



Access Denied™

S Y S T E M S

BeCrypt Protect Manager™

Provides a Central Management Resource for BeCrypt Modules

BeCrypt Protect Manager provides a secure, centralized resource for the management of encryption keys and the storage of recovery data, with controlled access via a management Console.

Feature Summary:

- Secure, centralized storage for the recovery data generated when BeCrypt DISK Protect is installed on a client computer.
- The easy-to-use Protect Manager Console provides controlled access to the Protect Manager database, permitting an administrator to monitor the entire installation.
- A distributed Device Recovery Console provides controlled, limited access to the Protect Manager database, permitting a Recovery Console User to help an end user unlock their protected machine without exposing the user's original password or compromising data



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

The BeCrypt Protect Manager™ :

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

The Way It Works

Protect Manager database

Client computers are automatically registered with the Key Manager database as part of a BeCrypt DISK Protect installation. Recovery data, including the encryption key used to encrypt the computer's hard disk, is written to the database. All data is asymmetrically encrypted before being transferred across the network. Once stored in the database, data is protected by AES encryption. The database remains 'locked' until the Protect Manager administrator logs in to the Protect Manager Console. Once the administrator has been authenticated, Protect Manager provides full access to the database, decrypting and re-encrypting data on the fly (as and when required). The database is re-locked when the administrator logs out.

Protect Manager Console

Initial encryption of a client computer does not begin until the appropriate recovery data has been written to the Protect Manager database. Once initial encryption is underway, the client sends regular status updates to Protect Manager, allowing the administrator to remotely monitor its progress.

Details of each protected machine may be viewed in the Protect Manager Console; specific data may be extracted using custom SQL queries.

In addition, the Protect Manager Console permits the export of DISK Protect Encryption Keys (for auditing purposes), the allocation and management of RSA Encryption Keys (which are used to secure communication between the various components of the Protect Manager system), and allows the administrator to

Device Recovery

If an authorised user enters the wrong DISK Protect password more than the permitted number of times the protected computer remains locked and the data it contains is inaccessible.

Device Recovery is a mechanism that allows an end user to unlock the machine with the help of an administrator, without exposing his or her password or compromising data security. It involves entering a code generated from recovery data that was saved during installation.

The Device Recovery Console may be installed on several clients. Each copy of the Console supports a single Console User and permits controlled, limited access to the Protect Manager database.

When helping an end user to unlock his or her computer, the Console User enters the 'challenge code' (displayed by the locked computer) into the Device Recovery Console which uses the appropriate recovery data to generate a 'response code' with which the end user can unlock the machine.

Monitoring Device Recovery

Details of each Device Recovery event, including the identities of both the Console User and the end user, are logged by Protect Manager and can be monitored by the Protect Manager administrator via the Protect Manager Console.

Flexible architecture

The components of Protect Manager may be installed on a single machine or distributed amongst several machines. Protect Manager is easily integrated into the existing IT structure.

Modules

DISK Protect™

Full disk encryption solution with strong pre-boot authentication and comprehensive removable media protection. Combines UK government-approved technology with additional features for business users.

BeCrypt Removable Media Module™

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

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 Connect Protect™

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

© 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.



Access Denied
S Y S T E M S

© 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