

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



System Requirements:

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