Removable Storage Encryption

Marc Lowe on December 5, 2018

Removable Storage Encryption

Dell Data Protection Encryption - External Media Shield (EMS)

UCSF's current standard encryption program, Dell Data Protection Encryption (DDPE), has the capability to encrypt data on removable storage devices through a feature called External Media Shield (EMS).

When you enable EMS on a removable storage device like a USB hard drive or flash drive, DDPE encrypts files that are copied from a UCSF computer to the drive. You can read and write encrypted data on the drive from any computer, even if it does not have DDPE installed. DDPE EMS is file-based encryption and is compatible with both Windows and Mac OS X, so you can read and write encrypted data from both platforms on the same external drive. EMS allows you to use common, inexpensive removable drives to securely store UCSF data.

UCSF IT Security & Policy will be rolling out EMS to UCSF Medical Center users, UCSF Campus users, BYOD Mac users, and finally BYOD PC users.

You will receive an email from IT Service Desk (ITServiceDesk@ucsf.edu) when EMS is enabled for your UCSF user account.

Remember: always have a backup of your data before encrypting or decrypting it.
Using DDPE Removable Storage Encryption

DDPE Removable Storage Encryption is currently enabled on UCSF PCs for Campus, SOM, and Medical Center accounts. It will be enabled on UCSF managed Macs in a staged rollout.

<table>
<thead>
<tr>
<th>Go Live Date</th>
<th>Macs enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 30, 2018</td>
<td>250 ITFS-managed Macs:</td>
</tr>
<tr>
<td></td>
<td>Mac desktops (iMac, Mac Mini, Mac Pro) with serial</td>
</tr>
<tr>
<td>February 6, 2018</td>
<td>500 ITFS-managed Macs:</td>
</tr>
<tr>
<td></td>
<td>Mac desktops (iMac, Mac Mini, Mac Pro) with serial</td>
</tr>
<tr>
<td></td>
<td>Mac laptops (Macbook Air, Pro, Retina, etc. models)</td>
</tr>
<tr>
<td>February 13, 2018</td>
<td>750 ITFS-managed Macs:</td>
</tr>
<tr>
<td></td>
<td>Mac laptops (Macbook Air, Pro, Retina, etc. models)</td>
</tr>
<tr>
<td>February 20, 2018</td>
<td>1000 ITFS-managed Macs:</td>
</tr>
<tr>
<td></td>
<td>Mac laptops (Macbook Air, Pro, Retina, etc. models)</td>
</tr>
<tr>
<td>TBD</td>
<td>UCSF Macs which are not managed by ITFS, deployed</td>
</tr>
</tbody>
</table>

Macs must have DDPE 8.16 or later installed to activate DDPE Removable Storage Encryption on an external drive. DDPE 8.16 is being automatically deployed by ITFS Desktop Engineering to Macs running OS X 10.11.6, 10.12.6, and 10.13.x.

If you have a Mac running an earlier version of OS X, you will need to upgrade it to OS X 10.11.6, 10.12.6, or 10.13.x to activate DDPE Removable Storage Encryption on a external drive.

To turn on EMS on a removable drive:
1. You will receive an email when EMS is activated for your UCSF user account
2. Log in as yourself to a Mac encrypted with DDPE or a UCSF PC encrypted with DDPE.
3. Plug in your removable storage device.
4. DDPE will prompt you to enable encryption the drive.

Click “Yes” to activate encryption on the removable drive
Click “No” to get read-only access to the removable drive

5. Create a password for the drive.
   Passwords should meet the same complexity rules as the UCSF Password Standard [2]:
   7+ characters, with an Upper Case, lower case, and number or symbol.
EMS does not encrypt data that is already stored on a removable drive. You will need to move files off the drive and then back on to encrypt them.

To access data on a drive with EMS:

To access data on a drive with EMS, you need either of the following:

- A Mac encrypted with DDPE or a UCSF PC encrypted with DDPE
  
  or

- The password you created when you activated EMS on the drive

If you are logged in to a UCSF PC or Mac with DDPE, DDPE will automatically unlock the drive based on your login. If you are sharing a drive with another person, they will need your drive password to access encrypted data on your EMS-encrypted drive.

If you are on a computer that is offline, does not have DDPE, or is logged in as somebody else, you will need to provide the drive password to access encrypted files.

DDPE includes a copy of EMS Explorer on each EMS-encrypted drive, which you can use to read and write encrypted data. You can access this by launching the "AccessEncryptedFiles" program on the drive.
EMS Explorer will allow you read+write access to encrypted data through the application, which works as a standalone file browser. You will need to access encrypted files through EMS explorer, rather than through your computer's normal file browser (Windows Explorer / Mac OS X Finder).

The EMS Service is recommended for non-UCSF computers that you frequently use, although computers frequently used for UCSF work should be encrypted [3]. It will install and run in the background, and transparently provides read+write access to encrypted data if the correct password is entered. It does require administrator rights to and a reboot to install before use.

Both are available for Mac and Windows, and the programs are automatically copied on to a drive when EMS is activated on it.

Resetting an EMS password

If you forget your EMS password:

1. Log in to a UCSF PC that has DDPE
2. Open the DDPE application
3. Click on "Removable Storage"
4. Click on "Change Password"
If you forget your EMS password and do not have access to a UCSF PC with DDPE:

1. Click the "I Forgot" button on the EMS password prompt
2. Call the IT Service Desk at 415-514-4100
3. Provide the IT Service Desk with the:

   Shield ID
   Device Code
   (Recovery Key ID is not necessary)
To avoid confusion, letters are colored blue and numbers are colored red.

4. The IT Service Desk will generate a corresponding Access Code, which will allow you to create a new password for your EMS-encrypted drive.

Removable Storage Encryption Policies

If you are using a UCSF PC and have a Medical Center (UCSFMC) user account

You will be prompted to enable encryption or have read-only access to any removable storage device you plug in to a UCSF PC. You will not be able to copy data from a UCSF PC to a non-encrypted removable drive.

If you are using a UCSF PC and have a Campus or SOM user account
You will be prompted to enable encryption or proceed with read and write access to any removable storage device you plug in to a UCSF PC. If you do not enable encryption on a removable drive, you will be asked the next time you plug in the drive. Some Campus departments may require you to enable encryption on removable drives, please ask your manager or departments’ IT liaison for more information.

If you are using a UCSF Mac with DDPE, or a personally-owned Mac with DDPE

You will be prompted to enable encryption or proceed with read and write access to any removable storage device you plug in to your Mac. If you do not enable encryption on a removable drive, you will be asked the next time you plug in the drive.

If you are using a personally-owned PC with DDPE

You will be prompted to enable encryption or proceed with read and write access to any removable storage device you plug in to your PC. If you do not enable encryption on a removable drive, you will be asked the next time you plug in the drive.

Frequently Asked Questions

See https://it.ucsf.edu/pages/ddpe-ems-frequently-asked-questions-faq [4]
If you have the ability, plug your removable media into a UCSF machine that you have previously logged into. This will enable you to reset your removable media password. Or please call the IT Service desk at 415.514.4100.

Volume: DDPE (D:\)
Shielded by: YourPC.ucsfmedicalcenter.edu: APerson@ucsfme...

Recovery Key Id: ABCD1234
Shield Id: ZYXW-VUTS-0987-4321
Endpoint Code: 1234-5678-ABCD-EFGH-0123-JKLM-4567-NOPQ

Access Code: 

OK  Cancel

Enter New Password

Please create a new password for this external media device. You may be prompted to enter this password whenever this device is inserted into a computer.

If you select "Cancel", the device will be left unshielded but you will be granted read-only access to the device.

Volume: (D:\)
New Password: ****************************************
Retype Password: ****************************************

OK  Cancel
Click “Yes” to activate encryption on the removable drive.

Click “No” to get read-only access to the removable drive.
The data on this external media device is encrypted by Dell EMS and can only be accessed using Dell EMS Service or EMS Explorer.

Install Dell EMS Service if you have administrator privileges and you will be using EMS encrypted media with this computer often. Dell EMS Service installation requires a one-time restart. EMS Explorer provides a less transparent experience, but does not require administrator privileges nor a restart.

**WARNING:** You can safely access encrypted data on this media using EMS Explorer at any time. Attempting to access, rename or move encrypted data on this media via Mac OS X Finder could make the encrypted file inaccessible.

[Cancel] [Launch EMS Explorer] [Install EMS Service]