

Device Lock®

锁定未授权主机外设，
保护企业网络安全，
阻止机密资料外泄！

为什么需要控管 主机外围设备的访问？

根据统计，外部的安全威胁实际上仅占有所有安全威胁的 20% 而已，其余 80% 往往是由于组织内部的员工行为导致。尽管在企业内，加密与防毒软件是基本配置，但却不是企业信息安全的唯一需求。

如同 Gartner 在其「如何解决移动存储设备的安全威胁」研究报告中所说的：「忽视移动存储设备的非授权与不受控管的滥用，正促使企业逐渐将本身暴露在安全风险之中」。事实上，随着 Memory Stick、Flash Card、Smartmedia Cards 等可移动存储设备，甚至是 CD-ROM 光驱、Floppy 软盘驱动器与 MP3 播放器等各种设备的急速增加，已经对企业安全管理造成了各式各样的安全威胁！





开放式 USB 与 FireWire 接口是你最大的安全漏洞？ 使用 DeviceLock® 立即关闭它！

※ 恶意或心怀不满的员工窃取公司的机密文件。

※ 员工将木马程序 (Trojans)、蠕虫 (Worms) 甚至病毒 (Viruses) 带进公司内部网络—其可能是心怀不轨想要采取报复行动，或者只是无知地在他们的个人计算机中使用即插即用 (plug and play) 设备。

※ 机密文件在不知不觉中被错误覆盖，以及在错误操作下发生损毁，例如：某一个员工为了在家里准备工作简报，而将文件保存在便于携带的 U 盘，但是却不小心遗失了存放数据的 U 盘。

DeviceLock®

可以阻止非授权的使用者访问 USB 与 FireWire 端口，以及其它即插即用 (Plug and Play) 的设备，以保护企业网络，可以完全地控管哪些使用者 (Users)、何时 (When) 以及如何 (How) 能够在企业网络内使用可移动的储存装置与设备。

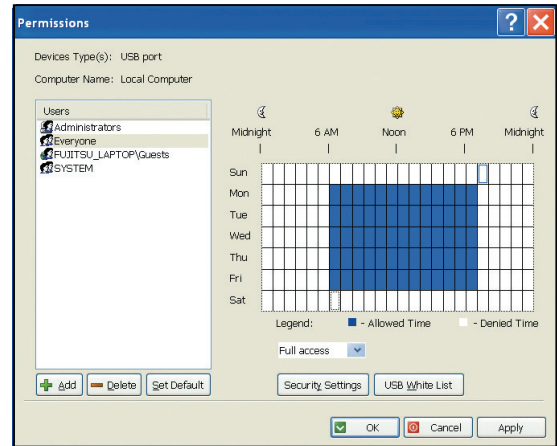
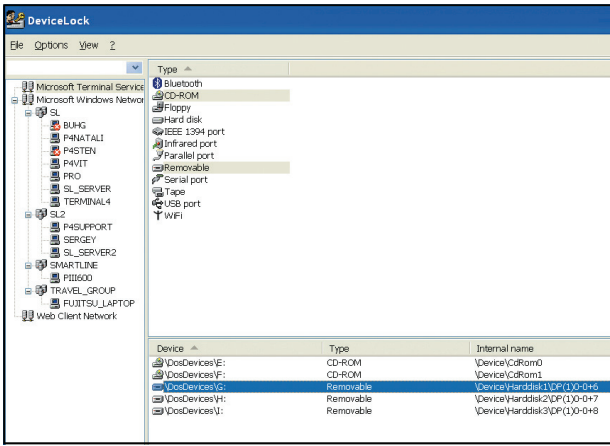
DeviceLock® 是一套用来控管个人计算机外围设备的工具软件，系统会限制一般使用者对于计算机接口设备的访问，杜绝员工私自携带 U 盘、数码相机等可移动式存储，以及蓝牙、无线网络设备等所带来的风险。依靠 DeviceLock®，网络管理员可以阻止非授权使用者使用 USB 与 FireWire 端口、WiFi 与蓝牙 (Bluetooth) 转接器，CD-Rom 光驱与 Floppy 软盘驱动器、串口和并口 (Serial & Parallel Ports)，以及其它即插即用 (plug-and-play) 设备。一旦安装 DeviceLock®，管理员即可以根据每日时间与每周日期，控管任何接口设备的访问。

DeviceLock® 为系统管理者提供以下功能：

- 通过中央管理平台，根据使用者、每日时间与每周日期，控管接口设备与连接端口的访问。
- 针对个别使用者以及使用者群组设定允许策略。
- 根据类别 (例如：所有的 USB 外设) 或者个别设备或端口 (例如：允许特定使用者在指定的机器上使用特定的 ZIP 驱动器)，以设置读取设备的权限。
- 让可读写的接口设备，例如软驱、光驱、ZIP 驱动器等，仅能在只读模式 (read-only mode) 下进行访问。



总的来说，DeviceLock® 可以为企业提供一套完善的企业内部主机外围设备的安全控管解决方案，具备完整的外围设备支持，可以灵活进行权限控制，同时具有大小企业内部网络均适用的后台管理架构，并且可以支持 Group Policy 的管理策略设置，以及具有灵活的授权模式。



可以同时控管不同类型的外设

依靠 DeviceLock[®]，网络管理者可以阻挡非授权使用者使用 U 盘与 USB 外接硬盘、FireWire 端口、WiFi 与无线蓝牙 (Bluetooth) 转接器、CD 与 DVD 光驱/刻录机与 Floppy 软驱、Tape drives (磁带机)/MO 光盘、串口与并口 (Serial & Parallel Ports)，以及其它即插即用 (plug-and-play) 外围设备等。

灵活设置使用策略

一旦安装 DeviceLock[®]之后，管理者即可以根据每日时间与每周日期，控管任何接口设备的读取。可以依据不同的使用者或群组而使用不同的权限规则，并且按照不同的工作日或时段来指定读取策略。也可对存储设备制定不同的读取权限。可以批量指定一群主机，一次性设置这些主机的使用策略和审计策略。也可针对一部主机的不同使用者或群组设置不同使用策略。

提供多种部署方式

部署 DeviceLock[®]时，可以通过以下不同的方案来进行：

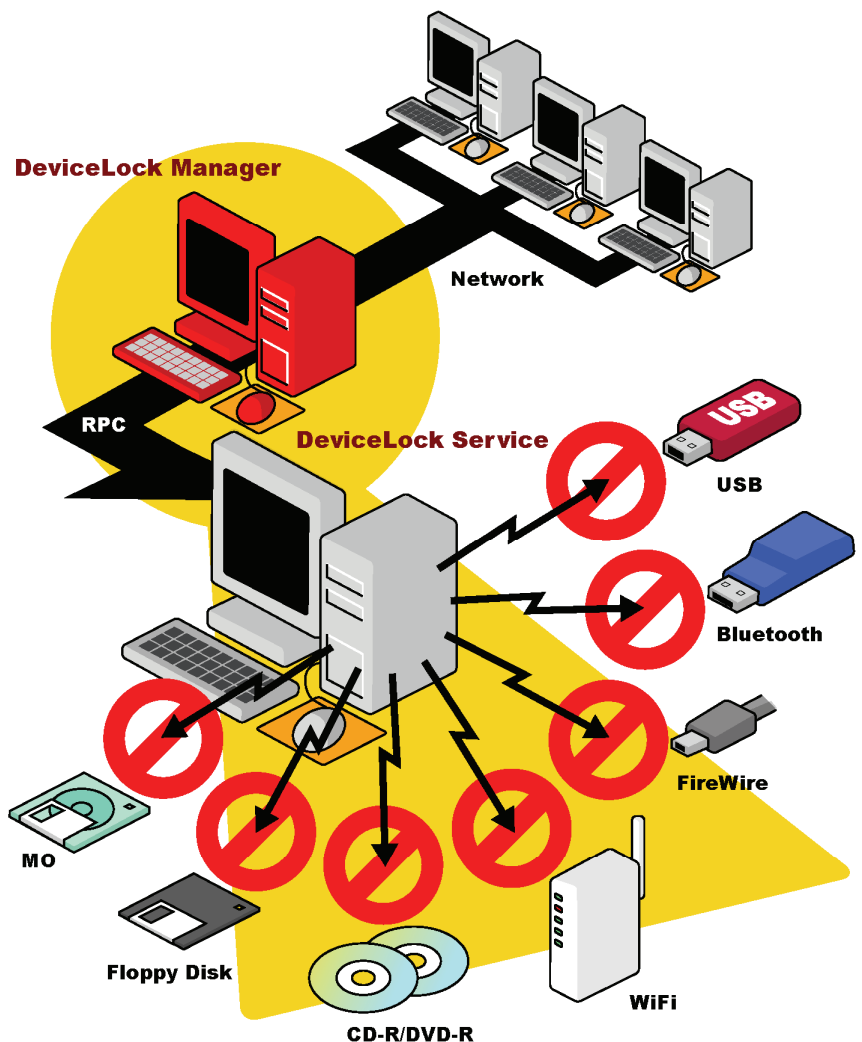
- 局域网环境中的自动化部署 (通过管理接口手动指派)
- 支持微软 SUS 集中部署 (提供 msi 安装程序)
- 支持 AD Group Policy (群组原则) 进行安装
- 通过局域网 Logon Script 自动化安装

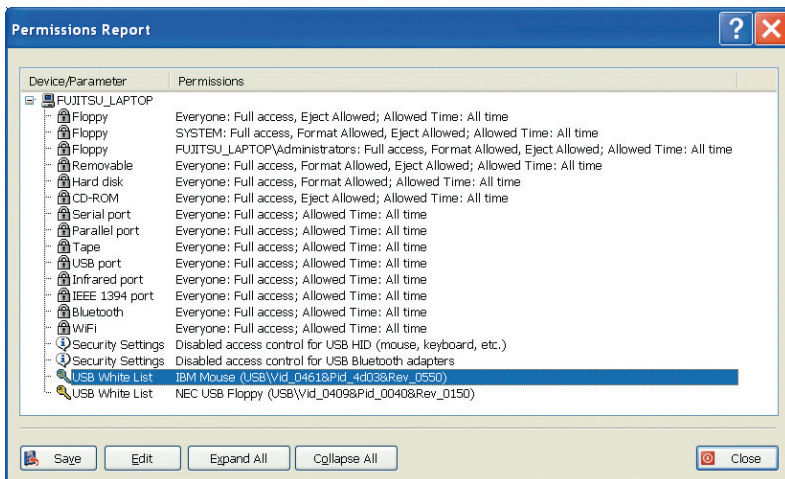
具备 USB 白名单 (White List) 机制

能够自动学习 Device ID，提供单一或部分设备的使用授权，此功能目的是允许使用特定设备 (例如：智能卡读取机)，同时对其它设备保持锁定。

限制储存装置的写入

针对可写入的存储设备可以制定只读 (Read-Only) 的存取权限，并可以制定策略防止可重复读写的媒体被格式化。





提供使用审计

DeviceLock®可以自动产生与 Windows 日志整合的审计日志 (Audit Log), 可设置何种情况需要进行审计, 纪录中包含该动作是由哪个使用者所驱动, 也包含所执行的程序名称。Audit Log 支持外围设备的插拔纪录, 并纪录开放读取时的文件读取纪录。

提供系统管理者权限

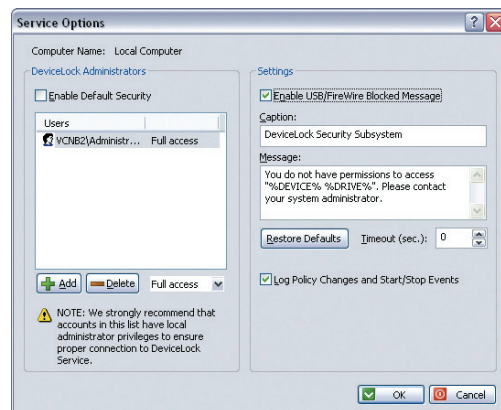
可以指定 DeviceLock® Administrators, 非此管理群组的用户无权限对 DeviceLock® Service 进行停止或卸载, 即使是本机管理员也不得任意停止或卸载该服务。根据目前企业 IT 管理的实际需要, DeviceLock®可以让管理员自行定义一个独立的账号列表, 并赋予该账户可以管理 (安装、卸载、修改许可原则以及其它设置等) DeviceLock®程序。因此, 如果一般使用者不在 DeviceLock®管理员列表中, 尽管该使用者具有本机计算机的管理员权限, 还是无法取消 DeviceLock®服务或者将其从计算机中卸载。

灵活的「临时白名单 (Temporary White List)」功能

在没有网络连接的情况下, 此功能允许使用者可以暂时存取各类 USB 设备。实际应用时, 管理员可以通过电话提供使用者特定的读取代码, 这些代码可以临时解除 DeviceLock®, 而使用者此时则可以访问所需要的设备。

报警机制

当使用者插入 USB 或者 FireWire 端口的意图遭受拒绝时, 系统管理者可以定义一串特别信息, 显示给使用者。



DeviceLock®可以同時支持管理以下的操作系統平台:

- Windows ME
- Windows 98
- Windows NT
- Windows 2000
- Windows XP
- Windows 2003 Server



有关 DeviceLock®的详细资料以及下载 30 天试用版, 请咨询代理商 - 达友科技 Docutek Solutions (Shanghai), Inc.