智权盾® 安全 U 盘
用户手册

广州极智信息科技有限公司
广州市黄埔区彩频路 11 号广东软件园 A 区 403-404
020-28105426

一、 前言

在信息技术早已渗入生产生活各个环节的今天，各种智力成果往往都以电子文档（内容、数据、程序等）的形式进行存储与传播。但人们在享受技术所带来便捷的同时，又不得不为担心自己的智力成果被非法复制、恶意扩散而大伤脑筋。

信息安全建设，大都着眼于平台级系统级的设备和软件。各种大型的高价的设备和软件大行其道。而信息安全体系的最末端——移动存储，却被各大厂商有意无意忽视了。事实上，重要资料的存储和传播，很大一部分是在线下采用移动存储设备进行的。人们最常用的 U 盘，虽小巧便捷，可随时贴身携带，却也是信息泄露的重灾区，往往稍有不慎便会导致重要信息的泄密。

近年来，个人隐私、智力成果、商业秘密甚至国家机密通过 U 盘外泄的事件时有发生，往往导致声誉尽毁，公司破产，责任人丢官甚至坐牢等严重后果。实现安全移动存储及可控传播，早已成为一个亟待解决的现实问题。

在政府和企业业务中，U 盘带来的威胁主要表现在以下几个方面：

1.无法保护终端数据私密性

由于普通 U 盘是一个不受管控存储介质，可以在任何计算机上使用。这就会出现员工使用 U 盘携带个人数据过程中，可能造成企业数据的无意外泄；或者出现员工故意窃取数据，而无法进行管理的情况。最终会均会导致内部数据外泄的情况。

2.无法保护 U 盘数据的私密性和完整性

由于普通 U 盘是一个不受保护的存储介质，对数据的访问并不会进行身份验证，数据也未进行加密处理。所以在 U 盘丢失、他人冒用、或被病毒木马感染的情况下，造成数据的丢失或损坏。

3.造成内部病毒木马传播

感染病毒的计算机会将病毒感染到 U 盘，一旦该 U 盘插入到其他计算机上，就会造成无毒计算机感染病毒。如此反复，相互感染，从而引发整个网络的病毒感染，造成系统损坏、数据丢失、死机，甚至整个网络瘫痪。

4.对于数据泄露的安全事件无法追踪

普通 U 盘无论在政府部门专网还是在互联网上使用，即使主动进行违规操作，也无法进行有效的审计和取证。

广州极智信息科技有限公司基于自己对安全移动存储技术和市场的深刻理解，自主创新研发，独创了全新概念的主动授权模式的 VNAS 技术，形成自主安全 U 盘开发平台，并在此基础上推出了“智权盾”系列产品。“智权盾”安全 U 盘不但从软件方面解决了木马摆渡、病毒传播、U 盘交叉使用和 U 盘文件使用缺乏审计等方面的安全问题，同时通过软硬结合的模式大大提高了 U 盘的安全特性，保证即使 U 盘丢失也依然可以有效保护 U 盘内的加密文件，从各个方面减少了因 U 盘使用而为政府和企业带来的安全隐患。

二、 产品特性

1. 平台兼容

本产品已兼容适配下列平台：

Windows：X86/X64 CPU，Windows7，Windows8，Windows8.1，Windows10

Linux：X86/X64/ARM64 CPU，支持多种国产操作系统发行版本

2. 安全特点

1) 防止非法拷出：

a. 特有受控阅读，可在受控模式下仅仅在盘内打开阅读。

b. 可防止通过另存、打印、截屏、录屏、剪贴板、拖拽、网络发送等方式将 U 盘内的文件及内容拷出 U 盘外。

2) 防止病毒木马主动传播：

a. 即使用户不小心把病毒木马拷入安全 U 盘，病毒木马在安全 U 盘中同样属于封存状态，无法主动运行并扩散到其他存储设备中。可以防止主动传播。

b. 安全U盘并非标准的移动存储设备，无法通过标准API拷贝文件，病毒木马无法在后台感染安全 U 盘内的文件，杜绝了主动传播的可能。

3) 防止病毒木马破坏数据：

a. “智权盾”安全 U 盘中的数据受到安全硬件的保护，只有通过专用接口的合法性认证，才可以访问其中的数据，可以防止病毒木马对数据进行非法访问，进而感染文件数据并造成损坏。

4) 高强度日志记录：

a. 日志抓取不受内外网限制，会如实抓取用户的操作行为。

b. 日志存储受到安全硬件保护，防止篡改。

c. 日志可以标准 SysLog 格式推送到日志服务器。

5) 防止未授权访问与篡改：

a. 安全 U 盘接入系统，在身份认证之前，“智权盾”安全 U 盘的用户数据区属于禁止访问状态，受软硬件全面保护。

b. 安全 U 盘的启动区属于只读状态，可防止攻击者进行篡改。

6) 防止第三方访问与篡改：

a. 安全 U 盘接入系统，在身份认证之后，对“智权盾”安全 U 盘用户数据区的访问，需要通过调用加密文件系统接口。

b. 接口会对访问用户数据区的进程进行合法性校验 ,第三方进程无法通过校验，从而阻止第三方的访问，规避了用户数据被篡改的潜在风险。

7) 防止逆向工程：

a. “智权盾”安全 U 盘的启动程序进行加壳、加花处理，可有效防止攻击者进行逆向工程分析。

8) 防止口令破解：

a. “智权盾”安全 U 盘接入系统，在身份认证过程中，存在口令尝试次数限制，可有效防止暴力破解。

b. 口令认证过程受到安全硬件保护。

9) 防止数据密钥破解：

a. “智权盾”安全 U 盘接入系统，在身份认证之前，因为无法访问数据区密文，无法获取数据明文密文的配对，加大攻击者对密钥的破解难度。

b. 加密方法无法被第三方程序调试，再次加大攻击者对密钥的破解难度。

c. 密钥的生成和维护机制合理，存储受到安全硬件保护。

10) 防止剖片攻击：

a. 即使安全 U 盘在被专业技术人员进行剖片攻击，安全 U 盘采用私有加密文件系统，剖片得出数据密文亦无法解出明文。

11) 支持统一管理：

a. 可开放用户及权限管理接口，便于统一管理。

b. 可开放标准日志读写接口，便于统一日志审计。

12) 国产化支持：

a. 可选用全国产硬件。

b. “智权盾”安全 U 盘支持国密算法：SM4 对称加密，SM2 非对称加密，SM3 消息摘要。

c. 适配主流的 CentOS、Debian 系国产 Linux 系统（红旗、中标麒麟、深度等等）。

13) 使用方便：

a. 可跨平台使用

b. 即插即用

三、 初始化与登陆

1. 运行

1) Windows 环境：

将安全 U 盘插入计算机 USB 接口，在操作系统的文件资源浏览器窗口中找到一个卷标为"SecU"的 CD 驱动器（如图 3.1 所示），双击该 CD 驱动器便可自动运行安全 U 盘程序

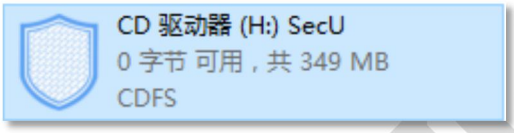


图 3.1 安全 U 盘 CD 驱动设备

注意：

- 若您的计算机关闭了光盘自动运行，则双击仅会打开此 CD 驱动器而不会运行安全 U 盘程序。此时需要进入 CD 驱动器内，双击盘内的可执行文件“.SecU.exe”（如图 3.2 所示）即可运行安全 U 盘程序

图 3.2 安全 U 盘程序

- 安全 U 盘会自动检测计算机上的系统环境，若所需的运行环境不完整，将自动安装相应缺失的组件，组件安装过程可能会弹出相应的提示（如图 3.3 所示），请按提示操作确保组件安装完成。

图 3.3 安装.NET 运行环境的提示

- 如果出现杀毒软件误报的情况（如图 3.4 所示），请勾选“记住我的选择，以后不再提醒”，并点击“允许”。

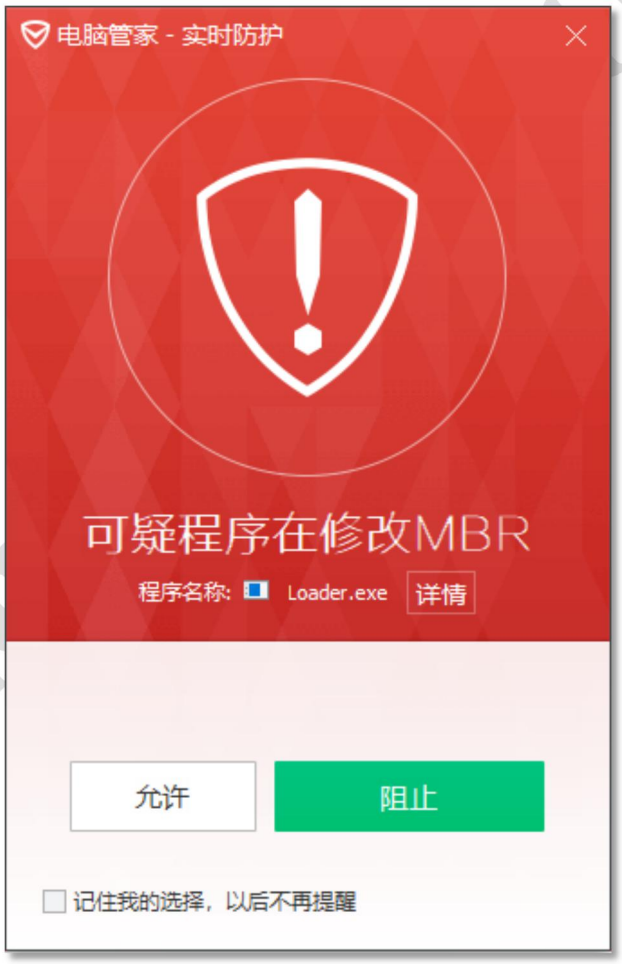


图 3.4 腾讯电脑管家误报

2) Linux 环境：

安全 U 盘接入系统，会弹出自动运行提示（如图 3.5 所示）

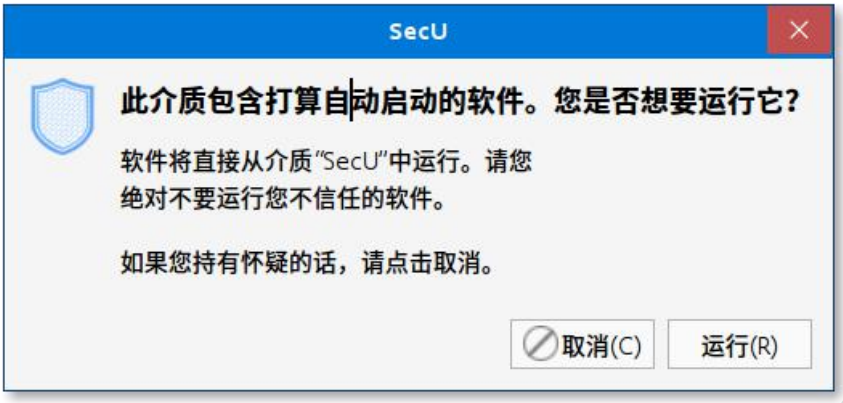


图 3.5 Linux 下自动运行提示对话框

点击“运行”，在新弹出的对话框（如图 3.6 所示）中输入操作系统 ROOT 密码，按“Enter”（回车）确认后即可正常运行

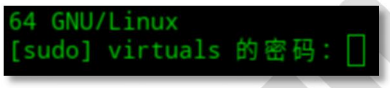


图 3.6 操作系统 Root 密码输入界面

注意：

- 若系统未弹出自动运行提示，也可在 SecU 目录下双击运行 autorun.sh 文件，在弹出的对话框中点击“在终端中运行”按钮（如图 3.7 所示），输入操作系统 ROOT 密码，以便能正常启动安全 U 盘。

图 3.7 双击“autorun.sh”文件运行提示对话框

图 3.8 输入操作系统 ROOT 密码界面

2. 初始配置

初次使用时，安全 U 盘需要进行初始配置。成功运行安全 U 盘程序后会自动弹出配置界面（如图 3.8 所示）

图 3.8 初始配置界面

此时，需要用户设置安全 U 盘的管理密码（长度至少 6 位）以及至少一个密码保护问题。

输入完成后，单击“确定”按钮，即可将配置保存，安全 U 盘就完成了初始配置。

注意：

- 初始配置需要在 Windows 系统下操作。
- Windows 系统下可以在管理模式与普通模式间切换，Linux 系统下默认是管理模式登陆。
- Windows 系统下 ,管理模式具有最高权限能随意拷贝安全 U 盘内的文件，并能限制普通模式下的功能，请务必保管好管理密码，勿外泄给他人。
- 请务必牢记设置的管理密码及密码保护问题答案。在您忘记密码的时候，可通过密码保护问答重设管理密码。

3. 登录

安全 U 盘程序运行起来时，会自动弹出软件登录对话框（如图 3.9 所示），需正确地输入已设置的登陆密码才能进入软件主界面。

图 3.9 安全 U 盘程序登陆界面

普通模式登陆（仅 Windows 系统）

在登录界面输入已设置的访客密码，会以普通模式打开安全 U 盘。普通模式下的操作权限受管理模式下“防拷选项”中选项设置的限制。

管理模式登陆

在登陆界面输入已设置的管理员密码，会以管理模式打开安全 U 盘。在管理模式可以通过设置“防拷选项”对普通模式下的操作权限进行限制。通过“格式化加密区”来格式化安全 U 盘，通过“修改管理密码”来修改原先设置的管理员密码。

注意：

1) Windows 环境：

- 如果管理员在“防拷选项”中设置了访客密码为空，则下次登录会先自动进入访客模式。此时若想进入管理模式，可通过“选项”->“模式切换”唤出登陆界面，输入管理密码，就能切换到管理模式。
- 如果忘记了管理密码，可通过点击登陆界面的“忘记密码”链接，在弹出的密保问题回答界面（如图 3.10 所示），填写正确的答案，点击“确定”后即可在设置界面重设管理密码。

图 3.10 密码保护回答界面

2) Linux 环境：

- Linux 环境下的登陆界面没有“忘记密码”链接，任何需要重设密码的操作需要在 windows 环境下操作。
- 如果“忘记密码”的链接为不可用的灰色状态，请输入任意字符，点击“确定”按钮，在关闭弹出的“登陆失败”窗口（如图 3.11 所示）后，“忘记密码”的链接即可用。但输入错误次数最高不得超过 5 次。

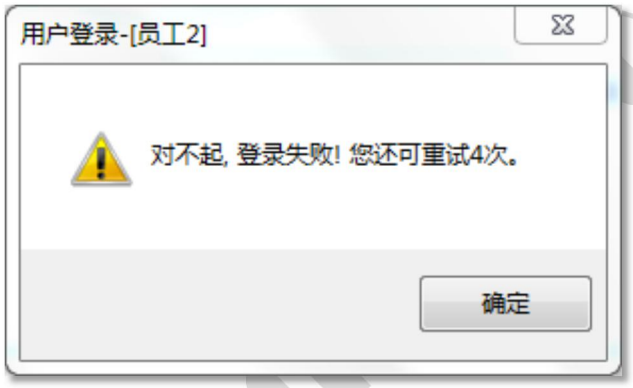


图 3.11 登陆密码错误提示框

警告：

- 若您的密码重试次数超过 5 次，将要求回答密保问答的答案，回答成功则可重置密码；
- 若密保问答答错次数超过 5 次，安全 U 盘将自动销毁，安全 U 盘内的文件将被删除且无法取回，需返厂重置才能继续使用。

四、 软件功能

1. 模式切换（仅 Windows）

“模式切换”选项允许用户在管理模式与普通模式间切换。

点击“选项->模式切换”菜单项，唤出软件“登陆界面”，如果输入管理密码将切换到管理模式，如果输入访客密码就将切换到普通模式。

2. 修改管理密码

“修改管理密码”选项允许管理模式下的用户修改管理模式的登陆密码，Windows 环境下还能更改或添加密码保护问答问题。

1) Windows 环境：

点击“选项->修改管理密码”菜单项，即可打开管理密码设置界面（如图 4.1 所示）

注意：

- 填写新管理密码和管理密码保护问答后，点击“确定”按钮才能立即应用当前设置。若点击取消，则不会修改当前的管理密码和管理密码保护问答。

2) Linux 环境：

点击“选项->修改管理密码”菜单项，即可打开管理密码设置界面（如图 4.2 所示）；

输入当前的管理密码和新的管理员密码，点击“确定”按钮，所做的更改就会立即应用。

如果需要修改密码保护问答，请在 Windows 环境下使用“修改管理密码”功能进行操作。

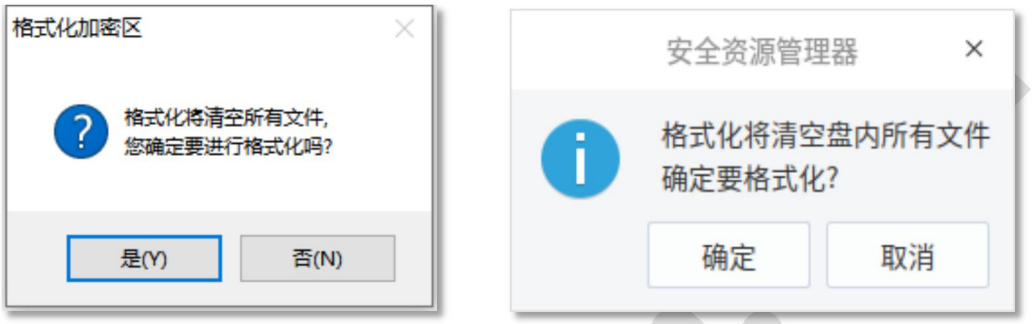
图 4.1 设置管理密码界面

图 4.2 修改密码界面

3. 格式化加密区

“格式化加密区”选项允许管理模式下的用户将安全 U 盘格式化。

点击“选项->格式化加密区”菜单项，在弹出的对话框中点击“是”按钮（如图 4.3 所示），即可开始格式化 SecU 盘加密区。



Windows 环境　　Linux 环境

图 4.3 格式化加密区确认对话框

警告：

- 格式化加密区将会清除当前安全 U 盘上的所有文件，请谨慎操作。

4. 桌面快捷方式（仅 Windows）

“桌面快捷方式”选项允许程序在桌面创建一个指向安全 U 盘驱动器的快捷方式，使得用户能够在安全 U 盘插入电脑的情况下通过双击此快捷方式快速打开安全 U 盘程序。

点击“选项->桌面快捷方式”菜单项，即可在操作系统的当前用户的桌面上创建一个快捷方式。

5. 设置防拷选项 （仅 Windows）

“防拷贝选项”选项允许管理员设置普通模式下的各种权限。

点击“选项->桌面快捷方式”菜单项，即可打开防拷选项设置界面(如图 4.4 所示)。防拷选项设置界面包括访客密码和访问限制项两部分。可以根据具体需要进行设置。

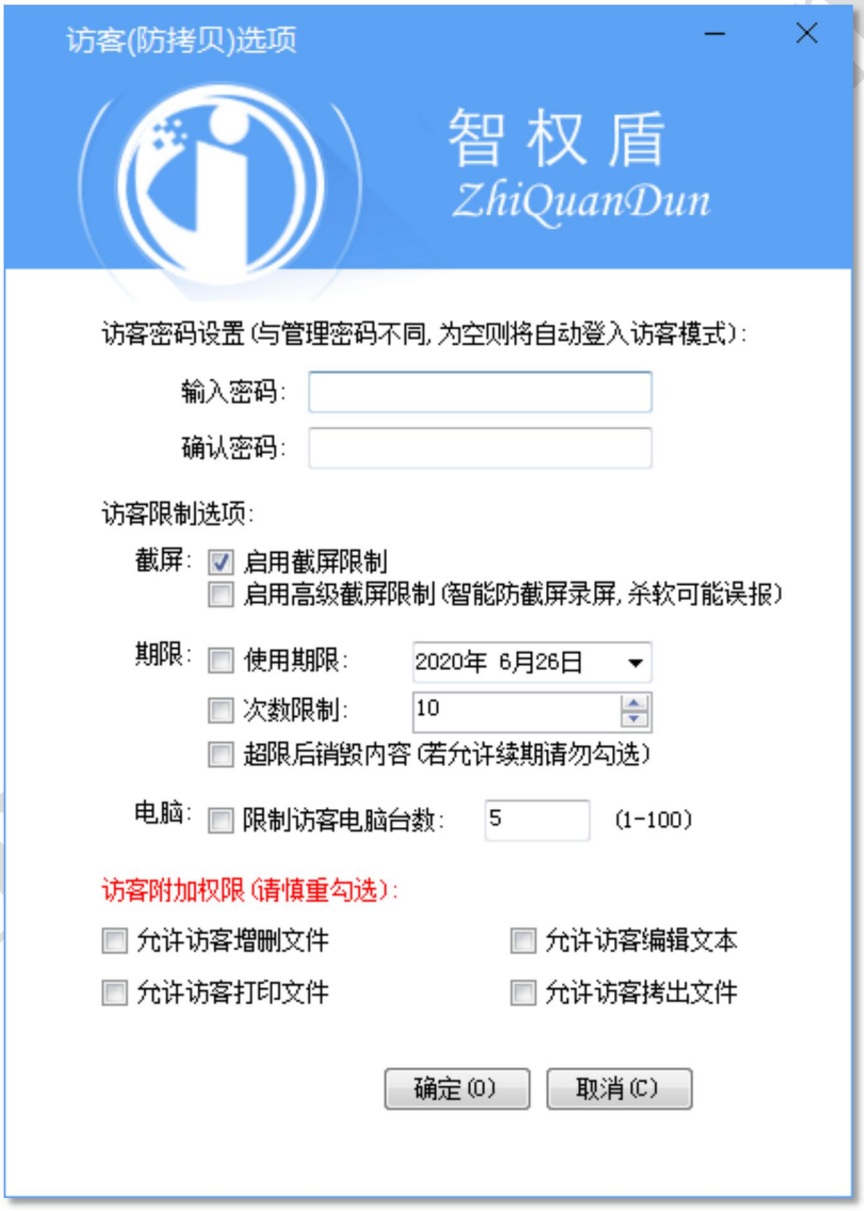


图 4.4 防拷选项设置界面

6. 关于

“关于”选项将向用户展示生产厂商及设备信息（如图 4.5 所示）

图 4.5 关于信息界面

注意：

- 不同时期的产品展示信息可能有所不同，具体以软件实际运行时展示信息为准。

7. 退出

点击“选项->退出”菜单项，安全 U 盘程序自动关闭所有已打开的文件，关闭文件盘，并结束运行。

待安全 U 盘程序成功退出之后，方可从 USB 口拔出安全 U 盘。

警告:

- 直接拔出设备，可能会导致文件损坏或硬件损坏，请务必先通过菜单项退出程序！

- SecU 程序有严格的自我保护机制，注入、调试、转储或非法终止进程等疑似破解的操作，都有可能导致您的计算机崩溃，请谨慎为之！

8. 更新

在联网状态下可自动检测、在线更新，保持最新版本状态。当有更新时会弹出更新确认对话框（如图 4.6 所示）。

当有可用的在线更新时，点击“更新”按钮即可在线更新。

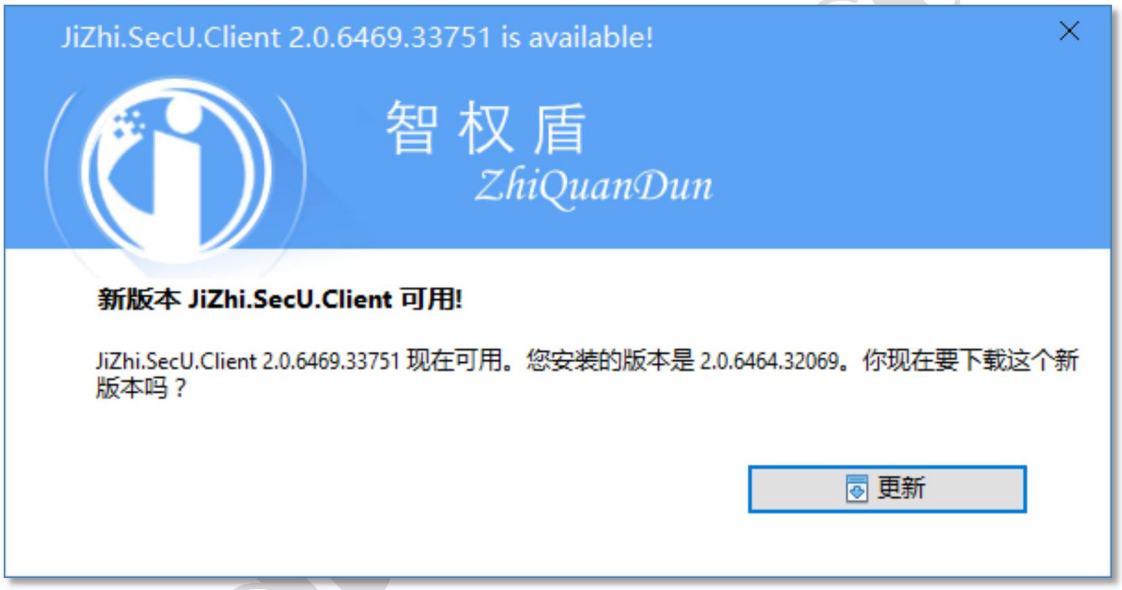


图 4.6 更新信息界面

五、 常用操作

1. 文件操作

可以在菜单栏通过“文件”菜单项或是在文件浏览列表中单击鼠标右键弹出右键菜单栏来使用常用的文件操作（如图 5.1 所示）。

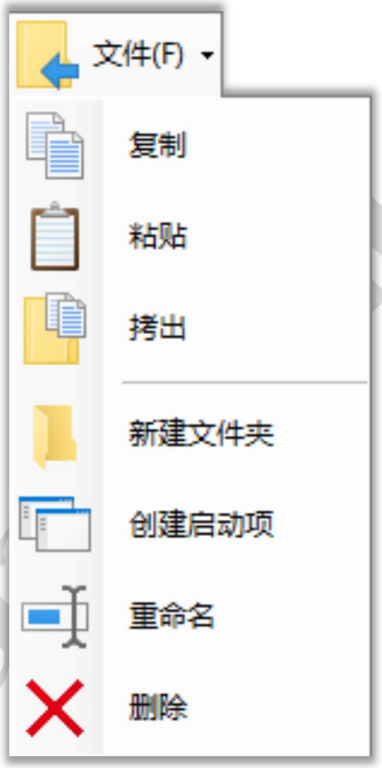


图 5.1 “文件”菜单列表

1) 复制

在单选或多选选中文件/文件夹后，可使用右键弹出菜单的“复制”选项，将选中的文件/文件夹列为数据来源。或是使用菜单栏的 “文件->复制”选项达到同样效果。

有了数据来源，便可在安全 U 盘中的其他文件夹下使用“粘贴”选项将数据

源复制到指定目录。

注意：

- 您无法通过“复制”功能复制安全 U 盘内的文件/文件夹到操作系统的任何文件夹，此时应使用“拷出”功能替代。

2) 粘贴

通过安全 U 盘程序的“复制”选项选定数据来源，或是在操作系统中通过鼠标右键菜单的“复制”、Ctrl+C 选中了数据来源，就可以通过“粘贴”选项复制数据到安全 U 盘的当前目录。

注意：

- 在通过鼠标右键菜单的“复制->粘贴”、键盘的“Ctrl+C->Ctrl+V”来选择的数据源，可以通过“粘贴”功能复制到安全 U 盘的当前目录。
- 通过在操作系统中选中文件/文件夹然后鼠标拖拽到安全 U 盘文件列表上，然后释放拖拽，安全 U 盘软件就会自动复制文件/文件夹到安全 U 盘内的当前目录

3) 拷出

在安全 U 盘中选中需要拷出的文件，点击右键菜单的“拷出”选项或是菜单栏的 “文件->拷出”选项；

在拷出路径选择对话框中选择拷出的目标路径，点击“确定”按钮，即可开始拷出数据。

4) 新建文件夹

在当前目录下新建一个名为“新建文件夹”的文件夹，如果当前目录下有已

有同名文件夹将会自动重命名。

5) 创建启动项（仅 Windows）

为安全 U 盘内的可执行文件(如.exe 文件)生成一个可双击运行的快捷方式，并允许设置运行的一些相关参数。

在安全 U 盘程序的文件浏览列表中选择一个需要创建启动项的可执行程勋；点击“文件->创建启动项”，设置好相关参数后，点击“确定”按钮即可在当前目录下创建一个指定可执行程序的启动项。

具体参数请安需求设置，设置界面如图 5.2 所示。

图 5.2 创建启动项界面

6) 重命名

修改选中文件/文件夹的名称。若新的文件名与已有的其他文件的名称冲突会弹出“重命名失败”的提示对话框，此时应更换新的文件名。

7) 删除

在单选或多选选中文件/文件夹后，可使用右键弹出菜单的“删除”选项，将选中的文件/文件夹删除。

也可使用菜单栏的 “文件->删除”选项达到同样效果。

警告：

- 被删除的文件/文件夹将直接销毁，一旦删除就无法找回。请谨慎操作。

2. 属性

当未选中任何对象，点击“属性”菜单按钮，会显示安全 U 盘信息，包括安全 U 盘容量与当前可用容量（如图所示）。

若选中文件/文件夹的属性，点击“属性”菜单按钮，包括其名称、位置、大小、创建日期、修改日期（如图 5.4 所示）。

Windows 环境　　Linux 环境

图 5.3 安全 U 盘空间信息

注意：

- Windows 环境下，可以在“属性”界面设置文件/文件夹的“只读”、“隐藏”属性（如图 5.3 所示）。

Windows 环境　　Linux 环境

图 5.4 文件属性界面

3. 视图（仅 Windows）

在 Windows 环境下，安全 U 盘程序提供三种不同的文件浏览视图，分别对应 windows 文件资源管理器内的“中等图标”、“平铺”、“详细信息”三种显示模式。

4. 导航（仅 Windows）

在 windows 环境下，可以通过在软件的地址栏输入目标路径，点击“转到”按钮，实现快速跳转。

商标声明

智权盾为广州极智信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受广州极智信息科技有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，广州极智信息科技有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。