
铁卷电子文档安全系统 FAQ

深圳市大成天下信息技术有限公司

ShenZhen Unnoo Information Tech., Inc.

二〇一一年一月

声明：本文档是深圳市大成天下信息技术有限公司(简称大成天下)解决方案的一部分，版权归大成天下所有，任何对文档的修改、发布、传播等行为都需获得大成科技书面授权，大成科技保留对违反以上声明的组织或个人追究责任，直至诉诸法律的权力。

1. 铁卷基本问题

铁卷的运行原理是什么？

铁卷采用的原理是内核文件实时透明加解密，在操作系统底层对文件进行加解密操作，不影响人员的原有使用习惯。安装铁卷的用户在使用文件时，运行于驱动层的用户终端自动将文件实时加解密；文件的接收者必须经过管理中心端的认证，才能够根据许可权限对文件进行操作。

所有的文档在用户创建、修改、保存时自动加密，完全无需用户手动操作。

铁卷是否支持多语言版本？

支持。铁卷设计的时候充分考虑了未来对多语种的支持，目前支持简体中文、繁体中文及英文版。如果有客户需求，可以在很短的时间内满足对其它语种的支持。

铁卷采用的加密方式安全吗？

铁卷默认采用的是业界最先进的 AES 256 加密算法，该算法获得过多项国际认证，并且该算法运算速度快、资源消耗低，已经成为包括金融、电信、政府等各行各业公认具备高安全强度的加密算法。同时，铁卷还能够让用户自行选择如 RC4、RC6 等其它加密算法。

可以在铁卷系统中直接找到加密的密钥吗？

铁卷系统的私钥已经经过高强度加密，在现有的计算能力下，即使使用高性能服务器也无法破解。

用户将文件的扩展名更改（例如将 **1.doc** 改为 **1.abc**）后拷贝回家，此时文件是否仍然处于加密状态？

是的。铁卷是在内核中对文件进行全文加解密操作，因此无论扩展名改成什么，文件内容始终是加密的。

用户将文档另存为其它格式，铁卷能保护吗？

可以，凡是受保护的文件，另存为其它格式（例如：html、txt、xml、jpg 等等）时，均会受铁卷控制，以加密形式储存，绝无泄密困扰。

铁卷能否防止用户拷贝粘贴？

可以。铁卷的防拷贝设计十分贴心，您只是无法从受信任进程（例如 OFFICE）文件将文字或图片等内容往非受信进程（例如 notepad）中拷贝，也无法采用各种应用软件特有的拖拽等机制将文字拷出。

但您仍然可以从非受信进程（例如 Web、txt 文本）将文字或图片拷入受信任进程中，也能够在受信任文件之间相互拷贝，这极大提高了使用的方便性和透明度。

铁卷能否防止内存转储？

可以。铁卷通过以下几种技术手段：

- 禁止 Windows 系统中的多种内存转储指令；
- 内存分段安全化处理；

能够有效防止内存转储，保证安全最大化。

铁卷能否防止各种截取屏幕的软件？

可以。铁卷支持超强型截屏防御，从设备驱动底层直接阻断屏幕截获的请求，全球上千种屏幕捕获录像软件均无法捕获正在打开的被保护文件屏幕内容。

铁卷能否控制非授权的文件打印？

可以。铁卷可以设置仅允许用户在管理中心注册的打印机上进行打印操作，并且能够控制虚拟打印机输出，有效防止用户将文档打印成 OCR、FLASH 等格式后传播扩散。

如果用户修改了程序的名称，例如：将 Office 中的 Winword.exe 改名为 a.exe，这时运行 a.exe 创建的 Word 文档还能加密吗？

可以。铁卷并不仅仅根据文件名称来进行可信进程判断的，而是综合多种特征进行判别，最大程度保证安全性。

如果用户在保存文件时设定了自己的后缀名，比如 **Word** 文档不保存为 **.doc**，而是保存为 **.abc** 时，是否仍然能够加密？

可以。应用铁卷后，受保护的应用程序产生的输出，无论后缀名是什么，都会受到保护。

如果用户将电脑做了 **Ghost** 镜像后，铁卷是否还能起到保护作用？

可以。铁卷在安装时会根据硬件信息生成唯一验证串后由服务器存储，如果将电脑做了 **Ghost** 镜像后在另一台机器恢复，由于硬件信息变化，将无法接入服务器并解密文档。

铁卷能否防止用户以“插入对象”的形式带走文件？

可以。铁卷对包括 **Office** 在内的多种应用程序中“插入对象”的功能进行了深入研究，可以完全控制对“插入对象”方法的安全控制。

铁卷能否防止一些内核工具禁用内核钩子后导出明文文件？

可以，铁卷通过对内核钩子运行结果的判断，可以防止内核工具单独禁用铁卷的某些功能。

铁卷是否可以将所有的加密文件批量解密？

铁卷可以在系统管理员提供正确的硬件标识、密钥的情况下将加密文档批量解密。但为了保证系统的安全性，批量解密功能组件在一家企业只能由信息主管持有，并且需要授权使用。

打开文档时的速度延迟如何？

打开文档时，铁卷将把解密后的数据递交给应用程序，解密的速度延迟跟铁卷所使用的加密算法和您使用的计算机硬件有关。经过我们测试，在使用 **AES 256** 算法，**Pentium III 1G, 256M** 内存的情况下，打开一个 **3M** 的 **DOC** 文档的延迟大约是 **0.3** 秒，几乎不会对您的体验产生任何影响。

铁卷的心跳监测，那对网络性能影响如何，会产生多大的网络流量？

在产品完全部署后，一个客户端每 5 秒产生一个字节的心跳信息，那么一个 **200 个客户端**的部署环境在一个小时内大约将有 $(60*60/5)/8/1024*200 \approx 17M$ 的非并发流量产生。这对于一个 10/100M 的 LAN 来说，几乎不构成任何压力。

铁卷的用户终端（Agent）能否在 UNIX 系统上使用？

暂时不能。目前铁卷采用的是在内核中对文件进行加解密，虽然理论上可行，但目前暂时没有成规模的需求，因此 UNIX 终端的开发计划尚未启动。

我的 U 盘插入后会不会把相应的文件加密不能在其他地方使用？

答：当优盘插入后不会加密里面相应的文件，但是当打开优盘里面的文件做了修改后就会被加密。如果需要安全级别设置很高，也可以做到打开文件不修改关闭后就加密。可灵活的根据需要修改。

我总是对外发送大量文件，需要每次都去解密，这样很麻烦，有什么解决方法没有？

答：对于经常外发的部门或者个人，可以设置为自己解密文件的权限，不需要申请，自己解密要外发的文件，我们对他的操作做记录以便日后审计。根据我们的经验，对有些部门设置专门对外的人员，有要外发的文件都由专人外发。这样就更好控制，好追查。

U key 万一被盗或丢失，能让他失效吗？

答：U key 在设置的时候就可以设置有效期，一般给 1 到 2 个月，到期了就不能用，需要管理员重新授权，所有丢失后也不用担心。另外我们的 U key 还有私人使用密码，别人捡到了也不知道密码，就算是自己公司的人拿到了想自己用，不知道密码也是无法使用的。每个 U key 使用者都可以自己修改自己的 U key 密码。U key 的安全性是非常高的，建议出差、和笔记本用户配备。

我要把保护文档内的内容粘贴到邮件发出去，岂不是也能泄密？

答：从我们保护的软件复制内容到没有保护的软件里面是被禁止的。例如保护了 word 和 excel 那么 word 和 excel 之间是可以相互复制的，word 和 excel 的内容是不能复制到邮件或者 QQ 等没有保护的软件里面的。也就是说只能进不能出，外面的内容随便复制到 word 和 excel 里面。

我用内部网里的 QQ 发送保护文档的内容行不行？

答：保护文档的内容也不可以复制到内部网里面的 QQ，如果能确保内部网的 QQ 使用安全，不能将信息发送到互联网，或者全公司都装了防泄密系统。那么也可以把内部网 QQ 添加到保护软件列表。那么就可以复制内同到内部网 QQ 里面去发送了。

文档之间能互相粘贴吗？

答：受保护的软件文档之间是可以相互复制粘贴的。

用引导盘启动，把硬盘里边的文档复制出来能用吗？

答：引导盘启动把文件复制出来也无法打开。因为文档在加密的时候采用防泄密系统重新编码了，没有得到解密，拿出去打开也是乱码。

必须要用 Ukey 才能解密吗？

答：解密的权限是有管理员配置的，Ukey 只是做客户端的认证，并没有解密文件的功能。普通员工要解密文件只能申请，公司领导要解密文件可以由管理员配置权限，让领导能自己解密文件。

Ukey 能只解密指定机器吗？

答 Ukey 可以指定在某台机器上使用。但是不能解密文件，只是身份认证的功能。

能够按照部门类型设置不同策略吗？

答：可以按照部门设置不同的策略，还可以按照单独的个人设置不同的策略。

能够设置组织结构和部门分支吗？

答：可以设置组织结构，可以划分部门和子部门。一个员工可以属于 A 部门也可以属于 B 部门，灵活分配。

UKEY 是否视同在线？

答：是的，就是当电脑连不上服务器了客户端不能得到认证，这时候插入 UKEY 然后输入自己的使用密码就能使用。

要 Ukey 的目的何在？

答：UKEY 的用处就是在电脑连不上服务器的时候提供离线认证的功能。

有些销售人员没有电脑，但经常在外地接收公司邮件如何处理？

答：对于这种情况建议解密后发出去，否则外面接收到不能使用。

员工要带文件回家工作如何处理

答：解决办法是解密回家使用，但是存在安全隐患。另外就是在员工家里电脑上安装客户端，使用 UKEY 认证。但是这样可能会造成员工将自己的私人文件也加密。

高管电脑如何处理？

答：高管电脑上可以设置允许自己解密文件这样他们要解密文件就不需要申请。但是会记录日志。

2. 铁卷部署问题

跨地域的公司是否可以通过部署铁卷来同时保障多个分支机构的安全？

可以。铁卷是采用 client-server 的架构模式，只要配合一定的网络设置，就可以让处于不同地点的分支机构同时使用铁卷。

铁卷的服务器是否可以架设在公网上？

可以。

铁卷服务器是否允许用户通过 VPN 拨入后进行验证？

可以。

不同公司部署的铁卷管理中心是否可以通用，会不会造成安全问题？

不会产生安全问题。因为铁卷会根据管理中心服务器的机器码经过运算得出一个认证码，不同的管理中心生成的用户终端及其密钥都是不同的。因此不同公司部署的铁卷之间无法相互接入，也无法解开彼此的加密文档。

怎样查看用户 PC 机上铁卷用户终端的版本？

只有铁卷管理员能够通过管理中心查看客户机上安装的铁卷用户终端版本号，详见下图：

IP地址	别名	当前用户	操作系统	终...	程序版本	允许接入
192.168.0.45	win2kpro	Administrator	Windows 2000	在线	1.1.1010	允许

怎样升级客户 PC 机上的铁卷用户终端？

在终端列表中右键点击一台在线终端，选择“升级终端程序”菜单，见下图：




选中由管理中心创建的的新版本终端程序“terminal.exe”后点击确定即可。升级完毕后客户 PC 机会弹出重新启动计算机的提示，当完成重启操作后，升级完成。

有位员工马上要离职了，我可以现在就禁止他阅读文档吗？

可以。在管理中心选中该员工的主机，右键单击后弹出如下菜单：



这时选择“拒绝接入”，当您看到该员工的电脑图标变为桔色 192.168.0.45 后，则该员工的阅读权限已经被取消。

铁卷的管理中心能否开放给外部用户使用？

可以。铁卷采用标准的 TCP/IP 协议进行通讯，如果您有外部用户需要接入，需要他有对外的 IP 地址，并且需要在防火墙上开放铁卷应用的端口，就能够正常接入。

我们采用了 XXX 杀毒软件，为什么会出现病毒提示？

因为铁卷采用了操作系统底层的文档安全防护技术，在这种情况下，会有少量杀毒软件的“启发式检测”功能产生误报。这种情况下需要在防病毒软件的中央服务器上设置铁卷的用户终端程序为可信程序即可。

在目前我们测试的二十多种杀毒软件中，仅有一种软件（NOD32）会产生类似的误报。

如果将来我们要卸载“铁卷”，如何对所有加密文档解密？

安装“铁卷”正式版后，应先通过主界面菜单中的“导出 KEY”将密钥导出并保存。需要批量解密的文档时候，使用我们提供的解密工具将保存的 KEY 文件导入，就可以批量解密了。KEY 文件被导出时可设置密码，所以别人在不知道密码的情况下，即使拿到了 KEY 文件和解密工具，加密文档也是安全的。

大规模部署“铁卷”前应该注意什么？

“正式版”的 License 由 Center 导出的注册文件 (.inf) 产生，安装完成后自带的 License 只允许 5 个终端连接。故安装“正式版”后应立即获取正式的 License 文件并导入。

“正式版”的 Center 端程序导出的 Key 文件内包含密钥信息，直接关系到加密文档是否能被解密，所以需要在安装 Center 后立即导出并妥善保存，以便在需要的时候可以批量解密文档。

由于每个 Center 安装时根据 USBKEY 信息产生密钥，所以若在多个部门部署多个 Center，且各个部门文档需要互通，就必须在安装第一个 Center 后导出 Key 文件，并在安装其他 Center 后分别导入，这样才能保证所有终端均采用相同的密钥加密文档。

如果我们的网络或服务器发生意外中断，“铁卷”有什么应急措施吗？

服务器方面，若需要保证不间断服务，建议同时在服务器 A、B 上安装“铁卷”。平时只启动 A 服务器上的 Center 程序，并定期备份配置信息。当 A 服务器发生故障时，将 USBKEY 换到 B 服务器上，立即启动 B 服务器的 Center 程序并导入配置信息，随后将 B 的 IP 地址更改为与 A 相同即可。

网络方面，若某些终端由于意外原因无法连接到服务器，可通过终端任务栏图标的右键菜单切换至“USBKEY 模式”。这时只要插入有效的“USBKEY”，终端程序便可正常工作，与连接到服务器无异。当故障排除后，可切换回常规模式，并收回“USBKEY”。

合作伙伴无法提供一台专用的 PC 让我们安装用户终端怎么办？

如果合作伙伴的 PC 上还需要执行其它任务，无法专用时，可以采用专用的 USB Key 来实现文档共享并且禁止传播。当 USB Key 插入电脑时，合作伙伴可以打开加密文档，但此时新建、复制、另存的文档全部是加密文档，因此无法再传播。当 USB Key 拨下后，所有加密文件就无法被打开。但此时用户新建的文件均为不加密文件，可以不影响合作伙伴电脑的正常运作。

未安装铁卷用户终端的计算机是否无法正常打开铁卷文档？

是的，在使用未安装铁卷的计算机上打开已经加密文档的时候，会出现乱码的情况，无法正常查阅文件内容。

但需要提醒的是：在安装铁卷客户端的计算机打开加密文件如 word 文档时，可能将文档中的某些乱码符号当作换行符处理。此时**请不要**将此文档保存。否则可能导致文档永久损坏。

客户端生成新的策略时要不要重新启动客户机？

客户端生成新的策略升级客户端后会提示客户机重新启动，但没有强制重启。但由于多数策略部署是需要要重新启动系统的，建议您在部署新策略后重新启动客户机。

3. 终端用户常见问题

安装用户终端后，我要如何使用铁卷？

铁卷的用户终端完全无须用户干预，因此核心驱动设计成为没有用户操作界面，仅有一个申请离线功能需要用户干预，因此您可以完全不用考虑使用问题。它的系统资源占用非常小，用户几乎不会发现它的存在。它对使用者来说是完全透明并且无法由用户自行终止的，会随 Windows 系统自动启动。客户端的加密文件类型、访问方式、离线策略由服务端控制。

若需要向别人提供不加密的文档，应该如何处理？

在“我的电脑”中找到需要提供给别人的文件或目录，在右键菜单中选择“解密申请”，需要解密的文件名会发送至服务器，管理员审批后文档即被解密。

我们公司业务复杂，系统管理员并不能清楚了解每个部门的文档密级情况，没办法有效地进行审批操作，是否有解决办法？

可以很好的解决。铁卷允许每个部门设置代理管理员，由该代理管理员执行解密申请和离线申请的审批操作。

为什么刚刚被解密的文档，我通过 U 盘复制给别人，依然无法打开？

管理员创建 `terminal.exe` 时，若同时设置了“强制加密以下类型的文档”和“复制时强制加密”，则在向 U 盘中复制特定后缀名的文档时会再次加密。对于需要向外传递解密文档的机器，创建 `terminal.exe` 时应该去掉“复制时强制加密”的选项。或者先将文档复制到 U 盘后再发送解密申请。

我必须带着笔记本电脑出差一段时间，怎样才能正常访问文档？

铁卷支持离线申请功能，用户如果需要携带笔记本电脑出差或加班，只需要通过用户终端进行离线申请，在管理中心批准后，即可以批准时间段内离线正常访问文档。

若员工需要出差或回家加班，同时又想保证文档不外泄，应该如何处理？

对于笔记本电脑，只要发放 USBKEY，出差或回家后将终端程序切换至“USBKEY 模式”即可。

对于台式机，需要管理员先创建一个特殊的 `terminal.exe`，配置为只通过 USBKEY 验证，不连接服务器。需要在家中打开加密文档时，只要插入 USBKEY 并运行这个 `terminal.exe` 即可，拔出 USBKEY 后 `terminal` 程序会自动退出。需要注意的是，`terminal.exe` 运行期间，可以打开加密文档，但同时也自动加密所有新建和被修改的文档，所以 `terminal.exe` 运行期间不要同时处理私人文档，否则会被加密。

安装铁卷之后，我要如何将文档发给我的合作伙伴，并且禁止他们传播？

通常情况下，需要合作伙伴设置一台专用 PC：

- 1) 该 PC 上已经安装好相应的软件（Office、AutoCAD、Acrobat PDF 等）；
- 2) 运行注册程序，将生成的硬件码发回给您；
- 3) 根据该硬件码生成一个专用的用户终端；

用户运行该终端程序后，就可以打开您发送的加密文档，并且无法将这些文档再次发布和传播。

为什么我的离线功能突然失效了？

请您确认是否对电脑时间做了回调操作。当电脑处于离线状态时，不允许对机器时钟进行回调等操作，如果铁卷判断到有类似操作，便会立即禁用离线阅读功能。

这时只能接入重新接入网络，铁卷用户终端会与管理中心自动联系，这时您可以重新发送离线申请。

为什么我不能卸载铁卷？

由于铁卷要执行对电子文档的“强制透明保护”，因此在驱动层将文件、注册表和进程进行了保护，只允许管理员通过管理中心从远程卸载，或者在用户机器上输入密码验证通过后卸载。用户一旦卸载铁卷，将无法打开企业内部的任何加密文档。

客户端装完铁卷，是否会将电脑上的全部文档加密？

当然，这可以确保所有用户机器上的文档都处于加密状态，没有泄密的可能。

在我当前电脑上，如何判断一份文件是否已经被铁卷加密过呢？

因为铁卷的透明机制，普通用户在使用时完全不改变习惯，因此无法察觉文件已经被加密。如果系统管理员希望察看某份文件是否被加密，可以采用 UltraEdit 或类似的十六进制编辑器打开该文档，通过察看文件头来判断文件是否已经被加密。

如果操作系统重装，那么已加密的文件还能打开吗？如果不能，重新设置是否麻烦？

不能，但只需重新安装一下客户端即可，无需做任何设置。

客户端安装好后，为什么不能和铁卷服务端正常通讯？

- 检查服务器上 2000 端口是否打开，在服务器上运行“程序→附件→命令提示符”，使用命令 telnet 127.0.0.1 2000 测试端口是否开放；

- 如果在服务端测试端口是正常的，那么可能是 Windows 自带的防火墙或者是安装了一些防火墙产品阻止客户机与服务端 2000 端口通信，通过设置防火墙打开 2000 端口；

4. 试用用户常见问题

“体验版”与“正式版”的区别是什么？

“体验版”与“正式版”在功能和加密算法方面都完全一样。主要区别是“体验版”使用默认的固定密钥加密，可以用我们公开的通用解密工具批量解密。“正式版”使用 USBKEY 产生的唯一密钥，被加密的文档无法使用通用工具解密。

我们试用完铁卷，将程序卸载了，但在试用期间操作过(创建、打开、复制等)的文档，都被加密了，怎么办？

由于铁卷的保护机制极其完善，在安装完软件后，所有操作过的文档均会被透明加密，这可以确保文档不会因为意外情况导致泄露。因此我们建议您不要在生产机上直接对软件进行测试，或者至少测试前将可能测试过程中可能使用到的文档先进行备份。如果您事前没有进行备份，也可以直接联系给您提供试用软件的经销商。

我们试用完铁卷，将程序卸载了，但某些机器打开 Office 文档时会提示“模板已损坏”，这是怎么回事？

因为每次打开 Office 文档时，均会对 normal.dot 进行操作，因此该文件会被铁卷加密。但如果我们设定不对该文档加密，又有可能导致一个 normal.dot 成为一个“泄密渠道”，即：恶意用户有可能将每个文档另存为 normal.dot 后再转寄出去，而系统不加干涉。考虑到上述可能存在的风险，我们采用了严格的策略，截断所有明文文件外泄的可能性。

当您遇到这类提示时，只需要点击“是”，Office 便会采用系统内置的文档模板替换当前模板，下次再打开文件时，就不会出现该提示了。

客户端装完铁卷，要怎样才能判断出文档的加密效果？

因为铁卷的使用完全透明，因此安装后并不影响用户的日常使用，要判断出铁卷的应用效果，您可以按以下流程测试铁卷功能：

1、创建一份新的 word 文档

2、检验文件防拷贝功能

- 将该文档复制到另一台电脑的 windows 共享目录，文档将被加密；
- 通过 email 将文件传出到未安装铁卷的电脑上，文档将无法打开；
- 将文件复制到 U 盘或移动硬盘，到未安装铁卷的电脑上打开，文档将无法打开；

3、文字防拷贝、防截屏功能

- 打开任意 word 文档后，选中一段文字，打开记事本，复制文字后尝试粘贴到记事本中，文字将无法复制；
- 采用 PrtScreen 键或任意截屏软件，尝试截取当前 word 文档的图片，将无法下载截取图片；