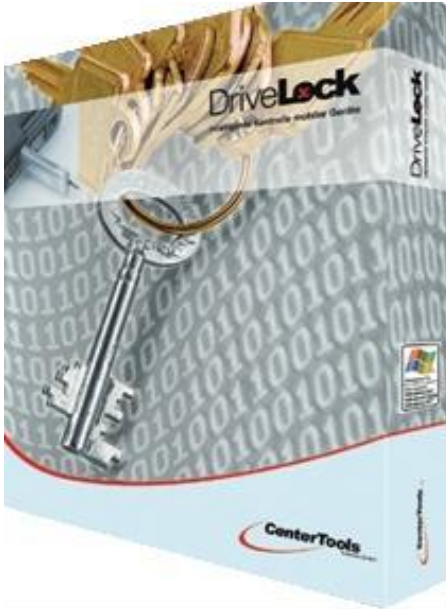


DriveLock[™] gives you total control over who can attach what to computers and which programs can run. Encryption keeps data confidential when a computer or storage device is lost. DriveLock[™] fits into your IT infrastructure for easy and effective administration.



Intelligent data protection made easy.

DriveLock[™] easily integrates into your existing infrastructure to help you protect your network and secure confidential data with minimal effort.

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

» **Control of mobile devices**

Unrestricted use of USB flash drives and other removable storage devices often results in data leakage or theft. DriveLock gives you granular control over who can use such devices and which data can be transferred.

» **Media encryption**

Sometimes employees need to copy data to mobile devices, but storage devices are frequently lost. *Encryption 2-Go* can encrypt this data, automatically and transparently and even burn encrypted CDs and DVDs. Password protection enables the secure access of data on computers without DriveLock. You can be confident no data is compromised when a device is lost.

» **Full Disk Encryption**

Protect data on laptops and other computers by encrypting all drives, even the system partition. Pre-boot authentication with single sign-on requires little or no end-user training.

» **Network Profiles**

DriveLock's Network Profiles let you create rules to control which networks users can connect to automatically apply different policies as computers move between network locations.

» **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. Best of all, configuring this protection is quick and easy.

» **Auditing**

DriveLock can monitor all device activity and establish an audit trail. It can even record the data copied to and from devices for bullet-proof evidence. The DriveLock Control Center lets you easily create comprehensive usage reports. Advanced forensic features let you quickly identify risks or find the source of a security breach.

» **Easy, efficient administration**

DriveLock fits into your existing IT infrastructure by providing several methods for policy distribution, including Active Directory Group Policy. Existing software distribution mechanisms can be used to deploy the client software. Intuitive tools guide you through most configuration tasks. Flexible, granular rules ensure that DriveLock can enforce your organization's security policy. Training and support costs are low for a high return on investment (ROI).

» **Mobile Encryption**

Access encrypted data on your Windows Mobile device.

» **Compatibility**

DriveLock runs on all recent versions of Windows, including 64-bit versions.

» **Find out more**

To learn more about how to 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

» Device and Drive Locking

- Dynamically locks removable drives (USB flash drives, floppy disks, CD-ROM, eSata, SD cards, 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 use of specific storage devices based on 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
- Highly granular rules based on computer, user, network connection, time of day, etc.

» Encryption 2-Go

- 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
- Portable application for using encrypted drives and files on computers without DriveLock
- Easy to use
- Wizard for creating encrypted CDs and DVDs
- Recovery of access to devices when a password is forgotten
- FIPS 140-2 compliant encryption algorithms

» Full Disk 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
- Multiple rule types for configuring protection in just a few minutes

» Auditing

- Auditing keeps complete record of device and application usage
- DriveLock Control Center: a central reporting console for all events
- Comprehensive reports on all endpoint activity
- Multiple alerting mechanisms for DriveLock events
- File shadowing keeps full record of the content of files that are copied to or from removable drives
- Sophisticated tools for forensic analysis

» 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, Novell eDirectory and ZENworks or configuration files
- Temporary suspension of device restrictions for online or offline clients
- Remote identification of devices connected to clients
- Quick policy deployment using templates
- Console guides administrators through most tasks and gives visual feedback about status
- Customizable taskbar notification with HTML text
- Multi lingual user interface (MUI)
- Protection against tampering or de-installation

» Network Profiles

- DriveLock dynamically detects the network a computer is connected to
- 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

» 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
- Device control and encryption for thin clients

» System requirements

- Windows XP or higher (including Windows 7) or Windows Server 2003 or higher, including 64-bit versions
- Active Directory recommended for central configuration