McAfee®

Protect what you value.

McAfee Encrypted USB Manager

(Formerly SafeBoot for USB Enterprise)

Manage and protect your McAfee Encrypted USB devices

McAfee® Encrypted USB Manager is a full-featured, centralized management software solution for McAfee Encrypted USB devices. It enforces compliance with corporate standards for data, authentication, and mobile application usage. As government and industry-specific regulations increase, and the penalties for non-compliance become more severe, corporations must protect sensitive information better—not only within the enterprise but also when data leaves via portable devices.

KEY ADVANTAGES

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**
- **No training required for end users**
- **Zero footprint with no client software to deploy**

Prove 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**
- **Recover passwords and devices remotely**
- **Gain FIPS 140-2 certification**

McAfee Encrypted USB device 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**
- **Use AES-256 encryption and fast USB 2.0 transfer speed**
- **Provide portable security token support**

Centralized Management

McAfee Encrypted USB devices provide the ability to easily and securely transport data outside of an organization. They have the highest levels of encryption and authentication. By centrally managing and administering corporate standards and audit requirements for USB devices, McAfee Encrypted USB Manager ensures compliance.

The centralized management of McAfee Encrypted USB devices will:

- 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 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.

User Identification

Your organization needs to know who is carrying what USB device. Furthermore, the identity of these individuals needs to come from the corporate identity store (typically a Lightweight Directory Access Protocol, or LDAP, directory). The last thing a company needs is another identity silo.

Tailored Authentication

Policies for authentication, such as password complexity rules, biometric security levels, and retry limits, must be tailored to the needs of each group of users in accordance with their role and operating environment. For example, mobile users may need biometric authentication, while internal users may only need password devices.

Digital Credentials

Some portable security devices have the capability to perform digital identity functions, such as generating one-time passwords and public key operations. Having one central point to provision digital credentials such as private keys, token seeds, and static credentials greatly simplifies the process of enabling these devices for use with your various authentication systems.

SYSTEM REQUIREMENTS

Centralized Management Operating Systems

- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2003

Database

- Microsoft SQL Server 2000 or 2005
- Informix
- Microsoft SQL Express

Browser

- Microsoft Internet Explorer 6.0 or 7.0

LDAP

- Microsoft Windows 2003 Active Directory (or higher)
- Microsoft ADAM

Portable Applications

One of the benefits of portable storage is that it can provide greater mobility for applications. Organizations can decide to control the set of applications that are appropriate for different groups of users. For example, mobile workers may need a remote access client on their devices, while internal employees do not need this type of access. The Portable Content Manager (PCM) allows IT administrators to simply drag and drop corporate applications that will be pre-loaded on portable security devices, such as single sign-on for web forms, portable secured Internet browsers, remote access clients, and virtual desktops.

User Rescue

Easy to implement password and biometric recovery options must be available to rescue blocked users, even if they're away from the corporate network.

Data Recovery

Data recovery options are available to security officers so that they can perform audits on the stored information and, if necessary, without the user being present. Help desk operators can re-establish device access or permanently erase all data.

Data Destruction

In some scenarios, consecutive failed user authentications indicate a potential attack. Organizations can decide to destroy data completely without the possibility of recovery if authentication becomes blocked on the portable security device.

Integrated Reporting Capability Helps Ensure Regulatory Compliance

Organizations must be compliant with regulations on data security and corporate governance. To fully ensure compliance when deploying security devices, administrative roles for different tasks must be separable and administrative operations must be logged.

Reuse and Recycle

When employees no longer need to use a USB device, there is no need to throw them away. Organizations can recycle and re-issue devices to other users.

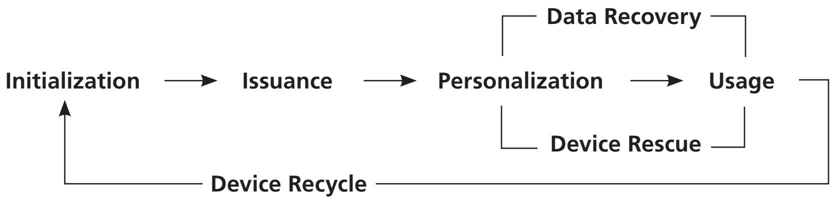

Figure 1. McAfee Encrypted USB device reuse and recycle management

	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*