

Dell Data Protection

USB Drive Encryption

Introduction

To further protect PC's that have access to sensitive data, the Dell Data Protection (DDP) client detects and encrypts USB/Flash drives when they are plugged into an encrypted system. To access these files, you will need a password. The goal of this is to protect the sensitive data in the event that the USB device is lost or stolen. Without the password to unlock the files, an unauthorized user will be unable to access the data.

Encrypting a USB Drive

Once a USB drive has been inserted into an encrypted machine, the Dell Data Protection software will recognize the unencrypted device.

1. Once the device drivers have loaded, the **Unprotected Media Found** window will appear. Click **No** if you want to view files but not access them.
2. To encrypt the drive for future use, click **Yes**. This will start the encryption process.



Figure 1

3. The **Enter New Password** box will appear. In the **New Password** box, enter a password for the device that meets the following criteria:
 - 8 characters long
 - At least 1 uppercase alpha character
 - At least 1 numeric character
 - At least 1 special character (!,@,#,\$,%,_ etc.)

4. Retype the password in the **Retype Password** box.



Figure 2

5. Click the **OK** button. The drive will begin encrypting.



Figure 3

6. After the encryption process completes, the **External Media Device Protected** window will appear. Click **OK** and begin using the USB drive as you would normally.



Figure 4

Accessing Encrypted Files from an Unencrypted PC

To access the files on an encrypted USB/Flash drive from an unencrypted system you must launch a software program on the USB drive. The following steps will walk you through the process.

1. Insert your USB drive into the unencrypted PC.
2. Locate your drive from the **Explorer** window and double-click on it to reveal the files. The USB drive will appear with a key beside it.

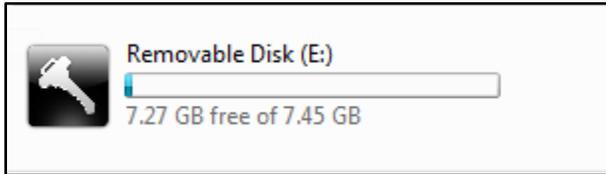


Figure 5

Note: You will not be able to open encrypted files directly from the USB drive on an unencrypted machine. You will be able to open unencrypted files.

3. Locate the **AccessEncryptedFiles.exe** file. Double-click the file to launch it.

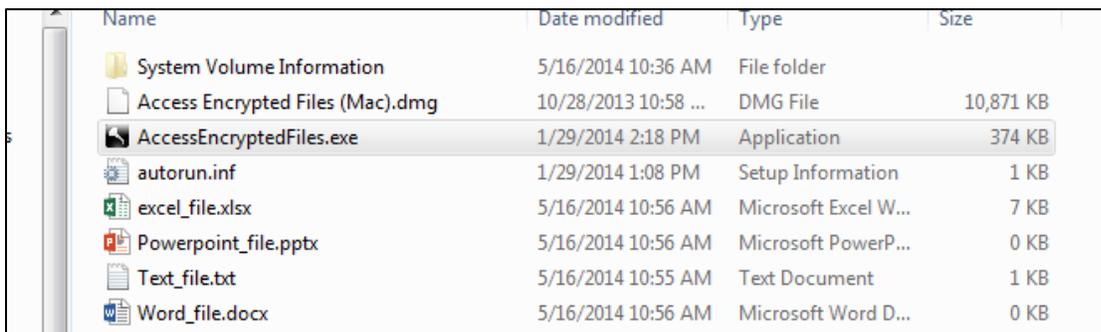


Figure 6

4. The **External Media Shield Options** screen dialog box will appear. Select **Run EMS Explorer** (recommended).

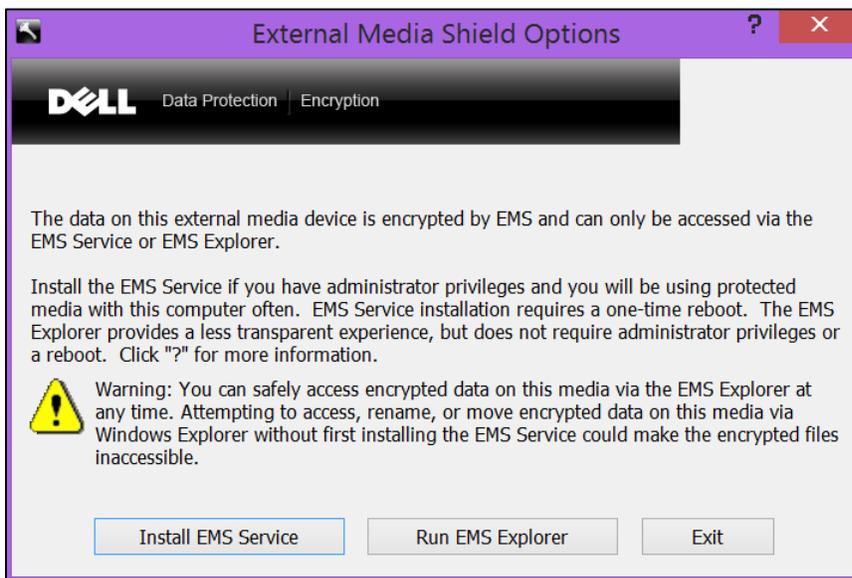


Figure 7

Dell Data Protection: USB Drive Encryption

Note: Install EMS Service is not recommended. A reboot of the system is required if you select **Install EMS Services** and you will also need Administrator Privileges.

5. The **Enter External Media Password** dialog box will appear. In the **Password** box, enter the passphrase you created when encrypting the drive and click **OK**.



Figure 8

6. The **EMS Explorer** window will launch and **Secured** will show up in the **Status** column of encrypted files. You will have the ability to open, copy, paste and delete files through the **EMS Explorer**.

Note: Any files that have not been encrypted may be opened up as you would normally through the Windows Explorer.

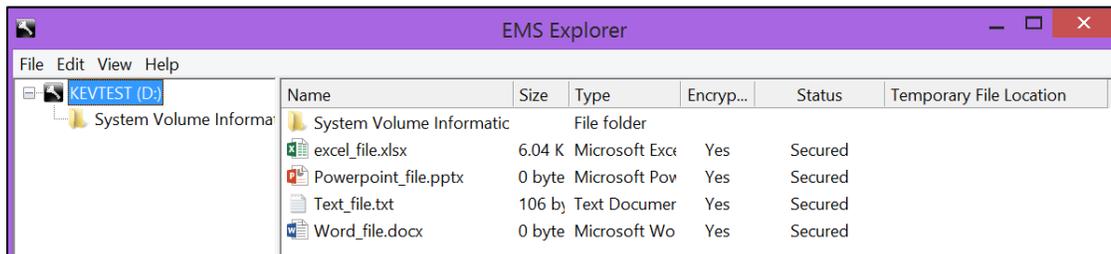


Figure 9

7. Double-click on a **Secured** file to open. The **Path to Temporary Files** dialog box will appear. This is a temporary location that will store your decrypted files. Accept the default file location by clicking the **OK** button. Your file will open and the **Status** will change to **Managed** in the **EMS Explorer** window. When finished, close the **EMS Explorer** window and safely eject the USB drive.

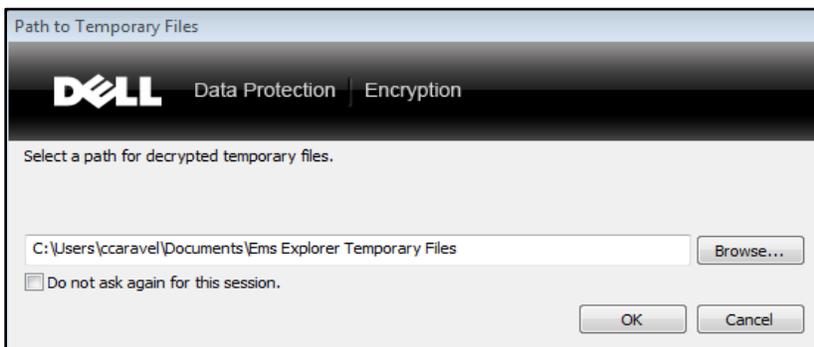


Figure 10

Note: You must safely eject the USB drive by clicking on the **USB icon** in the task bar and then by clicking on **Eject** from the menu.

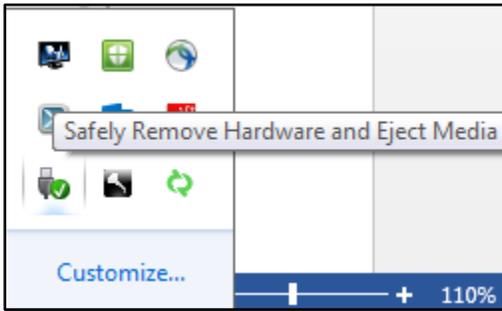


Figure 11

Accessing Encrypted Files from an Encrypted PC

1. Insert your USB drive into the encrypted PC.
2. The **Enter External Media Password** screen will appear. In the **Password** box, enter the passphrase you created when encrypting the drive and click **OK**.

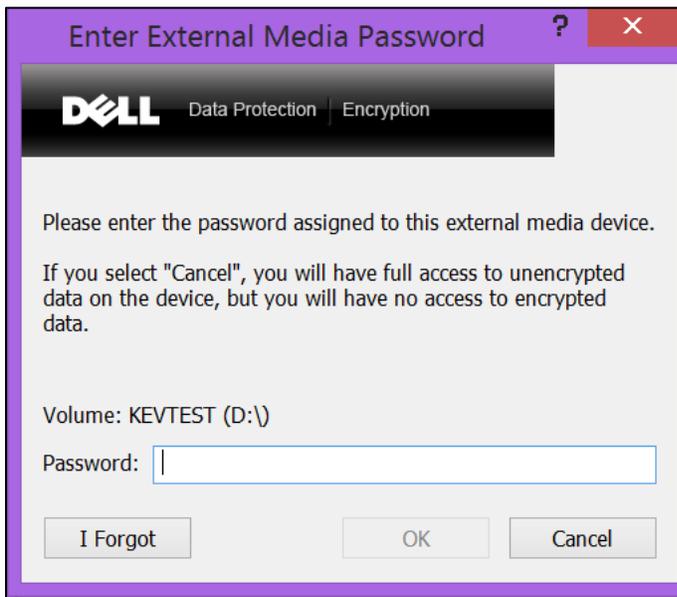


Figure 12

3. Locate your drive from the Explorer window and double-click on it to reveal the files. The USB drive will appear with a key beside it.

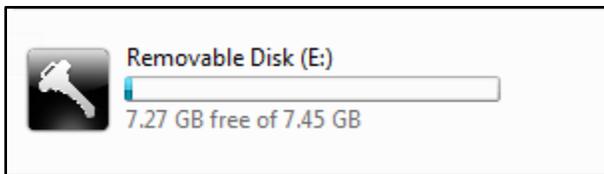


Figure 13

4. Locate the file you wish to open and double-click on it. When finished, close the **EMS Explorer** window and safely eject the USB drive.

Recovering from a Lost or Forgotten Password

If you forget your password or input the incorrect password 3 times, your device will become locked out.

1. At the **Enter External Media Password** box, click the **I Forgot** button. The **External Media Device Manual Authentication Failed** box will appear.



Figure 14

2. Contact the OTS Help Center at 410-704-5151 and provide the **Recovery Key ID** and **Shield ID**. The Help Center will provide you with an **Access Code**.
3. In the **Access Code** field, enter the code given to you by the Help Center and click **OK**. You will then be prompted to create a new pass phrase for your USB device.

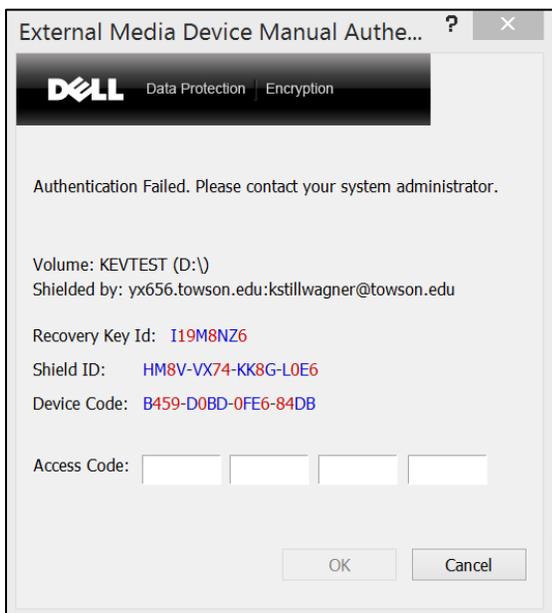


Figure 15