

## Advanced Port Control™

A CAPS approved solution that prevents the connection and use of unauthorised devices

Advanced Port Control is a CAPS approved peripheral device control solution that provides assured protection against a variety of risks associated with the use of such devices. It is specifically designed for use in environments that host protectively marked data.

### Feature summary

- Works at the bus level, automatically controlling all peripheral devices except essential Human Interface Devices and devices that have been explicitly enabled.
- Permits the system administrator to compile and maintain individual machine policies and user policies.
- Uses the CESG LOGFIRE algorithm for administrator authentication.
- Logs all connection events whether blocked or permitted.

### Installation

Advanced Port Control may be installed on individual client computers or via a software distribution platform.

### Device control

Advanced Port Control is managed via a password-protected Configuration Tool, which allows the administrator to create and maintain separate policies (white lists of allowed devices) for the client computer and for each individual user (if required).

Advanced Port Control can be configured to control by unique ID or by vendor/model data.

- if an enabled device has a unique ID, Advanced Port Control will allow access to **this specific device only**
- if an enabled device does not have a unique ID, Advanced Port Control identifies it by its vendor/model, and will allow access to all devices of the same vendor/model. If this level of access is not acceptable, the device may be disabled.

### Policy maintenance

Machine and user policies are created and maintained by compiling and editing lists of allowed devices.

Existing user policies may be exported as text files and imported onto additional machines. Since an imported user policy includes the user ID, Advanced Port Control automatically creates a new user on the second machine, if necessary.

Policy conflicts are resolved by applying the user policy in preference to the machine policy. If no policy exists, Advanced Port Control disables all devices except those that are enabled by default.

### Auditing

Advanced Port Control logs all connection events, permitted or blocked, to the Windows Event Log.



## DISK Protect™

PC security solution combining full disk encryption with strong boot time authentication and optional removable media encryption.

**DISK Protect 4.1** has been awarded the CCT Mark;

**DISK Protect Baseline** is CAPS approved to Baseline;

**DISK Protect Enhanced** is CAPS approved to Enhanced grade.

## Removable Media Module

Encryption of data on removable storage devices such as USB Flash Drives, memory devices and SD Cards.

## PDA Protect™

PDA security solution that enforces strong authentication, secured synchronisation and the encryption of removable memory cards.

**PDA Protect 4.1** has been awarded the CCT Mark.

## Connect Protect™

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

**Connect Protect 2.0** has been awarded the CCT Mark.

## Trusted Client™

Secure, isolated, configurable operating system for use in an unmanaged environment providing functionality customised to an organisation's requirements.

**Trusted Client 1.2** has been awarded the CCT Mark.

## BeCrypt Enterprise

Centralised, scalable security management suite based on Open Standards.

Provides comprehensive assurance for end-point and infrastructure, with low cost of ownership.

© Copyright 2008  
by BeCrypt Ltd.

All Rights Reserved.

The BeCrypt Logo and Trademarks  
are owned by BeCrypt Ltd.

No material may be reproduced for any  
purpose, private or commercial,  
without prior written  
permission from  
BeCrypt Ltd.