

Device Lock[®]

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 unwitting or witting employees 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.

SmartLine
Proactive Network Security



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 boards. 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 **permission**.

DeviceLock[®]

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 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.

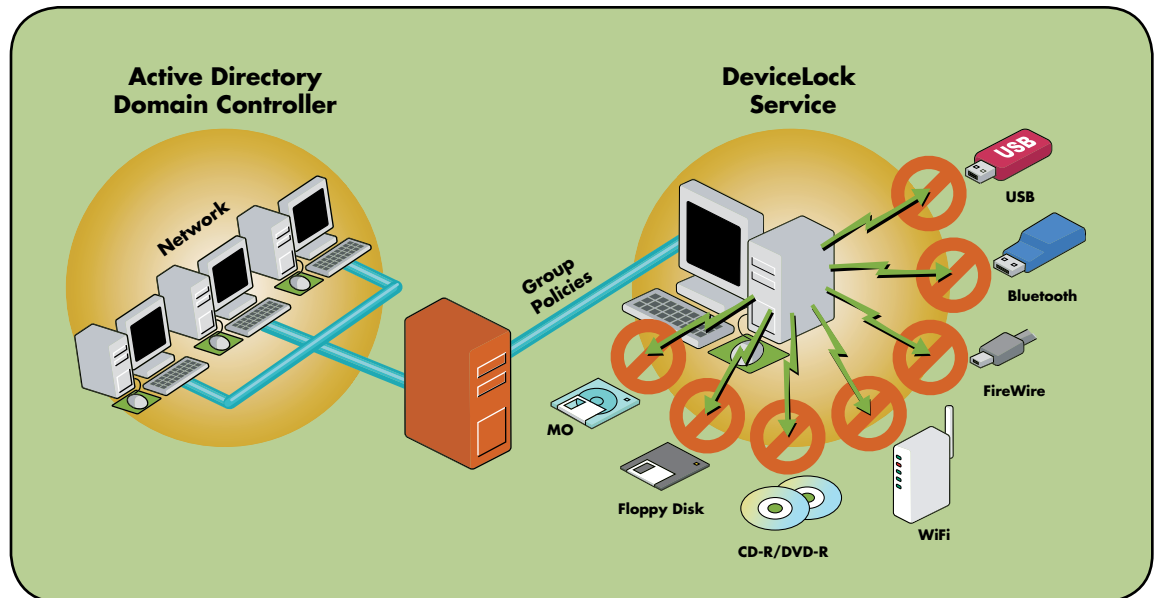
How it Works

DeviceLock consists of two parts:

DeviceLock Service, a software component installed invisibly on each client system, and a management console accessible only to designated DeviceLock administrators.

The management console can be installed as a separate interface, or, for those that prefer the Windows Group Policy interface, DeviceLock supports Active Directory integration. There is also a snap-in option for the Microsoft Management Console (MMC).

From the management console, you can set device permissions for all connected remote computers protected by DeviceLock Service. DeviceLock supports remote installing of the service module when necessary; DeviceLock administrators can remotely update an outdated service module from their DeviceLock console, as a Group Policy Object (GPO), through Microsoft Systems Management Server or using other deployment tools.



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

Data leaks

occur when

proprietary

information is

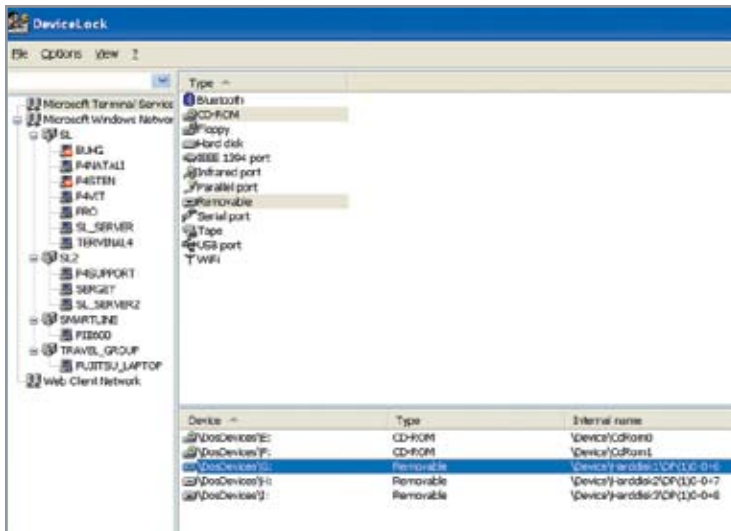
copied to

convenient

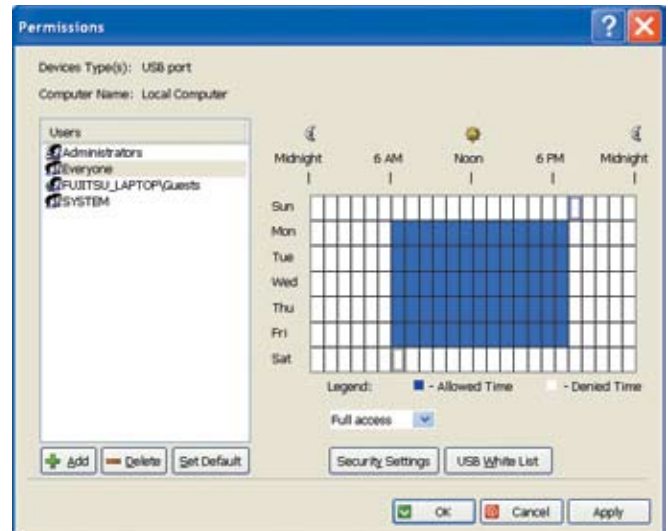
forms of

portable

storage.



- ▶ DeviceLock Manager's main dialog displays a tree of computers with DeviceLock Service status and from here it's easy to select and set user permissions for computers, device ports and individual devices.

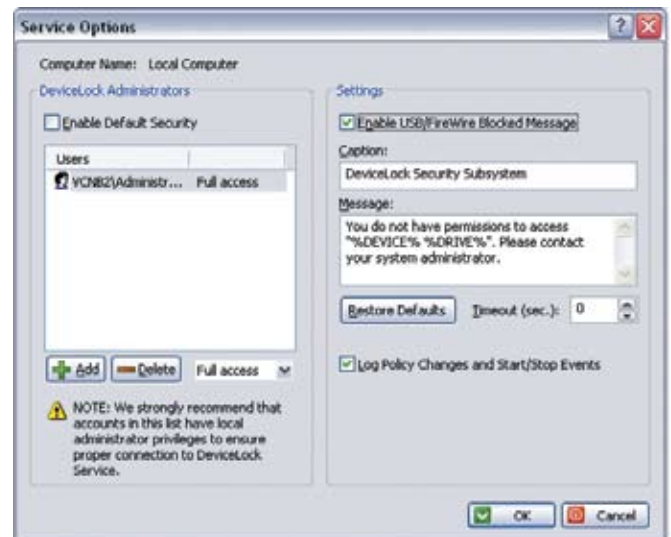


- ▶ DeviceLock administrators set the days and hours when a user or user group will have device access via a graphical time control screen.

The Permissions Dialog controls access to devices. Its menus progress through the setting of permissions for a device type or group of types and the specifying of accessibility by users and times (day of the month and/or day of the week). Next, administrators can define allowable actions, rights and privileges for a user or user group—no access, read-only access, full access etc.

DeviceLock also offers additional security settings that make it possible to generally lock COM, USB and FireWire ports, but allow the usage of some devices. This provides the flexibility needed to permit the use of USB-connected mouse and keyboard devices, while otherwise locking down the USB port.

You have the option of selecting among local system administrators when assigning DeviceLock administration privileges, and only designated DeviceLock administrators can set permissions. This provides another level of security, prohibiting an unauthorized person—even someone with local administrative privileges—from changing their profile in order to stop DeviceLock Service or change permissions.



- ▶ A super-administrator, such as a Security official, sets the list of DeviceLock administrators, controlling who can stop or remove the service.

DeviceLock® access management software
is a **flexible** and robust **solution**,
enforcing device-related **security** policy.

DeviceLock Features and Benefits

The SmartLine development team has designed the software to be robust and reliable when it comes to enforcing device security policy, while being easy and intuitive for DeviceLock administrators to use. It is continually evolving in both respects, and its current feature set is unmatched in the security software market.

Enhanced Security

Permissions Dialog: Allows you to easily define access permissions for a device type or for a group of types, specifying authorized users and authorized times (day of the month and/or day of the week).

Administration Assignment: 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.

Security Settings: Allows you to specify access to COM, USB and FireWire ports to accommodate the use of a whole class of equipment (human input devices, scanners, printers, etc.) that connects through a specified port, while generally denying access to that port by all other equipment classes.

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. You can set different permissions and/or audit rules for different types of devices.

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. DeviceLock can enforce whatever White Listing strategy is decided by Security Policy decision-makers and is feasible given DeviceLock administrator workloads.

Ease of Management

Group Policy/Active Directory Integration:

You have a choice of DeviceLock management consoles including the ability to set and manage DeviceLock permissions 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.

Batch Permissions: Allows you to set permissions for a class of similar computers with similar devices (e.g. all computers have floppy drives 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 the Batch Permissions function.

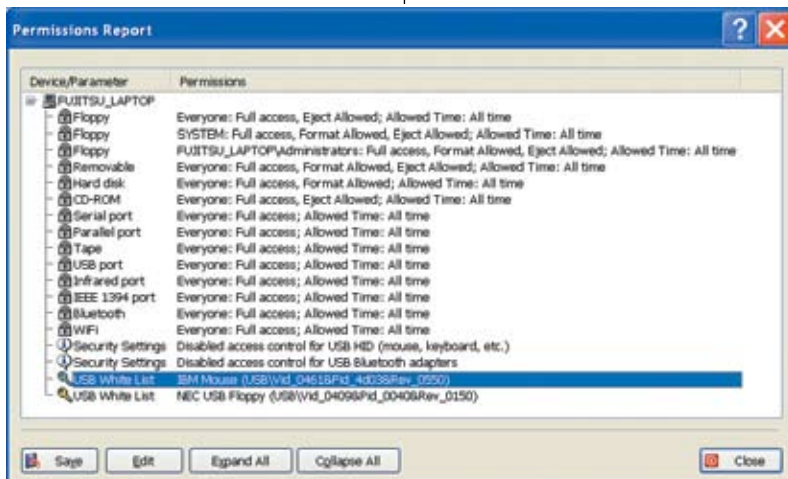
Permissions Report: Allows you to generate a report concerning the permissions that have been set. You can see which users are assigned what device, which parameters are disabled in Security Settings, and what devices are on the USB White List for all the computers across the network.

Report Plug-n-Play Devices:

This plug-in generates a report displaying the USB,

FireWire and PCMCIA devices currently connected to computers in the network and those that were connected.

Continued on back page.



- ▶ You select the computers to be included on this customizable report that can also be exported to an.xls or .txt file.

For those that

prefer the

Windows

Group Policy

interface,

DeviceLock

supports

Active

Directory

integration.

Continued from Features and Benefits.

Temporary USB 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.

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 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>Ports Locked</p> <ul style="list-style-type: none"> ▪ USB ▪ FireWire ▪ Infrared ▪ Serial and parallel 	<p>Device Types Locked Out</p> <ul style="list-style-type: none"> ▪ Floppies ▪ CD-ROMs/DVDs ▪ Any removable storage (Magneto-Optical disks, ZIPs, etc.) ▪ Hard drives ▪ Tape devices ▪ WiFi adapters ▪ Bluetooth adapters
<p>System Requirements</p> <ul style="list-style-type: none"> ▪ DeviceLock can be installed on any computer running Windows NT/2000/XP or Windows Server 2003. 	

For More Information

For more information on DeviceLock, check out our website.

[www.devicelock.com]

DeviceLock

Audit gives

I.T. staff a

complete

record of

device and

port activity.



SmartLine Inc.
 2010 Crow Canyon Place, Ste. 100
 San Ramon, CA 94583, USA
 email: support@protect-me.com
 Toll Free: +1.866.668.5625
 Fax: +1.646.349.2996

The 401 Centre, 302 Regent Street
 London, W1B 3HH, UK
 Phone: +44 (0) 7779 28 27 21
 Fax: +44 (0) 208 744 98 23

Via Falcone 7
 20123 Milan, Italy
 Phone: +39 02 86391432
 Fax: +39 02 86391407