

McAfee Endpoint Encryption for Files and Folders (EEFF) User Documentation

McAfee Endpoint Encryption for Files and Folders (EEFF) uses powerful encryption technology to allow you to protect information from access by unauthorized users. Your data is stored, managed, archived, and distributed as any other file is, however, only those who have been granted access can view it.

Using the Context Menu

The EEFF context menu provides easy access to EEFF options for files and folders.

When you right-click a file or a folder, the context menu appears and displays the options enabled by your administrator, according to your company's security policies.

Available Options:

Create a Self-Extractor

Attach a Self-Extractor to an Email

Attach an Encrypted File

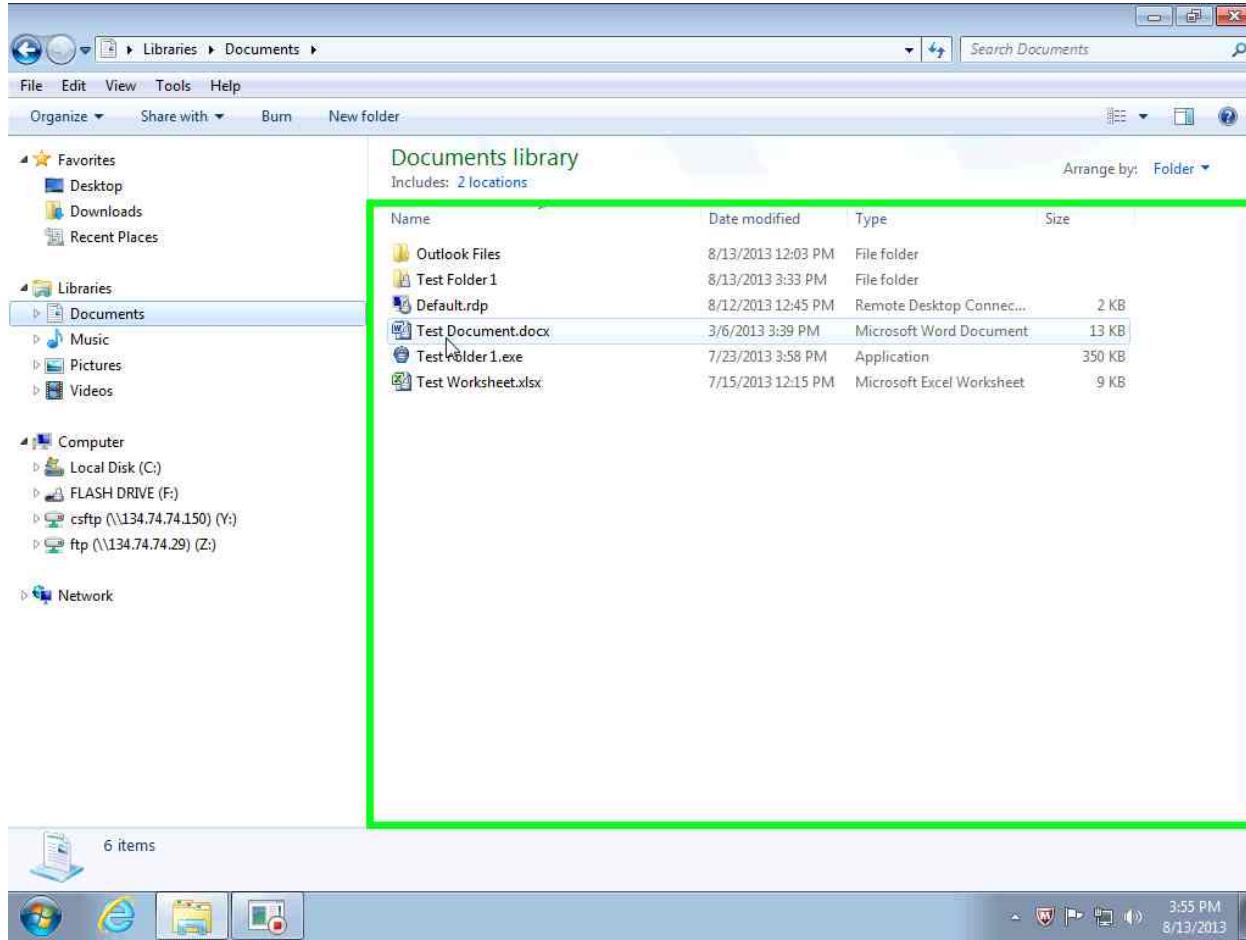
McAfee Endpoint Encryption for Files and Folders

Create a Self-Extractor

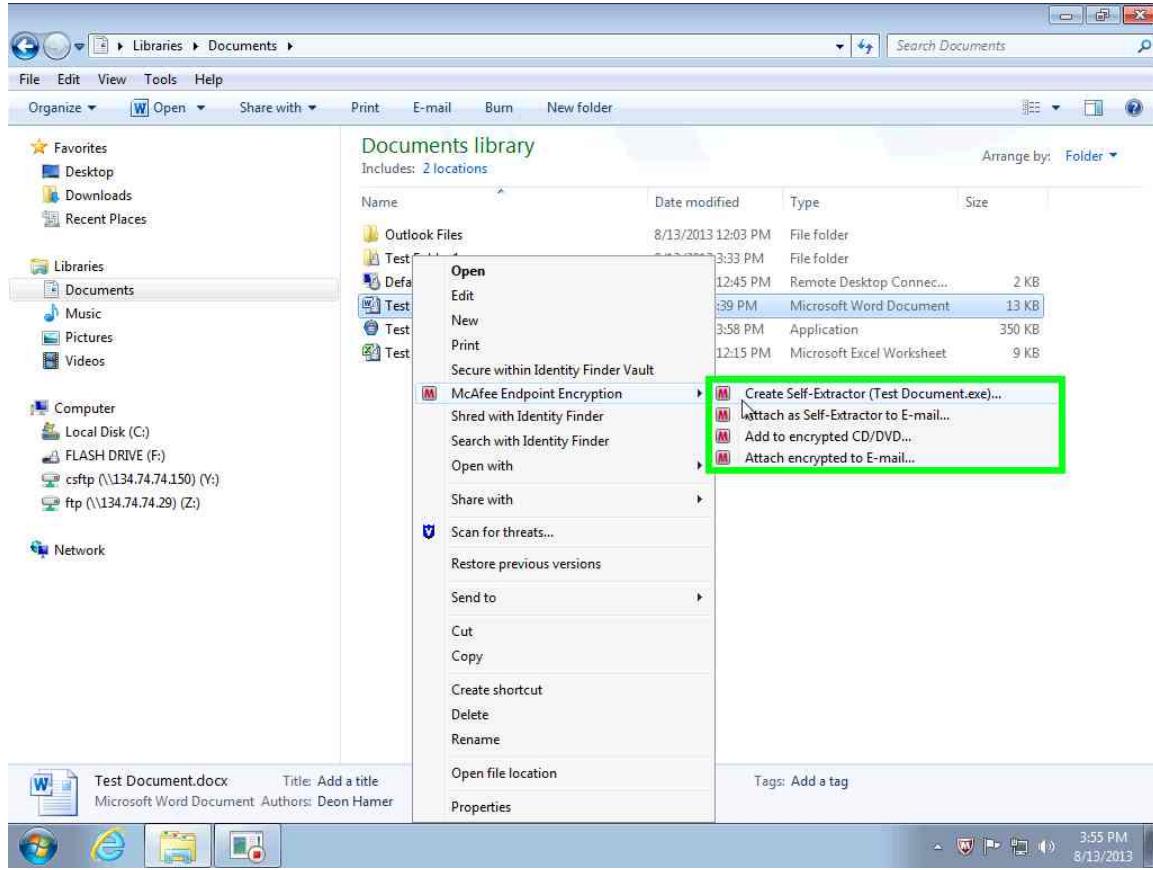
Self-extractors are password-encrypted executable files that can also be decrypted on systems that are not running EEFF. The password used to create the self-extractor is required to read it.

You can change the name of the self-extractor. By default, its name is the same as the source file/ folder with the *.exe extension.

1. Right click on the file or the folder for which you want to create a self-extractor



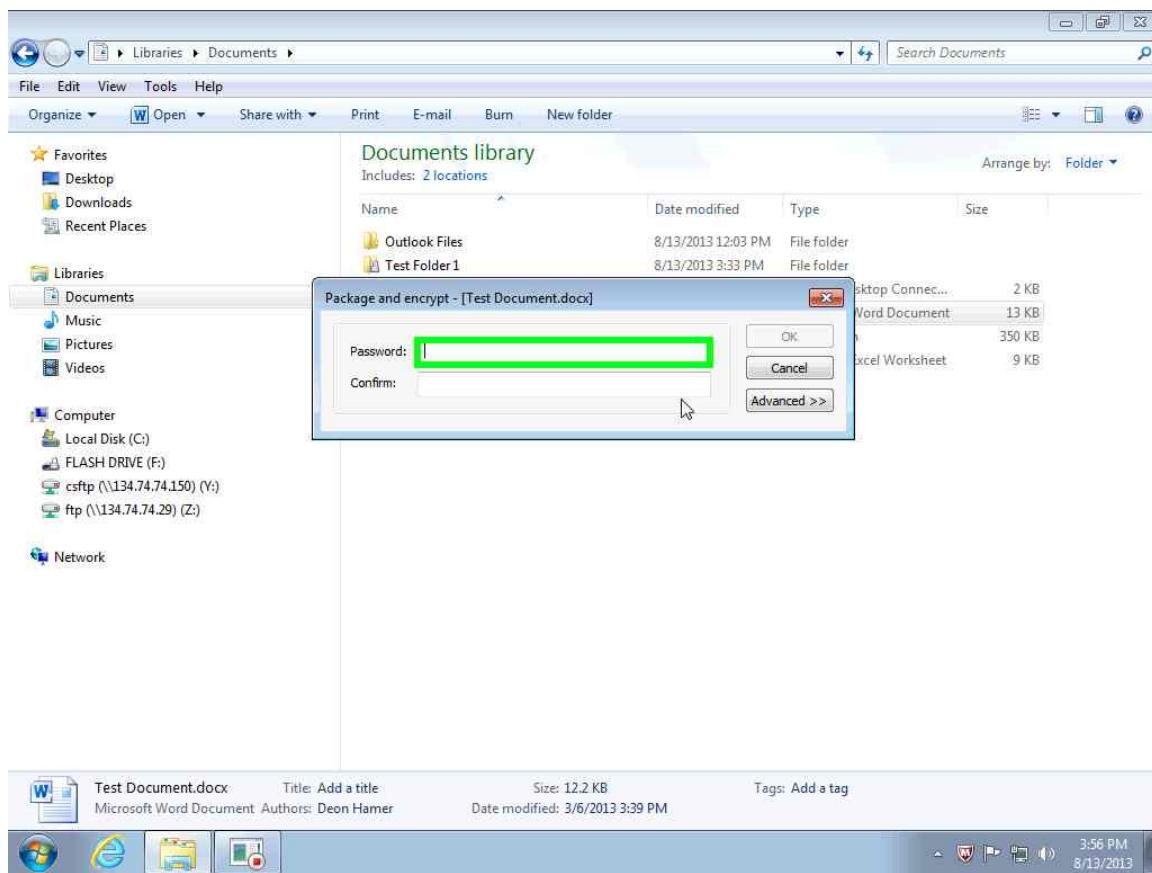
2. Select McAfee Endpoint Encryption | Create Self-Extractor (<filename>.exe)



The **Package and encrypt** dialog box appears.

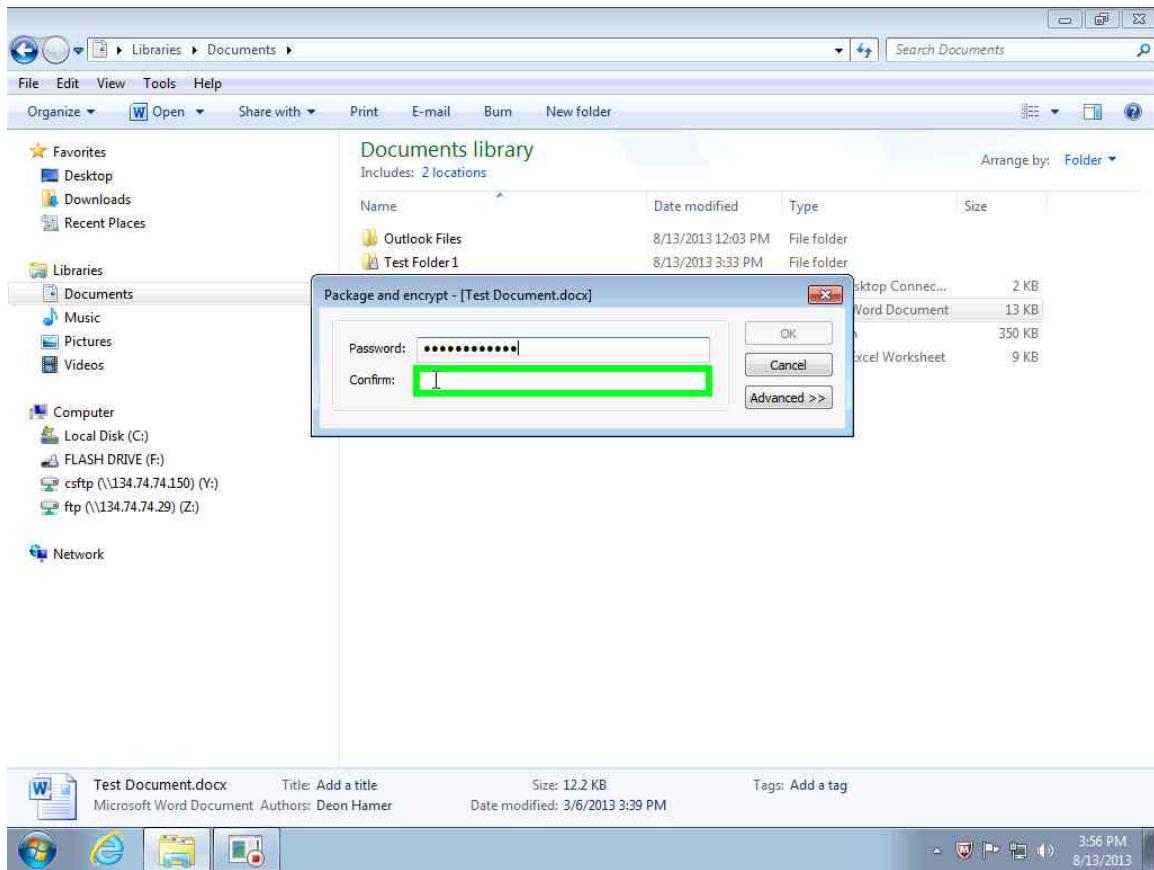
3. Enter the password you want to use to encrypt the self-extractor.

McAfee Endpoint Encryption for Files and Folders



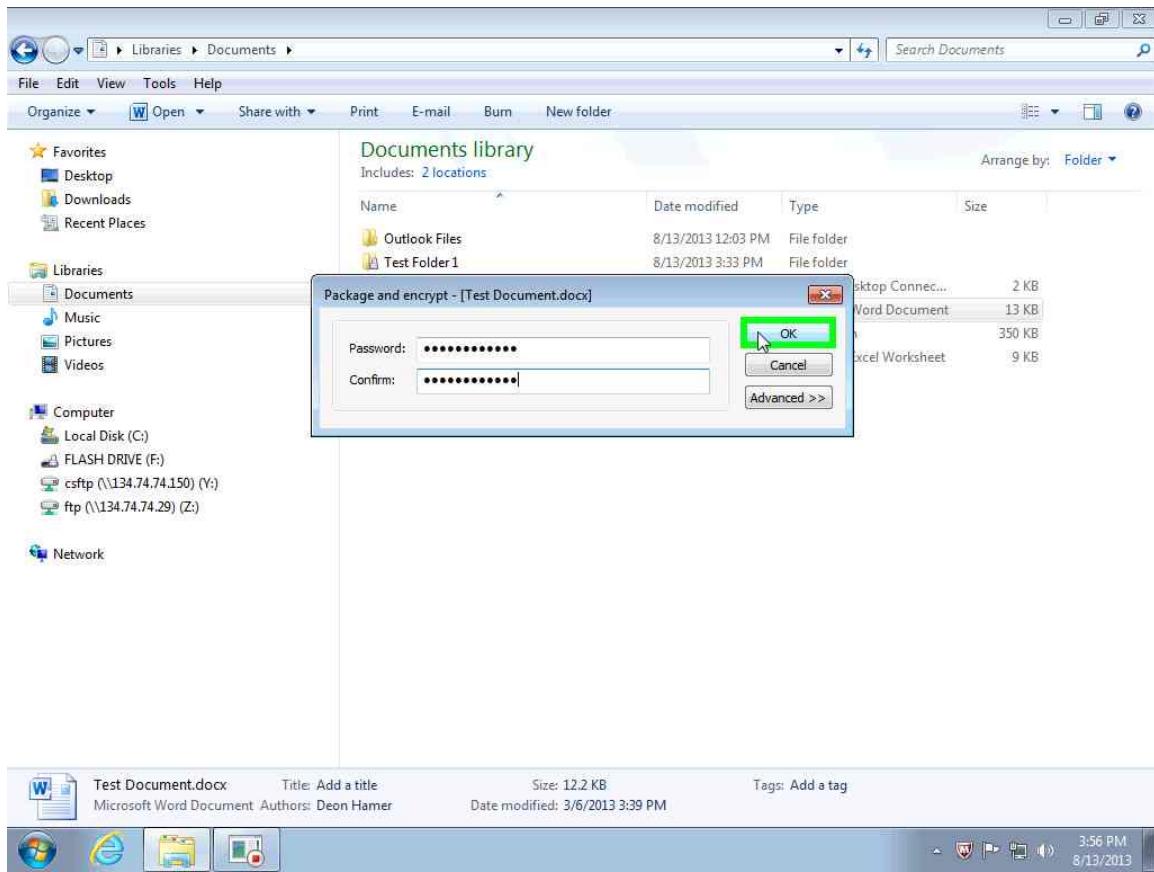
4. Re-enter the password that you want to use to encrypt the self-extractor.

McAfee Endpoint Encryption for Files and Folders



4. Click OK.

McAfee Endpoint Encryption for Files and Folders



The source file/folder remains intact on disk; only a copy of the file/folder is converted into a self-extractor.

You can also specify where to save the self-extractor. The default location is the same as the source file/folder location.

Attach a Self-Extractor to an Email

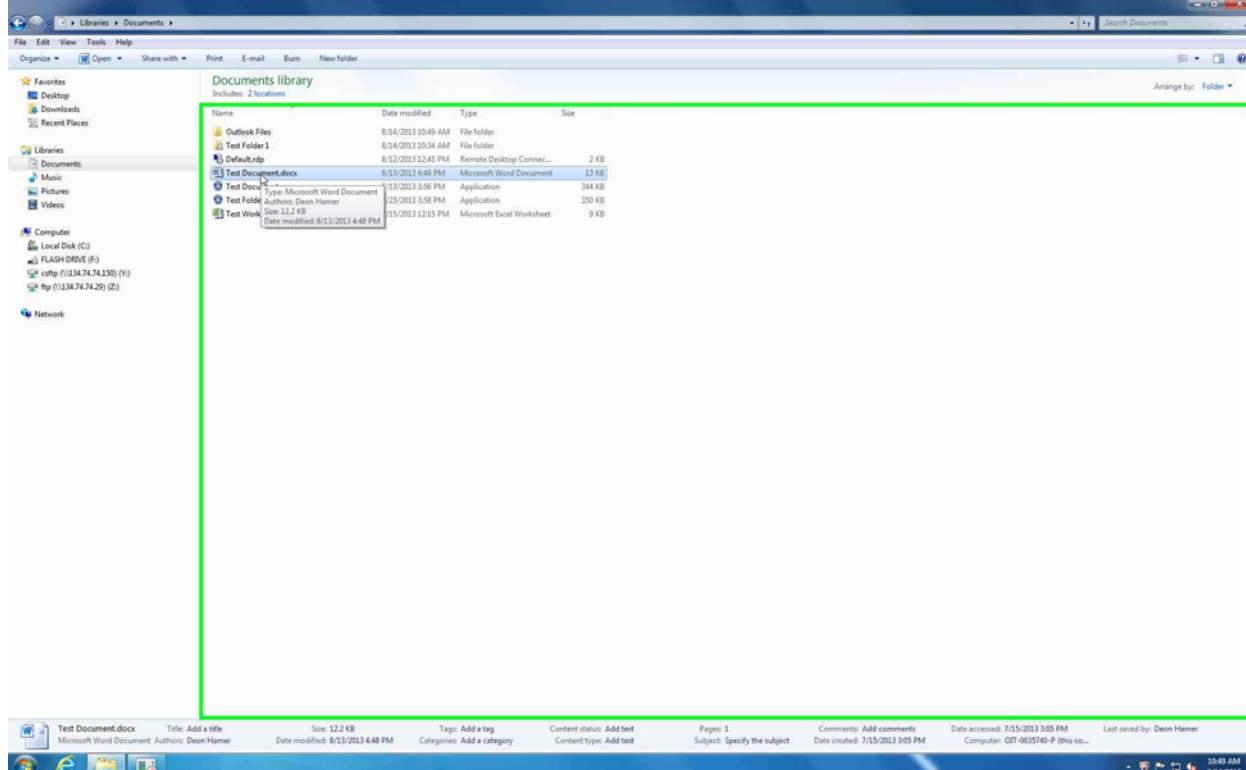
You can attach a file or a folder as a self-extractor to an email.

The self-extractor is packaged into a *.cab file, which can be attached to an email.

You can attach a file or a folder as a self-extractor using any email program.

*Email messages sent with a *.cab self-extractor attachment might be blocked by a recipient's virus protection program.*

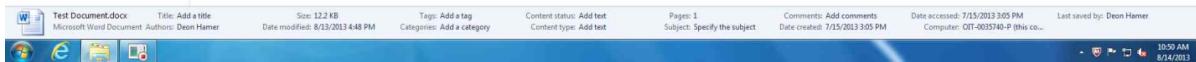
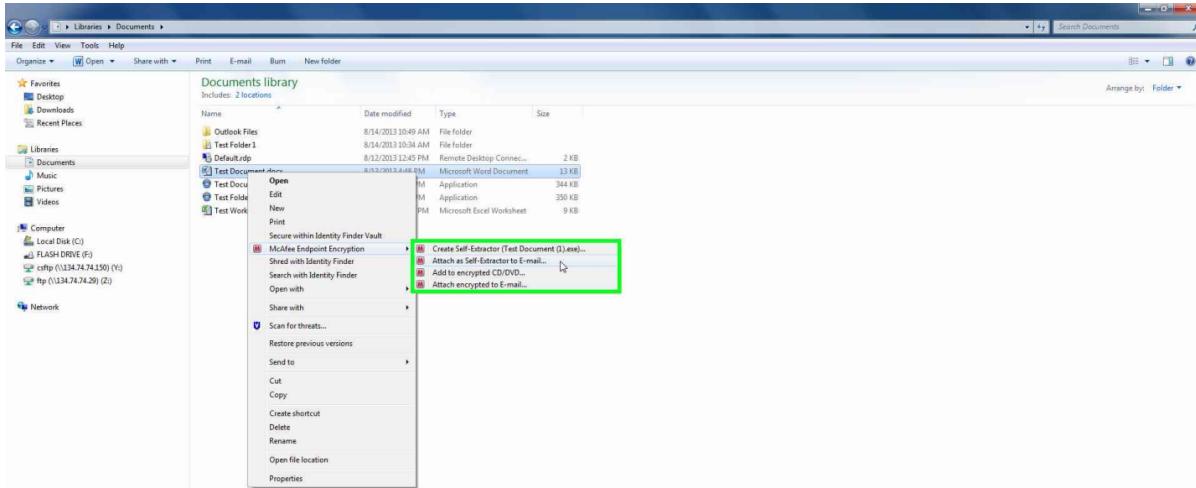
1. Right click the file or folder where you want to create a self-extractor.



2. Select

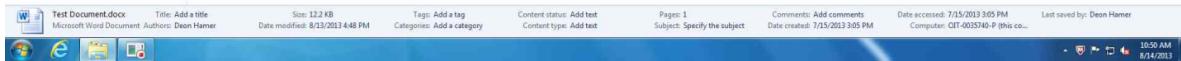
McAfee Endpoint Encryption | Attach Self-Extractor to E-mail

McAfee Endpoint Encryption for Files and Folders



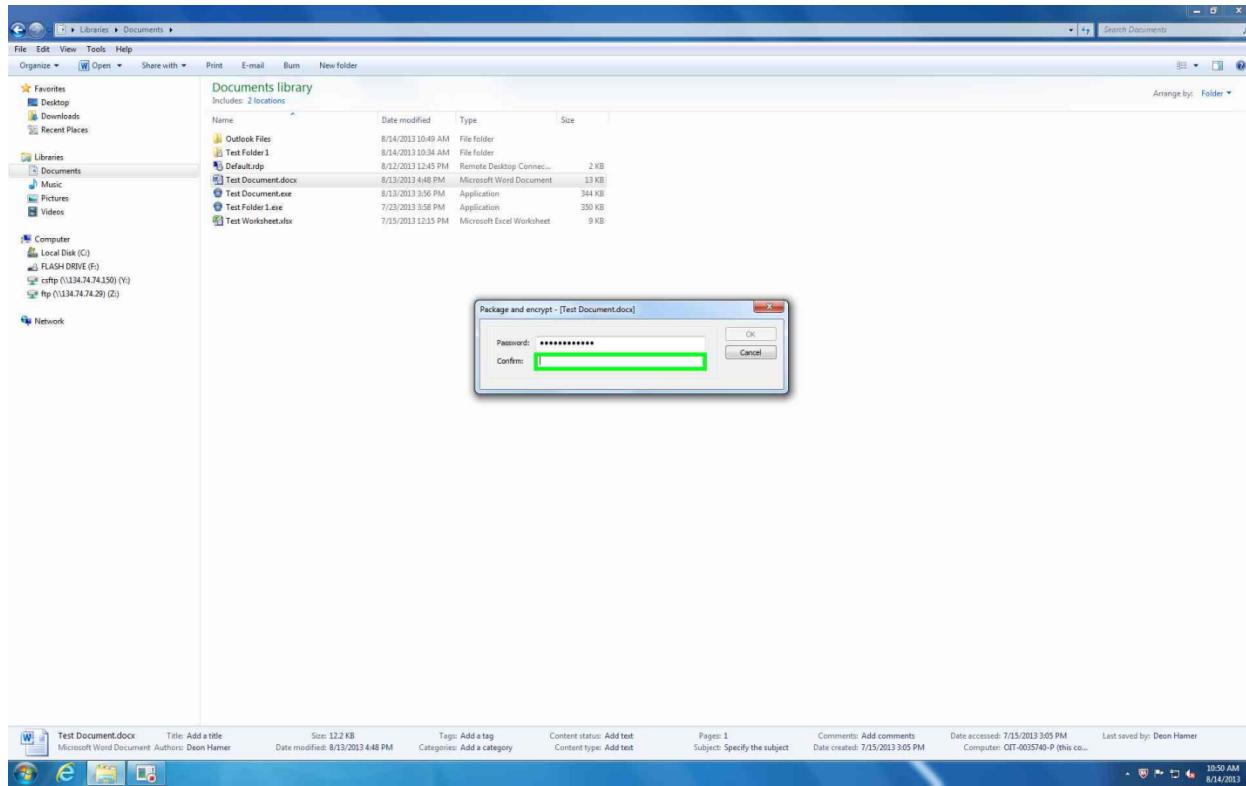
The **Package and encrypt** dialog box appears.

3. Enter the password you want to use to encrypt the self-extractor.



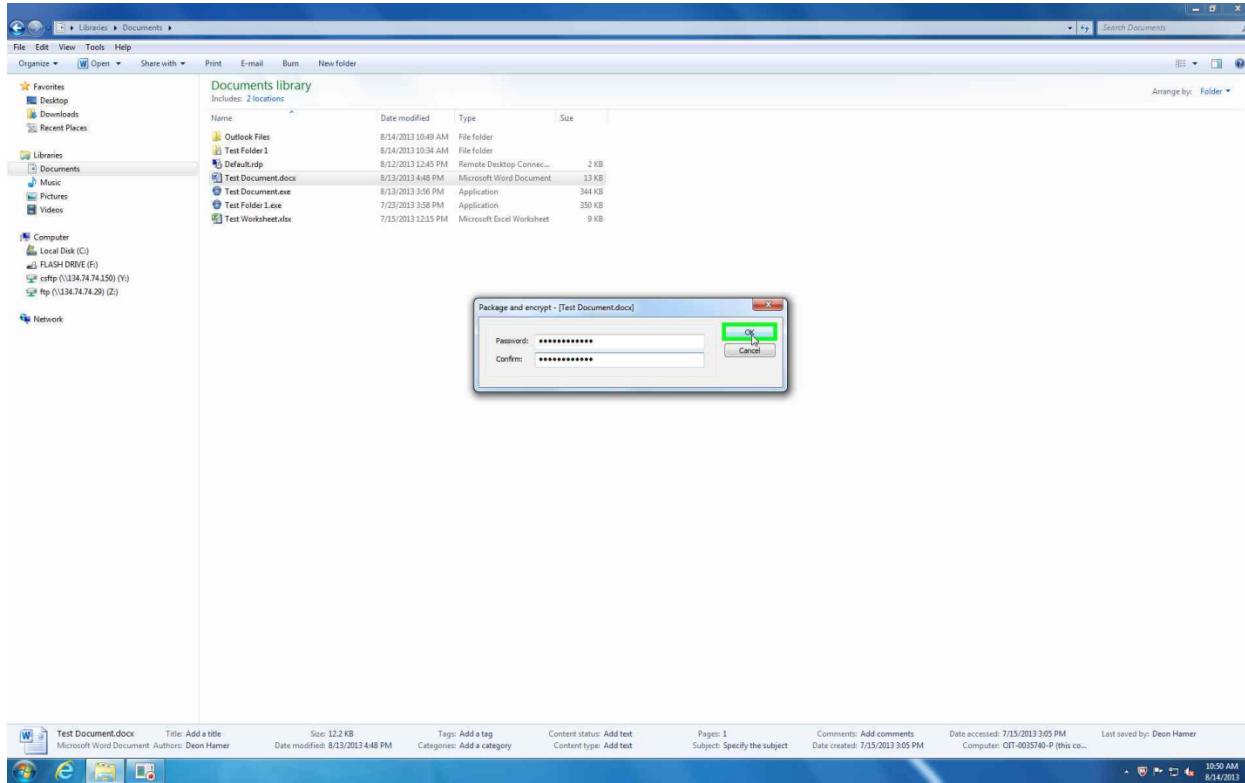
McAfee Endpoint Encryption for Files and Folders

4. Re-enter the password you want to use to encrypt the self-extractor.



5. Click OK.

McAfee Endpoint Encryption for Files and Folders



The source file/folder remains intact on disk; only a copy of the file/folder is converted into a self-extractor and attached to an email.

Attach an Encrypted File

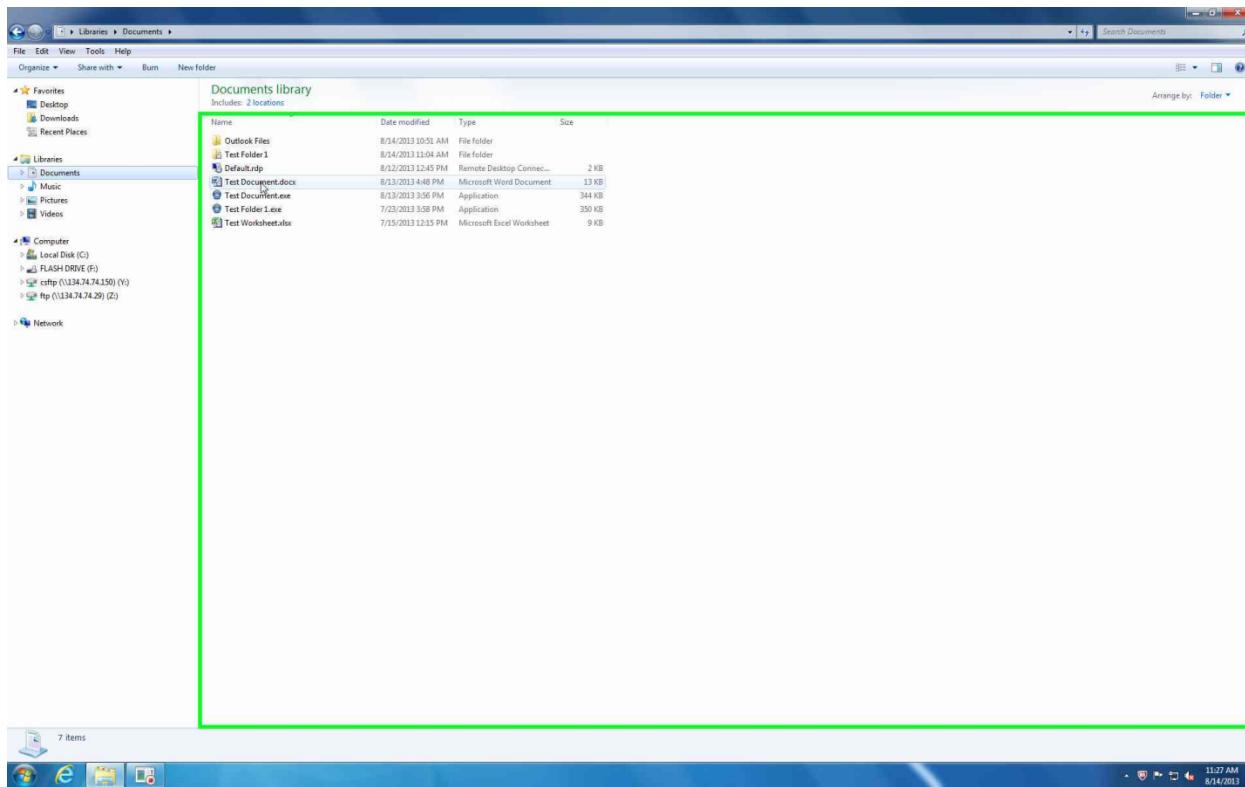
You can send a file (plain text or encrypted) in a protected way. The recipient must have EEFF installed and must have access to the encryption key.

If you attach an encrypted file to an email without using Attach encrypted to E-mail, the file is attached as plain text even if the file is encrypted on disk. The source file is still encrypted, but the copy attached to the email is sent to the recipient in plaintext (unprotected).

Email attachments of self-extractor files up to 10 MB in size are supported.

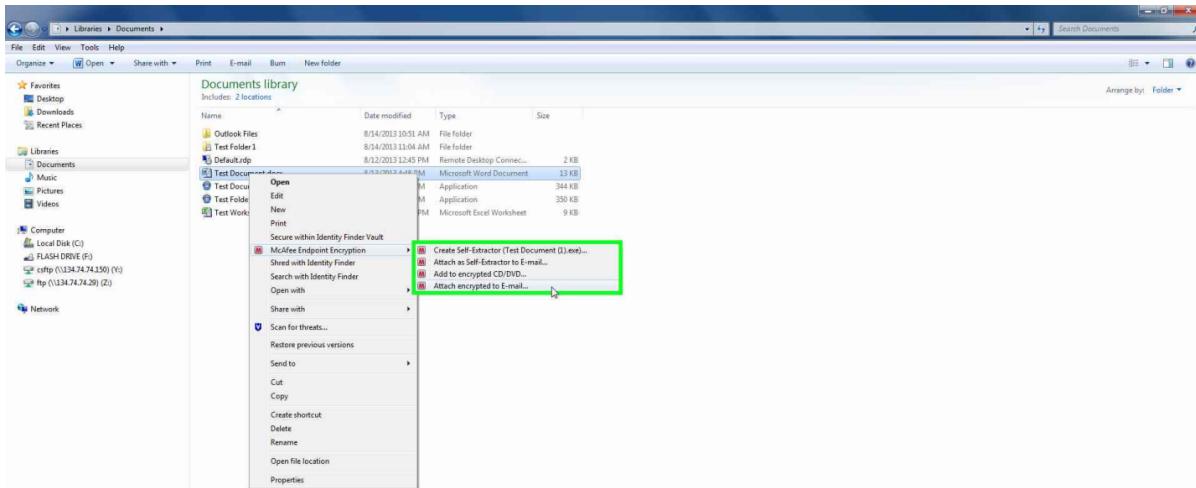
1. Right click the file.

McAfee Endpoint Encryption for Files and Folders



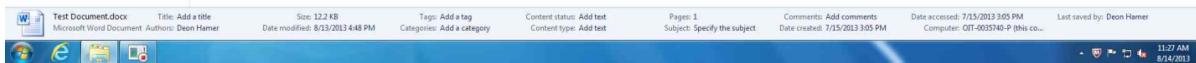
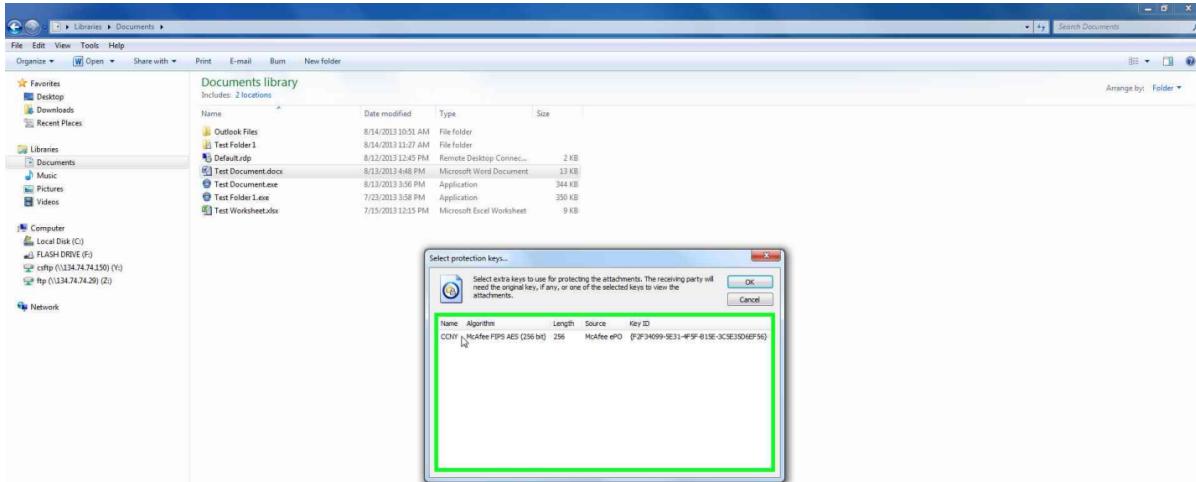
2. Select McAfee Endpoint Encryption | Attach encrypted to E-mail.

McAfee Endpoint Encryption for Files and Folders



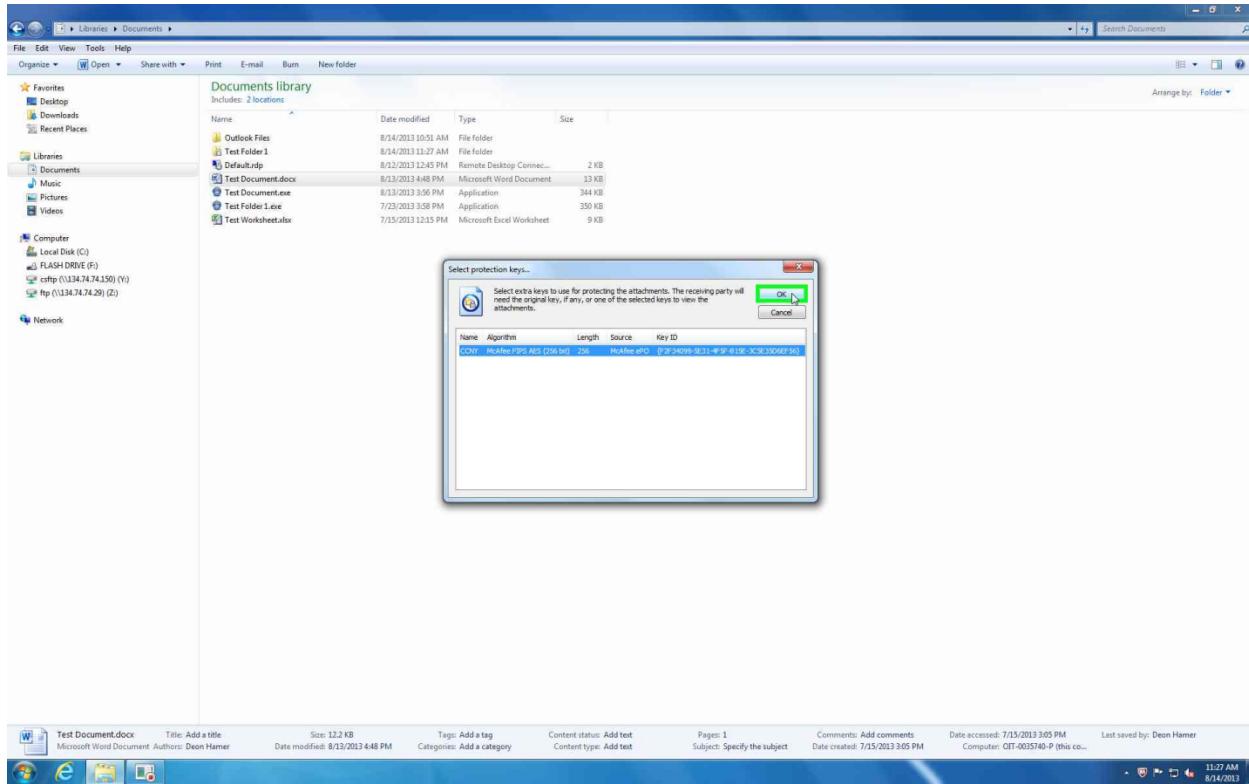
The **Select protection keys** dialog box appears.

3. Select CCNY as the key you want to encrypt the file with.



McAfee Endpoint Encryption for Files and Folders

3. Click OK.



A *.sba file is attached to the email.

Removable Media

McAfee Endpoint Encryption for Removable Media (EERM) is a software solution that encrypts removable devices to protect data stored in the device.

Available Options:

Initialize Removable Media

Recover Removable Media Password

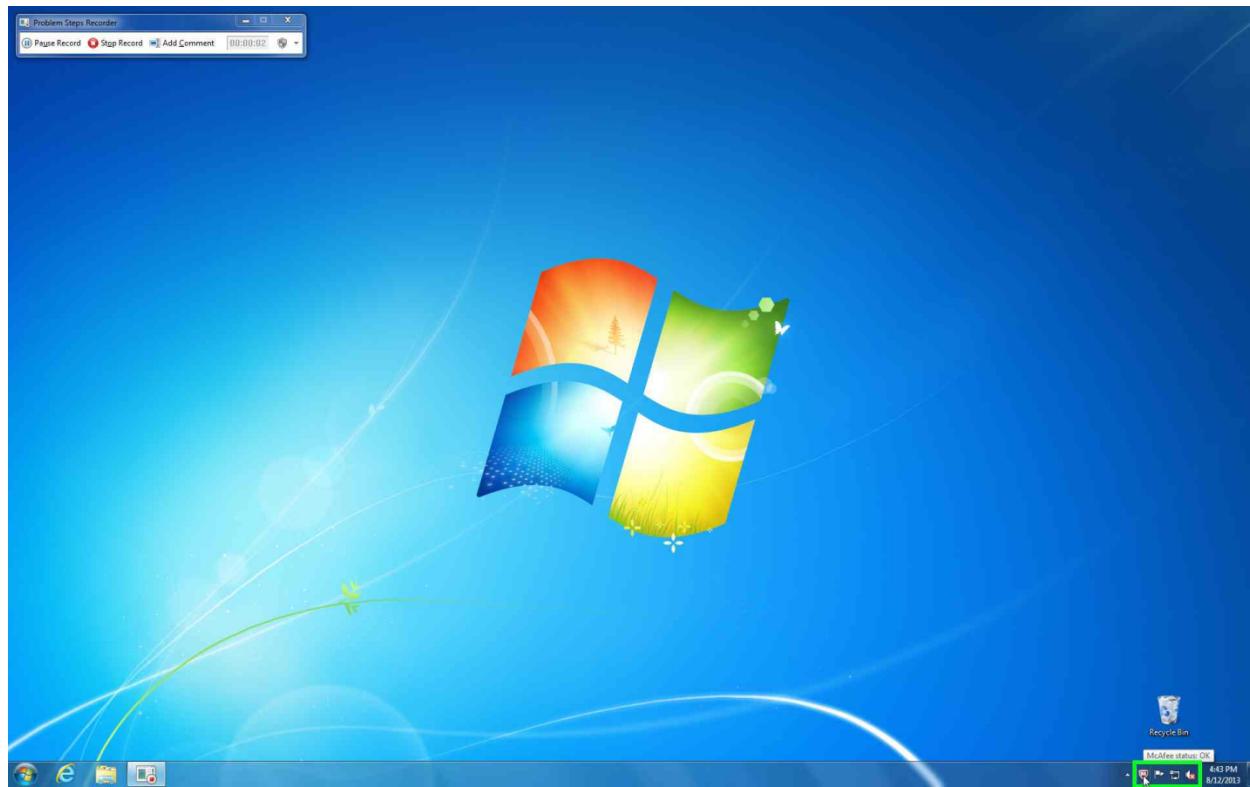
Initialize Removable Media

When you insert a non-protected removable device on a client with EEFF installed and the policy for removable media is enabled, you are prompted to initialize the device.

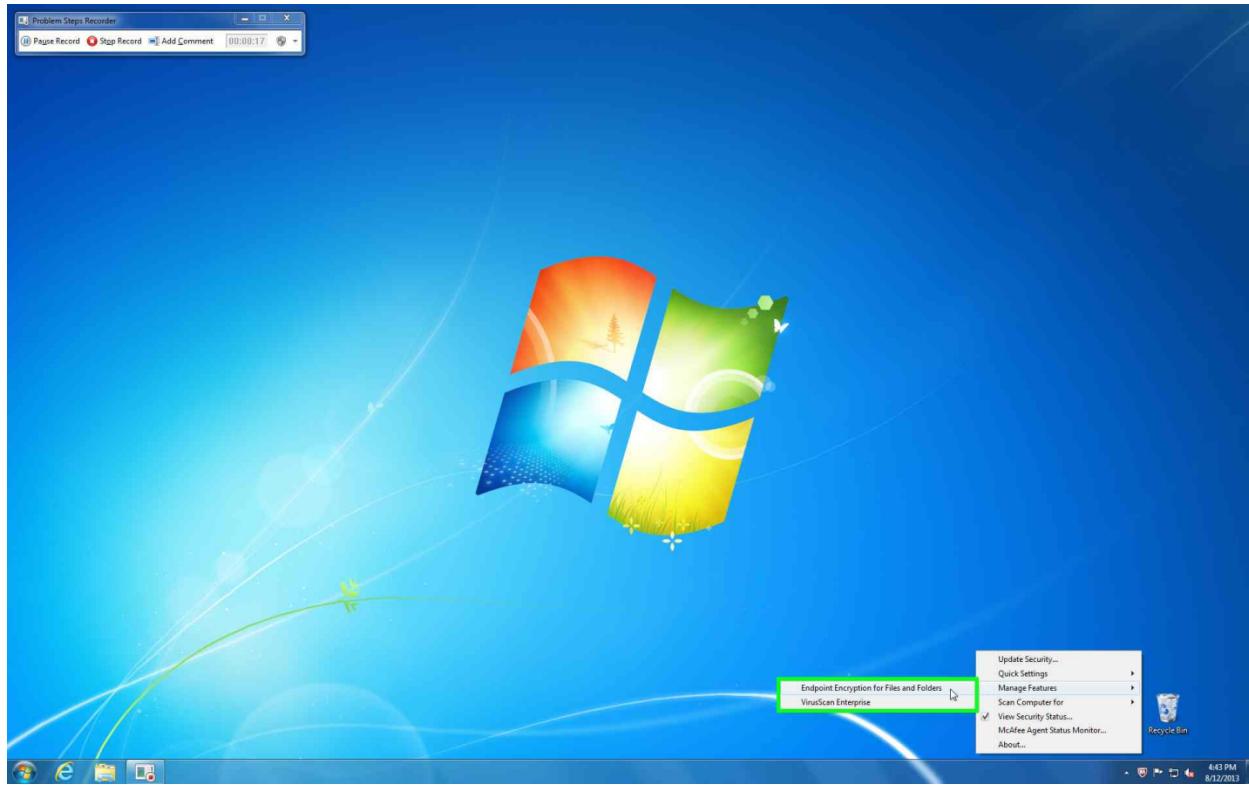
You can also initiate initialization of the removable media using **McAfee Endpoint Encryption for Files and Folders** client console.

If you have data on the removable media, BACK IT UP BEFORE YOU INITIALIZE!!!

1. Click the McAfee icon  on your taskbar.

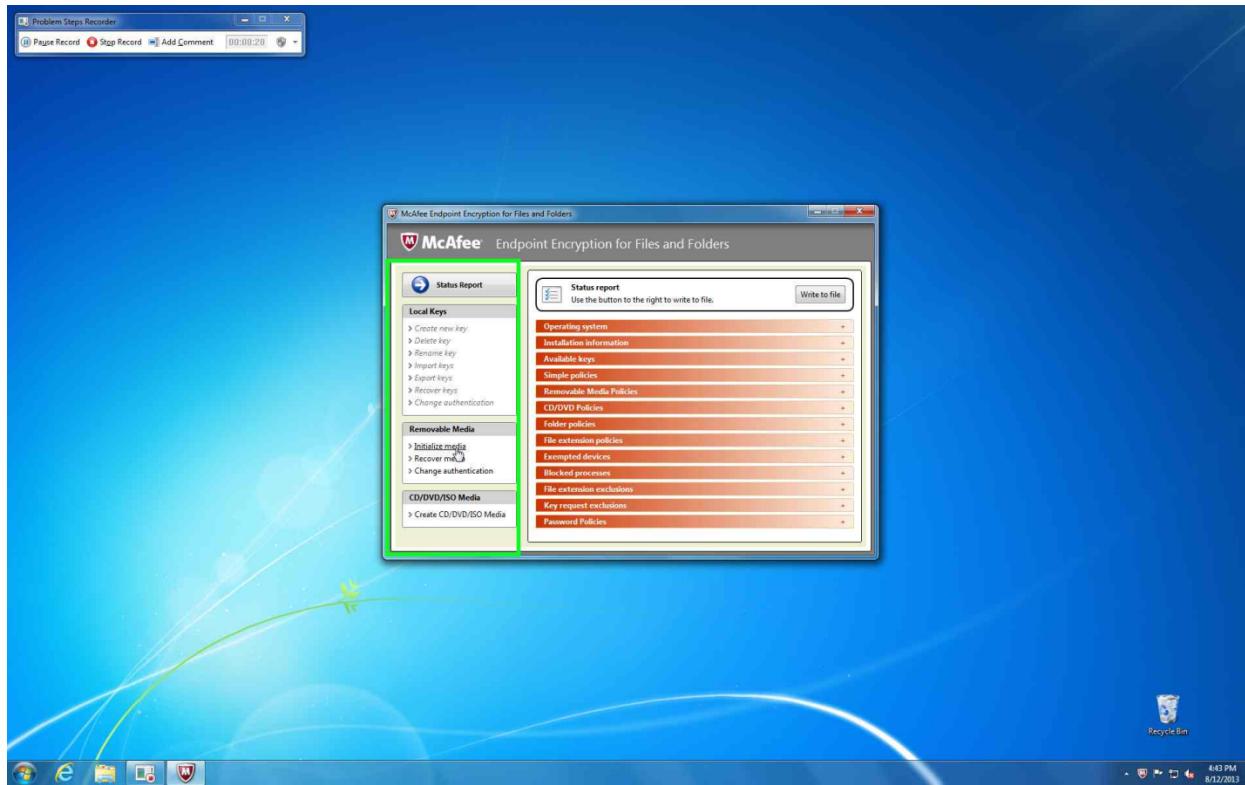


2. Select Manage Features | Endpoint Encryption for Files and Folders.



The **Endpoint Encryption for Files and Folders** client console appears.

3. In the left pane, click Initialize device.



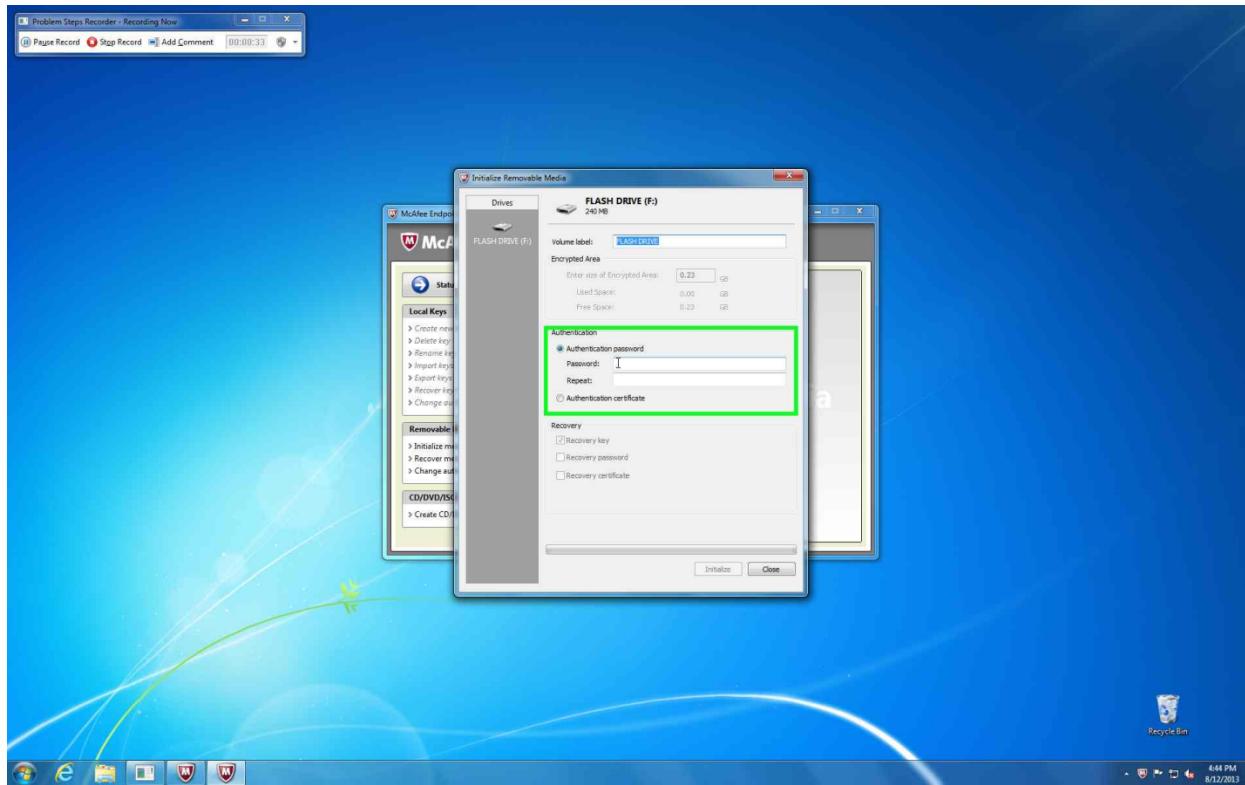
4. In the **Initialize Removable Media** dialog box, if the **Encrypted area** section is enabled, set the amount of space (in GB) on the device that you want to protect.

The ability to decide on the size of the protected area depends on the removable media encryption policy enforced on the system or user.

By Default, the policy gives users the ability to decide on the size of the protected area if the removable media is larger than 64 GB.

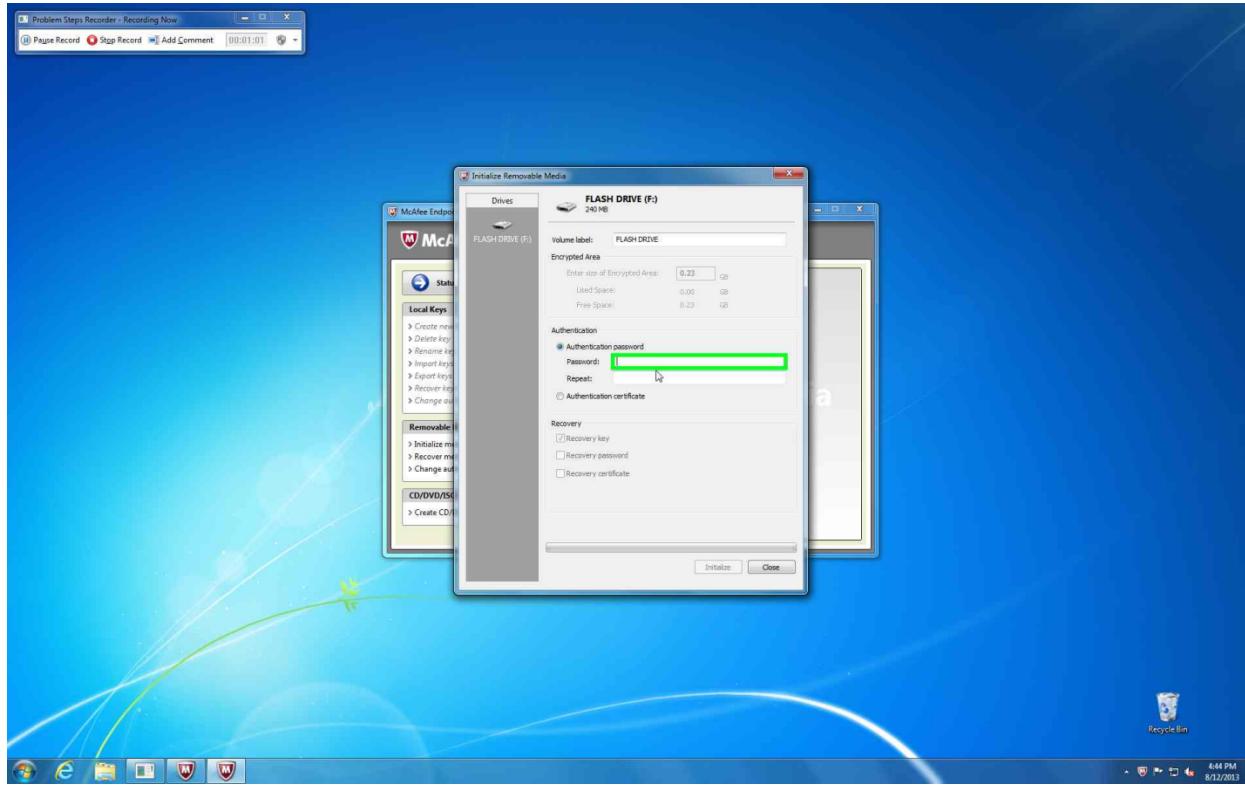
5. In the **Authentication** section, select **Authentication password**.

McAfee Endpoint Encryption for Files and Folders



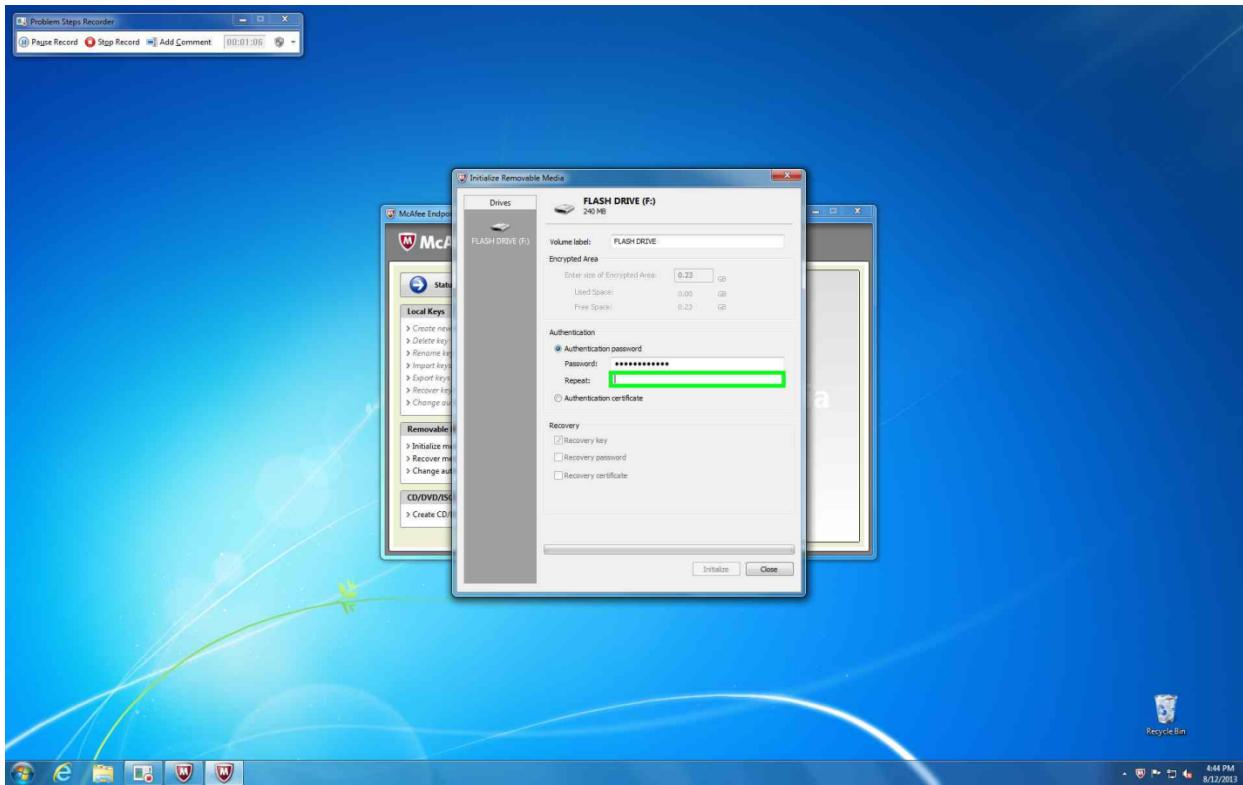
McAfee Endpoint Encryption for Files and Folders

6. Enter a password (must contain at least 8 characters, at least one upper case letter, at least one lower case letter, at least one number, and at least one symbol)

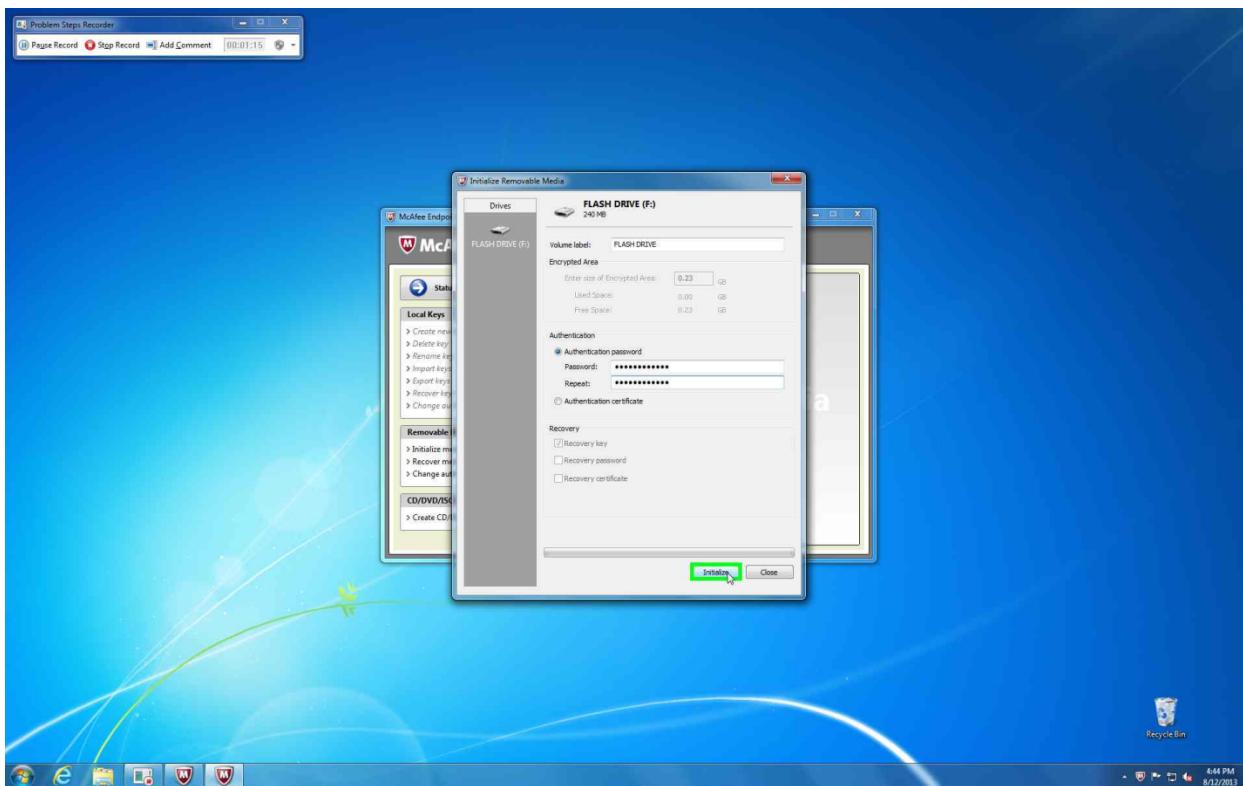


7. Re-enter Password.

McAfee Endpoint Encryption for Files and Folders



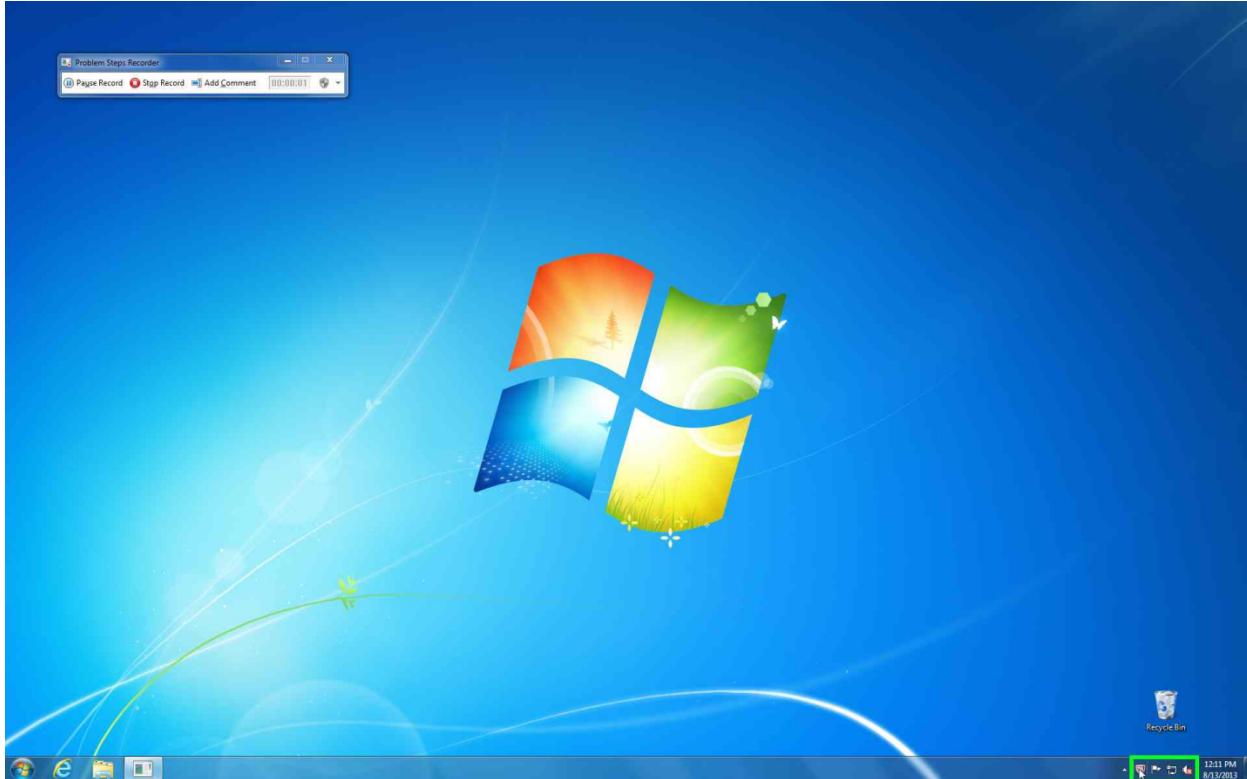
7. Click **Initialize**.



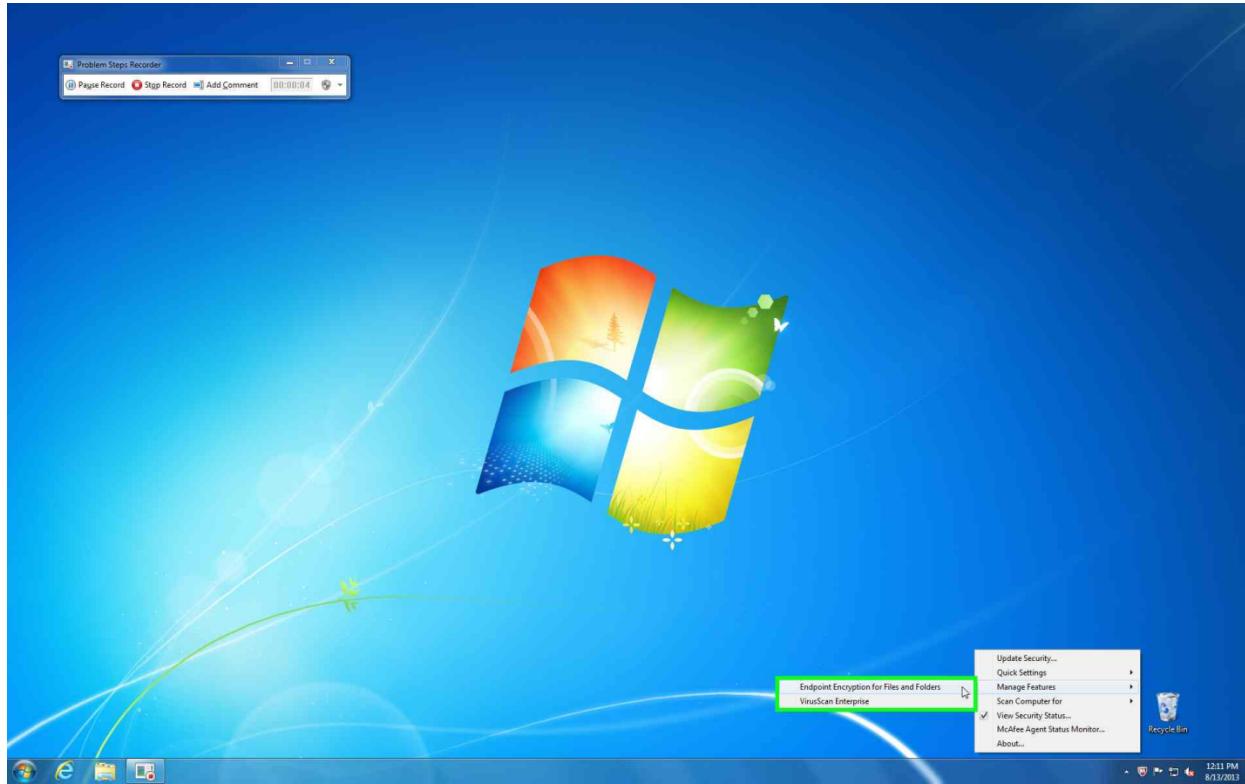
Recover Removable Media Password

You can recover (by resetting the password) access to the information on removable media using a recovery key located on the computer used to initialize the media.

1. Click the McAfee icon  on your taskbar.



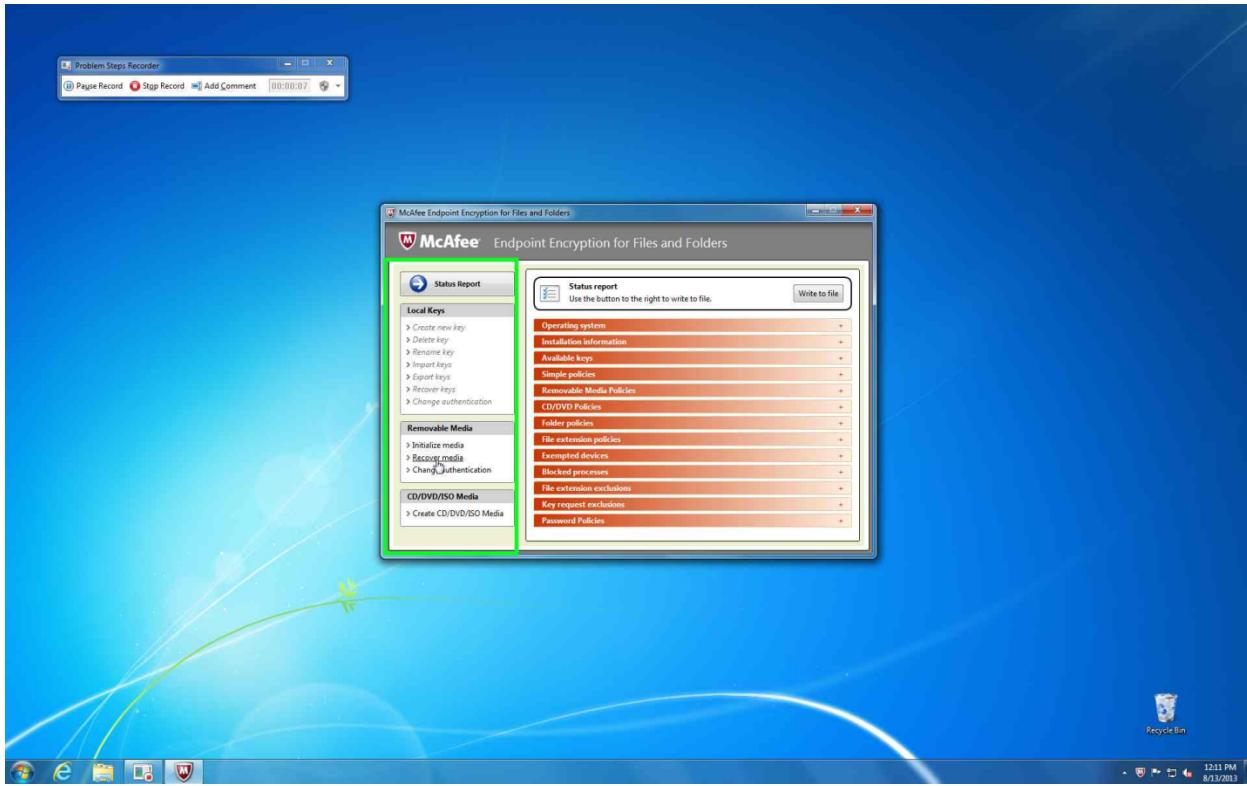
2. Select Manage Features | Endpoint Encryption for Files and Folders.



The **Endpoint Encryption for Files and Folders** client console appears.

McAfee Endpoint Encryption for Files and Folders

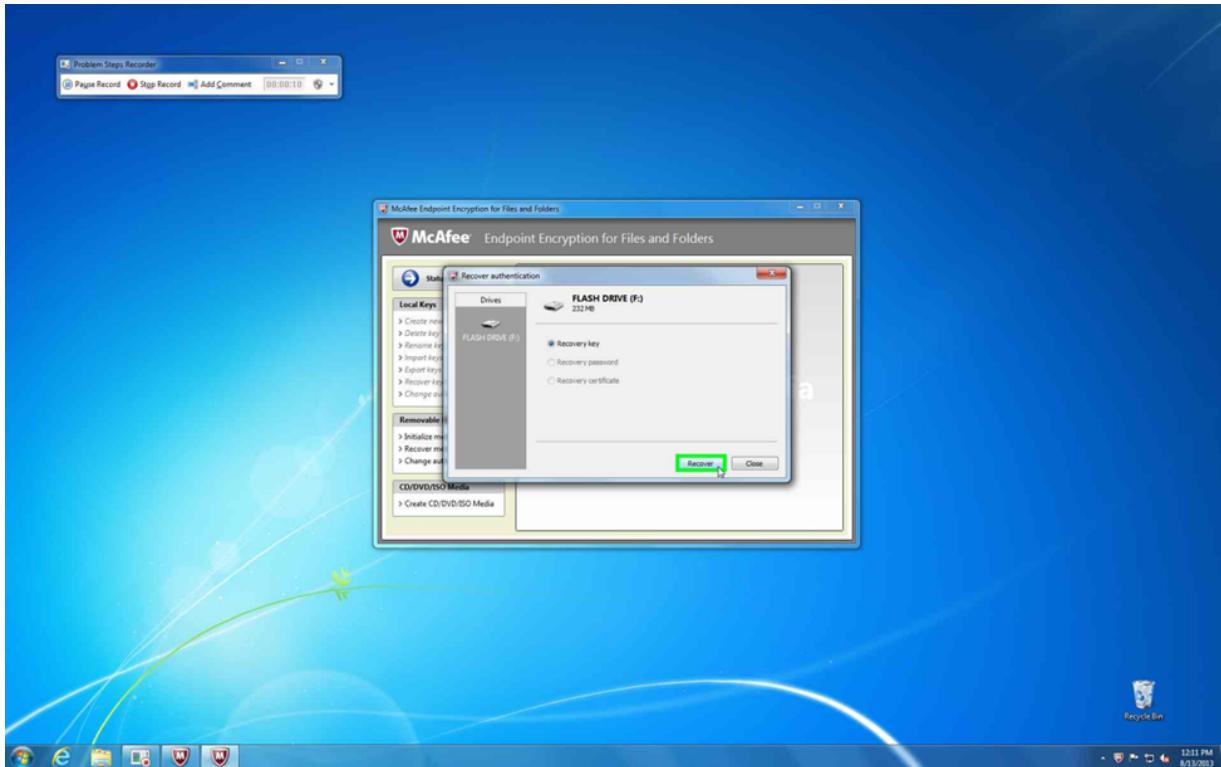
3. On the left pane, click **Recover media**.



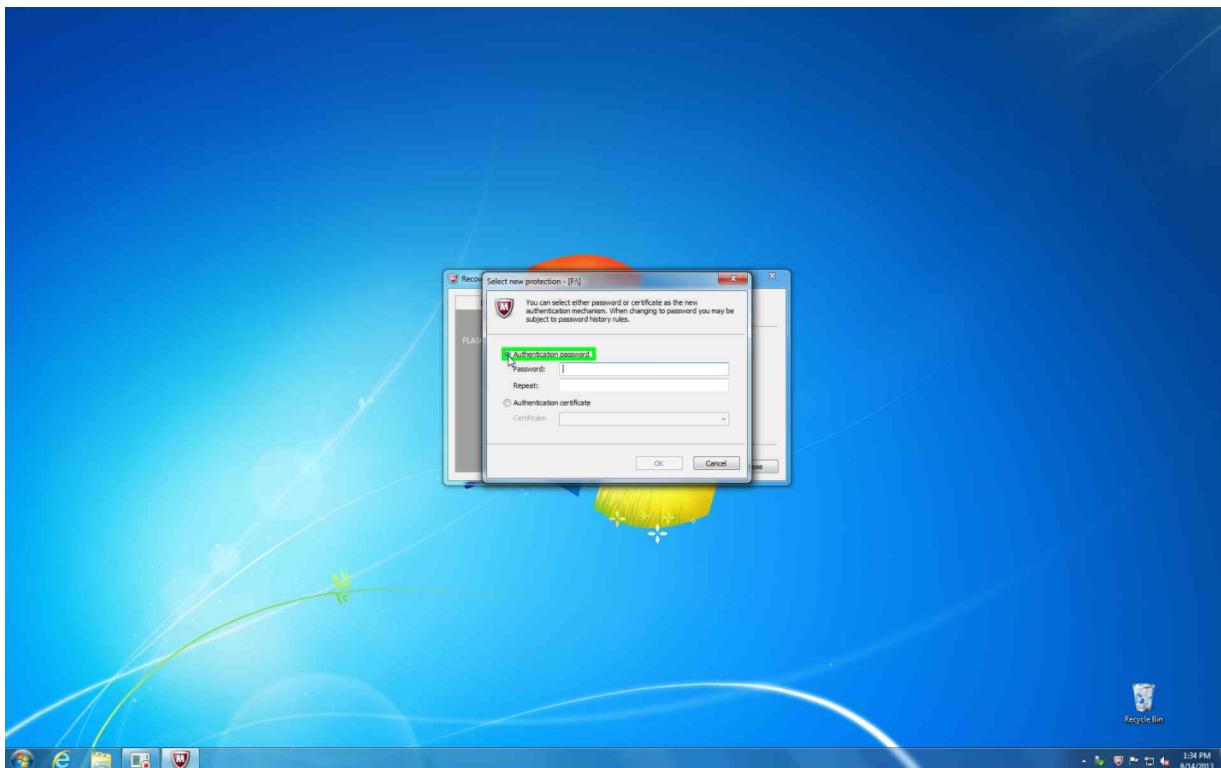
The **Recover Authentication** window appears.

McAfee Endpoint Encryption for Files and Folders

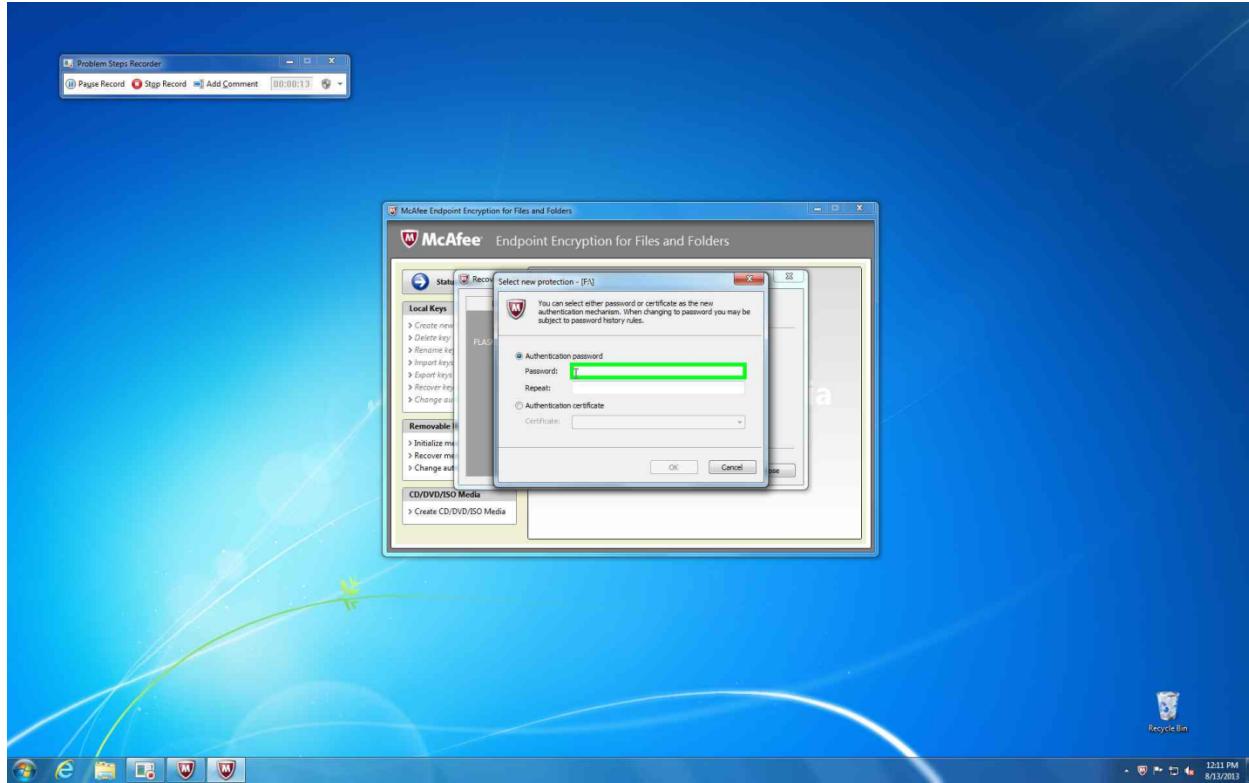
4. Click Recover.



5. Select Authentication password (radio button)

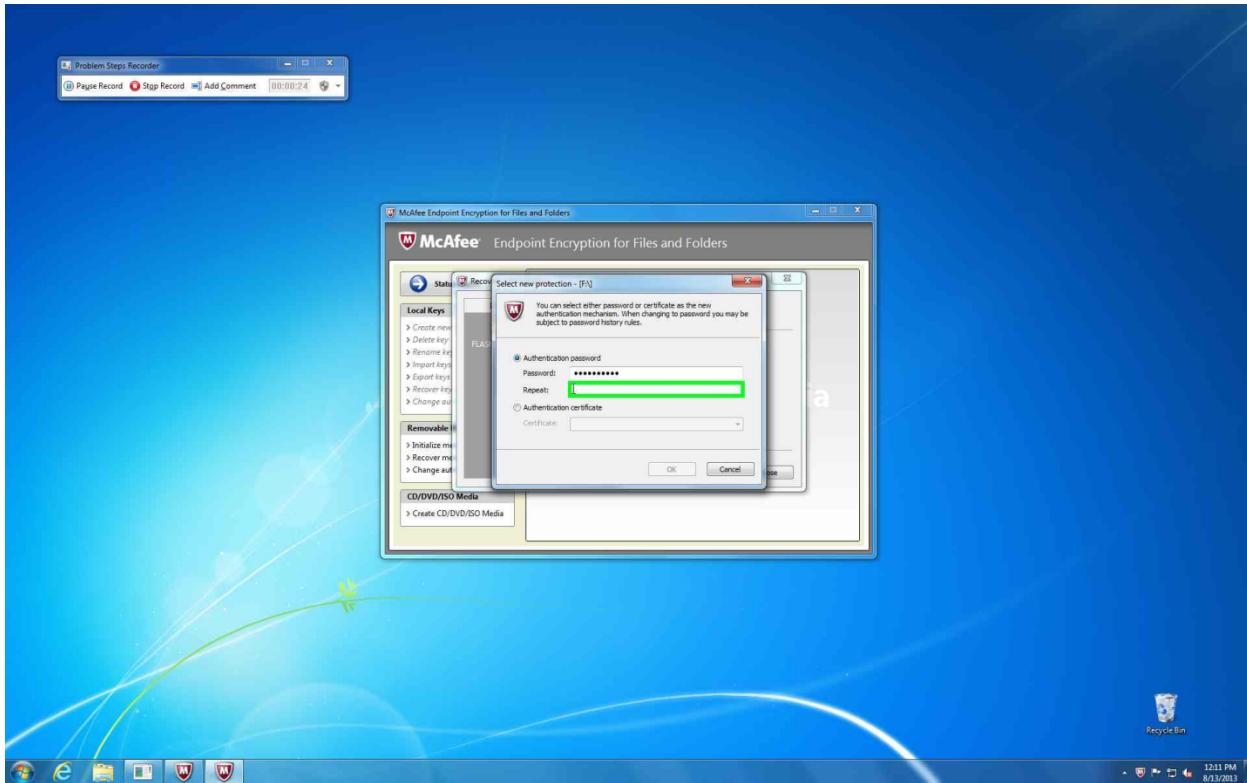


6. Enter new password



McAfee Endpoint Encryption for Files and Folders

7. Re-enter new password



McAfee Endpoint Encryption for Files and Folders

8. Click **OK**.

