DeviceLock Protects Data by Managing Peripheral Device Access

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[](http://itmanagersinbox.com/wp-content/uploads/2008/10/no-usb.jpg)Firewalls and antivirus software are no defense against acts of data theft and corruption from within your organization at local endpoints. You don’t have to be an administrator to connect a small digital camera, MP3 player, or flash memory stick to the USB and begin uploading or downloading whatever you want. If you are a system administrator, you know you can’t manage such device-level activity via Group Policy.

[IronKey](http://itmanagersinbox.com/369/ironkey-the-worlds-most-secure-usb-thumb-drive/)and DeviceLock recently partnered to sercure data and USB ports.

“Organizations today are looking for easy-to-use solutions that enable both the flexibility of using mobile data storage devices, as well as the assurance that sensitive data is encrypted and fully protected when transferred via USB ports,” said Steve Ryan, vice president of business development at IronKey. “The combined IronKey and DeviceLock solution provides the level of comprehensive protection against both internal and external threats to data privacy and security that our customers demand.”

**Using endpoint device security solution called DeviceLock®, network administrators can lock out unauthorized users from USB and FireWire devices, WiFi and Bluetooth adapters, CD-ROM and floppy drives, serial and parallel ports, PDAs and smartphones, local and network printers and many other plug-and-play devices**. Once DeviceLock® is installed, administrators can control access to any device, depending on the time of day and day of the week.

For enterprises standardized on software and hardware-based encryption solutions like PGP® Whole Disk Encryption, TrueCrypt and Lexar® SAFE PSD S1100 USB drives, DeviceLock® allows administrators to centrally define and remotely control the encryption policies their employees must follow when using removable devices for storing and retrieving corporate data. For example, certain employees or their groups can be allowed to write to and read from only specifically encrypted USB flash drives, while other users of the corporate network can be permitted to “read only” from non-encrypted removable storage devices but not write to them.

The USB white list allows you to authorize only specific devices that will not be locked regardless of any other settings. The intention is to allow special devices (e.g. smart card readers) but lock all other devices. Media White List feature allows you to authorize access to specific DVD/CD-ROM disks, uniquely identified by data signature, even when DeviceLock® has otherwise blocked the DVD/CD-ROM drive. A convenience when DVD/CD-ROM disks are routinely used for the distribution of new software or instruction manuals, Media White Listing can also specify allowed users and groups, so that only authorized users are able to access the contents of the DVD or CD-ROM.

The DeviceLock®’s optional data shadowing capability significantly enhances the corporate IT auditor’s ability to ensure that sensitive information has not left the premises on removable media. It captures full copies of files that are copied to authorized removable devices, Windows Mobile and Palm OS-based PDAs and smartphones, burned to CD/DVD or even printed by authorized end users. Shadow copies are stored on a centralized component of an existing server and any existing ODBC-compliant SQL infrastructure of the customer’s choosing.

DeviceLock® Enterprise Server can monitor remote computers in real-time, checking DeviceLock® Service status (running or not), policy consistency and integrity. The detailed information is written to the Monitoring log. Also, it is possible to define a master policy that can be automatically applied across selected remote computers in the event that their current policies are suspected to be out-of-date or damaged.

DeviceLock® allows you to generate a report concerning the permissions that have been set. You can see which users are assigned for what device and what devices are on the USB white list on all the computers across your network.
DeviceLock® provides a level of precision control over device resources unavailable via Windows Group Policy – and it does so with an interface that is seamlessly integrated into the Windows Group Policy Editor. As such, it’s easier to implement and manage across a large number of workstations.

**With DeviceLock® you can:**

* Control which users or groups can access USB, FireWire, Infrared, COM and LPT ports; WiFi and Bluetooth adapters; any type of printer, including local, network and virtual printers; Windows Mobile and Palm OS-based PDAs and smartphones; aswell as DVD/CD-ROMs, floppy drives, and other removable and Plug-and-Play devices
* Control access to devices depending on the time of day and day of the week
* Define which types of data (files, calendars, emails, tasks, notes, etc.) are allowed to synchronize between corporate PCs and personal mobile devices
* Detect encrypted PGP® and TrueCrypt disks (USB Flash Drives and other removable media) as well as Lexar® SAFE PSD encrypted flash drives and apply special “encrypted” permissions to them
* Authorize only specific USB devices that will not be locked regardless of any other settings
* Grant users temporary access to USB devices when there is no network connection (you provide users with the special access codes over the phone that temporarily unlock access to requested devices)
* Uniquely identify a specific DVD/CD-ROM disk by the data signature and authorize access to it, even when DeviceLock® has otherwise blocked the DVD/CD-ROM drive
* Protect against users with local administrator privileges so they can’t disable DeviceLock® Service or remove it from their computers, if they are not in the list of DeviceLock® administrators
* Set devices in read-only mode
* Protect disks from accidental or intentional formatting
* Detect and block hardware keyloggers (USB and PS/2)
* Deploy permissions and settings via Group Policy in an Active Directory domain
* Use the standard Windows RSoP snap-in to view the DeviceLock® policy currently being applied, as well as to predict what policy would be applied in a given situation
* Control everything remotely using the centralized management console
* Get a complete log of port and device activity, such as uploads and downloads by users and filenames in the standard Windows Event Log
* Mirror all data (shadowing) copied to external storage devices (removable, floppy, DVD/CD-ROM), Windows Mobile or Palm OS PDAs and smartphones, transferred via COM and LPT ports and even printed
* Store shadow data on a centralized component of an existing server and any existing ODBC-compliant SQL infrastructure
* Monitor remote computers in real-time, checking DeviceLock® Service status (running or not), policy consistency and integrity
* Generate a report concerning the permissions and settings that have been set
* Generate a report displaying the USB, FireWire and PCMCIA devices currently connected to computers and those that were connected
* Create a custom MSI package for DeviceLock® Service with predefined policies.