#becrypt

Central Management

Becrypt Enterprise Manager

A central management suite that enables organisations to manage and audit their estate of Becrypt data security products.

The Becrypt Enterprise Manager (BEM) is a centralised management solution that gives you full visibility and control of user activity. BEM enables you to easily create and apply policies, carry out fast risk assessments in the event of a lost or stolen device, easily address problems such as forgotten passwords, and aids in the set up and quick deployment of Becrypt software to your IT estate.

Management Overview

BEM's user management permits administrators to remove and control different levels of user access to devices and data. A password policy manager is integrated within user management to govern password complexity, expiration cycles and forgotten passwords, which can be reset remotely.

Should a device be lost or stolen administrators can access device management to ascertain the encryption status, and who has access immediately to assess the likely risk to the data.

Visibility and management of active and expired Becrypt security product licenses are displayed in a usable and easy to read fashion. This allows organisations to see at a glance what security products have been deployed, where, and most importantly, how effective they are.

Auditing and Reporting

Every user event is logged and reported in the BEM database, such events include; unsuccessful logon, successful logon, plugged in media and access to data. All user actions are reported and can be audited quickly, giving the organisation the ability to demonstrate compliance with minimal fuss.

Additionally administrators can apply Proactive Notifications, this is an event alert triggered from event identifiers. All possible user events are given an event identifier; Proactive Notifications can be customised to a specific event throughout the license estate or on an individual basis. A notification is sent to the administrator when a user is consistently having difficulties logging on in a short period, attempting to connect an external device that does not comply with the external plug-in policy, or attempting to access files that are not in their authorised permission. These events and many more can be setup to send an email directly to the administrators so that the situation can be investigated.

Key Management

BEM works with standard third party deployment tools as well as different domains to ensure that the roll out of encryption is faster and subsequent management overheads are minimised.
Key management is automated for Becrypt Disk Protect and Removable Media Module, greatly reducing the time and administration normally associated with key management, and helps to comply with key escrow regulations.

How it Works

BEM collects information in real-time from Becrypt software including Disk Protect, mShare Removable Media and Connect Protect. All data is stored in a database allowing easy central storage, backup and recovery. Auditing events such as password changes, key requests and user recovery are all logged centrally, and can be viewed by multiple authorised administrators from multiple locations.

Reporting functionality gives administrators an accurate picture of a devices estate and removable USB storage devices, with details such as the number of encrypted machines and devices, the users who can access them and any external devices that are being blocked.

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

info@becrypt.com

0845 838 2080

#becrypt.com

#becrypt

Central Management

Becrypt Enterprise Manager

Features and Specifications

User Management

> Aids in the set up and simultaneous mass deployment of Disk Protect
> Existing Active Directory user and machine hierarchies can be imported
> Remotely add and remove user access
> New users can be added quickly and existing users can be deleted
> User passwords can be remotely reset via device recovery

Key Management

> Keys are stored centrally in the encrypted Enterprise Manager database
> When using Removable Media, keys are stored in the users' profile and automatically made available when the user logs on

Audit and Reporting

> Real time audit trail of events
> Events can be archived or deleted
> Administrators can set email notification warnings of irregular events
> Library of pre-defined reports providing high level in-depth information
> Full search facility allows lost/stolen laptops to be quickly identified and encryption status immediately obtained

Hardware

> Minimum processor: 2.5 GHz
> Minimum RAM: 2GB
> Minimum Hard Disk space: 40 - 50MB

Operating System

Enterprise Manager Server:
> Microsoft Windows Server 2012 (64bit)
> Microsoft Windows Server 2008 R2 (64bit)
> Microsoft Windows Server 2008 (32bit and 64bit)

Enterprise Manager Console,
Managed Recovery Console:
> Microsoft Windows Server 2012 (64bit)
> Microsoft Windows Server 2008 R2 (64bit)
> Microsoft Windows Server 2008 (32bit and 64bit)
> Microsoft Windows 8.0 (32bit and 64bit)
> Microsoft Windows 7 (32bit and 64bit)
> Microsoft Windows XP (32bit)

Database

> SQL Server 2014 (64bit)
> SQL Server 2012 (64bit)
> SQL Server 2008 R2 (64bit)
> SQL Server 2008 (32bit and 64bit)