



Access Denied™

S Y S T E M S

BeCrypt Connect Protect™

Complete Port Control Solution for Plug and Play Devices

BeCrypt Connect Protect will:
protect an enterprise from
the accidental or malicious
leakage of private or sensitive
data



Connect Protect:

- Fine-grained control of Plug & Play devices
- Centralized management
- Protects against data leakage and the installation of unwanted software or the user's personal data (which can introduce viruses)
- Integrates with Microsoft Active Directory to permit the use of group policies
- Allows the auditing of device usage, logging connection and copy events to a Central Audit Server, where they may be viewed via the BeCrypt Event Viewer (supplied as an MMC snap-in), and/or to the local Windows Event Log
- Restricts the use of removable storage devices to approved vendor/models and/or to pre-approved or signed devices
- Permits the controlled, audited copy of unencrypted data to otherwise restricted removable media (Audited File Copy).

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



BeCrypt Connect Protect™

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

The Way It Works

Device control

Connect Protect is a port control solution that stops the accidental or malicious leakage of data via Plug and Play devices by preventing users connecting unauthorized devices to their computers (whether the computers are connected to the network or are mobile). Connect Protect is remotely installed using standard tools, and configured via Microsoft Active Directory or via the BeCrypt Configuration Tool. Devices are configured by type and may be set to

- Enabled
- Controlled access (via Audited File Copy)
- Read-only (if applicable)
- Disabled.

Fine-grained control

For some devices, Connect Protect allows fine-grained control—allowing access, for example, only to signed devices, to devices of a specified vendor/model, or to devices with an authorized unique ID. Connect Protect provides tools for signing and for obtaining vendor/model information and unique ID's.

Centralized management

The recommended configuration method for Connect Protect is via a Microsoft Active Directory group policy. Connect Protect provides a Group Policy template, which permits the configuration (for both machines and users) of access to Device Classes and to non-standard (or new) Device Classes, and the configuration of auditing, of user authorization, and of policy conflict resolution. (For standalone PCs, the same functionality is provided in the BeCrypt Configuration Tool).

Any conflict between the computer policy and the user policy is resolved by applying the user policy. If no policy exists, all devices are disabled by default, and auditing is enabled.

User experience

In normal use, Connect Protect runs invisibly. If, however, a user attempts to use a restricted device, Connect Protect displays a warning balloon informing him or her that access has been denied. The user need take no further action and can continue working as normal, but the event may be logged.

Central Auditing

Connect Protect can be configured to log connection events (such as the attempted use of a disabled device) and file copy events (if Audited File Copy is enabled). Logs are written to

- the local Windows Event Log, where they may be viewed via the standard Windows Event Viewer, or
- a Central Audit Server, where they may be viewed via the BeCrypt Central Audit Console.

On mobile machines, events are logged on the local machine and uploaded to the Central Audit Server when the client is re-connected to the network. In addition, Connect Protect may be configured to regularly check the Central Audit database for specified events and, if they have occurred, to send email notification to an administrator.

Audited File Copy

Audited File Copy permits a user to write unencrypted data to, and read it from, an otherwise disabled device. File copying is automatically audited, and the contents of the copied file are recorded by default. Audited file copy may optionally require user authentication before it permits copying, via a centrally controlled mechanism that allocates the user a finite length of time during which he or she can copy files.

Modules

BeCrypt Protect Manager™

Centralized security management and auditing functionality for the enterprise.

BeCrypt 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 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