Encrypting Removable Media Device – User Guide

(Revision Date: 07/16/2013)

Table of Contents

Introduction

The Endpoint Encryption for Removable Media is a subset of File and Folder encryption but works with a different key structure. It is not encrypting on an individual file basis but is encrypting a hidden partition on the drive.

The user of the USB key would be able to initialize the key with a password to access the key. The password must use a complex password with all four characteristics (upper and lower alphabetic, numeric and special characters). This USB key could then be used on any computer when the correct password is entered.

The initialization process would create a hidden personal key that would be used to recover the USB drive. This key would be associated with the username that is used to initialize the drive. If the password is lost and needs to be recovered, the original user would have the option to click the recover button and reset the password. This key would only be associated with the username and only available to the original user. In the event a user is unavailable, the recovery key can be made available to administrators.

Intended Audience

The intended audience for this procedure is:

- IT administrators
- Community College Employees

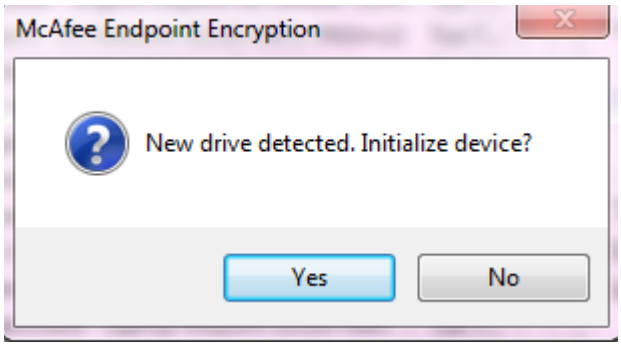
Procedure

Creating Encrypted drive

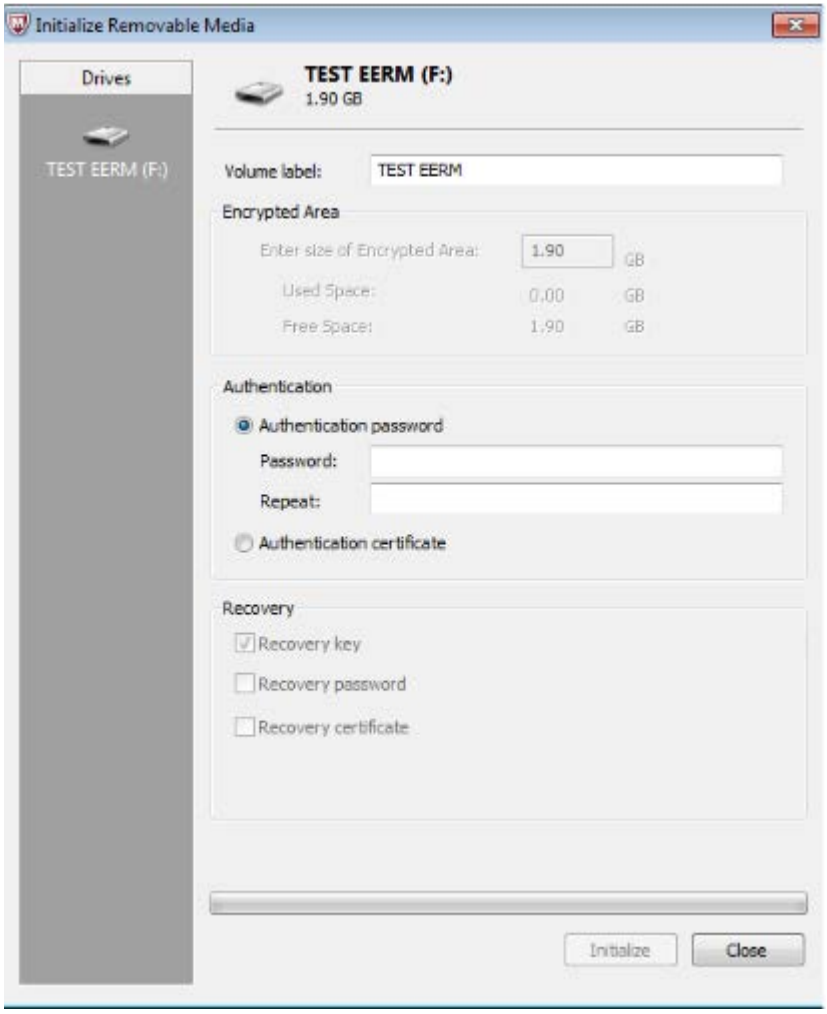
The process of creating an encrypted drive would depend on the Endpoint Encryption for Files and Folders software to be installed on the system. With this software the drive can be encrypted. An end user would be creating this drive and would also be creating the password to access it. The password must be complex and include all of these characteristics:

- 8 characters minimum
- Lower case
- Upper case
- Numeric
- Special characters

When the key is plugged in, you will see the following window pop up:



Then the initialize Removable Media Screen would appear:



In this screen the **Volume Label** and the **Authentication Password** would be entered. The recovery method would be locked by the policy.

If there is data on the drive before initializing, you will be asked if you want to save the data like this:

There must be enough free space on the local drive to save the data for this option to complete.

This will also add a significant amount of time to the initialization process.

Ejecting the drive

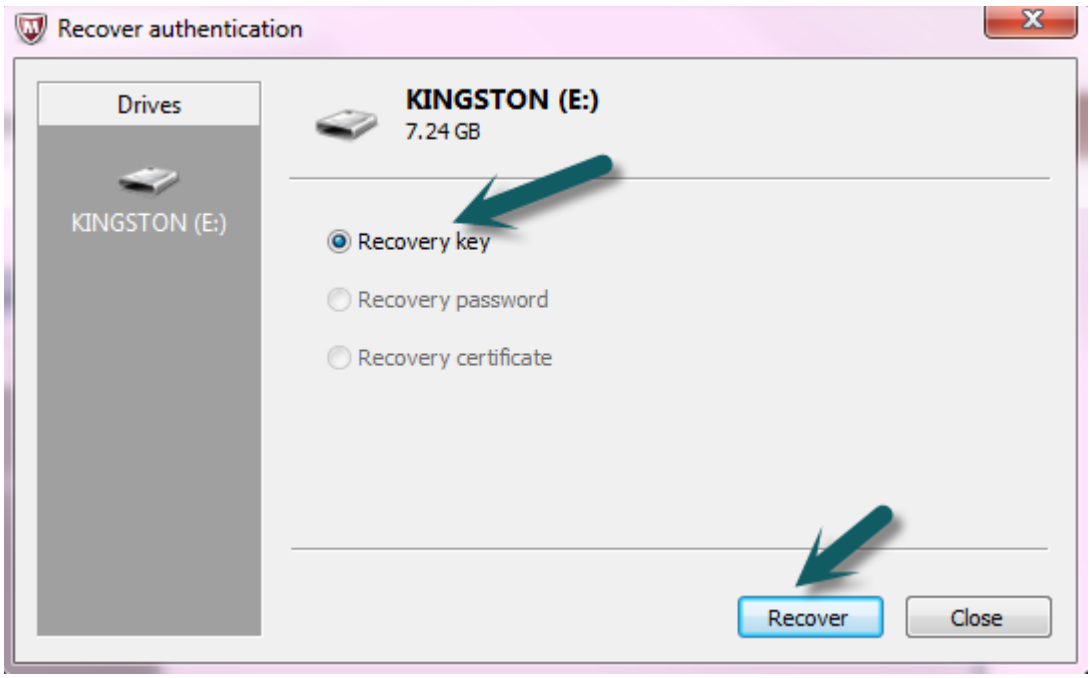
In order to eject the USB drive, right click on the drive listed under **Computer** and select **Eject** after which it is safe to remove the drive**.**

Using the key

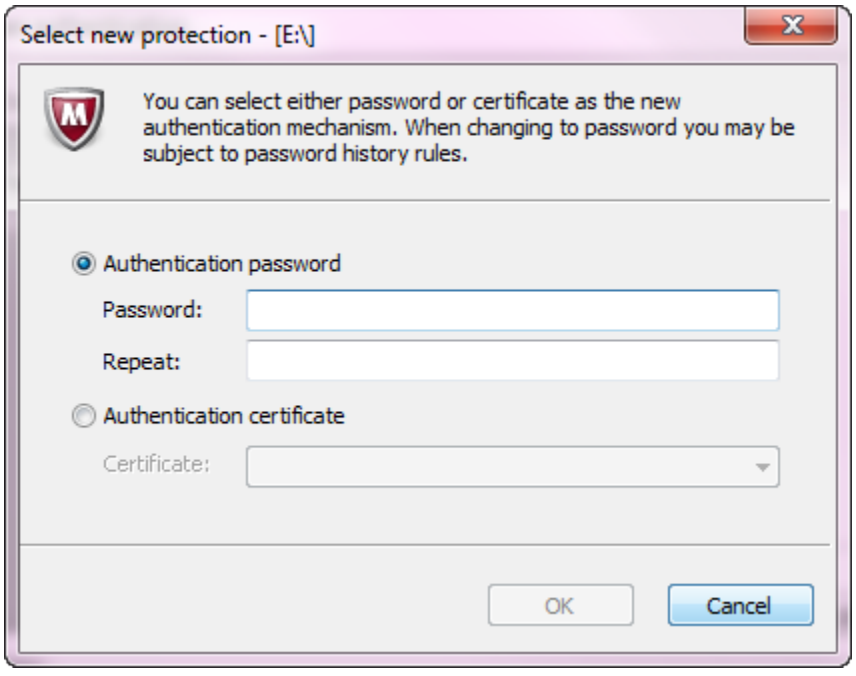
When plugging in the USB drive, the login screen will appear:

If the autorun script program does not force the login screen to appear, you may run the MfeEERM.exe program in the root directory of the flash drive. Enter the password for the USB key and access will be granted.

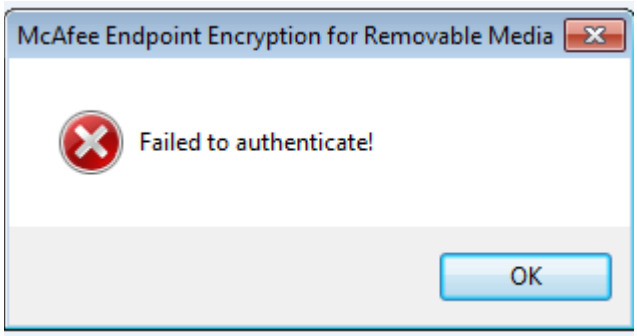
If the user who initialized the USB drive forgets the password, the user can utilize the **Recovery** option which brings up the following window:



Choose **Recover** which brings up the following window where you can change the password.



If it's a different user trying to do the **Recovery**, an authentication failed window pops up.



If the original user is unavailable, the personal key can be changed to a regular key and assigned to an administrator and then recovered. Contact your IT department if this option is required.

Usage Notes

Read Only Access

With the Endpoint Encryption for File and Folder software installed on a machine, any USB drive that is plugged into the machine would require removable media encryption or the drive would be read only access. This would provide protection against sensitive information being unencrypted on these portable drives.

Removing Encryption

It is not possible to remove the encryption and retain any data that is on the USB drive. This is part of the design to prevent the loss of data when the drive is lost or stolen. If the data needs to be saved, it should be copied from the drive and then the drive can be formatted and the data copied back.

Mac OS

Encrypted drives cannot be read on the Mac or other operating systems.

USB devices

Encryption can affect many types of USB devices that act like a drive. These should not be encrypted: iPods, iPhones, MP3 players, cameras, etc. The devices would be locked as read
Only and could not be written to.

Release History

- ☐ 02/28/2013 Initial Release
- ☐ 07/17/2013 Revised