#becrypt

Data Protection

Disk Protect : Enhanced

A full disk encryption solution for laptops, desktops, tablets and servers, Disk Protect Enhanced is CAPS approved to handle protectively marked data to Enhanced grade.

Disk Protect Enhanced is an approved solution for encrypting data on laptops, desktops, tablets and servers whilst enforcing a centrally defined security policy.

Full Disk Encryption

Disk Protect Enhanced transparently encrypts devices' hard disk(s) using entropy supplied by CESG. Once encrypted, data is automatically decrypted and re-encrypted, as and when required. Encryption overhead is minimal with no noticeable impact on performance.

Pre-boot Authentication

Disk Protect Enhanced enforces mandatory dual-factor authentication by username, password and token. Authenticating the user at pre-boot allows the software to encrypt the entire operating system, ensuring that data cannot be accessed using low-level tools. If users attempt to bypass authentication, the data is encrypted and unintelligible.

Removable Media

For safe transportation, Disk Protect Enhanced secures data on removable disk drives and USB-connected storage devices by encryption. Data may be encrypted using a shared key to allow the transfer of data between authorised users. Disk Protect Enhanced may also be configured to allow the use of unencrypted media. Use of specific removable media may require an additional port control solution, such as Becrypt Advanced Port Control, to provide the necessary level of security.

Transparency

Once the user has logged in to Windows, Disk Protect Enhanced operates transparently, with the ability for standard applications to be used as normal. Since all data is automatically encrypted, there is no risk that the user will forget or negate to encrypt sensitive files.

Device Recovery

Recovery data generated during installation permits an administrator to start up the device, without the touch token or password, in order to perform disk repairs.

Token Support

Disk Protect Enhanced enforces mandatory dual factor authentication using a USB token.

Specifications

- CAPS accredited
- Removable media encryption
- Pre-boot authentication
- Multi-user support at pre-boot
- Two-factor authentication (2FA)
- Stand-alone capability
- Requires CESG sales approval
- Requires CESG key material

CAPS
CESG Assisted Products Service

For more information on Becrypt and our solutions, contact us:

info@becrypt.com

0845 838 2080

#becrypt.com

#becrypt

Data Protection

Disk Protect : Enhanced

Specifications

Supported Hardware

> Laptops
> Desktops
> Tablets
> Servers

Boot Method

> BIOS

Supported Disk Format Types

> MBR

Types of Hard Disk Supported

> HDD (spinning)
> SSD

Operating Systems

Desktop;
> Microsoft Windows 7
> Microsoft Windows 8.1
Server;
> Windows Server 2008 R2
> Windows Server 2012 R2

Encryption Algorithm

AES 256 bit

Supported Tokens

> eToken PRO
> eToken Java
> SafeNet 5100
> SafeNet 5105
> SafeNet 5110
> Gemalto .NET v2+
> Gemalto .NET v3
> RSA SID 800 series
> Dallas/Maxim iButton tokens

Existing Data

It is a CESG requirement that the hard disk(s) must contain no protectively marked data prior to installation. Initial encryption of the hard drive(s) does not delete existing data, but it is recommended that existing data is backed up prior to installation, and you may prefer to perform a full system backup.

User Authentication

Authentication is by username, strong password and mandatory token. Password policy is set locally.

Multiple Users

Disk Protect Enhanced requires one System Administrator who manages user accounts and performs security-sensitive actions. Each machine also supports up to 16 users.

Purge

The purge feature may be triggered at pre-boot or following authentication. Purge destroys essential data, rendering the device unbootable and ensuring that any user data it contains is inaccessible.

Removable Media Encryption

Removable hard disk drives or USB devices may be encrypted using a Transport Key. Disk Protect Enhanced may also be configured to support pre-encrypted devices.

System Recovery

User passwords and tokens are updated or replaced locally by the System Administrator. Full system recovery is performed using recovery data generated during installation.