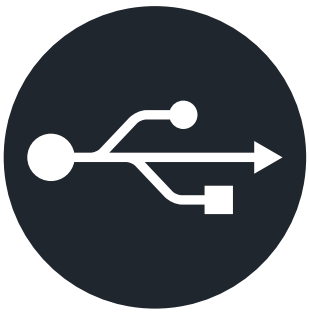
如何启用 USB 闪存盘访问权限
而又不危害端点安全性

#KingstonIsWithYou #KingstonIronkey

简介

1996 年 1 月，正式的 USB 1.0 规范发布，无论是对于外围设备供应商而言，还是对于最终用户而言，这都预示着一致性、便利性和通用性时代的来临。27 年后，USB 保持着对每个版本的向下兼容性；从服务器到智能手机，USB 作为计算机硬件接口的基石生存下来了。



凭借即插即用的简易性和不断提升的速度，USB 便携式存储设备已成为最大赢家之一。然而，考虑到数据安全性，这种便利性有利有弊。在当今世界中，如果不在主机上使用端点保护等合适工具并采用合适的数据安全实践，漫不经心使用便携式 USB 存储的用户可能导致自己和他人暴露于潜在数据泄露风险之中，而这可能让最终用户付出高昂代价，甚至可能危及整个组织或政府。

除了保护主机环境，也应使用密码保护并在设备上通过硬件对 USB 闪存盘进行加密。这样可以实现最强大的入侵防护。我们将详细介绍一些关于如何更安全地使用 USB 闪存盘的最佳实践，以及关于 USB 闪存盘一般性问题的深入洞见。

尽管最理想的是综合性方法，而加密的可靠性和 USB 闪存盘自身的硬件组件至关重要。从金融到医疗保健，再到制造和军事，USB 闪存盘造福了各行各业。在网络访问不可用、易受攻击或不实用的远程办公中，USB 闪存盘也发挥了作用。

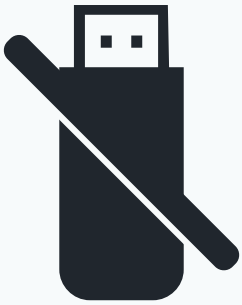
USB 硬件加密闪存盘包含不同的认证等级，并提供一系列的安全特性。通过考察它们的属性和定制机会，可以发现，它们在各种敏感环境中的巩固地位也证明了它们作为独立解决方案的适合性。

接口权限：USB 存储与端点管理数据丢失防护软件

数十年来，防病毒和防恶意软件应用程序在最基本的层面提供了保护 – 自动扫描下载文件和连接的设备，并报告可疑内容或对其采取行动。新一代防病毒 (NGAV) 软件提供的防护则更进一步。NGAV 并非仅仅依靠持续更新的病毒特征数据库，而是添加了机器学习和行为检测功能，可以识别并规避未知威胁。

这并非军械库中的唯一武器，对于需要针对用户外设等设备提供防弹级防护的用户，端点管理数据丢失防护 (DLP) 软件提供了多种方法，可拒绝对 USB 接口和其他接入点进行任何形式的访问。

“阻止全部接口”的安全态度无疑会消除风险，在一些情况下可能具有可取性，但这种政策可能常常被证明盲目性很大，后果不如人意。



然而，一些 IT 管理员倾向于拒绝在用户机器上启用 USB 接口的请求，因为在这些端点上这样做将允许穿过企业防火墙进行直接访问。这份谨慎心态是可以理解的，但在启用 USB 存储访问权问题上，只要遵循特定的先决条件，提供这项权限并不一定会造成巨大的安全问题。

其中一项基本要求是使用端点管理应用套件，该套件应包含防病毒/防恶意软件解决方案的威胁检测扫描功能，以及对所有用户端点进行集中监控和管理的功能。

一般而言，这种简单的方法以各种形式存在于主要供应商的统一解决方案中，例如 McAfee MVision、Sophos Intercept X、Symantec Endpoint Security、Trend Micro Smart Protection 和 WinMagic SecureDoc 等等。

白名单的改进

在保护 USB 存储设备问题上，要部署的方法取决于要求的防护等级。这里可以采用一个简单而有效的方法，即使用 USB 存储设备各自的供应商标识符 (VID) 和产品标志符 (PID) 值将该设备加入白名单。对于所有 USB 外设而言，每家制造商都有一个唯一的 VID，但发布的每款新产品都有不同的 PID。

对于白名单，仅使用制造商 VID 会过于宽泛而无法保证安全性，因为某制造商曾生产的每个 USB 设备都会获得批准。PID 提供了进一步改进，要求只有一个特定型号能获得访问主机系统的权限。

尽管这实现了改进，但仍不完美。USB 存储设备极受欢迎，因为这让用户可以自己准备与授权型号匹配的设备。不要忘记，金士顿科技提供一款定制解决方案，可以加强 USB 存储设备的安全性。

通过定制计划可以创造组织专属的 PID 配置文件，应用于一系列金士顿加密 USB 闪存盘。通过部署采用定制产品标识符的设备，公司不仅能受益于简化的白名单机制，还能大幅增强安全性。如果缺少匹配的定制 PID，即便员工独自购买的设备看似相同，也会被拒绝访问。

利用定制 PID，IT 管理员可以快速轻松地让新 USB 存储设备投入使用，但还有一种更精细的替代方案，那就是使用多数金士顿加密 USB 闪存盘带有的独特设备序列号。这种安排要求每个唯一设备序列号在端点管理

套件中进行注册。一开始，这需要 IT 员工进行处理，而金士顿可以为每个订单提供一个序列号列表，这些序列号总是非连续的字母数字。选择这种方法，可以根据各个闪存盘的所有权实现更加灵活的政策，而且还可以对设备进行精确的源头跟踪，这对于取证 IT 应用可能非常重要。一些 Kingston 闪存盘确实在外壳上包含了用于电子扫描的序列号和和条形码，其他闪存盘可以通过定制在外壳上添加条形码和序列号，并用于商业；这些都可以用于闪存盘跟踪。

默认情况下，端点管理系统提供 VID/PID 的访问权限，以支持接口阻止和白名单功能。金士顿提供更通用的方法来利用这些功能，可以实现更具包容性和创造性的策略，促进 USB 存储设备的使用。通过建立合适的识别方法，一刀切式的“☒阻止全部接口”的立场不仅过于简单化，而且也变得毫无必要。

面向远程用户的安全、合规的解决方案

在安全性问题上，把设备加入白名单仅解决了一半的问题，或者说只是一半的解决方案。

得益于自身的便利性和易用性，USB 存储设备成为许多企业和机构不可或缺的设备，在这些组织中，便携性是流畅数据传输的关键。在多数环境中，由于合规和良好 IT 卫生的缘故，有必要在此类工作中为员工配备加密 USB 闪存盘。通过综合利用密码保护和设备加密，一旦设备丢失、失窃或遗留在易受攻击的环境中，便携式存储设备会得到安全保护，阻止对敏感的数据进行访问。

由于加密技术各不相同，这并非万能解决方案；对软件加密解决方案和硬件加密解决方案进行比较，就会发现最显著的差异。那么，哪种更好呢？这取决于您的需求，但更深一步的问题应是“哪种更安全？”

软件加密基本上是实惠的选择，能够满足一些运营规模较小的行业。如果企业的数据传输不具有敏感性，并更加关注合规问题，那么也适合进行软件加密。

然而，软件加密的独特工作方式也是它的致命要害，因为它所需要的面向客户的应用依赖计算机执行加密任务。因此，由于这种关联性，软件加密的存储设备最多与主机一样安全。

随着获得计算机内存访问权限的黑客可以“嗅探”加密/解密密钥，漏洞风险也会加大。如果可以访问和复制加密的文件，闪存盘中的数据也可能遭到暴力破解攻击，因为这不需要密码访问防护。

记住，基于软件的加密很可能需要不时地进行软件更新，这会给 IT 员工带来额外负担，从而可能导致实施复杂化。最糟糕的是，如果员工在闪存盘的跨平台便携性方面遇到问题并遭受挫折，就可能完全移除软件加密。闪存盘用户可以将加密闪存盘中的数据复制到计算机，将闪存盘重新格式化为非加密闪存盘，然后再将数据重新复制到闪存盘。这时，数据会失去保护，面临全面的泄露风险。出于遵从数据隐私法律法规的目的，这种做法不可接受，因为 USB 闪存盘的安全性功能事实上被禁用了。

芯片上的加密：可靠、高效的解决方案

相比之下，硬件加密的 USB 闪存盘独立于计算机运行，得益于物理闪存盘中嵌入了一个专用处理器，用于管理加密。它具备始终在线的加密流程，可以防范暴力破解密码攻击；加密的数据无法被访问，也无法被复制。

Kingston 的企业级和专业级硬件加密 USB 闪存盘采用 XTS 模式下的 AES-256 硬件加密。作为一项获得全球认可的加密技术，AES 256 位提供了严格缜密的数据保护。通过在加密/解密流程的不同阶段使用两个独立的密钥，XTS 模式实现了类似两次加密数据的效果。

使用时，用户的密码解锁闪存盘控制器的随机数生成器，该生成器生成加密密钥。由于身份验证在设备的加密硬件中完成，加密密钥和其他关键安全功能得到保护，能够防范常见漏洞，例如 BadUSB、冷启动攻击、恶意代码和暴力破解攻击。

硬件加密最直接的一个优势在于，闪存盘性能较软件加密闪存盘大幅提升，得益于无需将加密任务转移给主机。一切操作都在闪存盘中完成。

Kingston IronKey D500S 等硬件加密 USB 闪存盘是用密码保护的设备，开箱就进行了加密。使用时，一开始只有写入保护的启动程序卷可见，其中包含用于鉴定密码和解锁主加密存储卷的应用程序。这个程序步骤避免了在主机 PC 上安装任何类型的驱动程序或软件。

此外，Kingston 硬件加密 USB 闪存盘使用数字签名驱动程序，可防止设备内出现任何固件操控。通过添加这个额外的安全层，可以防范 BadUSB 之类的攻击，这类攻击会利用 USB 设备固件内在的漏洞。该漏洞可能导致秘密执行的命令或恶意代码在主机上运行。

当然，“阻止全部接口”的方法可以限制 BadUSB 漏洞危险，但为什么要因为采用这种过时的做法而牺牲生产力呢？正如上文强调的，设立简单的采购和部署程序并引入硬件加密 USB 闪存盘，就能在使用便携存储设备的情况下维持一个安全的环境。

安全合规的远程办公

远程工作者脱离了组织安全工作环境的保护，需要经过修改的策略并重新审视首要工作。

在远程安全计划问题上，仅仅为了让员工通过互联网连接访问服务器来上传或检索文档而屏蔽员工笔记本电脑上的 USB 接口，是否有任何好处呢？在旅途中，唯一可用的可能是一个开放的互联网连接，例如不安全或不受信任的 Wi-Fi 接入点，这可能会引入各种各样的威胁因素，从而大幅增加泄露的风险。威胁可能包括通过欺骗、中间人 (MitM)

攻击和网络窃听实施的数据拦截和监视，而这些仅仅是网络犯罪分子日益复杂的黑客攻击方法的一小部分。即便是 VPN 也会出现漏洞。

组织的互联网连接是另一个端点，与生俱来的风险使其成为极易受攻击的目标切入点。为该连接开放远程访问本身就具有安全风险，尤其是在敏感数据问题上。

为远程办公者配备有密码保护的硬件加密 USB 闪存盘，可以有效地消除潜在的网络漏洞。然而，这种安排需要更仔细地考察可用的 USB 闪存盘，以及它们可以如何满足各个远程办公环境的要求。这并非只是简单地考察闪存盘的存储容量，或闪存盘是否应记录自己的序列号。而应关注设备自身的物理构造。

防篡改保护：可靠选项

这里的主要问题在于，硬件加密 USB 闪存是否具有防篡改特性。设备面对此类干扰的安全性有多强体现在 FIPS 140-3 之类的标准中；FIPS 140-2 包含多个级别，仔细考察了在不使用加密方法的情况下闪存盘物理构造的弹性。

相关的 FIPS-197 认证仅考察硬件加密属性以及 IronKey Vault Privacy 50 系列和 Vault Privacy 80 External SSD 之类的设备，这类设备属于面向企业的型号，数据安全要求未达到专业级。这些闪存盘比较便宜，但缺少防范物理闪存盘篡改的功能。

在 FIPS 140-3 Level 3 认证（待认证通过）中，部署用于揭示设备篡改的方法属于专业级。金士顿向世界各地的企业、政府和军队供应这些 FIPS 140-3 Level 3 闪存盘。

在内部使用环氧树脂对安全所需的所有闪存盘电路进行涂层覆盖，并将内部组件与外壳粘合在一起，可以再建立一道防火墙。打开金属壳将变得非常困难，并会导致内部芯片和其他组件的最终损坏，从而导致闪存盘无法运行。通过涂抹这层坚硬的不透明环氧树脂，篡改重要组件将变成一项几乎不可能的任务。诸如 Kingston IronKey D500S 和 S1000 等设备包含此附加安全措施。

这些设备保护并未局限于物理举措，金士顿 IronKey S1000 让防篡改功能更进一步。IronKey S1000 的内部加密芯片可以检测到任何物理篡改，一旦设备通电，就会立即让闪存盘变得无法使用。依靠硬件加密 USB 存储设备访问和传输敏感文件是务实的举措，可以促成流畅的远程操作并有效确保现场的安全性。

务必对 USB 闪存盘硬件和安全功能进行研究，了解闪存盘是否能满足您的特定需求和用例。您应逐一考察每款 USB 闪存盘，可靠的资格认证有助于您作出决定。无论优先考虑什么，金士顿以经济实惠的价格提供了一系列硬件加密 USB 闪存盘解决方案和定制方案，可满足各种环境的需求：从一般合规一直到最严苛的专业规范。

安全第一：没网络就没问题

今天，办公室失去了边界，随着居家办公不断蓬勃发展，远程访问漏洞问题引起了许多公司的关注。许多公司第一次遇到这些挑战，并在寻找更安全的方法适应这种日益盛行的趋势。

硬件加密 USB 存储设备已得到广泛认可，当由于多个原因导致通过网络传输数据可能不实用或不受欢迎时，这类存储设备能提供安全的解决方案，在众多行业满足这些需求。

在金融领域，监管部门常常要求公司提供数据，以检查公司的行为与合规状况。如果通过网络传输包含投资、市场交易和其他机密银行活动准确细节的敏感文档，暴露风险会非常大，因此这种方法不在考虑之列。一个简单而有效的解决方案就是利用硬件加密 USB 闪存盘交付这类信息。

在医疗保健领域，每一天都会使用安全加密 USB 闪存盘传输文件。这也是为了方便医生们分析文件、在研究中参考文件，或向医学学生演示病例。医学成像设备等专有系统还存在更为实际的需求，这些系统的网络是缺失或不安全的。通过利用合规的硬件加密 USB 闪存盘，可以轻松传输文件并在其他地方使用。

行为规范

✓ **务必使用合规的安全加密闪存盘**，并查阅规格，以采购符合各项部署需求的闪存盘。

✗ **请勿授权随意或个人自带设备 (BYOD) 政策** – 一旦丢失未加密的闪存盘，任何公司都会在财务和声誉两个方面付出巨大代价。

✓ **务必部署端点管理套件**，并使用可提供独特白名单功能的硬件加密 USB 闪存盘。

✗ **请勿碰运气。**妥善评估组织内部环境和远程工作环境的要求。

✓ **务必对员工进行**安全问题培训。公司持续防范安全漏洞也符合员工的利益。

✗ **请勿让安全问题令人感到痛苦**，否则用户会寻求变通方法，而这可能导致用户使用影子 IT 解决方案。一直在应用一刀切式的政策并不意味着它适合所有情形。工作场所在不断改变，通过选择合适的解决方案，可以制定和执行新政策。

在这种情形中，Kingston IronKey Keypad 200 (KP200) 有着显著优势。作为一款独立于操作系统的闪存盘，它没有用于输入密码的启动程序卷，而是配备了字母数字键盘，用于解锁设备以在任何平台上使用。硬件加密 USB 闪存盘如同一把瑞士军刀，应用范围拓展到了制造业；它可以安全地将在 IT 研究和开发领域创作的应用传输到由操作技术 (OT) 平台控制的机械装置。对于包含 Linux 的混合平台操作，KP200 是目前最简单、安全的解决方案之一。

硬件加密 USB 存储设备在执法领域也发挥着重要作用。它们可以保护案件卷宗、图片和其他证据，并将其安全地传输给现场人员、调查小组和法医团队。金士顿支持在闪存盘外壳上印上内部序列号和条形码，带来了额外优势。闪存盘的发放和编目工作变得简单起来，也易于跟踪。只需简单地手动记录序列号或快速扫描一下条形码 – 审计和库存管理从未如此简单。这项特性是 Kingston IronKey D500S、D500SM 和 S1000B/E 闪存盘的标配特性，但通过 Kingston 定制计划也可以在其他硬件加密型号中提供。

安全性和存储移动性：一流技术

密码保护、硬件加密、防篡改防护、精细白名单、专业级 FIPS 140-3 level 3 认证（待认证通过）和记录概览都是 Kingston USB 闪存盘的现成特性，可以立即进行部署，无需等待。

凭借这些强大的安全防范举措，可以确保 USB 闪存盘及其存储的数据在主机环境中依旧安全。书面上的规格看起来令人惊叹，然而，对于一些存在具体要求的组织而言，不做任何研究就随机挑选一个型号，并不一定能提供理想的解决方案。

作为独立制造商，金士顿提供广泛的方案，可满足客户需求。利用金士顿定制计划，可以创建高级解决方案并提供丝滑的用户体验。

安全定制不仅仅是向组织提供组织自己的 USB PID 以用于白名单。启动程序应用的安全配置文件也支持定制，从联系人和公司详情，到启用密码提示和确定最多密码尝试次数，有十五种不同的偏好选项可供选择。在外部，可为特定闪存盘选用公司品牌 (co-logo) 和一系列的颜色。只需至少订购五十件闪存盘，所有这些特性就能为设备部署提供丝滑的集成路径。

如果尚未部署适合安全加密 USB 存储的端点管理应用套件，那些希望管理自己的 Kingston 闪存盘的组织可以选用一个管理解决方案，包括远程重置密码的选项。

各种有前途的技术消逝不见，而普遍性和便利性让 USB 生存下来；对于许多任务而言，USB 存储的直接性和便利性会延续下来。即时可用、始终安全的 USB 闪存盘提供了可迅速获得青睐的简单解决方案。

为什么要担心远程环境中的网络数据泄露问题呢？利用 Kingston IronKey 硬件加密的 USB 存储设备，解决方案触手可及。

如需进一步了解 Kingston 可以如何提供帮助，请访问 kingston.com/ironkey；如有更具体的疑问，请咨询我们的加密 USB 专家。

#KingstonIsWithYou #KingstonIronkey