KYLINSOFT
麒麟软件

麒麟安全管理工具

帮助手册

麒麟软件有限公司

2020 年 10 月

目录

第一章 麒麟安全管理工具

1.1. 概述

麒麟安全管理工具是一款系统安全防护工具，界面简洁，旨在为用户提供快捷、便利的系统安全防护体验。

安全管理工具是基于麒麟系统安全机制实现保护系统应用程序和文件的完整性，确保系统运行环境的安全可靠。该机制支持对应用程序的执行权限控制，对系统文件的防篡改保护，对内核驱动模块的防卸载保护。同时，麒麟系统安全机制分为“强制模式”、“警告模式”和“记录模式”三种运行模式，在不同的应用场景下，以不同粒度的保护机制，维护用户系统运行环境的安全。

麒麟安全管理工具位置：开始菜单 > 所有程序 > 麒麟安全管理工具。软件打开后，如下图所示：

图 1-1 麒麟安全管理工具

1.2. Kysec 安全模式设置

麒麟系统的 KYSEC 安全机制分为“强制模式”、“警告模式”“记录模式”三种运行模式。

当处于“强制模式”时，系统自动阻止没有安全认证的程序、动态库的执行，

阻止用户篡改、删除、覆盖或重命名受保护文件，阻止用户加载未授信的内核驱动模块；

当处于“警告模式时”，系统会发出警告提醒用户是否执行相应的操作，会根据用户的选择决定是否执行。

“记录模式”模式也叫做“维护模式”，在该模式下，系统不会阻止或提示用户和程序的未授权行为，只在日志中进行记录违规行为。

在麒麟安全管理工具主界面右上角菜单中点击“状态设置”后，进入状态设置窗口，即可对系统安全机制运行模式进行选择和切换。

图 1-2 主窗口菜单

同时还可对执行控制、文件保护、内核模块保护三大子功能模块的运行状态进行设置，如下图所示：

图 1-3 状态设置

第二章 高级功能

2.1. 执行控制

执行控制主要目的是禁止系统外来文件和被篡改后的系统应用程序运行，在应用程序执行前检查应用的完整性，可有效阻止木马病毒或未知类型的应用执行，以杜绝对系统可能造成的侵害。

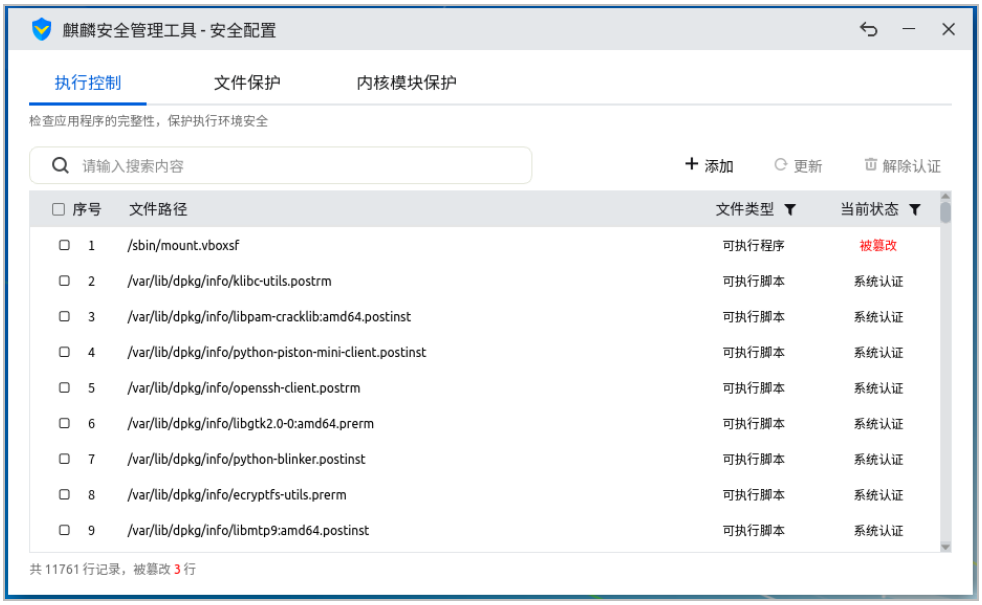

图 2-1 麒麟安全配置-执行控制

执行控制处于开启状态时，系统新创建的可执行文件、脚本、共享库（包括拷贝，编译，网络下载等方式生成的）无法直接运行，只有经授权认证或加入白名单后，才可以运行。

执行控制处于关闭状态，系统新创建的可执行文件、脚本、共享库（包括拷贝，编译，网络下载等方式生成的）可以直接运行，执行控制白名单则禁止各种更改操作。

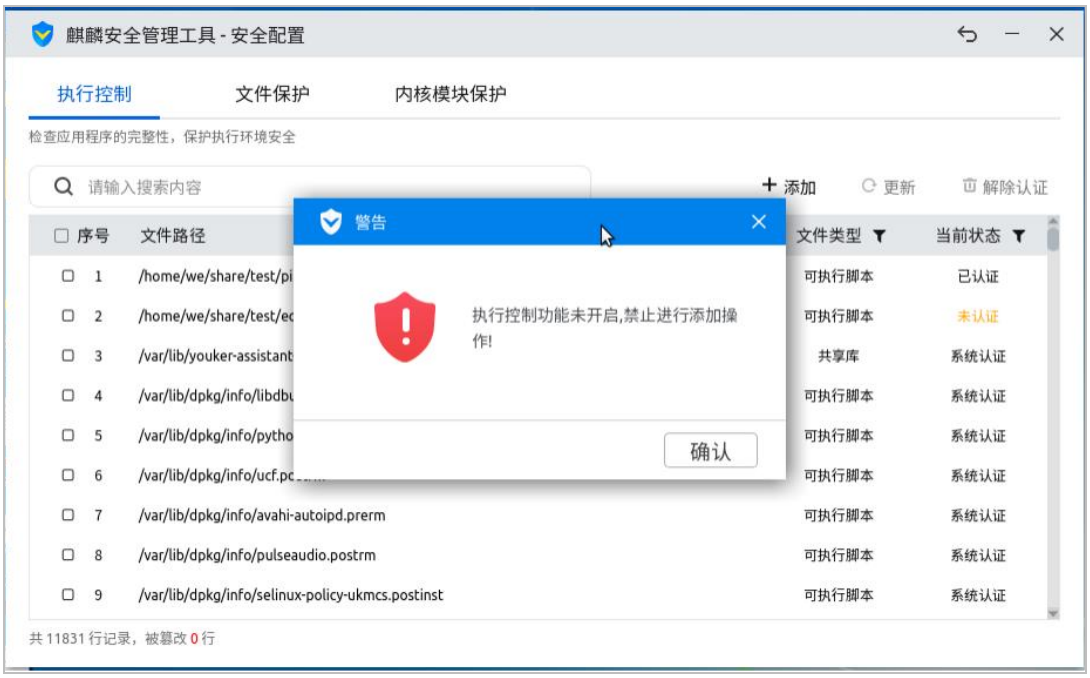

图 2-2 安全配置-功能未开启不可操作

执行控制功能启用情况下，用户可点击“添加”按钮，选择待认证的执行程序、脚本、动态库加入执行控制白名单，工具会从用户选择的目录和文件中自动筛选出满足要求的文件，添加至白名单，如下图所示：

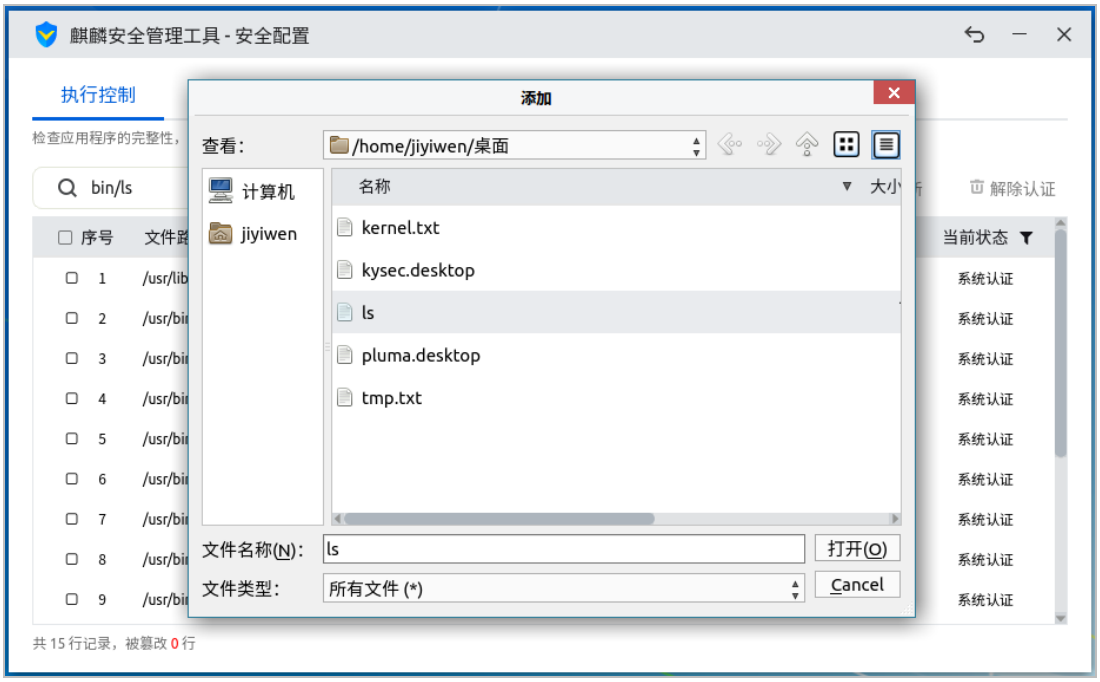

图 2-3 安全配置-执行控制-添加

当白名单列表中的文件被修改后，其对应的当前状态变为“被篡改”，此时该执行程序、脚本或动态库将不能执行，用户可通过勾选该文件，然后点击“更新”按钮恢复其“已认证”状态，如下图所示：

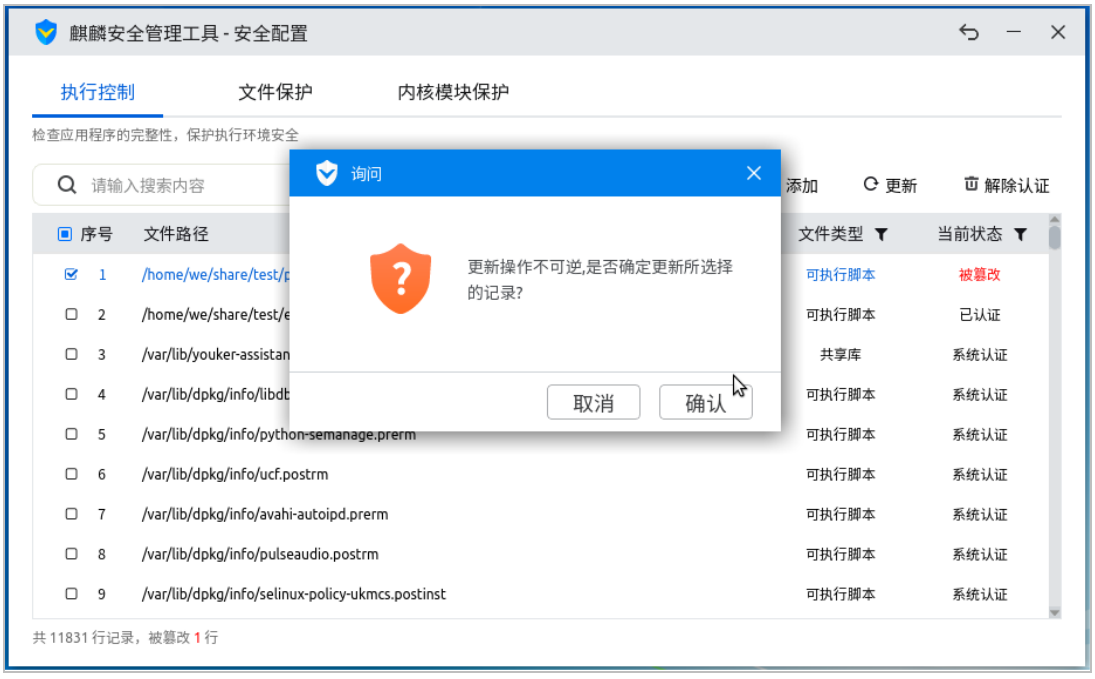

图 2-4 安全配置-执行控制-更新

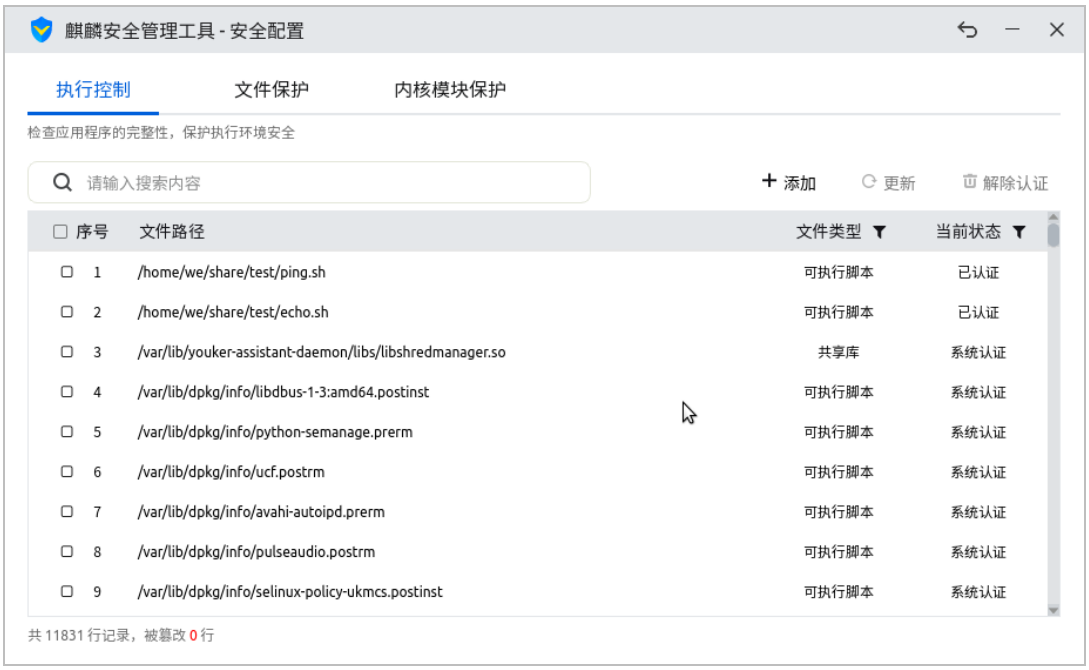

图 2-5 安全配置-执行控制-更新完毕

为方便用户从执行控制白名单查找文件，工具提供了搜索功能，在搜索框输入关键词后，点击搜索图标或者按回车键，即可查到文件路径含有关键词的记录，如下图所示：

图 2-6 安全配置-执行控制-查找

勾选列表中不再需要执行授权的记录，点击“解除认证”按钮，可以将其状态重置成“未认证”状态，如下两图所示：

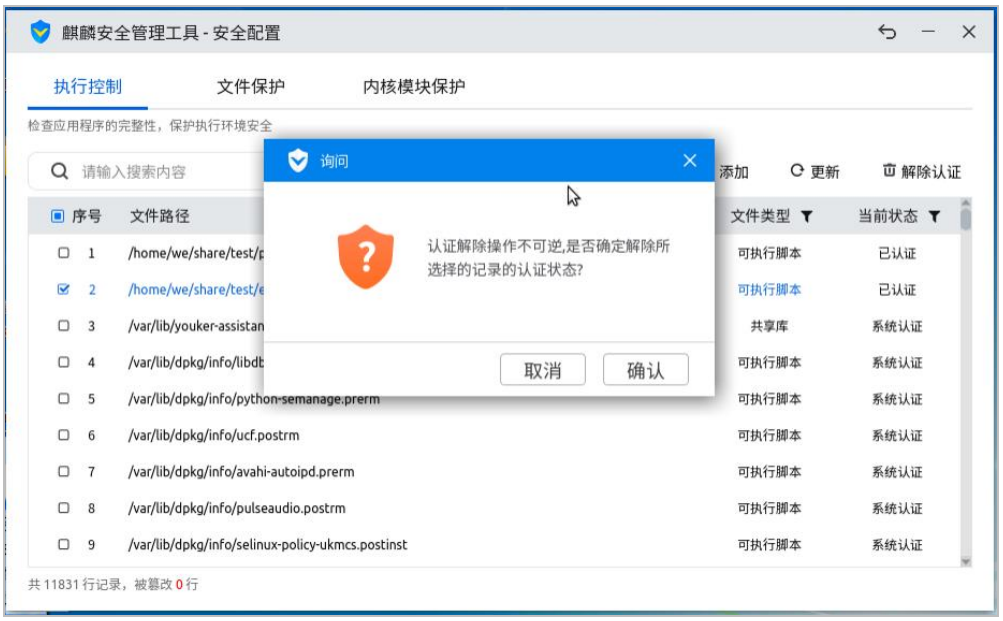

图 2-7 安全配置-执行控制-解除认证

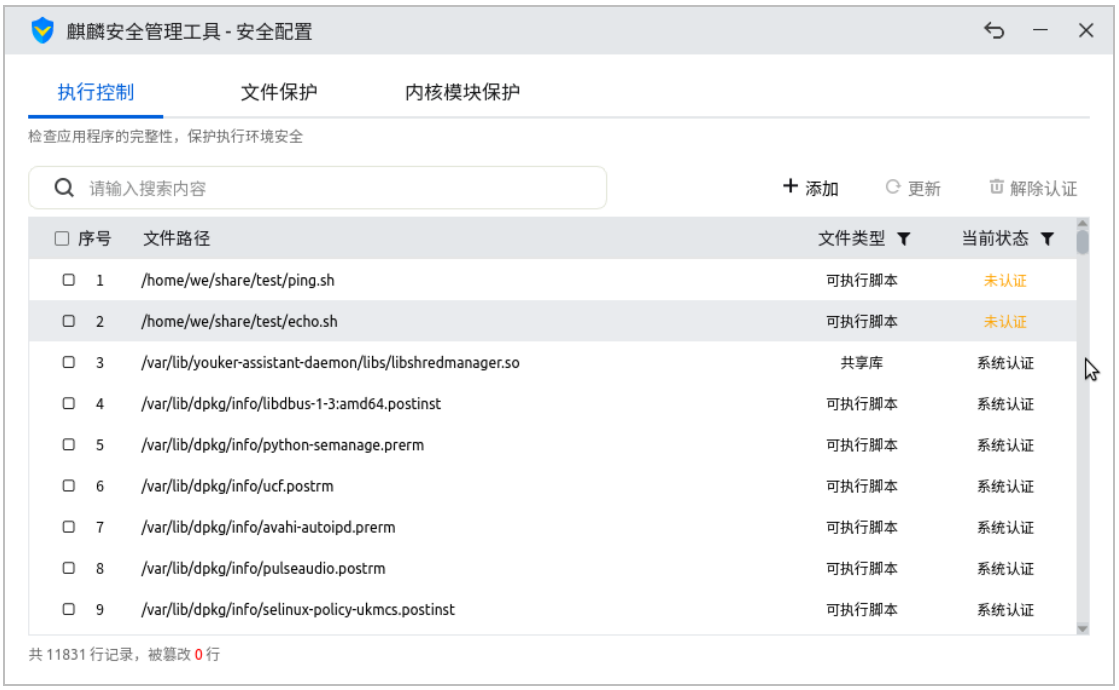

图 2-8 安全配置-执行控制-解除认证后

2.2. 文件保护

文件保护用于保护系统关键文件不被篡改、移动、删除、覆盖等操作，保证关键数据的完整性。

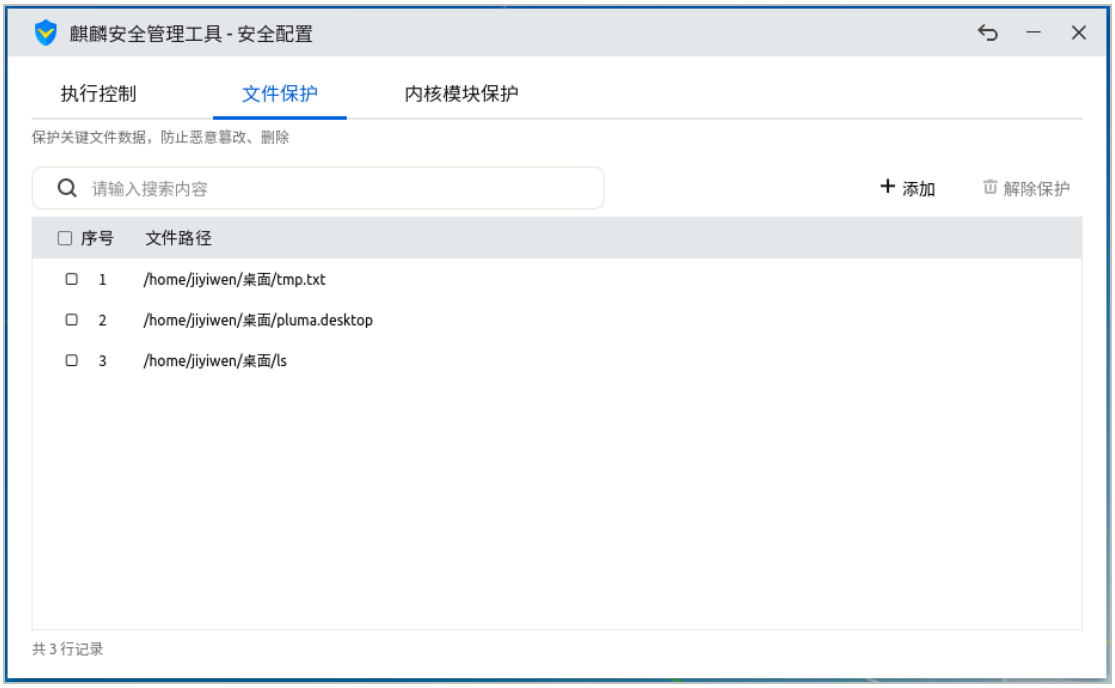

图 2-9 安全配置-文件保护

启用文件保护功能后，保护列表中的文件将得到全面保护，禁止所有用户对其进行修改、删除、移动等操作。

文件保护解除保护时，会同时从列表中删除文件对应记录，其他如添加、搜索功能与执行控制基本一致，在此不再赘述。

2.3. 内核模块保护

内核模块保护分为加载控制和防卸载保护，主要对系统加载的内核模块进行认证管控，只有经过认证的内核模块才允许加载，已开启防卸载保护的模块则禁止卸载。

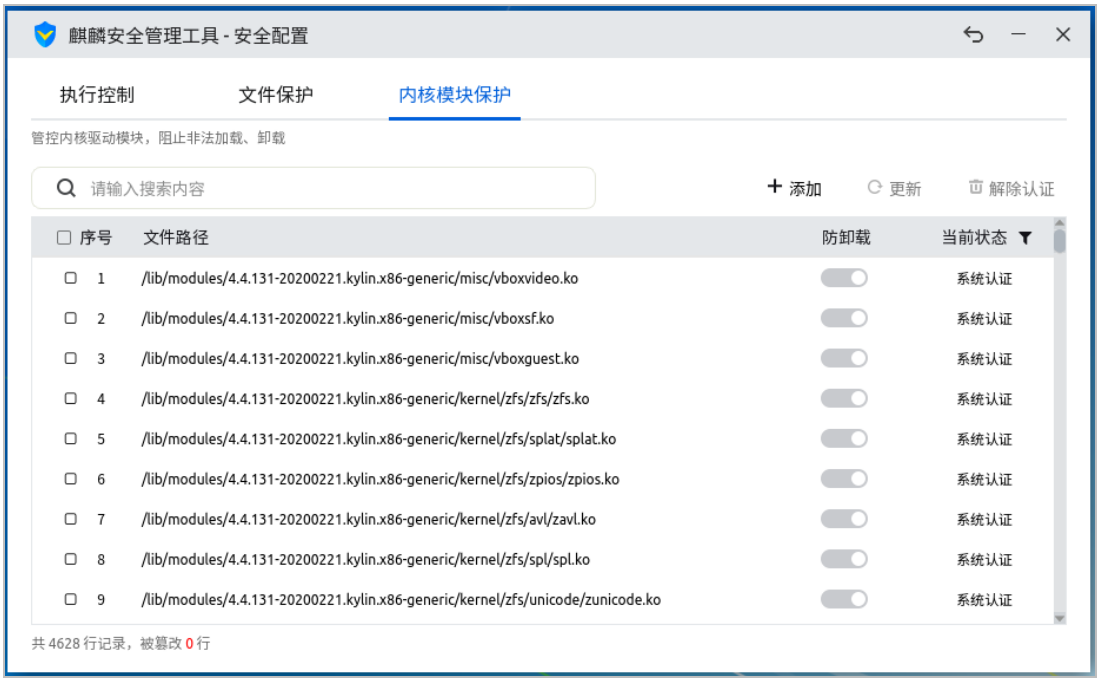

图 2-10 安全配置-内核模块保护

内核模块保护处于开启状态时，新拷贝或新编译，网络下载等方式新生成的内核模块将无法被系统加载，只有通过授权认证或加入白名单后，才可以正常加载至系统内核。

内核模块保护处于关闭状态下时，系统新创建的可执行文件、脚本、共享库（包括拷贝，编译，网络下载等方式生成的）就可以直接正常加载至系统内核。

添加至内核模块保护的内核模块还可设置其防卸载状态，设置防卸载后，该内核模块被加载至内核后，将无法被卸载，如下图所示：

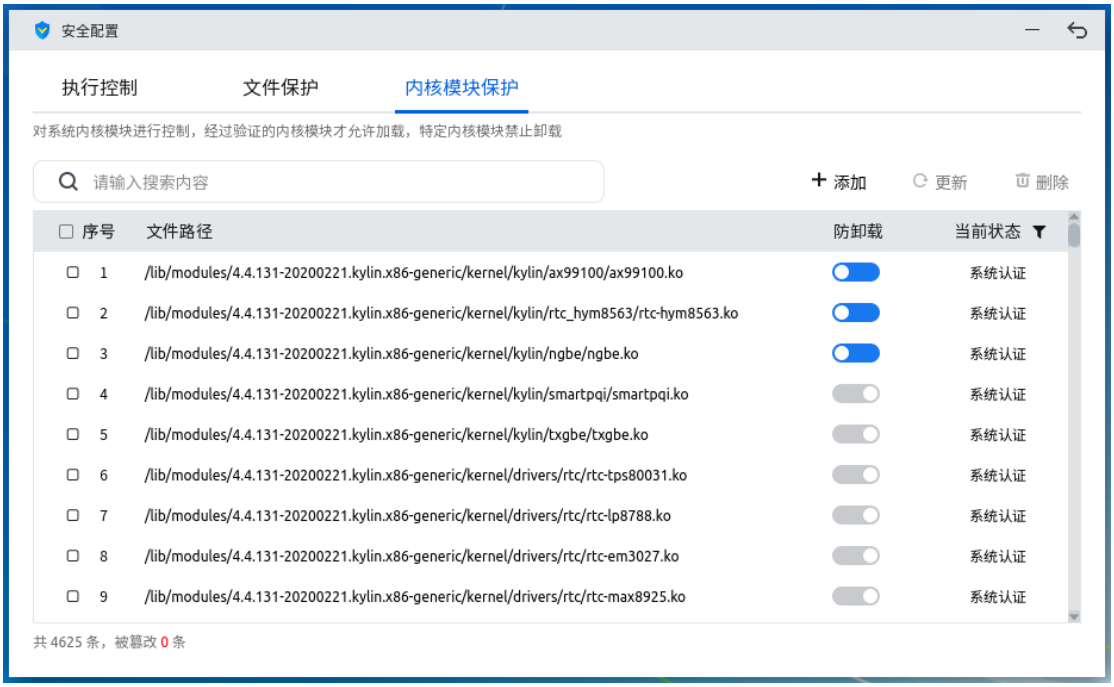

图 2-11 安全配置-内核模块保护-防卸载

内核模块保护的添加、更新、解除认证、搜索功能与执行控制一致，在此不再赘述。