# 安全盒

目录

[安全盒 1](#_Toc484008749)

[第一章、 软件简介 3](#_Toc484008750)

[1.1、介绍 3](#_Toc484008751)

[1.2、运行环境 3](#_Toc484008752)

[1.3、部署方式 3](#_Toc484008753)

[第二章、软件功能 3](#_Toc484008754)

[2.1、登录安全验证 3](#_Toc484008755)

[2.2、开启保护 3](#_Toc484008756)

[2.3、保护记录 3](#_Toc484008757)

[2.4、系统设置 3](#_Toc484008758)

1. 软件简介

1.1、介绍

安全盒允许用户设置一个目录作为安全盒，这个目录里面的文件会收到软件的保护，其他程序都只能查看，而不能修改，用户可以把一些重要的文件放置在此目录，防止被恶意修改和删除。

1.2、运行环境

运行环境为Linux操作系统，目前支持的操作系统为：

|  |  |  |
| --- | --- | --- |
| 操作系统 | 软件版本 | 备注 |
| CentOS\_6.4 x86/X64 | v1.0 | 支持 |
| CentOS\_6.5 x86/x64 | v1.0 | 支持 |
| 其他Linux系统 | v1.0 | 支持，但需要单独编译内核，额外耗时1周 |

1.3、部署方式

单机版部署。

第二章、软件功能

2.1、登录安全验证

登录采用密码认证，需要用户输入密码方可登录到软件界面。

2.2、开启保护

您需要先指定一个受保护的路径，然后点击开启保护，则该路径被保护，保护开启后，此路径下的文件只可被查看，不可被修改。保护关闭后，则保护失效。

注意：受保护的路径不可以是根路径。

版本支持路径数量：

|  |  |
| --- | --- |
| 可设置的被保护路径数量 | 备注 |
| 1个 | 标准版 支持 |
| 3个 | 增强版 支持 |
| 5个 | 超级版 支持 |
| 其他数量 | 可做定制版开发 |

2.3、保护记录

可以根据时间查看软件保护的记录，如果有软件进行过恶意操作，这里也可以看到恶意程序的路径和操作时间等信息。

2.4、系统设置

2.1.6.1、设置登录密码

修改登录密码后点击提交会返回是否修改成功，失败则提示错误原因。

软件授权：

我们会根据每个机器码生成一个注册码，用户将注册码复制粘贴后，点击注册，即可看到注册状态。未注册的用户，是无法正常使用软件的功能的。

2.1.6.2、设置白名单

在白名单里的程序，其所有操作都会被放行，此项用来过滤一些特程序以及做系统调优。

2.1.6.3、自保护

自保护是对防护系统自身的保护，防止有恶意软件去停止或者修改防护系统，开启后系统将不可卸载和停止，如果需要卸载防护系统，需要先停止自保护。