# 主机被连接端口限制

目录

[主机被连接端口限制 1](#_Toc484008741)

[第一章、 软件简介 3](#_Toc484008742)

[1.1、介绍 3](#_Toc484008743)

[1.2、运行环境 3](#_Toc484008744)

[1.3、部署方式 3](#_Toc484008745)

[第二章、软件功能 3](#_Toc484008746)

[2.1、登录安全验证 3](#_Toc484008747)

[2.2、开启保护 3](#_Toc484008748)

[2.3、保护记录 3](#_Toc484008749)

[2.4、系统设置 3](#_Toc484008750)

1. 软件简介

1.1、介绍

本软件可以限制主机上指定端口被连接，例如限制本机的sshd服务端口后，则其他用户连接本机的sshd端口会被拒绝。

开启保护时，限制生效，主机上指定的端口被限制连接，此时其他用户无法对主机进行远程操作。

关闭保护时，限制失效，其他用户可以远程对主机进行操作。

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

开启保护之前，需要先设置策略。

这里可以添加主机上需要被限制的端口，添加后的端口会受到软件的限制，未添加的端口则不受限制。

开启保护后，策略限制的端口，会拒绝被连接请求，关闭保护后，则可以正常连接。

请确保您对主机上的业务及端口非常熟悉，确保不要限制到正常的业务访问。

版本支持的端口限制数量：

|  |  |
| --- | --- |
| 可设置的被限制端口数量 | 备注 |
| 5个 | 标准版 支持 |
| 10个 | 增强版 支持 |
| 20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。