University IT Services

Installing and Using Sophos SafeGuard Native Disk Encryption for Mac

June 2016

Summary

Sophos Native Disk Encryption provides a managed disk encryption service for users of recent Mac models and OS X versions. It includes a process for securely recovering the encryption key/password should it be lost or forgotten.

Licensing and Permitted Use:

If you are the user of an Apple Mac purchased and owned by Cardiff University our current license agreement permits you to install and use this version of Sophos Disk Encryption for Mac. You are **not permitted** to install or use this software on any systems which are not purchased and owned by Cardiff University.

If you wish to use – **at your own risk** – Apple's FileVault 2 disk encryption on a personal Mac to secure the data stored on it there are instructions here: http://support.apple.com/en-us/HT4790

Please Note:
Failure to follow these instructions or preserve the encryption key/password may result in data loss.
If you lose the key/password you lose access to the stored data – **PERMANENTLY**.

Apple provide a FileVault 2 key recovery service for individual users that may allow access to an encrypted Mac if you forget the password.

University IT Services cannot help you recover encrypted data from a personal Mac with FileVault 2 enabled if the key/password is lost or forgotten.

Minimum system requirements:

To use Sophos Disk Encryption for Mac you **must** have:

- Mac OS X version 10.8, 10.9, 10.10 or 10.11 (previous versions are **NOT** supported).
- A Mac with an Intel CPU.
- at least 4GB of RAM.
- at least 40MB of available hard-disk space.
- a working direct connection to a Cardiff University network (wired or eduroam wireless).
- an admin privilege account for installation of the software.

The installer script will test the following before proceeding with the installation:

- the Mac is running OS X 10.8.x or later
- the Mac is not already joined to an Active Directory domain.

The script will exit if either of the tests fail.

If your Mac already has FileVault enabled you need to supply the existing recovery key to the SafeGuard server so that it is available for future use if required – see the section below the main installation instructions. If you do not know the existing FileVault key you will have to disable FileVault, wait for the disk to un-encrypt and then carry out the installation as described below.

You MUST also have a Time Machine and/or other regularly updated offline backup of any important data on your Mac in case it is needed in the unlikely event that something goes wrong with this installation or your system disk drive fails at some point in the future.

Installing Sophos Disk Encryption:

To set up this software on your Mac you **must** complete the following steps:
(You must be logged in as an admin privileged user to carry these out)

Stage 1: Remove any other disk encryption products & check whether FileVault is already enabled

1. If you have any another encryption product (e.g. TrueCrypt) installed on your Mac then you **must** remove it by following the suppliers instructions before attempting to install and use Sophos Disk Encryption.

2. Check whether FileVault 2 is already enabled by looking in System Preferences –> Security & Privacy –> FileVault. If it is already enabled you should have a copy of the recovery key that was set when it was enabled to hand as it will be needed later. *(If you do not have the key you should turn FileVault*

off, wait for the Mac to be un-encrypted and then run this installation. This will generate a new key that will be stored in the SafeGuard management console for recovery use if required).

If FileVault is not already enabled leave it switched off. The installation process below will do everything that is necessary to enable disk encryption.

Stage 2: Configure the Mac and Install the Sophos Disk Encryption client

This installation will:
• join the Mac to Active Directory and apply a disk encryption policy.
• add two certificates to the System Keychain to enable secure communications with the encryption service.
• install the Sophos Disk Encryption client and configure it for the encryption service.

These steps are accomplished by running a command line shell script and we strongly recommend that this installation is carried out by a suitably experienced person. Please request assistance from your local IT support staff if you do not feel confident enough to proceed.

1. Copy the "Sophos Encryption Installer" folder to the Desktop on your Mac.

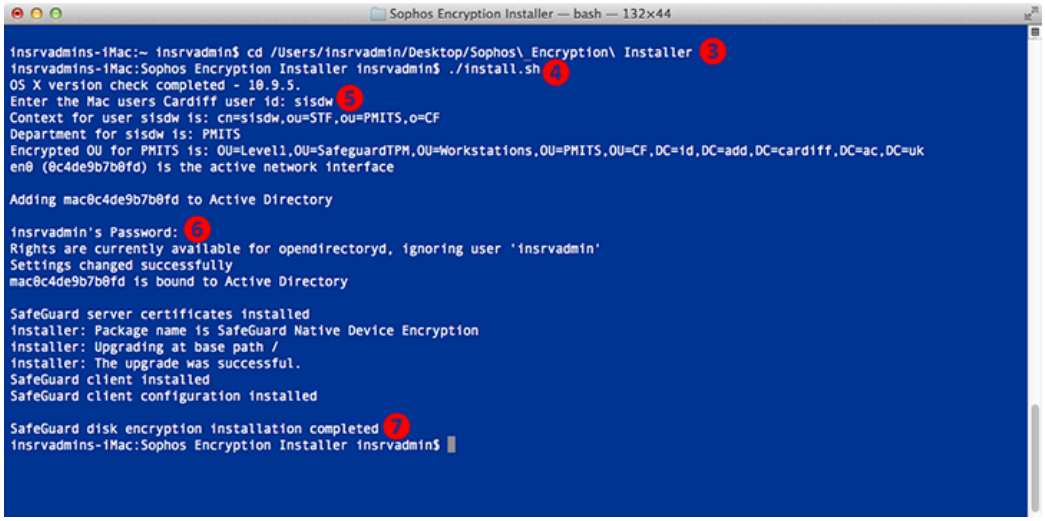
2. Open the folder and double-click on the "CU Password Policy.mobileconfig" file to install the configuration profile.
   (This profile sets the University's standard password complexity rules to ensure that user accounts do not have passwords that are blank or too simple to be secure.)

   Change the password for the local user account that has administrative privileges – normally the main user account.
   (Password changes can be done in the System Preferences – Users & Groups panel).

3. Open the Terminal application that's located in the main /Applications/Utilities/ folder.

4. At the Terminal $ prompt type "cd " (c + d + space) and then drag the "Sophos Encryption Installer" folder from the Desktop and drop in on the Terminal window to add the folder path to the command and press Return/Enter. (❸ below)

5. Type "./install.sh" (full stop + forward slash + install.sh) and press Return/Enter. (❹ below)



6. When prompted supply the user id of the main user of the Mac. (❺ above)
   (This will be used to determine which school/division the Mac belongs to and where in Active Directory the related computer account will be created).

7. When prompted supply the password for the local administrator account on the Mac. (❻ above)
   (You may get a second prompt for the local admin password at this stage)

8. The installation and configuration will now proceed to completion. (❼ above)

9. When completed the SafeGuard system preferences panel will open. You can check the status of the client and whether the Mac has picked up and applied the default encryption policy by checking the Server and Disk Encryption tabs.



10. The client should recognise the default encryption policy within 6 hours at which time you will be prompted for a password to use to encrypt the disk. You

can use the same password as your local Mac account if you wish as long as it is not too simple to guess.

You will be prompted for this password each time the Mac is rebooted (powered off and back on). **You will not be able to start up the Mac without the password.**

11. Once you have supplied a password encryption will begin and will continue in the background until the whole disk is encrypted. You can work on the Mac as normal and put it to sleep etc. without affecting the process.

    The installation is now completed.

Enrolling a Mac that already had FileVault 2 enabled:

If your Mac already had FileVault enabled you must supply the recovery key to the SafeGuard server so that it is available for future use if required.

If you do not complete this step IT Services will not be able to help you recover stored data if local account passwords are lost or forgotten.

After installing SafeGuard Disk Encryption do the following:

1. Open /Applications/Utilities/Terminal
2. At the Terminal prompt type: `sudo sgdeadmin --import-recoverykey AAAA-BBBB-CCCC-DDDD-EEEE-FFFF`

   Where `"AAAA-BBBB-CCCC-DDDD-EEEE-FFFF"` is the recovery key originally set when FileVault was enabled.
   (You should have kept a record of this recovery key for use if the local account password is forgotten or unavailable for any reason.)

Accessing the SafeGuard recovery key if a local account password is lost or forgotten:

If you need access to the recovery key please log a call with the Service Desk (contact details below). The call should include full details of the Mac (serial number and ethernet & Airport hardware addresses) and its main user.

Uninstalling Sophos Native Disk Encryption:

If you stop using your Mac for business purposes and want to remove the encryption service and un-encrypt the hard disk you need to do the following.
Please note that removing the service will identify the Mac as being un-compliant with University information management policies in the service management console.

1. Run the uninstaller package: /Library/Sophos SafeGuard DE/Sophos SafeGuard DE Uninstaller.pkg
2. Unbind the Mac from Active Directory by going into System Preferences –> Users & Groups –> Login Options and editing the Network Account Server settings to remove the "ID" domain.
   (*LCRs and other support staff will need an appropriately privileged AD domain account to complete this step*)
3. Un-encrypt the disk by opening System Preferences –> Security & Privacy –> FileVault and turning FileVault off.
   (It will take some time to un-encrypt the whole disk).

Reporting problems:

If you have any problems accessing or using this software service please contact the IT Services Service Desk by phone on extension **74487** or by email to **IT-Servicedesk@cardiff.ac.uk**

