Vista组策略保障移动储存设备的安全使用 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022_Vista_E7_BB_84_E7_AD_c100_259045.htm 通过组策略来限制可移动设备并不是一个十分出色的网络安全解决方案，因为一个已经安装了存储设备（如安装了一个USB驱动设备）的用户，可以继续使用它。不过我们还是可以进行一些细微的设置，这些设置可以允许你通过设备的ID来限制特定的可移动存储设备。很难说哪一种安全威胁对你的网络数据影响最大。由于几个原因，我趋向于认为可移动存储设备，特别是USB驱动设备，应该位于列表的顶部。 原因1：USB储存设备非常容易被忽略。第二个原因：有一个简单的事实是，你可以将很大的数据（如多达4GB的数据）存储到一个USB驱动器上，这也就意味着用户可以将同样大的应用程序带到企业中。它还意味着用户可以将多达4GB的数据从企业带走。用户可以访问的任何数据都可以轻松地复制到这些驱动器上。而且USB设备本身体积很小，这使得用户可以方便地将它带入、带出企业。笔者曾与一些网管员谈到USB储存设备的安全风险问题。不过，这些网管员最通用的做法是禁用工作站上的USB端口。有一些较新的机器允许你通过BIOS禁用USB端口，不过大多数老机器并没有提供这个能力。这种情况下，还有一种方案最常用，那就是用胶布将USB端口封住以此来阻止其使用。虽然这些方法都可以起到一定的作用，不过，都有一些缺点。对于操作者来说，这些方法都是“ 劳动密集型 ”的吧，也就是说太难于实施。另外一个问题是禁用USB端口并没有彻底地解决用户访问可移动媒体的问题。用户可以轻松地使

用FireWire硬盘驱动器、可移动的DVD驱动器作为另外一种选择。 在所有的这些方法中,最大的弊端就在于永久性地禁用USB端口会使用户没法使用USB设备并且使得这些端口不能被支持的用户访问。此外，偶尔也会有一些合法的理由使得USB端口应该可用。例如，有些工作需要用户拥有一个连接到其PC上的USB扫描仪。 幸运的是，微软的Windows vista（还有其著名的Windows Server 2008 (Longhorn)）一个重要目标就是就是给管理员控制工作站使用硬件的方法提供了更好的控制。现在我们可以借助于组策略来控制对可移动稿设备的访问。 限制对USB存储设备访问的组策略设置目前只是在Windows Vista中可用。目前，这也就意味着你只能在本地计算机的层次上设置组策略。在Windows Server 2008发布之后，你就可以在域中、站点中或OU层次上设置这些组策略（当然，前提是你有一个Windows Server 2008的域控制器）。 要访问必须的组策略设置，你必须打开“ 组策略对象编辑器 ”（ Group Policy Object Editor）。因此，请单击“ 开始 ”/“ 所有程序 ”/“ 附件 ”（ 英文操作系统是Start / All Programs/ AcCESsories，笔者用得是英文系统）。下一步，输入MMC命令。这会使Windows打开一个空的微软管理控制台（Microsoft Management Console）。在控制台打开后，从“ 文件（File）”菜单中选择“ 添加/删除管理单元 ”（ Add / Remove Snap-In ）。从管理单元列表中选择组策略对象（Group Policy Object ）选项，然后单击“ 添加（Add） ”按钮。默认情况下，这个管理单元会连接到本地计算机策略（Local Computer policy ），因此直接单击“ 确定（ok） ”,然后单击“ 完成（Finish）”即可。 本地计算机策略会被装载到控制台中。现在，导航

到“ 计算机配置 ”|“ 管理模板 ”|“ 系统 ”|“ 设备安装 ”|“ 设备安装限制 ”（英文系统是找到 Computer Configuration | Administrative Templates | System | Device Installation | Device Installation Restrictions）。在如此操作时，细节窗格会显示几个与安装硬件设备相关的几个限制。 从上图可以看出，有许多与限制设备安装相关的设置。这些设置并非必然地、特定地与可移动设备相关联，而是从总体上与硬件设备相关联。这里的基本思想也就是，如果你限制了用户安装设备，也就阻止了任何你没有专门启用的设备。 关于可移动设备问题，你可以对两项策略设置给予特别注意：第一项设置是“ 允许管理员覆盖设备安装限制 ”（ Allow Administrators to Override Device Installation Restrictions），如果你实施了任何的设备限制的设置，那么你有必要启用这项设置。否则，即使管理员也不能在工作站上安装任何的新硬件。 第二项重要的设置是“ 防止安装可移动设备 ”（ Prevent Installation of Removable Devices）。如果你启用了这项设置，那么用户就不能安装可移动设备。如果一个用户已经在系统中使用了一个可移动设备，就会存在一个此可移动设备的驱动程序，因此用户就会继续使用它。不过，该用户将绝不可能更新设备的驱动程序。 其实，我们通过Windows Vista可以设置的安全措施还有很多，这有待你去进一步去探索、发现。