

The Leader in Endpoint Data Protection

# GuardianEdge Encrypted Drive Manager

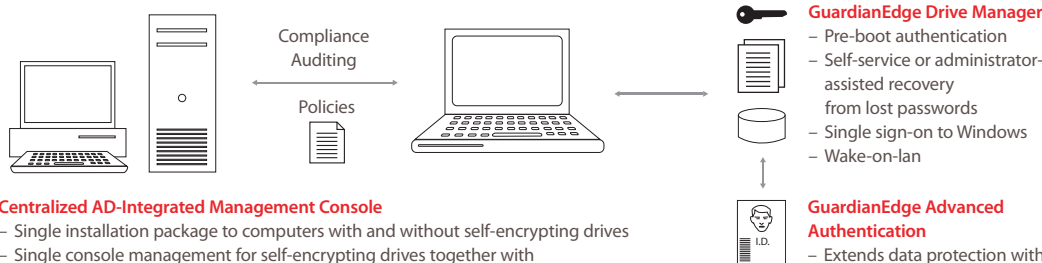
A new generation of self-encrypting Opal-compliant disk drives provides enhanced security for mobile data on PCs. GuardianEdge makes it possible to easily and effectively manage this new technology across the enterprise.

Organizations are well aware of the risks posed by unprotected data on laptop and desktop PCs. Self-encrypting drives based on the TCG (Trusted Computing Group) Opal standard protect consumers' private data, critical IP and customer or competitive information with built-in hardware encryption. They also deliver onboard key management, authentication capabilities and drive-speed encryption performance.

But protecting against the loss or theft of mobile data requires more than strong encryption. Effectively deploying Opal-compliant drives requires a standards-based solution that addresses the many operational challenges encountered when deploying any endpoint data protection technology. GuardianEdge™ Encrypted Drive Manager provides the proven management capabilities needed to reduce the cost and complexity of implementation, deployment and ongoing administration. These include activation, key escrow and recovery, policy management, directory services integration, end-user access recovery, and comprehensive reporting.

A common management interface for self-encrypting drives and the GuardianEdge Hard Disk Encryption software-based drive encryption product enables organizations to seamlessly manage hard disk encryption. In hybrid environments—where there are Opal-enabled PCs and legacy PCs with standard disk drives—organizations can easily deploy and manage both technologies from a common console.

## Enterprise-Class Protection Against Data Loss



### Centralized AD-Integrated Management Console

- Single installation package to computers with and without self-encrypting drives
- Single console management for self-encrypting drives together with software-based drive encryption
- Comprehensive reporting
- Native Active Directory integration
- eDirectory support and support for non-domain computers

### GuardianEdge Drive Manager

- Pre-boot authentication
- Self-service or administrator-assisted recovery from lost passwords
- Single sign-on to Windows
- Wake-on-lan

### GuardianEdge Advanced Authentication

- Extends data protection with certificate-based multi-factor authentication
- Pre-boot smart card, CAC, and PIV token support

## Key Features of Opal-enabled Drives Combined with GuardianEdge Encrypted Drive Manager

- “Always-on” hardware encryption
- True full disk or multi-partition encryption
- Full featured pre-boot authentication environment
- Smartcard and token multi-factor authentication with GuardianEdge Advanced Authentication
- Standards-based for industry's best scalability and availability
- Superior admin-assisted or self-service GuardianEdge Authenti-Check™ recovery of lost passwords
- Secure unattended wake-on-LAN administrative access
- Single Sign-On integration—Microsoft and Novell

# Technology Overview

GuardianEdge Self-Encrypting Drive Manager combines enterprise-class management for Opal-compliant drives with exceptional ease of use and world-class support. The result is a comprehensive and standards-based solution for protecting data from the loss or theft of a laptop or desktop. Native Microsoft Active Directory® integration enables administrators to easily manage and deploy policies via GPO. Policies can be granularly applied against groups, domains, organizational units and other Active Directory management structures.

Software deployment and updates are performed with standard system tools (SMS, Active directory GPO, etc.). Installation software detects and

responds to the presence of Opal-compliant drives when present, and can automatically install software-based encryption on legacy machines.

The GuardianEdge Encrypted Drive Manager provides support for Active Directory, Novell eDirectory, and non-domain endpoints. Single console administration with shared security and administrative services across all GuardianEdge data protection applications provides a robust, highly scalable, and complete data protection management solution for enterprise PCs.

## Technical Information

### Client Environment

- No additional log-in required (integrated with Microsoft and Novell Single Sign-On)
- Hardware-based encryption on the driver
- Secure client/server communications

### Pre-boot Authentication

- Microsoft and Novell Single Sign-on integration
- Password authentication (multi-factor authentication available with GuardianEdge Advanced Authentication)
- Secure Wake-on-LAN capability for seamless operation with enterprise patch and update management tools
- Lockout on maximum time-since-last-check-in exceeded (configurable)
- Password entry delay on failed password attempt threshold (configurable)
- Multiple user and administrator accounts

### Encryption

- "Always-on" hardware-based encryption
- Full disk or multi-partition including: master boot record, OS and system files, swap/hibernation files
- 128- or 256-bit AES (key strength dependent on drive vendor)

### Drive Disposal

- Secure, virtually instantaneous cryptographic erase for drive sanitization and disposal

### Administrative tools

- Remotely disable authentication of a targeted user
- Hard drive access tool to allow OS repair
- Remote, one-time password capability
- Integration with enterprise-grade deployment tools such as SMS, Tivoli, Altiris
- Real-time audit logging: policy changes, user actions (succeeded/failed authentication, attempts to uninstall the product, password recovery, change of password)

### Recovery from lost passwords

- Simple and secure access to encrypted PCs in the event of lost passwords with self-service or admin-assisted recovery

### Client Computers

- Microsoft Windows® XP Pro SP2 and SP3, XP Tablet Edition, 2000 SP4; Microsoft Vista (Business, Enterprise and Ultimate); Windows 7 (Professional, Ultimate and Enterprise)

### GuardianEdge Management Server

- Microsoft Server 2003 Standard or Enterprise (32-bit), Server 2008 Standard or Enterprise (32-bit or 64-bit)

### Database Server

- Microsoft SQL Server 2005 (32-bit) Express Edition with Advanced Services, Standard or Enterprise
- Microsoft SQL Server 2008 (32-bit or 64-bit) Express Edition with Advanced Services, Standard or Enterprise

### GuardianEdge Advanced Authentication Integration

- Extends data protection with certificate-based user authentication
- Pre-boot environment multi-factor authentication
- Smart card/common access card (CAC)/personal identity verification (PIV) support
- Extensive support for readers and tokens
- PKI environment support

### GuardianEdge — The Leader in Endpoint Data Protection

- **The only native Active Directory integration** – maximum use of existing infrastructure and training investments
  - Deploy and manage with existing infrastructure
  - Low training and support costs, fast rollouts
  - GPO-based policy deployment, MMC snap-in architecture
  - Role-based policy administration
  - Detailed auditing and reporting
- **Manage endpoint data protection for all PCs from a single console** – also supports Novell eDirectory and non-domain PCs
- **Proven ease of operation** – highest deployment success rates and millions of licenses deployed
- **Single-console administration** – common management for self-encrypting drives, GuardianEdge Hard Disk Encryption (software-based), Removable Storage Encryption, and Device Control
- **Non-disruptive to end users** – minimally intrusive; transparent operation and deployment

Corporate Headquarters t. +1.800.440.0419  
475 Brannan St., Suite 400 t. +1.415.683.2200  
San Francisco, California f. +1.415.683.2349  
94107-5421

[www.GuardianEdge.com](http://www.GuardianEdge.com)

GuardianEdge is a trademark of GuardianEdge Technologies Inc. All other products and services mentioned are the trademarks of their respective companies.