360 终端杀毒

控制中心独享版

用户手册

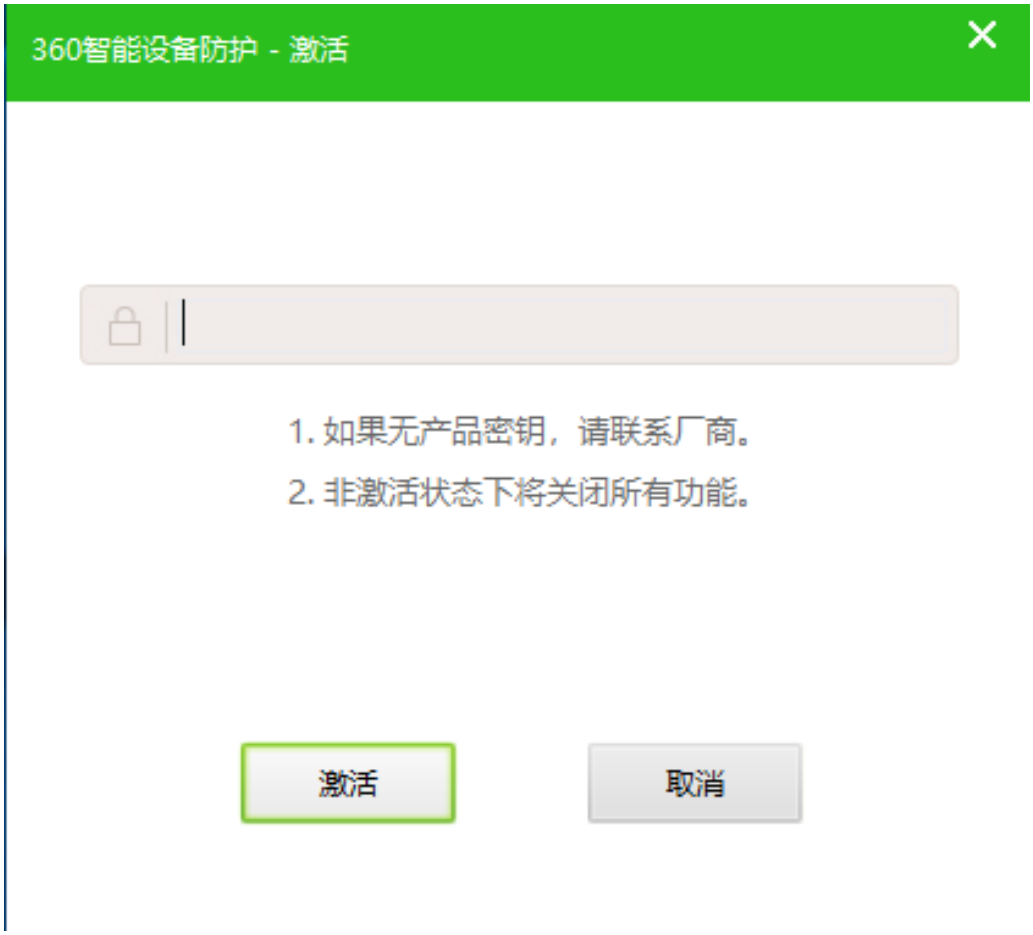
目 录 | Contents

1. 基本功能

本章介绍基本操作。

1.1 激活及设置管理密码

初次打开单机版防护时会提示输入密钥进行激活，此操作要求具备链接互联网的能力。



图：单机版防护激活界面

激活后会显示单机版防护主界面。


360智能设备防护
主菜单
设置
日志
检测更新
关于我们
退出
电脑还未进行过体检，建议立即体检
全新版本可以更全面、高效地查出影响电脑安全和性能的问题
全面体检
公告
反病毒界面入口
病毒扫描
管理员：天擎
电话：400-163-000
邮件：kefu@360.net
安全中心快捷入口
安全防护
功能大全

图：单机版防护主界面

首次进入设置界面或安全中心时会要求设置管理密码。密码要具有一定的复杂度，设置后每次进入设置界面前需输入管理密码，验证后才会打开设置界面。

2. 安全防护

本章介绍安全防护功能的使用方法。

2.1 安全防护功能介绍

随着黑客攻击手段的不断进化，新兴病毒样本成指数倍增长，传统杀毒引擎已疲于应对。单机版防护集成了强大的杀毒模块，拥有 AVE 启发式杀毒引擎、QEX 特征识别引擎、QVM 智能识别引擎、云查杀引擎，可对各种新兴变种病毒进行有效查杀与隔离。

安全防护功能包含了病毒扫描、文件实时防护、主动防御、系统修复等功能，主要由以下功能功能模块组成：

- 安全防护中心：

- 病毒查杀：
- 主界面：

2.2 典型场景的策略配置

2.2.1 强安全控制

2.2.1.1 设置退出密码和卸载密码

- **终端密码保护**
- 该模块可以设置终端卸载或者退出时要输入的密码，以防止终端用户随意的脱离控制。

图：设置客户端密码

2.3 日常运维管理

2.3.1 通过定期扫描提升内网安全

定期对内网终端进行病毒扫描，可以提高内网的安全等级。我们推荐一个星期至少进行一次快速扫描，一个月至少进行一次全盘扫描。可以设置定时杀毒任务来自动进行病毒扫描。

图：单机版防护定时杀毒设置

2.3.2 升级

单机版防护会每 3 小时到互联网检查一次病毒库与程序的版本信息。

点击主界面左上角的箭头也可手动触发即时检查。

2.3.3 处理紧急问题

2.3.3.1.1 信任区

在单机版防护“反病毒界面—信任区”中，可以对终端设备设置信任区：

图：单机版防护反病毒界面

图：单机版防护信任区

2.3.3.1.2隔离区恢复

在单机版防护“反病毒界面—恢复区”中，可以对选择终端的恢复区进行恢复：

图：单机版防护恢复区入口

2.4 安全防护设置项

2.4.1 安全防护中心

点击主界面安全防护快捷入口，认证后打开安全防护界面。

图：单机版防护安全防护中心

2.4.1.1 浏览器防护

该模块提供浏览器安全防护相关功能的开启与关闭配置。

- 网页安全防护：通过浏览器访问网页时，会自动鉴定访问的 URL，拦截挂马网站、欺诈信息、危险 Flash 等危险内容。

- 默认浏览器防护：能够锁定终端的默认使用浏览器，不被其他浏览器篡改设置。
- 邮件安全防护：

2.4.1.2 系统防护

该模块提供系统防护相关功能的开启与关闭配置。

- 网络安全防护：自动分析并拦截下载器下载木马，拦截恶意推广程序，拦截黑客远控本机，拦截盗号木马。
- 摄像头防护：防止恶意软件不经允许自动打开摄像头。
- 文件系统防护：针对文件的各种操作进行监控防护。
- 驱动防护：针对恶意驱动加载进行拦截。
- 进程防护：针对恶意进程创建、进程操作等行为进行拦截。
- 注册表防护：针对注册表的操作进行监控防护。

2.4.1.3 入口防护

该模块提供入口防护相关功能的开启与关闭配置。

- 下载安全防护：对 U 盘等移动设备和电脑硬盘间文件传输、共享文件传输进行严格检测。
- U 盘安全防护：对插入的 U 盘设备进行检测扫描，并提示相关信息。
- 黑客入侵防护：
- 局域网防护：

2.4.1.4 核晶防护引擎

核晶引擎是利用 Intel / AMD CPU 硬件虚拟化技术(Vanderpool Technology，简称 VT 技术)做的客户端防护引擎，主要用于实现 64 位操作系统上的主动防御功能。

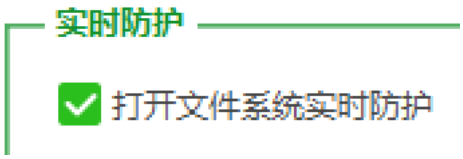
如果关闭核晶防护引擎，64 位操作系统上的主动防御功能将失效。

2.4.1.5 实时防护

该模块提供终端实时防护相关功能的配置，包括：是否打开文件系统实时防护，并可设置防护级别；监控的文件类型选择；实时防护时检测到病毒的处理方式；其他防护选项，如启用敲诈者木马防护功能和监控压缩包文件等。

- 实时防护开关

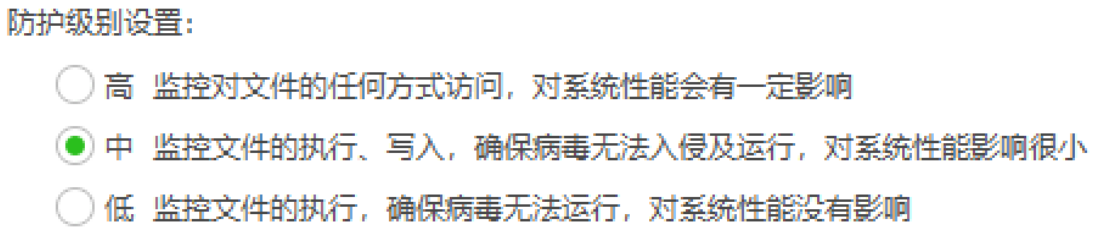
实时防护功能的总开关。除非明确知道不能开启实时防护，推荐针对所有操作系统打开实时防护功能，大大提升系统安全防护等级。



- 防护级别设置

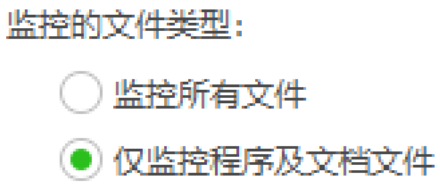
实时防护功能有 3 个安全级别：高级别会监控所有类型的文件访问操作，对系统性能有一定影响；中级别会监控文件执行及写入，确保病毒无法侵入及运行，对系统性能影响很小；低级别只监控文件执行，对系统性能没有影响。

普通场景推荐选择中防护级别，可以在安全性和系统性能影响之间达到比较好的平衡；对安全性要求特别高的场景，可以选择高防护级别；系统性能特别差，文件操作特别频繁的场景，可以选择低防护级别。



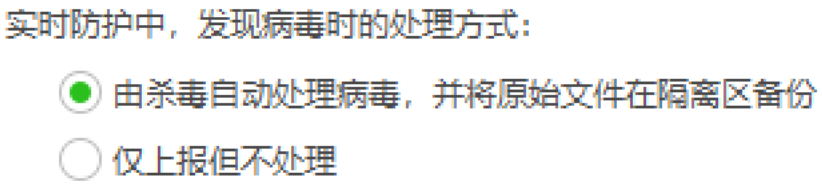
- 监控的文件类型

如果设置为“仅监控程序及文档文件”，只会监控可执行文件和常用文档类型的文件。



- 病毒处理方式

用来设置实时防护功能发现病毒后的处理方式，分为自动处理和仅上报日志。



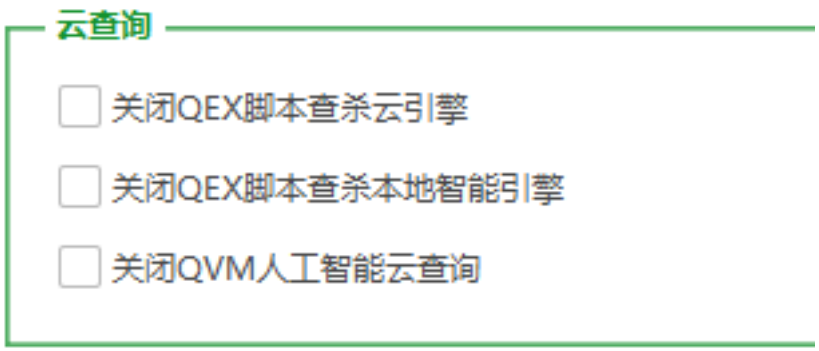
2.4.2 多引擎设置

该模块用来设置在“安全防护”“实时防护”两种模式下的查杀引擎，默认开启了云查杀引擎、启发式引擎、QEX 脚本查杀引擎。

2.4.3 云查杀设置

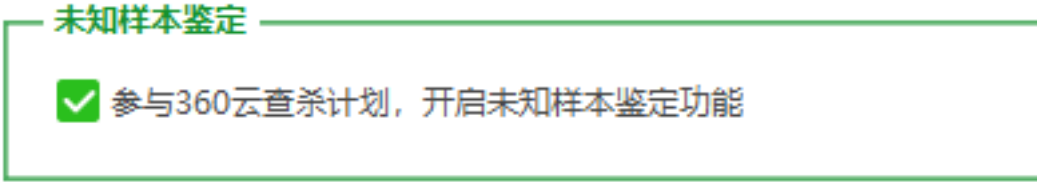
2.4.3.1 云查询

该模块可配置是否关闭 QVM 人工智能云查询、QEX 脚本查杀云引擎及 QEX 脚本查杀本地引擎，建议在可以连接互联网的环境下开启 QVM 人工智能云查询、QEX 脚本查杀云引擎及关闭 QEX 脚本查杀本地智能引擎，可增强对新型变种病毒的查杀能力。



2.4.3.2 未知样本鉴定

该模块可以设置是否开启未知样本鉴定功能。



2.4.4 云修复设置

在终端系统文件遭破坏或被感染时，扫描发现后能触发修复动作，可以通过云端把好的系统文件下载下来，并完成替换工作。

2.4.5 安全体检

可以通过点击主界面“全面体检”启动，体检内容包括检测系统启动项、内存是否存在病毒以及有风险的文件，检测相应的安全防护是否开启，是否存在系统故障，以及是否存在系统垃圾以及可以优化的启动项。

2.4.6 全盘扫描

该功能会对所选择的终端下发全盘扫描任务，扫描所有目录下的相关文件。

2.4.7 快速扫描

该功能会对所选择的终端下发快速扫描任务，扫描“系统启动项”“系统关键目录”下的相关文件。