



Protect what you value.

# McAfee Encrypted USB

(Formerly SafeBoot® for USB)

## Secure USB Storage

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 these devices 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
- Protect data using powerful encryption
- Provide portable security token support

#### Centralized management

- Deploy easily on an enterprise-wide scale
- Easily deploy and track devices through a single console
- Streamline workflow to save time and money
- Leverage Active Directory to match users and devices

#### 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

#### Protect your assets and your brand

Everyday, employees are walking out of their offices, unaware of how insecure their portable devices are. USB sticks, 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 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 devices are secure, portable storage devices 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 devices on an enterprise-wide scale, with virtually no impact on your existing IT infrastructure. Any number of users can be effectively managed, controlled, and bound to the corporate user from Microsoft Active Directory. 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 lost or stolen. Your organization can also prove that the device was encrypted using extensive auditing capabilities and existing reporting tools. Users who forget their passwords or lose their ability to access data via the biometric authentication are recovered and given access to their device using a challenge-response mechanism.

## SYSTEM REQUIREMENTS

System requirements vary depending on the device chosen by your organization:

### Standard secure USB flash storage

#### Operating systems

- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows 2000

#### Hardware details

- Available sizes: 512 MB to 4 GB

### Zero-footprint USB Storage

#### Operating systems

- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows 2000

#### Hardware details

- Sticks: Range from 512 MB to more than 8 GB
- Hard disk: Ranges from 80 GB to more than 100 GB

### Centralized management

#### Operating system

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows XP

#### Server

- Microsoft SQL Server 2000 SP4 or higher

#### Browser

- Microsoft Internet Explorer 6.0 or higher Microsoft Windows 2003 Active Directory or higher

## 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.

### Standard secure USB flash storage

- Provide strong access control for removable USB storage and encrypt data using AES-256 encryption to ensure data remains secure wherever it travels
- Support multiple users, giving each their own secure partition; individual passwords unlock the device and grant each user access to their respective data
- Set a maximum number of password retries for even more security
- Share a device with others without compromising non-shared information
- Create a "public area" to store information that will not be encrypted; this public area can also be used to transport non-sensitive information to an unsecured computer




### 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/or fingerprint
- Set a maximum number of password or biometric authentication retries to counter brute-force attacks
- Gain FIPS 140-2 certification

### Centralized management

- Demonstrate compliance with data security legislation. Security policies are enforced on the end-user, ensuring you that all data stored on a device is protected if lost or stolen
- Protect your assets and brand by providing empirical proof that a device 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

## McAfee Encrypted USB options

Standard secure USB flash storage	
	<ul style="list-style-type: none"> <li>• 512MB-4GB Flash Storage</li> <li>• Password Authentication</li> <li>• AES-256 Encryption</li> </ul>
Zero-footprint USB storage	
	<ul style="list-style-type: none"> <li>• 512MB-8GB Flash Storage</li> <li>• Password and/or Fingerprint Authentication</li> <li>• AES-256 Encryption</li> <li>• "Zero-Footprint" Technology</li> </ul>
	<ul style="list-style-type: none"> <li>• 80GB-100GB Hard Disk Storage</li> <li>• Password and/or Fingerprint Authentication</li> <li>• AES-256 Encryption</li> <li>• "Zero-Footprint" Technology</li> </ul>

For more information about Data Protection, visit [www.mcafee.com/data\\_protection](http://www.mcafee.com/data_protection).

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

McAfee 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-dp-usb-001-0108