#becrypt

Data Protection

Connect Protect

Becrypt's port control solution, Connect Protect, provides simple and efficient access control options for end point connectivity to removable devices and media.

Connect Protect is Becrypt's end point control solution that protects organisations against data leakage. By preventing unauthorised access or use of external devices and providing centrally managed audit trails for all connection events, Connect Protect enables full control.

Protecting your Data

Managing and protecting data is now top of the agenda for many senior personnel, but with an increasing number of external devices being used (flash memory sticks, cameras and mobile phones), organisations run the risk of their data being vulnerable to theft, accidental or malicious loss or even the risk of data or viruses being imported into the network.

To protect themselves from vulnerabilities, organisations require a centrally managed policy to ensure that the usage of such devices is controlled.

Connect Protect Overview

Connect Protect prevents unauthorised devices from connecting to the network, with the ability to restrict their use to approved devices only. Enabling organisations to enforce a usage policy, Connect Protect provides a full audit trail to track device usage and highlight denied and authorised connections.

Connect Protect's digital signing capability for approved devices allows organisations to strictly control what type and how many removable storage devices are in use. This also prevents authorised devices from being cloned.

How it Works

Connect Protect uses filter drivers to allow/deny access to devices. Depending on policy, any external device may be connected, but not accessible, unless the machine or user has permission to do so.

Connect Protect also allows the signing of removable media, allowing an administrator to sign any removable media device and prevent access to media that has not been signed. The product can also make use of Active Directory group polices, allowing simple and familiar management of the product and the policies across organisations.

All user and machine events can be logged (even if the device has not been blocked) allowing an administrator to closely monitor the external devices that are being connected to machines on the network.

Specifications

- Challenge responses
- Supports whitelisting
- Integrates with Active Directory groups
- Central auditing and reporting

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

info@becrypt.com

0845 838 2080

#becrypt.com

#becrypt

Data Protection

Connect Protect

Specifications

Supported Hardware

> Laptops
> Desktops
> Tablets

Operating Systems

> Microsoft Windows 10
> Microsoft Windows 8.1
> Microsoft Windows 7

Controlled Device Types

> Removable disk devices
> Optical disk devices
> Serial and parallel ports
> Modems
> Imaging devices
> Removable network devices
> Smartcard readers
> Infrared devices
> Bluetooth devices
> Printers
> PDAs
> Tape drives
> Internal disk drives
> Others

Whitelists

Connect Protect whitelists are created in the Becrypt Enterprise Manager console and pushed out as appropriate. Whitelists may be applied to individual devices and/or users, groups of devices or users or individual Active Directory OUs. Devices are whitelisted on the basis of device type, make and model, or unique ID.

Audits

All user actions and events are logged in the management platform.

Reports

Connect Protect offers a range of preformatted reports and can be configured to generate custom reports.

Lightweight Server Requirement

Connect Protect is designed to support up to 1000 separate users per server.

Removable Devices

Connect Protect can optionally enforce the encryption of removable media (via Becrypt mShare) throughout the estate.

E-mail Alerts

Connect Protect can optionally alert administrators by email when any non-compliant user actions occur.