#becrypt

Data Protection

Disk Protect : Standard

A full disk encryption solution to protect data-at-rest held on desktops, laptops, tablets and servers from theft or loss.

Disk Protect Standard is Becrypt's full disk encryption solution for securing organisations' data, whether on desktops, laptops, tablets or servers.

Disk Protect ensures that all data is safely encrypted, with no change in performance for the end user. Designed to enable security conscious organisations to deploy their workforce with confidence, the FIPS 140-2 accredited software is compatible with a range of devices and operating systems.

How it Works

Disk Protect encrypts every section of the hard drive, preventing unauthorised access. Using strong user authentication, unauthorised access is prevented.

Disk Protect provides full disk encryption, without any disruption to usability. Once the user has logged in to Windows, Disk Protect 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 can circumvent encryption.

Disk Protect can also encrypt the data on removable media such as, Firewire, USB devices, SD cards, other mass storage devices and local disks.

Full Management

When combined with Becrypt Enterprise Manager, Disk Protect can be deployed throughout an organisation with little or no disruption to business activities. The solution can be deployed to thousands of users in the organisation quickly, with devices secured within hours.

The combination of centralised management, one-factor authentication and single sign-on ensures that Disk Protect Standard is easy to deploy, manage and use.

Specifications

- FIPS 140-2 accredited
- Installation to Windows 10, 7 and 8, BIOS and UEFI from single installer
- Single sign-on
- Secure hibernation
- Secure wipe for decommissioning
- Removable media protection
- Multiple users per device

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

info@becrypt.com

0845 838 2080

#becrypt.com

#becrypt

Data Protection

Disk Protect : Standard

Specifications

Supported Hardware

> Laptops
> Desktops
> Tablets
> Servers

Supported Disk Format Types

> MBR
> GPT (fixed disk only)

Boot Methods

> MBR
> UEFI

Types of Hard Disk Supported

> HDD (spinning)
> SSD
> RAID

Operating Systems

Desktop;
> Microsoft Windows 10
> Microsoft Windows 8.1
> Microsoft Windows 7

Server;
> Windows Server 2012 R2
> Windows Server 2008 R2

Encryption Algorithm

> AES 128 bit

Accreditation

> FIPS 140-2

Existing Data

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 enforced by a local policy in the standalone variant, or a server-based policy in the managed variant. When used in the context of an Active Directory domain, Disk Protect supports single sign-on.

Multiple Users

A single Disk Protect device supports up to 25 pre-boot users. In the managed variant, all users can be provisioned and administered remotely via the management console.

Policy

Configurable settings include password policy (expiry, length, complexity, etc), password management, user account management.

Safe Decommission

Disk Protect's secure wipe function destroys essential data, rendering the device unbootable and ensuring that any user data it contains is inaccessible.

Device Recovery

If a user forgets their password, a dynamically generated challenge code is used by a Service Desk operator to generate a response code. The user enters this into the computer to gain temporary access and set a new password.