SOPHOS

simple + secure

SafeGuard Disk Encryption for Mac

Strong full-disk encryption for Macs

Protect private and confidential data on all your Macs with full-disk encryption that is transparent and easy to use. If a SafeGuard-encrypted Mac falls into the wrong hands, the data is inaccessible even if the hard disk is removed and connected to another computer. Whether for a single MacBook or for a mix of tens of thousands of Apple and Windows PCs and laptops, the SafeGuard product family allows easy implementation and enforcement of data protection.

What you get

- Unmatched data security with proven encryption algorithms for protecting lost or stolen Macs
- Encryption of operating system including page files for complete security
- Fast, user-transparent background encryption for high productivity
- Powerful controls for administration and recovery includes power-on authentication
- Comprehensive logging for compliance reporting
- Full set of recovery tools providing multiple recovery options
- Easy administration and deployment with visibility in SafeGuard Management Center
- Supports Apple's Boot Camp for compatibility with Windows

Try it now for free

Register for a free 30-day evaluation at sophos.com/products.

Strong, transparent encryption

Get sector-based encryption of disk volumes. This includes the Mac OS boot volume and data volumes.

Protects your sensitive data with our strong, standardized AES 256-bit encryption algorithm.

Your encrypted data cannot be accessed, even if the hard drives are removed from the Macs. Only your authorized users or security administrators have access to your data.

Highly optimized algorithms include support for Intel's AES-NI instruction set extensions in Core i5 and i7 processors.

Secure power-on authentication and authorization

Our EFI-based, power-on user authentication (POA) requires a username and password. Only after your users successfully logon will the encrypted volume boot and be readable.

Hardens the log-on process. Prevent password penetration attacks.

Generates comprehensive logs of user interactions during the power-on, authentication process, including failed logon attempts.

Provides multi-user power-on authentication for shared computers.

SafeGuard administration—independent from OS X ("sudo") administration—enforces the separation of duties between system and security administration.

Maintain the Mac look and feel with our user-friendly, graphical power-on authentication UI.

Allow your users to retain password privacy while still accessing their machines. Administrator accounts allow IT to securely access computers without requiring user passwords.

Flexible administration

Our GUI on the client allows for simplified user management and disk management.

SafeGuard Management Center integration lets you keep an eye on compliance. Get full visibility into your encryption status on the Mac.

Track your encryption status and progression using our Finder/System Menu icon.

Capture scripting and remote administration and status reporting using our command line tool (e.g., through ARD or third-party PC lifecycle management systems).

Requires SafeGuard administrator credentials for changes to POA user accounts and disk-encryption status. Allowing the registering of multiple independent admin accounts prevents bottlenecking.

Stores full audit trails of POA interaction and SafeGuard administrative actions in the OS X secure log.

Secure recovery of passwords, data and systems

One-time recovery credentials allow you to secure access systems and renew forgotten passwords.

Create emergency POAs on a USB key or CD. Securely boot and unlock your Macs with damaged EFI partitions.

Our secure emergency volume decryption option is available at the POA. Know that you can easily access and repair damaged operating systems.

Easy deployment

Our small ".dmg" installation package suits local and remote install.

Installation of the client is simple and fast. It requires no prior knowledge or document studies. Once you install the client software and create an administrator account, create the necessary user accounts with a few clicks or through the command line. Finally, a credential and/or kernel backup for future recovery purposes completes the installation.

Initial encryption runs transparently in the background. You can securely resume the initial encryption after powering down or a hard-reset of your Mac. If you don't need foreground responsiveness from your computer during initial encryption, try our "Fast" mode.

System requirements

Hardware[1]

- MacBook Pro, MacBook, MacBook Air, Mac Pro, iMac, Mac Mini
- 40-MB free disk space

Operating system

- OS X, 10.5.x, 10.6.x, 10.7.x

Language support

- English, French and German
- Runs on all international OS X languages

Interfaces

- Command line tool for scripting and remote administration
- GUI for intuitive local administration

Standards

- Encryption: AES-256
- Key Derivation: PKCS # 5v2
- Hash functions: SHA-256

[1]Intel-based systems/EFI 32- and 64-bit

Try it now for free

Register for a free 30-day evaluation at sophos.com/products.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

SOPHOS