

EMBASSY® Trusted Drive Manager

- Lifecycle management for Samsung, Seagate and all OPAL-compliant self-encrypting hard drives (SED)
- Pre-boot authentication and single sign-on to Windows®
- Manages the advanced security features of self-encrypting hard drives
- Provisions self-encrypting hard drives in minutes, not hours
- Enables remote management of self-encrypting drives using Wave Systems' EMBASSY Remote Administration Server
- Provides backup and recovery for user passwords of self-encrypting drives

Self-encrypting drives are laptop hard drives that integrate full disk encryption with the drive's hardware and firmware, offering state-of-the-art data protection for personal and corporate laptop users. They provide an on-board security controller for full disk encryption and pre-boot authentication based in hardware. Self-encrypting drives encrypt data with no performance overhead, are tamper-resistant and protect against brute force password attacks. Those important security features are what distinguish a self-encrypting drive from a standard hard drive. Wave Systems' EMBASSY Trusted Drive Manager is a software application that activates and manages the drive's advanced hardware security features.

Security from Start to Finish

Wave's Trusted Drive Manager handles all of the drive's lifecycle functions from initializing the pre-boot authentication to drive de-commissioning. The Wave pre-boot authentication feature enforces access control policies immediately as the drive powers up. The preboot authentication application displays the pre-boot screen to capture the user's drive credentials. These credentials are then compared against the credentials that were stored in the drive's hardware-protected credential cache during user enrollment.

Key Benefits

Ensures only authorized users gain access to sensitive data on self-encrypting drives

Supports environments that require shared workstations

Facilitates the speedy setup of self-encrypting drives with an easy-to-use graphical user interface

Locks down drive security settings to prove that encryption is continuous and operational

Eliminates significant costs associated with "wiping" data off a drive by performing an instantaneous cryptographic erase

Single Sign-On/Windows Password Synchronization

Support for single sign-on allows users to authenticate to the Trusted Drive and automatically log into Windows without authenticating separately to Windows. Additionally, when the drive administrator enables Windows Password Synchronization (WPS) on the platform, a user's drive password is automatically synchronized with the user's Windows password. In an enterprise environment that requires the changing of passwords at a predetermined time interval, this feature adds simplicity and ease of management for both administrators and users.

Zero-Touch Provisioning of FDE drives

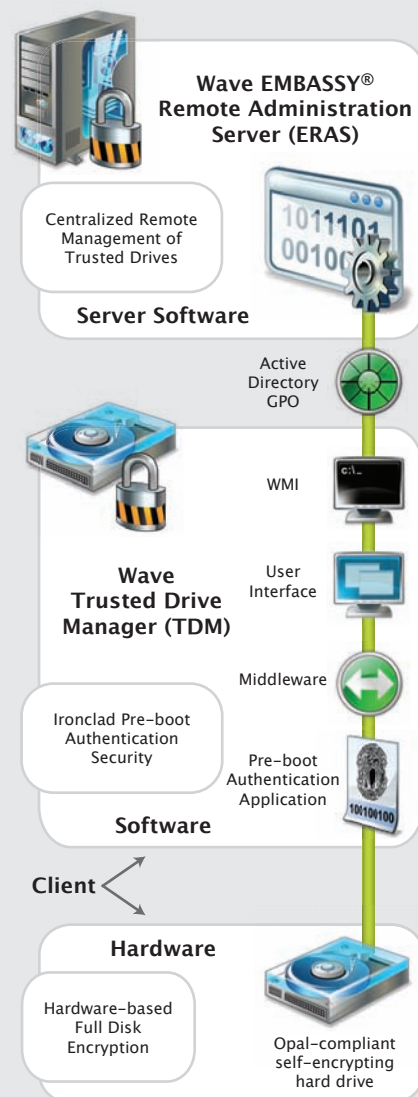
Used in conjunction with the Trusted Drive Manager on the client, the EMBASSY Remote Administration Server (ERAS) enables "zero-touch" deployment of self-encrypting drives in the enterprise. All Trusted Drive initialization and provisioning functions can be executed remotely using ERAS. ERAS references identities and access privileges against the policies defined in Active Directory. Automated scripts can also be created to have true zero-touch deployment and management of self-encrypting drives.

ERAS provides a critical time-saving advantage and cost reduction over solutions which employ software-based FDE. Deployment time can run several hours for software-based FDE, accounting for the time it takes to encrypt data bit-by-bit. In an enterprise with self-encrypting drives and ERAS, drives can be provisioned remotely in only a few minutes.

Secure and Easy Drive Re-Purposing and De-Commissioning

In today's dynamic business environment, PCs are frequently re-purposed when organizational structure changes or work is outsourced. Furthermore, drives are frequently disposed of. Typically, this is a time-intensive process to ensure that the data on the drive is completely destroyed. The Trusted Drive Manager makes it possible for a drive administrator to destroy the drive's encryption key, which renders all the data on the drive instantaneously and permanently unreadable. The entire file system is cryptographically wiped out, allowing the drive to be re-purposed or disposed of with confidence that no residual data can be recovered.

Technical Overview



Technical Requirements

System Hardware

Self-encrypting hard drive by Samsung, Seagate® or any approved Opal-compliant HDD manufacturer

Operating System

Microsoft Windows XP with SP2, or Windows Vista with SP1

Other Components

Wave EMBASSY Remote Administration Server (optional)