

# McAfee Encrypted USB

Protect mobile data with McAfee® Encrypted USB devices

High capacity, small form factor USB storage drives enable workers to transport large amounts of confidential company data anywhere. And, well-intentioned employees are often unaware of the significant security risks and costs that could impact their organization if the drives are lost or stolen. What's more, the vast majority of 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 data security in 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 for automated security reporting, auditing, monitoring, and policy administration
- Control data access with two- or three-factor authentication
- Secure data with industry-leading encryption algorithms and validations, such as AES-256 and FIPS 140-2, for strong protection

## Keep Data Safe and Secure

All the information copied onto McAfee Encrypted USB 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

Deploying and managing portable storage devices across an enterprise can be complex and expensive. And, USB drives are typically not managed by the IT organization, so they are often not covered by company-wide security policies. The McAfee ePolicy Orchestrator® (McAfee ePO™) platform addresses those issues by deploying and managing McAfee Encrypted USB devices centrally from a single console—which improves corporate security while reducing total cost of ownership. Users simply initialize devices by plugging them into a McAfee ePO-managed computer.

## Strong Hardware Encryption

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. With built-in hardware encryption, key generation, and certificate storage, encryption keys can not 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.

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 enabled by McAfee ePO software.

## 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

**Specifications**

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

**McAfee Encrypted USB Standard**

- Operating systems: Windows XP, Vista, 7 (32 and 64 bit)
- Hardware: Available sizes are 1 GB to 64 GB

**McAfee Encrypted USB Bio**

- Operating systems: Windows XP, Vista, 7 (32 and 64 bit). Mac OS 10.5 and 10.6 are supported for non-managed devices when using biometric authentication only (stand-alone, biometric)
- Hardware: Available sizes are 1 GB to 64 GB

**McAfee Encrypted USB Hard Disk**

- Operating systems: Windows XP, Vista, 7 (32 and 64 bit). Mac OS 10.5 and 10.6 are supported for non-managed devices when using biometric authentication only (stand-alone, biometric)
- Hardware: Available sizes are 250 GB to 500 GB

**McAfee Encrypted USB Hard Disk Non-Bio**

- Operating systems: Windows XP, Vista, 7 (32 and 64 bit)
- Hardware: Available sizes are 250 GB to 500 GB

- 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);<sup>1</sup> 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 management)

**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 1 GB to 64 GB; USB hard disks range in storage size from 250 GB to 500 GB.

**Simple Product Feature Matrix**

	McAfee Encrypted USB Standard	McAfee Encrypted USB Bio	McAfee Encrypted USB Hard Disk Non-Bio	McAfee Encrypted USB Hard Disk
Password or CAC/PIV Card Authentication	●	●	●	●
Biometric Authentication		●		●
AES-256 Bit Hardware Encryption	●	●	●	●
Virtualization Capable (PC-on-a-Stick) <sup>1</sup>	Optional	Optional	Optional	Optional
FIPS 140-2 validated	●	●	●	●
Centralized management via McAfee ePolicy Orchestrator (McAfee ePO) <sup>2</sup>	●	●	●	●
McAfee Anti-Malware Protection	●	●	●	●

<sup>1</sup> Third-party software required at additional cost.

<sup>2</sup> McAfee Encrypted USB Manager software is optional at additional cost for non-McAfee ePO customers and digital identity options.

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

