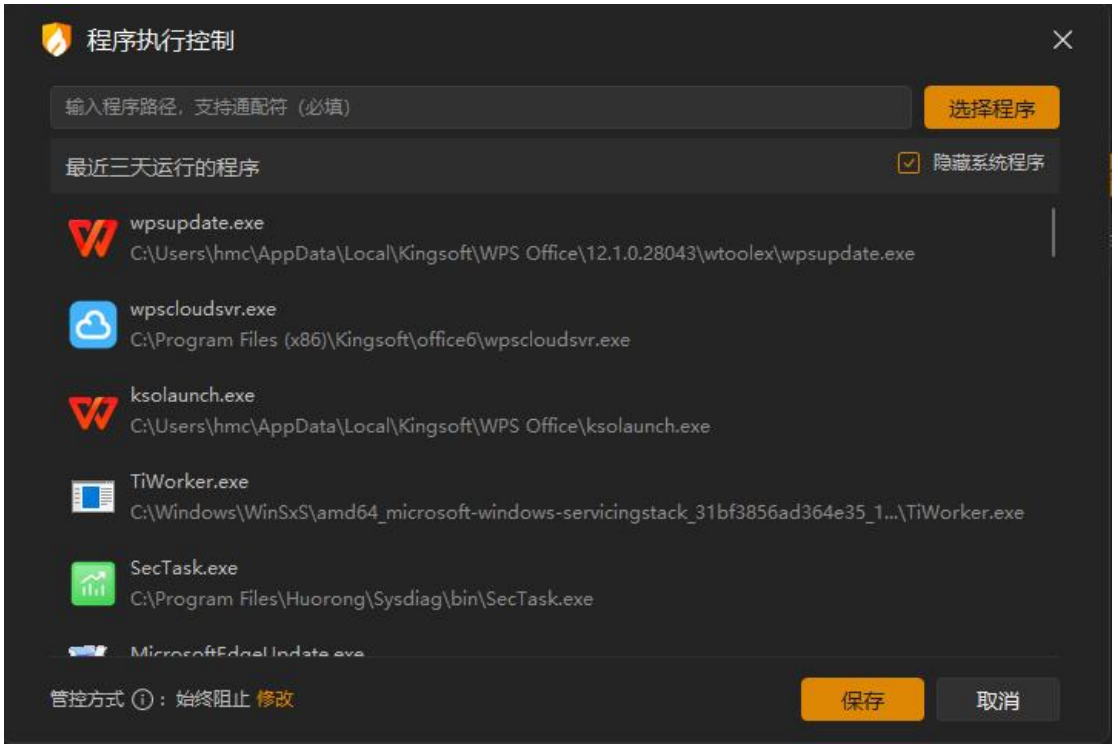
● 程序执行控制

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，以限制某个程序在电脑中的使用。

功能	说明
功能开关	开启，即程序执行控制功能生效。 关闭，即程序执行控制功能未生效。
阻止程序执行时弹窗通知	默认勾选；取消勾选后，阻止程序执行时将不会弹窗通知。
阻止程序执行时记录日志	默认勾选；取消勾选后，阻止程序执行时将不会记录日志。
拦截规则	点击进入拦截规则页面，管理您想要限制执行的程序（见下图）。

功能	说明
添加	支持 2 种方式添加规则：自定义选择程序路径、从规则库中选择程序。
删除	删除选中程序。
编辑	修改程序或管控方式。
管控方式	支持批量修改选中程序的管控方式。
状态开关	开启：规则生效，将按照管控方式设置限制对应的程序执行。 关闭：规则未生效。
搜索	支持通过程序或程序类型模糊搜索。
筛选	支持快速筛选不同管控方式的规则：始终阻止、按时段放行。

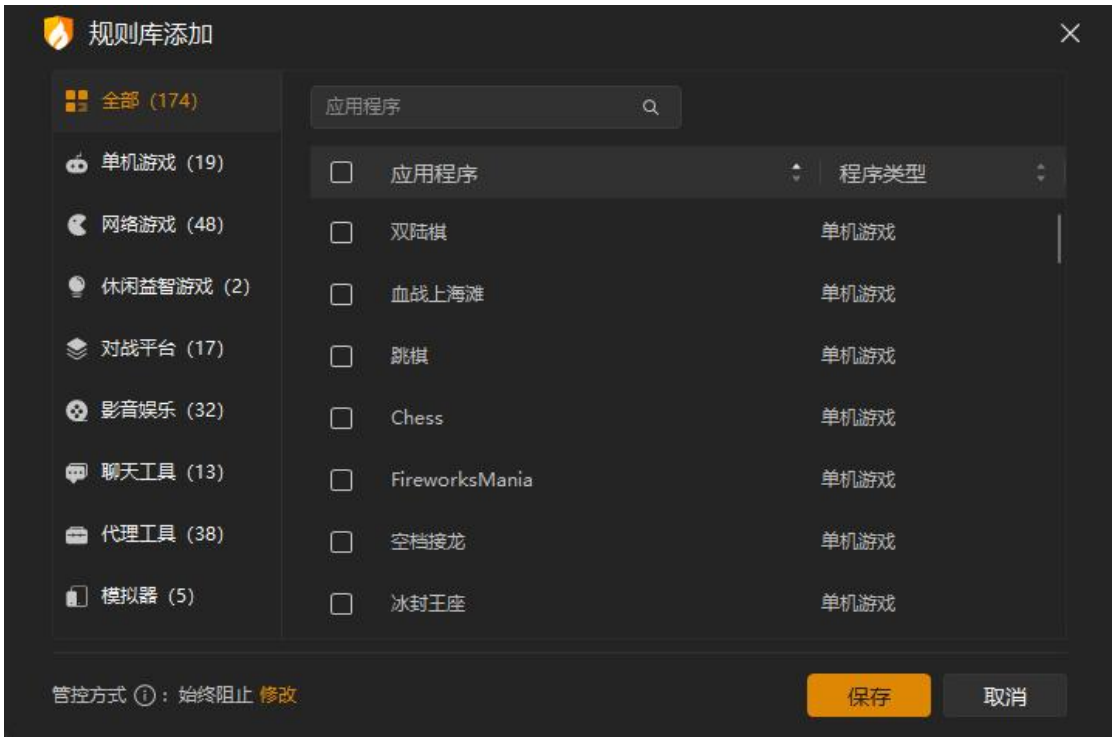
添加方式为【自定义添加】时：



功能	说明
选择程序	手动选择程序或快速在最近三天运行的程序中选择目标程序。
管控方式	默认管控方式为“始终阻止”，添加后将一直阻止程序运行。 若您需要程序在指定时间放行，其余时间阻止执行，可点击【修改】，进入管控方式页（见下图），调整管控方式为“按时段放行”。
保存	保存此规则。
取消	关闭窗口。

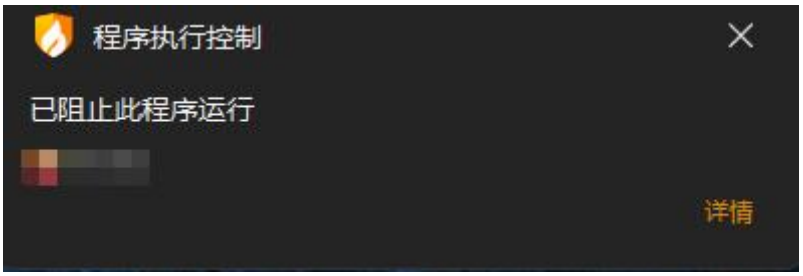
功能	说明
始终阻止	默认选中此项，将一直阻止程序运行。
按时段放行	可自定义设置放行时间，将在指定时间内允许程序运行，其余时间仍阻止程序运行。
确定	保存此设置。
取消	不保存设置，仅关闭窗口。

添加方式为【规则库添加】时：



功能	说明
选择程序	勾选目标程序，批量添加后将生成多条拦截规则。
管控方式	默认管控方式为“始终阻止”，添加后将一直阻止程序运行。 若您需要程序在指定时间放行，其余时间阻止执行，可点击【修改】，进入管控方式页，调整管控方式为“按时段放行”。
保存	保存此规则。
取消	关闭窗口。

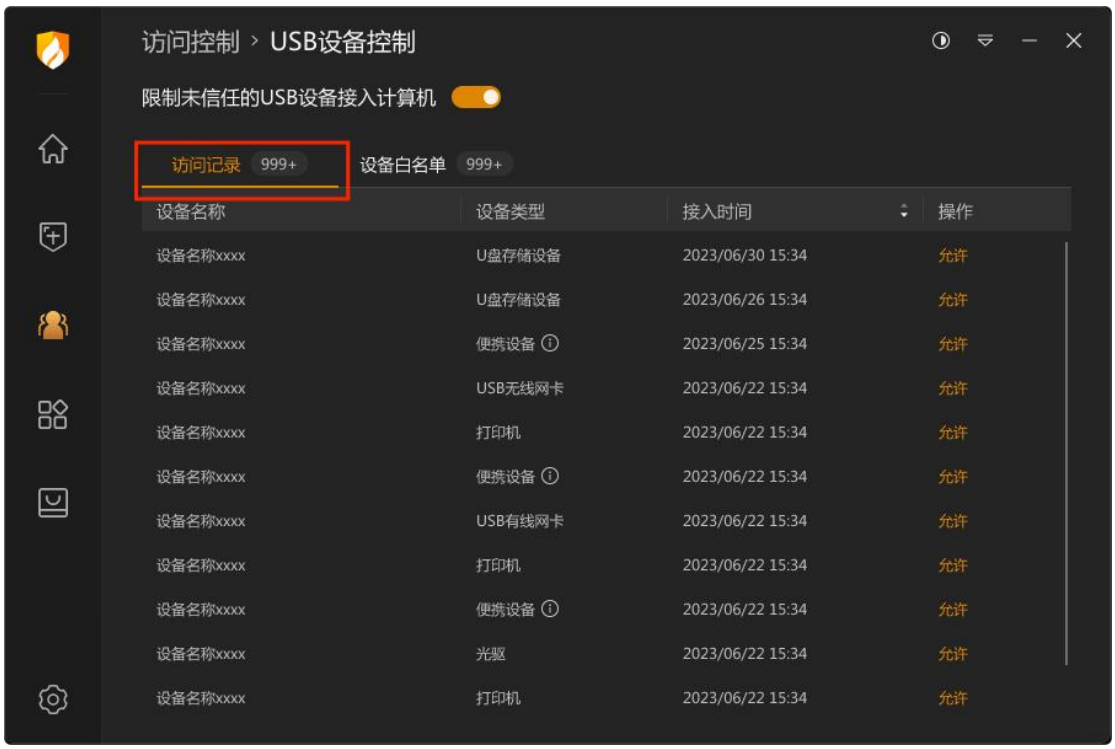
当程序启动时检测到当前时间不允许程序执行，火绒将弹窗提示您并阻止程序启动。点击【详情】会打开火绒的程序执行控制页面，若您已设置密码，还会在页面上弹出输入密码提示弹窗。



当程序已在运行，但检测到当前时间不允许程序执行，火绒将弹窗提示，需您手动退出程序。若不退出，后续会再次弹窗。（注：若您退出程序后仍弹窗提示，可能是程序未完全退出，可通过重启电脑解决）

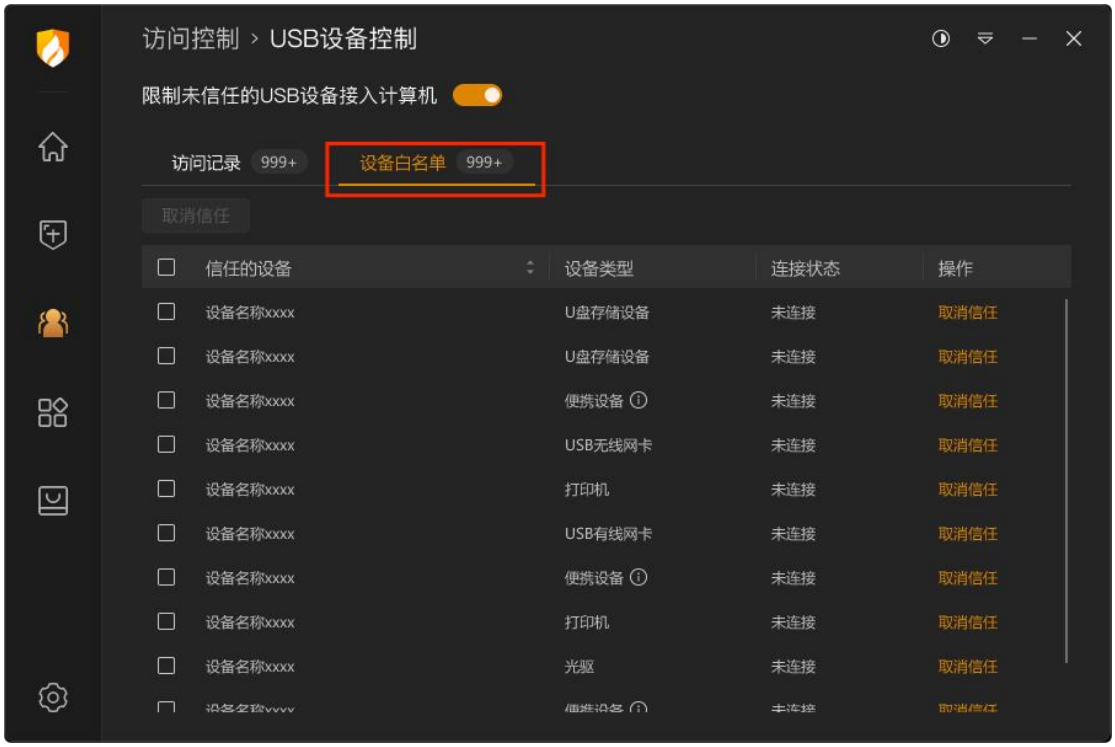
● USB 设备控制

火绒“USB 设备控制”提供了控制 USB 外接设备的接入与使用的功能。用户可以分别对不同 USB 设备类型加限制。



功能	说明
功能开关	开启，即 USB 设备控制功能生效。 关闭，即 USB 设备控制功能未生效。
设备类型	便携设备、USB 无线网卡、USB 有线网卡、打印机、光驱。
操作	允许：您允许该类 USB 设备接入计算机，允许后，设备进入白名单，下次接入不再通知您。

用户可将信任的 USB 设备添加到白名单中，白名单中的设备接入计算机时，将不会拦截。



功能	说明
重命名	鼠标移入设备名称显示编辑图标，点击可对设备进行重命名。
取消信任	不再信任勾选的设备，并从信任列表中移除。

当接入的 USB 设备不在白名单列表内时，火绒将弹出阻止窗口（见下图）。点击【详情】会打开火绒的 USB 设备控制页面，若您已设置密码，还会在页面上弹出输入密码提示弹窗。

● IP 协议控制

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。您可以自己编写 IP 协议规则，并且管理 IP 协议控制的相关规则。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。

功能	说明
搜索	可通过规则名称、应用程序和说明搜索规则，并实时展示搜索结果。
状态开关	开关亮色表示规则启用，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。
导入	点击搜索右侧图标，选择导入后，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	点击【添加】进入 IP 协议控制规则添加页面（见下图）。
功能开关	开启，即 IP 协议控制功能生效。

	关闭，即 IP 协议控制功能未生效。

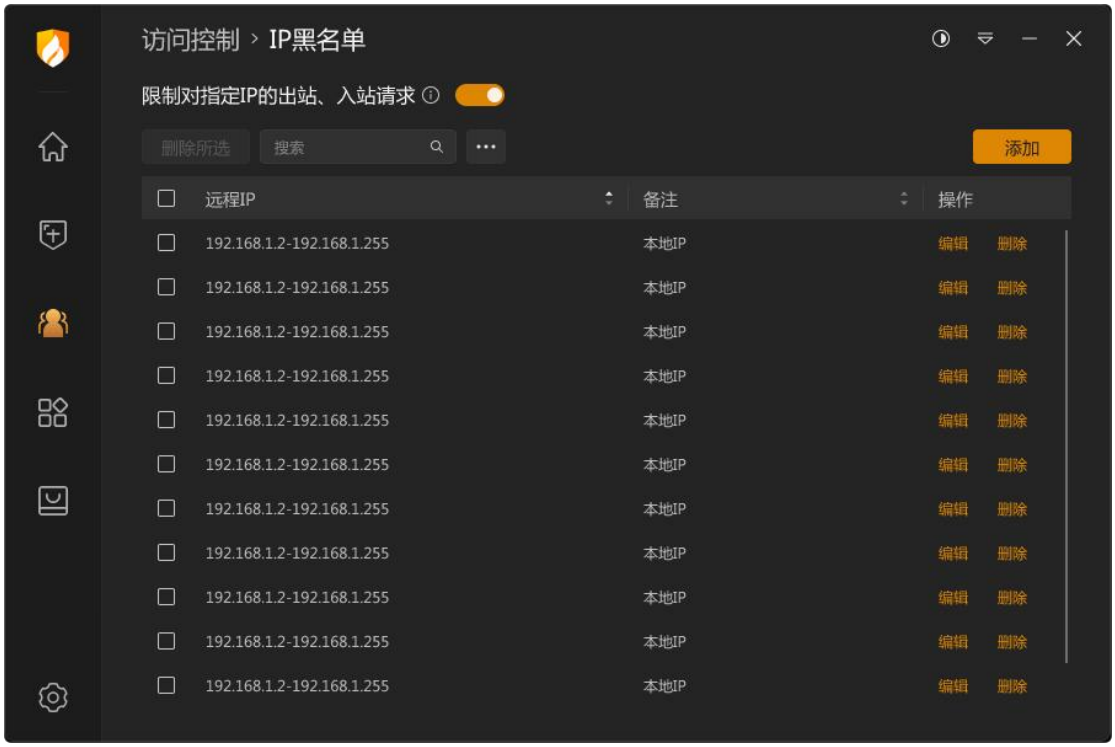
功能	说明
规则模板	为您提供了多个常用规则模板，选择后可快速设置添加规则页面。
规则名称	您可以自定义此规则名称。
应用程序	选择适用的应用程序，不填写默认为针对所有应用程序。
操作	针对触发符合下列设置的条件行为，是放行、放行（不记录日志）还是阻止。

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。可填写 IPv4（表示范围使用“_”）和 Ipv6（可缩写），支持 CDIR，多个 IP 请用“;”分隔。
本地端口	设置电脑本地的物理端口。多个端口请用“;”分隔。
远程 IP	设置需要访问的远程 IP 地址。可填写 IPv4（表示范围使用“_”）和 Ipv6（可缩写），支持 CDIR，多个 IP 请用“;”分隔。
远程端口	设置需要访问的远程端口。多个端口请用“;”分隔。
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。

● IP 黑名单

当您的电脑有不受欢迎的 IP 访问时，您可以将这些 IP 添加到 IP 黑名单中，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。



功能	说明
搜索	支持通过远程 IP 和备注搜索规则，并实时展示搜索结果。
编辑	编辑选中规则。
删除	删除所有选中的规则。
导入	点击搜索右侧图标，选择导入后，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	点击【添加】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 地址可填写 IPv4（表示范围使用“-”）和 IPv6（可缩写），支持 CIDR，多个 IP 请换行输入。
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。

➢ 安全工具

火绒还为用户提供了 14 个实用工具：漏洞修复、系统修复、弹窗拦截、垃圾清理、启动项管理、文件粉碎、右键管理、断网修复、流量监控、修改 HOSTS 文件、ARP 防护、DHCP 检测、安全分析工具、专杀工具，协助用户管理广告弹窗、启动项、右键菜单、流量、清理垃圾和修复系统故障。针对局域网环境的 ARP 攻击和 DHCP 劫持问题，还提供了 ARP 防护和 DHCP 检测小工具，有效解决局域网环境下的常见问题。

➢ 软件应用商店

提供了火绒应用商店的快捷入口，非内置软件，您可自行选择是否下载火绒应用商店。支持在安全设置-基础设置中配置是否显示该快捷入口，以及是否接收应用商店的通知。

➢ 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。

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。
游戏模式	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。
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。您也可以自行选择退出的时间，若时间结束且您持续处于开机状态，火绒将会重新自启（见下图）。

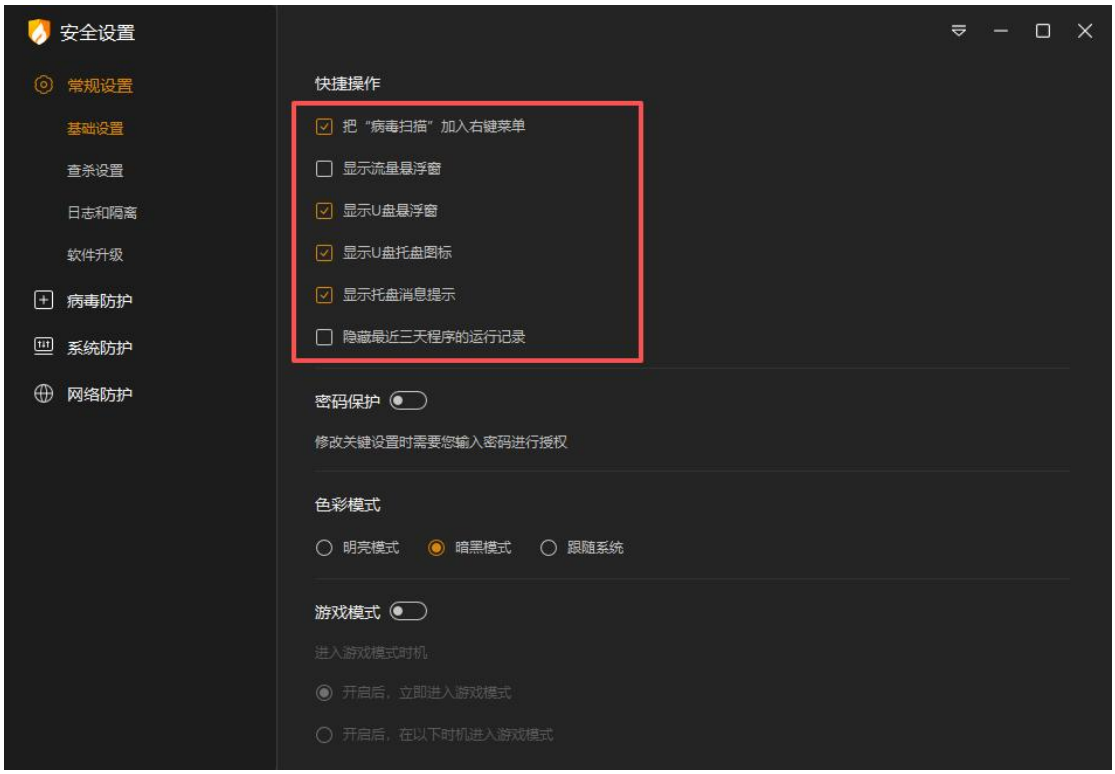
● 托盘消息

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。

➢ 常规设置-基础设置

● 快捷操作



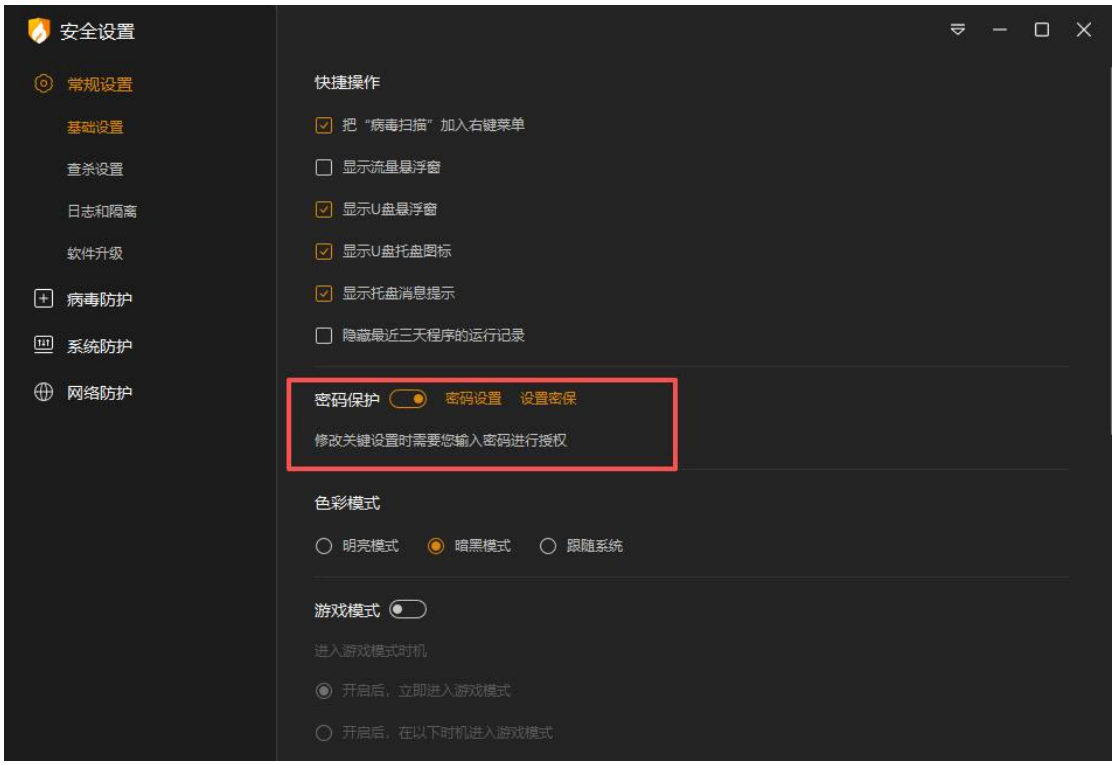
功能	说明
把“病毒扫描”加入右键菜单	文件右键菜单中支持快速自定义扫描该文件。
显示流量悬浮窗	勾选即在电脑右侧显示流量悬浮窗
显示 U 盘悬浮窗	计算机中插入 U 盘后，显示 U 盘悬浮窗。
显示 U 盘托盘图标	计算机中插入 U 盘后，任务栏中显示 U 盘托盘图标。
开启托盘消息	开启后，鼠标悬浮火绒托盘图标显示托盘消息。
隐藏最近三天程序的运行记录	勾选后将在隐私设备保护保护、联网控制、程序执行控制，添加规则页面下次打开时隐藏最近三天运行的程序。隐藏后界面按照暂无最近运行的程序来显示。默认不勾选。

● 密码保护

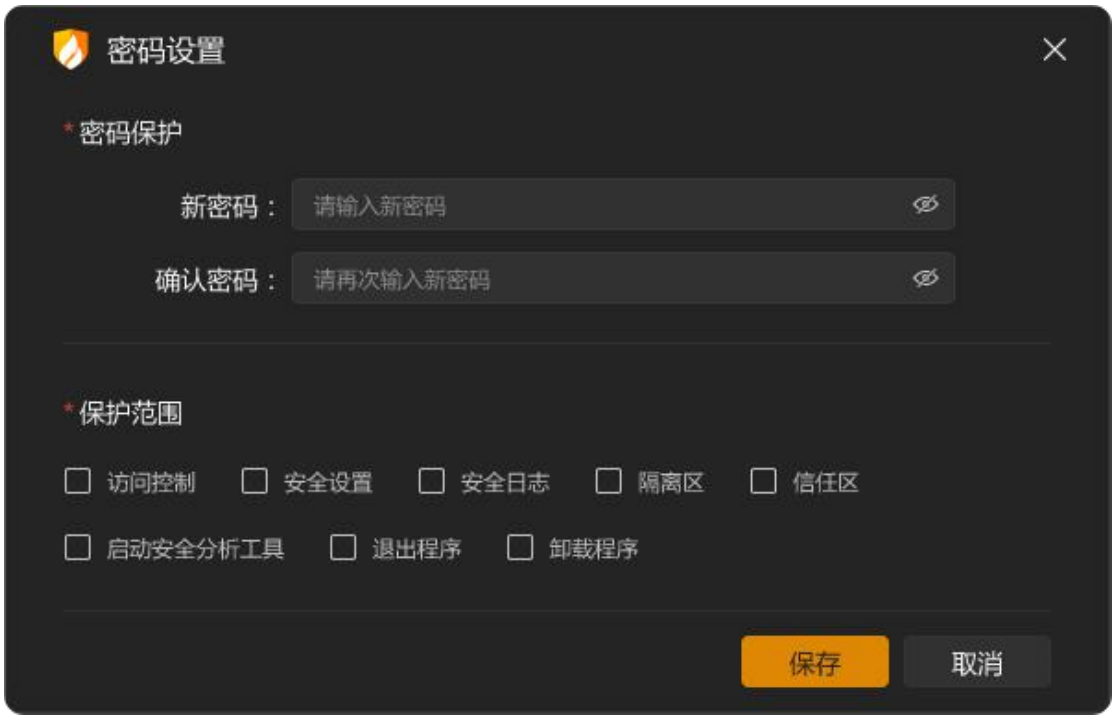
您可通过设置密码防止有人未经您的允许修改部分防护功能的配置。

➡ **1：设置密码**

打开启用开关，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。设置密码后会提示您是否设置密保（见下图）。



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：设置密保

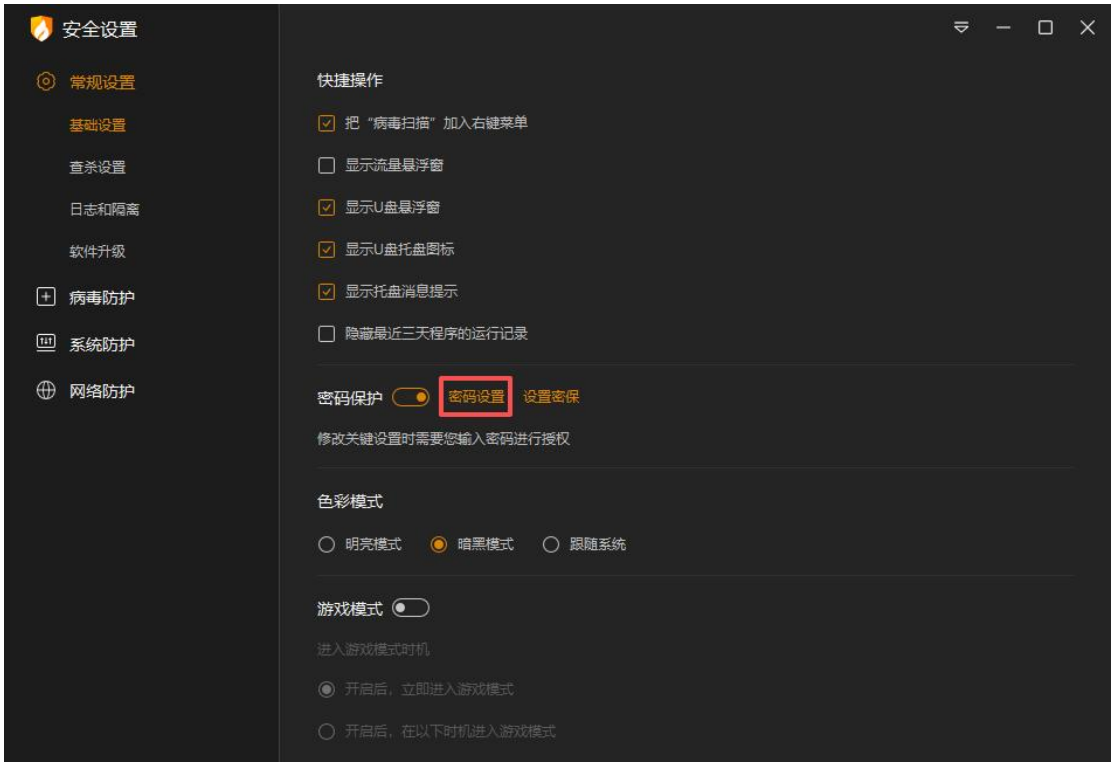
当您忘记密码时，可通过回答密保问题重新设置密码；若您忘记密保问题答案，将无法通过密保问题找回密码，请您谨记密保问题及答案。

设置完密保问题及答案后点击下一步，进入密保验证页面（见下图）。

点击“完成”按钮完成密保问题验证，验证通过后，密保设置成功。

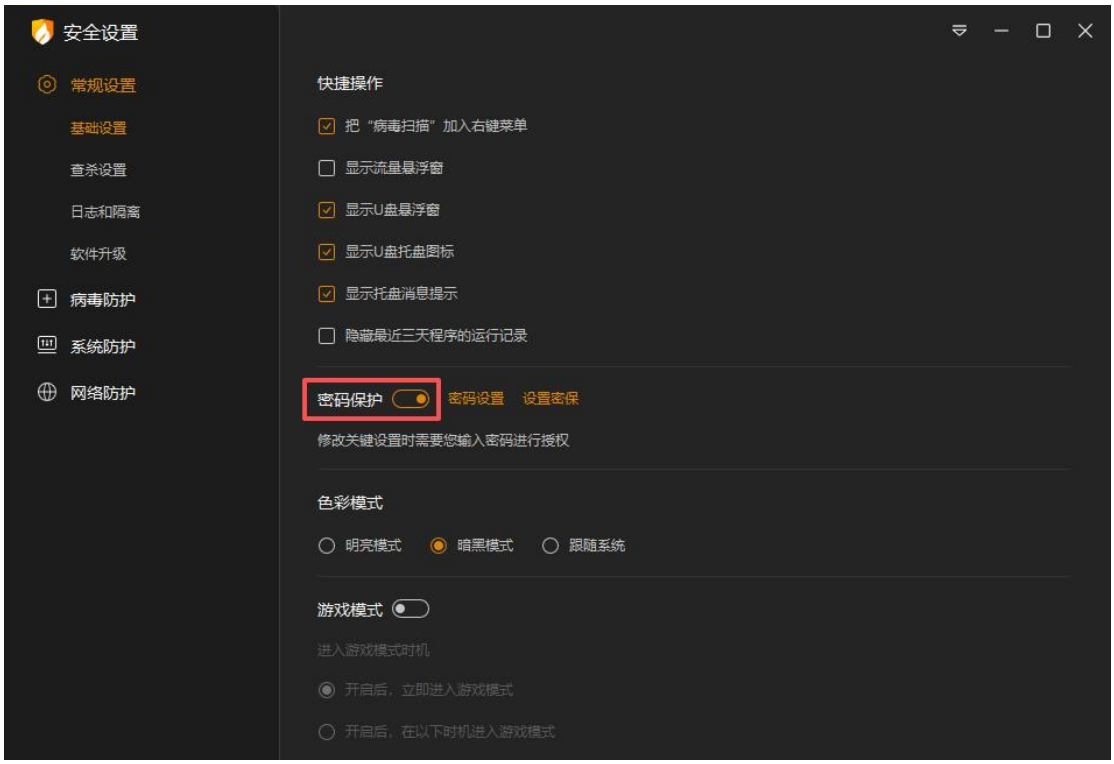
3：修改密码

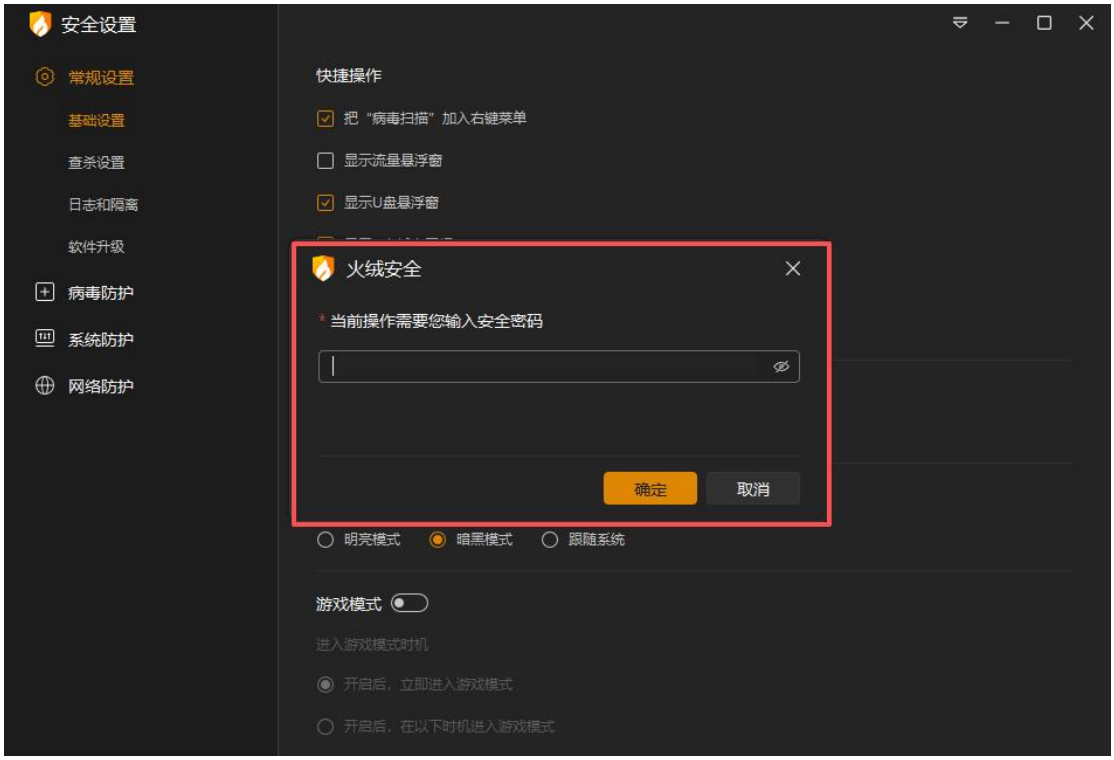
需要修改密码或修改密码保护范围时，您可在常规设置-基础设置中点击【密码设置】（见下图）再次打开密码设置页。进行修改密码或修改保护范围。



4：关闭密码保护

您需要在常规设置-基础设置中关闭密码保护功能开关，并且通过密码验证后，即可关闭密码保护。

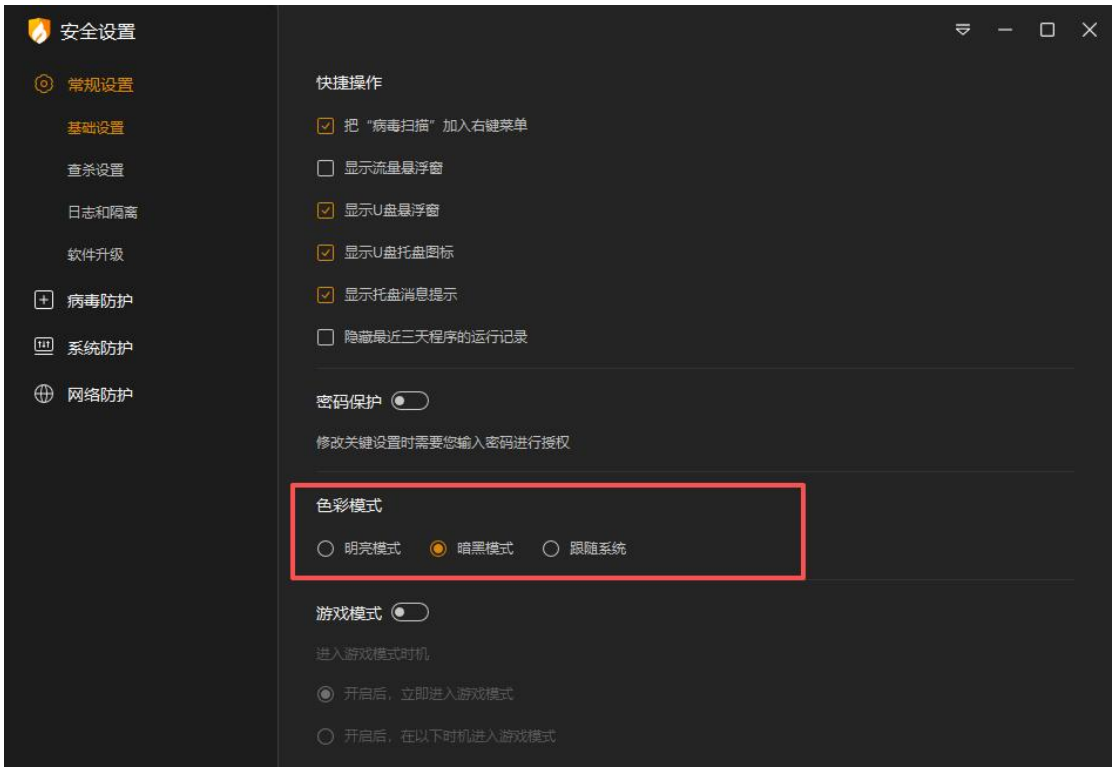




- 色彩模式

支持设置色彩模式为明亮模式、黑暗模式、跟随系统。

Windows10 14393.1607(19H1)以后版本才支持设置【跟随系统】。选中后，火绒界面将根据系统色彩（深色、浅色）模式变更为（黑暗、明亮）模式；

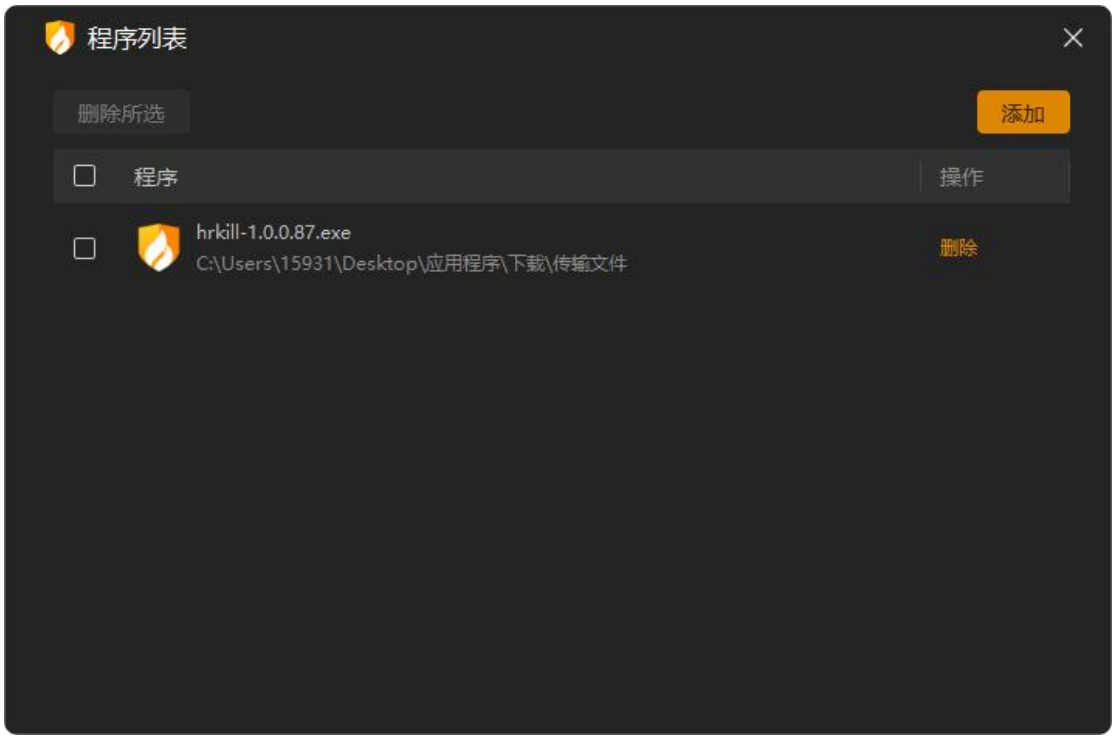


● 游戏模式

开启游戏模式开关后，将按照您的设置在具体的时机下自动进入游戏模式。进入游戏模式后，将暂停推送火绒部分提示弹窗，且按照您的设置是否推迟火绒自动升级（包括病毒库）、推迟 Windows 系统更新和不执行定时查杀，从而减少计算机卡顿。

功能	说明
开启后，立即进入游戏模式	开启游戏模式开关后，立即进入游戏模式。
开启后，在以下时机进入游戏模式	开启游戏模式开关后，只有在所设置的特定情况下才会自动进入游戏模式。
程序全屏运行时进入	任意程序全屏运行时，自动进入游戏模式。
指定程序运行进入	指定的程序运行时，自动进入游戏模式，您可自己添加程序（见下图）。
进入游戏模式后，将不推送火绒弹窗消息	进入游戏模式后，将不推送火绒部分弹窗。
推迟 Windows 更新	默认勾选，勾选时，进入游戏模式后，不会进行 Windows 更新。
推迟火绒自动升级	默认勾选，勾选时，进入游戏模式后，不会进行自动

	升级（包括病毒库升级）。
不执行定时查杀任务	默认勾选，勾选时，进入游戏模式后，不会执行定时查杀任务。



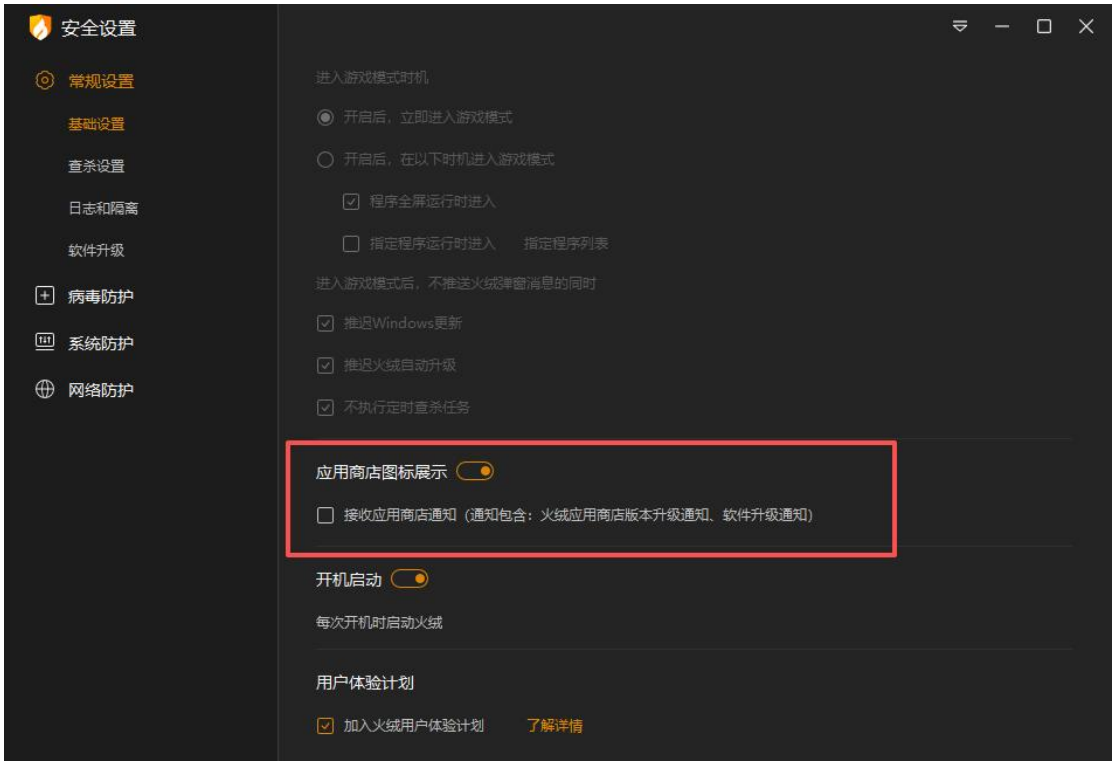
功能	说明
添加	将指定程序添加到列表中
删除	删除勾选的所有程序

● 应用商店图标展示

您可通过设置此开关设置【首页】-【左侧导航栏】是否展示火绒应用商店的图标，以及是否接收应用商店相关通知。

①：此开关默认打开，如您不需要展示，可设置为关闭状态。

②：接收应用商店通知：此项默认不勾选，如您需要接收火绒应用商店相关的通知，可勾选，勾选后，【首页】-【左侧导航栏】火绒应用商店的图标处则接收商店相关通知，以小红点角标形式提醒您。

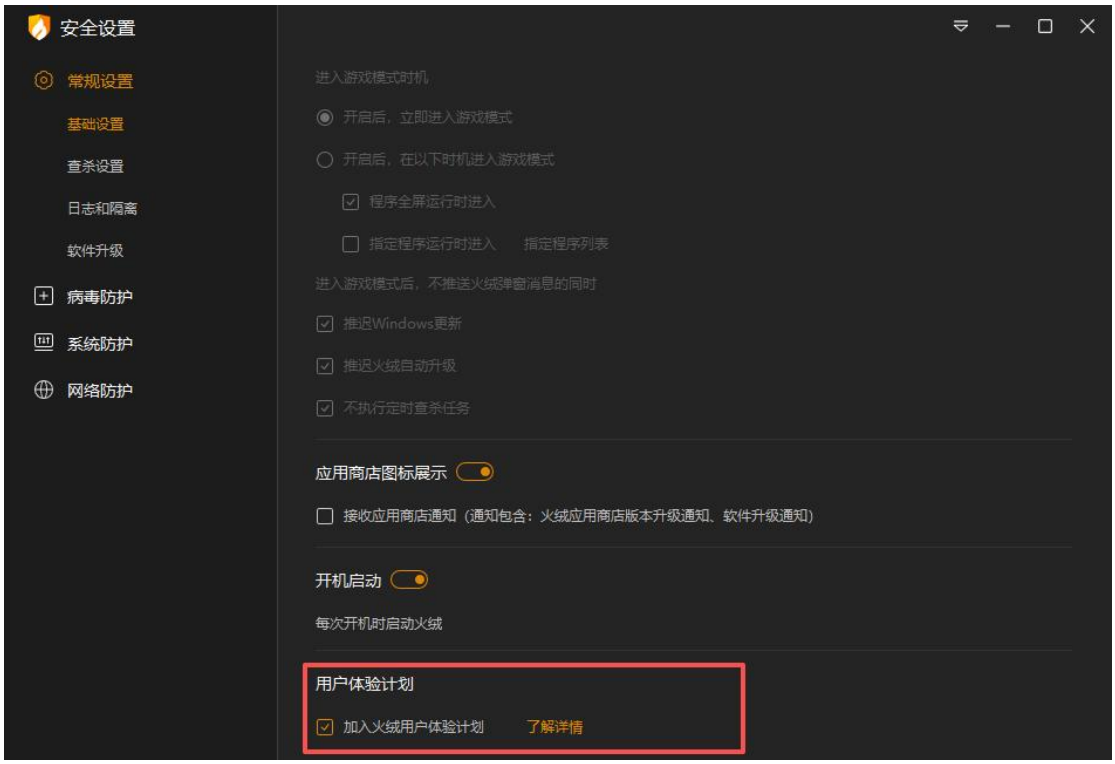


● 开机启动

您可设置是否开机自启火绒，默认开机自启，如您不想开机时启动火绒可关闭开关。

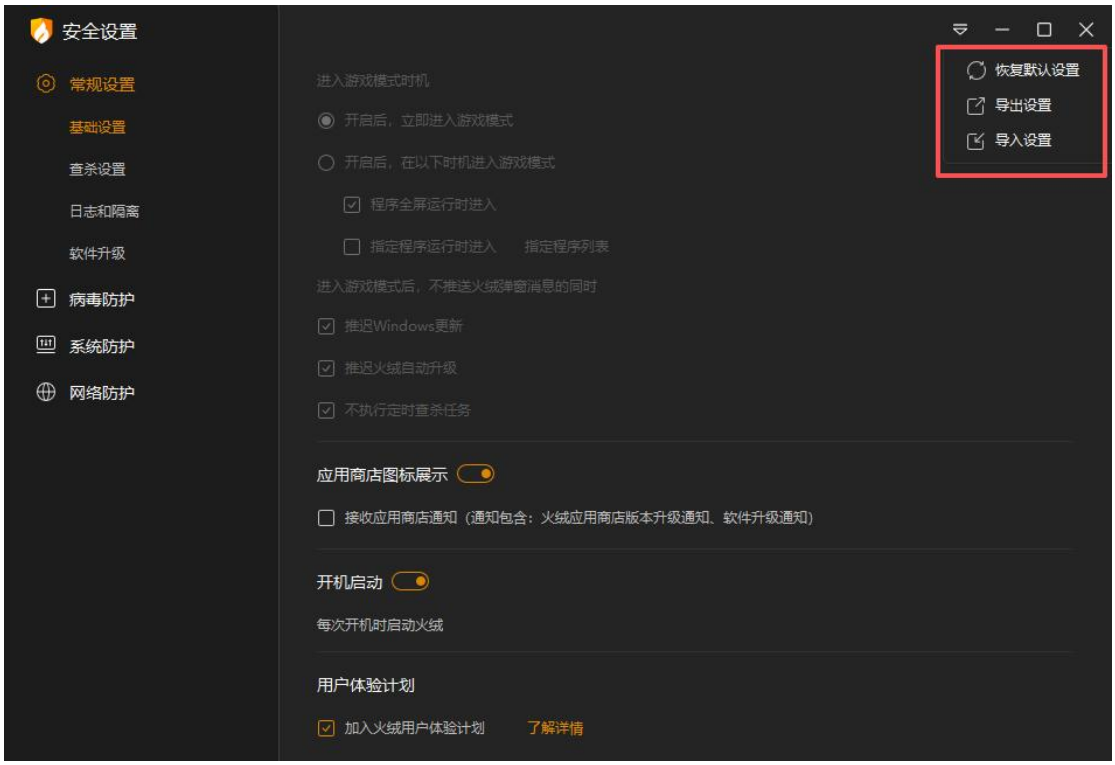
● 用户体验计划

您可设置是否加入火绒用户体验计划，参与用户体验改善计划后会自动上报火绒日常拦截威胁后产生的相关日志信息，这些信息只涉及威胁拦截日志相关内容，不涉及您的个人隐私信息或文件数据。



➢ 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。

➢ 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。

Windows11 任务栏开始按钮弹窗中，选择所有应用，在火绒安全实验室下拉 菜单中可以卸载火绒。

➡ 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。

功能	说明
狠心卸载	开始卸载，检测到隔离区存在文件时，弹出询问弹窗（见下图）。
继续保护	关闭卸载程序，继续运行火绒。

功能	说明
打开隔离区	打开隔离区窗口，根据您的需要可提取或恢复隔离区文件。
继续卸载	继续运行卸载程序。

注：为确保卸载之后无残留文件，请在卸载之后重启电脑。

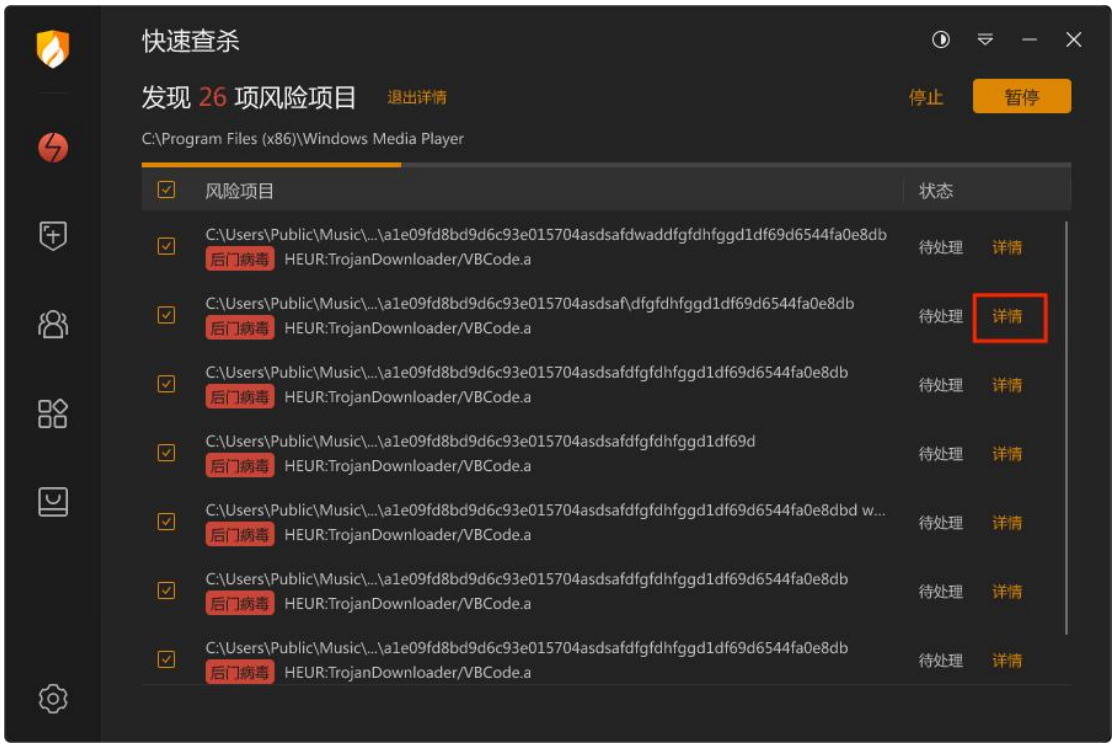
◆ 进阶功能说明

火绒为有一定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。

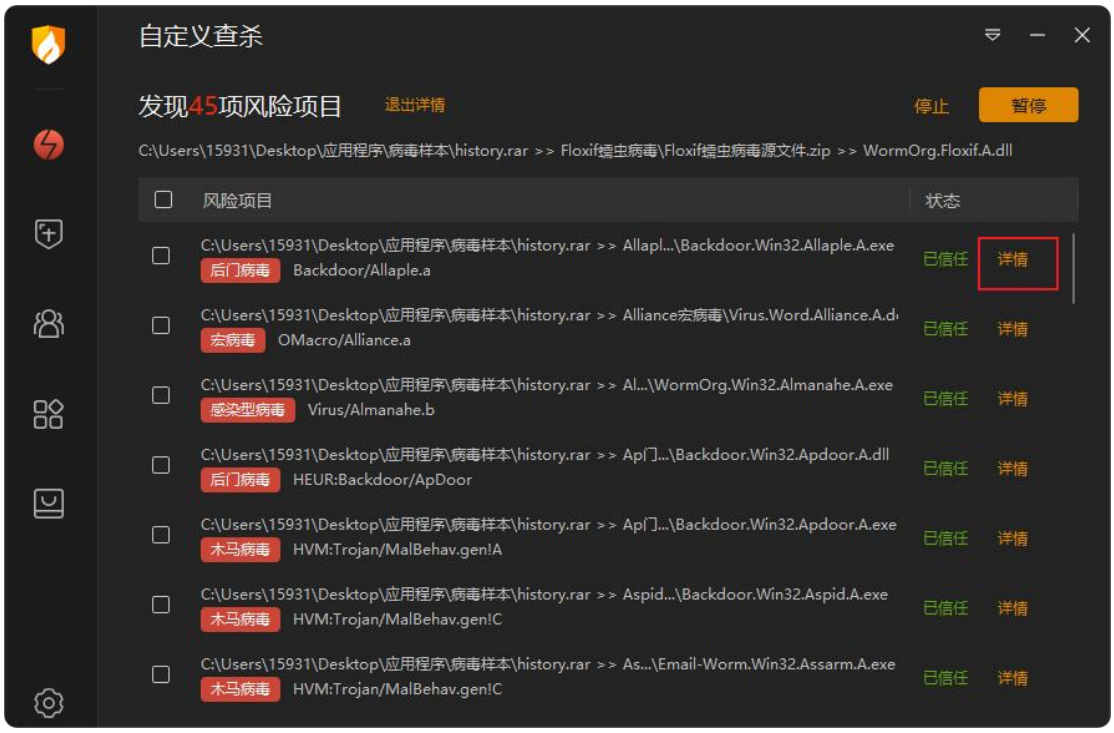
➢ 病毒查杀

● 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。

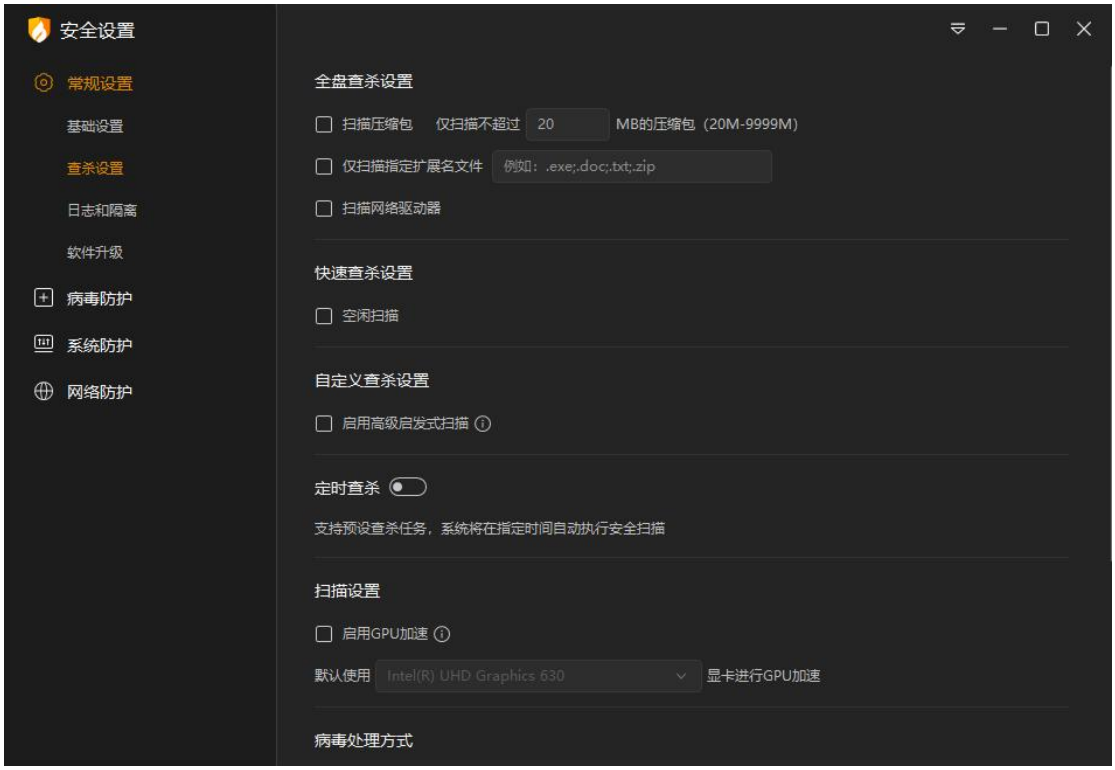


您仍可再次点击已信任文件的【详情】，再点击风险详情中的【取消信任】已继续查杀该风险文件。



● 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，如全盘查杀配置、快速查杀配置、修改病毒处理方式等。



功能		说明
全盘查杀设置	**扫描压缩包**	勾选后，全盘查杀时将扫描压缩包，但扫描时将自动跳过大于您填写的数值的压缩包，以加快扫描速度。 未勾选则在全盘查杀时不扫描压缩包。
	仅扫描指定扩展名文件	勾选此项后，填写文件扩展名，填写格式示。 例：.tmp;.txt;.log;.db 进行全盘查杀时，仅扫描设置的文件类型。 多个文件类型之间用英文“;”来隔开。
	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。
快速查杀配置	**空闲扫描**	勾选后，将在特定时机下自动进行快速扫描。 勾选后，您可进行高级设置（可设置空闲时扫描的时机，可设置病毒处理方式，可设置计算机使用蓄电池时不扫描）。
自定义查杀配置	**启用高级启发式扫描**	勾选后，自定义查杀时将会启用高启发式扫描。 高启发式扫描可提升新型未知病毒检出率，但误报率会随之上升，建议用户谨慎开启。
定时查杀		开关开启后，将按照您的设置定期自动进行病毒查杀（支持设置定时查杀的类型、执行频率和执行时间、以及可设置开始定时查杀前是否弹窗提示您）。
		勾选后，反病毒引擎会在此次扫描的适当时机使用 GPU

扫描设置	**启用 GPU 加速**	进行计算，进而提升扫描效率（仅 DirectX 11 及以上版本支持）。 针对存在多显卡的计算机，您可以设置使用哪个显卡去进行 GPU 加速；只有一个显卡的计算机，火绒默认使用唯一的显卡进行 GPU 加速。
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。

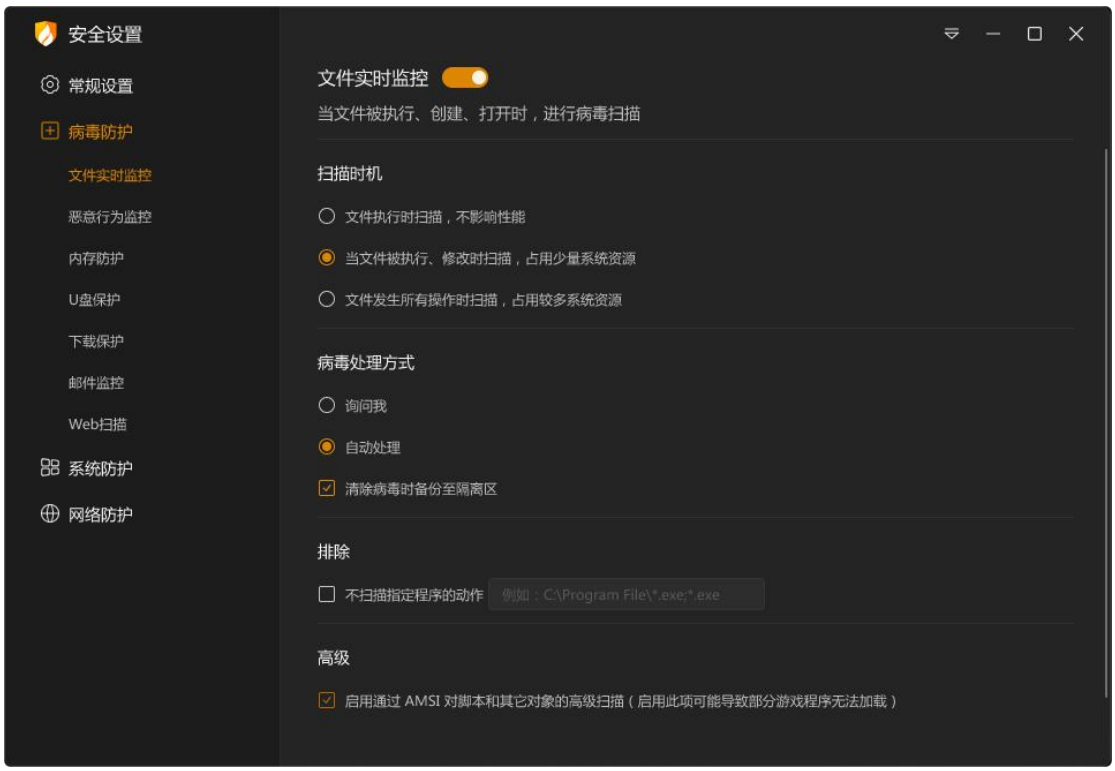
➢ 防护中心

● 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。
启用通过 AMSI 对脚本和其他对象的高级扫描	勾选后，文件实时监控时，会启用 ASMI 进行高级扫描，结合火绒虚拟技术可以高效地查杀新型未知病毒，但会有误报；仅 Windows10 及以上系统支持。 注意：AMSI 启动可能会造成部分游戏无法正常加载，建议避开游戏时机启用。 目前仅支持对 PowerShell、WScript、CScript 进程的脚本执行进行扫描。
功能开关	开启：文件实时监控功能生效。 关闭：文件实时监控功能未生效。

2：恶意行为监控设置说明

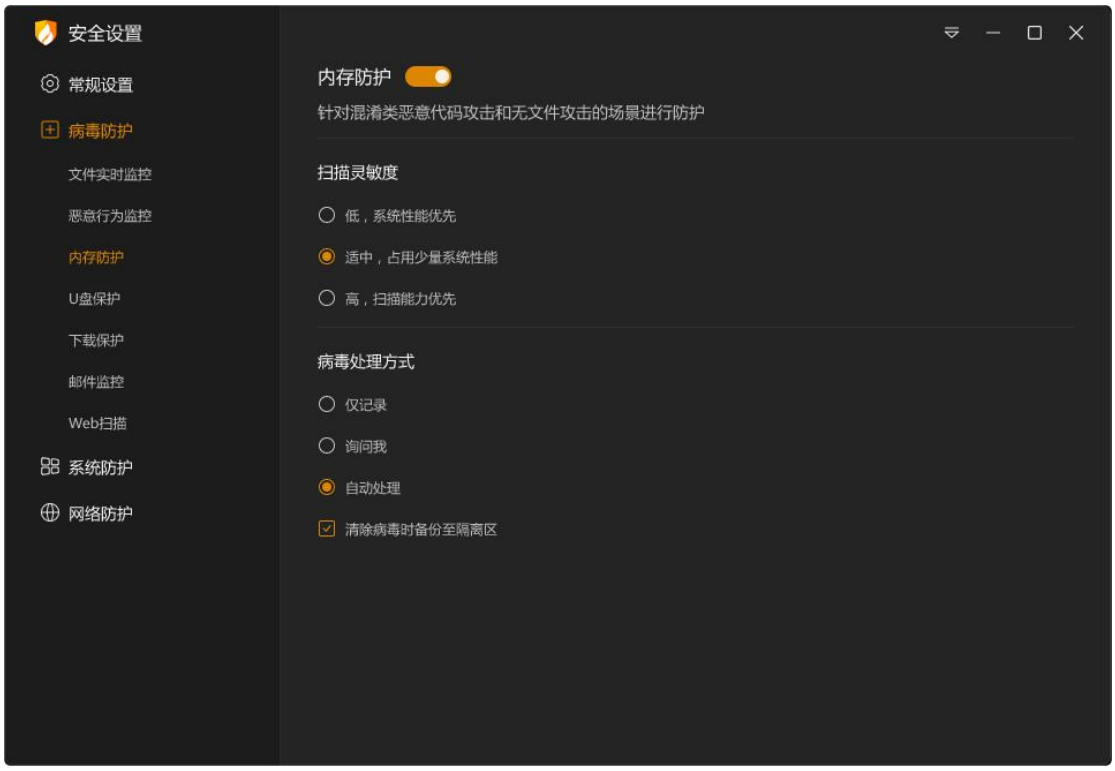
通过设置可以调整【恶意行为监控】发现威胁动作时是否自动处理，处理病毒与清除病毒后备份隔离区等设置项目。

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。
	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。
增强勒索病毒防护		勾选此项后，火绒会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。
检测到勒索行为时还原被修改的文件		勾选此项后，当检测到勒索行为时，火绒会自动还原被勒索病毒修改的文件。但此功能首次安装火绒，勾选此功能后需重启计算机才可生效。

功能开关	开启：恶意行为监控功能生效。 关闭：恶意行为监控功能未生效。

3：内存防护设置

通过设置可以调整【内存防护】功能的扫描灵敏度和病毒处理方式。



功能		说明
扫描灵敏度		根据您的需要和电脑配置情况选择扫描灵敏度。
病毒处理方式	**仅记录**	扫描出威胁后，将不予以处理仅记录至安全日志中。
	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。

功能开关	开启：内存防护功能生效。 关闭：内存防护功能未生效。

4：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。调整可修复项目、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		勾选后将扫描压缩包，但扫描时将自动跳过大于您填写的数值的压缩包，以加快扫描速度。 未勾选时不扫描压缩包。
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。
功能开关		开启：U 盘保护功能生效。 关闭：U 盘保护功能未生效。

U 盘修复功能简介：

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。

U 盘修复功操作说明：

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。

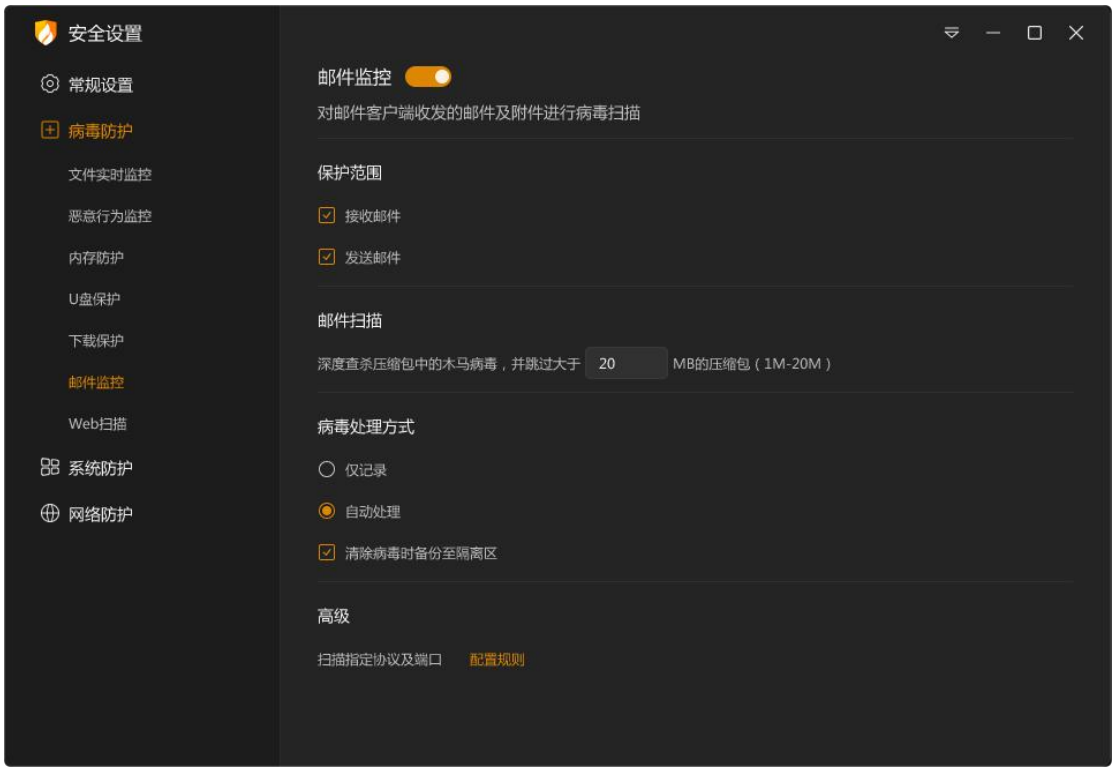
5：下载保护设置说明

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		勾选后将扫描压缩包，但扫描时将自动跳过大于您填写的数值的压缩包，以加快扫描速度。 未勾选时不扫描压缩包。
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。
功能开关		开启：下载保护功能生效。 关闭：下载保护功能未生效。

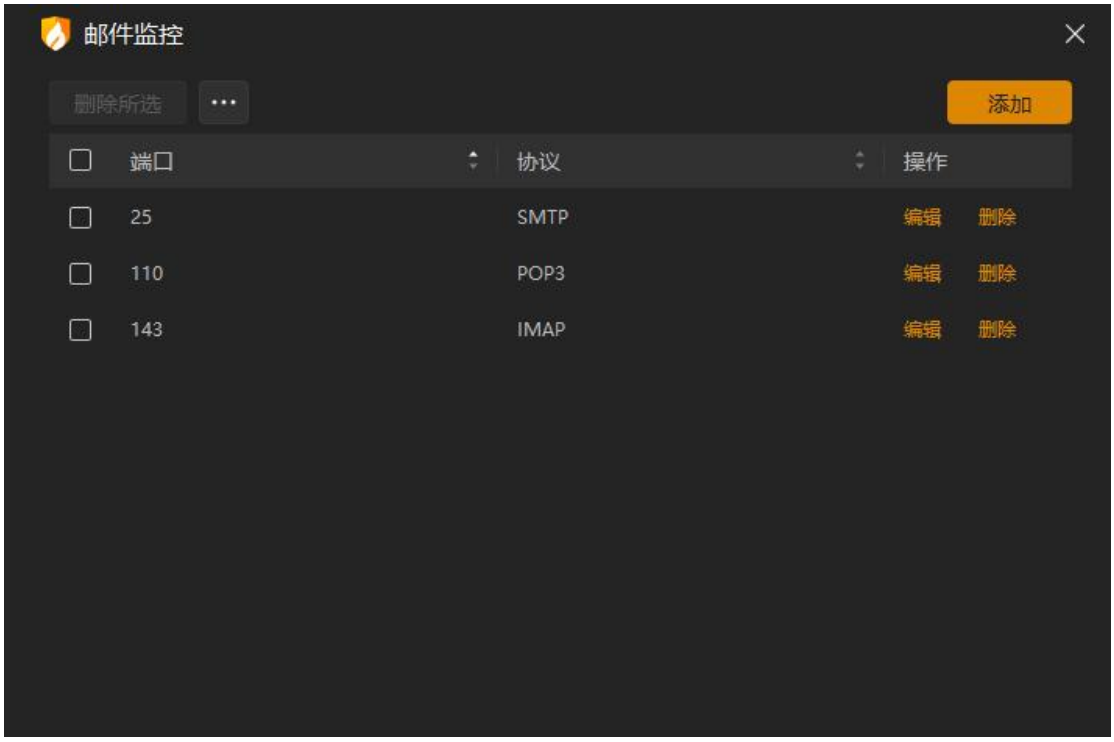
➡ 6：邮件监控设置说明

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保护范围。
邮件扫描		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）。 默认存在三个规则：25 端口 SMTP 协议、110 端口 POP3 协议、143 端口 IMAP 协议。
功能开关	开启：邮件监控功能生效。 关闭：邮件监控功能未生效。



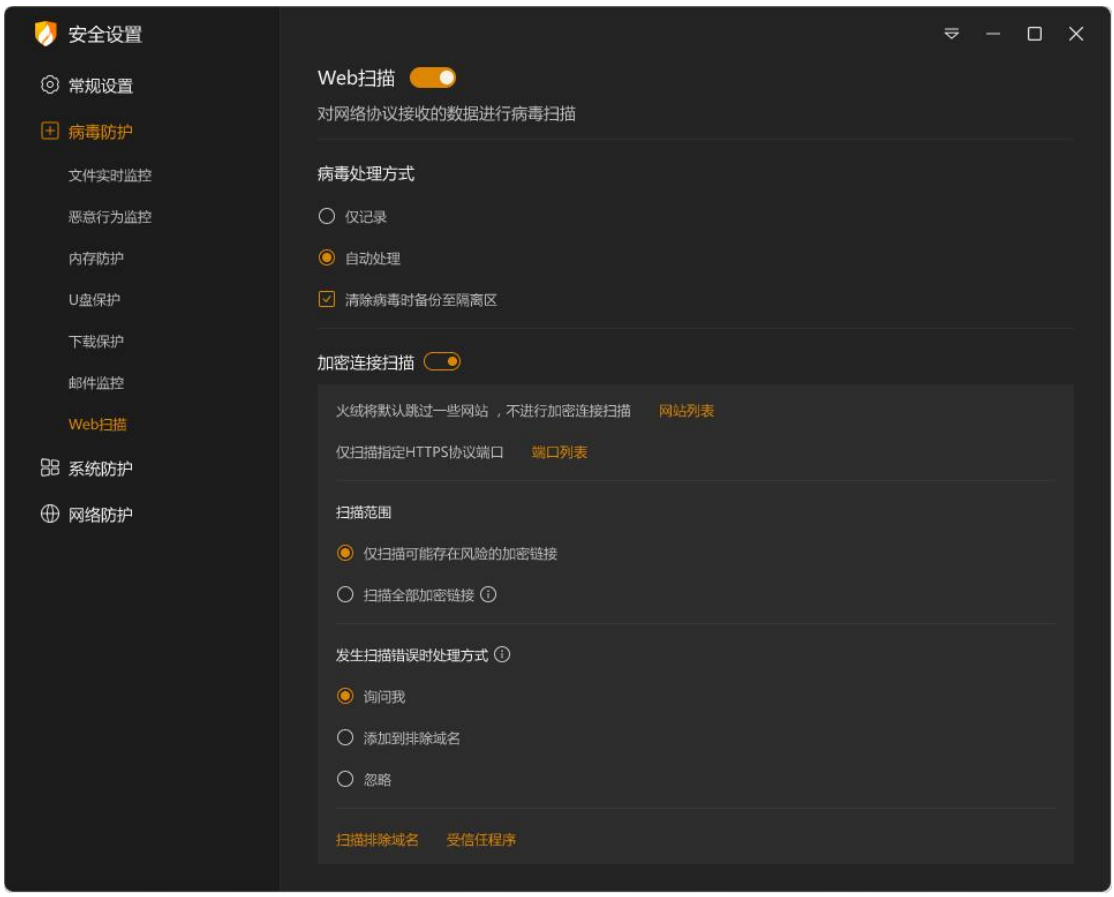
功能	说明
编辑	编辑勾选规则
删除	删除所有勾选规则
添加	添加新的需要扫描的协议和端口，点击后会以弹窗形式让您新建一条规则（见下图）供您填写添加。
导入	点击搜索右侧图标，选择导入后，选择需要导入的规则，点击确定等待规

	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。

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。

➡ 7：Web 扫描设置说明

通过设置可以管理【Web 扫描】是否检测 https 协议端口和病毒处理方式，以及加密扫描错误时处理方式，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。
加密链接扫描		开启后，支持检测 HTTPS 协议的端口。 1：火绒会默认跳过一些网站，您可通过【网站列表】查看内置跳过的网站。 2：火绒支持用户自定义扫描的 https 端口，默认扫描 443，如果您有其他 https 端口需要扫描，可点击【端口列表】，管理扫描的端口列表。

	3：扫描范围： ①：仅扫描可能存在风险的加密链接。 ②：扫描全部加密链接（注意：此项开启可能导致部分程序无法正常联网）。 4：发生扫描错误时处理方式： ①：火绒默认处理方式为弹窗询问，让您来自主处理。 ②：您也可以选择扫描错误时将域名添加至排斥列表，添加至排除列表后，后续加密扫描将自动跳过。 ③：或者您可以选择扫描错误时忽略此域名，下次加密扫描发生错误后，火绒将自动忽略，不再提示您。 5：扫描排除域名：如果您有信任的域名不需要进行加密扫描，或需要将排除的域名从排除列表移除，您可在此处管理排除域名裂变。 6：受信任的程序：如果您有信任的程序不需要进行加密扫描，或需要将信任的程序从列表移除，您可在此处管理信任的程序。添加到信任程序列表的程序，发生加密链接时，默认不扫描。
功能开关	开启：Web 扫描功能生效。 关闭：Web 扫描功能未生效。

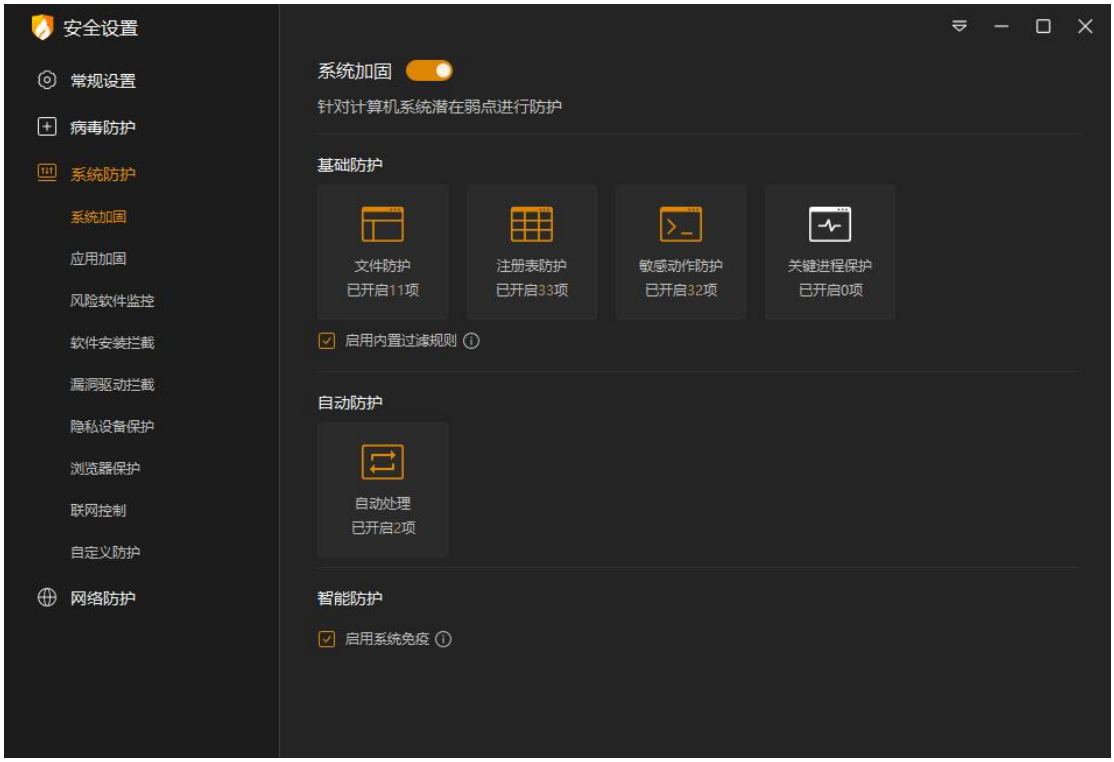
● 系统防护

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。
	关键进程保护	支持防护（关键的系统进程、IE 浏览器进程、资源管理器进程）对被保护的关键进程进行防篡改加固。
	启用内置过滤规则	监控针对系统的敏感行为，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。
功能开关		开启：系统加固功能生效。 关闭：系统加固功能未生效。

① 基础防护：

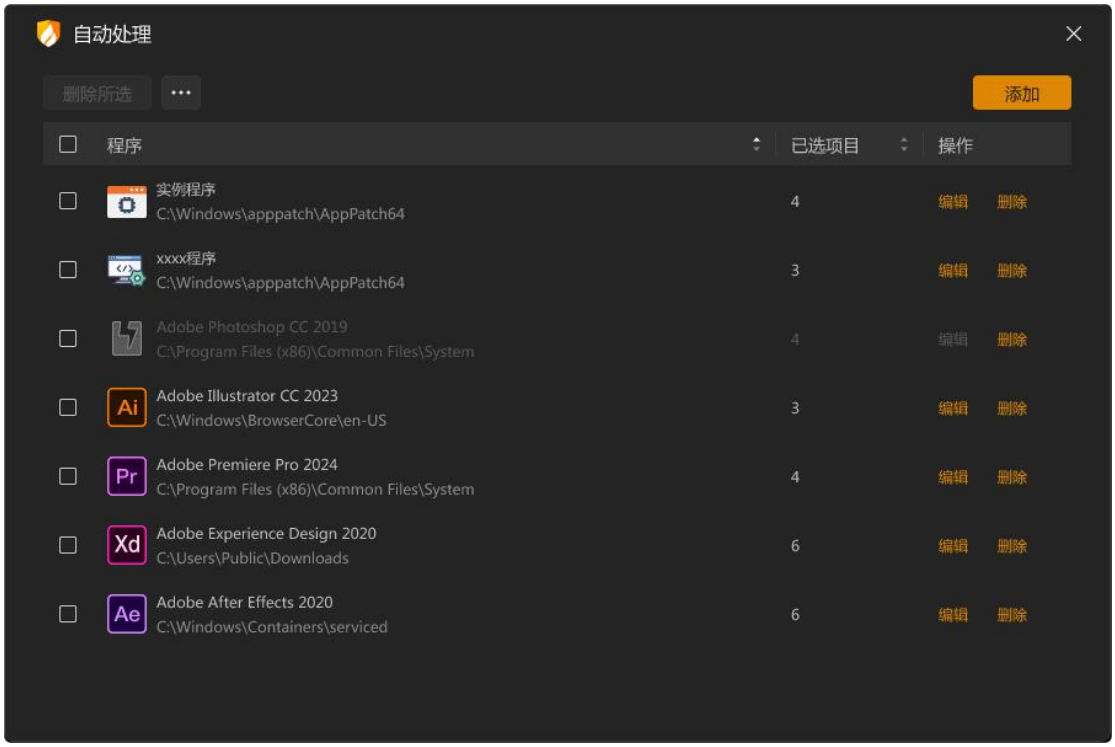
您可在基础防护中针对文件防护、注册表防护、执行防护、关键进程的防护的防护项目进行修改调整。火绒为您默认配置了相应规则，您可根据需要自行调整，勾选您需要启动的防护项目，选择对应的生效方式即可。防护项目对应说明可参看后方的防护说明内容。

点击【状态】或【处理方式】按钮可批量调整防护项目的状态和处理方式。

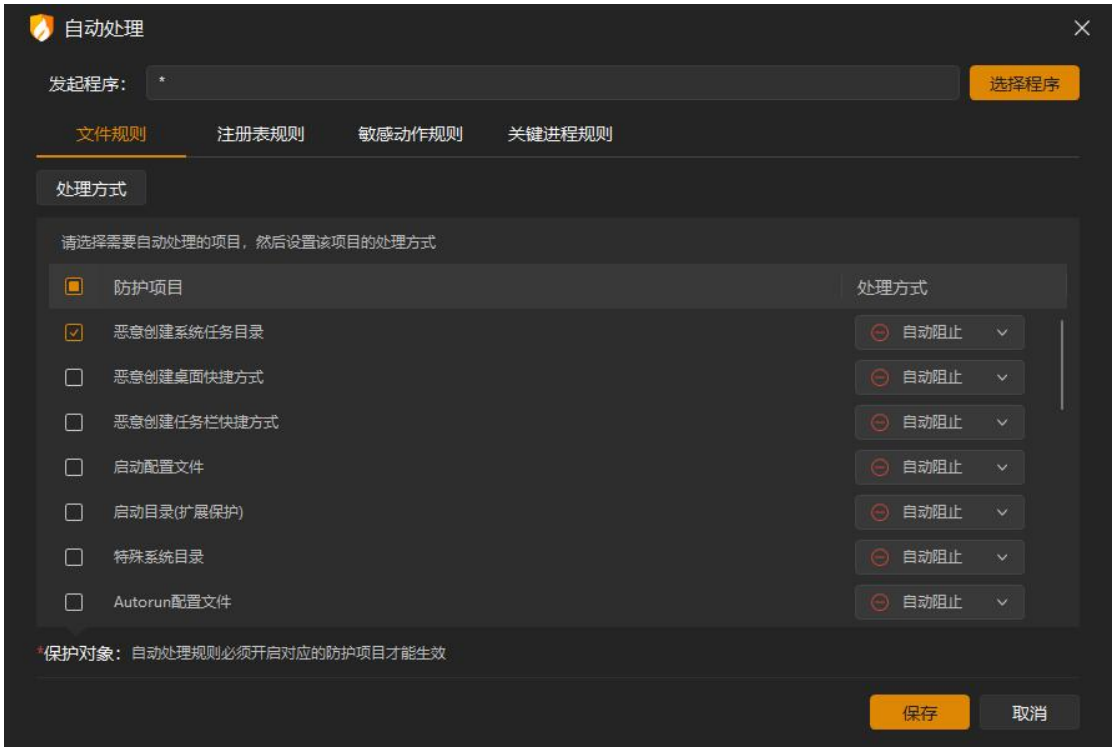
如您需恢复默认配置状态，您可点击页面左下角的【恢复默认】按钮。

② 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	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，同时点击【处理方式】可批量调整防护项目的处理方式。
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。

★ **保存规则-规则冲突：**

发现已存在相同发起程序的自动处理规则时您可以选择处理方式：

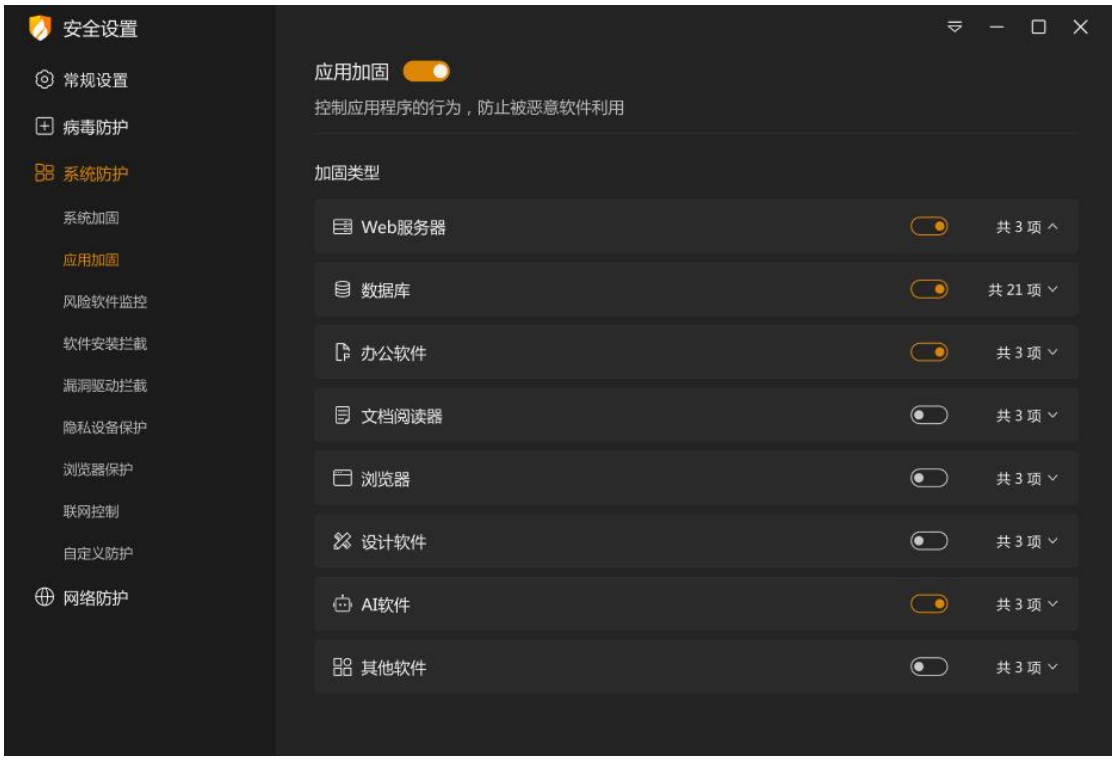
功能	说明
合并	合并新规则和旧规则的保护对象，新旧规则保护对象都保留。
替换	旧规则的保护对象将全部被替，仅保留新规则的保护对象。

★ **自动添加-自动防护：**

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。

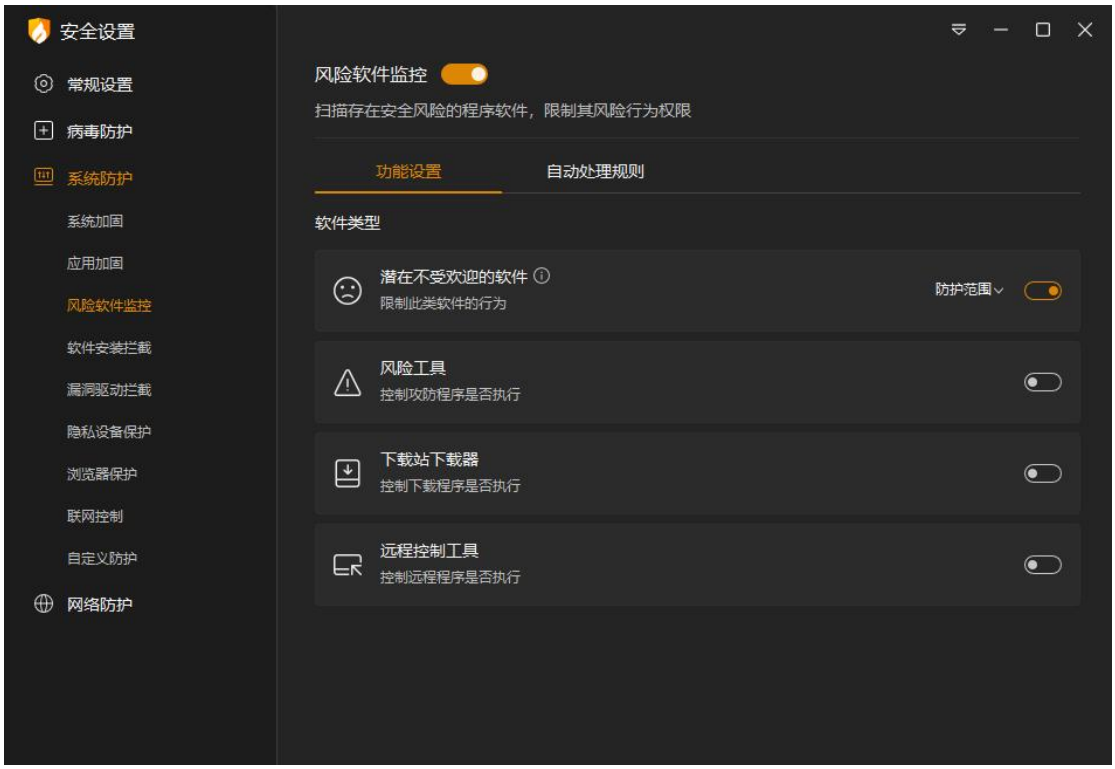
➡ **2：应用加固设置说明**

加固类型中开关开启，代表该防护规则开启，展开后为您电脑中对应安装的应用程序。程序卸载后，对应程序消失。

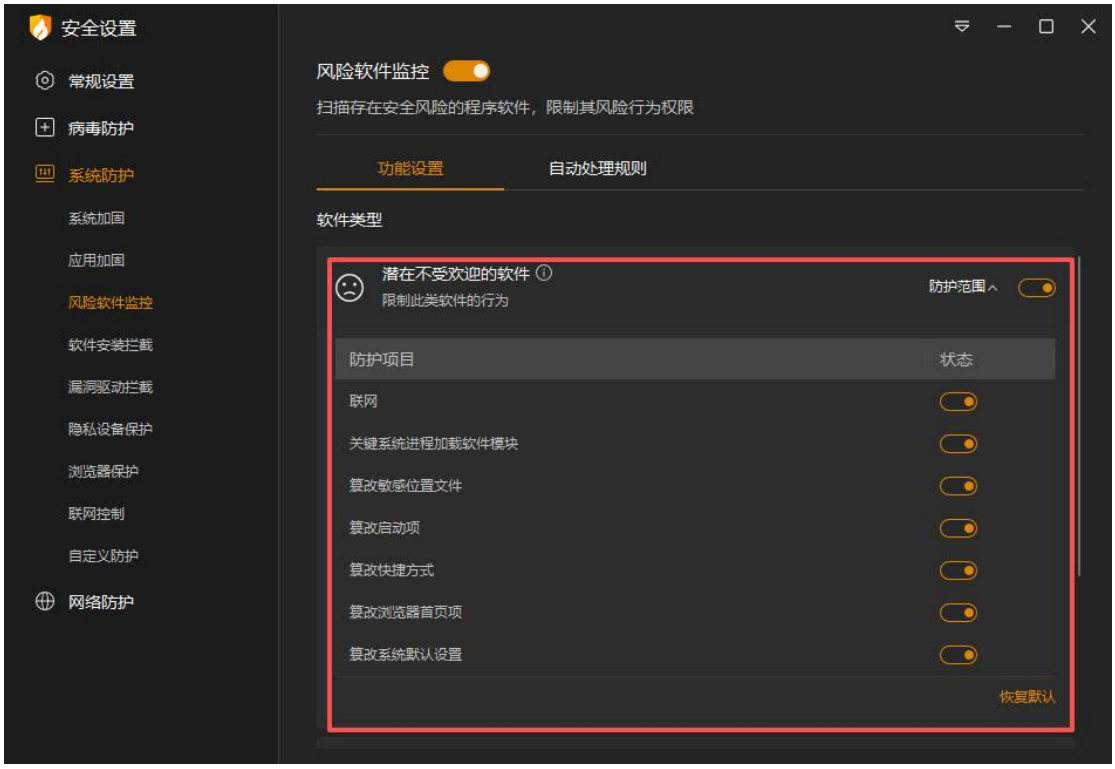


3：风险软件监控设置说明

您可在风险软件监控设置中，设置限制【潜在不受欢迎软件】的哪些软件行为。设置【控制风险工具】、【下载站下载器】、【远程控制工具】是否执行。

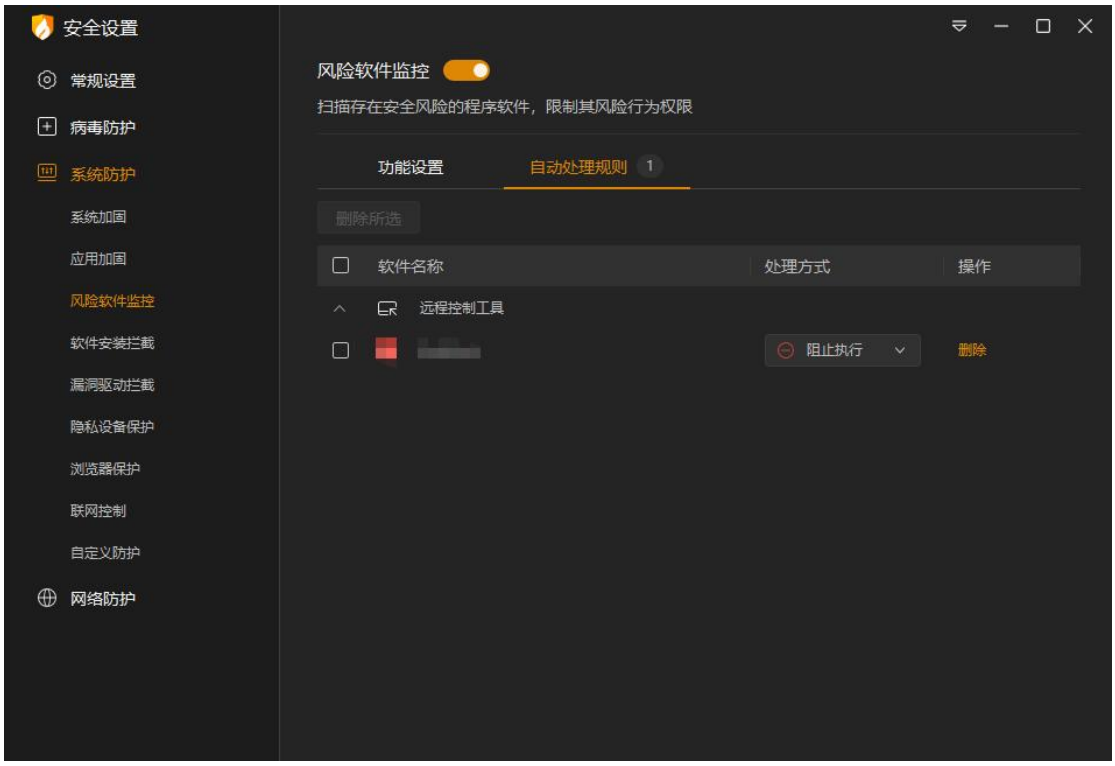


功能	说明
状态	开启：监控此类风险软件，风险软件运行时，弹窗询问用户。 关闭：不监控此类软件。
潜在不受欢迎软件防护范围	设置限制潜在不受欢迎软件的哪些行为，点击后弹出设置窗口（见下图）。
功能开关	开启：风险软件监控功能生效。 关闭：风险软件监控功能未生效。



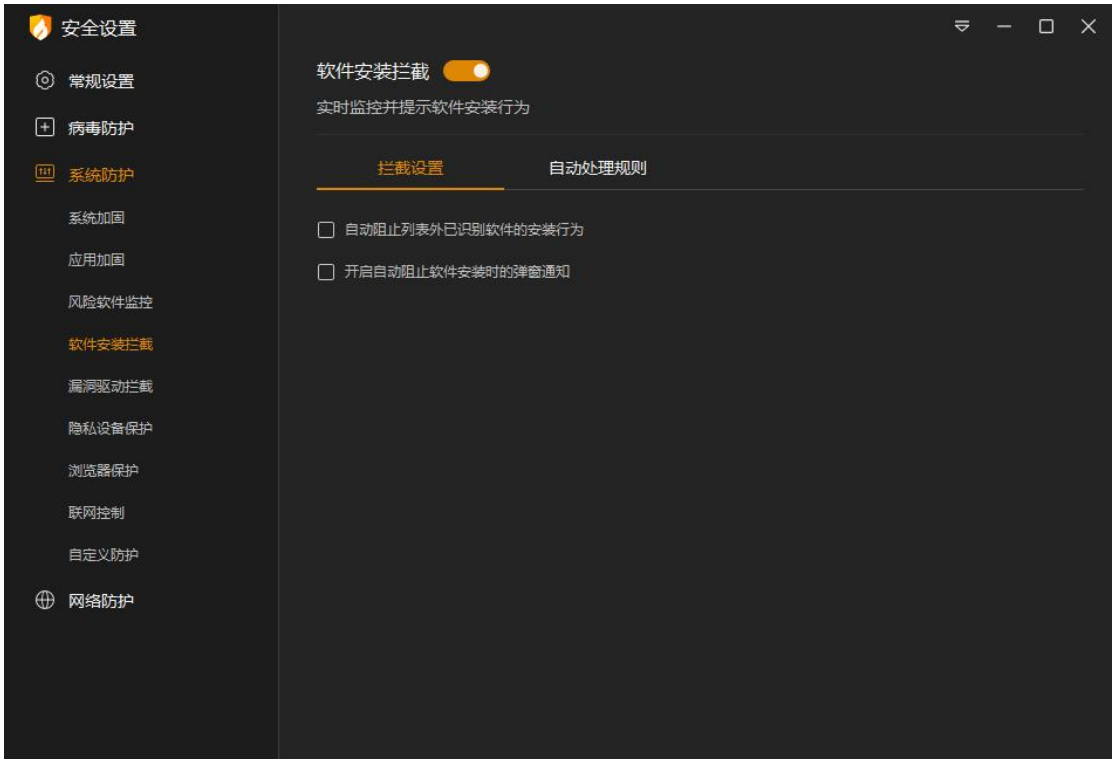
功能	说明
状态	开启：自动阻止潜在不受欢迎软件的该行为。 关闭：允许潜在不受欢迎软件的该行为。
恢复默认	状态全部恢复为开启状态。

检测到风险软件运行时，会弹出询问弹窗，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，下次该风险软件再次运行时，则自动处理。



4：软件安装拦截设置说明

您可在软件安装拦截设置中调整列表中软件的安装行为，还能在拦截设置中设置是否自动阻止可识别软件的安装行为和自动阻止软件安装时是否显示通知弹窗。



功能		说明
拦截设置	**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的安装行为。
	开启自动阻止软件安装时的弹窗通知	勾选后，自动阻止软件安装时将在屏幕右下角弹出通知弹窗。
功能开关		开启：软件安装拦截功能生效。 关闭：软件安装拦截功能未生效。

★ 在火绒发现存在软件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。**

✓ 火绒弹出安装拦截提示弹窗时，不会区分软件的安装形式，无论是正常安装还是通过捆绑、推广、静默或其他方式安装，都会统一提示用户。

✓ 软件安装拦截并非对软件安装包进行报毒，即使选”阻止“也不会删除软件安装包，您还可以再次执行，重新安装。

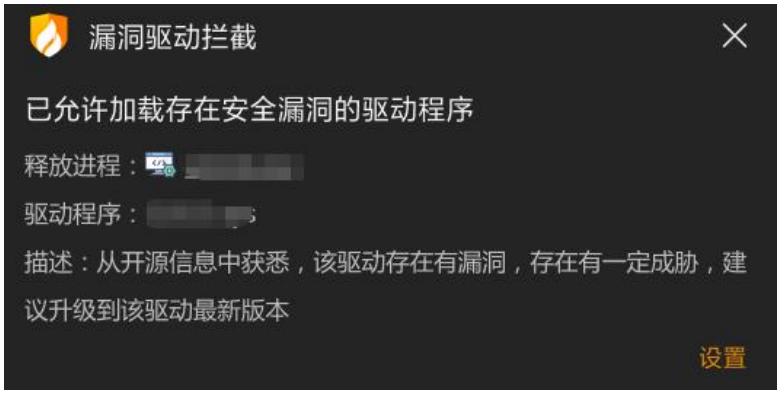
✓ 当您勾选了【开启自动阻止软件安装时的弹窗通知】勾选框时，并触发了自动阻止软件安装时，会弹出通知弹窗。

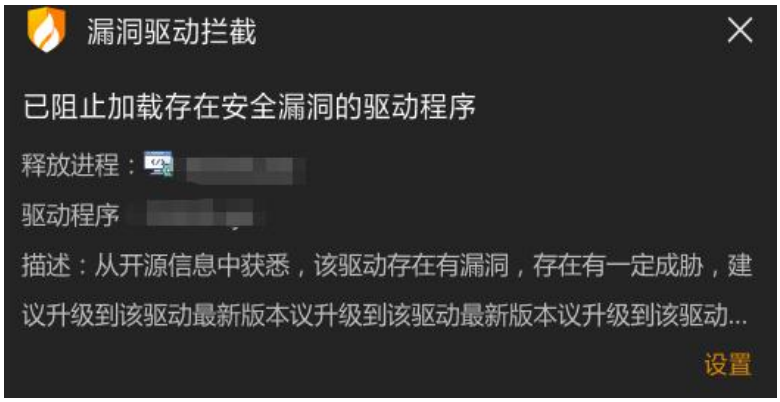
➡ 5：漏洞驱动拦截设置说明

✓ 拦截设置

您可在拦截设置中调整发现漏洞驱动加载时的处理方式：仅通知、自动阻止。

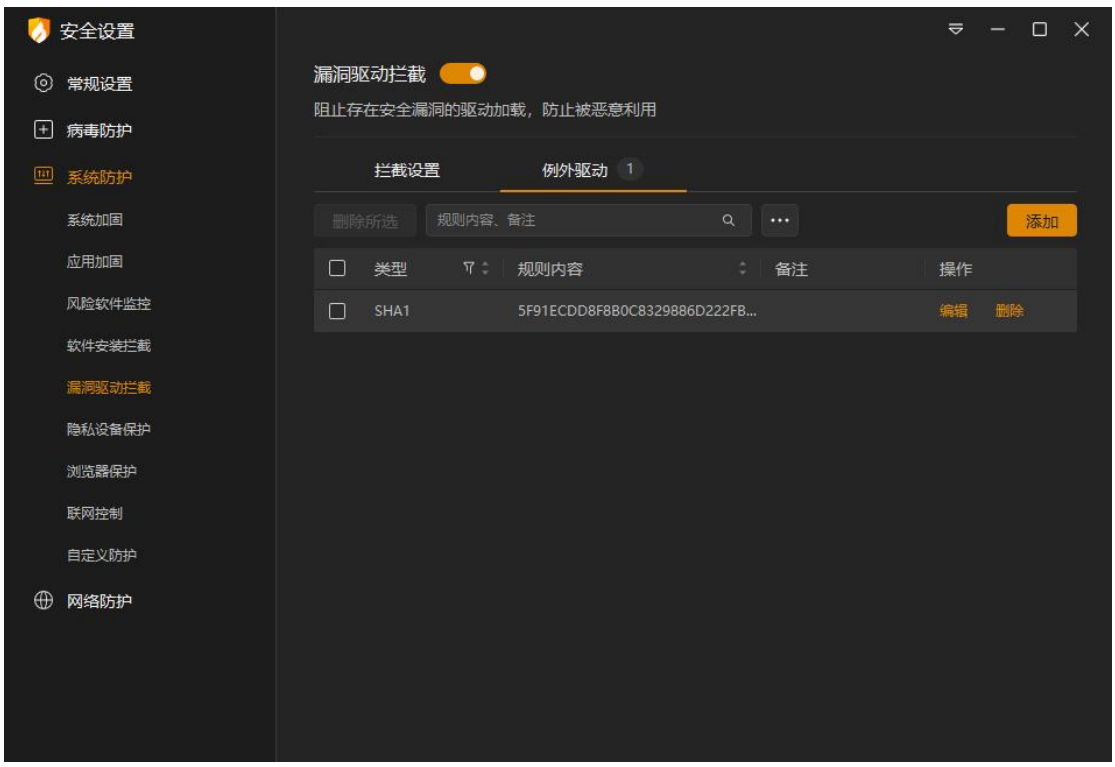
功能		说明
加载存在安全漏洞的驱动时	**仅通知**	选择此项后，加载存在安全漏洞的驱动时，将允许加载且弹窗提示
	自动阻止	默认选择此项，选择此项后，加载存在安全漏洞的驱动时，将阻止加载且弹窗提示
功能开关		开启：漏洞驱动拦截功能生效。 关闭：漏洞驱动拦截功能未生效。





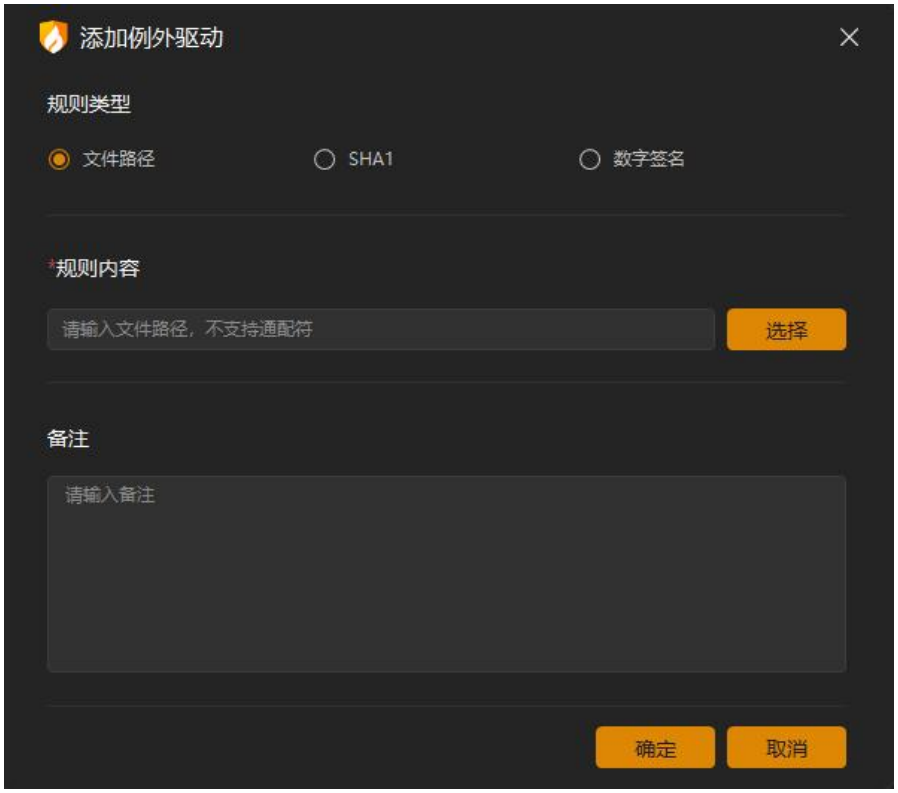
✓ **例外驱动**

如您想要允许加载某个存在安全漏洞的驱动，可将目标驱动添加至例外驱动列表。该列表中的驱动加载时将自动允许。



功能	说明
删除	删除所有选中规则。
搜索	支持通过规则内容或备注进行模糊搜索。
添加	弹出添加例外驱动窗口。
导入	导入例外驱动规则。
导出	导出选中的例外驱动规则。
编辑	编辑对应的规则。
筛选	通过类型筛选规则。

支持通过文件路径或SHA1值或数字签名3种方式添加例外驱动规则(注:WindowsXP系统不支持识别数字签名类型的例外驱动规则)。



6：隐私设备保护设置说明

✓ 功能设置

您可在隐私设备保护设置中调整规则列表中程序的启动摄像头和麦克风的权限。

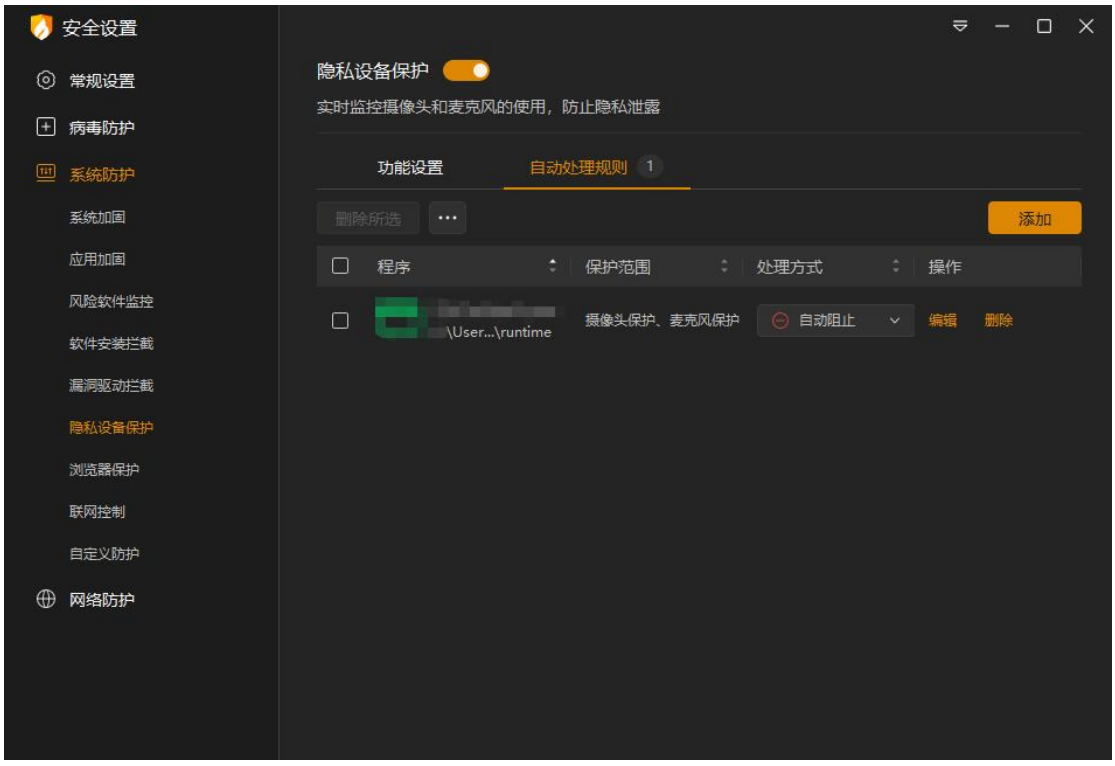
功能		说明
功能开关		开启：隐私设备保护功能生效。 关闭：隐私设备保护功能未生效。
摄像头保护开关		开启：摄像头保护功能生效。 关闭：摄像头保护功能未生效。
新程序启用摄像头时处理方式	**仅通知**	默认选择此项，选择后，新程序启用摄像头时将进行提示。
	自动阻止	选择此项后，将默认阻止新程序启用摄像头。阻止后将创建一条自动处理规则。

	询问我	选择此项后，当有新程序启用摄像头时，将弹窗询问您的操作。
麦克风保护开关		开启：麦克风保护功能生效。 关闭：麦克风保护功能未生效。
新程序启用麦克风时处理方式	**仅通知**	默认选择此项，选择后，新程序启用麦克风时将进行提示。
	自动阻止	选择此项后，将默认阻止新程序启用麦克风。阻止后将创建一条自动处理规则。
	询问我	选择此项后，当有新程序启用麦克风时，将弹窗询问您的操作。
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或麦克风时，将默认允许，不会弹窗提示，但会创建一条自动处理规则。
自动放行系统核心程序		勾选后，带有系统程序启用摄像头或麦克风时，将默认允许，不会弹窗提示。

★ 在设置为询问我时，火绒发现软件需要启动摄像头或麦克风时会弹出提示弹窗，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。


隐私设备保护
发现软件启用摄像头
建议您立即阻止
发起程序：示例程序.exe
数字签名：示例程序网络科技有限公司
推荐操作：如果不是您主动开启摄像头，建议您阻止。
记住本次操作，下次自动处理
阻止（30）
允许

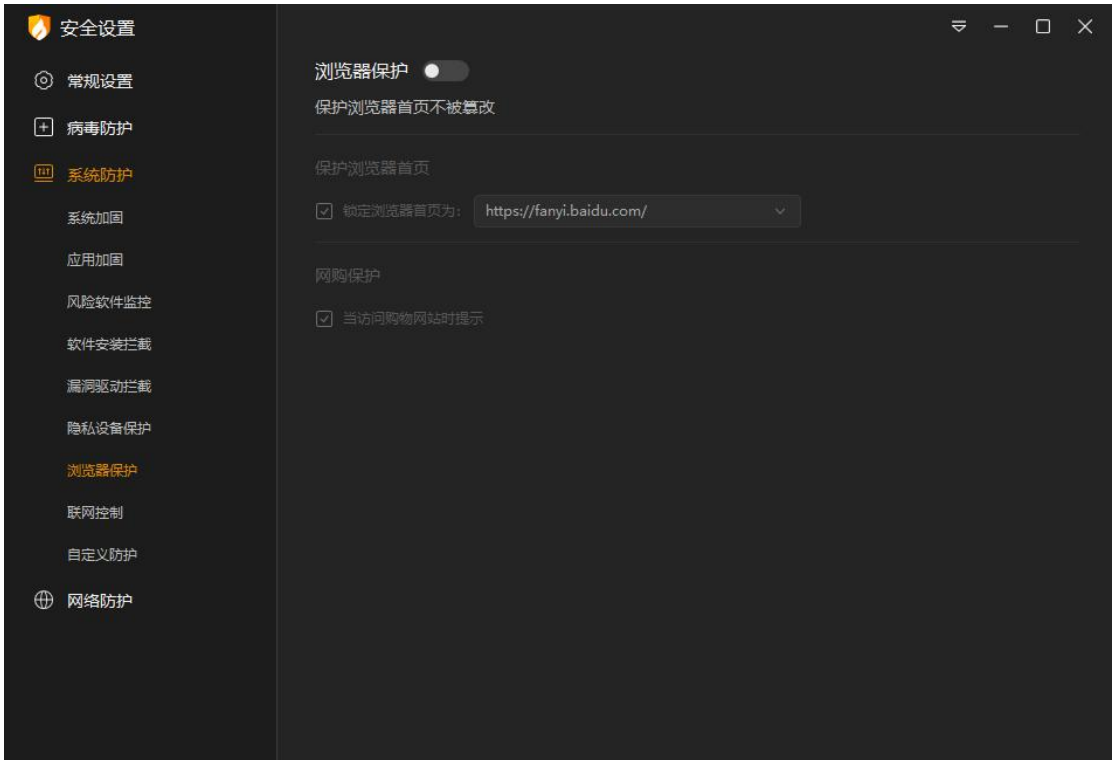
✓ 自定义规则


安全设置
常规设置
病毒防护
系统防护
系统加固
应用加固
风险软件监控
软件安装拦截
漏洞驱动拦截
隐私设备保护
浏览器保护
联网控制
自定义防护
网络防护
隐私设备保护
实时监控摄像头和麦克风的使用，防止隐私泄露
功能设置
自动处理规则 1
删除所选
添加
程序
保护范围
处理方式
操作
\User...\runtime
摄像头保护、麦克风保护
自动阻止
编辑
删除

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。
添加	点击打开添加规则窗口，为指定程序配置访问摄像头和麦克风行为的自动处理规则。
导入	导入隐私设备保护的规则。
导出	导出选中的隐私设备保护规则。
编辑	编辑选中的规则。

7：浏览器保护设置说明

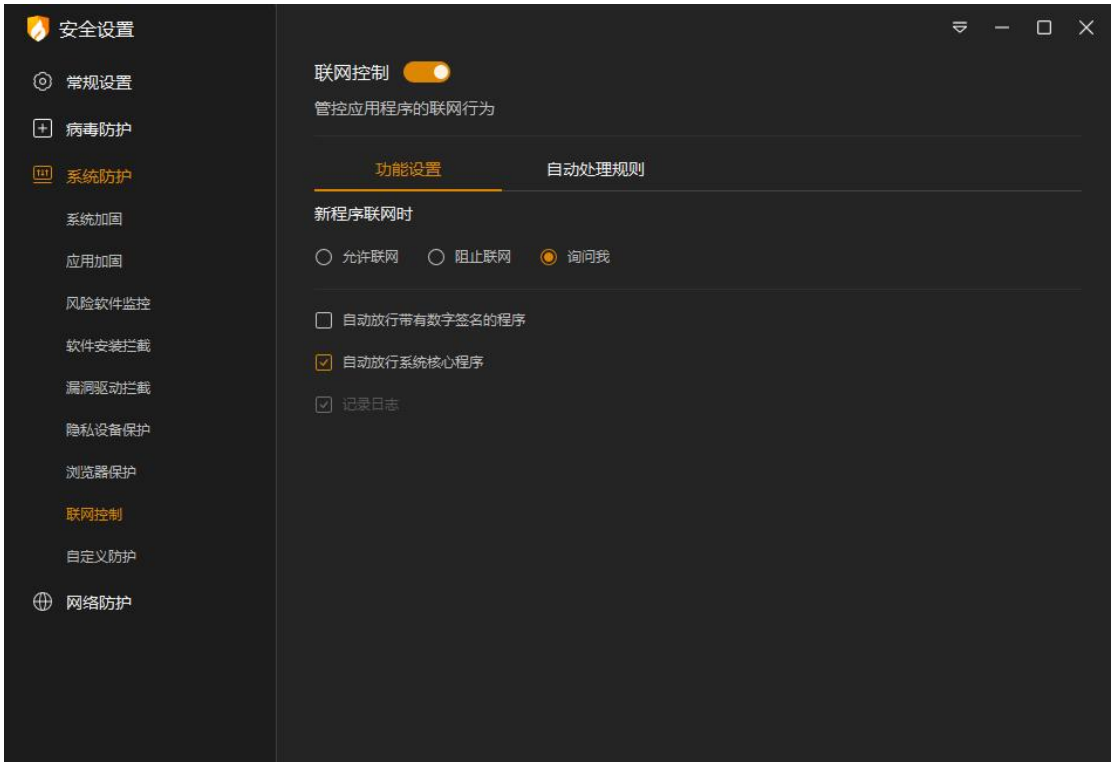
您可在浏览器保护设置中锁定浏览器首页、以及是否开启网购保护。



功能	说明
保护浏览器首页	保护浏览器的首页不被恶意篡改。
网购保护	当访问购物网站时，进行提示和保护。
功能开关	开启：浏览器保护功能生效。 关闭：浏览器保护功能未生效。

8：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。



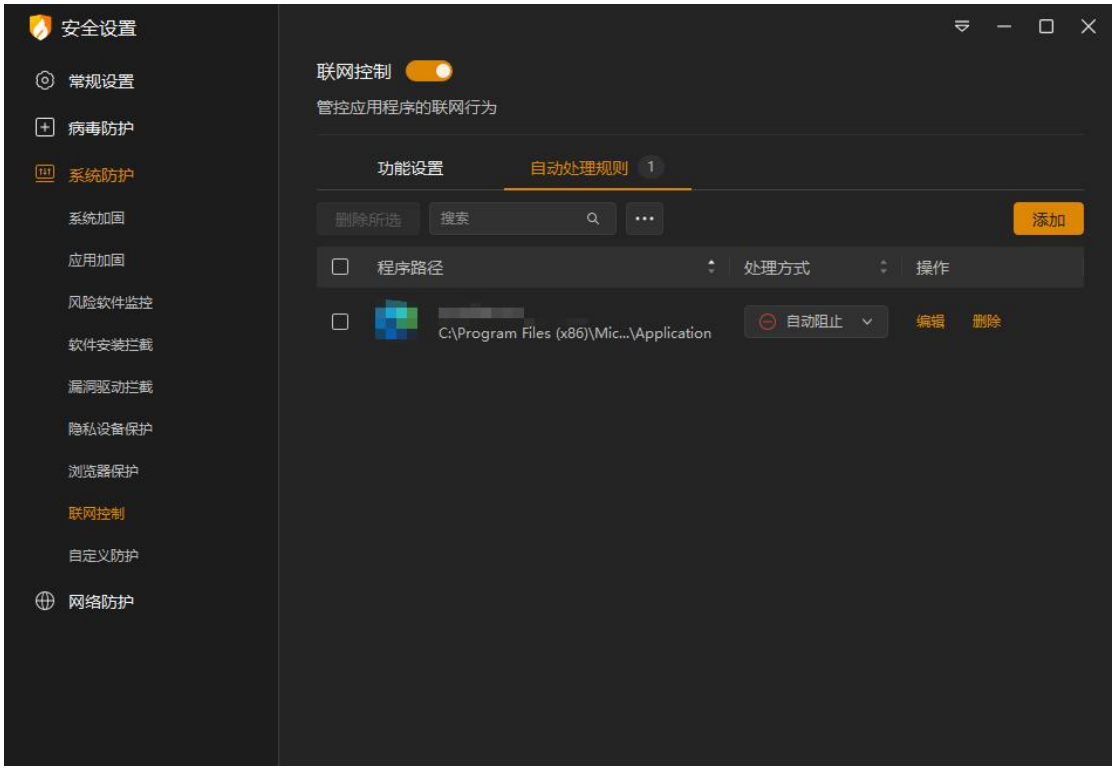
✓ **功能设置**

功能		说明
新程序联网时	**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。允许后将创建一条自动处理规则。
	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。阻止后将创建一条自动处理规则。
	询问我	未在自动处理规则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。
功能开关		开启：联网控制功能生效。 关闭：联网控制功能未生效。

★ 当【联网设置】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。

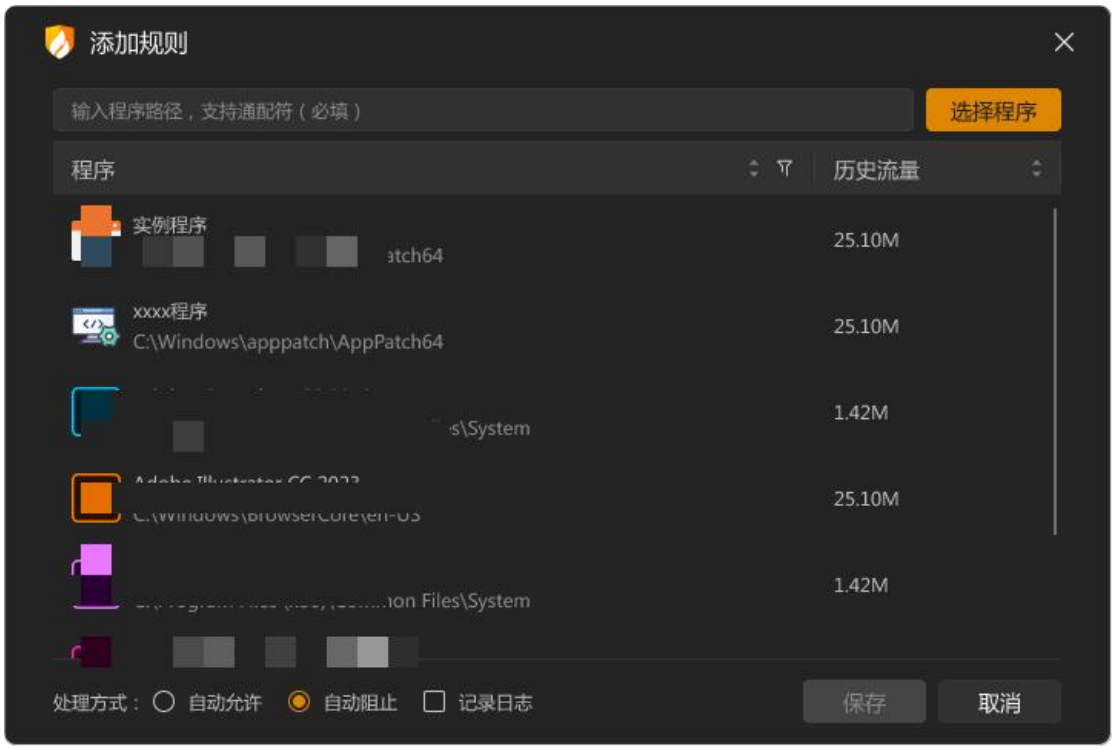

联网控制
发现程序联网行为
发起程序：示例程序.exe
数字签名：示例程序网络科技有限公司
记住本次操作，下次自动处理
阻止（30）
允许

✓ **自定义规则**


安全设置
常规设置
病毒防护
系统防护
系统加固
应用加固
风险软件监控
软件安装拦截
漏洞驱动拦截
隐私设备保护
浏览器保护
联网控制
自定义防护
网络防护
联网控制
管控应用程序的联网行为
功能设置
自动处理规则 1
删除所选
搜索
添加
程序路径
处理方式
操作
C:\Program Files (x86)\Mic...\Application
自动阻止
编辑
删除

功能	说明
搜索	支持通过程序路径来搜索规则，并实时展示搜索结果。
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。
添加	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控制联网的程序。



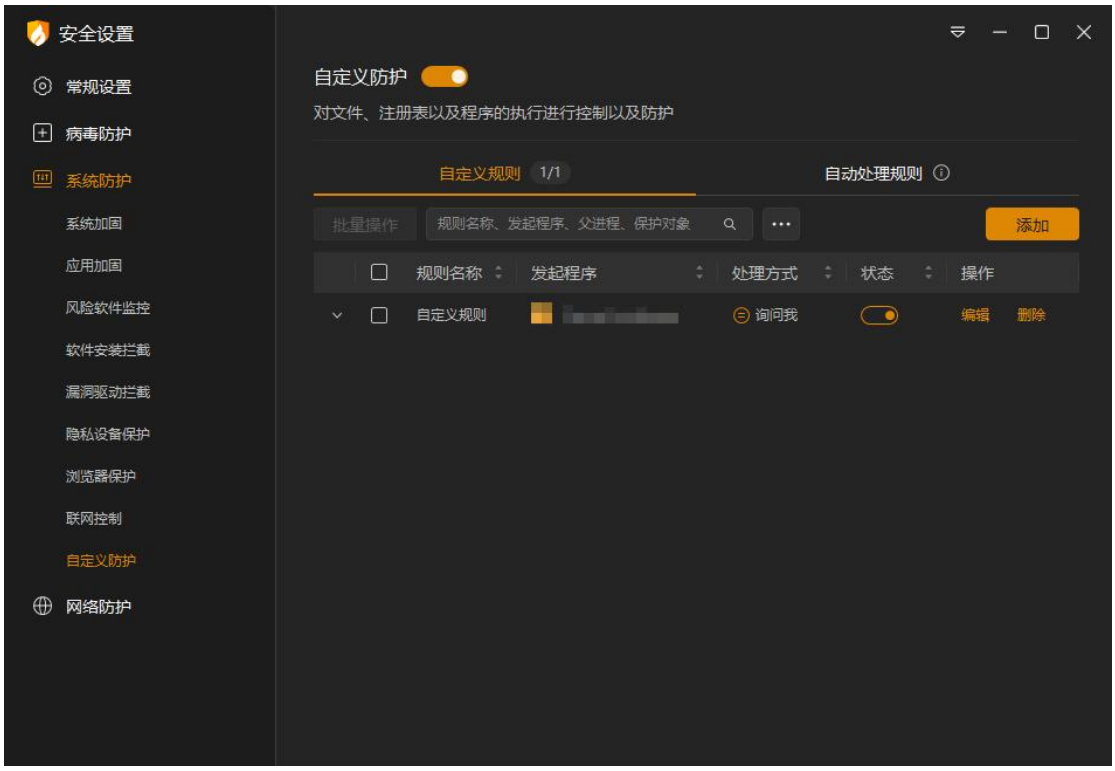
功能	说明
处理方式	为程序的联网行为选择处理方式，默认勾选阻止联网。
是否记录日志	复选框，勾选即针只针对本条数据的规则被触发时，记录相关日志。
保存	保存当前规则，添加至规则列表中。
取消	退出添加规则状态，不保存当前规则。

➡ 9：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。

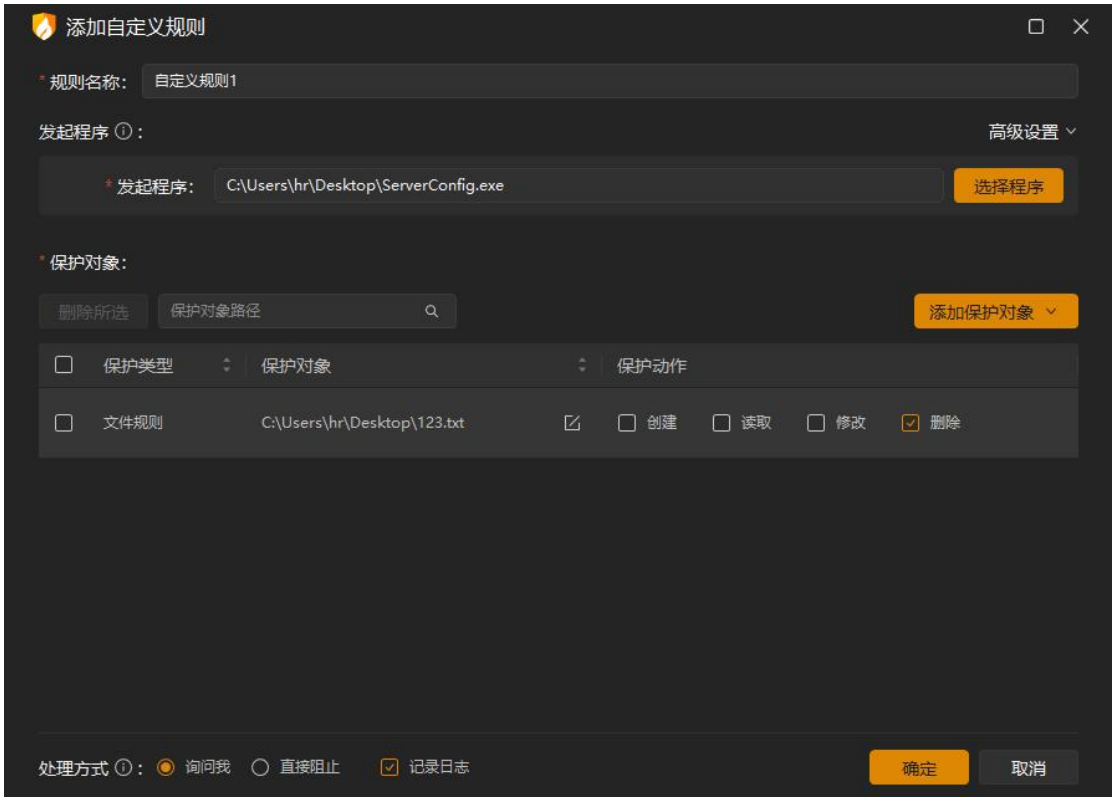
✓ 自定义防护-自定义规则

第一步：点击【自定义规则】（见下图），进入自定义规则页面。



功能	说明
搜索	支持通过规则名称、发起程序、父进程、保护对象搜索规则，并实时展示搜索结果。
状态开关	开关亮色表示规则启用，开关灰色表示规则未启用。
编辑	编辑对应的规则。
删除	删除对应的规则。
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	点击添加规则进入自定义防护规则添加页面（见下图）。
批量操作	点击可选择将选中的规则批量删除、批量修改状态、批量修改处理方式
功能开关	开启：自定义防护功能生效。 关闭：自定义防护功能未生效。

第二步：添加自定义规则

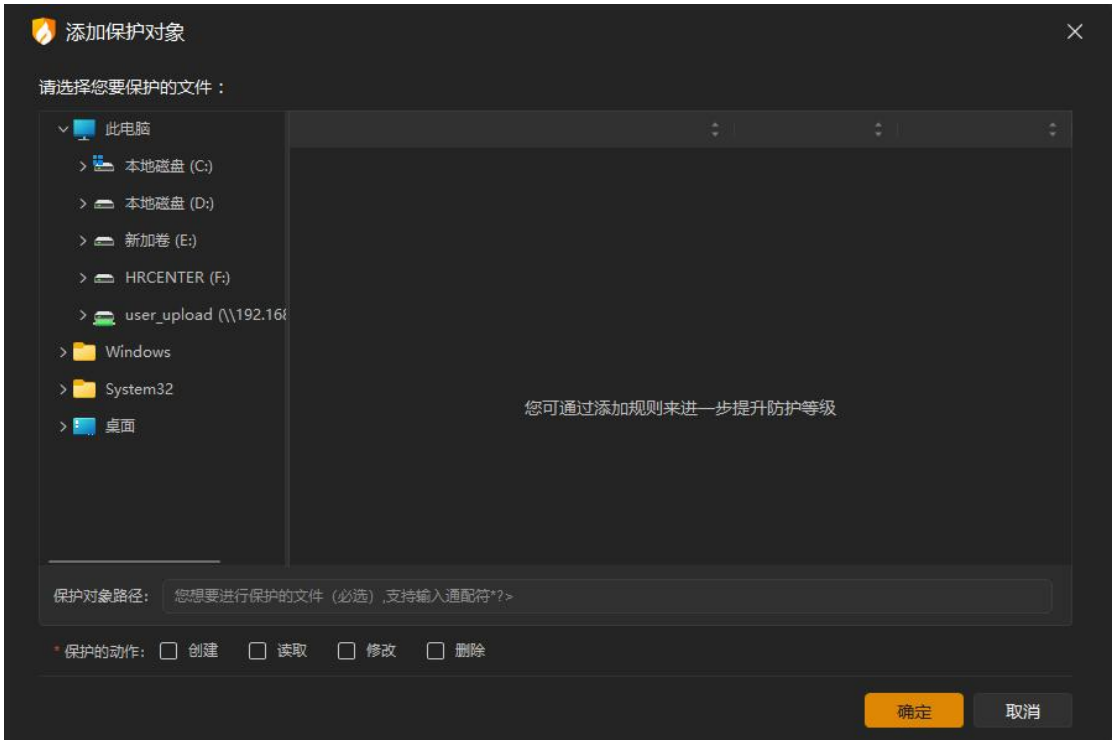


功能		说明
规则名称		有默认规则名称，可修改。
发起程序		选择需要控制操作的程序，支持通配符。
高级设置		需要更精准的识别发起程序时，可点击高级设置配置发起程序命令行、发起程序父进程和父进程命令行。
搜索		可针对保护对象内容进行搜索。
保护对象	**添加保护对象**	添加阻止程序操作的对象，点击后需选择要保护的类型：文件、注册表、执行程序，进入对应的选择保护对象页面（见下图）。
	编辑	编辑时支持修改保护对象路径和保护动作，不支持修改保护类型。 点击保护对象路径后的编辑图标，进入编辑态，可手动输入

		保护对象路径，也可点击【浏览】重新选择保护对象。
	删除	删除选中的保护对象。
处理方式	**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，不再弹窗询问您。
	记录日志	默认勾选，取消勾选后，则触发规则时不记录日志。
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。

第三步：添加保护对象-文件规则

点击【添加保护对象】时，需选择要添加的保护类型：文件规则、注册表规则、执行规则。选择保护类型后，进入对应的选择界面，下图为添加文件规则页面。

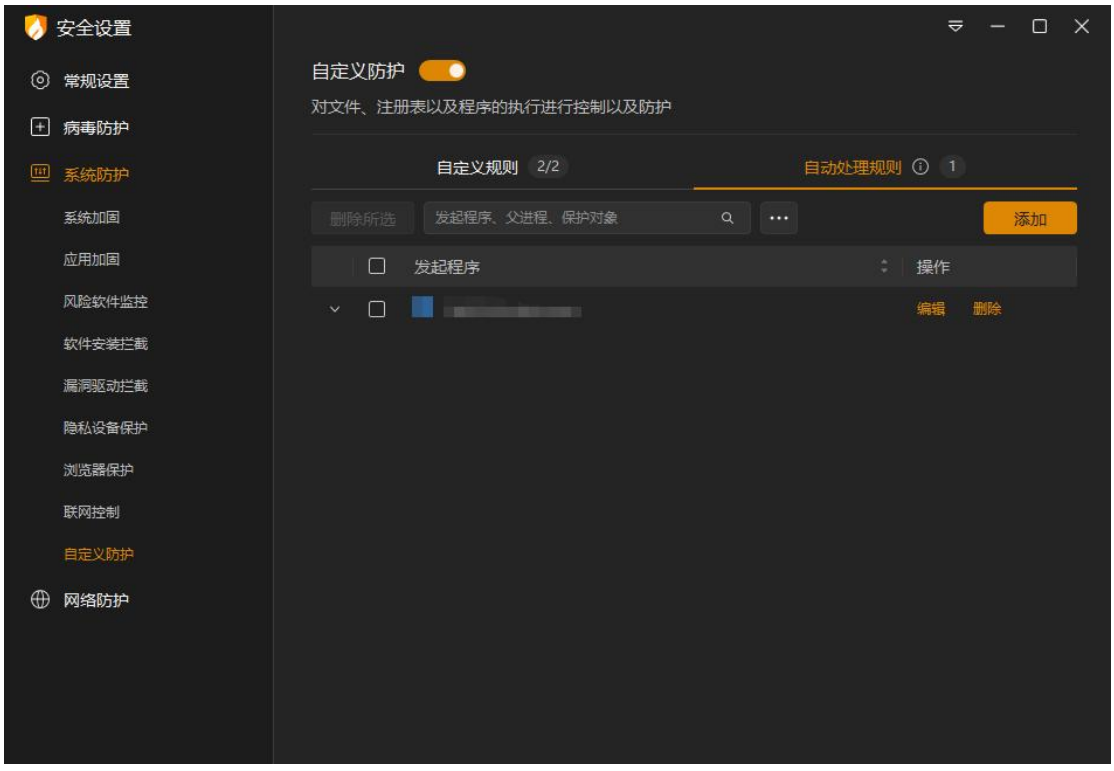


功能	说明

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。
保护动作		勾选要阻止的操作
保存		保存此保护对象，添加至保护对象列表中。
取消		关闭添加保护对象页，不保存该保护对象。

✓ **自定义防护-自动处理**

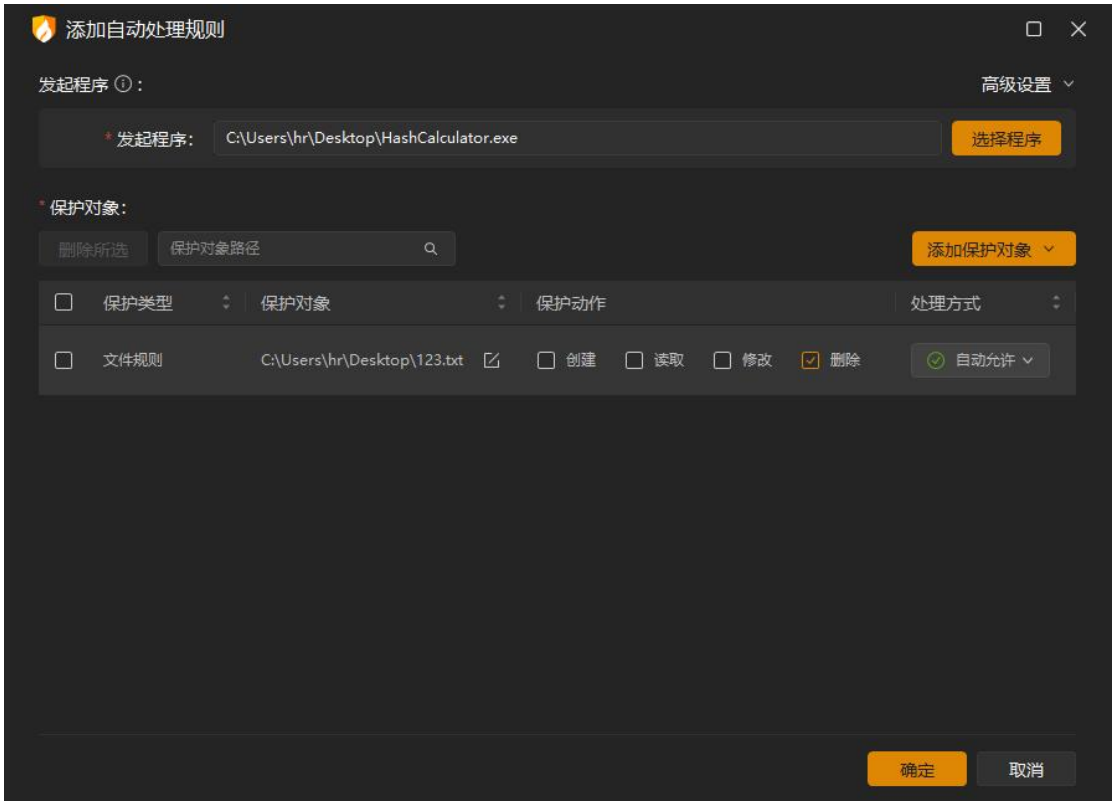
触发自定义规则后，才会继续匹配自动处理规则。自动处理规则的优先级高于自定义规则。点击【自动处理】（见下图）进入自动处理规则页面。



功能	说明
搜索	支持通过发起程序、父进程、保护对象搜索规则，并适时展示搜索结果。
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	点击后弹出添加自动处理规则弹窗。

添加自动处理规则：

第一步：点击【添加】，弹窗见下图。

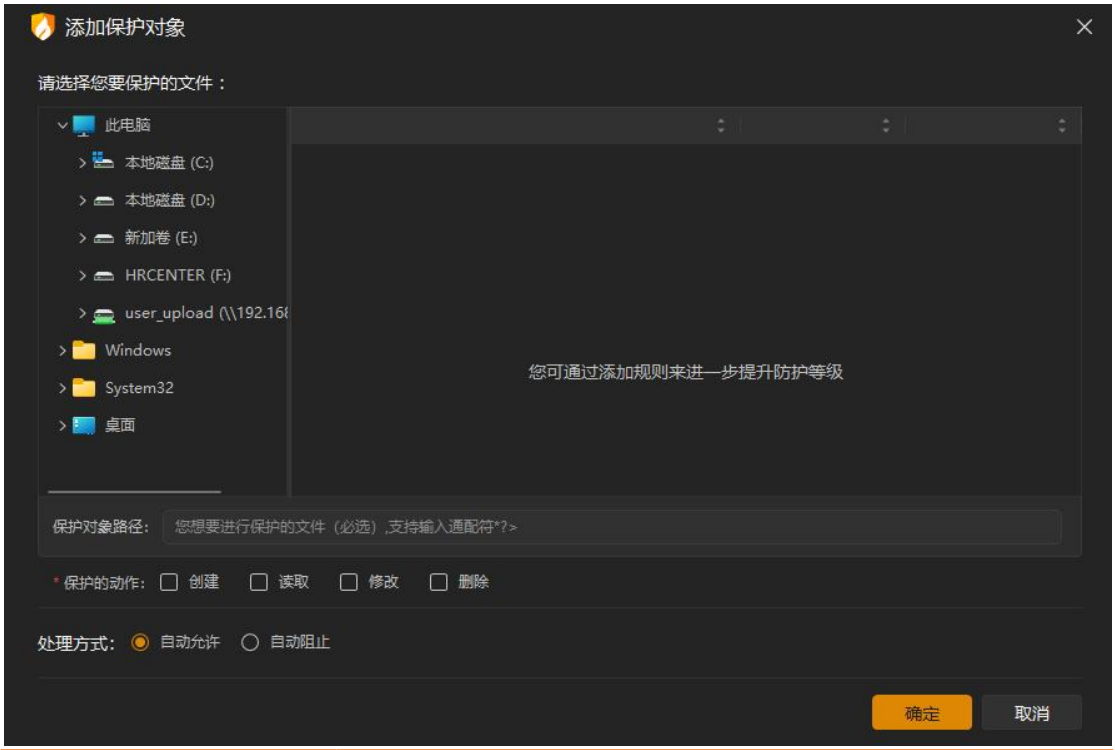


功能	说明
发起程序	选择需要阻止操作的程序，支持通配符。
高级设置	需要更精准的识别发起程序时，可点击高级设置配置发起程序

		命令行、发起程序父进程和父进程命令行。
搜索		可针对保护对象路径进行搜索。
保护对象	**添加**	添加阻止/允许程序操作的对象，点击后需选择要保护的类型：文件、注册表、执行程序，进入对应的选择保护对象页面（见下图）。
	编辑	编辑时支持修改保护对象路径、保护动作和处理方式，不支持修改保护类型。 点击保护对象路径后的编辑图标，进入编辑态，可手动输入保护对象路径，也可点击【浏览】重新选择保护对象。
	删除	删除选中的保护对象。
确定		保存当前规则，添加至自动处理规则列表中。
取消		点击关闭弹窗，不保存规则。

第二步：添加保护对象-文件规则

点击【添加保护对象】时，需选择要添加的保护类型：文件规则、注册表规则、执行规则。选择保护类型后，进入对应的选择界面，下图为添加文件规则页面。



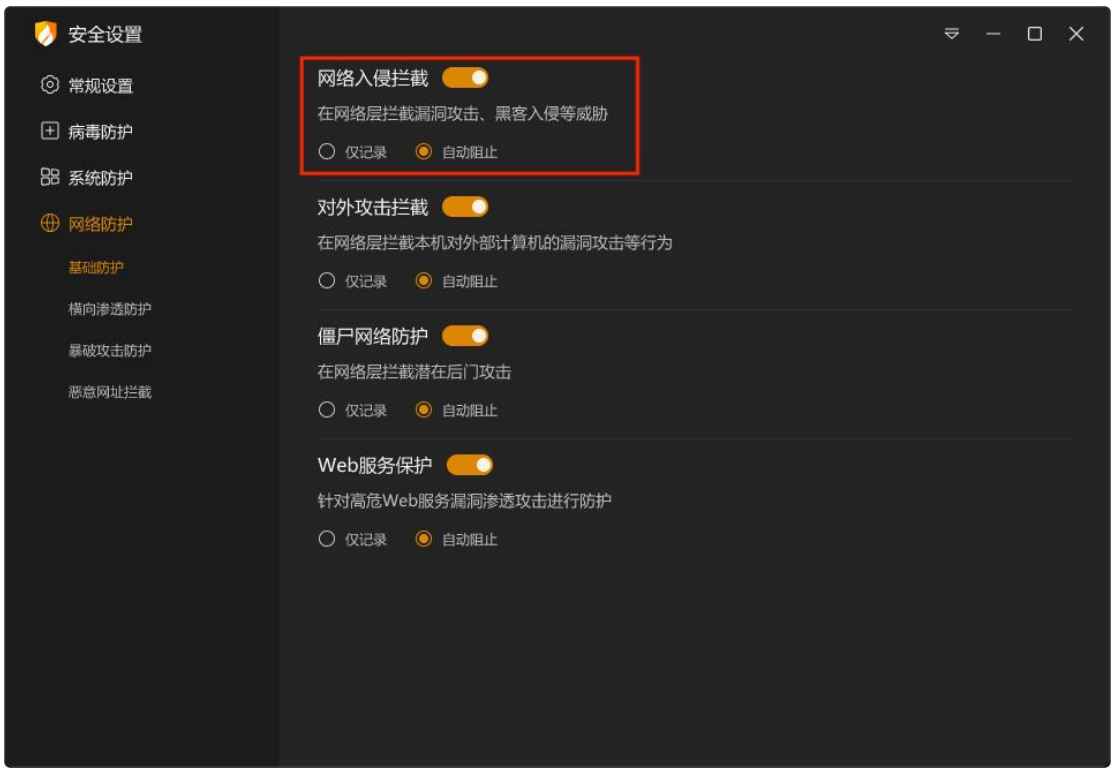
功能		说明
保护对象	**文件规则**	选择需要保护的文件，勾选需要阻止的操作，可选择创建、读取、写入、删除四项操作限制。
	注册表规则	选择需要保护的注册表，勾选需要阻止的操作，可选择创建、读取、写入、删除四项操作限制。
	执行规则	阻止程序运行其他程序。
保护动作		勾选要允许/阻止的操作。
处理方式		选择触发规则时的处理方式。 自动阻止：触发规则后自动阻止 自动允许：触发规则后自动放行
保存		保存此保护对象规则。
取消		关闭添加保护对象页，不保存规则。

★ 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，添加至自动处理规则】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（该途径创建的自动处理规则，默认【发起程序命令行】、【父进程】、【父进程命令行】均为“*”）。

● 网络防护

➡ 1：网络入侵拦截设置说明

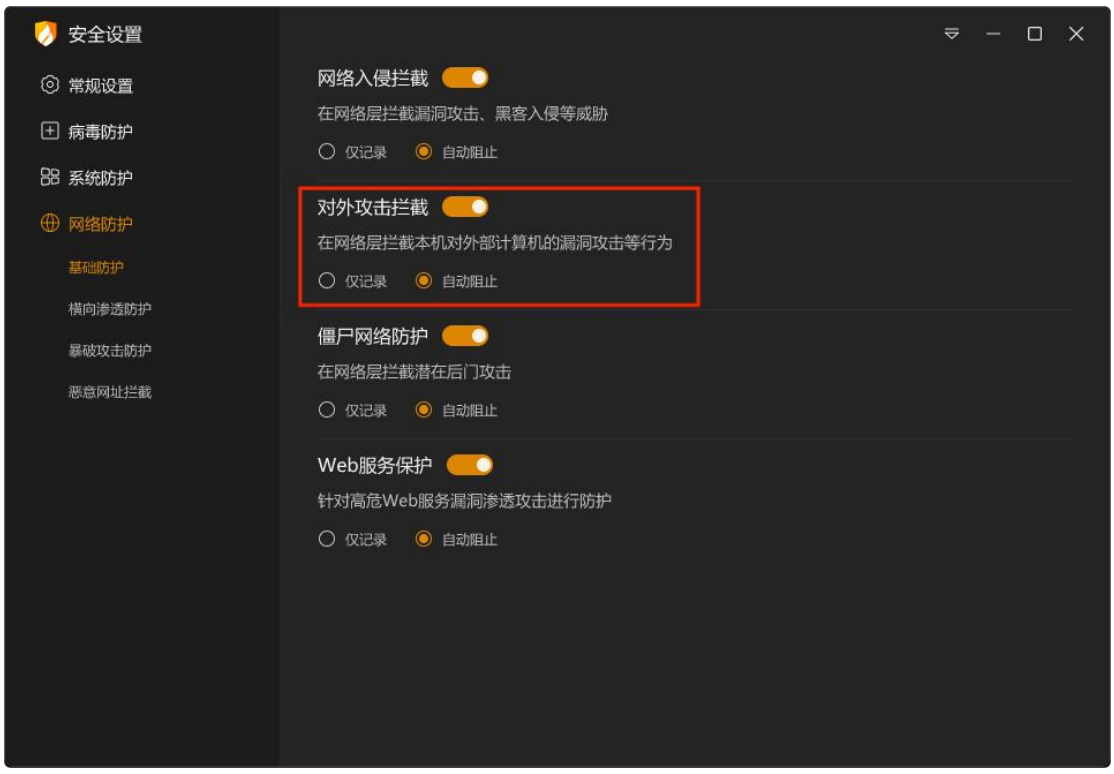
您可在设置中调整当发生黑客入侵或其他网络入侵行为时火绒需进行的操作。



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。
功能开关	开启：网络入侵拦截功能生效。 关闭：网络入侵拦截功能未生效。

2：对外攻击拦截设置说明

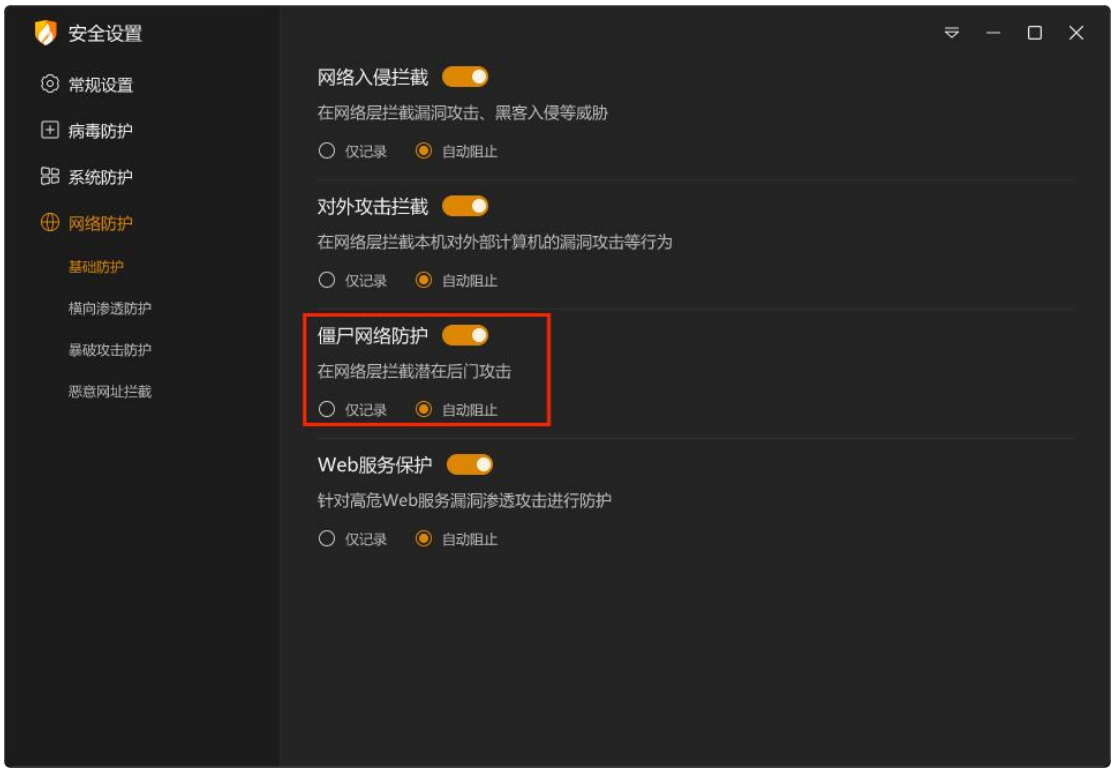
您可在设置中调整当本机发生对外攻击行为时火绒需进行的操作。



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。
功能开关	开启：对外攻击拦截功能生效。 关闭：对外攻击拦截功能未生效。

3： 僵尸网络防护设置说明

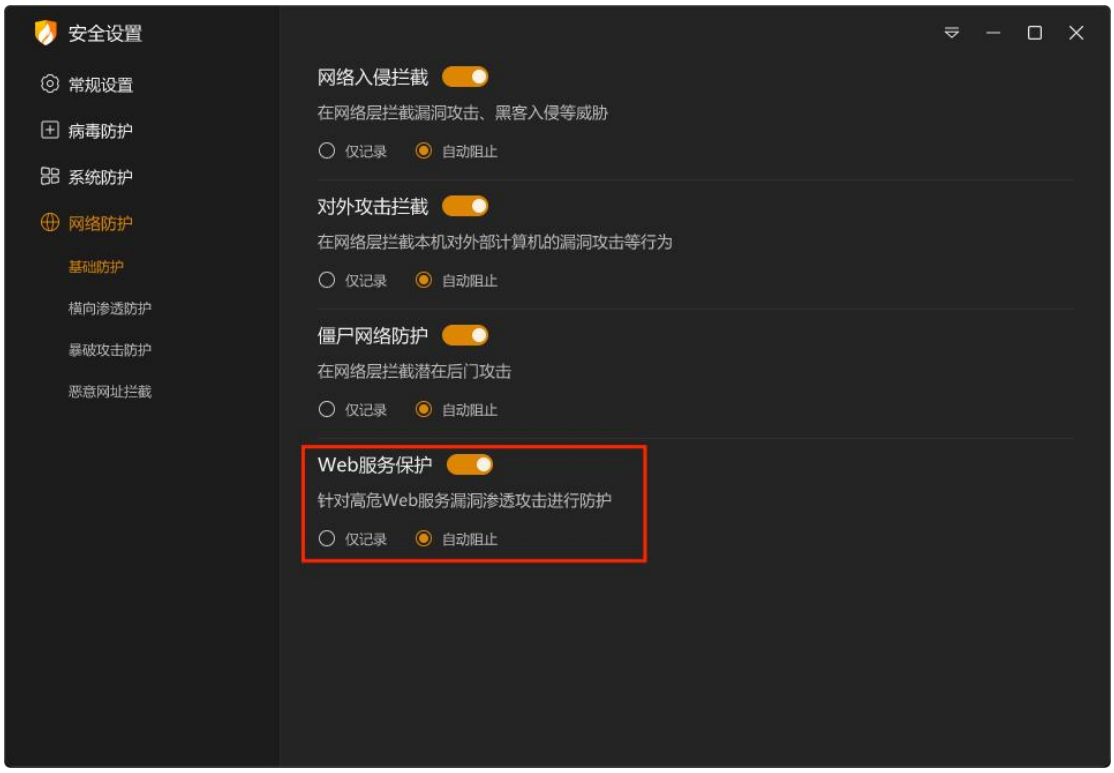
当您的计算机被非法远程控制时火绒需进行的操作。



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。
功能开关	开启：僵尸网络防护功能生效。 关闭：僵尸网络防护功能未生效。

4：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。

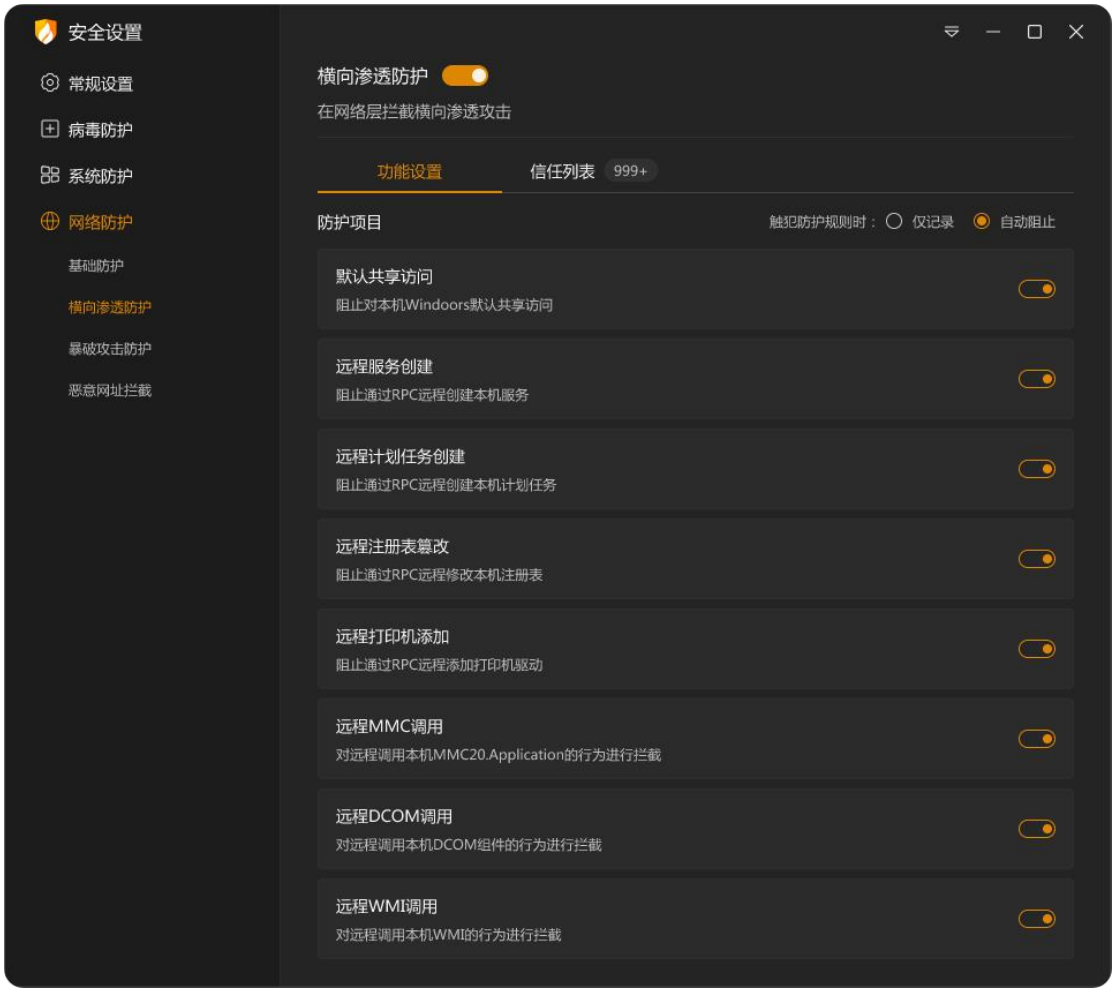


功能	说明
仅记录	不阻止对服务器软件的攻击，只在安全日志中记录攻击行为。
自动处理	阻止对服务器软件的攻击，并在安全日志中记录攻击行为。
功能开关	开启：Web 服务保护功能生效。 关闭：Web 服务保护功能未生效。

5：横向渗透防护设置说明

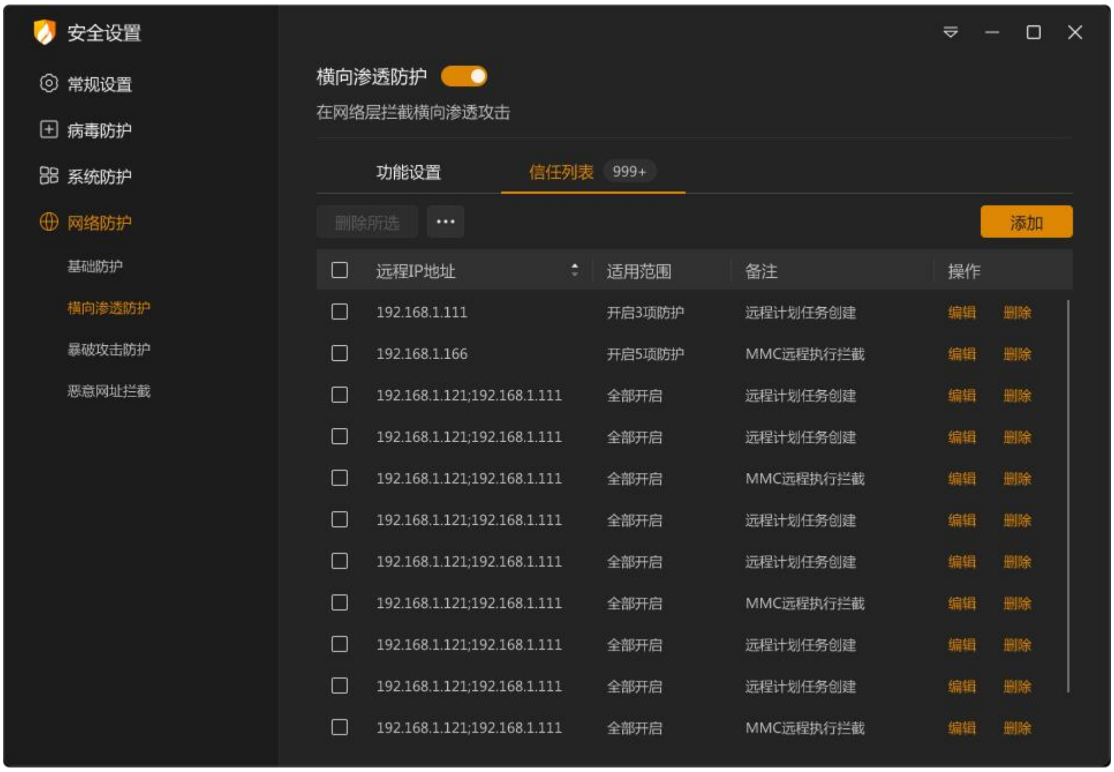
横向渗透防护开启后，触犯防护规则时默认设置为自动阻止。根据不同情况您也可调整为触犯防护规则时仅记录。同时也可以添加信任规则，对指定 IP 发起的横向渗透行为进行

放过。

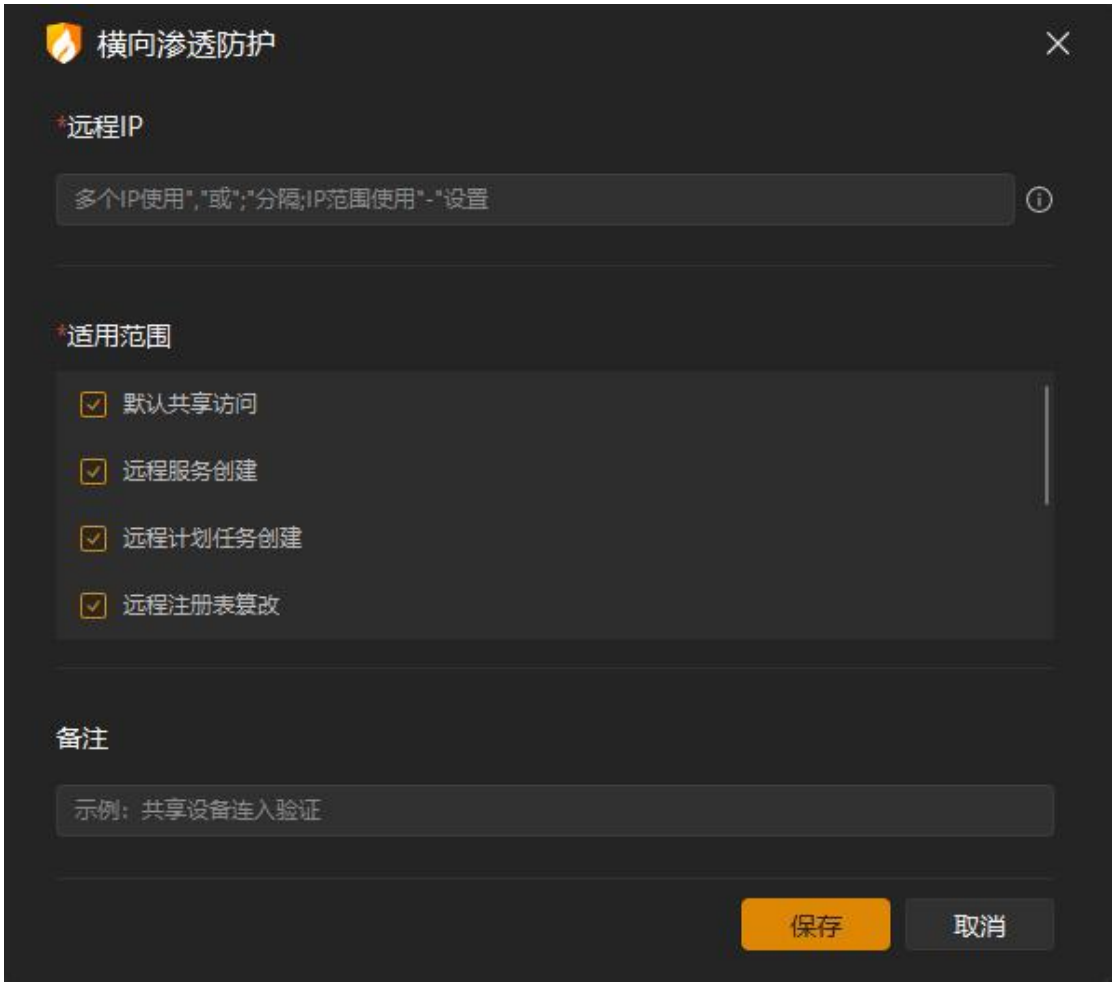


功能	说明
防护开关	某条防护项目的防护开关开启与关闭，影响着该防护项目的生效与否。
仅记录	发现横向渗透行为时，只在安全日志中记录渗透行为。
自动处理	发现横向渗透行为时，在安全日志中记录并阻止渗透行为。
功能开关	开启：横向渗透防护功能生效。 关闭：横向渗透防护功能未生效。

✓ **信任列表**



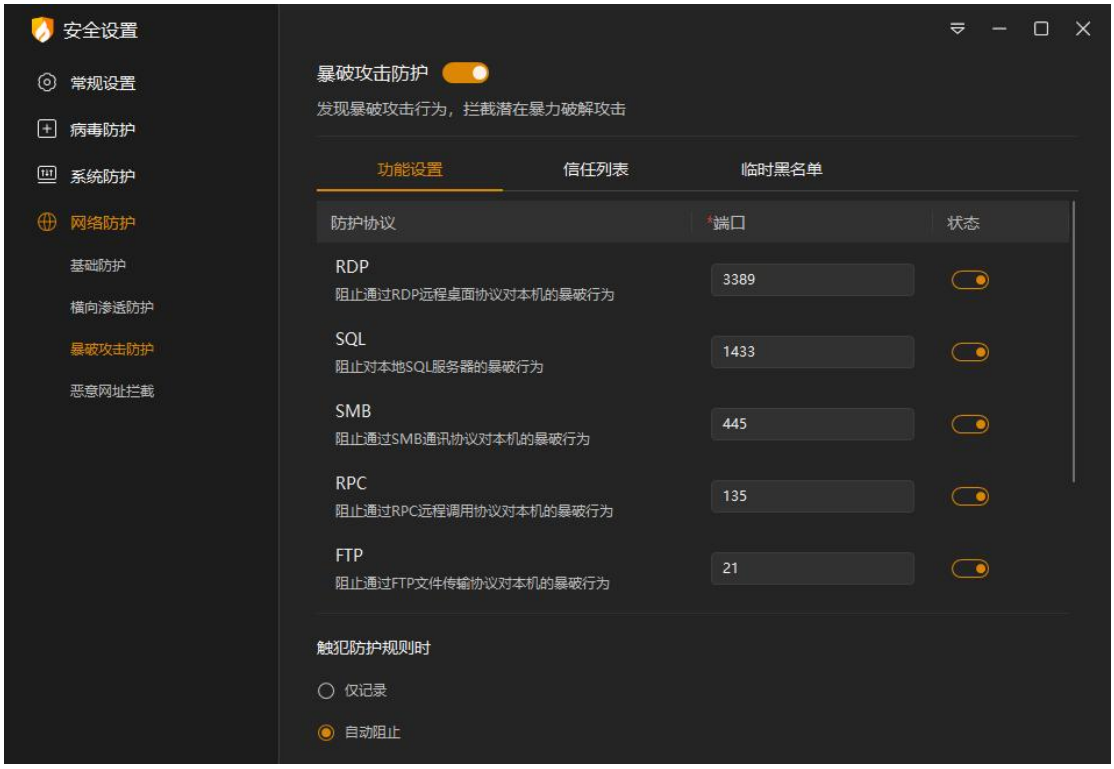
功能	说明
编辑	编辑选中的规则。
删除	删除所有选中的规则。
添加	点击添加规则打开规则添加页面（见下图）。
导入	导入信任规则。
导出	导出选中的信任规则。



功能	说明
远程 IP	设置需要访问的远程 IP 地址。可填写 IPv4（表示范围使用“_”）和 Ipv6（可缩写），支持 CDIR，多个 IP 请用“;”、“,”分隔；IP 范围使用“-”设置。
适用范围	设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一项。
备注	方便您辨识规则，可不填写。
保存	保存此规则。
取消	关闭添加规则页面，返回至信任列表页，不保存规则。

6：暴破攻击防护设置说明

您可在暴破攻击设置中设置自动拦截哪些协议的暴破攻击，不同协议的检测端口，检测暴破攻击的灵敏度，临时黑名单的生效时间和多源暴破攻击的处理方式。支持通过添加信任规则，对指定 IP 发起的远程登录行为进行放过。

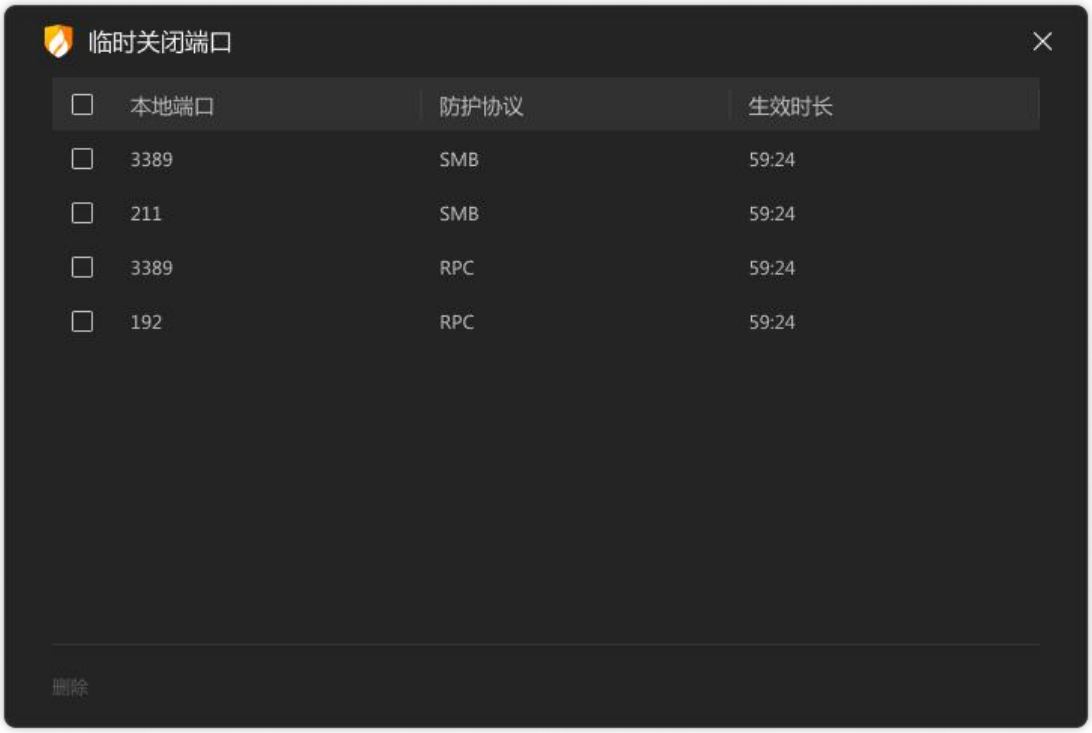


功能	说明
防护开关	防护开关开启与关闭，影响着该防护项目的生效与否。 可自定义不同协议的检测端口。
触犯防护规则时	仅记录：不阻止暴破攻击行为，只在安全日志中记录攻击行为。 自动阻止：阻止暴破攻击行为，并安全日志中记录攻击行为。
更多设置	打开设置窗口（见下图）。
功能开关	开启：暴破攻击防护功能生效。 关闭：暴破攻击防护功能未生效。

✓ **更多设置**

功能	说明
发现多源暴破攻击处理方式	仅记录：不拦截此类攻击，只在安全日志中记录攻击行为。 自动阻止：临时关闭端口 60 分钟以拦截此类攻击，并在安全日志中记录攻击行为，支持查看临时关闭的端口信息（见下图）。
检测灵敏度	灵敏度越高，可以检测到低频率的暴破攻击。
临时黑名单	设置临时黑名单的生效时长，默认 60 分钟。

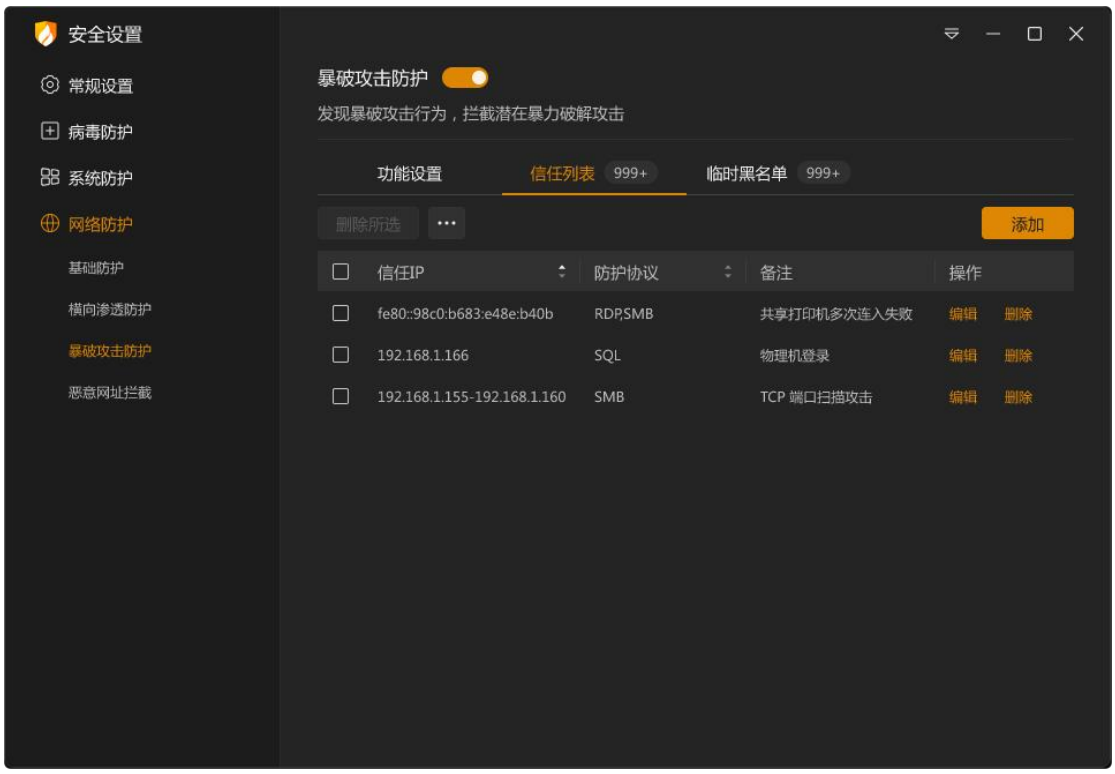
✓ **临时关闭端口**



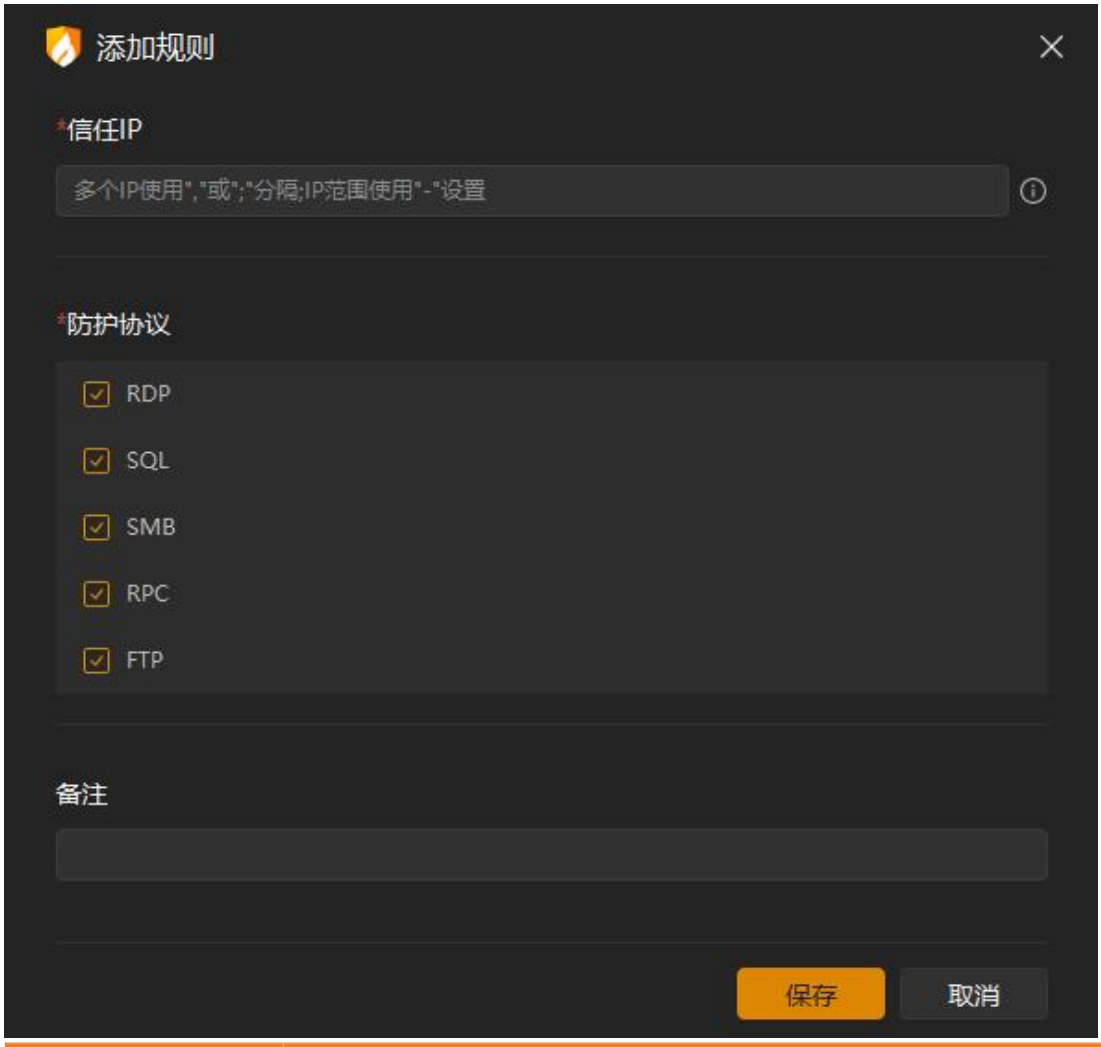
功能	说明
删除	删除选中的规则。

✓ **暴破攻击防护-信任列表**

添加信任规则，对指定 IP 发起的远程登录行为进行放过。

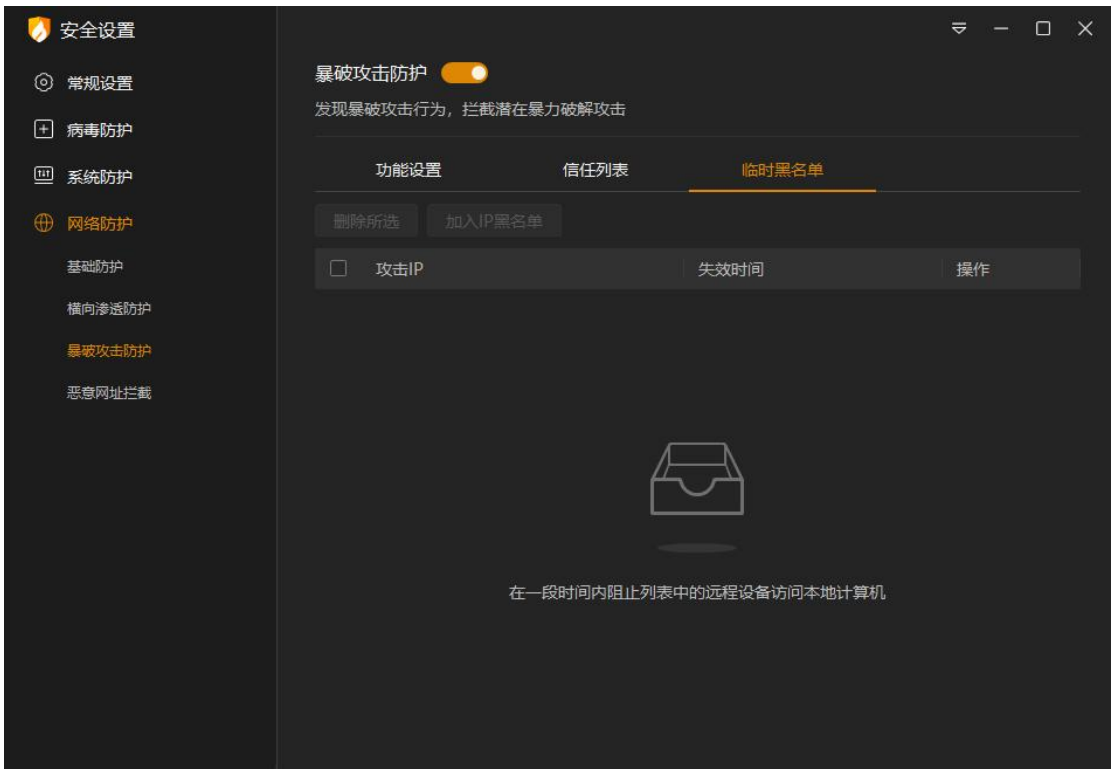


功能	说明
编辑	编辑选中的规则。
删除	删除选中的所有规则。
导入	导入信任规则。
导出	导出选中的所有信任规则。
添加规则	添加信任规则（见下图）。



功能	说明
信任 IP	填写允许登录本机的远程 IP 地址。
防护协议	选择允许采用的暴力破解攻击类型。
备注	方便您辨识规则，可不填写。
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。

✓ 临时黑名单



功能	说明
删除	将选中的攻击 IP 从临时黑名单移除。
加入 IP 黑名单	将攻击 IP 从临时黑名单移入至 IP 黑名单，永久拉黑直至手动删除。

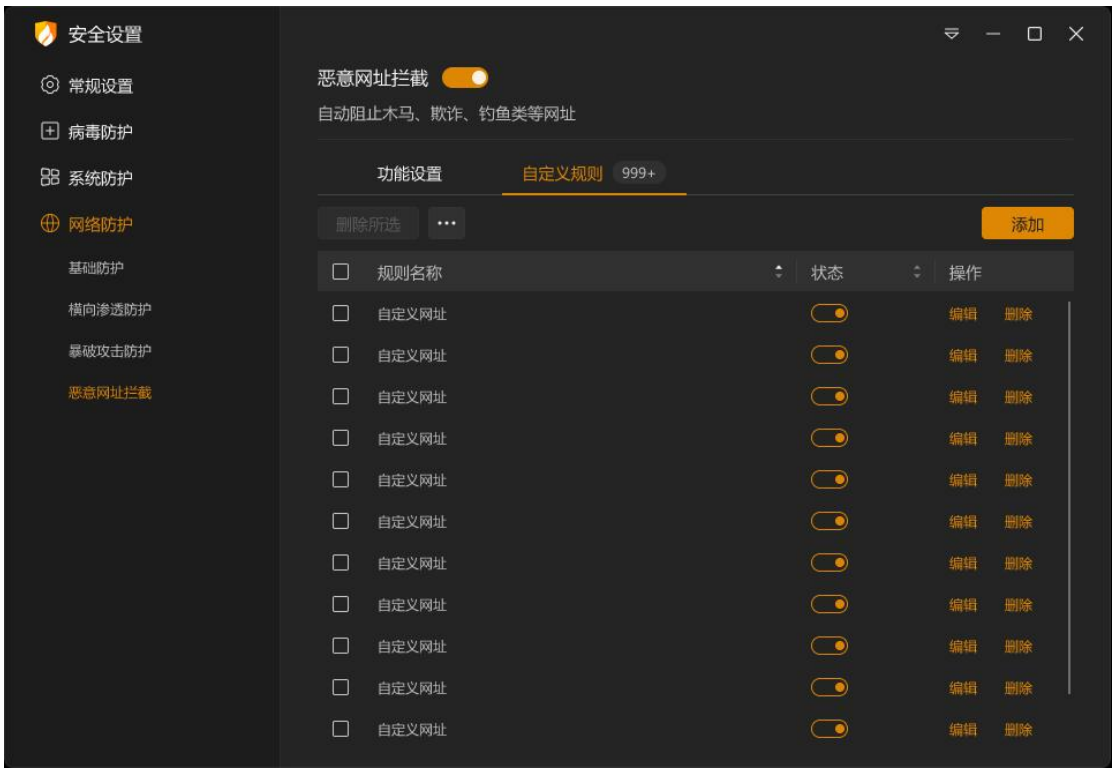
➡ 7：恶意网址拦截设置说明

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。

✓ **功能设置**

功能	说明
状态开关	开启：自动阻止打开该类网址。 关闭：允许打开该类网址。
开关状态	开启：恶意网址拦截功能生效。 关闭：恶意网址拦截功能未生效。

✓ 自定义规则



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	点击添加规则打开规则添加页面（见下图）。
状态开关	开启：自动阻止打开该类网址。 关闭：允许打开该类网址。

✓ **添加自定义规则**

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。

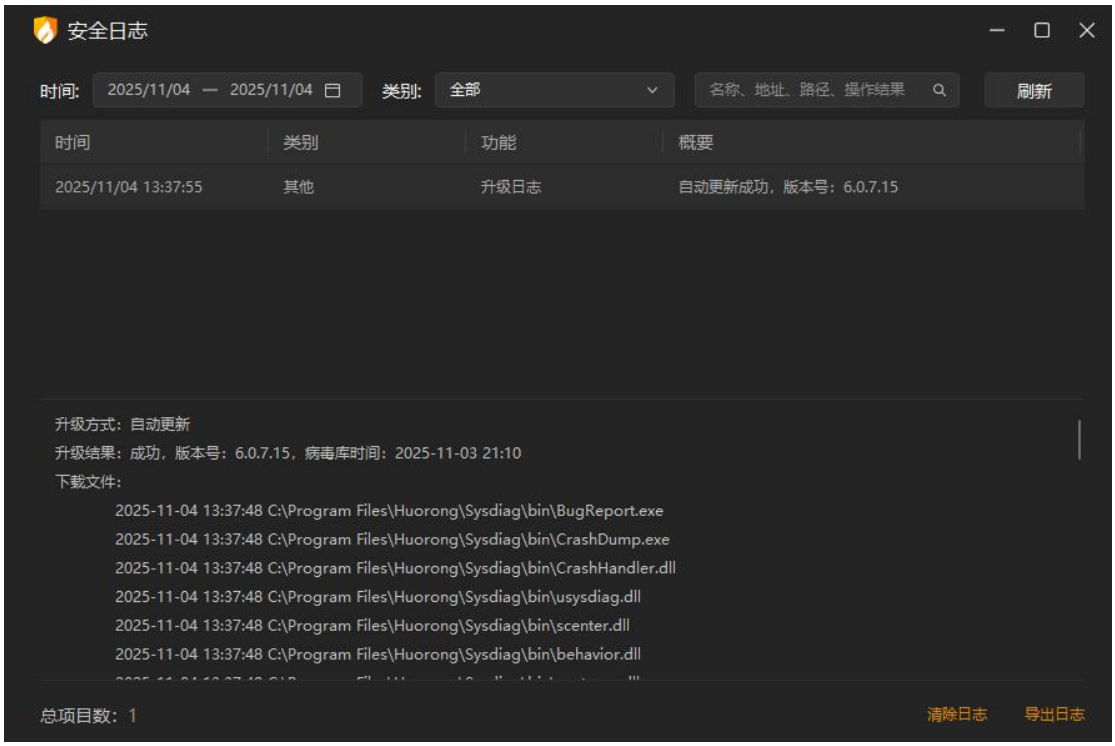
➢ 安全日志

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

您可在首页的主菜单中找到【安全日志】或首页的安全日志快捷入口（见下图），打开安全日志。

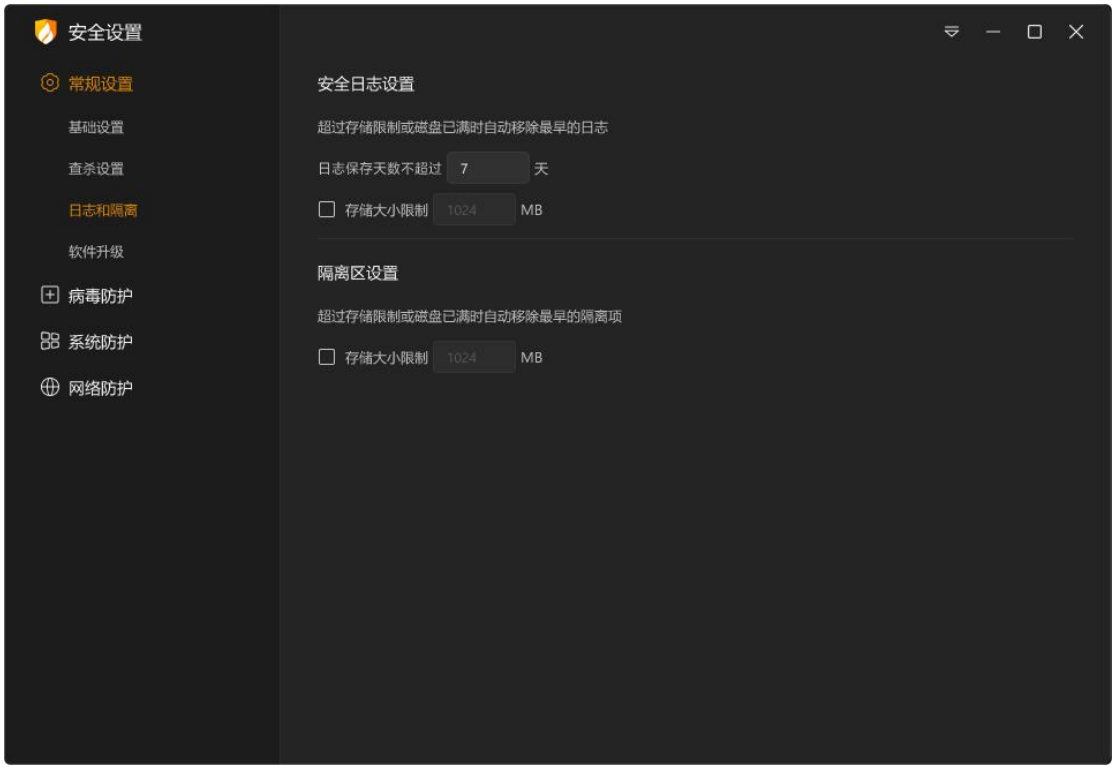
在安全日志中，您可根据需要自定义时间、类别、功能、关键词搜索过滤您要查看的内容。



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】、自定义时间段。
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、访问控制、安全工具、其他等。
功能	根据选择的【类别】显示需要具体查看的功能。
关键词搜索	支持通过【名称】【地址】【路径】【操作结果】字段进行模糊搜索符合条件的日志。 名称指：病毒名称、软件名称、设备名称、规则名称、补丁编号等字段； 地址指：远程地址、本地地址、访问地址等字段； 路径指：风险路径、进程路径、操作进程等字段； 操作结果指：处理结果、操作结果、防御结果、升级结果等字段；
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。
总项目数	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

您可在常规设置-日志和隔离设置中修改安全日志的保存天数、日志存储大小限制。



功能	说明
日志保存天数	根据需要选择日志保存天数，可自定义保存天数。
存储大小限制	根据需要设置是否限制日志存储大小，勾选后，超过存储限制或磁盘已满时自动移除最早的日志。

➢ 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】、首页的检查更新快捷入口（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。

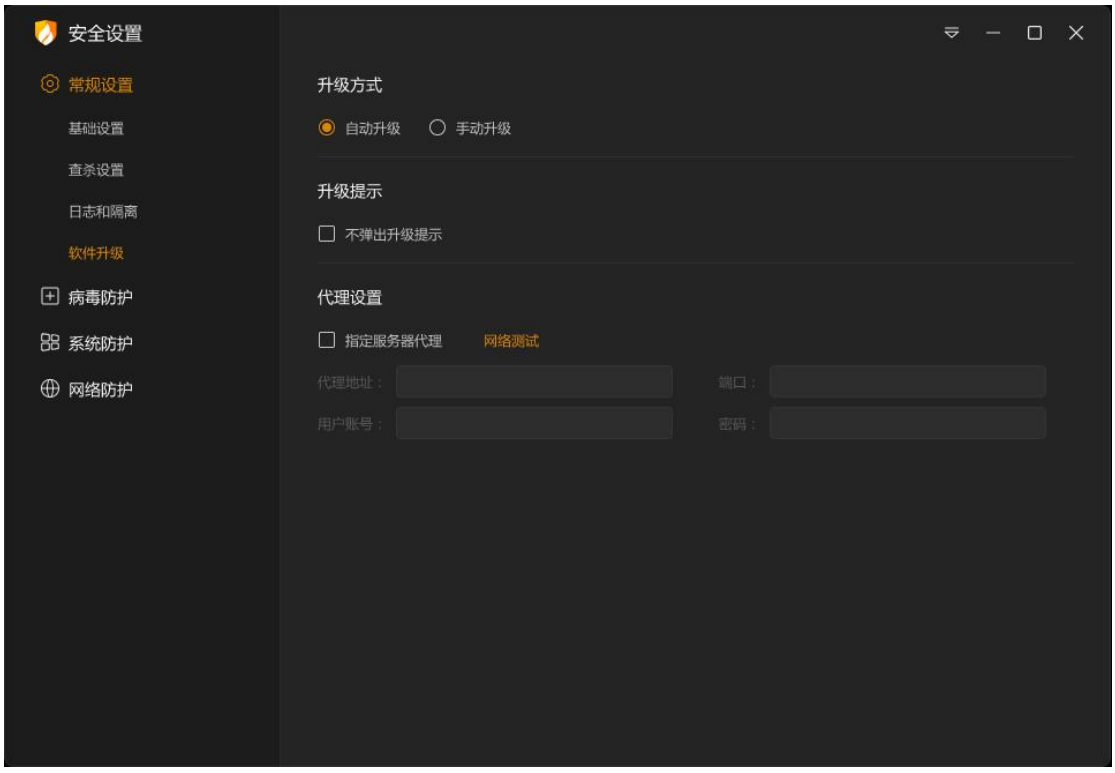
升级完成若是需要重启电脑，将弹出重启提示（见下图）。

为防止您设置手动更新后，出于各种原因，在一周内未进行病毒库更新，导致病毒库内

数据与最新数据不一致。系统将会在一周后您重启火绒或重启电脑时进行托盘消息提示。

● 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《用户操作手册》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：https://bbs.huorong.cn/

最后，再次感谢您选择火绒安全软件！