



# Integrated Laptop Encryption Drivelock FDE

*Certified Full Disk Encryption Solution  
Satisfy Compliance and Governance Requirements*

## •Key Features:

Two- Factor Authentication, supports tokens and smart cards

Single sign-on to pre-boot authentication with Windows® Log-in

Active Directory™ - fast integration with identity management

Multi-boot support for up to four bootable secured partitions with non-Windows® partitions allowed

100% full disk encryption of laptops:

· User data and files (system, hidden, page and temporary)

· Registry settings and hibernation files

· Password-based removable media

Strong authentication with password fallback

Master Virus Protection

Drivelock Management Console Integration

Easy-to-deploy across large environments

Efficient and secure data and remote password recovery

Full audit of pre-boot events, such as log-in attempts

## End-Point Security Data Loss Prevention

Emereo|EPS is a solution that helps organisations design and enable an IT security policy that will eradicate the threat of data loss, theft and unwanted intrusion.

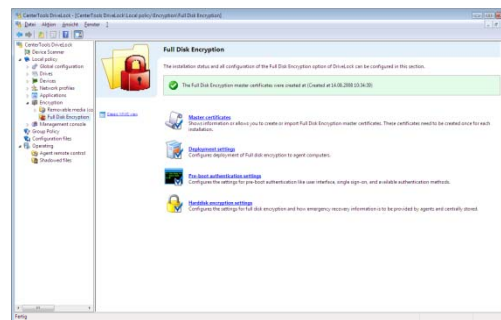
Emereo|EPS is powered by DriveLock™ from CenterTools, placing controls on devices and applications, in fact anywhere critical information resides electronically; from barring USB devices to hard-disk encryption.

DriveLock FDE stops data being lost on laptops, a scenario which continues to be the bane of many UK public and private sectors organisations. DriveLock FDE fully encrypts all hard disks (including temporary and paging files) right down to the system partition.

Once deployed a secure pre-boot authentication process with a single sign-on for Windows combine ease-of-use with added security. The authentication process can restrict access to any part of the hard drive. Full data recovery can be expedited with emergency log-on. Monitoring of encryption status can be facilitated using DriveLock's Security Reporting Centre.

## The Management Console Advantage

Many of the leading full disk encryption vendors provide standalone products with limited integration with wider data loss prevention solutions and there is no management view of encryption status. Because DriveLock FDE is deployed as part of the DriveLock family encryption status is viewable from within a Microsoft Management Console®.



Management reports to prove compliance or governance can be generated through the DriveLock Security Reporting Centre.



## Single Sign-On or Two Factor Authentication

DriveLock FDE presents two levels of secure sign-on and/or authentication.

Single sign-on to pre-boot authentication provides a seamless Windows® Log-in for users with no need to issue additional set of credentials (username & Password) for logging in to the pre-boot. Users will not place a burden on your IT help desk having forgotten multiple account details. Users only have to go through the log-in process once.

While an additional level of security is provided through DriveLock's compatibility with many 3<sup>rd</sup> party two-factor authentication tools such as tokens and smart cards. This allows fully secure access once users move from the pre-boot phase to the Windows environment after presenting a two-factor authentication tool with a given PIN or password.

## Fast Deployment Reduced Management Costs

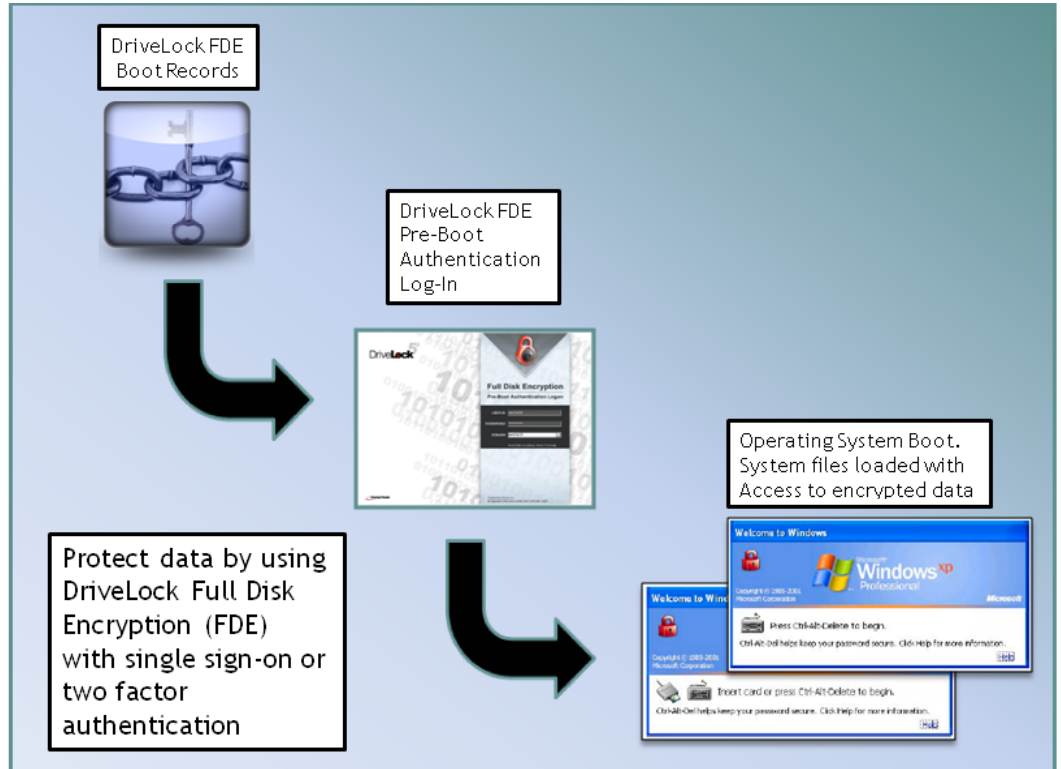
Because directory services are the most logical place to store information about network resources and domains it makes sense for DriveLock FDE to leverage these. Consequently DriveLock uses services such as Active Directory and e-Directory to speed deployments across large environments.

Complete roll-outs can be expedited using MSI Install parameters or Active Directory Group Policy Objects (GPO). The results are quick and with high user acceptance.

The advantages provided include the ability to centrally manage disk encryption functions in a framework many administrators will be familiar with while end-users need no training at all. Quick to realise and with low management overhead.

DriveLock FDE uses technology recognised as being certified to Common Criteria EAL4 by the National Technical Authority for Information Assurance or CESG and has FIPS 140-2 certified encryption algorithms.

DriveLock FDE encrypts and decrypts data 'on the fly' using strong encryption algorithms including AES-256.



**Secure, Manageable Removable Media  
Secure, Productive Staff**

Emereo's solution is based upon the mantra of "Protecting Your Organisation Without Inhibiting Your People". We recognise that in encrypting laptops many staff still legitimately need the freedom of using removable devices, such as a USB stick to pass a presentation to a colleague and IT don't need the burden of monitoring every usage event or changing rights on a one-by-one basis.

DriveLock FDE lets you set the standard. Once classes of removable media have been tagged as "Company approved for use", DriveLock FDE will recognise these, right down to unique serial numbers for devices. The solution then provides password-based protection which only authorised users can access. Some staff will be able to use these devices outside the IT perimeter while others can be restricted.

Additional configuration of allowable device types and port management brings all removable media under central control.

The net result is an organisation with data secure on every laptop and removable device and with staff able to work in the manner they want to.

**Compliance & Governance**

With IT Security and the need to prevent data loss high on public and private sector agendas, Emereo Solutions consulting approach is based upon a requirements methodology which can fast-track internal IT and corporate governance and achieve compliance.

Emereo Solutions has already satisfied the information management aspect for securing data and preventing loss and theft the Government Connect Code of Connection (CoCo), FSA, ISO 27001 and Sarbanes Oxley.

Emereo Solutions provides rapidly-deployed software solutions for infrastructure management covering network management and monitoring, network behaviour analysis, end-point security and data loss prevention. Our solutions help organisations secure greater resilience of their enterprise networks so IT can provide better services to the business and operations it supports. Best-of-Breed products adhere to ITIL and COBIT best practice and ensure compliance with initiatives such as Sarbanes Oxley, FSA, GSI, e-Health.

Emereo Solutions (UK) Limited was founded in 2004 and its installed base serves a diverse range of customer types base from Government, the NHS, Education, Financial Services, Law firms and many more where the goal is making IT effective and available. Our solutions have been deployed on over 15,000 servers across the UK and Ireland.