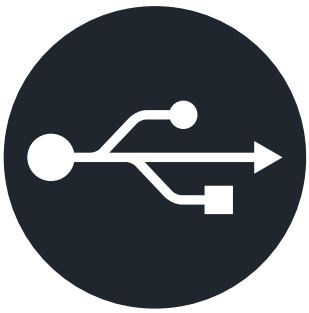
如何允許 USB 隨身碟存取
且不會影響端點安全

#KingstonIsWithYou #KingstonIronkey

簡介

1996 年 1 月所發佈的正式 USB 1.0 規格，為週邊裝置的供應商和最終使用者在統一、便利和多功能等方面開創了新時代。27 年之後，它仍然維持與每個修訂版本的向下相容性，從伺服器到智慧型手機，USB 持續成為電腦硬體介面的基石。



USB 的隨插即用簡單性與不斷提升的速度已經使得 USB 可攜式儲存裝置發展成為最大的贏家之一。但是，考慮到資料安全性，這樣的便利性需要權衡取捨。 在現今的世界中，倘若沒有在主機電腦使用適當工具 (例如端點保護) 以及採取適當的資料安全措施，粗心的 USB 使用者會讓自己和其他人曝露在資料外洩的風險之中，終端使用者勢必要付出昂貴的代價，甚至可能會危害整個企業或政府。

除了保護主機環境以外，USB 隨身碟還應該透過密碼保護以及裝置上的硬體加密來確保安全。如此將提供最強大的入侵防禦能力。 我們將介紹一些更安全的 USB 隨身碟使用方法，同時更深入瞭解 USB 隨身碟。

雖然整合的方法是理想的，但是加密的穩健性以及 USB 隨身碟本身的硬體元件更是重要。金融、醫療保健、製造業和軍方都能因此受益。它們也在網路存取無法使用、有弱點或是不可行的遠端工作中扮演重要角色。

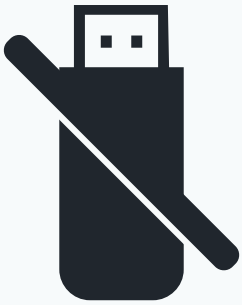
USB 硬體加密磁碟提供不同的認證等級，同時提供一系列安全功能。透過檢查它們的自訂屬性和機會，它們在各種敏感環境中鞏固的地位也證明了它們適合作為獨立的解決方案。

連接埠權限：USB 儲存裝置符合端點管理資料外洩防護軟體

幾十年來，防毒軟體和反惡意軟體應用程式已經提供了最基本的保護 – 自動掃描下載內容以及附加裝置，並且報告可疑內容或是採取行動。次世代防毒 (NGAV) 軟體則提供更進一步的保護。NGAV 的做法並非僅依靠不斷更新病毒識別碼資料，而是增加能夠識別並減輕未知威脅的機器學習以及行為偵測功能。

雖然這不是唯一的防衛武器，但是對於那些希望在使用者週邊以及其他裝置獲得防彈級保護的使用者而言，端點管理資料外洩防護 (DLP) 軟體能拒絕以任何型態存取 USB 連接埠以及其他存取點。

封鎖所有連接埠的安全態度無疑地能夠消弭風險，在某些情況下結果也令人滿意，但是這樣的政策通常會被證明是一種非常不好用的工具，會帶來不良後果。



然而某些 IT 管理員寧可拒絕在使用者機器上開放 USB 連接埠的要求，因為在這些端點上這麼做將會允許透過企業防火牆直接存取。這樣的謹慎是可以理解的，但是在提到可允許 USB 儲存裝置的存取時，如果能夠符合某些先決條件，那麼設定此權限並不會造成很大的安全麻煩。

基本要求是端點管理應用程式套件，該套件具有對防毒/反惡意軟體解決方案進行威脅偵測掃描，以及對所有使用者端點進行集中監視和管理的功能。

一般而言，這種直接且簡單的方法會以各種形式出現在熱門供應商的統一解決方案中，例如：McAfee MVision、Sophos Intercept X、Symantec Endpoint Security、Trend Micro Smart Protection 和 WinMagic SecureDoc 等等。

白名單的改善

每當提到確保 USB 儲存裝置安全，部署方法將取決於所需的保護級別。一個簡單但是有效的方法是利用它們各自的供應商識別碼 (VID) 以及產品識別碼 (PID)，將 USB 儲存裝置加入白名單。對於所有的 USB 週邊裝置，每個製造商都會有一個唯一的 VID，但是每次新產品發行時 PID 會變更。

在加入白名單時，單獨使用製造商的 VID 將會使得保護範圍太過廣泛，因為製造商曾經製造過的每個 USB 裝置都將會獲得允許。PID 提供了更多改進與要求，只有特定模式才會被授予存取主機系統的權限。

儘管已經有所改進，但依舊不理想。USB 儲存裝置廣受歡迎的原因在於它讓使用者能夠自行選購與授權型號符合的裝置。而 Kingston 金士頓提供這些定製解決方案以加強 USB 儲存裝置的安全性。

透過其客製化方案，可以建立企業特有的自訂 PID 設定檔並且應用至各種 Kingston 加密的 USB 快閃隨身碟。倘若公司所部署的裝置擁有量身打造的產品識別碼，不僅能夠因為簡化白名單而獲益，同時也大幅提高了安全性。倘若沒有相符的自訂 PID，即使員工個別購買相同的裝置也會被拒絕存取。

儘管使用自訂 PID 將使得 IT 管理員能夠快速而簡單地將新的 USB 儲存裝置投入生產，但是更細緻的替代做

法是使用個別的裝置序號，這是在多數 Kingston 加密 USB 隨身碟都具有的功能。如此一來，每個唯一的裝置序號需要註冊端點管理套件。 一開始需要 IT 人員介入處理，Kingston 可以提供每個訂單的序號清單 – 這些序號皆包含字母和數字，而且沒有先後順序。 選擇這種方法可根據個別磁碟機所有權提供更具彈性的政策，並加上裝置來精確地追蹤來源，對於 IT 情境而言是極為重要的。 某些 Kingston 磁碟在外殼有包括序號以及條碼以便可進行電子掃描，其他磁碟則可透過客製化為企業在外殼加入條碼與序號；這些資料可用於磁碟追蹤。

根據預設，端點管理系統提供存取 VID/PID 以便進行連接埠封鎖以及加入白名單。Kingston 所提供的是以更多元的方式利用這些功能，提供更加方便和更有創意的策略，便於 USB 儲存裝置的使用。 透過建立適當的識別方法，全體⊠封鎖所有連接埠的立場不僅過於簡單，而且變得不必要。

提供遠端使用者安全且合規的解決方案

在安全性方面，將裝置列入白名單僅能解決一半問題，換句話說，這只是一半的解決方案。

USB 儲存裝置的方便與簡單性使得它們在許多企業和機構中是必不可少的工具，其中可攜帶性是體驗無障礙資料傳輸的關鍵所在。在多數環境中，基於合規以及良好 IT 衛生的考量，工作人員進行此類任務時需要配備加密 USB 隨身碟。 透過結合使用密碼保護和裝置加密，可攜式儲存裝置可在裝置遺失、失竊或處於潛在有弱點狀況時提供保護措施，以避免敏感資料遭到存取。

由於加密技術各有不同，因此並不會有可應付所有情況的解決方案，而且在比較軟體與硬體的加密解決方案時，最明顯的差異便會顯露無遺。所以，哪個技術比較好呢？這需要視您的需要而定，但是更精確的問法應該是：「哪個技術比較安全？」

從本質上而言，軟體加密是一種經濟實惠的選擇，可以滿足某些營運規模較小產業的需求。軟體加密也適用於資料傳輸不被認定具有敏感性的企業，以及與政策合規性密切相關的企業。

但是，軟體加密方式同時也是其致命弱點，因為它需要針對客戶的應用程式，而這些應用程式則依賴電腦來執行加密任務。因此，透過這種關聯性，軟體加密的儲存裝置會與主機電腦一樣安全。

由於可存取電腦記憶體的駭客能夠「嗅探」出加密/解密金鑰，因此暴露於漏洞的機會也越來越大。磁碟上的資料也可能遭受暴力破解，因為如果可以存取和複製加密的檔案，則不需要密碼存取保護。

請記得，軟體型加密可能需要不時進行軟體更新，這可能替 IT 人員帶來額外負擔，進而使執行變得複雜。最糟糕的是，沮喪的員工可能會因為他們對該磁碟機跨平台的可攜帶性存疑，而將軟體加密完全移除。 磁碟機使用者可以將加密的磁碟機資料複製到電腦，將磁碟機格式化為非加密磁碟機，再將資料重新複製到磁碟機。 此時，資料不再安全，且有洩露的風險。 基於遵守資料隱私法律與法規的目的，這種情況是無法接受的，因為 USB 隨身碟的安全實際上會停用。

晶片加密：快速且可靠的解決方案

相比之下，硬體型加密 USB 隨身碟功能則與電腦無關，因為它配備有內嵌於實體磁碟的專屬處理器，可負責加密的管理。它具有隨時提供服務的加密過程，可以防止暴力密碼破解；加密的資料無法存取，同時無法複製。

Kingston 的企業和軍事級硬體加密 USB 隨身碟採用 XTS 模式 AES 256 位元加密。AES 256 位元是一種全球公認的加密技術，可提供嚴格的資料保護措施。透過在加密/解密過程的不同階段使用兩個單獨的金鑰，XTS 模式具有與加密資料兩次相似的效果。

在使用時，加密金鑰是源自磁碟控制器的隨機數產生器，使用者密碼可將其解鎖。由於身分驗證是在裝置的加密硬體中進行，因此可以保護加密金鑰和其他關鍵安全功能，使其免於遭受常見漏洞的侵害，例如 BadUSB、冷啟動攻擊、惡意代碼和暴力破解。

由於沒有將加密任務轉移到主機電腦上，因此磁碟效能明顯優於軟體加密型磁碟，這是硬體加密最直接的好處之一。一切都在磁碟內進行。

硬體加密型 USB 隨身碟 (例如 Kingston IronKey D500S) 屬於密碼保護的開箱即用加密裝置。在使用中，只有寫入保護的啟動器磁碟區才可見，因為它包含用於認證密碼和解鎖主要加密儲存磁碟區的應用程式。此程序避免在主機 PC 上安裝任何類型的驅動程式或軟體。

此外，Kingston 硬體加密型 USB 隨身碟具有數位簽名的韌體，可防止裝置中的任何韌體操作。有了這個額外的安全層保護，可以防止 BadUSB 攻擊 USB 裝置韌體中的固有漏洞。 這可能導致秘密執行的指令或惡意代碼在主機電腦上執行。

當然，⊠封鎖所有連接埠的方法將會限制 BadUSB 遭到利用的風險，但是何必要透過這種過時的做法犧牲生產力？如上所強調，如果採用簡易的採購和部署程序導入硬體加密型 USB 隨身碟，則可以在使用可攜式儲存裝置的同時維護安全環境。

安全且合規的遠端工作

對於遠端工作者，要遠離組織安全工作環境的保障，就需要修訂策略並重新考慮優先事項。

在提及遠端安全計劃時，封鎖員工筆記型電腦上的 USB 連接埠，僅僅為了讓他們透過網際網路連線以存取伺服器，以便上傳或檢索文件，是否有任何好處？外出時，可能只能使用不安全或不受信任的 Wi-Fi 存取點等開放網際網路連線，但這會帶來各式各樣的危險，大幅增加資料外洩的可能性。例如透過欺詐攻擊、中間人 (MitM) 攻擊以及網路竊聽等進行資料攔截和監視的威脅，只是網路犯罪者所利用

日益複雜的駭客方法的其中幾種。甚至是 VPN 也已遭到破壞。

企業與網際網路的網路連線只是另一個端點，固有的暴露風險是極大弱點，也是易受攻擊之處。將網路連線開啟以進行遠端存取有安全風險，尤其是在涉及敏感資料時。

委託遠端工作者使用密碼保護和硬體加密型 USB 隨身碟，可有效消除潛在的網路漏洞。然而，制定此類規定需要仔細檢查可用的 USB 隨身碟，以及檢視它們是否符合每個遠端工作環境的需求。 選擇磁碟機的容量或決定是否記錄序號並不是件簡單的事。 這涉及裝置身的實體結構。

防拆卸損壞設計措施：可靠的選擇

此處的主要問題是硬體加密型 USB 隨身碟是否有防拆卸損壞設計。FIPS 140-3 等標準反映了裝置對這種干擾的安全程度，該標準具有多個級別，可在不使用加密方法的情況下仔細檢查磁碟物理結構的彈性。

相關的 FIPS-197 認證僅遵守硬體加密屬性和裝置，例如 IronKey Vault Privacy 50 系列和 Vault Privacy 80 外接式 SSD 固態硬碟，這些都是企業導向的型號，其資料安全性要求未達到軍事級別。這些磁碟價格便宜，但是缺乏防止實體磁碟拆卸的保護措施。

具備 FIPS 140-3 3 級認證 (申請中)，防止裝置曝露遭到篡改所部署的方法被評為軍事級。Kingston 為全球的企業、政府以及軍事單位提供這些 FIPS 140-3 等級 3 磁碟。

在內部使用環氧樹脂來塗覆所有用於確保安全性的磁碟電路，並將內部組件黏合到外殼上形成另一道防線。想開啟金屬盒是非常困難的，並且會導致內部晶片和其他元件損壞，最終使磁碟機無法正常運作。使用這種堅硬且不透明的環氧樹脂，拆卸重要元件就幾乎變成不可能的任務。Kingston IronKey D500S 和 S1000 等裝置具備此額外安全措施。

這些裝置保護不僅限於實體措施，Kingston IronKey S1000 是將防拆卸損壞設計提升到另一個水準。IronKey S1000 的內部加密可以偵測到任何實體拆卸，並在裝置加電後立即讓磁碟機無法使用。 仰賴硬體加密型 USB 儲存裝置存取和傳輸敏感檔案是一項務實的措施，可促進無障礙的遠端操作，並有效地確保現場安全性。

請確保您已研究 USB 隨身碟硬體與安全功能，以瞭解是否適合您的特定需求和使用案例。每個 USB 隨身碟應該根據個案進行審查，並且提供有助於指導這些決策的可信賴認證。 無論優先級如何，Kingston 都以實惠的價格提供了一系列硬體加密的 USB 隨身碟解決方案和自訂選項，可應對各種環境：從一般合規性到最嚴格的軍事規格皆可滿足。

安全優先：沒有網路，就沒有問題

今日的辦公室已無國界，隨著在家工作的蓬勃發展，遠端存取漏洞問題受許多公司關注。許多人還是第一次遇到這些挑戰，並在尋找更安全的方式來因應此日益成長的趨勢。

硬體加密的 USB儲存裝置已經十分完善，當由於種種原因透過網路進行資料傳輸不切實際或不符合需要時，它為各行各業提供安全解決方案。

在金融領域，監管機構經常要求提供資料以檢查公司的行為和合規性。若使用網路來傳輸投資、市場交易和其他機密銀行業務活動等敏感文件，洩漏的風險實在太大了。 在硬體加密的 USB 隨身碟上傳送訊息是簡單有效的解決方案。

在醫療保健環境使用加密 USB 隨身碟傳輸檔案是常常發生的事。這對想要分析、參考檔案進行研究或向醫學系學生展示案例的醫生或顧問而言，更加方便。 當專有系統 (例如：醫學成像裝置) 無法存取網路或是有安全疑慮時，存在更多實際需求。 透過使用相容的硬體加密 USB 隨身碟，可以將檔案輕鬆地轉移到其他地方使用。

應做和不應做的事

✓ **請務必採用符合規定的安全磁碟**，並且審查規格以採購符合每項部署需求的磁碟。

✗ **不要授權隨機或是個人自攜裝置 (Bring Your Own Device，BYOD) 政策**，對於任何公司來說，遺失未加密磁碟的財務和商譽損失代價太高。

✓ **部署端點管理套件**，並且使用可提供獨特白名單功能的硬體加密型 USB 隨身碟。

✗ **不要把任何事情交給機率。**正確評估本地和遠端工作環境的要求。

✓ **對員工進行**安全教育。公司基於保護自身利益的目的，避免遭受安全漏洞的侵害。

✗ **不要增加執行安全的困難度**，避免使用者尋求變通方法，最終使用影子 IT 解決方案。長期的全面政策並不代表它適合所有情況。 工作場所正在不斷發生變化，透過選擇正確的解決方案，可以制訂和執行新的政策。

在這種情況下，Kingston IronKey Keypad 200 (KP200) 充分發揮了自身特色。作為獨立於作業系統的磁碟機，沒有啟動器磁碟區可以輸入密碼，而是具有包含字母和數字的鍵盤，可解鎖裝置以供在任何平台上使用。 硬體加密 USB 隨身碟就像多功能瑞士刀一樣，它的用途也延伸到製造業；可以將 IT 研發領域中編寫的應用程式安全地轉移到由營運技術 (OT) 平台控制的機械。在同時具有 Linux 功能的混合平台作業方面，KP200 是可用的最簡單的安全解決方案之一。

硬體加密的 USB 儲存裝置在執法方面也發揮至關重要的作用。它們保護案件檔案、影像和其他證據，並將其安全地傳輸給現場人員、偵查隊和法醫小組。Kingston 還有一個優勢就是可以為磁碟機提供內部序號，該序號印在外殼上條碼旁。發行和分類磁碟機變得簡單並且容易追蹤。就像手動記錄序號一樣容易，或者像掃描條碼一樣迅速 – 使稽核和庫存管理的工作再簡單不過。此功能已在 Kingston IronKey D500S、D500SM 和 S1000B/E 磁碟上成為標準配備，但其亦可作為 Kingston Customisation 計畫中的一部分，將該功能用於其他硬體加密型號。

安全和儲存行動性：最先進的技術

密碼保護、硬體加密、防拆卸損壞設計保護措施、精細端點白名單、軍事級 FIPS 140-3 3 級認證和快速記錄是 Kingston USB 隨身碟的現成功能，可立即完成部署。

這些強大的安全防護措施可確保 USB 隨身碟及其資料在其主機環境中保持安全。儘管書面的規格資料令人印象深刻，但在沒有任何研究的情況下隨機挑選型號，並不一定會為某些要求更高的企業提供理想的選擇。

作為獨立製造商，Kingston 提供多種選擇以滿足客戶需求。透過 Kingston Customisation 計劃可以獲得進階解決方案，這些解決方案旨在提供無縫的使用者體驗。

安全定制可以為企業提供自己的 USB PID 以便加入白名單。還可以使用 15 種不同的偏好選項來自訂啟動器應用程式的安全設定檔，從聯絡人和公司詳細資訊到啟用密碼提示以及確定最大密碼嘗試次數。在外觀方面，可以在特定磁碟機印上公司品牌以及一系列的顏色。 最低訂購量為五十台磁碟，所有這些功能為裝置部署提供了輕鬆的整合路徑。

如果還沒有適合安全 USB 儲存裝置的端點管理應用程式，有一個管理解決方案可供希望管理其 Kingston 磁碟機群的企業使用，其中包括遠端重設密碼的選項。

USB 的普遍性和便利性使它遠比各種具有前景的技術更早存在，並且在許多任務中，USB 儲存裝置的即時性和便利性得以持久。隨時可用、始終安全，受到保護的 USB 隨身碟提供可容易體會的簡單解決方案。

何必要擔心遠端環境的網路資料外洩？有了 Kingston USB 硬體加密儲存裝置，答案近在咫尺

如要了解 Kingston 如何提供協助的相關資訊，請至 kingston.com/ironkey；如有更多具體問題，請詢問我們的加密 USB 專家。

#KingstonIsWithYou #KingstonIronkey