奇安信网神终端安全管理系统 V8.0-信创单机版

用户手册

目 录 | Contents

1. 产品简介

奇安信网神终端安全管理系统 V8.0_信创单机版是一款面向国产系统推出的一套安全防护解决方案，能够保护国产系统的安全，使其不受病毒、蠕虫、木马等已知和未知威胁的攻击。奇安信网神终端安全管理系统 V8.0_信创单机版主要包含病毒扫描、文件实时防护、文件白名单、安全日志、隔离区、云查杀、远程连接云安全中心升级病毒库与主程序以及支持单向切换网络版等功能。

2. 运行环境

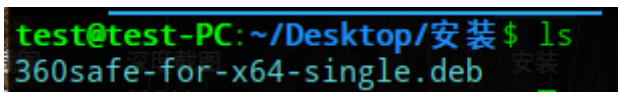
支持常见的国产操作系统，包括龙芯+中标，飞腾+银河，兆芯+中标，具体兼容列表如下：

中标麒麟（龙芯）桌面版 V7.0、中标麒麟（龙芯）服务器版 V7.0、中标麒麟（兆芯）桌面版 V7.0、银河麒麟（飞腾）桌面版 V4.0、银河麒麟（飞腾）服务器版 V4.0、uos-20-sp1（龙芯、兆芯、飞腾、鲲鹏）

3. 安装部署

具体安装和卸载过程如下：

1->首先将安装包拷贝到系统桌面或其他目录。



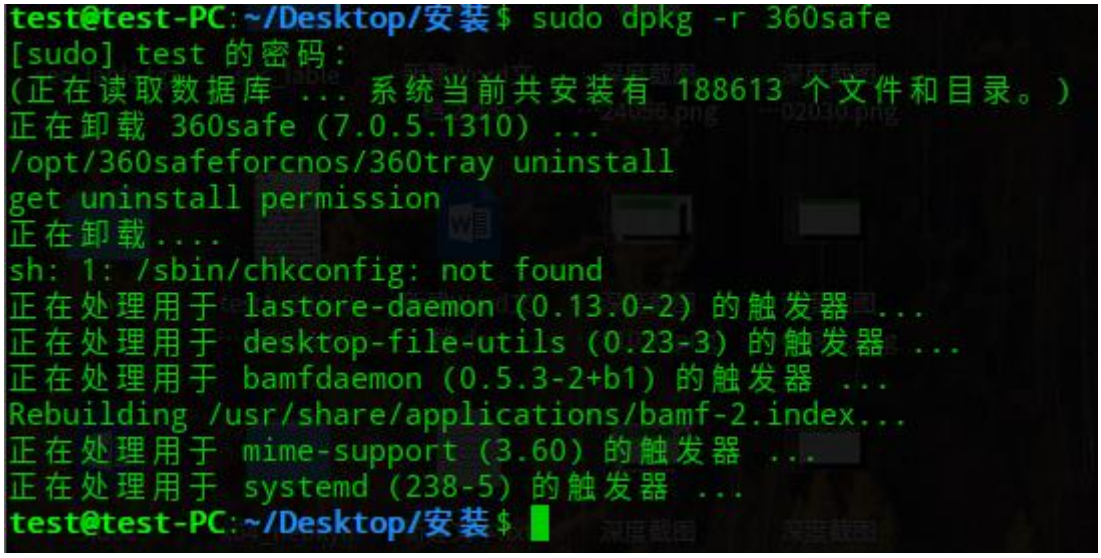
2->执行安装命令（注意需要管理员权限进行安装）

```
test@test-PC:~/Desktop/安装$ sudo dpkg -i 360safe-for-x64-single.deb
[sudo] test 的密码：
正在选中未选择的软件包 360safe。
(正在读取数据库 ... 系统当前共安装有 188501 个文件和目录。)
正准备解包 360safe-for-x64-single.deb  ...
正在解包 360safe (7.0.5.1310) ...
正在设置 360safe (7.0.5.1310) ...
正在处理用于 systemd (238-5) 的触发器 ...
正在处理用于 lastore-daemon (0.13.0-2) 的触发器 ...
正在处理用于 desktop-file-utils (0.23-3) 的触发器 ...
正在处理用于 bamfdaemon (0.5.3-2+b1) 的触发器 ...
Rebuilding /usr/share/applications/bamf-2.index...
正在处理用于 mime-support (3.60) 的触发器 ...
test@test-PC:~/Desktop/安装$
```

3->双击托盘图标，进入主界面。

图：系统主界面

4->卸载



4. 常见功能

4.1 授权

首次安装后，奇安信网神终端安全管理系统将会提供10天的试用授权，在试用授权有效期内，将无法使用在线升级相关功能，但是系统提供的其他功能可以正常使用；

本系统支持单机版单向切换网络版，需要先设置服务器 IP，首次连接到控制中心后将变为网络版，此时单机版授权失败，同时会减去网络版授权点数，建议联系商务，提前做好授权变更。

- **授权导入**

  首次安装后，查看授权信息：单击设置—授权信息，如下图：

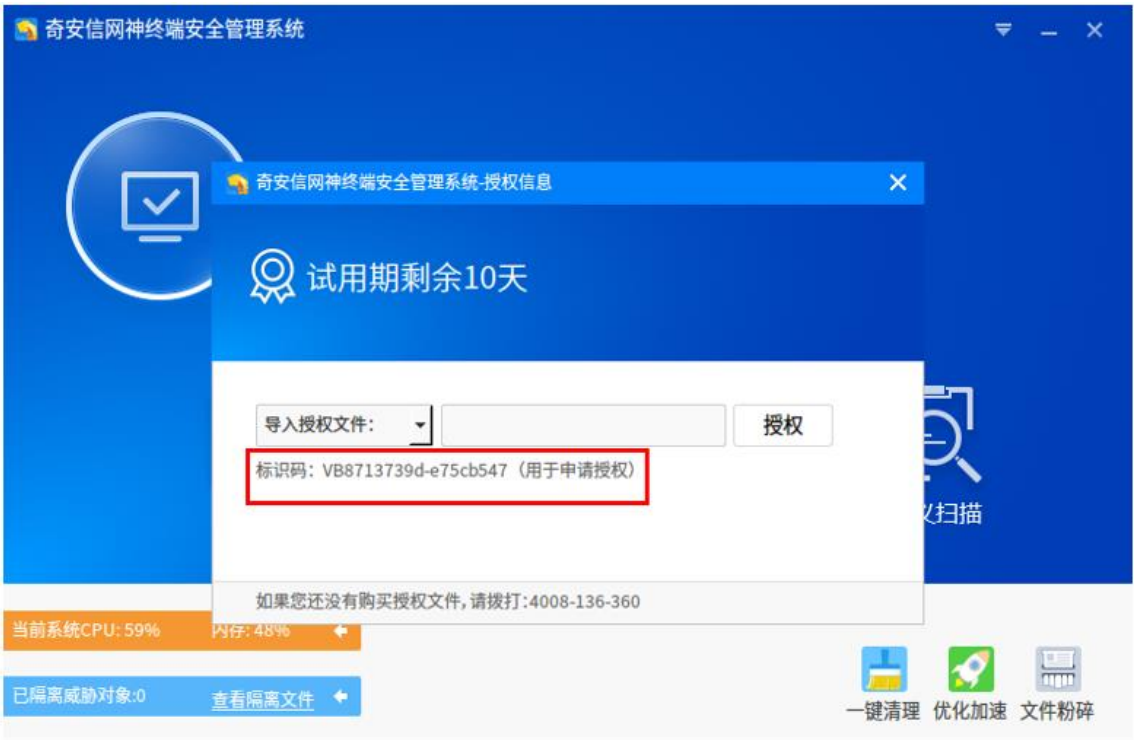
图：查看授权信息

弹窗提示授权状态信息，在该界面导入授权文件，完成授权（授权文件获取参见授权获取）。

图：授权信息界面

- **授权获取**

每个国产设备存在唯一标识码，非授权状态下，在产品授权信息界面里查看：



图：查看标识码

获取授权步骤：

1. 通过标识码，联系奇安信工作人员申请授权序列号（支持批量标识码申请序列号）；

2. 通过授权序列号下载授权文件，具体参考步骤如下：登录 https://www.qianxin.com/activation/index 进入”产品激活”--“序列号激活”，在该页面中输入你的产品序列号：

图：产品激活序列号输入

输入正确的序列号后，点击“下一步”，输入基本信息后即可获取到你的授权证书，授权证书为.qcert 格式。拿到授权后，即可在授权信息界面导入授权文件（参见授权导入）。

4.2 升级

4.2.1 离线升级病毒库

1. 打开主程序，单击 设置—离线升级：

图：离线升级

2. 弹出对话框，选择病毒库文件所在到文件夹，点击”打开”。

图：选择病毒库文件夹

3. 点击打开后即可执行升级操作，升级成功后可以正常使用。

图：离线升级病毒库成功

4.2.2 在线升级病毒库和主程序

当国产系统具备连接互联网到时候，可以通过远程到云安全中心进行在线升级病毒库和主程序。

1. 打开系统主界面，如下图所示，点击升级图标：

图：手动升级病毒库和主程序

2. 系统会自动连接云安全中心，同时会检查病毒库和主程序是否有新版本，如果有新版本，则直接自动完成相应到升级，并提示升级成功。

5. 客户端基础功能

5.1 系统首页

首页包括病毒扫描的三种扫描方式（快速扫描、全盘扫描、自定义扫描）、当前系统的资源占用（CPU、内存）、一键清理、优化加速、隔离区、文件粉碎工具、防护引擎展示、与云安全中心连接状态展示、以及版本显示。

图：系统联网主界面

5.2 病毒扫描

5.2.1 快速扫描

点击快速扫描对系统关键路径，系统内存进行病毒扫描动作，保证快速查杀病毒木马

图：快速扫描

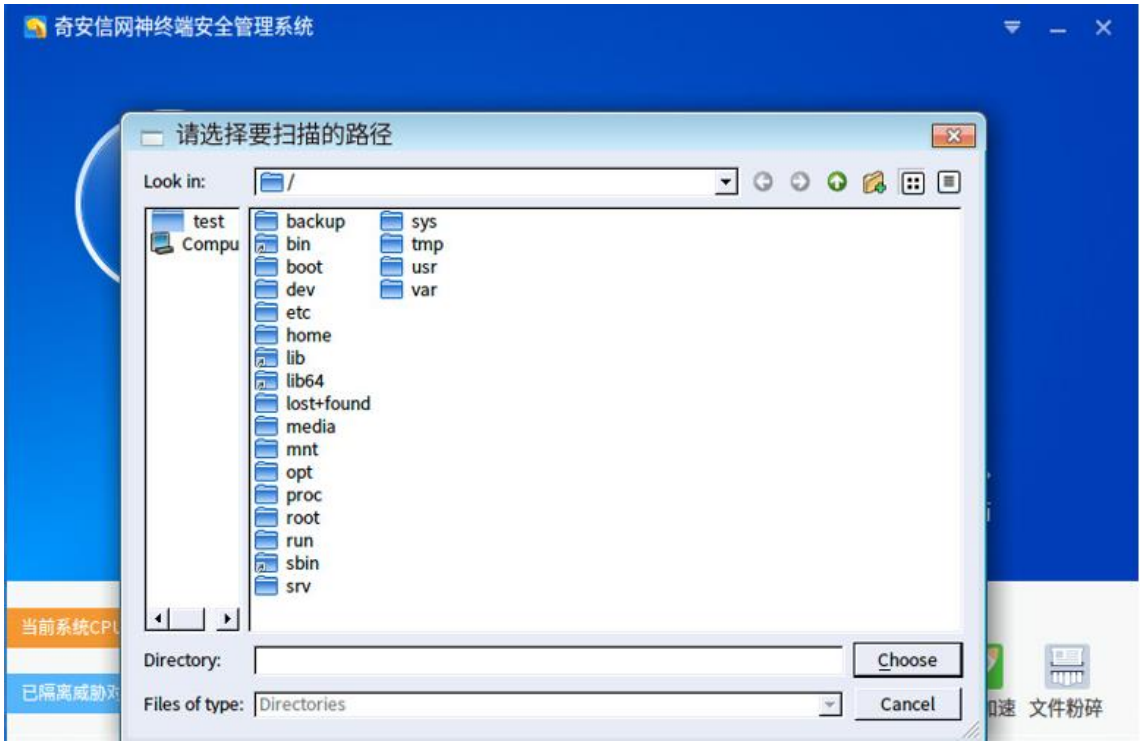
5.2.2 全盘扫描

可以扫描全盘当前用户可读文件，保证系统安全。

图：全盘扫描

5.2.3 自定义扫描

对指定目录按需扫描。



图：自定义扫描

5.3 文件粉碎机

难以手动删除的“顽固”文件或文件夹，通过文件粉碎机可彻底删除。

图：文件粉粹

5.4 一键清理

对 Cookies、电脑垃圾、上网痕迹等记录和垃圾文件进行清理，让电脑保持较好到工作状态。

图：一键清理

5.5 优化加速

可以对系统到启动项进行禁止启用和恢复启用，关闭一些不必要到启动项可以提升开机速度。

图：优化加速

5.6 文件实时防护功能

监控操作系统被病毒木马入侵时，实时清除/删除恶意代码，保证操作系统安全。文件实时防护拦截木马病毒时，默认在操作系统桌面右下角弹窗，提示使用者当前发现病毒文件，点击“确认”按钮后，会关闭弹窗。点击“查看已隔离的文件”，会打开隔离区，查看被处理的文件。

图：文件实时防护监控

文件实时防护弹窗上有“设置”按钮，可根据场景需要，选择是否弹窗提示，或者到设置中心里操作。

图：文件粉粹

5.7 隔离区

通过病毒扫描或者文件实时防护处理过的样本，会备份到隔离区中，并可以在隔离区里恢复处理后的文件

图：隔离区

5.8 安全日志

病毒扫描和文件实时防护查杀到危险项后，并且防护日志信息支持导出，便于查看统计。

- 病毒扫描

  执行快速扫描、全盘扫描、自定义扫描查杀的日志可以在这查看详细日志

图：病毒扫描日志

- 防护日志

  文件实时防护成功的日志，可以在这里查看详细的日志


奇安信网神终端安全管理系统 - 日志
病毒扫描
防护日志
时间 文件 防护说明 处理结果
2020-04-24 04:35:45 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:45 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:45 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:45 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:45 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:45 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:44 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:44 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:44 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:44 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:44 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:44 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
2020-04-24 04:35:44 /home/hanyu/桌面/TempSa··· 恶意软件(Virus.Win32.··· 已隔离
自动清理30天以上的记录
导出日志
清空记录
关闭

图：防护日志

5.9 系统设置

5.9.1 病毒扫描设置

图：病毒扫描设置

可以针对待扫描的文件类型、压缩包扫描设置、发现病毒到处理方式、是否开启文件实时防护以及是否开启云查杀防护进行策略设置。

- 文件扫描类型

  可以选择“全部文件”，“可执行文件与文档”进行扫描

- 压缩包扫描设置

  可以设置扫描压缩包到扫描边界，超过压缩包到最大层数和最大值将不再进行扫描。

- 大文件扫描

可以设置处压缩包之外文件扫描的最大边界。

- 发现病毒时的处理方式

可以选择发现病毒时的处理方式，如果需要自动处理的话则选择“由杀毒软件自动处理”，“由用户选择处理”

- 系统实时防护

可以选择开启文件实时防护，实时监控文件的读写，可以有效在落地时将病毒清理掉。

- 云查杀防护

可以选择是否开启云查杀防护功能，开启后，客户端在进行查杀时，会自动连接云安全中心。

5.9.2 文件白名单

可以将文件或目录加入文件白名单，奇安信网神终端安全管理系统 V8.0 不会扫描该文件或目录。如图：

图：文件白名单

5.9.3 服务器 IP 设置

服务器 IP 设置功能使用的场景是进行版本切换，即单机版切换为网络版，该过程为单向不可逆过程，设置完 IP 后，客户端会自动连接该 IP 指向到服务器，当连接成功后，单机版客户端自动转变为网络版客户端。

图：服务器地址设置

5.9.4 升级设置

系统支持自动升级和不自动升级，当选择自动升级功能时，系统默认开启病毒库和主程序自动检测新版本，如发现有新版本，则系统会自动升级；当选择不自动升级时，系统到主程序将会关闭自动检测新版本功能，可以选择是否自动升级病毒库，当勾选“不升级主程序，但仍然升级病毒库”时，系统会只检测病毒库是否有新版本，并根据新版本到情况，来自动升级病毒库版本。

图：升级设置

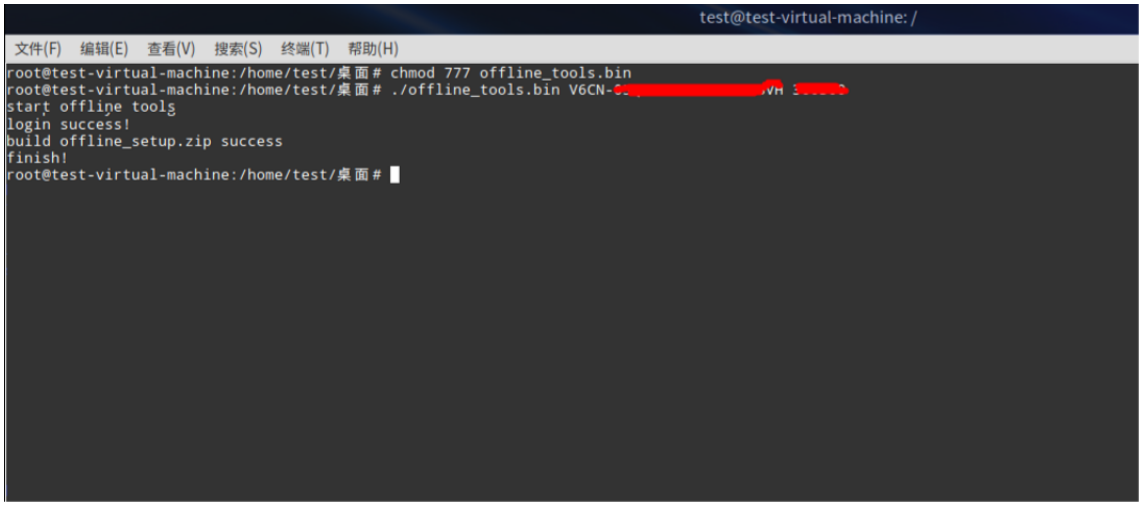
6. 其他事项

6.1 病毒库更新操作步骤

1）拷贝 Linux 版离线升级工具 offline_tools.bin 到能连互联网的 Linux 环境的设备上，打开系统终端；

2）在工具所在路径执行：chmod 777 offline_tools.bin

3）继续执行： “./offline_tools.bin 授权序列号 授权密码”，如截图所示：



4）执行成功后，会在当前目录下生成 offline_setup.zip 文件，即离线病毒库，离线病毒库下载成功。

5）将病毒库 offline_setup.zip 文件解压后即可生成病毒库文件夹，按照离线升级库库操作即可完成离线病毒库的升级。