



安全中心 V1.1

软件用户手册

KYJ S-KS-SC-1.1-SUM-V1.1



股票代码: 688152

变更记录

版本	修订时间	修订人	修订类型	修订章节	修订内容
V1.0	2026.4.1	潘虎春	A	ALL	ALL
V1.1	2026.5.21	潘虎春	M	封面、页眉、 章节 4	封面、页眉替 换新 Logo, 章节 4 替换 图片

注 1：修订类型分为 A-ADDED，M-MODIFIED，D-DELETED

注 2：对该文件内容增加、删除或修改均需填写此记录，详细记载变更信息，以保证其可追溯性

目 录

1 范围	1
1.1 标识	1
1.2 软件概述	1
1.3 文档概述	1
2 软件综述	1
2.1 操作系统版本及硬件配置	1
2.2 软件安装	1
3 帮助和问题报告	2
4 软件功能	2
4.1 设置	2
4.1.1 设置	2
4.1.2 帮助	3
4.1.3 关于	3
4.1.4 日志	4
4.2 基线加固	4
4.2.1 快速扫描	4
4.2.2 开始加固	5
4.2.3 生成报表	6
4.3 可信保护	7
4.3.1 执行文件保护	7
4.3.2 内核模块保护	9
4.3.3 文件保护	11
4.4 账户安全	13
4.4.1 三权分立	13
4.4.2 密码策略	14
4.4.3 登录失败锁定	15
4.5 漏洞修复	16

4.5.1 漏洞扫描	16
4.5.2 漏洞修复	17
4.6 进程保护	17
4.6.1 进程保护	17
4.7 外设管控	18
4.7.1 设备管理	18
4.7.2 接口管理	19
4.8 安装管理	21
4.8.1 安装管理	21
4.9 私密保险箱	21
4.9.1 创建保险箱	21
4.9.2 解锁	23
4.9.3 修改密码	24
4.9.4 删除	25
4.9.5 找回密码	25
5 FAQ	26

1 范围

1.1 标识

标识号：KYJ S-KS-SC-1.1-SUM-V1.1；

标题：安全中心 V1.1；

软件名称：KS-SC；

软件版本号：V1.1。

1.2 软件概述

将麒麟信安操作系统 V6 的安全功能进行产品化，开发一款图形界面安全中心组件，用于安全模块相关功能的控制、配置和展示，增强安全模块功能在麒麟信安操作系统上使用的灵活性和便捷性。

1.3 文档概述

本文档是安全中心 V1.1 用户手册，它包含以下内容：

安全中心 V1.1 概述；

安全中心 V1.1 使用指南。

2 软件综述

2.1 操作系统版本及硬件配置

请确定操作系统版本、硬件配置满足主机安全中心 V1 的运行要求。

表 2-2 系统要求

内容	参数
ISO	KylinSec-Server-V6 x86_64/aarch64/loongarch 架构
安装系统的设备	服务器/台式机/虚拟机
磁盘空间	50GB 及以上剩余空间
CPU	2 核 2.5GHz 及以上（2 核及以上）
内存	2GB 及以上

2.2 软件安装

表 2-1 软件清单

序号	软件
1	kss-xxx.rpm
2	ks-sc-1.1.x-xxx.rpm

安装步骤说明：

安装 V6 系统。

使用 `rpm -e kss ks-sc --nodeps` 卸载系统自带可信和安全管控软件。

配置 V6-SP1 系统的软件源。

使用 `yum install kernel` 安装内核(版本不低于 6.6.0-113.0.0.119.ks6.kb7)，重启系统进入新内核。

使用 `yum install ks-sc` 安装安全中心软件，重启系统。

3 帮助和问题报告

如果您有任何疑问，都可以通过以下方式获得帮助：

求助在线帮助：<https://www.kylinsec.com.cn>；

热线：400-012-6606；

扫描下方二维码，反馈相关问题；



4 软件功能

4.1 设置

4.1.1 设置

点击右上角，点击【设置】

打开【设置】界面，打开【可信保护】开关，可信数据开始初始化，等待一段时间后重启机器，后续可使用可信保护功能模块。

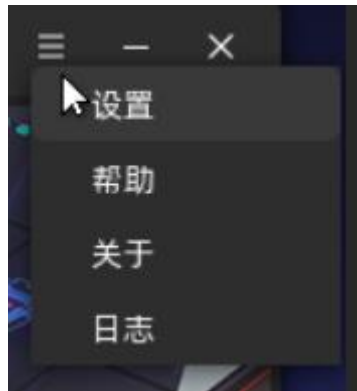


图 1 设置列表



图 2 设置窗口

4.1.2 帮助

点击右上角, 点击【帮助】可打开用户手册。

4.1.3 关于

点击右上角, 点击【关于】弹出软件版本信息。



图 3 关于窗口

4.1.4 日志

点击右上角，点击【日志】弹出安全中心软件相关所有操作日志。

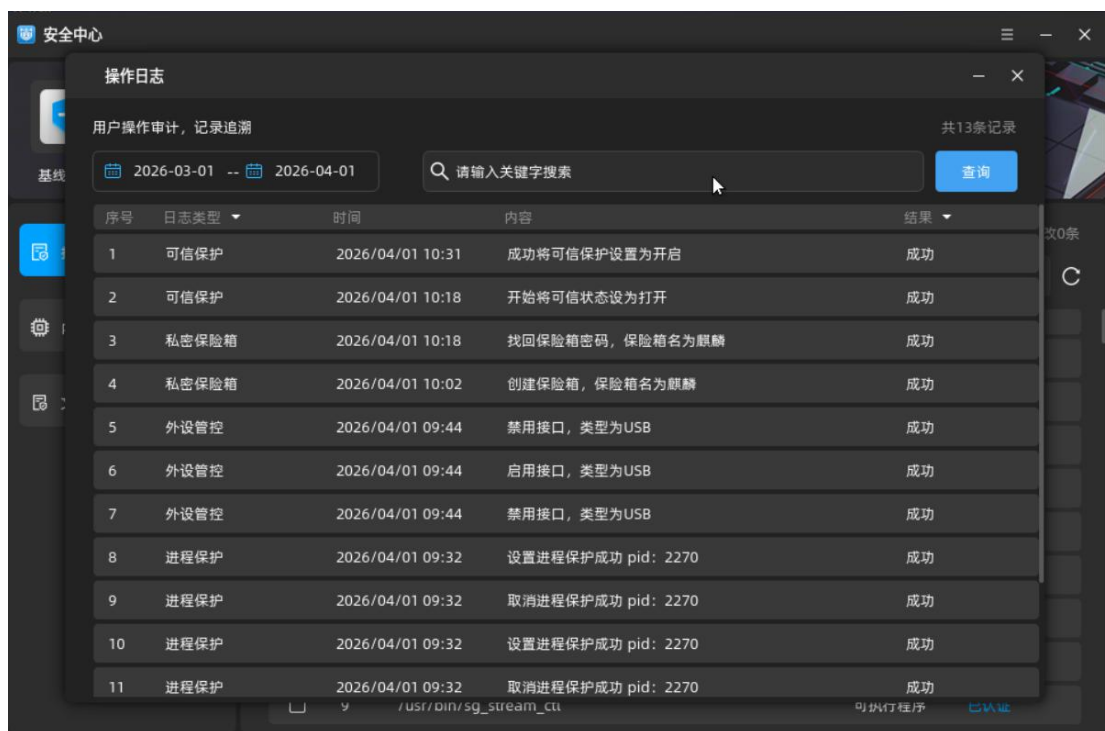


图 4 操作日志窗口

4.2 基线加固

基线加固功能提供系统安全配置的检测与修复能力。

扫描主要是为了对比加固项配置是否与系统标准一致。

加固前必须先进行一次扫描，扫描前可以选择策略。若加固项配置与系统标准一致时，扫描结果显示为“符合”，加固项配置与系统标准不一致时，扫描结果显示为“不符合”。

4.2.1 快速扫描

点击【快速扫描】勾选需要扫描的加固项，点击【开始扫描】：扫描完成，进度为100%，扫描开始时间和用时正确，各个加固项的状态为“符合”或“不符合”



图 5 基线加固

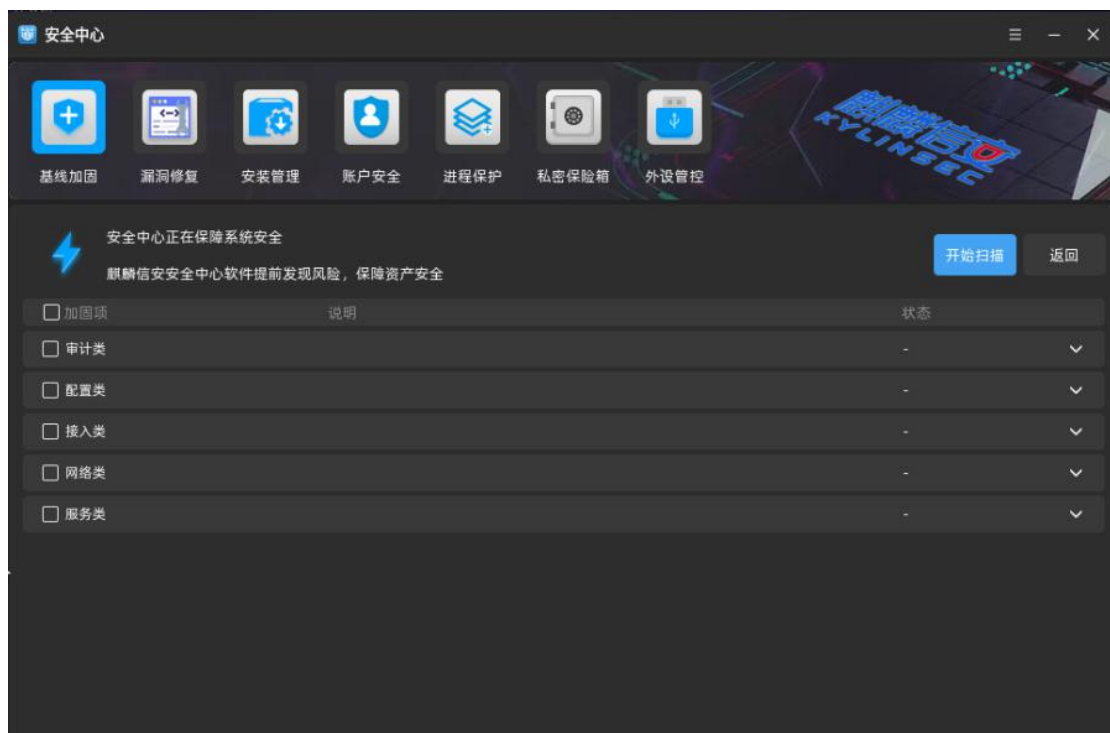


图 6 快速扫描

4.2.2 开始加固

快速扫描后点击【加固】会对所有加固项按照系统标准进行加固。



图 7 加固

4.2.3 生成报表

点击【生成报表】，生成报表的文件名称格式为“安全中心加固报告-主机名-主机 IP-时间戳”。



图 8 生成报表



图 9 生成报表文件位置

4.3可信保护

4.3.1 执行文件保护

- 1) 点击【可信保护】侧边栏中的【执行文件保护】
- 2) 点击【添加】选择文件
- 3) 点击【打开】，文件添加至白名单列表，对可执行文件进行防篡改保护

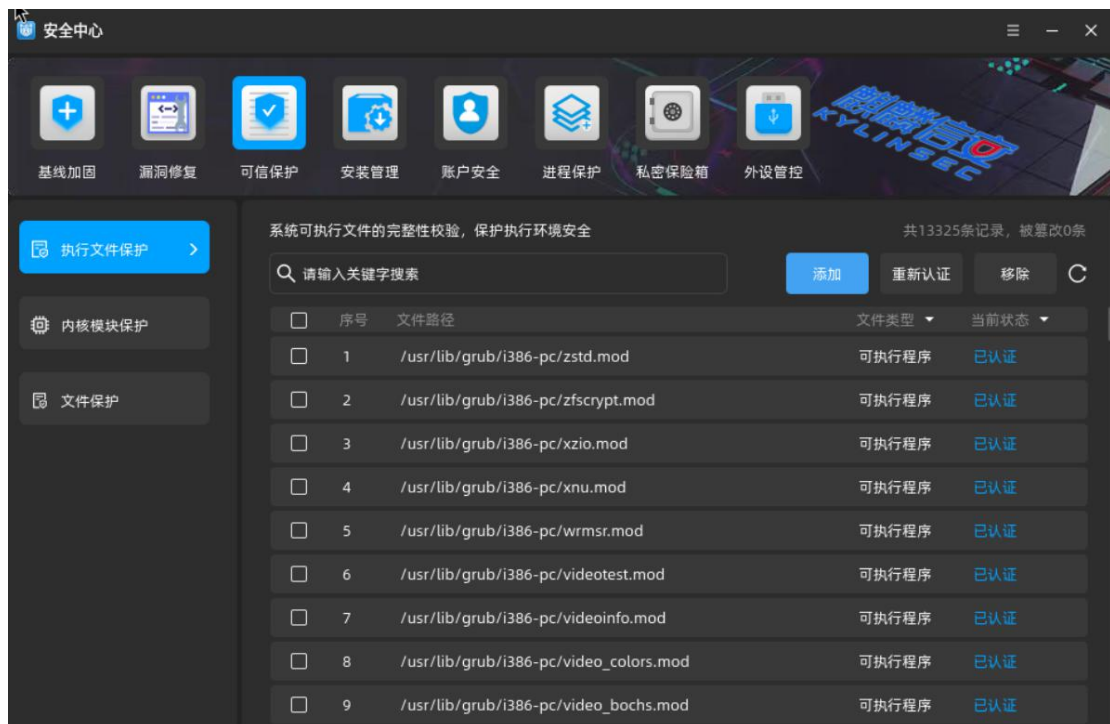


图 10 执行文件保护

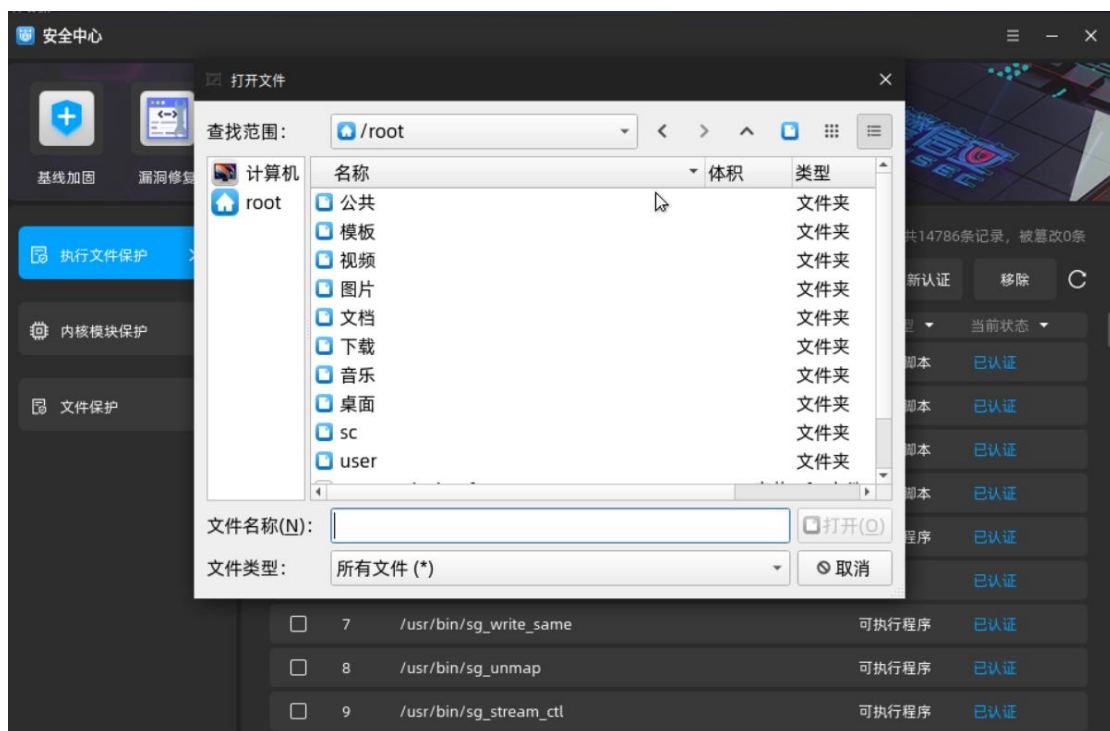


图 11 执行文件保护-添加文件

执行文件保护列表中文件编辑后无法执行且列表中会标注文件已被篡改

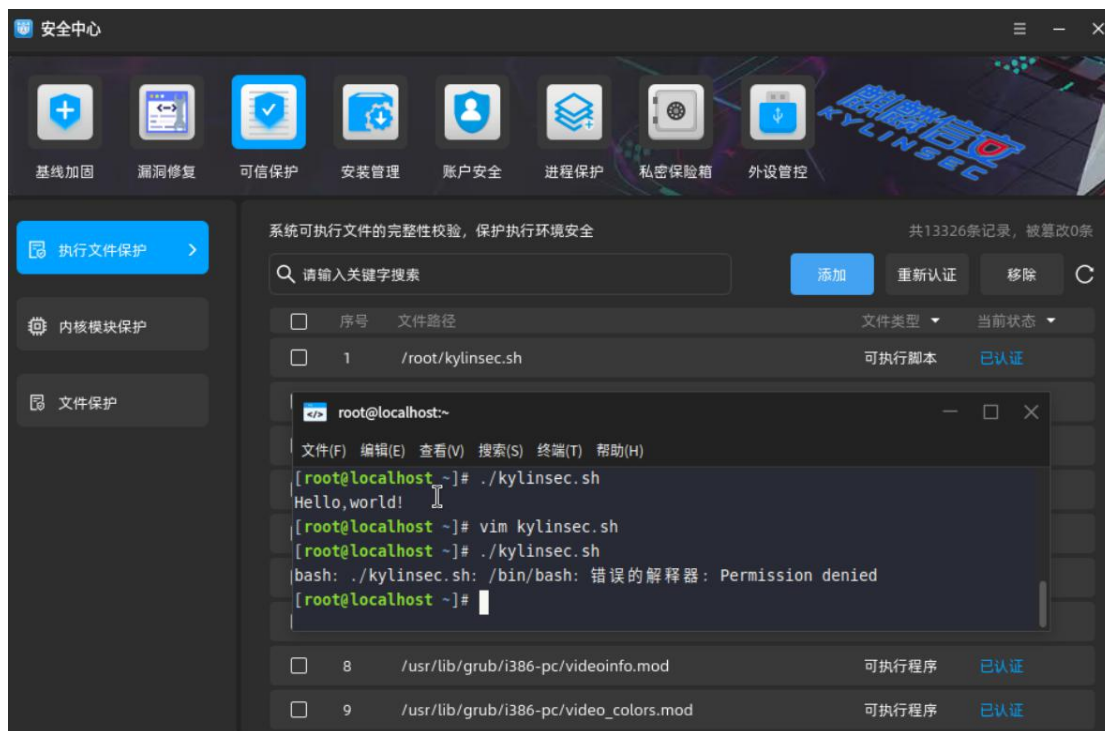


图 12 编辑执行文件

4.3.2 内核模块保护

- 1) 点击【可信保护】侧边栏中的【内核模块保护】
- 2) 点击【添加】选择文件
- 3) 点击【打开】，文件添加至白名单列表
- 4) 选择需要保护的文件，打开右侧的【防卸载】开关，所选择的文件受到保护，该文件的内核驱动模块无法卸载。

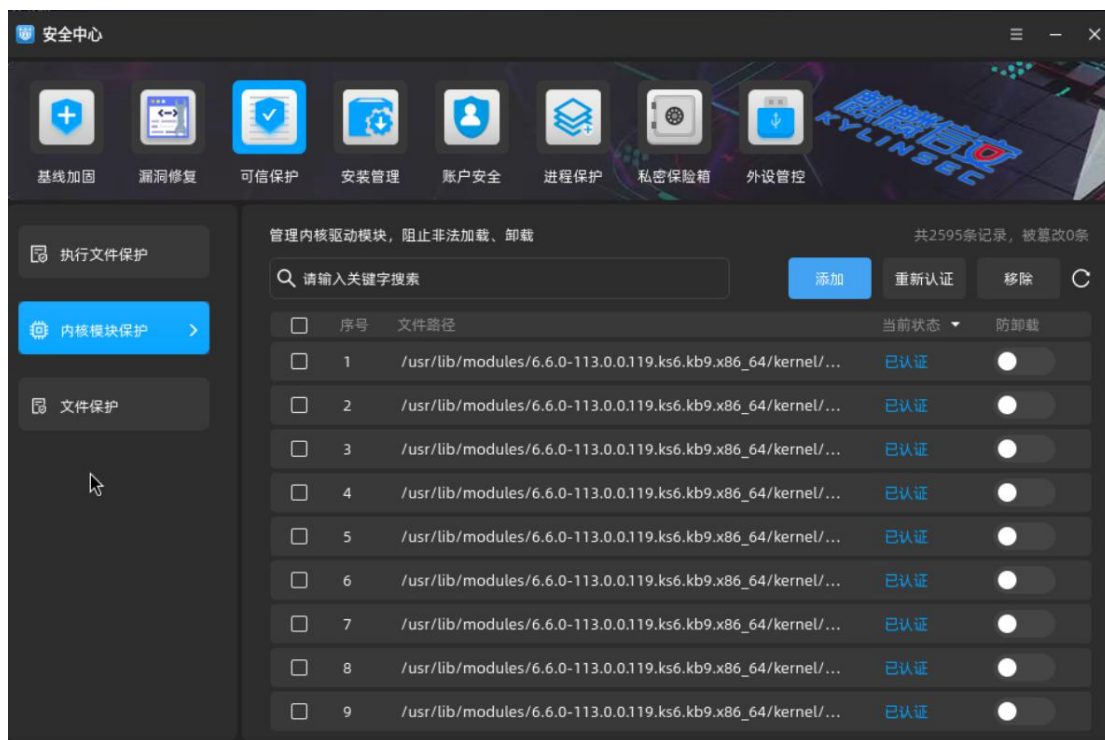


图 13 内核模块保护

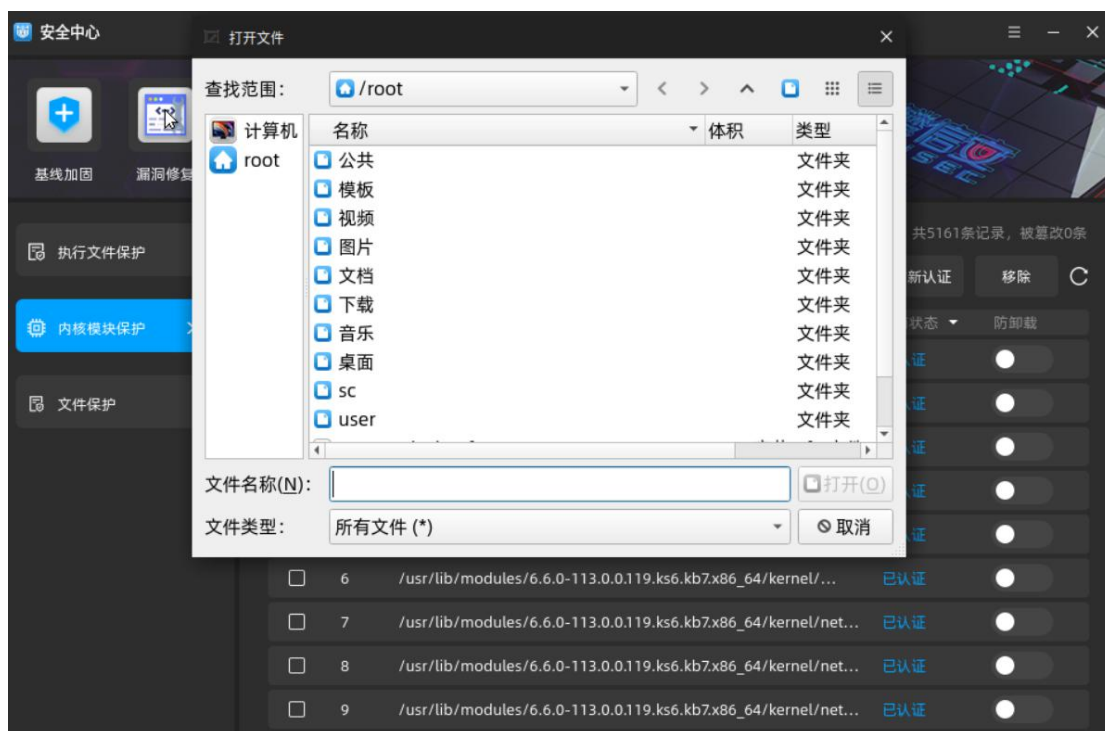


图 14 内核模块保护-添加文件

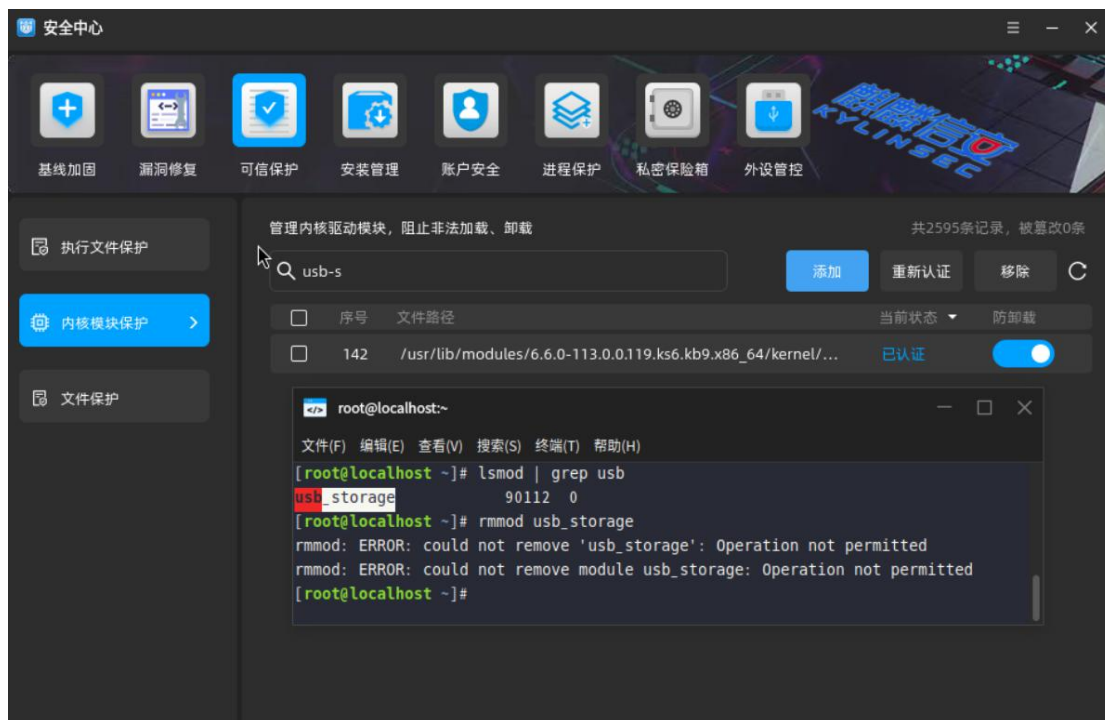


图 15 无法卸载已开启防卸载的模块

4.3.3 文件保护

- 1) 点击【可信保护】侧边栏中的【文件保护】
- 2) 点击【添加】选择文件
- 3) 点击【打开】，文件添加至白名单列表，添加到列表的文件，不允许篡改和删除

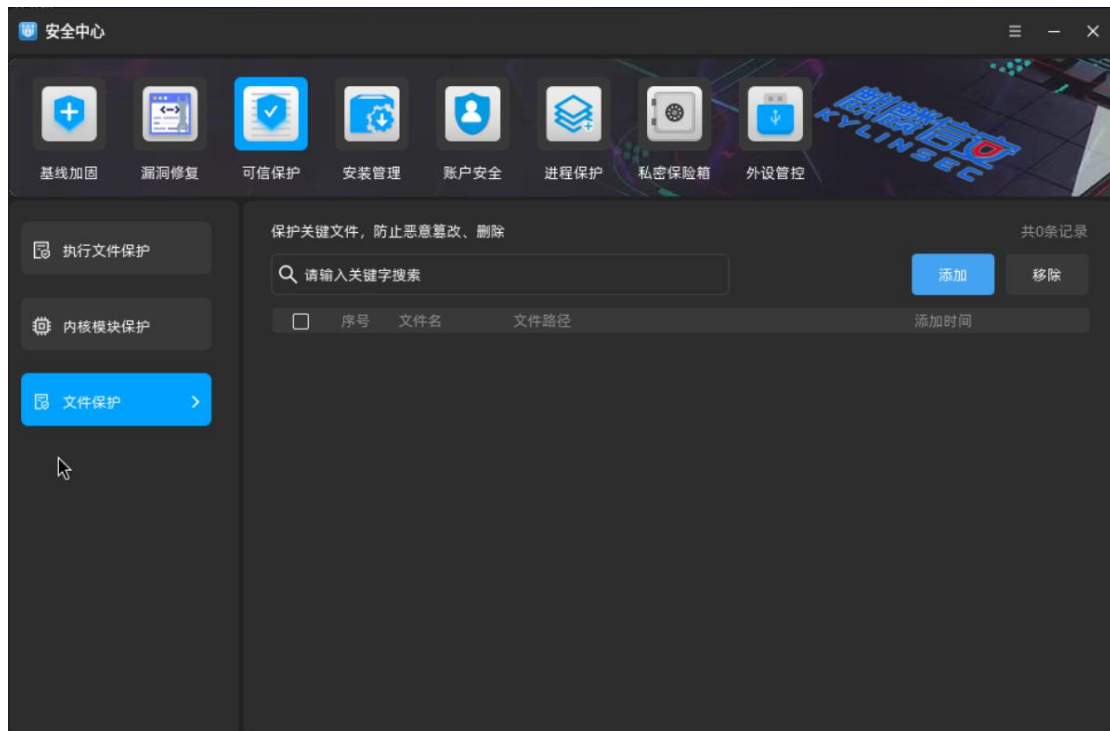


图 16 文件保护

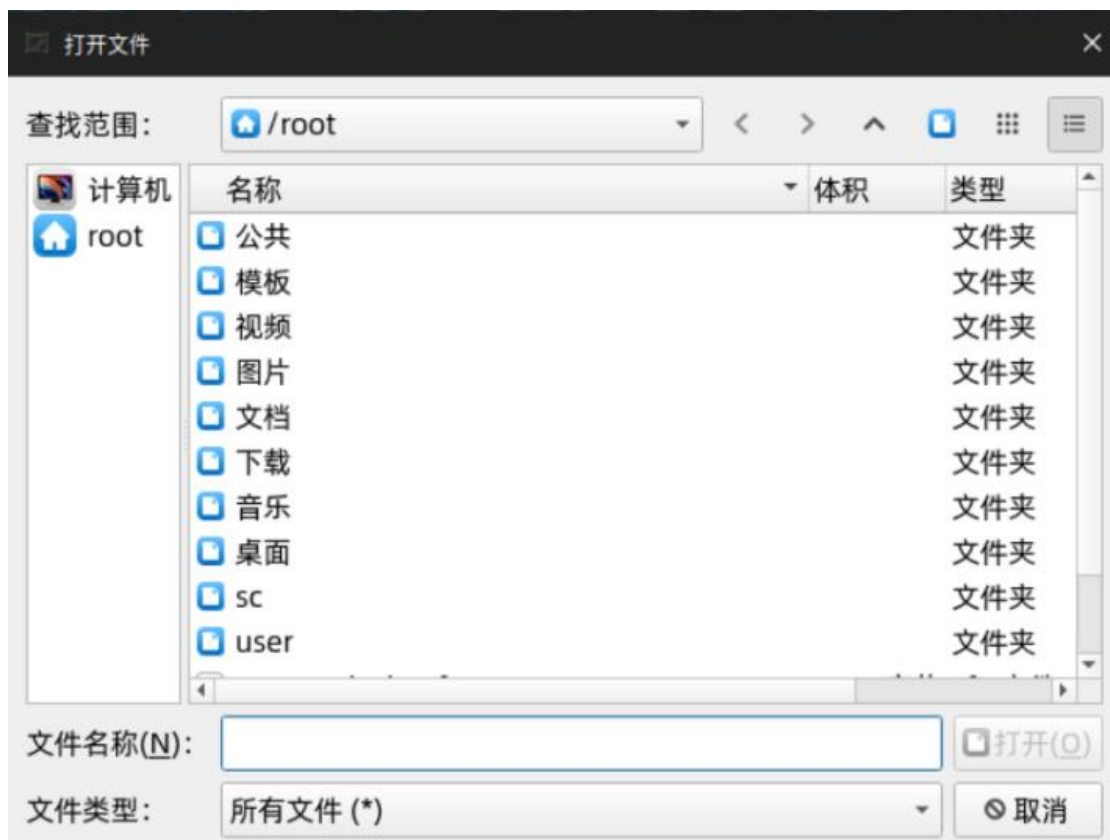


图 17 文件保护-添加文件

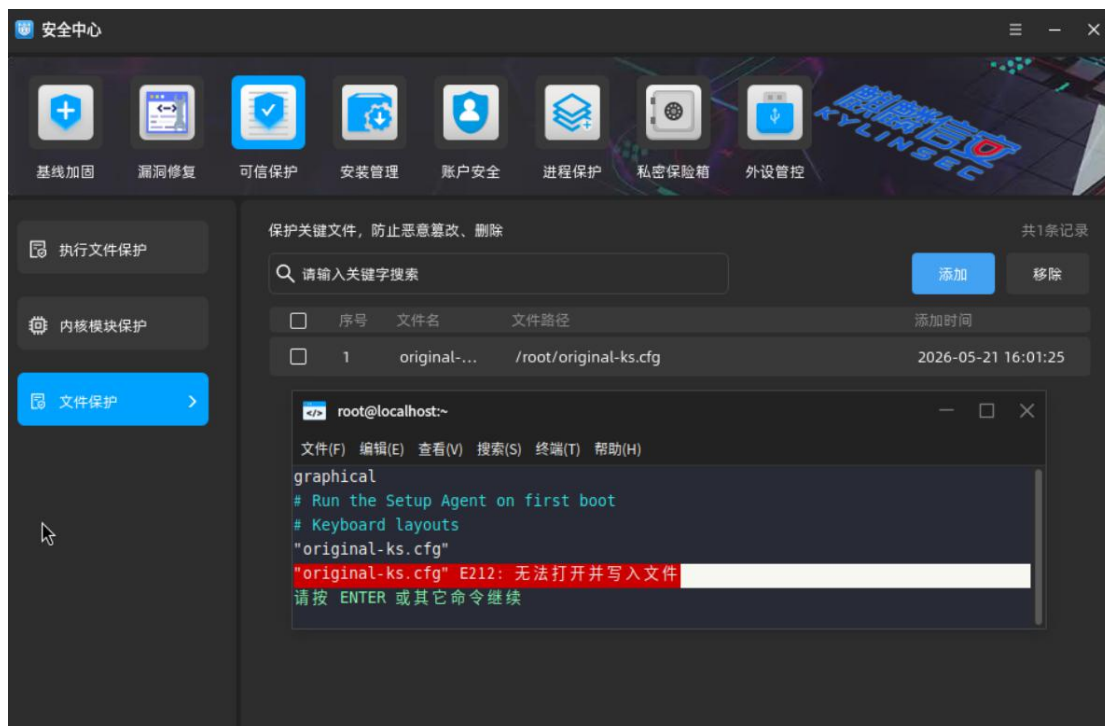


图 18 无法编辑文件保护列表中的文件

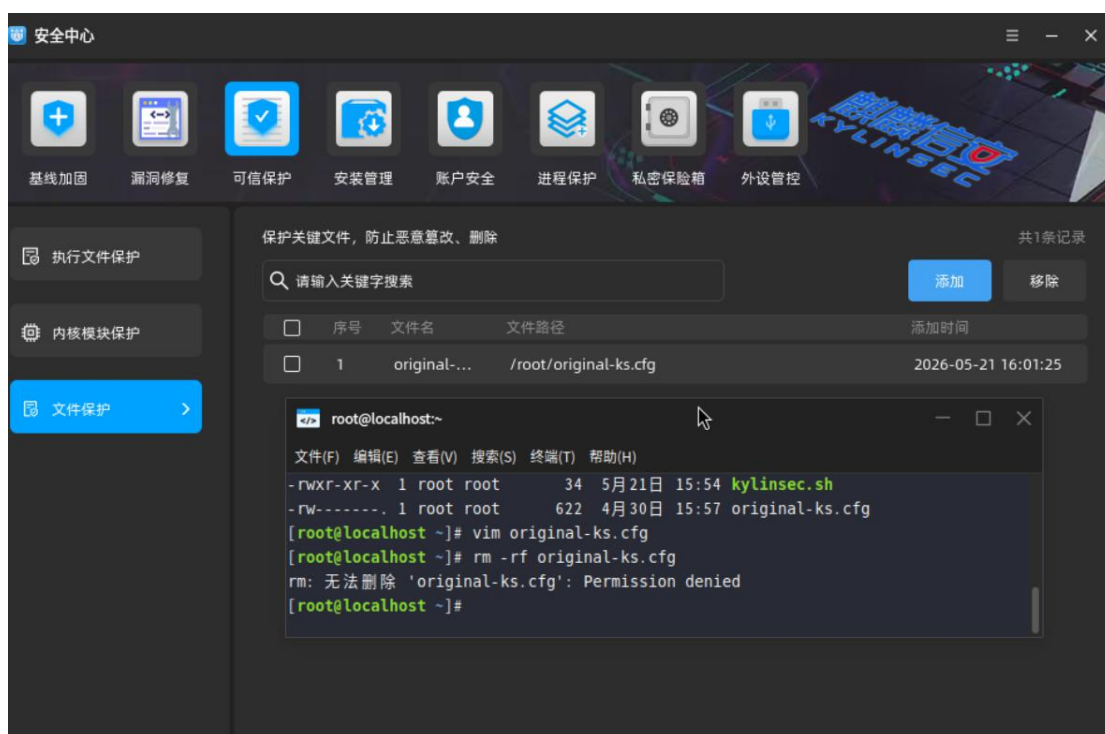


图 19 无法删除文件保护列表中的文件

4.4 账户安全

4.4.1 三权分立

- 1) 点击【账户安全】侧边栏中的【三权分立】

2) 开启【三权管理员开关】控制，如安装系统已选三权，则默认开启；如无三权管理员，开启开关则创建三权用户，需要手动设置三权管理员密码



图 20 三权分立

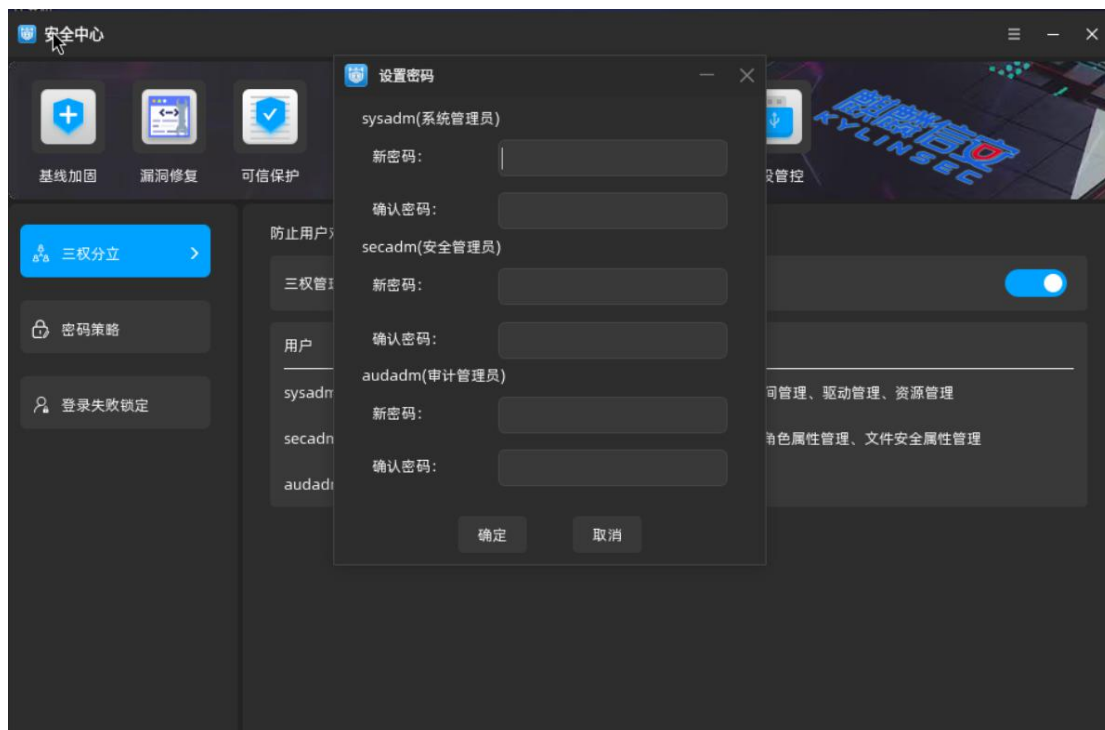


图 21 创建三权用户

4.4.2 密码策略

1) 点击【账户安全】侧边栏中的【密码策略】。

2) 打开【密码强度要求】开关，相关配置全部展示。配置如下：【密码强度要求、密码最小长度、密码至少包含字符类型数量、密码有效期、修改密码的最小间隔天数、密码到期提醒、密码加密



图 22 密码策略

4.4.3 登录失败锁定

- 1) 点击【账户安全】侧边栏中的【登录失败锁定】。
- 2) 打开【登录失败锁定】开关，相关配置全部展示。配置如下：密码错误次数、锁定后自动解锁时间、是否包含 root 用户



图 23 登录失败锁定

4.5漏洞修复

4.5.1 漏洞扫描

选择【漏洞修复】，点击【开始扫描】，扫描中会有扫描进度条、漏洞信息展示，扫描过程中也可以点击【取消】停止扫描。



图 24 漏洞扫描

4.5.2 漏洞修复

扫描后，漏洞列表显示扫描结果，勾选全部漏洞，点击【一键修复】，修复中会有扫描进度条、修复漏洞信息展示，扫描过程中也可以点击【取消】停止修复。



图 25 漏洞修复

4.6 进程保护

4.6.1 进程保护

点击【进程保护】，列表展示当前系统所有进程，列表字段包括序号、进程号、进程名称、进程路径、进程参数，可悬浮查看详细信息。每个进程提供放杀死保护开关，开启开关后该进程无法被杀死。在进程列表中或者通过搜索找到需要保护的进程，打开进程保护开关。

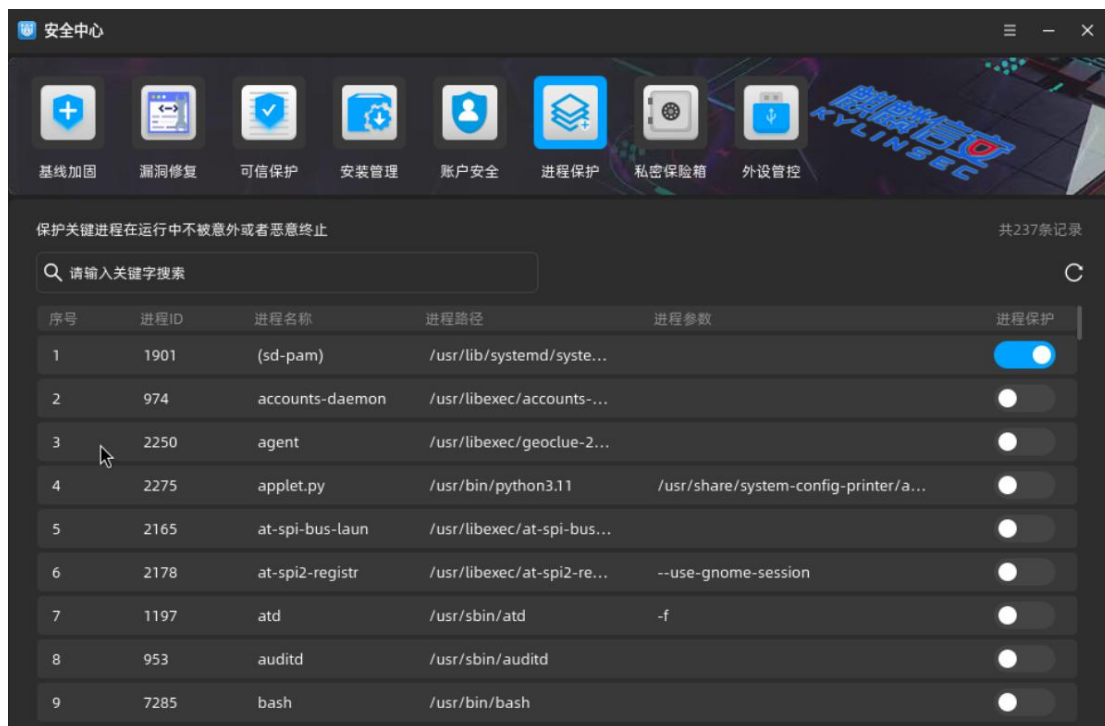


图 26 进程保护

4.7 外设管控

4.7.1 设备管理

- 1) 点击【外设管控】侧边栏中的【设备管理】。
- 2) 设备默认不管控，设备接入之后为启用状态，如需管控可将设备设置为禁用，设备状态仅包括启用和禁用状态。
- 3) 点击需要修改状态的设备【操作】一栏的【编辑】，状态为禁用的设备在操作系统无法正常使用。



图 27 设备管理

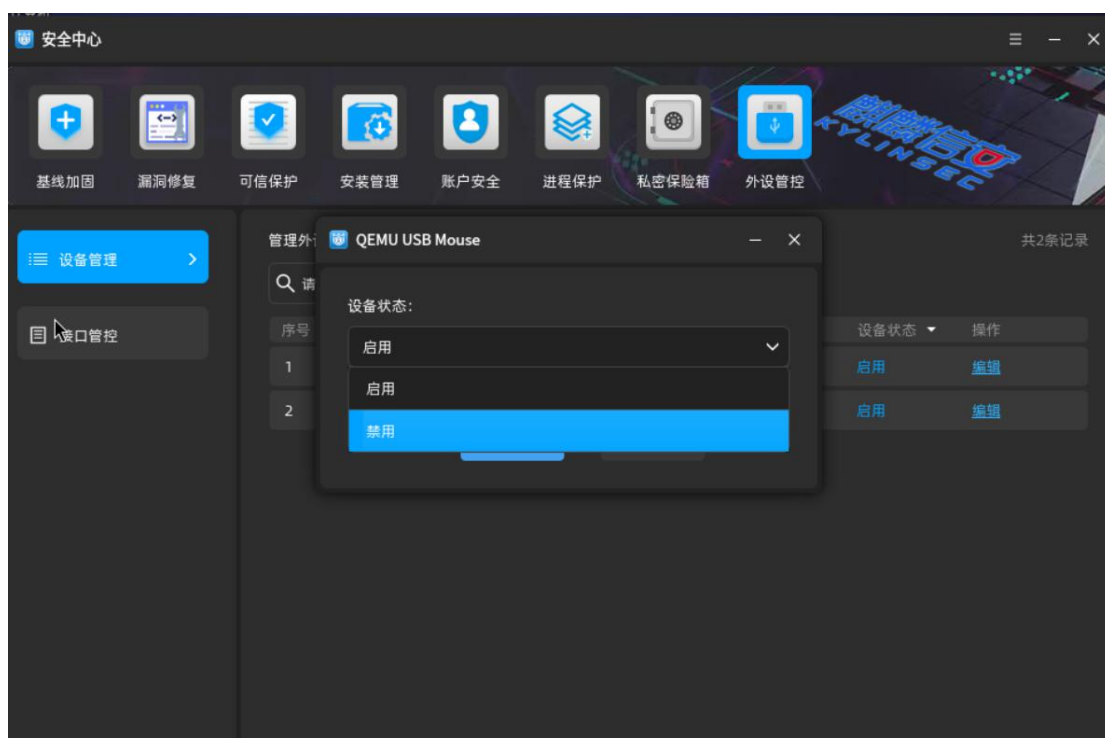


图 28 编辑设备状态

4.7.2 接口管理

- 1) 点击【外设管控】侧边栏中的【接口管控】。
- 2) 接口默认不管控，所有接口管控开关为关闭状态，如需管控可将接口管

控开关置为打开状态。

3) 打开各类别接口管控旁开关即可对该接口进行控制。

4) 开启【USB 接口管控】后，会额外显示【键盘接口管控】和【鼠标接口管控】两个开关来控制键鼠的接入。

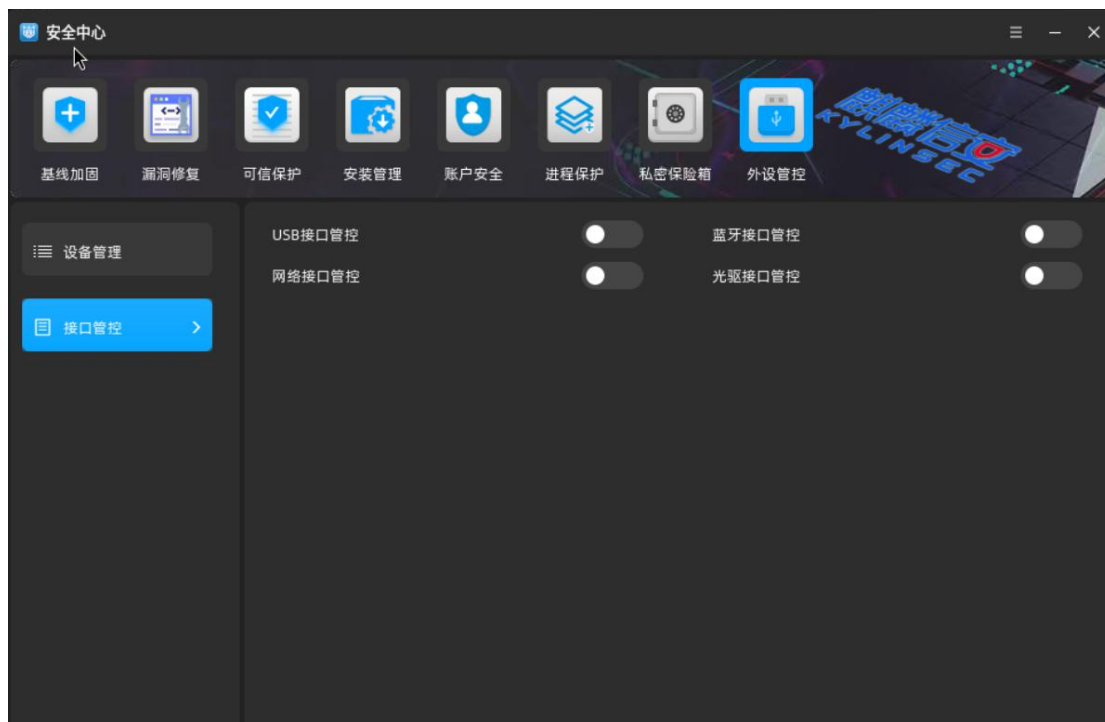


图 29 接口管控



图 30 开启 usb 接口管控

4.8 安装管理

4.8.1 安装管理

1) 点击【安装管理】，打开【软件包签名检测】开关，系统将对所有途径下的软件包进行签名检测，签名不合法的安装包无法安装，只有通过签名校验的软件包才能安装，默认不开启。

2) 支持软件源启停管理，打开【仓库源】中各仓库信息后的【仓库启停】开关，系统可正常使用对应的仓库源下载。

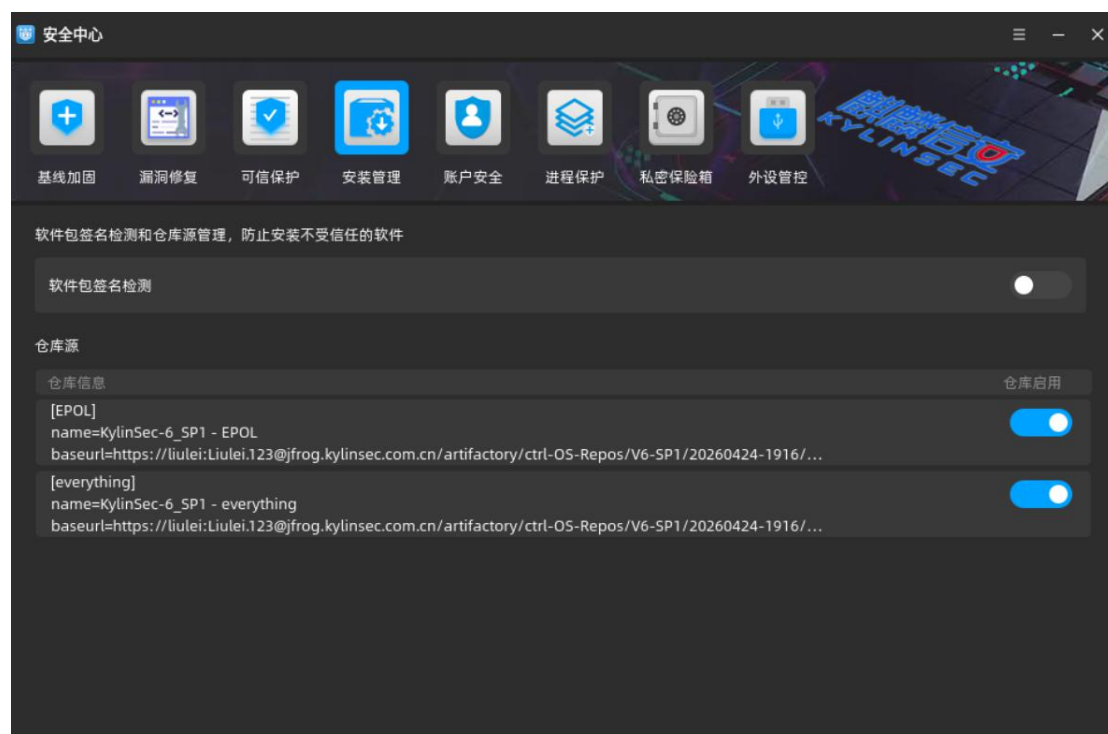


图 31 安装管理

4.9 私密保险箱

4.9.1 创建保险箱

- 1) 点击【私密保险箱】
- 2) 界面点击【新建】打开【创建保险箱】窗口
- 3) 输入名称、密码和确认密码即可创建保险箱

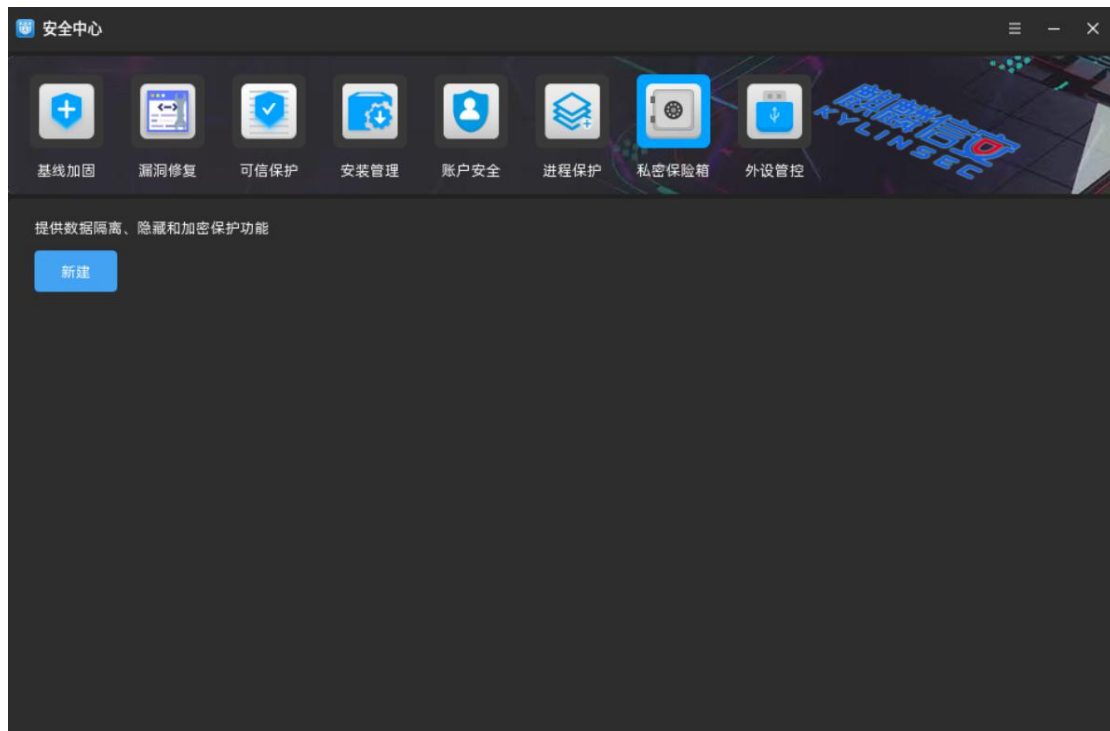


图 32 私密保险箱

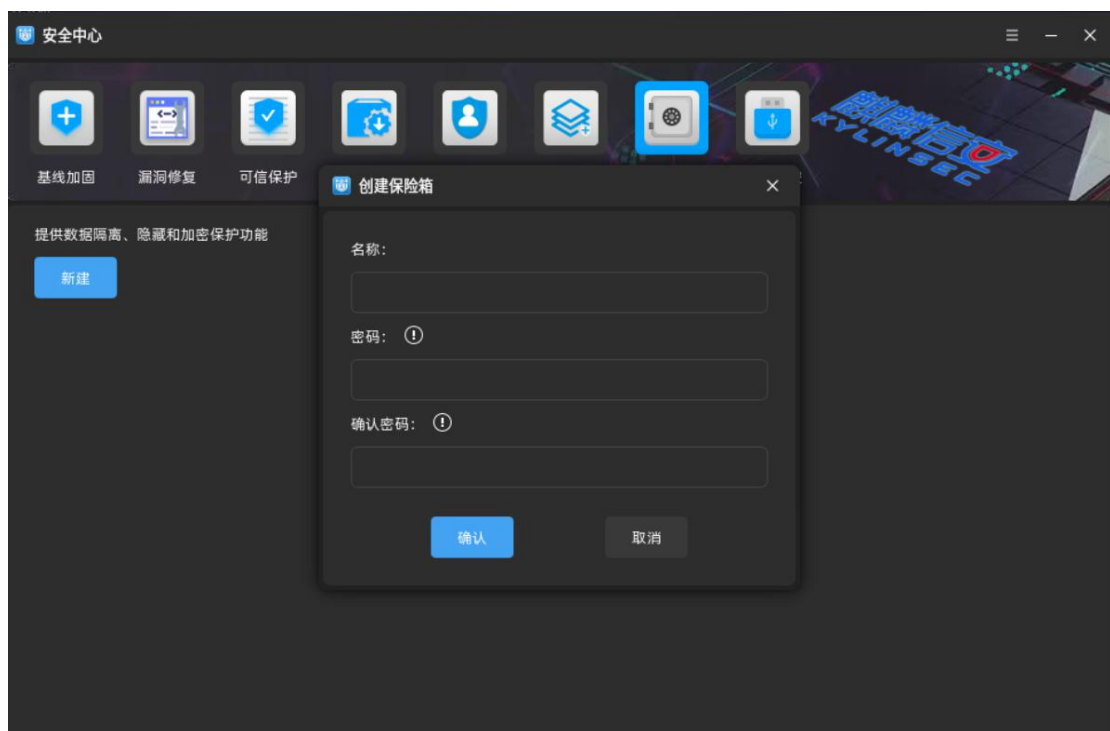


图 33 创建保险箱

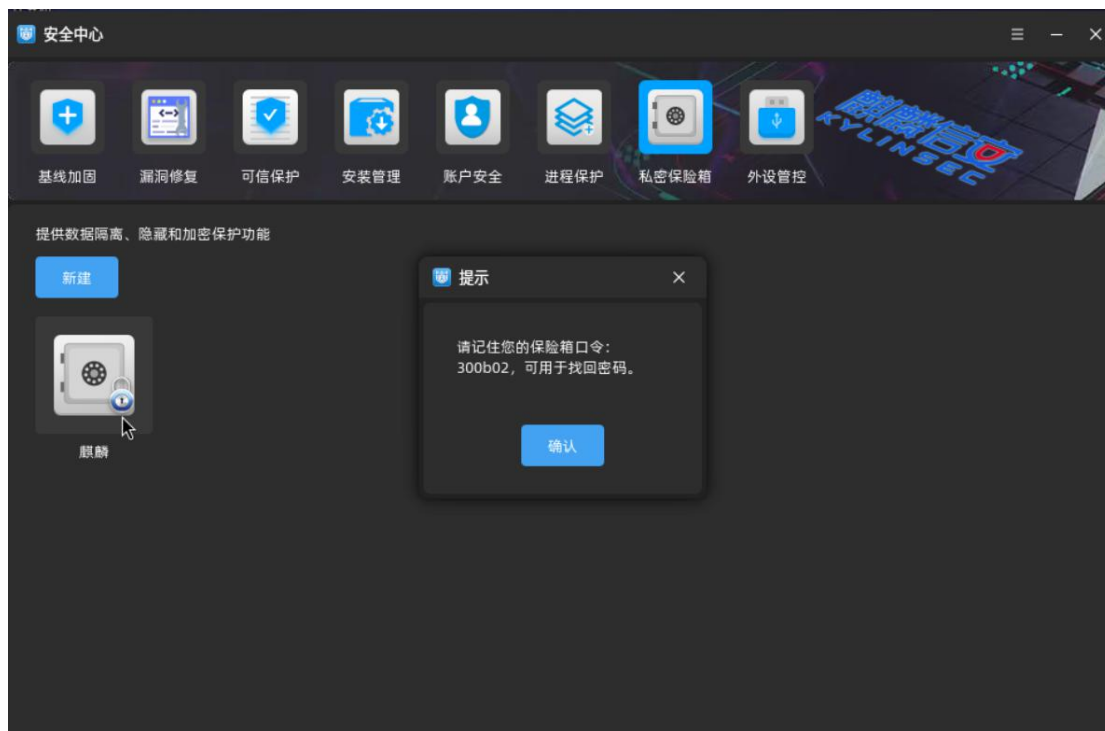


图 34 保险箱口令

4.9.2 解锁

选择需要解锁的保险箱点击鼠标右键，选择【解锁】。

弹出【解锁】窗口，输入解锁密码可解锁并使用保险箱。

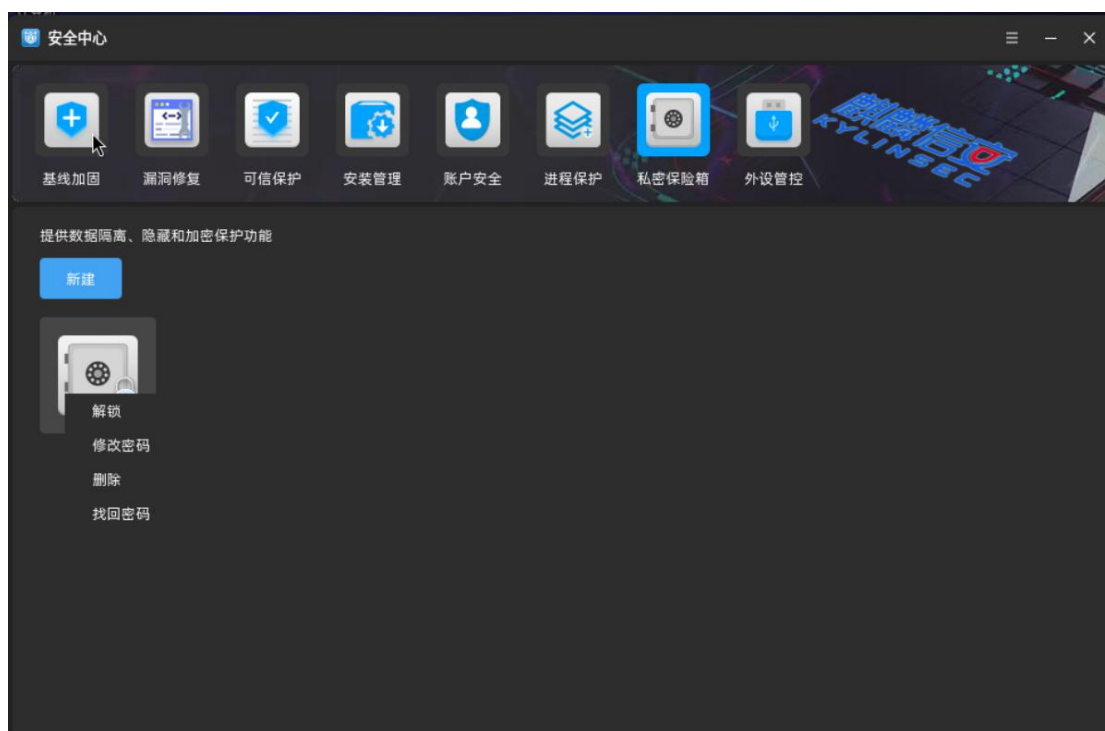


图 35 保险箱右键功能



图 36 解锁保险箱

4.9.3 修改密码

选择需要修改密码的保险箱点击鼠标右键，选择【修改密码】。

弹出【修改密码】窗口，输入正确的当前密码、新密码和确认密码，保险箱密码修改为新密码。



图 37 修改保险箱密码

4.9.4 删除

选择需要删除的保险箱点击鼠标右键，选择【删除】。

弹出【删除保险箱】窗口，输入正确的密码，可成功删除保险箱。



图 38 删除保险箱

4.9.5 找回密码

选择需要找回密码的保险箱点击鼠标右键，选择【找回密码】。

弹出【找回密码】窗口，输入创建保险箱时给出的保险箱口令，可成功找回保险箱密码。



图 39 找回保险箱密码

5 FAQ

问：三权用户开启的操作系统，安全中心关闭三权用户后重启再打开三权，重启后系统在标签阶段循环。

答：操作系统安全机制原因，无法从 disabled 直接转换到 enforcing 状态，需要中间转换成 permissive 过度。