

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 ¹	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	•	•	•	•

¹ 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.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, 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