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 making them 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 use of encrypted USB devices
- Provide data mobility without compromising security policies
- Track and manage encrypted USB storage devices company-wide using the McAfee ePolicy Orchestrator (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 certifications, 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 they pose to their organization if the drives are lost or stolen.

With McAfee Encrypted USB devices, the information copied onto or transported on these devices is encrypted and can only be read by authorized individuals. With built-in user access control and strong data encryption, McAfee Encrypted USB keeps sensitive data secure wherever it travels. Plus, user identities remain safe from prying eyes, thanks to integrated credentials protection and validation.

Centralized Management with award-winning McAfee ePolicy Orchestrator

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. Centralized management with McAfee ePolicy Orchestrator® (ePO™) enables 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.

The combination of ePolicy Orchestrator and our range of encrypted USB devices provides centralized management and deployment from a single console, improving corporate security while reducing total cost of ownership. The ePO management interface lets you initialize any McAfee encrypted USB device simply by plugging the device into any ePO-managed machine with its unique "no-touch" initialization capabilities.

Keep data safe and secure with strong 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 ePO.

With built-in encryption, key generation, and certificate storage, encryption keys can never be

Specifications

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 16 GB
- Disk space: Ranges from 80 GB to 320 GB

McAfee ePolicy Orchestrator details
- ePO 4.0 or higher
- Encrypted USB Extension required

Operating systems
- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2003
- Microsoft Windows 2000

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

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 are encrypted using the strongest, hardware-based, industry-standard encryption algorithms available, including AES-256, as well industry certifications, such as FIPS 140-2.

Demonstrate regulatory compliance

Because it is integrated with the ePO management console, McAfee Encrypted USB supports all 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. You can also 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 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 and fingerprint.
- **Install and run applications directly and securely from the USB device** (VPN, 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.

McAfee Encrypted USB Devices

The following table lists available features on the complete range of McAfee Encrypted USB devices. USB sticks range in storage size from 1 GB to 16 GB; USB hard disks range in storage size from 80 GB to 320 GB.

	Standard Driverless	Zero-Footprint Non-BIO	Zero-Footprint BIO	USB Hard Disk
				
Password Authentication	•	•	•	•
Biometric Authentication			•	•
Hardware Encryption	•	•	•	•
Digital Identity and Crypto Services		•	•	•
Managed by McAfee ePolicy Orchestrator	•	•	•	•

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

5599ds_encrypted-usb-0109