

McAfee Encrypted USB

Extend security to your mobile environment with McAfee® Encrypted USB devices

Organizations today store sensitive data on a variety of devices, including small form factor USB flash drives that fit in the palm of your hand. While the physical size of these drives continues to get smaller, their storage capacity is increasing, making them capable of storing a large amount of mission-critical information—and this creates a significant security risk if the device is lost or stolen. What's more, the vast majority of these USB drives are not controlled or managed by the IT department or covered by the organization's security policy, increasing the risk of unauthorized access, data loss, and regulatory noncompliance. Extending the centralized corporate security policy to control and manage USB drives is essential for today's mobile environments.

Key Advantages

- Comply with corporate security policies, data privacy legislation, and industry regulations through the use of hardware-encrypted USB devices
- Provide data mobility without compromising security policies
- Track and manage encrypted USB devices company wide using the McAfee ePolicy Orchestrator platform (McAfee ePO) for automated security reporting, auditing, monitoring, and policy administration*
- Control data access with two-factor authentication
- Secure data with industry-leading encryption algorithms and validations, such as AES-256 and FIPS 140-2**, for strong protection

Protect Your Assets and Your Brand

USB drives, because of their small size and portability, are great for storage, but they are also a security officer's biggest nightmare. Each day, individuals walk out of their offices with large amounts of sensitive corporate data stored on portable USB drives that are tucked into their pockets or briefcases, and they are unaware of the security risk posed to their organization if the drives are lost or stolen.

With McAfee Encrypted USB devices, the information copied onto these devices is encrypted and can only be read by authorized individuals. Built-in user access control and strong hardware data encryption keeps sensitive data secure wherever it travels.

Centralized Management with Award-Winning McAfee ePolicy Orchestrator® (McAfee ePO™)*

Deploying and managing portable storage devices across an enterprise can be extremely complex and expensive for an organization. Because USB drives are typically not managed by the IT organization, they are not covered by company-wide security policies. Too often, individuals copy intellectual property or other proprietary information onto USB drives in the clear—data that normally would be encrypted when attached to an email or stored on a laptop. McAfee Encrypted USB devices are

managed centrally through the McAfee ePO platform, enabling corporations to overcome these challenges by making it easy to get the encryption you need. You can deploy and manage McAfee Encrypted USB drives on an enterprise-wide scale, with virtually no impact on the existing IT infrastructure.

McAfee ePO software combines with our encrypted USB devices to provide centralized management and deployment from a single console, improving corporate security while reducing total cost of ownership. The McAfee ePO management interface lets you initialize any McAfee Encrypted USB device simply by plugging the device into a McAfee ePO-managed machine with its unique “no-touch” initialization capabilities.

Keep Data Safe and Secure with Strong Hardware Encryption

To access data on McAfee Encrypted USB devices, users must authenticate themselves using a password or fingerprint, preventing unauthorized access to data. For maximum security, two-factor authentication can be used. If users have forgotten a password or if they don't have the ability to perform biometric authentication, they can easily regain access to the data via a centralized password reset or self rescue through McAfee ePO software.

Specifications

Note: System requirements vary depending on the devices chosen by your organization.

McAfee Encrypted USB by SanDisk

Operating systems

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

Hardware details

- Available sizes: 1 GB to 8 GB

McAfee Encrypted USB Standard**

Operating systems

- Windows 2000, XP, Vista, 7
- Apple Mac OS X (standalone usage only)

Hardware details

- Available sizes: 1 GB to 32 GB

McAfee Encrypted USB Bio*

Operating systems

- Windows 2000, XP, Vista, 7
- Mac OS X (standalone usage only)
- Linux (biometric mode only)

Hardware

- Available sizes: 1 GB to 32 GB

McAfee Encrypted USB Hard Disk

Operating systems

- Windows 2000, XP, Vista, 7
- Mac OS X (standalone usage only)
- Linux (biometric mode only)

Hardware

- Available sizes: 160 GB to 500 GB

McAfee ePolicy Orchestrator

- McAfee ePO software 4.0 or higher
- McAfee Encrypted USB Extension required

Operating systems

- Windows 2000, 2003, XP, Vista

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

With built-in hardware encryption, key generation, and certificate storage, encryption keys can never be obtained or copied, as they never leave the USB drive. Optionally, you can store other encryption keys and/ or public key infrastructure (PKI) certificates***. All data on McAfee Encrypted USB devices is encrypted using the strongest, hardware-based, industry-standard encryption algorithms available, including AES-256, as well industry certifications, such as Federal Information Processing Standards (FIPS) 140-2** and Common Criteria (CC).

Demonstrate Regulatory Compliance

Because they are integrated with the McAfee ePO management console*, McAfee Encrypted USB devices support your compliance efforts, from corporate security policies to industry-specific regulations to data privacy legislation. You can prove that the data on a stolen or lost USB device was encrypted, and you can run reports that detail data access and USB usage for auditing purposes.

Key Features

- Implement strong access control for removable USB storage and encrypt data in hardware using Advanced Encryption Standard (AES-256) hardware encryption
- Set a maximum number of password or biometric authentication retries to counter brute-force attacks with options for user recovery or data destruction

- Maximize flexibility with a zero-client footprint, and provide security independent of the operating system environment; no software installation or administrator rights are required—all you need is a USB port
- Prevent unauthorized access to data with two-factor authentication that requires users to authenticate using a password or fingerprint
- Install and run applications directly and securely from the USB device (PC-on-a-stick, Internet browser, thin client, and more); users can conveniently and securely run applications wherever they go
- Built-in encryption key generation and certificate storage prevents encryption keys from being copied because they never leave the USB drive. There is also an option to store other encryption keys and/ or public key infrastructure (PKI) certificates***.
- Built-in anti-malware helps protect USB drives and the computers and networks they connect to with a malware scan engine that automatically detects and prevents USB-borne threats (requires McAfee ePO platform manageability)

McAfee Encrypted USB Devices

The following table lists key features on the range of McAfee Encrypted USB devices. USB sticks range in storage size from one GB to 32 GB; USB hard disks range in storage size from 160 GB to 500 GB.

	McAfee Encrypted USB by SanDisk	McAfee Encrypted USB Standard	McAfee Encrypted USB Bio	McAfee Encrypted USB Hard Disk
Password Authentication	•	•	•	•
Biometric Authentication			•	•
256-Bit AES Hardware Encryption	•	•	•	•
Virtualization (PC-on-a-Stick)***	(Optional)	(Optional)	(Optional)	(Optional)
FIPS 140-2 Validated	•	**	**	•
Digital Identity and Crypto Services			(Optional)	(Optional)
Centralized Management via McAfee ePolicy Orchestrator (McAfee ePO)	•	•	*	•
McAfee Anti-Malware Protection	•	(Optional)	(Optional)	(Optional)

For more information about McAfee Encrypted USB devices, please visit www.mcafee.com.

*The newest McAfee Encrypted USB Bio devices are standalone only and are not yet FIPS validated or McAfee ePO software manageable. FIPS validation is in progress.
 ** FIPS validation is in progress for McAfee Standard and Bio USB devices. Legacy driverless and zero-footprint devices are FIPS validated.
 ***Additional software is required.

