

# SecureDrive

A comprehensive data protection solution based on industry standards

Data compromise and breach can lead to strong fines for potential compliance violations and high-profile public disclosure embarrassment resulting in huge financial losses. Protecting data with strong encryption on the hard drive mitigates this risk and must be a top priority for any organization.

## Introduction to Self-Encrypting Drives (SED's) and the TCG Opal Specification

Hard-drive vendors are now building self-encrypted drives (SEDs) to adhere to the Opal specification as defined by the Trusted Computing Group or TCG. TCG's Opal specification (released in early 2009) adds security to hard drives and eliminates data breaches from a stolen or lost PC, by ensuring that every byte of data on the hard drive is encrypted using the hard drive's internal electronics. More information on the Opal Security Subsystem Class Specification for PC clients is available at [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)

Softex's SecureDrive product is developed to support the new Opal hard drives from manufacturers as they are released in the market.

## SecureDrive Data Protection Solution

Self-encrypting hard drives have clear advantages over traditional software-based encryption. First, deployment is much simpler and faster as the set up and configuration does not require any "conversion" of the drive to an encrypted state. This can save hours of setup time for the end user. Second, there is a significant performance improvement because the encryption is done using the hard drive's internal electronics thus consuming less computing horsepower on the CPU of the PC. And finally, this is a cost-effective solution over existing software-based encryption solutions.

SecureDrive is an addition to Softex's existing security suite of products to take full advantage of the encryption and security features of Opal self-encrypting drives (SED's). SecureDrive allows for easy set up and configuration of the encryption and access rights and allows for multiple authentication mechanisms such as fingerprint, smart card, RFID cards and TPM passphrase to unlock the Opal drive. Single Sign On (SSO) to the desktop is provided so that the user just has to authenticate once to unlock the hard disk encryption and boot into the Windows desktop. SecureDrive also allows administrators to remotely perform a secure erase of the data from the drive to simplify PC end of life processing. Seamless integration with the new Intel vPro Technology and Remote Encryption SDK (AMT) allows for PCs (powered on or off) to be remotely unlocked by the I/T administrator to perform management tasks such as software installation and patch management.

## Key Features at a glance

- Manage and configure Opal standard based Self-Encrypting Drives (SED).
- Unlock the Opal drive with pre-boot authentication (PBA) using strong authentication such as fingerprint, smart-card, TPM.
- Support for Single Sign On (SSO) to the desktop.
- Enterprise-class centralized manageability allows for policy control using MMC.
- Transparent file and folder encryption complimentary to Opal security.
- Secure Erase of data for PC end-of-life (EOL) or drive decommissioning.
- Remote, out-of-band management with Intel 2010 Intel® Core™ vPro™ Technology.
- Recovery capability of lost passwords with emergency login mechanisms.
- Strong tracking and auditing capability to support mandatory compliance.
- Supports Windows 7, Windows 8, Windows 8.1, Windows 10, Vista, XP and Server 2003.

## SecureDrive Features

### Management of self-encrypting drives(SED's)

- Easy set up and configuration of Opal encryption security features that are accessible by multiple users and/or groups of users (per the Opal spec)
- Comprehensive standards-based solution based on TCG Opal specification

### Pre-Boot Authentication (PBA) and SSO to Desktop

- Linux based PBA module running from the secure MasterBoot Record (MBR) shadow area of the Opal SED that allows for strong authentication and boot up to the Windows desktop
- PBA module can be enabled to support Single Sign On (SSO) to the PC, thus eliminating the need to reauthenticate at Windows login

### Strong Authentication and Multi-factor Login Support

- PBA module supports strong authentication mechanisms such as fingerprint, smartcard, passphrase, TPM, etc such that only authorized users will be able to unlock the drive and access the data
- Emergency login and recovery capability

### Enterprise-class Centralized Manageability

- Allows I/T management of SED users, policies, as well as system maintenance and end-of-life (EOL)
- Integration with existing Active Directory/ADAM and Novell eDirectory environment allows for easy deployment and management
- Standard Microsoft Management Console (MMC) plug-in

### Transparent File and Folder Encryption

- Complimentary feature to SED's secures sensitive data on files/folders once the drive is unlocked
- Enterprise-wide file sharing with strong authentication

### Secure Drive Erase capability

- Remotely initiate key erase to wipe out drive data at the end-of-life(EOL) of PC or drive de-commissioning
- Eliminates need for costly data destruction mechanisms

### Support for remote, out-of-band management features of the new 2010 Intel® Core™ vPro™ Technology

- Allows PC's (powered on or off) to be remotely unlocked by the I/T administrator to perform management tasks such as software installation and patch management
- Remote encryption management support in SecureDrive can be used in conjunction with thirdparty management consoles supporting the Intel vPro technology



*For more information about SEDs and the OPAL standard, visit the Trusted Computing Group Website at*

*[www.trustedcomputinggroup.org/solutions/dataprotection](http://www.trustedcomputinggroup.org/solutions/dataprotection)*

## Recovery capability of credentials or lost passwords

- Emergency login mechanism in case of any crashes or authentication device malfunction
- Self-service (self service password reset based on Q&A) or Admin-assisted (challenge-response) recovery

## Strong Tracking and Audit capability

- Strong audit and tracking capability to support mandatory compliance with privacy and data breach regulations such as HIPAA, Sarbox, etc
- Logs maintained in the event viewer of the server

## SecureDrive Modules

### SecureDrive Client Edition

Manages encryption for standalone PCs and is pre-loaded on multiple computing devices.

### SecureDrive Enterprise Edition

Allows centralized manageability of SED users, policies including backend integration with Active Directory/ADAM and Novell using a standard MMC (Microsoft Management Console) plug in.

## About Softex

Softex, founded in 1992 in Austin, Texas, is a market leader and provider of security software and solutions with innovative products focused on Enterprise Single Sign On (ESSO), Identity and Access Management (IAM), and Data Protection of Self-Encrypting Drives. Softex offers both on-premise and Cloud-based security solutions to HealthCare, Financial, Corporate, Government and OEM markets with a focus on strong user authentication and helping its customers meet industry compliance. Softex serves many of the top tier companies, such as Lenovo, Hewlett-Packard, Fujitsu, Samsung, Accenture and Motion Computing.

For more information about Softex, visit [www.softexinc.com](http://www.softexinc.com)

Corporate Headquarters

### Softex Inc.

9300 Jollyville Road  
Suite 201  
Austin, TX 78759 U. S. A.  
(512) 452 8836 Main  
(512) 795 8702 Fax  
[www.softexinc.com](http://www.softexinc.com)

Regional Headquarters

### Softex Infotech Pvt. Ltd.

No. 16, Shram Sadhana Bldg.,  
Hindu Colony Lane No 1,  
57 Dr. D. V. Pradhan Road, Dadar (E),  
Mumbai - 400014 I N D I A  
+91-22-2414 6432 Main  
[www.softexinc.com](http://www.softexinc.com)

© 2015 All rights reserved. All brand and product names and trademarks are property of their respective holders.

DOC#: SFTX-DS-SD-V1-042915