



Full Disk
Encryption
for All
Hard Drives

Encryption
for All
Windows Mobile
Devices

Secure Device and Application Management



CENTRALIZED SECURITY MANAGEMENT FOR ALL NETWORK CLIENTS

Features:

- » Dynamic and highly configurable access control for mobile drives (floppy disks, CD-ROM, USB flash drives, etc.)
- » Controls the use of most device types: Bluetooth, Palm, Windows Mobile, BlackBerry, virtual devices (VMware), smartphones, memory card readers, imaging devices, network adapters, modems, infrared controllers, USB controllers, FireWire controllers, audio, video and game controllers, PC Card controllers, printers, cellular phones, input devices (HID), media players, biometric devices, software protection devices (dongles), tape drives, Media Center devices, SideShow devices, flash-memory devices, IEC 61883 (AVC) bus devices
- » Controls the use of serial (COM) and parallel (LPT) ports
- » Drive whitelist rules: Access can be granted based on users, groups, device ID and serial number
- » Whitelist rules for drives can include size limitations or enforce that data can only be copied to encrypted drives
- » Device whitelist rules: Configuration based on device type and hardware ID
- » Device access can be limited to specific times or specific computers
- » Separate read and write permissions for removable drives
- » The current network connection is automatically recognized, rules can be enforced based on network connection
- » Temporary unlocking of devices can be performed while the computer is online or offline
- » Detailed auditing of all configuration changes
- » File filter: Allow or deny the copying of data based on file type
- » Device Scanner detects devices and drives on all computers in your network and can even report historical data
- » File auditing: Auditing of all read and write activity to and from removable drives, including who copied which files

- » Data Shadowing: Shadowing retains a copy of data copied to or from a removable device
- » **DriveLock** protection is active even in Windows Safe Mode
- » Support of several network operating systems, including Windows Active Directory and Novell NetWare (eDirectory)
- » Automatic detection of user logon and logoff to enforce policies based on current user's identity
- » Assigning of specific drive letters to removable devices
- » Alerting via SMTP or SNMP
- » Administrator-configured user notification via transparent popup windows that can include HTML-formatted text
- » Security Reporting Center (SRC), the central reporting console. The SRC consolidates all **DriveLock** events in a central location. Administrators can then use this data to create dynamic reports for auditing and report creation

Optional Features:

- » Full disk encryption with FIPS 140-2 certification, including pre-boot authentication and single sign-on
- » Encryption of data on Windows Mobile devices (Pocket PC 2003, Windows Mobile 5 und Windows Mobile 6)
- » Removable media encryption using standard encryption algorithms, such as AES and 3DES. Administrators can enforce the encryption of all data stored on removable drives. Access to encrypted data is possible without **DriveLock** being installed and without the need for local administrative rights
- » Application Control: The Application Launch Filter denies access to unauthorized programs using a flexible combination of whitelist and blacklist rules



Try it yourself!
www.drivelock.com

System Requirements:

- » Windows XP, Windows Server 2003 or Windows Vista
- » Active Directory is recommended for ease of administration

COMPREHENSIVE SECURITY FOR SENSITIVE DATA



DRIVELOCK AT WORK

“After receiving a short introduction to the product we were able to deploy DriveLock without any problems ...

Active Directory integration and simple handling were among the key aspects for us. DriveLock requires no separate management infrastructure.”

Werner Drescher,
Bundeszentralregister, IT-Operations

“We are completely satisfied. I’d even say we were pleasantly surprised.”

Bernd Bittner, City of Kempten,
Systems Technology Manager

“After evaluating a few different products and solutions, DriveLock was by far the best one. There were a few that were similar in concept, but not as granular or as easy to configure. I would recommend this to any corporation that wants to control access to their systems via external media.”

Joe Lio, Director of Information
Technology, South Florida
Educational Federal Credit Union

“Today we are even more convinced that we have made the right decision.”

Michael Böhme,
Premiere Fernsehen AG

» SECURITY TO GO



Security To Go – DriveLock 5.5

extends security to Windows Mobile devices. Certified Full Disk Encryption secures data on laptops and other high-risk computers. **DriveLock** gives you the peace of mind that your data remains confidential even when computers are away from your network.

DriveLock is a leading solution for controlling *all* peripherals in your network and securing your mobile data. Unparalleled flexibility and granular control mean that you can achieve this protection without adding to the workload of IT administrators.

Comprehensive control:

- » Full Disk Encryption
- » Encryption for Windows Mobile
- » Security Reporting Center (SRC)
- » Auditing and Shadowing
- » Device Scanner
- » Removable Media Encryption
- » Network Profiles
- » Application Launch Filter

DriveLock is the logical choice for data security. To find out more, visit us at www.drivelock.com or give us a call.

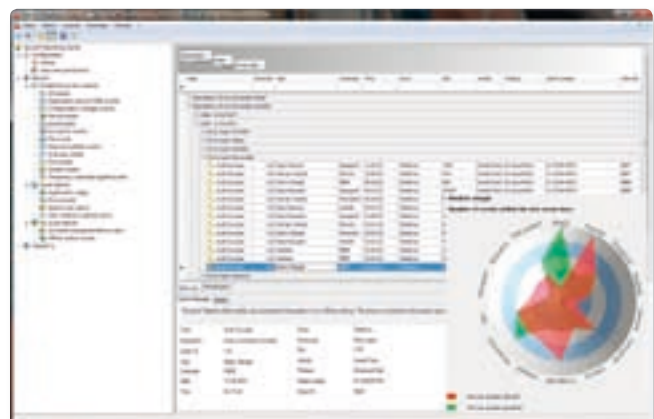
DriveLock: Always cutting edge

- » **DriveLock**'s product development is driven by real-world experiences and customer requirements. All features and configuration options are designed to achieve bullet-proof data security while maintaining ease of use and minimizing resource requirements. With these goals in mind, we constantly aim to improve on existing features. For example, we even further improved the whitelist rules for devices and drives.



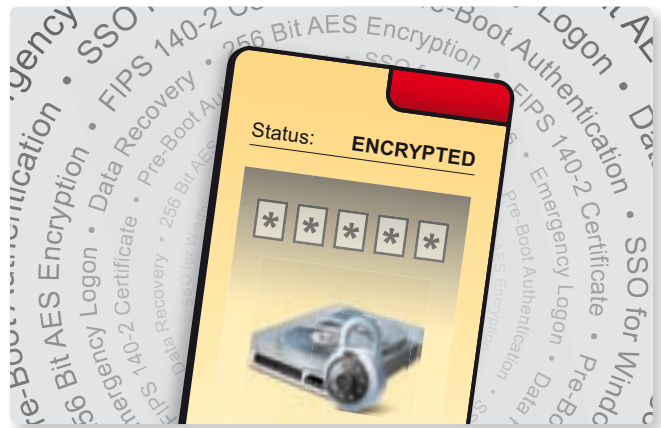
Security Reporting Center (SRC):

- » Monitoring network activity is crucial for ensuring compliance with legal and corporate requirements. You can consolidate network-wide information about device activity and data transfers by using the Security Reporting Center. Choose from standard report formats or create your own customized reports from the auditing data. Dynamic report creation, flexible filtering and sophisticated grouping functionality combine to let you find the information you're looking for within seconds. Once you have created a report, you can print it, export the data for further analysis or even send the report by e-mail.



Full Disk Encryption (FDE):

- » Transparent encryption protects all data on your hard drives without requiring users to change the way they work. **DriveLock** 5.5 secures all partitions using FIPS 140-2 certified encryption, including the system partition. Access is controlled using Pre-Boot Authentication. Encryption happens entirely in the background and doesn't disrupt the use of the computer. Single sign-on lets users log on using their regular Windows credentials and without multiple authentication prompts. Emergency logon and recovery tools ensure that you're in control, even when the unforeseen happens. Administration is intuitive and simple, as you would expect from **DriveLock**. All settings are configured using central policies that are controlled by a central management console and encryption is monitored by the Security Reporting Center.



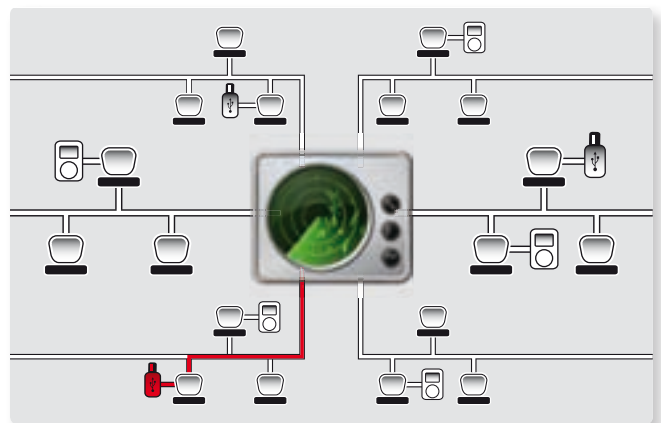
Encryption for Windows Mobile:

- » **DriveLock** 5.5 adds encryption for data stored on Windows Mobile devices (Pocket PC 2003, Windows Mobile 5 and Windows Mobile 6). You can open the same encrypted containers on your mobile device and your PC. Encrypted containers appear under Windows Mobile as virtual storage cards.



Device Scanner:

- » The Device Scanner creates an inventory of all devices that are currently or were ever attached to the computers in your network. You can easily use the Device Scanner results to create a **DriveLock** policy that allows the use of some of these devices.

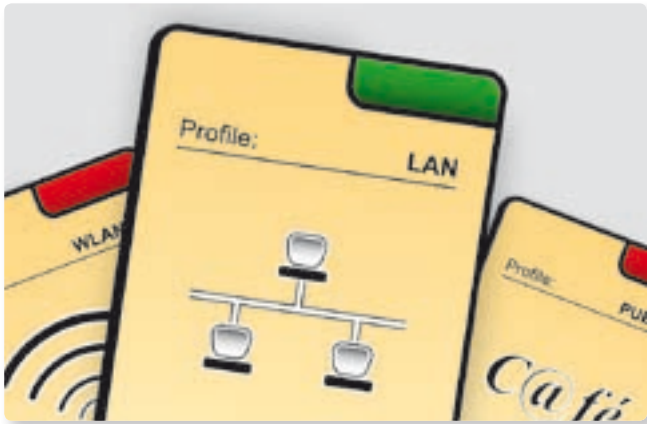


Companies have come to rely on CenterTools for efficient enterprise-ready tools – intelligent software solutions that solve tough problems, simplify difficult tasks and automate routine administration tasks.

We help IT professionals do their jobs securely.

DriveLock

Intelligent control of mobile devices



Network Profiles:

» **DriveLock** immediately recognizes when the computer is connected to a different network and applies the settings you configured for this network. Each drive, device or application whitelist rule can be set to apply to one or more network profiles, which correspond to specific networks. You can use network profiles to prevent connections to unapproved networks. You can also ensure whether devices or applications can be used while a computer is connected to your corporate network or while outside the office. To prevent network intrusions you can automatically disable wireless connections while a computer is connected to your company LAN.



Application Launch Filter:

» Protect your network against zero-day exploits and Trojan Horse programs by allowing only authorized programs to be used. You can also control who can run which application. This is especially useful on Terminal Servers. You can also make programs available only when a computer is connected to a specific network. The high flexibility and ease of configuration of the Application Launch Filter combine to make it an invaluable tool for making your network more secure.

File Filtering:

» Control what can be copied to or from removable media. **DriveLock** can allow or block the copying of files according to your rules. File types are identified based on content, not just by file extension. You can choose from the many file types that **DriveLock** can identify, or you can create additional file definitions and even extend the rule processing by creating your own custom DLLs.

Removable Media Encryption:

» Accidental disclosure of sensitive data due to lost or stolen storage devices can be very costly. **DriveLock** can give you peace of mind by automatically and transparently encrypting data that's copied to removable drives. When you need to ensure that only encrypted data is stored on these devices, **DriveLock** can enforce encryption and monitor data transfers for compliance reporting. If you need to work on your data at home or share files with someone else, the Mobile Encryption Application lets you access your encrypted information even on computers where **DriveLock** is not installed, and without the need for local administrative rights.