

Symantec™ Endpoint Encryption Removable Storage Edition

Protects data on removable storage and removable media

Data Sheet: Encryption

Overview

Removable storage devices are now common in offices everywhere and anywhere that today's mobile workers go. The proliferation of inexpensive USB thumb drives, portable hard drives, MP3 players, iPods®, digital cameras, mobile phones, personal digital assistants (PDAs), and CD/DVD burners puts organizations' data and business at risk.

Symantec™ Endpoint Encryption Removable Storage Edition addresses the operational issues that enterprises encounter when deploying a solution to protect data on removable storage devices from loss or theft, enabling organizations to benefit from the productivity gains associated with removable storage without putting data at risk.

Endpoint Encryption Removable Storage Edition is flexible—delivering the capability to encrypt data by policy on any storage device or media, allowing employees to safely transport and use data on portable media, and to securely distribute data via email. To speed adoption and acceptance, enterprises also need to ensure a non-disruptive user experience that protects data while having minimal impact on the way employees work. Endpoint Encryption Removable Storage Edition delivers this with capabilities such as shared workgroup keys that require no user intervention when data is written, and options for user registration that require little or no user interaction.

To minimize deployment, management, training, rollout, and support requirements, Endpoint Encryption Removable Storage Edition makes maximum use of existing infrastructure through its native Microsoft Active Directory® integration as well as Novell eDirectory™ support within a single management console. By leveraging accepted and proven enterprise software industry standard technologies, Endpoint Encryption Removable Storage Edition makes endpoint data protection across the enterprise simple to deploy and cost-effective to manage.

Key features

- Prevents unauthorized access to information on lost or stolen removable storage devices.
- Helps achieve compliance with governmental data protection directives and regulations.
- Automatic, on-demand, and content-driven encryption of removable storage.
- Extensive device and media support, including external hard drives, flash drives, CD/DVD media, floppy drives, and flash memory modules.
- Built-in CD/DVD burning application for creating encrypted optical media.
- Optional Access Utility for seamless access on systems without client software, such as home computers or business partner systems.
- Password or smart card-based authentication.
- Policy-based control for file type and device exclusions.
- Self-decrypting archives for secure, one-way distribution of encrypted files.
- Optional integration with Symantec™ Data Loss Prevention for Endpoints.
- Federal Information Processing Standard (FIPS) 140-2 validated, Common Criteria Evaluation Assurance Level 4+ (EAL4+) validated, and Section 508 compliant.
- Includes Microsoft Active Directory-integrated enterprise management console.
- Supports Microsoft Active Directory, Novell eDirectory, and non-domain endpoints.
- Provides extensive built-in compliance reporting with a custom report generator.

Technology overview

Endpoint Encryption Removable Storage Edition delivers enterprise-class encryption designed to safeguard sensitive, private, and legally protected data from loss on removable

storage devices and media that connect to laptop and desktop PCs.

Secure data portability is a critical requirement for successful use and deployment of any enterprise implementation of removable storage and removable media encryption. Included with Endpoint Encryption Removable Storage Edition is the capability to deploy, by policy, the Endpoint Encryption Access Utility, allowing data to be securely encrypted and decrypted from computers without Endpoint Encryption software, making it possible for users to easily take work home while protecting data should the device be lost or stolen. Another key safeguard that drives productivity while protecting data is the capability to create self-extracting encrypted file archives, making possible secure one-way distribution and group access models, such as e-mail distribution, FTP, and shared server use.

Endpoint Encryption platform

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
- Group policy object (GPO) based policy deployment
- Microsoft® Management Console snap-in architecture
- Role-based policy administration
- Detailed auditing and reporting

Manage endpoint data protection from a single console

—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 Endpoint Encryption products

Non-disruptive to end users—Minimally intrusive, transparent operation and deployment

Specifications

Supported ports and media

- USB-based removable storage (including flash drives and external hard drives), FireWire®-based storage, floppy disk drives, CD and DVD discs

Supported devices

- Flash media, including Secure Digital, CompactFlash®, MultiMediaCard™ (MMC), and more
- Memory sticks and thumb drives
- Internal and external floppy disk drives
- CD and DVD writers
- External hard drives with USB 3.0 and eSATA interfaces
- All devices recognized as removable storage by Windows®

CD/DVD support

- Encrypt data written to CDs and DVDs
- Native CD and DVD burner—can replace other CD and DVD burning software

Encryption

- 256 or 128-bit Advanced Encryption Standard
- Granular file-level data encryption policies
- Support for password or digital certificate user authentication keys
- Federal Information Processing Standard (FIPS) 140-2 validated cryptographic library

Authentication to encrypted data

- Administrative master recovery certificate
- Password
- Token/smart card
- Workgroup keys for seamless access to data by members of the same workgroup

Self-extracting archives

- Easily distribute encrypted data on storage devices, FTP sites, shared server volumes and through email
- Access data via password entry or smartcard authorization without requiring additional software

Endpoint Encryption Access Utility

- Enables access to encrypted data on Windows and Mac OS® X computers without Endpoint Encryption Removable Storage Edition installed
- Resides on removable storage media, requires a very small footprint
- Complete read/write access to encrypted files

Key and password administration and recovery

- Recovery of encrypted data in the event of lost tokens or passwords

Client platforms

- Windows 7 (x86 and x64)
- Windows Vista (x86 and x64)
- Windows XP (x86 and x64)
- Windows Server® 2003 and Server 2003 R2 (x86)
- Windows Server® 2008 and Server 2008 R2 (x86 and x64)
- Mac OS X 10.6, 10.7, and 10.8 (Intel-based) for Access Utility only

Management Server

- Windows Server 2003 and Server 2003 R2 (x86)
- Windows Server 2008 and Server 2008 R2 (x86 and x64)

Database

- Microsoft SQL Server® 2008 (x86 and x64), Standard, Enterprise, or Express Edition with Advanced Services
- Microsoft SQL Server® 2005 (x86 and x64), Standard, Enterprise, or Express Edition with Advanced Services

More Information

Visit our website

<http://enterprise.symantec.com>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com



SAVE PAPER. SAVE TREES.
SAVE THE Planet.



2F Republic Glass Bldg., 196 Salcedo St., Legaspi Village, Makati City
T: 813-4162/63 F: 812-9310 E: info@mannasoft.com
www.mannasoft.com