



Protect what you value.

# McAfee Encrypted USB

(Formerly McAfee SafeBoot for USB)

## Secure USB storage—avoid a moving liability

In today's organizations, sensitive data is stored and accessed on a variety of devices, including USB flash drives. The storage capacity of these devices has grown enormously—while their physical size has decreased. This makes them highly portable and capable of storing a wide variety of mission-critical information. However, reduced size makes these devices easier to lose, and a higher storage capacity increases the potential amount of data at risk for unauthorized access if a device is lost or stolen. Even more unfortunate is that the vast majority of USB drives go uncontrolled by IT departments.

### KEY ADVANTAGES

#### Strong access control and encryption

- Provide data mobility to users without compromising security policies
- Encrypt data "on the fly," without end-user interaction or training
- Use AES-256 encryption and fast USB 2.0 transfer speed
- Provide portable security token support

#### Centralized management

- Deploy easily on an enterprise-wide scale
- Easily deploy and track USB drives through a single console
- Streamline workflow to save time and money
- Regain access by leveraging Active Directory to match users to devices

#### Prove compliance

- Demonstrate compliance with data privacy legislation
- Enforce mandatory company-wide security policies
- Prove that the device was encrypted at the time of a loss
- Recover passwords and portable drives remotely
- Gain FIPS 140-2 certification

### Protect Your Assets and Your Brand

Everyday, employees are walking out of their offices, unaware of how unsecure their portable devices are. USB drives, due to their small size and portability, are great for storage but a security nightmare. They can easily be lost or even used for corporate espionage.

By using McAfee® Encrypted USB (formerly McAfee SafeBoot® for USB) storage devices, you are assured that the information copied and transported onto these devices is safe and can only be read by the authorized persons.

### Protection

McAfee Encrypted USB drives are secure, portable storage drives that incorporate built-in user access control and strong data encryption, ensuring that sensitive data remains secure wherever it travels. Data is encrypted "on the fly," with virtually no performance loss or special training required by the end user. It also provides personal and corporate credentials protection and validation, ensuring that identities remain secure.

### Central Management

Deploying and managing portable storage devices across an enterprise can be extremely complex and expensive for an organization. Centralized management enables corporations to overcome these challenges by making it easy to deploy and manage McAfee Encrypted USB drives on an enterprise-wide scale, with virtually no impact on your existing IT infrastructure. Any number of users can be effectively managed and controlled. Because each device name is linked to a unique serial number in the Microsoft Active Directory, USB drives can be easily traced back to the original user. The result is maximum protection over your organization's assets with a low total cost of ownership.

### Regulatory Compliance and Recovery

McAfee Encrypted USB supports your compliance efforts. Security policies are enforced on the end user, ensuring that data stored on the device is protected if the device is lost or stolen. Your organization can also prove that the device was encrypted with extensive auditing capabilities, using existing reporting tools. Users can regain access to data even if they forget their passwords or can no longer access drives via biometric authentication. Access recovery is accomplished through a challenge-response mechanism.

### Features

McAfee Encrypted USB includes a range of secure portable storage devices, each with its own unique features. Each device incorporates built-in user access control and strong data encryption, ensuring that sensitive data remains secure wherever it travels. There's virtually no performance loss or special training required by end users.

## SYSTEM REQUIREMENTS

### Standard Driverless Encrypted USB

#### Operating systems

- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2000

#### Hardware details

- Available sizes: 1 GB and 2 GB

### Zero-Footprint and Hard Disk

#### Operating systems

- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2000
- Mac OS X

#### Hardware Details

- Sticks: Range from 1 GB to more than 8 GB
- Disk space: Ranges from 80 GB to more than 120 GB

### Centralized Management

#### Operating systems

- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2003

#### Database

- Microsoft SQL Server 2000 or 2005
- Microsoft SQL Express
- Informix

#### Browser

- Microsoft Internet Explorer 6.0 or 7.0

#### LDAP

- Microsoft Windows 2003 Active Directory (or higher)
- Microsoft ADAM

## Standard Driverless Encrypted USB





- **Provide strong access control** for removable USB storage and encrypt data using Advanced Encryption Standard (AES)-256 hardware encryption to ensure data remains secure wherever it travels.
- **Achieve maximum flexibility and user convenience;** no software installation or administrator rights are required—all that is needed is a USB port.
- **Set a maximum number of password or biometric authentication retries** to counter brute-force attacks with options for user recovery or data destruction.

## Zero-Footprint Technology

- **Achieve maximum flexibility with a zero-client footprint,** and provide security independent of the operating system environment; no software installation or administrator rights are required—all that is needed is a USB port.
- **Prevent unauthorized access to data** with two-factor authentication that requires users to authenticate using a password and fingerprint.
- **Install and run applications directly and securely from the USB device** (VPN, Internet browser, thin client, etc.); allows users to conveniently and securely run applications wherever they go.
- **Built-in encryption key generation and certificate storage.** Encryption keys can never be obtained or copied as they never leave the USB drive. There is also an option to store other encryption keys and/or public key infrastructure (PKI) certificates.

## Centralized Management

- **Demonstrate compliance with data security legislation.** Security policies are enforced on the end user, ensuring that all data stored on a device is protected if the device is lost or stolen.
- **Protect your assets and brand** by providing empirical proof that a USB drive was encrypted at the time of loss with extensive auditing.
- **Recover user passwords centrally,** using a challenge-response mechanism. Even if a user leaves the organization, the organization can always access the data by performing a device rescue.
- **Control the way in which your organization manages its user devices** through one central management workstation or thousands of workstations in various locations around the world.

	Standard Driverless <sup>1</sup>	Zero-Footprint Non-BIO	Zero-Footprint BIO	USB Hard Disk
				
Password Authentication	•	•	•	•
Biometric Authentication			•	•
Hardware Encryption	•	•	•	•
Digital Identity and Crypto Services		•	•	•
Managed by McAfee Encrypted USB Manager	•	•	•	•

<sup>1</sup> The Standard Driverless is supported by recovery and central management but remote recovery is not possible.

For more information about McAfee Encrypted USB, please visit [www.mcafee.com](http://www.mcafee.com).

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, [www.mcafee.com](http://www.mcafee.com)



McAfee, SafeBoot, and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners. © 2008 McAfee, Inc. All rights reserved. 1-cor-encryp-usb-001-0608