

# Device Lock<sup>®</sup>

Protecting Your

Sensitive Data by

Managing Peripheral

Device Access.

## Why Manage Device Access?

The data you are striving to protect behind firewalls and passwords is likely still slipping through your fingers. For every lost or stolen laptop or backup tape that makes it into the headlines, consider the many unreported, undocumented data leaks that occur when proprietary information is copied by either unwitting employees or users with malicious intent from their PCs to flash memory sticks, cell phones, cameras, PDA's, or other convenient forms of portable storage. The information becomes fluid, on the move; and you have no control over whose hands it ultimately falls into.



Governments are **mandating** that any organization that compiles consumer data, healthcare records or **protected** intellectual property have adequate security procedures to protect against **data leaks**. HIPPA, Sarbanes-Oxley, and international **IT security** standards like ISO 17799 are specific not just about the need for firewalls to protect against **hacker threats** coming from across the Internet, but also about the need for protection from **insider threats**.

Today PCs are delivered with a multitude of **I/O options**, many unnecessary to a given job **function**. At the same time, 100GB of portable storage weighs just a few ounces, sells for just a few hundred dollars, **transfers** data at high speeds and connects **seamlessly** to any PC. No power source or password required. The combination has made it more difficult for **IT security** staffs to limit PC users to only the information and **computer** resources needed to do their jobs.

DeviceLock **empowers** IT management to enforce the limits set by internal security policy and external compliance authorities. It **stops** data leaks from happening locally by **denying access** to peripheral ports and drives when any employee or visitor attempts a **network** upload or download to a device without appropriate **permissions**.

DeviceLock<sup>®</sup>

DeviceLock access management software is a flexible and robust solution to enforcing device-related security policy. DeviceLock administrators can set permissions per peripheral port, device class, device type, device model, and unique device. Simultaneously, they can grant or deny access per user group and user, even specifying day of the week and time. In addition, DeviceLock will audit all uploading and downloading activity through local drives and ports.

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.

## How it Works

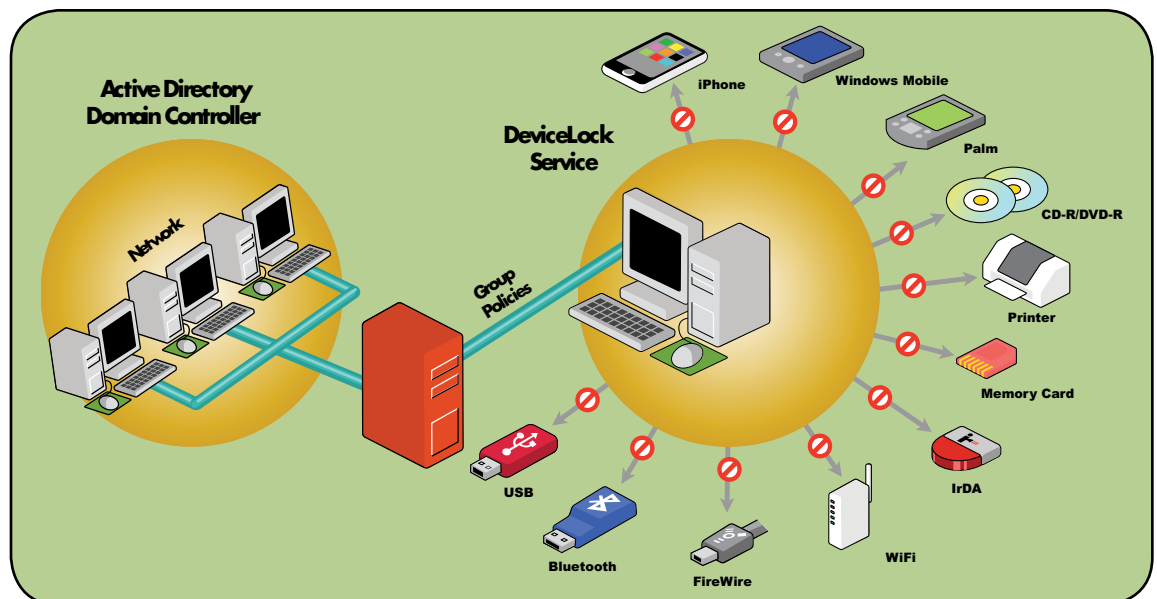
*DeviceLock consists of three parts:*

DeviceLock Service is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.

DeviceLock Enterprise Server is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock

Enterprise Server uses MS SQL Server to store its data.

The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor).



- ▶ Enterprises can secure any number of remote workstations with DeviceLock using Active Directory integration and the Windows Group Policy editor.

Data leaks

occur when

proprietary

information is

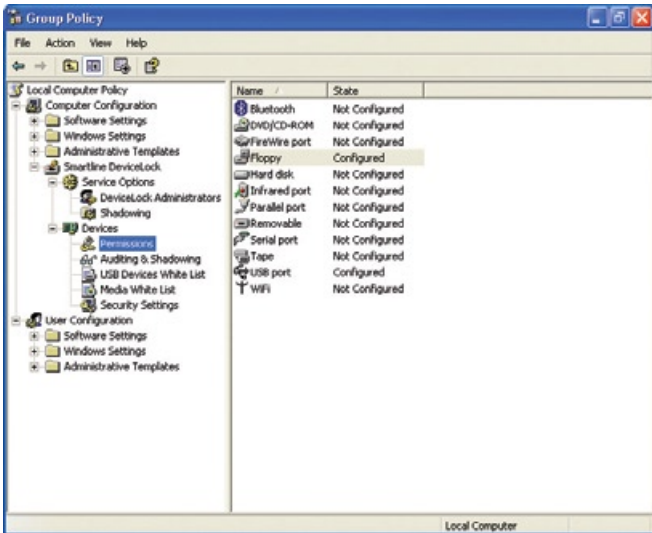
copied to

convenient

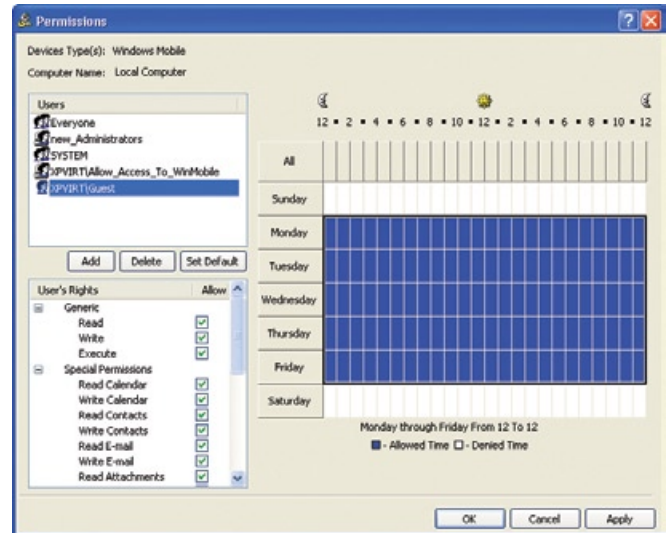
forms of

portable

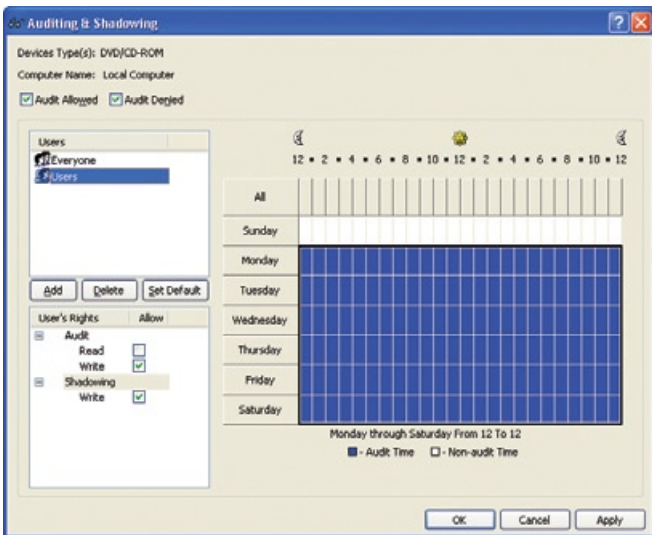
storage.



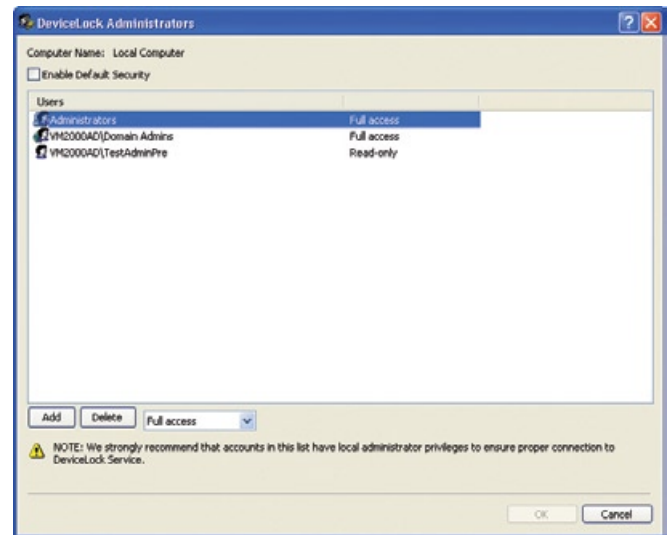
- ▶ DeviceLock Group Policy Manager integrates into the standard Windows Group Policy Editor. With DeviceLock Group Policy Manager, administrators can change DeviceLock's settings, permissions and audit rules across the entire Active Directory forest.



- ▶ DeviceLock administrators set the days and hours when a user or user group will have device access via a graphical time control screen.



- ▶ DeviceLock administrators can define audit rules and enable data shadowing for devices on a per-user basis.



- ▶ When DeviceLock Security is enabled, no one except authorized users can connect to DeviceLock Service or stop and uninstall it. Even members of the Administrators group can't circumvent DeviceLock Security.

DeviceLock's data leakage prevention software is a flexible and robust solution to enforcing device-related security policy.

# DeviceLock Features and Benefits

**Access Control.** 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; as well as DVD/CD-ROMs, floppy drives, and other removable and Plug-and-Play devices. It's possible to set access permissions for any user down to the time of day and day of the week.

**USB White List.** Allows you to authorize a specific model of device to access the USB port, while locking out all others. You can even "White List" a single, unique device, while locking out all other devices of the same brand and model, as long as the device manufacturer has supplied a suitable unique identifier, such as a serial number.

**Media White List.** 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.

**Temporary White List.** Allows granting temporary access to a USB-connected device by the issuing of an access code, rather than through regular DeviceLock permission setting/editing procedures. Useful when permissions need to be granted and the system administrator has no network connection; for example, in the exceptional case of accommodating a sales manager who calls in with a request for USB access when working outside the company's network.

**Device/Port Auditing.** Gives IT staff a complete record of port and device activity, such as uploads and downloads by user and filename in the standard Windows Event log. Also, audit records can be automatically collected from remote computers and centrally stored in SQL Server. Even users with local admin privileges can't edit, delete or otherwise tamper with audit logs set to transfer to DeviceLock Enterprise Server.

**Data Shadowing.** The DeviceLock 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, 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.

**Mobile Device Data Leakage Prevention.** With DeviceLock, you can set granular access control, auditing, and shadowing rules for mobile devices that use Windows Mobile or Palm OS. You can centrally set permissions with fine granularity, defining which types of data that specified users and/or groups are allowed to synchronize between corporate PCs and their personal mobile devices, such as files, pictures, calendars, emails, tasks and notes. DeviceLock detects the presence of mobile devices attempting to access ports through USB, COM, IrDA or Bluetooth interfaces.

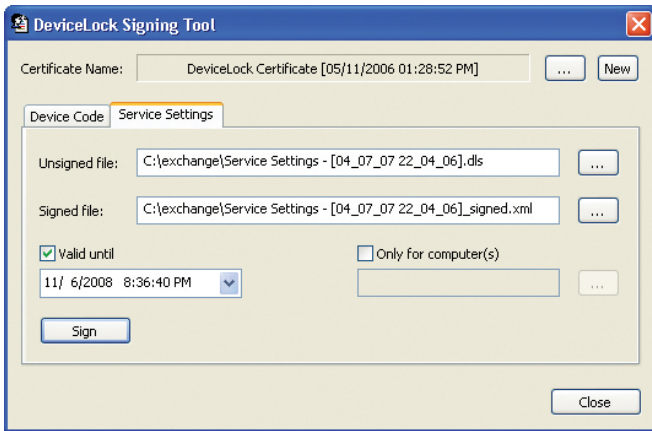
**Tamper Protection.** Every user with local administrator privileges is not automatically given DeviceLock administration privileges. The Chief Security Officer or other super-administrator has discrete control over who has DeviceLock administration privileges.

**Group Policy Integration.** You have a choice of DeviceLock management consoles including the ability to manage DeviceLock settings using the Windows standard Group Policy interface, making it easier for busy administrators to merge hardware lock-out tasks into their overall systems management workload.

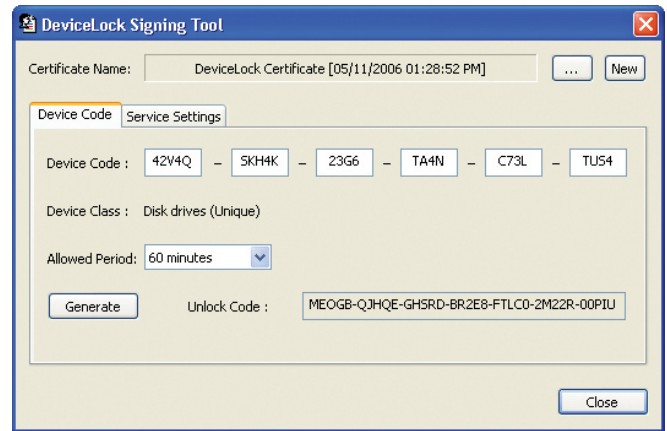
**TrueCrypt & PGP Whole Disk Encryption Integration.** DeviceLock can detect encrypted PGP and TrueCrypt disks (USB flash drives and other removable media) and apply special "encrypted" permissions to them. For enterprises standardized on encryption solutions, DeviceLock allows administrators to centrally 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.

**Lexar SAFE PSD Integration.** DeviceLock detects hardware-encrypted Lexar SAFE PSD S1100 USB drives and applies special "encrypted" permissions to them.

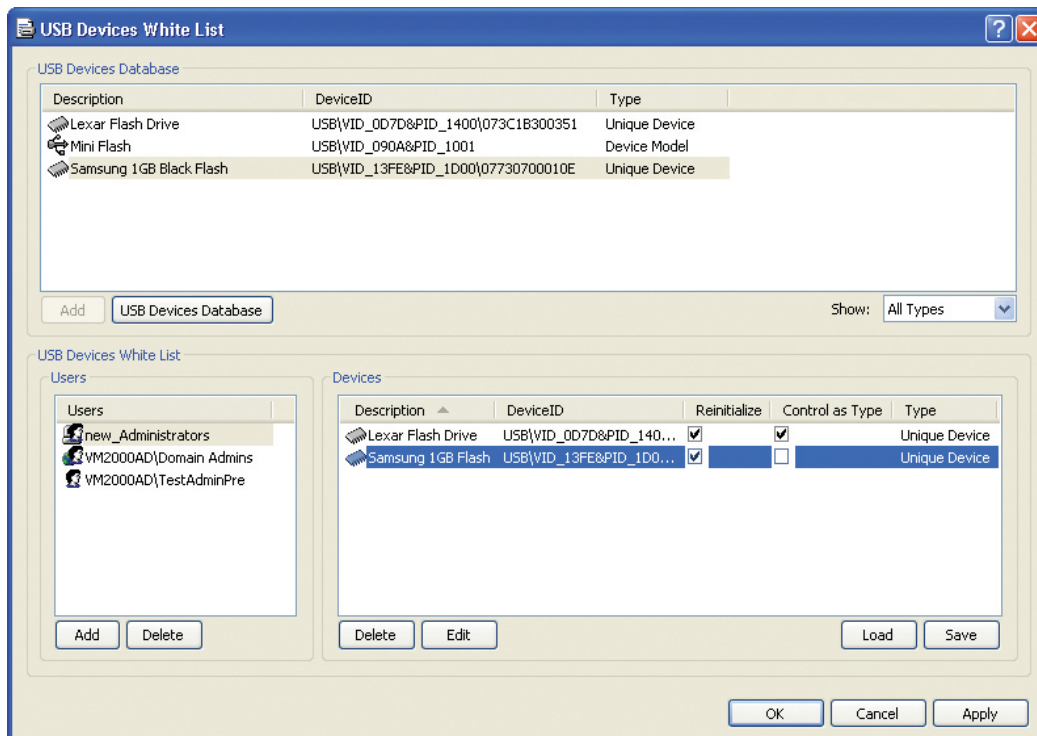
DeviceLock is  
fully integrated  
with  
ActiveDirectory  
Group Policy  
Interfaces.



- ▶ Using the DeviceLock signing tool, you can tamper-protect configuration files. Later these files can be sent to users whose computers are not online and thus out-of-reach via management consoles.



- ▶ Special access codes can be created to grant offline users temporary access to requested devices.



- ▶ Devices in the White List can be defined by model or unique ID and can be assigned per user, per group, per computer, and in any combination thereof.

# Extended DeviceLock Functions

**Anti-keylogger.** DeviceLock detects USB keyloggers and blocks keyboards connected to them. Also, DeviceLock obfuscates PS/2 keyboard input and forces PS/2 keyloggers to record garbage instead of the real keystrokes.

**Monitoring.** 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.

**RSoP Support.** You can use the Windows standard Resultant Set of Policy snap-in to view the DeviceLock policy currently being applied, as well as to predict what policy would be applied in a given situation.

**Batch Processing.** Allows you to define settings for a class of similar computers with similar devices (e.g. all computers have USB ports and CD-ROMs) across a large network in a fast and consistent manner. DeviceLock Service can be automatically installed or updated on all the computers in a network using DeviceLock Enterprise Manager.

**Permissions Report.** Allows you to generate a report displaying the permissions and audit rules that have been set on all the computers across the network.

**Report Plug-n-Play Devices.** Allows you to generate a report displaying the USB, FireWire and PCMCIA devices currently connected to computers in the network and those that were historically connected.

**Traffic Shaping.** DeviceLock allows you to define bandwidth limits for sending audit and shadow logs from DeviceLock Service to DeviceLock Enterprise Server. This Quality of Service (QoS) feature helps reduce the network load.

**Stream Compression.** You can instruct DeviceLock to compress audit logs and shadow data pulled from endpoints by DeviceLock Enterprise Server service. Doing this decreases the size of data transfers and thus reduces the network load.

**Optimal Server Selection.** For optimal transfer of audit and shadow logs, DeviceLock Services can automatically choose the fastest available DeviceLock Enterprise Server from a list of available servers.

Every time the  
user wants  
to access  
a device,  
DeviceLock  
intercepts this  
request at the  
kernel level of  
the OS.

# Capabilities and Requirements

DeviceLock allows IT security administrators to proactively and flexibly manage port-level and device-level access to local PC I/O resources. You can set permissions at multiple levels: port-level, device class-level, device type-level and individual device-level. This provides a full spectrum of options: you can block all ports or make them all read-only. You can selectively allow certain devices full or read-only access to certain ports, while blocking all others. Even when ports and drives are left unlocked to certain or all devices, you can rely upon DeviceLock's auditing capabilities to keep track of user access.

<p><b>Ports Secured</b></p> <ul style="list-style-type: none"> <li>▪ USB</li> <li>▪ FireWire</li> <li>▪ Infrared</li> <li>▪ Serial and parallel</li> </ul>	<p><b>Device Types Controlled</b></p> <ul style="list-style-type: none"> <li>▪ Floppies</li> <li>▪ CD-ROMs/DVDs</li> <li>▪ Any removable storage (flash drives, memory cards, etc.)</li> <li>▪ Hard drives</li> <li>▪ Tape devices</li> <li>▪ WiFi adapters</li> <li>▪ Bluetooth adapters</li> <li>▪ Windows Mobile and Palm OS devices</li> <li>▪ Printers (local, network and virtual)</li> </ul>
<p><b>Encryption Integration</b></p> <ul style="list-style-type: none"> <li>▪ PGP Whole Disk Encryption</li> <li>▪ TrueCrypt</li> <li>▪ Lexar SAFE PSD</li> </ul>	
<p><b>System Requirements</b></p> <ul style="list-style-type: none"> <li>▪ DeviceLock can be installed on any computer running Windows NT 4.0/2000/XP/Vista or Server 2003/2008. It supports 32-bit and 64-bit platforms.</li> </ul>	

## Support for SanDisk® Cruzer® Enterprise

DeviceLock's membership in SanDisk® Enterprise Solutions Technology Alliance ensures DeviceLock full compatibility with SanDisk's Cruzer® Enterprise USB drive.

## For More Information

For more information on DeviceLock, check out our website.

[ [www.deviceclock.com](http://www.deviceclock.com) ]

DeviceLock

Audit gives

I.T. staff a

complete

record of

device and

port activity.

**DeviceLock**  
Proactive Network Security

2010 Crow Canyon Place, Ste. 100  
San Ramon, CA 94583, USA

email: [support@deviceclock.com](mailto:support@deviceclock.com)

Toll Free: +1 866 668 5625

Phone: +1 925 231 4400

Fax: +1 925 886 2629

The 401 Centre, 302 Regent Street  
London, W1B 3HH, UK

Toll Free: +44 (0) 800 047 0969

Fax: +44 (0) 207 691 7978

Via Falcone 7  
20123 Milan, Italy

Phone: +39 02 86391432

Fax: +39 02 86391407

Halskestr. 21  
40880 Ratingen, Germany

Phone: +49 2102 89211-0

Fax: +49 2102 89211-29