



BeCrypt DISK Protect™

Full-Disk Encryption Solution for Laptop and Desktop Computers



The BeCrypt DISK Protect will:

- encrypt the entire drive
- enable all software to run
- compatible with all of the various ADS endpoint security options.

Three layers of security

- Full disk encryption. On installation, DISK Protect encrypts the hard disk(s) using a unique Encryption Key. From then on data is automatically decrypted and re-encrypted on the fly (as and when required). If an unauthorized user tries to bypass authentication, all data remains encrypted and unreadable. Encryption overhead is minimal with no noticeable impact on performance.
- Pre-boot authentication. DISK Protect can authenticate the user by password, by password and Clippy, or by smart card and PIN. Authenticating the user pre-boot allows DISK Protect to encrypt the entire hard drive, including the Operating System, preventing access using low level tools.
- Removable media encryption. Optional removable media encryption secures data on USB-connected storage devices and floppy disks. If the removable device contains unencrypted data, the user can opt to preserve the data during device encryption. Devices may be password protected to permit secure access by non-DISK Protect users.

Internal data security threats are no longer just an IT issue, but a business survival issue



The **BeCrypt Disk Protect** product:

- BeCrypt Protect Manager™
- BeCrypt Removable Media Module™
- BeCrypt Connect Protect™
- BeCrypt PDA Protect™

The Way It Works

FIPS 140-2 compliance

DISK Protect 4.2 is undergoing FIPS 140-2 Level 1 validation, and may optionally be installed in a FIPS-compliant mode.

Secure wipe mechanism

DISK Protect's built-in secure wipe mechanism greatly simplifies the decommissioning and recommissioning of machines.

Multiple users

Each protected machine supports one or more DISK Protect Administrator and multiple user accounts. Every user has a unique password or password and token.

Single Sign On (SSO)

Single Sign On simplifies start up by synchronizing the user's DISK Protect and Windows passwords—whenever the user changes his or her Windows password, DISK Protect sets its own password to the same value. From then on, the user simply enters his or her Windows password into the DISK Protect authentication screen, and (providing the password is correct) is automatically logged in to Windows. If authentication is by smart card, Single Sign On provides automatic PIN entry to confirm the user's Windows certificate.

Transparency

Once the user has logged in, DISK Protect operates transparently and standard Windows applications can be used as normal. All data is encrypted automatically, and there is no risk that the user will forget to encrypt sensitive files.

Secure hibernation

Hibernation allows a computer to start up rapidly by storing an image of system memory at shutdown. DISK Protect intercepts the hibernation process, encrypting the hibernation file as it is written to disk and decrypting it on start up, allowing the system to boot rapidly with no threat to security.

System management

The DISK Protect Management Tool is an easy-to-use interface that, for example, permits DISK Protect Administrators to add or remove users, reset a user's DISK Protect password (restoring access to the computer if the password is forgotten), and

Device recovery

If a user fails three attempts to authenticate, DISK Protect denies access and displays a challenge code. Using whatever secure procedure the organization has laid down, the user must contact an administrator and provide the challenge code, which is then used to generate a response code that must be entered into the locked computer to regain access. The user is then allowed to update the password. At no time in this procedure is the user's original password exposed.

Alternatively, if the administrator can physically access the locked computer, he or she may restart the machine, enter his or her own DISK Protect Username and password, log in to Windows, and use the Management Tool to reset the user's password.

Token support

DISK Protect supports Aladdin R2e and eToken PRO USB tokens, Setec smart cards, and RSA 5100, 5200, 6100 and SID800 smart cards to provide dual-factor authentication. Extended smart card support allows an organization to use a card that is already part of its security systems, issuing its staff with a single card for access control and authentication.

Easy installation

DISK Protect may be installed and configured on individual client computers; or installed on multiple clients via an Installation Package.

Modules

BeCrypt Protect Manager™

Centralized security management and auditing functionality for the enterprise.

BeCrypt Removable Media Module™

Cost effective encryption of data on removable storage devices such as USB thumb drives and SD Cards.

BeCrypt Connect Protect™

Port Controller for desktop and laptop PCs manages access to Plug and Play devices.

BeCrypt PDA Protect™

Comprehensive PDA security solution enforces strong authentication, secured synchronisation and encryption of removable memory cards. Combines UK-government-approved technology with additional features for business users.

© BeCrypt Inc. 2007 All Right Reserved. The BeCrypt Logo and Trademarks are owned by BeCrypt Inc. No material may be reproduced for any purpose, private or commercial, without prior written permission from BeCrypt Inc.



© ADS Inc. 2008 - All Right Reserved

Access Denied Systems, Inc.

10764 Indian Head Industrial Blvd.
St. Louis, Missouri 63132-1102

Phone: (314) 890-8566 Fax: (314) 890-9949
www.accessdeniedsystems.com