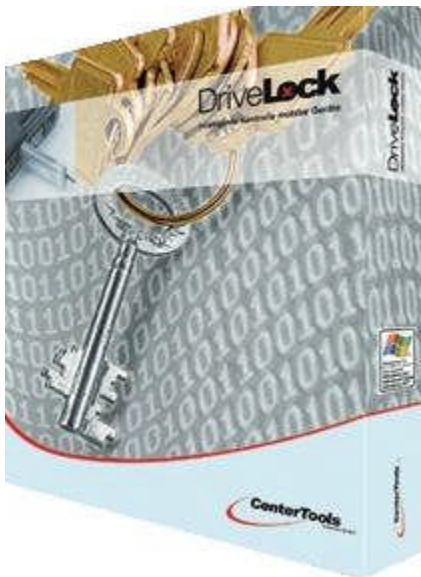




CenterTools DriveLock™

DriveLock™ gives you total control over who can attach what to your computers. Encryption keeps data confidential even when a computer or storage device is lost. Control which programs users can run and what networks they can connect to. DriveLock™ fits into your IT infrastructure for easy and effective administration.



DriveLock™ protects your network with unparalleled control over mobile devices, applications and network connections.

Control of mobile devices

USB thumb drives and other devices can expose corporate data to theft and disclosure. DriveLock™ gives you granular control over who is allowed to connect which device and what data users can copy to or from storage devices.

IMPROVED Media encryption

Sometimes employees need to copy data to mobile devices, but storage devices are frequently lost. DriveLock™ can encrypt this data, automatically and transparently. You can be confident no data is compromised when a device is lost.

NEW Full Drive Encryption

Protect data on laptops and other computers by encrypting all drives, even the system partition. Pre-boot authentication and single sign-on combine security and ease of use.

Network Profiles

DriveLock's Network Profiles let you create rules to control networks users can connect to and then configure settings for that network.

Application Launch Filter

DriveLock's new Application Launch Filter stops unwanted programs or limits users to run only the programs

you approve. It can even block zero-day attacks.

Auditing

DriveLock™ can monitor all device activity and create an audit trail. It can even record the data copied to and from devices for bullet-proof evidence. The Security Reporting Center lets you find information quickly and efficiently.

Easy, efficient administration

DriveLock easily fits into your existing IT infrastructure by utilizing Active Directory Group Policy, (DriveLock also fully supports Novell and other environments). Client deployment uses existing software distribution mechanisms. Training and support costs remain low for a high return on investment (ROI).

NEW Mobile Encryption

Access encrypted data on your Windows Mobile device.

Find out more

For more information about how DriveLock can help you secure your infrastructure or for a no-risk trial, contact CenterTools.

CenterTools, LLC
1001 SW Fifth Avenue
Suite 1100

Portland, OR 97211

(888) 627-7515

E-mail: info@centertools.com

Web: www.drivelock.com

Intelligent control of mobile devices made easy.

DriveLock fits into your infrastructure to help you protect your network and your data.

www.drivelock.com

» Device and Drive Locking

- Dynamically locks removable devices (USB flash drives, floppy disks, CD-ROM, etc.)
- Locks most types of devices: Scanners, cameras, network adapters, Palm, Windows Mobile, Smartphones, modems, game controllers and many more
- Locks most types of ports: USB, 1394/FireWire, Bluetooth, infrared, PCMCIA serial (COM) and parallel (LPT)
- Configurable whitelists allow access to device types or models
- Allows specific storage devices based on unique serial numbers
- Access can be granted to users or groups
- Fully integrated with Active Directory and Group Policy
- Support for Novell eDirectory and ZENworks.
- Dynamic policy enforcement according on logged-on user
- File Filter to allow or deny copying of specific file types
- Auditing of files that are read from or written to removable drives
- Separate Read and Write permissions for removable drives
- Drive access rules based on drive size or encryption status

» Removable Media Encryption

- Encrypt data on mobile devices or hard disks with up to 256-bit encryption strength
- Automatic and transparent encryption of data that's copied to mobile devices
- Encryption enforcement
- Access to encrypted drives and files from computers without DriveLock
- Easy to use
- Wizard for creating encrypted CDs and DVDs.

» Full Drive Encryption

- Proven technology for sector-by-sector encryption of all hard drives, including temporary and paging files

- Multiple encryption algorithms and FIPS 140-2 certification
- Pre-boot authentication to prevent unauthenticated access to any part of hard drive
- Automated installation and central monitoring
- Robust recovery and emergency logon tools

» Application Launch Filter

- Application Launch Filter determines which programs a user can run
- Blacklists prevent users from running unwanted programs
- Whitelists ensure that users run only approved applications.
- Block even zero-day attacks and dangerous programs that are not detected by antivirus software
- Templates for easy configuration
- Full auditing of user activities

» Network Profiles

- DriveLock dynamically detects which network a computer is connected to based on network profile definitions
- Disables network adapters when user attempts to connect to unapproved network
- Automatically configures settings based on current network
- Blocks devices and application based on current network

» Auditing

- Auditing keeps complete record of device and application usage
- Security Reporting Center: a central reporting console for all DriveLock events
- Customized reports on device and application usage
- Multiple alerting mechanisms for DriveLock events
- File shadowing keeps full record of the content of files that are copied to or from removable drives

» Administration

- No servers required to deploy policies
- All configuration is done using a Microsoft Management Console (MMC) snap-in
- Device Scanner creates inventory of all devices that are connected or were ever used on all computers
- Easy client deployment using existing deployment mechanisms
- Central configuration using Active Directory and Group Policy
- Configuration using Novell eDirectory and ZENworks
- Alternate configuration using configuration files (UNC-Path, HTTP or FTP)
- Administrators can temporarily suspend device restrictions whether client is online or offline
- Remote identification of devices connected to clients
- Quick policy deployment using templates
- Deployment Wizard
- Customizable taskbar notification with HTML text
- Multi lingual user interface (MUI)
- Protection against tampering or de-installation

» Mobile Encryption

- Encrypt data on Windows Mobile handheld devices and Smartphones
- Synchronize encrypted data between mobile device and desktop

» Terminal Server Support

- Application control for Windows and Citrix terminal servers
- Control over the use of client drives in terminal sessions

» System requirements

- Windows XP, Windows Vista or Windows Server 2003
- Active Directory with Group Policy recommended for central configuration